Mathematisch Instituut
Roetersstraat 15
Amsterdam-C. The Netherlands

# ON ARTIN's CONJECTURE AND EUCLID's ALGORITHM IN GLOBAL FIELDS

by H.W. Lenstra, Jr.

Report 77-03

Received February 1, 1977

March 1977

# On Artin's conjecture and Euclid's algorithm in global fields.

H.W. Lenstra, Jr.

Abstract.- This paper considers a generalization of Artin's conjecture on primes with prescribed primitive roots. The main result provides a necessary and sufficient condition for the conjectural density of certain sets of primes to be non-zero. As an application a theorem about the existence of a euclidean algorithm in rings of arithmetic type is proved.

Key words: Artin's conjecture, primitive roots, Euclid's algorithm.
AMS-MOS subject classification scheme (1970): 12A75, 10H15, 12A45, 13F10.

# On Artin's conjecture and Euclid's algorithm in global fields.

H.W. Lenstra, Jr.

## Introduction.

A famous conjecture of Artin (1927) [3, 9] asserts that for every non-zero rational number $t$ the set of prime numbers $q$ for which $t$ is a primitive root possesses a density inside the set of all prime numbers. The original conjecture included a formula for this density, but calculations by D.H. Lehmer [14] indicated that this formula must be wrong. A corrected version of the conjecture [31, intr., sec. 23; 2, intr.] was proved by Hooley [11, 12] under the assumption of certain generalized Riemann hypotheses.

In this paper we are concerned with a generalized form of Artin's conjecture, which recently arose in connection with Euclid's algorithm [23, 30, 19] and the construction of division chains [5, 20] in global fields. Our main contribution is a necessary and sufficient condition for the conjectural density of the set of primes in question to be non-zero. As an application of this result we prove a theorem about the existence of a euclidean algorithm in rings of arithmetic type. For an application to arithmetic codes we refer to [15].

We discuss the various ways in which Artin's conjecture has been generalized.

First, instead of the rational numbers one can consider an arbitrary global field $K$, as in [3]. Prime numbers are then replaced by non-archimedean prime divisors $\underline{p}$ of $K$.

Secondly, a congruence condition can be imposed on these primes [30, 19]. This is even of interest in the case $K = \mathbb{Q}$: for example, among all primes for which 27 is a primitive root there are no primes which are $-1 \bmod 4$, while, conjecturally, there are infinitely many which are

1 mod 4. Using class field theory we can formulate such a congruence condition on $\underline{p}$ as a condition on the Artin symbol $(\underline{p}, F/K)$, for some finite abelian extension $F$ of $K$. Thus, in the given example, the condition $q \equiv -1 \bmod 4$ is equivalent to the requirement that $(q, \mathbb{Q}(i)/\mathbb{Q})$ is the non-identity element of the Galois group $\mathrm{Gal}(\mathbb{Q}(i)/\mathbb{Q})$. A further generalization is achieved if we replace $F$ by an arbitrary finite Galois extension of $K$, and the Artin symbol by the Frobenius symbol.

The third generalization is due to Cooke and Weinberger [5]. The condition that the non-zero element $t$ of $K$ is a primitive root mod $\underline{p}$ can be reformulated as follows: if $\langle t \rangle$ denotes the subgroup of the multiplicative group $K^*$ of $K$ generated by $t$ and $\overline{K}_{\underline{p}}$ the residue class field at $\underline{p}$, then the map $\langle t \rangle \to \overline{K}^*_{\underline{p}}$ should be defined and surjective. The generalization consists in replacing $\langle t \rangle$ by an arbitrary finitely generated subgroup $W \subset K^*$. In the applications one often takes $W$ to be the group of units of a suitable subring of $K$.

A fourth generalization which has been considered [14, 17, 5] consists in weakening the condition that $W \to \overline{K}^*_{\underline{p}}$ be surjective. Instead, one requires that the index of the image of $W$ in $\overline{K}^*_{\underline{p}}$ divides some fixed positive integer $k$.

Other types of generalizations, not considered here, can be found in [6, 7, 8, 16]; compare also section 8.

We refer to section 2 for the precise formulation of the generalized conjecture, and its heuristic derivation. Not surprisingly, the various generalizations do not affect the status of the conjecture: in the function field case it is a theorem, and in the number field case it is true modulo certain generalized Riemann hypotheses. This is shown in section 3, by a trivial reduction to results of Bilharz and Queen [3, 19] and Cooke and Weinberger [5].

In the applications of the conjecture it is obviously relevant to know under which conditions the conjectural density vanishes. This problem is less trivial than in the case of Artin's original conjecture, since our formula is an infinite sum rather than an infinite product. Our solution is stated in section 4, and the proof occupies sections 5, 6 and 7.

In section 8 we mention various problems to which our results apply. The application to Euclid's algorithm is considered in detail in section 9.

## 1. Notations.

In this paper $K$ is a global field, i.e. a finite extension of the rational number field $\mathbb{Q}$ or a function field in one variable over a finite field. In the first case we simply call $K$ a number field, we denote by $\Delta_K$ its discriminant over $\mathbb{Q}$, and we put $p = 1$. In the second case, $K$ is called a function field, and $p$ denotes its characteristic.

Throughout this paper we use the letters $m$, $n$, $d$, possibly with subscripts, to denote squarefree integers $> 0$ which are relatively prime to $p$, also at places where this is not explicitly required. Similarly, by $\ell$ we always mean a prime number different from $p$. The functions of Moebius and Euler are denoted by $\mu$ and $\phi$, respectively; $q|r$ means that $q$ divides $r$, and $q\nmid r$ has the opposite meaning. The number of elements of a set $S$ is denoted by $\#S$.

Let $R$ be a ring. Then $R^*$ is its group of units, $R^{*q}$ is the subgroup of $q$-th powers, and if $t \in R^*$ then $\langle t \rangle$ is the subgroup generated by $t$. The ring of integers is indicated by $\mathbb{Z}$, and $\mathbb{F}_q$ is a finite field of $q$ elements.

The restriction of an automorphism $\sigma$ of a field $L$ to a subfield $L'$ of $L$ is denoted by $\sigma|L'$. If $L/L'$ is a Galois extension, then $\mathrm{Gal}(L/L')$ is its Galois group, and $\mathrm{id}_L$ is the identity automorphism of $L$. The composite of two fields $L_1$ and $L_2$ is denoted by $L_1 \cdot L_2$. By $\zeta_q$ we mean a primitive $q$-th root of unity.

A prime $\mathfrak{p}$ of $K$ is a non-archimedean prime divisor of $K$. The associated normalized exponential valuation is denoted by $\mathrm{ord}_{\mathfrak{p}}$, and $\overline{K}_{\mathfrak{p}}$ is the residue class field at $\mathfrak{p}$. We put $N\mathfrak{p} = \#\overline{K}_{\mathfrak{p}}$.

If $S$ is a set of primes of $K$, then the lower and upper Dirichlet densities $d_-(S)$ and $d_+(S)$ are defined by

$$d_-(S) = \liminf_{s \to 1+0} (\Sigma_{\underline{p} \in S} (N\underline{p})^{-s}) / (\Sigma_{\underline{p}} (N\underline{p})^{-s})$$

$$d_+(S) = \limsup_{s \to 1+0} (\Sigma_{\underline{p} \in S} (N\underline{p})^{-s}) / (\Sigma_{\underline{p}} (N\underline{p})^{-s})$$

(the sums in the denominators are over all primes $\underline{p}$ of $K$). Generally, $0 \le d_-(S) \le d_+(S) \le 1$. If $d_-(S) = d_+(S)$ then this common value is denoted by $d(S)$ and called the Dirichlet density of $S$. It may be remarked that all our results remain valid if, in the number field case, we replace Dirichlet density by natural density. For the function field case this is not true [3].

If $\underline{p}$ is a prime of $K$ and $L/K$ is Galois, then the Frobenius symbol $(\underline{p}, L/K)$ denotes the set of those $\sigma \in \mathrm{Gal}(L/K)$ for which there is a prime $\underline{q}$ of $L$ extending $\underline{p}$ such that $\sigma\underline{q} = \underline{q}$ and $\bar{\sigma}\alpha = \alpha^{N\underline{p}}$ for all $\alpha \in \bar{L}_{\underline{q}}$, where $\bar{\sigma}$ is the automorphism of $\bar{L}_{\underline{q}}$ induced by $\sigma$. This is a non-empty subset of $\mathrm{Gal}(L/K)$, and if $\underline{p}$ is not ramified in $L/K$ then it is a conjugacy class.

The notations $F$, $C$, $W$, $r$, $k$, $M$, $\psi$, $q(n)$, $L_n$, $C_n$, $a_n$, $a$ are introduced in section 2, and for "GRH" we refer to sections 3 and 9.

## 2. The generalized conjecture.

Let there be given a global field $K$, a finite Galois extension $F$ of $K$, a subset $C \subset \mathrm{Gal}(F/K)$ which is a union of conjugacy classes, a finitely generated subgroup $W \subset K^*$ of rank $r \geq 1$ modulo its torsion subgroup, and an integer $k > 0$ which is relatively prime to $p$. We are interested in the set $M = M(K, F, C, W, k)$ of primes $\underline{p}$ of $K$ which satisfy the following conditions:

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

$\mathrm{ord}_{\underline{p}}(w) = 0$ for all $w \in W$,

if $\psi: W \to \overline{K}^*_{\underline{p}}$ is the natural map, then the index of $\psi(W)$ in $\overline{K}^*_{\underline{p}}$ divides $k$.

Notice that we have excluded the case $W$ is finite. In this case it is easily seen that also $M$ is finite.

The conjecture is that $M$ has a density. In order to state the formula for the conjectural density we introduce some new notation. For a prime number $\ell \neq p$ let $q(\ell)$ be the smallest power of $\ell$ not dividing $k$ and let $L_\ell = K(\zeta_{q(\ell)}, W^{1/q(\ell)})$ be the field obtained by adjoining all $q(\ell)$-th roots of elements of $W$ to $K$. Notice that $q(\ell) = \ell$ for all but finitely many $\ell$, and that $L_\ell$ is a finite Galois extension of $K$. Similarly, if $n$ is a squarefree integer $> 0$, relatively prime to $p$, then we define $q(n) = \prod_{\ell | n} q(\ell)$, $L_n = K(\zeta_{q(n)}, W^{1/q(n)})$. Clearly, $L_n$ is the composite of the fields $L_\ell$, $\ell | n$. Further, we define $C_n \subset \mathrm{Gal}(F \cdot L_n/K)$ by

$$C_n = \{\sigma \in \mathrm{Gal}(F \cdot L_n/K): \ (\sigma|F) \in C, \text{ and } (\sigma|L_\ell) \neq \mathrm{id}_{L_\ell} \text{ for all } \ell | n\}$$

and we put

$$a_n = \#C_n/\#\mathrm{Gal}(F \cdot L_n/K) = \#C_n/[F \cdot L_n : K].$$

If $n$ divides $m$, then

(2.1) $\quad a_n \geq a_m \geq 0.$

It follows that the sequence $(a_n)$ has a limit, if $n$ ranges over all squarefree integers $> 0$ prime to $p$, ordered by divisibility. Let

(2.2) $\quad a = \lim_n a_n.$

(2.3) Conjecture. The density $d(M)$ exists and is equal to $a$.

We quickly review the heuristic reasoning underlying the conjecture, and will at the same time prove half of it:

(2.4) $\quad d_+(M) \leq a.$

(2.5) Lemma. Let $\underline{p}$ be a prime of $K$ which satisfies

(2.6) $\quad \mathrm{ord}_{\underline{p}}(w) = 0$ for all $w \in W$,

(2.7) $\quad \mathrm{ord}_{\underline{p}}(2 \cdot \Delta_K) = 0$ if $K$ is a number field.

Then the index of $\psi(W)$ in $\overline{K}^*_{\underline{p}}$ divides $k$ if and only if for all prime numbers $\ell \neq p$ we have

(2.8) $\quad (\underline{p}, L_\ell/K) \neq \{\mathrm{id}_{L_\ell}\}.$

Notice that only finitely many $\underline{p}$ are excluded by (2.6) and (2.7). Some condition on $\underline{p}$ is necessary: $-7$ is a primitive root mod 2, but $(2, \mathbb{Q}(\sqrt{-7})/\mathbb{Q}) = \{\mathrm{id}_{\mathbb{Q}(\sqrt{-7})}\}$.

Proof of (2.5). "If". If the index of $\psi(W)$ in $\overline{K}^*_{\underline{p}}$ does not divide $k$, then for some prime number $\ell$ it is divisible by $q(\ell)$; notice that the index is relatively prime to $p$, since $\#\overline{K}^*_{\underline{p}}$ is. That means

(2.9) $\quad q(\ell) \mid \#\overline{K}^*_{\underline{p}}$

(2.10) $\psi(W) \subset \overline{K}_{\underline{p}}^{*q(\ell)}$.

But, since $\underline{p}$ satisfies $\mathrm{ord}_{\underline{p}}(\ell \cdot 1) = 0$ and $\mathrm{ord}_{\underline{p}}(w) = 0$ for all $w \in W$, by (2.9) and (2.6), these conditions simply express that $\underline{p}$ splits completely in $K(\zeta_{q(\ell)}, W^{1/q(\ell)}) = L_\ell$, so $(\underline{p}, L_\ell/K) = \{\mathrm{id}_{L_\ell}\}$, contradicting (2.8).

"Only if". Let the index of $\psi(W)$ in $\overline{K}_{\underline{p}}^*$ divide $k$, and let $\ell$ be a prime number $\neq p$. If $\mathrm{ord}_{\underline{p}}(\ell \cdot 1) > 0$ then $K$ is a number field, and the presence of the $\ell$-th roots of unity in $L_\ell$ implies, by condition (2.7), that $\underline{p}$ ramifies in $L_\ell/K$, so $(\underline{p}, L_\ell/K) \neq \{\mathrm{id}_{L_\ell}\}$. Hence we may assume that $\mathrm{ord}_{\underline{p}}(\ell \cdot 1) = 0$. Then if $\underline{p}$ splits completely in $L_\ell/K$, we necessarily have (2.9) and (2.10) (again using (2.6)), contradicting that the index of $\psi(W)$ in $\overline{K}_{\underline{p}}^*$ divides $k$. We conclude that $\underline{p}$ does not split completely in $L_\ell/K$, so $(\underline{p}, L_\ell/K) \neq \{\mathrm{id}_{L_\ell}\}$. This proves (2.5).

Now let $M_n$ be the set of those primes $\underline{p}$ of $K$ for which

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

$$(\underline{p}, L_\ell/K) \neq \{\mathrm{id}_{L_\ell}\} \quad \text{for all } \ell \mid n.$$

Clearly

(2.11) $M_n \supset M_m$ if $n \mid m$,

and lemma (2.5) implies that $M$ differs by at most a finite set from the "limit" $\cap_n M_n$. We calculate the density of $M_n$. Formal properties of the Frobenius symbol imply that $M_n$ differs by at most a finite set from

(2.12) $\{\underline{p}: (\underline{p}, F \cdot L_n/K) \subset C_n\}$

so Tchebotarev's theorem [13, ch. VIII, sec. 4] implies that

$$d(M_n) = \#C_n/\#\mathrm{Gal}(F \cdot L_n/K) = a_n.$$

Thus we see that conjecture (2.3) is equivalent to the assertion that

(2.13) $\quad d(\cap_n M_n) = \lim_n d(M_n).$

A trivial example shows that (2.13) is certainly not a generality following from (2.11): if $M_n$ consists of all primes except the first $n$ ones, in some numbering of the primes, then $d(M_n) = 1$ for all $n$, and $\cap_n M_n = \emptyset$ so $d(\cap_n M_n) = 0$. Weinberger [29] proved that (2.13) even can fail in a situation closely resembling ours.

In any case, it is true that

$$d_+(M) = d_+(\cap_m M_m) \leq d_+(M_n) = d(M_n) = a_n$$

for all $n$, which, in the limit, gives (2.4).

(2.14) Proposition. We have

$$a_n = \Sigma_{d|n} \frac{\mu(d)c(d)}{[F\cdot L_d:K]}$$

where

$$c(d) = \#(C \cap \mathrm{Gal}(F/F \cap L_d)).$$

Proof. For $d|n$, put

$$D_d = \{\sigma \in \mathrm{Gal}(F\cdot L_n/K): \ (\sigma|F) \in C, \text{ and } (\sigma|L_\ell) = \mathrm{id}_{L_\ell} \text{ for all } \ell|d\}.$$

The principle of inclusion and exclusion [22] gives

$$\#C_n = \Sigma_{d|n} \mu(d)\cdot\#D_d.$$

To count $D_d$, notice that

$$D_d = \{\sigma \in \mathrm{Gal}(F\cdot L_n/L_d): \ (\sigma|F) \in C\}.$$

For every $\sigma \in D_d$, we clearly have $(\sigma|F) \in C \cap \mathrm{Gal}(F/F \cap L_d)$. Conversely, if $\tau \in C \cap \mathrm{Gal}(F/F \cap L_d)$, then $\tau$ has precisely one extension to an element of $\mathrm{Gal}(F \cdot L_d/L_d)$, which in turn can be extended in $[F \cdot L_n : F \cdot L_d]$ ways to an element $\sigma$ of $D_d$. We conclude that

$$\#D_d = [F \cdot L_n : F \cdot L_d] \cdot c(d)$$

so

$$a_n = \frac{\# C_n}{[F \cdot L_n : K]} = \Sigma_{d|n} \frac{\mu(d)c(d)}{[F \cdot L_d : K]}.$$

This proves (2.14).

Remark. It follows that

$$(2.15) \qquad a = \Sigma_n \frac{\mu(n)c(n)}{[F \cdot L_n : K]}$$

since the sum is absolutely convergent, as can be proved by the methods of sections 5 and 6. The formula leaves something to be desired, since it does not even enable us to answer the question of when $a = 0$. We return to this question in section 4. It will turn out that the definition of $a$ is a handier tool than formula (2.15).

## 3. The status of the conjecture.

(3.1) Theorem. If $K$ is a function field, then conjecture (2.3) is true. If $K$ is a number field, then conjecture (2.3) is true if for every squarefree integer $n > 0$ the $\zeta$-function of $L_n$ satisfies the generalized Riemann hypothesis.

We use "GRH" as an abbreviation for the Riemann hypotheses mentioned in (3.1). In the function field case "GRH" refers to an empty set of hypotheses. We refer to [27, 12] for a method to find, in the number field case, a smaller set of Riemann hypotheses which is also sufficient for the validity of (2.3).

Proof of (3.1). First let $K$ be a function field. In this case Bilharz [3] proved the original conjecture - i.e., $F = K$, $C = \{id_K\}$, $W$ infinite cyclic, $k = 1$ - modulo certain Riemann hypotheses for function fields, which were later shown by Weil to be correct [28, 4]. From what Bilharz actually proved [3, p. 485, italicized] it is not hard to derive the more general conjecture. Compare also the details given by Queen [19]. This finishes our discussion of the function field case.

Next let $K$ be a number field, and assume GRH. Then, according to Cooke and Weinberger [5, theorem 1.1], conjecture (2.3) is true at least in the case $F = K$, $C = \{id_K\}$. Thus, to prove (3.1) it suffices to prove the following lemma.

(3.2) Lemma. If (2.3) is true in the case $F = K$, $C = \{id_K\}$, then it is generally true.

Proof. Let $M = M(K, F, C, W, k)$ be as in section 2, and put $M' = M(K, K, \{id_K\}, W, k)$. We define $a$ as in (2.2), and $a'$ denotes the corresponding quantity for $M'$. We must prove: if $d(M')$ exists and

equals $a'$, then $d(M)$ exists and equals $a$.

To see this, let $C''$ be the complement of $C$ in $\mathrm{Gal}(F/K)$, put $M'' = M(K, F, C'', W, k)$, and let $a''$ correspond to $M''$. Then one easily sees that

$$a' = a + a''.$$

Also, $M'$ differs by only a finite set from the disjoint union $M \cup M''$, so

$$d_-(M') \leq d_-(M) + d_+(M'').$$

But, by assumption, $d_-(M') = d(M') = a'$, and from (2.4) it follows that $d_+(M'') \leq a''$. We conclude that $d_-(M) \geq a' - a'' = a$, and combined with (2.4) this gives $d(M) = a$, as required. This proves (3.2) and (3.1).

## 4. The non-vanishing of the density.

(4.1) Theorem. Let $h$ be the product of those prime numbers $\ell \neq p$ for which $W \subset K^{*q(\ell)}$. Then the following assertions are equivalent:

(4.2) $a \neq 0$;

(4.3) $a_n \neq 0$ for all $n$;

(4.4) there exists $\sigma \in \mathrm{Gal}(F(\zeta_h)/K)$ such that

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

$(\sigma|L_\ell) \neq \mathrm{id}_{L_\ell}$ for every $\ell$ with $L_\ell \subset F(\zeta_h)$.

Remark. It is not hard to show that $h$ is finite, cf. (5.1), (6.1).

The implication (4.2) $\Rightarrow$ (4.3) is trivial, since $a_n \geq a \geq 0$ for all $n$, by (2.1). The converse

(4.5) if $a_n \neq 0$ for all $n$ then $a \neq 0$

will be proved in sections 5 and 6.

Notice that the existence of $\sigma$ in (4.4) is equivalent to the non-vanishing of $a_m$, where $m$ is the product of those $\ell$ for which $L_\ell \subset F(\zeta_h)$; again, $m$ is finite. This remark makes (4.3) $\Rightarrow$ (4.4) obvious, and the remaining implication (4.4) $\Rightarrow$ (4.3) is proved in section 7.

(4.6) Theorem. Let $h$ be the product of those prime numbers $\ell \neq p$ for which $W \subset K^{*q(\ell)}$. Then if $M$ is infinite, there exists $\sigma \in \mathrm{Gal}(F(\zeta_h)/K)$ with

$(\sigma|F) \in C$

$(\sigma|L_\ell) \neq \mathrm{id}_{L_\ell}$ for every $\ell$ with $L_\ell \subset F(\zeta_h)$.

Conversely, if such a $\sigma$ exists and GRH is true, then $M$ is infinite and $d(M) > 0$.

Proof. If no such $\sigma$ exists then by (4.1) there exists $n$ with $a_n = 0$, so $C_n = \emptyset$. Then the set (2.12) is empty, so $M_n$ is finite, and the same is then true for $M$. Conversely, if such $\sigma$ exists and GRH is true, then $a > 0$ by (4.1) and $d(M) = a$ by (3.1). Hence, $d(M) > 0$ and $M$ is infinite. This proves (4.6).

Thus, modulo GRH, the set $M$ can only have density zero if it is finite.

In many applications, $W$ satisfies the condition

(4.7) there is no integer $q > 1$ with $W \subset K^{*q}$.

This is true, for example, if $W$ is the group of units of an integrally closed subring of $K$ with infinitely many units.

(4.8) Corollary. If $W$ satisfies (4.7) and GRH is true, then $M$ is infinite if and only if $C$ is not contained in $\bigcup_\ell \mathrm{Gal}(F/L_\ell)$, the union ranging over those prime numbers $\ell \neq p$ for which $L_\ell \subset F$.

Proof. Apply (4.6), and notice that $h = 1$. This proves (4.8).

## 5. Proof of (4.5): the number field case.

In this section we assume that $K$ is a number field.

(5.1) Lemma. For all but finitely many prime numbers $\ell$ the natural map $W/W^{\ell} \to K^*/K^{*\ell}$ is injective.

Proof. The group $K^*$ is the direct sum of a finite group and a free abelian group of infinite rank. Further, $W \subset K^*$ is finitely generated. These two facts easily imply that $K^*/W$ is again the direct sum of a finite group and a free abelian group of infinite rank. So for only finitely many prime numbers $\ell$ the group $K^*/W$ has $\ell$-torsion, and for all others the map $W/W^{\ell} \to K^*/K^{*\ell}$ is injective. This proves (5.1).

(5.2) Lemma. Let $\ell$ be a prime number satisfying

(5.3) $\ell$ does not divide $2 \cdot \Delta_K$

(5.4) the map $W/W^{\ell} \to K^*/K^{*\ell}$ is injective.

Then $[L_{\ell}:K] = q(\ell)^r \cdot \phi(q(\ell))$, and the largest abelian subextension of $K \subset L_{\ell}$ is $K(\zeta_{q(\ell)})$.

Proof. Clearly, $K(\zeta_{q(\ell)})$ is a subextension of $L$, and (5.3) implies that $[K(\zeta_{q(\ell)}):K] = \phi(q(\ell))$. To calculate $[L_{\ell}:K(\zeta_{q(\ell)})]$ we first prove that the natural map

(5.5) $W/W^{\ell} \to K(\zeta_{q(\ell)})^*/K(\zeta_{q(\ell)})^{*\ell}$

is injective.

Let $w \in W$, $w \notin W^{\ell}$. Then $w \notin K^{*\ell}$, by (5.4), so $X^{\ell} - w$ is irreducible over $K$. Combining this with $[K(\zeta_{\ell}):K] = \ell - 1$ we see that the splitting field of $X^{\ell} - w$ has degree $\ell(\ell - 1)$ over $K$, and has a non-abelian Galois group; here we use $\ell \neq 2$. Since $K(\zeta_{q(\ell)})$ has an

abelian Galois group, the splitting field of $X^{\ell} - w$ is not contained in $K(\zeta_{q(\ell)})$. We conclude that $w$ is no $\ell$-th power in $K(\zeta_{q(\ell)})$, thus establishing that (5.5) is injective.

An easy inductive argument now shows that the natural map $W/W^{q(\ell)} \to K(\zeta_{q(\ell)})^*/K(\zeta_{q(\ell)})^{*q(\ell)}$ is also injective, so Kummer theory tells us that $\mathrm{Gal}(L_\ell/K(\zeta_{q(\ell)}))$ is canonically isomorphic to the character group $\hat{W} = \mathrm{Hom}(W, <\zeta_{q(\ell)}>)$. Thus $[L_\ell : K(\zeta_{q(\ell)})] = \#\hat{W} = q(\ell)^r$ (since $W$ has no $\ell$-torsion, by (5.3)), which proves the first assertion of (5.2). Further, $\mathrm{Gal}(L_\ell/K)$ is isomorphic to the semidirect product of $\hat{W}$ by $\mathrm{Gal}(K(\zeta_{q(\ell)})/K)$, with the latter group acting on $\hat{W}$ via $<\zeta_{q(\ell)}>$. Again using that $\ell \neq 2$ one finds that the commutator subgroup of $\mathrm{Gal}(L_\ell/K)$ equals $\hat{W}$, so $K(\zeta_{q(\ell)})$ is the maximal abelian subextension of $K \subset L_\ell$. This proves (5.2).

(5.6) Lemma. Let $\ell$ be a prime number satisfying the following conditions.

(5.7) $\ell$ does not divide $2 \cdot \Delta_F$

(5.8) the map $W/W^{\ell} \to K^*/K^{*\ell}$ is injective,

(5.9) there exists no prime $\underline{p}$ of $K$ for which $\mathrm{ord}_{\underline{p}}(\ell) > 0$ and $\mathrm{ord}_{\underline{p}}(w) \neq 0$ for some $w \in W$.

Further, let $d$ be a squarefree integer, not divisible by $\ell$. Then the fields $L_\ell$ and $L_d \cdot F$ are linearly disjoint over $K$.

Proof. Since $L_\ell/K$ is Galois it suffices to prove that $L_\ell \cap L_d \cdot F = K$. Let $N = L_\ell \cap L_d \cdot F$. Then $N/K$ is a solvable Galois extension, so if $N \neq K$ then there exists an abelian subextension $N'/K$, $N' \subset N$, $N' \neq K$. From $N' \subset L_\ell$ and (5.2) we then have $N' \subset K(\zeta_{q(\ell)})$, which by (5.7) implies that $N'/K$ is ramified at every prime $\underline{p}$ lying over $\ell$ (i.e., for which $\mathrm{ord}_{\underline{p}}(\ell) > 0$). On the other hand, $N' \subset L_d \cdot F$ implies that $N'/K$ can only ramify at primes $\underline{p}$ of $K$ for which

$$\text{ord}_{\mathfrak{P}}(d) > 0,$$

or $\text{ord}_{\mathfrak{P}}(w) \neq 0$ for some $w \in W$,

or $\text{ord}_{\mathfrak{P}}(\Delta_F) > 0$.

By $(d, \ell) = 1$, (5.9) and (5.7) none of these primes lies over $\ell$, contradicting what we just proved. This proves (5.6).

Proof of (4.5) in the number field case. Suppose $a_n \neq 0$ for all $n$. We prove that $a \neq 0$.

Let $\ell$ and $d$ be as in (5.6). Then (5.6), the definition of $C_n$, and (5.2) give

$$[L_{d\ell} \cdot F : K] = [L_\ell : K] \cdot [L_d \cdot F : K]$$

$$\#C_{d\ell} = ([L_\ell : K] - 1) \cdot \#C_d$$

$$[L_\ell : K] = q(\ell)^r \cdot \phi(q(\ell)) = q(\ell)^{r+1} \cdot (1 - 1/\ell), \tag{5.10}$$

so

$$a_{d\ell} = a_d \cdot \left(1 - \frac{1}{[L_\ell : K]}\right).$$

Now let $n$ be the product of those $\ell$ which violate at least one of the conditions (5.7), (5.8), (5.9). Then for any multiple $m$ of $n$ it follows by induction on the number of prime numbers dividing $m/n$ that

$$a_m = a_n \cdot \Pi_{\ell \mid m/n} \left(1 - \frac{1}{[L_\ell : K]}\right)$$

so in the limit

$$a = a_n \cdot \Pi_{\ell \nmid n} \left(1 - \frac{1}{[L_\ell : K]}\right). \tag{5.11}$$

From (5.10) and $r \geq 1$ it is clear that the infinite product converges and is non-zero. So $a_n \neq 0$ indeed implies that $a \neq 0$. This proves (4.5) if $K$ is a number field.

## 6. Proof of (4.5): the function field case.

In this section $K$ is assumed to be a function field, and we denote by $P$ the free abelian group

$$P = \oplus_{\underline{p}} \mathbb{Z},$$

the direct sum ranging over all primes $\underline{p}$ of $K$. There is a natural group homomorphism $K^* \to P$ mapping $x$ to $(\mathrm{ord}_{\underline{p}}(x))_{\underline{p}}$, and the kernel of this map is finite, consisting of the non-zero constants in $K$.

(6.1) Lemma. For all but finitely many $\ell$ the induced map $W/W^{\ell} \to P/\ell P$ is injective.

Proof. Similar to the proof of (5.1). This proves (6.1).

(6.2) Lemma. Let $m$ be such that any $\ell | m$ satisfies

(6.3) $K$ contains no primitive $\ell$-th root of unity;

(6.4) $W/W^{\ell} \to P/\ell P$ is injective.

Then $[L_m : K(\zeta_{q(m)})] = q(m)^r$, and $K(\zeta_{q(m)})$ is the largest totally unramified subextension of $K \subset L_m$.

Proof. From (6.4) it follows that the natural map $W/W^{\ell} \to K^*/K^{*\ell}$ is injective, for any $\ell | m$. Using (6.3), one finds by the argument in the proof of (5.2) that also $W/W^{\ell} \to K(\zeta_{q(m)})^*/K(\zeta_{q(m)})^{*\ell}$ is injective. Kummer theory then implies that $[L_m : K(\zeta_{q(m)})] = \#(W/W^{q(m)})$, and by (6.3) this equals $q(m)^r$.

Let $N$ be the maximal totally unramified subextension of $K \subset L_m$. Clearly $K(\zeta_{q(m)}) \subset N$, and if the inclusion holds strictly then $N$ contains $w^{1/\ell}$ for some $\ell | m$ and some $w \in W$, $w \notin W^{\ell}$. By (6.4), we then have $\ell \nmid \mathrm{ord}_{\underline{p}}(w)$ for some prime $\underline{p}$ of $K$, so $N/K$ is ramified at this $\underline{p}$,

contradiction. This proves (6.2).

(6.5) Lemma. Let $n$ be the product of those prime numbers $\ell \neq p$ which satisfy at least one of the following conditions:

(6.6) $K$ contains a primitive $\ell$-th root of unity;

(6.7) the map $W/W^{\ell} \to P/\ell P$ is not injective;

(6.8) there is a prime $\underline{p}$ of $K$ which ramifies in $F/K$, with ramification index divisible by $\ell$.

Further, let $m$ be relatively prime to $n$. Then we have:

(6.9) $F \cdot L_n \cap L_m = F \cdot L_n \cap K(\zeta_{q(m)})$

(6.10) $[F \cdot L_{nm} : K] = [F \cdot L_n : K] \cdot q(n)^r \cdot [F \cdot L_n(\zeta_{q(m)}) : F \cdot L_n]$

(6.11) if $m = m_1 \cdot m_2$, then

$$(F \cdot L_n \cap L_{m_1}) \cdot (F \cdot L_n \cap L_{m_2}) = F \cdot L_n \cap L_m.$$

Proof. (6.9). The inclusion $\supset$ is clear. By (6.8), all ramification indices in the extension $K \subset F \cdot L_n$ are composed of prime numbers dividing $pn$, and all ramification indices in $K \subset L_m$ are composed of prime numbers dividing $m$. Since $(pn, m) = 1$, it follows that $F \cdot L_n \cap L_m$ is totally unramified over $K$, so (6.2) implies that $F \cdot L_n \cap L_m \subset K(\zeta_{q(m)})$. This implies the opposite inclusion.

(6.10). We have:

$$\begin{aligned}
[F \cdot L_{nm} : F \cdot L_n] &= [F \cdot L_n \cdot L_m : F \cdot L_n] \\
&= [L_m : F \cdot L_n \cap L_m] \\
&= [L_m : F \cdot L_n \cap K(\zeta_{q(m)})] && \text{by (6.9)} \\
&= q(m)^r \cdot [K(\zeta_{q(m)}) : F \cdot L_n \cap K(\zeta_{q(m)})] && \text{by (6.2)} \\
&= q(m)^r \cdot [F \cdot L_n(\zeta_{q(m)}) : F \cdot L_n].
\end{aligned}$$

Multiplying by $[F\cdot L_n:K]$ we obtain (6.10).

(6.11). Let $G = \mathrm{Gal}(K(\zeta_{q(m)})/K)$. This is a cyclic group, since $\zeta_{q(m)}$ lies in a finite subfield. Define the subgroups $H_1$, $H_2$, $H$ of $G$ by

$$H_i = \mathrm{Gal}(K(\zeta_{q(m)})/K(\zeta_{q(m_i)})), \qquad i = 1, 2,$$
$$H = \mathrm{Gal}(K(\zeta_{q(m)})/F\cdot L_n \cap K(\zeta_{q(m)})).$$

Since $m$ is squarefree, we have $(m_1, m_2) = 1$ so $K(\zeta_{q(m_1)})\cdot K(\zeta_{q(m_2)}) = K(\zeta_{q(m)})$ and $H_1 \cap H_2 = \{\mathrm{id}_{K(\zeta_{q(m)})}\}$. But $G$ is cyclic, so $\#H_1$ and $\#H_2$ are relatively prime. Then also the index of $H$ in $H\cdot H_1$ is relatively prime to the index of $H$ in $H\cdot H_2$, so

$$H\cdot H_1 \cap H\cdot H_2 = H.$$

In terms of fields, this means

$$(F\cdot L_n \cap K(\zeta_{q(m_1)}))\cdot(F\cdot L_n \cap K(\zeta_{q(m_2)})) = F\cdot L_n \cap K(\zeta_{q(m)}).$$

By (6.9), this is equivalent to (6.11). This proves (6.5).

(6.12) Lemma. Let $f$, $g$ be two functions defined on squarefree integers such that

(6.13) $f(d)$ is a real number, $0 \le f(d) \le 1$

(6.14) $g(d) \in \mathbb{Z}$, $g(d) > 0$

for all $d$, and such that

(6.15) $f(d_1d_2) = f(d_1)f(d_2)$

(6.16) $g(d_1d_2) =$ least common multiple of $g(d_1)$ and $g(d_2)$

for all $d_1$, $d_2$ with $(d_1, d_2) = 1$. Then for all $m$ we have

$$\Sigma_{d|m} \frac{\mu(d)f(d)}{g(d)} \ge \Pi_{\ell|m,\ \ell \text{ prime}} \left(1 - \frac{f(\ell)}{g(\ell)}\right).$$

Proof. See [10, 21]. This proves (6.12).

(6.17) Lemma. Let $s$ be an integer, $s > 1$, and for any integer $u > 0$ relatively prime to $s$ let $e(u)$ be the smallest integer $t > 0$ with $s^t \equiv 1 \bmod u$. Then

$$\Sigma_{u>0,\ (u,s)=1} \frac{1}{u \cdot e(u)}$$

is convergent.

Proof. See [18, Ch. V, Lemma 8.3; 21]. This proves (6.17).

Proof of (4.5) in the function field case. Let $n$ be as defined in (6.5). We prove that $a_n \neq 0$ implies that $a \neq 0$.

Let $m$ be relatively prime to $n$. For $\tau \in C_n$, define

$$C_m(\tau) = \{\sigma \in \mathrm{Gal}(F \cdot L_{nm}/K):\ (\sigma | F \cdot L_n) = \tau,\ \text{and}\ (\sigma | L_\ell) \neq \mathrm{id}_{L_\ell}\ \text{for all}\ \ell | m\},$$

$$a_m(\tau) = {}^{\#}C_m(\tau)/[F \cdot L_{nm} : K],$$

$$a(\tau) = \lim_m a_m(\tau)$$

the limit being over all squarefree integers $m > 0$ which are relatively prime to $pn$, ordered by divisibility; it is easily seen to exist.

Clearly, we have

$$C_{nm} = \cup_{\tau \in C_n} C_m(\tau) \qquad \text{(disjoint union)}$$

$$a_{nm} = \Sigma_{\tau \in C_n} a_m(\tau)$$

$$a = \Sigma_{\tau \in C_n} a(\tau).$$

We claim that $a(\tau) > 0$ for every $\tau \in C_n$. Since $C_n$ is non-empty (by $a_n \neq 0$) this implies $a > 0$. Put

$$c(\tau, m) = \begin{cases} 1 & \text{if } \tau \in \mathrm{Gal}(F \cdot L_n / F \cdot L_n \cap L_m), \\ 0 & \text{else.} \end{cases}$$

Notice that (6.11) implies

(6.18) $\quad c(\tau, m) = c(\tau, m_1)\cdot c(\tau, m_2) \quad$ if $\quad m = m_1 m_2$.

Applying the principle of inclusion and exclusion as in (2.14) we find that

$$a_m(\tau) = \Sigma_{d|m} \frac{\mu(d)\cdot c(\tau,d)}{[F\cdot L_{nd}:K]}$$

which by (6.10) is equal to

$$\frac{1}{[F\cdot L_n:K]}\cdot \Sigma_{d|m} \frac{\mu(d)\cdot c(\tau,d)\cdot q(d)^{-r}}{[F\cdot L_n(\zeta_{q(d)}):F\cdot L_n]}.$$

Putting $f(d) = c(\tau, d)\cdot q(d)^{-r}$, $g(d) = [F\cdot L_n(\zeta_{q(d)}):F\cdot L_n]$ we find

$$a_m(\tau) = \frac{1}{[F\cdot L_n:K]}\cdot \Sigma_{d|m} \frac{\mu(d)f(d)}{g(d)}.$$

We are in a position to apply lemma (6.12). Conditions (6.13) and (6.14) are obviously satisfied, and (6.15) is clear from (6.18). To prove (6.16), let $Q$ be the largest finite field contained in $F\cdot L_n$, and notice that

$$g(d) = [Q(\zeta_{q(d)}):Q] = \min\{t > 0: \quad (\#Q)^t \equiv 1 \bmod q(d)\}.$$

We conclude that

$$a_m(\tau) \geq \frac{1}{[F\cdot L_n:K]}\cdot \Pi_{\ell|m} \left(1 - \frac{f(\ell)}{g(\ell)}\right).$$

The infinite product

$$\Pi_{\ell \text{ prime},\ \ell\nmid np} \left(1 - \frac{f(\ell)}{g(\ell)}\right) = \Pi_{\ell\nmid n} \left(1 - \frac{c(\tau,\ell)}{g(\ell)\cdot q(\ell)^r}\right)$$

is clearly convergent if $r \geq 2$, and if $r = 1$ it converges by lemma (6.17). It follows that

$$a(\tau) \geq \frac{1}{[F\cdot L_n:K]}\cdot \Pi_{\ell\nmid n} \left(1 - \frac{f(\ell)}{g(\ell)}\right) > 0,$$

as required. This proves (4.5).

## 7. Proof of theorem (4.1).

In this section, $h$ is as defined in (4.1).

(7.1) Lemma. Let $\ell$ be a prime number $\neq p$. Then all prime numbers dividing $[L_\ell \cdot F(\zeta_h):F(\zeta_h)]$ are $\leq \ell$. Further, if $[L_\ell \cdot F(\zeta_h):F(\zeta_h)]$ is not divisible by $\ell$, then $L_\ell \subset F(\zeta_h)$.

Proof. The degree $[F(\zeta_h,\zeta_\ell):F(\zeta_h)]$ is a divisor of $\ell - 1$, and $L_\ell \cdot F(\zeta_h)$ is obtained from $F(\zeta_h, \zeta_\ell)$ by successively adjoining zeros of polynomials $X^\ell - \alpha$. At each stage, such a polynomial is either irreducible or completely reducible. Hence $[L_\ell \cdot F(\zeta_h):F(\zeta_h,\zeta_\ell)]$ is a power of $\ell$. This implies the first assertion of the lemma. Moreover, if $\ell$ does not occur in $[L_\ell \cdot F(\zeta_h):F(\zeta_h)]$, then $L_\ell \cdot F(\zeta_h) = F(\zeta_h, \zeta_\ell)$, so

$$L_\ell \subset F(\zeta_h, \zeta_\ell). \tag{7.2}$$

If now $W \subset K^{*q(\ell)}$, then $\ell$ divides $h$, so $\zeta_\ell \in F(\zeta_h)$, and this gives $L_\ell \subset F(\zeta_h)$, as required. So suppose $W$ is not contained in $K^{*q(\ell)}$. Then for some $w \in W$ the polynomial $X^{q(\ell)} - w$ has no zero in $K$, and this easily implies that for some $v \in K$ with $v^{q(\ell)/\ell} \in W$ the polynomial $X^\ell - v$ has no zero in $K$. Then $X^\ell - v$ is irreducible over $K$, and it has a zero in $L_\ell$ and hence in $F(\zeta_h, \zeta_\ell)$. Since $[F(\zeta_h,\zeta_\ell):F(\zeta_h)]$ is relatively prime to $\ell$, it must actually have a zero in $F(\zeta_h)$. But $F(\zeta_h)$ is normal over $K$, so it now follows that all zeros of $X^\ell - v$ are in $F(\zeta_h)$. Therefore $\zeta_\ell \in F(\zeta_h)$, so (7.2) gives $L_\ell \subset F(\zeta_h)$. This proves (7.1).

Proof of (4.1). We must prove that (4.4) implies (4.3). So let $m$ be the product of those $\ell$ for which $L_\ell \subset F(\zeta_h)$; then (4.4) means that $C_m \neq \emptyset$. We prove that this implies $C_n \neq \emptyset$ for every multiple $n$ of $m$. Then

$a_n \neq 0$ for all $n$, which is (4.3).

The proof that $C_n \neq \emptyset$ is by induction on the number $t$ of primes dividing $n/m$. The case $t = 0$ is obvious. So let $t > 0$, and let $\ell$ be the largest prime number dividing $n/m$. Put $n_0 = n/\ell$. The inductive hypothesis tells us that $C_{n_0} \neq \emptyset$. Since $\ell \nmid m$, we know from (7.1) that $\ell$ divides $[L_\ell \cdot F(\zeta_h) : F(\zeta_h)]$, while all prime factors of $[L_{n_0} \cdot F(\zeta_h) : F(\zeta_h)]$ are $\leq$ some prime number dividing $n_0$ and therefore $< \ell$. We conclude that $L_\ell \cdot F(\zeta_h)$ is not contained in $L_{n_0} \cdot F(\zeta_h)$, so a fortiori

$$(7.3) \qquad L_{n_0} \cdot F \subsetneq L_\ell \cdot L_{n_0} \cdot F = L_n \cdot F.$$

Now let $\tau \in C_{n_0}$; that is, $\tau$ is an automorphism of $L_{n_0} \cdot F$ with

$$(\tau | F) \in C$$

$$(\tau | L_{\ell'}) \neq \mathrm{id}_{L_{\ell'}} \quad \text{for all } \ell' | n_0.$$

By (7.3), we can extend $\tau$ to an automorphism of $L_n \cdot F$ which is not the identity on $L_\ell$. This gives an element of $C_n$, so $C_n \neq \emptyset$.

This proves theorem (4.1).

## 8. Examples.

Let $q$ be a prime number, and let $g$ be an integer. We say that $g$ is a Fibonacci primitive root [24, 1] modulo $q$ if $g$ is a primitive root mod $q$ and satisfies the congruence $g^2 \equiv g + 1 \bmod q$.

(8.1) Theorem. If GRH is true, then the set $S$ of prime numbers which have a Fibonacci primitive root has a density, and

$$d(S) = \frac{27}{38} \cdot \Pi_\ell \left(1 - \frac{1}{\ell(\ell - 1)}\right) = 0{\cdot}265705\ldots;$$

here $\ell$ ranges over all prime numbers.

Proof (sketch). Let $\theta = (1 + \sqrt{5})/2$ be a zero of $X^2 - X - 1$, and consider

$$M_1 = M(\mathbb{Q}(\theta),\ \mathbb{Q}(\theta,\ \zeta_4),\ \{id_{\mathbb{Q}(\theta,\zeta_4)}\},\ \langle\theta\rangle,\ 1),$$
$$M_2 = M(\mathbb{Q}(\theta),\ \mathbb{Q}(\theta,\ \zeta_4),\ \{\tau\},\ \langle\theta\rangle,\ 1)$$

where $\tau$ is the non-trivial automorphism of $\mathbb{Q}(\theta, \zeta_4)$ over $\mathbb{Q}(\theta)$. Then it is not hard to see (cf. [24]) that

$$d(\{q \in S:\ q \equiv 1 \bmod 4\}) = \tfrac{1}{2} d(M_1)$$
$$d(\{q \in S:\ q \equiv -1 \bmod 4\}) = d(M_2)$$

so

$$d(S) = \tfrac{1}{2} d(M_1) + d(M_2)$$

if $d(M_1)$ and $d(M_2)$ exist. If GRH is true, then (3.1), (5.11) and a short calculation show that

$$d(M_1) = d(M_2) = \frac{9}{40} \cdot \Pi_{\ell \nmid 10} \left(1 - \frac{1}{\ell(\ell - 1)}\right)$$

so

$$d(S) = \frac{3}{2}\cdot\frac{9}{40}\cdot 2\cdot\frac{20}{19}\cdot\Pi_\ell \left(1 - \frac{1}{\ell(\ell-1)}\right) = \frac{27}{38}\cdot A$$

where $A$ is Artin's constant:

$$A = \Pi_\ell \left(1 - \frac{1}{\ell(\ell-1)}\right) = 0{\cdot}3739558136\ldots \tag{8.2}$$

(see [32]). This proves (8.1).

(8.3) Theorem. Let $b$, $c$ be positive integers, $(b, c) = 1$, and let $t \in \mathbb{Q}$, $t \neq 0, 1, -1$. Put

$$d(t) = \Delta_{\mathbb{Q}(\sqrt{t})}.$$

Then the set of prime numbers $q$ for which

$$q \equiv b \bmod c \tag{8.4}$$

$$t \text{ is a primitive root mod } q \tag{8.5}$$

is finite if and, modulo GRH, only if we are in one of the following situations:

(8.6) $\ell \mid c$, $b \equiv 1 \bmod \ell$, $t \in \mathbb{Q}^{*\ell}$ for some prime number $\ell$;

(8.7) $d(t) \mid c$, $\left(\frac{d(t)}{b}\right) = 1$ (Kronecker symbol);

(8.8) $d(t) \mid 3c$, $3 \mid d(t)$, $\left(\frac{-d(t)/3}{b}\right) = -1$, $t \in \mathbb{Q}^{*3}$.

Proof (sketch). The set we are interested in is

$$M = M(\mathbb{Q}, \mathbb{Q}(\zeta_c), \{\sigma_b\}, \langle t\rangle, 1)$$

where $\sigma_b$ is the automorphism of $\mathbb{Q}(\zeta_c)$ mapping $\zeta_c$ to $\zeta_c^b$. By (4.6), this set is finite if and, modulo GRH, only if $\mathbb{Q}(\zeta_c, \zeta_h)$ does not have an automorphism satisfying certain requirements; here $h = \Pi_{t\in\mathbb{Q}^{*\ell}} \ell$. A straightforward analysis shows that the only obstructions preventing the existence of such a $\sigma$ are the conditions (8.6), (8.7) and (8.8). This

proves (8.3).

We remark that the if-part of (8.3) can be proved directly, using nothing more than quadratic reciprocity; in fact, one finds that in each of the situations (8.6), (8.7) and (8.8) the set of primes in question either is empty or only contains the prime number 2. But the advantage of our approach is 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 (mod GRH).

Using (5.11) it is possible to derive a formula for the conjectural density of the set of prime numbers satisfying (8.4) and (8.5). In each case the result is a rational number times Artin's constant (8.2).

The same remarks apply to other sets of primes of a similar type. For example, we can consider the prime numbers $q$ with the property that a given rational number $t \neq 0$ has <u>residue index</u> $k$ modulo $q$; i.e., the subgroup generated by $(t \bmod q)$ should have index $k$ in $\mathbb{F}_q^*$. Here $k$ is a given integer $\geq 1$. The set of such $q$ is a subset of

$$M(\mathbb{Q}, \mathbb{Q}, \{id_{\mathbb{Q}}\}, \langle t \rangle, k)$$

since here it is only required that the residue index of $t$ <u>divides</u> $k$. To force equality, we also require that $k$ divides the residue index, i.e. that $q$ splits completely in $F = \mathbb{Q}(\zeta_k, t^{1/k})$. This leads to the set

$$M = M(\mathbb{Q}, \mathbb{Q}(\zeta_k, t^{1/k}), \{id_F\}, \langle t \rangle, k).$$

Applying (4.6) one finds that $M$ is finite if and, modulo GRH, only if one of the following conditions is satisfied, with $t$ and $d(t)$ as in (8.3):

(8.9) $d(t) \mid k$, and $k$ is odd;

(8.10) $t = -u^2$, $d(2u) \mid 2k$, $k \equiv 2 \bmod 4$ for some $u \in \mathbb{Q}$;

(8.11) $t = u^{2^{m-1} \cdot 3}$, $d(-3u) \mid k$, $3 \nmid k$, $2^m \mid k$ for some $u \in \mathbb{Q}$, $m \in \mathbb{Z}_{\geq 1}$;

(8.12) $t = -u^{2^{m-1} \cdot 3}$, $d(-3u) \mid k$, $3 \nmid k$, $2^{m+1} \mid k$ for some $u \in \mathbb{Q}$, $m \in \mathbb{Z}_{\geq 2}$;

(8.13) $t = -u^6$, $d(-6u) \mid k$, $3 \nmid k$, $k \equiv 4 \bmod 8$ for some $u \in \mathbb{Q}$.

This answers a question left open in [17].

We can combine the various requirements. Thus, with $b$, $c$, $t$, $k$ as before, we can consider the set of prime numbers $q$ satisfying

$q \equiv b \bmod c$

$t$ has residue index $k$ modulo $q$.

This set differs by only finitely many elements from

$$M = M(\mathbb{Q}, F, C, \langle t \rangle, k)$$

where

$$F = \mathbb{Q}(\zeta_c, \zeta_k, t^{1/k})$$

and where $C$ consists of those automorphisms $\sigma$ of $F$ for which

$$\sigma(\zeta_c) = \zeta_c^b, \qquad \sigma(\zeta_k) = \zeta_k, \qquad \sigma(t^{1/k}) = t^{1/k}$$

(so $\#C \leq 1$). It is again possible, by a straightforward but tedious analysis, to find the complete list of obstructions preventing $M$ from being infinite (mod GRH).

For more details on a similar example, related to arithmetic codes, we refer to [15].

In the next section we apply our results to prove a theorem about euclidean rings. Another application of the same type is found at the end of Cooke's and Weinberger's paper [5]. Further, our corollary (4.8) can be used to improve slightly upon a result of Queen [20, th. 1].

To finish this section we mention some sets of prime numbers to which our results do not immediately apply. Most of these can be dealt with by small modifications of our method, and in case (8.16) the GRH can even be dispensed with.

(8.14) The set of primes $q$ for which $2$ is a primitive root modulo $q^2$.

(8.15) The set of primes $q$ for which the residue index of $2$ is a power of $2$.

(8.16) The set of primes $q$ for which the residue index of $2$ is squarefree (cf. [6]).

(8.17) The set of primes $q$ for which both $2$ and $3$ are primitive roots (cf. [16]).

(8.18) The set of primes $q$ for which a given positive integer $t$ is the smallest positive integral primitive root (cf. [11]).

## 9. Euclid's algorithm.

Let $K$ be a global field, and let $S$ be a non-empty set of prime divisors of $K$, containing the set $S_\infty$ of archimedean prime divisors of $K$. We denote by $R_S$ the ring of $S$-integers in $K$:

$$R_S = \{x \in K: \ \mathrm{ord}_{\mathfrak{p}}(x) \geq 0 \ \text{ for all primes } \ \mathfrak{p} \notin S\}.$$

Thus, if $K$ is a number field and $S = S_\infty$, then $R_S$ is the ring of algebraic integers in $K$.

We ask under which conditions there exists a <u>euclidean algorithm</u> on $R_S$, i.e. a function $\psi: R_S - \{0\} \to \mathbb{Z}_{\geq 0}$ such that for all $b, c \in R_S$, $c \neq 0$, there exist $q, r \in R_S$ with

$$b = qc + r, \qquad r = 0 \ \text{ or } \ \psi(r) < \psi(c).$$

If such a $\psi$ exists, we call $R_S$ <u>euclidean</u>. It is well known that a necessary condition for $R_S$ to be euclidean is that it is a principal ideal ring. If $R_S$ is euclidean, then its <u>smallest algorithm</u> $\theta$ is defined by

$$\theta(x) = \min\{\psi(x): \ \psi \ \text{ is a euclidean algorithm on } R_S\}.$$

It is easily verified that $\theta$ is indeed a euclidean algorithm on $R_S$, cf. [23].

If $S$ has precisely one element, then $R_S$ is euclidean if and only if it is isomorphic to one of the rings

$$\mathbb{Z}, \ \mathbb{Z}[\tfrac{1}{2}(1+\sqrt{-3})], \ \mathbb{Z}[\sqrt{-1}], \ \mathbb{Z}[\tfrac{1}{2}(1+\sqrt{-7})],$$
$$\mathbb{Z}[\sqrt{-2}], \ \mathbb{Z}[\tfrac{1}{2}(1+\sqrt{-11})], \ \mathbb{F}[X]$$

where $\mathbb{F}$ is a finite field. Up to isomorphism there are precisely eight principal ideal rings $R_S$ with $\#S = 1$ which are not euclidean. They are

$$\mathbb{Z}[\tfrac{1}{2}(1 + \sqrt{-19})], \quad \mathbb{Z}[\tfrac{1}{2}(1 + \sqrt{-43})],$$

$$\mathbb{Z}[\tfrac{1}{2}(1 + \sqrt{-67})], \quad \mathbb{Z}[\tfrac{1}{2}(1 + \sqrt{-163})],$$

$$\mathbb{F}_2[X, Y]/(Y^2 + Y + X^3 + X + 1),$$

$$\mathbb{F}_2[X, Y]/(Y^2 + Y + X^5 + X^3 + 1),$$

$$\mathbb{F}_3[X, Y]/(Y^2 - X^3 + X + 1),$$

$$\mathbb{F}_4[X, Y]/(Y^2 + Y + X^3 + \eta)$$

where $\eta \in \mathbb{F}_4$, $\eta \notin \mathbb{F}_2$. These results can be found in [23, 19].

In the case $\#S \geq 2$ we have the following theorem.

(9.1) Theorem. Suppose that $R_S$ is a principal ideal ring, and that $\#S \geq 2$. Further, if $K$ is a number field, assume that for every squarefree integer $n$ and every finite subset $S' \subset S$ the $\zeta$-function of the field $K(\zeta_n, R_{S'}^{*1/n})$ satisfies the generalized Riemann hypothesis. Then $R_S$ is euclidean, and its smallest algorithm $\theta$ is given by

$$\theta(x) = \Sigma_{\underline{p} \notin S} \operatorname{ord}_{\underline{p}}(x) \cdot n_{\underline{p}} \qquad (x \in R_S, \quad x \neq 0) \tag{9.2}$$

where the sum is over all primes of $K$ which are not in $S$, and

$n_{\underline{p}} = 1$ if the natural map $R_S^* \to \overline{K}_{\underline{p}}^*$ is surjective

$n_{\underline{p}} = 2$ else.

The Riemann hypotheses mentioned in this theorem will again be denoted by "GRH".

The function field case of (9.1) is due to Queen [19]. In the number field case only a partial result was known: Weinberger [30] proved, modulo certain generalized Riemann hypotheses, that if $K$ has class number one and $S = S_\infty$, $\#S \geq 2$, a euclidean algorithm on $R_S$ is given by

$$\psi(x) = \Sigma_{\underline{p} \notin S} \operatorname{ord}_{\underline{p}}(x) \cdot (n_{\underline{p}} + 1)$$

with $n_{\underline{p}}$ as defined in (9.1). Since this function does not assume the value 1, it is obviously not the smallest algorithm.

We remark that in the number field case all known euclidean rings $R_S$, $\#S < \infty$, are actually euclidean with respect to the norm function

$$N(x) = \#(R_S/R_S x), \qquad x \in R_S, \quad x \neq 0.$$

Here no Riemann hypotheses are assumed. The rings $\mathbb{Z}[\sqrt{14}]$, $\mathbb{Z}[\zeta_{32}]$ are examples of rings of unknown character: they are euclidean if GRH is true, but the norm function is not a euclidean algorithm.

Before giving the proof of (9.1) we introduce some terminology. A <u>divisor</u> of $K$ is a formal product $\prod_{\underline{p}} \underline{p}^{m(\underline{p})}$, $m(\underline{p}) \in \mathbb{Z}$, $m(\underline{p}) = 0$ for all but finitely many $\underline{p}$, with $\underline{p}$ ranging over the non-archimedean prime divisors of $K$. For $x \in K^*$, the <u>principal divisor</u> $(x)$ is defined by $(x) = \prod_{\underline{p}} \underline{p}^{\mathrm{ord}_{\underline{p}}(x)}$. The set of divisors of $K$ is an abelian group with respect to multiplication, and the principal divisors form a subgroup. Let $\underline{b} = \prod_{\underline{p}} \underline{p}^{n(\underline{p})}$ be a divisor with $n(\underline{p}) \geq 0$ for all $\underline{p}$. A subgroup $H$ of the group of divisors is said to have <u>modulus</u> $\underline{b}$ if

$$\text{for every } \prod_{\underline{p}} \underline{p}^{m(\underline{p})} \in H \text{ and all } \underline{p} \text{ with } n(\underline{p}) > 0$$
$$\text{we have } m(\underline{p}) = 0$$

and

$$(x) \in H \text{ for all } x \in K^* \text{ satisfying}$$
$$\mathrm{ord}_{\underline{p}}(x - 1) \geq n(\underline{p}) \text{ for all } \underline{p} \text{ with } n(\underline{p}) > 0.$$

The primes $\underline{p}$ of $K$ with $\underline{p} \nmid S$ are in one-to-one correspondence with the non-zero prime ideals of $R_S$. We identify the group of fractional $R_S$-ideals with the group of those divisors $\prod_{\underline{p}} \underline{p}^{m(\underline{p})}$ for which $m(\underline{p}) = 0$ for all $\underline{p} \in S$.

Proof of (9.1). Suppose, for the moment, that $R_S$ is euclidean, and let $\theta$ denote its smallest algorithm. If $\pi \in R_S$ is a prime element, $R_S\pi = \underline{p}$, then Samuel's results [23, sec. 4] easily imply that $\theta(\pi) \geq n_{\underline{p}}$. Since further $\theta(xy) \geq \theta(x) + \theta(y)$, by [23, prop. 12], we conclude that

$$\theta(x) \geq \Sigma_{\underline{p} \nmid S} \operatorname{ord}_{\underline{p}}(x) \cdot n_{\underline{p}}, \qquad x \in R_S, \quad x \neq 0.$$

So if the right hand side represents an algorithm on $R_S$, it is necessarily the smallest one.

In the rest of the proof let $\theta$ be defined by (9.2), and assume GRH. We must prove that $\theta$ is a euclidean algorithm on $R_S$. Let $b, c \in R_S$, $c \neq 0$. We look for an element

$$r \in b + R_S \cdot c$$

with

$$r = 0 \quad \text{or} \quad \theta(r) < \theta(c).$$

Dividing $b$ and $c$ by their greatest common divisor - they have one, since $R_S$ is a principal ideal ring - we may suppose that $(b, c) = 1$. Further, replacing $S$ by a finite subset which also yields a principal ideal ring and gives the same value for $\theta(c)$, we may suppose that $2 \leq \#S < \infty$.

If $\theta(c) = 0$, then $c \in R_S^*$, so we can take $r = 0$.

If $\theta(c) = 1$, then $c$ is a prime element: $R_S c = \underline{p}$, and $n_{\underline{p}} = 1$. Then the map $R_S^* \to \overline{K}_{\underline{p}}^* \cong (R_S/R_S c)^*$ is surjective, so we can find $r \in R_S^*$ with $r \equiv b \bmod R_S c$. Clearly, $\theta(r) = 0 < 1 = \theta(c)$.

If $\theta(c) \geq 3$, then a suitable generalization of Dirichlet's theorem on primes in arithmetic progressions [13] tells us that every residue class in $(R_S/R_S c)^*$ contains infinitely many prime elements. In particular, the

residue class $b + R_S c$ contains a prime element $r$, and then we have $\theta(r) \leq 2 < 3 \leq \theta(c)$.

We are left with the case $\theta(c) = 2$. It would, in this case, be sufficient to find a prime $\underline{r}$ of $K$, $\underline{r} \notin S$, with the following two properties:

(9.3) $\quad n_{\underline{r}} = 1$

(9.4) $\quad \underline{r} = R_S \cdot r \quad$ for some $\quad r \in b + R_S c$.

This would give $\theta(r) = n_{\underline{r}} = 1 < 2 = \theta(c)$, as required.

Condition (9.3) simply means that the natural map

$$R_S^* \to \overline{K}_{\underline{r}}^*$$

is surjective. Clearly, this is a condition of the type considered in section 2, with $W = R_S^*$, $k = 1$. Notice that the rank of $W$, modulo its torsion subgroup, equals $\#S - 1 \geq 1$.

Using class field theory [13] we translate the condition (9.4) into one of the type "$(\underline{p}, F/K) \subset C$", as follows. For $F$ we take what has been called the S-ray class field with modulus $c$. More precisely, $F$ is the class field of $K$ with respect to the smallest group of divisors with modulus $R_S c$ which contains all non-archimedean $\underline{p} \in S$. We call this group of divisors $H$. Properties of $F$ are:

(9.5) $\quad F/K$ is abelian

(9.6) $\quad$ the conductor of $F/K$ divides $R_S c$,

(9.7) $\quad$ all $\underline{p} \in S$ split completely in $F$,

and moreover $F$ is the largest field with these properties, inside an algebraic closure of $K$; cf. [5].

Let $I$ denote the group of divisors generated by all $\underline{p}$ not occurring

in $R_S c$, and let $P$ be the subgroup $\{(x) : x \in K^*, (x) \in I\}$. Since $R_S$ is a principal ideal ring, we can write any element of $I$ as the product of an element of $P$ and a factor $\prod_{\underline{p} \in S} \underline{p}^{m(\underline{p})}$, $m(\underline{p}) \in \mathbb{Z}$, the product ranging over the non-archimedean $\underline{p} \in S$. The latter factor is an element of $H$, so $I = P \cdot H$. Translating this statement on divisor groups into one about their class fields, we find that

(9.8) $K$ is the maximal totally unramified subextension of $K \subset F$.

By class field theory, the Frobenius symbol induces an isomorphism $I/H \cong \mathrm{Gal}(F/K)$. But we have $I = P \cdot H$, and a short calculation leads to

(9.9) $$(R_S/R_S c)^*/\psi(R_S^*) \cong \mathrm{Gal}(F/K)$$

where $\psi: R_S^* \to (R_S/R_S c)^*$ is the natural map. Let the automorphism of $F/K$ corresponding to $(b + R_S c) \bmod \psi(R_S^*)$ be denoted by $\sigma$. Then condition (9.4) is equivalent to

(9.10) $$(\underline{r}, F/K) \subset \{\sigma\}$$

if $\underline{r}$ does not divide $R_S c$. We conclude that to prove the existence of $\underline{r}$ satisfying (9.3) and (9.4) it certainly suffices to show that the set

$$M = M(K, F, \{\sigma\}, R_S^*, 1)$$

is infinite. By (4.8) and the GRH assumption we have made, we know that indeed $M$ is infinite, except if $\sigma \in \mathrm{Gal}(F/L_\ell)$ for some prime number $\ell \neq p$ with $L_\ell \subset F$; here $L_\ell = K(\zeta_\ell, R_S^{*1/\ell})$. That means

(9.11) $$L_\ell \subset F^\sigma$$

where $F^\sigma = \{x \in F: \sigma(x) = x\}$. To finish the proof of (9.1) it suffices to derive a contradiction from (9.11).

In the function field case we are immediately done. Namely, the definition of $L_\ell$ makes it clear that $L_\ell/K$ can only ramify at primes in S, if K is a function field; but F/K is unramified at these primes, by (9.6) or (9.7), so we can only have (9.11) if $L_\ell/K$ is totally unramified. By (9.8) this implies $L_\ell = K$, which is absurd, since $R_S^*$ contains elements which are no $\ell$-th powers in K.

In the remainder of the proof we therefore assume that K is a number field. The only reason that the preceding argument does not apply is that $L_\ell/K$ may ramify at primes dividing $\ell$. On the other hand, F/K only ramifies at primes dividing $R_S c$, so

(9.12) there exists a prime $\underline{\ell} \notin S$ with $\mathrm{ord}_{\underline{\ell}}(c) > 0$ and $\mathrm{ord}_{\underline{\ell}}(\ell) > 0$.

By (9.5) and (9.11), the field $L_\ell$ is abelian over K. Since $R_S^*$ contains elements which are no $\ell$-th powers in K, this implies

(9.13) $\zeta_\ell \in K$

and

(9.14) $[L_\ell : K]$ is divisible by $\ell$

(in fact, it is a power of $\ell$).

We distinguish cases. From $\theta(c) = 2$ and (9.12) we see that there are precisely three possibilities:

$$R_S c = \underline{\ell}, \quad n_{\underline{\ell}} = 2,$$

or $$R_S c = \underline{\ell}\cdot\underline{m}, \quad n_{\underline{\ell}} = n_{\underline{m}} = 1, \quad \underline{\ell} \neq \underline{m},$$

or $$R_S c = \underline{\ell}^2, \quad n_{\underline{\ell}} = 1.$$

First let $R_S c = \underline{\ell}$, $n_{\underline{\ell}} = 2$. Since $\mathrm{ord}_{\underline{\ell}}(\ell) > 0$, the characteristic of the field $R_S/\underline{\ell}$ equals $\ell$, so $\#(R_S/\underline{\ell})^* = \ell^f - 1$ for some integer

$f > 0$. By (9.11) and (9.9) it follows that $[L_\ell:K]$ divides $\ell^f - 1$, contradicting (9.14).

Next suppose that $R_S c = \underline{\ell}\cdot\underline{m}$, $n_{\underline{\ell}} = n_{\underline{m}} = 1$, $\underline{\ell} \neq \underline{m}$. Then $(R_S/R_S c)^* \cong (R_S/\underline{\ell})^* \oplus (R_S/\underline{m})^*$, and the subgroup $\psi(R_S^*)$ projects onto $(R_S/\underline{m})^*$ since $n_{\underline{m}} = 1$. Therefore $\#((R_S/R_S c)^*/\psi(R_S^*))$ divides $\#(R_S/\underline{\ell})^* = \ell^f - 1$, for some integer $f > 0$, and this leads to the same contradiction as in the preceding case.

In the remaining case: $R_S c = \underline{\ell}^2$, $n_{\underline{\ell}} = 1$, this contradiction cannot be derived. Here $\mathrm{Gal}(F/K)$ is isomorphic to $(R_S/\underline{\ell}^2)^*/\psi(R_S^*)$; since $\psi(R_S^*)$ maps onto $(R_S/\underline{\ell})^*$ this is a factor group of the kernel of the natural map $(R_S/\underline{\ell}^2)^* \to (R_S/\underline{\ell})^*$, which, in turn, is an elementary abelian $\ell$-group. Therefore Kummer theory and (9.13) tell us that

$$(9.15) \qquad F = K(x_1^{1/\ell}, \ldots, x_t^{1/\ell})$$

for some integer $t \geq 0$ and certain $x_i \in K^*$, $x_i \notin K^{*\ell}$.

Fix $i$, $1 \leq i \leq t$, for the moment. Since $F/K$ is unramified outside $\underline{\ell}$, by (9.6), we have $\mathrm{ord}_{\underline{p}}(x_i) \equiv 0 \bmod \ell$ for all primes $\underline{p} \neq \underline{\ell}$ of $K$. But $R_S$ is a principal ideal ring, so modifying $x_i$ by an $\ell$-th power we can achieve that

$$\mathrm{ord}_{\underline{p}}(x_i) = 0 \quad \text{for all } \underline{p} \notin S \cup \{\underline{\ell}\},$$
$$0 \leq \mathrm{ord}_{\underline{\ell}}(x_i) \leq \ell - 1.$$

We claim that $\mathrm{ord}_{\underline{\ell}}(x_i) = 0$. In fact, if $1 \leq \mathrm{ord}_{\underline{\ell}}(x_i) \leq \ell - 1$ then a strictly local computation shows that the $\underline{\ell}$-component of the discriminant of $K(x_i^{1/\ell})$ over $K$ equals $\underline{\ell}^{\ell-1+\ell\cdot\mathrm{ord}_{\underline{\ell}}(\ell)}$. The conductor-discriminant product formula then implies that the $\underline{\ell}$-component of the conductor of $K(x_i^{1/\ell})/K$ is equal to $\underline{\ell}^{1 + \ell\cdot\mathrm{ord}_{\underline{\ell}}(\ell)/(\ell-1)}$. On the other hand, from $K(x_i^{1/\ell}) \subset F$ and (9.6) we know that this conductor divides $R_S c = \underline{\ell}^2$.

Therefore $1 + \ell \cdot \mathrm{ord}_{\underline{\ell}}(\ell)/(\ell - 1) \leq 2$, which is impossible. This proves our claim that $\mathrm{ord}_{\underline{\ell}}(x_i) = 0$.

We now have $\mathrm{ord}_{\underline{p}}(x_i) = 0$ for all $\underline{p} \nmid S$, so $x_i \in R_S^*$ for all $i$. By (9.15) this yields

$$F \subset K(R_S^{*1/\ell}) = L_\ell$$

and combining this with (9.11) we find that $F \subset L_\ell \subset F^\sigma \subset F$, so $F = L_\ell = F^\sigma$ and $\sigma$ is the identity automorphism of $F$. This is no contradiction, but it solves our problem: namely, $\sigma = \mathrm{id}_F$ means, by definition of $\sigma$, that $(b + R_S \cdot c)$ is in the image $\psi(R_S^*)$ of $R_S^*$, so there exists $r \in R_S^*$ with $r \in b + R_S c$, and then $\theta(r) = 0 < 2 = \theta(c)$, as required. This proves (9.1).

It can be shown that the situation encountered at the end of this proof only occurs for $\ell = 2$. An example in which it does occur is given by

$$K = \mathbb{Q}(\zeta_5), \qquad S = S_\infty, \qquad R_S = \mathbb{Z}[\zeta_5],$$
$$c = 4, \qquad \ell = 2, \qquad \underline{\ell} = \text{the prime lying over } 2.$$

Thus, there exists no prime element $\pi \in \mathbb{Z}[\zeta_5]$ which is $1 \bmod 4$, for which the natural map $\mathbb{Z}[\zeta_5]^* \to (\mathbb{Z}[\zeta_5]/\mathbb{Z}[\zeta_5]\pi)^*$ is surjective. This disproves a conjecture of Queen [19, remark 2].

References.

1. Aigner, A., Quadratische und kubische Restkriterien für das Auftreten einer Fibonacci-Primitivwurzel, J. Reine Angew. Math. 274/275 (1975), 139-140.

2. Artin, E., Collected papers, Addison Wesley, Reading, Mass. 1965.

3. Bilharz, H., Primdivisoren mit vorgegebener Primitivwurzel, Math. Ann. 114 (1937), 476-492.

4. Bombieri, E., Counting points on curves over finite fields (d'après S.A. Stepanov), Sém. Bourbaki 25 (1973), exp. 430, Lecture Notes in Mathematics 383, Springer-Verlag, Berlin 1974.

5. Cooke, G. and P.J. Weinberger, On the construction of division chains in algebraic number fields, with applications to $SL_2$, Comm. Alg. 3 (1975), 481-524.

6. Goldstein, L.J., Analogues of Artin's conjecture, Trans. Amer. Math. Soc. 149 (1970), 431-442; Bull. Amer. Math. Soc. 74 (1968), 517-519.

7. Goldstein, L.J., Density questions in algebraic number theory, Amer. Math. Monthly 78 (1971), 342-351.

8. Goldstein, L.J., Some remarks on arithmetic density questions, Proc. Symp. Pure Math. 24 (Analytic number theory), 103-110, Amer. Math. Soc., 1973.

9. Hasse, H., Über die Artinsche Vermutung und verwandte Dichtefragen, Ann. Acad. Sci. Fennicae, Ser. A, 116 (1952).

10. Heilbronn, H.A., On an inequality in the elementary theory of numbers, Proc. Cambridge Philos. Soc. 33 (1937), 207-209.

11. Hooley, C., On Artin's conjecture, J. Reine Angew. Math. 225 (1967), 209-220.

12. Hooley, C., Applications of sieve methods to the theory of numbers, Cambridge University Press, Cambridge 1976.

13. Lang, S., Algebraic number theory, Addison Wesley, Reading, Mass. 1970.

14. Lehmer, D.H. and Emma Lehmer, Heuristics, anyone?, pp.202-210 in: G. Szegö et al. (eds), Studies in mathematical analysis and related topics, Essays in honor of George Pólya, Stanford University Press, Stanford 1962.

15. Lenstra, Jr., H.W., Perfect arithmetic codes of order one, in preparation.

16. Matthews, K.R., A generalization of Artin's conjecture for primitive roots, Acta Arith. 29 (1976), 113-146.

17. Möller, H., Zur Verteilung der Restindizes ganzer Zahlen, Ber. Ges. Math. Datenverarbeitung, Bonn, 57 (1972), 83-98.

18. Prachar, K., Primzahlverteilung, Springer-Verlag, Berlin 1957.

19. Queen, C., Arithmetic euclidean rings, Acta Arith. 26 (1974), 105-113.

20. Queen, C., Some arithmetic properties of subrings of function fields over finite fields, Arch. Math. 26 (1975), 51-56.

21. Rieger, G.J., Verallgemeinerung eines Satzes von Romanov und anderes, Math. Nachr. 20 (1959), 107-122.

22. Ryser, H.J., Combinatorial mathematics, Carus Math. Monographs 14, Math. Ass. of America, 1963.

23. Samuel, P., About euclidean rings, J. Algebra 19 (1971), 282-301.

24. Shanks, D., Fibonacci primitive roots, Fibonacci Qu. 10 (1972), 163-168, 181; cf. ibidem 11 (1973), 159-160.

25. Shanks, D., Review of: S. Yates, "Prime period lengths", Math. Comp. 29 (1975), 1162-1163.

26. Shanks, D., Review of: R. Baillie, "Data on Artin's conjecture", Math. Comp. 29 (1975), 1164-1165.

27. Vinogradov, A.I., Artin L-series and his conjectures, Proc. Steklov Inst. Math. 112 (1971), 124-142.

28. Weil, A., Sur les courbes algébriques et les variétés qui s'en déduisent,

Hermann, Paris 1948.

29. Weinberger, P.J., A counterexample to an analogue of Artin's conjecture, Proc. Amer. Math. Soc. 35 (1972), 49-52.

30. Weinberger, P.J., On euclidean rings of algebraic integers, Proc. Symp. Pure Math. 24 (Analytic number theory), 321-332, Amer. Math. Soc. 1973.

31. Western, A.E. and J.C.P. Miller, Tables of indices and primitive roots, University Press, Cambridge 1968.

32. Wrench, Jr., J.W., Evaluation of Artin's constant and the twin prime constant, Math. Comp. 15 (1961), 396-398.

H.W. Lenstra, Jr.

Mathematisch Instituut

Universiteit van Amsterdam

Roetersstraat 15

Amsterdam - The Netherlands.