On a conjecture stronger than Artin's primitive root conjecture

Pieter Moree

In 1927 Artin conjectured that if $a \neq -1$ or a perfect square, then a is a primitive root mod p for infinitely many primes p or, in other words, $< a >= \mathbb{F}_p^*$ for infinitely many primes p. Under the assumption that the Riemann Hypothesis holds for certain number fields, a quantitative version of the conjecture was proved by Hooley [4]. Hooley's result implies that $N_a(x)$, the number of primes $p \le x$ such that $< a >= \mathbb{F}_p^*$, grows asymptotically as $cAx/\log x$, where c is a non-zero rational number that depends on a and can be explicitly given and where

$$A = \prod_p (1 - \frac{1}{p(p-1)}) \approx 0.3739558,$$

is the *Artin constant.* The best known unconditional result today is due to Heath-Brown [2], who proved, extending work of Gupta and Ram Murty [2], the following result:

Theorem 1. *Let q, r, s be nonzero integers which are multiplicatively independent, i.e. if $q^e r^f s^g = 1$ and, e, f, g are integers, imply $e = f = g = 0$. Let us suppose that none of the integers q, r, s, $-3qr$, $-3qs$, qrs is a square. Then the number $N_{q,r,s}(x)$ of primes $p \le x$ for which at least one of q, r, s is a primitive root, satisfies $N_{q,r,s}(x) \gg x(\log x)^{-2}$.*

Corollary 1. *If q, r and s are three distinct primes, then at least one of them is a primitive root for infinitely many primes.*

In Reznikov's work the question comes up whether or not for a given prime l the set $\mathcal{P}_l$ of primes p such that l is a primitive root mod p and, moreover, $p \equiv \pm 1 (\mathrm{mod}\ l)$, is infinite. This question and the ensuing one about the prime density of the set $\mathcal{P}_l$ are considered in this appendix. (If S is a set of prime numbers, then $S(x)$ denotes the number of primes in S that do not exceed x. The set S is said to have a prime density (or natural density) if $\lim_{x\to\infty} S(x)/\pi(x)$ exists. Here $\pi(x)$ denotes the number of rational primes not exceeding x.) For $l = 2, 3$ the first question amounts to Artin's conjecture with $a = 2, 3$. If $l \equiv 1 (\mathrm{mod}\ 4)$, then l is not a primtive root mod p for any prime $p \equiv \pm 1 (\mathrm{mod}\ l)$. (By quadratic reciprocity one has $(l/p) = (p/l)$. Since $(p/l) = (\pm 1/l) = 1$, it follows that $(l/p) = 1$, therefore $l^{(p-1)/2} \equiv 1 (\mathrm{mod}\ p)$ and so l is not a primitve root mod p.) If $l \equiv 3 (\mathrm{mod}\ 4)$, it is easily seen that there are infinitely many primes p such that $(l/p) = -1$. Thus in this case there are no 'quadratic obstructions' for l to be a primitive root mod p. Indeed, the next result shows that, under an appropriate version of the Generalized Riemann Hypothesis, for these l there are no obstructions at all:

Theorem 2. *Let l be a rational prime. Put $K = \mathbb{Q}(\zeta_l + \zeta_l^{-1})$. For $r \ge 1$ put $K_r = K(\zeta_r, l^{1/r})$. Suppose the Riemann Hypothesis is true for the fields K_r for all squarefree r. Then the set $\mathcal{P}_l$ of primes p such that $< l >= \mathbb{F}_p^*$ and $p \equiv \pm 1 (\mathrm{mod}\ l)$ has a prime density $\delta(l)$. Furthermore,*

a) $\delta(2) = A$.

b) If $l \equiv 1 (\mathrm{mod}\ 4)$, then $\mathcal{P}_l$ is empty (thus $\delta(l) = 0$).

c) If $l \equiv 3 (\mathrm{mod}\ 4)$, then

$$\delta(l) = \frac{2l-1}{l^2-l-1} A > 0.$$

d) The set $\mathcal{P}_l$ *is infinite if and only if* $\sqrt{l} \notin K$.

Proof. a) This is a particular case of the Theorem of [4].

b) This is an easy consequence of quadratic reciprocity, as we have already seen and, moreover, is unconditionally true.

c) Put $n_r = [K_r : \mathbb{Q}]$. It is well-known that $p \equiv \pm 1 (\mathrm{mod}\ l)$ iff p splits completely in K. By [6, Theorem 3] one then finds that

$$\delta(l) = \sum_{r=1}^{\infty} \frac{\mu(r)}{n_r},$$

under the assumption on the fields K_r delineated in the statement of Theorem 2. Here μ denotes the Möbius function. If r is odd and $l \nmid r$, then $n_r = \varphi(rl)r/2$. If r is odd and $l|r$, then $n_r = \varphi(r)r$. If $r \equiv 2 (\mathrm{mod}\ 4)$ and $l \nmid r$, then $n_r = \varphi(rl)r/2$. If $r \equiv 2 (\mathrm{mod}\ 4)$ and $l|r$, then $n_r = \varphi(r)r$. (For details cf. [4] or [1, Chapter 3].) Thus

$$\begin{aligned}\delta(l) &= \frac{2}{\varphi(l)} \sum_{\substack{r=1 \\ 2\nmid r,\ l\nmid r}}^{\infty} \frac{\mu(r)}{\varphi(r)r} + \sum_{\substack{r=1 \\ 2\nmid r,\ l|r}}^{\infty} \frac{\mu(r)}{\varphi(r)r} + \frac{2}{\varphi(l)} \sum_{\substack{r=1 \\ 2|r,\ l\nmid r}}^{\infty} \frac{\mu(r)}{\varphi(r)r} + \sum_{\substack{r=1 \\ 2|r,\ l|r}}^{\infty} \frac{\mu(r)}{\varphi(r)r} \\ &= S_1 + S_2 + S_3 + S_4.\end{aligned}$$

Put $A_l = \prod_{p\nmid 2l}(1-1/p(p-1))$. Using the multiplicativity of μ and φ one easily checks that $S_1 = A_l 2/\varphi(l)$, $S_2 = -A_l/(l\varphi(l))$, $S_3 = -A_l/\varphi(l)$ and that $S_4 = A_l/(2l\varphi(l))$. Summing them together yields $\delta(l) = A(2l-1)/(l^2-l-1)$, as required.

d) K is the maximal real subfield of $\mathbb{Q}(\zeta_l)$. Since $\sqrt{l}$ is real it is in K if and only if it is in $\mathbb{Q}(\zeta_l)$. From [8, p. 263] for example, it follows that $\sqrt{l} \in \mathbb{Q}(\zeta_l)$ if and only if $l \equiv 1 (\mathrm{mod}\ 4)$. By a), b) and c) these are precisely the primes l for which $\mathcal{P}_l$ is finite. ■

Remark 1. We have $\delta(3) = A$, in agreement with the Theorem of [4].

Remark 2. If one calculates $\delta(l)$ in case $l \equiv 1 (\mathrm{mod}\ 4)$ by Hooley's method, one finds $\delta(l) = S_1 + S_2 + 2S_3 + 2S_4 = 0$, as one should.

Remark 3. Put $m_r = [K_r : K]$. A heuristic reasoning, cf. Murty [7], leads to an expected prime density of

$$\delta_{heur}(l) = \frac{1}{[K:\mathbb{Q}]} \prod_p (1 - \frac{1}{m_p}).$$

Indeed, on comparing the heuristic density with that obtained above, one finds that $\delta_{heur}(l) = \delta(l)$ for every prime l.

Theorem 2 shows what should be true, unconditionally, however, one has to be satisfied with a much more modest result:

Theorem 3. *If* $q,\ r,\ s$ *are three distinct primes each congruent to* $3 (\mathrm{mod}\ 4)$, *then for at least one of them, say* q, *there are infinitely many primes* p *such that* q *is a primitive root mod* p *and* $p \equiv \pm 1 (\mathrm{mod}\ q)$, *and moreover,* $|\{p \le x : \langle q \rangle = \mathbb{F}_p^*,\ p \equiv -1 (\mathrm{mod}\ q)\}| \gg x(\log x)^{-2}$.

The proof can be obtained by making minor modifications to Heath-Brown's proof of Theorem 1. We start with a lemma.

Lemma 1. *Let q, r and s be three non-zero integers which are multiplicatively independent. Suppose that none of q, r, s, $-3qr$, $-3qs$, $-3rs$ and qrs is a square. Then there exists a prime p_0 such that*

$$(\frac{-3}{p_0}) = (\frac{q}{p_0}) = (\frac{r}{p_0}) = (\frac{s}{p_0}) = -1$$

and $(p_0 - 1, 16qrs)|8$.
Proof. Asymptotically the sum

$$\sum_{p \le x} (1 - (\frac{-3}{p}))(1 - (\frac{q}{p}))(1 - (\frac{r}{p}))(1 - (\frac{s}{p}))$$

is not less than $\pi(x)$ (see [3, p. 35]). Thus there are infinitely many primes p satisfying

$$(1) \qquad (\frac{-3}{p}) = (\frac{q}{p}) = (\frac{r}{p}) = (\frac{s}{p}) = -1.$$

Using quadratic reciprocity and the supplementary law of quadratic reciprocity, we see that there exists an integer d with $16 \nmid d$ such that, for all p large enough, p satisfies (1) iff p is in a set of progressions modulo d. Since there are infinitely many primes p satisfying (1), this set must be non-empty. Since $16 \nmid d$, it follows using the prime number theorem for arithmetic progressions, that the number of primes $p \le x$ satisfying (1) and $p \not\equiv 1 (\text{mod } 16)$ is $\gg x/\log x$. Let $\omega(n)$ denote the number of distinct prime factors of n. Notice that there are at most $\ll \log^{\omega(qrs)} x$ primes $p \le x$ such that $p \not\equiv 1 (\text{mod } 16)$ and $(p-1, 16qrs) \nmid 8$. By taking x large enough, it then follows there exists a prime p_0 satisfying the conditions such that $(p_0 - 1, 16qrs)|8$. ■

From the proof of Theorem 1 given in [3] it is clear (see especially pp. 35-36) that it is actually a proof of the following slightly stronger statement:
Theorem 4. *Let q, r, s be nonzero integers which are multiplicatively independent. Suppose none of q, r, s, $-3qr$, $-3qs$, qrs is a square. Then the number $N'_{q,r,s}(x)$ of primes $p \le x$, $p \equiv p_0 (\text{mod } 16qrs)$, with p_0 as in Lemma 1, for which at least one of q, r, s is a primitive root, satisfies $N'_{q,r,s}(x) \gg x(\log x)^{-2}$.*

Now we are in the position to prove Theorem 2.
Proof of Theorem 2. We show that we can find p_0 satisfying the conditions of Lemma 1 and, in addition, $p_0 \equiv -1 (\text{mod } qrs)$. The result then follows from Theorem 4. So let p be a prime satisfying

$$(2) \qquad p \equiv 5 (\text{mod } 6), \ p \equiv 5 (\text{mod } 8) \text{ and } p \equiv -1 (\text{mod } qrs).$$

(There exist infinitely many such primes by the chinese remainder theorem and the prime number theorem for arithmetic progressions.) Since $p \equiv 5 (\text{mod } 6)$, $(-3/p) = -1$. Since $p \equiv 1 (\text{mod } 4)$, $(q/p) = (p/q)$. So, since $p \equiv -1 (\text{mod } q)$ and, by assumption, $q \equiv 3 (\text{mod } 4)$, $(q/p) = (-1/q) = -1$. Similarly, $(r/p) = (s/p) = -1$. By an argument as in the proof of Lemma 1 it can be shown that there exists a prime p_0 satisfying (2) such that in addition $(p_0 - 1, 16qrs)|8$. Thus p_0 satisfies the conditions of Lemma 1 and in addition $p_0 \equiv -1 (\mathrm{mod}\ qrs)$. Theorem 3 now follows from Theorem 4. ■

As we have seen Reznikov's question can be reformulated as: for which primes l are there infinitely many primes p such that l is a primitive root mod p and, moreover, p splits completely in $\mathbb{Q}(\zeta_l + \zeta_l^{-1})$. Under an appropriate version of the GRH, the answer is for those primes l such that $\sqrt{l} \notin \mathbb{Q}(\zeta_l + \zeta_l^{-1})$. This is a particular case of the following result.

Theorem 5. *Assume GRH. Let l be a rational prime and M an abelian number field. Put*

$$\mathcal{P}_M(l) := \{p > 2 : \langle l \rangle = \mathbb{F}_p^*,\ p \text{ splits completely in } M\}.$$

The set $\mathcal{P}_M(l)$ is infinite if and only $\sqrt{l} \notin M$. Moreover, if $\mathcal{P}_M(l)$ is infinite, then it has a positive prime density.

Proof. Since for odd q, $\mathbb{Q}(l^{1/q})$ is not normal, $\mathbb{Q}(\zeta_q, l^{1/q}) \not\subseteq M$. Using this and [5, Corollary 4.8], it then follows that $\mathcal{P}_M(l)$ is infinite if and only if $\sqrt{l} \in M$. The latter part of the assertion follows from [5, Theorem 4.6]. ■

Remark. It is easy to see that the condition $\sqrt{l} \notin M$ is necessary for $\mathcal{P}_M(l)$ to be infinite, for if $\sqrt{l} \in M$, then the equation $x^2 \equiv l (\mathrm{mod}\ p)$ has a solution for all odd primes p that split completely in M and thus $\mathcal{P}_M(l)$ is empty.

REFERENCES

[1] C. Ballot, Density of prime divisors of linear recurrences, *Mem. of the Amer. Math. Soc.* **551**, 1995.

[2] R. Gupta and P. M. Ram Murty, A remark on Artin's conjecture, *Invent. Math.* **78** (1984), 127-130.

[3] R. Heath-Brown, A remark on Artin's conjecture, *Quart. J. Math. Oxford* **37** (1986), 27-38.

[4] C. Hooley, Artin's conjecture for primitive roots, *J. Reine Angew. Math.* **225** (1967), 209-220.

[5] H. W. Lenstra, jr., On Artin's conjecture and Euclid's algorithm in global fields, *Invent. Math.* **42** (1977), 201-224.

[6] P. Moree, On a conjecture of Rodier on primitive roots, MPI-preprint 117, Bonn, 1996.

[7] P. M. Ram Murty, Artin's conjecture for primitive roots, *Math. Intelligencer* **10** (1988), 59-67.

[8] E. Weiss, *Algebraic Number Theory*, McGraw-Hill, New York etc., 1963.

Max-Planck-Institut für Mathematik
Gottfried-Claren-Str. 26
53225 Bonn
Germany
E-mail: moree@antigone.mpim-bonn.mpg.de