Séminaire Delange-Pisot-Poitou.
Théorie des nombres

H. W., Jr. Lenstra

# Artin's conjecture on primes with prescribed primitive roots

*Séminaire Delange-Pisot-Poitou. Théorie des nombres*, tome 18, n° 1 (1976-1977), exp. n° 14, p. 1-8

<http://www.numdam.org/item?id=SDPP_1976-1977__18_1_A11_0>

Séminaire DELANGE-PISOT-POITOU
(Théorie des nombres)
18e année, 1976/77, n° 14, 8 p.



31 janvier 1977

# ARTIN'S CONJECTURE ON PRIMES WITH PRESCRIBED PRIMITIVE ROOTS

by H. W. LENSTRA, Jr

## 1. Introduction.

In 1927, E. ARTIN formulated a conjecture about the density of the set of primes for which a given non-zero integer $t$ is a primitive root. His conjecture would imply that there exist infinitely many such prime numbers, provided that $t \neq -1$ and $t \neq$ square ; a proviso which is clearly necessary. It is our aim to see what takes the place of this clearly necessary proviso in certain generalized forms of Artin's conjecture.

To give an example, suppose that, besides requiring that $t$ is a primitive root modulo the prime $q$, we also require that $q$ is in a given arithmetic progression:

$$q \equiv b \mod c \qquad (b, c \text{ integers}, \ (b, c) = 1) .$$

Under which conditions on $t$, $b$, $c$ is it reasonable to expect that there are infinitely many such $q$ ? We should not think of both requirements on $q$ being independent : if, for example, $q$ is required to be $1 \mod 8$, then 2 will be a square mod $q$, hence no primitive root. Similarly, but more subtly, one observes that there are no primes $q$ which are $3 \mod 4$ for which 27 is a primitive root : since 27 is a third power, such $q$ would have to be $2 \mod 3$, so $11 \mod 12$, and 27 would be a square mod $q$. The question is to list all such obstructions.

The generalized form of Artin's conjecture we have in mind is stated in section 2. The derivation follows Artin's original heuristics. The status of the conjecture is discussed in section 3. The question under which conditions the set of primes under consideration may be expected to be infinite is answered in section 4. In section 5, we discuss some examples. Among these is an application to the existence of a euclidean algorithm in rings of arithmetic type.

## 2. A generalization of Artin's conjecture.

Let $K$ be a global field. By a prime $p$ of $K$ we mean a non-archimedean prime divisor of $K$ ; its residue class field is denoted by $\overline{K}_p$, and $\overline{K}_p^* = \overline{K}_p - \{0\}$. Next, let $W$ be an infinite, finitely generated subgroup of $K^* = K - \{0\}$. Clearly, for all but finitely many $p$, there is a natural group homomorphism $W \longrightarrow K_p^*$, and we are interested in those $p$ for which

(2.1) the natural map $W \longrightarrow K_p^*$ is surjective.

Thus, in the case of Artin's original conjecture one should take $W = \langle t \rangle$, the subgroup generated by $t$.

Let $F$ be a finite Galois extension of $K$, with group $\mathcal{G}$. By $(p, F/K)$, we denote the Frobenius symbol :

$(p, F/K) = \{\sigma \in \mathcal{G}$ : there is a prime $q$ of $F$ extending $p$, such that $\sigma x \equiv x^{\#K_p} \bmod q$ for all $q$-integral $x \in F\}$.

This is a non-empty subset of $\mathcal{G}$, and it is a conjugacy class if $p$ is unramified in $F/K$. Let $C \subset \mathcal{G}$ be a subset which is a union of conjugacy classes. The condition

$$(p, F/K) \subset C \tag{2.2}$$

can, for suitable choices of $F$ and $C$, be used to express various requirements on $p$ : that certain polynomials should, or should not, have a zero mod $p$ ; that $p$ belongs to a certain arithmetic progression or, if say, $K = \mathbb{Q}$, is represented by a certain binary quadratic form ; or any finite logical combination of such conditions.

We denote by $M = M(K, W, F, C)$ the set of primes $p$ of $K$ satisfying both conditions (2.1) and (2.2). We are interested in a formula for the density of $M$. Here "density" means Dirichlet density in the function field case, and natural density in the number field case.

The heuristic derivation of such a formula is classical. For a positive squarefree integer $n$, not divisible by $\mathrm{char}(K)$, let $L_n = K(\zeta_n, W^{1/n})$, with $\zeta_n$ a primitive $n$-th root of unity. Then a standard argument shows that, for all but finitely many primes $p$ of $K$, the prime $p$ satisfies (2.1) if, and only if,

$$(p, L_\ell/K) \neq \{\mathrm{id}_{L_\ell}\} \tag{2.3}$$

for all prime numbers $\ell \neq \mathrm{char}(K)$. Let $M_n$ be the set of primes $p$ satisfying (2.3), for all prime numbers $\ell$ dividing $n$, and (2.2).

Then $M_m \supseteq M_n$ if $n$ is a multiple of $m$, and $M$ differs by only finitely many elements from the "limit" $\bigcap_n M_n$. The density of $M_n$ is easily calculated using Tchebotarev's theorem :

If $C_n = \{\sigma \in \mathrm{Gal}(F.L_n/K)$ : $(\sigma|F) \in C$, and $(\sigma|L_\ell) \neq \mathrm{id}_{L_\ell}$ for all prime numbers $\ell$ dividing $n\}$,
then, if $p$ is outside some finite set, $p \in M_n$ if, and only if, $(p, F.L_n/K) \subset C_n$. So Tchebotarev's theorem implies that the density $d(M_n)$ of $M_n$ exists and equals $a_n$, where

$$a_n = \#C_n/[F.L_n:K] .$$

We have $a_m \geq a_n$ if $n$ is a multiple of $m$, so if we let $n$ range over all squarefree positive integers not divisible by $\mathrm{char}(K)$, ordered by divisibility, then the sequence $(a_n)$ has a limit, which we call $a$ :

$$a = \lim_n a_n .$$

Since $M$ is the limit of the sets $M_n$, this leads to the following conjecture.

(2.4) CONJECTURE. - The density $d(M)$ exists and equals $a$.

## 3. The status of the conjecture.

In 1967, HOOLEY proved Artin's original conjecture (with a corrected formula for the conjectural density) on the assumption of a sequence of generalized Riemann hypotheses [4]. Not surprisingly, the various generalizations do not affect the status of the conjecture.

(3.1) THEOREM. - If $K$ is a number field, then (2.4) is true if for every $n$ the $\zeta$-function of $L_n$ satisfies the generalized Riemann hypothesis. If $K$ is a function field, then (2.4) is true.

In the function field case, BILHARZ [1] proved a version of Artin's conjecture modulo the Riemann hypothesis for curves over finite fields, which was later shown by WEIL to be correct. From what BILHARZ actually proved ([1], p. 485), it is not hard to derive the more general statement in (2.4) (Cf. [4]).

We turn to the number field case. Generalizing Hooley's approach, COOKE and WEINBERGER [2] proved a result implying (2.4) for $F/K$ abelian, modulo certain generalized Riemann hypotheses. Using a device employed in the proof of Tchebotarev's theorem as given in [5], p. 169, one easily reduces (2.4) to the case $F/K$ is abelian, and this gives the statement in (3.1), with a different set of Riemann hypotheses. A simpler approach is based on the observation that the condition (2.2) may be disregarded in the proof of (2.4), i. e. :

(3.2) If (2.4) is true in the case $F = K$, it is generally true.

To see this, notice that the arguments in section 1 yield at least an upper bound for the upper density $d^+(M)$ of $M$ : Since $M \subset M_n \cup$ (finite set), we have $d^+(M) \leqslant d(M_n) = a_n$ for all $n$, so in the limit

$$d^+(M) \leqslant a .$$

Applying this to the set $M' = M(K, W, F, \mathfrak{S} - C)$, we find $d^+(M') \leqslant a'$, where $a'$ denotes the conjectural density of $M'$. Since the case $F = K$ of (2.4) asserts that $d(M \cup M') = a + a'$ we conclude that

$$d^-(M) \geqslant d(M \cup M') - d^+(M') \geqslant (a + a') - a' = a ,$$

so $d(M) = a$, which proves (3.2). Combining (3.2) with a special case of the result of COOKE and WEINBERGER, we obtain the number field part of (3.1).

## 4. The non-vanishing of $a$.

In the applications of Artin's conjecture, it is of obvious practical importance to know under which conditions $a$ vanishes. The following theorem answers this question, at least in principle.

(4.1) THEOREM. - We have $a = 0$ if, and only if, $a_n = 0$ for some $n$. Moreover, if $a = 0$ then the set $M$ is finite.

That $a_n = 0$ implies $a = 0$ is obvious from the monotonicity of the limit $a = \lim_n a_n$. Further, if $a_n = 0$, then from section 1, we know that $M_n$, and hence $M$, is finite. Thus it suffices to prove that $a = 0$ implies $a_n = 0$ for some $n$.

In the number field case, this is done as in Artin's original conjecture, by expressing $a$ as an infinite product. Let $n$ be the product of those prime numbers $\ell$ which satisfy at least one of the following conditions :

$\ell = 2$ ;
$\ell$ divides the discriminant of $F$ over $\mathbb{Q}$ ;
the natural map $W/W^\ell \longrightarrow K^*/K^{*\ell}$ is not injective ;
there is a prime $p$ of $K$ lying over $\ell$ such that

$$\mathrm{ord}_p(w) \neq 0 \quad \text{for some} \quad w \in W .$$

It is easily seen that $n$ is finite. Let $m = n\,\ell_1\,\ell_2 \ldots \ell_t$ be any squarefree number divisible by $n$, with $\ell_1, \ell_2, \ldots, \ell_t$ prime numbers. Then one checks that the field $F.L_m$ is the linear disjoint composite of the fields $F.L_n$, $L_{\ell_1}$, $L_{\ell_2}, \ldots, L_{\ell_t}$ over $K$, and that $[L_{\ell_i} : K] = \varphi(\ell_i).\ell_i^r$ where $r$ denotes the rank of $W$ modulo its torsion subgroup and $\varphi$ the Euler-function. An easy calculation then yields

$$a_m = a_n \prod_{i=1}^{t} \left(1 - \frac{1}{\varphi(\ell_i)\ell_i^r}\right) ,$$

so in the limit

$$a = a_n \prod_{\ell} \left(1 - \frac{1}{\varphi(\ell)\ell^r}\right)$$

the product ranging over all prime numbers $\ell$ not dividing $n$. Since the product is absolutely convergent and all factors are non-zero, we conclude that $a$ can only vanish if $a_n$ does.

This proves (4.1) in the number field case.

In the function field case this argument collapses :

Here cyclotomic extensions of $K$ are constant field extensions, and outside any finite set of prime numbers one can find prime numbers $\ell$ and $\ell'$ such that $L_\ell$ and $L_{\ell'}$ are not linearly disjoint over $K$.

Instead a rather more delicate treatment is required, into the details of which we do not wish to enter. Suffice it to say that, as in the number field case, the number $n$ can be explicitly constructed.

In principle, it is possible, using (4.1) and its proof, to decide whether $a \neq 0$ in a given situation : all one has to do is considering the Galois extension

$F.L_n/K$ and investigating whether or not $C_n$ is empty, where $n$ is the value yielded by the proof of (4.1). For this procedure to be practicable, it is desirable that $n$ be small. This is, essentially, what is achieved by the following theorem.

(4.2) THEOREM. - Let $h$ be the product of all prime numbers $\ell \neq \mathrm{char}(K)$ for which $W \subset K^{*\ell}$. Then $a \neq 0$ if, and only if, there is an automorphism $\sigma$ of $F(\zeta_h)$ such that

$(\sigma|F) \in C$ ;

$(\sigma|L_\ell) \neq \mathrm{id}_{L_\ell}$ for all prime numbers $\ell$ for which $L_\ell \subset F(\zeta_h)$.

In many applications, the number $h$ in (4.2) is 1. Combining (4.1), (4.2) and (3.1) we obtain the following theorem.

(4.3) THEOREM. - Suppose there exists no prime number $\ell \neq \mathrm{char}(K)$ for which $W \subset K^{*\ell}$. Then the set $M$ is finite if and, modulo the Riemann hypotheses, only if, $C \subset \bigcup_\ell \mathrm{Gal}(F/L_\ell)$, the union ranging over those prime numbers $\ell \neq \mathrm{char}(K)$ for which $L_\ell \subset F$.

The existence of $\sigma$ in (4.2) is clearly equivalent to the condition $a_n \neq 0$, where $n$ now denotes the product of all prime numbers $\ell$ with $L_\ell \subset F(\zeta_h)$. So the "only if" part of (4.2) is obvious. To prove the "if" part it suffices, by (4.1), to show that $a_n \neq 0$ implies $a_m \neq 0$ for every squarefree multiple $m = n\ell_1 \ldots \ell_t$ of $n$, with $\ell_1, \ldots, \ell_t$ prime numbers $\neq \mathrm{char}(K)$. To this end one proves the following lemma :

(4.4) LEMMA. - Let $\ell$ be a prime number, $\ell \neq \mathrm{char}(K)$, with $L_\ell \not\subset F(\zeta_h)$. Then the degree $[F(\zeta_h).L_\ell : F(\zeta_h)]$ is divisible by $\ell$, and all prime numbers dividing this degree are $\leqslant \ell$.

Applying (4.4) to $\ell_1, \ell_2, \ldots, \ell_t$, and assuming that $\ell_1 < \ell_2 < \ldots < \ell_t$, we find that in the chain of $t+1$ fields

$$F(\zeta_h) \subset F(\zeta_h).L_{\ell_1} \subset F(\zeta_h).L_{\ell_1}.L_{\ell_2} \subset \ldots \subset F(\zeta_h).L_{\ell_1} \ldots L_{\ell_t}$$

the $i$-th extension has a degree which is divisible by $\ell_i$, for $1 \leqslant i \leqslant t$.

In particular, this degree is $> 1$, so no two of the $t+1$ fields coincide. Thus, we can extend the automorphism $\sigma$ step-wise to an automorphism $\tau$ of $F(\zeta_h).L_{\ell_1} \ldots L_{\ell_t} = F(\zeta_h).L_m$ such that

$$\tau|L_{\ell_i} \neq \text{identity on } L_{\ell_i}, \quad \text{for } i = 1, 2, \ldots, t .$$

By definition of $C_m$, this means $a_m \neq 0$, as required.

5. Examples.

(5.1) THEOREM. - Let $b$, $c$ be positive integers, $(b, c) = 1$, and let $t \in \underset{\sim}{Q}$, $t \neq 0, 1, -1$. Let $\alpha(t)$ denote the discriminant of $\underset{\sim}{Q}(\sqrt{t})$ over $\underset{\sim}{Q}$. Then the set of prime numbers $q$ in the arithmetic progression $b, b+c, b+2c, \ldots$ for which $t$ is a primitive root is finite if and, modulo certain generalized Riemann hypotheses, only if, one of the following conditions is satisfied :

(a) $\ell | c$, $b \equiv 1 \mod \ell$, $t \in \underset{\sim}{Q}^{*\ell}$ for some prime number $\ell$ ;

(b) $\alpha(t) | c$, $\left(\frac{\alpha(t)}{b}\right) = 1$ (Kronecker-symbol) ;

(c) $\alpha(t) | 3c$, $3 | \alpha(t)$, $\left(\frac{-\alpha(t)/3}{b}\right) = 1$, $t \in \underset{\sim}{Q}^{*3}$.

To prove this theorem, we apply (3.1) and (4.2) to the set $M = M(\underset{\sim}{Q}, <t>, \underset{\sim}{Q}(\zeta_c), \{\sigma_b\})$, where $\sigma_b$ is the automorphism of $\underset{\sim}{Q}(\zeta_c)$ mapping $\zeta_c$ to $\zeta_c^b$. It is then found that $M$ is finite if and, modulo the Riemann hypotheses, only if, $\underset{\sim}{Q}(\zeta_c, \zeta_h)$ does not have an automorphism satisfying certain requirements ; here $h$ is the product of those prime numbers $\ell$ for which $t$ is an $\ell$-th power in $\underset{\sim}{Q}$. A straightforward analysis shows that the only obstructions preventing the existence of such an automorphism are the conditions (a), (b) and (c), and (5.1) follows.

It may be remarked that the "if"-part of (5.1) has a direct proof, using nothing more than quadratic reciprocity. In fact, it turns out that in each of the situations (a), (b) and (c) the set of primes in question either is empty or only contains the prime 2. But our approach has the advantage that one need not know beforehand the list of exceptional situations : they are just the obstructions encountered during the construction of $\sigma$, and if in all other situations $\sigma$ can be constructed one knows that the list is complete (modulo the Riemann hypotheses).

Our next example is taken from COOKE and WEINBERGER [2]. Let $S$ be a finite set of prime divisors of $K$ containing the set $S_\infty$ of archimedean prime divisors, such that $\# S \geqslant 2$. Let

$$R_S = \{x \in K : \operatorname{ord}_p(x) \geqslant 0 \text{ for all primes } p \text{ of } K \text{ which are not in } S\} .$$

Then $R_S$ is a Dedekind domain with an infinite unit group $R_S^*$.

A theorem of VASERSTEIN asserts that $SL_2(R_S)$ is generated by the elementary matrices $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ x & 1 \end{pmatrix}$, with $x \in R_S$. COOKE and WEINBERGER proved the following theorem.

(5.2) THEOREM. - Let $K$ be a number field, and assume certain generalized Riemann hypotheses. Then any element of $SL_2(R_S)$ is a product of nine elementary matrices. If $S \neq S_\infty$, or if $R_S$ is a principal ideal domain, eight elementary matrices suffice. Seven suffice if $K$ can be embedded in the field of real numbers.

The proof of this theorem makes use of Artin's conjecture with $W = R_S^*$, and em-

ploys condition (2.2) with $F/K$ abelian. Actually a further generalization of Artin's conjecture is needed, in which (2.1) is replaced by the condition that the index of the image of $W$ in $\overline{K}_p^*$ divides a given integer $k$. Our results easily carry over to this more general situation.

Our final example concerns the existence of a euclidean algorithm on $R_S$, i. e., a map $\Psi : R_S - \{0\} \longrightarrow \{0, 1, 2, \ldots\}$ such that for all $b, c \in R_S$, $c \neq 0$, there exist $q, r \in R_S$ with $b = qc + r$, and $r = 0$ or $\Psi(r) < \Psi(b)$. If such a map exists, then $R_S$ is a principal ideal domain. The following theorem states that the converse is true modulo certain Riemann hypotheses, and gives, moreover, a description of the smallest euclidean algorithm [7].

(5.3) THEOREM. - Suppose that $R_S$, with $\# S \geqslant 2$, is a principal ideal domain, and that certain generalized Riemann hypotheses are true.

Then a euclidean algorithm on $R_S$ is given by the map $\vartheta$ defined by

$$\vartheta(x) = \sum_{p \notin S} \mathrm{ord}_p(x)\, n_p \qquad (x \in R_S,\ x \neq 0)$$

with

- $n_p = 1$ if the natural map $R_S^* \longrightarrow \overline{K}_p^*$ is surjective,
- $n_p = 2$ else.

Moreover, $\vartheta$ is the smallest euclidean algorithm on $R_S$.

The function field case of (5.3) is due to QUEEN [6]. In the number field case, a weaker statement was obtained by WEINBERGER [8].

If the map $\vartheta$, defined in (5.3), is a euclidean algorithm on $R_S$ then SAMUEL's results [7] easily imply that it is the smallest one. So it suffices to prove the first statement of (5.3).

Let $b, c \in R_S$, $c \neq 0$. We look for an element $r \equiv b \mod c$ for which $r = 0$ or $\vartheta(r) < \vartheta(b)$. Dividing $b$ and $c$ by their greatest common divisor, we may assume that $(b, c) = 1$.

The existence of $r$ is trivial if $\vartheta(c) \neq 2$ : If $\vartheta(c) = 0$ then $c$ is a unit and one can take $r = 0$ ; if $\vartheta(c) = 1$ then $c$ is a prime element of $R_S$ for which $R_S^* \longrightarrow (R_S/(c))^*$ is surjective, and we can take $r =$ unit ; and, finally, if $\vartheta(c) \geqslant 3$ then using a generalization of Dirichlet's theorem on primes in arithmetic progressions one can take $r$ to be a prime element which is $b \mod c$, which indeed gives

$$\vartheta(r) \leqslant 2 < 3 \leqslant \vartheta(c).$$

Hence let $\vartheta(c) = 2$. In this case, it would be sufficient to find a prime element $r$ of $R_S$ with $\vartheta(r) = 1$ and $r \equiv b \mod c$.

Let $\mathfrak{r}$ denote the prime divisor of $K$ corresponding to the prime ideal $(r)$ of $R_S$. Then the condition $\vartheta(r) = 1$ means :

the natural map $R_S^* \longrightarrow \overline{K}_r^*$ is surjective,

and the condition $r \equiv b \mod c$ can, using class field theory, be translated into one of the type (2.2), with $F$ a suitably chosen abelian extension of $K$. Thus the question is, whether the set $M = M(K, R_S^*, F, C)$ contains an element outside $S$.

This question is analyzed using (4.3), and it turns out that the answer may be negative : For example, the ring $\mathbb{Z}[\zeta_5]$ contains no prime element $r$ which is $1 \mod 4$ for which $\mathbb{Z}[\zeta_5]^* \longrightarrow (\mathbb{Z}[\zeta_5]/(r))^*$ is surjective ; here indeed $\vartheta(4) = 2$.

The same analysis shows, however, that by a fortunate coincidence the set $M$ can, in our situation, only be finite, modulo Riemann hypotheses, in case we have something better : namely, if $b$ is congruent to a unit $\mod c$, in which case, of course, we take for $r$ this unit.

Finally, we mention that our results may be applied to yield existence theorems, modulo Riemann hypotheses, for perfect, one-error-correcting arithmetical codes (Cf. [3]).

## REFERENCES


[1] BILHARZ (H.). - Primdivisoren mit vorgegebener Primitivwurzel, Math. Annalen, t. 114, 1937, p. 476-492.

[2] COOKE (G.) and WEINBERGER (P. J.). - On the construction of division chains in algebraic number fields, with applications to $SL_2$, Comm. in Algebra, t. 3, 1975, p. 481-524.

[3] GOTO (M.) and FUKUMURA (T.). - Perfect nonbinary AN codes with distance three, Inform. and Control, t. 27, 1975, p. 336-348.

[4] HOOLEY (C.). - On Artin's conjecture, J. reine und angew. Math., t. 225, 1967, p. 209-220.

[5] LANG (S.). - Algebraic number theory. - Reading, Addison Wesley publishing Company, 1970.

[6] QUEEN (C.). - Arithmetic euclidean rings, Acta Arithm., Warszawa, t. 26, 1974, p. 105-113.

[7] SAMUEL (P.). - About euclidean rings, J. of Algebra, t. 19, 1971, p. 282-301.

[8] WEINBERGER (P. J.). - On euclidean rings of algebraic integers, "Analytic number theory", p. 321-332. - Providence, American mathematical Society, 1973 (Proceedings of Symposia in pure Mathematics, 24).


(Texte reçu le 7 février 1977)

H. W. LENSTRA, Jr
15 Roetersstraat
AMSTERDAM C (Pays-Bas)