ISBN 0-315-55645-5

The University of Alberta

# On Carmichael Type Problems for the Schemmel Totients and Some Related Questions

by

Lee-Wah Yip

A thesis
submitted to the Faculty of Graduate Studies and Research
in partial fulfillment of the requirements for the degree
of Doctor of Philosophy

Department of Mathematics

Edmonton, Alberta
Fall 1989

# THE UNIVERSITY OF ALBERTA

## *RELEASE FORM*

NAME OF AUTHOR: Lee-Wah Yip

TITLE OF THESIS: On Carmichael Type Problems for the Schemmel Totients and Some Related Questions

DEGREE: Doctor of Philosophy

YEAR THIS DEGREE GRANTED: 1989



(Signed) ..........................................

Permanent Address:
#418-430, Hennessy Road,
6/F, Flat #2,
Wanchai,
Hong Kong.

Date: ..........................................

THE UNIVERSITY OF ALBERTA

FACULTY OF GRADUATE STUDIES AND RESEARCH

The undersigned certify that they have read, and recommend to the Faculty of Graduate Studies and Research, for acceptance, a thesis entitled **On Carmichael Type Problems for the Schemmel Totients and Some Related Questions** submitted by **Lee-Wah Yip** in partial fulfillment of the requirements for the degree of Doctor of Philosophy.

..................................................
(Supervisor)

..................................................

..................................................

..................................................

..................................................

..................................................

Date: ..................................

*To my parents:*

Yip Pik-Kwong
Lo Lee-Hong

# Abstract

Let $N(m)$ denote the number of solutions of $\varphi(x) = m$, where $\varphi$ is the Euler totient. A deep conjecture of R.D. Carmichael states that $N(m)$ never takes the value 1. Besides Carmichael, several later authors provided some theoretical and numerical evidence in support of this conjecture.

We here consider an analogous problem in a more general setting provided by Schemmel's totient $\Phi_k$, which is a multiplicative function such that for primes $p$, $\Phi_k(p^a) = 0$ or $p^{a-1}(p-k)$ according as $p \leq k$ or $p > k$. Let $N_k(m)$ denote the number of solutions of $\Phi_k(x) = m$. It is found that the analogue of Carmichael's conjecture fails for the functions $\Phi_k$ and $N_k$ for any odd $k > 1$ and for some even values of $k$. This Carmichael type conjecture may hold for some other even values of $k$. For example, we conjecture that $N_2(m) \neq 1$ for any $m$. In support of this conjecture, we show that if $N_2(\Phi_2(x)) = 1$, then $x > 10^{120000}$. Many other related results and conjectures are contained in Chapter 2.

The main results of Chapter 3 include the following: a) the normal num-

ber of prime factors of $p-k(\leq x)$ is $\log\log x$; b) if $V_k(x)$ denotes the number of natural numbers not exceeding $x$ which are values of $\Phi_k$, then we have $V_k(x) = O(\pi(x)\exp(c\sqrt{\log\log x}))(x \to \infty)$ for any constant $c > \sqrt{8/\log 2}$; c) we apply the Brun-Titchmarsh theorem and Bombieri's theorem to show that $N_k(m) > m^{0.55}$ for infinitely many $m$.

Chapter 4 is devoted to the unitary totient $\varphi^*$, which is a multiplicative function with $\varphi^*(p^a) = p^a - 1$ for any prime $p$. We discuss the equation $\varphi^*(x) = m$ for two special types of $m$, namely i) $m = 2^n$, ii) $m = 4(2^p - 1)$, where $p \neq 5$, $p \equiv 1(\text{mod}4)$ and $2^p - 1$ is a prime. Case ii) provides a non-trivial example for which the unitary analogue of the Carmichael conjecture fails. This is connected to the complete solution of the diophantine equation $2^x - 5^y = 3$, and therefore a detailed discussion of this equation is included. We also show that for almost all $n$, the equation $\varphi^*(x) = n$ has no solution.

# Acknowledgements

I would like to express my heart-felt thanks to my supervisor Prof. M.V. Subbarao for his help and encouragement throughout the preparation of this thesis. The professional assistance of our computer analyst W.G. Aiello is greatly appreciated. Thanks are also due to Mr. Gordon Fong for generously taking on the laborious task of typing the entire manuscript, to Mr. Anthony Ng for his helpfulness in finishing the final version. Finally, I would like to thank the supervisory committee members for their valuable suggestions.

# Table Of Contents

# Chapter 1

# Introduction and preliminaries.

As usual, let $\varphi(n)$ denote the Euler totient (which represents the number of natural numbers $\leq n$ that are relatively prime to $n$). We write $N(m)$ for the number of solutions of $\varphi(x) = m$. The behaviour of the function $N(m)$ is very erratic. For instance, $N(1438) = 2$, $N(1440) = 72$ while $N(1442) = N(1444) = 0$. One of the oldest conjectures about $N(m)$ is the following:

1.1 **Conjecture** (Carmichael). $N(m) \neq 1$ for any $m$.

This assertion first appeared as a proposition in a 1906 paper by Carmichael. Eight years later it was an exercise in his number theory book [Car14]. Eight years after that an error in the 1906 proof was discovered and the statement became a conjecture [Car22].

Several authors worked on the Carmichael conjecture, especially, in trying to find a counter-example to it. These include V.L. Klee ([Kle47, Kle69]), H. Donnelly [Don73], E. Grosswald [Gro73], C. Pomerance [Pom74], A. Schinzel [Sch61], P. Erdős [Erd58], P. Masai and A. Valette [Mas82], besides of course Carmichael himself.

Most of these authors tried to find a lower bound for a counter-example to the Carmichael conjecture by examining the structure of the integer $x$ for which $N(\varphi(x)) = 1$. Klee [Kle47] showed that such an integer $x$ must be greater than $10^{400}$. The best lower bound so far known is $\varphi(x) > 10^{10000}$ due to P. Masai and A. Valette [Mas82]. The technique used to get a lower bound for the counter-example $x$ is to find more prime factors of $x$ if we already know some, and is based on the ideas of Carmichael and Klee in their papers and may be summarized in the following theorem.

1.2 **Theorem** (Carmichael-Klee). Let $x = \prod_A p_i^{a_i}$ ($A$ being the range of $i$) be the intended counter-example $x$ to the Carmichael conjecture. Find a prime $p$ such that $p - 1 = \prod_B p_i^{a_i - 1}(p_i - 1)\prod_C p_i^{c_i}$, where $B$ and $C$ are disjoint, possibly empty, subsets of $A$, such that $c_i \leq a_i - 1$ for $i$ in $C$. Then $p \mid x$. Further, if $B$ is such that for any $j$ in $B$ any prime divisor of $p_j - 1$ also divides $x$, then $p^2 \mid x$. In particular, this is true when $B$ is empty.

The proof is simple and is found in [Mas82].

Sierpinski conjectured that for every integer $n > 1$, there exist infinitely many $m$ such that $N(m) = n$. In 1958, Erdös [Erd58] showed that if there is one such $m$, then there are infinitely many. This is true even for $n = 1$, so that if the Carmichael conjecture fails for one $m$, then it fails for infinitely many $m$. A. Schinzel [Sch61] showed that Sierpinski's conjecture follows from his hypothesis H, which is quoted below. However, we do not know if hypothesis H is useful in settling the Carmichael conjecture.

1.3 **Hypothesis H.** Let $s$ be a natural number. Let $f_1(x), \ldots, f_s(x)$ be irreducible polynomials with integral coefficients, and for each polynomial the leading coefficient is positive, and there is no integer $d > 1$ that is a divisor of each of the numbers $P(x) = f_1(x) \cdot f_2(x) \cdots f_s(x), x$ being an integer. Then there exist infinitely many natural values of $x$ for which the numbers $f_1(x), f_2(x), \ldots, f_s(x)$ are all primes.

In fact, Schinzel [Sch61] gave an equivalent statement of his hypothesis which looks stronger than the one stated above. This apparently stronger proposition shall be referred to as the Hypothesis H as well, and is quoted below for future use.

1.4 **Hypothesis H.** Let $f_1(x), f_2(x), \ldots, f_s(x), g_1(x), \ldots, g_t(x)$ be irreducible integer-valued polynomials of positive degree with positive leading coefficients. If there does not exist any integer $> 1$ dividing the product $f_1(x) \cdot f_2(x) \cdots f_s(x)$ for every $x$, and if $g_j(x) \not\equiv f_i(x)$ for all $i \leq s$, $j \leq t$, then there exist infinitely many positive integers $x$ such that the numbers $f_1(x)$, $f_2(x), \ldots, f_s(x)$ are primes and the numbers $g_1(x), g_2(x), \ldots, g_t(x)$ are composite.

Instead of working on numerical estimates for $x$ for which $N(\varphi(x)) = 1$, Pomerance [Pom74] gave an interesting and elegant sufficient condition for such an $x$ to exist, as follows.

1.5 **Theorem** (Pomerance). Suppose $x$ is a natural number such that for every prime $p$, $(p-1) \mid \varphi(x)$ implies $p^2 \mid x$. Then $N(\varphi(x)) = 1$.

However, no such $x$ is likely to exist. He showed that such an $x$ does not indeed exist if the following conjecture of his holds:

1.6 **Conjecture** (Pomerance). If $p_i$ denotes the $i$-th prime, then for $n \geq 2$,

$$(p_n - 1) \mid \prod_{i=1}^{n-1} p_i(p_i - 1).$$

This conjecture is very likely to be true, but it is not likely to be settled in the near future. As Pomerance noted, his conjecture fails if there is a prime $q$ such that the smallest prime which is $\equiv 1 \pmod{q}$ is also $\equiv 1 \pmod{q^2}$. However, there is no such prime $q$ if Schinzel's hypothesis $\mathrm{H}_2$ ([Sch58], p. 207) is true. It is quoted below for convenience.

1.7 **Hypothesis $\mathrm{H}_2$**. If for a natural number $n > 1$, the numbers 1, 2,

$3, \ldots, n^2$ are arranged in ascending order in $n$ rows, $n$ numbers in each row, then if $(m,n) = 1$, the $m$-th column contains at least one prime number.

There are infinitely many $m$, such as $m = 2 \cdot 7^a$ with $a > 0$, for which $N(m) = 0$. One can therefore ask: how many natural numbers $m \le x$ are there for which $N(m) > 0$. Let $V(x)$ denote this number. In 1929, S.S. Pillai initiated the study of the function $V(x)$; he showed [Pil29] that

$$V(x) = O(x/(\log x)^{(\log 2)/e}).$$

In 1935, Erdös [Erd35] improved this to

$$V(x) = O(x/(\log x)^{1-\epsilon})$$

for every positive $\epsilon$. Starting from the 1970's, Erdös, R.R. Hall, C. Pomerance and H. Maier ([Erd73, Erd76, Pom86, Mai88]) made further improvements on the upper bound as well as the lower bound estimates for $V(x)$. The best result of this kind is obtained by Maier and Pomerance [Mai88], wherein it is proved that

$$V(x) = \frac{x}{\log x} \exp((c + o(1))(\log\log\log x)^2)$$

for a certain explicit constant $c$ $(= 0.81781465\ldots)$.

We next ask for the upper and lower bounds for $N(m)$.

Pomerance [Pom80] gave what he believes is the best possible upper bound, namely

$$N(m) \leq m \exp(-(1+o(1)) \log m \log\log\log m / \log\log m).$$

He has a heuristic argument that the above result is best possible in that there are infinitely many $m$ for which equality holds.

Regarding the lower bound for $N(m)$, the first result is due to S.S. Pillai [Pil29], who showed that there are infinitely many integers $m$ for which

$$N(m) \gg (\log m)^{(\log 2)/e}.$$

By using Brun's method, Erdös [Erd35] improved this by showing the existence of a constant $c > 0$ such that

$$N(m) > m^c \text{ for infinitely many } m. \tag{1.8}$$

What is the least upper bound $C$ for the values of $c$ for which (1.8) holds? Erdös [Erd56] conjectured that $C = 1$, and this is still open. Recently there is a succession of improvements to the value of $c$ in (1.8). In 1979, K.R. Wooldridge [Woo79] used Selberg's upper bound sieve to show that

$$C \geq 3 - 2\sqrt{2} = 0.17157\ldots$$

Pomerance [Pom80] used the new improvements on the Brun-Titchmarsh theorem due to H. Iwaniec [Iwa80] (it is too long and complicated to quote his results here) together with Bombieri's theorem (see section 3 of Chapter 3) to show that

$$C > 0.55655.$$

There is still a wide gap between this result and Erdös' conjecture that $C = 1$.

In 1869, Schemmel (see [Dic71], p. 147) introduced a generalization of $\varphi$, which will be denoted by $\Phi_k$ ($k$ being a fixed natural number). It is a multiplicative function, with $\Phi_k(1) = 1$, and for primes $p, \Phi_k(p^a) = 0$ or $p^{a-1}(p-k)$ according as $p \leq k$ or $p > k$. $\Phi_k(n)$ can be interpreted as the number of sets of $k$ consecutive natural numbers not exceeding $n$ each of which is relatively prime to $n$. Let $N_k(m)$ denote the number of solutions of $\Phi_k(x) = m$. This is well-defined, i.e. $N_k(m)$ is always a finite number; we will justify this in the next chapter.

We will see in the next two chapters that the above results and conjectures have their analogues for the functions $\Phi_k$ and $N_k$. This forms the main subject of investigation of this thesis, such detailed investigation does not seem to have been carried out so far. However, there is a joint paper by Subbarao and Yip [Sub87], which can be considered as part of this thesis. Besides this, there is nothing in the existing literature on this problem.

Chapter 4 is devoted to the unitary totient $\varphi^*$, which is a multiplicative function with $\varphi^*(p^a) = p^a - 1$ for any prime $p$ (and $a > 0$). $\varphi^*(n)$ gives the number of natural numbers not exceeding $n$ and unitarily prime to $n$. (An integer $m$ is said to be unitarily prime to $n$ if the largest divisor of $m$ which is a unitary divisor of $n$ is unity — a unitary divisor of $n$ being defined as a divisor $d$ of $n$ which is relatively prime to $n/d$.)

The last chapter contains some concluding remarks and open problems.

We conclude this chapter with a few words on the notation that we would use throughout this thesis. (The following list is not intended to be complete though, since some notations are now so well-understood in mathematics that no further explanation in this thesis is needed.)

$\mathbb{N}$ denotes the set of all natural numbers.

$\wp$ denotes the set of all primes.

For a set $A$ (usually a subet of $\mathbb{N}$), $|A|$ denotes the cardinality of $A$.

$p, p_1, p_2, \ldots, q, q_1, q_2, \ldots$ always denote primes.

$p^a \parallel n$ means that $p^a \mid n$ but $p^{a+1} \nmid n$.

For each $n \in \mathbb{N}$, we write $\omega(n)$ for the number of distinct prime factors of $n$, $\Omega(n)$ for the number of prime factors of $n$ counted according to multiplicity, $d(n)$ for the number of positive divisors of $n$, and $P(n)$ for the largest prime factor of $n$ if $n > 1$ (we define $P(1) = 1$).

For integers $a, b, (a, b)$ denotes the greatest common divisor of $a$ and $b$.

For a real number $x$, $[x]$ denotes the greatest integer $\leq x$.

For a real number $x$, $a \in \mathbb{N}$ and an integer $b$ with $(a, b) = 1$, we write $\pi(x; a, b) = |\{p \in \wp \cap (0, x] : p \equiv b \pmod{a}\}|$; and as usual, we write $\pi(x)$ for $\pi(x; 1, 0)$.

For real numbers $x$, $y \geq 1$, and $k \in \mathbb{N}$, we write

$$\Psi(x, y) = | \{n \in \mathbb{N} : n \leq x \text{ and } P(n) \leq y\} |,$$

and

$$\Pi_k(x,y) = |\{p \in \wp \cap (k,x] : P(p-k) \le y\}|,$$

provided that in the latter case $x > k$.

We would adopt the $O$- and $o$- notations of Landau as well as the $\ll$- (or $\gg$-) notation of Vinogradov. The constants implied by the $O$- or $\ll$-notation would be absolute, unless otherwise stated.

Finally, $c, c_0, c_1, \ldots$ stand for positive absolute constants, not necessarily the same at each occurrence, and, for example, $C(\epsilon, k)$ stands for positive constant depending only on the parameters $\epsilon$ and $k$.

# Chapter 2

# The functions $\Phi_k$ and $N_k$.

## § 2.1 The basic property of $N_k$.

Recall that $\Phi_k$ is a multiplicative function with $\Phi_k(1) = 1$, and for arbitrary $p \in \wp, a \in \mathbb{N}$,

$$\Phi_k(p^a) = \begin{cases} 0 & \text{if} \quad p \leq k, \\ p^{a-1}(p-k) & \text{if} \quad p > k; \end{cases}$$

and that $N_k(m)$ denotes the number of solutions of $\Phi_k(x) = m$ ($m \in \mathbb{N}$), where $k$ is an arbitrary but fixed natural number.

We claim that $N_k(m)$ is well-defined, i.e. the equation $\Phi_k(x) = m$ can have only finitely many (possibly 0) solutions for any $m \in \mathbb{N}$. First of all, we need a non-trivial lower bound estimate for $\Phi_k(n)/n$ whenever $\Phi_k(n) > 0$. For this purpose, we introduce the set $\mathcal{U}_k = \{n \in \mathbb{N} : p \mid n \Rightarrow p > k\}$. Note that $1 \in \mathcal{U}_k$, and $\Phi_k(n) > 0$ if and only if $n \in \mathcal{U}_k$. We have

**2.1.1 Theorem.** There exist positive constants $c_1(k), c_2(k)$ which depend on $k$ only such that

$$\frac{\Phi_k(n)}{n} \geq \frac{c_1(k)}{(\log\log 3n)^k}, \tag{2.1.2}$$

$$n \leq c_2(k)\Phi_k(n)(\log\log(3\Phi_k(n)))^k, \tag{2.1.3}$$

for all $n \in \mathcal{U}_k$.

*Proof.* It should be pointed out that (2.1.3) is an easy consequence of (2.1.2), and that it suffices to prove (2.1.2) for sufficiently large $n \in \mathcal{U}_k$.

By considering $\log(\prod_{k<p\leq x}(1-\frac{k}{p}))$ and by making use of the standard fact that $\sum_{p\leq x}\frac{1}{p} = \log\log x + c + O(\frac{1}{\log x})$ ( $c$ being some absolute constant) (see, for example, [Apo76] Theorem 4.12), it is not difficult to obtain

$$\prod_{k<p\leq x}(1-\frac{k}{p}) = \frac{A_k}{(\log x)^k}(1+O(\frac{1}{\log x})), \tag{2.1.4}$$

where $A_k$ is a constant depending on $k$ only and the constant implied by the $O$-notation depends also on $k$.

Now let $n \in \mathcal{U}_k$ be large. We have

$$\frac{\Phi_k(n)}{n} = \prod_{p|n}(1-\frac{k}{p}) = \prod_{\substack{p|n \\ p\leq\log n}}(1-\frac{k}{p})\prod_{\substack{p|n \\ p>\log n}}(1-\frac{k}{p}). \tag{2.1.5}$$

By (2.1.4), the first product $\geq (1+o(1))A_k/(\log\log n)^k$. Suppose that there are $r$ factors in the second product. Then $n > (\log n)^r$, that is, $r <$

$\log n / \log\log n$, and so

$$\prod_{\substack{p|n \\ p>\log n}} (1 - \frac{k}{p}) > (1 - \frac{k}{\log n})^r > (1 - \frac{k}{\log n})^{\frac{\log n}{\log\log n}}.$$

It is easy to show that the function $(1 - k/x)^{x/\log x}$ defined for $x > k$ is strictly increasing on $(k, \infty)$ and is approaching 1 as $x \to \infty$. It follows from (2.1.5) that

$$\frac{\Phi_k(n)}{n} \geq \frac{(1 + o(1))A_k}{(\log\log n)^k}.$$

This completes the proof.

As a corollary, we get

2.1.6 **Theorem.** For all $m \in \mathbb{N}, N_k(m) \leq c_2(k)m(\log\log 3m)^k$, where $c_2(k)$ is the same constant as in (2.1.3).

*Proof.* Let $m \in \mathbb{N}$ be given. Consider the equation $\Phi_k(x) = m$.

Suppose that this equation has at least one solution (otherwise $N_k(m) = 0$), say $x_0$. Then $\Phi_k(x_o) = m > 0$, and hence by (2.1.3), $x_0 \leq c_2(k) \cdot m(\log\log 3m)^k$. This means that the equation can have only finitely many solutions, and that $N_k(m) \leq c_2(k)m(\log\log 3m)^k$.

We will give a discussion on the lower bound estimate of $N_k(m)$ in the next chapter.

## § 2.2 The case $k = 2$.

Let

(2.2.1) $$q_1, q_2, q_3, q_4, \ldots$$

be a sequence of primes defined inductively by

(2.2.2) $q_1 = 3$, and for $n \geq 1$, $q_{n+1}$ is the smallest prime $> q_n$ for which

$$(q_{n+1} - 2) \mid (q_1 q_2 \cdots q_n).$$

The first few terms of the sequence (2.2.1) of primes are

3, 5, 7, 17, 19, 23, 37, 53, 59, 61, 71, 73, 97, 107, 109, 113, 163, ....

In fact the first 10000 terms of this sequence are calculated. We have

$$q_{10000} = 4873801,$$

this being the 340256-th prime in the sequence of all primes 2,3,5,7,11,.... A complete list of the first 1000 terms of the sequence can be found in Appendix I. (The complete list of the first 10000 terms is available upon request.)

We make the following

2.2.3 **Conjecture** . The sequence $\{q_n\}_{n\geq 1}$ defined by (2.2.2) is infinite.

As P. Erdös mentioned in a letter to us, this conjecture is undoubtedly true, but a proof of this is beyond the present resources of number theory.

2.2.4 **Remark**. The corresponding sequence of primes in the case of $\varphi$ would be

$$r_1, r_2, r_3, r_4, \ldots,$$

where $r_1 = 2$, and $r_{n+1}$ is the smallest prime $> r_n$ for which $(r_{n+1} - 1) \mid (r_1 r_2 \cdots r_n)(n \geq 1)$. However this sequence has only four terms: $2, 3 = 2 + 1, 7 = 2 \cdot 3 + 1$ and $43 = 2 \cdot 3 \cdot 7 + 1$. Note that the possible candidates for the next term are $87 = 2 \cdot 43 + 1, 259 = 2 \cdot 3 \cdot 43 + 1$, $603 = 2 \cdot 7 \cdot 43 + 1$ and $1807 = 2 \cdot 3 \cdot 7 \cdot 43 + 1$, and all these are composite.

We next make the following

2.2.5 **Conjecture**. There is no integer $m$ for which $N_2(m) = 1$.

Equivalently, this conjecture says that the equation $\Phi_2(x) = m$, for any given $m$, has either no solution or at least two solutions. For example, $N_2(15) = 7$, $N_2(51) = N_2(87) = 5$, $N_2(22499) = N_2(35) = N_2(9) = 4$, $N_2(321) = N_2(123) = N_2(33) = N_2(3) = 3$, $N_2(209) = N_2(161) = N_2(57) = N_2(55) = N_2(11) = N_2(5) = 2$, $N_2(91) = N_2(7) = N_2(m) = 0$ for any even $m \in \mathbb{N}$.

This is analogous to the Carmichael conjecture (1.1). In attempting to prove or disprove this conjecture, the importance of the sequence (2.2.1) arises, as shown in the following:

2.2.6 **Theorem**. If there is a natural number $x$ for which $N_2(\Phi_2(x)) = 1$, then $q_n^2 \mid x$ for each $n$.

This is just a special case of a more general theorem, namely, Theorem 2.4.7, where the details of proof are given.

Now in view of Theorem 2.2.6 we can see that Conjecture 2.2.3 implies Conjecture 2.2.5, because Theorem 2.2.6 and Conjecture 2.2.3 imply that there is no finite integer $m$ for which $N_2(m) = 1$.

In support of Conjecture 2.2.5, we have

2.2.7 **Theorem.** If $N_2(\Phi_2(x)) = 1$, then $x > 10^{120000}$.

*Proof.* By taking the first 10000 terms of the sequence (2.2.1), we get $(q_1 q_2 \cdots q_{10000})^2 \mid x$. Our conclusion follows from the fact that

$$\log_{10}(q_1 q_2 \cdots q_{10000}) = 60341.9\ldots.$$

Analogous to the Pomerance's results for the Carmichael conjecture stated in the introductory chapter, we have the following theorem which gives a sufficient condition for Conjecture 2.2.5 to hold.

2.2.8 **Theorem.** If there is a natural number $x$ such that for every odd prime $p$, $(p-2) \mid \Phi_2(x)$ implies $p^2 \mid x$, then $N_2(\Phi_2(x)) = 1$.

*Proof.* For every $n \in \mathbb{N}$, denote by $S(n)$ the set of primes dividing $n$. For every prime $p$, denote by $\nu_p(n)$ the exponent (possibly 0) on $p$ in the prime factorization of $n$. Then for odd $n$ and odd prime $p$,

$$\nu_p(\Phi_2(n)) = \begin{cases} \sum_{q \in S(n)} \nu_p(q-2), & \text{if } p \nmid n; \\ \nu_p(n) - 1 + \sum_{q \in S(n)} \nu_p(q-2), & \text{if } p \mid n. \end{cases}$$

Suppose that $x$ satisfies the condition in the theorem, and let $y$ be such that $\Phi_2(y) = \Phi_2(x)$. If $p \in S(y)$, then $(p-2) \mid \Phi_2(y) = \Phi_2(x)$, so by assumption, $p \in S(x)$. That is, $S(y) \subset S(x)$. Now let $p \in S(x)$. Then $(p-2) \mid \Phi_2(x)$, so $p^2 \mid x$. If $p \notin S(y)$, then

$$\begin{aligned} \nu_p(x) - 1 + \sum_{q \in S(x)} \nu_p(q-2) &= \nu_p(\Phi_2(x)) = \nu_p(\Phi_2(y)) \\ &= \sum_{q \in S(y)} \nu_p(q-2) \leq \sum_{q \in S(x)} \nu_p(q-2), \end{aligned}$$

contradicting $p^2 \mid x$. Hence $S(x) = S(y)$. Now if $p \in S(x) = S(y)$, then

$$\nu_p(x) = \nu_p(\Phi_2(x)) + 1 - \sum_{q \in S(x)} \nu_p(q-2) = \nu_p(\Phi_2(y)) + 1 - \sum_{q \in S(y)} \nu_p(q-2) = \nu_p(y).$$

This proves $x = y$, and hence establishes the theorem.

2.2.9 **Remark.** In the above proof, we follow exactly the same argument as given by Pomerance [Pom74]. We reproduce this argument here (but not just refer to [Pom74]) because it is not long and we want to make this thesis as self-contained as possible. There is no such integer $x$ described in the theorem if the following conjecture holds.

2.2.10 **Conjecture.** Let $p_i$ denote the $i$-th odd prime. Then for $n \geq 2$,

$$(p_n - 2) \mid \prod_{i=1}^{n-1} p_i(p_i - 2).$$

2.2.11 **Remark.** As Pomerance stated about his conjecture (1.6) in [Pom74], we wish to note that Conjecture 2.2.10 fails if there is a prime $p$ such that the smallest prime which is $\equiv 2 \pmod{p}$ is also $\equiv 2 \pmod{p^2}$. However, if Schinzel's hypothesis $H_2$ (1.7) holds, then there is no such $p$.

One might be tempted to make a more general conjecture, namely, that for the sequence of primes $p_1 = 2, p_2 = 3, \ldots,$

$$(p_{n+1} - k) \mid \prod_{\substack{i \le n \\ p_i > k}} p_i(p_i - k).$$

However, this can be false in general. For instance, it is false for $k = 3$ (take $p_{n+1} = 7$) and $k = 4$ (take $p_{n+1} = 7$).

## § 2.3 The case $k \geq 2$.

We first prove the following:

2.3.1 **Theorem.** For any odd integer $k > 1$, there are infinitely many integers $m$ for which $N_k(m) = 1$.

*Proof.* Take any odd prime $p > k$ which satisfies

$$p \equiv \begin{cases} 1 \pmod{4} \text{ if } k \equiv 3 \pmod{4}, \\ 3 \pmod{4} \text{ if } k \equiv 1 \pmod{4}, \end{cases}$$

as well as

$$p \equiv k + 1 \pmod{(2k+1)}.$$

We note that there are infinitely many such $p$, in view of $(k+1, 2k+1) = 1$ on utilizing Dirichlet's theorem for primes in an arithmetic progression and the Chinese remainder theorem.

Let $m = p^2 - kp$. Then the equation $\Phi_k(x) = m$ has at least one solution, viz. $x = p^2$. We claim that this is the only solution.

Suppose $x_o$ is a solution to $\Phi_k(x) = m = p(p-k)$.

By our choice of $p$, $2 \parallel p(p-k) = \Phi_k(x_o)$. Thus $x_o$ is divisible by only one prime, say $x_o = q^a$, $q$ being an odd prime. It remains to show that $q = p$ (note that this implies $a = 2$ immediately).

If $q \neq p$, then $p \mid (q-k)$, and so $q > p$. Furthermore, if $a \geq 2$, then

$$\Phi_k(\frac{x_o}{q}) = \Phi_k(x_o)/q = p(p-k)/q,$$

which implies $q \mid p(p-k)$, but this is impossible since $q > p > p-k$ and $q$ is a prime. Hence $a = 1$, and consequently $q - k = \Phi_k(x_o) = p(p-k)$, and this implies

$$q = p(p-k) + k \equiv 0 \pmod{2k+1}$$

by our choice of $p$. This is possible only if $q = 2k+1$. But then $k + 1 = q - k = p(p-k) \geq 2(k+1)$, a contradiction. Thus $q = p$, and the theorem is proved.

We may have $N_k(m) = 1$ for certain even values of $k$ also, as seen from the following

2.3.2 **Theorem.** Let $p, q$ be odd primes with $p > q, p \neq 2q - 1$ such that

(2.3.3) $p - q + 1$ is a prime,

(2.3.4) $2q - 1$ is composite,

(2.3.5) $q(p-q+1)+q-1$ is composite.

Then $N_{q-1}(q(p-q+1)) = 1$, the unique solution being $q^2p$.

*Proof*: Firstly, we assume all the given conditions except (2.3.4) and (2.3.5).

Under this assumption, consider the equation

$$\Phi_{q-1}(x) = q(p-q+1). \tag{2.3.6}$$

Let $x = p_1^{a_1}\cdots p_r^{a_r}$ be a solution of (2.3.6), where $q \le p_1 < p_2 < \cdots < p_r$ are primes, $a_i \ge 1, 1 \le i \le r, r \ge 1$. Suppose $p_1 > q$. Then $p_i - q + 1 \ge 3$ for all $i$, and $q \mid (p_j - q + 1)$ for some $1 \le j \le r$. Writing (2.3.6) in the form

$$p_1^{a_1-1}(p_1-q+1)\cdots p_j^{a_j-1}((p_j-q+1)/q)\cdots p_r^{a_r-1}(p_r-q+1)=p-q+1, \tag{2.3.7}$$

we see that $r \le 2$ (since the right-hand side is prime by (2.3.3)), i.e. we have i) $x = p_1^{a_1}$, or ii) $x = p_1^{a_1}p_2^{a_2}$.

i) The case $x = p_1^{a_1}$. Here (2.3.6) becomes $p_1^{a_1-1}(p_1-q+1) = q(p-q+1)$. Since the right-hand side of this last equality is square-free, we infer that $a_1 = 1$ or $2$. If $a_1 = 1$, then $p_1 - q + 1 = q(p-q+1)$, and $q(p-q+1)+q-1 = p_1$ is a prime, and so in this case $x = p_1^1 = q(p-q+1)+q-1$, provided (2.3.5) is not true. If $a_1 = 2$, then $p_1(p_1-q+1) = q(p-q+1)$, and since $p_1 > q$, we have $q \mid (p_1-q+1)$, and from $p_1((p_1-q+1)/q) = p-q+1$, we conclude that $(p_1-q+1)/q = 1$, i.e. $p_1 = 2q-1 = p-q+1$, and so $x = p_1^2 = (2q-1)^2$, provided $p = 3q-2$ and (2.3.4) is not true.

ii) The case $x = p_1^{a_1}p_2^{a_2}$. We may write (2.3.7) as

$$p_1^{a_1-1}p_2^{a_2-1}((p_1-q+1)(p_2-q+1)/q) = p-q+1.$$

Note that $(p_1 - q + 1)(p_2 - q + 1)/q \geq 3$. It follows that $a_1 = a_2 = 1$, and hence that $\{p_1 - q + 1, p_2 - q + 1\} = \{q, p - q + 1\}$. This implies that $2q - 1$ is prime and $x = (2q - 1)p$.

Next suppose that $p_1 = q$. Then (2.3.6) becomes

$$(2.3.8) \quad q^{a_1 - 1} p_2^{a_2 - 1}(p_2 - q + 1) \cdots p_r^{a_r - 1}(p_r - q + 1) = q(p - q + 1).$$

Similar to the above, we have $a_1 = 1$ or $2$ and $r \geq 2$. If $a_1 = 1$, from the above argument, we get

$$x = q(q(p - q + 1) + q - 1) \text{ provided (2.3.5) is not true,}$$

or $$x = q(2q - 1)^2 \text{ provided } p = 3q - 2 \text{ and (2.3.4) is not true,}$$

or $$x = qp(2q - 1) \text{ provided (2.3.4) is not true.}$$

If $a_1 = 2$, then it is easy to see from (2.3.8) that $r = 2$ and $x = q^2 p$.

Summing up, all the possible solutions of (2.3.6) are given by

$$\begin{cases} x = q(p - q + 1) + q - 1 & \text{or} \quad q(q(p - q + 1) + q - 1) \\ & \quad \text{provided (2.3.5) is false ,} \\ x = (2q - 1)^2 & \text{or} \quad q(2q - 1)^2 \\ & \quad \text{provided } p = 3q - 2 \text{ and (2.3.4) is false ,} \\ x = p(2q - 1) & \text{or} \quad qp(2q - 1) \\ & \quad \text{provided (2.3.4) is false ,} \\ x = q^2 p. & \end{cases}$$

Now it is clear that $x = q^2 p$ is the only solution under the given conditions of the theorem.

**2.3.9 Example.** The only solution of $\Phi_{46}(x) = 47 \cdot 7 = 329$ is $x = 47^2 \cdot 53$.

**2.3.10 Remark.** The case in which $p = 2q - 1$ will be considered in the last part of the next section.

We are now going to prove that for any given $k \geq 2$, there exist infinitely many non-trivial integers $m$ such that $N_k(m) = 0$ (it is trivial that $N_k(m) = 0$ whenever $k, m$ are of same parity). More precisely, we have

**2.3.11 Theorem.** Let $n \in \mathbb{N}$ be arbitrary, and let $d_1, d_2, \ldots, d_s$ be all the positive factors of $n$. Suppose $p$ is a prime such that $p \equiv 1 \pmod{(d_i + k)}$ for all $1 \leq i \leq s$. Then the equation $\Phi_k(x) = p^\ell n$ has no solutions for any $\ell > 0$.

(**Remark.** This theorem holds also for $k = 1$. This is due to A. Schinzel [Sch56a].)

*Proof.* We note that Dirichlet's theorem implies the existence of infinitely many such primes.

Suppose to the contrary that $x_o$ satisfies the equation $\Phi_k(x) = p^\ell n (\ell > 0)$.

If $p \mid x_o$, then $(p-k) \mid \Phi_k(x_o)$, i.e. $(p-k) \mid p^\ell n$, and so $(p-k) \mid n$, (since $(p-k, p) = 1$). This implies that $p - k \leq n$, or $p \leq n + k$, which is impossible since $p \equiv 1 \pmod{(n+k)}$.

Thus $(p, x_o) = 1$. Let $x_o = q_1^{\alpha_1} q_2^{\alpha_2} \cdots q_r^{\alpha_r}$ be the prime factorization of

$x_o$. We have

$$q_1^{\alpha_1-1}(q_1-k)\cdots q_r^{\alpha_r-1}(q_r-k)=p^\ell n.$$

Since $(p,x_o)=1$, there exists $1\le i_o\le r$ such that $p\mid(q_{i_o}-k)$, and so $q_{i_o}-k=p^m d_{j_o}$ for some $m\ge 1$ and $1\le j_o\le s$. It follows from the choice of $p$ that

$$q_{i_o}=p^m d_{j_o}+k\equiv 1\cdot d_{j_o}+k\equiv 0 \pmod{(d_{j_o}+k)}.$$

But $q_{i_o}=p^m d_{j_o}+k>d_{j_o}+k$ and $q_{i_o}$ is prime. This contradiction proves the theorem.

2.3.12 **Corollary**. For every $n\in\mathbb{N}$, there exist infinitely many multiples $m$ of $n$ such that the equation $\Phi_k(x)=m$ has no solutions.

2.3.13 **Examples**. a) The equation $\Phi_2(x)=7^\ell$ has no solutions unless $\ell=0$ (in which case $x=1$ or 3). b) The equation $\Phi_2(x)=3\cdot 31^\ell$ has no solutions unless $\ell=0$ (in which case $x=5$, 9 or 15).

Contrary to Theorem 2.3.11, we have the following result: "For any $n\in\mathbb{N}$, there exist infinitely many $m\in\mathbb{N}$ such that $N_k(m)>n$." The proof of this needs more sophisticated technique. We postpone it to section 3 of the next chapter. A simple proof of this in the case when $k=1$ can be found in [Sch56b].

## § 2.4 The case in which $k$ is a natural number of special type.

We start with the following:

**2.4.1 Theorem.** Let $k \geq 3$, $k+2 = p_o{}^{\alpha}$, where $p_o$ is an odd prime and $\alpha \in \mathbb{N}$. Then Hypothesis H implies that for any given integer $n > 1$, there exist infinitely many integers $m$ such that $\Phi_k(x) = m$ has exactly $n$ solutions (i.e. $N_k(m) = n$).

*Proof.* Let $q_o$ denote the smallest prime factor of $k+4$ (which is odd), and let $r = (p_o - 1)(q_o - 1)/2$. Observe that $r \geq (3-1)(5-1)/2 = 4$.

Set $A = \{a \in \mathbb{N} : (p_o - 1) \nmid a\} = \{a_1, a_2, a_3, \ldots\}$, where $1 = a_1 < a_2 < a_3 < \cdots$ (note that $a_i < 2i$ for all $i$ since $A$ contains all odd numbers).

For any given $n > 1$, consider the irreducible polynomials defined by

$$f_i(x) = 2x^{a_i} + k, f_{n+i}(x) = 2x^{rn-a_i} + k, i = 1, 2, \ldots, n; f_{2n+1}(x) = x.$$

The irreducibility of $2x^a + k$ follows from Eisenstein's criterion. Note that $(rn - a_n) - a_n = rn - 2a_n \geq 4n - 2a_n = 2(2n - a_n) > 0$, so that $f_{n+i}(x) (1 \leq i \leq n)$ is distinct from $f_1(x), \cdots, f_n(x)$.

We have $\prod_{i=1}^{2n+1} f_i(1) = (k+2)^{2n} = p_o{}^{2\alpha n}$. Let $g$ be a primitive root modulo $p_o$. Observe that $2g^a + k \equiv 0 \pmod{p_o}$ iff $2g^a - 2 \equiv 0 \pmod{p_o}$ iff $g^a \equiv 1 \pmod{p_o}$ iff $(p_o - 1) \mid a$. Since, by the definition of $A, (p_o - 1) \nmid a_i$ and $(p_o - 1) \nmid (rn - a_i)$ for all $1 \leq i \leq n$, we conclude that $p_o \nmid \prod_{i=1}^{2n+1} f_i(g)$. Therefore, the condition of Hypothesis H is satisfied.

Define $b_1 < b_2 < \cdots < b_{(r-2)n}$ in such a way that

$$\{b_1, b_2, \ldots, b_{(r-2)n}\} = \{1, 2, \ldots, rn\} \setminus \bigcup_{i=1}^{n} \{a_i, rn - a_i\},$$

and define

$$g_j(x) = 2x^{b_j} + k, j = 1, 2, \ldots, (r-2)n; g_{(r-2)n+1}(x) = 4x^{rn} + k.$$

By Hypothesis H (1.4), there exist infinitely many integers $x_o$ such that all the $f_i(x_o)(1 \le i \le 2n+1)$ are prime and all the $g_j(x_o)(1 \le j \le (r-2)n+1)$ are composite (in particular, $2x_o{}^{rn} + k$ and $4x_o{}^{rn} + k$ are composite).

Consider, for such an $x_o$ with $x_o > k+4$, the equation

$$\Phi_k(y) = 4x_o{}^{rn}. \tag{2.4.2}$$

If $y$ is a solution of (2.4.2), then obviously $y$ can have at most two distinct prime factors, i.e. $y$ is of the form $p^a$ or $p^a q^b$. If $a > 1$, then $p(p-k) \mid 4x_o{}^{rn}$, so $p = x_o$ and $(x_o - k) \mid 4x_o{}^{rn}$, which is impossible since $x_o > k+4$. Similarly we must have $b = 1$ in the latter case. If $y = p$, then $p - k = 4x_o{}^{rn}$, i.e. $p = 4x_o{}^{rn} + k$, which is impossible since $4x_o{}^{rn} + k$ is composite. Now we conclude that $y = pq$ for some distinct primes $p, q$, and we may write (2.4.2) as

$$\left(\frac{p-k}{2}\right)\left(\frac{q-k}{2}\right) = x_o{}^{rn}.$$

Both factors on the left-hand side are greater than 1, for if $(p-k)/2 = 1$ (say), then $(q-k)/2 = x_o{}^{rn}$, and so $q = 2x_o{}^{rn} + k$, contradicting the fact that $2x_o{}^{rn} + k$ is composite. It follows that $\{p, q\} = \{f_{i_o}(x_o), f_{n+i_o}(x_o)\}$ for some $1 \leq i_o \leq n$, i.e. $y = f_{i_o}(x_o) f_{n+i_o}(x_o)$.

Obviously, for any $i \in \{1, 2, \ldots, n\}$, $f_i(x_o) f_{n+i_o}(x)$ is a solution of (2.4.2). Thus (2.4.2) has exactly $n$ solutions.

2.4.3 **Remark**. In a certain sense, the above theorem is a generalization of Schinzel's work on the Sierpinski conjecture (see p.3 or [Sch61]). We would expect that this theorem holds for any odd $k$ (or even any $k \in \mathbb{N}$). But it seems to be extremely difficult to settle this problem.

In the rest of this section, our consideration is devoted to a special type of even numbers $k$, namely that $k + 1$ and $2k + 1$ are both primes. (The density of the set of all such $k$'s is zero, as we can easily see from the prime number theorem.)

It is easy to prove that if $k \geq 4$ and $k + 1, 2k + 1$ are prime, then $6 \mid k$ and $k \equiv 0, 6, \text{or}, 8 \pmod{10}$. For instance, all the $k$'s satisfying the above conditions with $4 \leq k \leq 100$ are 6, 18, 30, 36, 78, and 96.

Just like (2.2.1) we introduce the sequence

$$(2.4.4) \qquad q_{k,1},\ q_{k,2},\ q_{k,3}, \cdots,$$

which is defined by

$$q_{k,1} = k + 1,\ q_{k,2} = 2k + 1, \text{and}$$

(2.4.5) $$q_{k,n+1} = \text{ smallest prime } > q_{k,n} \text{ such that}$$

$$(q_{k,n+1} - k) \mid (q_{k,1}, \ldots, q_{k,n}) \text{ for } n \geq 2.$$

Furthermore, we define $\ell_k = |\{q_{k,n}\}_{n\geq 1}|$.

The number $\ell_k$ could be finite, for example

$$\ell_k = 2 \text{ for } k = 18, 30, 78, 96, 138, 228, 438, 498;$$

$$\ell_k = 3 \text{ for } k = 156, 270, 366, 726, 828, 936;$$

$$\ell_k = 4 \text{ for } k = 378, 600, 618, 810.$$

With the help of a computer, the sequences $\{q_{k,n}\}_{n\geq 1}$ for $2 < k \leq 1000$ are examined. Within this interval, there are 33 values of $k$ for which $k + 1$ and $2k + 1$ are both prime, and that $\ell_k = 2$ for 15 values of $k$, $\ell_k = 3$ for 6 values, $\ell_k = 4$ for 4 values, $\ell_k = 5$ only for $k = 576$, $\ell_k = 6$ only for $k = 336$, and $\ell_k \geq 8$ for all the remaining values of $k$. For more details, see Appendices II and III.

From the above data, it is natural to make the following:

2.4.6 **Conjecture**. For any given integer $m \geq 2$, there exist infinitely many integers $k$ for which $\ell_k = m$.

In fact, this conjecture follows from Hypothesis H. The proof goes as follows. In Hypothesis H (1.4), take $s = m, t = 2^m - m$. Let $f_i(x) = ix + 1, 1 \leq i \leq s$. Clearly, these $f_i$'s satisfy the condition of the hypothesis. We define the polynomials $g_1(x), g_2(x), \ldots, g_t(x)$ in the following manner. Let $g_1(x) = (m+1)x + 1$ and let $\mathcal{A}$ denote the family of all subsets of $\{1, 2, \ldots, m\}$ each of which contains at least two elements. Then $|\mathcal{A}| = 2^m - m - 1 = t - 1$. Write $\mathcal{A} = \{A_1, A_2, \ldots, A_{t-1}\}$ (in any arbitrary but fixed order). For $2 \leq j \leq t$, define $g_j(x) = x + \prod_{a \in A_{j-1}} f_a(x)$. Note that except for the irreducibility, the polynomials $g_j(x)(1 \leq j \leq t)$ also satisfy the condition of the hypothesis. But we should point out that in (1.4), the irreducibilities of the polynomials $g_1(x), g_2(x), \ldots, g_t(x)$ are not essential, that is, the conclusion of the hypothesis still holds even if these polynomials are reducible. Thus there exist infinitely many $x \in \mathbb{N}$ such that $f_1(x), f_2(x), \ldots, f_s(x)$ are prime and $g_1(x), g_2(x), \ldots, g_t(x)$ are composite. Let $k$ be any such natural number. It follows immediately from the definition of $\{q_{k,n}\}_{n\geq 1}$ (see (2.4.5)) that $q_{k,n} = f_n(k)$ for $n = 1, 2, \ldots, m$. The possible candidate for the next term $q_{k,m+1}$ (if it exists) is $g_1(k) = q_{k,m} + k$ or of the form $q_{k,i_1} \cdots q_{k,i_r} + k = f_{i_1}(k) \cdots f_{i_r}(k) + k = g_j(k)$ for some $2 \leq j \leq t$, where $1 \leq i_1 < \cdots < i_r \leq m, r \geq 2$. Since $g_1(k), g_2(k), \ldots, g_t(k)$ are all composite, such a term cannot exist, and so $\ell_k = m$.

Now we go back to the very basic property of the sequence $\{q_{k,n}\}_{n\geq 1}$.

2.4.7 **Theorem.** If $N_k(\Phi_k(x)) = 1$, then $(q_{k,n})^2 \mid x$ for each $n$.

*Proof.* Here, we write $q_n$ for $q_{k,n}$ for the sake of convenience.

Firstly, we have $q_1 \mid x$, for if $q_1 \nmid x$, then $\Phi_k(q_1 x) = \Phi_k(q_1 x)\Phi_k(x) = (q_1 - k)\Phi_k(x) = \Phi_k(x)$, contradicting $N_k(\Phi_k(x)) = 1$.

We also have $q_1{}^2 \mid x$, otherwise $\Phi_k(x/q_1) = \Phi_k(q_1)\Phi_k(x/q_1) = \Phi_k(q_1 \cdot x/q_1) = \Phi_k(x)$, a contradiction.

Now suppose $q_i{}^2 \mid x$ for $1 \le i \le n$. Let $q_{n+1} = q_{r_1} \cdots q_{r_s} + k$, where $1 \le r_1 < r_2 < \cdots < r_s \le n$.

If $q_{n+1} \nmid x$, then

$$\begin{aligned}\Phi_k\left(q_{n+1} \cdot \left(\frac{x}{q_{r_1} \cdots q_{r_s}}\right)\right) &= \Phi_k(q_{n+1})\Phi_k\left(\frac{x}{q_{r_1} \cdots q_{r_s}}\right) \\ &= q_{r_1} \cdots q_{r_s}\Phi_k\left(\frac{x}{q_{r_1} \cdots q_{r_s}}\right) = \Phi_k(x),\end{aligned}$$

which is a contradiction (the last equality can be seen by using the prime factorization of $x$).

If $q_{n+1} \parallel x$, then

$$\Phi_k\left(\frac{xq_{r_1} \cdots q_{r_s}}{q_{n+1}}\right) = \frac{\Phi_k\left(\frac{xq_{r_1} \cdots q_{r_s}}{q_{n+1}}\right)\Phi_k(q_{n+1})}{q_{r_1} \cdots q_{r_s}} = \frac{\Phi_k(xq_{r_1} \cdots q_{r_s})}{q_{r_1} \cdots q_{r_s}} = \Phi_k(x),$$

again a contradiction.

Thus we have shown that $q_{n+1}{}^2 \mid x$, and the induction is therefore complete.

An immediate consequence of this theorem is the following:

2.4.8 **Corollary**. If $\ell_k$ is not finite, then $N_k(m) \neq 1$ for any $m \in \mathbb{N}$.

In other words, when $\ell_k$ is not finite, the conjecture of the Carmichael type for the function $\Phi_k$ is indeed a theorem. Is the converse also true? That is, when $\ell_k < \infty$, does there exist a natural number $m$ such that $N_k(m) = 1$? For instance, let us consider the simplest case, viz. $\ell_k = 2$. If, in that case, $N_k(\Phi_k(x)) = 1$, then $p^2q^2|x$ by Theorem 2.4.7, where $p = k+1$ and $q = 2k+1$. For the sake of simplicity, consider $\Phi_k(p^2q^2) = p(p-k)q(q-k) = p^2q$. Is $x = p^2q^2$ the only solution of $\Phi_k(x) = p^2q$ if we assume $\ell_k = 2$? This leads us to

2.4.9 **Theorem.** If $p = k+1, q = 2k+1$ are prime, and if $q+k, pq+k, p^2q+k$ are composite, then $N_k(p^2q) = 1$ (the unique solution being $p^2q^2$).

*Proof.* From the above, we see that it suffices to prove the uniqueness.

Let $x = p_1^{\alpha_1}\cdots p_r^{\alpha_r}$ be a solution of $\Phi_k(x) = p^2q$, where $p_1 < p_2 < \cdots < p_r, \alpha_i \geq 1, 1 \leq i \leq r$.

That is, we have

$$p_1^{\alpha_1-1}(p_1-k)\cdots p_r^{\alpha_r-1}(p_r-k) = p^2q. \tag{2.4.10}$$

We want to show $x = p^2q^2$.

Firstly, observe that $p_i > k$, i.e. $p_i \geq k+1 = p$, for all $1 \leq i \leq r$. In particular, $p_1 \geq p$. We distinguish two cases.

Case I. $\mathbf{p_1 > p}$.

In this case, $p \neq p_i$ for all $i$, and so from (2.4.10) we have $p \mid (p_{i_o} - k)$ for some $1 \leq i_o \leq r$. We may write (2.4.10) as

$$p_1^{\alpha_1-1}(p_1-k)\cdots p_{i_o}^{\alpha_{i_o}-1}((p_{i_o}-k)/p)\cdots p_r^{\alpha_r-1}(p_r-k) = pq. \tag{2.4.11}$$

Since the right-hand side of (2.4.11) is a product of two distinct primes, we infer that $r \leq 3$, i.e. $r = 1, 2$, or 3.

a) $\mathbf{r = 1}$.

Equation (2.4.10) becomes

$$p_1^{\alpha_1 - 1}(p_1 - k) = p^2 q. \tag{2.4.12}$$

The assumption $p \neq p_1$ implies $p^2 \mid (p_1 - k)$, and from $p_1^{\alpha_1-1}((p_1 - k)/p^2) = q$, we get $\alpha_1 = 1$ or 2.

If $\alpha_1 = 1$, then (2.4.12) becomes $p_1 - k = p^2 q$, or $p^2 q + k = p_1$, which contradicts the fact that $p^2 q + k$ is composite.

If $\alpha_1 = 2$, then $p_1(p_1 - k) = p^2 q$, and this implies $p_1 = q$ and $p_1 - k = p^2$. But if $p_1 = q$, then $p_1 - k = q - k = p$, a contradiction.

b) $\mathbf{r = 2}$.

We may write (2.4.11) as

$$p_1^{\alpha_1-1} p_2^{\alpha_2-1}((p_1 - k)(p_2 - k)/p) = pq\,. \tag{2.4.13}$$

This implies $\alpha_1 \leq 2, \alpha_2 \leq 2$, and $\alpha_1, \alpha_2$ cannot be 2 at the same time (because $p_1 > p_2 > p$). Thus, there are two subcases: i) $\alpha_1 = \alpha_2 = 1$, ii) $\{\alpha_1, \alpha_2\} = \{1, 2\}$.

If i) holds, then $(p_1 - k)(p_2 - k) = p^2 q$, and so $\{p_1 - k, p_2 - k\} = \{q, p^2\}$ or $\{p, pq\}$. In the former case, we have $p_1 - k = q$, i.e. $q + k = p_1$, which contradicts the fact that $q + k$ is composite. In the latter case, $pq + k = p_2$, which contradicts the fact that $pq + k$ is composite.

If ii) holds, without loss of generality, assume $\alpha_1 = 1, \alpha_2 = 2$. Then we have $p_2(p_1 - k)(p_2 - k) = p^2q$, this implies $p_2 = q$, and hence $p_2(p_2 - k) = q(q - k) = qp$. Putting this back into the equation, we obtain $p_1 - k = p$, i.e. $p_1 = p + k = q = p_2$, which is impossible.

c) $\mathbf{r = 3}$.

Here (2.4.11) may be written as

$$(2.4.14) \qquad {p_1}^{\alpha_1 - 1}{p_2}^{\alpha_2 - 1}{p_3}^{\alpha_3 - 1}((p_1 - k)(p_2 - k)(p_3 - k)/p) = pq\,.$$

By the same reasoning as in b), we conclude that $\alpha_i \leq 2$ for all $i$, and $\alpha_i = 2$ for at most one $i$.

If $\alpha_{i_o} = 2$ for some $1 \leq i_o \leq 3$, then (2.4.14) implies $p_{i_o} = q$, and so $p_{i_o} - k = p$. Consequently, (2.4.14) becomes $q(p_1 - k)(p_2 - k)(p_3 - k)/p = pq$, i.e. $(p_1 - k)(p_2 - k)(p_3 - k)/p = p$, which is impossible since the left-hand side contains two factors greater than 1 (because $p_3 > p_2 > p_1 > p > k$) while the right-hand side is a prime.

Next consider the case $\alpha_1 = \alpha_2 = \alpha_3 = 1$. (2.4.14) becomes $(p_1 - k)(p_2 - k)(p_3 - k) = p^2q$. Note that each factor on the left-hand side is at least 2, and that the only way to express $p^2q$ as a product of three numbers each of which is greater than 1 is $p \cdot p \cdot q$. Hence this last equation actually does not hold.

Summing up, we have shown that (2.4.10) has no solutions for which $p_i \neq p$ for all $i$.

Case II. $p_1 = p$.

Here (2.4.10) becomes (note that $p_1 - k = p - k = 1$)

$$p^{\alpha_1 - 1} \cdot p_2^{\alpha_2 - 1}(p_2 - k) \cdots p_r^{\alpha_r - 1}(p_r - k) = p^2 q. \tag{2.4.15}$$

It is easy to see that $\alpha_1 \leq 3$, i.e. $\alpha_1 = 1, 2$ or 3, and that $r \geq 2$.

a) If $\alpha_1 = 1$, then we are back to Case I, and we know already that (2.4.15) has no solutions.

b) Next suppose $\alpha_1 = 2$, and write (2.4.15) as

$$p_2^{\alpha_2 - 1}(p_2 - k) \cdots p_r^{\alpha_r - 1}(p_r - k) = pq\,. \tag{2.4.16}$$

This implies $r \leq 3$, i.e. $r = 2$ or 3.

When $r = 2$, (2.4.16) becomes $p_2^{\alpha_2 - 1}(p_2 - k) = pq$. Clearly $\alpha_2 \leq 2$. If $\alpha_2 = 1$, then we have $p_2 - k = qp$, i.e. $pq + k = p_2$, contradicting the fact that $pq + k$ is composite. Hence we must have $\alpha_2 = 2$, and so $p_2(p_2 - k) = pq$. Since $p_2 > p$, we have $p_2 = q$. Thus in this case, $x = p_1^2 p_2^2 = p^2 q^2$.

It remains to show that all the other cases lead to contradictions.

When $r = 3$, (2.4.16) becomes $p_2^{\alpha_2 - 1} p_3^{\alpha_3 - 1}(p_2 - k)(p_3 - k) = pq$. Since $p_3 - k > p_2 - k \geq 2$, we infer that $\alpha_2 = \alpha_3 = 1$. In that case $p_2 - k = p$ and $p_3 - k = q$. The last equality contradicts the fact that $q + k$ is composite.

c) Finally, suppose $\alpha_1 = 3$. Then (2.4.15) becomes $p_2^{\alpha_2 - 1}(p_2 - k) \cdots p_r^{\alpha_r - 1}(p_r - k) = q$. It follows that $r = 2$, i.e. we have $p_2^{\alpha_2 - 1}(p_2 - k) = q$, and this implies that $\alpha_2 = 1$ and $p_2 - k = q$, which is again a contradiction.

This completes the proof.

2.4.17 **Remark.** Taking a closer look at the above proof, we see that if $p = k+1, q = 2k+1$ are primes, and if $\ell_k = 2$, then $N_k(p^2q) = 1$ or 3 according as $p^2q+k$ is composite or not. In the latter case, the solutions of $\Phi_k(x) = p^2q$ are $x = p^2q^2, p^2q+k, p(p^2q+k)$. For example, $N_{18}(13357) = N_{660}(577172641) = N_{996}(1981059937) = 1$, and $N_{546}(327035437) = N_{966}(1807527037) = 3$.

# Chapter 3

# Further study of $\Phi_k$ and $N_k$.

Throughout this chapter, $k$ denotes an arbitrary but fixed natural number.

## § 3.1 The normal number of prime factors of $p - k$.

Firstly, we have to explain what the title of this section actually means. Recall that for $n \in \mathbb{N}, \omega(n)$ denotes the number of distinct prime factors of $n$.

3.1.1 **Definition.** Let $\mathcal{A}$ be an infinite subset of $\mathbb{N}$, and let $A(x) = |\mathcal{A} \cap (0, x]|$, where $x$ is an arbitrary positive real number (i.e. $A(x)$ counts the numbers in $\mathcal{A}$ not exceeding $x$). Let $f(x)$ be an increasing function of $x$ (for large $x$). By saying that the normal number of prime factors of $a \in \mathcal{A}$ is $f(x)$, we mean that for every (small) $\epsilon > 0$, we have

$$|\{a \in \mathcal{A} \cap (0, x] : |\omega(a) - f(x)| \geq \epsilon f(x)\}| = o(A(x)) \quad (x \to \infty).$$

In other words, the normal number of prime factors of $a \in \mathcal{A}$ is $f(x)$ if and only if for any small $\epsilon > 0$, the number of prime factors of $a$ lies between $(1 - \epsilon)f(x)$ and $(1 + \epsilon)f(x)$ for almost every $a \in \mathcal{A}$.

The purpose of this section is to prove that the normal number of prime factors of $p - k$ ($k < p \leq x$) is $\log \log x$ (i.e. here we take $\mathcal{A} = \{p - k : p \in \wp, p > k\}$). (For $k = 1$, Erdös[Erd35] already proved this.) In fact, we are going to prove a result more precise than this. Before we give a statement of this result, we state and prove a couple of lemmas.

First of all, we quote a result from [Hal74] (Corollary 2.4.1, p. 80):

3.1.2 **Theorem.** Let $a \in \mathbb{N}$ and let $b$ be a non-zero integer. Then for any $x > 1$,

$$|\{p \in \wp \cap (0, x] : ap + b \in \wp\}| \ll \prod_{p|ab} \left(1 - \frac{1}{p}\right)^{-1} \cdot \frac{x}{\log^2 x}.$$

We want to mention once again (as we already did in the introductory chapter) that the constants implied by the $\ll$- symbol (or $O$-symbol) would be absolute, unless otherwise stated.

Now we deduce from Theorem 3.1.2 that

**3.1.3 Lemma.** For each real $x > k$, and for $a \in \mathbb{N}$, let $g(x,a) = |\{p \in \wp \cap (k,x] : \frac{p-k}{a} \in \wp\}|$. Then

$$g(x,a) \ll \frac{\log\log(3ka)}{a} \cdot \frac{x}{\log^2\left(\frac{x}{a}\right)} \cdot$$

*Proof.* It is straightforward to verify that $g(x,a) = |\{p \in \wp \cap (0, \frac{x-k}{a}] : ap + k \in \wp\}|$. It follows from Theorem 3.1.2 that

$$g(x,a) \le |\{p \in \wp \cap (0, \frac{x}{a}] : ap+k \in \wp\}| \ll \frac{ka}{\varphi(ka)} \cdot \frac{\frac{x}{a}}{\log^2 \frac{x}{a}} \ll \frac{\log\log(3ka)}{a} \cdot \frac{x}{\log^2 \frac{x}{a}},$$

in which we have applied the well-known facts that $\prod_{p|n}(1 - \frac{1}{p})^{-1} = \frac{n}{\varphi(n)}$ and $\frac{n}{\varphi(n)} \le c_o \log\log(3n)$ for every $n \in \mathbb{N}$ (the last inequality is in fact a special case of (2.1.2), see Theorem 2.1.1).

Next we prove

**3.1.4 Lemma.** For all sufficiently large $x$,

$$|\{n \in \mathbb{N} \cap (0,x] : P(n) \le x^{\frac{1}{12\log\log x}} \text{ or } P(n)^2 | n\}| \le \frac{4x}{\log^3 x} \cdot$$

(Recall that $P(n)$ denotes the largest prime factor of $n$ if $n > 1$ and $P(1) = 1$.)

*Proof.* For simplicity, write $y = \log x$, $z = \log\log x$.

We divide the natural numbers under consideration into three classes:

$$S_1 = \{n \in \mathbb{N} \cap (0,x] : P(n) \le x^{\frac{1}{12z}} \text{ and } \omega(n) \le 6z\},$$

$$S_2 = \{n \in \mathbb{N} \cap (0,x] : P(n) \leq x^{\frac{1}{12z}} \text{ and } \omega(n) > 6z\},$$

and $$S_3 = \{n \in \mathbb{N} \cap (0,x] : P(n) > x^{\frac{1}{12z}} \text{ and } P(n)^2 | n\}.$$

For each $n \in S_1$, write $n = p_1{}^{\alpha_1} \cdots p_r{}^{\alpha_r}$. Then for each $i, \alpha_i \leq \dfrac{\log n}{\log 2} \leq \dfrac{y}{\log 2}$ and $p_i \leq x^{\frac{1}{12z}}$, and hence there are at most $x^{\frac{1}{12z}} \cdot y / \log 2$ choices for $p_i{}^{\alpha_i}$. Since $r \leq 6z$, we infer that for large $x$,

$$|S_1| \leq \left( x^{\frac{1}{12z}} \frac{y}{\log 2} \right)^{6z} = x^{\frac{1}{2}} \left( \frac{y}{\log 2} \right)^{6z} \leq \frac{x}{y^3}.$$

In order to estimate $|S_2|$, we need the fact that $\sum_{n \leq x} d(n) \leq 2x \log x$ when $x \geq e$, where $d(n)$ denotes the number of divisors of $n$. This can be proved as follows:

$$\sum_{n \leq x} d(n) = \sum_{m \leq x} \left[ \frac{x}{m} \right] \leq x \sum_{m \leq x} \frac{1}{m} \leq x \left( \int_1^x \frac{dt}{t} + 1 \right) \leq 2x \log x$$

if $x \geq e$. Now write $a = |S_2|$ and $S_2 = \{n_1, n_2, \ldots, n_a\}$. Since $d(n) \geq 2^{\omega(n)}$, for each $i = 1, 2, \ldots, a$, we have $d(n_i) \geq 2^{\omega(n_i)} > 2^{6z}$. It follows that

$$2^{6z} |S_2| < d(n_1) + d(n_2) + \cdots + d(n_a) \leq \sum_{n \leq x} d(n) \leq 2xy \ ,$$

and so

$$|S_2| \leq \frac{2xy}{2^{6z}} = \frac{2x}{y^{6 \log 2 - 1}} < \frac{2x}{y^3} \ .$$

For each $n \in S_3, n$ is divisible by a square greater than $x^{\frac{1}{6z}}$, and therefore

$$|S_3| \leq \sum_{m^2 > x^{\frac{1}{6z}}} \frac{x}{m^2} < \frac{2x}{x^{\frac{1}{12z}}} = \frac{2x}{y^{\frac{y}{12z^2}}} \leq \frac{x}{y^3}$$

when $x$ is large enough (it is easily seen that $\sum_{m^2>t} \frac{1}{m^2} < \frac{2}{\sqrt{t}}$ for any $t \geq 1$).

Thus our lemma is proved.

We require one more lemma.

3.1.5 **Lemma.** Let $0 < \epsilon < 1/4$ and let $c$ be a fixed positive constant. Then there exists an $x_o = x_o(\epsilon)$ such that for any $x \geq x_o$,

$$\sum_{n=0}^{[(1-\epsilon)x]} \frac{x^n}{n!} < e^{(1-\frac{\epsilon^2}{4})x} , \tag{3.1.6}$$

$$\sum_{n>(1+\epsilon)x} \frac{(x+c)^{n-1}}{(n-1)!} < e^{(1-\frac{\epsilon^2}{4})x} . \tag{3.1.7}$$

*Proof.* It is easy to show by induction that

$$N! > \left(\frac{N+1}{e}\right)^N \text{ for all } N \in \mathbb{N}. \tag{3.1.8}$$

and

$$\sum_{n=0}^{N} \frac{x^n}{n!} < N \cdot \frac{x^N}{N!} \text{ for all } N \geq 2, x \geq \max\{N,3\} . \tag{3.1.9}$$

Combining (3.1.8) and (3.1.9), we have

$$\sum_{n=0}^{N} \frac{x^n}{n!} < N\left(\frac{ex}{N+1}\right)^N \text{ for all } N \geq 1, x \geq \max\{N,3\} .$$

By choosing $N = [(1-\epsilon)]$ in the above inequality (with $x \geq 3$), we obtain

$$\begin{aligned}\sum_{n=0}^{[(1-\epsilon)x]} \frac{x^n}{n!} &< (1-\epsilon)x\left(\frac{ex}{(1-\epsilon)x}\right)^{(1-\epsilon)x} \\ &= \exp\left\{((1-\epsilon)(1-\log(1-\epsilon)) + \frac{\log x}{x} + \frac{\log(1-\epsilon)}{x})x\right\} .\end{aligned}$$

Taylor series expansion gives $(1-\epsilon)(1-\log(1-\epsilon)) = 1 - \frac{\epsilon^2}{1\cdot 2} - \frac{\epsilon^3}{2\cdot 3} - \cdots$ $< 1 - \frac{\epsilon^2}{2}$. Therefore, (3.1.6) is established if we choose $x$ so large that

$$\frac{\log x}{x} + \frac{\log(1-\epsilon)}{x} < \frac{\epsilon^2}{4}\,.$$

To prove (3.1.7), let $m = [(1+\epsilon)x]$. Then

$$\begin{aligned}\sum_{n>(1+\epsilon)x} \frac{(x+c)^{n-1}}{(n-1)!} &= \frac{(x+c)^m}{m!} + \frac{(x+c)^{m+1}}{(m+1)!} + \cdots \\ &= \frac{(x+c)^m}{m!}\left(1 + \frac{x+c}{m+1} + \frac{(x+c)^2}{(m+1)(m+2)} + \cdots\right).\end{aligned}$$

Observe that for $i \geq 1, m+i \geq m+1 > (1+\epsilon)x$, and so $\frac{x+c}{m+i} < \frac{x+c}{(1+\epsilon)x} \leq \frac{1}{1+\epsilon/2}$ provided $x \geq (2+\epsilon)c/\epsilon$. Hence, for such $x$,

$$\sum_{n>(1+\epsilon)x} \frac{(x+c)^{n-1}}{(n-1)!} < \frac{(x+c)^m}{m!}\left(1 + \frac{1}{1+\frac{\epsilon}{2}} + \frac{1}{(1+\frac{\epsilon}{2})^2} + \cdots\right) = \frac{2+\epsilon}{\epsilon}\cdot\frac{(x+c)^m}{m!}\,.$$

By applying (3.1.8) again, we get

$$\begin{aligned}\sum_{n>(1+\epsilon)x} \frac{(x+c)^{n-1}}{(n-1)!} &< \frac{2+\epsilon}{\epsilon}\left(\frac{(x+c)e}{m+1}\right)^m < \frac{2+\epsilon}{\epsilon}\left(\frac{(x+c)e}{(1+\epsilon)x}\right)^{(1+\epsilon)x} \\ &\leq \frac{2+\epsilon}{\epsilon}\exp\left\{(1+\epsilon)x(1+\log(1+\frac{c}{x}) - \log(1+\epsilon))\right\} \\ &< \frac{2+\epsilon}{\epsilon}\exp\left\{(1+\epsilon)x(1+\frac{c}{x} - \epsilon + \frac{\epsilon^2}{2})\right\} \\ &= \frac{2+\epsilon}{\epsilon}\,\frac{e^{(1-\frac{\epsilon^2}{4})x}}{\exp\left\{(\frac{\epsilon^2}{4} - \frac{\epsilon^3}{2})x - (1+\epsilon)c\right\}} \\ &\leq e^{(1-\frac{\epsilon^2}{4})x}\end{aligned}$$

if $x \geq x_o$ for some $x_o = x_o(\epsilon)$. This completes the proof.

3.1.10 **Remark.** There are much better inequalities than (3.1.6) and (3.1.7), namely that for $x > 0, 0 < \alpha < 1 < \beta$,

$$\sum_{n \leq \alpha x} \frac{x^n}{n!} < \frac{1}{1-\alpha} \frac{e^{(1-Q(\alpha))x}}{\sqrt{\alpha x}} \text{ and } \sum_{n \geq \beta x} \frac{x^n}{n!} < \frac{1}{\beta - 1} \sqrt{\frac{\beta}{2\pi x}} e^{(1-Q(\beta))x},$$

where $Q(\lambda) := \lambda \log \lambda - \lambda + 1 (= \frac{(\lambda-1)^2}{1\cdot 2} - \frac{(\lambda-1)^3}{2\cdot 3} + \cdots$ if $|\lambda - 1| < 1)$. A proof of these inequalities can be found in [Nor76], pp. 692-694. For our purpose, Lemma 3.1.5 is already good enough.

Now we are ready to state and prove the main theorem of this section.

3.1.11 **Theorem.** For every $0 < \epsilon < 1/4$, we have

$$|\{p \in \wp \cap (k, x] : |\omega(p-k) - \log\log x| \geq \epsilon \log\log x\}| = O\left(\frac{x}{(\log x)^{1+\frac{\epsilon^2}{8}}}\right) \quad (x \to \infty).$$

*Proof.* Suppose $x$ is large, and write $y = \log x, z = \log\log x$.

For each $n \in \mathbb{N}$, let $\mathcal{A}_n = \{a \in \mathbb{N} : \omega(a) = n\}$ and $f(x,n) = |\{p \in \wp \cap (k, x] : (p-k) \in \mathcal{A}_n\}|$.

What we want to show is the same as

$$\sum_{n < (1-\epsilon)z} f(x,n) + \sum_{n > (1+\epsilon)z} f(x,n) = O\left(\frac{x}{y^{1+\delta}}\right),$$

where $\delta = \epsilon^2/8$.

By Lemma 3.1.4, $f(x,n) = |\mathcal{B}(x,n)| + O(x/y^3)$, where $\mathcal{B}(x,n) = \{p \in \wp \cap (k, x] : (p-k) \in \mathcal{A}_n,\ P(p-k) > x^{\frac{1}{12z}}$ and $P(p-k) \parallel (p-k)\}$. For each $p \in \mathcal{B}(x,n), p-k = aq$ for some $a \in \mathcal{A}_{n-1}$ and $q \in \wp$ with $q > x^{\frac{1}{12z}}$ (this implies $a < x^{1-\frac{1}{12z}}$). Thus, in the notation of Lemma 3.1.3, we get $|\mathcal{B}(x,n)| \leq \sum'_{a<x^{1-\frac{1}{12z}}} g(x,a)$, where (and in what follows) $\sum'$ denotes a sum restricted to elements of $\mathcal{A}_{n-1}$. On utilizing Lemma 3.1.3, we find an absolute constant $c_1$ such that

$$\begin{aligned} f(x,n) &\leq c_1 \sum'_{a<x^{1-\frac{1}{12z}}} \frac{\log\log(3ka)}{a} \cdot \frac{x}{\log^2(x/a)} + O(\frac{x}{y^3}) \\ &\leq c_2 \sum'_{a<x^{1-\frac{1}{12z}}} \frac{z}{a} \cdot x \cdot \frac{z^2}{y^2} + O(\frac{x}{y^3}) \\ &\leq c_2 \frac{xz^3}{y^2} \sum'_{a\leq x} \frac{1}{a} + O(\frac{x}{y^3}), \end{aligned}$$

where $c_2$ is some absolute constant.

From the definition of $\mathcal{A}_{n-1}$, we clearly have

$$\sum'_{a\leq x} \frac{1}{a} \leq \frac{\left(\sum_{p\leq x}\sum_{\alpha=1}^{\infty} p^{-\alpha}\right)^{n-1}}{(n-1)!} \leq \frac{(z+c_3)^{n-1}}{(n-1)!}$$

since $\sum_{p\leq x} \frac{1}{p-1} = \sum_{p\leq x} \frac{1}{p} + O(1) \leq \log\log x + c_3$ for some absolute constant $c_3$.

Summing up, we have shown that

$$f(x,n) \leq c_2 \frac{xz^3}{y^2} \cdot \frac{(z+c_3)^{n-1}}{(n-1)!} + O(\frac{x}{y^3}).$$

It follows from (3.1.6) that

$$\begin{aligned} \sum_{n<(1-\epsilon)z} f(x,n) &\leq c_2 \frac{xz^3}{y^2} \sum_{n=1}^{[(1-\epsilon)z]} \frac{(z+c_3)^{n-1}}{(n-1)!} + O(\frac{xz}{y^3}) \\ &< c_2 \frac{xz^3}{y^2} e^{(1-\frac{\epsilon^2}{4})(z+c_3)} + O(\frac{xz}{y^3}) \\ &< c_4 \frac{xz^3}{y^{1+2\delta}} + O(\frac{xz}{y^3}) < \frac{x}{y^{1+\delta}}. \end{aligned}$$

For the other sum $\sum_{n>(1+\epsilon)z} f(x,n)$, we observe that $f(x,n) = 0$ whenever $n \geq \log x/\log 2$. Therefore, by (3.1.7), we have

$$\begin{aligned}\sum_{n>(1+\epsilon)z} f(x,n) &\leq c_2 \frac{xz^3}{y^2} \sum_{n>(1+\epsilon)z} \frac{(z+c_3)^{n-1}}{(n-1)!} + O(\frac{xy}{y^3}) \\ &< c_2 \frac{xz^3}{y^2} e^{(1-\frac{\epsilon^2}{4})z} + O(\frac{x}{y^2}) \\ &= c_2 \frac{xz^3}{y^{1+2\delta}} + O(\frac{x}{y^2}) \\ &< \frac{x}{y^{1+\delta}}.\end{aligned}$$

This ends the proof.

3.1.12 **Remark**. Take $\mathcal{A} = \{p - k : p \in \wp \text{ and } p > k\}$. Then, by the prime number theorem, $A(x) = \pi(x+k) - \pi(k) \sim x/\log x$, and so Theorem 3.1.11 says that for $0 < \epsilon < 1/4$,

$$|\{a \in \mathcal{A} \cap (0,x] : |\omega(a) - \log\log x| \geq \epsilon \log\log x\}| = O(\frac{A(x)}{\log^\delta x}) \quad (x \to \infty),$$

where $\delta = \epsilon^2/8$. Trivially, $O(A(x)/\log^\delta x) = o(A(x))$. Thus Theorem 3.1.11 is much stronger than just saying that the normal number of prime factors of $p - k$ is $\log\log x$. In the above proof, we follow the same line of thought as given by P. Erdös [Erd35]. Theorem 3.1.11 will serve as a foundation for the next section.

## § 3.2 Distinct values of $\Phi_k$.

For each $x \geq 1$, define $V_k(x) = |\{n \in \mathbb{N} \cap (0,x] : n = \Phi_k(m)$ for some $m \in \mathbb{N}\}|$. That is, $V_k(x)$ denotes the number of distinct values of $\Phi_k$ not exceeding $x$. Note also that $V_k(x) = |\{n \in \mathbb{N} \cap (0,x] : N_k(n) > 0\}|$, so that $V_k$ is a generalization of the function $V$ mentioned in the introductory chapter (with $V_1 = V$).

Since $p-k = \Phi_k(p)$ for any prime $p > k$, we have $V_k(x) \geq \pi(x+k)-\pi(k) = (1+o(1))\pi(x)$. Our main object here is to give an upper bound estimate for $V_k(x)$. Again, in order to make the idea in the proof of the main result more transparent, we first state and prove some lemmas.

3.2.1 **Lemma**. For any real number $y \geq 0$, the series $\sum_{\substack{p>k \\ \omega(p-k)\leq y}} \frac{1}{p}$ converges. Moreover, for any $0 < \epsilon < 1$, there exists a constant $C(\epsilon)$ which depends on $\epsilon$ only (in fact, if we consider $k$ as a variable as well, then we should write $C(\epsilon) = C(\epsilon, k)$, but since $k$ is considered as fixed, we put the emphasis on the dependence on $\epsilon$ only) such that

$$\sum_{\substack{p>k \\ \omega(p-k)\leq y}} \frac{1}{p} \leq \frac{y}{1-\epsilon} + C(\epsilon).$$

*Proof.* Firstly, suppose $0 < \epsilon < \frac{1}{4}$ and $y$ is so large that $e^y > \log k$.

Set $z = \exp\exp\left(\frac{y}{1-\epsilon}\right)$.

Consider the sum $\sum_{\substack{k<p\leq t \\ \omega(p-k)\leq y}} 1$, where $t \geq z$. We have $(1-\epsilon)\log\log t \geq y \geq \omega(p-k)$, and so $|\omega(p-k) - \log\log t| \geq \epsilon \log\log t$. By Theorem 3.1.11, this

sum is $O(t(\log t)^{-1-\delta})$, where $\delta = \epsilon^2/8$. It follows that the improper integral

$$\int_z^\infty \frac{1}{t^2} \cdot \left( \sum_{\substack{k<p\leq t \\ \omega(p-k)\leq y}} 1 \right) dt$$

is convergent, and

$$\sum_{p>z}{}' \frac{1}{p} = \sum_{p>z}{}' \int_p^\infty \frac{1}{t^2} dt \leq \int_z^\infty \frac{1}{t^2} \left( \sum_{k<p\leq t}{}' 1 \right) dt = O\left( \int_z^\infty \frac{dt}{t(\log t)^{1+\delta}} \right) \leq C_1(\epsilon)$$

for some constant $C_1(\epsilon)$ depending on $\epsilon$ only, where $\sum'$ denotes a sum over primes $p$ satisfying the condition $\omega(p-k) \leq y$.

Therefore

$$\sum_{p>k}{}' \frac{1}{p} = \sum_{k<p\leq z}{}' \frac{1}{p} + \sum_{p>z}{}' \frac{1}{p} \leq \sum_{p\leq z} \frac{1}{p} + C_1(\epsilon) \leq \log\log z + c + C_1(\epsilon) = \frac{y}{1-\epsilon} + C_2(\epsilon),$$

where $c$ is some absolute constant and $C_2(\epsilon) = C_1(\epsilon) + c$. This is what we want to prove for $y \geq y_o$, where $y_o$ is any non-negative real number satisfying $e^{y_o} > \log k$ (so that $y_o$ depends only on $k$).

The required result follows for all $y \geq 0$ if we choose $C(\epsilon) = \frac{y_o}{1-\epsilon} + C_2(\epsilon)$ (with $0 < \epsilon < \frac{1}{4}$).

Now, the case in which $\frac{1}{4} \leq \epsilon < 1$ becomes trivial.

3.2.2 **Lemma.** Let $0 < \theta < 1$. Then the series $\sum_{p>k} \frac{\theta^{\Omega(p-k)}}{p-\theta}$ converges (recall that $\Omega(n)$ denotes the number of prime factors of $n$ counted according to multiplicity), and for any $0 < \epsilon < 1$ there is a constant $C_o(\epsilon)$ depending on

$\epsilon$ only (again, we may write $C_o(\epsilon) = C_o(\epsilon, k)$) such that

$$\sum_{p>k} \frac{\theta^{\Omega(p-k)}}{p-\theta} \le \frac{\theta}{(1-\epsilon)(1-\theta)} + C_o(\epsilon).$$

*Proof.* By Lemma 3.2.1, we have

$$\begin{aligned}
\sum_{p>k} \frac{\theta^{\omega(p-k)}}{p} &= \sum_{m=0}^{\infty} \theta^m \sum_{\substack{p>k \\ \omega(p-k)=m}} \frac{1}{p} \\
&= (1-\theta) \sum_{n=0}^{\infty} \theta^n \sum_{\substack{p>k \\ \omega(p-k)\le n}} \frac{1}{p} \\
&\le (1-\theta) \sum_{n=0}^{\infty} \left( \frac{n}{1-\epsilon} + C(\epsilon) \right) \theta^n \\
&= \frac{\theta}{(1-\epsilon)(1-\theta)} + C(\epsilon).
\end{aligned}$$

Since $\Omega \ge \omega$, we obtain

$$\begin{aligned}
\sum_{p>k} \frac{\theta^{\Omega(p-k)}}{p-\theta} &\le \sum_{p>k} \theta^{\Omega(p-k)} \left( \frac{1}{p} + \frac{1}{p(p-1)} \right) \\
&\le \sum_{p>k} \frac{\theta^{\omega(p-k)}}{p} + \sum_{p} \frac{1}{p(p-1)} \\
&\le \frac{\theta}{(1-\epsilon)(1-\theta)} + C_o(\epsilon).
\end{aligned}$$

**3.2.3 Lemma.** $|\{n \in \mathbb{N} \cap (0,x] : \Omega(n) \ge 2\log\log x/\log 2 \text{ or } P(n) \le x^{\frac{1}{6\log\log x}}\}| = O(\pi(x)\log\log x)$.

*Proof.* This is in fact a combination of Lemmas 1 and 2 in [Erd73]. Since the proof is quite long, and we would give nothing new in our proof, we refer the proof to that of the above mentioned lemmas (see [Erd73], pp. 202–203).

We may now state and prove our main result.

**3.2.4 Theorem.** For every $c > 2\sqrt{2/\log 2}(= 3.397\ldots)$, we have

$$V_k(x) = O(\pi(x)\exp(c\sqrt{\log\log x})).$$

*Proof.* Recall that $\mathcal{U}_k = \{n \in \mathbb{N} : p \mid n \Rightarrow p > k\} = \{n \in \mathbb{N} : \Phi_k(n) > 0\}$.

Using the notation of Lemma 2.1.1, we have that if $0 < \Phi_k(m) \leq x$, then $m \leq c_2(k)x(\log\log 3x)^k$.

For simplicity, write $\ell_1 = c_2(k)(\log\log 3x)^k$, $\ell_2 = 6\log\log x$, $\beta = 2/\log 2(= 2.885\ldots)$, and $\ell_3 = \beta\log\log x$.

Suppose that $n \in \mathbb{N}$ is a value of $\Phi_k$ not exceeding $x$. Then either $\Omega(n) \geq \ell_3$, or $n = \Phi_k(m)$ for some $m \in \mathcal{U}_k \cap (0, x\ell_1]$ with $\Omega(\Phi_k(m)) < \ell_3$. Therefore, by Lemma 3.2.3,

$$V_k(x) \leq \sideset{}{'}\sum_{\substack{m \leq x\ell_1 \\ \Omega(\Phi_k(m)) < \ell_3}} 1 + O(\pi(x)\log\log x),$$

where $\sum'$ represents a sum restricted to elements of $\mathcal{U}_k$.

We further restrict the above sum to those $m$ for which $P(m) > x^{\frac{1}{\ell_2}}$. Observe that $x^{\frac{1}{\ell_2}} \leq (x\ell_1)^{\frac{1}{6\log\log(x\ell_1)}}$ if $x$ is large enough. Hence, by Lemma 3.2.3 again, the number of $m \leq x\ell_1$ ignored is $O(\pi(x\ell_1)\log\log(x\ell_1)) = O(\pi(x)(\log\log x)^{k+1})$, where the constant implied by the second $O$-notation depends on $k$. Thus

$$V_k(x) \le \sideset{}{'}\sum_{\substack{m \le x\ell_1, P(m) > x^{1/\ell_2} \\ \Omega(\Phi_k(m)) < \ell_3}} 1 + O(\pi(x)(\log\log x)^{k+1}).$$

Let us call the last sum $\sum_1$. By writing $m = pn$ in this sum, where $p$ is a prime $> x^{1/\ell_2}$ (and so $n < \ell_1 x^{1-\frac{1}{\ell_2}}$ and $\Phi_k(n) \mid \Phi_k(m)$), we see that

$$\begin{aligned} \sum\nolimits_1 \;&\le \sideset{}{'}\sum_{\substack{n < \ell_1 x^{1-1/\ell_2} \\ \Omega(\Phi_k(n)) < \ell_3}} \pi\left(\frac{x\ell_1}{n}\right) \\ &\ll \sideset{}{'}\sum_{\substack{n < \ell_1 x^{1-1/\ell_2} \\ \Omega(\Phi_k(n)) < \ell_3}} \frac{x\ell_1/n}{\log(x\ell_1/n)} \\ &\ll \pi(x)(\log\log x)^{k+1} \sideset{}{'}\sum_{\Omega(\Phi_k(n)) < \ell_3} \frac{1}{n}, \end{aligned}$$

in which the constant implied by the last $\ll$- symbol depends on $k$, and we do not restrict the size of the very last sum because the series is convergent, as we are now going to show. So for we have shown that

$$V_k(x) \ll \pi(x)(\log\log x)^{k+1} \sideset{}{'}\sum_{\Omega(\Phi_k(n)) < \ell_3} \frac{1}{n}\,. \tag{3.2.5}$$

Let $0 < \theta < 1$. Define $g_\theta : \mathbb{N} \to \mathbb{R}$ by $g_\theta(n) = \theta^{\Omega(\Phi_k(n))}$ or $0$ according as $n \in \mathcal{U}_k$ or not. Since $\Phi_k$ is multiplicative and $\Omega$ is completely additive, it is straightforward to verify that $g_\theta$ is a multiplicative arithmetic function. Next, define

$$f(\theta) = \sum_{n=1}^{\infty} \frac{g_\theta(n)}{n}.$$

Since $g_\theta$ is multiplicative, $f(\theta)$ is well-defined (i.e. the series is convergent) if and only if its Euler product is convergent, and in that case

$$(3.2.6)\qquad \begin{aligned} f(\theta) &= \prod_p \left(1 + \sum_{m=1}^{\infty} \frac{g_\theta(p^m)}{p^m}\right) \\ &= \prod_{p>k} \left(1 + \sum_{m=1}^{\infty} \theta^{\Omega(p-k)} \frac{\theta^{m-1}}{p^m}\right) \\ &= \prod_{p>k} \left(1 + \frac{\theta^{\Omega(p-k)}}{p-\theta}\right). \end{aligned}$$

By Lemma 3.2.2, the last product is convergent, and so $f$ is indeed well-defined. From the definition of $g_\theta$, we have $f(\theta) = \sum_n' \dfrac{\theta^{\Omega(\Phi_k(n))}}{n}$, and therefore

$$(3.2.7)\qquad \sum_{\Omega(\Phi_k(n))<\ell_3}' \frac{1}{n} \leq f(\theta)\theta^{-\beta \log\log x}.$$

In particular, (3.2.7) shows that the series on the left-hand side converges.

Suppose $0 < \epsilon < 1$ is given.

Since $1 + t < e^t$ for all $t > 0$, it follows from (3.2.5), (3.2.7), (3.2.6) and Lemma 3.2.2 that

$$(3.2.8)\ V_k(x) \ll \pi(x)(\log\log x)^{k+1} \exp\left\{\frac{\theta}{(1-\epsilon)(1-\theta)} - \beta(\log\log x)\log\theta\right\},$$

where the $\ll$- constant depends on $k$ and $\epsilon$ only.

Now we choose $\theta$ optimally that

$$\left(\frac{\theta}{1-\theta}\right)^2 = (1-\epsilon)\beta\log\log x.$$

For this value of $\theta$, we have

$$(3.2.9)\quad \frac{\theta}{1-\theta} = \sqrt{(1-\epsilon)\beta \log\log x} \text{ and } \log\frac{1}{\theta} < \frac{1}{\sqrt{(1-\epsilon)\beta\log\log x}}.$$

Our theorem follows inmediately from (3.2.8) and (3.2.9).

3.2.10 **Corollary.** $V_k(x) = o(x)$, i.e. for almost all $n$ the equation $\Phi_k(y) = n$ has no solutions.

3.2.11 **Remark.** Theorem 3.2.4 generalizes the result due to Erdös and Hall [Erd73]. We suspect that a result similar to the one obtained by Maier and Pomerance [Mai88] holds for $V_k$, namely

$$V_k(x) = \frac{x}{\log x}\exp((c+o(1))(\log\log\log x)^2)$$

for some constant $c$ (it may depend on $k$). Maier and Pomerance pointed out that "the same estimate can be obtained for the number of distinct integers which are products of the members of $\{p+a : p \text{ is prime}, a \in S\}$, where $S$ is any finite set of non-zero integers." ([Mai88], p. 275) However, their method is too technically involved to be contained in this thesis.

## § 3.3 Values taken many times by $\Phi_k$.

Recall that $\Psi(x,y) = |\{n \in \mathbb{N} : n \leq x \text{ and } P(n) \leq y\}|$ $(x, y \geq 1)$ and $\Pi_k(x,y) = |\{p \in \wp \cap (k,x] : P(p-k) \leq y\}|$ $(x > k, y \geq 1)$.

We first give an estimate for $\Psi(x, \log x)$.

3.3.1 **Lemma.** For any $\epsilon > 0$, $\Psi(x, \log x) = o(x^\epsilon)$ $(x \to \infty)$.

*Proof.* Write $y = \log x$. Let $n$ be a natural number $\leq x$ with $P(n) \leq y$.

Let $m$ be an integer $\geq 2$. We can always write $n = a^m b$, where $a, b$ are natural numbers with $b$ $m$-free (i.e. $b$ is free from $m$-th power divisors $> 1$). Then $a \leq x^{\frac{1}{m}}$, and since $P(n) \leq y$, $b$ is a term in the expansion of $\prod_{p \leq y}(1 + p + \cdots + p^{m-1})$. Obviously, there are $m^{\pi(y)}$ terms in this expansion. It follows that

$$\Psi(x,y) \leq x^{\frac{1}{m}} m^{\pi(y)} = x^{\frac{1}{m}} m^{O(\frac{\log x}{\log\log x})} = x^{\frac{1}{m} + O(\frac{\log m}{\log\log x})} \leq x^{\frac{\epsilon}{2}}$$

if we choose $m \geq 4/\epsilon$ and if $x$ is large. *A fortiori*, $\Psi(x, \log x) = o(x^\epsilon)$.

We need the Brun-Titchmarsh Theorem in later argument. We quote the following version from [Hal74] (Theorem 3.8, p.110):

3.3.2 **Theorem** (Brun-Titchmarsh). If $1 \leq a < x$ and $(a,b) = 1$, then

$$\pi(x; a, b) < \frac{3x}{\varphi(a)\log(\frac{x}{a})}.$$

We apply this to prove

**3.3.3 Lemma.** Suppose there exist $0 < \theta_o, c_o < 1$ such that $\Pi_k(x, x^{\theta_o}) \geq c_o x/\log x$ for all large $x$. Then there exists $0 < \theta_1 < \theta_o$ such that $\Pi_k(x, x^{\theta_1}) \geq \frac{c_o}{2} x/\log x$ for all large $x$.

*Proof.* Let $0 < \theta < \theta_o$. Brun-Titchmarsh Theorem yields

$$\begin{aligned}
\Pi_k(x, x^{\theta_o}) - \Pi_k(x, x^{\theta}) &= |\{p \in \wp \cap (k, x] : x^{\theta} < P(p-k) \leq x^{\theta_o}\}| \\
&\leq |\bigcup_{x^{\theta} < q \leq x^{\theta_o}} \{p \in \wp \cap (k, x] : p \equiv k (\mathrm{mod}\, q)\}| \\
&\leq \sum_{x^{\theta} < q \leq x^{\theta_o}} \pi(x; q, k) \\
&< \sum_{x^{\theta} < q \leq x^{\theta_o}} \frac{3x}{\varphi(q) \log(x/q)} \\
&\leq \frac{3x}{(1-\theta_o)\log x} \sum_{x^{\theta} < q \leq x^{\theta_o}} \frac{1}{q-1},
\end{aligned}$$

in which $q$ denotes a variable prime.

From the standard result $\sum_{p \leq x} \frac{1}{p} = \log\log x + c + O(1/\log x)$, we have

$$\sum_{z < p \leq y} \frac{1}{p-1} = \log\left(\frac{\log y}{\log z}\right) + O\left(\frac{1}{\log z}\right) \quad (z < y).$$

Thus

$$\Pi_k(x, x^{\theta_o}) - \Pi_k(x, x^{\theta}) \leq \frac{3}{1-\theta_o}\left(\log(\frac{\theta_o}{\theta}) + O(\frac{1}{\theta \log x})\right)\frac{x}{\log x} \leq \frac{c_o}{2}\frac{x}{\log x}$$

if $\theta$ is sufficiently close to $\theta_o$ and if $x$ is sufficiently large. This implies immediately what we want to prove.

We are now in a position to prove

**3.3.4 Theorem.** Suppose there exist $0 < \theta_o, c_o < 1$ such that $\Pi_k(x, x^{\theta_o}) \geq$

$c_o x/\log x$ for all large $x$. Then $N_k(m) > m^{1-\theta_o}$ for infinitely many $m$.

*Proof*: By Lemma 3.3.3, there is a positive number $\theta_1 < \theta_o$ such that

$$\Pi_k(x, x^{\theta_1}) \geq c_1 x/\log x \tag{3.3.5}$$

for all large $x$, where $c_1 = c_o/2$.

Let $x$ be large, and let $y = (\log x)^{\frac{1}{\theta_1}}$.

Consider the following sets:

$$F = \{p \in \wp \cap (k, y] : P(p-k) \leq \log x\},$$

$$A = \{n \in \mathbb{N} \cap (0, x] : n \text{ is square-free and } p \mid n \Rightarrow p \in F\},$$

$$B = \{\Phi_k(a) : a \in A\}.$$

Obviously, $|F| = \Pi_k(y, \log x) = \Pi_k(y, y^{\theta_1})$ and $B \subset \{n \in \mathbb{N} \cap (0, x] : P(n) \leq \log x\}$ (so that $|B| \leq \Psi(x, \log x)$).

Let $r = [\log x/\log y]$. Then the product of any $r$ distinct primes in $F$ does not exceed $y^r \leq y^{\log x/\log y} = x$, and hence this product is in $A$. By (3.3.5),

$$|F| \geq c_1 y/\log y = c_1(\log x)^{\frac{1}{\theta_1}}/\log y \geq \log x/\log y \geq r.$$

Therefore, $A$ contains at least $\binom{|F|}{r}$ elements, and so

$$|A| \geq \binom{|F|}{r} \geq \left(\frac{|F|}{r}\right)^r \geq \left(c_1(\log x)^{\frac{1-\theta_1}{\theta_1}}\right)^r > \left(c_1(\log x)^{\frac{1-\theta_1}{\theta_1}}\right)^{\frac{\theta_1 \log x}{\log\log x} - 1}$$
$$= x^{1-\theta_1+o(1)}.$$

On the other hand, it is evident from the definition of $B$ that

$$|A| \leq \sum_{b \in B} N_k(b).$$

Thus we obtain

$$x^{1-\theta_1+o(1)} \leq \sum_{b \in B} N_k(b) \leq |B| \max_{b \in B} N_k(b). \tag{3.3.6}$$

Now suppose to the contrary that $N_k(m) > m^{1-\theta_o}$ for only finitely many $m$. Then there exists a constant $c_2$ such that $N_k(m) \leq c_2 m^{1-\theta_o}$ for all $m \in \mathbb{N}$.

Since $|B| \leq \Psi(x, \log x)$, and since $\Psi(x, \log x) = o(x^\epsilon)$ for any $\epsilon > 0$ by Lemma 3.3.1, we deduce from (3.3.6) (by choosing $\epsilon = (\theta_o - \theta_1)/2$) that

$$x^{1-\theta_1+o(1)} \leq x^{\frac{\theta_o-\theta_1}{2}} \cdot c_2 x^{1-\theta_o} = c_2 x^{1-\frac{\theta_o+\theta_1}{2}}.$$

But this is impossible since $1 - \theta_1 > 1 - (\theta_o + \theta_1)/2$. The theorem is thus proved.

It remains to show that the constants $\theta_o, c_o$ in Theorem 3.3.4 do exist. To this end, we quote two more results from [Gol69] and [Hoo73]:

3.3.7 **Theorem** (Goldfeld-Hooley). Let $\sqrt{e} < x^{\frac{1}{2}} < y \leq x$. Define

$$T_x(y) = \sum_{x^{1/2} < q \leq y} \pi(x; q, k) \log q,$$

where $q$ denotes a variable prime. Then we have

$$T_x(x) = \frac{x}{2} + O(x \log\log x / \log x), \tag{3.3.8}$$

$$(3.3.9) \qquad T_x(y) < (4 + o(1))x \log(yx^{-\frac{1}{2}})/\log x$$

for all large $x$.

We may now prove

3.3.10 **Theorem.** $\Pi_k(x, x^{\frac{1}{2}}) \geq cx/\log x$ for all large $x$, where $c$ is any positive constant less than $1 - 4\log(\frac{5}{4})(= 0.1074\ldots)$.

*Proof.* We clearly have

$$\pi(x) - \pi(k) - \Pi_k(x, x^{\frac{1}{2}}) = \sum_{x^{\frac{1}{2}} < q \leq x} \pi(x; q, k),$$

and hence by partial summation and by using the notation in the Goldfeld-Hooley Theorem, we obtain

$$(3.3.11) \qquad \pi(x) - \pi(k) - \Pi_k(x, x^{\frac{1}{2}}) = \frac{T_x(x)}{\log x} + \int_{x^{\frac{1}{2}}}^{x} \frac{T_x(y)}{y\log^2 y} dy.$$

For $x^{\frac{1}{2}} < y \leq x^{\frac{5}{8}}$, we use (3.3.9), and for $x^{\frac{5}{8}} < y \leq x$, we use $T_x(y) \leq T_x(x) \sim \frac{x}{2}$. Thus

$$\begin{aligned} &\pi(x) - \pi(k) - \Pi_k(x, x^{\frac{1}{2}}) \\ \leq\ & \left(\tfrac{1}{2} + o(1)\right)\frac{x}{\log x} + \frac{(4 + o(1))x}{\log x}\int_{x^{1/2}}^{x^{5/8}} \frac{\log(yx^{-\frac{1}{2}})}{y\log^2 y} dy \\ &\quad + \left(\tfrac{1}{2} + o(1)\right)x\int_{x^{5/8}}^{x} \frac{dy}{y\log^2 y} \\ =\ & \left(4\log\left(\tfrac{5}{4}\right) + o(1)\right)\frac{x}{\log x}, \end{aligned}$$

and our result follows since $\pi(x) - \pi(k) \sim x/\log x$ $(x \to \infty)$.

A combination of Theorems 3.3.4 and 3.3.10 yields

**3.3.12 Theorem.** $N_k(m) > m^{\frac{1}{2}}$ for infinitely many $m$.

As a consequence, we get the following result which is already stated at the end of section 2.3:

**3.3.13 Corollary.** For any $n \in \mathbb{N}$, there exist infinitely many $m \in \mathbb{N}$ such that $N_k(m) > n$.

Theorem 3.3.12 shows the existence of a positive constant $c$ for which

$$N_k(m) > m^c \text{ for infinitely many } m. \tag{3.3.14}$$

Let $C_k$ denote the least upper bound for the values of $c$ for which (3.3.14) holds. Analogous to the Erdös conjecture stated in the introductory chapter, we make the following:

**3.3.15 Conjecture.** $C_k = 1$ for all natural numbers $k$.

It is readily seen from Theorem 2.1.6 that $C_k \leq 1$. Thus, in order to settle Conjecture 3.3.15, it remains to show $C_k \geq 1$. What we have shown in Theorem 3.3.12 implies that $C_k \geq \frac{1}{2}$ (for all $k \in \mathbb{N}$). This estimate can be improved by using the Brun-Titchmarsh Theorem (3.3.2) and the well-known theorem of Bombieri, which is stated below (see also Lemma 3.3 of [Hal74], p. 111).

**3.3.16 Theorem** (Bombieri). For each real $x \geq 2$, and $a \in \mathbb{N}$, let

$$E(x;a) = \max_{2\leq y\leq x} \max_{\substack{1\leq b\leq a\\(b,a)=1}} |\pi(y;a,b) - \frac{\pi(y)}{\varphi(a)}|.$$

Then, given any positive constant $B$, there exists a positive constant $C$ such that

$$\sum_{a<x^{\frac{1}{2}}/\log^C x} E(x;a) = O\left(\frac{x}{\log^B x}\right),$$

where the implied $O$-constant depends on $B$.

**3.3.17 Theorem.** Suppose $c_o$ is a positive constant such that $\Pi_k(x, x^{\frac{1}{2}}) \geq (c_o + o(1))x/\log x$ for all large $x$. Then for any $\frac{1}{2}e^{-c_o} < \theta < \frac{1}{2}$, $\Pi_k(x, x^\theta) \gg x/\log x$. Hence, $C_k \geq 1 - \frac{e^{-c_o}}{2}$. In particular, we have $C_k \geq 1 - 625/512e (= 0.5509\ldots)$ and $N_k(m) > m^{0.55}$ for infinitely many $m$ (for all $k \in \mathbb{N}$).

*Proof.* As in the proof of Lemma 3.3.3, we have

$$\Pi_k(x, x^{\frac{1}{2}}) - \Pi_k(x, x^\theta) \leq \sum_{x^\theta < q \leq x^{\frac{1}{2}}} \pi(x; q, k) = \sum\nolimits_1,$$

in which $\frac{e^{-c_o}}{2} < \theta < \frac{1}{2}$ and $q$ denotes a variable prime. We are now going to estimate $\sum_1$ by using Bombieri's theorem and the Brun-Titchmarsh Theorem.

From Bombieri's theorem, there exists a positive constant $C$ such that

$$\begin{aligned}\sum_{x^\theta<q\le x^{\frac12}/\log^C x}\pi(x;q,k) &= \pi(x)\sum_{x^\theta<q\le x^{\frac12}/\log^C x}\frac{1}{q-1}+O\left(\frac{x}{\log^2 x}\right)\\ &= \pi(x)\log\left(\frac{1}{2\theta}-\frac{C\log\log x}{\theta\log x}\right)+O\left(\frac{x}{\log^2 x}\right)\\ &= \log\left(\frac{1}{2\theta}\right)\cdot\frac{x}{\log x}+O\left(\frac{x\log\log x}{\log^2 x}\right).\end{aligned}$$

From the Brun-Titchmarsh Theorem (3.3.2), we have

$$\sum_{x^{\frac12}/\log^C x<q\le x^{\frac12}}\pi(x;q,k)\le\frac{6x}{\log x}\sum_{x^{\frac12}/\log^C x<q\le x^{\frac12}}\frac{1}{q-1}=O\left(\frac{x\log\log x}{\log^2 x}\right).$$

Thus we have shown that

$$\sum\nolimits_1=\log\left(\frac{1}{2\theta}\right)\frac{x}{\log x}+O\left(\frac{x\log\log x}{\log^2 x}\right),$$

and hence

$$\begin{aligned}\Pi_k(x,x^\theta) &\ge \Pi_k(x,x^{\frac12})-\sum\nolimits_1\\ &\ge (c_o+o(1))\frac{x}{\log x}-\left(\log\left(\frac{1}{2\theta}\right)+O\left(\frac{\log\log x}{\log x}\right)\right)\frac{x}{\log x}\\ &\gg \frac{x}{\log x}\end{aligned}$$

since $\theta>\frac12 e^{-c_o}$.

The remaining conclusion of the theorem follows from Theorem 3.3.4 and Theorem 3.3.10 (in which $c_o=1-4\log(\frac54)$).

3.3.18 **Remark.** The above theorem shows that an improvement of the constant $c_o$ implies that of $C_k$. For instance, Pomerance stated without proof in [Pom74] that he used the results of Iwaniec [Iwa80] to obtain $\Pi_1(x, x^{\frac{1}{2}}) \geq 0.120025\pi(x)$ for all large $x$. That is, in the case of $k = 1$, we may take $c_o = 0.120025$, and so $C_1 \geq 1 - \dfrac{e^{-c_o}}{2} = 0.55655\ldots$, as mentioned in the introductory chapter. This is the latest published estimate on $C_1$. We want to point out that Theorem 3.3.17 is not strong enough to prove Conjecture 3.3.15 even if we have the best possible value for the constant $c_o$. For if $c_o$ is the constant in Theorem 3.3.17, then we infer from (3.3.11) and (3.3.8) that $c_o \leq \frac{1}{2}$, i.e. the best possible value of $c_o$ does not exceed $\frac{1}{2}$, and hence the best possible estimate of $C_k$ by Theorem 3.3.17 is that $C_k \geq 1 - \frac{1}{2\sqrt{e}} = 0.6967\ldots$. In a private communication to M.V. Subbarao, C. Pomerance claimed that $C_1 \geq 0.68$.

# Chapter 4

# Carmichael's problem for the unitary totient.

Let $a, b \in \mathbb{N}$. We recall that $b$ is called a unitary divisor of $a$ if $b \mid a$ and $(b, a/b) = 1$, and that $b$ is said to be unitarily prime to $a$ if the largest divisor of $b$ which is a unitary divisor of $a$ is unity. The unitary totient $\varphi^*(a)$ may be defined as the number of natural numbers not exceeding $a$ which are unitarily prime to $a$. This unitary analogue of the Euler $\varphi$-function is due to E. Cohen [Coh60]. It is shown (see, for example, [Coh60]) that $\varphi^*$ is a multiplicative function with $\varphi^*(p^a) = p^a - 1$ for any prime $p$ and $a \in \mathbb{N}$.

The analogue of Carmichael's conjecture for the unitary totient $\varphi^*$ is false, because it is easy to see that for any $a \in \mathbb{N}$, the equation $\varphi^*(x) = 2^a - 1$ has a unique solution, viz. $x = 2^a$.

The principal aim of this chapter is to discuss the equation $\varphi^*(x) = m$ for two special types of $m$, namely i) $m = 2^n (n \in \mathbb{N})$, and ii) $m = 4(2^p - 1)$, where $p \neq 5$, $p \equiv 1 (\mathrm{mod}\, 4)$ and $2^p - 1$ is a prime (so that $p$ itself is a prime). Case i) is already considered in a paper by M. Ismail and M.V. Subbarao [Ism76]. However, in this paper, there are mistakes in the statement of the related theorem (Theorem 1.1, p. 51) as well as in the proof of a lemma (Lemma 2.3, p. 50) upon which the theorem depends. We will make the corrections in section 4.1. As for case ii), C. Pomerance noted in a private communication to M.V. Subbarao that the equation $\varphi^*(x) = m$ has a unique solution (viz. $x = 5 \cdot 2^p$), so that this provides a non-trivial example for which the unitary analogue of the Carmichael conjecture fails (Subbarao had conjectured that if $n$ is even, then $\varphi^*(x) = n$ never has a unique solution. Case ii) is thus also a counter-example to this conjecture) No proof of this has been published so far. We will give a proof of this in section 4.3. This proof depends on the complete solution of the diophantine equation $2^x - 5^y = 3$, therefore, we insert a detailed discussion of this diophantine equation in section 4.2.

We conclude this chapter by giving a brief discussion of the solvability of the equation $\varphi^*(x) = n$ in general.

## § 4.1 The equation $\varphi^*(x) = 2^n$.

It is an elementary fact that if $2^a + 1 (a \in \mathbb{N})$ is prime, then $a = 2^b$ for some non-negative integer $b$. A number of the form $F_n = 2^{2^n} + 1 (n \geq 0)$ is called a Fermat number (of course, it is called a Fermat prime when it is a prime). Up to now, only five Fermat primes are known (viz. when $0 \leq n \leq 4$). Recently, with the help of supercomputers, $F_{20}$ is proved to be composite by J. Young and D.A. Buell [You88]. From this together with the work of earlier writers, we now know that $F_n$, for $n$ equal to 5 through 21, are all composite. $F_{22}$ is the smallest Fermat number of unknown character.

With the above up-to-date information about the Fermat numbers, we may now give a corrected and modified version of Theorem 4.1 of [Ism76]:

4.1.1 **Theorem** (Ismail Subbarao). The equation

$$\varphi^*(x) = 2^n \tag{4.1.2}$$

has no solution for $32 \leq n < 2^{22}$. If $n \leq 31$, then the only solutions of (4.1.2) are

$$\prod_{j=0}^{4} (2^{2^j a_j} + 1)^* \text{ and } 2 \prod_{j=0}^{4} (2^{2^j a_j} + 1)^* \quad \text{if } n \not\equiv 3 (\text{mod} 4),$$

or

$$\prod_{j=0}^{4} (2^{2^j a_j} + 1)^*, 2 \prod_{j=0}^{4} (2^{2^j a_j} + 1)^* \text{ and } 3^2 \prod_{j=2}^{4} (2^{2^j a_j} + 1)^* \quad \text{if } n \equiv 3 (\text{mod} 4),$$

where $n = a_0 + 2a_1 + \cdots + 2^r a_r, a_i \in \{0, 1\}$, and

$$(2^b + 1)^* = \begin{cases} 1 & \text{if } b = 0, \\ 2^b + 1 & \text{if } b \neq 0. \end{cases}$$

As remarked in [Ism76], the number $2^{22}$ may be replaced by $2^m$ where $F_m$ is the smallest Fermat prime greater than $F_4$ (however no such prime is known so far). The proof of this theorem depends on the following two lemmas. The first one is quoted from [Utz61]. The proof of the second one in [Ism76] contains many minor mistakes. We conclude this section by providing a corrected proof of this second lemma.

4.1.3 **Lemma** (Utz). The only solutions of the diophantine equation

$$2^x + 1 = 3^y$$

are

$$\begin{cases} x = 1 \\ y = 1 \end{cases} \quad \text{and} \quad \begin{cases} x = 3 \\ y = 2\,. \end{cases}$$

4.1.4 **Lemma**. Let $p$ be a prime $> 3$. Then the diophantine equation

$$2^x + 1 = p^y \tag{4.1.5}$$

has no solution unless $p$ is a Fermat prime and $y = 1$.

*Proof.* Since $p$ is odd, we can always write $p = 2^m n + 1$ with $n$ odd.

Suppose (4.1.5) is satisfied for some $x, y \in \mathbb{N}$.

Then $n \mid (p^y - 1) = 2^x$ since $n \mid (p-1)$ and $(p-1) \mid (p^y - 1)$. Therefore, $n = 1$ and $p$ is a Fermat prime.

Next suppose $y > 1$. From the above, $p = 2^m + 1$. Clearly, $1 < m < x$. Hence (4.1.5) implies

$$(4.1.6) \qquad 2^{x-m} = \sum_{j=1}^{y} \binom{y}{j} 2^{(j-1)m} = y + 2^m \sum_{j=2}^{y} \binom{y}{j} 2^{(j-2)m},$$

so that $2 \mid y$. Now suppose $2^a \mid y$ for some $a \in \mathbb{N}$. We assert that $2^{a+1}$ divides each term in the above sum. This is seen as follows. The $j$-th term, $j \geq 2$, of the sum can be written as

$$(4.1.7) \qquad \frac{y(y-1)\cdots(y-j+1)}{j!} 2^{(j-1)m}.$$

Write $j = a_o + 2a_1 + \cdots + 2^r a_r$, $a_i \in \{0, 1\} (a_r \neq 0)$. Then the highest power of 2 in $j!$ is $a_1 + (2^2 - 1)a_2 + \cdots + (2^r - 1)a_r = j - (a_o + a_1 + \cdots + a_r)$. Since the highest power of 2 in $y \cdot 2^{(j-1)m}$ is at least $a + (j-1)m$, the highest power of 2 in (4.1.7) is at least

$$a + (j-1)m - j + (a_o + \cdots + a_r) \geq a + 2(j-1) - j + 1 \geq a + 1.$$

Therefore $2^{a+1} < 2^{x-m}$, so that $2^{a+1} \mid 2^{x-m}$, and hence $2^{a+1} \mid y$ by (4.1.6). This is obviously impossible, thus completing the proof.

## § 4.2 The diophantine equation $2^x - 5^y = 3$.

Throughout this section, $x, y$ denote positive integers.

Many diophantine equations have only finitely many solutions. The equation

$$2^x - 5^y = 3 \tag{4.2.1}$$

is one such example, as we are going to show in Lemma 4.2.5 (see also Theorem 4.2.26). In order to solve equations of this kind completely, one needs explicit upper bounds for the size of all the solutions of these equations. The first useful result in this direction is the following well-known theorem of A. Baker [Bak68].

4.2.2 **Theorem** (A. Baker). Let $\alpha_1, \dots, \alpha_n (n \geq 2)$ be non-zero algebraic numbers with heights and degrees not exceeding integers $A, d$ respectively, where $A \geq 4, d \geq 4$. Suppose $0 < \delta < 1$. If rational integers $b_1, \dots, b_n$ exist, with absolute values at most $H$, such that

$$0 < |b_1 \log \alpha_1 + \cdots + b_n \log \alpha_n| < e^{-\delta H},$$

where "log" means the principal logarithm, then

$$H < (4^{n^2} \delta^{-1} d^{2n} \log A)^{(2n+1)^2}.$$

However we are not going to use this theorem, because for our purpose it can be replaced by a recent result of P. Philippon and M. Waldschmidt [Phi88]. We quote Baker's theorem only for comparison (see Remarks 4.2.8 and 4.2.25 below).

**4.2.3 Theorem** (Philippon-Waldschmidt). Let $\alpha_1, \ldots, \alpha_n$ be non-zero algebraic numbers and $\beta_o, \ldots, \beta_n$ be algebraic numbers. For $1 \le j \le n$, let $\log \alpha_j$ be any determination of the logarithm of $\alpha_j$. Assume that the number

$$\Lambda = \beta_o + \beta_1 \log \alpha_1 + \cdots + \beta_n \log \alpha_n$$

does not vanish. For an algebraic number $\alpha$, we denote by $H(\alpha)$ the height of $\alpha$.

Let $D$ be a positive integer and $A_1, \ldots, A_n, A, B$ be positive real numbers satisfying

$$D \ge [\mathbf{Q}(\alpha_1, \ldots, \alpha_n, \beta_o, \ldots, \beta_n) : \mathbf{Q}],$$

$$A_j \ge \max \{H(\alpha_j), \exp |\log \alpha_j|, e^n\}, 1 \le j \le n,$$

$$A = \max\{A_1, \ldots, A_n, e^e\},$$

and
$$B = \max\{H(\beta_j) : 0 \le j \le n\}.$$

Then

$$|\Lambda| \ge e^{-U},$$

where

$$U = C(n) D^{n+2} \log A_1 \cdots \log A_n (\log B + \log\log A)$$

and
$$C(n) \le 2^{8n+53} \cdot n^{2n}.$$

Before applying the above theorem, we prove a little lemma.

4.2.4 **Lemma**. If $0 < t < \frac{1}{2}$, then $|\log(1-t)| < 2t$. Moreover, if $u \ge 570$, then $6 \cdot 2^{-u} < e^{-0.69u}$.

*Proof.* Consider the function $f(t) = |\log(1-t)| - 2t = \log(1-t)^{-1} - 2t$. We have $f'(t) = \dfrac{1}{1-t} - 2 = \dfrac{2t-1}{1-t} < 0$ for $0 \le t < \frac{1}{2}$, and so $f(t)$ is decreasing on $[0, \frac{1}{2})$. Therefore, $f(t) < f(0) = 0$ for $0 < t < \frac{1}{2}$. This proves the first statement.

For the second statement, we note that $\dfrac{\log 6}{\log 2 - 0.69} = 569.322\ldots < 570$. Thus if $u \ge 570$, then $u > \log 6/(\log 2 - 0.69)$, and hence

$$e^{(\log 2 - 0.69)u} > e^{\log 6} = 6 ,$$

i.e.
$$2^u \cdot e^{-0.69u} > 6 ,$$

or
$$6 \cdot 2^{-u} < e^{-0.69u}.$$

We may now apply the Philippon-Waldschmidt Theorem to prove

4.2.5 **Lemma**. If $2^x - 5^y = 3$, then $x < 10^{25}$.

*Proof.* We may suppose $x \ge 570$ (otherwise, there is nothing to prove). It follows from Lemma 4.2.4 that

$$(4.2.6) \qquad |x \log 2 - y \log 5| = \left| \log\left(\frac{2^x}{5^y}\right) \right| = |\log(1 - 3 \cdot 2^{-x})| < 2 \cdot 3 \cdot 2^{-x} = 6 \cdot 2^{-x} < e^{-0.69x}.$$

Clearly $|x \log 2 - y \log 5| > 0$. Therefore, the Philippon-Waldschmidt Theorem is applicable with $n = 2$, $\alpha_1 = 2$, $\alpha_2 = 5$, $\beta_o = 0$, $\beta_1 = x$, $\beta_2 = -y$, $D = 1$, $A_1 = A_2 = e^2$, $A = e^e$ and $B = x$. Using the notation of the theorem, we have

$$U \le 2^{16+53} \cdot 2^4 \cdot 1 \cdot 2 \cdot 2 \cdot (\log x + \log\log e^e) = 2^{75}(\log x + 1),$$

and so $|x \log 2 - y \log 5| \geq e^{-2^{75}(\log x+1)}$. This together with (4.2.6) implies

$$e^{-0.69x} > e^{-2^{75}(\log x+1)}. \tag{4.2.7}$$

It is straightforward to verify that $0.69x > 2^{75}(\log x + 1)$ whenever $x \geq 10^{25}$. Thus our conclusion follows immediately from (4.2.7).

4.2.8 **Remark.** If we apply Baker's theorem to equation (4.2.1), we can get only that $x < (4^4 \cdot 0.69^{-1} \cdot 4^4 \cdot \log 5)^{25} = 4.0516\ldots \cdot 10^{129} < 10^{130}$. Thus Lemma 4.2.5 gives a much better upper bound, and this would save us a lot of computer time.

Now we know that equation (4.2.1) has finitely many solutions with $x < 10^{25}$. It is easy to see that this equation has at least two solutions, namely

$$\begin{cases} x = 3 \\ y = 1, \end{cases} \qquad \begin{cases} x = 7 \\ y = 3. \end{cases}$$

After determining the upper bound for the size of the solutions of a diophantine equation, in order to solve the equation completely, one has to make use of the special property of the equation. The remaining discussion of this section is devoted to showing that equation (4.2.1) has no solutions for which $x \geq 8$. This will be accomplished in a series of lemmas. Firstly we prove

4.2.9 **Lemma.** Let $j \in \mathbb{N}$ be given, and let $a_j$ be determined by the congruence $2^{4\cdot 5^{j-1}} \equiv a_j 5^j + 1 \pmod{5^{2j}}$ together with $0 \le a_j < 5^j$. Then

$$2^{4\cdot 5^{n-1}} \equiv a_j 5^n + 1 (\text{mod } 5^{n+j}) \text{ for all } n \geq j.$$

(**Remark.** By the Euler-Fermat Theorem, $2^{4\cdot 5^{j-1}} = m5^j + 1$ for some integer $m$. Dividing $m$ by $5^j$ and taking modulo $5^{2j}$, we get $2^{4\cdot 5^{j-1}} \equiv a_j 5^j + 1 \pmod{5^{2j}}$ for some $0 \le a_j < 5^j$. It is easy to see that this $a_j$ is uniquely determined.)

*Proof.* Denote by $S(n)$ the statement " $2^{4\cdot 5^{n-1}} \equiv a_j 5^n + 1 \pmod{5^{n+j}}$".

The definition of $a_j$ implies that $S(j)$ is true.

Suppose $S(n)$ is true for some $n \ge j$. Then $2^{4\cdot 5^{n-1}} = b \cdot 5^{n+j} + a_j 5^n + 1$ for some integer $b$. It follows that

$$\begin{aligned} 2^{4\cdot 5^{(n+1)-1}} &= ((b \cdot 5^j + a_j)5^n + 1)^5 \\ &\equiv 5(b \cdot 5^j + a_j)5^n + 1 \equiv a_j 5^{n+1} + 1 \pmod{5^{n+1+j}}. \end{aligned}$$

That is, $S(n+1)$ is also true. Therefore, $S(n)$ is true for all $n \ge j$.

4.2.10 **Corollary.** We have

(4.2.11) $2^{4\cdot 5^{n-1}} \equiv 3 \cdot 5^n + 1 \pmod{5^{n+1}}$ for all $n \ge 1$,

(4.2.12) $2^{4\cdot 5^{n-1}} \equiv 621018 \cdot 5^n + 1 \pmod{5^{n+10}}$ for all $n \ge 10$.

*Proof.* It is computed (with the help of a computer) that

$$a_1 = 3,\ a_2 = a_3 = 18,\ a_4 = 393,\ a_5 = 2268,\ a_6 = 11643,$$

$$a_7 = 74143, \quad a_8 = 230393, \quad a_9 = a_{10} = 621018.$$

4.2.13 **Remark.** Clearly, 2 is a primitive root modulo 5. From (4.2.11) we see that 2 is also a primitive root modulo $5^n$ for any $n \geq 2$ (of course, this follows also from standard results). (4.2.12) will be needed for further computation.

We prove the following property of the $a_j$'s for future use.

4.2.14 **Lemma.** $a_j \equiv a_\ell \pmod{5^\ell}$ for all $j \geq \ell$. In particular, $a_j \equiv 3 \pmod 5$ for all $j \geq 1$.

*Proof.* It is sufficient to prove $a_{j+1} \equiv a_j \pmod{5^j}$ for all $j \geq 1$.

By the definition of the $a_j$'s, we have $a_{j+1}5^{j+1} + 1 \equiv 2^{4\cdot 5^j} \pmod{5^{2j+2}}$ and $2^{4\cdot 5^{j-1}} = b \cdot 5^{2j} + a_j 5^j + 1$ for some integer $b$.

Now taking this modulo $5^{2j+1}$, we obtain

$$a_{j+1}5^{j+1} + 1 \equiv ((b \cdot 5^j + a_j)5^j + 1)^5 \equiv 5(b \cdot 5^j + a_j)5^j + 1 \equiv a_j 5^{j+1} + 1.$$

This implies immediately that $a_{j+1} \equiv a_j \pmod{5^j}$.

Next we introduce the following definition which is legitimate since 2 is a primitive root modulo $5^n$ for all $n \geq 1$.

4.2.15 **Definition.** For each $n \in \mathbb{N}$, denote by $r_n$ the smallest positive integer for which $2^{r_n} \equiv 3 \pmod{5^n}$.

We give some basic properties of the $r_n$'s in the following

4.2.16 **Lemma.** For any $n \in \mathbb{N}$,

i) $r_n < 4 \cdot 5^{n-1}$ ,

ii) $r_{n+1} \geq r_n$ ,

iii) $r_{n+1} = 4 \cdot 5^{n-1} s_n + r_n$ for some $0 \leq s_n < 5$ .

*Proof*: i) and ii) follow immediately from the definition and the fact that $\varphi(5^n) = 4 \cdot 5^{n-1}$.

Consider $2^{r_n}(2^{r_{n+1}-r_n} - 1) = 2^{r_{n+1}} - 2^{r_n} \equiv 3 - 3 = 0 \pmod{5^n}$. This means that $5^n | 2^{r_n}(2^{r_{n+1}-r_n} - 1)$. Since $(5^n, 2^{r_n}) = 1$, we have $5^n | (2^{r_{n+1}-r_n} - 1)$, i.e. $2^{r_{n+1}-r_n} \equiv 1 \pmod{5^n}$. Since 2 is a primitive root modulo $5^n$, we get $4 \cdot 5^{n-1} | (r_{n+1} - r_n)$, i.e. $r_{n+1} = 4 \cdot 5^{n-1} s_n + r_n$ for some non-negative integer $s_n$. In fact, $s_n < 5$, for if $s_n \geq 5$, then $r_{n+1} \geq 4 \cdot 5^{n-1} \cdot 5 = 4 \cdot 5^n$, contradicting i).

Suppose $n$ and $r_n$ are known. Then $r_n$ can be calculated from formula iii) of Lemma 4.2.16 if $s_n$ is computable from the known value of $r_n$. Since $r_{n+1}$ is determined by the congruence $2^{r_{n+1}} \equiv 3 \pmod{5^{n+1}}$, it is natural to consider the least non-negative residue of $2^{r_n}$ modulo $5^{n+1}$. It follows from Definition 4.2.15 that

$$(4.2.17) \qquad 2^{r_n} \equiv 5^n t_n + 3 \pmod{5^{n+1}}$$

for some integer $0 \leq t_n < 5$. Note that the number $t_n$ is computable. We are now going to derive a relationship between $s_n$ and $t_n$. Taking modulo $5^{n+1}$

and utilizing (4.2.11) and (4.2.17), we have

$$\begin{aligned} 0 &\equiv 2^{r_{n+1}} - 3 = 2^{4\cdot 5^{n-1}s_n + r_n} - 3 = \left(2^{4\cdot 5^{n-1}}\right)^{s_n} \cdot 2^{r_n} - 3 \\ &\equiv (3\cdot 5^n + 1)^{s_n}(5^n t_n + 3) - 3 \equiv (3\cdot 5^n s_n + 1)(5^n t_n + 3) - 3 \\ &\equiv 9\cdot 5^n s_n + 5^n t_n + 3 - 3 = (9s_n + t_n)5^n. \end{aligned}$$

This implies that $9s_n + t_n \equiv 0 \pmod 5$, and so $s_n \equiv t_n \pmod 5$, i.e. $s_n = t_n$ since both numbers lie in the interval $[0,5)$.

Summing up, we obtain

4.2.18 **Lemma.** For any $n \in \mathbb{N}$,

$$r_{n+1} = 4\cdot 5^{n-1} t_n + r_n,$$

where $t_n$ is uniquely determined by

$$2^{r_n} \equiv 5^n t_n + 3 \pmod{5^{n+1}} \quad \text{and} \quad 0 \le t_n < 5.$$

Using this lemma, we found that

$$\begin{aligned} &r_1 = 3,\ r_2 = r_3 = 7,\ r_4 = 107,\ r_5 = 607,\ r_6 = 8107, \\ &r_7 = r_8 = 45607,\ r_9 = 358107 \quad \text{and} \quad r_{10} = 1920607. \end{aligned}$$

Our purpose is to compute $r_n$ for $n$ large (say $n = 40$) (see Lemma 4.2.24, where this is needed). Note that we do not need to know every intermediate value of the $r_j$'s. From this point of view, Lemma 4.2.18 is not effective enough. However, the idea involved in proving this lemma is still useful. In order to make the idea more transparent, we put our discussion in a more general setting.

Let $j$ be a given integer $\geq 2$, and let $r_n$ be given for some $n \geq j$. We would like to calculate $r_{n+j}$ from $r_n$. Firstly, consider $2^{r_n}$ modulo $5^{n+j}$ (this is computable). From Definition 4.2.15, we know that $2^{r_n} = m \cdot 5^n + 3$ for some integer $m$, but we can always write $m = m' \cdot 5^j + t_n$ with $0 \leq t_n < 5^j$, and so

$$2^{r_n} \equiv 5^n t_n + 3 \pmod{5^{n+j}}, \quad 0 \leq t_n < 5^j. \tag{4.2.19}$$

Similar to iii) in Lemma 4.2.16, we have $r_{n+j} = 4 \cdot 5^{n-1} s_n + r_n$ for some $0 \leq s_n < 5^j$. Taking modulo $5^{n+j}$ and utilizing (4.2.19) and Lemma 4.2.9, we have

$$\begin{aligned} 0 &\equiv 2^{r_{n+j}} - 3 = \left(2^{4 \cdot 5^{n-1}}\right)^{s_n} \cdot 2^{r_n} - 3 \\ &\equiv (a_j 5^n + 1)^{s_n} (5^n t_n + 3) - 3 \\ &\equiv (a_j 5^n s_n + 1)(5^n t_n + 3) - 3 \\ &\equiv (3 a_j s_n + t_n) 5^n. \end{aligned}$$

Consequently,

$$3 a_j s_n + t_n \equiv 0 \pmod{5^j}. \tag{4.2.20}$$

Let $k_j$ be defined by $3 a_j k_j + 1 \equiv 0 \pmod{5^j}$ with $0 \leq k_j < 5^j$. Then by multiplying both sides of (4.2.20) by $k_j$, we get

$$s_n \equiv k_j t_n \pmod{5^j}.$$

When $j$ is large (say $j \geq 5$), the congruence $3 a_j x + 1 \equiv 0 \pmod{5^j}$ is not easy to solve directly. However, there is an inductive way to calculate $k_j$ if $k_{j-1}$ and $a_j$ are known. Consider $3 k_{j-1} a_j + 1$. From Lemma 4.2.14, this number is congruent to $3k_{j-1}a_{j-1}+1$ modulo $5^{j-1}$, but in turn the last number is congruent to 0 modulo $5^{j-1}$ by the definition of $k_{j-1}$. Thus we may write $3k_{j-1}a_j + 1 \equiv \ell_j 5^{j-1} \pmod{5^j}$ for some $0 \leq \ell_j < 5$. Note that this $\ell_j$ is computable. Next, consider

$$\begin{aligned}3(\ell_j 5^{j-1} + k_{j-1})a_j + 1 &= 3a_j\ell_j 5^{j-1} + 3k_{j-1}a_j + 1 \\ &\equiv 3a_j\ell_j 5^{j-1} + \ell_j 5^{j-1} \qquad \pmod{5^j} \\ &= (3a_j+1)\ell_j 5^{j-1} \\ &\equiv (3\cdot 3+1)\ell_j 5^{j-1} \equiv 0 \qquad \pmod{5^j},\end{aligned}$$

in which we have applied the last statement of Lemma 4.2.14.

Observe that $0 \leq \ell_j 5^{j-1} + k_{j-1} < 4\cdot 5^{j-1} + 5^{j-1} = 5^j$. It follows from the definition of $k_j$ that $k_j = \ell_j 5^{j-1} + k_{j-1}$. Summing up, we proved the following: suppose $k_{j-1}$ and $a_j$ are known, compute $\ell_j$ such that $3k_{j-1}a_j+1 \equiv \ell_j 5^{j-1} \pmod{5^j}$ with $0 \leq \ell_j < 5$, then $k_j = \ell_j 5^{j-1} + k_{j-1}$ (equivalently, $k_j \equiv (3a_j+1)k_{j-1}+1 \pmod{5^j}$ with $0 \leq k_j < 5^j$). In this way, we found that

$$k_1 = 1, \quad k_2 = 6, \quad k_3 = 81, \quad k_4 = k_5 = 581, \quad k_6 = 13081,$$
$$k_7 = 75581, \quad k_8 = 231831, \quad k_9 = 1794331, \quad k_{10} = 7653706.$$

In particular, we obtain a method to calculate $r_{n+10}$ from $r_n$, which is the following:

4.2.21 **Lemma.** For any $n \geq 10$,

$$r_{n+10} = 4\cdot 5^{n-1}s_n + r_n,$$

where $s_n$ is (uniquely) determined by

$$\begin{cases} 0 \leq s_n < 9765625 (= 5^{10}), \\ s_n \equiv 7653706 t_n \pmod{9765625}, \\ t_n 5^n \equiv 2^{r_n} - 3 \pmod{5^{n+10}}. \end{cases}$$

Since $r_{10} = 1920607$, by using Lemma 4.2.21, the values of $r_{20}, r_{30}, r_{40}$ are calculated (on a computer). We have

$$r_{20} = 2922\ 73378\ 58107,$$

$$r_{30} = 5\ 19917\ 09770\ 87831\ 70607,$$

$$r_{40} = 161\ 53787\ 80529\ 58550\ 17519\ 20607.$$

In particular, note that

$$r_{40} > 10^{27}. \tag{4.2.22}$$

We are now ready to solve equation (4.2.1) completely. Before doing so, we prove two more lemmas.

4.2.23 **Lemma**. If $x \geq 5$ and $2^x - 5^y = 3$, then $y > 0.4x$.

*Proof*. Consider the function $f(t) = 2^t - 5^{0.4t}$, $t > 0$.

We have $f'(t) = (\log 2)2^t - (0.4 \log 5)5^{0.4t} > 0$ for all $t > 0$ (note that $5^{0.4} = 1.90365\ldots$). Thus $f(t)$ is increasing throughout $(0, \infty)$, and so

$$f(t) \geq f(5) = 2^5 - 5^2 = 7 > 3 \text{ for all } t \geq 5.$$

Hence if $x \geq 5$ and $y \leq 0.4x$, then $2^x - 5^y \geq 2^x - 5^{0.4x} = f(x) > 3$, a contradiction.

4.2.24 **Lemma.** If $x \geq 8$ and $2^x - 5^y = 3$, then $x > 10^{25}$.

*Proof.* Clearly $y \geq 4$. By rewriting the equation in the form $2^x - 3 = 5^y$, we see that $2^x \equiv 3 \pmod{5^4}$. It follows that $x \geq r_4 = 107$. Now Lemma 4.2.23 implies that $y > 0.4(107) > 40$, and this in turn implies that $2^x \equiv 3 \pmod{5^{40}}$. Hence, by (4.2.22), $x \geq r_{40} > 10^{25}$.

4.2.25 **Remark.** If we know only that $x < 10^{130}$ (as Baker's theorem gives), then we need to know the values of $r_n$ for $n$ up to 200.

Combining Lemmas 4.2.5 and 4.2.24, we conclude that

4.2.26 **Theorem.** The diophantine equation $2^x - 5^y = 3$ has exactly two solutions, namely

$$\begin{cases} x = 3 \\ y = 1 \end{cases} \quad \text{and} \quad \begin{cases} x = 7 \\ y = 3 \end{cases}.$$

4.2.27 **Remark.** After the above method was derived, we found a paper by R.J. Stroeker and R. Tijdeman [StT2], which contains the following result:

**Theorem** (Stroeker-Tijdeman). The only solutions to the inequality $0 < |p^x - q^y| < p^{x/2}$ in primes $p, q$ with $1 < p < q < 20$ are $(p, q, x, y)$ (2,3,1,1), (2,3,2,1), (2,3,3,2), (2,3,5,3), (2,3,8,5), (2,5,2,1), (2,5,7,3), (2,7,3,1), (2,11,7,2), (2,13,4,1), (2,17,4,1), (2,19,4,1), (3,5,3,2), (3,7,2,1), (3,11,2,1), (3,13,7,3), (5,7,1,1), (5,11,3,2), (7,19,3,2), (11,13,1,1), and (17,19,1,1).

Theorem 4.2.26 follows easily from this theorem. However, the method given in the above needs only the basic tool from transcendental number theory (and the help of a computer, of course). Because of the originality of the above method, it is worthwhile giving complete details.

## § 4.3 The equation $\varphi^*(x) = 4(2^p - 1)$.

With the help of Theorem 4.2.26, we are able to show

4.3.1 **Theorem.** Suppose $p \neq 5$, $p \equiv 1 \pmod 4$ and $2^p - 1$ is a prime.

Then $\varphi^*(x) = 4(2^p - 1)$ has a unique solution, viz. $x = 5 \cdot 2^p$.

*Proof.* Assume $\varphi^*(x) = 4(2^p - 1)$.

Clearly $x$ has at least one odd prime factor and not more than two.

If $q_1^{a_1} \parallel x$ and $q_2^{a_2} \parallel x$ for some odd primes $q_1 \neq q_2 (a_1, a_2 \in \mathbb{N})$, then

$$(4.3.2) \qquad (q_1^{a_1} - 1)(q_2^{a_2} - 1) \mid 4(2^p - 1).$$

Since $q_i^{a_i} - 1 (i = 1, 2)$ are both even, and since $q_1^{a_1} \neq q_2^{a_2}$, it follows from (4.3.2) that

$$q_1^{a_1} - 1 = 2 \text{ and } q_2^{a_2} - 1 = 2(2^p - 1) ,$$

(or the other way round; here we have made use of the primality of $2^p - 1$)

i.e. $$q_1^{a_1} = 3 \quad \text{and} \quad q_2^{a_2} = 2^{p+1} - 1 .$$

But it is obvious that $3 \mid (2^{p+1} - 1)$, and so the last two equations imply $q_1 = q_2 = 3$, which is impossible.

Thus we have shown that $x$ has exactly one odd prime factor. That is, $x = 2^a q^b$ for some odd prime $q$, and $a \geq 0, b \geq 1$.

Suppose $a = 0$, i.e. $x = q^b$. Then $q^b - 1 = 4(2^p - 1)$, i.e.

$$q^b = 2^{p+2} - 3. \tag{4.3.3}$$

Since $p \equiv 1 \pmod 4$, $p = 4n + 1$ for some $n \in \mathbb{N}$, and since $16 \equiv 1 \pmod 5$, we have

$$2^{p+2} - 3 = 2^{4n+3} - 3 \equiv 1 \cdot 2^3 - 3 = 8 - 3 \equiv 0 \pmod 5.$$

It follows from (4.3.3) that $q = 5$, and (4.3.3) becomes

$$2^{4n+3} - 5^b = 3\,. \tag{4.3.4}$$

By Theorem 4.2.26, $b = 1$ or 3. It is easy to see that $b = 1$ cannot happen, and so $b = 3$. Putting this into (4.3.3), we get $2^{p+2} - 3 = 125$, i.e. $p = 5$, contradicting the hypothesis of the theorem.

Thus $a \neq 0$.

Next if $a = 1$, then $\varphi^*(2^a q^b) = \varphi^*(q^b)$, and from this we will obtain (4.3.3) again, which is proved to be impossible.

Hence $a > 1$, and from $(2^a - 1)(q^b - 1) = \varphi^*(x) = 4(2^p - 1)$, we conclude that $2^a - 1 = 2^p - 1$ and $q^b - 1 = 4$ (note that $2^a - 1 > 1$ is odd and $q^b - 1$

is even, and also that $2^p - 1$ is prime), i.e. $a = p, q^b = 5$, i.e. $x = 5 \cdot 2^p$, as desired.

4.3.5 **Remark.** When $p = 5$, the equation $\varphi^*(x) = 4(2^p - 1)$ has three solutions, viz. $x = 5 \cdot 2^5, 5^3$ and $2 \cdot 5^3$. The condition $p \equiv 1 \pmod 4$ is also necessary. For instance, the equation $\varphi^*(x) = 4(2^7 - 1)$ has three solutions, viz. $x = 5 \cdot 2^7$, 509 and 1018.

## § 4.4 The solvability of $\varphi^*(x) = n$.

Let $V^*(x) = |\{n \in \mathbb{N} \cap (0, x] : n = \varphi^*(m) \text{ for some } m \in \mathbb{N}\}|$ $(x \geq 1)$.

It is easy to see that $\varphi^*(n) \geq \varphi(n)$ for all $n \in \mathbb{N}$. Thus, there is an absolute constant $c_o$ such that $n \leq c_o \varphi^*(n) \log\log(3\varphi^*(n))$ for all $n \in \mathbb{N}$ (to see this, we may take $k = 1$ in (2.1.3)).

Now we may apply the same technique as in section 3.2 to obtain

4.4.1 **Theorem.** For every $c > 2\sqrt{2/\log 2}$, we have

$$V^*(x) = O(\pi(x)\exp(c\sqrt{\log\log x})).$$

*Proof.* By using exactly the same argument as given in the first part of the proof of Theorem 3.2.4, we get

$$V^*(x) \ll \pi(x)(\log\log x)^2 \theta^{-\beta\log\log x} f^*(\theta)$$

for any $0 < \theta < 1$ and large $x$, where $\beta = 2/\log 2$ and $f^*(\theta) = \sum_{n=1}^{\infty} \frac{\theta^{\Omega(\varphi^*(n))}}{n}$.

The required conclusion follows from Lemma 3.2.1 and the fact that

$$f^*(\theta) = \prod_p \left(1 + \sum_{m=1}^{\infty} \frac{\theta^{\Omega(p^m-1)}}{p^m}\right) \leq \prod_p \left(1 + \frac{\theta^{\Omega(p-1)}}{p-1}\right) \leq \exp\left(\sum_p \frac{\theta^{\Omega(p-1)}}{p-1}\right).$$

4.4.2 **Corollary**. For almost all $n$, the equation $\varphi^*(x) = n$ has no solutions.

# Chapter 5

# Concluding remarks and open problems.

In the introductory chapter, we mentioned the following results:

(5.1) Erdös [Erd58] showed that if $n$ is a natural number with the property that $N(m_o) = n$ for some $m_o \in \mathbb{N}$, then $N(m) = n$ for infinitely many $m \in \mathbb{N}$.

(5.2) Pomerance [Pom80] showed that for all large $m$,

$$N(m) \leq m \exp(-(1 + o(1)) \log m \log\log\log m / \log\log m) \ .$$

(5.3) Maier and Pomerance [Mai88] showed that

$$V(x) = \frac{x}{\log x} \exp((c + o(1))(\log\log\log x)^2)$$

for some explicitly determined constant $c$ $(= 0.8178\ldots)$.

It is expected that all these results can be generalized to the functions $N_k$ and $V_k$ (see sections 2.1 and 3.2 for their definitions), i.e. (5.1) and (5.2) are still true if $N(m)$ is simply replaced by $N_k(m)$, and (5.3) is still true if $V(x)$ is replaced by $V_k(x)$ and $c$ is replaced by some suitably determined constant (which may depend on $k$). However, we do not know how to determine $c$ in the general case. Moreover, we are not sure if the exponent 2 in (5.3) still holds for $V_k$ (should it be $k+1$?).

We hope that these problems can be settled in a near future.

Finally we would like to raise the following questions and conjectures (some of them have been mentioned in previous chapters).

(5.4) Does Hypothesis H imply the Carmichael conjecture?

(5.5) **(Conjecture)** Let $k$ be an arbitrary natural number. Then for any integer $n > 1$, there exist infinitely many $m$ such that $N_k(m) = n$. (This is a generalization of the Sierpinski conjecture mentioned in Chapter 1.)

(5.6) Does Conjecture 5.5 follow from Hypothesis H?

(5.7) **(Conjecture)** Let $p_i$ denote the $i$-th odd prime. Then for $n \geq 2$,

$$(p_n - 2) \mid \prod_{i=1}^{n-1} p_i(p_i - 2) .$$

(5.8) Let $k \in \mathbb{N}$ be such that $k+1$ and $2k+1$ are both prime. Define the sequence$\{q_{k,n}\}_{n\geq 1}$ as in (2.4.5), and define $\ell_k = |\{q_{k,n}\}_{n\geq 1}|$. We conjecture that

(5.8.1) $\ell_2 = \ell_6 = \infty$ .

(5.8.2) $\ell_k = \infty$ for infinitely many $k$ (satisfying the above condition).

(5.8.3) For any integer $m \geq 2$, there exist infinitely many $k$ for which $\ell_k = m$. (We know already that this follows from Hypothesis H, see section 2.4.)

(5.8.4) If $\ell_k < \infty$, then $N_k(m) = 1$ for some $m \in \mathbb{N}$. (Thus $N_k(m) \neq 1$ for all $m \in \mathbb{N}$ if ar.d only if $\ell_k = \infty$. See Theorem 2.4.7 .)

(5.9) (**Conjecture**) Let $k \in \mathbb{N}$ be arbitrary, and let $0 < \epsilon < 1$. Then $N_k(m) > m^{1-\epsilon}$ for infinitely many $m$. (This is equivalent to Conjecture 3.3.15.).

(5.10) (**Conjecture**) Let $r_n$ be defined as in Definition 4.2.15. Then

$$\varliminf_{n\to\infty} \frac{r_n}{5^n} > 0 .$$

(5.11) Determine all $m \in \mathbb{N}$ for which $\varphi^*(x) = m$ has a unique solution.

# Bibliography


[Apo76] T.M. Apostol, *Introduction to analytic number theory,* New York: Springer-Verlag, 1976.

[Bak68] A. Baker, "Linear forms in the logarithms of algebraic numbers (IV)", *Mathematika,* **15**(1968), pp. 204-216.

[Car07] R.D. Carmichael, "On Euler's $\phi$ -function", *Bull. Amer. Math. Soc.,* **13**(1907), pp. 241-243.

[Car14] R.D. Carmichael, *The theory of numbers,* New York: Wiley, 1914, p. 36.

[Car22] R.D. Carmichael, "Note on Euler's $\phi$ -function", *Bull. Amer. Math. Soc.,* **28**(1922), pp. 109-110.

[Coh60] E. Cohen, "Arithmetical functions assoicated with the unitary divisors of an integer", *Math. Zeitschr.,* **74**(1960), pp. 66-80.

[Dic71] L.E. Dickson, *History of the theory of numbers,* Vol. I, New York: Chelsea, 1971.

[Don73] H. Donnelly, "On a problem concerning Euler's phi-function", *Amer. Math. Monthly.,* **80**(1973), pp. 1029-1031.

[Erd35] P. Erdös, "On the normal number of prime factors of $p-1$ and some related problems concerning Euler's $\varphi$-function, " *Quart. J. Math.* (Oxford Series) 6(1935), pp. 205-213.

[Erd45] P. Erdős, "Some remarks on Euler's $\varphi$-function and some related problems", *Bull. Amer. Math. Soc.,* **51**(1945), pp. 540-544.

[Erd56] P. Erdős, "On pseudoprimes and Carmichael numbers", *Publ. Math. Debrecen,* **4**(1956), pp. 201-206.

[Erd58] P. Erdős, "Some remarks on Euler's $\varphi$-function", *Acta Arith.,* **4**(1958), pp. 10-19.

[Erd73] P. Erdős and R.R. Hall, "On the values of Euler's $\varphi$-function", *Acta Arith.,* **22**(1973), pp. 201-206.

[Erd76] P. Erdős and R.R. Hall, "Distinct values of Euler's $\varphi$-function", *Mathematika,* **23**(1976), pp. 1-3.

[Gol69] M. Goldfeld, "On the number of primes p for which p+a has a large prime factor", *Mathematika,* **16**(1969), pp. 23-27.

[Gro73] E. Grosswald, "Contribution to the theory of Euler's function $\varphi(x)$", *Bull. Amer. Math. Soc.,* **79**(1973), pp. 337-341.

[Hal74] H. Halberstam and H.-E. Richert, *Sieve methods,* London: Academic Press, 1974.

[Hoo73] C. Hooley, "On the greatest prime factor of p+a", *Mathematika,* **20**(1973), pp. 135-143.

[Ism76] M. Ismail and M.V. Subbarao, "Unitary analogue of Carmichael's problem", *Indian J. Math.,* **18**(1976), pp. 49-55.

[Iwa80] H. Iwaniec, "On the Brun-Titchmarsh theorem and related questions", *Proc. Queen's Number Theory Conf. 1979,* ( P. Ribenboim ed. ), Kingston: Queen's Univ., 1980, pp. 67-78.

[Kle47] V.L. Klee, "On a conjecture of Carmichael", *Bull. Amer. Math. Soc.,* **53**(1947), pp. 1183-1186.

[Kle69] V.L. Klee, "Is there an $n$ for which $\phi(x) = n$ has a unique solution?", *Amer. Math. Monthly,* **76**(1969), pp. 288-289.

[Mai88] H. Maier and C. Pomerance, "On the number of different values of the Euler function", *Acta Arith.*, **49**(1988), pp. 263-275.

[Mas82] P. Masai and A. Valette, "A lower bound for a counterexample to Carmichael's conjecture", *Bollettino delta Unione Matematica Italiana*, Serie VI, **1-A**(1982), pp. 313-316.

[Nor76] K.K. Norton, "On the number of restricted prime factors of an integer I", *Ill. J. Math.*, **20**(1976), pp. 681-705.

[Phi88] P. Philippon and M. Waldschmidt, "Lower bounds for linear forms in logarithms", *New Advances in Transcendence Theory*, ( A. Baker ed. ), Cambridge Univ. Press, 1988, Chapter 18.

[Pil29] S.S. Pillai, "On some functions connected with $\varphi(n)$", *Bull. Amer. Math. Soc.*, **35**(1929), pp. 832-836.

[Pom74] C. Pomerance, "On Carmichael's conjecture", *Proc. Amer. Math. Soc.*, **43**(1974), pp. 297-298.

[Pom80] C. Pomerance, "Popular values of Euler's function", *Mathematika*, **27**(1980), pp. 84-89.

[Pom86] C. Pomerance, "On the distribution of the values of Euler's function", *Acta Arith.*, **47**(1986), pp. 63-70.

[Sch56a] A. Schinzel, "Sur l' équation $\varphi(x) = m$", *Elem. Math.*, **11**(1956), pp. 75-78.

[Sch56b] A. Schinzel, "Sur un problème concernant la fonction $\varphi(n)$", *Czechoslovak Math. J.*, 6(81)(1956), pp. 164-165.

[Sch61] A. Schinzel, "Remarks on the paper 'Sur certaines hyopthèses concernant les nombers premiers'", *Acta Arith.*, **7**(1961), pp. 1-8.

[Sch58] A. Schinzel and W. Sierpinski, "Sur certaines hyopthèses concernant les nombers premiers", *Acta Arith.*, 4(1958), pp. 185-208.

[Str82] R.J. Stroeker and R. Tijdeman, "Diophantine equations", *Computational methods in number theory,* Part II, Math. centre tracts, 155, Amsterdam: Math. Centrum, 1982, pp. 321-369.

[Sub87] M.V. Subbarao and L.W. Yip, " Carmichael's conjecture and some analogues", *Proc. International Number Theory Conf. at Univ. Laval 1987* (De Koninck and Levesque ed.), Berlin: Walter de Gruyter, 1989, pp. 928-941.

[Utz61] W.R. Utz, "A conjecture of Erdös concerning consecutive integers", *Amer. Math. Monthly,* **68**(1961), pp. 896-897.

[Woo79] K.R. Wooldridge, "Values taken many times by Euler's phi function", *Proc. Amer. Math. Soc.,* **76**(1979), pp. 229-234.

[You88] J. Young and D.A. Buell,"The twentieth Fermat number is composite", *Math. Comp.,* **50**(1988), pp. 261-263.

**Appendix I. The sequence $\{q_{2,n}\}_{1\leq n\leq 1000}$.**

| | | | | | |
|---|---|---|---|---|---|
| 1 | 3 | 5 | 7 | 17 | 19 |
| | 23 | 37 | 53 | 59 | 61 |
| 2 | 71 | 73 | 97 | 107 | 109 |
| | 113 | 163 | 179 | 181 | 257 |
| 3 | 293 | 307 | 347 | 349 | 359 |
| | 367 | 373 | 401 | 439 | 487 |
| 4 | 491 | 499 | 547 | 557 | 631 |
| | 751 | 773 | 797 | 853 | 881 |
| 5 | 883 | 887 | 907 | 971 | 1009 |
| | 1039 | 1049 | 1051 | 1097 | 1103 |
| 6 | 1123 | 1283 | 1297 | 1319 | 1321 |
| | 1495 | 1499 | 1607 | 1609 | 1637 |
| 7 | 1697 | 1699 | 1747 | 1787 | 1789 |
| | 1801 | 1867 | 1889 | 1997 | 1999 |
| 8 | 2039 | 2053 | 2111 | 2113 | 2137 |
| | 2393 | 2417 | 2437 | 2447 | 2557 |
| 9 | 2663 | 2687 | 2689 | 3011 | 3023 |
| | 3061 | 3079 | 3119 | 3121 | 3371 |
| 10 | 3373 | 3517 | 3623 | 3659 | 3761 |
| | 3803 | 3851 | 3853 | [illegible] | 4051 |
| 11 | 4073 | 4211 | 4397 | 4481 | 4483 |

**Appendix I**(*cont'd*).

| | | | | | |
|---|---|---|---|---|---|
| | 4507 | 5039 | 5099 | 5101 | 5197 |
| 12 | 5237 | 5387 | 5399 | 5413 | 5507 |
| | 5531 | 5569 | 5581 | 5669 | 5779 |
| 13 | 5807 | 5869 | 6037 | 6101 | 6197 |
| | 6199 | 6211 | 6337 | 6343 | 6449 |
| 14 | 6451 | 6529 | 6551 | 6553 | 6607 |
| | 6823 | 7253 | 7307 | 7309 | 7331 |
| 15 | 7333 | 7457 | 7459 | 7487 | 7489 |
| | 7523 | 7541 | 7621 | 7673 | 7681 |
| 16 | 7723 | 7741 | 7883 | 8069 | 8167 |
| | 8423 | 8443 | 8581 | 8641 | 8689 |
| 17 | 8737 | 9007 | 9221 | 9239 | 9241 |
| | 9293 | 9337 | 9437 | 9439 | 9467 |
| 18 | 9511 | 9619 | 10099 | 10267 | 10313 |
| | 10357 | 10453 | 10567 | 10687 | 10729 |
| 19 | 10799 | 10979 | 11251 | 11287 | 11411 |
| | 11447 | 11489 | 11491 | 11597 | 11699 |
| 20 | 11701 | 11867 | 11953 | 12101 | 12149 |
| | 12491 | 12511 | 12569 | 12583 | 12841 |
| 21 | 12853 | 12923 | 12973 | 13109 | 13217 |
| | 13219 | 13451 | 13523 | 13687 | 13729 |

**Appendix I**(*cont'd*).

| | | | | | |
|---|---|---|---|---|---|
| 22 | 14503 | 14779 | 15013 | 15031 | 15107 |
| | 15137 | 15139 | 15217 | 15299 | 15307 |
| 23 | 15551 | 15607 | 15619 | 15679 | 15737 |
| | 15739 | 15767 | 15773 | 16273 | 16547 |
| 24 | 16703 | 16741 | 16921 | 17047 | 17117 |
| | 17333 | 17387 | 17389 | 17443 | 17467 |
| 25 | 17551 | 17609 | 18169 | 18287 | 18289 |
| | 18311 | 18313 | 18451 | 18503 | 18593 |
| 26 | 18617 | 18719 | 18797 | 19013 | 19031 |
| | 19267 | 19457 | 19583 | 19661 | 19949 |
| 27 | 20219 | 20357 | 20359 | 20393 | 20593 |
| | 20611 | 20663 | 20681 | 20807 | 20809 |
| 28 | 20921 | 20947 | 20959 | 21149 | 21163 |
| | 21169 | 21191 | 21193 | 21391 | 21799 |
| 29 | 21821 | 21929 | 22031 | 22051 | 22073 |
| | 22391 | 22397 | 22469 | 22571 | 22573 |
| 30 | 22859 | 22861 | 23021 | 23039 | 23041 |
| | 23071 | 23209 | 23269 | 23581 | 23599 |
| 31 | 23873 | 23899 | 24071 | 24083 | 24107 |
| | 24109 | 24137 | 24379 | 24749 | 24781 |
| 32 | 24907 | 25349 | 25457 | 25601 | 25603 |

**Appendix I**(*cont'd*).

| | | | | | |
|---|---|---|---|---|---|
| | 25903 | 25919 | 26209 | 26449 | 26959 |
| 33 | 26987 | 27017 | 27067 | 27239 | 27241 |
| | 27647 | 27701 | 27743 | 27763 | 27847 |
| 34 | 28319 | 28403 | 28409 | 28411 | 28463 |
| | 28499 | 28513 | 28603 | 28817 | 28859 |
| 35 | 29129 | 29131 | 29167 | 29179 | 29269 |
| | 29347 | 29443 | 29587 | 29833 | 29947 |
| 36 | 30187 | 30293 | 30319 | 30497 | 30517 |
| | 30781 | 30803 | 30941 | 31139 | 31181 |
| 37 | 31183 | 31333 | 31481 | 31567 | 31667 |
| | 31687 | 31721 | 31723 | 31741 | 31751 |
| 38 | 32057 | 32059 | 32063 | 32183 | 32189 |
| | 32191 | 32237 | 32257 | 32401 | 32647 |
| 39 | 32939 | 32941 | 33037 | 33247 | 33487 |
| | 33749 | 33751 | 33791 | 33857 | 33863 |
| 40 | 34183 | 34469 | 34471 | 34631 | 34693 |
| | 34721 | 35099 | 35107 | 35317 | 35407 |
| 41 | 35437 | 35603 | 35897 | 35899 | 35923 |
| | 35969 | 36787 | 37447 | 37529 | 37571 |
| 42 | 37573 | 37607 | 37987 | 38201 | 38303 |
| | 38371 | 38561 | 38707 | 38839 | 38921 |

**Appendix I**(*cont'd*).

| | | | | | |
|---|---|---|---|---|---|
| 43 | 38923 | 38971 | 39079 | 39133 | 39209 |
| | 39439 | 39659 | 39671 | 40063 | 40111 |
| 44 | 40343 | 40591 | 40739 | 40813 | 41057 |
| | 41149 | 41183 | 41189 | 41479 | 41737 |
| 45 | 41893 | 41981 | 41983 | 42391 | 42667 |
| | 42709 | 42821 | 42943 | 43207 | 43403 |
| 46 | 43541 | 43543 | 43711 | 44389 | 44879 |
| | 45413 | 45491 | 45691 | 45887 | 45979 |
| 47 | 46153 | 46187 | 46237 | 46457 | 46589 |
| | 46591 | 46687 | 46817 | 46819 | 46853 |
| 48 | 47221 | 47303 | 47407 | 47497 | 47629 |
| | 48073 | 48497 | 48619 | 48623 | 48731 |
| 49 | 48733 | 48821 | 48823 | 49429 | 49523 |
| | 50111 | 50329 | 50333 | 50497 | 50599 |
| 50 | 50773 | 51137 | 51151 | 51461 | 51683 |
| | 51787 | 51913 | 52163 | 52201 | 52267 |
| 51 | 52673 | 52757 | 52807 | 52837 | 53161 |
| | 53323 | 53437 | 53479 | 53699 | 53987 |
| 52 | 54059 | 54347 | 54503 | 54581 | 54583 |
| | 54679 | 54869 | 54941 | 55207 | 55243 |
| 53 | 55259 | 55511 | 55949 | 56053 | 56237 |

**Appendix I**(*cont'd*).

| | | | | | |
|---|---|---|---|---|---|
| | 56239 | 56393 | 56417 | 56431 | 56437 |
| 54 | 56467 | 57041 | 57047 | 57173 | 57457 |
| | 57803 | 58193 | 58963 | 59233 | 59263 |
| 55 | 59387 | 59467 | 59497 | 59791 | 60457 |
| | 60497 | 60659 | 60661 | 60719 | 60737 |
| 56 | 61757 | 61781 | 61813 | 61991 | 62011 |
| | 62171 | 62423 | 62473 | 62617 | 62791 |
| 57 | 62873 | 63667 | 63761 | 64013 | 64283 |
| | 64399 | 64567 | 64661 | 64663 | 65053 |
| 58 | 65393 | 65537 | 65539 | 65543 | 65699 |
| | 65701 | 65707 | 65789 | 65957 | 66047 |
| 59 | 66067 | 66221 | 66271 | 66797 | 66919 |
| | 67153 | 67217 | 67219 | 67247 | 67271 |
| 60 | 67273 | 67409 | 67411 | 67607 | 68261 |
| | 68437 | 68743 | 69119 | 69623 | 69809 |
| 61 | 69991 | 70793 | 70979 | 70981 | 71233 |
| | 71347 | 71693 | 71699 | 72221 | 72223 |
| 62 | 72251 | 72253 | 72337 | 72383 | 73133 |
| | 73771 | 73859 | 73897 | 74623 | 74717 |
| 63 | 74719 | 74797 | 74887 | 75223 | 75703 |
| | 76213 | 76487 | 76537 | 76579 | 77351 |

**Appendix I**(*cont'd*).

| | | | | | |
|---|---|---|---|---|---|
| 64 | 77489 | 77491 | 77647 | 77711 | 77713 |
| | 77747 | 78173 | 78583 | 78623 | 78697 |
| 65 | 78857 | 78901 | 79349 | 79451 | 79973 |
| | 80341 | 80963 | 81013 | 81181 | 81197 |
| 66 | 81199 | 81203 | 81689 | 82499 | 82549 |
| | 83071 | 83231 | 83233 | 83537 | 83717 |
| 67 | 83719 | 85037 | 85103 | 85229 | 85237 |
| | 85297 | 85597 | 85847 | 86137 | 86201 |
| 68 | 86453 | 86579 | 86719 | 87337 | 87539 |
| | 87541 | 87803 | 88007 | 88037 | 88069 |
| 69 | 88469 | 88471 | 88667 | 88873 | 88897 |
| | 88997 | 89123 | 89371 | 89431 | 89501 |
| 70 | 89567 | 89959 | 90793 | 90847 | 91139 |
| | 91141 | 91151 | 91153 | 91237 | 91493 |
| 71 | 91957 | 92317 | 92507 | 92593 | 92717 |
| | 92761 | 92957 | 92959 | 92987 | 93083 |
| 72 | 93419 | 93637 | 94117 | 94321 | 94483 |
| | 94649 | 94651 | 94819 | 94933 | 95003 |
| 73 | 95063 | 95219 | 95287 | 95813 | 95857 |
| | 96179 | 96181 | 96289 | 96337 | 96731 |
| 74 | 96737 | 96739 | 96821 | 96823 | 97943 |

Appendix I(*cont'd*).

| | | | | | |
|---|---|---|---|---|---|
| | 98297 | 98299 | 98459 | 98479 | 98533 |
| 75 | 98897 | 98899 | 98953 | 99347 | 99349 |
| | 99581 | 99859 | 100103 | 100391 | 100393 |
| 76 | 100591 | 101197 | 101561 | 101573 | 101797 |
| | 101957 | 102259 | 102317 | 102367 | 102551 |
| 77 | 102811 | 102967 | 103307 | 103409 | 103991 |
| | 103993 | 104047 | 104471 | 104473 | 104597 |
| 78 | 105323 | 105751 | 105817 | 105907 | 105953 |
| | 105967 | 106217 | 106219 | 106261 | 106307 |
| 79 | 106411 | 106531 | 106957 | 106993 | 107123 |
| | 107137 | 107323 | 107693 | 107699 | 107713 |
| 80 | 108739 | 108887 | 108991 | 109097 | 109139 |
| | 109141 | 109741 | 110161 | 111409 | 111667 |
| 81 | 111779 | 111781 | 111857 | 112031 | 112337 |
| | 112339 | 112459 | 112589 | 112951 | 113117 |
| 82 | 113341 | 113381 | 113383 | 113783 | 113899 |
| | 113957 | 113963 | 114343 | 115331 | 115807 |
| 83 | 115831 | 116047 | 116663 | 116923 | 117023 |
| | 117167 | 117203 | 117239 | 117241 | 117809 |
| 84 | 117811 | 117917 | 117973 | 118057 | 118247 |
| | 118249 | 118297 | 118543 | 119503 | 119533 |

**Appendix I(*cont'd*).**

| | | | | | |
|---|---|---|---|---|---|
| 85 | 120011 | 120163 | 121333 | 121697 | 121711 |
| | 122219 | 122533 | 123209 | 123217 | 123269 |
| 86 | 123449 | 123551 | 123553 | 123737 | 124133 |
| | 124433 | 124471 | 124669 | 124799 | 125113 |
| 87 | 125117 | 125119 | 125207 | 125497 | 125617 |
| | 126001 | 126653 | 127247 | 127249 | 127447 |
| 88 | 127859 | 127873 | 127997 | 128629 | 128717 |
| | 128831 | 128833 | 129517 | 129587 | 129589 |
| 89 | 130211 | 130307 | 130337 | 130343 | 130409 |
| | 130411 | 130579 | 130631 | 130633 | 130969 |
| 90 | 131129 | 131293 | 131581 | 131707 | 132247 |
| | 132929 | 133169 | 133979 | 133981 | 134053 |
| 91 | 134161 | 134639 | 134857 | 134989 | 135271 |
| | 135431 | 135433 | 135571 | 136093 | 136207 |
| 92 | 136393 | 136403 | 137573 | 137771 | 137933 |
| | 138191 | 138461 | 138497 | 138563 | 138587 |
| 93 | 138617 | 138797 | 138799 | 138841 | 138937 |
| | 139291 | 139397 | 139487 | 140009 | 140057 |
| 94 | 140453 | 140639 | 141157 | 141461 | 141587 |
| | 141719 | 141931 | 142007 | 142057 | 142217 |
| 95 | 142223 | 142357 | 142501 | 142567 | 142939 |

**Appendix I(*cont'd*).**

| | | | | | |
|---|---|---|---|---|---|
| | 143159 | 143243 | 143281 | 144139 | 144247 |
| 96 | 144259 | 144583 | 144629 | 144847 | 145063 |
| | 145207 | 145637 | 145661 | 145753 | 145799 |
| 97 | 145879 | 145897 | 145903 | 146347 | 146449 |
| | 146563 | 146617 | 146701 | 147517 | 147547 |
| 98 | 147607 | 147937 | 148171 | 148339 | 148411 |
| | 148531 | 148537 | 148829 | 149269 | 150169 |
| 99 | 150721 | 150989 | 150991 | 151573 | 151597 |
| | 151687 | 151729 | 151799 | 151897 | 152197 |
| 100 | 152857 | 153313 | 153343 | 153449 | 153563 |
| | 153953 | 155137 | 155741 | 155809 | 156011 |

## Appendix II. The sequence $\{q_{6,n}\}_{1\leq n\leq 300}$.

| | | | | | |
|---|---|---|---|---|---|
| 1 | 7 | 13 | 19 | 97 | 103 |
| | 109 | 139 | 727 | 733 | 739 |
| 2 | 769 | 1423 | 1429 | 2647 | 5179 |
| | 9613 | 9619 | 9967 | 9973 | 10009 |
| 3 | 12907 | 13933 | 14323 | 14503 | 18493 |
| | 18583 | 25447 | 25453 | 27043 | 67339 |
| 4 | 74017 | 74887 | 76123 | 76129 | 79903 |
| | 80557 | 96697 | 96703 | 98407 | 100267 |
| 5 | 101527 | 101533 | 125053 | 129457 | 129499 |
| | 130087 | 178093 | 182653 | 182659 | 189307 |
| 6 | 189493 | 189949 | 190063 | 197803 | 198637 |
| | 213319 | 240883 | 272029 | 288529 | 352057 |
| 7 | 483499 | 522157 | 532867 | 541693 | 541699 |
| | 554707 | 676927 | 688813 | 875377 | 907549 |
| 8 | 970297 | 970303 | 973459 | 973537 | 981493 |
| | 1021663 | 1029697 | 1030933 | 1047247 | 1089679 |
| 9 | 1090333 | 1094293 | 1094299 | 1226959 | 1256989 |
| | 1278819 | 1319779 | 1325617 | 1335379 | 1389589 |
| 10 | 1446457 | 1493197 | 1530589 | 1561213 | 1797319 |
| | 1837249 | 1904167 | 1913437 | 1920013 | 1935859 |

**Appendix II.**(*cont'd*)

| | | | | | |
|---|---|---|---|---|---|
| 11 | 2015089 | 2016397 | 2016403 | 2016409 | 2019709 |
| | 2025553 | 2035549 | 2315683 | 2376013 | 2460373 |
| 12 | 2460487 | 2460919 | 2467783 | 2575537 | 2575543 |
| | 2575549 | 2773153 | 2796559 | 3383773 | 3537973 |
| 13 | 3537979 | 3544339 | 3611203 | 3750883 | 3758263 |
| | 3774109 | 3791899 | 3978043 | 4053067 | 4576669 |
| 14 | 4590007 | 4590013 | 6285493 | 6767599 | 6771673 |
| | 6796117 | 6814219 | 6926653 | 6934687 | 6934693 |
| 15 | 7042093 | 7211119 | 7216537 | 7216543 | 7263463 |
| | 7305817 | 7330693 | 7339303 | 7339309 | 7339957 |
| 16 | 7392403 | 7392409 | 7396657 | 7396663 | 7627717 |
| | 7636873 | 7660057 | 7660099 | 775059 | 77813453 |
| 17 | 7813459 | 8297413 | 8298067 | 8588719 | 8950339 |
| | 8954497 | 8955043 | 9186487 | 9238459 | 9347659 |
| 18 | 9460513 | 9460837 | 9538279 | 9544903 | 9727129 |
| | 9738763 | 9847543 | 9847549 | 9959797 | 10292059 |
| 19 | 10292173 | 10409299 | 10457287 | 10539979 | 10581937 |
| | 10584703 | 10584709 | 10622203 | 10713289 | 10714129 |
| 20 | 11148199 | 11837923 | 11837929 | 12560827 | 12568393 |
| | 12568399 | 12617863 | 13386067 | 13394023 | 13441723 |

**Appendix II.**(*cont'd*)

| | | | | | |
|---|---|---|---|---|---|
| 21 | 13551019 | 13616947 | 13621627 | 13692937 | 13728409 |
| | 13732843 | 14110819 | 14114869 | 14115397 | 14174257 |
| 22 | 14174263 | 14183047 | 14216509 | 15976027 | 16043389 |
| | 16275733 | 17223373 | 17223379 | 17232949 | 17243437 |
| 23 | 17295739 | 17561953 | 17717929 | 18021217 | 18064663 |
| | 18075427 | 18280723 | 18358129 | 18362203 | 18369187 |
| 24 | 18380827 | 18435649 | 18495613 | 18497209 | 18504337 |
| | 18648373 | 18802387 | 18803947 | 19178503 | 19412143 |
| 25 | 19412149 | 19419523 | 19419529 | 19568749 | 19575877 |
| | 19587619 | 19738783 | 19743067 | 19897663 | 19897699 |
| 26 | 19909837 | 19910263 | 20550757 | 20634469 | 20704447 |
| | 20716873 | 20724793 | 20796073 | 21651439 | 21920359 |
| 27 | 23312227 | 23319679 | 23433169 | 23884243 | 24293653 |
| | 24765859 | 24810337 | 24874687 | 24882643 | 25078657 |
| 28 | 25176937 | 25389607 | 26307847 | 26322853 | 26322859 |
| | 26402083 | 26402197 | 26417929 | 26435077 | 26446183 |
| 29 | 26543299 | 27610549 | 27878563 | 28382377 | 28382383 |
| | 28855249 | 32036689 | 32130013 | 33416857 | 33416863 |
| 30 | 33416869 | 33481909 | 33482143 | 34087393 | 34149067 |
| | 36179863 | 36210583 | 36261259 | 36355273 | 36480253 |

**Appendix III. The sequences $\{q_{k,n}\}_{n\geq 1}$, $6 < k < 1000$.**

| $k$ | $\ell_k$ | $\{q_{k,n}\}_{n\geq 1}$ |
|---|---|---|
| 18 | 2 | 19, 37. |
| 30 | 2 | 31, 61. |
| 36 | $\geq 11$ | 37, 73, 109, 7993, 295777, 21589129, 32239729, 798797809, 798893713, 798893749, 2353215097 |
| 78 | 2 | 79, 157. |
| 96 | 2 | 97, 193. |
| 138 | 2 | 139, 277. |
| 156 | 3 | 157, 313, 49297. |
| 198 | $\geq 8$ | 199,397,79201,79399,15761197,1245181846789, 495576117748207,496815942399589 |
| 210 | $\geq 13$ | 211, 421, 631, 89041, 133351, 265861, 56052571, 56185081, 111927691, 111927901, 11827092691, 17754485701, 35369172511. |
| 228 | 2 | 229, 457. |
| 270 | 3 | 271, 541, 811. |
| 306 | $\geq 8$ | 307, 613, 919, 282439, 86709079, 159111163639, 137963337697399052S3, 1267883073439097292781З. |
| 330 | $\geq 8$ | 331, 661, 991, 1321, 865322701, 865323031, 571978523821, 189324819074821. |
| 336 | 6 | 337, 673, 1009, 340369, 231129952369, 786694707578844 97. |

**Appendix III**(*cont'd*).

| $k$ | $\ell_k$ | $\{q_{k,n}\}_{n\geq 1}$ |
|---|---|---|
| 366 | 3 | 367, 733, 269377. |
| 378 | 4 | 379, 757, 287281, 82421781121. |
| 438 | 2 | 439, 877. |
| 498 | 2 | 499, 997. |
| 546 | 2 | 547, 1093. |
| 576 | 5 | 577, 1153, 665857, 666433, 2952178304148O6337. |
| 600 | 4 | 601, 1201, 1801, 1299964201. |
| 606 | 2 | 607, 1213. |
| 618 | 4 | 619, 1237, 766321, 766939. |
| 660 | 2 | 661, 1321. |
| 690 | 2 | 691, 1381. |
| 726 | 3 | 727, 1453, 2179. |
| 810 | 4 | 811, 1621, 1315441, 1316251. |
| 828 | 3 | 829, 1657, 1374481. |
| 876 | 2 | 877, 1753. |
| 936 | 3 | 937, 1873, 1755937. |
| 966 | 2 | 967, 1933. |
| 996 | 2 | 997, 1993. |