COMPUTING PRIMITIVE ROOTS ACCORDING TO ARTIN'S CONJECTURE

ANTONELLA PERUCCA AND MIA THOLL

Abstract. If p is a prime number, a primitive root modulo p is an integer a such that (a mod p) generates multiplicatively the group of non-zero residues modulo p. For finding a primitive root modulo p, one can try out candidates. The aim of this text is discussing which candidates to try first, heuristically, according to Artin's conjecture on primitive roots.

1. Introduction

Primitive roots are key to modular arithmetic. If p is a prime number, then an integer a is called a *primitive root* modulo p if (a mod p) is a generator of the multiplicative group at p. The aim of this text is discussing how to find a primitive root modulo p by testing candidates, according to the predictions of *Artin's conjecture on primitive roots*. This conjecture deals with certain sets of prime numbers, whose size can be measured by a so-called *natural density* (which is a real number from 0 to 1). Intuitively, if a set of primes is defined by some condition, then one may think of its density as the probability for primes, on average, to satisfy the given condition. For example, 50% of the primes p are such that $p \equiv 1 \bmod 3$ means that the density of the primes p with this property among all primes is 0.5.

Under the Generalized Riemann Hypothesis, Artin's conjecture is a mathematical theorem that determines the natural density of the primes p for which some given integer a is a primitive root modulo p. We call this the *Artin density* of a. Thanks to the Artin densities and related densities we get expectations for primitive roots modulo a fixed prime p.

This text relies on well-known facts about modular arithmetic, group theory, and number theory. For a friendly introduction to Artin's conjecture we recommend the survey by Pieter Moree [2]. Kummer theory is explained for example in [1]. The only result that we apply which might be less known to the reader is Schinzel's theorem on Abelian radical extensions [3, Theorem 2].

1.1. The candidates 2 and −3.

Denoting by

$$A := \prod_{\ell\,\mathrm{prime}} \Big(1 - \frac{1}{\ell(\ell-1)}\Big) \sim 0.37$$

the Artin constant, the Artin density for 2 is $A \sim 37\%$ while the Artin density for -3 is as large as possible, namely it is $\frac{6}{5}A \sim 45\%$. Suppose that you search for a primitive root modulo p by trying out candidates from a list, one after the other. Believing in Artin's conjecture, the first candidate to try seems to be -3. However, the conditions "2 is a primitive root" and "-3 is a primitive root" are not independent and, in some sense, it may not matter much which candidate one tries first, as we explain below.

For p an odd prime, an integer a can only be a primitive root modulo p if it is a non-square modulo p (if a is not a square, the set of primes p such that a is a non-square modulo p has density $1/2$). So let's restrict to the primes such that 2 and -3 are both non-squares modulo p, and let's rescale the density so that this overset has density 1. This conditional Artin density is the same for 2 and -3, namely it is $\frac{12}{5}A \sim 90\%$. So, if testing for squares modulo p takes negligible effort, then it would not matter (heuristically) which candidate between 2 and -3 we test first for being a primitive root.

2. Preliminaries

2.1. **Primitive roots.** If we fix some prime number p, then a *primitive root modulo* p is some integer a coprime to p such that the smallest integer x such that $(a^x \bmod p) \equiv (1 \bmod p)$ equals $p-1$. The residues classes of the primitive roots are then precisely the generators of the *multiplicative group* at p (namely, the cyclic group of order $p-1$ consisting of the non-zero residues modulo p with the multiplicative structure).

Since 1 is a primitive root modulo 2 and -1 is a primitive root modulo 3, we may suppose in what follows that $p \geq 5$. Thanks to this assumption, any square modulo p is not a primitive root, and -1 is also not a primitive root.

Remark that a is a primitive root modulo p if and only if for every prime $\ell \mid (p-1)$ the element $(a \bmod p)$ has no ℓ-th roots, which equivalently means that $(a \bmod p)$ is not an ℓ-th power. We also remark that, if n is coprime to $p-1$, then a^n is a primitive root if and only if a is a primitive root.

Every element in the multiplicative group at p has an *index* and an *order*, that are positive integers whose product is $p-1$. In particular, to ensure that the index is 1, we only have to show that the index is not divisible by any prime divisor of $p-1$.

For a coprime to p, the property that a is a primitive root modulo p is equivalent to saying that the index of $(a \bmod p)$ equals 1. Moreover, $(a \bmod p)$ is not an ℓ-th power if and only if its index is coprime to ℓ.

We discuss a list of integers to be tested for being primitive roots. We may restrict to considering the integers in the range from 2 to $\frac{p-1}{2}$ and their negatives. Let a be an integer in this set. If $a = \pm b^n$ holds for some integer b and for some $n > 1$, then we may discard $\pm a$ provided that we test $\pm b$ (in fact, neither a nor $-a$ are primitive roots if $\pm b$ were no primitive roots).

2.2. **Group theory.** We consider a cyclic group of prime order ℓ. In such a group, the identity is the only non-generator. Thus the product of two non-generators is a non-generator, while the product of a generator and a non-generator is a generator. We consider a probability framework where we extract elements of this group, each element having the same probability $\frac{1}{\ell}$.

Remark 1. *An element of the group is a generator with probability* $1 - \frac{1}{\ell}$ *(we have to exclude the identity) while the product of two generators is a generator with probability* $1 - \frac{1}{\ell - 1}$ *(we have to exclude that the second factor is the multiplicative inverse of the first). So the product of two generators is biased towards being a* *non-generator. The product of a fixed element and an element over which we have no information has the usual probability of being a generator ($1-\frac{1}{\ell}$ probability).*

2.3. **Kummer theory.** Let ℓ be an odd prime, and let a be an integer that is not an ℓ-th power. Then the extension $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{a})/\mathbb{Q}(\zeta_\ell)$ is a cyclic extension of order ℓ and a Kummer extension (remark that the degree of the cyclotomic extension is coprime to ℓ). Call G_ℓ its Galois group, and fix some root of unity ζ_ℓ of order ℓ.

The Kummer map for the above Kummer extension is the group homomorphism

$$G_\ell \to \langle \zeta_\ell \rangle \qquad \sigma \mapsto \frac{\sigma(\sqrt[\ell]{a})}{\sqrt[\ell]{a}}$$

which does not depend on the choice of $\sqrt[\ell]{a}$. Supposing that $\ell \mid (p-1)$ we call $Frob_p$ the Frobenius at p in the Galois group of $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{a})/\mathbb{Q}(\zeta_\ell)$, which we see as a subgroup of $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{a})/\mathbb{Q}$. The image under the Kummer map of $Frob_p$ is a root of unity of order dividing ℓ, which we call ζ_ℓ^t (remark that t depends on p).

For later use, remark that if $\zeta_\ell^{t_a}$ and $\zeta_\ell^{t_b}$ are the images of the Frobenius at p considering integers a and b respectively, then the image considering ab is the product $\zeta_\ell^{t_a}\zeta_\ell^{t_b} = \zeta_\ell^{t_a+t_b}$.

Remark 2. *Suppose that $\ell \mid (p-1)$, which means that p splits completely in $\mathbb{Q}(\zeta_\ell)$. Assuming that a and p are coprime, the index of $(a \bmod p)$ is divisible by ℓ if and only if p splits completely in $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{a})$.*

The divisibility conditions in the above remark for $\ell \neq 2$ are independent thanks to the following lemma.

Lemma 3. *Fix an integer a. For any finite set S of odd prime numbers the following holds: for $\ell \in S$ the fields $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{a})$ are linearly disjoint over $\mathbb{Q}$.*

Proof. By Schinzel's Theorem on Abelian radical extensions [3, Theorem 2] we have for every integer $n \geq 1$

$$\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{a}) \cap \mathbb{Q}(\zeta_{n\ell}) = \mathbb{Q}(\zeta_\ell)\,.$$

We may easily conclude by considering that the Kummer extensions (on top of the cyclotomic extensions) have pairwise coprime degrees. □

3. Negative numbers as primitive roots

3.1. **Excluding negative numbers if $p \equiv 1 \bmod 4$.** Suppose that $p \equiv 1 \bmod 4$. In this case, if some integer a is not a primitive root modulo p, then the same holds for $-a$. This is because if a is a square modulo p (respectively, the index of ($a \bmod p$) has some odd prime factor) then the same holds for $-a$. Consider the integers in the range from 1 to $\frac{p-1}{2}$ and their negatives (such numbers represent all non-zero residue classes modulo p). We may then restrict to only test the positive integers in the above range for being a primitive root.

3.2. **Including negative numbers if $p \equiv 3 \bmod 4$.** Suppose that $p \equiv 3 \bmod 4$, and let a be some integer coprime to p. There are two reasons for a not being a primitive root modulo p. On the one hand, if a is a square modulo p, then surely $-a$ is not a square modulo p. On the other hand, if the index of ($a \bmod p$) has some odd prime factor, then the same holds for $-a$. If we discard a for being a square modulo p and we do not make further checks, then there is no reason to discard $-a$.

Remark 4. *We should choose as candidate for being a primitive root modulo p the integer a with best chances so that the index of $(a \bmod p)$ has no odd prime factors. This is because, if this condition is met, then the integer among $\pm a$ that is not a square modulo p is a primitive root. In fact, we should immediately test whether $(a \bmod p)$ has no odd prime factors in the index. Only in the affirmative we should test whether $(a \bmod p)$ is a square to select correctly the primitive root among a and $-a$.*

3.3. **Safe primes.** Suppose that p is a safe prime, by which we mean that $p-1$ is two times a cryptographically large prime number. Examples where $p-1$ is twice an odd prime are the following: $p = 7, 11, 23, 47, 59, 83, \ldots$ Then the following applies:

Remark 5. *If $p-1$ is twice an odd prime, then the only non-square modulo p that is not a generator of the multiplicative group is $(-1 \bmod p)$. Consequently, -4 is a primitive root and either 2 or -2 is a primitive root.*

More generally, suppose to test whether a is a primitive root in the setting where $p-1 = sq$, where s is a small number and q is a large prime. Then for every prime $\ell \mid s$ one could test whether a has no ℓ-th roots modulo p. In the affirmative, either the index of $(a \bmod p)$ is 1 (which means that a is a primitive root) or the index of $(a \bmod p)$ is q. To rule out the latter possibility, we have to exclude that the order of $(a \bmod p)$ equals s. In case we know the non-zero residue classes modulo p of order dividing s, we have an alternative strategy: we can construct a primitive root from a non-zero residue class whose index is coprime to q (by multiplying it with the appropriate residue class of order dividing s).

4. Heuristical framework

For a fixed integer a and by varying p, the conditions "a is a square modulo p" and "the index of a modulo p has some odd prime factor" are not independent. This is precisely the reason for the correction factor in Hooley's formulas for the Artin density. Consequently, if the Artin density of a is less than/equal to/larger than the Artin constant, then the fact that a is a square modulo p makes it less likely/equally likely/more likely that the index of $(a \bmod p)$ has some odd prime factor. Our setting is different, namely we fix p and vary a. Nevertheless, we study it with "expectations" that come by considering all primes. For example, we say that the expectation that 2 is a primitive root modulo 3 is $A \sim 37\%$ (despite the fact that 2 is a primitive root modulo 3).

We call *odd expectation* the expectation for an integer a of being a primitive root modulo the given prime p conditioned to the information that $(a \bmod p)$ is not a square. Let ℓ be an odd prime divisor of $p-1$. We call *ℓ-expectation* the expectation for an integer a coprime to p of having index coprime to ℓ, conditioned to the property that $(a \bmod p)$ is not a square.

The following two claims are the simplifications that we require for our heuristics. In the claims ℓ is an odd prime divisor of $p-1$ and a is an integer coprime to p that is not an n-th power for any $n > 1$. In particular, p splits completely in $\mathbb{Q}(\zeta_\ell)$.

(i) The expectation that p splits completely in $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{a})$ equals $\frac{1}{\ell}$, and also if we condition this with information about the splitting behavior of p in finitely many quadratic extensions.

(ii) Let ζ_ℓ^t be the root of unity defined in Section 2.3. Then $(t \bmod \ell)$ has expectation $\frac{1}{\ell}$ of being any fixed residue modulo ℓ. This still holds if we condition this with information about the splitting behavior of p in finitely many quadratic extensions.

The last part of the first claim is because the splitting behavior in an extension of odd degree is not affected by the splitting behavior in an extension of degree 2. Moreover, both claims are true "on average" by the Dirichlet density theorem. Indeed, on average, the first (respectively, second) claim amounts to that result applied to the identity (respectively, any element) of the Galois group of the Kummer extension $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{a})/\mathbb{Q}(\zeta_\ell)$, which is a cyclic group of order ℓ.

According to the following heuristics, all non-squares modulo p are equally eligible for being primitive roots.

Remark 6. *By the first claim, all integers that are not n-th powers for $n > 1$ have the same odd expectation*

$$\prod_{\substack{\ell \text{ prime} \\ \ell \mid (p-1)}} \left(1 - \frac{1}{\ell}\right).$$

Indeed, call S the set of odd prime divisors of $p-1$, and let a be an integer that is not a square modulo p. Then a is a primitive root modulo p if and only if for every $\ell \in S$ the index of $(a \bmod p)$ is coprime to ℓ. Such coprimality conditions are independent by Lemma 3 and we may conclude by the first claim.

Remark 7. *Let a, b, c be integers coprime to p satisfying $a = bc$. Suppose that a, c are not n-th powers for $n > 1$. By the second claim, the odd expectation for a is the same after conditioning it with information on the odd expectation of b, provided that the odd expectation for c is unaltered when conditioned to information concerning the odd expectation for b. Indeed, as before, we may fix some prime $\ell \mid (p-1)$ and investigate whether the index of $(a \bmod p)$ is coprime to ℓ. By the second claim, we can apply the last assertion of Remark 1 to the group of roots of unity of order dividing ℓ, seen as the codomain of the Kummer map applied to the Galois group of the Kummer extension $\mathbb{Q}(\zeta_\ell, \sqrt[\ell]{a})/\mathbb{Q}(\zeta_\ell)$.*

With a similar reasoning we have:

Remark 8. *Let ℓ be an odd prime divisor of $p-1$. By the first claim, all integers that are not n-th powers for $n > 1$ have the same ℓ-expectation, namely $(1 - \frac{1}{\ell})$. Moreover, we may replace odd expectation by ℓ-expectation in Remark 7.*

5. Composite numbers as primitive roots

The considerations in this section are heuristics based on a uniformity assumption (namely, the two claims seen in the previous section). In fact, composite numbers don't have specific reasons for not being primitive roots (see Remark 6). However, the odd expectation for a composite number is affected by information that we gain by having tested candidates for being primitive roots.

Example 9. *Suppose that you have tested 2 and 3 and none of them is a primitive root and suppose that precisely one of them is a square modulo p, so that $(6 \bmod p)$ is not a square and hence is potentially eligible as being a primitive root. Without loss of generality, suppose that $(2 \bmod p)$ was discarded for being a square and that $(3 \bmod p)$ was discarded for having odd factors in the index. Then we have* *no information on the odd expectation for* 2 *(the fact that* 3 *is multiplicatively independent from* 2 *ensures that the odd expectation for* 2 *is not affected by the behavior of* 3*). Then by Remark 7 we have no information on the odd expectation for* 6 *and hence no reason to discard it from our list of candidates.*

Clearly, when in doubt, we should rather discard an element from the list of candidates. However, as the following example also shows, a finite check involving small numbers might tell us that in some cases we may safely keep a composite number on our list of candidates according to the previously collected information.

Example 10. *Suppose that the following numbers have been tested and they are all not primitive roots modulo* p*:*

$$2 \qquad 3 \qquad 5 \qquad 6 \qquad 7\,.$$

Moreover, suppose that $(10 \bmod p)$ *is not a square.*

If $(5 \bmod p)$ *is a square, then we can apply Remark 7 with* $b = 5$ *(because* 5 *is not affected by the information at* $2, 3, 6, 7$*). In this case, we should keep* 10 *on the list of candidates.*

Else, $(2 \bmod p)$ *is a square so having discarded* $2, 5, 7$ *gives no information on the odd expectation of* 2*. If* $(3 \bmod p)$ *is a square, then we also have not collected information on the odd expectation of* $3, 6$ *hence by Remark 7 with* $b = 2$ *we should keep* 10 *on the list of candidates.*

Finally notice that, if we know the odd primes $\ell \mid (p-1)$, the above analysis should be refined by replacing the odd expectation with the list of ℓ-expectations.

Acknowledgements

The authors thank Yannick Baraud, Fritz Hörmann, Olli Järviniemi, Hendrik Lenstra, Pieter Moree, Francesco Pappalardi, Giovanni Peccati, Tim Seuré, Igor Shparlinski, and especially Andrew Sutherland (MIT) for fruitful exchanges, explanations or comments.

References

[1] Lang, S., *Algebra*, Graduate Texts in Mathematics 211, Springer New York (2011).

[2] Moree, P., *Artin's primitive root conjecture – a survey*, Integers **12** (2012), no. 6, 1305–1416.

[3] Schinzel, A., *Abelian binomials, power residues and exponential congruences*, Acta Arith. **32** (1977), no. 3, 245–274. Addendum, ibid. **36** (1980),101–104. See also Andrzej Schinzel Selecta Vol.II, European Mathematical Society, Zürich, 2007, 939–970.

Department of Mathematics, University of Luxembourg, 6 av. de la Fonte, 4364 Esch-sur-Alzette, Luxembourg

Email address: antonella.perucca@uni.lu