Artin's Conjecture on primitive roots

Edwina Aylward

December 18, 2024

Take $\frac{1}{p}$ for p a prime and consider its decimal expansion:

$$\frac{1}{11} = 0.09090909\cdots \qquad \frac{1}{7} = 0.142857142857\cdots$$

For $p \neq 2,5$, this decimal expansion is periodic. The length of the period, k, is the smallest integer such that

$$10^k \equiv 1 \mod p,$$

i.e. is the order of 10 in $\mathbb{F}_p^\times$.
Thus the decimal expansion of $\frac{1}{p}$ has maximal period length of $p-1$ when 10 is a primitive root mod p.

Question (Gauss) : Is this period maximal for infinitely many p?

Conjecture (Artin, 1927)

Let $a \in \mathbb{Z}$ be such that $a \neq \pm 1$ and a is not a perfect square.

- *(Qualitative) There exists infinitely many primes p such that a is a primitive root mod p.*
- *(Quantitative) Let $N_a(x) = \#\{p \text{ prime} : a \text{ is a primitive root mod } p\}$ for $x \in \mathbb{R}$. Then*

$$N_a(x) \sim A(a) \cdot \frac{x}{\log x}, \qquad \text{as } x \to \infty,$$

where $A(a)$ is a positive constant depending on a.

There is no integer a for which this is known.

∞ many primes of the form ...

Example

Consider a prime of the form $q = 4p + 1$ with p prime and $p \equiv 2 \mod 5$. Then 10 is a primitive root mod p. Indeed,

$$10^{2p} \equiv \left(\frac{10}{q}\right) = (-1)^{\frac{q^2-1}{8}} \left(\frac{q}{5}\right) = -\left(\frac{4}{5}\right) \equiv -1 \mod q$$

and no prime divisor of $10^4 - 1$ satisfies the requirements of q.

Therefore we expect that there exists infinitely many primes of this form.

Constant $A(a)$

Let $a \in \mathbb{Z}$ and h the largest integer such that a is a h-th power. Artin originally defined $A(a)$ as

$$A(a) = \prod_{q \nmid h} \left(1 - \frac{1}{q(q-1)}\right) \prod_{q \mid h} \left(1 - \frac{1}{q-1}\right).$$

For a prime p, a is a primitive root mod p if and only if the events

$$p \equiv 1 \mod q, \quad a^{\frac{p-1}{q}} \equiv 1 \mod p$$

do not occur. Equivalently, a is a primitive root mod p if and only if

$$p \text{ does not split completely in } L_q = \mathbb{Q}(\zeta_q, a^{1/q}).$$

Assume that splitting completely in L_q and $L_{q'}$ are independent events for q, q' distinct primes.

Chebotarev $\rightsquigarrow$ density of primes that do not split completely in any L_q is

$$\prod_q \left(1 - \frac{1}{[L_q : \mathbb{Q}]}\right).$$

Splitting completely in L_q and $L_{q'}$ for $q \neq q'$ aren't independent events. For example, if $a = 5$ then $L_2 = \mathbb{Q}(\sqrt{5}) \subset L_5 = \mathbb{Q}(\zeta_5, 5^{1/5})$.

Density of primes p that do not split completely in any L_q is

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{[L_k : \mathbb{Q}]} = 1 - \frac{1}{[L_2 : \mathbb{Q}]} - \frac{1}{[L_3 : \mathbb{Q}]} + \frac{1}{[L_6 : \mathbb{Q}]} + \cdots,$$

where L_k for squarefree k is the compositum of $\{L_q : q \mid k\}$.

Let d be the discriminant of $\mathbb{Q}(\sqrt{a})$. Then

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(\zeta_k, a^{1/k}) : \mathbb{Q}]} = \begin{cases} A(a) & d \not\equiv 1 \mod 4 \\ \delta(a) \cdot A(a) & \text{otherwise.} \end{cases}$$

where

$$\delta(a) = \left(1 - \mu(|d|) \prod_{q \mid d} \frac{1}{[L_q : \mathbb{Q}] - 1}\right)$$

Correction

$$\sum_{k=1}^{\infty} \frac{\mu(k)}{[\mathbb{Q}(\zeta_k, a^{1/k}) : \mathbb{Q}]} = \begin{cases} A(a) & d \not\equiv 1 \mod 4 \\ \delta(a) \cdot A(a) & \text{otherwise} \end{cases} := C(a)$$

where

$$\delta(a) = \left(1 - \mu(|d|) \prod_{q|d} \frac{1}{[L_q : \mathbb{Q}] - 1}\right).$$

When k is odd then $\{L_q : q \mid k\}$ are linearly disjoint. When k is odd and squarefree,

$$[L_{2k} : \mathbb{Q}] = \begin{cases} [L_k : \mathbb{Q}] & \sqrt{a} \subset \mathbb{Q}(\zeta_k) \\ 2 \cdot [L_k : \mathbb{Q}] & \sqrt{a} \not\subset \mathbb{Q}(\zeta_k) \end{cases}.$$

Letting $a = bc^2$ with b squarefree, $\sqrt{a} \subset \mathbb{Q}(\zeta_k) \Leftrightarrow b \mid k,\ b \equiv 1 \mod 4$.

e.g. $a = 5$, correct density is $A(5) \cdot (1 + \frac{1}{19})$.

Theorem (Hooley, 1967)

Assume that the extended Riemann hypothesis holds. Then

$$N_a(x) = C(a) \cdot \frac{x}{\log x} + O\left(\frac{x \log\log x}{\log^2 x}\right)$$

as $x \to \infty$.

Let

$$\begin{aligned} N_a(x,\eta) &= \#\{p \le x \colon p \text{ doesn't split completely in } L_q \ \forall q \le \eta\}, \\ P(x,k) &= \#\{p \le x \colon p \text{ splits completely in } L_k\}, \quad k \text{ squarefree} . \end{aligned}$$

Then $N_a(x) = N_a(x, x-1)$, and

$$N_a(x,\eta) = \sum_{\ell'} \mu(\ell') P(x,\ell')$$

where ℓ' ranges over divisors of $\prod_{q \le \eta} q$.

One has $N_a(x) \le N_a(x,\epsilon)$ where $\epsilon = \frac{1}{6}\log x$. In fact

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

- $N_a(x) = N_a(x,\epsilon) + O\left(\frac{x\log\log x}{\log^2 x}\right), \quad \epsilon = \frac{1}{6}\log x,$
- $N_a(x,\epsilon) = \sum_{\ell'} \mu(\ell')P(x,\ell').$

Note

$$\ell' \leq \prod_{q\leq\epsilon} q = e^{\sum_{q\leq\epsilon}\log q} \leq e^{2\epsilon} = x^{1/3}.$$

Hooley proves that, assuming the Riemann Hypothesis for the field L_k,

$$P(x,k) = \frac{1}{[L_k : \mathbb{Q}]}\operatorname{Li}(x) + O\left(\sqrt{x}\log(kx)\right).$$

Then since ϵ is small one can estimate

$$N_a(x,\epsilon) = C(a)\cdot\frac{x}{\log x} + O\left(\frac{x}{log^2 x}\right).$$

- 1983: Gupta & Murty. Let q, r, s be three distinct primes. Consider the set

$$S = \{qs^2,\ q^3r^2,\ q^2r,\ r^3s^2,\ r^2s,\ q^2s^3,\ qr^3,\ q^3rs^2,\ rs^3,\ q^2r^3s,\ q^3s,\ qr^2s^3,\ qrs\}.$$

For at least one of these integers, Artin's conjecture is true.

Theorem. *For some* $a \in S$, *there is a* $\delta > 0$ *such that for at least* $\delta x/\log^2 x$ *primes* $p \leqq x$, *a is a primitive root* $(\bmod\, p)$.

Our theorem is proved in the following way. First we show that there are at least $cx/\log^2 x$ primes $p \leqq x$ such that all odd prime divisors of $(p-1)$ exceed $x^{\frac{1}{4}+\varepsilon}$. For such primes, we prove that $\mathbb{F}_p^* = \langle q, r, s \rangle$ with at most $o(x/\log^2 x)$ exceptional primes $p \leqq x$. Hence, for at least $cx/\log^2 x$ primes $p \leqq x$, $\mathbb{F}_p^*$ has a generator of the form $q^u r^v s^w$ for some u, v, w. The final step is to show that we can find u, v, w bounded by three. In fact, we can take a generator as in the set S above.

- Best result: Heath-Brown (1986) reduced this set to size 3. In particular one of 2, 3, 5 is a primitive root mod p for infinitely many primes p.

Elliptic curve analogue

Let $E/\mathbb{Q}$ be an elliptic curve of rank ≥ 1, $a \in E(\mathbb{Q})$ a point of infinite order.
Does there exist infinitely many prime p such that

$$\overline{E}(\mathbb{F}_p) = \langle \overline{a} \rangle$$

where $\overline{E}/\mathbb{F}_p$ is the reduction of E mod p, $\overline{a} = a \mod p$? If so, say a is a *primitive point mod* p.
This depends on E, e.g. if $E[2] \subset E(\mathbb{Q})$ then $\overline{E}(\mathbb{F}_p)$ is non-cyclic.

Theorem (Gupta–Murty, 1986)

Let $E/\mathbb{Q}$ be an elliptic curve with complex multiplication by $\mathcal{O}_k$ and let $a \in E(\mathbb{Q})$ be a point of infinite order. Let $N_a(x) = \#\{p \leq x \colon a$ is a primitive point mod $p\}$. Assuming the extended Riemann hypothesis,

$$N_a(x) = C_E(x)\frac{x}{\log x} + O\left(\frac{x \log\log x}{\log^2 x}\right)$$

as $x \mapsto \infty$, where C_E is a constant depending on a and E.

Function field analogue

Let K be a global function field, $K = \mathbb{F}_q(C)$ where $C/\mathbb{F}_q$ is a non-singular projective curve. The zeta functions of C and K are given by

$$Z_c(t) = \exp\left(\sum_{i=1}^{\infty} N_C(q^i)\frac{t^i}{i}\right), \quad \zeta_K(s) = Z_C(u), \quad u = q^{-s}.$$

Weil conjectures $\implies \zeta_K(s) = \frac{L_C(u)}{(1-u)(1-qu)}$ with

$$L_C(u) = \prod_{i=1}^{2g}(1-\alpha_i u), \quad |\alpha_i| = \sqrt{q}.$$

This implies the Riemann Hypothesis holds for $\zeta_K(s)$, i.e. the zeros of $\zeta_K(s)$ lie on $\mathrm{Re}(s) = \frac{1}{2}$.

Theorem (Bilharz, 1937)

Let $K = \mathbb{F}_q(C)$ be a global function field. Consider $g \in K$ such that

- $g \notin \mathbb{F}_q$,
- *g is not an l-th power for any $l \mid q-1$.*

Then g is a primitive root modulo $\mathfrak{p}$ for infinitely many closed points $\mathfrak{p} \in C$.

$\mathbb{F}_p(x)$ example

Let $a(x) \in \mathbb{F}_p(x)$ be a rational function. There are ∞ many monic irr. polys $p(x) \in \mathbb{F}_p[x]$ such that

$$\langle a(x) \text{ mod } p(x) \rangle = \left(\mathbb{F}_p[x]/p(x)\right)^*.$$

Recall if $p(x)$ is of degree n, then $\mathbb{F}_p[x]/(p(x)) \simeq \mathbb{F}_{p^n}$, hence the multiplicative group is of order $p^n - 1$.

Proposition (Indicator function formula)

Let G be a finite cyclic group of order n, f the function on G given by $f(g) = \begin{cases} 1 & \langle g \rangle = G, \\ 0 & \text{otherwise.} \end{cases}$. Then

$$f(g) = \frac{\varphi(n)}{n} \sum_{d|n} \frac{\mu(d)}{\varphi(d)} \sum_{\operatorname{ord}\chi = d} \chi(g).$$

Thus

$$\#\{p(x) \colon \deg p(x) = n,\ a(x) \text{ generates } (\mathbb{F}_p[x]/p(x))^*\}$$

$$= \sum_{p(x)\colon \deg p(x) = n} \frac{\varphi(p^n - 1)}{p^n - 1} \sum_{d|p^n-1} \frac{\mu(d)}{\varphi(d)} \sum_{\operatorname{ord}\chi = d} \chi(\overline{a(x)}).$$

$$\#\{p(x)\colon \deg p(x) = n,\ a(x) \text{ generates } (\mathbb{F}_p[x]/p(x))^*\}$$
$$= \sum_{p(x)\colon \deg p(x)=n} \frac{\varphi(p^n-1)}{p^n-1} \sum_{d \mid p^n-1} \frac{\mu(d)}{\varphi(d)} \sum_{\operatorname{ord}\chi = d} \chi(\overline{a(x)}).$$

The number of monic irreducible polynomials of degree n in $\mathbb{F}_p[x]$ is given by

$$\frac{1}{n}\sum_{d \mid n} \mu(d) p^{n/d} = \frac{p^n}{n} + O(\frac{p^{n/2}}{n}).$$

Thus the contribution from the main term $(d=1)$ of our expression is

$$\frac{\varphi(p^n-1)}{p^n-1}\,\frac{p^n + O(p^{n/2})}{n}.$$

The error term can be bounded. If $N_a(\mathbb{F}_p, n)$ denotes the number of irreducible polynomials $p(x)$ of degree n such that $a(x)$ is a primitive root mod $\mathbb{F}_p[x]/p(x)$, then

$$\boxed{N_a(\mathbb{F}_p, n) = \frac{\varphi(p^n-1)}{n}(1 + O(mp^{-n(\frac{1}{2}-\epsilon)})),}$$

for any $\epsilon > 0$, with $m = \deg a(x)$.

End

Thank you for listening :)