Artin's Primitive Root Conjecture

Vivaan Daga

vivaandaga@gmail.com

Euler Circle

Table of Contents

Table of Contents

Primitive Roots mod p

The notion of a primitive root mod p was introduced by Gauss when he was investigating the period of the decimal expansion of $\frac{1}{p}$ for prime $p \neq 2, 5$.

Primitive Roots mod p

The notion of a primitive root mod p was introduced by Gauss when he was investigating the period of the decimal expansion of $\frac{1}{p}$ for prime $p \neq 2, 5$.

Gauss proved the following lemma:

Primitive Roots mod p

The notion of a primitive root mod p was introduced by Gauss when he was investigating the period of the decimal expansion of $\frac{1}{p}$ for prime $p \neq 2, 5$.

Gauss proved the following lemma:

Lemma

The period of the decimal expansion of $\frac{1}{p}$ for prime $p \neq 2, 5$ is the least positive number k such that $10^k = 1 \mod p$.

Primitive Roots mod p

The notion of a primitive root mod p was introduced by Gauss when he was investigating the period of the decimal expansion of $\frac{1}{p}$ for prime $p \neq 2, 5$.

Gauss proved the following lemma:

Lemma

The period of the decimal expansion of $\frac{1}{p}$ for prime $p \neq 2, 5$ is the least positive number k such that $10^k = 1 \mod p$.

So if we have a prime p, for which the decimal expansion of $\frac{1}{p}$ has period $p - 1$, the maximum possible, then $p - 1$ must the least positive k for which $10^k = 1 \mod p$ holds. In such a case, we say 10 is a primitive root mod p.

Primitive Roots mod p

More generally, we have the following definition of primitive root mod p:

Primitive Roots mod p

More generally, we have the following definition of primitive root mod p:

Definition

Given a prime p, an integer a is said to be a primitive root mod p if $p - 1$ is the least positive integer k such that $a^k = 1 \mod p$.

Primitive Roots mod p

More generally, we have the following definition of primitive root mod p:

Definition

Given a prime p, an integer a is said to be a primitive root mod p if $p-1$ is the least positive integer k such that $a^k = 1 \mod p$.

Or in more modern terms:

Primitive Roots mod p

More generally, we have the following definition of primitive root mod p:

Definition

Given a prime p, an integer a is said to be a primitive root mod p if $p-1$ is the least positive integer k such that $a^k = 1 \mod p$.

Or in more modern terms:

Definition

An integer a is a primitive root mod p if the subgroup generated by a in the cyclic group $(\mathbb{Z}/p\mathbb{Z})^\times$ is the whole group.

Table of Contents

Artin's Conjecture

We can now state qualitative and quantitative forms of Artin's Primitive Root Conjecture:

Artin's Conjecture

We can now state qualitative and quantitative forms of Artin's Primitive Root Conjecture:

Qualitative Form

Given a non-zero integer a other than -1 or a perfect square, there exist infinitely many primes p for which a is a primitive root mod p.

Artin's Conjecture

We can now state qualitative and quantitative forms of Artin's Primitive Root Conjecture:

Qualitative Form

Given a non-zero integer a other than -1 or a perfect square, there exist infinitely many primes p for which a is a primitive root mod p.

Quantitative Form

Given a non-zero integer a other than -1 or a perfect square, if $\mathcal{P}_a(x)$ denotes the number of primes less than equal to x for which a is a primitive root, then we have that $\mathcal{P}_a(x) \sim \delta(a)\frac{x}{\log x}$, where $\delta(a)$ is a specific positive function of a.

Artin's Conjecture

We can now state qualitative and quantitative forms of Artin's Primitive Root Conjecture:

Qualitative Form

Given a non-zero integer a other than -1 or a perfect square, there exist infinitely many primes p for which a is a primitive root mod p.

Quantitative Form

Given a non-zero integer a other than -1 or a perfect square, if $\mathcal{P}_a(x)$ denotes the number of primes less than equal to x for which a is a primitive root, then we have that $\mathcal{P}_a(x) \sim \delta(a)\frac{x}{\log x}$, where $\delta(a)$ is a specific positive function of a.

In the qualitative form, $\delta(a)$ is the density or proportion of primes for which a is a primitive root since by the Prime Number Theorem $\pi(x) \sim \frac{x}{\log x}$. Of course, the quantitative form implies the qualitative form.

Table of Contents

The function $\delta(a)$

Remark

From this slide onward, we shall be using notions and theorems from algebraic number theory. If you do not know algebraic number theory, take these as black-boxes.

The function $\delta(a)$

Remark

From this slide onward, we shall be using notions and theorems from algebraic number theory. If you do not know algebraic number theory, take these as black-boxes.

Let a be a non-zero integer that is not -1 or a perfect square. Let us now try to get a conjectural value for $\delta(a)$. To do this, we shall require notions from algebraic number theory. The connection to algebraic number theory is seen from the following theorem:

The function $\delta(a)$

Remark

From this slide onward, we shall be using notions and theorems from algebraic number theory. If you do not know algebraic number theory, take these as black-boxes.

Let a be a non-zero integer that is not -1 or a perfect square. Let us now try to get a conjectural value for $\delta(a)$. To do this, we shall require notions from algebraic number theory. The connection to algebraic number theory is seen from the following theorem:

Theorem

Given a prime p, a is a primitive root mod p if and only if p does not split completely in any K_q, where q is prime and $K_q = \mathbb{Q}(\zeta_q, a^{1/q})$.

The function $\delta(a)$

Remark

From this slide onward, we shall be using notions and theorems from algebraic number theory. If you do not know algebraic number theory, take these as black-boxes.

Let a be a non-zero integer that is not -1 or a perfect square. Let us now try to get a conjectural value for $\delta(a)$. To do this, we shall require notions from algebraic number theory. The connection to algebraic number theory is seen from the following theorem:

Theorem

Given a prime p, a is a primitive root mod p if and only if p does not split completely in any K_q, where q is prime and $K_q = \mathbb{Q}(\zeta_q, a^{1/q})$.

Now, Chebotarev's Density Theorem implies that the density of primes which split in K_k is $\frac{1}{n(k)}$, where $n(k)$ is the degree of the extension $K_k/\mathbb{Q}$.

The function $\delta(a)$

Using Chebotarev's Density Theorem and the fact that a prime p splits completely in K_k and K_l if and only if it splits completely in $K_{\text{lcm}(k,l)}$, we can find a heuristic for $\delta(a)$ using the inclusion-exclusion principle:

The function $\delta(a)$

Using Chebotarev's Density Theorem and the fact that a prime p splits completely in K_k and K_l if and only if it splits completely in $K_{\mathrm{lcm}(k,l)}$, we can find a heuristic for $\delta(a)$ using the inclusion-exclusion principle:

$\delta(a)$ gives us the density of primes which split in none of the K_q, for prime q. To "compute" this density subtract the density for each prime:

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

The function $\delta(a)$

Using Chebotarev's Density Theorem and the fact that a prime p splits completely in K_k and K_l if and only if it splits completely in $K_{\mathrm{lcm}(k,l)}$, we can find a heuristic for $\delta(a)$ using the inclusion-exclusion principle:

$\delta(a)$ gives us the density of primes which split in none of the K_q, for prime q. To "compute" this density subtract the density for each prime:

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

Then add the densities for product of two primes:

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

The function $\delta(a)$

Using Chebotarev's Density Theorem and the fact that a prime p splits completely in K_k and K_l if and only if it splits completely in $K_{\mathrm{lcm}(k,l)}$, we can find a heuristic for $\delta(a)$ using the inclusion-exclusion principle:

$\delta(a)$ gives us the density of primes which split in none of the K_q, for prime q. To "compute" this density subtract the density for each prime:

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

Then add the densities for product of two primes:

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

And so on.

The function $\delta(a)$

Using Chebotarev's Density Theorem and the fact that a prime p splits completely in K_k and K_l if and only if it splits completely in $K_{\mathrm{lcm}(k,l)}$, we can find a heuristic for $\delta(a)$ using the inclusion-exclusion principle:

$\delta(a)$ gives us the density of primes which split in none of the K_q, for prime q. To "compute" this density subtract the density for each prime:

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

Then add the densities for product of two primes:

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

And so on. In this way, we get that $\delta(a)$ "=" $\sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)}$, where μ is the Möbius function.

The function $\delta(a)$

In the previous slide, we gave a heuristic for $\delta(a) = \sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)}$. Letting a_1 be the square free part of a and h be the largest integer such that a is an h-th power, it turns out we have the following theorem:

The function $\delta(a)$

In the previous slide, we gave a heuristic for $\delta(a) = \sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)}$. Letting a_1 be the square free part of a and h be the largest integer such that a is an h-th power, it turns out we have the following theorem:

Theorem

Let $A(h) = \prod_{q \nmid h} \left(1 - \frac{1}{q(q-1)}\right) \prod_{q \mid h} \left(1 - \frac{1}{q-1}\right)$, *where q is prime. Then we have that*

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)} = \begin{cases} A(h) & \text{if } a_1 \neq 1 \mod 4 \\ \left(1 - \mu(|a_1|) \prod_{q \mid a_1, q \mid h} \frac{1}{q-2} \prod_{q \mid a_1, q \nmid h} \frac{1}{q^2-q-1}\right) A(h) & \text{if } a_1 = 1 \mod 4 \end{cases}$$

The function $\delta(a)$

In the previous slide, we gave a heuristic for $\delta(a) = \sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)}$. Letting a_1 be the square free part of a and h be the largest integer such that a is an h-th power, it turns out we have the following theorem:

Theorem

Let $A(h) = \prod_{q \nmid h} \left(1 - \frac{1}{q(q-1)}\right) \prod_{q \mid h} \left(1 - \frac{1}{q-1}\right)$, where q is prime. Then we have that

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)} = \begin{cases} A(h) & \text{if } a_1 \neq 1 \mod 4 \\ \left(1 - \mu(|a_1|) \prod_{q \mid a_1, q \mid h} \frac{1}{q-2} \prod_{q \mid a_1, q \nmid h} \frac{1}{q^2-q-1}\right) A(h) & \text{if } a_1 = 1 \mod 4 \end{cases}$$

Since $\sum_{k=1}^{\infty} \frac{1}{k(k-1)}$ converges, $A(h)$ is positive. Therefore, if the heuristic holds, then $\delta(a)$ is also positive and Artin's Primitive Root Conjecture is true.

Table of Contents

Hooley's Conditional Proof

Subject to the truth of the Generalized Riemann Hypothesis Cristopher Hooley proved that our heuristic value for $\delta(a)$ is indeed correct.

Hooley's Conditional Proof

Subject to the truth of the Generalized Riemann Hypothesis Cristopher Hooley proved that our heuristic value for $\delta(a)$ is indeed correct.

Intuitively, the Generalized Riemann Hypothesis gives us an effective version of Chebatorev's Density Theorem, which allows us to make the inclusion-exclusion argument rigorous. Except not quite since the error term ends up being two large. Nevertheless, Hooley was able to introduce some intermediate quantities that made everything work.

Hooley's Conditional Proof

Subject to the truth of the Generalized Riemann Hypothesis Cristopher Hooley proved that our heuristic value for $\delta(a)$ is indeed correct.

Intuitively, the Generalized Riemann Hypothesis gives us an effective version of Chebatorev's Density Theorem, which allows us to make the inclusion-exclusion argument rigorous. Except not quite since the error term ends up being two large. Nevertheless, Hooley was able to introduce some intermediate quantities that made everything work.

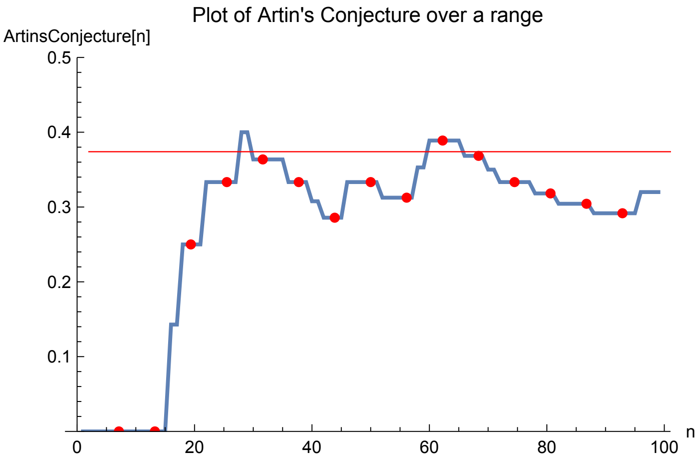
Hooley proved:

Theorem

$$\mathcal{P}_a(x) = \left(\sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)}\right) \frac{x}{\log x} + O\left(\frac{x \log \log x}{\log^2 x}\right)$$

Thank You! Questions?

Artin's Conjecture for $a = 10$



Credit: Navye Anand