Finding primitive roots according to Artin's conjecture

Antonella Perucca & Carlo Sanna

University of Luxembourg & Politecnico di Torino

Artin's conjecture on primitive roots and Artin type problems provide expectations for an integer to be a primitive root modulo a random prime number (possibly with certain restrictions on the prime). These predictions — that we describe in [3] — are relevant to algorithms that find primitive roots by testing candidates.

What is a primitive root?

Let p be a prime number. If a is an integer such that $p \nmid a$, then

$$(a \bmod p) \in (\mathbb{Z}/p\mathbb{Z})^\times \simeq \mathbb{Z}/(p-1)\mathbb{Z}\,.$$

If $(a \bmod p)$ is a generator for this cyclic group, we call a a **primitive root modulo** p. Equivalently, the index of the subgroup $\langle (a \bmod p)\rangle$ must be 1.

What is the density of a set of primes?

Let $\mathcal{P}$ be the set of all prime numbers. Let $S \subseteq \mathcal{P}$. If the following limit exists we call it the **natural density** of S:

$$\lim_{x\to\infty} \frac{\#\{p \in S, p \le x\}}{\#\{p \in \mathcal{P}, p \le x\}}$$

Artin's conjecture on primitive roots (1927)

While looking for primitive roots modulo a given prime p we may restrict to consider integers that are not perfect powers because of the following:

- 0 is never a primitive root; ± 1 are not primitive roots modulo p for $p \ge 5$;
- If a is a primitive root modulo p and $a = b^n$ holds for some integer b and for some $n > 1$, then b is also a primitive root.

The **Artin constant** is the real number

$$A := \prod_{q \text{ prime}} \Big(1 - \frac{1}{q(q-1)}\Big) = 0.374\ldots$$

Suppose that a is an integer that is not a perfect power. Call a_{sqf} the squarefree integer such that a/a_{sqf} is a square and let d be the number of prime divisors of a_{sqf}. The set of primes for which a is a primitive root modulo p admits a natural density (we call it $\mathrm{dens}(a)$). We have

$$\mathrm{dens}(a) = A$$

unless $a_{\mathrm{sqf}} \equiv 1 \bmod 4$, in which case we have

$$\mathrm{dens}(a) = A \cdot \Big(1 + (-1)^{d+1} \prod_{\substack{q \text{ prime} \\ q \mid a_{\mathrm{sqf}}}} \frac{1}{q^2 - q - 1}\Big)\,.$$

The above conjecture has been proven by Hooley [1] assuming the Generalized Riemann Hypothesis (GRH) for the Dedekind zeta function of $\mathbb{Q}(\zeta_n, \sqrt[n]{a})$ for n squarefree.

We consider the density in Artin's conjecture the "expectation" for a to be a primitive root modulo a random p.

Proposition (assuming GRH):

Let a be an integer that is not a perfect power. The density of the primes $p \nmid a$ for which the index of $\langle (a \bmod p)\rangle$ has no odd prime factor exists and it is $2A \sim 75\%$.

The difference among integers concerning the density in Artin's conjecture is because the conditions "the index is odd" and "the index has no odd prime factors" are not independent.

The record integer -3

Generically, $\mathrm{dens}(a) = A \sim 37\%$. For example, $\mathrm{dens}(2) = A$. The maximal density is

$$\mathrm{dens}(-3) = \frac{6}{5}A \sim 45\%\,.$$

The reason is that, if -3 is not a square modulo p, then $3 \nmid (p-1)$ so the index of $\langle (-3 \bmod p)\rangle$ is coprime to 3. However, if $3 \nmid (p-1)$, then any index is coprime to 3. In fact, we have:

Proposition (assuming GRH):

Let a and b be integers that are not perfect powers. Then, restricting to the primes p for which a and b are not squares modulo p, the expectation for a and b to be a primitive root is the same (the corresponding sets of primes have the same density).

Making use of negative numbers

If $p \equiv 1 \bmod 4$, then the sign of a does not matter for a being a primitive root modulo p, so suppose that $p \equiv 3 \bmod 4$.

If an integer a (such that $p \nmid a$) is a square modulo p, then $-a$ is not a square modulo p. So to find a primitive root we can test whether the index of $\langle (a \bmod p)\rangle$ has no odd prime factors, and then choose the sign of a correctly to obtain a primitive root.

We would then have, for a candidate $|a|$ (not a perfect power) that we test, the expectation of $2A \sim 75\%$ of finding a primitive root, compared to the expectation of at most $\frac{6}{5}A \sim 45\%$ in case we do not make use of negative numbers.

Disclaimer: There seems to be a small bias for the least primitive root in absolute value to be positive (experiments suggest a density that is slightly above 50%).

Remark: The expectation that -3 is a primitive root is higher than the one for 3. However, if we suppose that ± 2 are not primitive roots, then the expectation that -3 is a primitive root is lower than the one for 3.

On the candidates to be tested

It would be possible to keep track of information from previously discarded candidates and construct primitive roots that are not necessarily prime numbers. (And it would also be possible to allow rational numbers to be primitive roots.) Without those information, heuristics say that it is slightly more advantageous to take a new candidate that is multiplicatively independent from the previous ones, as in the list of prime numbers.

By considering the primes p up to 10^9 (if $p \equiv 3 \bmod 4$ we consider candidates up to sign) it does not seem that taking as candidate a combination of previously tested primes is significantly more promising than testing the next prime:

candidate (in absolute value)	$p \equiv 1 \bmod 4$	$p \equiv 3 \bmod 4$
2 or 3	61.9%	90.6%
a combination of 2,3	71.1%	93.0%
2 or 3 or 5	73.3%	96.2%
a combination of 2,3,5	85.9%	97.9%
2 or 3 or 5 or 7	81.2%	98.4%
a combination of 2,3,5,7	93.2%	99.334%
2 or 3 or 5 or 7 or 11	86.6%	99.282%
a combination of 2,3,5,7,11	96.7%	99.785%
2 or 3 or 5 or 7 or 11 or 13	90.5%	99.670%

Selecting a candidate according to $p \bmod f$

Let $f \ge 2$ be an integer and $m \le f$ a positive integer coprime to f. We consider the set $\mathcal{P}_{m,f}(a)$ of primes p such that $p \equiv m \pmod f$ and a is a primitive root modulo p. Under GRH, the density of $\mathcal{P}_{m,f}(a)$ exists and it depends on a, see [2] by Moree.

As a precomputation, we fix f and for each m compute an integer g (not a perfect power) such that the density of $\mathcal{P}_{m,f}(g)$ is maximal. The expectation P_k that g selected with $f = 2p_1 \cdots p_k$ (p_i being the i-th prime number) is a primitive root is at most $2A \sim 75\%$, and we have

k	P_k/A	$P_k \sim$	k	P_k/A	$P_k \sim$
1	1	37%	4	1522/779	73.1%
2	9/5	67%	5	167878/84911	73.9%
3	181/95	71%	6	26172722/13161205	74.4%

One choice of g depending on $p \bmod 4 \cdot 3 \cdot 5 \cdot 7$ is as follows:

$p \bmod 4$	$p \bmod 3$	$p \bmod 5$	$p \bmod 7$	g
1	1	1 or 4	1, 2, or 4	2
1	1	1 or 4	3, 5, or 6	7
1	1	2 or 3	any	5
1	2	any	any	3
3	1	any	any	3
3	2	any	any	-3

References

[1] C. Hooley. *On Artin's conjecture*. J. Reine Angew. Math. 225 (1967), 209–220.

[2] P. Moree. *On primes in arithmetic progression having a prescribed primitive root. II*. Funct. Approx. Comment. Math. 39 (2008), 133–144.

[3] A. Perucca and C. Sanna. *Primitive root candidates*. Submitted for publication, available online:

https://orbilu.uni.lu/handle/10993/67069