THREE PROBLEMS IN ARITHMETIC

by

Nicholas Egbert

A Dissertation

Submitted to the Faculty of Purdue University

In Partial Fulfillment of the Requirements for the degree of

Doctor of Philosophy

Department of Mathematics

West Lafayette, Indiana

December 2021

THE PURDUE UNIVERSITY GRADUATE SCHOOL
STATEMENT OF COMMITTEE APPROVAL

Dr. Samuel Wagstaff, Chair

Center for Education and Research in Information Assurance and Security, and
Department of Computer Sciences

Dr. Trevor Wooley

Department of Mathematics

Dr. Tong Liu

Department of Mathematics

Dr. Kenji Matsuki

Department of Mathematics

Approved by:

Dr. Plamen Stefanov

To my son, Camden, and his future brother Levi.

ACKNOWLEDGMENTS

The journey to and through graduate school is hardly an easy one and would not be possible without the help of many others. Both professionally and personally, there are far more people than I can reasonably mention here that have played a part in this effort.

First, I must thank my advisor, Samuel Wagstaff. He has served as a great mentor as he has guided me through this whole research process, from suggesting each problem to providing guidance toward a solution when I have been stuck. Additional thanks is necessary for helping me to graduate a semester earlier than we had originally planned.

I owe my parents a great deal of thanks for teaching me good work ethic and determination. Their faith in me is most clearly demonstrated when they supported me to pursue B.S. and then a Ph.D. in mathematics without a clear path to a career outside of academia.

In alphabetical order, to Roy Araiza and Matt Weaver, thank you for the years of friendship and giving me a space to talk about all the math things that no one else wants to hear about.

To the many great math professors that I have had both here at Purdue and at Indiana as an undergraduate. Special mention at IU must go to Kent Orr and Alberto Torchinsky, who were not only great professors but mentors too, as well as Kevin Pilgrim, who provided much needed advice as I considered going to graduate school. For the professors at Purdue, special mention must go to the other members of my committee: Trevor Wooley, Tong Liu, and Kenji Matsuki.

I also owe thanks to Brian Lukich, my high school calculus teacher. At that time I thought I wanted to become a medical doctor but was still undecided in terms of a major. It sounds really cheesy, but in just sharing how he decided to become a math teacher, he made me realize that I should study math. Needless to say, I did not end up going to medical school.

While my role as a graduate student is research-focused, a great deal of this experience has been in teaching. In that regard, I would like to thank Dominic Naughton for giving me such a wide range of courses to teach. I believe that has helped me immensely to improve my

communication skills. I would also like to thank Brooke Max for all of her help in teaching mathematics for elementary teachers.

Lastly, I can only begin to express sufficient gratitude for the sustained support from my wife, Christina. By virtue of getting married toward the beginning of graduate school, the honeymoon period came to an abrupt end after we returned from our actual honeymoon, as I juggled teaching calculus and studying for qualifying exams that first summer. She has helped to pick me up from various lows and has been with me to celebrate each little success.

Christina has sacrificed so much in how we have started our lives together in order to make this possible—from making career moves based on our financial needs, to quiet nights on the couch as I tried to catch up on work, to being the default caretaker when our son gets sick. Over the last six years, Christina has done nothing but put myself and my education above her own needs, and I hope I can give back that same level of support and commitment as we enter a new chapter in our lives.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF SYMBOLS

$(a \mid n)$	Jacobi symbol
$\binom{n}{k}$	binomial coefficient
c_2	twin prime constant, approximately 0.6601618
$\mathbb{C}$	complex numbers
$E(K)$	elliptic curve over the field K
$\mathbb{F}_q$	finite field with q elements
$\Phi_n(x)$	nth cyclotomic polynomial
G	abelian group
G^*	group of units of G
$\gcd(a, b)$	greatest common divisor of a and b
$\lambda(G)$	largest order of an element of G
$\mathrm{li}(x)$	logarithmic integral of x, $\int_2^x \frac{1}{\log t}\,\mathrm{d}t$
$\log(x)$	natural logarithm of x
$\mathrm{lprp}(P, Q)$	Lucas probable prime with parameters P, Q
$\mathrm{lpsp}(P, Q)$	Lucas pseudoprime with parameters P, Q
$n(G)$	Davenport's constant
$\mathcal{O}$	point at infinity for an elliptic curve $E(K)$
$O(g(n))$	big O notation
$\omega(n)$	number of distinct prime divisors of n
$\Omega(n)$	number of prime divisors of n, counted with multiplicity
$P(n)$	largest prime divisor of n
$\mathrm{psp}(a)$	pseudoprime to base a
$\pi(z; d, a)$	number of primes $p \leq z$ such that $p \equiv a \pmod{d}$
$\pi(x)$	number of primes $p \leq x$
$\pi_{a,b}(x)$	number of primes $p \leq x$ such that $ap + b$ is prime
$\Pi_{a,b}$	product of $\frac{p-1}{p-2}$ taken over primes p dividing ab with $p > 2$
$\mathrm{rad}(n)$	radical of n, i.e., the product of distinct primes dividing n
ρ	$8 \cdot 3 \cdot 7 \cdot 11 \cdot 19 \cdot 43 \cdot 67 \cdot 163$

$\mathbb{Q}$	rational numbers
$\mathbb{R}$	real numbers
$\mathrm{slprp}(P, Q)$	strong Lucas probable prime with parameters P, Q
$\mathrm{slpsp}(P, Q)$	strong Lucas pseudoprime with parameters P, Q
$\mathrm{spsp}(a)$	strong pseudoprime to base a
$\mathcal{S}_{a,b}$	set of primes p such that $ap + b$ is prime
$S_{a,b}$	sum of $\frac{1}{p}$ for $p \in \mathcal{S}_{a,b}$
$S_{a,b}(x)$	sum of $\frac{1}{p}$ for $p \in \mathcal{S}_{a,b}$ with $p \leq x$
$s(G)$	$\lceil 5\lambda(G)^2\Omega(\lambda(G))\log(3\lambda(G)\Omega(\#G))\rceil$
$\mathrm{vprp}(P, Q)$	Lucas-V probable prime with parameters P, Q
$\mathrm{vpsp}(P, Q)$	Lucas-V pseudoprime with parameters P, Q
ζ_k	primitive kth root of unity
$\zeta(s)$	Riemann zeta function
$\mathbb{Z}$	integers
$\mathbb{Z}_n$	integers modulo n

ABSTRACT

It is well-known that the sum of reciprocals of twin primes converges or is a finite sum. In the same spirit, Samuel Wagstaff proved in 2021 that the sum of reciprocals of primes p such that $ap + b$ is prime also converges or is a finite sum for any a, b where $\gcd(a, b) = 1$ and $2 \mid ab$. Wagstaff gave upper and lower bounds in the case that ab is a power of 2. Here, we expand on his work and allow any a, b satisfying $\gcd(a, b) = 1$ and $2 \mid ab$. Let $\Pi_{a,b}$ be the product of $\frac{p-1}{p-2}$ over the odd primes p dividing ab. We show that the upper bound of these sums is $\Pi_{a,b}$ times the upper bound found by Wagstaff and provide evidence as to why we cannot hope to do better than this. We also give several examples for specific pairs (a, b).

Next, we turn our attention to elliptic Carmichael numbers. In 1987, Dan Gordon defined the notion of an elliptic Carmichael number as a composite integer n which satisfies a Fermat-like criterion on elliptic curves with complex multiplication. More recently, in 2018, Thomas Wright showed that there are infinitely such numbers. We build off the work of Wright to prove that there are infinitely many elliptic Carmichael numbers of the form $a \pmod{M}$ for a certain M, using an improved lower bound due to Carl Pomerance. We then apply this result to comment on the infinitude of strong pseudoprimes and strong Lucas pseudoprimes.

Finally, we consider the problem of classifying for which k does one have $\Phi_k(x) \mid \Phi_n(x) - 1$, where $\Phi_n(x)$ is the nth cyclotomic polynomial. We provide a motivating example as to how this can be applied to primality proving. Then, we complete the case $k = 8$ and give a partial characterization for the case $k = 16$. This leads us to conjecture necessary and sufficient conditions for when $\Phi_k(x) \mid \Phi_n(x) - 1$ whenever k is a power of 2.

1. INTRODUCTION

Mathematics is queen of the sciences and arithmetic the queen of mathematics. She often condescends to render service to astronomy and other natural sciences, but under all circumstances the first place is her due.

Carl Friedrich Gauss

The greatest endeavor of number theory is the study of prime numbers. Since the time of Euclid c. 300 BC, we have known that there are infinitely many primes. And Euclid's proof, as it is translated into modern English, is so elementary that the non-mathematician can easily follow it and be convinced of this fact. Yet, despite thousands of years of great progress in studying prime numbers, we still know surprisingly little about them.

Given an integer N, there are three basic questions concerning primes that we can ask:

- How likely is it that N is prime?
- How can we determine whether N is prime?
- If N is composite, how can we determine its prime factorization?

Each of the problems that we address in this thesis is related to one of these questions. To get a better idea of how it all fits together, we survey what is already known about these three questions.

1.1 How rare are the prime numbers?

Given a random integer n less than x, how likely is it that n is prime? The prime number theorem answers this. Let $\pi(x)$ denote the number of primes less than or equal to x.

Theorem 1.1.1 (Prime number theorem)**.** There is a positive constant c such that

$$\pi(x) = \mathrm{li}(x) + O\Big(x \cdot \exp(-c\sqrt{\log x})\Big),$$

where

$$\mathrm{li}(x) = \int_2^x \frac{\mathrm{d}t}{\log t}.$$

is the logarithmic integral.

As with any estimate, one strives for the best possible bounds. In his only paper in the field of number theory, Riemann [32] in 1859 used methods from complex analysis to connect what we now call the Riemann zeta function and the distribution of prime numbers.

1.1.1 The Riemann hypothesis

Let $s = \sigma + i\tau$, where σ, τ are real numbers with $\sigma > 1$. The Riemann zeta function is defined by

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

The connection between this function and the prime numbers is far from obvious. But in 1737, Euler proved the identity

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \text{ prime}} \frac{1}{1 - p^{-s}}. \tag{1.1}$$

The Riemann zeta function has a simple pole at $s = 1$, and thus has a unique analytic continuation to a meromorphic function on the complex plane with a simple pole at $s = 1$. That is, there exists a unique complex function that is analytic on $\mathbb{C} \setminus \{1\}$ and agrees with $\zeta(s)$ for $\sigma > 1$. For $0 < \sigma < 1$, $\zeta(s)$ satisfies the functional equation

$$\zeta(s) = 2^s \pi^{s-1} \sin \frac{\pi s}{2} \Gamma(1-s)\zeta(1-s).$$

From the functional equation, it is easy to see that there are so-called *trivial zeros* for $\zeta(s)$ whenever s is a negative even integer, as the sine term evaluates to 0 in this case. The Riemann hypothesis makes an assertion on the location of the nontrivial zeros of $\zeta(s)$:

Conjecture (Riemann Hypothesis)**.** *The zeros of $\zeta(s)$ in the strip $0 < \sigma < 1$ satisfy $s = \frac{1}{2}$.*

Using the ideas of Riemann, Hadamard and de la Vallée Poussin proved in 1896 that there are no zeros to the Riemann zeta function on the line $1 + it$. It turns out that this implies a slightly weaker version of the prime number theorem than is stated in Theorem 1.1.1. Namely, we have

$$\pi(x) \sim \frac{x}{\log x}.$$

Though the error $|\pi(x) - x/\log x|$ is larger than the error $|\pi(x) - \mathrm{li}(x)|$, the prime number theorem in this form gives a more intuitive notion of how often prime numbers occur. Given a random integer N, the probability that N is prime is about $\frac{1}{\log N}$. Given how slowly $\log N$ grows relative to N, we see that prime numbers are fairly common in some sense.

In 1901, von Koch [37] gave the best estimate on the error $|\pi(x) - \mathrm{li}(x)|$ in terms of an unspecified constant c as a consequence of the Riemann hypothesis. Schoenfeld [34] later found that one can take the constant in the theorem to be $c = 1/8\pi$ for $x \geq 2657$.

Theorem 1.1.2. Assuming the Riemann hypothesis is true, for some positive constant c, we have

$$|\pi(x) - \mathrm{li}(x)| < c\sqrt{x}\log x.$$

1.1.2 Sums of reciprocals of primes

In an introductory calculus course, the first example of a divergent series that students learn is the harmonic series

$$\sum_{n=1}^{\infty} \frac{1}{n}.$$

More precisely, one has $\sum_{n=1}^{x} \frac{1}{n} = \log x + O(1)$. A natural question is whether the set of primes is rare enough that the above sum converges when we restrict to summing over just the primes. It turns out the answer is no. By Equation (1.1), we have

$$\sum_{n \leq x} \frac{1}{n} \leq \prod_{p \leq x} \left(1 - \frac{1}{p}\right)^{-1}.$$

Taking the logarithm of both sides, we have

$$-\sum_{p \leq x} \log\left(1 - \frac{1}{p}\right) \geq \log\log x + O\left(\frac{1}{\log x}\right).$$

The left hand side of the above inequality is

$$\sum_{p \leq x} \left(\frac{1}{p} + \frac{1}{2p^2} + \frac{1}{3p^3} + \cdots\right) = \sum_{p \leq x} \frac{1}{p} + O(1).$$

From this we can conclude that

$$\sum_{p \leq x} \frac{1}{p} \geq \log\log x + O(1),$$

hence the sum of reciprocals of primes also diverges.

Although $\sum_p \frac{1}{p}$ diverges when the sum is taken over all primes p, we can consider subsets $\mathcal{S}$ of primes where we do have convergence (or a finite sum). Most famously, Brun [8] proved that the sum

$$\sum_{p \in \mathcal{S}} \left(\frac{1}{p} + \frac{1}{p+2} \right),$$

where $\mathcal{S}$ is the set of twin primes (Sequence A001359 in the OEIS [26]), converges or is finite. It is worth noting that we still do not know whether the set of twin primes is infinite. It is widely believed that there are infinitely many twin primes, and substantial progress has been made in recent years. In 2013, Zhang [41] proved that there are infinitely many primes differing by at most 70 million. Using different methods, Maynard [22] improved this bound to 600, and the Polymath Project [29] improved this to 246.

There are many other possible sets $\mathcal{S}$ of interest. Wagstaff [38] considered the set of Germain primes, that is, the set $\mathcal{S} = \{p \text{ prime} \colon 2p+1 \text{ is prime}\}$. Such primes are named after Sophie Germain, who proved the first case of Fermat's last theorem is true for these primes. As with twin primes, it is not known whether there are infinitely many Germain primes. However, for fixed a, b with $\gcd(a,b) = 1$ and $2 \mid ab$, Theorem 1 of Wagstaff [38] shows that the sum

$$\sum_{p \in \mathcal{S}_{a,b}} \frac{1}{p}$$

either converges or is finite, where $\mathcal{S}_{a,b} = \{p \text{ prime} \colon ap+b \text{ is prime}\}$. Thus, the primes p such that $ap+b$ is prime are rarer than all primes.

1.2 Primality testing

After determining the distribution of primes, we have a good estimate on how likely a randomly chosen integer is prime. But given a random integer N, how do we determine whether it is prime? The naïve approach would be to use the sieve of Eratosthenes to check if any of the primes up to $\sqrt{N}$ divide N. This is, of course, extremely impractical for large values of N.

1.2.1 Pseudoprimes and Carmichael numbers

It is desirable to have an efficient test to determine whether a number is prime. The first step toward this is Fermat's little theorem:

Theorem (Fermat)**.** *If p is prime and a is an integer such that $\gcd(a, p) = 1$, then*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Unfortunately, the converse of Fermat's little theorem is not true. In fact, $341 = 11 \cdot 31$, yet $2^{340} \equiv 1 \pmod{341}$. We call 341 a *pseudoprime to base 2*, and it is the smallest composite number with this property. The pseudoprimes to base 2 are Sequence A001567 in the OEIS [26]. A composite number n that satisfies the conclusion of Fermat's little theorem for every a coprime to n is called a *Carmichael number*. The Carmichael numbers are Sequence A002997 in the OEIS, and the smallest such number is $561 = 3 \cdot 11 \cdot 17$. Not only are there infinitely many Carmichael numbers, but Wright [39] proved that for every positive integer m, there are infinitely many Carmichael numbers of the form $a + km$ if $\gcd(a, m) = 1$.

Let N be an odd positive integer. In 1927, Lehmer [20] proved an extra condition needed to get the converse to Fermat's little theorem provided that we know the complete factorization of $N - 1$.

Theorem (Lehmer)**.** *Suppose N satisfies the conclusion of Fermat's little theorem for some integer a. If, moreover, $a^{(N-1)/q} \not\equiv 1 \pmod{N}$ for every prime q dividing $N - 1$, then N is prime.*

Of course, it can be very difficult to completely factor $N - 1$. If replace the divisibility condition in Lehmer's theorem with a gcd condition, Pocklington [28] proved that only a partial factorization of $N - 1$ is needed to prove that N is prime.

Theorem 1.2.1 (Pocklington)**.** Suppose $N - 1 = FR$, where $\gcd(F, R) = 1$, $F \geq \sqrt{N}$ and the complete factorization of F is known. If there exists an integer a such that for every prime factor p of F, we have $a^{N-1} \equiv 1 \pmod{N}$ and $\gcd(a^{(N-1)/p} - 1, N) = 1$, then N is prime.

1.2.2 Probabilistic tests for primality

Having even a partial factorization of $N-1$ is not always an easy task. There are other tests for special probable primes. One is Pepin's test, which can be used for Fermat numbers, that is, numbers of the form $2^{2^k}+1$ for $k \geq 0$. Another is the Lucas-Lehmer test, which can be used to prove whether a Mersenne number is prime, that is, a number of the form 2^p-1, where p is a prime number. These tests are also very limiting, but if we are willing to allow for a small chance of error, there are many probabilistic tests for primality.

Miller-Rabin primality test

Suppose $N > 2$ is an odd integer, and write $N-1 = 2^f d$, where f, d are positive integers and $2 \nmid d$. If either $a^d \equiv 1 \pmod{N}$ or $a^{d \cdot 2^e} \equiv -1 \pmod{N}$ for some e with $0 \leq e < f$, then we call N a *strong probable prime to base a*. If N is composite, then we call N a *strong pseudoprime to base a*. There is no analogue of Carmichael numbers for strong pseudoprimes, as the following theorem suggests:

Theorem (Monier [24], Rabin [31])**.** *Let $N > 9$ be an odd integer. Then the number of bases a to which N is a strong pseudoprime is at most $\phi(N)/4$.*

This provides the basis for the Miller-Rabin primality test. If we randomly choose a base a with $1 \leq a \leq N$ and perform the strong probable prime test, then the above theorem shows that if N is composite, the probability that a reveals the compositeness of N is at least $3/4$. Thus, the probability that a composite N is a strong probable prime for k randomly chosen bases is less than 4^{-k}.

Lucas probable prime test

Some of the basic definitions are revisited in Chapter 3, but we review more of the background information regarding Lucas probable primes. Let P, Q be integers. There are two kinds of Lucas sequences, $U_n(P,Q)$, $V_n(P,Q)$, with parameters P, Q that are recursively defined as follows: put $U_0(P,Q) = 0$, $U_1(P,Q) = 1$, and

$$U_n(P,Q) = P \cdot U_{n-1}(P,Q) - Q \cdot U_{n-2}(P,Q), \quad n > 1;$$

Table 1.1. The first few terms of the Lucas sequences $U_n(P,Q)$ and $V_n(P,Q)$

n	$U_n(P,Q)$	$V_n(P,Q)$
0	0	2
1	1	P
2	P	P^2-2Q
3	P^2-Q	P^3-3PQ
4	P^3-2PQ	$P^4-4P^2Q+2Q^2$
5	$P^4-3P^2Q+Q^2$	$P^5-5P^3Q+5PQ^2$

and similarly, put $V_0(P,Q)=2$, $V_1(P,Q)=P$, and

$$V_n(P,Q)=P\cdot V_{n-1}(P,Q)-Q\cdot V_{n-2}(P,Q),\quad n>1.$$

The Lucas sequences are a generalization of the Fibonacci sequence. If we take $(P,Q)=(1,-1)$, then $U_n(1,-1)$ gives the nth Fibonacci number. The first few terms of $U_n(P,Q)$ and $V_n(P,Q)$ are given in Table 1.1.

Let P and Q be integers such that $D=P^2-4Q\neq 0$ and $P>0$. For an odd positive integer n, let $\varepsilon(n)=(D\,|\,n)$ denote the Jacobi symbol, and write $\delta(n)=n-\varepsilon(n)$. If n is an odd prime and $\gcd(n,Q)=1$, then the following congruences hold:

$$U_{\delta(n)}\equiv 0 \pmod{n}, \tag{1.2}$$

$$V_{\delta(n)}\equiv 2Q^{(1-\varepsilon(n))/2} \pmod{n}\quad \text{provided } \gcd(n,D)=1, \tag{1.3}$$

$$U_n\equiv \varepsilon(n) \pmod{n}, \tag{1.4}$$

$$V_n\equiv V_1=P \pmod{n}. \tag{1.5}$$

Any of the congruences (1.2)–(1.5) could be used as a probable prime test. An integer n satisfying (1.2) is called a *Lucas probable prime with parameters P and Q*. If n is composite, we call n a *Lucas pseudoprime with parameters P and Q*.

Baillie-Wagstaff [4] also defined the notion of a *strong Lucas probable prime*: for an odd integer n, write $n+1 = d \cdot 2^s$, where d is odd. If n is prime and $(D \,|\, n) = -1$, then either

$$U_d \equiv 0 \pmod{n}, \quad \text{or} \tag{1.6}$$

$$V_{d \cdot 2^r} \equiv 0 \pmod{n}, \quad \text{for some } r \text{ with } 0 \leq r < s. \tag{1.7}$$

A composite n satisfying (1.6) or (1.7) is called a *strong Lucas pseudoprime*.

Baillie-PSW primality test

In Baillie-Wagstaff [4], the authors combined a base 2 strong probable prime test with a strong Lucas probable prime test to obtain a very effective test. The original Baillie-PSW works in the following way:

1. If n is not a strong base-2 pseudoprime, then output composite.
2. Let D be the first element of the sequence $5, -7, 9, -11, 13, -15, \ldots$ for which $(D \,|\, n) = -1$. Let $P = 1$ and $Q = (1-D)/4$. If $Q = -1$, change both P and Q to 5. If you encounter D such that $(D \,|\, n) = 0$ with either $|D| < n$ or $|D| \geq n$ but $n \nmid |D|$, then output composite.
3. If n does not satisfy either (1.6) or (1.7), then output composite. Otherwise, output probably prime.

In Baillie-Fiori-Wagstaff [3], the authors give an enhanced test that adds a step to check if (1.3) holds as well as a check for Euler's criterion. The added steps require little extra computation, but because so few composite n satisfy (1.3), this is a more powerful test. It is worth noting that no composite n is known that passes steps 1 through 3 enumerated above.

Elliptic curves in primality testing

Elliptic curves have many number-theoretic applications. One such application is primality testing. As we will see in Chapter 3, we can define an analogue of Carmichael numbers on elliptic curves. There's also an analogue of Pocklington's theorem without the requirement of finding enough prime factors of $N-1$ to obtain $F \geq \sqrt{N}$. The following theorem is due to Goldwasser-Kilian [13]:

Theorem. *Let $N > 1$ and let E be an elliptic curve* mod N. *Suppose there exist distinct prime numbers $\ell_1, \ldots, \ell_k$ and finite points $P_i \in E(\mathbb{Z}_N)$ such that*

$$\ell_i P_i = \mathcal{O} \text{ for } 1 \leq i \leq k \quad \text{and} \quad \prod_{i=1}^{k} \ell_i > \left(N^{1/4}+1\right)^2.$$

Then N is prime.

1.3 Factoring integers

Factoring integers is intimately related to determining which integers are prime, as it is ill-advised to try to factor a prime number. As we discussed in Section 1.2, one way to prove that a number p is prime is by (at least partially) factoring $p-1$. The main general-purpose factoring methods are the quadratic sieve and the general number field sieve.

Two particular special-purpose factoring algorithms are worth mentioning: the elliptic curve method (ECM), originally proposed by Hendrik Lenstra in 1987, which can reliably find prime factors of less than 60 decimal digits, and Pollard's $p-1$ algorithm. If we are trying to factor an integer N, ECM works by fixing a point P on an elliptic curve E modulo N and computing kP for some integer k. If this computation fails, we have found a factor of N. If p is a prime factor of N, Pollard's algorithm leverages Fermat's little theorem to try to find a multiple of $p-1$ by computing $\gcd(a^k-1, N)$.

1.4 Applications to cryptography

Two of the most widely used public key cryptosystems today are RSA and an elliptic curve variant of the Diffie-Helman key exchange (ECDH). We recall the basics of each of these cryptosystems and state the relevance of the results of Chapter 4 to each cryptosystem. The typical players are Alice and Bob, who are trying to establish a secure connection over an insecure channel.

Let ζ_n be a primitive nth root of unity, and write

$$\Phi_n(x) = \prod_{\substack{1 \le k < n \\ \gcd(n,k)=1}} (x - \zeta_n^k),$$

for the nth cyclotomic polynomial. In Section 4.2, we give an example of how one can prove that, for some integer b, $p = \Phi_n(b)$ is prime using the results of Chapter 4.

1.4.1 RSA protocol

Let $n = pq$ be the product of two large primes. Choose a random integer e coprime to $\phi(n) = \phi(pq) = (p-1)(q-1)$. Compute d such that $ed \equiv 1 \pmod{\phi(n)}$. Given a plaintext message encoded as an integer M, where $0 < M < n$, the ciphertext is $C = M^e \pmod{n}$. To recover M, one computes

$$C^d \equiv (M^e)^d \equiv M \pmod{n}.$$

Thus, one could choose a prime $p = \Phi_n(b)$, provided that $n = pq$ is large enough so that the Number Field Sieve will not factor n in a reasonable amount of time, and $p-1 = \Phi(b)-1$ should have large prime factors to prevent Pollard's $p-1$ algorithm from finding a factor. Of course, the method in which p was obtained should be kept secret.

1.4.2 ECDH protocol

Let $q = p^e$, where p is prime and e is an integer with $e \ge 1$. The ECDH key exchange has the following steps:

1. Alice and Bob agree on an elliptic curve E over a finite field $\mathbb{F}_q$ such that the discrete log problem is hard for $E(\mathbb{F}_q)$. They also agree on a point $P \in E(\mathbb{F}_q)$ of large prime order.

2. Alice chooses a secret integer a and computes aP. She sends this point to Bob.

3. Similarly, Bob chooses a secret integer b, computes bP and sends this point to Alice.

4. Alice computes $a(bP) = (ab)P$ and Bob computes $b(aP) = (ba)P = (ab)P$.

5. Alice and Bob use the shared secret abP to derive a shared secret key.

If we wanted to use the cyclotomic method to find a prime p to use for ECDH, we need $\sqrt{q}$ to be large enough to ensure that the discrete log problem on the elliptic curve $E(\mathbb{F}_q)$ cannot be solved in a reasonable amount of time from attacks such as the MOV attack, Pollard's rho method, or pairing attacks.

1.5 Outline of this work

In Chapter 2, we expand on the work of Wagstaff [38] and give upper and lower bounds on the sum $S_{a,b} = \sum_{p \in \mathcal{S}_{a,b}} 1/p$, where $\mathcal{S}_{a,b}$ is the set of primes p such that $ap + b$ is prime. We obtain results similar to those of Wagstaff [38], but we allow for any positive integers a, b with $\gcd(a, b) = 1$ and $2 \mid ab$.

The best-known lower bound for $S_{a,b}$ is found by simply computing $S_{a,b}(x_0)$, which we define to be the sum of $1/p$, where $p \in \mathcal{S}_{a,b}$ and $p \leq x_0$. Then the best upper bound for $S_{a,b}$ is given by

$$S_{a,b} < S_{a,b}(x_0) - \frac{\pi_{a,b}(x_0)}{x_0} + \prod_{\substack{p>2 \\ p \mid ab}} \frac{p-1}{p-2} \int_{x_0}^{\infty} \frac{\pi_{a,b}(t)}{t^2} \, \mathrm{d}t.$$

By explicit computation, we find that $1.2608 < S_{1,6} < 1.9760$, $1.5952 < S_{2,3} < 2.3289$, $1.5762 < S_{4,3} < 1.6737$, $1.6779 < S_{2,15} < 2.6316$, and $1.1580 < S_{1,210} < 2.3023$.

In Chapter 3, we combine the ideas of Wright [39, 40] and Pomerance [30] to prove that there are infinitely many elliptic Carmichael numbers in certain arithmetic progressions. More specifically, let $\rho = 8 \cdot 3 \cdot 7 \cdot 11 \cdot 19 \cdot 43 \cdot 67 \cdot 163$, let M be a positive integer, and let a be such that $\gcd(a, M) = 1$. Moreover, assume that either $\gcd(M, \rho) = 1$ or $\gcd(M, \rho) > 1$ and $a \equiv -1 \pmod{\gcd(M, \rho)}$. Then there are infinitely many elliptic Carmichael numbers m such that $m \equiv a \pmod{M}$. For a precise definition of an elliptic Carmichael number, see Section 3.1.2. By following Pomerance [30], we are able to say explicitly that the number of elliptic Carmichael numbers up to some number X that are congruent to a modulo M is bounded below by $X^{1/6 \log\log\log X}$.

We then use this result to make statements about strong pseudoprimes and Lucas pseudoprimes. More specifically, the same lower bound on the number of elliptic Carmichael numbers up to X congruent to a modulo M applies to the number of elliptic Carmichael numbers that are also strong Lucas pseudoprimes.

In Chapter 4, we are interested in determining all integers n for which $\Phi_k(x)$ divides $\Phi_n(x) - 1$, where $\Phi_n(x)$ is the nth cyclotomic polynomial and k is a power of 2. In the case $k = 8$, we have $\Phi_n(\zeta_8) = 1$ if and only if one of the following conditions holds:

- $n = p^e n'$ with $p \nmid n'$, $p \equiv 1 \pmod 8$ and $n' \neq 8$;
- $8 \mid n$ and $n \neq 8p^e$ with p prime and e a nonnegative integer;
- $n = p^e n'$ with $p \nmid n'$, $p \equiv -1 \pmod 8$ and $8 \mid \phi(n')$;
- $n = 4m$, where m is odd but $m \neq q_1^{e_1} q_2^{e_2}$, where $q_i \equiv 3 \pmod 4$ and $e_j > 0$.

More generally, we have $\Phi_n(\zeta_k) = 1$ if

- $n = p^f n'$ with $p \nmid n'$, $p \equiv 1 \pmod k$ and $n' \neq k$;
- $k \mid n$ and $n \neq kp^f$ with p prime and f a nonnegative integer;
- $n = p^f n'$ with $p \nmid n'$, $p \equiv -1 \pmod k$ and $k \mid \phi(n')$.

If m is odd and $e \geq 3$, then $\Phi_{2^{e-1}m}(\zeta_k) = \Phi_{2m}(\zeta_k^{2^{e-2}})$. By repeatedly using this identity to add conditions to the list above, we conjecture that this process finds all n such that $\Phi_n(\zeta_k) = 1$.

This result has applications in primality proving: we show that if $\Phi_n(b)$ is a probable prime and k is large enough relative to n, knowing whether $\Phi_k(b)$ divides $\Phi_n(b) - 1$ can be used to prove that $\Phi_n(b)$ is prime.

2. SUMS OF RECIPROCALS OF CERTAIN PRIMES

2.1 Introduction

It is well-known that the sum $\sum_p \frac{1}{p}$ taken over all primes p diverges. However, if we restrict this sum to certain primes, we can say that it is either finite or converges. For example, in 1919 Brun [8] proved that the sum

$$B = \frac{1}{3} + \frac{1}{5} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \frac{1}{19} + \cdots$$

of reciprocals of twin primes is finite or convergent. Twin primes are the primes p such that $p+2$ is also prime. Various authors have given estimates on the lower and upper bounds for B. Klyve [18] showed that $B < 2.347$, and, using the number of twin primes up to $4 \cdot 10^{18}$ computed by Oliveira e Silva [36], Platt and Trudgian [27] improved the bounds on B to $1.840503 < B < 2.288513$.

Wagstaff [38] uses an idea of Klyve [38] to put bounds on the sum of reciprocals of Germain primes. These are the primes p such that $2p+1$ is also prime. They are named after Sophie Germain, who proved in the early 19th century that the first case of Fermat's last theorem is true for these primes. With little extra work, Wagstaff studies more generally the primes p such that $2^k p + 1$ is also prime for k a positive integer. We will use the ideas of Klyve and Wagstaff to study the primes p such that $ap + b$ is also prime, where a, b are positive integers such that $\gcd(a, b) = 1$ and $2 \mid ab$.

2.2 Notation

Throughout this chapter, p will always denote a prime number. Let

$$c_2 = \prod_{p>2} \left(1 - \frac{1}{(p-1)^2}\right) \approx 0.6601618158468695739278121100$$

denote the twin prime constant. Since we will use it often, write $\Pi_{a,b} = \prod_{\substack{p>2 \\ p \mid ab}} \frac{p-1}{p-2}$.

Following the notation of Wagstaff [38], let a and b be positive integers with $\gcd(a,b)=1$ and $2\,|\,ab$. Let $\mathcal{S}_{a,b}=\{p : ap+b \text{ is prime}\}$. For $x>0$, let

$$S_{a,b}(x)=\sum_{\substack{p\in\mathcal{S}_{a,b}\\ p\le x}}\frac{1}{p} \quad\text{and}\quad S_{a,b}=\lim_{x\to\infty}S_{a,b}(x).$$

Theorem 1 of Wagstaff [38] shows that the limit defined above indeed exists. With this notation, for example,

$$S_{1,6}=\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{23}+\frac{1}{31}+\cdots$$

Some values of $S_{a,b}(x)$ are listed in Table 2.1.

Hardy-Littlewood [16] gave the following heuristic estimate to $\pi_{a,b}(x)$ for fixed integers a,b with $\gcd(a,b)=1$:

$$\pi_{a,b}(x)\approx 2c_2\int_2^x\frac{\mathrm{d}t}{(\log t)^2}\Pi_{a,b}.$$

Assuming this heuristic, we have

$$S_{a,b}-S_{a,b}(x_0)\approx 2c_2\int_{x_0}^{\infty}\frac{\mathrm{d}t}{t(\log t)^2}\Pi_{a,b}=\frac{2c_2}{\log x_0}\Pi_{a,b}.$$

This tells us that the most probable value for $S_{a,b}$ is $S_{a,b}(x_0)+2c_2\Pi_{a,b}/\log x_0$, and these values are shown in Table 2.2. Though these values fall within the proved bounds for $S_{a,b}$, there is no proof that they are close to the actual values.

2.3 Upper bound on $S_{a,b}$

The upper bound for $S_{a,b}$ is a consequence of Lemma 5 of Riesel and Vaughan [33]. We quote the lemma as it was stated in Wagstaff [38] and Klyve [18] using Inequality (3.20) from the proof of the lemma.

Theorem 2.3.1. *Let a and b be integers with $a>0$, $b\neq 0$ and $(a,b)=1$. Let*

$$R(x,a,b)=\sup_I\sum_{\substack{p\in I\\ ap+b \text{ prime}}}1,$$

Table 2.1. Some values of $S_{a,b}(x)$

x_0	$S_{1,6}(x_0)$	$S_{2,3}(x_0)$	$S_{4,3}(x_0)$	$S_{2,15}(x_0)$	$S_{1,210}(x_0)$
10^2	0.804185874	1.179287658	1.193283754	1.118577288	0.461540610
10^3	0.980166932	1.335566331	1.326291712	1.324714081	0.714813987
10^4	1.077007694	1.419969395	1.408207973	1.442899187	0.863457788
10^5	1.133265114	1.472766204	1.458448578	1.515002978	0.953932023
10^6	1.171252493	1.509006595	1.492879361	1.562916841	1.014589034
10^7	1.198509361	1.535061658	1.517928733	1.597571402	1.058313024
10^8	1.218942074	1.554732337	1.536874048	1.623831797	1.091077663
10^9	1.234866106	1.570107346	1.551737985	1.644327983	1.116558352
10^{10}	1.247606323	1.582456463	1.563720191	1.660794818	1.136945140
10^{11}	1.258031457	1.592590215	1.573579054	1.674307435	1.153626418
$2 \cdot 10^{11}$	1.260808459	1.595294297	1.576213781	1.67791286	1.158069940

Table 2.2. Most probable values of $S_{a,b}$

x_0	$S_{1,6}$	$S_{2,3}$	$S_{4,3}$	$S_{2,15}$	$S_{1,210}$
10^2	1.377595141	1.752696925	1.766693022	1.883122978	1.378995438
10^3	1.362439777	1.717839176	1.708564557	1.834411208	1.326450539
10^4	1.363712328	1.706674028	1.694912607	1.825172032	1.322185202
10^5	1.362628821	1.702129911	1.687812285	1.820821254	1.320913954
10^6	1.362388916	1.700143017	1.684015784	1.817765404	1.320407310
10^7	1.362340581	1.698892878	1.681759952	1.816013028	1.320442975
10^8	1.362294391	1.698084654	1.680226365	1.81496822	1.320441370
10^9	1.362290387	1.697531628	1.679162267	1.814227025	1.320437203
10^{10}	1.362288176	1.697138317	1.678402045	1.813703956	1.320436106
10^{11}	1.362287687	1.696846445	1.677835284	1.813315742	1.320436387
$2 \cdot 10^{11}$	1.362287575	1.696773413	1.677692897	1.813218348	1.320436526

Table 2.3. L and C from Theorem 2.3.1

L	C	L	C
24	0.97	48	8.2054
25	2.31	60	8.302
26	3.4	82	8.3503
27	4.28	100	8.3708
28	5.00	127	8.3905
29	5.58	147	8.404
31	6.45	174	8.4102
34	7.24	214	8.4201
36	7.56	278	8.4301
42	8.04	396	8.4404
44	8.11	690	8.45001

where the supremum is taken over all intervals of length x. Suppose that L and $C = C(L)$ are related by Table 2.3. Then, whenever $x \geq e^L$, we have

$$R(x, a, b) < \left(\frac{16c_2 x}{(\log x)(C + \log x)} + 2\sqrt{x} \right) \Pi_{a,b}.$$

In order to avoid the annoying "$+2\sqrt{x}$" in the upper bound of $R(x, a, b)$, Klyve [18] gives the following corollary. Note that the table that Klyve gives has a small typo for the entry corresponding to $L = 25$. We have corrected this in Table 2.4.

Corollary 2.3.2. Let a and b be positive integers with $(a, b) = 1$ and ab a power of 2. Suppose that L and D are related by Table 2.4. Then whenever $x \geq e^L$, we have

$$\pi_{a,b}(x) < \frac{16c_2 x}{(\log x)(D + \log x)}.$$

Since Klyve is interested in twin primes and Wagstaff investigates primes such that $2^k p+1$ is prime, both restrict to the case when ab is a power of 2. If we lift this restriction, we can obtain results similar to those in Wagstaff [38]. In order to obtain slightly better bounds, we have slightly increased the values for D that Klyve found, where possible.

Table 2.4. L and D from Corollary 2.3.2

L	D	L	D
24	0.95	48	8.20
25	2.296	60	8.30
26	3.39	82	8.35
27	4.27	100	8.37
28	4.99	127	8.39
29	5.57	147	8.40
31	6.44	174	8.41
34	7.23	214	8.42
36	7.55	278	8.43
42	8.03	396	8.44
44	8.10	690	8.45

Table 2.5. L and D from Corollary 2.3.3

L	D	L	D
24	0.9526	48	8.20539
25	2.29684	60	8.30199
26	3.39038	82	8.35029
27	4.27314	100	8.37079
28	4.99519	127	8.39049
29	5.57668	147	8.40399
31	6.44847	174	8.41019
34	7.23954	214	8.42009
36	7.5598	278	8.43009
42	8.03998	396	8.44003
44	8.10999	690	8.45

Corollary 2.3.3. Let a and b be positive integers with $(a,b)=1$. Suppose that L and D are related by Table 2.5. Then whenever $x \geq e^L$, we have

$$\pi_{a,b}(x) < \frac{16c_2 x}{(\log x)(D+\log x)}\Pi_{a,b}.$$

Proof. We wish to find $D = D(L)$ such that

$$\frac{16c_2 x}{(\log x)(D+\log x)}\Pi_{a,b} < \left(\frac{16c_2 x}{(\log x)(C+\log x)} + 2\sqrt{x}\right)\Pi_{a,b}.$$

We immediately see that we can cancel $\Pi_{a,b}$ from both sides and that the (L,D) pairs found in Table 2.4 work. To get the (L,D) pairs in Table 2.5, we just increased the values for D as much as possible going out to 5 decimal places. □

It's worth noting that the inequality from Corollary 2.3.3 is as tight as we can make it. Suppose there is some $\Theta = \Theta(a,b) < \Pi_{a,b}$ such that

$$\frac{16c_2 x}{(\log x)(D+\log x)}\Theta < \left(\frac{16c_2 x}{(\log x)(C+\log x)} + 2\sqrt{x}\right)\Pi_{a,b}.$$

After multiplying both sides of the above inequality by

$$\frac{(\log x)(C+\log x)(D+\log x)}{16c_2 x\Pi_{a,b}},$$

and after some rearranging, we obtain

$$\left(1-\frac{\Theta}{\Pi_{a,b}}\right)\log x + 2\sqrt{x}\log x(C+\log x)(D+\log x) < \Theta C - D. \tag{2.1}$$

For Equation (2.1) to hold, we need the left hand side to be strictly decreasing for $x \geq e^L$. Differentiating and clearing denominators yields

$$\left(1-\frac{\Theta}{\Pi_{a,b}}\right)\sqrt{x} - (C+D-6)(\log x)^2 + 4(D-C(D-4))\log x + 2CD - (\log x)^3 < 0.$$

However, if $\Theta < \Pi_{a,b}$, then

$$\left(1-\frac{\Theta}{\Pi_{a,b}}\right)\sqrt{x} \gg (\log x)^3 + (C+D-6)(\log x)^2 - 4(D-C(D-4))\log x - 2CD.$$

Table 2.6. Some values of $\pi_{a,b}(x)$

x_0	$\pi_{1,6}(x_0)$	$\pi_{2,3}(x_0)$	$\pi_{4,3}(x_0)$	$\pi_{2,15}(x_0)$	$\pi_{1,210}(x_0)$
10^2	16	14	13	17	16
10^3	74	67	60	89	107
10^4	411	368	354	508	641
10^5	2447	2298	2172	3106	3928
10^6	16386	15592	14874	20698	26178
10^7	117207	112118	107705	149316	187731
10^8	879908	846341	815013	1128959	1409150
10^9	6849047	6613233	6392963	8815739	10958370
10^{10}	54818296	53137080	51557968	70845558	87712009
10^{11}	448725003	436212462	424416473	581648645	717976137
$2 \cdot 10^{11}$	848122150	825139331	803381324	1100215270	1357053226

Hence the left hand side of Equation (2.1) is eventually increasing.

Inconveniently, the upper bound in Corollary 2.3.3 depends on the prime divisors of ab unlike the case treated in Wagstaff [38], where ab is a power of 2. We could put a crude asymptotic bound on $\Pi_{a,b}$. First note that

$$\prod_{\substack{p>2\\ p\,|\,ab}} \frac{p-1}{p-2} \le \prod_{2<p\le ab} \frac{p-1}{p-2} = \prod_{\substack{p>2\\ p\,|\,ab}} \left(\frac{p}{p-1}\right)\left(1+\frac{1}{p(p-2)}\right) = \frac{ab}{2\phi(ab)} \prod_{\substack{p>2\\ p\,|\,ab}} \left(1+\frac{1}{p(p-2)}\right).$$

It is also easy to see that

$$\prod_{\substack{p>2\\ p\,|\,ab}} \left(1+\frac{1}{p(p-2)}\right) \le \left(\prod_{p>2}\left(1-(p-1)^{-2}\right)\right)^{-1} \le \left(\prod_{p\ge 2}\left(1-p^{-2}\right)\right) = 1/\zeta(2).$$

Because $\frac{ab}{2\phi(ab)} \ll \log\log ab$, we find that

$$\prod_{\substack{p>2\\ p\,|\,ab}} \frac{p-1}{p-2} \ll \frac{3}{\pi^2}\log\log ab.$$

However, this is not helpful in our explicit computations.

Theorem 2.3.4. We have $1.2608 < S_{1,6} < 1.9760$, $1.5952 < S_{2,3} < 2.3289$, $1.5762 < S_{4,3} < 1.6737$, $1.6779 < S_{2,15} < 2.6316$, and $1.1580 < S_{1,210} < 2.3023$.

Proof. The lower bound comes from Table 2.1 with $x_0 = 10^{11}$. To obtain the upper bounds, we follow the methods of Wagstaff [38]. Note that

$$S_{a,b} = S_{a,b}(x_0) + \sum_{\substack{p \geq x_0 \\ p \in \mathcal{S}_{a,b}}} \frac{1}{p} = S_{a,b}(x_0) + \sum_{t=x_0}^{\infty} \frac{\pi_{a,b}(t) - \pi_{a,b}(t-1)}{t}. \tag{2.2}$$

To estimate the tail sum, we will leverage the values given in Table 2.5 by partitioning the interval $[x_0, \infty)$ into subintervals $[M, N) = [e^L, e^{L'})$ and bound the sums for $e^L \leq t < e^{L'}$. Let $0 < M < N$. Then Stieltjes integration by parts gives

$$\sum_{t=M}^{N} \frac{\pi_{a,b}(t) - \pi_{a,b}(t-1)}{t} = \frac{\pi_{a,b}(N)}{N} - \frac{\pi_{a,b}(M)}{M} + \int_M^N \frac{\pi_{a,b}(t)}{t^2}\,\mathrm{d}t. \tag{2.3}$$

We can then bound the integral in Equation (2.3) using Corollary 2.3.3: let L, L' be consecutive entries in Table 2.5. Then

$$\begin{aligned}
\frac{1}{\Pi_{a,b}} \int_{e^L}^{e^{L'}} \frac{\pi_{a,b}(t)}{t^2}\,\mathrm{d}t &\leq \int_{e^L}^{e^{L'}} \frac{16c_2 t}{t^2 (\log t)(D(L) + \log t)}\,\mathrm{d}t \\
&= 16c_2 \int_L^{L'} \frac{\mathrm{d}s}{s(s + D(L))} \qquad (s = \log t) \\
&= \frac{16c_2}{D(L)} (\log s - \log(s + D(L)))\Big|_L^{L'} \\
&= \frac{16c_2}{D(L)} \log\left(\frac{L'(L + D(L))}{L(L' + D(L))}\right).
\end{aligned}$$

As one would expect from Corollary 2.3.3, our bound is just $\Pi_{a,b}$ times the bound found in Wagstaff [38]. With $L = 26$, $L' = 27$ and $x_0 = 2 \cdot 10^{11}$, we have $\log x_0 \approx 26.02158320$, so that $L \leq \log x_0 < L'$. Thus $\frac{1}{\Pi_{a,b}} \int_{x_0}^{e^{L'}} \pi_{a,b}(t)/t^2\,\mathrm{d}t$ is bounded by

$$\frac{16c_2}{D(L)} \log\left(\frac{L'(\log x_0 + D(L))}{(\log x_0)(L' + D(L))}\right) \approx 0.012667060.$$

For the final integral, observe that

$$\log\left(\frac{L'(L + D(L))}{L(L' + D(L))}\right) \to \log\left(\frac{(L + D(L))}{L}\right) \quad \text{as} \quad L' \to \infty.$$

Hence, $\frac{1}{\Pi_{a,b}}\int_{e^{690}}^{\infty} \pi_{a,b}(t)/t^2 \, \mathrm{d}t$ is bounded by

$$\frac{16c_2}{8.45}\log\left(\frac{8.45+690}{690}\right) \approx 0.015216.$$

The values for the upper bounds for each interval $[e^L, e^{L'})$ is found in Table 2.7. Summing over all the values in the table gives

$$\frac{1}{\Pi_{a,b}}\int_{x_0}^{\infty} \frac{\pi_{a,b}(t)}{t^2}\,\mathrm{d}t < 0.359690542.$$

This is slightly higher than the upper bound given in Wagstaff [38] because we have only computed $S_{a,b}(x_0)$ up to $x_0 = 10^{11}$. Let a, b, c, d be positive integers. When summing Equation (2.3) over all intervals $[e^L, e^{L'})$, the first two terms telescope, and we are left with

$$-\frac{\pi_{a,b}(x_0)}{x_0} + \int_{x_0}^{\infty}\frac{\pi_{a,b}(t)}{t^2}\,\mathrm{d}t.$$

Thus, for any (a,b) with $\gcd(a,b) = 1$ and $2 \mid ab$, we have

$$S_{a,b} < S_{a,b}(x_0) - \frac{\pi_{a,b}(x_0)}{x_0} + 0.359690542\Pi_{a,b}. \tag{2.4}$$

Observe that for $ab = 6, 12, 30, 210$, we have $\Pi_{a,b} = 2, 2, \frac{8}{3}, \frac{16}{5}$, respectively. Then using the values computed in Table 2.1 and Table 2.6, we explicitly compute Equation (2.4):

$$\begin{aligned}
S_{1,6} &< 1.260808459 - 0.004240610750 + 0.719381084 = 1.975948932\\
S_{2,3} &< 1.595294297 - 0.004125696655 + 0.719381084 = 2.310549684\\
S_{4,3} &< 1.576213781 - 0.004016906620 + 0.719381084 = 1.67367599\\
S_{2,15} &< 1.677912860 - 0.005501076350 + 0.959174778 = 2.631586562\\
S_{1,210} &< 1.158069940 - 0.006785266130 + 1.151009734 = 2.302294408
\end{aligned}$$

□

Table 2.7. M, N and the upper bound for $\frac{1}{\Pi_{a,b}} \int_M^N \pi_{a,b}(t) t^{-2}\,\mathrm{d}t$

M	N	Upper Bound	M	N	Upper Bound
x_0	e^{27}	0.012667060032356922	e^{60}	e^{82}	0.042181811595529330
e^{27}	e^{28}	0.012089516054081605	e^{82}	e^{100}	0.021220275174530828
e^{28}	e^{29}	0.011066121746457940	e^{100}	e^{127}	0.020893379303998833
e^{29}	e^{31}	0.019809987725398367	e^{127}	e^{147}	0.010659386897618544
e^{31}	e^{34}	0.025077365824123524	e^{147}	e^{174}	0.010591349409301834
e^{34}	e^{36}	0.014299003124370907	e^{174}	e^{214}	0.010870401831116214
e^{36}	e^{42}	0.035077186206136810	e^{214}	e^{278}	0.010980722705107563
e^{42}	e^{44}	0.009629885625463509	e^{278}	e^{396}	0.011036971804937732
e^{44}	e^{48}	0.017001986354427920	e^{396}	e^{690}	0.011177701187286296
e^{48}	e^{60}	0.038145305248693340	e^{690}	∞	0.015215124007049930

3. ON ELLIPTIC CARMICHAEL NUMBERS IN ARITHMETIC PROGRESSIONS

3.0.1 Carmichael numbers

The Fermat primality test is one of the simplest primality tests. It is derived from Fermat's little theorem, which states that for a prime p and an integer a with $\gcd(a, p) = 1$, one has $a^{p-1} \equiv 1 \pmod{p}$. It is well-known that the converse of Fermat's little theorem is false. A composite number n satisfying $a^{n-1} \equiv 1 \pmod{n}$ is called a *pseudoprime to base a*, or psp(a).

More generally, a *Carmichael number* is a composite number n which satisfies the conclusion to Fermat's little theorem for every integer a coprime to n. That is,

$$a^{n-1} \equiv 1 \pmod{n}$$

for all a with $\gcd(a, n) = 1$. In 1899 Korselt gave an equivalent characterization of Carmichael numbers that can be more easily tested.

Theorem 3.0.1 (Korselt's criterion)**.** A composite number n is a Carmichael number if and only if n is squarefree and for each prime divisor p of n one has $p - 1 \mid n - 1$.

In their famous 1994 paper, Alford, Granville and Pomerance [2] used this characterization to show that there are infinitely many Carmichael numbers. A natural next question is to ask whether there are infinitely many Carmichael numbers in various arithmetic progressions. Wright [39] proved this to be the case in 2013 after progress had been made on this problem by Banks and Pomerance [6] and Matomäki [21].

An analogous story can be told in the case of so-called *elliptic Carmichael numbers*. Dan Gordon [14] defined the notion of an elliptic Carmichael number in 1987 when he devised a primality test in the spirit of the Fermat test using the arithmetic of elliptic curves with complex multiplication. Following his earlier paper, Wright [40] proved in 2018 that there are infinitely many elliptic Carmichael numbers. We finish the story in proving the following assertion. Here, ρ is a constant, which we define in (3.1).

Theorem 3.0.2. Let M be a positive integer, and let a be such that $\gcd(a, M) = 1$. Moreover, assume that either $\gcd(M, \rho) = 1$, or that $\gcd(M, \rho) > 1$ and $a \equiv -1 \pmod{\gcd(M, \rho)}$. Then there are infinitely many elliptic Carmichael numbers m such that $m \equiv a \pmod{M}$.

3.0.2 Organization of this chapter

In Section 3.1, we give the basic background material on elliptic curves with complex multiplication and elliptic Carmichael numbers. We then recall the definitions of pseudoprimes related to Lucas sequences first given in Baillie and Wagstaff [4, 3]. In Section 3.2, we modify the arguments of Wright [39, 40] and Pomerance [30], and then apply them to show that there are infinitely many elliptic Carmichael numbers in some arithmetic progressions. Finally, in Section 3.3, we show that there are infinitely many elliptic Carmichael numbers which are also (strong) Lucas pseudoprimes.

3.1 Preliminaries

3.1.1 Elliptic curves

We recall some basic theory of elliptic curves needed for this discussion. The standard reference here is Silverman [35]. For our purposes, an elliptic curve E over $\mathbb{Q}$ is a smooth projective curve that satisfies the short Weierstrass equation

$$E : Y^2 = X^3 + aX + b,$$

with $a, b \in \mathbb{Q}$ and nonzero discriminant $\Delta = 4a^3 + 27b^2$. The set of rational points of E plus the point at infinity $\mathcal{O}$ form an additive group $E(\mathbb{Q})$.

We may then consider the endomorphism ring of $E(\mathbb{Q})$. Using the group law, for an integer n and a point $P \in E$, one clearly has $nP \in E$, so that $\mathbb{Z} \subset \operatorname{End} E$. If $\operatorname{End} E$ is strictly larger than $\mathbb{Z}$, then we say that E has complex multiplication (CM), or that E is a CM-elliptic curve. In this case, $\operatorname{End} E$ is isomorphic to an order in an imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ with class number 1, and we say that E has complex multiplication by $\mathbb{Q}(\sqrt{-d})$. By the Stark-Heegner theorem, the values of d for which $\mathbb{Q}(\sqrt{-d})$ has class number 1 are precisely $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$.

3.1.2 Elliptic Carmichael numbers

With this, we can consider the following primality test due to Dan Gordon [14]. For an elliptic curve E with complex multiplication by $\mathbb{Q}(\sqrt{-d})$, let $P \in E(\mathbb{Q})$ be a rational point of infinite order on E. Moreover, let n be a natural number such that $\gcd(n, 6\Delta) = 1$ and $(-d \,|\, n) = -1$, where $(-d \,|\, n)$ denotes the Jacobi symbol. If n is prime, then

$$[n+1]P \equiv \mathcal{O} \pmod{n}.$$

If the primality of n is not known, and n satisfies the above congruence, then n is a probable prime by Gordon's primality test. The setup here is analogous to that of Carmichael numbers. In this way, we can define elliptic Carmichael numbers.

Definition 3.1.1. Let n be a composite natural number. Given a CM-elliptic curve E, if n satisfies the Gordon primality test then n is called an *elliptic Carmichael number for E*. If n is an E-elliptic Carmichael number for every CM-elliptic curve with complex multiplication by $\mathbb{Q}(\sqrt{-d})$ where $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$, then n is an *elliptic Carmichael number*.

Note that such numbers exist, although they are relatively rare. Ekstrom et al. [11] give the smallest known example of an elliptic Carmichael number:

$$617\,730\,918\,224\,831\,720\,922\,772\,642\,603\,971\,311 = p(2p+1)(3p+2),$$

where $p = 468\,686\,771\,783$.

We wish to use a Korselt-like criterion for elliptic Carmichael numbers first proved in Ekstrom et al. [11]. Consider the condition $(-d \,|\, n) = -1$ in Gordon's primality test. In the case $d \in \{1, 2\}$, then $n \equiv -1 \pmod{8}$ satisfies this condition. For the other values of d listed in Definition 3.1.1, note that each of these d's is congruent to $-1 \pmod{4}$. Thus one has $(-d \,|\, n) = (n \,|\, d)$ and $(n \,|\, d) = -1$ whenever $n \equiv -1 \pmod{d}$. So put

$$\rho = 8 \cdot 3 \cdot 7 \cdot 11 \cdot 19 \cdot 43 \cdot 67 \cdot 163, \tag{3.1}$$

and note that $n \equiv -1 \pmod{\rho}$ satisfies the condition $(-d \,|\, n) = -1$ for all d listed in Definition 3.1.1. Now we have the following elliptic Carmichael condition due to Ekstrom et al. [11].

Theorem 3.1.1 (Elliptic Carmichael condition)**.** Let n be a squarefree, composite positive integer with an odd number of prime factors. Then n is an elliptic Carmichael number if for each prime p dividing n, one has $\rho \,|\, p+1$ and $p+1 \,|\, n+1$.

3.1.3 Lucas sequences and pseudoprimes

We will later show that there are infinitely many elliptic Carmichael numbers that are also (strong) Lucas pseudoprimes. To this end, we summarize some basic definitions. For integers D, P, Q with $P > 0$ and $D = P^2 - 4Q \neq 0$, define $U_0 = 0$, $U_1 = 1$, $V_0 = 2$ and $V_1 = P$. Then the Lucas sequences U_k, V_k with parameters P, Q are defined for $k \geq 2$ by the recursive equations

$$U_k = PU_{k-1} - QU_{k-2} \quad \text{and} \quad V_k = PV_{k-1} - QV_{k-2}.$$

Let α and β be the distinct roots of the polynomial $f(x) = x^2 - Px + Q$. Then $\alpha\beta = Q$, $\alpha + \beta = P$, and for $k \geq 0$, we have

$$U_k = \frac{\alpha^k - \beta^k}{\alpha - \beta} \quad \text{and} \quad V_k = \alpha^k + \beta^k.$$

If $n > 1$ is an odd integer and D, P, Q are chosen so that $(D \,|\, n) = -1$, and if n is prime and $\gcd(n, Q) = 1$, then by Theorem 8 of Brillhart-Lehmer-Selfridge [7]

$$U_{n+1} \equiv 0 \pmod{n}, \tag{3.2}$$

$$V_{n+1} \equiv 2Q \pmod{n}. \tag{3.3}$$

In Baillie-Wagstaff [4], they first defined a *Lucas pseudoprime* with parameters P and Q, denoted lpsp(P, Q), to be a composite integer n satisfying Equation (3.2). If n satisfies Equation (3.2), but it is not known whether n is prime or composite, then n is said to be a *probable* Lucas pseudoprime with parameters P and Q, or lprp(P, Q). Then in Baillie-Fiori-Wagstaff[3] they give the following definition.

Definition 3.1.2. If n satisfies Equation (3.3), we call n a *Lucas-V probable prime* with parameters P and Q, or vprp(P, Q). If n is composite and satisfies Equation (3.3) with parameters P and Q, we call n a *Lucas-V pseudoprime*, or vpsp(P, Q).

We further have the notion of *strong* Lucas pseudoprimes as defined in Brillhart-Lehmer-Selfridge [7]. For n odd, we can write $n + 1 = d \cdot 2^s$ with d odd for some $s > 0$. If n is prime and $(D \,|\, n) = -1$, then either

$$U_d \equiv 0 \pmod{n}, \quad \text{or} \tag{3.4}$$

$$V_{d\cdot 2^r} \equiv 0 \pmod{n}, \quad \text{for some } r \text{ with } 0 \le r < s. \tag{3.5}$$

Definition 3.1.3. If $(D \,|\, n) = -1$ and n satisfies Equation (3.4) or Equation (3.5), then n is called a *strong Lucas probable prime* with parameters P and Q, or slprp(P, Q). If n is also composite, then n is called a *strong Lucas pseudoprime*, or slpsp(P, Q).

3.2 Elliptic Carmichael numbers in arithmetic progressions

In proving Theorem 3.0.2, the main idea is to construct a number L which has many factors d yielding many primes of the form $dk - 1$ for some k relatively prime to L. We find a particular k that gives sufficiently many primes of this form and combine subsets of these primes to form elliptic Carmichael numbers. As in Wright [40], we will additionally require that these primes be quadratic nonresidues modulo L. Unlike Wright, though, we will require that L has an even number of prime factors. We supplement the ideas of Wright [39, 40] with those of Pomerance [30] in order to utilize the better lower bound obtained in Pomerance [30].

Throughout the rest of this discussion, we assume $M \ge 2$ and let $\mu = 4\phi(M)$ so that $4 \,|\, \mu$. Let $P(q - 1)$ denote the largest prime divisor of $q - 1$. We define the following set:

$$\mathcal{Q}_0 := \mathcal{Q}_0(y) = \{q \text{ prime} : y < q \le y \log^2 y,\, q \equiv -1 \pmod{\mu},\, P(q-1) \le y\}.$$

Note that this deviates from the set $\mathcal{Q}$ that Wright defines, where he considers the primes q not dividing M on the interval $[\frac{y^\theta}{\log y}, y^\theta]$ with $q \equiv -1 \pmod{\mu}$ and $P(q - 1) \le y$ for θ fixed between 1 and 2.

As noted in Pomerance [30], if $q \le y \log^2 y$ and $P(q-1) > y$, then $q = mr + 1$, where $m < \log^2 y$ and r is prime. Then by Brun's sieve, the number of such primes q is at most

$$\sum_{m<\log^2 y} \sum_{\substack{r \text{ prime} \\ mr \le y \log^2 y \\ rm+1 \text{ prime}}} 1 \ll \sum_{m<\log^2 y} \frac{y \log^2 y}{\phi(m) \log^2 y} \ll y \log\log y. \tag{3.6}$$

And by the prime number theorem for arithmetic progressions, the number of primes $q \le y \log^2 y$ with $q \equiv -1 \pmod{\mu}$ is asymptotic to $\frac{1}{\phi(\mu)} y \log y$. This, together with Equation (3.6) gives

$$\#\mathcal{Q}_0 \sim \frac{1}{\phi(\mu)} y \log y \quad \text{and} \quad \prod_{q \in \mathcal{Q}_0} q = \exp\left(\frac{1+o(1)}{\phi(\mu)} y \log^2 y\right), \, y \to \infty. \tag{3.7}$$

We will also make use of the following fact:

$$\sum_{q \in \mathcal{Q}_0} \frac{1}{q} < \sum_{\substack{y < q \le y \log^2 y \\ q \text{ prime}}} \frac{1}{q} = o(1), \quad y \to \infty. \tag{3.8}$$

We fix B such that $0 < B < \frac{5}{12}$; later, we will choose B to be near $\frac{5}{12}$. Let $\pi(z; d, a)$ denote the number of primes up to z which are congruent to a modulo d. Then we have the following theorem due to Alford et al. [2].

Theorem 3.2.1. For any x, there exists a set $\mathcal{D}_B(x)$ of at most D_B integers, all of which exceed $\log x$, such that if d is not divisible by an element in $\mathcal{D}_B(x)$ and $d \le \min\left\{x^B, z/x^{1-B}\right\}$ then

$$\pi(z; d, a) \ge \frac{\pi(z)}{2\phi(d)}$$

for any a with $\gcd(a, d) = 1$.

With $\mathcal{Q}_0$ as defined above, let $L' = \prod_{q \in \mathcal{Q}_0} q$, and let

$$x = (M \rho L')^{1/B}.$$

Then by Theorem 3.2.1 if $n \le x^B$, n is not divisible by any element of $\mathcal{D}(x)$, $\gcd(b, n) = 1$, and $z \ge n x^{1-B}$, then

$$\pi(z; n, b) \ge \frac{\pi(z)}{2\phi(n)}.$$

We can construct a set of primes $P_B(x)$ with $\#P_B(x) \leq D_B$ in the following way: for each number d in $\mathcal{D}_B(x)$, choose a prime factor of d and add it to $P_B(x)$ if it is not already in there. Thus any element of $\mathcal{D}_B(x)$ is divisible by at least one of the primes in $P_B(x)$. With this, we define $\mathcal{Q} = \mathcal{Q}_0 \setminus P_B(x)$. We will assume that $\#\mathcal{Q}$ is even. Then put

$$L = \prod_{q \in \mathcal{Q}} q \tag{3.9}$$

so that no factor of L is divisible by any element in $\mathcal{D}_B(x)$. One also has that $\gcd(q, M) = 1$ for all $q \in \mathcal{Q}$, and hence $\gcd(M, L) = 1$. Notice that we still have that $\mathcal{Q}$ satisfies Equation (3.7) and Equation (3.8). In terms of L, this means

$$L = \exp\left(\frac{1 + o(1)}{\phi(\mu)} y \log^2 y\right), \tag{3.10}$$

$$\omega(L) \sim \frac{1}{\phi(\mu)} y \log y, \quad \text{and} \quad \sum_{q \,|\, L} \frac{1}{q} = o(1) \quad \text{as} \quad y \to \infty, \tag{3.11}$$

where $\omega(L)$ is the number of distinct prime divisors of L.

Analogous to Pomerance [30], for each $d \,|\, L$ and each quadratic nonresidue $b \pmod{L/d}$ we consider the primes p such that

- $p \leq dx^{1-B}$
- $p \equiv -1 \pmod{d}$,
- $p \equiv a \pmod{M}$ and
- $p \equiv b \pmod{L/d}$.

Note that for y sufficiently large relative to M, $\mathcal{D}_B(x)$ contains no factors of M, and by construction L has no factors in $\mathcal{D}_B(x)$, hence ML has no factors in $\mathcal{D}_B(x)$. Moreover, since $\gcd(M, L) = 1$, we can combine the above congruences to obtain a single congruence modulo ML and apply Theorem 3.2.1 to reduced residue classes modulo ML. Consequently, we have the following analogue of Lemma 2.2 of Wright [39].

Lemma 3.2.2. Let L be as in (3.9), and let $\gcd(a, M) = 1$. Then for each $d \mid L$ and each quadratic nonresidue $b \pmod{L/d}$, the number of primes p satisfying $p \le dx^{1-B}$, $p \equiv -1 \pmod{d}$, $p \equiv a \pmod{M}$ and $p \equiv b \pmod{L/d}$ is greater than

$$\frac{dx^{1-B}2^{\omega(d)}}{3 \cdot 2^{\omega(L)}\phi(Md)\log x}.$$

Proof. The absolute number of congruence classes that are quadratic nonresidues modulo each $q \mid L$ is $\frac{q-1}{2}$ of the $q - 1$ classes which can contain more than one prime number. By the Chinese Remainder Theorem, we get that for a given divisor d, the number of congruence classes modulo L/d which are quadratic nonresidues for every q is

$$\prod_{q \mid L/d} \frac{q-1}{2} = \frac{\phi(L/d)}{2^{\omega(L/d)}} \quad \text{of the} \quad \prod_{q \mid L/d} (q-1) = \phi(L/d)$$

congruence classes which contain more than one prime. Now, there are $\phi(ML)$ congruence classes modulo ML which can contain more than one prime, and by Theorem 3.2.1, the number of primes in such a class is at least

$$\frac{\pi(dx^{1-B})}{2\phi(ML)} > \frac{dx^{1-B}}{3\phi(ML)\log x},$$

and thus the number of classes which are quadratic nonresidues modulo L/d and congruent to $a \pmod{M}$ is at least

$$\frac{\pi(dx^{1-B})2^{\omega(d)}}{3 \cdot 2^{\omega(L)}\phi(Md)} > \frac{dx^{1-B}2^{\omega(d)}}{3 \cdot 2^{\omega(L)}\phi(Md)\log x}. \qquad \square$$

For a given divisor d of L and our fixed B, we want to count the number of primes $p \equiv -1 \pmod{d}$ that also satisfy $\gcd((p+1)/d, L) = 1$. Analogous to Alford et al. [2], note that for our chosen x, we have $1 \le d \le x^B$ for any $d \mid L$. We find the following lower bound on primes satisfying the above conditions. Here, and throughout the rest of this section, ρ is as defined in (3.1). We will also abbreviate quadratic nonresidue as QNR.

Lemma 3.2.3. Let $B < 5/12$, L as above. Let $M > 2$ be such that $\gcd(M,\rho) = 1$ or $\gamma := \gcd(M,\rho) > 1$ with $a \equiv -1 \pmod{\gamma}$. Then there exists an integer $k \leq x^{1-B}$ with $\gcd(k,L) = 1$ such that

$$\begin{aligned}\#\{d \,|\, L : p = dk-1 &\text{ is prime, } p \text{ a QNR mod } q \text{ for every } q \,|\, L,\\ &\qquad\qquad \rho \,|\, p+1,\ p \equiv a \bmod M,\ p \leq dx^{1-B}\}\\ &> \frac{(3/2)^{\omega(L)}}{4\phi(M)\phi(\rho)\log x}.\end{aligned}$$

Proof. In Lemma 3.2.2 we showed that for a given divisor d of L, the number of primes $p \leq dx^{1-B}$ that are both quadratic nonresidues modulo L/d and congruent to $a \pmod{M}$ is greater than

$$\frac{dx^{1-B}2^{\omega(d)}}{3 \cdot 2^{\omega(L)}\phi(M)\log x}.$$

We want to add the additional requirement that the primes p be congruent to $-1 \pmod{\rho}$. That is, we are looking to satisfy

$$\begin{aligned} p &\equiv \ \ a \pmod{M}\\ p &\equiv -1 \pmod{\rho}. \end{aligned} \tag{3.12}$$

We claim that the number of such primes is greater than

$$\frac{dx^{1-B}2^{\omega(d)}}{3 \cdot 2^{\omega(L)}\phi(Md)\phi(\rho)\log x}. \tag{3.13}$$

To see this, first consider the case $\gcd(\rho, M) = 1$. Then $t\rho + sM = 1$ for some integers t, s. Then a solution to Equation (3.12) is given by $p = at\rho - sM$, so

$$p \equiv at\rho - sM \pmod{M\rho}. \tag{3.14}$$

Then we can replace a by $at\rho - sM$ and M by $M\rho$ in Lemma 3.2.2 to obtain the inequality in Equation (3.13).

Next consider the case when $\gcd(\rho, M) > 1$. Let $\gamma = \gcd(\rho, M)$, and write $\gamma = t\rho + sM$. If $a \equiv -1 \pmod{\gamma}$, then Equation (3.12) has a unique solution modulo $[\rho, M] = \rho M/\gamma$ given by

$$p = \frac{at\rho - sM}{\gamma}.$$

Otherwise, no solution exists. So in the case $a \equiv -1 \pmod{\gamma}$, we can replace a by $(at\rho - sM)/\gamma$ and M by $\rho M/\gamma$ in Lemma 3.2.2 to obtain the inequality in Equation (3.13).

We further want to constrain to have $p \equiv -1 \pmod{d}$ for a given divisor d of L. We claim that there are more than

$$\frac{dx^{1-B}2^{\omega(d)}}{2^{\omega(L)+2}\phi(M)\phi(\rho)\log x}. \tag{3.15}$$

such primes. In counting the number of primes in various residue classes, allow us to abuse intersection notation, and let $\pi(d, q, a) \cap \pi(d, r, b)$ denote the number of primes up to d that are both congruent to a modulo q and congruent to b modulo r. Then in the case that $\gcd(M, \rho) = 1$, we have

$$\pi(dx^{1-B}, M, a) \cap \pi(dx^{1-B}, \rho, -1) = \pi(dx^{1-B}, M\rho, at\rho - sM),$$

where t, s are as in Equation (3.14). The claim then follows immediately from proof of Lemma 6.2 of Wright [40]. Next, in the case that $\gcd(\rho, M) > 1$ with $a \equiv -1 \pmod{M\rho}$, we have

$$\pi(dx^{1-B}, M, a) \cap \pi(dx^{1-B}, \rho, -1) = \pi\left(dx^{1-B}, \frac{M}{\gamma}\rho, \frac{at\rho - sM}{\gamma}\right),$$

and then Equation (3.15) follows in the same way as in the first case.

We wish to determine how many of these primes satisfy $\gcd\left(\frac{p+1}{d}, L\right) = 1$. Using the notation of Wright [40], let $\pi(x, L, \mathrm{QNR})$ denote the number of primes up to x which are quadratic nonresidues modulo every divisor of L. Now, for any prime $q \mid L$, we have by the Brun-Titchmarsh inequality (see Montgomery and Vaughan [25]) that

$$\begin{aligned}
\pi(dx^{1-B}, dq, -1) \cap \pi(dx^{1-B}, L, \mathrm{QNR}) \cap \pi(dx^{1-B}, M, a) \cap \pi(dx^{1-B}, \rho, -1)& \\
\ll \frac{dx^{1-B} 2^{\omega(d)}}{2^{\omega(L)} q\phi(Md)\phi(\rho)\log(x/(qML))}& \\
\ll \frac{dx^{1-B} 2^{\omega(d)}}{2^{\omega(L)} q\phi(Md)\phi(\rho)\log x}.& \qquad (3.16)
\end{aligned}$$

Now combining Equation (3.13) and Equation (3.16), one has

$$\begin{aligned}
&\pi(dx^{1-B}, d, -1) \cap \pi(dx^{1-B}, L, \mathrm{QNR}) \cap \pi(dx^{1-B}, M, a) \cap \pi(dx^{1-B}, \rho, -1) \\
&- \sum_{\substack{q \mid L \\ q \text{ prime}}} \pi(dx^{1-B}, dq, -1) \cap \pi(dx^{1-B}, L/d, \mathrm{QNR}) \cap \pi(dx^{1-B}, M, a) \cap \pi(dx^{1-B}, \rho, -1) \\
&> \frac{dx^{1-B} 2^{\omega(d)}}{3 \cdot 2^{\omega(L)} \phi(Md)\phi(\rho)\log x} - \sum_{\substack{q \mid L \\ q \text{ prime}}} \frac{dx^{1-B} 2^{\omega(d)}}{2^{\omega(L)} q\phi(Md)\phi(\rho)\log x} \\
&> \frac{x^{1-B} 2^{\omega(d)}}{4 \cdot 2^{\omega(L)} \phi(M)\phi(\rho)\log x}, \qquad (3.17)
\end{aligned}$$

where the last inequality uses the fact that $\sum_{q \mid L} \frac{1}{q} = o(1)$ and that $d > \phi(d)$.

Summing over all divisors d of L, the inequality in Equation (3.17) implies that we have at least

$$\sum_{d \mid L} \frac{x^{1-B} 2^{\omega(d)}}{4 \cdot 2^{\omega(L)} \phi(M)\phi(\rho)\log x}$$

pairs (p, d) such that all of the following requirements hold: $p \leq dx^{1-B}$ is prime, d divides L, $\frac{p+1}{d}$ is coprime to L, $p \equiv -1 \pmod{\rho}$, $p \equiv a \pmod{M}$, p is a quadratic nonresidue modulo L, and $d \leq x^B$. Now since the number of distinct values of $\frac{p+1}{d}$ is bounded by x^{1-B}, there must be some k coprime to L having at least

$$\sum_{d \mid L} \frac{2^{\omega(d)}}{4 \cdot 2^{\omega(L)} \phi(M)\phi(\rho)\log x} \qquad (3.18)$$

representations as $\frac{p+1}{d}$ for p, d as above. For the numerator in Equation (3.18), one has

$$\sum_{d \,|\, L} 2^{\omega(d)} = \sum_{i=0}^{\omega(L)} \binom{\omega(L)}{i} 2^{\omega(L)-i} = (2+1)^{\omega(L)} = 3^{\omega(L)},$$

which gives

$$\sum_{d \,|\, L} \frac{2^{\omega(L)}}{4 \cdot 2^{\omega(L)} \phi(M)\phi(\rho) \log x} = \frac{\left(\frac{3}{2}\right)^{\omega(L)}}{4 \cdot \phi(M)\phi(\rho) \log x},$$

and this completes the proof. □

Let k_0 be the k found by the above lemma and define

$$\begin{aligned} \mathcal{P} = \{&p \text{ prime} \colon p = dk_0 - 1 \text{ for some } d \,|\, L, p \text{ is a QNR mod } q \text{ for every } q \,|\, L, \\ &p \equiv a \bmod M, \rho \,|\, p+1, p \le x\}\,. \end{aligned} \tag{3.19}$$

We will generate pseudoprimes by taking products of elements of $\mathcal{P}$. Note that Lemma 3.2.3 gives a lower bound on the size of $\mathcal{P}$. We will make use of this in the proof of Theorem 3.2.6.

We require the use of Lemma 6 from Matomäki [21]. Here, $\Omega(n)$ denotes the number of prime factors of n, counted with multiplicity. For a multiplicative abelian group G, $\lambda(G)$ denotes the largest order of an element in G, and $n(G)$ is Davenport's constant—the smallest number such that a collection of at least $n(G)$ elements must contain some subset whose product is the identity. Then we have

$$\lambda(G) \le n(G) \le \lambda(G)\left(1 + \frac{\log(\#G)}{\lambda(G)}\right).$$

The first inequality is clear, and the second is due to van Emde Boas–Kruyswijk [12] and Meshulam [23]. For a simplified proof of this result, see Theorem 1.1 of Alford et al. [2].

As noted in Matomäki [21], the following lemma is a consequence of Proposition 1.2 of Alford et al. [2] and Proposition 1 of Baker [5].

Lemma 3.2.4 ([21])**.** For any multiplicative abelian group G, write

$$s(G) = \lceil 5\lambda(G)^2 \Omega(\lambda(G)) \log(3\lambda(G)\Omega(\#G)) \rceil.$$

Let A be a sequence of length n consisting of non-identity elements of G. Then there exists a nontrivial subgroup $H \subset G$ such that the following conditions are satisfied:

i. If $n \geq s(G)$, then for every $h \in H$, $A \cap H$ has a subsequence whose product is h.

ii. If t is an integer such that $s(G) < t < n - n(G)$, then for every $h \in H$, A has at least $\binom{n-n(G)}{t-n(G)} / \binom{n}{n(G)}$ distinct subsequences of length at most t and at least $t - n(G)$ whose product is h.

Lemma 3.2.5. Let H be the subgroup of $(\mathbb{Z}/kML\mathbb{Z})^*$ of residues congruent to $-1 \pmod{k}$. Let $G = H \times \{-1, 1\}$. For $n(G)$ and $s(G)$ as above, we have $n(G) \leq e^{2y}$ and $s(G) \leq e^{3y}$.

Proof. First note that $\#G \leq 2ML$. Denoting $\lambda((\mathbb{Z}/L\mathbb{Z})^*)$ by $\lambda(L)$, this is the lcm of $q-1$ for the primes $q \mid L$. By assumption the largest prime dividing $q-1$ is less than or equal to y. Thus if q^e is the largest prime power dividing $\lambda(L)$, then $q^e \leq y \log^2 y$; hence

$$\lambda(L) \leq (y \log^2 y)^{\pi(y)}.$$

On noting that $\lambda(G) \leq 2M\lambda(L)$ and using Equation (3.10), we obtain

$$n(G) \leq 2M(y \log^2 y)^{\pi(y)} \log(ML) \leq e^{2y}.$$

Finally, the estimate on $s(G)$ follows from Lemma 3.2.4 and our estimate on $\lambda(G)$. □

With this, we can state the key theorem which combines the ideas of Wright [39, Theorem 5.1] and [40, Theorem 8.1].

Theorem 3.2.6. Let $\mathcal{P}$ be the set of primes defined in Equation (3.19). Let G be the group defined in Lemma 3.2.5 and let $s(G)$ be as in Lemma 3.2.4. Then $\#\mathcal{P} > s(G)$. If H is the subgroup of G guaranteed by Lemma 3.2.4, then there exists an element $h \in H$ such that

$$h = (\zeta, -1),$$

with

$$\begin{aligned} \zeta &\equiv -1 \mod L \\ \zeta &\equiv \quad a \mod M. \end{aligned} \tag{3.20}$$

Equivalently, there exists a subset of $\mathcal{P}$ whose product multiplies to a number m for which $m \equiv a \pmod{M}$ and $p \,|\, m$ implies $p + 1 \,|\, m + 1$.

Proof. First note that we have $s(G) < \#\mathcal{P}$. Let $A = \{(p, -1) \colon p \in \mathcal{P}\}$ be the sequence referenced in Lemma 3.2.4. Then clearly $\#A = \#\mathcal{P} > s(G)$. Then in particular, it follows from part (i) of Lemma 3.2.4 that $A \cap H \neq \varnothing$. So let $\hat{p}$ be a prime such that $(\hat{p}, -1) \in A \cap H$.

Since $\hat{p} \in \mathcal{P}$, $\hat{p}$ is a quadratic nonresidue modulo each q dividing L. Put

$$j = \prod_{q \,|\, L} \frac{q-1}{2},$$

and note that j is necessarily odd since each $q \equiv 3 \pmod{4}$. Consequently, we have

$$\hat{p}^j \equiv \left(\hat{p}^{\frac{q-1}{2}}\right)^{j/\left(\frac{q-1}{2}\right)} \equiv (-1)^{j/\left(\frac{q-1}{2}\right)} \equiv -1 \pmod{q}$$

for each $q \,|\, L$, and $(-1)^j \equiv -1 \pmod{q}$. Also note that by assumption we have $q \equiv -1 \pmod{4\phi(M)}$. But this gives

$$\frac{q-1}{2} \equiv -1 \pmod{2\phi(M)}$$

so that $\frac{q-1}{2} \equiv -1 \mod \phi(M)$. Then since by assumption L has an even number of factors, we obtain

$$j \equiv 1 \pmod{\phi(M)},$$

giving

$$\hat{p}^j \equiv a \pmod{M}.$$

So putting $h = (\hat{p}, -1)^j = (\hat{p}^j, (-1)^j)$ gives the desired congruences in Equation (3.20), proving the first half of the theorem.

For the second half, by Lemma 3.2.4, there exists a sequence $\{p_1, \dots, p_s\} \subset \mathcal{P}$ such that

$$(p_1, -1) \cdots (p_s, -1) = h.$$

Put $m = p_1 \cdots p_s$. Since each $p_i \in \mathcal{P}$ is -1 mod k_0 and s is odd (being that $(-1)^s = -1$), it must be that $m \equiv -1 \pmod{k_0}$. Hence modulo L, one has

$$m \equiv p_1 \cdots p_s \equiv -1 \pmod{L}.$$

Note also that we still have $m \equiv a \pmod{M}$, so m satisfies Equation (3.20). Putting this all together, for any prime p_i dividing m, one has $\rho \,|\, p_i + 1$ and

$$p_i + 1 \,|\, dk \,|\, Lk \,|\, m + 1. \qquad \square$$

In the next theorem, we give an explicit lower bound on the number of elliptic Carmichael numbers up to X. The proof appears in Pomerance [30] for the case of Carmichael numbers. It still applies to the present case, so we include it here.

Theorem 3.2.7. Let $\mathcal{N}_{M,a}(X)$ be the number of elliptic Carmichael numbers up to X congruent to a modulo M. Then $\mathcal{N}_{M,a}(X) \geq X^{1/(6 \log\log\log X)}$ for all sufficiently large X depending on the choice of M.

Proof. We define $t = \lceil e^{3y} \rceil$ so that $t \geq s(G)$. Then, by Lemma 3.2.4, $\mathcal{P}$ has at least

$$N := \binom{\#\mathcal{P} - n(G)}{t - n(G)} \Big/ \binom{\#\mathcal{P}}{n(G)}$$

distinct products of at most t primes which are congruent to -1 mod L. Moreover, it follows from Lemma 3.2.5 that for y large enough, one has $n(G) > (\#P)^2 e$. This, combined with the standard bounds

$$\left(\frac{\alpha}{\beta}\right)^{\beta} \leq \binom{\alpha}{\beta} \leq \left(\frac{\alpha e}{\beta}\right)^{\beta}$$

gives the following string of inequalities:

$$\begin{aligned} N &> \left(\frac{\#\mathcal{P} - n(G)}{t - n(G)}\right)^{t-n(G)} (\#\mathcal{P})^{-n(G)} \\ &> \left(\frac{\#\mathcal{P}}{t}\right)^{t-n(G)} (\#\mathcal{P})^{-n(G)} > (\#\mathcal{P})^{t-2n(G)} t^{-t}. \end{aligned}$$

Now, define $X := x^t$. Note that each $p \in \mathcal{P}$ satisfies $p \leq x$. Hence, all of the elliptic Carmichael numbers constructed in Theorem 3.2.6 are at most X. Then using Equation (3.7), Lemma 3.2.5 and the definition of x, we obtain

$$X = \exp\left(\frac{1/B + o(1)}{\phi(\mu)} ty \log^2 y\right).$$

Moreover, using Equation (3.10) and the lower bound on $\#\mathcal{P}$ obtained in Lemma 3.2.3, we have

$$\begin{aligned} N &\geq \exp\left(\frac{\log(3/2) + o(1)}{\phi(\mu)} ty \log y - t \log t\right) \\ &= \exp\left(\frac{\log(3/2) + o(1)}{\phi(\mu)} ty \log y\right), \end{aligned}$$

giving $N \geq X^{(B \log(3/2) + o(1))/\log y}$. Now, $\log X$ is asymptotic to

$$\frac{1}{B\phi(\mu)} ty \log^2 y,$$

and using the definition of t, we see

$$\log\log X = 3y + O(\log y), \quad \log\log\log X = \log y + O(1).$$

Hence $N \geq X^{(B \log(3/2) + o(1))/\log\log\log X}$. Because $B < 5/12$ can be chosen to be arbitrarily close to $5/12$ and $(5/12)\log(3/2) > 1/6$, this completes the proof. □

3.3 Elliptic Carmichael numbers and (strong) Lucas pseudoprimes

We prove an analogue of Theorem 2 of Baillie-Fiori-Wagstaff [3]. This requires the following lemma from the same paper. The number a constructed in the proof is used in Theorem 3.3.2; consequently, we must modify the proof given in Baillie et al. [3] to be able to use it.

Lemma 3.3.1. For every positive integer r, there exists an integer $a \equiv 3 \pmod 4$ such that for every odd prime p, if $p \equiv a \pmod{4r}$, then r is a quadratic residue modulo p, i.e., $(r \,|\, p) = +1$.

Proof. Write $r = 2^s t$ with t odd. If s is even, let $a = 4t - 1$, and if s is odd, let $a = 8t - 1$. Then clearly $a \equiv 3 \pmod 4$. Suppose p is an odd prime with $p \equiv a \pmod{4r}$. In particular, we have $p \equiv 3 \pmod 4$.

If $t = 1$, we have two possibilities: r is a power of 4, or r is twice a power of 4. In the first case, s is even, $a = 3$ and $(r \,|\, p) = (1 \,|\, p) = +1$. In the second case, s is odd, so $(r \,|\, p) = (2 \,|\, p) = +1$ by the supplement to the law of quadratic reciprocity since $p \equiv 7 \pmod 8$.

Now suppose $t > 1$ and s is even; then $a = 4t - 1$. If $t \equiv 1 \pmod 4$, then

$$\left(\frac{r}{p}\right) = \left(\frac{2^s t}{p}\right) = \left(\frac{t}{p}\right) = \left(\frac{p}{t}\right) = \left(\frac{4t-1}{t}\right) = \left(\frac{-1}{t}\right) = +1.$$

And if $t \equiv 3 \pmod 4$, then

$$\left(\frac{r}{p}\right) = \left(\frac{2^s t}{p}\right) = \left(\frac{t}{p}\right) = -\left(\frac{p}{t}\right) = -\left(\frac{4t-1}{t}\right) = -\left(\frac{-1}{t}\right) = +1.$$

Finally suppose $t > 1$ and s is odd. Then $a = 8t - 1$. If $t \equiv 1 \pmod 4$, then

$$\left(\frac{r}{p}\right) = \left(\frac{2t}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{t}{p}\right) = \left(\frac{p}{t}\right) = \left(\frac{8t-1}{t}\right) = \left(\frac{-1}{t}\right) = +1.$$

And if $t \equiv 3 \pmod 4$, then

$$\left(\frac{r}{p}\right) = \left(\frac{2t}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{t}{p}\right) = -\left(\frac{p}{t}\right) = -\left(\frac{8t-1}{t}\right) = -\left(\frac{-1}{t}\right) = +1. \qquad \square$$

We can now prove the following theorem. Unlike the analogous theorem in Baillie-Fiori-Wagstaff [3], we must take special care in the case that $\gcd(r, \rho) > 1$.

Theorem 3.3.2. If $r > 1$ is an integer, there are infinitely many elliptic Carmichael numbers $m \equiv 3 \pmod 4$ that are also strong pseudoprimes to base r. Moreover, the number of such $m < X$ is at least $X^{1/(6 \log\log\log X)}$ for all sufficiently large X.

Proof. Write $r = 2^s t$, with t odd. If $s = 0$, let $M = 4r$; if $s = 1$, take $M = 2r$; if $s \geq 2$, let $M = r$, and choose a according to Lemma 3.3.1. Then in any case, $a \equiv -1 \pmod M$, which implies that $a \equiv -1 \pmod{\gcd(M, \rho)}$. Thus by Theorem 3.2.7, we have $\mathcal{N}_{M,a}(X) \gg X^{1/(6 \log\log\log X)}$. Note also that since $a \equiv 3 \pmod 4$ and $4 \mid M$, one has $m \equiv 3 \pmod 4$. By construction each p dividing m is odd and congruent to a modulo M, and congruent to 3 modulo 4. Hence by Lemma 3.3.1 for each $p \mid M$ we have $(r \mid p) = +1$. By Corollary 1.2 of Alford et al. [1], since for each p dividing M, $(r \mid p)$ takes the same value, m is a strong pseudoprime to base r. □

In light of Theorem 3.3.2, we can actually say that there are infinitely many elliptic Carmichael numbers that are also strong lpsp's and vpsp's for certain parameters P and Q.

Corollary 3.3.3. Let k be a positive integer. Let $P = 2^k$ and $Q = 2^{2k-1}$. Then there exist infinitely many elliptic Carmichael numbers $m \equiv 3 \pmod 4$ that are strong pseudoprimes to base 2, strong lpsp(P, Q) and vpsp(P, Q). Moreover, the number of such $m < X$ is at least $X^{1/(6 \log\log\log X)}$ for all sufficiently large X.

Corollary 3.3.4. Let k be a positive integer. Let $P = 4 \cdot r^k$ and $Q = 8 \cdot r^{2k}$. Then there exist infinitely many elliptic Carmichael numbers $m \equiv 3 \pmod 4$ that are strong pseudoprimes to base r and strong lpsp(P, Q). Moreover, the number of such $m < X$ is at least $X^{1/(6 \log\log\log X)}$ for all sufficiently large X.

These corollaries immediately follow from Theorem 3.3.2 and the following two theorems. The first is due to Baillie-Fiori-Wagstaff [3], and the second is analogous, which we prove.

Theorem 3.3.5. *[3, Theorem 1]* Let $n \equiv 3 \pmod 4$ be a strong pseudoprime base 2. Let $k \geq 0$ be an integer. Set $P = 2^k$ and $Q = 2^{2k-1}$. Then n is also a strong lpsp(P, Q) and a vpsp(P, Q).

Theorem 3.3.6. Let $n \equiv 3 \pmod 4$ be a strong pseudoprime base r. Let $k \geq 0$ be an integer. Set $P = 4 \cdot r^k$ and $Q = 8 \cdot r^{2k}$. Then n is also a strong lpsp(P, Q).

Proof. Note that $D = P^2 - 4Q = 16 \cdot r^{2k} - 4 \cdot 8 \cdot r^{2k} = -16(r^k)^2$. Then since $n \equiv 3 \pmod 4$, one has

$$\left(\frac{D}{n}\right) = \left(\frac{-1}{n}\right)\left(\frac{4^2}{n}\right)\left(\frac{(r^k)^2}{n}\right) = -1.$$

Now write $n + 1 = d \cdot 2^s$ where $2 \nmid d$. Then $s > 1$ and $\frac{n+1}{2}$. We want to prove that $V_{2d} \equiv 0 \pmod n$ since then the congruence in Equation (3.5) will imply that n is a slpsp(P, Q).

Let α, β be the roots of the equation $x^2 - Px + Q = 0$. Then we have

$$\alpha = \frac{P + \sqrt{D}}{2} = \frac{4 \cdot r^k + \sqrt{-16 \cdot r^{2k}}}{2} = 2 \cdot r^k(1 + i)$$
$$\beta = \frac{P - \sqrt{D}}{2} = \frac{4 \cdot r^k - 2\sqrt{-16 \cdot r^{2k}}}{2} = 2 \cdot r^k(1 - i),$$

and after observing that $(1 + i)^2 = 2i$ and $(1 - i)^2 = -2i$, we see that

$$\alpha^{2d} = (2 \cdot r^k)^{2d}(1 + i)^{2d} = 2^{3d} \cdot r^{2kd} \cdot i^d$$
$$\beta^{2d} = (2 \cdot r^k)^{2d}(1 - i)^{2d} = 2^{3d} \cdot r^{2kd} \cdot (-i)^d.$$

Whence,

$$V_{2d} = \alpha^{2d} + \beta^{2d} = 2^{3d} \cdot r^{2kd}\big(i^d + (-i)^d\big) = 0.$$

Thus, by Equation (3.5) n is a slpsp(P, Q). □

Note that the key in the proof of Theorem 3.3.6 is that $4^2 = 2 \cdot 8$ when obtaining the values for α and β. Therefore the proof works exactly the same for any even integer A where $P = A \cdot r^k$ and $Q = \frac{A^2}{2} \cdot r^{2k}$.

We also have an analogue to the second part of Theorem 3.3.5. However, we need to further assume that the number $n \equiv 3 \pmod 4$ is an Euler pseudoprime to base 2 in addition to being a strong pseudoprime to base r. By an Euler pseudoprime we mean an odd composite integer n that satisfies Euler's criterion:

$$2^{(n-1)/2} \equiv \left(\frac{2}{n}\right) \pmod{n}.$$

Theorem 3.3.7. Let $n \equiv 3 \pmod 4$ be a strong pseudoprime base r that is also an Euler pseudoprime base 2. Let $k \geq 0$ be an integer. Set $P = r^k$ and $Q = 2r^{2k}$. Then n is also a $\mathrm{vpsp}(P, Q)$.

Proof. We will prove that $V_{n+1} \equiv 2Q \pmod n$ as this will show that n is a $\mathrm{vpsp}(P, Q)$ by Equation (3.3). As in the proof of Theorem 3.3.6, let α, β be the roots of the equation $x^2 - Px + Q = 0$. In this case we have

$$\alpha = r^k(1+i) \quad \text{and} \quad \beta = r^k(1-i).$$

Write $n+1 = 4M$, and note that $(1+i)^4 = (1-i)^4 = -4$, hence

$$\alpha^{n+1} = \beta^{n+1} = \left(r^k\right)^{n+1}(-1)^M \cdot 4^M,$$

and so

$$\begin{aligned} V_{n+1} = \alpha^{n+1} + \beta^{n+1} &= 2 \cdot \left(r^k\right)^{n+1}(-1)^M \cdot 4^M \\ &= 2 \cdot \left(r^2 r^{n-1}\right)^k (-1)^M \cdot 4^M \\ &= 2 \cdot r^{2k}\left(r^k\right)^{n-1}(-1)^M \cdot 2^{2M} \\ &= 2Q\left(r^k\right)^{n-1}(-1)^M \cdot 2^{2M-1} \\ &= 2Q\left(r^k\right)^{n-1}(-1)^M \cdot 2^{(n-1)/2}. \end{aligned} \tag{3.21}$$

Now since n is $\mathrm{spsp}(r)$, one has $2^{n-1} \equiv 1 \pmod n$. Moreover, by assumption n is also an Euler pseudoprime base 2, which gives that $2^{(n-1)/2} \equiv (2 \,|\, n) \pmod n$. This gives rise to two possible cases for Equation (3.21). Suppose $n \equiv 3 \pmod 8$. Then M is odd, which forces

$(-1)^M = -1$ and $(2 \,|\, n) = -1$. On the other hand suppose $n \equiv 7 \pmod 8$. Then M is even, and in this case $(-1)^M = 1$ and $(2 \,|\, n) = 1$. In either case, this simplifies Equation (3.21) to

$$V_{n+1} = 2Q(r^k)^{n-1}(-1)^M \cdot 2^{(n-1)/2} \equiv 2 \cdot 1 \cdot (-1)^M \cdot (2 \,|\, n) \equiv 2Q \pmod n. \qquad \square$$

4. CYCLOTOMIC POLYNOMIALS AT ROOTS OF UNITY

4.1 Introduction

The nth cyclotomic polynomial can be defined in the following way:

$$\Phi_n(x) = \prod_{\substack{1 \leq k < n \\ \gcd(n,k)=1}} (x - \zeta_n^k),$$

where ζ_n denotes a primitive nth root of unity. We recall that cyclotomic polynomials are irreducible over $\mathbb{Q}$ and satisfy the relation

$$x^n - 1 = \prod_{d \,|\, n} \Phi_n(x). \tag{4.1}$$

For $n > 1$ we have $\Phi_n(0) = 1$, so that the polynomial $\Phi_n(x) - 1$ is reducible. We want to know for what values k does $\Phi_k(x)$ divide $\Phi_n(x) - 1$. Since the roots of $\Phi_k(x)$ are precisely the primitive kth roots of unity, it is equivalent to determine for which values k does one have $\Phi_n(\zeta_k) = 1$.

There are two natural ways of addressing this question—to fix n, then find which values k satisfy $\Phi_n(\zeta_k) = 1$, or to fix k, then find the corresponding values of n for this k. Caldwell [10] took the former approach in searching for unique period primes. He found several sufficient criteria for k, given n. Bzdęga et al. [9] instead started with k and evaluated cyclotomic polynomials at roots of unity for all n for $k \leq 6$.

In this paper, we make incremental progress by restricting ourselves to k a power of 2. We prove that Bzdęga et al. [9] found all values n such that $\Phi_n(\zeta_k) = 1$ in the case $k = 8$. We make some progress on the case $k = 16$ and conjecture more generally that Bzdęga et al. [9] found all n for $k = 2^e$. It would be nice to have similar characterizations when k is an odd prime power, and more generally for any composite k.

4.2 A motivating example

One practical application for having an efficient method of determining which k satisfy $\Phi_k(x) \,|\, \Phi_n(x) - 1$ is in proving primality of integers of the form $\Phi_n(b)$. Take $n = 102 = 2 \cdot 3 \cdot 17$

and $b = 4500000000000420$, and let $N = \Phi_{102}(b)$. Then N is a 501-digit integer, and, as we will see in Section 4.4.2, $\Phi_k(b)$ divides $\Phi_{102}(b) - 1$ for $k \in \{1, 2, 4, 8, 16\}$:

$$\begin{aligned} N - 1 = b \cdot \Phi_1(b)\Phi_2(b)\Phi_4(b)\Phi_8(b)\Phi_{16}(b) \\ \cdot (b^{15} + b^{14} - b^{12} - b^{11} + b^9 + b^8 - b^6 - b^5 + b^3 + b^2 - 1). \end{aligned}$$

Thus, we were able to find a 267-digit (composite and completely factored) factor of $N - 1$ using our knowledge of the factorization of $\Phi_{102}(b) - 1$. Write

$$F = b \cdot \Phi_1(b)\Phi_2(b)\Phi_4(b)\Phi_8(b)\Phi_{16}(b)$$

and $R = (N - 1)/F$. Then F is 267 decimal digits and R is 235 decimal digits. The first five factors of F are all small, so their prime factorizations are easy to find. Searching small prime factors of $\Phi_{16}(b)$, we find 97 as a factor. The cofactor $\Phi_{16}(b)/97$ is a 124-digit composite number which can be split in a few minutes using the general number field sieve. With this, we can completely factor F:

$$\begin{aligned} F = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \cdot 19^2 \cdot 37 \cdot 79 \cdot 97 \cdot 181 \cdot 373 \cdot 2521 \cdot 2801 \cdot \\ \cdot 22901 \cdot 29921 \cdot 42457 \cdot 220939 \cdot 628997 \cdot 4191599 \cdot \\ \cdot 60307757 \cdot 1341640373 \cdot 17841327819089 \cdot \\ \cdot 8611682802363716529810782313724090135903849129512569693953 \cdot \\ \cdot 28924876127991751377374504318364186875465010728139464929066673 \cdot \\ \cdot 59931737437293016614567930699198100171879663785233449880539121. \end{aligned}$$

Using Pocklington's theorem (Theorem 1.2.1), we can prove that N is prime. First, note that $\gcd(F, R) = 1$. It is also easy to verify that $6^{N-1} \equiv 1 \pmod{N}$, and that, for every prime p dividing F, we have

$$\gcd\left(6^{(N-1)/p} - 1, N\right) = 1.$$

Then, since $F > \sqrt{N}$, we conclude that N is prime. If we had not known that $\Phi_{16}(b)$ divides $N - 1$, and had tried to factor $N - 1$ directly using trial division and ECM, we would not have found enough factors for F to satisfy $F > \sqrt{N}$, so we could not have proved N to be prime in this simple way.

4.3 Background

As always, $\phi(n)$ is the Euler phi function, that is, the number of positive integers up to n which are relatively prime to n. We record some well-known facts about cyclotomic polynomials needed for our discussion.

Lemma 4.3.1. For a prime number p and a positive integer n, we have

(a) $\Phi_{pn}(x) = \Phi_n(x^p)$ if $p \mid n$;

(b) $\Phi_{pn}(x) = \Phi_n(x^p)/\Phi_n(x)$ if $p \nmid n$;

(c) $\Phi_n(x) = x^{\phi(n)}\Phi_n(1/x)$ for $n > 1$.

The following important result due to Kurshan and Odlyzko [19] considerably reduces the possible values for k for a given n.

Lemma 4.3.2. *[9, Lemma 15]* Let $n > 1$. Then $\Phi_n(\zeta_k)$ is a nonzero real number if and only if k divides $\phi(n)$.

Proof. It is well-known that $\Phi_n(x)$ is a self-reciprocal polynomial. This implies that $\Phi_n(\zeta_k) = \zeta_k^{\phi(n)}\Phi_n(\zeta_k^{-1})$. On the other hand, $\Phi_n(\zeta_k) \in \mathbb{R}$ if and only if $\Phi_n(\zeta_k) = \overline{\Phi_n(\zeta_k)} = \Phi_n(\overline{\zeta}_k) = \Phi_n(\zeta_k^{-1})$. Thus we must have $\Phi_n(\zeta_k) = \zeta_k^{\phi(n)}\Phi_n(\zeta_k)$, which can only happen if $n = k$ or $k \mid \phi(n)$. Noting that $\Phi_n(\zeta_k) = 0$ if and only if $n = k$ completes the proof. □

We present the main results of Caldwell [10] without proof. Writing $n = p_1^{e_1} \cdots p_r^{e_r}$, we define $\operatorname{rad}(n) = p_1 \cdots p_r$.

Theorem 4.3.3. *[10, Theorem 2]* Let $n > 1$. Let $R = \operatorname{rad}(n)$ and let L be such that $n = LR$. Let p be any prime divisor of n. Then $\Phi_n(\zeta_k) = 1$ for all k such that

(a) $k \mid L$, whenever R is not a prime,

(b) $k \mid 2L$, $k \nmid L$, whenever R is not 2 or twice a prime,

(c) $k \mid (p-1)L$, whenever $pk \neq \gcd(k,L)R$,

(d) $k \mid \gcd\big(p+1, \phi(R/p)\big)L$, whenever $pk \neq \gcd(k,L)R$.

Caldwell [10] tested this theorem experimentally for $n \leq 2000$. He found 21206 solutions to $\Phi_n(\zeta_k) = 1$, and of those solutions, only eighteen of them were not a consequence of Theorem 4.3.3. The following three theorems account for those eighteen solutions.

Theorem 4.3.4. *[10, Corollary 3]* Let $p \equiv 19$, $q \equiv 11 \pmod{24}$, and suppose $3pq \mid n$. Then $\Phi_n(\zeta_k) = 1$ for all $k \mid 24L$, except when $k/\gcd(k,L) = 8$.

Theorem 4.3.5. *[10, Theorem 4]* Let p, q, r be distinct primes dividing n. If

$$k \mid \gcd(p^2-1, q^2-1, pqr-1)L \quad \text{or} \quad k \mid \gcd(p^2-1, q^2-1, pqr+1, L\phi(R/r)),$$

then $\Phi_n(\zeta_k) = 1$.

Theorem 4.3.6. *[10, Theorem 5]* Let p, q, r be distinct primes dividing n with p and q odd. If $k \mid \gcd(q \pm 1, r(p \pm 1), \phi(rpq)/2)L$, $k \nmid rpq$, then $\Phi_n(\zeta_k) = 1$. Here all four combinations $q \pm 1$ and $p \pm 1$ are possible.

The following theorem, which gives an explicit formula for evaluating $\Phi_n(\zeta_k)$ using Dirichlet characters, is due to Bzdęga et al. [9]. While theoretically nice, the formula would be computationally unwieldy as k gets large.

Theorem 4.3.7. *[9, Theorem 1]* Let $n, k > 1$ with $\gcd(n,k) = 1$. Denote by $G(k)$ the multiplicative group modulo k and by $\widehat{G}(k) = \hom((\mathbb{Z}/k\mathbb{Z})^\star, \mathbb{C}^\star)$ the set of Dirichlet characters modulo k. For all $\chi \in \widehat{G}(k)$ let

$$C_\chi(\zeta_k) = \sum_{g \in G(k)} \overline{\chi}(g) \log(1 - \zeta_k^g),$$

where we take the logarithm with imaginary part in $(-\pi, \pi]$. Then

$$\Phi_n(\zeta_k) = \exp\left(\frac{1}{\phi(k)} \sum_{\chi \in \widehat{G}(k)} C_\chi(\zeta_k) \chi(n) \prod_{p \mid n} (1 - \overline{\chi}(p)) \right).$$

In order to obtain a more easily computable characterization of when $\Phi_n(\zeta_k) = 1$, we will make use of the following two lemmas.

Lemma 4.3.8. *[9, Lemma 18]* Assume there exists a prime factor p of n such that $p \equiv 1 \pmod{k}$ and $e \geq 1$ such that $n = p^e n'$ with $p \nmid n'$.

(a) If $n' \neq k$, then $\Phi_n(\zeta_k) = 1$.

(b) If $n' = k$, then $\Phi_n(\zeta_k) = p$.

Proof. If $n' \neq k$, then by Lemma 4.3.1, we have $\Phi_n(x) = \Phi_{n'}(x^{p^m})/\Phi_{n'}(x^{p^{m-1}})$. Since $p \equiv 1 \pmod{k}$, we have $\zeta_k^p = \zeta_k$. Thus,

$$\Phi_n(\zeta_k) = \frac{\Phi_{n'}(\zeta_k^{p^m})}{\Phi_{n'}(\zeta_k^{p^{m-1}})} = \frac{\Phi_{n'}(\zeta_k)}{\Phi_{n'}(\zeta_k)} = 1.$$

On the other hand, if $n' = k$, the identity $\Phi_n(x) = \Phi_k(x^{p^m})/\Phi_k(x^{p^{m-1}})$ yields the indeterminate form $0/0$. Applying L'Hôpital's rule, we obtain

$$\Phi_n(\zeta_k) = \frac{p^m \zeta_k^{p^m - 1} \Phi'_k(\zeta_k^{p^m})}{p^{m-1} \zeta_m^{p^{m-1}-1} \Phi'_k(\zeta_k^{p^{m-1}})} = \frac{p^m \zeta_k^{-1} \Phi'_k(\zeta_k)}{p^{m-1} \zeta_m^{-1} \Phi'_k(\zeta_k)} = p. \qquad \square$$

Lemma 4.3.9. *[9, Lemma 19]* Assume there exists a prime factor p of n such that $p \equiv -1 \pmod{k}$ and $e \geq 1$ such that $n = p^e n'$ with $p \nmid n'$.

(a) If $n' = 1$, then $\Phi_n(\zeta_k) = -\zeta_k^{(-1)^e}$.

(b) If $n' \neq k$, then $\Phi_n(\zeta_k) = \zeta_k^{(-1)^e \phi(n')}$. Furthermore, if $n' \geq 3$, then $\Phi_n(\zeta_k) = \zeta_k^{\phi(n)/2}$.

(c) If $n' = k$, then $\Phi_n(\zeta_k) = -p\zeta_k^{(-1)^e \phi(k)}$.

Proof.

(a) By Equation (4.1), one has

$$\begin{aligned} x^{p^e} - 1 &= \prod_{d \,|\, p^e} \Phi_d(x) = \prod_{j=0}^{e} \Phi_{p^j}(x) \\ &= \Phi_{p^e}(x) \prod_{j=0}^{e-1} \Phi_{p^j}(x) = \Phi_{p^e}(x)(x^{p^{e-1}} - 1). \end{aligned}$$

The last equality uses the fact that for a prime p and positive integer e, one has $\Phi_{p^e}(x) = \sum_{j=0}^{p-1} x^{jp^{e-1}}$, and $\Phi_{p^0}(x) = \Phi_1(x) = x - 1$. This, together with the assumption that $p \equiv -1 \pmod{k}$, gives

$$\Phi_{p^e}(\zeta_k) = \frac{\zeta_k^{p^e} - 1}{\zeta_k^{p^{e-1}} - 1} = \frac{\zeta_k^{(-1)^e-1}}{\zeta_k^{(-1)^{e-1}} - 1} = -\zeta_k^{(-1)^e}$$

(b) By Lemma 4.3.1, we have $\Phi_n(x) = \Phi_{pn'}(x^{p^{e-1}}) = \Phi_{n'}(x^{p^e})/\Phi_{n'}(x^{p^{e-1}})$. Evaluating at ζ_k, we obtain

$$\Phi_n(\zeta_k) = \frac{\Phi_{n'}(\zeta_k^{p^e})}{\Phi_{n'}(\zeta_k^{p^{e-1}})} = \frac{\Phi_{n'}(\zeta_k^{(-1)^e})}{\Phi_{n'}(\zeta_k^{(-1)^{e-1}})} = \zeta_k^{(-1)^e\phi(n')},$$

where the last equality uses part (c) of Lemma 4.3.1.

(c) With $n' = k$, first observe that differentiating the identity $\Phi_k(x) = x^{\phi(k)}\Phi_k(1/x)$ yields

$$\Phi_k'(x) = \phi(k)x^{\phi(k)-1}\Phi_k(1/x) - x^{\phi(k)-2}\Phi_k'(1/x).$$

Note that $\Phi_k(\zeta_k) = \Phi_k(1/\zeta_k) = 0$, hence evaluating at $x = \zeta_k^{(-1)^e}$ gives

$$\Phi_k'(\zeta_k^{(-1)^e}) = -\zeta_k^{(-1)^e(\phi(k)-2)}\Phi_k'(\zeta_k^{(-1)^{(e+1)}}). \tag{4.2}$$

On the other hand, by L'Hôpital's rule, we have

$$\Phi_n(\zeta_k) = \frac{p^e\zeta_k^{p^e-1}\Phi_k(\zeta_k^{p^e})}{p^{e-1}\zeta_k^{p^{e-1}-1}\Phi_k'(\zeta_k^{e-1})} = p\zeta_k^{2(-1)^e}\frac{\Phi_k'(\zeta_k^{(-1)^e})}{\Phi_k'(\zeta_k^{(-1)^{e+1}})}.$$

After comparing with the identity in (4.2), the claim follows immediately. □

The property from part (c) of Lemma 4.3.1 implies that for $n \geq 2$, one has $\Phi_n(\zeta_k) = \pm|\Phi_n(\zeta_k)|\,\zeta_k^{\Phi(n)/2}$. The following lemma determines the sign.

Lemma 4.3.10. *[9, Lemma 16]* Write $\xi_k = e^{2j\pi i/k.}$ For $n \geq 2$ we have

$$\Phi_n(\xi_k) = (-1)^{\phi(nj/k;n)}|\Phi_n(\xi_k)|\,\xi_k^{\phi(n)/2},$$

where $\phi(x;n)$ is the number of positive integers $j \leq x$ with $\gcd(j,n) = 1$.

Denote by $\Omega(n)$ the number of prime divisors of n, counted with multiplicity, and let $\omega(n)$ be the number of distinct prime divisors of n.

Theorem 4.3.11. *[9, Corollary 22]* Let $k \in \{5, 8, 10, 12\}$ and $n > 1$ with $\gcd(n, k) = 1$. Suppose that n has no prime divisor $\pm 1 \pmod{k}$. Then

$$\log|\Phi_n(\zeta_k)| = (-1)^{\Omega(n)-1} 2^{\omega(n)-1} \log|\gamma_k|\,,$$

where

$$\gamma_k = \begin{cases} 1 + \zeta_k & k = 5; \\ 1 + \zeta_k + \zeta_k^2 & k \in \{8, 10\}\,; \\ 1 + \zeta_k + \zeta_k^2 + \zeta_k^3 + \zeta_k^4 & k = 12. \end{cases}$$

For low order k, Bzdęga et al. [9] computes $\Phi_n(\zeta_k)$ explicitly for $k \in \{1, 2, 3, 4, 5, 6\}$. In the case $k = 5$, the authors use Theorem 4.3.11 and Lemma 4.3.10 and mention that the case $k \in \{8, 10, 12\}$ can be obtained by a similar procedure, however they do not actually carry out these computations. Note that as we are primarily interested in finding when $\Phi_n(\zeta_k) = 1$, Theorem 4.3.11 will not produce any results in the case of $k = 8$, as $\log|\gamma_8| = \log(\sqrt{2}+1) \neq 0$.

4.4 Evaluating $\Phi_n(\zeta_k)$ for $k = 2^e$

Throughout this section whenever we write a number $n = p_1^{e_1} \cdots p_r^{e_r} q_1^{f_1} \cdots q_s^{f_s}$, where e_i, f_j are nonnegative integers, each of the p_i, q_j are assumed to be distinct prime numbers. We will clarify the distinction between p and q later.

4.4.1 Case $k = 8$

Since we are ultimately concerned when $\Phi_n(\zeta_k) = 1$, we will assume throughout that k divides $\phi(n)$ so that $\Phi_n(\zeta_k)$ is real. We will make extensive use of the following well-known fact. We will treat the cases $8 \mid n$ and $8 \nmid n$ separately. More generally, whenever k is a power of 2 dividing n, we have the following:

Theorem 4.4.1. Let $k = 2^e$ with $e \geq 1$. Suppose $k \mid n$. Then we have

$$\Phi_n(\zeta_k) = \begin{cases} 0 & n = k \\ p & n = 2^e p^r \\ 1 & \text{otherwise} \end{cases}$$

with p a prime number and $r \geq 1$.

Proof. For $n = k$ this is clear. The case $k = 2$ is well-known. We proceed by induction on e. Assume the theorem holds for $k = 2^e$. Denote by $\nu_p(a)$ the p-adic valuation of a; by assumption $\nu_2(n) \geq 3$. Then by Lemma 4.3.1,

$$\Phi_n(\zeta_{2k}) = \Phi_{n/2}(\zeta_{2k}^2) = \Phi_{n/2}(\zeta_k),$$

and the result follows by the induction hypothesis. □

Next we consider the case $8 \nmid n$. In light of Lemma 4.3.8 we further assume that n has no prime factor $p \equiv 1 \pmod 8$. If n has a prime factor congruent to -1 modulo 8, then carrying out Lemma 4.3.9 explicitly, write $n = p^e n'$ with $p \nmid n'$ with $p \equiv -1 \pmod 8$:

(a) If $n' = 1$, then

$$\Phi_n(\zeta_8) = -\zeta_8^{(-1)^e} = \begin{cases} -\zeta_8 & \text{if } e \equiv 0 \pmod 2 \\ \zeta_8^3 & \text{if } e \equiv 1 \pmod 2 \end{cases}.$$

(b) If $n' \neq 8$, then

$$\Phi_n(\zeta_8) = \zeta_8^{(-1)^e \phi(n')} = \begin{cases} -1 & \text{if } 4 \mid \phi(n') \text{ but } 8 \nmid \phi(n') \\ 1 & \text{if } 8 \mid \phi(n') \end{cases}.$$

(c) If $n' = 8$, then $\Phi_n(\zeta_8) = -p\zeta_8^{(-1)^e \phi(8)} = p$. Note that this also follows from Theorem 4.4.1.

Now we may assume that n is an integer whose odd prime factors are all 3 or 5 modulo 8. We consider three possible cases: $n = 4q_1^{e_1} \cdots q_r^{e_r}$, $n = 2q_1^{e_1} \cdots q_r^{e_r}$ and $n = q_1^{e_1} \cdots q_r^{e_r}$ with $q_i \equiv 3$ or $5 \pmod 8$ distinct primes. Denote $m = q_1^{e_1} \cdots q_r^{e_r}$.

Case $n = 4m$: Here we easily reduce to the case $k = 4$. (See Bzdęga et al. [9, Lemma 23].)

Let e_1, e_2 be positive integers. Then we have

$$\Phi_n(\zeta_8) = \Phi_{2m}(\zeta_8^2) = \Phi_{2m}(\zeta_4) = \begin{cases} 0 & \text{if } m = 1 \\ -1 & \text{if } m = q_1^{e_1} q_2^{e_2},\ q_j \equiv 3 \bmod 4 \\ 1 & \text{otherwise} \end{cases}$$

Case $n = 2m$: Using Lemma 4.3.1,

$$\Phi_n(\zeta_8) = \frac{\Phi_m(\zeta_8^2)}{\Phi_m(\zeta_8)} = \frac{\Phi_m(\zeta_4)}{\Phi_m(\zeta_8)}. \tag{4.3}$$

If some $q_j \equiv 5 \pmod 8$, then $q_j \equiv 1 \pmod 4$, and $\Phi_m(\zeta_4) = 1$ by Lemma 4.3.8. Otherwise all $q_j \equiv 3 \pmod 4$. Since by assumption 8 divides $\phi(n) = \phi(m)$, we must have $r \geq 3$, as $\phi(q_j^{e_j}) = q^{e_j - 1}(q_j - 1)$ is divisible by 2 but not 4. So again by Lemma 4.3.9, $\Phi_n(\zeta_4) = 1$. We have now determined the numerator in (4.3), and we are left now with the final case.

Case $n = m$: By assumption we have $8 \mid \phi(n) = q_1^{e_1 - 1} \cdots q_r^{e_r - 1}(q_1 - 1) \cdots (q_r - 1)$. So either all $q_i \equiv 3 \pmod 8$ with $r \geq 3$ or there exists some $q_j \equiv 5 \pmod 8$ with $r \geq 2$. To finish this case, we start with some lemmas.

Lemma 4.4.2. If $n = p_1 \cdots p_r$ with all $p_i \equiv 3 \pmod 8$, then

$$\Phi_n(\zeta_8) = \left(\frac{\zeta_8 - 1}{\zeta_8^3 - 1}\right)^{(-1)^r 2^{r-1}} = (\zeta_8^2 + \zeta_8 + 1)^{(-2)^{r-1}}.$$

Proof. Through repeated use of Lemma 4.3.1, when $r > 1$ we have that

$$\begin{aligned}\Phi_{p_1\cdots p_r}(x) &= \left(\frac{\prod \Phi_{p_1}(x^{p_2^{e_2}\cdots p_r^{e_r}})}{\prod \Phi_{p_1}(x^{p_2^{f_2}\cdots p_r^{f_r}})}\right)^{(-1)^r} \\ &= \left(\frac{\prod (x^{p_1 p_2^{e_2}\cdots p_r^{e_r}}-1)/(x^{p_2^{e_2}\cdots p_r^{e_r}}-1)}{\prod (x^{p_1 p_2^{f_2}\cdots p_r^{f_r}}-1)/(x^{p_2^{f_2}\cdots p_r^{f_r}}-1)}\right)^{(-1)^r}, \end{aligned} \tag{4.4}$$

where the product in the numerator is taken over the 2^{r-2} odd-cardinality subsets of the set $\{p_2, \ldots, p_r\}$ and the product in the denominator is taken over the 2^{r-2} even-cardinality subsets of $\{p_2, \ldots, p_r\}$. Now since $\sum e_i \equiv 1 \pmod 2$ and $\sum_{f_i} \equiv 0 \pmod 2$, we have

$$\zeta_8^{p_1 p_2^{e_2}\cdots p_r^{e_r}} = \zeta_8^{3^{1+\sum e_i}} = \zeta_8 \quad \text{and} \quad \zeta_8^{p_1 p_2^{f_2}\cdots p_r^{f_r}} = \zeta_8^{3^{1+\sum f_i}} = \zeta_8^3.$$

Combining this with (4.4), we obtain

$$\Phi_{p_1\cdots p_r}(\zeta_8) = \left(\frac{\zeta_8 - 1}{\zeta_8^3 - 1}\right)^{(-1)^r 2^{r-1}}.$$

Noting that this identity is also valid for $r = 1$ completes the proof. □

Lemma 4.4.3. If $n = q_1 \cdots q_s$ with all $q_i \equiv 5 \pmod 8$, then

$$\Phi_n(\zeta_8) = \left(\frac{\zeta_8 - 1}{-\zeta_8 - 1}\right)^{(-1)^s 2^{s-1}} = (\zeta_8^3 + \zeta_8^2 + \zeta_8)^{(-2)^{s-1}}.$$

Proof. Upon noting that $\zeta_8^5 = -\zeta_8$, the proof is the same as Lemma 4.4.2, mutatis mutandis. □

Lemma 4.4.4. Let $n = p_1 \cdots p_r q_1^{f_1} \cdots q_s^{f_s}$ with $p_i \equiv 3 \pmod 8$ and $q_j \equiv 5 \pmod 8$. Let $\sigma = \sum f_i$. Then

$$\Phi_n(\zeta_8) = \left((-1)^\sigma 2\zeta_8^3 - (-1)^\sigma 2\zeta_8 + 3\right)^{(-1)^r 2^{r+s-2}}$$

Proof. Through repeated use of Lemma 4.3.1, we see that

$$
\begin{aligned}
\Phi_n(\zeta_8) &= \left(\frac{\Phi_{p_1 \cdots p_r}\big((-1)^{\sigma}\zeta_8\big)}{\Phi_{p_1 \cdots p_r}\big((-1)^{1+\sigma}\zeta_8\big)} \right)^{2^{s-1}} \\
&= \left[\left(\frac{(-1)^{\sigma}\zeta_8 - 1}{(-1)^{\sigma}\zeta_8^3 - 1} \right)^{(-2)^{r-1}} \left(\frac{(-1)^{\sigma+1}\zeta_8 - 1}{(-1)^{\sigma+1}\zeta_8^3 - 1} \right)^{(-2)^{r-1}} \right]^{2^{s-1}} \\
&= \left[\left(\frac{(-1)^{\sigma}\zeta_8 - 1}{(-1)^{\sigma}\zeta_8^3 - 1} \right) \left(\frac{(-1)^{\sigma+1}\zeta_8^3 - 1}{(-1)^{\sigma+1}\zeta_8 - 1} \right) \right]^{(-1)^r 2^{r+s-2}} \\
&= \begin{cases} (2\zeta_8^3 - 2\zeta_8 + 3)^{(-1)^r 2^{r+s-2}} & \text{if } \sigma \equiv 0 \pmod 2 \\ (-2\zeta_8^3 + 2\zeta_8 + 3)^{(-1)^r 2^{r+s-2}} & \text{if } \sigma \equiv 1 \pmod 2 \end{cases} \\
&= \Big((-1)^{\sigma} 2\zeta_8^3 - (-1)^{\sigma} 2\zeta_8 + 3 \Big)^{(-1)^r 2^{r+s-2}},
\end{aligned}
$$

as desired. □

Theorem 4.4.5. Let $n = p_1^{e_1} \cdots p_r^{e_r} q_1^{f_1} \cdots q_s^{f_s}$ with $p_i \equiv 3 \pmod 8$ and $q_j \equiv 5 \pmod 8$. Let $\rho = \sum e_i$ and $\sigma = \sum f_j$. Assume $r > 0$; then

$$\Phi_n(\zeta_8) = \left(\frac{2 - (-1)^{\rho+\sigma-r}(\zeta_8 + \zeta_8^{-1})}{2 + (-1)^{\rho+\sigma-r}(\zeta_8 + \zeta_8^{-1})} \right)^{(-1)^r 2^{r+s-2}}$$

Proof. As we saw in the previous lemma,

$$\Phi_n(\zeta_8) = \left(\frac{\Phi_{p_1^{e_1} \cdots p_r^{e_r}}\big((-1)^{\sigma}\zeta_8\big)}{\Phi_{p_1^{e_1} \cdots p_r^{e_r}}\big((-1)^{1+\sigma}\zeta_8\big)} \right)^{2^{s-1}} = \left(\frac{\Phi_{p_1 \cdots p_r}\left(((-1)^{\sigma}\zeta_8)^{3^{\rho-r}} \right)}{\Phi_{p_1 \cdots p_r}\left(((-1)^{1+\sigma}\zeta_8)^{3^{\rho-r}} \right)} \right)^{2^{s-1}} \tag{4.5}$$

$$
\begin{aligned}
&= \Phi_{p_1 \cdots p_r}\left(\left((-1)^{\rho+\sigma-r} \zeta_8^{(-1)^{\rho-r}} \right) \right)^{2^{s-1}} \Phi_{p_1 \cdots p_r}\left(\left((-1)^{1+\sigma+\rho-r} \zeta_8^{(-1)^{\rho-r}} \right) \right)^{2^{1-s}} \\
&= \left[\left(\frac{(-1)^{\rho+\sigma-r}\zeta_8^{(-1)^{\rho-r}} - 1}{(-1)^{1+\rho+\sigma-r}\zeta_8^{(-1)^{1+\rho-r}} - 1} \right) \left(\frac{(-1)^{\sigma+\rho-r}\zeta_8^{(-1)^{1+\rho-r}} - 1}{(-1)^{1+\sigma+\rho-r}\zeta_8^{(-1)^{\rho-r}} - 1} \right) \right]^{(-1)^r 2^{r+s-1}} \qquad (4.6) \\
&= \left(\frac{2 - (-1)^{\rho+\sigma-r}(\zeta_8 + \zeta_8^{-1})}{2 + (-1)^{\rho+\sigma-r}(\zeta_8 + \zeta_8^{-1})} \right)^{(-1)^r 2^{r+s-2}},
\end{aligned}
$$

where in (4.5) we use Lemma 4.3.1 and in (4.6) we use Lemma 4.4.2. □

Finally, since Theorem 4.4.5 assumes $r > 0$, it remains to deal with the case $n = q_1^{f_1} \cdots q_s^{f_s}$ with all $q_i \equiv 5 \pmod 8$. But this is just an application of Lemma 4.3.1 followed by Lemma 4.4.3.

Lemma 4.4.6. Let $n = q_1^{f_1} \cdots q_s^{f_s}$ with all $q_i \equiv 5 \pmod 8$. Let $\sigma = \sum f_i$. Then

$$\Phi_{q_1^{f_1} \cdots q_s^{f_s}}(\zeta_8) = \left((-1)^{\sigma - s}\zeta_8^3 + \zeta_8^2 + (-1)^{\sigma - s}\zeta_8\right)^{(-2)^{s-1}}.$$

We sum up these results with the following theorem.

Theorem 4.4.7. We have $\Phi_n(\zeta_8) = 1$ if and only if one of the following conditions holds:

- $n = p^e n'$ with $p \nmid n'$, $p \equiv 1 \pmod 8$ and $n' \neq 8$;
- $8 \mid n$ and $n \neq 8p^e$ with p prime and e a nonnegative integer;
- $n = p^e n'$ with $p \nmid n'$, $p \equiv -1 \pmod 8$, $n' \neq 8$ and $8 \mid \phi(n')$;
- $n = 4m$, where m is odd but $m \neq q_1^{e_1} q_2^{e_2}$, where $q_i \equiv 3 \pmod 4$ and $e_j > 0$.

Proof. It only remains to verify that $\Phi_n(\zeta_8) \neq 1$ for $n = p_1^{e_1} \cdots p_r^{e_r} q_1^{f_1} \cdots q_s^{f_s}$. From Theorem 4.4.5 if $r > 0$, we have

$$\Phi_n(\zeta_8) \begin{cases} \left((-1)^{\rho+\sigma-r}\zeta_8^3 - \zeta_8^2 + 1\right)^{(-1)^r 2^{r+s-2}} & \text{if } \rho \equiv r \pmod 2 \\ \left(\zeta_8^2 + (-1)^{\rho-r}\zeta_8 + 1\right)^{(-1)^r 2^{r+s-2}} & \text{if } \rho \not\equiv r \pmod 2, \end{cases}$$

but $\left|(-1)^{\rho+\sigma-r}\zeta_8^3 - \zeta_8^2 + 1\right| \neq 1$ and $\left|\zeta_8^2 + (-1)^{\rho-r}\zeta_8 + 1\right| \neq 1$. Hence $\Phi_n(\zeta_8) \neq 1$ in this case. Similarly, if $r = 0$, we have

$$\Phi_{q_1^{f_1} \cdots q_s^{f_s}}(\zeta_8) = \left((-1)^{\sigma - s}\zeta_8^3 + \zeta_8^2 + (-1)^{\sigma - s}\zeta_8\right)^{(-2)^{s-1}},$$

but $\left|(-1)^{\sigma-s}\zeta_8^3 + \zeta_8^2 + (-1)^{\sigma-s}\zeta_8\right| \neq 1$, hence $\Phi_n(\zeta_8) \neq 1$. □

4.4.2 Case $k = 16$

As we will see, the case $k = 16$ is already much more complicated than the case $k = 8$. We start by carrying out Lemma 4.3.9. Write $n = p^e n'$ with $p \equiv -1 \pmod{16}$, where $p \nmid n'$. Then

(a) If $n' = 1$, then $\Phi_n(\zeta_{16}) = -\zeta_{16}^{(-1)^e}$.

(b) If $n' \notin \{1, 16\}$, then $\Phi_n(\zeta_{16}) = \zeta_{16}^{(-1)^e \phi(n')}$.

(c) If $n' = 16$, then $\Phi_n(\zeta_{16}) = p$, which again follows from Theorem 4.4.1 as well.

In case (b), we see that $\Phi_n(\zeta_{16})$ is real-valued if and only if $\Phi_n(\zeta_{16}) = \pm 1$, and

$$\Phi_n(\zeta_{16}) = \begin{cases} 1 & \text{if } 16 \mid \phi(n') \\ -1 & \text{if } 8 \mid \phi(n') \text{ but } 16 \nmid \phi(n'). \end{cases}$$

Writing $n' = 2^f p_1^{e_1} \cdots p_r^{e_r}$, we have $16 \mid \phi(n')$ in the following cases:

- $r \geq 4$;
- $r = 3$ and $f \geq 2$;
- $r = 3$ and some p_j is congruent to one of $\{5, 9, 13\}$ modulo 16;
- $r = 2$ and $f \geq 3$;
- $r = 2$ and some p_j is congruent to 9 modulo 16; or
- $r = 1$ and $f \geq 5$.

Moreover, we have $8 \mid \phi(n')$ in the following cases:

- $r \geq 3$;
- $r = 2$ and $f \geq 3$;
- $r = 2$ and some p_j is 5 modulo 8; or
- $r = 1$ and $f \geq 4$.

From here on we will assume that n has no prime factor $p \equiv \pm 1 \pmod{16}$. In light of Theorem 4.4.1, we will also assume that 16 does not divide n. Looking back at the proof of Lemma 4.4.2 and Lemma 4.4.3, we see that we only needed the fact that $3 = 8/2 - 1$ and

$5 = 8/2 + 1$. This immediately leads to the following generalization which gives a similar result in the case $k = 16$.

Lemma 4.4.8. Let $k = 2^e$. If $n = p_1 \cdots p_r$ with all $p_i \equiv k/2 + 1 \pmod{k}$, then

$$\Phi_n(\zeta_k) = \left(\frac{\zeta_{16} - 1}{\zeta_{16}^{k/2+1} - 1} \right)^{(-1)^r 2^{r-1}}.$$

Similarly, if all $p_i \equiv k/2 - 1 \pmod{k}$, then

$$\Phi_n(\zeta_k) = \left(\frac{\zeta_{16} - 1}{\zeta_{16}^{k/2-1} - 1} \right)^{(-1)^r 2^{r-1}}.$$

Other possible values of n require more work. In a similar fashion to our work for $k = 8$, we start with n having primes of a certain form and work our way to a more general n. We recall the following identities, which can be found in Gradshteyn and Ryzhik[15]:

$$\begin{aligned}
\alpha_n &= \sum_{k \equiv 0 \bmod 4} \binom{n}{k} = \frac{1}{2}\left(2^{n-1} + 2^{n/2} \cos \frac{\pi n}{4}\right) \\
\beta_n &= \sum_{k \equiv 2 \bmod 4} \binom{n}{k} = \frac{1}{2}\left(2^{n-1} - 2^{n/2} \cos \frac{\pi n}{4}\right) \\
\gamma_n &= \sum_{k \equiv 1 \bmod 4} \binom{n}{k} = \frac{1}{2}\left(2^{n-1} + 2^{n/2} \sin \frac{\pi n}{4}\right) \\
\delta_n &= \sum_{k \equiv 3 \bmod 4} \binom{n}{k} = \frac{1}{2}\left(2^{n-1} - 2^{n/2} \sin \frac{\pi n}{4}\right)
\end{aligned}$$

Lemma 4.4.9. Let $n = p_1 \cdots p_r$ with $p_i \equiv m \pmod{16}$, where $m \in \{3, 5, 11, 13\}$. Then

$$\Phi_n(\zeta_{16}) = \left(\frac{(\zeta_{16} - 1)^{\alpha_r} (-\zeta_{16} - 1)^{\beta_r}}{(\zeta_{16}^m - 1)^{\gamma_r} (-\zeta_{16}^m - 1)^{\delta_r}} \right)^{(-1)^r}.$$

Proof. For $m \in \{3, 5, 11, 13\}$, we have

$$\zeta_{16}^{m^e} = \begin{cases} \zeta_{16} & \text{if } e \equiv 0 \pmod 4 \\ \zeta_{16}^m & \text{if } e \equiv 1 \pmod 4 \\ -\zeta_{16} & \text{if } e \equiv 2 \pmod 4 \\ -\zeta_{16}^m & \text{if } e \equiv 3 \pmod 4. \end{cases}$$

Combining this fact with (4.4), the result follows. □

In the same way that we could generalize Lemma 4.4.2 and Lemma 4.4.3, we have the following generalization of Theorem 4.4.5.

Theorem 4.4.10. Let $k = 2^e$. Let $n = p_1^{e_1} \cdots p_r^{e_r} q_1^{f_1} \cdots q_s^{f_s}$ with $p_i \equiv k/2 - 1 \pmod k$ and $q_j \equiv k/2 + 1 \pmod k$. Let $\rho = \sum e_i$, $\sigma = \sum f_j$, and assume $r \neq 0$. Then

$$\Phi_n(\zeta_k) = \left(\frac{2 - (-1)^{\rho+\sigma-r}\left(\zeta_k + \zeta_k^{-1}\right)}{2 + (-1)^{\rho+\sigma-r}\left(\zeta_k + \zeta_k^{-1}\right)} \right)^{(-1)^r 2^{r+s-2}}.$$

Theorem 4.4.11. Let $n = p_1^{e_1} \cdots p_r^{e_r} q_1^{f_1} \cdots q_s^{f_s}$ with $p_i \equiv 3 \pmod{16}$ and $q_j \equiv 5 \pmod{16}$. Let $\rho = \sum e_i$ and $\sigma = \sum f_j$. Then

$$\Phi_n(\zeta_{16}) = \frac{\displaystyle\prod_{i=0}^{\lfloor s/2 \rfloor} \left(\frac{\left(\zeta_{16}^{5^{\sigma-2i}3^{\rho-r}} - 1\right)^{\alpha_r} \left(-\zeta_{16}^{5^{\sigma-2i}3^{\rho-r}} - 1\right)^{\beta_r}}{\left(\zeta_{16}^{5^{\sigma-2i}3^{1+\rho-r}} - 1\right)^{\gamma_r} \left(-\zeta_{16}^{5^{\sigma-2i}3^{1+\rho-r}} - 1\right)^{\delta_r}} \right)^{(-1)^r \binom{s}{2i}}}{\displaystyle\prod_{i=0}^{\lfloor (s-1)/2 \rfloor} \left(\frac{\left(\zeta_{16}^{5^{\sigma-2i-1}3^{\rho-r}} - 1\right)^{\alpha_r} \left(-\zeta_{16}^{5^{\sigma-2i-1}3^{\rho-r}} - 1\right)^{\beta_r}}{\left(\zeta_{16}^{5^{\sigma-2i-1}3^{\rho-r}} - 1\right)^{\gamma_r} \left(-\zeta_{16}^{5^{\sigma-2i-1}3^{1+\rho-r}} - 1\right)^{\delta_r}} \right)^{(-1)^r \binom{s}{2i+1}}}$$

Proof. Using the usual reductions, we have

$$\Phi_n(\zeta_{16}) = \frac{\displaystyle\prod_{i=0}^{\lfloor s/2 \rfloor} \left(\Phi_{n_{p_1^{e_1}\cdots p_r^{e_r}}}\left(\zeta_{16}^{5^{\sigma-2i}}\right)\right)^{\binom{s}{2i}}}{\displaystyle\prod_{i=0}^{\lfloor (s-1)/2 \rfloor} \left(\Phi_{n_{p_1^{e_1}\cdots p_r^{e_r}}}\left(\zeta_{16}^{5^{\sigma-2i-1}}\right)\right)^{\binom{s}{2i+1}}} = \frac{\displaystyle\prod_{i=0}^{\lfloor s/2 \rfloor} \left(\Phi_{n_{p_1\cdots p_r}}\left(\zeta_{16}^{5^{\sigma-2i}3^{\rho-r}}\right)\right)^{\binom{s}{2i}}}{\displaystyle\prod_{i=0}^{\lfloor (s-1)/2 \rfloor} \left(\Phi_{n_{p_1\cdots p_r}}\left(\zeta_{16}^{5^{\sigma-2i-1}3^{\rho-r}}\right)\right)^{\binom{s}{2i+1}}}.$$

Applying Lemma 4.4.9 completes the proof. □

Remark 1. Replacing 3 by 11 and 5 by 13, we get an analogous statement whose proof is the same.

In a way similar to the case $k = 8$, we can build this up to get an extremely complicated expression for $\Phi_n(\zeta_{16})$. However, unless there is a way to greatly simplify the expression in Theorem 4.4.11, writing it down is far too unwieldy. It certainly seems that the expressions in Lemma 4.4.9 and Theorem 4.4.11 should never be equal to 1, and we have verified this in some subcases in Mathematica. That said, we believe the case for $k = 8$ can be generalized in the following way. Let $k = 2^e$. Then we have established $\Phi_n(\zeta_k) = 1$ if

- $n = p^f n'$ with $p \nmid n'$, $p \equiv 1 \pmod{k}$ and $n' \neq k$;
- $k \mid n$ and $n \neq kp^f$ with p prime and f a nonnegative integer;
- $n = p^f n'$ with $p \nmid n'$, $p \equiv -1 \pmod{k}$ and $k \mid \phi(n')$.

In the case $k = 8$ we had one final condition to make the statement biconditional. Namely, if $n = 4m$, where m is odd but $m \neq q_1^{e_1} q_2^{e_2}$, where $q_i \equiv 3 \pmod 4$ and $e_j \geq 0$. More generally, suppose m is odd. Then $\Phi_{2^{e-1}m}(\zeta_k) = \Phi_{2m}(\zeta_k^{2^{e-2}})$. For $2 \leq j < e-1$ we similarly find $\Phi_{2^{e-j}m}(\zeta_k) = \Phi_{2m}(\zeta_k^{2^{e-j-1}})$. Using these identities, we can recursively apply the above conditions to find when $\Phi_n(\zeta_k) = 1$.

We carried this out in Sage for $k = 16$ and n up to 10 000. We found 2375 values of n such that $\Phi(\zeta_{16}) = 1$. Of these, 1390 such n could be explained by the first condition above, 488 could be explained by the second, and 183 could be explained by the third. The above conditions are not mutually exclusive, so after eliminating repeats, there were 488 values of n not explained by these first three conditions.

Upon inspecting these unexplained values of n, we found that all of them were evenly divisible by 4 or 8. For those evenly divisible by 4, say $n = 4m$ with m odd. Then applying the above identity, we have $\Phi_{4m}(\zeta_{16}) = \Phi_{2m}(\zeta_{16}^2) = \Phi_{2m}(\zeta_8)$ so that we can apply Theorem 4.4.7. In the situation where $n = 8m$ with m odd, we get $\Phi_{8m}(\zeta_{16}) = \Phi_{2m}(\zeta_{16}^4) = \Phi_{2m}(\zeta_4)$, in which case we may apply Lemma 23 of Bzdęga et al. [9]. This explained every value of n.

Conjecture. For $k = 2^e$, the above procedure finds all possible values n such that $\Phi_n(\zeta_k) = 1$.

5. CONCLUSION AND FUTURE WORK

Let $\gcd(a, b) = 1$. It has been known for more than a century that the primes p for which $ap + b$ is also prime are rarer than all primes, in the sense that the sum of the reciprocals of such primes converges or is finite, while the sum of the reciprocals of all primes diverges. Our Theorem 2.3.4 quantifies this rarity by estimating the sum of the reciprocals of the primes p with $p + 6$ also prime. Since we do not know whether there are infinitely many such primes all we can do is bound this sum in an interval $(1.2608, 1.9760)$. We have done this for only a few cases, but it is clear that one could do it for any a, b, with $\gcd(a, b) = 1$. (If $\gcd(a, b) > 1$, the problem is much easier because $ap + b$ is always divisible by $\gcd(a, b)$, so the sum of the reciprocals of such primes would be the empty sum.)

Because the tightness of the upper bounds we have found depends on explicitly computing the lower bounds, one could obtain better bounds by computing the sums $S_{a,b}(x_0)$ up to a larger limit x_0. As noted in Wagstaff [38], one could probably achieve slightly better upper bounds with the same x_0 by assuming the Extended Riemann Hypothesis as was done in Klyve [18] for the sum of reciprocals of twin primes.

Knowledge of the existence of Carmichael numbers dates back to the early 1900s. Alford et al. [2] proved in 1994 that there are infinitely many Carmichael numbers. In 2013, Wright [39] gave the first unconditional proof that there are infinitely many Carmichael numbers in every possible arithmetic progression. Using his methods, along with recent results from Pomerance [30], we were able to give an explicit lower bound on the number of elliptic Carmichael numbers up to X that are congruent to a modulo M for particular M in our Theorem 3.2.7.

We recently noticed a paper by Kellner and Sondow [17] that gives a new characterization of Carmichael numbers. By specializing one parameter in the new characterization, they define a proper subset of Carmichael numbers they call primary Carmichael numbers. Numerical experiments suggest that a sizable proportion of all Carmichael numbers are primary, but it is not even known whether there are infinitely many of them. It may be possible to prove a characterization of primary Carmichael numbers similar to Korselt's criterion. If this is done, one should be able to modify the results of Chapter 3 to show there are infinitely many primary Carmichael numbers in many arithmetic progressions. Perhaps one can define primary elliptic Carmichael numbers and prove similar results.

At the end of Chapter 3, we gave several results on strong Lucas pseudoprimes and Lucas V-pseudoprimes. As noted in Baillie et al. [3], there are many related open questions. It would be nice to have a formula that bounds the number of D or the number of pairs (P, Q) for which n is a vpsp. Another open question is the asymptotic growth rate for the number of vpsp's up to x. This growth rate probably depends on the algorithm for choosing the parameters P and Q as described in Baillie et al. [3].

Let r be an integer > 1. Our Corollary 3.3.4 shows that there are infinitely elliptic Carmichael numbers $m \equiv 3 \pmod 4$ that are also strong pseudoprimes to base r and strong lpsp(P, Q) and vpsp(P, Q) for $P = 4 \cdot r^k$ and $Q = 8 \cdot r^{2k}$. Perhaps one could prove an analogous corollary with a different (P, Q) pair such that (P, Q) would be chosen by the algorithm described in Baillie et al. [3]. Such a result would prove that there are infinitely many counterexamples to the Baillie-PSW primality test.

Let $\Phi_n(x)$ be the nth cyclotomic polynomial. Many authors have made contributions to characterizing for which pairs (k, n) does one have $\Phi_k(x) \mid \Phi_n(x) - 1$. Some of the more general results, such as those in Bzdęga et al. [9] are not efficiently computable. In Chapter 4, we gave simple necessary and sufficient conditions for which values n does one have $\Phi_8(x) \mid \Phi_n(x) - 1$. We listed several analogous sufficient conditions to find which n satisfy $\Phi_{16}(x) \mid \Phi_n(x) - 1$.

More generally, let k be a power of 2. Then we believe by applying well-known identities, one can build up a complete characterization for when $\Phi_k(x) \mid \Phi_n(x) - 1$ using our Chapter 4 results. It seems feasible that one can obtain similar characterizations for $k = p^e$, where p is an odd prime and $e \geq 1$. Then by using various cyclotomic identities, obtain results for a general k. Such an elementary characterization would be useful in applying these results to primality proving.

REFERENCES

[1] W. R. Alford, A. Granville, and C. Pomerance. “On the difficulty of finding reliable witnesses”. In: *Algorithmic number theory (Ithaca, NY, 1994)*. Vol. **877**. Lecture Notes in Comput. Sci. Springer, Berlin, 1994, pp. 1–16.

[2] W. R. Alford, A. Granville, and C. Pomerance. “There are infinitely many Carmichael numbers”. In: *Ann. of Math. (2)* **139**.3 (1994), pp. 703–722. ISSN: 0003-486X.

[3] R. Baillie, A. Fiori, and S.S. Wagstaff Jr. “Strengthening the Baillie-PSW primality test”. In: *Math. Comp.* 90.330 (2021), pp. 1931–1955. ISSN: 0025-5718. DOI: 10.1090/mcom/3616. URL: https://doi.org/10.1090/mcom/3616.

[4] R. Baillie and S. S. Wagstaff Jr. “Lucas pseudoprimes”. In: *Math. Comp.* **35**.152 (1980), pp. 1391–1417. ISSN: 0025-5718.

[5] R. C. Baker and W. M. Schmidt. “Diophantine problems in variables restricted to the values 0 and 1”. In: *J. Number Theory* **12**.4 (1980), pp. 460–486. ISSN: 0022-314X.

[6] W. D. Banks and C. Pomerance. “On Carmichael numbers in arithmetic progressions”. In: *J. Aust. Math. Soc.* **88**.3 (2010), pp. 313–321. ISSN: 1446-7887.

[7] J. Brillhart, D. H. Lehmer, and J. L. Selfridge. “New primality criteria and factorizations of $2^m \pm 1$”. In: *Math. Comp.* **29** (1975), pp. 620–647. ISSN: 0025-5718.

[8] V. Brun. “La série 1/5+ 1/7+ 1/11+ 1/13+ 1/17+ 1/19+ 1/29+ 1/31+ 1/41+ 1/43+ 1/59+ 1/61+..., où les dénominateurs sont ‘nombres premieres jumeaux’ est convergente ou finie”. In: *Bulletin des sciences mathématiques* 43.100-104 (1919), pp. 124–128.

[9] B. Bzdęga, A. Herrera-Poyatos, and P. Moree. “Cyclotomic polynomials at roots of unity”. In: *Acta Arith.* 184.3 (2018), pp. 215–230. ISSN: 0065-1036. DOI: 10.4064/aa170112-20-12. URL: https://doi.org/10.4064/aa170112-20-12.

[10] C. K. Caldwell. “Unique (period) primes and the factorization of cyclotomic polynomials minus one”. In: *Math. Japon.* 46.1 (1997), pp. 189–195. ISSN: 0025-5513.

[11] A. Ekstrom, C. Pomerance, and D. S. Thakur. “Infinitude of elliptic Carmichael numbers”. In: *J. Aust. Math. Soc.* **92**.1 (2012), pp. 45–60. ISSN: 1446-7887.

[12] P. van Emde Boas and D. Kruyswijk. “A combinatorial problem on finite Abelian groups”. In: *Math. Centrum Amsterdam Afd. Zuivere Wisk.* **1967**.ZW-009 (1967), p. 27. ISSN: 0373-9716.

[13] S. Goldwasser and J. Kilian. "Primality testing using elliptic curves". In: *J. ACM* 46.4 (1999), pp. 450–472. ISSN: 0004-5411. DOI: 10.1145/320211.320213. URL: https://doi.org/10.1145/320211.320213.

[14] D. M. Gordon. "Pseudoprimes on elliptic curves". In: *Théorie des nombres (Quebec, PQ, 1987)*. de Gruyter, Berlin, 1989, pp. 290–305.

[15] I. S. Gradshteyn and I. M. Ryzhik. *Table of integrals, series, and products*. Seventh. Translated from the Russian, Translation edited and with a preface by Alan Jeffrey and Daniel Zwillinger. Elsevier/Academic Press, Amsterdam, 2007, pp. xlviii+1171.

[16] G. H. Hardy and J. E. Littlewood. "Some Problems of 'Partitio Numerorum' (VIII): The Number $\Gamma(k)$ in Waring's Problem". In: *Proc. London Math. Soc. (2)* 28.7 (1928), pp. 518–542. DOI: 10.1112/plms/s2-28.1.518. URL: https://doi.org/10.1112/plms/s2-28.1.518.

[17] B. C. Kellner and J. Sondow. "On Carmichael and polygonal numbers, Bernoulli polynomials, and sums of base-P digits". In: *Integers* 21 (2021), Paper No. A52, 21.

[18] D. Klyve. *Explicit bounds on twin primes and Brun's Constant*. Thesis (Ph.D.)–Dartmouth College. ProQuest LLC, Ann Arbor, MI, 2007, p. 226. ISBN: 978-0549-86813-2. URL: http://gateway.proquest.com/openurl?url_ver=Z39.88-2004&rft_val_fmt=info:ofi/fmt:kev:mtx:dissertation&res_dat=xri:pqdiss&rft_dat=xri:pqdiss:3334102.

[19] R. P. Kurshan and A. M. Odlyzko. "Values of cyclotomic polynomials at roots of unity". In: *Math. Scand.* 49.1 (1981), pp. 15–35. ISSN: 0025-5521. DOI: 10.7146/math.scand.a-11919. URL: https://doi.org/10.7146/math.scand.a-11919.

[20] D. H. Lehmer. "Tests for primality by the converse of Fermat's theorem". In: *Bull. Amer. Math. Soc.* 33.3 (1927), pp. 327–340. ISSN: 0002-9904. DOI: 10.1090/S0002-9904-1927-04368-3. URL: https://doi.org/10.1090/S0002-9904-1927-04368-3.

[21] K. Matomäki. "Carmichael numbers in arithmetic progressions". In: *J. Aust. Math. Soc.* **94**.2 (2013), pp. 268–275. ISSN: 1446-7887.

[22] J. Maynard. "Small gaps between primes". In: *Ann. of Math. (2)* 181.1 (2015), pp. 383–413. DOI: 10.4007/annals.2015.181.1.7. URL: https://doi.org/10.4007/annals.2015.181.1.7.

[23] R. Meshulam. "An uncertainty inequality and zero subsums". In: *Discrete Math.* **84**.2 (1990), pp. 197–200. ISSN: 0012-365X.

[24] L. Monier. “Evaluation and comparison of two efficient probabilistic primality testing algorithms”. In: *Theoret. Comput. Sci.* 12.1 (1980), pp. 97–108. ISSN: 0304-3975. DOI: 10.1016/0304-3975(80)90007-9. URL: https://doi.org/10.1016/0304-3975(80)90007-9.

[25] H. L. Montgomery and R. C. Vaughan. “The large sieve”. In: *Mathematika* **20** (1973), pp. 119–134. ISSN: 0025-5793.

[26] *On-Line Encyclopedia of Integer Sequences*. 2021. URL: https://oeis.org.

[27] D. Platt and T. Trudgian. “Improved bounds on Brun’s constant”. In: *From analysis to visualization*. Vol. 313. Springer Proc. Math. Stat. Springer, Cham, 2020, pp. 395–406. DOI: 10.1007/978-3-030-36568-4_25. URL: https://doi.org/10.1007/978-3-030-36568-4_25.

[28] H. C. Pocklington. “The determination of the prime or composite nature of large numbers by Fermat’s theorem”. In: *Proc. Cambridge Philosophical Society, 1914* 18 (1914), pp. 29–30.

[29] D. H. J. Polymath. “Variants of the Selberg sieve, and bounded intervals containing many primes”. In: *Res. Math. Sci.* 1 (2014), Art. 12, 83. DOI: 10.1186/s40687-014-0012-7. URL: https://doi.org/10.1186/s40687-014-0012-7.

[30] C. Pomerance. “A note on Carmichael numbers in residue classes”. In: *Integers* 21A. Ron Graham Memorial Volume (2021), Paper No. A19, 7.

[31] M. O. Rabin. “Probabilistic algorithm for testing primality”. In: *J. Number Theory* 12.1 (1980), pp. 128–138. ISSN: 0022-314X. DOI: 10.1016/0022-314X(80)90084-0. URL: https://doi.org/10.1016/0022-314X(80)90084-0.

[32] B. Riemann. “Ueber die Anzahl der Primzahlen unter einer gegebenen Grosse”. In: *Ges. Math. Werke und Wissenschaftlicher Nachlaß* 2 (1859), pp. 145–155.

[33] H. Riesel and R. C. Vaughan. “On sums of primes”. In: *Ark. Mat.* 21.1 (1983), pp. 46–74. DOI: 10.1007/BF02384300. URL: https://doi.org/10.1007/BF02384300.

[34] L. Schoenfeld. “Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$. II”. In: *Mathematics of Computation* 30.134 (1976), pp. 337–360.

[35] J. H. Silverman. *The Arithmetic of Elliptic Curves*. Vol. **106**. Graduate Texts in Mathematics. Springer-Verlag, New York, 1986, pp. xii+400. ISBN: 0-387-96203-4.

[36] *Tables of values of pi(x) and of pi2(x)*. 2015. URL: http://sweet.ua.pt/tos/primes.html.

[37] H. Von Koch. “Sur la distribution des nombres premiers”. In: *Acta Mathematica* 24.1 (1901), p. 159.

[38] S.S. Wagstaff Jr. “Sum of reciprocals of Germain primes”. In: *J. Integer Seq.* 24 (2021), Article 21.9.5.

[39] T. Wright. “Infinitely many Carmichael numbers in arithmetic progressions”. In: *Bull. Lond. Math. Soc.* **45**.5 (2013), pp. 943–952. ISSN: 0024-6093.

[40] T. Wright. “There are infinitely many elliptic Carmichael numbers”. In: *Bull. Lond. Math. Soc.* **50**.5 (2018), pp. 791–800. ISSN: 0024-6093.

[41] Y. Zhang. “Bounded gaps between primes”. In: *Ann. of Math. (2)* 179.3 (2014), pp. 1121–1174. DOI: 10.4007/annals.2014.179.3.7. URL: https://doi.org/10.4007/annals.2014.179.3.7.

VITA

Nicholas Egbert is from Greenwood, Indiana. After graduating from Whiteland Community High School in 2011, he attended Indiana University Bloomington where he received a B.S. in Mathematics in 2015. After reading *Nine Algorithms That Changed the Future: The Ingenious Ideas That Drive Today's Computers*, he was inspired to study number theory and cryptography. This led him to Purdue University in 2015 to pursue doctoral work.

While at Purdue, he has had several teaching roles, from all levels of calculus to math for elementary teachers. In summer 2018 he served on a committee to reshape how the Math Resource Room services undergraduate students seeking math help, and in fall 2021 he served as the graduate representative on the computer committee as well as the web committee.