On the Existence of a Euclidean Algorithm in Number Rings with Infinitely Many Units

Jake Parkhurst

Faculty Advisor:
Martin Thanh Luu

A thesis presented for the degree of
Bachelors of Science in Mathematics

Department of Mathematics
University of California, Davis
Winter 2019

Contents

1 Introduction

The classification of rings of interest in number theory using ring-theoretic properties (such as Euclidean domains, principal ideal domains, unique factorization domains, etc.) is a valuable branch of research because it can determine when theorems carry between similar domains. Additionally, domain classification gives insight into what types of proofs will be fruitful or invalid for a certain type of domain. A historical example from early attempts to prove Fermat's Last Theorem highlights how information about a domain could have prevented misguided research. One attempt analyzed numbers of the shape $a_0 + a_1\zeta + a_2\zeta^2 + \ldots + a_{n-1}\zeta^{n-1}$ where $\zeta^n = 1$ and a_i are in $\mathbb{Z}$. However, this proof failed because it incorrectly assumed unique factorization within numbers of this form. If the mathematician had known that he was not working in a unique factorization domain, he could have pursued a proof more likely to succeed.

This thesis will elaborate on Hendrik W. Lenstra Jr.'s work [1], [2], [3] regarding sufficient conditions for a number ring with infinitely many units to be a Euclidean domain. Lenstra connects several observations that suggest that the Generalized Riemann Hypothesis (GRH) can be used to prove that certain rings are Euclidean. This thesis will illustrate the topics Lenstra presents, including a Euclidean function ψ, in order to help someone with an undergraduate level of mathematics understand the reasoning behind Lenstra's proof. This ψ is defined as follows:

Definition. *Given a ring R, let $R_{-1} = \{0\}$ and $R_n = \{\alpha \in R$: residues of α are contained in $R_{n-1}\}$, and let $\psi(\alpha) = n$ when α is in R_n but α is not in R_{n-1}.*

Lenstra applies ψ to number fields, which are sets of elements $q_n\eta^n + q_{n-1}\eta^{n-1} + \ldots + q_1\eta + q_0$ where η is a root of an irreducible polynomial $p_m x^m + p_{m-1}x^{m-1} + \ldots + p_1 x + p_0$ and p_j, q_i are in $\mathbb{Q}$. He then analyses number rings R (which are subsets of number fields) that satisfy the following properties:

Given a number field K:
1) for every element α in K, there is an integer m such that $m\alpha$ is in R.
2) There are fixed elements $\theta_0, \theta_1, \ldots \theta_d$ in K such that every element α of K that is in R can be written as $\alpha = a_0\theta_0 + a_1\theta_1 + \ldots + a_d\theta_d$ where a_i are integers (i.e. every element of R is a linear combination of $\theta_0, \theta_1, \ldots \theta_d$ with coefficients in $\mathbb{Z}$).

In order for a domain D to be Euclidean, there must be a function

$$norm : D \to \mathbb{N} \cup \{0\}$$

(called a Euclidean function) such that for α and β in D and $\beta \neq 0$, there exist κ and ρ in D such that $\alpha = \beta\kappa + \rho$ and either $\rho = 0$ or $norm(\rho) < norm(\beta)$. For convenience, "Euclidean function" and "norm" will be used interchangeably throughout this paper. A common norm in undergraduate mathematics is the absolute value function for $\mathbb{Z}$.

Let us define a norm N that is commonly used in number fields: Given a number field K generated by η, with η being a root of an irreducible polynomial $p(x) = p_m x^m + p_{m-1}x^{m-1} + \ldots + p_1 x + p_0$, where p_j are in $\mathbb{Q}$, let τ be an element of K written as $\tau = q_n\eta^n + q_{n-1}\eta^{n-1} + \ldots + q_1\eta + q_0$, where q_i are in $\mathbb{Q}$. Define the norm $N(\tau)$ as the product:

$$N(\tau) = \left| \prod_{\iota} (q_n\iota^n + q_{n-1}\iota^{n-1} + \ldots + q_1\iota + q_0) \right|$$

where ι are all of the roots of $p(x)$. If R is a number ring of K, then for elements α and β in R, let us write α/β as τ, which is an element of K. We can now rewrite $\alpha = \beta\kappa + \rho$ as $\tau - \kappa = \rho/\beta$. If R is Euclidean with respect to N, then $\rho = 0$ or $N(\rho) < N(\beta)$, and by taking N of both sides we get $N(\tau - \kappa) = N(\rho)/N(\beta) < 1$ (note that the converse is also true, a fact we will use shortly). After making this observation, Lenstra presents a theorem by Hurwitz [2].

Theorem 1. **[Hurwitz]** *Given a number field K and an associated number ring R, there is an integer $m > 1$, so that for each τ in K there is a κ in R and an integer j, $0 < j < m$ such that $N(j\tau - \kappa) < 1$, with N as defined above.*

Lenstra then modifies the proof of this theorem to extend it to the following:

Theorem 2. *There is an integer $m > 1$, so that for all $\omega_1, \omega_2, \ldots, \omega_m, \tau$ in K there is a κ in R such that $N((\omega_j - \omega_i)\tau - \kappa) < 1$ for some integers i, j, $1 \leqslant i < j \leqslant m$.*

Note that by taking $\{\omega_1, \omega_2, \ldots, \omega_m\} = \{1, 2, \ldots, m\}$, we recover Hurwitz's Theorem. Lenstra points out that if it is possible to pick $\omega_1, \omega_2, .., \omega_m$ such that $\omega_j - \omega_i$ is a unit of R, then $\omega_j - \omega_i$ has an inverse. This gives $N(\omega_j - \omega_i) = 1$ because for any α in R, $N(\alpha)$ is a positive integer and thus if α is a unit, $1 = N(1) = N(\alpha\alpha^{-1}) = N(\alpha)N(\alpha^{-1})$ which implies that both $N(\alpha)$ and $N(\alpha^{-1})$ are 1. Then using Theorem 2

$$N(\tau - \kappa(\omega_j - \omega_i)^{-1}) < 1$$

Thus, $\rho = \kappa(\omega_j - \omega_i)^{-1}$ is in R and every element τ of K can be written as the sum of an element ρ of R and an element $\tau - \rho$ of K with $N(\tau - \rho) < 1$, implying that R is Euclidean. This observation leads to the idea that a large enough set of units in a given number ring can make it possible to show that ring is Euclidean. Lenstra's Theorem 3 is a result of the investigation into this idea.

Theorem 3. **[Lenstra]** *Given a number ring R with unique factorization and infinitely many units, if one assumes several of the Generalized Riemann Hypotheses, then R is Euclidean using ψ (as previously defined) as the Euclidean function.*

Aside from the assumption of the GRH which generalizes the Riemann Hypothesis to extensions of $\mathbb{Q}$, the proof of Theorem 3 relies on the following proposition:

Proposition 1. *Given a number ring R with infinitely many units, let P be the set of primes p in R such that for every element β in R, either $p \mid \beta$ or $\beta \equiv u \bmod p$, with u being a unit of R. Then for every β in R such that either β is a prime not in P or $\beta = p_1 p_2$ where p_1 and p_2 are in P, for all α coprime with β, there exists ρ in R with $\rho \equiv \alpha \bmod \beta$ where ρ is either a unit of R or ρ is in P.*

After illustrating how ψ suggests a method of proving Theorem 3, this paper will heuristically verify the existence of infinitely many primes in P in rings of the form $\frac{\beta}{\alpha^j}$ where α is a fixed integer, and both β and j range over $\mathbb{Z}$. These heuristics are related to Artin's conjecture, which is subsequently verified using heuristics. These heuristics are followed by a discussion of the nuance in using ψ and the GRH to prove Theorem 3.

2 ψ: A Novel Norm

As mentioned, the norm function most familiar to an undergraduate math student is the absolute value function for $\mathbb{Z}$. Lenstra constructs a function ψ modeled after the properties of a Euclidean

function. Thus, if ψ is defined for every α in R, ψ will be a Euclidean function. To reiterate, Lenstra aims to create a ψ that satisfies:

For all α and β in R and $\beta \neq 0$, there exists κ and ρ in R such that $\alpha = \beta\kappa + \rho$ with either $\rho = 0$ or $\psi(\rho) < \psi(\beta)$.

Lenstra begins by identifying the β in R that should satisfy $\psi(\beta) = 0$. For ψ to be a Euclidean function, which are non-negative, it is impossible for ρ to be nonzero, because that would give $\psi(\rho) < \psi(\beta) = 0$. So for $\psi(\beta) = 0$, then $\rho = 0$, giving $\alpha = \beta\kappa$ for all α in R. Setting $\alpha = 1$ implies that β must be a unit. Thus, Lenstra defines $\psi(\beta) = 0$ when β is a unit.

For $\psi(\beta) = 1$, ρ can be 0 or $\psi(\rho) = 0$. If $\rho = 0$, then $\beta \mid \alpha$. If $\psi(\rho) = 0$, then ρ is a unit. Thus $\psi(\beta) = 1$ implies that either β divides α or leaves a remainder of a unit. (As Lenstra phrases it: every residue class of β either contains 0 or a unit.) Lenstra expands this by categorizing R into sets R_n where:

$$R_{-1} = \{0\}$$
$$R_n = \{\beta \in R : \text{ residues of } \beta \text{ are contained in } R_{i,i<n}\}$$

This categorization gives $\psi(\beta) = n$ when β is in R_n but β is not in R_{n-1}. If every β is contained in some R_n, then ψ is defined for every β, and thus by construction ψ is a Euclidean function. Let us now consider the application of this norm to two rings, $\mathbb{Z}$ and $(\mathbb{Z}/5\mathbb{Z})[x]$.

2.1 ψ for $\mathbb{Z}$

Lenstra shows this categorization for $R = \mathbb{Z}$. For x in $\mathbb{Z}$:

$\psi(x) = 0$ for $x = \pm 1$
± 1 are the only units of $\mathbb{Z}$

$\psi(x) = 1$ for $x = \pm 2$ and ± 3
0 and 1 are the residues mod 2; 0 and ± 1 are the residues mod 3. Note that -1 $\equiv$ 2 mod 3.

$\psi(x) = 2$ for $x = \pm 4$, ± 5, ± 6, and ± 7
In the case of $x = 7$, 0, ± 1, ± 2, and ± 3 are the residues mod 7 since -1 $\equiv$ 6 mod 7, -2 $\equiv$ 5 mod 7, and -3 $\equiv$ 4 mod 7. If $\mid x \mid > 7$, x would have a residue ρ with $\mid \rho \mid > 3$ which is not contained in the set of elements satisfying $\psi(x) = 0$ or $\psi(x) = 1$. Thus ± 7 are the largest elements satisfying $\psi(x) = 2$.

$\psi(x) = 3$ for $x = \pm 8, \ldots, \pm 15$
Similarly, for the case when $x = 15$, 0, $\pm 1, \ldots, \pm 7$, are the residues mod 15 and thus there are no x larger than ± 15 that satisfy $\psi(x) = 3$.

The corresponding R_n, using the above categorization, gives:

$$\begin{aligned}
R_0 &= \{-1, 0, 1\} \\
R_1 &= \{-3, -2, -1, 0, 1, 2, 3\} \\
R_2 &= \{-7, \ldots, -1, 0, 1, \ldots, 7\} \\
R_3 &= \{-15, \ldots, -1, 0, 1 \ldots, 15\} \\
&\ldots \\
R_n &= \{-(2^{n+1} - 1), \ldots, -1, 0, 1 \ldots, 2^{n+1} - 1\}
\end{aligned}$$

This give the following formula for ψ applied to $\mathbb{Z}$:

$$\psi(x) = n \text{ for } x = \pm 2^n, \pm(2^n + 1), \ldots, \pm(2^{n+1} - 1)$$

Note that $n = \log_2(2^n) < \log_2(2^{n-1} + 1) < \ldots < \log_2(2^{n+1} - 1) < n + 1$. Using $[x]$ to denote the step function that rounds x down to the nearest integer, we can rewrite ψ as:

$$\psi(x) = [\log_2(\mid x \mid)] = \left[\frac{\ln(\mid x \mid)}{\ln(2)}\right] \tag{1}$$

2.2 ψ for $F[x]$

Another example is in applying ψ to $F[x]$, where F is a field. Let α be a polynomial in x with coefficients in F. In order for $\psi(\alpha) = 0$, α must be a unit. The only units of $F[x]$ are the nonzero elements of F, (i.e. the nonzero elements of $F[x]$ with degree 0). The elements that satisfy $\psi(\alpha) = 1$ are the ones such that every residue class contains either 0 or a unit. These turn out to be the elements of degree 1. To see this, consider $F[x] = (\mathbb{Z}/5\mathbb{Z})[x]$. In this field, $0 = 0$, and the units are 1, 2, 3, 4. Any element with degree greater than 0 does not have an inverse because $(\mathbb{Z}/5\mathbb{Z})[x]$ does not contain x^{-1}. Let us look at the residue class of $3x + 2$.

We want to determine whether all the nonzero congruence classes of $3x + 2$ contain a unit. In other words, can we always find a unit u that satisfies $\alpha \equiv u \bmod 3x + 2$ for every α in R, when α is not divisible by $3x + 2$? Take any polynomial $\alpha = a_n x^n + \cdots + a_1 x^1 + a_0$ in $(\mathbb{Z}/5\mathbb{Z})[x]$. Using long division, we can always find an element ρ with degree$(\rho) \leqslant$ degree$(3x + 2) = 1$. Let $\alpha = 2x^4 + 4x^3 + x + 2$, long division gives:

$$\begin{array}{r}
4x^3 + 2x^2 + 2x + 4 \\
3x + 2 \,\overline{)\, 2x^4 + 4x^3 + 0x^2 + x + 2} \\
\underline{2x^4 + 3x^3} \\
x^3 + 0x^2 \\
\underline{x^3 + 4x^2} \\
x^2 + x \\
\underline{x^2 + 4x} \\
2x + 2 \\
\underline{2x + 3} \\
4
\end{array}$$

Note that it is always possible to cancel the terms $a_i x^i$ with degree greater than $3x + 2$ (i.e. all the $a_i x^i$ when $i > 1$) at each step of long division because the coefficients are all units since F is a field. For example $3x$ was multiplied by $2x^2$ to cancel the x^3 term.

In the case of $3x + 2$, $\rho = 0$ is in the congruence class of α only if $3x + 2$ divides α. Otherwise it is only possible to find ρ with degree$(\rho) = 0$ meaning that ρ is a unit. Thus for every α in R, α is either divisible by $3x + 2$ or is congruent to a unit; so $\psi(3x + 2) = 1$. The reasoning that shows that $\psi(3x + 2) = 1$ holds for every element β of degree 1 in $F[x]$.

Let us now examine an element of degree 2: $3x^2 + 3x + 1$. We can see from long division that every α in R is in the same congruence class as an element ρ with degree less than 2. To show that we can find at least one ρ with degree equal to 1 (otherwise $\psi(3x^2 + 3x + 1) < 1$), consider $\alpha = x$: there is no element κ such that $x = \kappa(3x^2 + 1) + \rho$, where ρ is 0 or a unit (i.e. 1, 2, 3, or 4). In fact, for any β we can always find an element α not congruent to any elements ρ with degree$(\rho) <$ degree$(\beta) - 1$ by simply adding x^{n-1} where $n =$ degree(β). Using the example $\beta = 3x^2 + 3x + 1$, pick $\alpha = \beta + x = 3x^2 + 3x + 1 + x = 3x^2 + 4x + 1$:

$$\begin{array}{r} 1 \\ 3x^2 + 3x + 1 \,\overline{)\, 3x^2 + 4x + 1} \\ \underline{3x^2 + 3x + 1} \\ x \end{array}$$

This reasoning holds with all elements of degree equal to 2. More generally, for any element β with degree$(\beta) = n$, then: 1) every element α is congruent to some ρ with degree$(\rho) < n$, and 2) there exists some element γ that is not congruent to any elements with degree less than $n - 1$. From this we can easily construct ψ. $\psi(\beta) = 0$ iff β is a unit (i.e. a nonzero element of $F[x]$ with degree$(\beta) = 0$). From there by induction, $\psi(\beta) =$ degree(β):

$$\begin{aligned} \psi(\beta) = 0 &\iff \text{degree}(\beta) = 0 \\ \psi(\beta) = 1 &\iff \text{degree}(\beta) = 1 \\ \psi(\beta) = 2 &\iff \text{degree}(\beta) = 2 \\ &\cdots \\ \psi(\beta) = n &\iff \text{degree}(\beta) = n \end{aligned}$$

3 A first attempt to prove Theorem 3

In [3], Lenstra shows that it is possible to "prove" Theorem 3 using the following assumption (which turns out to be false):

Assumption 1. *Given a number ring R, for each pair of relatively prime elements a and b in $R, b \neq 0$, there is a prime p such that $p \equiv a \bmod b$ and every x in R is divisible by p or is congruent to a unit mod p.*

This set of primes will be referred to throughout this paper, so let us define them:

Definition. *Let P be the set of primes p such that every x in R is divisible by p or is congruent to a unit mod p.*

We saw earlier that for β in R, $\psi(\beta) = 1$ if every α in R is divisible by β or congruent to a unit mod β. Thus if $\psi(\beta) = 1$, for every α not divisible by β, there exist κ such that $\alpha = \kappa\beta + u$, where u is a unit. A quick proof by contradiction shows that β must be prime. Assuming that α and β share a common factor d that is not a unit, then d must also divide u. If d divides u, then there exists a q such that $qd = u$. But since u is a unit, it has a multiplicative inverse u^{-1}. Thus d also has a multiplicative inverse since $d(qu^{-1}) = uu^{-1} = 1$. Thus d is a unit, which give a contradiction. Thus α and β share no common factors. Since this is true for all α not divisible by β, β must be prime.

Note that P is the set of primes p such that $\psi(p) = 1$. Thus for all other primes q, $\psi(q) \geqslant 2$. Let β in R decompose into $\epsilon p_1 p_2 \dots p_n q_1 q_2 \dots q_m$, where ϵ is a unit, primes p_i are in P, and primes q_i are not in P (note that we area allowing $p_i = p_j$ and $q_i = q_j$). Given the property of ψ [5, Proposition 12] that

$$\psi(\alpha\beta) \geqslant \psi(\alpha) + \psi(\beta) \tag{2}$$

we can apply this property to the factorization of β, which gives us $\psi(\beta) \geqslant n + 2m$. If we define a function $\chi : R \to \mathbb{N} \cup \{0\}$:

$$\chi(\beta) = n + 2m \tag{3}$$

we can prove Theorem 3 by using Assumption 1 and showing that χ is a Euclidean function.

Let us separately consider the cases when α and β are coprime and when they share a common divisor. When α and β are coprime, consider three sub cases: $\chi(\beta) = 0, 1$, or $\chi(\beta) > 1$. If $\chi(\beta) = 0$, then β is a unit and $\alpha = \beta(\beta^{-1}\alpha) + 0$, which trivially satisfies the Euclidean function criterion. If $\chi(\beta) = 1$, β is in P which by definition of P guarantees a unit ρ that satisfies $\alpha = \beta\kappa + \rho$, thus giving $\chi(\rho) = 0 < 1 = \chi(\beta)$. If $\chi(\beta) > 1$, Assumption 1 guarantees a prime p in P that satisfies $p \equiv \alpha \bmod \beta$. Since $\chi(p) = 1 < \chi(\beta)$, the Euclidean function criterion is met.

When α and β share a common divisor, let d be their greatest common divisor and let $\alpha = d\alpha'$ and $\beta = d\beta'$. Then α' and β' are coprime and there exist κ' and ρ' such that $\alpha' = \beta'\kappa' + \rho'$, with $\chi(\rho') < \chi(\beta')$. Thus $\alpha = d\alpha' = d\beta'\kappa' + d\rho' = \beta\kappa' + d\rho'$. And since $\chi(d\rho') = \chi(d) + \chi(\rho') < \chi(d) + \chi(\beta') = \chi(d\beta') = \chi(\beta)$, there exist κ and ρ (namely κ' and $d\rho'$) such that χ satisfies the requirements of a Euclidean function. This covers all of the cases, thus proving Theorem 1.

Although we will see later that Assumption 1 is untrue, the "proof" that χ is a Euclidean function using Assumption 1 establishes the idea that if P is large enough, then R can be Euclidean (if it is a unique factorization domain).

4 The set of primes in P

To give an example of the set P in a ring with infinitely many units, consider the subring of $\mathbb{Q}$:

$$R = \left\{ \frac{\beta}{2^j} : \beta, j \in \mathbb{Z} \right\}$$

In this case, units are numbers in the form $\pm 2^j, j \in \mathbb{Z}$, so there are an infinite number of units. P is the set of prime numbers p (excluding 2) up to units such that there exists a j in $\mathbb{Z}$ for every positive integer $\beta < p$ that satisfies $\beta \equiv \pm 2^j \bmod p$. For example, for $p = 7$,

$$\{2^0, 2^1, 2^2, 2^3, 2^4, 2^5, 2^6, -2^0, -2^1, -2^2, -2^3, -2^4, -2^5, -2^6\} \equiv \{1, 2, 4, 1, 2, 4, 1, 6, 5, 3, 6, 5, 3, 6\} \bmod 7$$

We can see that when 2 is a primitive root of a prime number p, p is in P. Additionally, when both positive and negative powers of 2 (i.e. $\pm 2^j$, not $2^{\pm j}$) span the set $\{1, 2, \ldots, p-1\}$ mod p, then p is also in P. We saw earlier that Assumption 1 implies Theorem 3. Even though Assumption 1 is false, it gives the insight that the set P must be suitably large in order for R to be Euclidean. So to investigate whether R is Euclidean, we should assess how big P is. Let $f(x)$ give the fraction of primes in P less than or equal to x compared to the total number of primes less than or equal to x, written symbolically as:

$$f(x) = \frac{|\ \{p \leqslant x \mid p \in P\}\ |}{|\ \{p \leqslant x \mid p \text{ prime}\}\ |} \tag{4}$$

Below is a table of how big P is with respect to the set of primes. The data in the table does not appear to immediately converge, although $f(x)$ does seem to remain close to 0.7. Luckily, with modern computational power, we can create a graph that gives a more detailed picture of the behavior of $f(x)$.

Figures 1 through 5 plot $f(x)$ for different sets of the form $\{\frac{\beta}{\alpha^j} : \beta, j \in \mathbb{Z}\}$ (specifically, $\alpha = 2, 3, 7, 41$, and 101). Matlab was used to make the graphs. In the code, a loop cycles through the prime numbers less than a specified n. For each prime p the code calculates the residues mod p of positive and negative powers of α. It then checks to see if these residues cover all integers less than p. If all the integers less than p are represented, then p is in P. As each p is checked, the code keeps track of how $f(x)$ increases. Reading over the code, one can note that the code performs a similar task to determine when α is a primitive root of p, the relevance of which will be discussed in the next section.

Calculating residues was the only part of the code that required optimization. Matlab's built-in moding function is only able to handle numbers less than 2^{1024} and I needed calculate up to $2^{1000000}$ mod p. Since I needed to calculate every value of 2^j mod p, I used the property that $2^{b+(p-1)n} \equiv 2^b$ mod p and calculated the value of each 2^j mod p iteratively by multiplying the value of 2^{j-1} mod p by 2, and then modding the result. For example, 2^{1023} mod $7673 \equiv 3177$. To calculate 2^{1024} mod 7673, I calculated 2*3177 mod 7673, which in this case is 6354.

Below is the Matlab code for finding primes in P in the ring R with $\alpha = 2$.

```
alpha = 2; % This is the number that we will be checking to see if a
    given prime is in P or if alpha is primitive root of p
n = 1000000; % This is how high in the integers we will be rchecking
ps = primes(n); % a list of the primes less than n to test.
ps = (ps ~= alpha).*ps;
ps = ps(ps ~= 0);
```

Table 1: Fraction of primes in P for the ring of rational numbers $\{\frac{\beta}{2^j} : \beta, j \in \mathbb{Z}\}$

x	number of primes $\leqslant x$	number of primes in $P \leqslant x$	$f(x)$
10	4	3	0.75
20	8	6	0.75
50	15	5	0.6667
100	25	17	0.6800
200	46	31	0.6739
500	95	57	0.6800

```
counter = 1; % This variable keeps track of how many primes less than p
    that we have checked
primSumCounter = 0; %This variable keeps track of how many primes less
    than p that alpha is a primitive root for
PSumCounter = 0; %This variable keeps track of how many primes less
    than p are in P
primFraction = zeros(1,length(ps)); %This array store the fraction of
    primes less than p that alpha is a primitive root for
PFraction = zeros(1,length(ps)); %This array store the fraction of
    primes less than p that are in P
k_pVals = zeros(1,length(ps));
for p = ps(1:length(ps)) % cycling through primes to test
    plusRes = ones(1, p-1); % for each prime p, we create a list to
        store residues of +alpha^j, the list starts as all ones since
        one is always the first element of the list
    minusRes = (p-1)*ones(1, p-1);  % for each prime p, we create a
        list to store residues of -alpha^j, the list starts as all p-1
        since p-1 is always the first element of the list (i.e. -1 = p-1
         mod p)
    ListedP = 0; %reset ListedP for each p.
                 % If ListedP stays 0, p is not a prime in P and alpha
                     is not primitive root
                 % If ListedP gets changed to 1, alpha is a primitive
                     root but p is not a prime in P
                 % If ListedP gets switched to 2, alpha is both a
                     primitive root and p is a prime in P

    % for each p, this loop calculates residues mod p, no integers are
        primitive roots of 1, so start at 2
    % also, if residues get to (p-1)/2 + 1 without repeating, then
        alpha is a primitive root of p and p is in P
    for i = 2:(1+(p-1)/2)
        plusRes(i) = mod(alpha*plusRes(i-1),p); % calculating residues
            +alpha^j mod p by multiplying the previous residue by alpha,
             i.e. alpha^j mod p = alpha^(j-1)*alpha mod p
        minusRes(i) = mod(-alpha*plusRes(i-1),p); % calculating
            residues -alpha^j mod p by multiplying the previous positive
             residue by -alpha, i.e. -alpha^j mod p = alpha^(j-1)*-alpha
             mod p
        if (plusRes(i) == 1) % stop when plusRes equals 1 because the
            residues will just start repeating. % if plusRes does not
            equal 1 by the time i = (p-1)/2, than alpha is a primitive
            root so stop the loop
            break
        end
    end
```

```
29
30      % when p = 2, i = 2:(p-1) skips over 2, so we have to check if
            alpha is odd, in which case, it is a primitive root of 2 and 2
            is in P
31      if (p == 2)
32          if (mod(alpha,2) == 1)
33              ListedP = 2;
34          end
35
36      % if plusRes made it to 1 + (p-1)/2 without repeating, than alpha
            is a primitive root and p is in P
37      % if plusRes made it to 1 + (p-1)/2, but that last term was 1, than
             alpha is not a primitive root, but we need to check if p is in
            P
38      elseif ( i == (1 + (p-1)/2) )
39          if (plusRes(i) ~= 1)
40              ListedP = 2;
41          elseif (sum(unique([plusRes minusRes]) >=1) == (p-1)) % if
                there are p-1 unique values greater than 0 between the
                plusRes and negRes, than p is in P
42              ListedP = 1;
43          end
44
45      end % if i doens't make it to 1+ (p-1)/2, alpha is not a primitive
            root of p and p is not in P
46
47
48      if (ListedP == 2) % if alpha is a primitive root of p and p is in P
            :
49          primSumCounter = primSumCounter + 1; % sum of primes for which
                alpha is primitive goes up by 1
50          primFraction(counter) = primSumCounter/counter; % keep track of
                 fraction of primes for which alpha is primitive
51          PSumCounter = PSumCounter + 1; % sum of primes in P goes up by
                1
52          PFraction(counter) = PSumCounter/counter; % keep track of
                fraction of primes in P
53
54      elseif (ListedP == 1) % if listed, then:
55          primFraction(counter) = primSumCounter/counter; % sum of primes
                 for which alpha is primitive does not go up by 1, but still
                 keep track of fraction of primes for which alpha is
                primitive
56          PSumCounter = PSumCounter + 1; % sum of primes in P goes up by
                1
57          PFraction(counter) = PSumCounter/counter; % keep track of
```

```
            fraction of primes in P
    else
        primFraction(counter) = primSumCounter/counter; % sum of primes
            for which alpha is primitive does not go up by 1, but still
            keep track of fraction of primes for which alpha is
            primitive
        PFraction(counter) = PSumCounter/counter; % sum of primes in P
            does not go up by 1, but still keep track of fraction of
            primes in P
    end
    if (ListedP == 0)
        k_pVals(counter) = (p-1)/i;
    elseif (ListedP)
        k_pVals(counter) = 1;
    counter = counter + 1; % keeping track of how many primes have been
        checked
end

%using the average of the last 10% of values as a represenative of the
%convergance value
primAve_limit = mean(primFraction(floor(.9*length(primFraction)):length
    (primFraction)));
PAve_limit = mean(PFraction(floor(.9*length(PFraction)):length(
    PFraction)));


%ploting the data
figure
hold
plot([1,n],primAve_limit*[1,1],'Color','k')
plot(ps,primFraction,'Color',[0  0.4470  0.7410]);
ylim([0,1]);

figure
hold
plot([1,n],PAve_limit*[1,1],'Color','k')
plot(ps,PFraction,'Color',[0  0.4470  0.7410]);
ylim([0,1]);
```

The graphs created in Matlab suggest that $f(x)$ converges (i.e. there is a positive fraction of primes in P). Below are the graphs of $f(x)$ for the sets $\{\frac{\beta}{2^j} : \beta, j \in \mathbb{Z}\}$, $\{\frac{\beta}{3^j} : \beta, j \in \mathbb{Z}\}$, $\{\frac{\beta}{7^j} : \beta, j \in \mathbb{Z}\}$, $\{\frac{\beta}{41^j} : \beta, j \in \mathbb{Z}\}$, and $\{\frac{\beta}{101^j} : \beta, j \in \mathbb{Z}\}$. Additionally, the last graph in this section, Figure 6, summarizes the results of similar computations for the rings $\{\frac{\beta}{\alpha^j} : \beta, j \in \mathbb{Z}\}$ as α ranges from 1 to 1000.

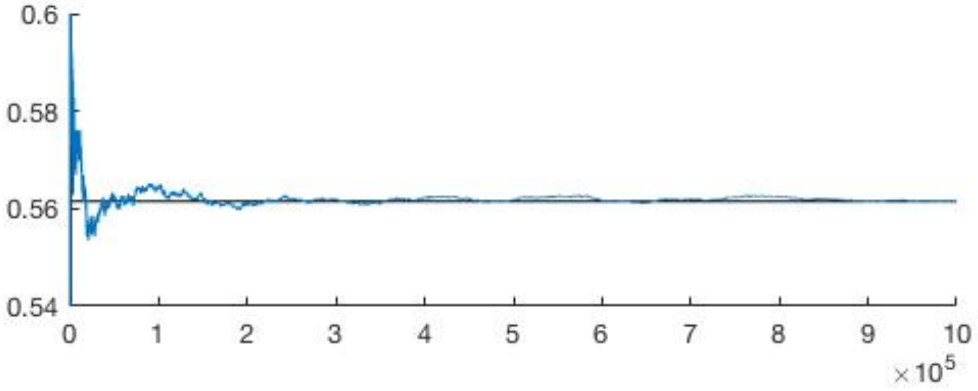

Figure 1: Fraction of primes p in P, $p < x$, for the ring of rational numbers $\{\frac{\beta}{2^j} : \beta, j \in \mathbb{Z}\}$

As seen in Figure 1, the fraction of primes in P appears to converge to a limit of about 0.56. In rings with different denominator bases (i.e. $\frac{\beta}{3^j}$ instead of $\frac{\beta}{2^j}$) the fraction of primes in P does not always stabilize around 0.56. For example, for $\alpha = 3$, $f(x)$ converges to about 0.6.

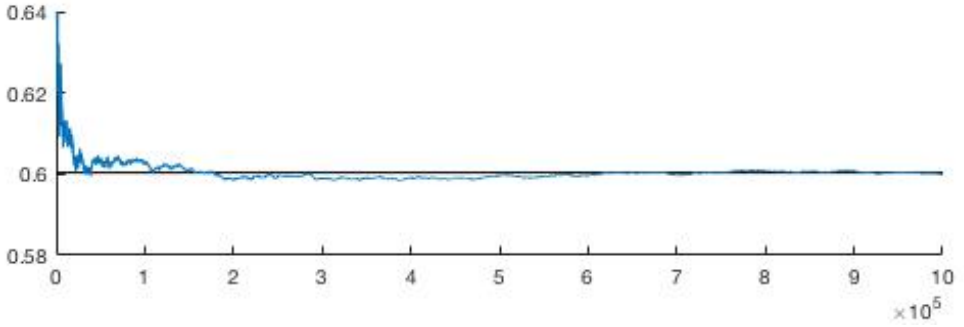

Figure 2: Fraction of primes p in P, $p < x$, for the ring of rational numbers $\{\frac{\beta}{3^j} : \beta, j \in \mathbb{Z}\}$

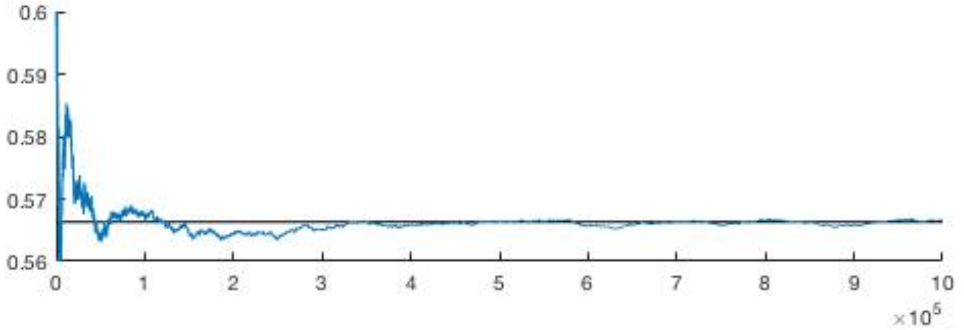

Figure 3: Fraction of primes p in P, $p < x$, for the ring of rational numbers $\{\frac{\beta}{7^j} : \beta, j \in \mathbb{Z}\}$

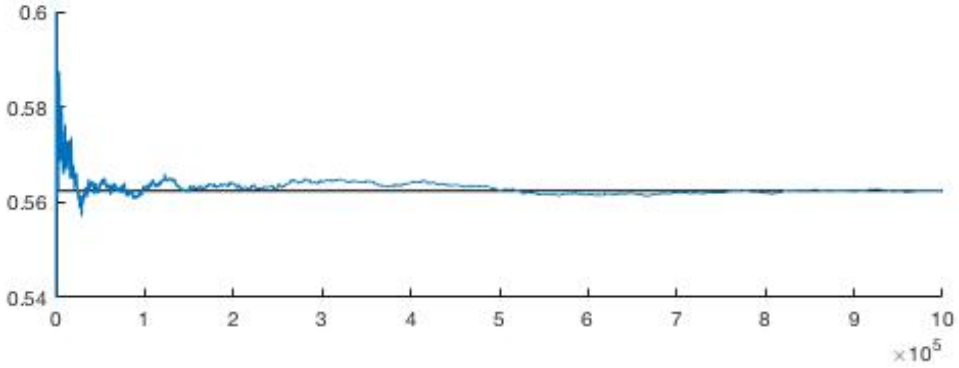

Figure 4: Fraction of primes p in P, $p < x$, for the ring of rational numbers $\{\frac{\beta}{41^j} : \beta, j \in \mathbb{Z}\}$

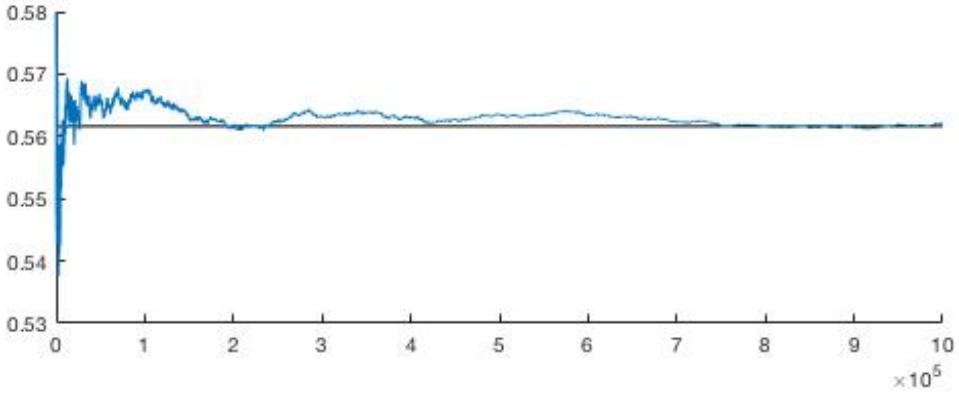

Figure 5: Fraction of primes p in P, $p < x$, for the ring of rational numbers $\{\frac{\beta}{101^j} : \beta, j \in \mathbb{Z}\}$

By running the same algorithm that created Figures 1-5, we can approximate the fraction of primes that are in P for similar rings that have the form $\{\frac{\beta}{\alpha^j}, \beta, j \in \mathbb{Z}\}$ with α a fixed integer. Figure 6, below, shows these approximations plotted against the value of α.

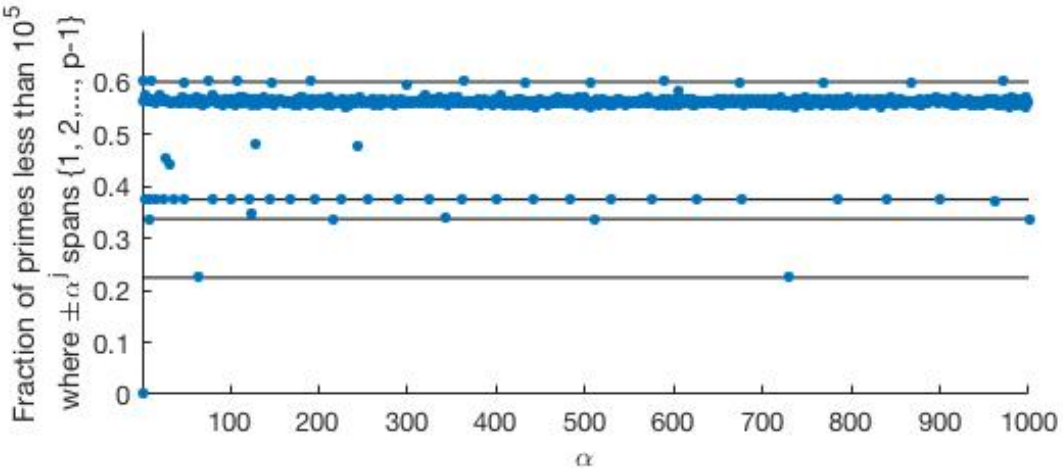

Figure 6: $f(10^5)$ calculated for rings $\{\frac{\beta}{\alpha^j} : \beta, j \in \mathbb{Z}\}$, $1 \leqslant \alpha \leqslant 1000$ and then plotted against α

For most α, it appears that $f(x)$ converges to about 0.5634 (the mean of values between 0.5 and 0.59). There are a few other common values for the limit of $f(x)$: 0.6017, 0.3752, 0.3379, and 0.2245, These values are the means of values clustered together and are visualized as horizontal lines in Figure 6. The α that correspond with $f(10^5) \approx 0.38$ are all squares. However, $\alpha = 64$ and 729, which are also sixth powers, correspond to the two points with $f(10^5) \approx 0.23$. Table 2 below clearly organizes the factorization for the rest of the α with $f(10^5) \not\approx 0.56$.

Table 2: Factorization of α for which $f(10^5) \not\approx 0.5634, 0.3752$, or 0.2245

$f(10^5) \approx 0.6017$		$f(10^5) \approx 0.3379$		$f(10^5) \approx$ other		
α	factors	α	factors	α	factors	$f(10^5)$
3	$\{3\}$	8	$\{2^3\}$	27	$\{3^3\}$	0.4523
12	$\{2^2, 3\}$	125	$\{5^3\}$	32	$\{2^5\}$	0.4427
48	$\{2^4, 3\}$	216	$\{2^3, 3^3\}$	128	$\{2^7\}$	0.4828
75	$\{3, 5^2\}$	343	$\{7^3\}$	243	$\{3^5\}$	0.4768
108	$\{2^2, 3^3\}$	512	$\{2^9\}$			
147	$\{3, 7^2\}$	1000	$\{2^3, 5^3\}$			
192	$\{2^6, 3\}$					
300	$\{2^2, 3, 5^2\}$					
363	$\{3, 11^2\}$					
432	$\{2^4, 3^3\}$					
507	$\{3, 13^2\}$					
588	$\{2^2, 3, 7^2\}$					
675	$\{3^3, 5^2\}$					
768	$\{2^8, 3\}$					
867	$\{3, 17^2\}$					
972	$\{2^2, 3^5\}$					

From the table, it is clear that factorization affects the size of P. The numbers such that $f(10^5) \approx 0.6017$ all contained an odd power of 3 and a high even power of one or more primes. The numbers such that $f(10^5) \approx 0.3379$ are all perfect cubes. In the next section, we will look at a related problem to gain insight into how factorization affects $\lim_{x\to\infty} f(x)$.

5 Artin's Conjecture

In the previous section, $f(x)$ was calculated for the set $\{\frac{\beta}{\alpha^j} : \beta, j \in \mathbb{Z}\}$ by checking for each prime p whether the set $\{\pm\alpha^j \bmod p, 1 \leqslant j < p\}$ contained $\{1, 2, ..., p-1\}$. As noted, if we remove the $\pm$, the set P would simply be the set of primes that have α as a primitive root. Since we are interested in how large P is, the question of whether $f(x)$ converges is similar to Artin's conjecture that every number α (that is not a square number) is a primitive root for a positive fraction of primes. In other words, for non-square α in $\mathbb{Z}, \alpha > 1$, the following limit converges:

$$\lim_{x\to\infty} g(x) = \lim_{x\to\infty} \frac{|\ \{\text{primes} \leqslant x \text{ which have } \alpha \text{ as a primitive root}\}\ |}{|\ \{\text{primes} \leqslant x\}\ |} \tag{5}$$

Christopher Hooley [6] proved this conjecture assuming the GRH, along with Hans Heilbronn's proposed formula for this limit. The formula is:

Artin's Conjecture. *Given any nonzero integer α, $\alpha \neq \pm 1$ and $\alpha \neq \beta^2$ for any β in $\mathbb{Z}$, let $N_\alpha(x)$ be the number of primes not exceeding x for which α is a primitive root. Let α_1 be the squarefree part of α, let h be be the largest integer with the property that α is a perfect h'th power. Lastly, let*

$$C_h = \prod_{\substack{q|h \\ q \text{ prime}}} (1 - \frac{1}{q-1}) \prod_{\substack{q\nmid h \\ q \text{ prime}}} (1 - \frac{1}{q(q-1)})$$

Note that since q ranges across all primes, the second product is an infinite product since there are infinitely may primes that do not divide h. If $\alpha_1 \not\equiv 1 \bmod 4$, then as $x \to \infty$,

$$N_\alpha(x) = C_h \frac{x}{\ln(x)} + O\Big(\frac{x\ln(\ln(x))}{\ln(x)^2}\Big)$$

If $\alpha_1 \equiv 1 \bmod 4$, then as $x \to \infty$,

$$N_\alpha(x) = C_h\Big(1 - \mu(|\ \alpha_1\ |) \prod_{\substack{q|h \\ q|\alpha_1 \\ q \text{ prime}}} \frac{1}{q-2} \prod_{\substack{q\nmid h \\ q|\alpha_1 \\ q \text{ prime}}} \frac{1}{q^2-q-1}\Big)\frac{x}{\ln(x)} + O\Big(\frac{x\ln(\ln(x))}{\ln(x)^2}\Big)$$

where μ is the Möbius function:

$$\mu(n) = \begin{cases} 1 & n \text{ is a squarefree integer with an even number of prime factors} \\ -1 & n \text{ is a squarefree integer with an odd number of prime factors} \\ 0 & \text{otherwise} \end{cases}$$

Since the number of primes less than x, denoted by $\pi(x)$, approaches $\frac{x}{ln(x)}$ as $x \to \infty$, and all of the above infinite products converge, then

$$\lim_{x\to\infty} g(x) = \lim_{x\to\infty} \frac{N_\alpha(x)}{\pi(x)}$$

also converges. Note that if $\alpha_1 \not\equiv 1 \bmod 4$, then $\lim_{x\to\infty} g(x) = C_h$. Additionally, the overwhelming majority of α give a corresponding value of $h = 1$ which in turn gives $C_h = 0.3795....$

To heuristically verify Artin's conjecture, $g(x)$ was graphed using Matlab (Figures 7 - 13). The graphs of $g(x)$ were made using the same code that made the graphs of the previous section because both algorithms check to see if all $n < p$ are congruent to a power of α mod p. The only difference is that for $g(x)$, the algorithm checks if only the residues of α^i mod p (and not the residues of $-\alpha^i$ mod p) cover the integers less than p. Below are the graphs.

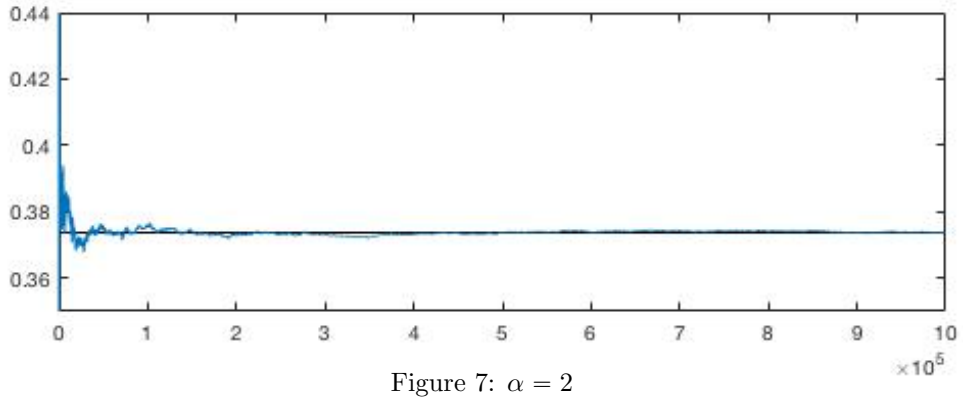

Figure 7: $\alpha = 2$

As seen in Figure 7, the fraction of primes that have 2 as a primitive root appears to converge to a limit of about 0.375. For each of the other primitive roots assessed ($\alpha = 3, 7, 41, 101$), the fraction of primes with α as a primitive root also stabilizes around 0.375. Although primes are not the only numbers that can be primitive roots, Hooley's formula shows a relationship between factorization and $g(x)$. So to keep test cases similar, I picked numbers that were primes.

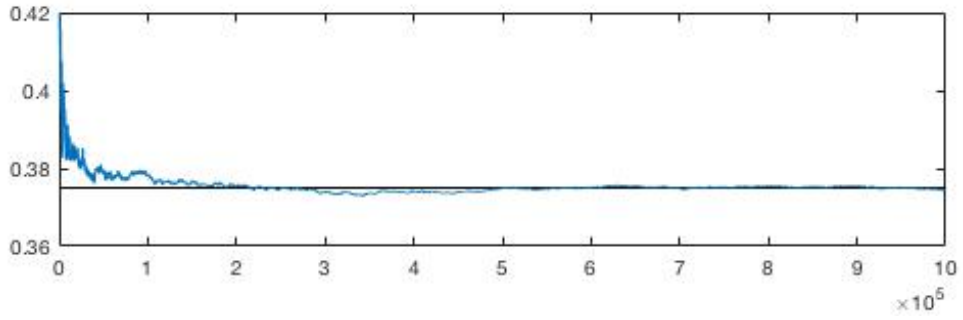

Figure 8: $\alpha = 3$

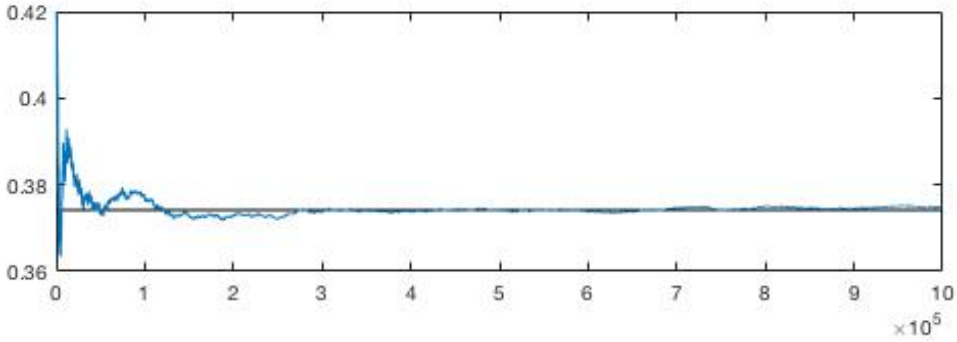

Figure 9: $\alpha = 7$

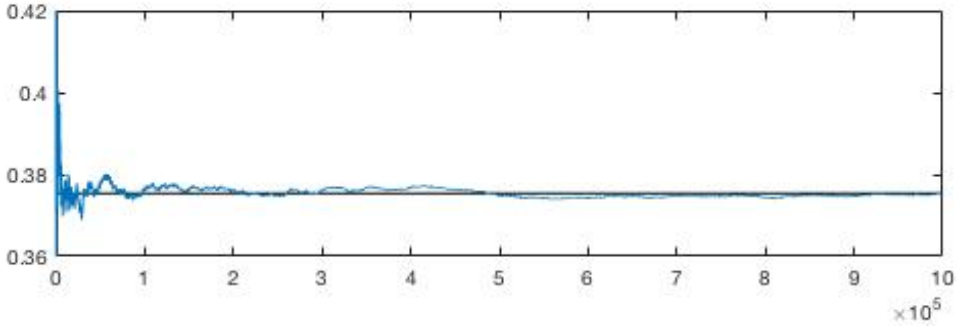

Figure 10: $\alpha = 41$

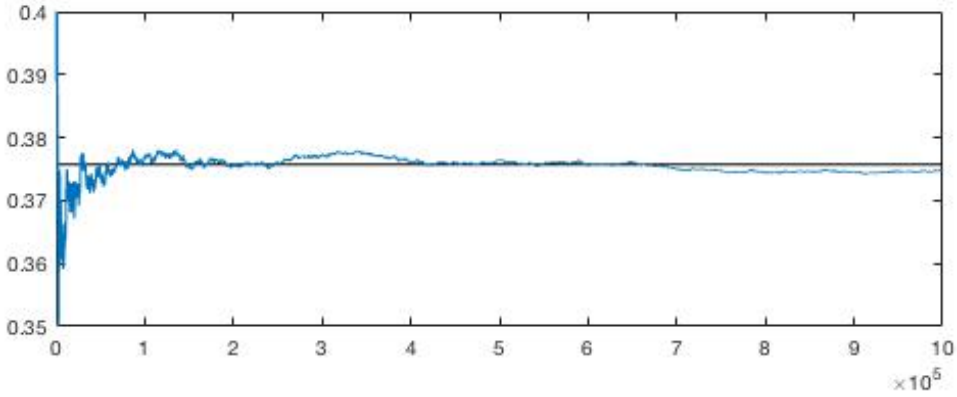

Figure 11: $\alpha = 101$

Figures 12 and 13 below respectively compare the predicted values of $g(x)$ with the computed values for $1 \leqslant \alpha \leqslant 1000$. By plotting Heilbronn's prediction for $\lim_{x\to\infty} g(x)$ for $1 \leqslant \alpha \leqslant 1000$, see Figure 12 below, we can see that most integers are primitive roots for about 38% of all primes. We can see that there are some numbers that deviate from the limit of 0.38. Integer squares are never

primitive roots, as seen by the points in the graph that lie on the horizontal axis. Looking back at Heilbronn's formula, non-square numbers that contain high powers of primes, such as 27, 32, 125, and 128, tend to have lower values.

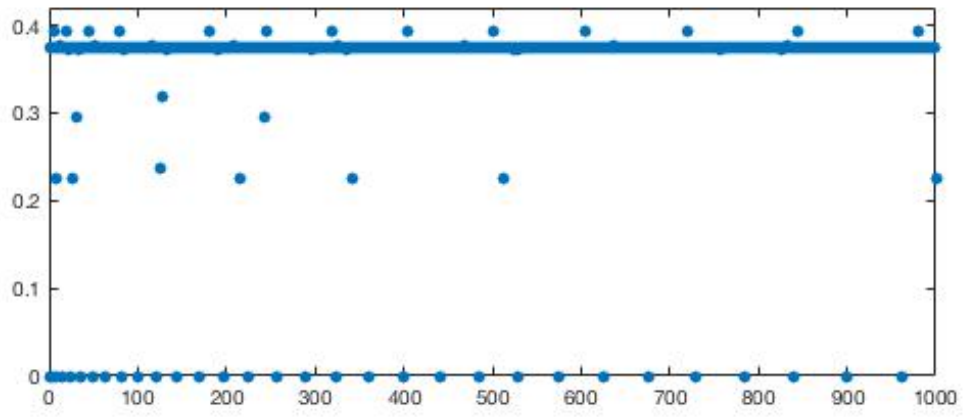

Figure 12: Heilbronn's prediction for $\lim_{x\to\infty} g(x)$, horizontal axis corresponds to α.

The actual fraction of primes less than 100,000 for which α is a primitive root is shown below in Figure 13, which closely resembles Heilbronn's predictions. Figure 13 was created by looping the code that generated Figures 7 - 11 and changing α each cycle.

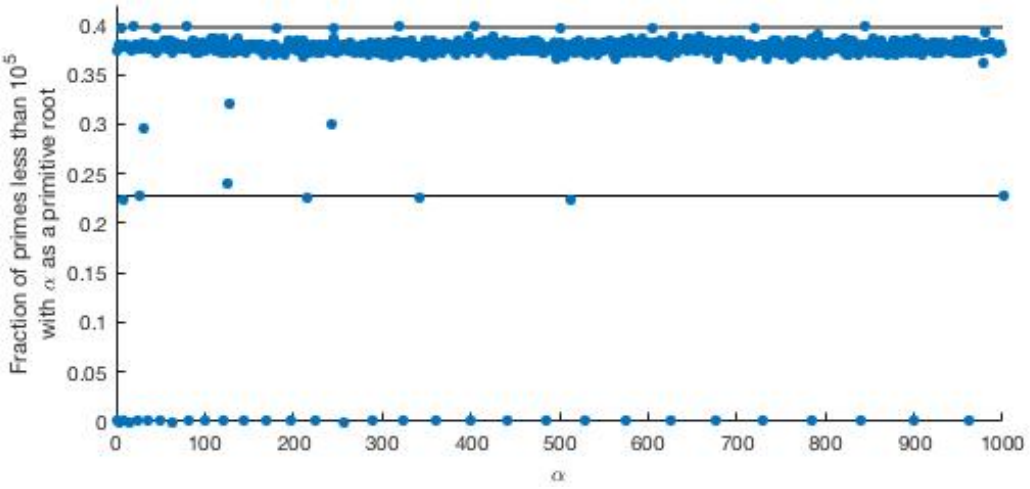

Figure 13: Actual fraction of primes less than 10^5 for which α is a primitive root.

Figure 13 is very similar to the corresponding Figure 6 that plots $f(10^5)$ vs α. Square integers can not be primitive roots which is why $g(\alpha) = 0$ for squares. However, Figure 6 suggests that if

negative powers of square α are considered, a fraction of all primes are in P for $\{\frac{\beta}{\alpha^j} : \beta \in \mathbb{Z}\}$, albeit this fraction appears to be much less than for non-squares, 0.38 instead 0.5576. Other similarities can be seen for $\alpha = 8, 27, 32, 125,$ and 128, all of which fall outside of the clusters of the rest of the numbers around 0.5576 and 0.374, for Figure 6 and Figure 13 respectively. All of these similarities suggest that Figure 6 depicts a similar pattern that depends on the factorization of α.

6 A counterexample to Assumption 1

Although Assumption 1 would allow for a tidy proof of Theorem 3, it is untrue. Lenstra provides a simple example that, while not an exact counterexample to Assumption 1, still illustrates how Assumption 1 could be invalid. Consider primes $p \equiv 1 \bmod 8$. By Gauss's Lemma [7, pg. 52], given below, 2 is a quadratic residue of p, meaning that there is an x in $(\mathbb{Z}/p\mathbb{Z})^\times$ with $2 \equiv x^2 \bmod p$. Thus, 2 cannot be a primitive root of p. This dependence between $p \equiv 1 \bmod 8$ and 2 not being a primitive root of p suggests that Assumption 1 has exceptions; in this case we have p and 2 which are relatively prime but 2 is not a primitive root for these primes, which as we have seen is related to whether p is in P for some rings. Before stating Gauss's Lemma, we must first define the function γ:

Definition. *Given coprime p and a, where p is an odd prime, consider the residues of $ai \bmod p$, $1 \leqslant i \leqslant \frac{p-1}{2}$ that fall in the set $\{-\frac{p-1}{2}, \ldots, -1, 0, 1, \ldots \frac{p-1}{2}\}$. Let $\gamma(p, a)$ be the number of these residues that are less than 0.*

For example, $\gamma(7, 5) = 1$ because $\{i5 \bmod 7, 1 \leqslant i < \frac{7-1}{2} = 3\} \equiv \{5, 10, 15\} \equiv \{-2, 3, 1\} \bmod 7$ which contains 1 negative element.

Gauss's Lemma. *Let a be coprime to p. $(a|p) = (-1)^{\gamma(p,a)} \bmod p$, where $(a|p)$ is 1 if a is a square mod p and -1 if a is not a square mod p.*

If we let $a = 2$ in Gauss's lemma, the following reasoning proves 2 can not be a primitive root if $p \equiv 1 \bmod 8$. Let m be the positive integer such that $2m \leqslant \frac{p-1}{2}$ and $2(m+1) > \frac{p-1}{2}$. Thus for all i such that $m < i \leqslant \frac{p-1}{2}$, the residue of $2i$ in the set $\{-\frac{p-1}{2}, \ldots, \frac{p-1}{2}\}$ is less than 0. Thus m is the number of i that give a positive residue and $\frac{p-1}{2} - m$ is the number of i that give a negative residue; thus $\frac{p-1}{2} - m = \gamma(p, 2)$. Therefore if $p = 8n + 1$, for some integer n, then $m = 2n$ (based on the condition that m is that largest integer that satisfies $2m \leqslant \frac{p-1}{2} = \frac{8n+1-1}{2} = 4n$) and thus $\gamma(p, 2)$ is even since $\gamma(p, 2) = \frac{(8n+1)-1}{2} - m = \frac{(8n+1)-1}{2} - 2n = 4n - 2n = 2n$. Since $\gamma(p, 2)$ is even and $(2|p) = (-1)^{\gamma(p,2)} \bmod p$, $(2|p) = 1$, which means that 2 must be a square mod p and therefore cannot be a primitive root. For $R = \{\frac{\beta}{2^j} : \beta, j \in \mathbb{Z}\}$, if P was defined at the set of primes for which 2 is a primitive root, we would have a counterexample for Assumption 1 since 1 and 8 are relatively prime and there exist no primes p such that $p \equiv 1 \bmod 8$ and 2 is a primitive root of p. Unfortunately, the condition on P is a bit looser, allowing both positive and negative powers of 2 to span $\{1, 2, \ldots, p-1\} \bmod p$. But this does suggest that a counterexample exists.

Indeed, Lenstra provides a definitive counterexample in [3] by considering the elements in the number ring $\mathbb{Z}[\zeta]$, where $\zeta^5 = 1$, and $\zeta \neq 1$. The elements of this ring look like $a_0 + a_1\zeta + a_2\zeta^2 + a_3\zeta^3$, where a_i are in $\mathbb{Z}$. Note that the highest power of ζ included is ζ^3 since $\zeta^4 = -(1 + \zeta + \zeta^2 + \zeta^3)$. To see this consider the sum of the five fifth-roots of unity, $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4$. Since these are

symmetrically spaced around 0 in the complex plane, their real and imaginary components cancel to 0. Thus $1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 = 0$, giving $\zeta^4 = -(1 + \zeta + \zeta^2 + \zeta^3)$.

To fully satisfy our inquiry of Assumption 1, this number ring must have an infinite number of units. An easy way to verify that $\mathbb{Z}[\zeta]$ has infinitely many units is to note that $(1+\zeta)(-\zeta-\zeta^3) = 1$. Since the complex absolute value of elements α in $\mathbb{Z}[\zeta]$, written as $\mid \alpha \mid$, is equal to $\sqrt{a^2 + b^2}$ where a and b are real numbers such that $\alpha = a + bi$, one has

$$\begin{aligned}
|1 + \zeta| &= |1 + \cos(\frac{2\pi}{5}) + i * \sin(\frac{2\pi}{5})| \\
&= \sqrt{(1 + \cos(\frac{2\pi}{5}))^2 + \sin^2(\frac{2\pi}{5})} \\
&= \sqrt{1 + 2\cos(\frac{2\pi}{5}) + 1} \\
&= \sqrt{2(1 + \cos(\frac{2\pi}{5}))} \\
&> 1
\end{aligned}$$

If we examine powers of $(1 + \zeta)$ we see that all powers of must be unique since their complex absolute value is constantly increasing since $\mid 1 + \zeta \mid > 1$ (based on the property that for α in $\mathbb{Z}[\zeta]$, $\mid \alpha^n \mid = \mid \alpha \mid^n$). Since $(-\zeta - \zeta^3)^n$ is the inverse of $(1 + \zeta)^n$, $\mathbb{Z}[\zeta]$ has infinitely many units.

Alternatively, the fact that $\mathbb{Z}[\zeta]$ has infinitely many units is implied by the Dirichlet Unit Theorem:

Dirichlet Unit Theorem. *Let K be an arbitrary number field with r real embeddings and $2s$ complex embeddings. Let G be the group of units for K and let U be the subgroup of units that are also roots of unity. Dirichlet's Unit Theorem states that G mod U is a finitely generated group with $r + s - 1$ independent generators.*

In order for a number field to have a finite unit group, it must have $r + s - 1 = 0$. The minimal polynomial for ζ is the cyclotomic polynomial

$$\Phi_5(x) = x^4 + x^3 + x^2 + x^1 + 1$$

which has degree 4 (see [8, chapter 7] for a more detailed discussion). Thus $\mathbb{Z}[\zeta]$ has four embeddings, and since all four are complex embeddings, $r + s - 1 = 0 + 2 - 1 = 1 > 0$. Therefore $\mathbb{Z}[\zeta]$ can not have a finite unit group (not to be confused with the false statement that $\mathbb{Z}[\zeta]$ can not have a finitely generated unit group modulo the roots of unity.)

However, although $\mathbb{Z}[\zeta]$ satisfies the condition of having infinitely many units, it turns out that for primes π, if $\pi \equiv 1 \bmod 4$, then the natural reduction map from $\mathbb{Z}[\zeta]^\times \to (\mathbb{Z}[\zeta]/\mathbb{Z}[\zeta]\pi)^\times$ is not surjective (see [4, Theorem 9.1] which gives this result). In other words, the quotient map from the group of units of $\mathbb{Z}[\zeta]$ to the group of units of $\mathbb{Z}[\zeta]$ mod π is not surjective (note: the group of units of $\mathbb{Z}[\zeta]$ mod π is the same as the group of non zero congruence classes of π since π is prime). Since the quotient map is not surjective, π has at least one congruency class that does not contain a unit. Therefore π is not in P, thus providing a counterexample to Assumption 1 for number rings with infinitely many units.

7 The use of the Generalized Riemann Hypothesis

As discussed, Assumption 1 is not true and this invalidates the "proof" of Theorem 3 that we saw in Section 3. However this proof can be salvaged if instead of Assumption 1 we use Proposition 1, rewritten below. But first, let us restate the definition of χ from Section 3:

$$\chi(\alpha) = n + 2m : \ \alpha = \epsilon p_1 p_2 \dots p_n q_1 q_2 \dots q_m$$

where ϵ is a unit and p_i and q_j are primes with p_i in P and q_j not in P.

Proposition 1. *Let R be a number ring with infinitely many units, and let P be as previously defined. Then for every β such that $\chi(\beta) = 2$ (i.e. β is a prime not in P or $\beta = p_1 p_2$ where both p_1 and p_2 are primes in P) and all α coprime with β, there exists ρ in R with $\rho \equiv \alpha \ mod \ \beta$ where ρ is either a unit of R or ρ in P*

In order to show that χ is a Euclidean function given Proposition 1, let us separately consider the cases when α and β are coprime and when they share a common divisor. When α and β are coprime, consider four sub cases: $\chi(\beta) = 0, 1, 2$ or $\chi(\beta) > 2$. If $\chi(\beta) = 0$, then β is a unit and $\alpha = \beta(\beta^{-1}\alpha) + 0$, which trivially satisfies the Euclidean function criterion. If $\chi(\beta) = 1$, β is in P which by definition of P guarantees a unit ρ that satisfies $\alpha = \beta\kappa + \rho$, thus giving $\chi(\rho) = 0 < 1 = \chi(\beta)$.

Here is where the proof differs. If $\chi(\beta) = 2$, by Proposition 1 there is a ρ that satisfies $\alpha = \beta\kappa + \rho$ with ρ being either a unit or an element of P, thus giving $\chi(\rho) \leqslant 1 < 2 = \chi(\beta)$. If $\chi(\beta) > 2$, since α and β are coprime, the Dirichlet Theorem of Prime Numbers in Arithmetic Progressions generalized to number rings guarantees a prime p that satisfies $p \equiv \alpha \bmod \beta$ (in fact we are guaranteed infinitely many such primes). Since $\chi(p) \leqslant 2 < \chi(\beta)$, the Euclidean function criterion is met.

When α and β share a common divisor, let d be their greatest common divisor and let $\alpha = d\alpha'$ and $\beta = d\beta'$. Then α' and β' are coprime and there exist κ' and ρ' such that $\alpha' = \beta'\kappa' + \rho'$, with $\chi(\rho') < \chi(\beta')$. Thus $\alpha = d\alpha' = d\beta'\kappa' + d\rho' = \beta\kappa' + d\rho'$. And since $\chi(d\rho') = \chi(d) + \chi(\rho') < \chi(d) + \chi(\beta') = \chi(d\beta') = \chi(\beta)$, there exist κ and ρ (namely κ' and $d\rho'$) such that χ satisfies the requirements of a Euclidean function. This covers all of the cases, thus proving Theorem 1.

The GRH is used in proving Proposition 1 as seen in the following outline of the proof. For each prime p in R, the residue classes that do not contain 0 form a group G_p under multiplication. Within G_p, the residue classes that contain a unit of R make a subgroup $H_p \subset G_p$. A prime p is in P when all of its residue classes that do not contain 0, do contain a unit; symbolically, $[G_p : H_p] = 1$.

Let $k_p = [G_p : H_p]$ and let $P_n = \{p : k_p \text{ has no prime factors less than } n\}$. Figure 14 shows the smallest factor of k_p for primes p of $\{\frac{\beta}{2^j} : \beta, j \in \mathbb{Z}\}$, which correlates with the largest P_n that would contain p. For example: for $p = 8191$, only 26 of the residue classes contain a unit, so $k_{8191} = 315$ since $8190/26 = 315$. Since 315 factors into $3, 3, 5$, and 7, 8191 is in P_2 and P_3, but not P_4. As n increases, $\mid P_n \mid$ decreases, containing fewer primes that are not in P. Since for any prime p not in P, we can find an n such that $p \notin P_{m>n}$, this gives

$$P = \bigcap_{n=1}^{\infty} P_n$$

So p with large spikes in Figure 14 are in more P_n.

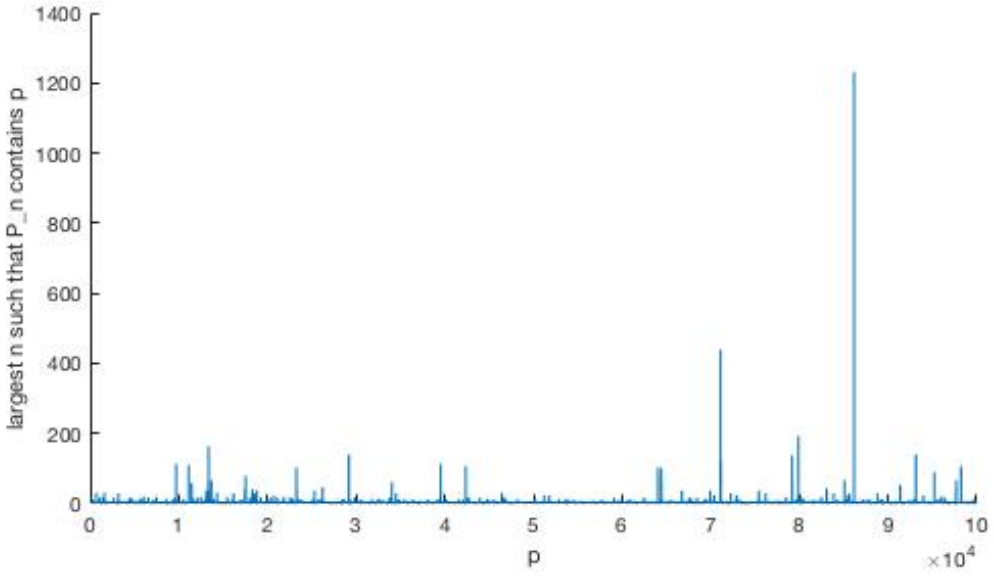

Figure 14: Graph of the largest n such that P_n contains p vs p.

Given coprime elements α, β, and assuming that α is not congruent to a unit mod β, we want to know if there is a prime p in P such that $p \equiv \alpha \bmod \beta$. By analyzing the set

$$V_m = \{p : p \equiv \alpha \bmod \beta, p \in P_m\}$$

we can look at the fraction δ_m of primes that are in V_m. Letting V represent the intersection of all V_m as m goes to infinity, the GRH is used to show that

$$\lim_{m \to \infty} \delta_m = \delta$$

where δ is the fraction of primes that are in V. As such, the GRH can be used to show that V contains a positive fraction of primes, which can then be used to show that P is large enough to establish Proposition 1, which in turn gives Theorem 3.

References

[1] H. W. Lenstra, Jr, *Euclidean Number Fields 1.* The Mathematical Intelligencer 2 (1979), pg 6-15

[2] H. W. Lenstra, Jr, *Euclidean Number Fields 2.* The Mathematical Intelligencer 2 (1979), pg 73-83

[3] H. W. Lenstra, Jr, *Euclidean Number Fields 3.* The Mathematical Intelligencer 2 (1979), pg 99-103

[4] H. W. Lenstra, Jr and A. J. van der Poorten, *On Artin's Conjecture and Euclid's Algorithm in Global Fields.* Inventiones Mathmaticae 42 (1977), pg 201 - 224

[5] P. Samuel, *About Euclidean Rings.* Journal of Algebra 19 (1971), pg 282-301

[6] C. Hooley, *On Artin's Conjecture.* Journal fur die reine und angewandte Mathematik 225 (1967), pg 209-220

[7] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory.* Springer, 2nd edition (1998)

[8] R. Ash, *A Course in Algebraic Number Theory.* University of Illinois, 1st edition (2003)