

On fixed points for discrete logarithms

by

Mariana Elaine Campbell

B.A. (University of California, San Diego) 2000

A thesis submitted in partial satisfaction of the
requirements for the degree of
Master of Arts

in

Mathematics

in the

GRADUATE DIVISION
of the
UNIVERSITY of CALIFORNIA at BERKELEY

Committee in charge:

Professor Paul Vojta, Chair
Visiting Assistant Professor Kiran S. Kedlaya
Professor Hendrik W. Lenstra, Jr.
Professor Doug Tygar

Spring 2003

Abstract

On fixed points for discrete logarithms

by

Mariana Elaine Campbell

Master of Arts in Mathematics

University of California at Berkeley

Professor Paul Vojta, Chair

Brizolis asks for which primes p does there exist a primitive root $g \bmod p$ such that $g^h \equiv h \bmod p$. In this thesis, we show that for every prime $p \neq 3$, there exists such a primitive root. An initial computer check shows that Brizolis' question is answered in the affirmative for all primes p such that $3 < p < 6.8 \times 10^8$. We then prove that for $p \neq 3$, there always exists a primitive root g such that $(g, p-1)=1$. This condition is sufficient to imply the existence of a pair (g, h) satisfying the condition in Brizolis' question. The first stage in proving the sufficient condition is to provide an asymptotic formula for $N(p)$, the number of primitive roots g such that $(g, p-1) = 1$. We provide an explicit bound of 8.3×10^{36} , after which $N(p) > 0$. This initial bound is intractable. We use combinatorial sieve techniques to lower this bound substantially to a tractable level (for $p > 7.5 \times 10^{11}$). We then argue that the majority of primes in the remaining range $6.8 \times 10^8 < p < 7.5 \times 10^{11}$ cannot be counterexamples. We use Mathematica and C++ programs to check the outstanding cases. In the final chapter, we discuss the problem of finding all pairs (g, h) that are solutions to Brizolis' question.

Acknowledgements

I first thank Carl Pomerance, who expertly guided me through everything—from research to the writing of the final draft. I am very grateful for his patience with me and am fortunate to have the opportunity to work with him.

I would like to thank Paul Vojta and Kiran Kedlaya at Berkeley for their valuable suggestions and encouragement in completing the final thesis. I thank David Harbater, Antonella Grassi, and Stephen Shatz for teaching excellent courses and for taking good care of me at Penn.

I am grateful to the GRPW Committee at Lucent Technologies for funding my graduate studies through a generous fellowship and for the opportunity to work with the wonderful mathematicians at Bell Labs.

I thank Joshua Holden, Andrew Granville, Olav Richter, and Margaret Robinson for inviting me to speak on this research. I'd like to thank Sasha Barg and Daniel Bleichenbacher for previewing a preliminary version of my first talk on this subject.

Thanks are also due to Francis Zane for his help with various aspects of the programming on this project and Don Coppersmith for his helpful comments related to Lemma 3.3.

I owe thanks to thank Harold Stark, Audrey Terras, and Ron Evans, whose courses at UCSD inspired me to want to learn as much about number theory as I can.

I am indebted to my parents, Kaye and Bruce, who taught me the joy of learning, worked hard to provide many wonderful opportunities, and who have had absolute confidence in me. I also thank Jerry and Victoria, who are the most wonderful in-laws a person could ask for.

Finally, I thank my husband, Aaron, who has shared my happiness and who has been immensely supportive and patient while I was writing this thesis.

Contents

1	Introduction	1
1.1	A Problem of Brizolis	1
2	An Asymptotic Result	4
2.1	Statement and Proof of the Asymptotic Result	4
2.2	What is “sufficiently large”?	8
3	Combinatorial Sieves	10
3.1	The Descent Strategy	10
3.2	The Double Sieve	11
3.3	Double Dyads	12
3.4	Useful Lemmas for Explicit Computation	17
3.5	Numerics with Double Dyads	21
3.6	Double Tetrads in the case $3 p-1$	23
3.7	Numerics with Double Tetrads	26
3.8	Double Dyads for the case $3 \nmid p-1$	28
4	Identifying potential counterexamples	31
4.1	Identifying the remaining intervals	31
4.2	Program Strategy	32
4.3	Statement of Results	34
5	Fixed Points for Discrete Logarithms	35
6	Appendix A: Computer Programs	37
6.1	Mathematica Program I	37
6.2	Mathematica Program II	39
6.3	C++ Program	39
	Bibliography	43

Chapter 1

Introduction

1.1 A Problem of Brizolis

This thesis will explore the use of combinatorial sieve techniques together with standard methods in analytic number theory, such as the Pólya-Vinogradov inequality, to address questions concerning primitive roots mod p . The research in this thesis was carried out during two summer internships at Bell Labs, and is joint work with Carl Pomerance.

The work in this thesis is motivated by a problem of D. Brizolis which appears in Richard Guy's book *Unsolved Problems in Number Theory*. Brizolis asks:

For which primes p does there exist a primitive root $g \bmod p$ and an integer h with $1 \leq h \leq p - 1$ such that $g^h \equiv h \bmod p$?

Recall that for g to be a primitive root mod p means that g generates the cyclic group of units of $\mathbb{Z}/p\mathbb{Z}$. Given one primitive root, g , it is easy to find all $\varphi(p - 1)$ primitive roots mod p by raising g to the $\varphi(p - 1)$ powers relatively prime to $p - 1$. However, the problem of finding a primitive root is a nontrivial computational issue.

Brizolis' question can be rephrased using the language of discrete logarithms as follows:

For which primes does there exist a primitive root $g \bmod p$ such that the discrete logarithm to the base g has a fixed point?

Cryptographers are especially interested in understanding discrete logarithms. Several encryption schemes are based on discrete logarithms because raising a number to a power mod p is easy, but inverting this process is thought to be difficult.

Note that in the statement of Brizolis' question, a restriction on the range of h is necessary because otherwise we could take g to be any primitive root mod p and $h = (p - 1)^2$. Notice also that the result does not hold for $p = 3$, as is easily checked. We conjectured that for all $p \neq 3$ there exists a primitive root $g \bmod p$ such that the discrete logarithm to the base g has a fixed point. A computer check determines that this is the case for primes up to 6.8×10^8 .

Brizolis' problem has an existing history in the literature. Zhang (1995), using the Pólya-Vinogradov inequality, showed that the Brizolis problem holds for all sufficiently large primes p , but he gave no explicit estimate for "sufficiently large." Cobeli and Zaharescu (1999) were able to settle Brizolis' problem asymptotically using somewhat different methods. Using Weil's theorem, they obtained an explicit bound of 10^{50} after which the conjecture holds. Our method, which also involves the Pólya-Vinogradov inequality, yields an explicit bound of 8.3×10^{36} . Holden (2002), has studied variations on Brizolis' problem including the question of two-cycles of the discrete logarithm. It is thought that the methods presented in this thesis may be applied to these problems.

Our bound of 8.3×10^{36} is intractable for finishing the problem by a brute force computer program. The heart of this thesis explores the use of combinatorial methods to lower this bound significantly to a tractable level. I will also explain the programs that we wrote to close the remaining gap between the bound obtained from theory and the "bottom-up" program that checked Brizolis' claim for primes up to 6.8×10^8 .

We first show how Brizolis' question can be reduced to the question of the existence of

a primitive root $g \pmod{p}$, $1 \leq g \leq p-1$, such that $(g, p-1) = 1$.

Lemma 1.1 *Let p be prime. Given a primitive root $h \pmod{p}$, $1 \leq h \leq p-1$, such that $(h, p-1) = 1$, there exists a primitive root $g \pmod{p}$ such that $g^h \equiv h \pmod{p}$.*

Proof: Let $a = h^{-1} \pmod{p-1}$. We can then write

$$h \equiv h^1 \equiv h^{ah} \equiv (h^a)^h \pmod{p}.$$

Let $g = h^a \pmod{p}$. Then g is a primitive root, as $(a, p-1) = 1$. ■

In fact, we can give a characterization of all h such that $g^h \equiv h \pmod{p}$. Let $\text{ord}_p(h)$ denote the order of h in $(\mathbb{Z}/p\mathbb{Z})^*$.

Lemma 1.2 *Let p be prime. Let h be an integer, $1 \leq h \leq p-1$ with $\text{ord}_p(h) = (p-1)/d$. There exists a primitive root g where $g^h \equiv h \pmod{p} \iff (p-1, h) = d$.*

Proof: Fix a primitive root $g_0 \pmod{p}$. Then, the general form of a primitive root mod p is g_0^s for $(s, p-1) = 1$. Let $h = g_0^t$ for $1 \leq t \leq p-1$. Since the order of h is $(p-1)/d$, we have $(t, p-1) = d$. Then there exists a primitive root g such that $g^h \equiv h \pmod{p} \iff$ there exists s with $(s, p-1) = 1$ such that $g_0^{hs} \equiv g_0^t \pmod{p} \iff$ there exists s with $(s, p-1) = 1$ such that $hs \equiv t \pmod{p-1} \iff (p-1, h) = (p-1, t)$. ■

We make the following definition

$$N(p) = \#\{g : 1 \leq g \leq p-1, (g, p-1) = 1, g \text{ is a primitive root}\}.$$

In view of Lemma 1, to attack the Brizolis problem, we now focus on the question:

“For which primes p is $N(p) > 0$?”

Heuristically, one would conjecture that

$$N(p) \approx \frac{\varphi(p-1)^2}{p-1}$$

given that the probability that an integer in the range $1, \dots, p-1$ is relatively prime to $p-1$ is $\varphi(p-1)/p-1$ and there are $\varphi(p-1)$ primitive roots mod p .

In the next chapter, we will prove a precise asymptotic formula for $N(p)$ in which the heuristic conjecture is the main term.

Chapter 2

An Asymptotic Result

2.1 Statement and Proof of the Asymptotic Result

In this chapter, our goal is to prove:

Theorem 2.1

$$N(p) = \frac{\varphi(p-1)^2}{p-1} + O(p^{1/2+\epsilon}).$$

We will then show that this theorem implies that $N(p) > 0$ for p sufficiently large. Hence, Brizolis' problem will be settled for p sufficiently large.

We will first need to find useful expressions for the characteristic functions which select for g satisfying $(g, p-1) = 1$ and for g being a primitive root mod p .

Lemma 2.1 *The characteristic function, ψ_1 , of the set of integers g with $(g, p-1) = 1$ satisfies*

$$\psi_1(g) = \sum_{d|(g, p-1)} \mu(d)$$

where μ is the Möbius function.

Proof: This follows from the well known formula involving the μ function

$$\sum_{d|k} \mu(d) = \begin{cases} 1 & k = 1 \\ 0 & k > 1. \end{cases}$$

■

The expression for the characteristic function for g to be a primitive root mod p involves Dirichlet characters. Let χ be a character of order $p-1$ and modulus p . That is, we have $\chi : (\mathbb{Z}/p\mathbb{Z})^* \rightarrow \mathbb{C}^*$ and there exists a primitive root g_0 modulo p such that $\chi(g_0^a) = \zeta_{p-1}^a$ for every integer a .

Lemma 2.2 *Let χ be a character of order $p-1$ and modulus p , let $m|p-1$, and $g \in (\mathbb{Z}/p\mathbb{Z})^*$.*

Then

$$\frac{1}{m} \sum_{j=1}^m \chi(g)^{j(p-1)/m} = \begin{cases} 1 & g^{(p-1)/m} \equiv 1 \pmod{p} \\ 0 & \text{else.} \end{cases}$$

Proof: We have

$$\frac{1}{m} \sum_{j=1}^m \chi(g)^{j(p-1)/m} = \frac{1}{m} \sum_{j=1}^m \chi(g^{(p-1)/m})^j.$$

Clearly, if $g^{(p-1)/m} \equiv 1 \pmod{p}$, then

$$\frac{1}{m} \sum_{j=1}^m \chi(g)^{j(p-1)/m} = 1.$$

Otherwise, since χ has order $p-1$, which implies that $\chi(g^{(p-1)/m}) \neq 1$, we may rewrite the above expression as

$$\frac{1}{m} \sum_{j=1}^m \chi(g^{(p-1)/m})^j = \frac{\chi(g^{(p-1)/m})(1 - \chi(g^{(p-1)/m})^m)}{m(1 - \chi(g^{(p-1)/m}))}.$$

The numerator of this expression is 0 and the lemma is proved. ■

Lemma 2.3 *The characteristic function, ψ_2 , of the set of integers g , which are primitive roots mod p satisfies*

$$\psi_2(g) = \sum_{m|p-1} \frac{\mu(m)}{m} \sum_{j=1}^m \chi(g)^{j(p-1)/m} = \begin{cases} 1 & g \text{ is a primitive root for } p \\ 0 & \text{else.} \end{cases}$$

Proof: Let $\text{ord}(g \bmod p) = k$. Then $g^{(p-1)/m} \equiv 1 \pmod{p}$ if and only if $m \mid \frac{p-1}{k}$. By Lemma 4, we have

$$\sum_{m \mid p-1} \frac{\mu(m)}{m} \sum_{j=1}^m \chi(g)^{j(p-1)/m} = \sum_{m \mid \frac{p-1}{k}} \mu(m) = \begin{cases} 1 & g \text{ is a primitive root for } p \\ 0 & \text{else.} \end{cases}$$

■

We will use the characteristic functions ψ_1, ψ_2 to obtain a useful expression for $N(p)$. First, we write $N(p)$ as a sum and incorporate the characteristic function for $(g, p-1) = 1$:

$$N(p) = \sum_{\substack{1 \leq g \leq p-1 \\ (g, p-1)=1 \\ g \text{ a prim. rt.}}} 1 = \sum_{\substack{1 \leq g \leq p-1 \\ g \text{ a prim. rt.}}} \sum_{d \mid (g, p-1)} \mu(d).$$

Interchanging the order of summation and incorporating the characteristic function for g to be a primitive root gives

$$\begin{aligned} N(p) &= \sum_{d \mid p-1} \mu(d) \sum_{\substack{1 \leq g \leq p-1 \\ d \mid g \\ g \text{ a prim. rt.}}} 1 \\ &= \sum_{d \mid p-1} \mu(d) \sum_{\substack{g=1 \\ d \mid g}}^{p-1} \sum_{m \mid p-1} \frac{\mu(m)}{m} \sum_{j=1}^m \chi(g)^{j(p-1)/m}. \end{aligned}$$

Let $g = d \cdot h$, use the fact that χ is a homomorphism, and change the order of summation to give

$$N(p) = \sum_{m \mid p-1} \frac{\mu(m)}{m} \sum_{d \mid p-1} \mu(d) \sum_{j=1}^m \chi(d)^{j(p-1)/m} \sum_{h=1}^{(p-1)/d} \chi(h)^{j(p-1)/m}.$$

Let's first look at the contribution from the principal character (i.e., when $j = m$). Using a well known formula for $\varphi(n)/n$, the contribution is

$$\sum_{m \mid p-1} \frac{\mu(m)}{m} \sum_{d \mid p-1} \mu(d) \frac{p-1}{d} = \frac{\varphi(p-1)^2}{p-1}.$$

Recall that this was our expectation for what the size of $N(p)$ should be.

It remains for us to show that the contribution from the nonprincipal characters is small compared with this term. The contribution from the nonprincipal characters, which is our error term, is:

$$|\text{error term}| \leq \sum_{m|p-1} \frac{\mu^2(m)}{m} \sum_{d|p-1} \mu^2(d) \sum_{j=1}^{m-1} \left| \sum_{h=1}^{(p-1)/d} \chi(h)^{j(p-1)/m} \right|.$$

The expression in the last absolute value bars is a sum over consecutive character values of a nonprincipal character mod p . To estimate it, we will use the celebrated Pólya-Vinogradov inequality from analytic number theory (see Davenport, Chapter 23).

Proposition 2.1 (*Pólya-Vinogradov*) *Let χ be a nonprincipal character of modulus q , where q is not necessarily prime. Then*

$$\sum_{n=a}^{a+N} \chi(n) \leq C\sqrt{q} \log q$$

where C is an absolute constant.

Note that the function $\mu^2(m)$ is the characteristic function for the squarefree numbers, namely numbers which are not divisible by a square larger than 1. Thus, using the Pólya-Vinogradov inequality gives

$$\begin{aligned} |\text{error term}| &\leq \sum_{m|p-1} \frac{\mu^2(m)}{m} \sum_{d|p-1} \mu^2(d) \sum_{j=1}^{m-1} C\sqrt{p} \log p \\ &= \sum_{m|p-1} \mu^2(m) \sum_{d|p-1} \mu^2(d) \frac{1}{m} (m-1) C\sqrt{p} \log p \\ &< \tau_0 (p-1)^2 C\sqrt{p} \log p \end{aligned}$$

where τ_0 counts the number of squarefree divisors of $p-1$.

It can be shown that given $\varepsilon > 0$, there is some number c_ε such that $\tau_0(p-1) \leq c_\varepsilon p^\varepsilon$ for all primes p . Therefore, the error term is $O(p^{1/2+\varepsilon})$.

A well known asymptotic lower bound for $\varphi(n)$ is

$$\varphi(n) > \frac{c \cdot n}{\log \log n}$$

for some positive constant c and for n sufficiently large (see Hardy and Wright, Theorem 328).

Using this, we have

$$\frac{\varphi(p-1)^2}{p-1} > \frac{c^2(p-1)}{(\log \log(p-1))^2}$$

for p sufficiently large. We thus have that

$$N(p) \geq \frac{c^2(p-1)}{(\log \log(p-1))^2} + O(p^{1/2+\varepsilon}).$$

This shows that $N(p) > 0$ for p sufficiently large.

2.2 What is “sufficiently large”?

We will now attempt to find exactly how large “sufficiently large” is as a first step towards proving the conjecture for all $p \neq 3$.

We now face 3 immediate difficulties.

- We need an explicit version of the Pólya-Vinogradov inequality. Most of the literature on this celebrated inequality focuses on improvements to the main term, with inexplicit secondary terms.

We will use the following result of Bachman and Rachakonda (2001).

Proposition 2.2 *If χ is a nonprincipal character of modulus p , then*

$$\left| \sum_{h=a}^{a+N} \chi(h) \right| \leq \frac{\sqrt{p} \log p}{3 \log 3} + 6.5\sqrt{p}.$$

- What is c_ε ? We can estimate c_ε as follows:

$$\frac{\tau_0(n)}{n^\varepsilon} = \prod_{p^a \parallel n} \frac{2}{p^{a\varepsilon}} \leq \prod_{p \mid n} \frac{2}{p^\varepsilon} \leq \prod_{p^\varepsilon < 2} \frac{2}{p^\varepsilon}.$$

Taking $\varepsilon = 1/7$, we find that

$$\prod_{p < 2^7} \frac{2}{p^{1/7}} \leq 244.7.$$

Therefore, $\tau_0(n) \leq (244.7)n^{1/7}$, so that

$$\tau_0(p-1) \leq (244.7)p^{1/7}.$$

- What is c in the lower bound for $\varphi(n)$?

We can take c to be $1/2$. Exercise 4.1 of Crandall and Pomerance [3] outlines an argument that for primes $p > 200560490131$, we have $\varphi(p-1) > (p-1)/(2 \log \log p)$.

Using the above tools, we have that for $p > 200560490131$,

$$N(p) \geq \frac{p-1}{4(\log \log(p-1))^2} - (244.7)^2 p^{1/2+2/7} \left(\frac{\log p}{3 \log 3} + 6.5 \right).$$

Thus, we find that

$$N(p) > 0 \text{ for } p > 2 \times 10^{38}.$$

The product of the first 25 primes is slightly greater than 2.3×10^{36} , and the product of the first 26 primes is slightly greater than 2.32×10^{38} . Thus, we have Brizolis for any prime p where $p-1$ is divisible by at least 26 primes. So, assume that $p-1$ has at most 25 distinct prime factors. Replacing the $\tau_0(p-1)^2$ estimate with 2^{50} , we get that $N(p) > 0$ for $p > 8.3 \times 10^{36}$.

We now have an explicit bound beyond which Brizolis' problem is settled, but this bound is by no means a tractable bound for a direct search. We need to check that for each prime, p , there exists a primitive root that is relatively prime to $p-1$. Although it is fairly easy to check the Brizolis property for any one specific prime $p < 8.3 \times 10^{36}$, there are just too many of these primes to be able to check each and every one of them individually. In the next chapter, we will discuss the combinatorial methods we used for lowering this bound substantially.

Chapter 3

Combinatorial Sieves

3.1 The Descent Strategy

In this chapter, we will use combinatorial sieving methods to lower the explicit bound obtained in the previous chapter.

In the main term and error term expression we derived for $N(p)$, the largest contributor to the error term, beyond the factor of \sqrt{p} , is the factor of $\tau_0^2(p-1)$. We replaced the estimate for the τ_0 function by its exact value $\tau_0(p-1) = 2^r$, where r is the number of distinct prime factors of $p-1$. Using the exact value of $\tau_0(p-1)$ would seem to not allow for further improvement. But the expression $\tau_0(p-1)^2$ represents a complete double inclusion-exclusion over the squarefree divisors of $p-1$. We will now use combinatorial sieve techniques to rework the lower bound expression for $N(p)$ so that we reduce the number of squarefree factors of $p-1$ that we need to consider. We prove that $N(p) > 0$ for all primes $p > 8.4 \times 10^{11}$.

3.2 The Double Sieve

Recall that $N(p)$ is the number of primitive roots g modulo p with $1 \leq g \leq p-1$ and $(g, p-1) = 1$. Let R_m denote the number of integers g with $1 \leq g \leq p-1$, $(g, p-1) = 1$ and $g^{(p-1)/m} \equiv 1 \pmod{p}$. Then

$$N(p) = \sum_{m|p-1} \mu(m)R_m.$$

Our expression for $N(p)$ can be thought of as encoding an inclusion-exclusion argument. Stopping after an inclusion in an inclusion-exclusion argument yields an upper bound. Likewise, stopping after an exclusion yields a lower bound. These inequalities are called the *Bonferroni inequalities*. We can apply the Bonferroni inequalities to our expression for $N(p)$. This gives us

$$\sum_{\substack{m|p-1 \\ \omega(m) \leq 2j-1}} \mu(m)R_m \leq N(p) \leq \sum_{\substack{m|p-1 \\ \omega(m) \leq 2j'}} \mu(m)R_m,$$

for any positive integer j , any non-negative integer j' , and where $\omega(m)$ denotes the number of distinct prime factors of m .

We can further rewrite the original expression in a way that allows us to view $N(p)$ as an inclusion-exclusion within an inclusion-exclusion.

Let $R_{m,d}$ be the number of integers g such that $1 \leq g \leq p-1$, $d|g$, and $g^{(p-1)/m} \equiv 1 \pmod{p}$. Then

$$R_m = \sum_{d|p-1} \mu(d)R_{m,d},$$

so that

$$N(p) = \sum_{m|p-1} \mu(m) \sum_{d|p-1} \mu(d)R_{m,d}. \quad (3.1)$$

As above, we can apply the Bonferroni inequalities to the inner sum to get

$$\sum_{\substack{d|p-1 \\ \omega(d) \leq 2l-1}} \mu(d)R_{m,d} \leq R_m \leq \sum_{\substack{d|p-1 \\ \omega(d) \leq 2l'}} \mu(d)R_{m,d}.$$

Using both the upper and lower bounds obtained from the Bonferroni inequalities on the inside inclusion-exclusion and the lower bound for the outer inclusion-exclusion, we get the following lower bound for $N(p)$. We call this expression the *double sieve*:

$$N(p) \geq \sum_{\substack{m|p-1 \\ \mu(m)=1 \\ \omega(m) \leq 2j-1}} \sum_{\substack{d|p-1 \\ \omega(d) \leq 2l-1}} \mu(d)R_{m,d} - \sum_{\substack{m|p-1 \\ \mu(m)=-1 \\ \omega(m) \leq 2j-1}} \sum_{\substack{d|p-1 \\ \omega(d) \leq 2l'}} \mu(d)R_{m,d}. \quad (3.2)$$

In obtaining this new lower bound for $N(p)$, we have reduced the main term. However, in the new expression we only have to consider sums over a subset of the divisors of $p-1$. With judicious choices for j, l, l' , this new expression greatly reduces the contribution to the error term and allows us to continue to reduce the bound for p such that $N(p) > 0$.

3.3 Double Dyads

In this section, we derive an expression for a lower bound of $N(p)$ as a sum over divisors m, d of $p-1$ where both m and d are odd. For m and d odd, define

$$\begin{aligned} D_m &= R_m - R_{2m} \\ D_{m,d} &= R_{m,d} - R_{2m,d} \\ D_{m,d}^* &= D_{m,d} - D_{m,2d}. \end{aligned}$$

We can give a combinatorial interpretation of the above expressions. Let S_m be the set of integers g such that $1 \leq g \leq p-1$, g is a quadratic nonresidue, and $\text{ord}_p(g)|(p-1)/m$. Then D_m counts the number of elements of S_m that are relatively prime to $p-1$. $D_{m,d}$ counts the number of elements of S_m that are divisible by d , and $D_{m,d}^*$ counts the number

of elements of S_m that are odd and divisible by d .

$$\begin{aligned}
D_m &= R_m - R_{2m} \\
&= \sum_{d|p-1} \mu(d)R_{m,d} - \sum_{d|p-1} \mu(d)R_{2m,d} \\
&= \sum_{d|p-1} \mu(d)D_{m,d} \\
&= \sum_{\substack{d|p-1 \\ d \text{ odd}}} \mu(d)D_{m,d} + \mu(2d)D_{m,2d} \\
&= \sum_{\substack{d|p-1 \\ d \text{ odd}}} \mu(d)(D_{m,d} - D_{m,2d}) \\
&= \sum_{\substack{d|p-1 \\ d \text{ odd}}} \mu(d)D_{m,d}^*.
\end{aligned}$$

In order to obtain the lower bound expression using the double sieve and double dyads, we need the following two pairs of inequalities:

$$\sum_{\substack{m|p-1 \\ m \text{ odd} \\ \omega(m) \leq 2j-1}} \mu(m)D_m \leq \sum_{\substack{m|p-1 \\ m \text{ odd}}} \mu(m)D_m \leq \sum_{\substack{m|p-1 \\ m \text{ odd} \\ \omega(m) \leq 2j}} \mu(m)D_m \quad (3.3)$$

and

$$\sum_{\substack{d|p-1 \\ d \text{ odd} \\ \omega(d) \leq 2l-1}} \mu(d)D_{m,d}^* \leq D_m \leq \sum_{\substack{d|p-1 \\ d \text{ odd} \\ \omega(d) \leq 2l'}} \mu(d)D_{m,d}^*. \quad (3.4)$$

We have

$$N(p) = \sum_{m|p-1} \mu(m)R_m = \sum_{\substack{m|p-1 \\ m \text{ odd}}} \mu(m)(R_m - R_{2m}) = \sum_{\substack{m|p-1 \\ m \text{ odd}}} \mu(m)D_m.$$

Thus,

$$N(p) = \sum_{\substack{m|p-1 \\ m \text{ odd}}} \mu(m) \sum_{\substack{d|p-1 \\ d \text{ odd}}} \mu(d)D_{m,d}^*.$$

In analogy with the previous section, we use only the lower bound from (3.3) and both the upper and lower bounds from (3.4). This yields:

$$N(p) \geq \sum_{\substack{m|p-1 \\ \mu(m)=1 \\ \omega(m) \leq 2j-1 \\ m \text{ odd}}} \sum_{\substack{d|p-1 \\ \omega(d) \leq 2l-1 \\ d \text{ odd}}} \mu(d) D_{m,d}^* - \sum_{\substack{m|p-1 \\ \mu(m)=-1 \\ \omega(m) \leq 2j-1 \\ m \text{ odd}}} \sum_{\substack{d|p-1 \\ \omega(d) \leq 2l' \\ d \text{ odd}}} \mu(d) D_{m,d}^*. \quad (3.5)$$

The advantage of this method is that the prime 2 is accounted for exactly. To use this lower bound expression of $N(p)$, we need to use an expression for $D_{m,d}^*$ in terms of characters. We will first express $R_{m,d}$ in terms of characters. Using Lemma 4, we have

$$\begin{aligned} R_{m,d} &= \frac{1}{m} \sum_{\substack{g=1 \\ d|g}}^{p-1} \sum_{s=1}^m \chi(g)^{(p-1)s/m} \\ &= \frac{1}{m} \sum_{h=1}^{(p-1)/d} \sum_{s=1}^m \chi(dh)^{(p-1)s/m} \\ &= \frac{p-1}{dm} + \frac{1}{m} \sum_{h=1}^{(p-1)/d} \sum_{s=1}^{m-1} \chi(dh)^{(p-1)s/m} \\ &= \frac{p-1}{dm} + \frac{1}{m} \sum_{s=1}^{m-1} \sum_{h=1}^{(p-1)/d} \chi(dh)^{(p-1)s/m}. \end{aligned}$$

We can now use this expression for $R_{m,d}$ to find an expression for $D_{m,d}^*$. Since $D_{m,d}^* = R_{m,d} - R_{2m,d} - R_{m,2d} + R_{2m,2d}$, we can substitute the expressions for each of the $R_{j,m,kd}$. We obtain a contribution of

$$\frac{p-1}{dm} - \frac{p-1}{2dm} - \frac{p-1}{2dm} + \frac{p-1}{4dm} = \frac{p-1}{4dm}$$

from the principal character. From the nonprincipal characters, we get a contribution, $C_{m,d}$, to $D_{m,d}^*$ of

$$\begin{aligned} C_{m,d} &= \frac{1}{m} \sum_{s=1}^{m-1} \sum_{h=1}^{(p-1)/d} \chi(dh)^{(p-1)s/m} - \frac{1}{2m} \sum_{s=1}^{2m-1} \sum_{h=1}^{(p-1)/d} \chi(dh)^{(p-1)s/2m} \\ &\quad - \frac{1}{m} \sum_{s=1}^{m-1} \sum_{h=1}^{(p-1)/2d} \chi(2dh)^{(p-1)s/m} + \frac{1}{2m} \sum_{s=1}^{2m-1} \sum_{h=1}^{(p-1)/2d} \chi(2dh)^{(p-1)s/2m}. \end{aligned}$$

The first and third double sums combine to

$$\frac{1}{2m} \sum_{s=1}^{m-1} \left[\sum_{\substack{h=1 \\ h \text{ odd}}}^{(p-1)/d} \chi(dh)^{(p-1)s/m} \right],$$

while the second and fourth double sums combine to

$$\frac{1}{2m} \sum_{\substack{s=1 \\ s \text{ odd}}}^{2m-1} \left[\sum_{\substack{h=1 \\ h \text{ odd}}}^{(p-1)/d} \chi(dh)^{(p-1)s/2m} \right].$$

Thus,

$$\begin{aligned} C_{m,d} &= \frac{1}{2m} \sum_{s=1}^{m-1} \left[\sum_{\substack{h=1 \\ h \text{ odd}}}^{(p-1)/d} \chi(dh)^{(p-1)s/m} \right] - \frac{1}{2m} \sum_{\substack{s=1 \\ s \text{ odd}}}^{2m-1} \left[\sum_{\substack{h=1 \\ h \text{ odd}}}^{(p-1)/d} \chi(dh)^{(p-1)s/2m} \right]. \\ &= \frac{1}{2m} \sum_{s=1}^{m-1} \chi(d)^{(p-1)s/m} \sum_{\substack{h=1 \\ h \text{ odd}}}^{(p-1)/d} \chi(h)^{(p-1)s/m} - \frac{1}{2m} \sum_{\substack{s=1 \\ s \text{ odd}}}^{2m-1} \chi(d)^{(p-1)s/2m} \sum_{\substack{h=1 \\ h \text{ odd}}}^{(p-1)/d} \chi(h)^{(p-1)s/2m}. \end{aligned}$$

So,

$$|C_{m,d}| \leq \frac{1}{2m} \sum_{s=1}^{m-1} \left| \sum_{\substack{h=1 \\ h \text{ odd}}}^{(p-1)/d} \chi(h)^{(p-1)s/m} \right| + \frac{1}{2m} \sum_{\substack{s=1 \\ s \text{ odd}}}^{2m-1} \left| \sum_{\substack{h=1 \\ h \text{ odd}}}^{(p-1)/d} \chi(h)^{(p-1)s/2m} \right|. \quad (3.6)$$

We now have

$$\left| D_{m,d}^* - \frac{p-1}{4dm} \right| \leq |C_{m,d}|.$$

As one can see from what we have derived above, we will need a version of the Pólya-Vinogradov inequality where the character sum in question runs over odd numbers. The following proposition follows from a modification of the argument given in Bachman and Rachakonda and was worked out by Carl Pomerance. The argument is beyond the scope of this thesis, but will appear in a forthcoming joint paper [2]. We will also refer later to a corresponding result where the character sum runs over numbers relatively prime to 6.

Proposition 3.1 *If χ is a nonprincipal character to the modulus p , then for any a, N ,*

$$\left| \sum_{\substack{s=a+1 \\ d \text{ odd}}}^{a+N} \chi(d) \right| \leq \frac{1}{3 \log 3} \sqrt{p} \log p + 3.204 \sqrt{p}.$$

Let the expression on the right hand side of this inequality be called P_2 .

An additional improvement can be made for characters χ such that $\chi(-1) = 1$. Such a character is called an *even character*. Note that any character raised to an even power is an even character. We have

Lemma 3.1 *Suppose that χ is a nonprincipal even character. Then*

$$\left| \sum_{m=1}^n \chi(m) \right| \leq \frac{1}{2} \max_{a, N} \left| \sum_{m=a+1}^{a+N} \chi(m) \right|.$$

Proof: We will use the fact that the sum of consecutive character values over the period is 0. Note that

$$\sum_{m=1}^n \chi(m) = - \sum_{m=n+1}^{p-1} \chi(m) = - \sum_{m=1}^{p-1-n} \chi(-m) = - \sum_{m=1}^{p-1-n} \chi(m).$$

Thus, we can assume that $n \leq (p-1)/2$. Further, from what we have just shown,

$$\sum_{m=1}^n \chi(m) = - \sum_{m=1}^n \chi(m) - \sum_{m=n+1}^{p-1-n} \chi(m).$$

Thus,

$$2 \sum_{m=1}^n \chi(m) = - \sum_{m=n+1}^{p-1-n} \chi(m)$$

and so the result follows. ■

Referring back to display (3.6), we see that since the first character sum in the display is a sum of even characters, we can use Lemma 3.1 and Proposition 3.1 to obtain

$$|C_{m,d}| \leq \frac{1}{2} \cdot \frac{1}{2} P_2 + \frac{1}{2} P_2.$$

Hence, for $m|p-1$, $d|p-1$ both odd, we have that

$$|C_{m,d}| \leq \frac{3}{4} P_2. \tag{3.7}$$

For a positive integer n , let

$$A(j, l, l', n) = \frac{p-1}{4} \left[\sum_{\substack{m|n \\ \omega(m) \leq 2j-1 \\ \mu(m)=1 \\ m \text{ odd}}} \frac{1}{m} \sum_{\substack{d|n \\ \omega(d) \leq 2l-1 \\ d \text{ odd}}} \frac{\mu(d)}{d} - \sum_{\substack{m|n \\ \omega(m) \leq 2j-1 \\ \mu(m)=-1 \\ m \text{ odd}}} \frac{1}{m} \sum_{\substack{d|n \\ \omega(d) \leq 2l'}} \frac{\mu(d)}{d} \right].$$

Note that for a prime p , $A(j, l, l', p-1)$ is the sum of the main terms in the lower bound for $N(p)$ as given in (3.5). From (3.7), we can estimate the contribution from the nonprincipal characters

$$|\text{contribution}| \leq \frac{3}{4} P_2 E_2(j, l, l', r) \quad (3.8)$$

where $r = \omega(p-1)$ and

$$E_2(j, l, l', r) = \sum_{\substack{i=0 \\ i \text{ even}}}^{2j-1} \binom{r-1}{i} \sum_{k=0}^{2l-1} \binom{r-1}{k} + \sum_{\substack{i=1 \\ i \text{ odd}}}^{2j-1} \binom{r-1}{i} \sum_{k=0}^{2l'} \binom{r-1}{k}.$$

Thus from (3.8), we have

$$N(p) \geq A(j, l, l', p-1) - \frac{3}{4} P_2 E_2(j, l, l', r) \quad (3.9)$$

3.4 Useful Lemmas for Explicit Computation

We will now prove some lemmas that will allow us to bound $A(j, l, l', p-1)$ from below. Specifically, we will show that

$$A(j, l, l', p-1) \geq A \left(j, l, l', \prod_{i=1}^r p_i \right) := A_2(j, l, l', r)$$

for $(j, l, l') = (2, 2, 2)$ and $(2, 3, 2)$, where $\omega(p-1) = r$ and p_1, \dots, p_r are the first r primes. We have a similar result in the case of $(j, l, l') = (1, 2, 1)$. We will use symmetric polynomial expressions in q_i to facilitate our computation with $A(j, l, l', \prod q_i)$. We therefore make the following definitions. Let T_1, \dots, T_n be the elementary symmetric polynomials in the variables x_1, \dots, x_n . We will be using the symmetric polynomial expressions with $n = r-1$.

Also, let $T_0 = 1$. Let

$$S_j = \sum_{i=1}^n x_i^j.$$

The T_i can be computed recursively using the S_j as follows

$$T_i = \sum_{j=1}^i \frac{(-1)^{j+1}}{j} S_j T_{i-j}.$$

The recursive formulas given above are known as the *Newton-Girard* formulas. The recursive formula is useful because for a given numerical choice of x_1, \dots, x_n , it is much easier to compute a value of S_i than a value of T_i using the definition. We make the following definitions:

$$U_j = \sum_{i=0}^j (-1)^i T_i, \text{ for } j = 0, 1, \dots, n,$$

$$A_{j,l,l'} = U_{2l-1} \sum_{\substack{i=0 \\ i \text{ even}}}^{2j-1} T_i - U_{2l'} \sum_{\substack{i=0 \\ i \text{ odd}}}^{2j-1} T_i, \text{ for } 1 \leq j, l \leq n/2, 0 \leq l' \leq n/2$$

Notice that $A_{j,l,l'} = A(j, l, l', \prod_{i=1}^r p_i)$ when we set $x_i = 1/p_{i+1}$ for $i = 1, \dots, r$. The prime 2 has been accounted for exactly and so p_1 doesn't appear in these expressions. In this case, we also have

$$U_{2l-1} = \sum_{\substack{d|p_1 \cdots p_r \\ \omega(d) \leq 2l-1 \\ d \text{ odd}}} \frac{\mu(d)}{d}$$

$$\sum_{\substack{i=0 \\ i \text{ even}}}^{2j-1} T_i = \sum_{\substack{m|p_1 \cdots p_r \\ \omega(m) \leq 2j-1 \\ \mu(m)=1 \\ m \text{ odd}}} \frac{1}{m}$$

$$U_{2l'} = \sum_{\substack{d|p_1 \cdots p_r \\ \omega(d) \leq 2l' \\ d \text{ odd}}} \frac{\mu(d)}{d}$$

$$\sum_{\substack{i=0 \\ i \text{ odd}}}^{2j-1} T_i = \sum_{\substack{m|p_1 \cdots p_r \\ \omega(m) \leq 2j-1 \\ \mu(m)=-1 \\ m \text{ odd}}} \frac{1}{m}$$

The following results allow us to conclude that in the cases of interest, $(j, l, l') = (2, 2, 2), (2, 3, 2),$ and $(1, 2, 1)$, our expression for $A_{j,l,l'}$ is minimized for the reciprocals of the first r odd primes. In the case where $3 \nmid p-1$, we can conclude that $A_{1,2,1}$ is minimized for $1/p_3, \dots, 1/p_{r+1}$.

Lemma 3.2 *For $0 < x_1, \dots, x_n < 1$ and $1 \leq j \leq n$ with j odd, the function U_j is decreasing in each variable.*

Proof: Since U_j is a symmetric function, it suffices to prove the result for the variable x_n . For $j \leq n-1$, let $U_j^{(n-1)}$ be the corresponding U -function in the variables x_1, \dots, x_{n-1} . Then

$$\frac{\partial U_j}{\partial x_n} = -U_{j-1}^{(n-1)}.$$

By the Bonferroni inequalities, we have that

$$\prod_{i=1}^{n-1} (1 - x_i) \leq U_{j-1}^{(n-1)}$$

since $j-1$ is even. Hence $U_{j-1}^{(n-1)} > 0$, so that $\frac{\partial U_j}{\partial x_n} < 0$. ■

Lemma 3.3 *At points (x_1, \dots, x_n) where $0 < x_1, \dots, x_n < 1$ and $U_1 > 0$, the function $A_{1,2,1}$ is decreasing in each variable.*

Proof: We have

$$A_{1,2,1} = U_3 - T_1 U_2 = U_2 - T_3 - T_1 U_2 = U_1 U_2 - T_3.$$

Since the nonzero coefficients of the polynomial T_3 are positive and the variables are positive, we have that $-T_3$ is decreasing in each variable. The previous lemma implies that U_1 is decreasing in each variable. By the Bonferroni inequalities, U_2 is positive. Since the product of two positive decreasing functions is also decreasing, the lemma will follow if we show that U_2 is decreasing in each variable. By symmetry it suffices to consider only the variable x_n .

We have

$$\frac{\partial U_2}{\partial x_n} = -1 + \sum_{i=1}^{n-1} x_i < -1 + T_1 = -U_1 < 0,$$

so we are done. ■

Lemma 3.4 *At points (x_1, \dots, x_n) where $0 < x_1, \dots, x_n < 1$ and $U_3 > 0$, the functions $A_{2,2,2}$ and $A_{2,3,2}$ are decreasing in each variable.*

Proof: We have

$$A_{2,2,2} = (1 + T_2)U_3 - (T_1 + T_3)U_4 = (1 + T_2)U_3 - (T_1 + T_3)(U_3 + T_4) = U_3^2 - (T_1 + T_3)T_4.$$

By Lemma 3.2 and the assumption that $U_3 > 0$, we have that U_3^2 is decreasing in each variable. As in the previous lemma, we easily see that $-(T_1 + T_3)T_4$ is decreasing in each variable. Thus $A_{2,2,2}$ is decreasing in each variable.

We have

$$A_{2,3,2} = (1 + T_2)U_5 - (T_1 + T_3)U_4 = (1 + T_2)(U_4 - T_5) - (T_1 + T_3)U_4 = U_3U_4 - (1 + T_2)T_5.$$

The proof will follow as before if we show that U_4 is positive and decreasing in each variable. It is positive from the assumptions and the Bonferroni inequalities. So, it is sufficient to show that U_4 is decreasing in the variable x_n . We have

$$\frac{\partial U_4}{\partial x_n} = -U_3^{(n-1)} = -U_3 - x_n U_2^{(n-1)}.$$

As $U_2^{(n-1)}$ is positive from the Bonferroni inequalities, and U_3, x_n are positive by assumption, it follows that the partial derivative is negative, thus completing the proof. ■

We remark that it follows that if $0 < a_1, \dots, a_n < 1$ and $U_3(a_1, \dots, a_n) > 0$, then for any point (x_1, \dots, x_n) with $0 < x_i \leq a_i$ for $i = 1, \dots, n$, we have

$$A_{2,2,2}(x_1, \dots, x_n) \geq A_{2,2,2}(a_1, \dots, a_n) \quad \text{and} \quad A_{2,3,2}(x_1, \dots, x_n) \geq A_{2,3,2}(a_1, \dots, a_n).$$

A similar remark pertains to $A_{1,2,1}$.

3.5 Numerics with Double Dyads

From the previous section, we have the following corollary to Lemma 3.4.

Corollary 3.1 *If $U_3(1/p_2, \dots, 1/p_r) > 0$, then for any (x_1, \dots, x_{r-1}) with $0 < x_{i-1} \leq 1/p_i$ for $i = 2, \dots, r$ we have*

$$A_{2,2,2}(x_1, \dots, x_{r-1}) \geq A_{2,2,2}(1/p_2, \dots, 1/p_r)$$

and

$$A_{2,3,2}(x_1, \dots, x_{r-1}) \geq A_{2,3,2}(1/p_2, \dots, 1/p_r).$$

Using (3.9), we have that if

$$\frac{p-1}{4} A_{j,l,l'}(1/p_2, \dots, 1/p_r) > \frac{3}{4} \sqrt{p} E_2(j, l, l', r) \left\{ \frac{\log p}{3 \log 3} + 3.204 \right\},$$

then $N(p) > 0$ for any prime p with $\omega(p-1) = r$. The above inequality is equivalent to

$$p > \sqrt{p} \frac{3E_2(j, l, l', r)}{A_{j,l,l'}(1/p_2, \dots, 1/p_r)} \left\{ \frac{\log p}{3 \log 3} + 3.204 \right\} + 1.$$

We use instead a slightly weaker version of this inequality that is easier to compute with. The weaker inequality is based on the fact that $p > (s+1)^2 \Rightarrow p \geq s\sqrt{p} + 1$ where

$$s = \frac{3E_2(j, l, l', r) P_2}{A_{j,l,l'}(1/p_2, \dots, 1/p_r)} \left\{ \frac{\log p}{3 \log 3} + 3.204 \right\}.$$

Theorem 3.1 *If p is a prime with $\omega(p-1) = r$, $(j, l, l') = (2, 2, 2)$ or $(2, 3, 2)$, and we have*

$$p \geq \left(\frac{3E_2(j, l, l', r)}{A_{j,l,l'}(1/p_2, \dots, 1/p_r)} \left\{ \frac{\log p}{3 \log 3} + 3.204 \right\} + 1 \right)^2$$

at $p = p_0 > 7$, then $N(p) > 0$ for all $p \geq p_0$.

Proof: One can prove this using the following lemma derived from elementary calculus. ■

Lemma 3.5 *Let a, b be any real numbers. If at $p = p_0$ we have $p > 2a^2$, $p > 2a(a \log p + b)$, and $p > (a \log p + b)^2$, then $p > (a \log p + b)^2$ for all $p \geq p_0$.*

Proof: It suffices to show that $p - (a \log p + b)^2$ is an increasing function in the variable p . Taking the first derivative, we see that this happens iff $p > 2a(a \log p + b)$. By hypothesis, this condition holds at $p = p_0$. We want to show that this condition holds for all $p \geq p_0$. We again differentiate in order to show that the difference is increasing. This translates into the condition that $p > 2a^2$. Again, by assumption this condition holds at $p = p_0$. ■

All the conditions in the lemma are satisfied because $a > 0, b \geq 0$, and $\log p > 2$ in our application. The theorem implies that it suffices to verify the inequality for the smallest p in the range of interest. Hence, we have derived a lower bound after which $N(p) > 0$, using the double sieve with double dyads expression.

In the following table, we summarize the calculation of $A_{j,l,l'}(1/p_2, \dots, 1/p_r)$ and $E_2(j, l, l', r)$. For a given r , we choose the smallest value of j, l, l' such that $A_{j,l,l'}(1/p_2, \dots, 1/p_r)$ is positive. To compute the values of $A_{j,l,l'}$ given in the table, we use the recursive formulas for the elementary symmetric functions given in section 3.4.

r	$U_3(1/p_2, \dots, 1/p_r)$	$A_{j,l,l'}(1/p_2, \dots, 1/p_r)$	$E_2(j, l, l', r)$	(j, l, l')
25	.1910	.0309	41884683	(2, 3, 2)
24	.1956	.0336	30876190	(2, 3, 2)
23	.2005	.0365	22451034	(2, 3, 2)
22	.2058	.0394	16082053	(2, 3, 2)
21	.2112	.0425	11332060	(2, 3, 2)
20	.2171	.0458	7841776	(2, 3, 2)
19	.2231	.0492	5318896	(2, 3, 2)
18	.2295	.0527	3528232	(2, 3, 2)
17	.2363	.0068	1534129	(2, 2, 2)
16	.2434	.0151	973326	(2, 2, 2)
15	.2512	.0240	599278	(2, 2, 2)

For each r , we find upper and lower bounds for regions where we need to check the Brizolis conjecture.

Definition 3.1 Let p_1, \dots, p_r be the first r primes. Let $(j, l, l') = (2, 2, 2)$ or $(2, 3, 2)$. Then

$$L(r) = 1 + \prod_{i=1}^r p_i$$

and

$$U_{\text{dyad}}(r) = \left(\frac{3E_2(j, l, l', r)}{A_{j, l, l'}(1/p_2, \dots, 1/p_r)} \left\{ \frac{\log p}{3 \log 3} + 3.204 \right\} + 1 \right)^2.$$

Thus, for $p > U_{\text{dyad}}(r)$ and $\omega(p-1) = r$, we have $N(p) > 0$.

Theorem 3.2 *If $L(r) > U_{\text{dyad}}(r)$, then $N(p) > 0$ for every prime p with $\omega(p-1) = r$.*

Using the sieve machinery, we were able to show that for larger r , the largest number with r prime factors that could possibly be a counterexample to Brizolis was smaller than the product of the first r primes. Thus, from our theory we could conclude that no counterexamples with r prime factors could occur. We could then assume that $p-1$ must have $r-1$ prime factors and so hope to repeat the argument. Using the method of double dyads, we are able to conclude that a counterexample to the Brizolis conjecture would have 15 or fewer prime factors. To compute $U_{\text{dyad}}(r)$, we use only p_2, \dots, p_r because the prime 2 is accounted for explicitly.

r	$L(r)$	$U_{\text{dyad}}(r)$	(j, l, l')
25	2.3055×10^{36}	1.4764×10^{22}	(2, 3, 2)
24	2.3768×10^{34}	6.1975×10^{21}	(2, 3, 2)
23	2.6706×10^{32}	2.5227×10^{21}	(2, 3, 2)
22	3.2176×10^{30}	9.9973×10^{20}	(2, 3, 2)
21	4.0729×10^{28}	3.8291×10^{20}	(2, 3, 2)
20	5.5794×10^{26}	1.4130×10^{20}	(2, 3, 2)
19	7.8583×10^{24}	5.0301×10^{19}	(2, 3, 2)
18	1.1728×10^{23}	1.7078×10^{19}	(2, 2, 2)
17	1.9227×10^{21}	1.6895×10^{20}	(2, 2, 2)
16	3.2589×10^{19}	1.2096×10^{19}	(2, 2, 2)
15	6.1489×10^{17}	1.5815×10^{18}	(2, 2, 2)

So, for $r = 15$, we still need to consider the range $6.1489 \times 10^{17} \leq p \leq 1.58156 \times 10^{18}$.

In summary, we have now proved that $N(p) > 0$ for all $p > 1.58156 \times 10^{18}$.

3.6 Double Tetrads in the case $3|p-1$

We have used the method of double dyads until it gave us an upper bound for the largest number with r prime factors that needed to be checked that was greater than the lower

bound for the largest number with r prime factors that needed to be checked. We can continue with the reasoning we used in creating the double dyad method by considering the case when $3|p-1$ separately from the case when $3 \nmid p-1$. When $3|p-1$, we can introduce “double tetrads” in analogy with our expression for double dyads. In our expression for $N(p)$, we will now sum over m and d relatively prime to 6. For $(m,6) = (d,6) = 1$, we define

$$\begin{aligned} T_m &= R_m - R_{2m} - R_{3m} + R_{6m} \\ T_{m,d} &= R_{m,d} - R_{2m,d} - R_{3m,d} + R_{6m,d} \\ T_{m,d}^* &= T_{m,d} - T_{m,2d} - T_{m,3d} + T_{m,6d}. \end{aligned}$$

As with the case of double dyads, we can give a combinatorial interpretation of these expressions. Let S_m be the set of integers g such that $1 \leq g \leq p-1$, g is both a quadratic and cubic nonresidue, and $\text{ord}_p(g)|(p-1)/m$. Then T_m counts the number of elements of S relatively prime to $p-1$. $T_{m,d}$ counts the number of elements of S_m that are divisible by d , and $T_{m,d}^*$ counts the number of elements of S_m that are divisible by d , but not divisible by 2 or 3. Then, we have

$$\begin{aligned} N(p) &= \sum_{\substack{m|p-1 \\ (m,6)=1}} \mu(m)T_m \\ &= \sum_{\substack{m|p-1 \\ (m,6)=1}} \mu(m) \sum_{\substack{d|p-1 \\ d \text{ odd}}} \mu(d)(T_{m,d} - T_{m,2d}) \\ &= \sum_{\substack{m|p-1 \\ (m,6)=1}} \mu(m) \sum_{\substack{d|p-1 \\ (d,6)=1}} T_{m,d}^*. \end{aligned}$$

In an analogous way to how we derived a lower bound expression using double dyads and the double sieve, we obtain

$$N(p) \geq \sum_{\substack{m|p-1 \\ \omega(m) \leq 2j-1 \\ (m,6)=1 \\ \mu(m)=1}} \sum_{\substack{d|p-1 \\ \omega(d) \leq 2l-1 \\ (d,6)=1}} \mu(d)T_{m,d}^* - \sum_{\substack{m|p-1 \\ \omega(m) \leq 2j-1 \\ (m,6)=1 \\ \mu(m)=-1}} \sum_{\substack{d|p-1 \\ \omega(d) \leq 2l' \\ (d,6)=1}} \mu(d)T_{m,d}^* \quad (3.10)$$

We obtain a contribution of

$$\frac{p-1}{3md} - \frac{p-1}{2 \cdot 3md} - \frac{p-1}{3 \cdot 3md} + \frac{p-1}{3 \cdot 6md} = \frac{p-1}{9md}$$

from the principal character when we look at T_m in terms of the character expressions for R_m . Let $C_{m,d}$ be the contribution from the nonprincipal characters. Then,

$$\begin{aligned} C_{m,d} &= \frac{1}{3m} \sum_{j=1}^{m-1} \left[\sum_{\substack{h=1 \\ (h,6)=1}}^{(p-1)/d} \chi(dh)^{j(p-1)/m} \right] \\ &- \frac{1}{3m} \sum_{\substack{j=1 \\ j \text{ odd}}}^{2m-1} \left[\sum_{\substack{h=1 \\ (h,6)=1}}^{(p-1)/d} \chi(dh)^{j(p-1)/2m} \right] \\ &- \frac{1}{6m} \sum_{\substack{j=1 \\ 3 \nmid j}}^{3m-1} \left[\sum_{\substack{h=1 \\ (h,6)=1}}^{(p-1)/d} \chi(dh)^{j(p-1)/3m} \right] \\ &+ \frac{1}{6m} \sum_{\substack{j=1 \\ (j,6)=1}}^{6m-1} \left[\sum_{\substack{h=1 \\ (h,6)=1}}^{(p-1)/d} \chi(dh)^{j(p-1)/6m} \right]. \end{aligned}$$

Within the double tetrad framework, we will need a version of the Pólya-Vinogradov inequality where the character sum runs over d such that $(d, 6) = 1$. We will use the following proposition

Proposition 3.2 *If χ is a nonprincipal character to the modulus p , then for any a, N ,*

$$\left| \sum_{\substack{s=a+1 \\ (d,6)=1}}^{a+N} \chi(d) \right| \leq \frac{\sqrt{2}}{3 \log 3} \sqrt{p} \log p + 4.786 \sqrt{p}.$$

We call the right side of this inequality P_6 .

We have that

$$\left| T_{m,d}^* - \frac{p-1}{9md} \right| \leq |C_{m,d}|$$

and we find that

$$\begin{aligned} |C_{m,d}| &\leq \frac{1}{3}P_6 + \frac{1}{3}P_6 + \frac{1}{3}P_6 + \frac{1}{3}P_6 \\ &= \frac{4}{3}P_6. \end{aligned}$$

Noticing that the first and third character sums above are sums of even characters, we can use apply Lemma 6 to find that $|C_{m,d}| \leq P_6$. We will now make some useful definitions that are analogous to those in the double dyad case:

$$B(j, l, l', p-1) = \frac{p-1}{9} \sum_{\substack{m|p-1 \\ \omega(m) \leq 2j-1 \\ \mu(m)=1 \\ (m,6)=1}} \frac{1}{m} \sum_{\substack{d|p-1 \\ \omega(d) \leq 2l-1 \\ (d,6)=1}} \frac{\mu(d)}{d} - \sum_{\substack{m|p-1 \\ \omega(m) \leq 2j-1 \\ \mu(m)=-1 \\ (m,6)=1}} \frac{1}{m} \sum_{\substack{d|p-1 \\ \omega(d) \leq 2l' \\ (d,6)=1}} \frac{\mu(d)}{d}.$$

We also have

$$B_6(j, l, l', r) = \sum_{\substack{m|p_1 \cdots p_r \\ \omega(m) \leq 2j-1 \\ \mu(m)=1 \\ (m,6)=1}} \frac{1}{m} \sum_{\substack{d|p_1 \cdots p_r \\ \omega(d) \leq 2l-1 \\ (d,6)=1}} \frac{\mu(d)}{d} - \sum_{\substack{m|p_1 \cdots p_r \\ \omega(m) \leq 2j-1 \\ \mu(m)=-1 \\ (m,6)=1}} \frac{1}{m} \sum_{\substack{d|p_1 \cdots p_r \\ \omega(d) \leq 2l' \\ (d,6)=1}} \frac{\mu(d)}{d}$$

so that

$$B_6(j, l, l', r) = A_{j,l,l'}(1/p_3, \dots, 1/p_r).$$

As before, we define

$$E_6(j, l, l', r) = \sum_{\substack{i=0 \\ i \text{ even}}}^{2j-1} \binom{r-2}{i} \sum_{k=0}^{2l-1} \binom{r-2}{k} + \sum_{\substack{i=1 \\ i \text{ odd}}}^{2j-1} \binom{r-2}{i} \sum_{k=0}^{2l'} \binom{r-2}{k}.$$

Here we have also taken into consideration the improvement that can be made when χ is an even character.

3.7 Numerics with Double Tetrads

As a corollary to Lemma 3.3 we have the following result

Corollary 3.2 *If $U_1(1/p_3, \dots, 1/p_r) > 0$, then for any (x_1, \dots, x_{r-2}) with $0 < x_{i-2} \leq 1/p_i$ for $i = 3, \dots, r$ we have*

$$A_{1,2,1}(x_1, \dots, x_{r-2}) \geq A_{1,2,1}(1/p_3, \dots, 1/p_r).$$

Using (3.10), we have that if

$$\frac{p-1}{9} A_{1,2,1}(1/p_3, \dots, 1/p_r) > \sqrt{p} E_6(1, 2, 1, r) \left\{ \frac{\sqrt{2} \log p}{3 \log 3} + 4.786 \right\}.$$

then $N(p) > 0$ for any prime p with $\omega(p-1) = r$. We then have the equivalent inequality:

$$p > \frac{\sqrt{p} E_6(1, 2, 1, r)}{A_{1,2,1}(1/p_3, \dots, 1/p_r)} \left\{ \frac{3\sqrt{2} \log p}{\log 3} + 9 \cdot 4.786 \right\} + 1. \quad (3.11)$$

We use the following weaker inequality:

Theorem 3.3 *If p is prime with $\omega(p-1) = r$, $3|p-1$, and*

$$p > \left(1 + \frac{E_6(j, l, l', r)}{A_{1,2,1}(1/p_3, \dots, 1/p_r)} \left(\frac{3\sqrt{2} \log p}{\log 3} + 4.786 \cdot 9 \right) \right)^2$$

at p_0 , then $N(p) > 0$ for all $p \geq p_0$.

The following table summarizes the calculation of $A_{1,2,1}(1/p_3, \dots, 1/p_r)$ and $E_6(1, 2, 1, r)$ as described in the previous section. When computing these quantities, we use p_3, \dots, p_r because the primes 2 and 3 are accounted for exactly in the double tetrad formulation.

r	$U_1(1/p_3, \dots, 1/p_r)$	$A_{1,2,1}(1/p_3, \dots, 1/p_r)$	$E_6(1, 2, 1, r)$
15	.1717	.0180	1574
14	.1930	.0348	1247
13	.2163	.0531	969
12	.2407	.0722	736
11	.2677	.0934	544

In the case where $3|p-1$ we can use the double tetrad theory to further eliminate intervals that need to be considered for Brizolis counterexamples. As before, we have

Definition 3.2 *Let p_1, \dots, p_r be the first r primes. Then*

$$L(r) = 1 + \prod_{i=1}^r p_i$$

and

$$U_{\text{tetrad}}(r) = \left(1 + \frac{E_6(1, 2, 1, r)}{A_{1,2,1}(1/p_3, \dots, 1/p_r)} \left(\frac{3\sqrt{2} \log p}{\log 3} + 4.786 \cdot 9 \right) \right)^2.$$

Thus, for $p > U_{\text{tetrad}}(r)$ and $\omega(p-1) = r$, we have $N(p) > 0$.

Theorem 3.4 *If $L(r) > U_{\text{tetrad}}(r)$, then $N(p) > 0$ for every prime p with $3 \nmid p-1$ and $\omega(p-1) = r$.*

r	$L(r)$	$U_{\text{tetrad}}(r)$
15	6.1480×10^{17}	3.5568×10^{14}
14	1.3082×10^{16}	5.1718×10^{13}
13	3.0425×10^{14}	1.1535×10^{13}
12	7.4207×10^{12}	3.0617×10^{12}
11	2.0056×10^{11}	8.4059×10^{11}

For $r \leq 11$, we found that the upper bound for $r = 11$ is larger than the product of the first 11 primes. We have now shown that in the case $3 \nmid p-1$, $N(p) > 0$ for all $p > 8.40598 \times 10^{11}$. On the interval $2.0056 \times 10^{11} \leq p \leq 8.40598 \times 10^{11}$, we must still show that $N(p) > 0$ in order to assume that $p-1$ has less than 11 prime factors.

3.8 Double Dyads for the case $3 \nmid p-1$

Let $A_2^{(3)}(j, l, l', r)$ denote $A_2(j, l, l', r)$ where we replace the product of the first r primes with the product of the first r primes not equal to 3. We then have that

$$A_2^{(3)}(j, l, l', r) = A_{j,l,l'}(1/p_3, \dots, 1/p_{r+1}).$$

We have a corollary to Lemma 3.3 for the case of double dyads where $3 \nmid p-1$.

Corollary 3.3 *If $U_1(1/p_3, \dots, 1/p_{r+1}) > 0$, then for any (x_1, \dots, x_{r-1}) with $0 < x_{i-1} \leq 1/p_i$ for $i = 3, \dots, r+1$ we have*

$$A_{1,2,1}(x_1, \dots, x_{r-1}) \geq A_{1,2,1}(1/p_3, \dots, 1/p_{r+1}).$$

r	$U_1(1/p_3, \dots, 1/p_{r+1})$	$A_{1,2,1}(1/p_3, \dots, 1/p_{r+1})$	$E_2(1, 2, 1, r)$
15	.1529	.0030	1954
14	.1717	.0180	1574
13	.1930	.0348	1247
12	.2163	.0531	969
11	.2407	.0722	736
10	.2676	.0934	544

When computing $A_{1,2,1}$, we use p_3, \dots, p_{r+1} in our calculations because $p - 1$ has r prime factors, prime 2 is accounted for exactly, and 3 is not a factor of $p - 1$. For the case of $3 \nmid p - 1$ we can use our previous expression for double dyads assuming that $3 \nmid p - 1$ to obtain upper and lower bounds for the interval that we would need to check. We then get the following corresponding inequality for p in the case that $3 \nmid p - 1$:

Theorem 3.5 *If p is a prime with $\omega(p - 1) = r$ and $3 \nmid p - 1$, we have*

$$p > \left(\frac{3E_2(1, 2, 1, r)}{A_{1,2,1}(1/p_3, \dots, 1/p_{r+1})} \left\{ \frac{\log p}{3 \log 3} + 3.204 \right\} + 1 \right)^2$$

at p_0 , then $N(p) > 0$ for all $p \geq p_0$.

Again, we define

Definition 3.3 *Let p_1, \dots, p_r be the first r primes. Then*

$$L(r) = 1 + \prod_{i=1}^r p_i$$

and

$$U_{\text{dyad}}^{(3)}(r) = \left(\frac{3E_2(1, 2, 1, r)}{A_{1,2,1}(1/p_3, \dots, 1/p_{r+1})} \left\{ \frac{\log p}{3 \log 3} + 3.204 \right\} + 1 \right)^2.$$

Theorem 3.6 *If $L(r) > U_{\text{dyad}}^{(3)}$, then $N(p) > 0$ for every prime p such that $\omega(p - 1) = r$ and $3 \nmid p - 1$.*

We compute the upper and lower bounds for p that need to be checked such that $p - 1$ has r prime factors and $3 \nmid p - 1$.

r	$L(r)$	$U_{\text{dyad}}^{(3)}(r)$
15	6.1489×10^{17}	1.0522×10^{15}
14	1.3082×10^{16}	1.9344×10^{13}
13	3.0425×10^{14}	2.4041×10^{12}
12	7.4207×10^{12}	5.3043×10^{11}
11	2.0056×10^{11}	1.3874×10^{11}
10	6.4689×10^9	3.7568×10^{10}

We have now shown that, in the case $3 \nmid p - 1$, $N(p) > 0$ for $p > 3.7568 \times 10^{10}$. Recall that in the case where $3|p - 1$, we had shown $N(p) > 0$ for $p > 8.40598 \times 10^{11}$. We have now

that $N(p) > 0$ for $p > 8.40598 \times 10^{11}$ with no restriction on p .

In the next chapter, we discuss how to identify the potential counterexamples in the remaining intervals and verify the conjecture in the cases that remain.

Chapter 4

Identifying potential counterexamples

In the previous chapter we used sieve machinery combined with the ideas involved in double dyads and double tetrads in order to lower the bound beyond which the conjecture holds to a tractable level for a computer program. However, the remaining gap ($6.8 \times 10^8 \leq p \leq 8.4 \times 10^{11}$) is actually still not small enough to be convenient for an exhaustive case checking program. We will make arguments for why most numbers in this range could not be a counterexample to our conjecture. Then, we will describe a program that identifies the remaining primes which can be checked individually.

4.1 Identifying the remaining intervals

The numbers, $p-1$, in the remaining range have at most 11 prime factors. We use the double dyad and double tetrad expressions for $N(p)$ developed in the previous chapter to compute upper and lower bounds assuming $r = 6, 7, 8, 9, 10, 11$, respectively. Since the upper bound for a counterexample to Brizolis with at most 6 prime factors is 6.8×10^8 , we know that no counterexamples with at most 6 prime factors can occur since our original program checked up to this point. Recall that in the previous chapter, we were able to conclude that no counterexamples with, say 15 prime factors could occur, because the lower bound for p with $r = 15$ in our expression was smaller than the product of the first 15 primes. This allowed

us to use $r = 14$ and repeat this process. However, when we now compute this upper bound with $r \leq 11$, an interval remains to be checked. From the double tetrad framework (recall that this carries with it the assumption that $3 \mid p - 1$), we have the following table where the upper bound is computed as described above and the lower bound is the product of the first r primes. When computing the following tables, we used the more precise inequality (3.11) rather than the inequality in Theorem 3.3. Notice that for $r = 11$, the more precise inequality (3.11) gives 7.5×10^{11} rather than 8.4×10^{11} .

r	$U_1(1/p_3, \dots, 1/p_r)$	$L(r)$	$U_{\text{tetrad}}(r)$
11	.2676	2.0056×10^{11}	7.5×10^{11}
10	.2998	6.4686×10^9	2.3×10^{11}
9	.3343	2.2309×10^8	6.5×10^{10}
8	.3778	9.6996×10^6	1.7×10^{10}
7	.4304	510510	3.7×10^9
6	.4893	30030	6.8×10^8

Since our initial program checked exhaustively up to 6.8×10^8 , the “lower bounds” for $r = 7, 8, 9$ in the right column of the table may all be replaced by 6.8×10^8 .

From the double dyad framework assuming that $3 \nmid p - 1$, we have the following table. Recall using double dyads with $3 \nmid p - 1$ the first place that our upper bound was larger than our lower bound (and hence left an interval to be checked) was when $r = 10$.

r	$U_1(1/p_3, \dots, 1/p_{r+1})$	$L(r)$	$U_{\text{dyad}}^{(3)}(r)$
10	.2676	6.4686×10^9	3.5×10^{10}
9	.2998	2.2309×10^8	1.2×10^{10}
8	.3343	9.6996×10^6	3.0×10^9
7	.3778	510510	7.5×10^8
6	.4304	30030	9×10^7

Notice that since our initial program checked up to 6.8×10^8 , we do not need to check numbers with 6 prime factors.

4.2 Program Strategy

Finishing the problem via programming came in two stages. We first wrote a C++ program that created files with the potential counterexamples to the conjecture. Then, we wrote a

Mathematica program which verified the conjecture for these numbers. The numbers that needed to be checked are:

Range	Report p such that $p - 1$ has
$2.3 \times 10^{11} \leq p \leq 7.5 \times 10^{11}$	11 factors and $30 p - 1$
$2.0 \times 10^{11} \leq p \leq 2.3 \times 10^{11}$	11 factors and $30 p - 1$ 10 factors and $30 p - 1$
$6.5 \times 10^{10} \leq p \leq 2.0 \times 10^{11}$	10 factors and $30 p - 1$
$3.5 \times 10^{10} \leq p \leq 6.5 \times 10^{10}$	10 factors and $30 p - 1$ 9 factors and $30 p - 1$
$1.7 \times 10^{10} \leq p \leq 3.5 \times 10^{10}$	10 factors 9 factors
$6.46 \times 10^9 \leq p \leq 1.7 \times 10^{10}$	10 factors 9 factors 8 factors
$3.7 \times 10^9 \leq p \leq 6.46 \times 10^9$	9 factors 8 factors
$6.8 \times 10^8 \leq p \leq 3.7 \times 10^9$	9 factors 8 factors 7 factors

In the above table, “factors” is taken to mean “distinct prime factors.” The reason why we need to report only those numbers where $30|p - 1$ in the first four intervals in the table is that our calculation using double tetrads showed that for $r = 10$ and $3 \nmid p - 1$ the upper bound is 3.5×10^{10} . Using double tetrads and assuming instead that $5 \nmid p - 1$ gives us a bound of 1.41×10^{10} . Therefore, we know that primes p that are potential counterexamples above 3.5×10^{10} all have $30|p - 1$.

For each r , the number of primes for which the conjecture needed to be checked by a program is summarized in the following table

r	Number of Candidate Primes
11	43
10	24,715
9	689,184
8	793,630
7	1,728,679
Total	3,236,251

Although the original interval that remained to be checked was $6.8 \times 10^8 \leq p \leq 7.5 \times 10^{11}$, we only needed to check the conjecture for 3,236,251 individual primes. Using the PrimePi

function in Mathematica, we calculate that the total number of primes in the interval $6.8 \times 10^8 \leq p \leq 7.5 \times 10^{11}$ is 28,479,698,207.

4.3 Statement of Results

We now have

Theorem 4.1 *For all primes $p \neq 3$ there exists a primitive root g modulo p such that $(g, p-1) = 1$.*

Consequently, we have also settled the problem of Brizolis for all primes $p \neq 3$.

Corollary 4.1 *For all primes $p \neq 3$, there exists a primitive root g modulo p and an integer h with $1 \leq h \leq p-1$ such that*

$$g^h \equiv h \pmod{p}.$$

The theorem above produces some of the primitive roots g that will satisfy the congruence in Brizolis' problem. In the next chapter, we will discuss the problem of determining all primitive roots which satisfy this congruence.

Chapter 5

Fixed Points for Discrete Logarithms

In Lemma 1.2 we showed that if $1 \leq h \leq p-1$ and h has order $(p-1)/d$ in $(\mathbb{Z}/p\mathbb{Z})^*$, then there exists a primitive root $g \pmod{p}$ such that $g^h \equiv h \pmod{p} \iff (p-1, h) = d$. In analogy with our prior work, let

$$N_d(p) = \#\{g : 1 \leq g \leq p-1, (g, p-1) = d, \text{ord}_p(g) = (p-1)/d\}$$

We have the following characteristic function

$$\psi_1(g) = \sum_{dl|(g, p-1)} \mu(l) = \begin{cases} 1 & (g, p-1) = d \\ 0 & \text{else.} \end{cases}$$

We also have

$$\psi_2(g) = \sum_{m|\frac{p-1}{d}} \frac{\mu(m)}{md} \sum_{j=1}^{md} \chi(g)^{j(p-1)/md} = \begin{cases} 1 & g \text{ has order } (p-1)/d \\ 0 & \text{else.} \end{cases}$$

As in Chapter 2, we may make the following argument to obtain an asymptotic formula:

$$\begin{aligned} N_d(p) &= \sum_{\substack{1 \leq g \leq p-1 \\ \text{ord}_p(g) = (p-1)/d \\ (g, p-1) = d}} 1 = \sum_{\substack{1 \leq g \leq p-1 \\ \text{ord}_p(g) = (p-1)/d}} \sum_{dl|(g, p-1)} \mu(l) \\ &= \sum_{dl|p-1} \mu(l) \sum_{\substack{1 \leq g \leq p-1 \\ dl|g \\ \text{ord}_p(g) = (p-1)/d}} 1. \end{aligned}$$

We can then obtain

$$N_d(p) = \sum_{dl|p-1} \mu(l) \sum_{\substack{g=1 \\ d|g}}^{p-1} \sum_{m|\frac{p-1}{d}} \frac{\mu(m)}{md} \sum_{j=1}^{md} \chi(g)^{j(p-1)/md}.$$

Let $g = d \cdot l \cdot h$. This gives us

$$N_d(p) = \sum_{m|\frac{p-1}{d}} \frac{\mu(m)}{md} \sum_{dl|p-1} \mu(l) \sum_{j=1}^{md} \chi(dl)^{j(p-1)/md} \sum_{h=1}^{(p-1)/dl} \chi(h)^{j(p-1)/md}.$$

Looking at the contribution from the principal character, we have:

$$\begin{aligned} & \sum_{m|p-1} \frac{\mu(m)}{md} \sum_{l|\frac{p-1}{d}} \mu(l) \frac{(p-1)}{ld} \\ &= \sum_{m|\frac{p-1}{d}} \frac{\mu(m)}{m} \sum_{l|\frac{p-1}{d}} \frac{\mu(l)}{l} \left(\frac{p-1}{d^2} \right) \\ &= \frac{\varphi\left(\frac{p-1}{d}\right)^2}{p-1}. \end{aligned}$$

We can estimate the contribution from the $md - 1$ nonprincipal characters as

$$\begin{aligned} |\text{contribution}| &\leq \sum_{m|\frac{p-1}{d}} \frac{\mu(m)}{md} \sum_{dl|p-1} \mu^2(l) \sum_{j=1}^{md-1} \left| \sum_{h=1}^{(p-1)/dl} \chi(h)^{j(p-1)/md} \right| \\ &\leq \sum_{m|\frac{p-1}{d}} \mu^2(m) \sum_{dl|p-1} \mu^2(l) \frac{md-1}{md} C\sqrt{p} \log p \\ &= \tau_0 \left(\frac{p-1}{d} \right)^2 C\sqrt{p} \log p \\ &= O(p^{1/2+\varepsilon}). \end{aligned}$$

We now have

Theorem 5.1 *Let p be prime. Let $\varepsilon > 0$. Let $N_d(p)$ be the number of integers h , in the range $1, \dots, p-1$ with order $(p-1)/d$ in $(\mathbb{Z}/p\mathbb{Z})^*$ such that $(h, p-1) = d$. Then*

$$N_d(p) = \frac{\varphi\left(\frac{p-1}{d}\right)^2}{p-1} + O(p^{1/2+\varepsilon}).$$

where the implied constant depends only on ε .

One can obtain an expression for the total number of pairs (g, h) , with g a primitive root, such that $g^h \equiv h \pmod{p}$ and $1 \leq h \leq p-1$, by summing $N_d(p)$ over the d dividing $p-1$.

Chapter 6

Appendix A: Computer Programs

6.1 Mathematica Program I

Our first program, written in Mathematica code, runs through a list of numbers and prints out the counterexamples to Brizolis' conjecture. The desired output is an empty file. Refer to the list of potential counterexamples to Brizolis that was displayed in a previous chapter. This program reads in the list of potential counterexamples with 8 prime factors that meet the specific criteria. The first part of the program identifies the primes in the list. We should note that our program uses the PrimeQ command which is rigorous only in the range up to 10^{15} . We use this program only in the rigorous range (in fact only up to 10^{12}). The primes are output to a file 8fprimes.dat and then are tested to see if they are Brizolis counterexample primes. We use the sufficient condition for Brizolis to test whether the given prime is a counterexample.

For each prime p , the program tests the numbers in the range 1 to $p - 1$ first to see if the given integer is relatively prime to $p - 1$. If not, the program goes on to the next number in the range 1 to $p - 1$. If so, the program checks to see if the Jacobi symbol of the number over p is -1 . If not, the number cannot be a primitive root and the program goes on to the next integer in the range. If so, the program tests to see if the integer is in fact a primitive root. If so, the program moves on to the next prime. If not, the program moves to the next integer in the range 1 to $p - 1$ for the same prime. For a given prime p , if

the program runs through all the numbers in the range in this fashion and does not find a primitive root that is relatively prime to $p-1$, then the program is to print out BadPrime, p .

In testing that this program ran properly, we had the witnesses printed out for a large range. However, once we were convinced it was running properly we decided just to have the (hypothetical) counterexamples printed out for space reasons.

```

Let A=ReadList["8factors"];
b=Length[A];
For[i = 1, i ≤ b, i ++,
If[PrimeQ[Part[A, i]]==True,
PutAppend[Part[A, i], "8fprimes.dat"]]]
M=ReadList["8fprimes.dat"];
c=Length[M]

k=2;
j=1;
i=1;
While[j ≤ c, p=Part[M, j]];
L=First[Transpose[FactorInteger[p - 1]]];
While[i ≤ p, If[i == p, Print["BadPrime", p]];
If[GCD[i, p - 1]==1,
If[JacobiSymbol[i, p]==-1,
While[k < Length[L]+1,
If[PowerMod[i, ((p - 1)/Part[L, k]), p]==1,
k=Length[L]+2, k++]]]];
If[k==Length[L]+1,
PutAppend[SequenceForm[i, p], "8fwitnesses.dat"]]] i = p + 1, k = 2; i ++]; i = 1; k = 2; j ++]

```

6.2 Mathematica Program II

This Mathematica program is the program that we used to check the conjecture case by case up to 6.8×10^8 . The program checks the sufficient condition and outputs to the screen the first instance of a primitive root mod p that is relatively prime to $p - 1$.

```

i = 1;
j = 2;
k = 1;
While[j < 10, p=Prime[j];L=First[Transpose[FactorInteger[p - 1]]];
While[i ≤ p, If[i == p, Print["BadPrime", p]];
While[k < Length[L]+1,
If[PowerMod[i, ((p - 1)/Part[L, k]), p] == 1, k=Length[L]+2, k + +]];
If[k == Length[L]+1, Print[i, j, p];
i = p + 1, k = 1; i + +]]; i = 1; k = 1; j + +

```

6.3 C++ Program

This is the program that actually identifies the potential counterexamples to Brizolis which meet certain parameters. The program first uses a Sieve of Eratosthenes to make a file with all the primes up to 100,000. Then we use those primes and a modified Sieve of Eratosthenes where we tabulate for each position in the range how many prime factors the number in that position has. Lastly, we output to a file the integers with the number of prime factors we identified earlier. The output from this program then gets tested by Mathematica Program I.

We used a Perl script to automate the iteration of this program in a given range. Recall that there were several ranges that we were interested in. Thanks to Francis Zane for writing the Perl script and for help with the writing of this program so that the program could handle very large integers and files.

```
#include<stdlib.h>
#include<iostream.h>
#include<math.h>
#include<fstream.h>
#include<sys/types.h>

using namespace std;
const int sievemax=100000;

void main()
{
ofstream out_stream;
out_stream.open("data.dat");

long long START = 66000;
START=START*100000;
long long interval_length=100000000;
long long MAXIMUM = START + interval_length;
long long i, j, k, l, m, r, q, M, n, s;
int number_of_primes;
int *PrimeTable;
PrimeTable = (int*) malloc(sizeof(int)*sievemax);
int *Primes;
Primes=(int*) malloc(sizeof(int)*sievemax);
int *number_of_factors = (int *) malloc(sizeof(int)*interval_length);

//Initialize all elements in the array to 1

for(i = 2, i < sqrt(sievemax);i ++)
{
if(PrimeTable[i]==1)
```

```

{
k=i*i;
for(j = k; j < sievemax; j = j + i)
{
PrimeTable[j]=0;
} } }

//The following array compresses the array PrimeTable to just the primes.

k = 1;
for(j = 2; j < sievemax; j++)
{
if(PrimeTable[j]==1)
{ Primes[k]=j;
k++; }}
number_of_primes=k-1;

//Initialize the number_of_factors array to 3 (for 2,3,5)

for(l = 1; l < interval_length; l++)
{
number_of_factors[l]=3;
}
for(l = 4; l <= number_of_primes; l++)
{
i=Primes[l];
n = i*((START-1)/i+1);
m = n;
M =(MAXIMUM-m)/i;
q = n-START;
for(j = 0; j < M; j++)

```

```
{  
number_of_factors[q]=number_of_factors[q]+1;  
q = q + i;  
} }  
for(s = 1; s < interval_length; s + +)  
{  
if(number_of_factors[s]==10 || number_of_factors[s]==11)  
out_stream<<30*(s+START)<<endl; } out_stream.close(); }
```

Bibliography

- [1] G. Bachman and L. Rachakonda. On a Problem of Dobrowolski and Williams and the Pólya-Vinogradov inequality. *Ramanujan J.*, **5** 2001, 65-71.
- [2] M. Campbell and C. Pomerance. On fixed points for discrete logarithms. *to be submitted*.
- [3] R. Crandall and C. Pomerance. *Prime numbers: A computational perspective* Springer-Verlag, New York 2001.
- [4] H. Davenport. *Multiplicative Number Theory*, Second Edition, Springer-Verlag, New York, 1980.
- [5] C. Cobeli and A. Zaharescu. An exponential congruence with solutions in primitive roots. *Rev. Roumaine Math. Pures Appl.* **44**, (1999), 15-22.
- [6] R.K. Guy. *Unsolved Problems in Number Theory*. Springer-Verlag, New York-Berlin, 1981. (2nd edition 1994)
- [7] G.H. Hardy and E.M. Wright. *An introduction to the theory of numbers*. Fourth Edition, Oxford University Press, London 1968.
- [8] J. Holden. Fixed Points and Two-cycles of the Discrete Logarithm. In: *Algorithmic number theory: 5th international symposium; proceedings*, **2369** in Spinger Lecture Notes in Computer Science, Springer-Verlag, 2002.
- [9] W-P. Zhang. On a problem of Brizolis. (Chinese. English, Chinese summary), *Pure Appl. Math.* **11** (1995) suppl., 1-3.