On a conjecture of Rodier on primitive roots

Pieter Moree

Max-Planck-Institut
für Mathematik
Gottfried-Claren-Str. 26
53225 Bonn

Germany

MPI 96-117

On a conjecture of Rodier on primitive roots

Pieter Moree

September 5, 1996

Keywords: Artin's conjecture, primitive root, natural density, uniform distribution. Let $\{p_j\}$ be the ordered sequence of primes p such that 2 is a primitive root mod p. Weakly uniform distribution (WUD) mod 28 of this sequence would imply a conjecture of Rodier. However, on the Generalized Riemann Hypothesis (GRH), it is shown that $1, 2$ and 4 are the only values of d such that $\{p_j\}$ is WUD mod d. Moreover, Rodier's conjecture is disproved, on GRH.

1 Introduction

An integer a is said to be a primitive root mod p if its order in $\mathbb{Z}/p\mathbb{Z}$ is $p-1$ (and thus maximal). Let $\mathcal{P}_{28}$ denote the set of primes p such that $p \equiv -1, 3, 19 (\text{mod } 28)$ and 2 is a primitive root mod p. In [5] Rodier, in connection with a coding theoretical result involving Dickson polynomials, made the conjecture that the (natural) density of the set $\mathcal{P}_{28}$ is $A/4$, where

$$A = \prod_{p \text{ prime}} (1 - \frac{1}{p(p-1)}) \quad (\approx 0.3739558136192),$$

is *Artin's constant.* On noticing that the primes $p \equiv -1, 3, 19 (\text{mod } 28)$ are precisely those such that $(p/7) = -1$ and $p \equiv 3 (\text{mod } 4)$, it follows from Theorem 1 that, on GRH, the prime density of $\mathcal{P}_{28}$ is $21A/82$. Thus Rodier's conjecture, if true, would imply the falsity of the Generalized Riemann Hypothesis.

Theorem 1 (GRH). *Let $l_1, \ldots, l_s$ be distinct odd primes and $\epsilon_0, \ldots, \epsilon_s \in \{\pm 1\}$. Let $N(x)$ denote the number of primes $p \le x$ satisfying*

i) 2 is a primitive root mod p,

ii) $(p/l_j) = \epsilon_j$, $1 \le j \le s$.

Then

$$N(x) = \frac{A}{2^s} \prod_{j=1}^{s} (1 - \frac{\epsilon_j}{l_j^2 - l_j - 1}) \frac{x}{\log x} + O(\frac{x \log\log x}{\log^2 x}). \quad (1)$$

Moreover, if in addition to i) and ii) it is required that $p \equiv \epsilon_0$ (mod 4), then (1) holds with $A/2^s$ replaced by $A/2^{s+1}$.

Taking an heuristic approach might lead one to think that the density of $\mathcal{P}_{28}$ should be $A/4$. Let $\mathcal{P}$ denote the set of primes p such that 2 is a primitive root mod p. Subject to GRH the density of $\mathcal{P}$ is A, as was shown by Hooley in his classical memoir [1], in which he proved, on GRH, a quantitative version of a conjecture made by Emil Artin in 1927. Since there are $\varphi(28) = 12$ primitive congruence classes mod 28, the density of primes from $\mathcal{P}$ in each of them would be $A/12$, on assuming WUD (see [4] for a definition) mod 28. Thus one arrives at a density of $A/4$ for the set $\mathcal{P}_{28}$. The sequence $\{p_j\}$ is, however, not WUD mod 28. Indeed Theorem 1 can be used to show:

Theorem 2 (GRH). *The sequence $\{p_j\}$ is WUD mod d if and only if $d \in \{1, 2, 4\}$.*

A. Reznikov [3], in the course of his investigations of a conjecture of Lubotzky and Shalov on three-manifolds, arrived at the problem whether for a given prime l, the set of primes p such that l is a primitive root mod p and $p \equiv \pm 1 \pmod{l}$ is infinite. Reznikov's question and Rodier's conjecture suggest a more general problem: Let $a \neq \pm 1$ be a integer and M a number field. Determine whether or not the set of primes p such that a is a primitive root mod p and, moreover, p splits completely in M, is infinite. In case it is infinite, determine whether it has a density, and if yes, compute the density. A first step in this is made by the following generalization of Hooley's classical result, that will be proved in the next section. Theorem 3 will be the starting point of the proof of Theorem 1, which on its turn is the starting point of the proof of Theorem 2. (As usual μ denotes the Möbius function.)

Theorem 3 *Let M be Galois and $a \neq \pm 1$ an integer. Suppose the Riemann Hypothesis holds for the fields $M_r := M(\zeta_r, a^{1/r})$ for every squarefree r. Then $N_M(a;x)$, the number of primes p not exceeding x that split completely in M and such that a is a primitive root mod p, satisfies*

$$N_M(a;x) = \delta(M)\frac{x}{\log x} + O\left(\frac{x \log\log x}{\log^2 x}\right), \tag{2}$$

where

$$\delta(M) = \sum_{r=1}^{\infty} \frac{\mu(r)}{[M_r : \mathbb{Q}]}. \tag{3}$$

(Since $[M_r : \mathbb{Q}] \geq [\mathbb{Q}_r : \mathbb{Q}] \gg r\varphi(r) \gg r^2/\log\log r$, the series for $\delta(M)$ is convergent.)

The author thanks Don Zagier for some helpful suggestions, Patrick Solé for pointing out Rodier's conjecture to him and F. Rodier for sending [5].

2 Proof of Theorem 3

Since the proof is a straightforward generalization of Hooley's proof in [1], we will only discuss the fine points. Let $\mathfrak{P}_M$ denote the set of primes that split completely in M. Put $m_r = [M_r : \mathbb{Q}]$. The analysis of the error terms can be taken over unchanged on using that the set of primes that split completely in M is a subset of the set of all primes. Thus the problem reduces to showing that (2) holds with $N_M(a;x)$ replaced by $N_M(a;x,\zeta_1)$, which is defined as the cardinality of the set

$$\{p \leq x: \ p \in \mathfrak{P}_M, \ l \leq \zeta_1, \ l \nmid [\mathbb{F}_p^* :< a >] \ \}, \ l \text{ prime},$$

with $\zeta_1 = \log x/6$. By inclusion and exclusion one finds

$$N_M(a;x,\zeta_1) = \sum_{P(r)\leq\zeta_1} \mu(r)\pi_{M_r}(x),$$

where

$$\pi_{M_r}(x) = |\{p \leq x : p \in \mathcal{P}_M, \ r|[\mathbb{F}_p^* :< a >]\}|,$$

and $P(r)$ denotes the greatest prime divisor of r. Now $r|[\mathbb{F}_p^* :< a >]$ and p splits completely in M if and only if p splits completely in M_r. Thus $\pi_{M_r}(x)$ is the number of primes not exceeding x that splits completely in M_r. The analysis of Hooley of this quantity ([1, §5]) in case $M = \mathbb{Q}$ rests on the fact that the discriminant of $\mathbb{Q}_r$ is bounded by r^{cm_r}, where c is a constant and the fact that $\mathbb{Q}_r$ is Galois. One checks that both properties are satisfied for M_r as well. Thus, we deduce that, under the Riemann Hypothesis for M_r, the following estimate holds true:

$$\pi_{M_r}(x) = \frac{\mathrm{li}(x)}{m_r} + O(\sqrt{x}\log(rx)), \tag{4}$$

where $\mathrm{li}(x)$ denotes the logarithmic integral and the implied constant depends at most on M. Thus, equation (29) of [1] now becomes

$$N_M(a;x,\zeta_1) = \mathrm{li}(x)\sum_{r=1}^{\infty}\frac{\mu(r)}{m_r} + O(\mathrm{li}(x)\sum_{r>\zeta_1}\frac{1}{r\varphi(r)}) + O(\frac{x}{\log^2 x}),$$

on using that $m_r \gg r\varphi(r)$. This simplifies to

$$N_M(a;x,\zeta_1) = (\sum_{r=1}^{\infty}\frac{\mu(r)}{m_r})\frac{x}{\log x} + O(\frac{x}{\log^2 x}).$$

Thus (2) holds with $N_M(a;x)$ replaced by $N_M(a;x,\zeta_1)$. □

Remark. An alternative way of establishing (4) is to make use of $(11RH)$ of [2], which together with the upper bound r^{cm_r} for the discriminant of M_r, where c is a constant depending at most on M, yields that [1, (27)] is valid for M_r, under RH on M_r. From this estimate and the fact that M_r is Galois, (4) is easily deduced.

3 Proof of Theorem 1

We start by a few propositions involving degrees of certain number fields M_r, $r \geq 1$. Since these degrees are only used in the context of computing $\delta(M)$, see (3), it is enough to compute them for r squarefree only. As usual $\omega(d)$ denotes the number of distinct prime divisors of d.

Proposition 1 *Put* $n_r = [\mathbb{Q}(\zeta_r, 2^{1/r}) : \mathbb{Q}]$. *Then, for* $8 \nmid r$, $\mathbb{Q}(\zeta_r)$ *and* $\mathbb{Q}(2^{1/r})$ *are linearly disjoint and hence* $n_r = r\varphi(r)$.

Proof. Every subfield of $\mathbb{Q}(\zeta_r)$ is normal. All the normal subfields of $\mathbb{Q}(2^{1/r})$ are contained in $\mathbb{Q}(\sqrt{2})$. Since $\sqrt{2} \in \mathbb{Q}(\zeta_r)$ if and only if $8|r$, it follows that for $8 \nmid r$, $\mathbb{Q}(2^{1/r})$ and $\mathbb{Q}(\zeta_r)$ are linearly disjoint and thus $n_r = r\varphi(r)$. □

Proposition 2 *Let* $l_1, \ldots, l_s$ *be distinct odd primes. Put* $l_j^* = (-1/l_j)l_j$, $1 \le j \le s$. *Let* $r \ge 1$. *Put* $d = (l_1 l_2 \cdots l_s, r)$. *Then, for* $8 \nmid r$, $[\mathbb{Q}(\sqrt{l_1^*}, \ldots, \sqrt{l_s^*}, \zeta_r, 2^{1/r}) : \mathbb{Q}] = 2^{s-\omega(d)} r\varphi(r)$.

Proof. Clearly $[\mathbb{Q}(\sqrt{l_1^*}, \ldots, \sqrt{l_s^*}) : \mathbb{Q}] = 2^s$. Suppose $8 \nmid r$. Then, by Proposition 1, $[\mathbb{Q}(\zeta_r, 2^{1/r}) : \mathbb{Q}] = r\varphi(r)$. Thus the sought for degree equals

$$\frac{2^s r\varphi(r)}{[\mathbb{Q}(\sqrt{l_1^*}, \ldots, \sqrt{l_s^*}) \cap \mathbb{Q}(\zeta_r, 2^{1/r})]} \tag{5}$$

Since $l_1, \ldots, l_s$ are the only primes that ramify in $\mathbb{Q}(\sqrt{l_1^*}, \ldots, \sqrt{l_s^*})$ and primes not dividing $2r$ do not ramify in $\mathbb{Q}(\zeta_r, 2^{1/r})$, one has that

$$\mathbb{Q}(\sqrt{l_1^*}, \ldots, \sqrt{l_s^*}) \cap \mathbb{Q}(\zeta_r, 2^{1/r}) \subseteq \mathbb{Q}(\cup_{l_i | d} \sqrt{l_i^*}). \tag{6}$$

Using that $\sqrt{l_i^*} \in \mathbb{Q}(\zeta_{l_i})$, it is seen that actually equality holds in (6). The (absolute) degree of the fields occurring in (6) is $2^{\omega(d)}$. This together with (5) completes the proof. □

Proposition 3 [1] (GRH). $\delta(\mathbb{Q}) = A$.

Proposition 4 (GRH). $\delta(\mathbb{Q}(i)) = A/2$.

Proof. Put $M = \mathbb{Q}(i)$. For $4 \nmid r$, the fields $\mathbb{Q}(i)$, $\mathbb{Q}(\zeta_r)$ and $\mathbb{Q}(2^{1/r})$ are seen to be mutually linearly disjoint on using Proposition 1. Thus $[M_r : \mathbb{Q}] = 2n_r = 2r\varphi(r)$, by Proposition 1 again. Recalling (3) one finds,

$$\delta(M) = \sum_{r=1}^{\infty} \frac{\mu(r)}{[M_r : \mathbb{Q}]} = \frac{1}{2} \sum_{r=1}^{\infty} \frac{\mu(r)}{r\varphi(r)}.$$

On using the fact that $\mu(r)/(r\varphi(r))$ is a multiplicative function and Euler's identity, the result follows. □

Proposition 5 (GRH). *Let* $l_1^*, \ldots, l_s^*$ *be as in Proposition 2. For notational convenience put* $\delta(l_1 \cdots l_s) = \delta(\mathbb{Q}(\sqrt{l_1^*}, \ldots, \sqrt{l_s^*}))$. *Then*

$$\delta(l_1 \cdots l_s) = \frac{A}{2^s} \prod_{j=1}^{s} (1 - \frac{1}{l_j^2 - l_j - 1}).$$

Proof. Put $M = \mathbb{Q}(\sqrt{l_1^*}, \ldots, \sqrt{l_s^*})$ and $\lambda = l_1 \cdots l_s$. Let $r \geq 1$. If $(\lambda, r) = d$, then, by Proposition 2, $[M_r : \mathbb{Q}] = 2^{s-\omega(d)} r\varphi(r)$. Thus

$$\delta(\lambda) = \sum_{d|\lambda} \sum_{(\lambda,r)=d} \frac{\mu(r)}{[M_r : \mathbb{Q}]} = \frac{1}{2^s} \sum_{d|\lambda} \sum_{\substack{d|r \\ (r,\lambda/d)=1}} \frac{2^{\omega(d)}\mu(r)}{r\varphi(r)}.$$

On noticing that the inner sum equals

$$2^{\omega(d)} \frac{\mu(d)}{d\varphi(d)} \sum_{(r,\lambda)=1} \frac{\mu(r)}{r\varphi(r)},$$

one finds that

$$\begin{aligned} \delta(\lambda) &= \frac{1}{2^s} \sum_{d|\lambda} \frac{2^{\omega(d)}\mu(d)}{d\varphi(d)} \sum_{(r,\lambda)=1} \frac{\mu(r)}{r\varphi(r)} \\ &= \frac{1}{2^s} \prod_{l_j|\lambda} (1 - \frac{2}{l_j(l_j-1)}) \prod_{p\nmid\lambda} (1 - \frac{1}{p(p-1)}) \\ &= \frac{A}{2^s} \prod_{l_j|\lambda} (1 - \frac{1}{l_j^2 - l_j - 1}). \end{aligned}$$

This completes the proof. □

Since, for $4 \nmid r$, $\mathbb{Q}(i)$ is linearly disjoint from $\mathbb{Q}(\sqrt{l_1^*}, \ldots, \sqrt{l_s^*}, \zeta_r, 2^{1/r})$, one has

$$\delta(\mathbb{Q}(\sqrt{l_1^*}, \ldots, \sqrt{l_s^*}, i)) = \delta(\mathbb{Q}(\sqrt{l_1^*}, \ldots, \sqrt{l_s^*}))/2.$$

Thus

Proposition 6 (GRH). *Let $l_1^*, \ldots, l_s^*$ be as in Proposition 2. Then*

$$\delta(\mathbb{Q}(\sqrt{l_1^*}, \ldots, \sqrt{l_s^*}, i)) = \frac{A}{2^{s+1}} \prod_{j=1}^{s} (1 - \frac{1}{l_j^2 - l_j - 1}).$$

Proposition 7 (GRH). *Let $l_1^*, \ldots, l_s^*$ be as in Proposition 2. Put $\lambda = l_1 \cdots l_s$. The density $\delta'(\lambda)$ of primes p such that 2 is a primitive root mod p and p does not split completely in any of the quadratic fields $\mathbb{Q}(\sqrt{l_1^*}), \ldots, \mathbb{Q}(\sqrt{l_s^*})$ equals*

$$\delta'(\lambda) = \frac{A}{2^s} \prod_{j=1}^{s} (1 + \frac{1}{l_j^2 - l_j - 1}).$$

Proof. Let $\delta(1)$ denote the density of the primes p such that 2 is a primitive root mod p. The sought for density, $\delta'(\lambda)$, equals, by inclusion and exclusion,

$$\delta'(\lambda) = \sum_{d|\lambda} \mu(d)\delta(d). \tag{7}$$

By Proposition 5 δ/A is a multiplicative function on the odd squarefree integers. The same holds for the Möbius function and for δ'/A, the Cauchy product of δ/A and μ. Using Propositions 3 and 5 one finds, for $1 \le j \le s$,

$$\delta'(l_j) = \delta(1) - \delta(l_j) = \frac{A}{2}(1 + \frac{1}{l_j^2 - l_j - 1}).$$

In combination with the multiplicativity of δ'/A, this yields the result. □

Remark (Don Zagier). Put $\epsilon_j = -1,\ 1 \le j \le s$. Using Theorem 1 it is seen that the density of primes p satisfying i) and ii) of Theorem 1 and in addition $p \equiv 3 (\mathrm{mod}\ 8)$ is

$$\frac{A}{2^{s+1}} \prod_{j=1}^{s} (1 + \frac{1}{l_j^2 - l_j - 1}) = \frac{1}{2^{s+1}} \prod_{p \nmid \lambda} (1 - \frac{1}{p(p-1)}).$$

The density of the primes p satisfying ii) of Theorem 1 and $p \equiv 3(\mathrm{mod}\ 8)$ equals 2^{-2-s}. Thus the relative density of primes p such that 2 is a primitive root is

$$2 \prod_{p \nmid \lambda} (1 - \frac{1}{p(p-1)}).$$

By taking λ to be the product of the first s consecutive odd primes and s large enough, the relative density can be made arbitrary close to 1. The conditions imposed ensure that $p - 1$ contains only 2 (to the first power) and some prime factors larger than the sth prime. Thus if 2 is not primitive mod p, 2 must have a small order mod p, which is something rarely happening. Another interpretation is obtained on noting that $1/(l(l-1))$ in the factor $1 - 1/(l(l-1))$, l odd, in Artin's constant is due to the primes that split completely in $\mathbb{Q}(\zeta_l, 2^{1/l})$, that is satisfy at least $p \equiv 1(\mathrm{mod}\ l)$. But $(p/l) = -1$ ensures $p \not\equiv 1(\mathrm{mod}\ l)$ and thus the factor $1 - 1/(l(l-1))$ should be replaced by 1. For $l = 2$ the $1/2$ in the factor $1 - 1/2$ comes from the primes that split completely in $\mathbb{Q}(\sqrt{2})$. Since $p \equiv 3(\mathrm{mod}\ 8)$ implies $(2/p) = -1$, this factor should be replaced by 1 as well.

Proof of Theorem 1. Let $J = \{j : \epsilon_j = 1\}$. Put $\lambda_1 = \prod_{j \in J} l_j$ and $\lambda_2 = \lambda/\lambda_1$. Except for at most finitely exceptions a prime p satisfies ii) if and only if p splits completely in $\mathbb{Q}(\sqrt{l_j^*})$, $j \in J$ and does not split completely in $\mathbb{Q}(\sqrt{l_j^*})$, for j not in J. By inclusion and exclusion the sought for density is seen to equal $\sum_{d|\lambda_2} \mu(d)\delta(d\lambda_1)$. By the multiplicativity of δ/A and (7) this equals $\delta'(\lambda_2)\delta(\lambda_1)/A$. Now (1) follows from Theorem 3, Propositions 5 and 7. The proof of the remaining part is similar, instead of Proposition 5 one now uses Proposition 6. □

4 Proof of Theorem 2

The proof of Theorem 2 is an almost immediate consequence of Propositions 3 and 4 and Theorem 1.

Proof of Theorem 2. Clearly the sequence $\{p_j\}$ is WUD mod 1 and WUD mod 2. By Propositions 3 and 4 the sequence is WUD mod 4. Since $2^{(p-1)/2} \equiv 1 (\mathrm{mod}\ 8)$, for every prime p satisfying $p \equiv 1(\mathrm{mod}\ 8)$, and hence none of these primes is such that 2 is a primitive root mod p, the sequence is not WUD mod 8. To finish the proof it is enough to show that for every odd prime l the sequence is not WUD mod l. Consider the set $\mathcal{A}_l$ of residue class a mod l such that $(a/l) = 1$. Notice that $|\mathcal{A}_l| = \varphi(l)/2$. If the sequence $\{p_j\}$ were WUD mod l, then the density of primes $p \in \mathcal{P}$ such that $p \equiv a_j (\mathrm{mod}\ l)$ for some $a_j \in \mathcal{A}_l$, would be $A/2$. On the other hand, using quadratic reciprocity, this density equals the density of $p \in \mathcal{P}$ such that p splits completely in $\mathbb{Q}(\sqrt{l^*})$. Now Proposition 5 with $s = 1$ and $l_1 = l$ leads to a contradiction. □

References

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

[2] S. Lang, On the zeta function of number fields, *Invent. Math.* **12** (1971), 337-345.

[3] W. Narkiewicz, *Uniform distribution of sequences of integers in residue classes,* LNIM 1087, Springer.

[4] A. Reznikov, Three-manifolds subgroup growth, in preparation. (With an appendix by P. Moree.)

[5] F. Rodier, Estimation asymptotique de la distance minimale du dual des codes BCH et polynômes de Dickson, *Discrete Math.* **149** (1996), 205-221.

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