PROBLEMS IN ALGORITHMIC NUMBER THEORY

by

S. V. NAGARAJ

A THESIS IN COMPUTER SCIENCE

Submitted to the University of Madras in partial fulfillment of
the requirement for the degree of Doctor of Philosophy

MARCH 1999

The Institute of Mathematical Sciences
C.I.T. Campus, Tharamani
Chennai (Madras), Tamilnadu - 600 113, INDIA

CERTIFICATE

This is to certify that the Ph.D. thesis titled **Problems in algorithmic number theory** submitted to the University of Madras by S V NAGARAJ is a record of bonafide research work done under my supervision. The research work presented in this thesis has not formed the basis for the award to the candidate of any Degree, Diploma, Associateship, Fellowship or other similar titles.

It is further certified that the thesis represents independent work by the candidate and collaboration when existed was necessitated by the nature and scope of problems dealt with.

Dr. Venkatesh Raman

March 1999

Thesis Supervisor

THE INSTITUTE OF MATHEMATICAL SCIENC
C.I.T. CAMPUS, MADRAS-600 113.

The Institute of Mathematical Sciences
C.I.T. Campus, Tharamani
Chennai (Madras), Tamilnadu - 600 113

Abstract

This thesis presents new results for four problems in the field of algorithmic and computational number theory.

The first gives an improved analysis of algorithms for testing whether a given positive integer n is a perfect power. Bach and Sorenson gave two algorithms for this problem with average running time $O(\log^2 n)$ under the assumption that n is chosen uniformly from an interval of length at least $(\log n)^{3 \log \log \log n}$. They conjectured that the interval length L can be reduced to polynomial size. We solve their conjecture by modifying their algorithms to reduce the interval size to $L \geq (\log n)^{30}$.

The second comes very close to settling a conjecture of A. Granville. He conjectured that the number of Carmichael numbers up to x with three prime factors, $C_3(x)$ is $O(x^{1/3+o(1)})$. We show that $C_3(x)$ is $O(x^{5/14+o(1)})$. This gives an improved upper bound on the worst case numbers for a variant of the strong pseudo-prime test.

The third result is about progress towards a conjecture of S. W. Graham. He conjectured that $C_3(x)$ is $\leq \sqrt{x}$. We show that his conjecture is true for $x \leq 10^{18}$ and $x \geq 2 * 10^{40}$ improving on his result of $x \leq 10^{16}$ and $x > 10^{126}$.

The fourth deals with the problem of finding the least witness $w(n)$ of a composite number n. A number w is a witness for a composite number n if n is not a strong pseudo-prime to the base w. We show except for Carmichael numbers of the form $n = pqr$ with $\nu_2(p-1) = \nu_2(q-1) = \nu_2(r-1)$ (see section 1.3 for the definition of ν_2) we have $w(n) = O(n^{1/(8\sqrt{e})+o(1)})$ for every composite n. For the exceptional numbers we also conjecture $w(n) = O(n^{1/(8\sqrt{e})+o(1)})$. We present other interesting algorithmic results about witnesses.

Acknowledgments

I am greatly indebted to Dr. Venkatesh Raman for his guidance even during my Masters program and for taking a personal interest in my research and guiding me. I thank him for the freedom he gave me to pursue research topics of my interest and to collaborate with Prof R. Balasubramanian. I thank him for stimulating me with his algorithms expertise.

This thesis would not have been possible without the many suggestions of Prof. R. Balasubramanian. Though he was often very busy; he was very kind to permit me to collaborate with him and gave me the opportunity to learn how to tackle unsolved problems. Learning from a leading authority has been beneficial to me.

I also thank my other teachers at the Institute of Mathematical Sciences, Drs. V. Arvind, K. Lodaya, M. Mahajan, R. Ramanujam and A. Seth for guiding me in my research and giving me helpful suggestions. I thank Dr. K. V. Subrahmanyam of the doctoral committee.

This research has been possible due to the Research Fellowship offered by the Institute of Mathematical Sciences. I acknowledge use of the various excellent facilities provided by the Institute. I am thankful to the Institute Director and other staff members who have encouraged me and helped me in various ways.

I am thankful to experts in disciplines related to my research who have helped me in several ways providing comments, suggestions, and their articles. I specially thank Profs. E. Bach, R. Burthe, A. Granville, D. R. Heath-Brown, R. Peralta, C. Pomerance, J. Sorenson and others.

Contents

Chapter 1

Introduction

This thesis presents new results for four problems in algorithmic and computational number theory.

Number theory has a long history of over two millenia. Its focus is on the properties of the natural numbers and problems that arise in their study. Since 1977, when Rivest, Shamir and Adleman [55] introduced the RSA public key cryptosystem based on the apparently intractable problem of integer factorization, there has been a lot of research on the algorithmic complexity of problems in number theory. Some of these problems like the problem of factoring an integer into its prime factors have been well known and studied since the time of Euclid. However a lot of insight into these problems has been gained only recently [36].

It is no surprise that many of the modern encryption techniques used in practice depend on the present intractability of problems in number theory such as integer factorization and computing discrete logarithms [26]. Hence the study of number-theoretic algorithms becomes interesting in theory and useful in practice.

Several problems in algorithmic number theory that currently have only exponential / sub-exponential time deterministic algorithms have efficient polynomial time algorithms when analyzed assuming the as yet unproved Generalized Riemann Hypothesis (GRH) (see [3]). One result of ours makes use of this hypothesis.

In this thesis we look at four problems in algorithmic and computational number theory and present new results for them.

We present

- an improved analysis of two algorithms due to Bach and Sorenson [12] for testing whether a given positive integer is a perfect power assuming the Generalized Riemann Hypothesis (GRH), thereby solving a conjecture due to them.
- an improved upper bound on the number of Carmichael numbers up to x with three prime factors, thereby making progress towards a conjecture of A. Granville (see [50]).
- progress towards a conjecture of S. W. Graham [29] on Carmichael numbers up to x with three prime factors.
- bounds for the least witness of a composite number without assuming the GRH.

1.1 Overview of the thesis

This thesis presents new results related to four problems in algorithmic and computational number theory.

Chapter 2 deals with algorithms for testing whether a given positive integer n is a perfect power. An integer n is a perfect power if there are integers $x, k \geq 2$ such that $n = x^k$. Bach and Sorenson [12] gave two algorithms for this problem. Their algorithms had an average running time of $O(\log^2 n)$ under the assumption that n is chosen uniformly from an interval of length L where $L \geq (\log n)^{3 \log\log\log n}$. They conjectured that the interval length can be reduced to polynomial size. We solve their conjecture by suitably modifying their algorithms to reduce the interval length to $L \geq (\log n)^{30}$. Our algorithms assume the Generalized Riemann Hypothesis (GRH). These results have appeared in [13].

Chapter 3 deals with the problem of finding an improved upper bound on the number $C_3(x)$ of Carmichael numbers up to x with three prime factors. A positive integer n is a *Carmichael number* (see [39] for definitions) if and only if n is square-free and $p-1$ properly divides $n-1$ for every prime factor p of n. Carmichael numbers occur in the study of algorithms for determining the prime or composite nature of a positive integer. A. Granville (see [50]) has conjectured that $C_3(x) = O(x^{1/3+o(1)})$. We come very close to settling his conjecture by showing $C_3(x) = O(x^{5/14+o(1)})$ for sufficiently large x. These results are presented in [14]. As an application we also show that our result gives an improved upper bound on the worst case numbers of a variant of the *strong pseudo-prime test* (see Chapter 5 for definition). The reader is referred to A. Granville's review of our paper [14] in [34] and also to his notes in [33] on our method.

Chapter 4 describes progress towards a conjecture of S. W. Graham [29]. He conjectured that the number $C_3(x)$ of Carmichael numbers up to x with three prime factors is $\leq \sqrt{x}$. He showed that his conjecture is true for $x \leq 10^{16}$ and $x > 10^{126}$. We improve his result by showing that his conjecture is true for $x \leq 10^{18}$ and $x \geq 2 * 10^{40}$. In both cases analytical methods establish the conjecture for large x and tables of Carmichael numbers [48, 49] are used for small x.

Chapter 5 deals with the problem of finding the least witness $w(n)$ of a composite number n (see [7, 22]). A number w is a *witness* for a composite number n if n is not a strong pseudo-prime [39] to the base w. We show $w(n) = O(n^{1/(8\sqrt{e})+o(1)})$ for all composite numbers n except Carmichael numbers of the form $n = pqr$ with $\nu_2(p-1) = \nu_2(q-1) = \nu_2(r-1)$ (see section 1.3 for the definition of ν_2). For the exceptional numbers we conjecture $w(n) = O(n^{1/(8\sqrt{e})+o(1)})$.

1.2 Background for the thesis

In this thesis we give only important definitions. The reader is referred to survey articles [3, 9, 26, 36] and text books [11, 39] for further information about problems in algorithmic number theory.

For describing our results we make use of terms such as the Generalized Riemann Hypothesis, Chinese Remainder Theorem, sieve of Eratosthenes, sieve methods, Carmichael numbers, witness of a composite number, strong pseudo-prime test, character sum estimates. Almost all of these can be found in standard text books [11, 35, 39, 54] and expository articles [3, 9, 26]. For brevity, we don't include proofs of specialized lemmas found in original papers.

1.3 Notation

The following notation will be used in the thesis. If Q is a prime number then $\nu_Q(p-1)$ denotes the highest power of Q that divides $p-1$. The Extended Riemann Hypothesis (ERH) is the Riemann Hypothesis applied to Dirichlet L-functions [28]. $\pi_p(x)$ denotes the number of primes that are at most x and congruent to 1 mod p. GRH denotes the Generalized Riemann Hypothesis. Let f and g be real-valued functions. We say $f = O(g)$ if there exists an absolute constant $c > 0$ such that $f(x) < c.g(x)$ for all $x > x_0$. $f = \Theta(g)$ if $f = O(g)$ and $g = O(f)$. $f = o(g)$ if $\lim_{x \to \infty} f(x)/g(x) = 0$. If O or o is subscripted by a variable, for example $f = O_\epsilon(g)$, then the implied constant is a function of that variable.

Chapter 2

Perfect Power Testing

2.1 Introduction

In this chapter we analyze two algorithms due to Bach and Sorenson [12] for testing whether a given positive integer is a perfect power and solve a conjecture made by them. The results presented here have appeared in [13].

A positive integer n is a *perfect power* if there exist integers $x, k \geq 2$ such that $n = x^k$. The simplest algorithm for testing whether n is a perfect power involves trying all possible powers; it has a time complexity of $O(\log^3 n \log\log n)$. The time can be reduced to $O(\log^3 n \log\log\log n)$ by trying only prime values of k. Bach and Sorenson [12] further reduce the time to $O(\log^3 n)$ by using a modification of Newton's method for finding roots. The average and worst-case running times of these algorithms are the same. Bach and Sorenson [12] develop an algorithm. They prove that if n is chosen uniformly from an interval of length L, $L \geq (\log n)^{3 \log\log\log n}$ then the running time of their algorithm averaged over all inputs in L is $O(\log^2 n)$ (given a *sieve table* of certain small precomputed primes). They also improve the average running time to $O(\log^2 n / \log^2 \log n)$ by incorporating trial division. We modify their algorithms to reduce the interval size to $L \geq (\log n)^{30}$, while preserving the average running time.

The *sieve table*, which requires $O(\log n)$ space can be quickly constructed. The

Extended Riemann Hypothesis is used to bound the largest prime in the table. The following idea is used in the algorithms. Let p be a prime. If n is not a p^{th} power mod q for some small prime q, then it cannot be a p^{th} power. The time needed to check this condition is much less than the time needed to compute a p^{th} root of n to high precision. The disadvantage of this approach is that a p^{th} power mod q need not be a p^{th} power. Hence, tests using more than one q are necessary. Enough tests are done to ensure that p^{th} root computations are rare.

2.2 Assumptions

Following Bach and Sorenson [12], we assume that classical methods are used for arithmetic on large numbers and note only that the asymptotic time complexity of the algorithms gets improved if faster methods such as the Schönhage-Strassen [56] algorithm are used. Hence, the complexity of basic arithmetic is:

- Computing ab or $a \bmod b$: $O(\log a \log b)$ time
- Computing $a \pm b$: $O(\log a + \log b)$ time
- Computing $c = a^b$: $O(\log^2 c)$ time
- Computing $a^b \bmod m$: $O(\log a \log m + \log b \log^2 m)$ time

2.3 The sieve idea of Bach and Sorenson

Many numbers are not perfect powers, so we must quickly reject non-perfect powers. The following lemma is the basis of this idea.

Lemma 2.3.1 *If p and q are primes with $q \equiv 1 \bmod p$ and n is a perfect p^{th} power and* $\gcd(n,q) = 1$, *then* $n^{(q-1)/p} \equiv 1 \bmod q$.

If $n^{(q-1)/p} \not\equiv 1 \bmod q$, then n cannot be a perfect p^{th} power (assuming that all other conditions of the lemma are satisfied). If $n^{(q-1)/p} \equiv 1 \bmod q$ then, n need not be a perfect p^{th} power, so tests with more than one q are needed. The number of these tests must be chosen so that not many non-perfect powers pass all the tests and not too many of them are performed. The computation of $n^{(q-1)/p} \bmod q$ in the lemma is called a *sieve test*, and the prime modulus q is called the *sieve modulus*.

The following algorithm, due to Bach and Sorenson [12], is based on the above idea.

Algorithm A

```
{Bach and Sorenson's algorithm for testing if $n$ is a perfect power}

For each prime $p \le \log n$:
  Perform up to $R_p = \lceil 2 \log\log n / \log p \rceil$ different sieve
    tests on $n$, stopping when $n$ fails a test;
  If $n$ passed all the tests then,
    If $n = \lfloor n^{1/p} \rfloor^p$ then accept and halt;
Reject and halt
```

The following results of Bach and Sorenson [12] assume the Extended Riemann Hypothesis.

Lemma 2.3.2 [ERH] For any input ≤ n to algorithm A , the largest sieve modulus needed is $O(\log^2 n \log^4 \log n)$.

Lemma 2.3.3 [ERH] Let integer n be chosen uniformly from an interval of length L and assume, for every such n, $L \ge (\log n)^{3 \log\log\log n}$. Then the probability that n passes $\lceil 2 \log\log n / \log p \rceil$ different sieve tests for a fixed p in algorithm A is bounded above by $O(\log\log n / \log^2 n)$.

Theorem 2.3.4 [ERH] Let n, L be as in lemma 2.3.3 and assume that a sieve table is available. Then the running time of algorithm A averaged over all inputs in L is $O(\log^2 n)$.

The *sieve table* is a table of the first $R_p = \lceil 2 \log \log n / \log p \rceil$ sieve moduli for each prime $p \leq \log n$. The number of entries in this table is $O(\log n / \log \log n)$ and the total space used is $O(\log n)$. The sieve of Eratosthenes or its variants may be used to construct the table in $O(\log^{2+\epsilon} n)$ time for some small constant $\epsilon > 0$. Since we will be interested only in the average case analysis under the assumption that the table is available, the computation time for this table is not important. However we note that it is efficient in practice.

By incorporating trial division in algorithm A, Bach and Sorenson [12] reduce the average running time to $O(\log^2 n / \log^2 \log n)$. We don't describe this algorithm here.

2.4 Our algorithm and its analysis

Bach and Sorenson's proof of lemma 2.3.3 uses the Chinese Remainder Theorem. We modify algorithm A, use Montgomery's large sieve estimate [28] instead, giving algorithm B below. The correctness of Algorithm B follows from Lemma 2.3.1.

Algorithm B

```
{Our algorithm for testing if $n$ is a perfect power}

For each prime $p \leq \log n$:
    If $p \leq \sqrt{\log \log n}$ then do up to $(\log n)^{3/4}$ sieve tests on $n$;
    If $p > \sqrt{\log \log n}$ then do up to $R_p = \lceil 2 \log \log n / \log p \rceil$ sieve tests on $n$;
    If $n$ passed all the tests then:
        If $n = \lfloor n^{1/p} \rfloor^p$, then accept and halt;
Reject and halt
```

Montgomery's large sieve estimate [28] gives an upper bound on the number of integers that remain in an interval of length L after $f(q)$ different residue classes mod q have been removed for each prime q. The upper bound is $(L + Q^2)/S(Q)$, where $S(Q) = \sum_{x \le Q} \mu^2(x) \prod_{q|x} f(q)/(q - f(q))$ and $\mu^2(x) = 1$ if and only if x is square-free. To minimize the bound, Q is usually chosen to be about $\sqrt{L}$.

We now show that the results hold for an interval L of polynomial size.

Lemma 2.4.1 Let p be a prime $\le \log n$. Let $R_p = (\log n)^{3/4}$ if $p \le \sqrt{\log\log n}$ and $R_p = \lceil 2\log\log n/\log p \rceil$ if $\sqrt{\log\log n} < p \le \log n$. Let $L \ge \log^{30} n$. Then, the number of n passing all R_p different sieve tests is $O(L/\log^2 N)$ if n is chosen from an interval of length L.

In the course of proving this lemma, we use the following lemma. It makes use of known results [25] for a number-theoretic function $\Psi(X, Y)$. Function $\Psi(X, Y)$ is the number of integers $\le X$ all of whose prime factors are $\le Y$. A good reference for this function is [38].

Lemma 2.4.2 The number of square-free integers $\le X$ having all prime factors $\le X^{1/4}$ is a positive fraction, $c_3 X$, of X.

Proof. The number of integers $\le X$ having all prime factors $\le X^{1/4}$ is known [25] to be $\Psi(X, X^{1/4}) \asymp \rho(4)X$ where $\rho(4) > 0$ is a constant. Function ρ is called the Dickman-DeBruijn function [25].

Let B be a very large but fixed number. If a number is not square-free then either it is divisible by a square k^2 with $1 < k < B$ or $k \ge B$. The number of such numbers in the second category up to X is bounded by X/B. Choose B so that $1/B < \rho(4)/100$. For every number k in the first category, the number of numbers up to X is at most $\Psi(X/k^2, X^{1/4})$. This is asymptotic to $(\rho(4) + O(1/\log X))X/k^2$ [25]. The sum of $1/k^2$ for $1 < k < B$ is a positive number less than 1. Hence, among the integers counted by $\Psi(X, X^{1/4})$, the fraction that are not square-free is a fraction, say c_2X, of $\rho(4)X$. This leaves a positive fraction, say c_3X, of $\rho(4)X$ that are square-free. □

We also require the following bound under ERH, on the j^{th} prime $q_j \equiv 1 \bmod p$ for a fixed prime $p \leq \log n$, where $1 \leq j \leq R_p$.

Lemma 2.4.3 [ERH] *Let $1 \leq j \leq R_p$. The j^{th} prime $q_j \equiv 1 \bmod p$ satisfies $q_j = O((p^2 \log^5 p)(j \log j))$.*

Proof. We use a result of Titchmarsh [58], as stated in Bach and Sorenson [12]: Assume the ERH. Let x be a positive integer and let p be a prime. There is a constant $A > 0$ independent of p and x such that

$$\pi_p(x) \quad \geq \quad \frac{1}{p-1}\int_2^x \frac{dt}{\ln t} - A\sqrt{x}\ln x.$$

From this result it follows that

$$\pi_p(x) \quad \geq \quad \frac{1}{p-1}\frac{x}{\ln x}(1 - O(\frac{\ln^2 C}{\sqrt{C}}))$$

if $x = Cp^2 \log^4 p$, since $\int_2^x dt/\ln t \geq (x-2)/\ln x$, $1/x \leq 1/C$, $\ln x/\log p \leq \ln C + 6$.

Let T be the set of sieve moduli from the sieve table of a fixed prime $p \leq \log n$ and let $C = O(\log p \mid T \mid \log \mid T \mid)$. Then $C \to \infty$ as $n \to \infty$, since $\mid T \mid = R_p = (\log n)^{3/4}$ if $p \leq \sqrt{\log\log n}$ and $\mid T \mid = R_p = \lceil 2\log\log n/\log p \rceil$ if $\sqrt{\log\log n} < p \leq \log n$. Therefore,

$$\pi_p(x) \quad \geq \quad \frac{x(1-o(1))}{p\ln x} \quad \geq \quad (p\log^4 p) \mid T \mid \quad > \quad \mid T \mid$$

for sufficiently large n. Hence, the largest sieve modulus in T is at most $x = O((p^2 \log^5 p)(\mid T \mid \log \mid T \mid))$. Since $1 \leq j \leq R_p = \mid T \mid$, the j^{th} prime $q_j \equiv 1 \bmod p$ satisfies $q_j = O((p^2 \log^5 p)(j \log j))$. □

We now prove lemma 2.4.1.

Proof of Lemma 2.4.1. We note that $f(q) = q - (q-1)/p$ for our problem and

$$\begin{aligned} S(Q) &= \sum_{x \le \sqrt{L}} \mu^2(x) \prod_{q|x} \frac{f(q)}{q - f(q)} \\ &= \sum_{x \le \sqrt{L}} \mu^2(x) \prod_{q|x} \frac{q-(q-1)/p}{(q-1)/p} \\ &> \sum_{x \le \sqrt{L}} \mu^2(x) \prod_{q|x} \frac{q-1-(q-1)/p}{(q-1)/p} \\ &= \sum_{x \le \sqrt{L}} \mu^2(x) \prod_{q|x} (p-1) \\ &= \sum^{*}_{x \le \sqrt{L}} (p-1)^{\omega(x)} \end{aligned}$$

where $\omega(x)$ denotes the number of different prime factors of x and the $*$ on the summation sign denotes that we are summing over all the sub-products of $\{q_1, q_2, \cdots, q_{R_p}\}$ that are $\le \sqrt{L}$.

We divide the analysis for $S(Q)$ into two cases: $p \le \sqrt{\log\log n}$ and $p > \sqrt{\log\log n}$.

Case (i) $p \le \sqrt{\log\log n}$. We show that there are sufficiently many sub-products x of $\{q_1, q_2, \cdots, q_{R_p}\}$ that are $\le \sqrt{L}$, so $S(Q) > c\log^3 n$, where c is a positive constant.

We know under ERH, from Lemma 2.4.3, that the j^{th} prime $q_j \equiv 1 \bmod p$ satisfies $q_j = O((p^2 \log^5 p)(j \log j))$ for $1 \le j \le R_p$. Since the j^{th} ordinary prime λ_j is asymptotic to $j \ln j$, q_j is $O(p^3 \lambda_j)$ for a fixed prime $p \le \log n$.

Let $X = \log^3 n$. Suppose $q_{a_1} \cdots q_{a_J}$ is a sub-product of $q_1 \cdots q_{R_p}$ such that $q_{a_1} \cdots q_{a_J} \le \sqrt{L}$. Then $q_{a_1} \cdots q_{a_J} < \lambda_{a_1} \cdots \lambda_{a_J} p^{3J}$. Suppose we are choosing $\lambda_{a_1} \cdots \lambda_{a_J}$ such that $\lambda_{a_1} \cdots \lambda_{a_J} < \log^3 n$. Then $p^{3J} < \log^{12} n$ if $\lambda_{a_1} \cdots \lambda_{a_J} p^{3J} < \sqrt{L} = (\log n)^{15}$. Therefore $J < 4 \log\log n$. Hence, if we show that there are enough numbers less than $\log^3 n$ that have less than $\log\log n$ different prime factors, then we can get an estimate for $S(Q)$. For this purpose, consider the numbers $\le X$ and omit those having a prime factor $> X^{1/4}$. Lemma 2.4.2 states that a positive fraction, $c_3 X$, of these numbers are square-free. Hence $S(Q) > c_3 X = c_3 \log^3 n$.

Case (ii) $p > \sqrt{\log\log n}$. Let $m = q_1 \cdots q_{R_p}$. Then we know from Lemma 2.4.3 that under ERH $q_{R_p} = O((p^2 \log^5 p)(R_p \log R_p))$

$$\begin{aligned}
m &< (q_{R_p})^{R_p} \\
&= O(((p^2 \log^5 p)(R_p \log R_p))^{R_p}) \\
&= O((p^3 R_p^2)^{R_p}) \\
&= O((p^7)^{R_p}) \text{ since } R_p \text{ is } O(p^2) \\
&= O(\log^{14} n) \text{ since } R_p = \lceil 2 \log\log n / \log p \rceil .
\end{aligned}$$

Since

$$\begin{aligned}
S(Q) &> \dot{\sum_{x \le \sqrt{L}}} (p-1)^{\omega(x)} \\
&= \dot{\sum_{x \le \log^{15} n}} (p-1)^{\omega(x)} \\
&= \dot{\sum_{x \le q_1 \cdots q_{R_p} = O(\log^{14} n)}} (p-1)^{\omega(x)} \\
&= \sum_{0 \le \lambda \le R_p} \binom{R_p}{\lambda} (p-1)^{\lambda} \\
&= (1 + (p-1))^{R_p} \\
&= p^{R_p} = \log^2 n
\end{aligned}$$

we get, considering both cases, $L/S(Q) = O(L/\log^2 n)$. □

As a corollary, we obtain the following result, which is similar to Lemma 2.3.3.

Corollary 2.4.4 Let $n > 0$ be chosen uniformly from an interval of length L and assume for every such n, $L \geq \log^{30} n$. Then the probability that n passes R_p different sieve tests for a fixed exponent p in algorithm B is bounded above by $O(1/\log^2 n)$, where $R_p = (\log n)^{3/4}$ if $p \leq \sqrt{\log\log n}$ and $R_p = \lceil 2 \log\log n / \log p \rceil$ if $\sqrt{\log\log n} < p \leq \log n$.

Using this result we obtain a theorem similar to Theorem 2.3.4. The proof of our theorem is similar to that for Theorem 4.4 in Bach and Sorenson [12].

Theorem 2.4.5 [ERH] Let n, L be as in Corollary 2.4.4 and assume that a sieve table is available. Then the running time of Algorithm B, averaged over all the inputs in L, is $O(\log^2 n)$.

Proof. To get an upper bound on the running time, assume that all possible sieve tests are performed. From Lemma 2.4.3, it follows that $\log q = O(\log\log n)$ for $p \leq \sqrt{\log\log n}$ and $j \leq (\log n)^{3/4}$ and also for $\sqrt{\log\log n} < p \leq \log n$ and $j \leq \lceil 2\log\log n/\log p\rceil$. Since the sieve table is precomputed, the time to find each sieve modulus q is $O(1)$. Computing $n^{(q-1)/p} \bmod q$ can be done using one division and then one modular exponentiation in time $\log n \log q + \log^3 q = O(\log n \log\log n)$. If $p \leq \sqrt{\log\log n}$ and all the $R_p = (\log n)^{3/4}$ sieve tests are performed, the total time spent is at most $O((\log n)^{7/4}\log\log n)$ for each prime exponent p. If $\sqrt{\log\log n} < p \leq \log n$ and all the $R_p = \lceil 2\log\log n/\log p\rceil$ sieve tests are performed, the total time spent is at most $O(\log n \log^2 \log n/\log p)$ for each prime exponent p.

The average time spent in computing the p^{th} power of an approximate p^{th} root of n is $O(\log^2 \log n)$, as in the proof of theorem 4.4 of Bach and Sorenson [12].

For each prime exponent p, the average time spent is $O((\log n)^{7/4}\log\log n)$ for $p \leq \sqrt{\log\log n}$ and $O(\log n \log^2\log n/\log p)$ for $\sqrt{\log\log n} < p \leq \log n$. Hence, the average running time is

$$\sum_{p\leq\sqrt{\log\log n}} O((\log n)^{7/4}\log\log n) + \sum_{\sqrt{\log\log n}<p\leq\log n} O(\log n \log^2\log n/\log p)$$
$$= O((\log n)^{7/4+o(1)}) + O(\log^2 n) = O(\log^2 n).$$

We have used the fact that $\sum_{p\leq\log n} 1/\log p = O(\log n/\log^2\log n)$. □

Thus, increasing the R_p from $\lceil 2\log\log n/\log p\rceil$ to $(\log n)^{3/4}$ for $p \leq \sqrt{\log\log n}$ has not affected the running time. This is because many tests are performed for small values of p, which are not time consuming. The space used by Algorithm B can be shown to be the same as for Algorithm A, i.e. $O(\log n)$.

Bach and Sorenson [12] improved the average time of algorithm A to $O(\log^2 n/\log^2\log n)$ by incorporating trial division by small primes. Their trial division bound b satisfies $b = \Theta(\log n/\log^2\log n)$. Our modification to algorithm A, by performing $R_p = (\log n)^{3/4}$ sieve tests for $p \le \sqrt{\log\log n}$ and $R_p = \lceil 2\log\log n/\log p\rceil$ sieve tests for $\sqrt{\log\log n} < p \le \log n$, reducing the interval size L to $L \ge (\log n)^{30}$ works even in this case. The proof given by them for the improved algorithm needs only one change. They use a large sieve estimate of Jurkat and Richert to get an upper bound on the probability that no prime below b divides n where n is an integer chosen from an interval of length L. The upper bound obtained on the probability of escaping trial division is $O(1/\log b)$. This estimate requires that b, L satisfy the condition $\log b \le (\log L)/(2\log\log(3L))$. This condition is not satisfied for our choice of L. However, we get the same upper bound of $O(1/\log b)$ by a simple application of the 1-dimensional Selberg sieve (see theorem 3.3 in [35]).

Thus, we have succeeded in preserving the average times of the algorithms while reducing the interval size L to $L \ge (\log n)^{30}$.

2.5 Discussion

By arguing a bit more carefully it is possible to get a slightly better constant instead of 30. In this chapter our emphasis has been on solving the conjecture of Bach and Sorenson rather than improving the running time of the algorithms. Bernstein [17] gives an essentially linear time algorithm ($(\log n)^{1+o(1)}$ as $n \to \infty$) for the perfect power testing problem based on ideas in [42]. His method uses theorems on multiple linear forms in logarithms.

Chapter 3

Density of Carmichael Numbers with Three Prime Factors

3.1 Introduction

In this chapter we give an improved upper bound on the number of Carmichael numbers up to x with three prime factors; $C_3(x)$. In the process, we come very close to settling a conjecture due to A. Granville (see [50]). The results described here are presented in a slightly different form in [14]. The reader is referred to A. Granville's review of our paper [14] in [34] and to his notes in [33] on our method. Here we include an application not presented in [14].

A *Carmichael number* is a composite number n which satisfies the condition $a^n \equiv a \bmod n$ for every integer a. The smallest Carmichael number is 561. The Carmichael numbers have many interesting properties. For example, it is known that they are square-free and the product of at least three primes [39]. The reader may consult [30], [47], [50], [54] for more on Carmichael numbers.

The problem of proving the existence of infinitely many Carmichael numbers was a long-standing open problem until it was solved recently, by Alford, Granville and Pomerance [5]. They also gave a lower bound for the number of Carmichael numbers less than a given number x. Let $C(x)$ denote the number of Carmichael numbers up to x. They showed that $C(x) > x^{2/7}$ for all sufficiently large x.

Let $C_k(x)$ denote the number of Carmichael numbers up to x with k prime factors where $k \geq 3$. It is an open problem to show that the function $C_3(x)$ is unbounded. It is not known whether any of the functions $C_k(x)$ is unbounded. Pomerance et al. [51] proved that $C_3(x) = O(x^{2/3})$. Damgård et al.[27] improved this to $C_3(x) \leq (1/4)x^{1/2}(\log x)^{11/4}$ for all $x \geq 1$. An estimate of $O(x^{2/5+o(1)})$ for $C_3(x)$ was obtained by S. W. Graham [29]. We show that for sufficiently large x, $C_3(x) = O(x^{5/14+o(1)})$. Granville (see [50]) has conjectured that $C_k(x) = x^{1/k+o_k(1)}$ for $x \to \infty$. Our upper bound for $C_3(x)$ comes very close to his conjectured value.

3.2 Proof of our bound

We state our result on the upper bound for $C_3(x)$ and give its proof. We need the following lemma.

Lemma 3.2.1 *The equation $aXY + bX + cY + d = 0$, $a, b, c, d \in \mathbf{Z}$ and $ad \neq bc$ has at most $O((abcd)^{o(1)})$ solutions in a, b, c, d.*

Proof. The equation can be rewritten as $(aX + c)(aY + b) = bc - ad$. Hence $aX + c$ (and consequently X) has $O((bc - ad)^{o(1)})$ divisors and once X is fixed, Y is also fixed. □

Theorem 3.2.2 *Let $C_3(x)$ denote the number of Carmichael numbers up to x with exactly three prime factors. Then, for all sufficiently large x we have $C_3(x) = O(x^{5/14+o(1)})$.*

Proof. If n is a Carmichael number with three prime factors p, q, r with $2 < p < q < r$ then $n - 1 \equiv 0 \bmod p - 1$, $n - 1 \equiv 0 \bmod q - 1$, $n - 1 \equiv 0 \bmod r - 1$.

Let $g = \gcd(p-1, q-1, r-1)$ and a, b, c be such that $p - 1 = ga$, $q - 1 = gb$, $r - 1 = gc$; then $a < b < c$. The congruences given above imply $gbc + b + c \equiv 0 \bmod a$,

$gac + a + c \equiv 0 \bmod b$ and $gab + a + b \equiv 0 \bmod c$. These three congruences can be replaced by the single congruence $g(ab + ac + bc) + a + b + c \equiv 0 \bmod abc$ by observing that a, b, c are pair-wise coprime. Hence, if a, b, c are given then g is determined modulo abc.

Let $g(ab+bc+ac)+a+b+c = \lambda abc$. Since $gbc < g(ab+bc+ac)+a+b+c = \lambda abc$, we get $g < \lambda a$. Let $g = \lambda a - r$. Using this value of g and simplifying the equation for λabc we get $(\lambda a^2 + 1)(b + c) + a = r(ab + bc + ac)$.

We have $\lambda a \leq 6g$ since $\lambda abc = g(ab + bc + ac) + a + b + c \leq 6gbc$. Also $rbc \leq r(ab + bc + ac) = (\lambda a^2 + 1)(b + c) + a \leq 5\lambda a^2 c$ and hence $rb \leq 5\lambda a^2$.

Now

$$\begin{aligned}
(abr)^2(ab\lambda)^{11}(a\lambda r)^1 &= a^{14}b^{10}(br)^3\lambda^{12}\\
&\leq 5^3a^{14}b^{10}(\lambda a^2)^3\lambda^{12}\\
&= 5^3(\lambda a)^{15}a^5b^5b^5\\
&\leq 5^3(6g)^{15}a^5b^5c^5\\
&\leq 5^36^{15}(ga)^5(gb)^5(gc)^5\\
&= 5^36^{15}(p-1)^5(q-1)^5(r-1)^5\\
&\leq 5^36^{15}(pqr)^5\\
&\leq 5^36^{15}x^5
\end{aligned}$$

Consequently for every solution, either $abr = O(x^{5/14})$ or $ab\lambda = O(x^{5/14})$ or $a\lambda r = O(x^{5/14})$. If $abr = O(x^{5/14})$ then fix a, b, r and look at the equation $(\lambda a^2 + 1)(b + c) + a = r(ab + ac + bc)$ in the remaining variables λ and c. This is exactly of the form considered in the lemma. In fact the equation becomes $a^2(\lambda c) + (a^2b)\lambda + (1 - ra - rb)c + a + b - rab = 0$. Hence from the lemma this has $O(x^{o(1)})$ solutions. Since $abr = O(x^{5/14})$, the number of choices of (a, b, r) is $O(x^{5/14+o(1)})$. Hence the total number of solutions in this case is $O(x^{5/14+o(1)})$. The other cases are similar.

□

A. Granville remarks in [34] that an approach similar to the one given above might lead to the solution of his conjecture. The reader is also referred to his notes in [33].

3.3 An application

Damgård et al [27] showed that the worst case numbers for the strong pseudo-prime test are numbers of the type
(i) $(m+1)(2m+1)$, where $m+1$, $2m+1$ are odd primes
(ii) $(m+1)(3m+1)$, where $m+1$, $3m+1$ are primes that are 3 mod 4
(iii) $p_1p_2p_3$, where p_1, p_2, p_3 are primes, $p_1p_2p_3$ is a Carmichael number and there is some integer s with $2^s \parallel p_i - 1$ for $i = 1, 2, 3$,
(iv) 9, 25, 49.

It is easy to design a variant of the strong pseudo-prime test that detects numbers of the type (i), (ii) or (iv). We can detect numbers of the type (i) or (ii) by solving quadratic equations in m. This can be done in time polynomial in $\log m$.

However, it is an open problem to recognize numbers of the type (iii) in polynomial time.

Damgård et al [27] require an improved upper bound on $C_3(x)$. In their analysis (see p. 190 of [27]) they remark that except for a factor of $k^{O(1)}$ their bound is best possible. That this is true follows from our bound for $C_3(x)$.

Chapter 4

Progress Towards a Conjecture of S. W. Graham

4.1 Introduction

Let $C_3(X)$ denote the number of Carmichael numbers up to X with three prime factors. It is an open problem to show that the function $C_3(X)$ is unbounded.

Pomerance et al. [51] proved that $C_3(X) = O(X^{2/3})$. Damgård et al.[27] improved this to $C_3(X) \leq (1/4)X^{1/2}(\log X)^{11/4}$ for all $X \geq 1$. An estimate of $O(X^{2/5+o(1)})$ for $C_3(X)$ was obtained by S. W. Graham [29]. We showed in [14] that for sufficiently large X, $C_3(X) = O(X^{5/14+o(1)})$. Granville (see [50]) has conjectured that $C_3(X) = X^{1/3+o(1)}$ for $X \to \infty$.

S. W. Graham [29] conjectured that $C_3(X) \leq \sqrt{X}$ for all X. He proved this for $X \leq 10^{16}$ and $X > 10^{126}$. We prove his conjecture for $X \leq 10^{18}$ and $X \geq 2 * 10^{40}$. It is easy to see that a brute force computation of Carmichael numbers up to 10^{126} (or even $2 * 10^{40}$) with three distinct prime factors is prohibitive in practice for solving S. W. Graham's conjecture.

4.2 The conjecture of S.W.Graham

S. W. Graham in an unpublished manuscript [29] conjectured that $C_3(X) \leq \sqrt{X}$ for all X. He showed this for $X \leq 10^{16}$ and $X > 10^{126}$. He proved this for $X \leq 10^{16}$ by using a table of Carmichael numbers [48] and for $X > 10^{126}$ by showing $C_3(X) \leq 131X^{5/11}(\log X)^{16/11}$. We improve on S. W. Graham's result and show that his conjecture is true for $X \leq 10^{18}$ and $X \geq 2 * 10^{40}$. For the range $10^{16} \leq X \leq 10^{18}$ we can verify that $C_3(X) \leq \sqrt{X}$ by using Pinch's table of Carmichael numbers up to 10^{18} with three prime factors [49].

We also require the following results:

Lemma 4.2.1 *Let $a \in \Re$ and $a > 1$ and $N \geq 0$ then*

$$\sum_{y \leq N} a^y \leq a^N(1-1/a)^{-1}$$

and

$$\sum_{y \geq N} a^{-y} \leq a^{-N}(1-1/a)^{-1}$$

Theorem 4.2.2 *Let a, b, c, A, B, C be positive real numbers such that $a/A > b/B$ and $a/A > c/C$. Then*

$$\sum_{Ax+By+Cz \leq N} 2^{ax+by+cz} \leq (1-2^{-a})^{-1}2^{aN/A}(1-2^{b-aB/A})^{-1}(1-2^{c-aC/A})^{-1}$$

Proof. Assume a, b, c, A, B, C satisfy $a/A > b/B$, $a/A > c/C$. Then

$$\begin{aligned}
\sum_{Ax+By+Cz \leq N} 2^{ax+by+cz} &= \sum_{y,z} 2^{by+cz} \sum_{x \leq (N-By-Cz)/A} 2^{ax} \\
&\leq \sum_{y,z} 2^{by+cz+a(N-By-Cz)/A}(1-2^{-a})^{-1} \\
&\leq (1-2^{-a})^{-1}2^{aN/A} \sum_{y} 2^{(b-aB/A)y} \sum_{z} 2^{(c-aC/A)z} \\
&\leq (1-2^{-a})^{-1}2^{aN/A}(1-2^{b-aB/A})^{-1}(1-2^{c-aC/A})^{-1}
\end{aligned}$$

□

Theorem 4.2.3 *Let a, b, c, A, B, C be positive real numbers such that $a/A < b/B$ and $a/A < c/C$. Then*

$$\sum_{Ax+By+Cz\geq N} 2^{-ax-by-cz} \leq (1-2^{-a})^{-1}2^{-aN/A}(1-2^{-(b-aB/A)})^{-1}(1-2^{-(c-aC/A)})^{-1}$$

Proof. Assume a, b, c, A, B, C satisfy $a/A < b/B$, $a/A < c/C$. Then

$$\begin{aligned}\sum_{Ax+By+Cz\geq N} 2^{-ax-by-cz} &= \sum_{y,z} 2^{-by-cz} \sum_{x\geq(N-By-Cz)/A} 2^{-ax} \\ &\leq \sum_{y,z} 2^{-by-cz-a(N-By-Cz)/A}(1-2^{-a})^{-1} \\ &\leq (1-2^{-a})^{-1}2^{-aN/A}\sum_{y} 2^{-(b-aB/A)y}\sum_{z} 2^{-(c-aC/A)z} \\ &\leq (1-2^{-a})^{-1}2^{-aN/A}(1-2^{-(b-aB/A)})^{-1}(1-2^{-(c-aC/A)})^{-1}\end{aligned}$$

□

We now state our main result.

Theorem 4.2.4 *Let $C_3(X)$ denote the number of Carmichael numbers up to X with exactly three prime factors. Then $C_3(X) \leq \sqrt{X}$ for $X \leq 10^{18}$ and $X \geq 2 * 10^{40}$.*

Proof. If n is a Carmichael number with exactly three prime factors p, q, r with $p < q < r$ then $n - 1 \equiv 0 \bmod p - 1$, $n - 1 \equiv 0 \bmod q - 1$, $n - 1 \equiv 0 \bmod r - 1$.

Let $g = \gcd(p-1, q-1, r-1)$ and a, b, c be such that $p - 1 = ga$, $q - 1 = gb$, $r - 1 = gc$, then $a < b < c$. The congruences given above imply that $gbc + b + c \equiv 0 \bmod a$, $gac + a + c \equiv 0 \bmod b$ and $gab + a + b \equiv 0 \bmod c$. These three congruences can be replaced by the single congruence $g(ab + ac + bc) + a + b + c \equiv 0 \bmod abc$. Hence, if a, b, c are given then g is determined modulo abc.

Damgård et al. [27] showed that $C_3(X) \leq (1/4)X^{1/2}(\ln X)^{11/4}$ for all $X > 1$. They obtained this result by estimating three sums. We use their estimates.

Let M be the number of quadruples (g, a, b, c) which satisfy the above conditions and $g^3abc \leq X$. Then $C_3(X) \leq M$. Let $M = N_1 + N_2 + N_3$, where in N_1 we count those quadruples with $g > abc$, in N_2 we count those quadruples with $G < g \leq abc$ and in N_3 we count those quadruples with $g \leq G$ and $g \leq abc$. Here G is a parameter dependent on X. Damgård et al. [27] work with $G = X^{1/6}/(\ln X)^{1/4}$.

It is easy to estimate N_1.

Estimate for N_1

If (a, b, c) are given then the number of g with $g^3abc \leq X$, g in a particular residue class modulo abc and $g > abc$ is at most $(X/abc)^{1/3}/abc$, which is $X^{1/3}/(abc)^{4/3}$. Hence

$$N_1 \leq \sum_{a<b<c} \frac{X^{1/3}}{(abc)^{4/3}} < \frac{\zeta^3(4/3)X^{1/3}}{6}$$

where ζ is the Riemann zeta function. Thus $N_1 < (1/6)\zeta^3(4/3)X^{1/3}$.

Estimate for N_2

For each coprime triple (a, b, c) there is at most one g that satisfies the condition $g(ab + ac + bc) + a + b + c \equiv 0 \bmod abc$ and $g \leq abc$. If $g > G$ and $g^3abc \leq X$ then $abc \leq X/G^3$. Thus N_2 is at most the number of triples (a, b, c) with $a < b < c$ and $abc \leq X/G^3$. Hence,

$$\begin{aligned}
N_2 &\leq \sum_{1\leq a<X^{1/3}/G} \ \sum_{a<b<(X/aG^3)^{1/2}} \ \sum_{b<c\leq X/abG^3} 1 \\
&< \sum_{a}\sum_{b} \frac{X}{abG^3} \quad < \quad \sum_{a} \frac{X}{aG^3} \ln\left(\left(\frac{X}{aG^3}\right)^{1/2}\right) \\
&< \frac{X}{2G^3}\left(1 + \ln\left(\frac{X^{1/3}}{G}\right)\right) \ln\left(\frac{X}{G^3}\right) \quad < \quad \frac{X}{6G^3}(\ln(X))^2
\end{aligned}$$

Thus $N_2 \leq (1/6)(X/G^3)(\ln(X))^2$.

Damgård et al [27] were able to show that $N_3 \leq 3X^{1/3}G(1+\ln(3G))(2+\ln(2G))^2$. Their choice of $G = X^{1/6}/(\ln X)^{1/4}$ gives $N_2 \leq (1/6)X^{1/2}(\ln X)^{11/4}$ and $N_3 \leq (3/64)X^{1/2}(\ln X)^{11/4}$. We had obtained (see Chapter 3 or [14]) an upper bound of $C_3(X) = O(X^{5/14+o(1)})$ by choosing $G = X^{3/14}$ and estimating N_3 differently from that in [27]. However, we were not able to obtain an useful explicit bound for solving S. W. Graham's conjecture.

Since $g(ab+ac+bc)+a+b+c \equiv 0 \bmod abc$ assume $g(ab+ac+bc)+a+b+c = \lambda abc$ where $\lambda \geq 1$ is an integer. Then it is easy to show that $\lambda a < 3.75g$. This is true because $(\lambda a - g)bc = g(ab+ac)+a+b+c$ implies $(\lambda a - g)/g = (ab+ac)/bc + (a+b+c)/gbc < 2bc/bc + 3c/gbc \leq 2 + 3/4 = 2.75$ as $g \geq 2$ and $b \geq 2$. Therefore $\lambda a < 3.75g$. A more careful calculation gives $3 + 7/12$ instead of 3.75.

To simplify the exposition of our proofs we use $\lambda a < 4g$ but in the final calculation we use the sharper estimate $\lambda a < (3 + 7/12)g$.

We show $C_3(X) \leq \sqrt{X}$ for $X \geq 7 * 10^{47}$ by showing $N_1 < (1/6)\zeta^3(4/3)X^{1/3} \leq \sqrt{X}/125$ and $N_2 + N_3 \leq (124/125)\sqrt{X}$. Now $N_1 < (1/6)\zeta^3(4/3)X^{1/3} \leq \sqrt{X}/125$ for $X \geq 10^{18}$. Hence we can assume $g \leq abc$.

Let $X = 2^N$. Consider (A, Λ, x, y) where $2^A \leq a < 2^{A+1}$, $2^\Lambda \leq \lambda < 2^{\Lambda+1}$, $2^{A+x} \leq b < 2^{A+x+1}$, $2^{A+y} \leq c < 2^{A+y+1}$.

We have $g^3abc \leq 2^N$, $\lambda a \leq 4g$ so $\lambda^3 a^4 bc \leq 2^{N+6}$.

We consider various cases in our proof.

I $\quad A + x < \Lambda$

I(a) $\quad j_2 \leq A + j_1$

I(b) $\quad j_2 > A + j_1$

II $\quad A + x \geq \Lambda$

II(a) $\quad A \geq \Lambda$

II(a) (i) $\quad 2\Lambda + j_1 < x$

II(a) (ii) $\quad 2\Lambda + j_1 \geq x$

II(a) (ii) (I) $j_2 \le (2\Lambda + j_1 - x)/2$

II(a) (ii) (II) $j_2 \ge (2\Lambda + j_1 - x)/2$

II(b) $A < \Lambda$

II(b) (i) $j_2 > 2A$

II(b) (ii) $j_2 \le 2A$

II(b) (ii) (I) $j_3 \le (2A - j_2)/2$

II(b) (ii) (II) $j_3 > (2A - j_2)/2$

For proving our result we use three formulas:

(i) abc formula

(ii) $a\lambda c$ formula

(iii) $\lambda^2 a^3 b/c$ formula

Explanation of the formulas:

(i) abc formula

Since $g(ab + ac + bc) + a + b + c \equiv 0 \bmod abc$ and $g \le abc$; for a given choice of a, b and c, g is unique. Hence, to count the number of quadruples (g, a, b, c) such that $g^3abc \le X$, we need to count only the number of triples (a, b, c) such that $g^3abc \le X$. Since $2^A \le a < 2^{A+1}$, $2^{A+x} \le b < 2^{A+x+1}$, $2^{A+y} \le c < 2^{A+y+1}$ the number of triples (a, b, c) such that $g^3abc \le X$ is $\le 2^A 2^{A+x} 2^{A+y}$.

(ii) $a\lambda c$ formula

$g(ab + ac + bc) + a + b + c = \lambda abc$. Let $r = \lambda a - g$ then $\lambda a^2(b + c) - r(bc + ac + ab) + a + b + c = 0$. Hence $rbc - (\lambda a^2 + 1 - ra)(b + c) - a = 0$. If we fix a, λ, r then viewing this equation modulo r we get $-(\lambda a^2 + 1)(b + c) - a \equiv 0 \bmod r$. The number of choices for $b + c$ is less than the number of choices for c which is $\le 2^{A+y}$. Hence the number of solutions for the congruence $-(\lambda a^2 + 1)(b + c) - a \equiv 0 \bmod r$

is $< 2^{A+y}/r$. a, λ, r can be fixed in $a\lambda r$ ways. c can be fixed in $\leq 2^{A+y}/r$ ways. So a, λ, r, c can be fixed in at most $2a\lambda c$ ways (taking in to account the case when $2^{A+y} < r$).

(iii) $\lambda^2 a^3 b/c$ formula

Consider the equation $rbc - (\lambda a^2 + 1 - ra)(b+c) - a = 0$. This can be rewritten as $(r(a+b) - (\lambda a^2+1))c = (\lambda a^2+1)b - rab + a$. Hence $r - (\lambda a^2+1)/(a+b) = ((\lambda a^2 + 1)b - rab + a)/(c(a+b))$. We show $((\lambda a^2+1)b - rab + a)/(c(a+b) \leq \lambda a^2/c$. $a \leq \lambda a^2 a$ and $b \leq rab$ imply $b + a - rab \leq \lambda a^2 a$ which implies $(\lambda a^2+1)b - rab + a \leq \lambda a^2(a+b)$. This yields the desired result.

Hence

$$\begin{aligned} |\, r - (\lambda a^2 + 1)/(a+b) \,| &\leq \lambda a^2/c \\ &\leq 2^{\Lambda+1+2A+2-A-y} = 2^{\Lambda+A-y+3} \end{aligned}$$

a, λ, b can be fixed in $a\lambda b$ ways. r can be fixed in at most $\lambda a^2/c$ ways. The total number of ways of fixing a, λ, b and r is $\leq a\lambda b\lambda a^2/c = \lambda^2 a^3 b/c \leq 2^A 2^\Lambda 2^{A+x} 2^{\Lambda+A-y+3} = 2^{3+3A+2\Lambda+x-y}$.

We now look at the individual cases:

Case I: $A + x < \Lambda$

(A, Λ, x, y) can be written as $(A, A + x + j_1, x, x + j_2)$

Case I(a): $j_2 \leq A + j_1$

Use the formula abc

$$\sum_{A,x,j_1,j_2} 2^{A+(A+x)+(A+y)} = \sum_{A,x,j_1,j_2} 2^{3A+x+y} = \sum_{A,x,j_1,j_2} 2^{3A+2x+j_2}$$

subject to $\lambda^3 a^4 bc \leq 2^{N+6}$ i.e $3\Lambda + 4A + (A+x) + (A+y) \leq N+6$ i.e $3(A + x + j_1) + 6A + 2x + j_2 \leq N + 6$ i.e $9A + 5x + 3j_1 + j_2 \leq N + 6$

$$\sum_{A,x,j_1,j_2} 2^{3A+2x+j_2} = \sum_{A,j_1} 2^{3A} \sum_{j_2 \leq A+j_1} 2^{j_2} \sum_{x \leq (N+6-9A-3j_1-j_2)/5} 2^{2x}$$

$$
\begin{aligned}
&\le \sum_{A,j_1} 2^{3A} \sum_{j_2 \le A+j_1} 2^{j_2}(2^2)^{(N+6-9A-3j_1-j_2)/5}(1-1/2^2)^{-1} \\
&= (4/3)\sum_{A,j_1} 2^{3A} \sum_{j_2 \le A+j_1} 2^{j_2} 2^{(2N+12-18A-6j_1-2j_2)/5} \\
&= (4/3)\sum_{A,j_1} 2^{3A} \sum_{j_2 \le A+j_1} 2^{(2N+12-18A-6j_1+3j_2)/5} \\
&= (4/3)\sum_{A,j_1} 2^{(2N+12-3A-6j_1)/5} \sum_{j_2 \le A+j_1} 2^{3j_2/5} \\
&\le (4/3)\sum_{A,j_1} 2^{(2N+12-3A-6j_1)/5}(2^{3/5})^{A+j_1}(1-1/2^{3/5})^{-1} \\
&= (4/3)(1-1/2^{3/5})^{-1}\sum_{A,j_1} 2^{(2N+12-3A-6j_1)/5+(3A+3j_1)/5} \\
&= (4/3)(1-1/2^{3/5})^{-1} 2^{(2N+12/5)} \sum_{A,j_1} 2^{-3j_1/5} \\
&= (4/3)(1-1/2^{3/5})^{-1} 2^{(2N+12/5)} \sum_{j_1} 2^{-3j_1/5} \sum_{A} 1 \\
&\le ((N+6)/9)(4/3)(1-1/2^{3/5})^{-1} 2^{(2N+12/5)} 1/(2^{3/5}-1)
\end{aligned}
$$

(Note $j_1 \ge 1$ and $A \le (N+6)/9$)

Case I(b): $j_2 > A + j_1$

(A, Λ, x, y) can be written as $(A, A + x + j_1, x, x + j_2)$

Use $\lambda^2 a^3 b/c$ formula

$$\sum_{A,x,j_1,j_2} 2^{3+3A+2\Lambda+x-y}$$

subject to $9A + 5x + 3j_1 + j_2 \le N + 6$ i.e $10A + 5x + 4j_1 \le N + 6$

$$
\begin{aligned}
\sum_{A,x,j_1,j_2} 2^{3+3A+2\Lambda-j_2} &= \sum_{A,x,j_1,j_2} 2^{3+3A+2(A+x+j_1)-j_2} \\
&= \sum_{A,x,j_1,j_2} 2^{3+5A+2x+2j_1-j_2} \\
&= \sum_{A,x,j_1} 2^{3+5A+2x+2j_1} \sum_{j_2 > A+j_1} 2^{-j_2} \\
&\le \sum_{A,x,j_1} 2^{3+5A+2x+2j_1} 2^{-(A+j_1+1)} 2^{1} \\
&= \sum_{A,x,j_1} 2^{3+4A+2x+j_1} \quad \text{(subject to } \; 10A + 5x + 4j_1 \le N + 6) \\
&= 2^3 \sum_{10A+5x+4j_1 \le N+6} 2^{4A+2x+j_1}
\end{aligned}
$$

Let $2A + x = k$. Note that $5k + 4j_1 \le N + 6$ implies $k \le (N + 6)/5$. Hence the above sum is

$$\begin{aligned}
&\leq 2^3\left(\sum_{5k+4j_1\leq N+6} 2^{2k+j_1}\right)(k/2) \quad \text{where} \quad 5k+4j_1 \leq N+6 \\
&\leq 2^3((N+6)/10) \sum_{5k+4j_1\leq N+6} 2^{2k+j_1} \\
&\leq 2^3((N+6)/10)(1-2^{-2})^{-1}(1-2^{1-2*4/5})^{-1}2^{2(N+6)/5}
\end{aligned}$$

(Note $2/5 > 1/4$)

Case II: $A + x \geq \Lambda$

Case II(a): $A \geq \Lambda$

(A, Λ, x, y) can be written as $(\Lambda + j_1, \Lambda, x, x + j_2)$

Sub-case: $2\Lambda + j_1 < x$

$(\Lambda + j_1, \Lambda, x, x + j_2)$ can be written as $(\Lambda + j_1, \Lambda, 2\Lambda + j_1 + j_3, 2\Lambda + j_1 + j_3 + j_2)$ subject to $\lambda^3 a^4 bc \leq 2^{N+6}$ i.e

$$3\Lambda + 4(\Lambda + j_1) + \Lambda + j_1 + 2\Lambda + j_1 + j_3 + \Lambda + j_1 + 2\Lambda + j_1 + j_3 + j_2 \leq N + 6$$

i.e $13\Lambda + 8j_1 + j_2 + 2j_3 \leq N + 6$

Use $\lambda^2 a^3 b/c$ formula

$$\begin{aligned}
\sum 2^{3+3A+2\Lambda+x-y} &= 2^3 \sum 2^{2\Lambda+3A+x-y} \\
&= 2^3 \sum 2^{2\Lambda+3(\Lambda+j_1)-j_2} \\
&= 2^3 \sum 2^{5\Lambda+3j_1-j_2} \\
&\qquad \text{(subject to } 13\Lambda + 8j_1 + j_2 + 2j_3 \leq N+6) \\
&= 2^3 \sum_{\Lambda, j_1} 2^{5\Lambda+3j_1} \sum_{j_2} 2^{-j_2} \quad \text{(subject to } 13\Lambda + 8j_1 + j_2 \leq N+6) \\
&\leq 2^3 \sum_{\Lambda, j_1, j_3} (2^{5\Lambda+3j_1+0j_3})(2^1) \quad \text{(subject to } 13\Lambda + 8j_1 + 2j_3 \leq N+6) \\
&\leq 2^4(1-2^{-5})^{-1}2^{5(N+6)/13}(1-2^{3-5*8/13})^{-1}
\end{aligned}$$

(Note that $5/13 > 3/8$ and $5/13 < 2/5$)

Sub-case: $2\Lambda + j_1 \geq x$

Sub-cases:

(i) $j_2 \leq (2\Lambda + j_1 - x)/2$

(ii) $j_2 \geq (2\Lambda + j_1 - x)/2$

Sub-case: $j_2 \leq (2\Lambda + j_1 - x)/2$

(A, Λ, x, y) can be written as $(\Lambda + j_1, \Lambda, x, x + j_2)$

Use $a\lambda c$ formula

$$\sum 2^{1+A+\Lambda+A+y}$$

subject to $\lambda^3 a^4 bc \leq 2^{N+6}$ i.e $3\Lambda + 4(\Lambda + j_1) + 2(\Lambda + j_1) + 2x + j_2 \leq N + 6$ i.e $9\Lambda + 6j_1 + 2x + j_2 \leq N + 6$

$$2\sum 2^{2A+\Lambda+x+j_2} = 2\sum 2^{2(\Lambda+j_1)+\Lambda+x+j_2} = 2\sum 2^{3\Lambda+2j_1+x+j_2}$$

subject to $9\Lambda + 6j_1 + 2x + j_2 \leq N + 6$

We consider two cases

(i) $10\Lambda + (13/2)j_1 + (3/2)x \leq N + 6$

(ii) $10\Lambda + (13/2)j_1 + (3/2)x \geq N + 6$

Case (i)

$$\begin{aligned}
& 2\sum 2^{3\Lambda+2j_1+x+j_2} \\
= \; & 2\sum_{\Lambda, j_1, x} 2^{3\Lambda+2j_1+x} \sum_{j_2} 2^{j_2} \text{ where } j_2 \leq (2\Lambda + j_1 - x)/2 \\
\leq \; & 2^2 \sum_{\Lambda, j_1, x} 2^{3\Lambda+2j_1+x+(2\Lambda+j_1-x)/2} \\
\leq \; & 2^2 \sum_{\Lambda, j_1, x} 2^{4\Lambda+(5/2)j_1+x/2} \\
& \quad \text{subject to} \quad 10\Lambda + (13/2)j_1 + (3/2)x \leq N + 6
\end{aligned}$$

We consider two sub-cases:

(i) $13\Lambda + 8j_1 \leq N + 6$

(ii) $13\Lambda + 8j_1 > N + 6$

Sub-case: $13\Lambda + 8j_1 \leq N + 6$

Use $x \leq 2\Lambda + j_1$

$$\begin{aligned}
& 2^2 \sum_{\Lambda, j_1, x} 2^{4\Lambda + (5/2)j_1 + x/2} \\
= \ & 2^2 \sum_{\Lambda, j_1} 2^{4\Lambda + (5/2)j_1} \sum_{x \leq 2\Lambda + j_1} 2^{x/2} \\
\leq \ & 2^2 \sum_{\Lambda, j_1} 2^{4\Lambda + (5/2)j_1} 2^{(2\Lambda + j_1)/2} (1 - 1/2^{1/2})^{-1} \\
\leq \ & 2^2 (1 - 1/2^{1/2})^{-1} \sum_{13\Lambda + 8j_1 \leq N+6} 2^{5\Lambda + 3j_1} \\
\leq \ & 2^2 (1 - 1/2^{1/2})^{-1} (1 - 2^{-5})^{-1} 2^{5(N+6)/13} (1 - 2^{3 - 5 * 8/13})^{-1}
\end{aligned}$$

Sub-case: $13\Lambda + 8j_1 > N + 6$

Use $10\Lambda + (13/2)j_1 + (3/2)x \leq N + 6$. This gives $x \leq (2/3)(N + 6 - 10\Lambda - (13/2)j_1)$

$$\begin{aligned}
& 2^2 \sum_{\Lambda, j_1, x} 2^{4\Lambda + (5/2)j_1 + x/2} \\
= \ & 2^2 \sum_{\Lambda, j_1} 2^{4\Lambda + (5/2)j_1} \sum_{x \leq (2/3)(N+6-10\Lambda-(13/2)j_1)} 2^{x/2} \\
\leq \ & 2^2 \sum_{\Lambda, j_1} 2^{4\Lambda + (5/2)j_1} 2^{(1/2)(2/3)(N+6-10\Lambda-(13/2)j_1)} (1 - 1/2^{1/2})^{-1} \\
\leq \ & 2^2 (1 - 1/2^{1/2})^{-1} \sum 2^{4\Lambda + (5/2)j_1 + (1/3)(N+6-10\Lambda-(13/2)j_1)} \\
\leq \ & 2^2 (1 - 1/2^{1/2})^{-1} 2^{(N+6)/3} \sum_{10\Lambda + (13/2)j_1 \leq N+6} 2^{2\Lambda/3 + j_1/3} \\
\leq \ & 2^2 (1 - 1/2^{1/2})^{-1} 2^{(N+6)/3} (1 - 2^{-2/3})^{-1} 2^{(2/30)(N+6)} (1 - 2^{1/3 - (2/3)(13/2)/10})^{-1} \\
\leq \ & 2^2 (1 - 1/2^{1/2})^{-1} (1 - 2^{-2/3})^{-1} (1 - 2^{1/3 - (2/3)(13/2)/10})^{-1} 2^{2(N+6)/5}
\end{aligned}$$

Case (ii)

Here we use the condition $9\Lambda + 6j_1 + 2x + j_2 \leq N + 6$

$$
\begin{aligned}
& 2 \sum_{\Lambda, j_1, x, j_2} 2^{3\Lambda+2j_1+x+j_2} \\
= \; & 2 \sum_{\Lambda, j_1, x} 2^{3\Lambda+2j_1+x} \sum_{j_2 \leq N+6-(9\Lambda+6j_1+2x)} 2^{j_2} \\
\leq \; & 2^2 \sum_{\Lambda, j_1, x} 2^{3\Lambda+2j_1+x+N+6-(9\Lambda+6j_1+2x)} \\
\leq \; & 2^{N+8} \sum_{\Lambda, j_1, x} 2^{-6\Lambda-4j_1-x} \\
& \quad \text{subject to} \quad 10\Lambda + (13/2)j_1 + (3/2)x \geq N + 6 \\
\leq \; & 2^{N+8}(1-2^{-6})^{-1}(1-2^{-(1-6(3/2)/10)})^{-1}(1-2^{-(4-6(13/2)/10)})^{-1}2^{-6(N+6)/10} \\
\leq \; & 2^2 2^{4(N+6)/10}(1-2^{-6})^{-1}(1-2^{-(1-6(3/2)/10)})^{-1}(1-2^{-(4-6(13/2)/10)})^{-1}
\end{aligned}
$$

Note that $6/10 < 8/13$ and $6/10 < 2/3$.

Sub-case: $j_2 \geq (2\Lambda + j_1 - x)/2$

(A, Λ, x, y) can be written as $(\Lambda + j_1, \Lambda, x, x + j_2)$

Use $\lambda^2 a^3 b/c$ formula

$$\sum 2^{3+2\Lambda+3A+x-y}$$

subject to $\lambda^3 a^4 bc \leq 2^{N+6}$ i.e $3\Lambda + 4(\Lambda + j_1) + 2(\Lambda + j_1) + 2x + j_2 \leq N + 6$ i.e. $3\Lambda + 6(\Lambda + j_1) + 2x + (2\Lambda + j_1 - x)/2 \leq N + 6$ i.e $10\Lambda + (13/2)j_1 + 3x/2 \leq N + 6$

$$
\begin{aligned}
& \sum_{\Lambda, x, j_1, j_2} 2^{3+2\Lambda+3(\Lambda+j_1)-j_2} \\
= \; & \sum_{\Lambda, x, j_1} 2^{3+5\Lambda+3j_1} \sum_{j_2 \geq (2\Lambda+j_1-x)/2} 2^{-j_2} \\
\leq \; & \sum_{\Lambda, x, j_1} 2^{3+5\Lambda+3j_1} 2^{-(2\Lambda+j_1-x)/2)} 2^1 \\
\leq \; & \sum_{\Lambda, x, j_1} 2^{4+5\Lambda+3j_1-\Lambda-j_1/2+x/2} \\
= \; & \sum_{\Lambda, x, j_1} 2^{4+4\Lambda+(5/2)j_1+x/2} \\
= \; & 2^4 \sum_{\Lambda, x, j_1} 2^{4\Lambda+5(j_1/2)+x/2} \\
& \quad (\text{subject to} \quad 10\Lambda + (13/2)j_1 + (3/2)x \leq N + 6)
\end{aligned}
$$

The sum here is similar to one we encountered earlier. As before we consider two sub-cases:

(i) $13\Lambda + 8j_1 \leq N + 6$

(ii) $13\Lambda + 8j_1 > N + 6$

Corresponding to these sub-cases we get the following estimates:

$$\leq 2^4(1 - 1/2^{1/2})^{-1}(1 - 2^{-5})^{-1}2^{5(N+6)/13}(1 - 2^{3-5*8/13})^{-1}$$

and

$$\leq 2^4(1 - 1/2^{1/2})^{-1}(1 - 2^{-2/3})^{-1}(1 - 2^{1/3-(2/3)(13/2)/10})^{-1}2^{2(N+6)/5}$$

Case II(b): $A < \Lambda$

Since $A + x \geq \Lambda$ we have $x \geq \Lambda - A$. (A, Λ, x, y) can be written as $(A, A + j_1, j_1 + j_2, j_1 + j_2 + j_3)$.

Sub-cases:

(i) $j_2 > 2A$

(ii) $j_2 \leq 2A$

Sub-case: $j_2 > 2A$

(A, Λ, x, y) can be written as $(A, A + j_1, j_1 + 2A + j_4, j_1 + 2A + j_4 + j_3)$

Use $\lambda^2 a^3 b/c$ formula

$$\sum 2^{3+2\Lambda+3A+x-y}$$

subject to $\lambda^3 a^4 bc \leq 2^{N+6}$ i.e $3\Lambda + 4A + A + x + A + y \leq N + 6$ i.e $3(A + j_1) + 6A + 2(j_1 + 2A + j_4) + j_3 \leq N + 6$ i.e $13A + 5j_1 + 2j_4 + j_3 \leq N + 6$

$$\begin{aligned} \sum 2^{3+2(A+j_1)+3A-j_3} &= 2^3 \sum_{A,j_1,j_3,j_4} 2^{5A+2j_1-j_3} \\ &\leq 2^3 \sum_{A,j_1} 2^{2j_1+5A} \sum_{j_3} 2^{-j_3} \end{aligned}$$

$$
\begin{aligned}
& \text{(subject to} \quad 5j_1 + 13A \leq N + 6) \\
\leq \quad & 2^3 \sum_{5j_1+13A \leq N+6} 2^{2j_1+5A} 2^1 \\
\leq \quad & 2^4(1-2^{-2})^{-1} 2^{2(N+6)/5}(1-2^{5-2*13/5})^{-1}
\end{aligned}
$$

Sub-case: $j_2 \leq 2A$

(A, Λ, x, y) can be written as $(A, A+j_1, j_1+j_2, j_1+j_2+j_3)$. Two cases can be considered

(i) $j_3 \leq (2A - j_2)/2$

(ii) $j_3 > (2A - j_2)/2$

Sub-case: $j_3 \leq (2A - j_2)/2$

Use $a\lambda c$ formula

$$
\begin{aligned}
\sum 2^{1+A+\Lambda+A+y} &= 2\sum 2^{2A+\Lambda+y} \\
&= 2\sum 2^{2A+A+j_1+j_1+j_2+j_3} \\
&= 2\sum 2^{3A+2j_1+j_2+j_3}
\end{aligned}
$$

subject to $\lambda^3 a^4 bc \leq 2^{N+6}$ i.e $3\Lambda + 4A + A + j_1 + j_2 + A + j_1 + j_2 + j_3 \leq N + 6$ i.e $3\Lambda + 6A + 2j_1 + 2j_2 + j_3 \leq N + 6$ i.e $3(A + j_1) + 6A + 2j_1 + 2j_2 + j_3 \leq N + 6$ i.e $9A + 5j_1 + 2j_2 + j_3 \leq N + 6$

$$
\begin{aligned}
& 2 \sum_{A,j_1,j_2,j_3} 2^{3A+2j_1+j_2+j_3} \\
= \quad & 2 \sum_{A,j_2,j_3} 2^{3A+j_2+j_3} \sum_{j_1 \leq (N+6-9A-2j_2-j_3)/5} 2^{2j_1} \\
= \quad & 2 \sum_{A,j_2,j_3} 2^{3A+j_2+j_3} 2^{2(N+6-9A-2j_2-j_3)/5}(1-2^{-2})^{-1} \\
\leq \quad & (8/3) \sum_{A,j_2,j_3} 2^{(15A+5j_2+5j_3+2N+12-18A-4j_2-2j_3)/5} \\
= \quad & (8/3) \sum_{A,j_2,j_3} 2^{(2N+12-3A+j_2+3j_3)/5} \\
= \quad & (8/3) 2^{(2N+12)/5} \sum_{A,j_2,j_3} 2^{(-3A+j_2+3j_3)/5}
\end{aligned}
$$

$$\begin{aligned}
&= (8/3)2^{(2N+12)/5}\sum_{A,j_2}2^{(-3A+j_2)/5}\sum_{j_3\le(2A-j_2)/2}2^{3j_3/5}\\
&\le (8/3)2^{(2N+12)/5}\sum_{A,j_2}2^{(-3A+j_2)/5}2^{((2A-j_2)/2)(3/5))}(1-1/2^{3/5})^{-1}\\
&\le (8/3)2^{(2N+12)/5}(1-1/2^{3/5})^{-1}\sum_{A,j_2}2^{(-3A+j_2)/5+3A/5-3j_2/10}\\
&= (8/3)2^{(2N+12)/5}(1-1/2^{3/5})^{-1}\sum_{j_2}2^{-j_2/10}\sum_{A}1\\
&\le ((N+6)/9)(8/3)2^{(2N+12)/5}(1-1/2^{3/5})^{-1}(1/(1-2^{-1/10}))\\
&\le ((N+6)/9)(8/3)(1-1/2^{3/5})^{-1}(1/(1-2^{-1/10}))2^{(2N+12)/5}
\end{aligned}$$

Sub-case: $j_3 > (2A-j_2)/2$

(A, Λ, x, y) can be written as $(A, A+j_1, j_1+j_2, j_1+j_2+j_3)$

Use λ^2a^3b/c formula

$$\sum 2^{3+2\Lambda+3A+x-y}$$

subject to $\lambda^3a^4bc \le 2^{N+6}$ i.e $3(A+j_1)+6A+2(j_1+j_2)+j_3 \le N+6$ i.e $9A+5j_1+2j_2+j_3 \le N+6$ i.e $9A+5j_1+2j_2+(2A-j_2)/2 \le N+6$ i.e $10A+5j_1+3j_2/2 \le N+6$

$$\begin{aligned}
2^3\sum 2^{2(A+j_1)+3A-j_3} &= 2^3\sum_{A,j_1}2^{5A+2j_1}\sum_{j_3\ge(2A-j_2)/2}2^{-j_3}\\
&\le 2^3\sum_{A,j_1}2^{5A+2j_1}2^{-((2A-j_2)/2)}2^1\\
&\le 2^4\sum_{A,j_2,j_1}2^{4A+j_2/2+2j_1}\\
&\qquad\text{(subject to}\quad 10A+3j_2/2+5j_1\le N+6)\\
&\le 2^4\sum_{10A+5j_1+3j_2/2\le N+6}2^{4A+2j_1+j_2/2}
\end{aligned}$$

Let $2A+j_1=k$. Then the above sum is

$$\begin{aligned}
&\le 2^4\sum_{5k+3j_2/2\le N+6}\left(\left(2^{2k+j_2/2}\right)(k/2)\right)\\
&\le 2^4((N+6)/10)\sum_{5k+3j_2/2\le N+6}2^{2k+j_2/2}
\end{aligned}$$

Note that $5k+3j_2/2 \le N+6$ implies $k \le (N+6)/5$. Also $2/5 > (1/2)/(3/2)$.

Hence the above sum is

$$\leq \; 2^4((N+6)/10)(1-2^{-2})^{-1}2^{2(N+6)/5}(1-2^{1/2-(2)(3/2)/5})^{-1}$$

Adding all the estimates and by solving the resulting inequality by Mathematica we get $x \geq 7 * 10^{47}$.

Since N is about 150 the sums in the various sub-cases turn out to be easy to calculate directly. A slightly more careful calculation was done using a high precision arithmetic software UBASIC on a PC. This leads to a result sharper than $7 * 10^{47}$. The calculations yield $x \geq 2 * 10^{40}$.

□

4.3 Discussion

Though we have been able to get a significant improvement on the range proved by S. W. Graham, establishing his conjecture for the range $10^{18} < X < 2 * 10^{40}$ is still open.

Chapter 5

The Least Witness of a Composite Number

5.1 Introduction

This chapter deals with the problem of finding the least witness $w(n)$ of a composite number n (see [7, 22]). A number w is a witness for a composite number n if n is not a strong pseudo-prime [39] to the base w. We show $w(n) = O(n^{1/(8\sqrt{e})+o(1)})$ for all composite numbers n except Carmichael numbers of the form $n = pqr$ with $\nu_2(p-1) = \nu_2(q-1) = \nu_2(r-1)$. For the exceptional numbers we conjecture $w(n) = O(n^{1/(8\sqrt{e})+o(1)})$. The results in this chapter also appear in [15].

The problem of quickly determining the prime or composite nature of a number n is a very important problem in algorithmic number theory and cryptography and has been the subject of much research [1, 2, 4, 7, 16, 52]. An $O((\log n)^{4+o(1)})$ time deterministic algorithm for this problem is known under the assumption of the as yet unresolved Generalized Riemann Hypothesis (GRH) [7, 43]. However the best known deterministic algorithm for this problem without the assumption of any unproved hypothesis [4] runs in sub-exponential time having a time complexity of $O((\log n)^{O(\log\log\log n)})$. It has also been proved that there is a probabilistic algorithm [1] that for prime n leads to a primality proof (proof that the number is actually a prime) in $O((\log n)^k)$ expected time for some $k \geq 1$.

A first approach to test if a given positive integer n is a prime, is to choose an integer a such that $1 < a < n$ and $\gcd(a, n) = 1$ and n passes the Fermat test i.e. $a^{n-1} \equiv 1 \bmod n$. If $a^{n-1} \not\equiv 1 \bmod n$ then n is not a prime. A composite number n which passes the Fermat test for a given base a is called a *Fermat pseudo-prime* to the base a. There are certain composite numbers n called as *Carmichael numbers* [39] for which $a^{n-1} \equiv 1 \bmod n$ for every a for which $\gcd(a, n) = 1$. It has been proved recently [5] that there are infinitely many Carmichael numbers. Hence a different approach is required.

A further improvement to the Fermat test is known which uses the Legendre-Jacobi symbol (see [39]). If p is an odd prime and $\gcd(a, p) = 1$ then $a^{(p-1)/2} \equiv (\frac{a}{p}) \bmod p$. This test recognizes composite numbers not recognized as composite by the Fermat test.

A composite number n is called an *Euler pseudo-prime* to the base a if $\gcd(a, n) = 1$ and $a^{(n-1)/2} \equiv (\frac{a}{n}) \bmod n$. It is known [39] that no odd composite number can be a Euler pseudo-prime for all the possible bases a for which $\gcd(a, n) = 1$.

An improvement on the Euler pseudo-prime test is the **strong pseudo-prime test** also called as the **Miller-Rabin test** [52]. Let n be a positive odd number for which $n - 1 = 2^s t$ where t is odd. If $1 \leq a \leq n - 1$ then n is defined to be a **strong pseudo-prime** to the base a if:

$$\textit{either } a^t \equiv 1 \bmod n \textit{ or } a^{2^i t} \equiv -1 \bmod n \text{ for some } i \in \{0, 1, \ldots, s-1\} \quad .$$

Many of the problems we consider have polynomial time algorithms for solving them if the Generalized Riemann Hypothesis (GRH) is true. However, we are interested in algorithms for these problems, which do not assume the GRH.

Definition 1 (Witness) *Let n be a composite number. We define an integer a for which $1 < a < n$ to be a "witness" to the compositeness of n if either* $\gcd(a, n) > 1$ *or n is not a strong pseudo-prime to the base a.*

From our definition of "witness" it follows that we can test if a given integer a

produces a certificate of compositeness of a given composite number n, in polynomial time. This property is very helpful in practice when we want to quickly convince anyone (or ourselves) that a particular number is in fact composite.

A natural way to find the least witness of a composite number n is as follows:

Algorithm

```
{Trivial algorithm for the least witness of a composite number $n$ }
w:=2
while  ($n$ is a strong pseudo-prime to the base $w$)   do
  w:= w+1
return w (the least witness $w(n)$ of the composite number $n$)
```

In this chapter we analyze this algorithm.

For a composite number n it is desirable to give a good upper bound on the least witness $w(n)$ to the compositeness of n. It is known that $w(n) < 2\log^2 n$ under the assumption of the GRH [7]. From this, it is easy to show that the average of $w(n)$ taken over odd composite numbers $\leq x$ is asymptotic to 2 as $x \to \infty$ [22]. Burthe [22] showed that this is true even without the GRH assumption.

The last result has an interesting algorithmic interpretation:

Theorem 5.1.1 *There is a deterministic algorithm which finds a certificate of compositeness of a given composite number n, whose average running time is polynomial (asymptotically), without the assumption of any unproved hypothesis (such as the Generalized Riemann Hypothesis).*

We are not aware of any such result prior to Burthe's [22]. The average running time of the basic version of the fastest deterministic primality testing algorithm [4] is not polynomial as there are essentially no good cases for that algorithm, they are all the same case. There are versions of that algorithm [19] which use partial factorizations of $n^2 - 1$ etc., but few n's will have a factored portion big enough to influence the average running time.

The analogue of the above theorem for primes involves finding certificates of primality. There is an open problem here:

Open Problem 1 *Give a deterministic algorithm, which does not assume any unproved hypothesis, which finds certificates of primality for prime numbers, whose average running time is polynomial.*

In order to solve this open question one would at least have to show that a positive proportion of the primes can be recognized in deterministic polynomial time. The best result in this direction is that of S. Konyagin and C. Pomerance [40] who showed that $> x^{1-\epsilon}$ primes up to x can be recognized in deterministic polynomial time for any $\epsilon > 0$.

The study of $w(n)$ is closely related [22] to $G(n)$, the smallest positive integer G such that the subgroup generated by the integers b for which $1 \leq b \leq G$ and $\gcd(b, n) = 1$ is $(\mathbf{Z}/n\mathbf{Z})^*$. For odd composite numbers n it is known [22] that $w(n) \leq G(n)$. Bach [7] showed that the GRH implies $G(n) \leq 3 \log^2 n$.

Number-theoretic estimates obtained without assuming the GRH are generally very weak when compared to those obtained using it. This observation also applies to estimates for $G(n)$.

Bach and Huelsbergen [10] offer heuristic arguments and numerical data supporting the idea that $G(n) \leq (\log 2)^{-1} \log n \log\log n$ asymptotically. They remark that by the Polya-Vinogradov inequality [28], for odd composite n, $G(n) = O(\sqrt{n} \log n \log\log n)$ hence $w(n) = O(\sqrt{n} \log n \log\log n)$. For a composite n we can show trivially that $w(n) \leq \sqrt{n}$ by observing that such a n has a non-trivial divisor less than or equal to $\sqrt{n}$.

Burthe [22] showed that $G(n) = O_\epsilon(n^{3/(8\sqrt{e})+\epsilon})$ for all $n \in \mathbf{Z}^+$ and if n is cube-free, then one can replace 3/8 with 1/4.

Lenstra [41] obtained the following theorems, of independent interest. They give an algorithm useful for finding witnesses of numbers that are not square-free.

Theorem 5.1.2 *[41] Let n be a positive integer, $n \neq 4$, and assume that $a^{n-1} \equiv 1 \bmod n$ for every prime number $a < (\log n)^2$. Then n is the product of distinct prime numbers.*

Theorem 5.1.3 *[41] Let p be an odd prime. Then we have $a^{p-1} \not\equiv 1 \bmod p^2$ for some prime number $a < 4(\log p)^2$.*

Burthe [22] obtained the following variation of the above results of Lenstra, by a different technique.

Theorem 5.1.4 *[22] If n is an odd composite number that is not square-free then $w(n) < \log^2 n$.*

Lenstra's result has an interesting algorithmic consequence:

Theorem 5.1.5 *There is a deterministic algorithm that finds a certificate of compositeness of a number n that is not square-free, in polynomial time.*

Theorem 5.1.6 *There is a $O((\log n)^{4+o(1)}/\log\log n)$ time deterministic algorithm, for producing a certificate of compositeness of a number n that is not square-free.*

If we are able to improve on the exponent of $\log n$ in Lenstra's theorem then we improve on the above theorem but this appears to be very difficult [31]. We get an open problem here:

Open Problem 2 *Obtain a $o((\log^4 n)/\log\log n)$ time deterministic algorithm for finding a certificate of compositeness of a number n that is not square-free.*

Granville [32] showed that we can assume $a < (\log p)^2$ in Lenstra's theorem 5.1.3. Hence we get $w(n) < (1/4)\log^2 n$ in theorem 5.1.4.

We note that the algorithm referred to in theorem 5.1.5 may produce a certificate of compositeness of a composite n that is square-free. Hence it is not useful for distinguishing between square-free composites and integers that are not square-free. However we get an interesting result:

Theorem 5.1.7 *If there is a polynomial time algorithm for producing a certificate of compositeness of a square-free composite number n then we can transform that algorithm to a polynomial time algorithm for establishing the primality of any positive integer n.*

It is interesting to note that while there is a deterministic polynomial time algorithm for producing certificates of compositeness of numbers that are not square-free, there is no known deterministic polynomial time algorithm (see [3]) for testing if a number is square-free.

By using the results of Lenstra and Burthe we get $w(n) = O_\epsilon(n^{1/(4\sqrt{e})+\epsilon})$ for every odd composite number n.

By a careful consideration of the number of prime factors of n Burthe [22] obtained:

Theorem 5.1.8 *[22] If n is an odd composite number and is not the product of three distinct primes then $w(n) = O_\epsilon(n^{1/(8\sqrt{e})+\epsilon})$ for every $\epsilon > 0$.*

Theorem 5.1.9 *[22] If n is an odd composite number with exactly three prime factors then for every $\epsilon > 0$, $w(n) = O_\epsilon(n^{1/(6\sqrt{e})+\epsilon})$.*

Thus Burthe was able to show that for every odd composite number n, $w(n) = O_\epsilon(n^{1/(6\sqrt{e})+\epsilon})$.

5.2 Improving Burthe's Theorem

An interesting problem is to improve 1/6 to 1/8 in Burthe's theorem for odd composite numbers with three prime factors. Burthe [22] requires the following results for his theorem 5.1.9:

Lemma 5.2.1 *[22] If n is odd and p and q are primes dividing n with $\nu_2(p-1) < \nu_2(q-1)$ and if $(\frac{a}{q}) = -1$ for $a \in \mathbf{Z}^+$ then a is a witness for n. Furthermore if $\nu_2(p-1) = \nu_2(q-1)$ and $(\frac{b}{pq}) = -1$ for $b \in \mathbf{Z}^+$ then b is witness for n.*

Lemma 5.2.2 *[22] For every $\epsilon > 0$ there is some number C_ϵ with the following property: if p and q are primes that divide an odd number n and $\nu_2(p-1) < \nu_2(q-1)$ then $w(n) < C_\epsilon q^{1/(4\sqrt{e})+\epsilon}$.*

Theorem 5.2.3 *[22] Let χ be a character mod n. For non-principal characters χ, define $B(\chi)$ to be the least positive integer a such that $\chi(a) \neq 1$ and $\chi(a) \neq 0$. Then for every $\epsilon > 0$, we have $B(\chi) = O_\epsilon(n^{3/(8\sqrt{e})+\epsilon})$. If in addition n is cube-free then for all $\epsilon > 0$, $B(\chi) = O_\epsilon(n^{1/(4\sqrt{e})+\epsilon)})$.*

Burthe [22] in his proof of theorem 5.1.9 showed that we need to consider only the case $\nu_2(p-1) = \nu_2(q-1)$. By using the above results we strengthen this to $\nu_2(p-1) = \nu_2(q-1) = \nu_2(r-1)$ by proving for non-Carmichael numbers $n = pqr$ the least witness $w(n) = O_\epsilon(n^{1/(8\sqrt{e}+\epsilon)})$. Hence we have to solve our problem just for Carmichael numbers $n = pqr$ for which $\nu_2(p-1) = \nu_2(q-1) = \nu_2(r-1)$. This particular result also follows by a direct application of following lemmas in Adleman and Leighton's paper (see [2]).

Lemma 5.2.4 *[2] For any $\epsilon > 0$, there is a constant C such that, for every pair of primes p and q with $q \mid (p-1)$, there is a qth non-residue of p less than $Cp^{1/(4\sqrt{e})+\epsilon}$.*

Lemma 5.2.5 *[2] If $p \mid n$ and $p' \mid n$ for two primes p and p', $\nu_q(p-1) > \nu_q(p'-1) \geq 0$ for some prime q, a is a qth non-residue of p, and $\lambda(n) \mid (n-1)s$ for some s, then* *either a or $(a^{(n-1)s/q^k} \bmod n) - 1$ has a nontrivial greatest common divisor with n for some $1 \le k \le \nu_q((n-1)s)$.*

These two lemmas also tell us more, namely that if $n = pqr$ is a Carmichael number then there exists a prime Q such that the condition $\nu_Q(p-1) = \nu_Q(q-1) = \nu_Q(r-1)$ fails to hold and there will be an a satisfying $a = O_\epsilon(n^{1/(8\sqrt{\epsilon})+\epsilon})$ which will produce a certificate to the compositeness of n (by producing a nontrivial gcd as guaranteed by the lemma just stated). But it is not clear how we can quickly find such a Q.

Lemma 5.2.6 *If $n = pqr$ where $p < q < r$ are odd primes and n is not a Carmichael number then $w(n) = O_\epsilon(n^{1/(8\sqrt{\epsilon}+\epsilon)})$.*

Proof. Assume that n satisfies the given conditions but is not a Carmichael number. If $pq <= \sqrt{n}$ then $w(n) = O_\epsilon((n^{1/(8\sqrt{\epsilon})+\epsilon})$ by using $w(n) < O_\epsilon((pq)^{1/(4\sqrt{\epsilon})+\epsilon})$. Hence we assume $pq > \sqrt{n}$. Then $r < \sqrt{n}$ gives $p < q < r < \sqrt{n}$. By Burthe [22], we have for a prime P, $G(P) = O_\epsilon(P^{1/(4\sqrt{\epsilon})+\epsilon})$. This implies that the set of numbers $\{1, \ldots, l\}$ where $l = O_\epsilon(P^{1/(4\sqrt{\epsilon})+\epsilon})$ generate $(\mathbf{Z}/p\mathbf{Z})^*$. The number n must satisfy $a^{n-1} \equiv 1 \bmod n$ for every $a = O_\epsilon(n^{1/(8\sqrt{\epsilon}+\epsilon)})$ otherwise we are done.

Say $P = p$. Since the numbers $1, \ldots, l$ generate G, and since $a^{n-1} \equiv 1 \bmod n$ for all a in $\{1 \ldots l\}$, therefore $a^{n-1} \equiv 1 \bmod P$ for a in G. But G is cyclic, so $g^{n-1} \equiv 1 \bmod P$ for g a primitive root of P. Hence $\mid G \mid= P - 1$ divides $n-1$. Similarly, setting $P = q$, $P = r$ and using the fact that n is square-free we get n is a Carmichael number. This contradiction concludes our proof. □

Note that in the above proof, we only require the weaker assumption that n is a pseudo-prime for the bases under consideration.

We also make use of the following lemma:

Lemma 5.2.7 *Assume $n = pqr$ where $p < q < r$ are odd primes. If n is a Carmichael number for which $\nu_2(p-1) = \nu_2(q-1) = \nu_2(r-1)$ then if n is a* *strong pseudo-prime to the base a then* $(a/p) = (a/q) = (a/r)$.

5.3 Least witnesses for special Carmichaels

Except for the case when the given composite number n is a Carmichael number with three prime factors with $\nu_2(p-1) = \nu_2(q-1) = \nu_2(r-1)$, we have succeeded in showing that the least witness $w(n)$ for a composite number n satisfies $w(n) = O_\epsilon(n^{1/(8\sqrt{e})+\epsilon})$. These exceptional numbers are in fact, among the worst case numbers for the strong pseudo-prime test [27]. The other numbers are 9, 25, 49 and numbers of the form $(m+1)(2m+1)$ and $(m+1)(3m+1)$. While these numbers can be recognized in deterministic polynomial time we have an open problem for the special Carmichaels.

Open Problem 3 *Give a deterministic polynomial time algorithm for producing a certificate of compositeness of a Carmichael number of the form* $n = pqr$ *where* $p < q < r$ *are odd primes, for which* $\nu_2(p-1) = \nu_2(q-1) = \nu_2(r-1)$.

In fact the problem is open for any Carmichael number.

5.3.1 Improved estimate for the special Carmichaels

For the special Carmichaels we improve the Burthe estimate $w(n) = O_\epsilon(n^{1/(6\sqrt{e})+\epsilon})$ by using an argument due to Heath-Brown [37] to show $w(n) = O_\epsilon(n^{1/(6.568\sqrt{e})+\epsilon})$.

Theorem 5.3.1 *If* $n = pqr$ *is a Carmichael number for which* $\nu_2(p-1) = \nu_2(q-1) = \nu_2(r-1)$ *then* $w(n) = O_\epsilon(n^{1/(6.568\sqrt{e})+\epsilon})$.

Proof. Let $n = pqr$ be a Carmichael number for which $\nu_2(p-1) = \nu_2(q-1) = \nu_2(r-1)$.

Let $p < q < r$, and suppose that $(m/p) = (m/q) = (m/r)$ for $m < M$. Then $(m/pq) = (m/qr) = (m/pr) = 1$ for $m < M$, except when p or q or r divides m.

Method (i): we may apply the standard technique of Vinogradov for the least quadratic non-residue of the character $(*/pq)$. Let $K > M$ and sum (k/pq) for $k < K$, with $K = (pq)^{1/4+o(1)}$. By Burgess' bound (see [21] or p. 263 of [57]) this is $o(K)$. On the other hand we get a contribution $+1$ except when k has a prime factor at least M (or if p or q divides k). The sum is therefore at least $K - K/p - K/q - 2K\sum_{M\leq s<K} 1/s$, where s runs over primes. Hence

$$o(K) \geq K\left(1 - 2\log(\frac{\log K}{\log M}) - o(1)\right)$$

since p must tend to infinity as n does. Thus

$$M < (pq)^{1/4\sqrt{e}+o(1)}.$$

Method (ii): This time we consider $\sum_{k\leq K}(k/pq) + (k/pr) + (k/qr)$ for $K = (qr)^{1/4+o(1)}$, so that Burgess' bound shows the sum to be $o(K)$. This time we get a contribution of $+3$ unless k has a prime factor $s \geq M$ (or k is divisible by p, q, or r). However, for any k, the summand is at least -1 (this is the key point in the argument; the summand can never be -2 or -3). It follows that

$$o(K) \geq K\left(3 - 4/p - 4/q - 4/r - 4\sum_{M\leq s<K} 1/s\right)$$

and hence that

$$o(K) \geq K\left(3 - 4\log(\frac{\log K}{\log M}) - o(1)\right)$$

We deduce that

$$M < (qr)^{1/4e^{3/4}+o(1)}.$$

Conclusion: It remains to use the two bounds as efficiently as possible, and this depends on what information one has as to the relative sizes of p, q and r. We have $r < pq$, and $q = O(p^2)$ (as well as $p < q < r$, of course) but there may be other constraints. Setting $p = n^a$, $q = n^b$, $r = n^c$ and $M = n^x$, one has $0 \leq a \leq b \leq c$, $a + b + c = 1$, $c < a + b$, $b \leq 2a + o(1)$ and we have to find the maximum of

$$x = min(\frac{(a+b)}{4\sqrt{e}}, \frac{(b+c)}{4e^{3/4}}) + o(1)$$

subject to these constraints. This is a linear programming problem: Maximize x so that $x \leq (a+b)/(4\sqrt{e})$, $x \leq (b+c)/(4e^{3/4})$, $0 \leq a \leq b \leq c$, $a+b+c=1$, $c < a+b$, $b \leq 2a + o(1)$. We solved this using Mathematica to get $x \approx 1/(6.568\sqrt{e})$.

This establishes that $w(n) = O_\epsilon(n^{1/(6.568\sqrt{e})+\epsilon})$. □

5.4 Discussion

Finally we are led to the following conjecture:

Conjecture 1 *For every composite number n we have $w(n) = O_\epsilon(n^{1/(8\sqrt{e})+\epsilon})$.*

Our conjecture is based on Lemma 5.2.7. Obviously, our conjecture is true if the GRH holds; due to Bach's result for $w(n)$ [7]. However it appears difficult to prove this without using the GRH.

It is easy to see that if our conjecture is true then we get an improvement over the primality test of Adleman and Leighton [2]. The new primality test will have a running time of $O_\epsilon(n^{1/(8\sqrt{e})+\epsilon})$.

No deterministic polynomial time algorithm is known for recognizing whether a number is a Carmichael number. However it is easy to show that these numbers can actually be factored in random polynomial time [16]. Finally, we note that the number of special Carmichaels up to x is actually $O(x^{5/14+o(1)})$ since it is known (see Chapter 3) that the number of Carmichael numbers up to a given number x, with exactly three prime factors is $O(x^{5/14+o(1)})$.

It will be interesting to make our bounds explicit and explore the connections of our results to [46].

Bibliography

[1] L. Adleman and M. Huang, Primality testing and two dimensional Abelian varieties over finite fields, *Lec. Notes in Math.* **1512**, Springer-Verlag (1994).

[2] L. Adleman and F. T. Leighton, An $O(n^{1/10.89})$ primality testing algorithm, *Math. Comp.* **36** (1981) 261–266.

[3] L. Adleman and K. S. McCurley, Open problems in number-theoretic complexity-II, in: L. M. Adleman and M. D. Huang (eds.), Algorithmic Number Theory, *LNCS* 877, Springer-Verlag, Berlin (1994), 291–322.

[4] L. Adleman, C. Pomerance and R. Rumely, On distinguishing prime numbers from composite numbers, *Ann. of Math.* **117** (1983) 173–206.

[5] W. R. Alford, A. Granville, and C. Pomerance, There are infinitely many Carmichael numbers, *Ann. of Math.* **140** (1994), 703–722.

[6] W. R. Alford, A. Granville and C. Pomerance, On the difficulty of finding reliable witnesses, in: L. M. Adleman and M. D. Huang (eds.), Algorithmic Number Theory, *LNCS* 877, Springer-Verlag, Berlin (1994), 1–16.

[7] E. Bach, Analytic methods in the analysis and design of number-theoretic algorithms, MIT Press, Cambridge, Mass. (1985).

[8] E. Bach, Explicit bounds for primality testing and related problems, *Math. Comp.* **55** (1990) 355-380.

[9] E. Bach, Number-theoretic Algorithms, in: *Ann. Rev. of Computer Science* **4** (1990) 119–172.

[10] E. Bach and L. Huelsbergen, Statistical evidence for small generating sets, *Math. Comp.* **61** (1993), 69–82.

[11] E. Bach and J. O. Shallit, *Algorithmic Number Theory* Vol. **I** (MIT Press, MA 1996).

[12] E. Bach and J. Sorenson, Sieve algorithms for perfect power testing, *Algorithmica* **9** (1993), 313–328.

[13] R. Balasubramanian and S. V. Nagaraj, Perfect power testing, *Info. Proc. Letters* **58** (2) (1996), 59–63.

[14] R. Balasubramanian and S. V. Nagaraj, Density of Carmichael numbers with three prime factors, *Math. Comp.* **66** (1997), 1705–1708.

[15] R. Balasubramanian and S. V. Nagaraj, The least witness of a composite number, in: E. Okamoto et al. (eds.), Information Security, *LNCS* 1396, Springer-Verlag, Berlin (1998), 66–74.

[16] P. Beauchemin, G. Brassard, C. Crepeau, C. Goutier and C. Pomerance, The generation of random numbers that are probably prime, J. Crypt. **1** (1988) 53–64.

[17] D. J. Bernstein, Detecting perfect powers in essentially linear time, *Math. Comp.* **67** (1998) 1253–1283.

[18] D. Bleichenbacher, Efficiency and security of cryptosystems based on number theory, Ph.D Thesis, Swiss Federal Institute of Technology, Diss. ETH No. 11404, Zurich 1996.

[19] W. Bosma and M. P. van der Hulst, Primality testing with cyclotomy, Ph.D Thesis, Faculteit Wiskunde en Informatica, Univ. of Amsterdam (1990).

[20] D. A. Burgess, On character sums and primitive roots, *Proc. London Math. Soc.* **12** (1962) 179–192.

[21] D. A. Burgess, On character sums and L-series II, *Proc. London Math. Soc.* **13** (1963) 524–536.

[22] R. J. Burthe, The average witness is 2, Ph.D Thesis, University of Georgia (1995).

[23] R. J. Burthe Jr., Upper bounds for least witnesses and generating sets, *Acta Arith.* **80** (1997) 311–326.

[24] R. J. Burthe Jr., The average witness is 2, *Acta Arith.* **80** (1997) 327–341.

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

[26] C. Pomerance, (ed.) Computational Number Theory and Cryptography, *Proc. of AMS Symp. in Appl. Math.* AMS (1990).

[27] I. Damgård, P. Landrock, and C. Pomerance, Average case error estimates for the strong probable prime test, *Math. Comp.* **61** (1993) 177–194.

[28] H. Davenport, *Multiplicative Number Theory,* (Springer Verlag, New York, 1980).

[29] S. W. Graham, Carmichael numbers with three prime factors, Unpublished Manuscript.

[30] A. Granville, Primality testing and Carmichael numbers, *Notices Amer. Math. Soc.* **39** (1992) 696–700.

[31] A. Granville, Some conjectures related to Fermat's last theorem, in: Proc. of the First Conference of the CNTA, Alberta, April 1988, pp. 177–192, (Walter de Gruyter, Berlin 1990).

[32] A. Granville, On pairs of co-prime integers with no large prime factors, *Expo. Math.* **9** (1991), 335–350.

[33] A. Granville, Carmichael numbers with exactly three prime factors, Unpublished Notes.

[34] A. Granville, Review of "Density of Carmichael numbers with three prime factors" by R. Balasubramanian and S. V. Nagaraj, *Math. Reviews.*

[35] H. Halberstam and H. E. Richert, *Sieve Methods*, (Academic Press, London, 1974).

[36] A. K. Lenstra and H. W. Lenstra Jr., Algorithms in Number Theory, in: P. M. Vitanyi and D. S. Johnson (eds.) Handbook of Theoretical Computer Science, Elsevier Science B.V. 1992.

[37] D. R. Heath-Brown, Personal Communication, April 1997.

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

[39] N. Koblitz, *A Course in Number Theory and Cryptography*, Graduate Texts in Mathematics, (Springer Verlag, New York 1987).

[40] S. Konyagin and C. Pomerance, On primes recognisable in deterministic polynomial time, in: R. L. Graham and J. Nesetril (eds.), Mathematics of Paul Erdos, Springer-Verlag, Berlin (1997).

[41] H. W. Lenstra, Jr., Miller's primality test, *Info. Proc. Lett.* **8** (1979) 86–88.

[42] J. H. Loxton, Some problems involving powers of integers, *Acta Arith.* **46** (1986) 113–123.

[43] G. L. Miller, Riemann hypothesis and tests for primality, *J. Comput. System Sci.* **13** (1976), 300–317.

[44] L. Monier, Evaluation and comparison of two efficient probabilistic primality testing algorithms, *Theoret. Comput. Sci.* **12** (1980) 97–108.

[45] Mohan Nair, Multiplicative functions of polynomial values in short intervals , *Acta Arith.* (3) **62** (1992) 257–269.

[46] R. Peralta and V. Shoup, Primality testing with fewer random bits, *Comp. Compl.* **3** (1993) 355-367.

[47] R. G. E. Pinch, The Carmichael numbers up to 10^{15}, *Math. Comp.* **61** (1993) 381–392.

[48] R. G. E. Pinch, The Carmichael numbers up to 10^{16}, Preprint (1993).

[49] R. G. E. Pinch, The Carmichael numbers up to 10^{18} with three prime factors, Unpublished Tables (1997).

[50] C. Pomerance, Carmichael Numbers, *Nieuw Archief voor Wiskunde* **11** (1993) 199–209.

[51] C. Pomerance, J. L. Selfridge, and S. S. Wagstaff, Jr. The pseudoprimes to $25 \cdot 10^9$, *Math. Comp.* **53** (1980) 1003-1026.

[52] M. O. Rabin, Probabilistic algorithm for testing primality, *J. Number Theory* **12** (1980) , 128–138.

[53] S. Ramanujan, Highly Composite Numbers, *Proc. London Math. Soc.* (2) **14** (1915) 347–409.

[54] P. Ribenboim, The Book of Prime Number Records (Second Edition), Springer Verlag, New York (1989).

[55] R. L. Rivest, A. Shamir and L. Adleman, A method for obtaining digital signatures and public key cryptosystems, *Comm. ACM* **21** (1978) 120–126.

[56] A. Schönhage and V. Strassen, Schnelle Multiplikation grosser Zahlen, *Computing* **7** (1971), 281–292.

[57] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge Studies in Advanced Mathematics No. 46, (Cambridge University Press, 1995).

[58] E. C. Titchmarsh, A divisor problem, *Rend. Circ. Mat. Palermo* **54** (1930), 414–429.