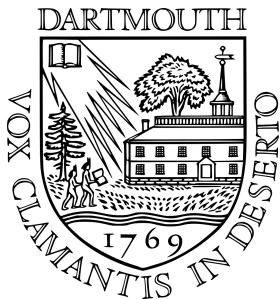


Artin's Primitive Root Conjecture



Lola Thompson

Dartmouth College

December 3, 2010

Introduction



In *Disquisitiones Arithmeticae*, Gauss examined the period length of the repeating decimals arising from numbers of the form $\frac{1}{p}$, with p prime.

Example:

- $\frac{1}{7} = 0.\overline{142857}$ has period length 6.

Introduction



In *Disquisitiones Arithmeticae*, Gauss examined the period length of the repeating decimals arising from numbers of the form $\frac{1}{p}$, with p prime.

Example:

- $\frac{1}{7} = 0.\overline{142857}$ has period length 6.
- $\frac{1}{11} = 0.\overline{09}$ has period length 2.

Introduction

For $p \neq 2, 5$, he observed that the decimal expansions for $\frac{1}{p}$ are purely periodic and the length of the period is the smallest integer k for which

$$10^k \equiv 1 \pmod{p}.$$

In other words, the period length will always divide $p - 1$ and it will be equal to $p - 1$ if 10 is a primitive root mod p .

Gauss created a table containing several examples of primes p for which $\frac{1}{p}$ has period length $p - 1$. He conjectured that there are infinitely many primes p with this property, but was unable to prove his conjecture.

Introduction

It is natural to ask the more general question: “For which integers a are there infinitely many primes p such that a is a primitive root modulo p ?”

- If we exclude 2, as Gauss did, then all of the groups $(\mathbb{Z}/p\mathbb{Z})^\times$ have even order, so that squares cannot be cyclic generators.

Introduction

It is natural to ask the more general question: “For which integers a are there infinitely many primes p such that a is a primitive root modulo p ?”

- If we exclude 2, as Gauss did, then all of the groups $(\mathbb{Z}/p\mathbb{Z})^\times$ have even order, so that squares cannot be cyclic generators.
- Another obvious value of a that we can exclude is $a = -1$, since -1 has order dividing 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$.

Introduction

It is natural to ask the more general question: “For which integers a are there infinitely many primes p such that a is a primitive root modulo p ?”

- If we exclude 2, as Gauss did, then all of the groups $(\mathbb{Z}/p\mathbb{Z})^\times$ have even order, so that squares cannot be cyclic generators.
- Another obvious value of a that we can exclude is $a = -1$, since -1 has order dividing 2 in $(\mathbb{Z}/p\mathbb{Z})^\times$.
- Thus, a necessary condition on a for there to be infinitely many primes p with a as a primitive root would be that a cannot be a square and $a \neq -1$.

Introduction



In 1927, Artin conjectured that these trivially necessary conditions are also sufficient:

Conjecture

If the integer a is not a square and not -1 , then there are infinitely many primes with a as a primitive root.

Artin's Primitive Root Conjecture (Quantitative Form)

Conjecture

If the integer a is not a square and not -1 , then there are infinitely many primes with a as a primitive root.

Throughout this talk, we shall refer to the statement above as the **qualitative form** of Artin's conjecture. We will also discuss a stronger version, which we shall call the **quantitative form** of Artin's conjecture:

Conjecture

If the integer a is not a square and not -1 , then there is a positive number $A(a)$ such that the number of primes $p \leq x$ with primitive root a is $\sim A(a)\pi(x)$.

The Constant $A(a)$

In most cases, $A(a)$ is a rational number times *Artin's Constant*:

$$A = \prod_{q \text{ prime}} \left(1 - \frac{1}{q(q-1)}\right) = 0.3739558136\dots$$

To find $A(a)$: write $a = a_1 \cdot a_2^2$, where a_1 is square-free. Let h be the largest integer for which a is an h^{th} power. Then, if $h = 1$,

$$A(a) = \begin{cases} A, & \text{if } a_1 \not\equiv 1 \pmod{4} \\ A \left(1 - \prod_{q|a_1} \frac{1}{1+q-q^2}\right) & \text{if } a_1 \equiv 1 \pmod{4} \end{cases}$$

There is a similar (albeit slightly more complicated) formula for $A(a)$ when $h > 1$.

Outline

Introduction

A Naive Heuristic Approach

A Parallel Problem

An Approach Using Kummerian Fields

Artin's Heuristic

Hooley's Proof

What Is Known (and What Isn't)

A Naive Heuristic Approach

To provide some intuition for why the quantitative form of Artin's Conjecture should be true, we'll start with a heuristic argument.

Condition

a is a primitive root $(\text{mod } p) \iff$ for all q dividing $p - 1$, a is not a q^{th} power $(\text{mod } p)$.

For each fixed prime q , we'll compute the density of primes p for which the condition above does not hold.

A Naive Heuristic Approach

In other words, we'll find the density of primes p such that

$$p \equiv 1 \pmod{q} \tag{1}$$

and

$$a^{\frac{p-1}{q}} \equiv 1 \pmod{p}. \tag{2}$$

We'll say that a prime p “fails the q -test” if it satisfies both of these conditions.

A Naive Heuristic Approach

It is not difficult to determine the proportion of primes that “fail the q -test” when p is fixed and a is random. Namely, $\frac{1}{q}$ of all values of a will work.

On the other hand, it is quite difficult to determine this proportion when a is fixed and p varies over all primes that are $\equiv 1 \pmod{q}$.

A Naive Heuristic Approach

For a fixed prime q :

A Naive Heuristic Approach

For a fixed prime q :

- Dirichlet's Theorem on Primes in Arithmetic Progressions implies that $p \equiv 1 \pmod{q}$ occurs with frequency $\frac{1}{\varphi(q)} = \frac{1}{q-1}$.

A Naive Heuristic Approach

For a fixed prime q :

- Dirichlet's Theorem on Primes in Arithmetic Progressions implies that $p \equiv 1 \pmod{q}$ occurs with frequency $\frac{1}{\varphi(q)} = \frac{1}{q-1}$.
- Fermat's Little Theorem implies that $a^{p-1} \equiv 1 \pmod{p}$ if $p \nmid a$. In other words, when $p \nmid a$, $a^{\frac{p-1}{q}}$ is a solution to the equation

$$x^q \equiv 1 \pmod{p}.$$

So, the proportion of primes that satisfy condition (2) is $\frac{1}{q}$.

A Naive Heuristic Approach

If p has a as a primitive root, then conditions (1) and (2) can't occur simultaneously for **any** q .

Thus, we'd expect a natural density of

$$\prod_q \left(1 - \frac{1}{q(q-1)}\right)$$

for primes p for which a is a primitive root mod p .

A Naive Heuristic Approach

Therefore, we'd expect that

$$\begin{aligned} & \#\{p \leq x : a \text{ is a generator (mod } p)\} \\ &= \prod_q \left(1 - \frac{1}{q(q-1)}\right) \frac{x}{\log x} + \text{Some Error Term.} \end{aligned}$$

Why The Heuristic Argument Fails

This **almost** gives the quantitative form of Artin's Conjecture. The problem is that we're not excluding from our product the primes $q > \psi(x)$ which fail the q -test.

The best upper bound that we know for this quantity is c/q , from the Brun-Titchmarsh inequality:

$$\pi(x; q, a) \leq \frac{2x}{\varphi(q) \log \frac{x}{q}}.$$

Unfortunately, this is not good enough.

A Parallel Problem

Our naive approach to Artin's Conjecture may not have worked. However, perhaps a similar problem will shed some light on the issues at hand:

“What is the density of primes p with $p - 1$ squarefree?”

Let π^* denote the number of primes up to x for which $p - 1$ is squarefree.

Mirsky proved that, as $x \rightarrow \infty$,

$$\pi^*(x) \sim A \frac{x}{\log x},$$

where A is Artin's constant!

The New “ q -test”

In this situation, a prime p will fail the “ q -test” if $p \equiv 1 \pmod{q^2}$.

For a fixed prime q , the proportion of primes p for which $p \equiv 1 \pmod{q^2}$ is $\frac{1}{\varphi(q^2)} = \frac{1}{q(q-1)}$.

Thus, the proportion of primes p which don't fail the q -test is $1 - \frac{1}{q(q-1)}$. Along the same lines, we would expect that, if we required $p \not\equiv 1 \pmod{q^2}$ for all primes q , the proportion of remaining primes is

$$\prod_q \left(1 - \frac{1}{q(q-1)} \right).$$

The Point of Departure

So far, our approach to Mirsky's problem looks identical to the approach that we took in the naive heuristic argument. However, in this case we won't run into any problems with our error term.

We will divide our primes q into 3 classes:

- $q < \log \log x$

The Point of Departure

So far, our approach to Mirsky's problem looks identical to the approach that we took in the naive heuristic argument. However, in this case we won't run into any problems with our error term.

We will divide our primes q into 3 classes:

- $q < \log \log x$
- $\log \log x \leq q < x^{\frac{1}{100}}$

The Point of Departure

So far, our approach to Mirsky's problem looks identical to the approach that we took in the naive heuristic argument. However, in this case we won't run into any problems with our error term.

We will divide our primes q into 3 classes:

- $q < \log \log x$
- $\log \log x \leq q < x^{\frac{1}{100}}$
- $q > x^{\frac{1}{100}}$

Our Strategy

We will begin by counting the number of primes $p \leq x$ that don't fail the q test for all values of q in the interval $q < \log \log x$. Afterwards, we'll show that the other values of q don't “mess up” our count from the first interval.

The Region $q < \log \log x$

For all $q < \log \log x$, the congruence $p \equiv 1 \pmod{q^2}$ amounts to a congruence on p modulo M , where $M = \prod_{q < \log \log x} q^2$.

By the Prime Number Theorem, $\log M \sim 2 \log \log x$ for large values of x , so $M < (\log x)^{2+o(1)}$. Thus, we have

$$\#\{p \leq x : p \equiv 1 \pmod{q^2}, q < \log \log x\} \sim \pi(x) \prod_{q < \log \log x} \left(1 - \frac{1}{q-1}\right).$$

As $x \rightarrow \infty$, this is asymptotic to $A\pi(x)$.

The Region $\log \log x \leq q < x^{\frac{1}{100}}$

Now, we'll show that the number of primes that fail the q -test for all values of q in the first region but don't fail the test in the other two regions is $o(\pi(x))$.

Suppose $\log \log x < q < x^{\frac{1}{100}}$. By the Brun-Titchmarsh inequality:

$$\begin{aligned} \#\{p \leq x : p \equiv 1 \pmod{q^2}, \log \log x < q < x^{\frac{1}{100}}\} &\ll \frac{x}{\varphi(q^2) \log(\frac{x}{q^2})} \\ &\ll \frac{x}{q^2 \log x}. \end{aligned}$$

Summing over $q > \log \log x$ shows that this contribution is $\ll \frac{x}{\log x \log \log x} = o(\pi(x))$.

The Region $q > x^{\frac{1}{100}}$

Suppose that $q > x^{\frac{1}{100}}$.

We'll overcount by finding the number of natural numbers (instead of primes) $1 < n \leq x$ that satisfy $n \equiv 1 \pmod{q^2}$. That number is $\leq \frac{x}{q^2}$.

Summing over $q > x^{\frac{1}{100}}$ gives a bound of $\ll x^{.99}$, which is also $o(\pi(x))$.

Thus, we were able to prove Mirsky's Theorem without running into the obstructions that kept us from making the heuristic for Artin's Conjecture into a proof!

An Approach Using Kummerian Fields

Let $K_q := \mathbb{Q}(\zeta_q, a^{1/q})$. From basic properties of Kummerian fields, we know that:

p splits completely in $K_q \iff p \equiv 1 \pmod{q}$ and $a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$.

Thus, we can translate “failing the q -test” into a problem in algebraic number theory.

Chebotarev's Density Function

A special case of the Chebotarev Density Theorem implies that

$$\sum_{\substack{p \leq x \\ p \text{ splits} \\ \text{completely in } K_q}} 1 \sim \frac{1}{[K_q : \mathbb{Q}]} \frac{x}{\log x},$$

as $x \rightarrow \infty$. Thus, if $n(q) = [K_q : \mathbb{Q}]$, we have

$$\sum_{\substack{p \leq x \\ p \text{ does not split} \\ \text{completely in } K_q}} 1 \sim \left(1 - \frac{1}{n(q)}\right) \frac{x}{\log x}.$$

Failure of This Approach

So, we'd expect the density of primes p for which a is a primitive root (mod p) to be

$$\prod_q \left(1 - \frac{1}{n(q)}\right).$$

Failure of This Approach

So, we'd expect the density of primes p for which a is a primitive root (mod p) to be

$$\prod_q \left(1 - \frac{1}{n(q)}\right).$$

- The problem with this approach arises in going from a finite product to an infinite product. As in our naive approach, the error term becomes too large.

Artin's Heuristic

Let m be square-free. Let K_m be the compositum of fields K_q , with $q \mid m$, q prime.

It can be shown that $K_m = \mathbb{Q}(\zeta_m, a^{1/m})$. We want to find the density of primes p that do not split completely in any K_q . In order to compute this, we can do a simple inclusion-exclusion.

Artin's Heuristic

- Start with:

$$1 - \frac{1}{n(2)} - \frac{1}{n(3)} - \frac{1}{n(5)} - \dots$$

Artin's Heuristic

- Start with:

$$1 - \frac{1}{n(2)} - \frac{1}{n(3)} - \frac{1}{n(5)} - \dots$$

- The subtraction above double-counts primes that split completely in both K_i and K_j , so we need to add back terms to account for these primes. So, we'll add

$$\frac{1}{n(6)} + \frac{1}{n(10)} + \frac{1}{n(14)} + \frac{1}{n(15)} + \dots$$

Artin's Heuristic

- Start with:

$$1 - \frac{1}{n(2)} - \frac{1}{n(3)} - \frac{1}{n(5)} - \dots$$

- The subtraction above double-counts primes that split completely in both K_i and K_j , so we need to add back terms to account for these primes. So, we'll add

$$\frac{1}{n(6)} + \frac{1}{n(10)} + \frac{1}{n(14)} + \frac{1}{n(15)} + \dots$$

- Continuing in this fashion, we would expect to obtain something like:

$$\#\{p \leq x : a \text{ is a generator mod } p\} \sim \sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)} \frac{x}{\log x},$$

as $x \rightarrow \infty$.

Artin's Heuristic

In the case where K_{q_1} and K_{q_2} are independent over \mathbb{Q} , then $[K_{q_1 q_2} : \mathbb{Q}] = [K_{q_1} : \mathbb{Q}][K_{q_2} : \mathbb{Q}]$ and $A(a) = A$.

Hence, for squarefree m , we have $n(m) = m\varphi(m)$. Thus, Artin's method yields

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)} = \sum_{k=1}^{\infty} \frac{\mu(k)}{k\varphi(k)} = \prod_p \left(1 - \frac{1}{p(p-1)}\right) = A,$$

i.e.

$$\#\{p \leq x : a \text{ is a generator mod } p\} \sim A \frac{x}{\log x}.$$

Hooley's Proof

In 1966, Hooley succeeded in turning these heuristic arguments into a rigorous proof by assuming the Generalized Riemann Hypothesis:

- The GRH yields a stronger form of the Chebotarev Density Theorem, which gives an estimate of $\frac{\pi(x)}{n(q)} + O(\sqrt{x} \log qx)$ primes up to x which fail the q -test, for values of q up to $\sqrt{x}/\log^2 x$.

Hooley's Proof

In 1966, Hooley succeeded in turning these heuristic arguments into a rigorous proof by assuming the Generalized Riemann Hypothesis:

- The GRH yields a stronger form of the Chebotarev Density Theorem, which gives an estimate of $\frac{\pi(x)}{n(q)} + O(\sqrt{x} \log qx)$ primes up to x which fail the q -test, for values of q up to $\sqrt{x}/\log^2 x$.
- The primes q that are larger than this bound can then be dealt with using a completely elementary argument that does not require the GRH.

Hooley's Approach for Large q

We'll split up the region $\frac{\sqrt{x}}{\log^2 x} \leq q \leq x - 1$ into two subregions that we'll deal with separately:

The first region is the “hard” region. For notational convenience, we'll let $\eta_1 = \frac{\sqrt{x}}{\log^2 x}$ and $\eta_2 = \sqrt{x} \log x$.

Hooley's Approach for Large q

We'll split up the region $\frac{\sqrt{x}}{\log^2 x} \leq q \leq x - 1$ into two subregions that we'll deal with separately:

- $\frac{\sqrt{x}}{\log^2 x} \leq q \leq \sqrt{x} \log x$

The first region is the “hard” region. For notational convenience, we'll let $\eta_1 = \frac{\sqrt{x}}{\log^2 x}$ and $\eta_2 = \sqrt{x} \log x$.

Hooley's Approach for Large q

We'll split up the region $\frac{\sqrt{x}}{\log^2 x} \leq q \leq x - 1$ into two subregions that we'll deal with separately:

- $\frac{\sqrt{x}}{\log^2 x} \leq q \leq \sqrt{x} \log x$
- $\sqrt{x} \log x \leq q \leq x - 1$

The first region is the “hard” region. For notational convenience, we'll let $\eta_1 = \frac{\sqrt{x}}{\log^2 x}$ and $\eta_2 = \sqrt{x} \log x$.

The Region $\eta_1 \leq q \leq \eta_2$

For q in this range:

- Primes p counted by $P(x, y)$ certainly satisfy $p \equiv 1 \pmod{q}$.
Thus, $P(x, y) \leq \pi(x; q, 1)$.

The Region $\eta_1 \leq q \leq \eta_2$

For q in this range:

- Primes p counted by $P(x, y)$ certainly satisfy $p \equiv 1 \pmod{q}$. Thus, $P(x, y) \leq \pi(x; q, 1)$.
- The Brun-Titchmarsh inequality yields

$$\pi(x; q, 1) \leq \frac{2x}{\varphi(q) \log(x/q)}$$

for $1 \leq q \leq x$.

The Region $\eta_1 \leq q \leq \eta_2$

Thus,

$$\#\{p \leq x : p \text{ splits completely in some } K_q, \eta_1 \leq q \leq \eta_2\}$$

$$\begin{aligned} &\leq \sum_{\eta_1 \leq q \leq \eta_2} P(x, q) \\ &\leq \sum_{\eta_1 \leq q \leq \eta_2} \pi(x; q, 1) \\ &= O\left(\frac{x}{\log x} \sum_{\eta_1 \leq q \leq \eta_2} \frac{1}{q}\right). \end{aligned}$$

The Region $\eta_1 \leq q \leq \eta_2$

By Mertens' Theorem: $\sum_{q \leq x} \frac{1}{q} = \log \log x + \text{constant} + O\left(\frac{1}{\log x}\right)$.

Thus, $\sum_{\eta_1 \leq q \leq \eta_2} \frac{1}{q} = O\left(\frac{\log \log x}{\log x}\right)$.

Therefore,

$$\#\{p \leq x : p \text{ splits completely in some } K_q, \eta_1 \leq q \leq \eta_2\}$$

$$= O\left(\frac{x \log \log x}{\log^2 x}\right).$$

The Region $\eta_2 \leq q \leq x - 1$

All that remains is for us to consider values of q in $(\sqrt{x} \log x, x - 1)$:

- If p is counted in $\#\{p \leq x : p \text{ splits completely in some } K_q, \eta_2 \leq q \leq x - 1\}$, then $a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$ and $p \equiv 1 \pmod{q}$, so $\ell_a(p) \leq a^{\frac{p-1}{\eta_2}} \leq a^{\frac{x}{\eta_2}}$.

The Region $\eta_2 \leq q \leq x - 1$

All that remains is for us to consider values of q in $(\sqrt{x} \log x, x - 1)$:

- If p is counted in $\#\{p \leq x : p \text{ splits completely in some } K_q, \eta_2 \leq q \leq x - 1\}$, then $a^{\frac{p-1}{q}} \equiv 1 \pmod{p}$ and $p \equiv 1 \pmod{q}$, so $\ell_a(p) \leq a^{\frac{p-1}{\eta_2}} \leq a^{\frac{x}{\eta_2}}$.
- Thus, p divides $a^m - 1$ for some $m < \frac{\sqrt{x}}{\log x}$.

The Region $\eta_2 \leq q \leq x - 1$

Let $M(x, \eta_2, x - 1) :=$

$\#\{p \leq x : p \text{ splits completely in some } K_q, \eta_2 \leq q \leq x - 1\}.$

Observe that

$$a^{M(x, \eta_2, x-1)} < \prod_{\substack{p \text{ counted by} \\ M(x, \eta_2, x-1)}} p \leq \prod_{m < \frac{\sqrt{x}}{\log x}} a^m - 1.$$

Thus,

$$M(x, \eta_2, x - 1) < \sum_{m < \frac{\sqrt{x}}{\log x}} m = O\left(\frac{x}{\log^2 x}\right).$$

The Unsatisfying State of Affairs

- Hooley's method yields a proof of the quantitative form of Artin's Conjecture, but his proof is conditional on GRH.

The Unsatisfying State of Affairs

- Hooley's method yields a proof of the quantitative form of Artin's Conjecture, but his proof is conditional on GRH.
- We still don't know a single value of a for which the qualitative form of Artin's Conjecture holds!

What Is Known

- We may not know definitively whether the quantitative form of Artin's conjecture holds, but it is not difficult to show that it holds unconditionally *on average*.

What *Is* Known

- We may not know definitively whether the quantitative form of Artin's conjecture holds, but it is not difficult to show that it holds unconditionally *on average*.
- Although we don't have any examples of values of a for which Artin's Conjecture holds, we do have some good candidates for possible examples...

A Surprising Result



In 1986, Heath-Brown showed (based on earlier work of Gupta and Murty) that, for any three numbers which are multiplicatively independent over \mathbb{Q} , the qualitative form of Artin's Conjecture holds for at least one of them. In particular, this implies that there are at most two prime values of a for which the weak form of Artin's conjecture does not hold!

Analogues of Artin's Conjecture in Other Settings

Artin's primitive root conjecture has been proven unconditionally in the function field setting. Bilharz gave a conditional proof in 1937 that depended on the Riemann Hypothesis for function fields (which has since been proven by Weil).

Analogues of Artin's Conjecture in Other Settings

There is also an analogue of Artin's conjecture over elliptic curves:

Let $a \in E(\mathbb{Q})$ be a point of infinite order, p be a prime of good reduction for E , \overline{E}/F_p be the reduction of E modulo p and \overline{a} be the reduction of a modulo p . We say that a is a *primitive point of E modulo p* if $\overline{E}(F_p) = \langle \overline{a} \rangle$.

The elliptic curve analogue of Artin's Conjecture is to determine the density of primes p for which a is a primitive point of E modulo p . In 1976, Lang and Trotter conjectured that this density exists.

Analogues of Artin's Conjecture in Other Settings

Lang and Trotter also conjectured that there exists a constant $C_E(a) \geq 0$, depending on E and a , such that

$$\#\{p \leq x : \bar{E}(F_p) = \langle \bar{a} \rangle\} \sim C_E(a) \frac{x}{\log x}.$$

In most cases, this is still an open question. The only result known is due to Gupta and Murty, who proved that, if E/\mathbb{Q} has complex multiplication by the full ring of integers of an imaginary quadratic field K , then, under GRH,

$$\#\{p \leq x : a_p \neq 0, \bar{E}(F_p) = \langle \bar{a} \rangle\} = C_E(a)\pi(x) + O\left(\frac{x \log \log x}{\log^2 x}\right).$$

References

Hooley, Christopher. *On Artin's conjecture*. Journal für die reine und angewandte Mathematik (Crelles Journal), 1967.

Li, Shuguang and Pomerance, Carl. *Primitive roots: a survey*. New Aspects of Analytic Number Theory, 2002.

Moree, Pieter. *Artin's primitive root conjecture - a survey*.
(unpublished draft)

Pollack, Paul. *Not always buried deep: a second course in elementary number theory*. AMS, 2009.