DECIMAL EXPANSIONS OF THE INVERSES OF PRIME NUMBERS

SHELLY MANBER, NIZAMEDDIN ORDULU, KUAT YESSENOV

Abstract. In this paper we look at the decimal expansion of $\frac{1}{p}$ for different primes p. We find the set of numbers that can occur as the length of the period. We illustrate some statistics about the density of the primes for which the period is maximal. We also explain Artin's heuristic argument about this density.

1. Introduction

This paper investigates some interesting properties of the decimal expansion of $1/p$ for prime numbers p. For example,

$$\frac{1}{7} = 0.142857142857142857...,$$

where the digits 142857 repeat, so 1/7 is periodic, and the period has length 6.

We can look at this expansion in base 10, or in any other base a. The expansion terminates whenever p divides a, otherwise it is periodic. We are concerned here with the properties of its period.

We begin by reducing the problem into a problem that is stated in terms of number theoretic notions. The main result of the paper is that, given a base $a \neq 2$,and an integer $d \neq 2$, there is a prime p such that the length of the period of the expansion $1/p$ is d. There is a prime such that the expansion of $1/p$ has period 2 if and only if $a \neq 2^k - 1$ for any k. There exists no prime p for which $1/p$ has period 6 in base 2. For $d \neq 6$ there exists p such that the period of $1/p$ has length d base 2.

It is not hard to show that the length of the period of the decimal expansion of $1/p$ is no more than $p-1$. More interesting is the problem of when the length is in fact $p-1$, in other words, when $1/p$ has maximal period. To investigate this, we present computer-generated graphs of the density of primes with maximal period in a given base. We prove that if the base is a square number, there are no primes with maximal period. If the base is not a square then the graphs suggest that the density of primes that have maximal period is well defined.

This paper is organized as follows: Section 2 deals with reducing the problem into a number theory problem, section 3 explores the basic properties of cyclotomic polynomials and prove the main result, and section 4 illustrates the heuristics and the graphs related to the density of primes with maximal periods.

Date: March 12, 2007.

2. Restatement of The Problem with Number Theoretic Notions

In this section, we prove that the decimal expansion of $\frac{1}{p}$ is periodic in base a whenever $p \nmid a$ and that the length of the period is the order of $a \pmod{p}$. If $p|a$ then the decimal expansion of $\frac{1}{p}$ in base a truncates.

First consider the case $p|a$ and let $q = \frac{a}{p}$. Then $\frac{1}{p} = \frac{q}{a}$. So the decimal expansion of $\frac{1}{p}$ in base a is $0.q$ and truncates.

Now consider the case $p \nmid a$ and let d be the order of $a \pmod{p}$. Then d is the smallest integer such that $a^d \equiv 1 \pmod{p}$, and there is some integer x such that $a^d - 1 = xp$. We can rearrange the terms to achieve the following expression.

$$\begin{aligned}\frac{1}{p} &= \frac{x}{(a^d - 1)}\\ &= x((\frac{1}{a^d}) + (\frac{1}{a^d})^2 + (\frac{1}{a^d})^3 ...)\\ &= (\frac{1}{a^d})x + (\frac{1}{a^d})^2 x + (\frac{1}{a^d})^3 x...\end{aligned}$$

So the decimal expansion of $\frac{1}{p}$ in base a is $x(0.0...010...010...01...)$, thus $\frac{1}{p}$ is periodic with a period of length d.

3. Background and Proof of the Main Result

The main result of this paper is as follows:

Theorem 3.1. *Given a base a and integer $d \neq 2$ we can find a prime p such that a has order d in $\mathbb{F}_p^*$ unless $a = 2$ and $d = 6$. If $d = 2$ we can find such a prime if and only if $a + 1$ is a not a power of 2.*

Together with our discussion in section 2, this theorem addresses the question, "What are the possible lengths of the repeating string of digits in the decimal expansion of $1/p$?"

We use $a|b$ and $a \nmid b$ to mean a divides b and a does not divide b respectively. $ord_p a$ denotes the order of a modulo the prime number p. $p^k || a$ means $p^k | a$ but $p^{k+1} \nmid a$. $\mathbb{Z}$ denotes the ring of integers, $\mathbb{Z}_+$ positive integers, $\mathbb{F}_p$ the field with p elements, and $\mathbb{Z}[x]$ denotes ring of the polynomials in x with integer coefficients. Φ_n denotes the nth *cyclotomic polynomial* defined as follows:

Definition 3.2. *The cyclotomic polynomials $\Phi_n, n = 1, 2, 3, \ldots$ are the unique irreducible polynomials that satisfy the following formula:*

$$\Phi_n(x) = \prod_{\substack{0<k<n \\ gcd(k,n)=1}} (x - e^{\frac{2i\pi k}{n}})$$

Using the below theorems, it can be shown that the order of a in $\mathbb{F}_p^*$ is the minimum positive integer d such that p divides $\Phi_d(a)$. This observation leads us to investigate the properties of cyclotomic polynomials. The next three theorems are the main theorems that will help us prove our main theorem. Their proofs will follow later in the section.

Theorem 3.3. *Let p be a prime and d be a divisor of $p - 1$. Then the order of a in $\mathbb{F}_p^*$ is d if and only if p divides $\Phi_d(a)$.*

Theorem 3.4. *Let $m,\ n \in \mathbb{Z}_+, m < n$.*

$$\Phi_m\mathbb{Z}[x] + \Phi_n\mathbb{Z}[x] = \begin{cases} q\mathbb{Z}[x] & \text{if } \frac{n}{m} = q^\alpha \text{ where } q \text{ is a prime} \\ \mathbb{Z}[x] & \text{otherwise} \end{cases}$$

Theorem 3.5. *Let p be an odd prime and $p|d$. If $p|\Phi_d(a)$ then $p||\Phi_d(a)$.*

Following identity about the cyclotomic polynomials is going to be useful for the rest of the theorems and lemmata.

Lemma 3.6. *The following identity holds for all n:*

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

Proof. The roots of $x^n - 1$ are the roots of unity: $e^{\frac{2\pi ik}{n}}$ for $k = 0, \ldots, n-1$. So $x^n - 1$ factors as

$$x^n - 1 = \prod_{0 \le k < n} (x - e^{\frac{2i\pi k}{n}}).$$

Then the set of fractions $\{\frac{2i\pi k}{n}|0 \le k < n\}$ is exactly

$$\bigcup_{d'|n} \{\frac{2i\pi kd'}{\frac{n}{d'}d'}|\gcd(k, \frac{n}{d'}) = 1\}$$

and written in reduced form is simply

$$\bigcup_{d|n} \{\frac{2i\pi k}{d}|\gcd(k, d) = 1\}$$

Hence we can group the terms $(x - e^{\frac{2i\pi k}{n}})$ by denominator of the exponent and see the equivalence

$$x^n - 1 = \prod_{0 \le k < n} (x - e^{\frac{2i\pi k}{n}}) = \prod_{d|n} \Phi_d(x)$$

□

Lemma 3.7.

$$x^{p-1} - 1 \equiv \prod_{1 \le i \le p-1} (x - i)\ (mod\ p)$$

Proof. The set $S = \{a \in \mathbb{Z}|0 < a < p\}$ is a group under the operation of multiplication in $\mathbb{F}_p$. Hence the order, ord_pa, of each element of S divides the order, $p - 1$, of the group. This means that for every $0 < a < p$, we have $a^{p-1} \equiv 1(mod\ p)$. In other words, each integer $0 < a < p$ is a root of the polynomial $x^{p-1} - 1$ modulo p. From this, we conclude that $(x-a)|(x^{p-1}-1)(mod\ p)$ for every $0 < a < p$. Hence $(x-1)\ldots(x-(p-1))|x^{p-1}-1(mod\ p)$. Since the degree of $(x-1)\ldots(x-(p-1))$ is $p-1$, and the coefficients of the leading terms agree, it must be true that $x^{p-1} - 1 \equiv (x-1)\ldots(x-(p-1))(mod\ p)$. □

The idea behind the proof of the main result is to choose a prime factor p of $\Phi_d(a)$ and combine Theorems 3.3 and 3.4 above to relate the ord_pa and d. Finally, we use Theorem 3.5 to show that if $d \neq ord_pa$, then $p = \Phi_d(a)$ and a size argument shows that $p = \Phi_d(a)$ is almost always impossible; hence, $d = ord_pa$ except for $a = 2$, $d = 6$ and $p = 3$.

We begin by proving the first step, Theorem 3.3.

Proof of 3.3: Let d be the order of $a \pmod p$. Then $a^d \equiv 1 (\mathrm{mod}\ p)$, so $p|(a^d-1)$. By definition,

$$a^d - 1 = \prod_{m|d} \Phi_m(a),$$

$p|\Phi_m(a)$ for some $m|d$.

Assume that $m < d$. Then $p|\Phi_m(a)$ and $\Phi_m(a)|(a^m-1)$ so by transitivity, $p|(a^m-1)$. The statement $p|(a^m-1)$ is equivalent to $a^m \equiv 1(mod\, p)$, which contradicts the initial assumption that d is the order of $a(mod\ p)$. Hence $m = d$ and $p|\Phi_d(a)$.

To prove the other direction, let $p|\Phi_d(a)$. By definition, $p|(a^d-1)$, so $ord_p a|d$. Furthermore, $p|\Phi_d(a)$ implies that a is a root of $\Phi_d(x)$ in $\mathbb{F}_p$, so $(x-a)|\Phi_d(x)$ in $\mathbb{F}_p$.

Let a have order $k < d$. Then $a^k \equiv 1(mod\ p)$, so a is a root of $x^k - 1$ in $\mathbb{F}_p$. This means that $(x-a)|(x^k-1)$ in $\mathbb{F}_p$, or equivalently

$$(x-a)|\prod_{m|k} \Phi_m(x) \text{ in } \mathbb{F}_p$$

Then $(x-a)|\Phi_m(x)$ in $\mathbb{F}_p$ for some $m|(p-1)$ and $m < d$. Recall that $(x-a)|\Phi_d(x)$ in $\mathbb{F}_p$. Lemma 3.7 states that $x^{p-1} - 1 \equiv (x-1)\dots(x-(p-1)) \pmod p$, or equivalently,

$$\prod_{w|n} \Phi_w(x) \equiv (x-1)\dots(x-(p-1)) \mod p$$

Since $(x-a_0)$ is irreducible for all a_0, each term $(x-a_0)$ divides exactly one of the cyclotomic polynomials on the left hand side. Since $m|(p-1)$ and $d|(p-1)$, it is not possible that $(x-a)|\Phi_m(x)$ and $(x-a)|\Phi_d(x)$. This is a contradiction, so it must be true that $k = d$ and $ord_p a = d$. □

Theorem 3.4, which is the next step toward the main result, relies on several lemmata providing further results concerning cyclotomic polynomials.

Lemma 3.8. *Let $m, n \in \mathbb{Z}_+$. Then*

$$(x^m-1)\mathbb{Z}[x] + (x^n-1)\mathbb{Z}[x] = (x^{gcd(m,n)}-1)\mathbb{Z}[x]$$

Proof. Let $h(x) \in \mathbb{Z}[x]$ be the polynomial of the smallest degree such that

$$h(x) = (x^n-1)f(x) + (x^m-1)g(x)$$

for some $f(x), g(x) \in \mathbb{Z}[x]$. Equivalently, we can write $h(x) = \gcd((x^n-1),(x^m-1))$. Notice that

$$\begin{aligned}\gcd((x^n-1),(x^m-1)) &= \gcd((x^m-1),(x^n-1) - x^{n-m}(x^m-1)) \\ &= \gcd((x^m-1),(x^{n-m}-1))\end{aligned}$$

We can apply the Euclidean Algorithm on n and m by subtracting m from n repeatedly until the remainder r is less than m, then subtracting r from m repeatedly and so on, concluding with

$$h(x) = \gcd((x^n-1),(x^m-1)) = (x^{gcd(m,n)}-1).$$

Hence $(x^{gcd(m,n)}-1) \subset (x^m-1)\mathbb{Z}[x] + (x^n-1)\mathbb{Z}[x]$.

Since $h(x)$ is the polynomial of the smallest degree in $(x^m-1)\mathbb{Z}[x]+(x^n-1)\mathbb{Z}[x]$ and $\mathbb{Z}[x]$ is a principal ideal domain, $h(x)$ must generate $(x^m-1)\mathbb{Z}[x]+(x^n-1)\mathbb{Z}[x]$. So

$$(x^m-1)\mathbb{Z}[x]+(x^n-1)\mathbb{Z}[x]=(x^{gcd(m,n)}-1)\mathbb{Z}[x].$$

□

Lemma 3.9. *Let $m,n\in\mathbb{Z}_+$ and $\frac{n}{m}=p^\alpha$ where p is a prime. We have the following equalities modulo p.*

$$\begin{aligned}\Phi_n(x) &\equiv \Phi_m(x)^{p^\alpha}(mod\ p) && \textit{if } p|m\\ \Phi_n(x) &\equiv \Phi_m(x)^{p^\alpha-p^{\alpha-1}}(mod\ p) && \textit{if } p\nmid m\end{aligned}$$

Proof. It follows from the definition 3.2 of cyclotomic polynomials that

$$\begin{aligned}\Phi_n(x) &= \Phi_m(x^{p^\alpha}) && \text{if } p|m\\ \Phi_n(x) &= \frac{\Phi_m(x^{p^\alpha})}{\Phi_m(x^{p^{\alpha-1}})} && \text{if } p\nmid m\end{aligned}$$

Looking at this in $\mathbb{F}_p$ gives

$$\begin{aligned}\Phi_n(x) &\equiv \Phi_m(x)^{p^\alpha}(mod\ p) && \text{if } p|m\\ \Phi_n(x) &\equiv \Phi_m(x)^{p^\alpha-p^{\alpha-1}}(mod\ p) && \text{if } p\nmid m\end{aligned}$$

□

We are now ready to present the proof of Theorem 3.4. Recall that the statement of Theorem 3.4 is that for $m,\ n\in\mathbb{Z}_+, m<n$.

$$\Phi_m\mathbb{Z}[x]+\Phi_n\mathbb{Z}[x]=\begin{cases} q\mathbb{Z}[x] & \text{if } \frac{n}{m}=q^\alpha \text{ where } q \text{ is a prime}\\ \mathbb{Z}[x] & \text{otherwise}\end{cases}$$

Proof of 3.4 We divide the proof onto three cases.

Case 1: Let $m,n\in\mathbb{Z}$ and $m\nmid n$.

From Lemma 3.8, there exist polynomials $f(x),g(x)\in\mathbb{Z}[x]$ such that

$$(x^n-1)f(x)+(x^m-1)g(x)=(x^{gcd(m,n)}-1)$$

Equivalently,

$$\prod_{w|n}\Phi_w(x)f(x)+\prod_{u|m}\Phi_u(x)g(x)=\prod_{v|gcd(m,n)}\Phi_v(x)$$

Clearly, if $v|gcd(m,n)$ then $v|n$ and $v|m$ so

$$\Phi_v(x)|\prod_{w|n}\Phi_w(x) \text{ and } \Phi_v(x)|\prod_{u|m}\Phi_u(x).$$

for all $v|gcd(m,n)$. Furthermore, since m doesn't divide n, $v|gcd(m,n)\Rightarrow v<m<n$ so

$$\Phi_n(x)|\frac{\prod_{w|n}\Phi_w(x)}{\prod_{v|gcd(m,n)}\Phi_v(x)} \text{ and } \Phi_m(x)|\frac{\prod_{u|m}\Phi_u(x)}{\prod_{v|gcd(m,n)}\Phi_v(x)}.$$

Then there are polynomials $\tilde{f}(x),\tilde{g}(x)\in\mathbb{Z}[x]$ such that

$$\Phi_n(x)\tilde{f}(x)+\Phi_m(x)\tilde{g}(x)=1$$

so $\Phi_m\mathbb{Z}[x] + \Phi_n\mathbb{Z}[x] = \mathbb{Z}[x]$.

Case 2: Let $m, n \in \mathbb{Z}$, $m|n$, and $p, q|\frac{n}{m}$ where p and q are distinct primes.

Because $\Phi_p(x) \in \mathbb{Q}[x]$, there exists a polynomial $f(x)$ such that

$$\Phi_p(x) - \Phi_p(a) = f(x)(x - a)$$

Reducing the above expression and evaluating at $a = 1$ yields

$$\frac{x^p - 1}{x - 1} - f(x)(x - 1) = p.$$

Substituting $x = y^{\frac{n}{p}}$, we have

$$\frac{y^n - 1}{y^{\frac{n}{p}} - 1} - f(y^{\frac{n}{p}})(y^{\frac{n}{p}} - 1) = p.$$

Notice that $\Phi_n(y)|y^n - 1$ and $\Phi_n(y) \nmid y^{\frac{n}{p}} - 1$. Similarly, $\Phi_m(y)|y^{\frac{n}{p}} - 1$. So we can rewrite the above expression as

$$g(y)\Phi_n(y) + h(y)\Phi_m(y) = p$$

for some $g(y), h(y) \in \mathbb{Q}[y]$. We can make the same argument for q, so we can find $\tilde{g}(y), \tilde{h}(y) \in \mathbb{Q}[y]$ such that

$$\tilde{g}(y)\Phi_n(y) + \tilde{h}(y)\Phi_m(y) = q.$$

But p and q are distinct primes, so $\gcd(p, q) = 1$ and there exist integers a and b such that $ap + bq = 1$. So

$$(ag(y) + b\tilde{g}(y))\Phi_n(y) + (ah(y) + b\tilde{h}(y))\Phi_m(y) = 1.$$

so $\Phi_m\mathbb{Z}[x] + \Phi_n\mathbb{Z}[x] = \mathbb{Z}[x]$.

Case 3: Let $m, n \in \mathbb{Z}$, $m|n$, and $\frac{n}{m} = p^\alpha$ for some prime p .

Applying the argument of Case 2, it is clear that we can find polynomials $g(y), h(y) \in \mathbb{Q}[y]$ so that

$$g(y)\Phi_n(y) + h(y)\Phi_m(y) = p.$$

Then $p\mathbb{Z}[x] \subset \Phi_m\mathbb{Z}[x] + \Phi_n\mathbb{Z}[x]$. In order to show the opposite inclusion, recall from Lemma 3.9 that

$$\begin{aligned} &\Phi_n(x) \equiv \Phi_m(x)^{p^\alpha}(mod\ p) &&\text{if } p|m \\ &\Phi_n(x) \equiv \Phi_m(x)^{p^\alpha - p^{\alpha-1}}(mod\ p) &&\text{if } p \nmid m. \end{aligned}$$

Hence, $\Phi_m(x)|\Phi_n(x)$ (mod p). If there were an element $c \in \mathbb{Z}$ and polynomials $A(x), B(x) \in \mathbb{Z}[x]$ such that $A(x)\Phi_n(x) + B(x)\Phi_m(x) = c$ then $A(x)\Phi_n(x) + B(x)\Phi_m(x) = c$ (mod p). Since $\Phi_m(x)$ divides the left side of the equation, it must divide c (mod p). But $c \in \mathbb{Z}$ so $\Phi_m(x)|c$ (mod p) if and only if $c \equiv 0$ (mod p). Hence, $p|c$ and $p\mathbb{Z}[x] \supset \Phi_m\mathbb{Z}[x] + \Phi_n\mathbb{Z}[x]$.□

The third and last step toward the main result follows directly from two Lemmas. Recall the statement of Theorem 3.5, which says that for p an odd prime such that $p|d$ and $p|\Phi_d(a)$, we have $p||\Phi_d(a)$.

Lemma 3.10. *Let p be an odd prime and a an integer such that $p|a-1$. If $p^\alpha||a-1$ and $p^\beta||n$, then $p^{\alpha+\beta}||a^n-1$*

Proof. The proof is based on induction on β. For $\beta = 0$ the proof is obvious. Assume that the hypothesis holds for β. Let $a^n - 1 = p^{\alpha+\beta}k, p \nmid k$. The induction step is as follows:

$$\begin{aligned} a^{np} - 1 &= ((a^n-1)+1)^p - 1 \\ &= (p^{\alpha+\beta}k+1)^p - 1 \\ &= \binom{p}{p}(p^{\alpha+\beta}k)^p + \binom{p}{p-1}(p^{\alpha+\beta}k)^{p-1} + \cdots + \binom{p}{1}p^{\alpha+\beta}k \end{aligned}$$

In the above sum all the terms are divisible by $p^{\alpha+\beta+2}$ except for the last term, which is divisible by $p^{\alpha+\beta+1}$. Therefore, the whole sum is exactly divisible by $p^{\alpha+\beta+1}$. □

Lemma 3.11. *If p divides $\Phi_m(a)$ and not m, then m is the order of a mod p.*

Proof. Assume that d is the order of a mod p. Then $p|\Phi_d(a)$ by 3.3. We also know that $p|\Phi_m(a)$. Therefore, $\Phi_m\mathbb{Z}[x] + \Phi_d\mathbb{Z}[x]$ can not be $\mathbb{Z}[x]$. If $m \neq d$ then by 3.4 either d/m or m/d must be a power of p. Since both of the cases are impossible, we deduce that $m = ord_p a$. □

Lemma 3.12. *Let p be an odd prime, m an integer such that $p \nmid m$, $\alpha, \beta \geq 1$ and $p^\alpha||\Phi_m(a)$.If $d = p^\beta m$, then $p||\Phi_d(a)$.*

Proof. We prove the statement for $\beta = 1$. Let $d = mp$. By 3.9 $\Phi_{mp}(x) \equiv \Phi_m(x)^{p-1}(mod\ p)$. Since $p|\Phi_m(a)$ we get $p|\Phi_d(a)$. Since $p \nmid m$ and $p|\Phi_m(a)$ by 3.11 it must be that $m = ord_p a$. Therefore $p^\alpha||a^m - 1$ (because among the cyclotomic factors of $a^m - 1$ only $\Phi_m(a)$ is divisible by p). It follows from 3.10 that $p^{\alpha+1}||a^d - 1$. Since $p|\Phi_d(a)|\frac{a^d-1}{\Phi_m(a)}$ we get $p||\Phi_d(a)$. The induction step $\beta \longrightarrow \beta + 1$ is very similar and left to the reader. □

Proof of 3.5. Let $d = p^\beta m,\ p \nmid m$. Since $\Phi_d(x) \equiv \Phi_m(x)^{p^\beta - p^{\beta-1}}(mod\ p)$ from Lemma 3.9 it follows that $p|\Phi_m(a)$. It follows from 3.12 that $p||\Phi_d(a)$.□

Notice that Theorem 3.5 only covers the cases in which p is odd. The following lemma proves the equivalent result for $p = 2$.

Lemma 3.13. *Let $d > 2$ and a an integer. Then $\Phi_d(a)$ is either odd or $2||\Phi_d(a)$.*

Proof. If a is even then $\Phi_d(a)$ is odd b/c $\Phi_d(0) = 1$. If a is odd then $\Phi_d(a) \equiv \Phi_d(1)(mod\ 2)$ and we know that $\Phi_d(1)$ is 1 unless $d = p^k$ in which case $\Phi_d(1) = p$. Therefore we just need to consider $d = 2^k,\ k \geq 2$, in which case $\Phi_{2^k}(x) = x^{2^{k-1}} + 1$. It's easy to show that $\Phi_{2^k}(a) = 2(mod\ 4)$ if a is odd. Therefore $\Phi_d(a)$ is odd unless a is odd and $d = 2^k$, in which case $2||\Phi_d(a)$. □

We are finally prepared to prove the main result for $a, d > 2$.

Proof of 3.1 We show that there is a prime divisor p of $\Phi_d(a)$ for which $ord_p a = d$. Let p be a prime divisor of $\Phi_d(a)$ and $m = ord_p a$ and assume that $d \neq m$. It follows from 3.3 that $p|\Phi_m(a)$. Consider the ideal $U = \Phi_m\mathbb{Z}[x] + \Phi_d\mathbb{Z}[x]$. We know that $U \neq \mathbb{Z}[x]$ because $p|\Phi_m(a)$ *and* $p|\Phi_d(a)$. From 3.4 it follows that either $\frac{m}{d}$ or $\frac{d}{m}$ is a power of p. The former is impossible because $m \leq p-1$. In the case of the latter, $m|p-1$ so p is the greatest prime divisor of d.

If $\Phi_d(a)$ has a divisor q, $q \neq p$, then let $m' = ord_q a$ we can apply the same argument to show that $d \neq m' \Rightarrow q$ is the greatest prime divisor of d. As p and q cannot both be greatest prime divisors, either $d = m$ or $d = m'$. Hence there is only one prime divisor p_0 of $\Phi_d(a)$, whether p or q, for which $ord_{p_0} a = d$.

If $\Phi_d(a)$ does not have a divisor q, $q \neq p$, then $\Phi_d(a) = p^\alpha$. Let $d > 2$. By theorem 3.5 and 3.13, we must have $\Phi_d(a) = p$. As concluded above, p is the greatest prime divisor of d. Recall the definition of $\Phi_d(a)$,

$$\Phi_n(x) = \prod_{\substack{0<k<n \\ gcd(j,n)=1}} (a - e^{\frac{2i\pi k}{n}})$$

Examining each term as an element of $\mathbb{C}$, we have

$$|\Phi_n(x)| = \prod_{\substack{0<k<n \\ gcd(j,n)=1}} |a - e^{\frac{2i\pi k}{n}}|$$

Assume that $a > 2$ then $|a - e^{\frac{2i\pi k}{n}}| > 2$ so $|\Phi_n(x)| > 2^{\phi(d)}$ where $\phi(d)$ represents the number of integers $m < d$ such that $\gcd(m, d) = 1$. Since $p|d$, we have $p - 1|\phi(d)$, so $|\Phi_n(x)| > 2^{p-1}$. But $|\Phi_n(x)| = |p| = p$ so $p > 2^{p-1}$. But $p \leq 2^{p-1}$ for all p, so this is impossible. Hence we must have $m = d$.

Now assume that $a = 2$, $p|n$, $\Phi_n(2) = p$. Let $\omega = e^{2i\pi/n}$. We have:

$$\begin{aligned}\Phi_n(2) &= \prod_{gcd(l,n)=1,\ l<n/2} (2-\omega^l)(2-\omega^{-l}) \\ &= \prod_{gcd(l,n)=1,\ l<n/2} (5 - 2\cos(\frac{2\pi l}{n})) \\ &\geq 3^{\Phi(n)/2} \geq 3^{\frac{p-1}{2}}\end{aligned}$$

We find that if $\Phi_n(2) = p$ and $p|n$ then $3^{\frac{p-1}{2}} \leq p$. This only holds if $p = 2$ or $p = 3$. It also follows from above that if $p = 2$ then $\Phi(n) < 2$ so n has to be 2. We see that $\Phi_2(2) = 3$ so this is not a solution. If $p = 3$ then $\Phi(n) \leq 2$. This leads us to the following possible solutions $(n,\ p,\ a)$: $(6,\ 3,\ 2)$, $(4,\ 3,\ 2)$, $(3,\ 3,\ 2)$. Trial and error shows that the only solution is $n = 6$, $p = 3$ and $a = 2$ ($\Phi_6(2) = 3$). Indeed there is no prime p for which 2 has order 6 in $\mathbb{F}_p$. □

4. Distribution of Prime Numbers for which a is a Primitive Root

Although the values of the order of the base a modulo prime numbers can attain arbitrary values, it is an interesting question to study the distribution of primes such that a has some *special* order modulo these primes. One such approach could be to look for all prime numbers p such that a has order k modulo p for some fixed positive integer k. However, all such primes must be divisors of $n^k - 1$, so there are finitely many of them.

A more interesting question arises if we look at the primes which give the *maximal* order of a. As we know, the maximal order is $p-1$ for prime number p, and a has order $p-1$ if and only if it is a primitive root modulo p. Let us denote the set of all prime numbers for which a is a primitive root as $S(a)$. We would like to study the *density* of this set within the set of all prime numbers. The density can be defined in a natural way as follows:

$$D(n, N) = \frac{\#\{n \in S(a) \mid n \leq N\}}{\#\{n \in \mathbb{P} \mid n \leq N\}}$$

$$D(n) = \lim_{N \to \infty} D(n, N)$$

If the sequence under the limit converges, then the density is well-defined, and it tells us the "probability" that for a randomly chosen prime number, a is a primitive root. Note, it is not even immediate whether $S(a)$ is finite or not. In fact, one might easily notice the following fact:

Proposition 4.1. *If a is a perfect square, then $S(a)$ is empty.*

Proof: Assuming $a = b^2$, we obtain $a^{\frac{p-1}{2}} \equiv b^{p-1} \equiv 1 \pmod{p}$ from Fermat's theorem. □

Using computational software (see section 6 for the code), we can plot the sequence elements under the limit, and observe that the sequence appears to stabilize. Moreover, after calculating the final probabilities for various values of n we also notice that this density value is the same for the majority of the numbers. This observation led us to the following conjecture, first discovered by Artin in 1927 [1]:

Conjecture 4.2 (Artin)**.** *For any positive integer a which is not a perfect square, the set $S(a)$ is infinite. Moreover, if a is a squarefree number, then the density of $S(a)$ in prime numbers is independent of a.*

The constant mentioned in the conjecture carries the name *Artin's constant* and it is equal to

$$C_A = \prod_{k=1}^{\infty} \left(1 - \frac{1}{p_k(p_k - 1)}\right) = 0.3739558136\ldots,$$

where p_k is the k-th prime number.

There have been numerous attempts to prove this conjecture, and it is commonly believed to be true. However, apart from the conditional results relying on the Generalized Riemann Hypothesis, it is not known whether the qualitative form holds, i.e. given any positive integer a whether the set $S(a)$ is infinite [2]. An interesting non-constructive result by Heath-Brown states that there could be at most *three* squarefree numbers a with finite set $S(a)$, but unfortunately, the proof does not show what these exceptions might be.

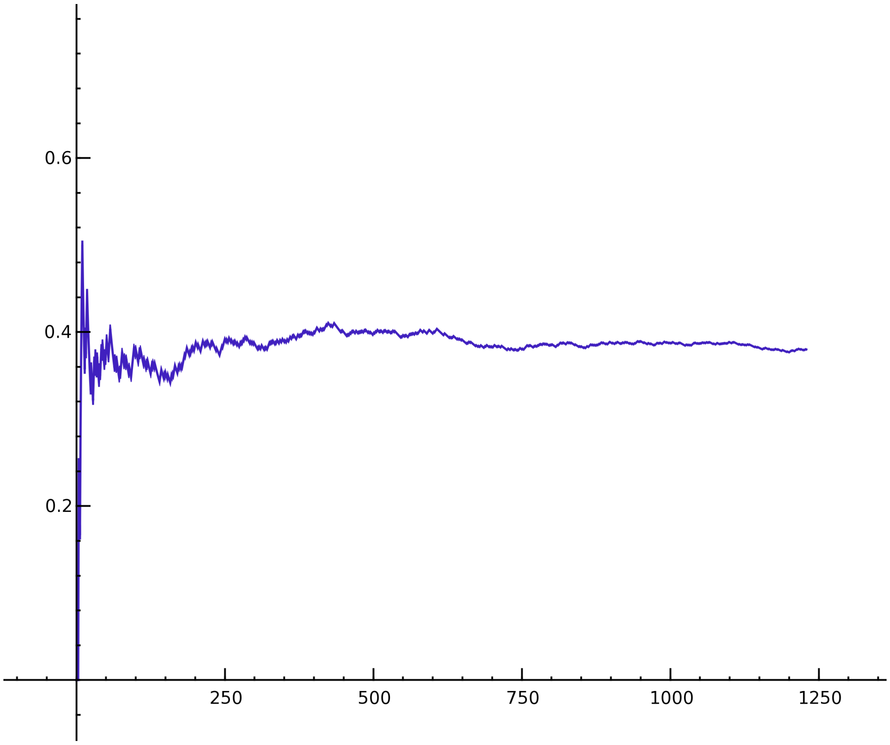

FIGURE 1. The plot of intermediate values of $D(10, p_i)$ for prime numbers $p_i \leq 10000$. The horizontal axis shows the index i of the prime number.

It is important to understand the reasoning that led Artin to his conjecture as it might give us some insight into why the conjecture might hold. In particular, it can provide a "heuristic" explanation of the Artin's constant. His argument relies on certain probabilistic assumptions and employs notions of algebraic number theory. We would like to explain the details of his argument below.

Proposition 4.3. *For any positive integer a and a prime number p the following statements are equivalent:*

(i) *a is a primitive root modulo p;*
(ii) *for any prime divisor q of $p-1$, $a^{\frac{p-1}{q}} \not\equiv 1 \pmod p$;*
(iii) *for any prime divisor q of $p-1$, $x^q - a$ is irreducible modulo p.*

Proof: Let us first show the equivalence of (i) and (ii). If a has order d which is less than $p-1$, then we can pick a prime divisor q of $\frac{p-1}{d}$ as d divides $p-1$ by Fermat's theorem. In that case, $a^{\frac{p-1}{q}}$ is a power of a^d and it is 1 (mod p). On the other hand, a is a primitive root if and only if $p-1$ is the minimal power of a which is congruent to 1 modulo p.

Now we would like to prove the rest by showing that the negatives of (ii) and (iii) are equivalent. If $x^q - a$ has a root modulo p, then a is a q-th power and so $a^{\frac{p-1}{q}} \equiv 1 \pmod p$. For the other side, note that if $a^{\frac{p-1}{q}} \equiv 1 \pmod p$ then if we write $a = g^d$ for the primitive

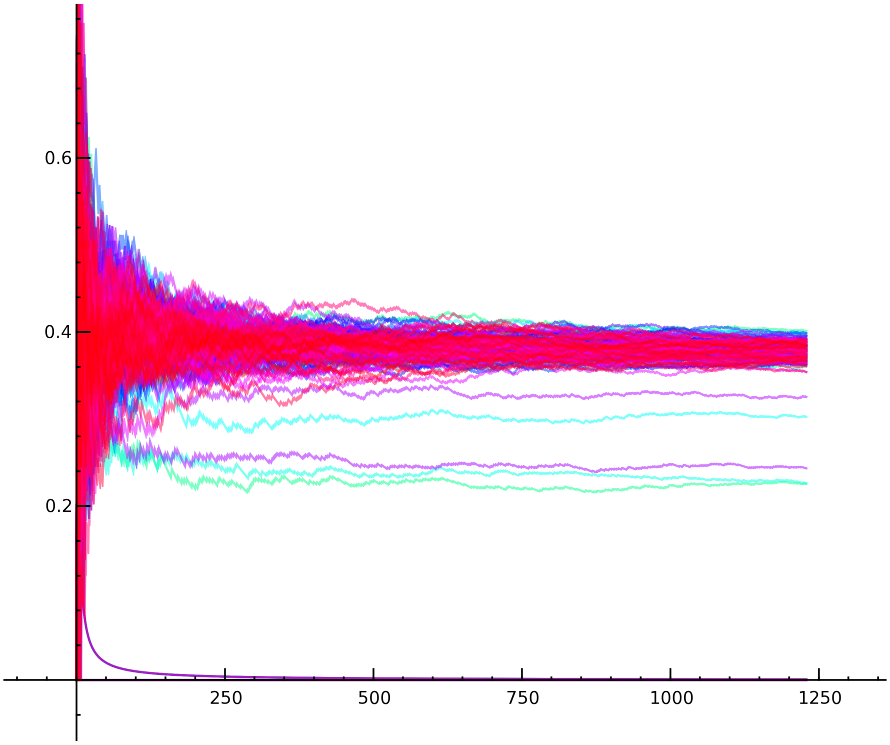

FIGURE 2. The composite plot of intermediate values of $D(a, p_i)$ for a range of values of a up to 200 and $p_i \leq 10000$. The color indicates relative order of a with red being the highest one.

root g modulo p, the power d must be divisible by q, and so $g^{\frac{d}{q}}$ is a root of the polynomial. □

Given a prime number p, we are interested in the factorization of the prime ideal generated by p in certain algebraic number fields. The following theorem [3] gives us an easy way to factor ideals in extensions:

Theorem 4.4 (Kummer)**.** *Suppose R is a Dedekind ring with quotient field K, and R' is its integral closure in a finite dimensional extension L of K. Let $\mathfrak{p}$ be a nonzero prime ideal of R. Suppose there is an element $\alpha \in L$ such that the integral closure of $R_{\mathfrak{p}}$ in L is $R_{\mathfrak{p}}[\alpha]$. Let $f(x)$ be the minimal polynomial of α over $R_{\mathfrak{p}}$. Suppose $f(x)$ factors modulo $\mathfrak{p}$ after reduction of its coefficients as $f(x) \equiv \prod g_i(x)^{e_i}$ where $g_i(x)$ are irreducible polynomials. Then:*

$$\mathfrak{p}R = \prod (\mathfrak{p}, g_i(\alpha))^{e_i}$$

where the ideals $(\mathfrak{p}, g_i(\alpha))$ in the factorization are prime and distinct.

Here we use the notation $R_{\mathfrak{p}}$ to denote a localization of the ring R at the multiplicative set $R - \mathfrak{p}$. An interesting implication of using localization is that if $L = K[\theta]$ for some element $\theta \in R'$ and the ideal $\mathfrak{p}$ does not contain the discriminant $\Delta(\theta)$, then we have $R'_{\mathfrak{p}} = R_{\mathfrak{p}}[\theta]$ and we can apply the theorem. A reader may refer to [3] for the proof of this fact.

Proposition 4.5. *Given a positive integer a and prime numbers p and q such that p does not divide a, the following statements are equivalent:*

(i) $p \equiv 1$ *(mod q) and* $a^{\frac{p-1}{q}} \equiv 1$ *(mod p);*

(ii) *principal ideal generated by p splits completely in* $K_q = \mathbb{Q}(\sqrt[q]{1}, \sqrt[q]{a})$.

Proof: (i) => (ii). By the previous proposition, the polynomial $x^q - a$ has a root modulo p. We can easily obtain all the other roots through multiplication by a nontrivial root of $x^q - 1$ modulo p as there exists one for q being a divisor of $p - 1$. Hence, $x^q - a$ splits completely modulo p. The discriminant of $\sqrt[q]{a}$ can be calculated by the following well-known formula:

$$\Delta(\sqrt[q]{a}) = (-1)^{\frac{q(q-1)}{2}} N(\frac{d}{dx}(x^q - a) \mid_{x=\sqrt[q]{a}}) = (-1)^{\frac{(q+2)(q-1)}{2}} q^q a^{q-1}$$

Since it is not divisible by p, we can use Theorem 4.4 to deduce that p splits completely in the ring of integers of $F = \mathbb{Q}(\sqrt[q]{a})$. Finally, for any prime ideal $\mathfrak{p}$ in the factorization, we can repeat the same reasoning for the polynomial $x^q - 1$ and the field extension K_q over F. After combining the two factorizations, we deduce that p splits completely in K_q.

(ii) => (i). Given that p splits completely in K_q, it must also split completely in the subfields $\mathbb{Q}(\sqrt[q]{1})$ and $\mathbb{Q}(\sqrt[q]{a})$. By Theorem 4.4 and unique factorization of ideals, the polynomials $x^q - a$ and $x^q - 1$ must both split completely modulo p. The conditions of (i) follow directly in the same way as above. □

As a direct consequence of the above propositions, we have:

Proposition 4.6. *a is a primitive root modulo p if and only if p does not split completely in* $K_q = \mathbb{Q}(\sqrt[q]{1}, \sqrt[q]{a})$ *for any prime q.*

Now we note an implication of the Chebotarev theorem [3] on the splitting behavior of primes in field extensions. The notion of density for a subset of prime numbers is the same used before.

Theorem 4.7 (Chebotarev)**.** *The density of primes p which split completely in a Galois extension K of $\mathbb{Q}$ is* $\frac{1}{[K:\mathbb{Q}]}$.

By this theorem, the probability that a given prime p does not split completely in K_q for some prime q is:

$$1 - \frac{1}{[K_q : \mathbb{Q}]}$$

Therefore, one would expect that the density of primes for which a is a primitive root is a product of such probabilities over all fields K_q for prime integers q:

$$\prod_{q \in \mathbb{P}} (1 - \frac{1}{[K_q : \mathbb{Q}]})$$

The latter expression can be used to calculate the constant C_A. Indeed, in a generic case the degree of K_q over $\mathbb{Q}$ is $q(q-1)$ since both polynomials $x^{q-1} + x^{q-2} + \ldots + 1$ and $x^q - a$ are irreducible (here a is not a q-th power.) If a has a square divisor, then some of the fields K_q have a lower degree, so that the constant needs a rational correction factor to cover integers a which are not squarefree. Looking at the statistical data we collected, one can notice on the plots that the density for some of these integers a is lower than C_A and in fact, it is a rational multiple of C_A.

In conclusion, the last step of the argument given above is rather questionable as it relies on the independence of the infinite number of probabilities over fields K_q, and that prevents the above reasoning to become a valid proof.

5. Group Work

We decided to break our work as follows. Introduction and section 2 were written by Shelly, outlines of the theorems are written by Nizam. In section 3, first half of the proofs were written by Shelly and the second half of the proofs were written by Nizam. Kuat wrote section 4 including the plots and the code to generate them.

6. Program Code

The following source code is written for *SAGE* open source math software, which is well-suitable for number theoretical computations.

The software package can be obtained at:
http://modular.math.washington.edu/sage/.

The complete source code can be obtained at:
http://mit.edu/kuat/www/18821.

```
""" Excerpt from utility methods to study the Artin's conjecture"""

def get_order(n, p):
        """Return the order of $n$ in the group $ZZ/pZZ$"""
        F = GF(p)
        k = F(n).multiplicative_order()
  return k

def get_orders(n, max):
        """Returns the list of orders of $n$ for primes up to $max$"""
        L = []
        for p in prime_range(max):
                if not ZZ(p).divides(n):
                        L.append(get_order(n, p))
        return L

def order_probability(n, max):
        """Returns a line showing the asymptotic probability that a prime has maximal order
            for given $n$"""
        count = 0
        max_count = 0
        L = [[0,0]]
        for p in prime_range(max):
                count = count + 1
                if not ZZ(p).divides(n):
                        k = get_order(n, p)
                        if k == (p - 1):
                                max_count = max_count + 1
                L.append([count, max_count / count])
        print "Last proportion: ", max_count / count
        return L

def plot_probability(n, max):
        return line(order_probability(n, max), rgbcolor=(1/4, 1/8, 3/4))

def get_sorted_orders(n, max):
        """Outputs the set of values which the order $n$ can take with respect to primes up
            to $max$"""
        L = list(set(get_orders(n, max)))
        L.sort()
        return L

def possible_order(n, max):
        """Checks if every number up to $max$ is an order of $n$ for some prime; outputs all
             invalid samples"""
        R = []
        for k in range(2, max):
                print "Checking order ", k
                L = (n^k - 1).factor()
                check = false
                for t in L:
                        p = t[0]
                        if k == get_order(n, p):
                                check = true
                                print "Found prime factor: ", p
                                break
                if not check:
                        R.append(k)
        return R

def get_primes(n, d):
        """Returns a list of primes for which $n$ has order $d$ modulo that prime"""
        primes = map(lambda x: x[0], cyclotomic_polynomial(d)(n).factor())
        divisors = map(lambda x: x[0], Integer(d).factor())
        s = set(primes).difference(set(divisors))
        return list(s)
```

References

[1] R. Murty, "On Artin's Conjecture," *J. of Number Theory* **16** (1983), 147-168.

[2] Mathworld on-line encyclopedia. Accessed on March 12, 2007.
http://www.mathworld.org.

[3] G.J. Janusz, *Algebraic Number Fields.* Vol. 7. Graduate Studies in Mathematics. Amer. Math. Soc.