Reprinted from JOURNAL OF NUMBER THEORY
All Rights Reserved by Academic Press, New York and London

Vol. 16, No. 2, April 1983
*Printed in Belgium*

# On Artin's Conjecture

M. RAM MURTY

*School of Mathematics, Institute for Advanced Study, Princeton, New Jersey 08540*

*Communicated by S. Chowla*

Received March 30, 1981

Let $\mathscr{F}$ be a family of number fields which are normal and of finite degree over a given number field $K$. Consider the lattice $L(\mathscr{F})$ spanned by all the elements of $\mathscr{F}$. The generalized Artin problem is to determine the set of prime ideals of $K$ which do not split completely in any element $H$ of $L(\mathscr{F})$, $H \neq K$. Assuming the generalized Riemann hypothesis and some mild restrictions on $\mathscr{F}$, we solve this problem by giving an asymptotic formula for the number of such prime ideals below a given norm. The classical Artin conjecture on primitive roots appears as a special case. In another case, if $\mathscr{F}$ is the family of fields obtained by adjoining to $\mathbf{Q}$ the $q$-division points of an elliptic curve $E$ over $\mathbf{Q}$, the Artin problem determines how often $E(\mathbf{F}_p)$ is cyclic. If $E$ has complex multiplication, the generalized Riemann hypothesis can be removed by using the analogue of the Bombieri–Vinogradov prime number theorem for number fields.

## 1. INTRODUCTION

In his studies of the law of quadratic reciprocity, Gauss [4] was led to investigate the period in the decimal expansion of $1/p$, when $p$ is a prime. He noticed that the period was equal to the order of 10 (mod $p$), if $p \neq 2$ or 5. Therefore, the longest period occurs whenever 10 is a primitive root (mod $p$). From his tables, Gauss was undoubtedly led to wonder whether there are an infinite number of primes $p$ such that 10 is a primitive root (mod $p$).

No progress on this question was made until 1927, when Artin [1] was led by probability considerations to make the following conjecture: if $a$ is a rational integer $\neq 1, -1$, or a square, then $a$ is a primitive root (mod $p$) for infinitely many primes $p$. It is clear that the restrictions on $a$ are necessary. Furthermore, letting $N_a(x)$ be the number of such primes up to $x$, Artin conjectured the existence of a constant $A(a)$ such that

$$N_a(x) \sim A(a)\frac{x}{\log x} \qquad \text{as} \quad x \to \infty.$$



0022-314X/83 $3.00

His idea was as follows: First, $a$ is a primitive root $\pmod p$ if and only if

$$a^{(p-1)/q} \not\equiv 1 \pmod p$$

for all prime divisors $q$ of $(p-1)$. According to a principle of Dedekind, $p$ splits completely in

$$K_q = Q(\sqrt[q]{1}, \sqrt[q]{a})$$

if and only if

$$a^{(p-1)/q} \equiv 1 \pmod p.$$

Hence, Artin deduced that $a$ is a primitive root $\pmod p$ if and only if $p$ does not split completely in any $K_q$. Next, he realized that the prime ideal theorem gives the density of primes which split completely in $K_q$ as

$$1/[K_q : Q].$$

Therefore, the probability that $p$ does not split completely is

$$1 - (1/[K_q : Q]).$$

So, one would expect

$$A(a) = \prod_q (1 - (1/[K_q : Q]))$$

as the density of primes for which $a$ is a primitive root.

This expression for $A(a)$ was questioned by Lehmer [14] who made some calculations. Heilbronn [9] suggested a correction because he had realized that the events

"$p$ does not split completely in $K_q$"

are not independent, as $p$ and $q$ range through all primes. For example, if $a = 5$, then

$$\{p : p \text{ does not split completely in } K_2\}$$
$$= \{p : (5/p) = -1\} = \{p : p \equiv 2 \text{ or } 3 \pmod 5, p \neq 2\}$$

and

$$\{p : p \text{ does not split completely in } K_5\}$$
$$= \{p : p \not\equiv 1 \pmod 5 \text{ or } 5^{(p-1)/5} \not\equiv 1 \pmod p\}$$
$$\supseteq \{p : p \equiv 2 \text{ or } 3 \pmod 5\}.$$

Heilbronn's correction agreed with Lehmer's machine calculations.

In 1937, Bilharz [2] proved the function field analogue of Artin's conjecture assuming the Riemann hypothesis for congruence zeta functions, which was subsequently proved by Weil. A natural question to raise is whether Artin's original conjecture could be proved assuming the generalized Riemann hypothesis (GRH) for the $L$-series of the number fields involved. This was answered in the affirmative by Hooley [10] in 1967. His expression for $A(a)$ agreed with that predicted by Heilbronn.

Lenstra [15] considered the following generalization of Artin's conjecture: Let $K$ be a global field and $F$ a finite normal extension of $K$. Let $C$ be a subset of the Galois group of $F/K$ which is stable under conjugation, and let $d$ be a positive integer (coprime to the characteristic of $K$ in the case of a function field). Consider a finitely generated subgroup $W$ of $K^*$ which has (modulo torsion) rank $r \geqslant 1$, and let $M$ be the set of prime ideals $\mathfrak{P}$ of $K$ satisfying

(i) the Artin symbol $[(F/K)/\mathfrak{P}] \subseteq C$,

(ii) the normalized exponential valuation attached to $\mathfrak{P}$ satisfies $\mathrm{ord}_{\mathfrak{P}}(w) = 0$ for all $w \in W$,

(iii) if $\psi: W \to (O_K/\mathfrak{P})^*$ is the natural map, then $[(O_K/\mathfrak{P})^*: \psi(W)]$ divides $d$, where $O_K$ is the ring of integers of $K$.

Lenstra conjectured that $M$ has a density. He also obtained necessary and sufficient conditions for this density to be nonzero.

In this paper, we consider another generalization of Artin's conjecture. Let $K$ be an algebraic number field. Let $\mathscr{F}$ be a family of number fields, normal and of finite degree over $K$. Consider the lattice $L(\mathscr{F})$ spanned by all the elements of $\mathscr{F}$. Determine the number of prime ideals $\mathfrak{P}$ of $K$ such that $N_{K/Q}(\mathfrak{P}) \leqslant x$ and which do not split completely in any element $\neq K$ of $L(\mathscr{F})$. For example, if $\mathscr{F} = \{K_q : q \text{ prime}\}$ and $K = Q$, this is Artin's conjecture.

In Sections 2 and 3, we solve this problem assuming the GRH for the zeta functions of the number fields of $\mathscr{F}$ and some restrictions on the growth of the discriminants of the fields of $\mathscr{F}$. Our theorem has some interesting applications which we give in sections 4 and 5. Lang and Trotter [13] formulated an analogue of Artin's conjecture for elliptic curves. If $E$ is an elliptic curve over $Q$ and $a$ is a rational point of infinite order, they asked for the density of those primes $p$ such that the group $E$ $(\mathbb{F}_p)$ of rational points $(\mathrm{mod}\, p)$ is cyclic and generated by the reduction of $a$ $(\mathrm{mod}\, p)$. This conjecture seems to be very difficult. Serre [18] answered the simpler question of how often $E(\mathbb{F}_p)$ is cyclic for a given elliptic curve $E$, by assuming the GRH. This is discussed in Section 5.

We then investigate, in Section 6, a method of eliminating the GRH from the above results. In one direction, we are able to show that if $E$ has complex multiplication, then the number of primes $p$ up to $x$ such that $E(\mathbb{F}_p)$ is cyclic is

$$\sim c_E(x/\log x) \quad \text{as} \quad x \to \infty.$$

The GRH is avoided by making use of sieve methods and Bombieri's theorem in algebraic number fields.

## 2. The Generalized Artin Problem

Let $\mathscr{F}$ be a family of algebraic number fields which are normal and of finite degree over a fixed number field $K$. Denote by $L(\mathscr{F})$ the lattice spanned by $\mathscr{F}$. That is, elements of $L(\mathscr{F})$ are joins of finite subsets of $\mathscr{F}$. Let $f(x, K)$ be the number of prime ideals $\mathfrak{P}$ of $K$ such that $N_{K/Q}(\mathfrak{P}) \leqslant x$ and $\mathfrak{P}$ does not split completely in any $H \in L(\mathscr{F})$ for $H \neq K$. We consider the problem of determining the asymptotic behaviour of $f(x, K)$ as $x \to \infty$.

This problem cannot be handled in this generality and we need to make some assumptions on $\mathscr{F}$. One of the first assumptions we need is the following: For each prime ideal $\mathfrak{P}$ of $K$, define

$$R(\mathfrak{P}) = \prod_{\substack{\mathfrak{P} \text{ splits} \\ \text{completely} \\ \text{in } H \in L(\mathscr{F})}} H.$$

We assume throughout that $R(\mathfrak{P}) \in L(\mathscr{F})$ for all prime ideals $\mathfrak{P}$.

Let $A$ and $B$ be algebraic number fields of finite degree over $K$. We know that a prime ideal $\mathfrak{P}$ splits completely in $A$ and $B$ if and ony if $\mathfrak{P}$ splits completely in $AB$. So we find that $\mathfrak{P}$ splits completely in $R(\mathfrak{P})$ and in no larger field in the lattice. Therefore, for $A \in L(\mathscr{F})$, let us define $f(x, A)$ to be the number of prime ideals $\mathfrak{P}$ in $O_K$ with $N_{K/Q}(\mathfrak{P}) \leqslant x$ and $R(\mathfrak{P}) = A$. This coincides with our previous definition if $A = K$.

Letting $\pi_1(x, A)$ be those prime ideals $\mathfrak{P}$ of $K$ such that $R(\mathfrak{P}) \supseteq A$ and $N_{K/Q}(\mathfrak{P}) \leqslant x$, we have

$$\pi_1(x, A) = \sum_{\substack{H \supseteq A \\ H \in L(\mathscr{F})}} f(x, H).$$

For fixed $x$, this sum is actually finite by our assumption and so we may apply Möbius inversion (see Rota [16]) on $L(\mathscr{F})$ to get

$$f(x, A) = \sum_{\substack{H \supseteq A \\ H \in L(\mathscr{F})}} \mu(A, H)\, \pi_1(x, H),$$

where $\mu$ is the Möbius function of $L(\mathscr{F})$. In particular, we get for $A = K$,

$$f(x, K) = \sum_{\substack{H \supseteq K \\ H \in L(\mathscr{F})}} \mu(K, H)\, \pi_1(x, H).$$

Hence, we have to study the behaviour of this sum as $x \to \infty$.

Goldstein [5], on the other hand, considered the following setting for $K = Q$. Let $S$ be a set of rational primes and for $q \in S$, let $L_q$ be a finite normal extension of $Q$. Let $S^*$ be the set of all squarefree numbers (including 1) composed of all the primes in $S$. For each $k \in S^*$, define $L_1 = Q$, and

$$L_k = \prod_{q \mid k} L_q, \qquad n(k) = [L_k : Q].$$

Then, Goldstein conjectured that

$$f(x, Q) \sim \delta(S)\, x/\log x$$

as $x \to \infty$, where

$$\delta(S) = \sum_{k \in S^*} \frac{\mu(k)}{n(k)}.$$

We now show that both of these settings are the same if $\sum 1/n(k) < \infty$. The transition is achieved by Rota's cross-cut theorem. Let us recall what this theorem says.

A *cross cut* of a finite lattice $L$ is a subset $C$ of $L$ satisfying

(i) subset $C$ does not contain the minimum $\hat{0}$ or the maximum $\hat{1}$ of $L$,

(ii) no two elements of $C$ are comparable;

(iii) any maximal chain stretched between $\hat{0}$ and $\hat{1}$ meets $C$. For any cross cut $C$, we have

$$\mu(\hat{0}, \hat{1}) = \sum_{r \geq 1} (-1)^r g_r,$$

where $g_r$ is the number of $r$-subsets of $C$ whose join equals the maximum.

We want to show

$$\sum_{H \in L(\mathscr{F})} \frac{\mu(Q, H)}{[H : Q]} = \sum_{k \in S^*} \frac{\mu(k)}{n(k)},$$

where $\mathscr{F} = \{L_q : q \in S\}$.

Suppose first that $L_q \leqslant L_{q'}$ for $q, q' \in S$, $q \neq q'$. Then,

$$\sum_{k \in S^*} \frac{\mu(k)}{n(k)} = \sum_{\substack{k \in S^* \\ q' \nmid k}} \frac{\mu(k)}{n(k)} + \sum_{\substack{k \in S^* \\ q' \mid k}} \frac{\mu(k)}{n(k)}.$$

The second sum is

$$\sum_{\substack{k \in S^* \\ q' \mid k, q \mid k}} \frac{\mu(k)}{n(k)} + \sum_{\substack{k \in S^* \\ q' \mid k, q \nmid k}} \frac{\mu(k)}{n(k)} = - \sum_{\substack{k \in S^* \\ q' \mid k, q \nmid k}} \frac{\mu(k)}{n(k)} + \sum_{\substack{k \in S^* \\ q' \mid k, q \nmid k}} \frac{\mu(k)}{n(k)} = 0.$$

Therefore,

$$\sum_{k \in S^*} \frac{\mu(k)}{n(k)} = \sum_{\substack{k \in S^* \\ q' \nmid k}} \frac{\mu(k)}{n(k)},$$

and so $L_{q'}$ can be removed from $\mathscr{F}$ without changing the sum. On the other hand, a theorem of Hall [8] tells us that $\mu(\hat{0}, \hat{1}) = 0$ unless $\hat{1}$ is the join of atoms in $L$. This means that

$$\sum_{H \in L(\mathscr{F})} \frac{\mu(Q, H)}{[H : Q]} = \sum_{H \in L(\mathscr{F}')} \frac{\mu(Q, H)}{[H : Q]},$$

where $\mathscr{F}'$ is the maximal set of atoms in $\mathscr{F}$. Therefore, without any loss of generality, we may assume that no two elements of $\mathscr{F}$ are comparable. Applying the cross-cut theorem to the interval $[Q, H]$, we have,

$$\sum_{H \in L(\mathscr{F})} \frac{1}{[H : Q]} \sum_{r \geqslant 1} \sum_{L_{q_1} \cdots L_{q_r} = H} (-1)^r$$

$$= \sum_{H \in L(\mathscr{F})} \frac{1}{[H : Q]} \sum_{\substack{L_k = H \\ k \in S^*}} \mu(k) = \sum_{k \in S^*} \frac{\mu(k)}{n(k)},$$

as desired.

Goldstein's formulation has the advantage of indexing the fields in a natural way. The former setting removes the arbitrariness of the index set and applies Möbius inversion directly.

In this generality, Goldstein's conjecture has been shown to be false by Weinberger [21] and Serre (independently).

## 3. Conditional Theorems

Let $S$ be the set of rational primes and for each $q \in S$, let $L_q/K$ be normal and of finite degree $n(q)$ over a fixed algebraic number field $K$. Define for each squarefree number $k$,

$$L_k = \prod_{q|k} L_q, \qquad d_k = \operatorname{disc}(L_k/Q).$$

Set $L_1 = K$ and $n(k) = [L_k : K]$. Denote by $f(x, K)$ the number of prime ideals $\mathfrak{P}$ of $K$ such that $N_{K/Q}(\mathfrak{P}) \leqslant x$ and $\mathfrak{P}$ does not split completely in any $L_q$, $q \in S$.

Theorem 1. *Suppose that*

$$\sum_{k=1}^{\infty} \frac{\mu^2(k)}{n(k)} < \infty$$

*and*

(i) *we have* $(1/n(k)) \log |d_k| = O(\log k)$,

(ii) *the number of prime ideals* $\mathfrak{P}$ *in* $K, N_{K/Q}(\mathfrak{P}) \leqslant x$, *which split completely in some* $L_q$, $q > x^{1/2}/\log^2 x$ *is* $o(x/\log x)$.

*Suppose further that the Riemann hypothesis is true for each of the Dedekind zeta functions* $\zeta(s, L_k/Q)$. *Then*

$$f(x, K) = \delta(S)\, x/\log x + o(x/\log x)$$

*as* $x \to \infty$, *where*

$$\delta(S) = \sum_{k=1}^{\infty} \frac{\mu(k)}{n(k)}.$$

*Proof.* From our previous considerations, we know that

$$f(x, K) = \sum_{k=1}^{\infty} \mu(k)\, \pi_1(x, L_k/K).$$

Define, as usual, $N(x, y)$ to be the number of prime ideals $\mathfrak{P}$, $N_{K/Q}(\mathfrak{P}) \leqslant x$, which do not split completely in any $L_q$ for $q \leqslant y$. Clearly,

$$N(x, y) = \sum{}' \mu(k)\, \pi_1(x, L_k/K),$$

where the dash on the sum indicates that all prime divisors of $k$ are $\leqslant y$, and $f(x, K) \leqslant N(x, y)$. Now define $M(x, \xi_1, \xi_2)$ to be the number of prime ideals

$\mathfrak{P}$ of $K$ with $N_{K/Q}(\mathfrak{P}) \leqslant x$ and $\mathfrak{P}$ splits completely in some $L_q$, $\xi_1 \leqslant q \leqslant \xi_2$. Clearly, if $g(x)$ is the largest index $m$ such that some $\mathfrak{P}, N_{K/Q}(\mathfrak{P}) \leqslant x$, splits completely in $L_m$, then

$$f(x, K) \geqslant N(x, y) - M(x, y, g(x)).$$

We first estimate $M(x, y, g(x))$. Let us write

$$\begin{aligned} M(x, y, g(x)) &\leqslant \sum \pi_1(x, L_q/K) + M(x, x^{1/2}/\log^2 x, g(x)) \\ &= \sum\nolimits_1 + M(x, x^{1/2}/\log^2 x, g(x)) \end{aligned}$$

(say), where in the first sum, $y < q < x^{1/2}/\log^2 x$. Assumption (ii) says that the second term is $o(x/\log x)$. To estimate the first sum, we apply GRH in the following form: We know from Lagarias–Odlyzko [11] that on this hypothesis,

$$\pi_1(x, L_k/K) = \frac{\operatorname{li} x}{n(k)} + O\left(\frac{x^{1/2}}{n(k)} \log |d_k|\, x^{n(k)}\right),$$

where $\operatorname{li} x$ is the usual logarithmic integral and the constants implied are absolute. Applying this, we get that the first sum is bounded by

$$\sum_{y<q<x^{1/2}/\log^2 x} \frac{\operatorname{li} x}{n(q)} + \sum_{y<q<x^{1/2}/\log^2 x} E(x, q),$$

where we have set for convenience

$$E(x, q) = \left| \frac{\operatorname{li} x}{n(q)} - \pi_1(x, L_q/K) \right|.$$

We now use (i) to get

$$\begin{aligned} \sum E(x, q) &\ll \sum x^{1/2}\left(\log x + \frac{\log |d_q|}{n(q)}\right) \\ &\ll \sum x^{1/2}(\log x + \log q), \end{aligned}$$

where all the sums are in the range $y < q < x^{1/2}/\log^2 x$. But now, elementary estimates (which go back to Tschebyscheff) suffice to give

$$\sum E(x, q) \ll \frac{x}{\log^2 x} = o(x/\log x).$$

Finally, using

$$\sum_{k=1}^{\infty} 1/n(k) < \infty,$$

we deduce,

$$\sum_{y<q<x^{1/2}/\log^2 x} \frac{\operatorname{li} x}{n(q)} = o(x/\log x),$$

provided $y = y(x) \to \infty$ as $x \to \infty$.

Therefore,

$$f(x, K) = N(x, y) + o(x/\log x).$$

Again using GRH, we have by (i)

$$N(x, y) = \sum{}' \mu(k) \left\{ \frac{\operatorname{li} x}{n(k)} + O\left( \frac{x^{1/2}}{n(k)} \log(|d_k|\, x^{n(k)}) \right) \right\},$$

$$= \sum{}' \mu(k) \left\{ \frac{\operatorname{li} x}{n(k)} + O(x^{1/2} \log kx) \right\},$$

where the dash on both sums indicates that all prime divisors of $k$ are $\leqslant y$. As there are at most $2^y$ squarefree numbers composed of primes $\leqslant y$, we see by elementary estimates that

$$N(x, y) = \left( \sum{}' \frac{\mu(k)}{n(k)} \right) \operatorname{li} x + O(x^{1/2} 2^y (y + \log x)).$$

Choosing $y(x)$ so that

$$2^{y(x)} \ll x^{1/2}/\log^3 x$$

and $y(x) \to \infty$, we find that $y(x) = O(\log x)$. Therefore,

$$y 2^y x^{1/2} \ll x/\log^2 x = o(x/\log x).$$

Hence, we deduce

$$f(x, K)/(x/\log x) \to \delta(S),$$

because $y(x) \to \infty$ as $x \to \infty$. This completes the proof of the theorem.

*Remark.* In order to verify condition (i) of the theorem, the following result of Hensel is quite useful (see Serre [17]):

If $E/Q$ is normal and ramified only at the primes $p_1,\dots, p_m$, then,

$$\frac{1}{n}\log|d_{E/Q}| \leqslant \log n + \sum_{j=1}^{m}\log p_j,$$

where $n = [E: Q]$. This result enables us to deduce

COROLLARY. *Suppose that* $\sum_{k=1}^{\infty} 1/n(k) < \infty$ *and* $D$ *is a finite set of primes such that*

(i) $p \mid d_q \Rightarrow p = q$ *or* $p \in D$.

*If in addition,* $n(k) = O(k^A)$ *for some* $A > 0$, *and* (ii) *is also satisfied, then*

$$f(x, K) = \delta(S)\, x/\log x + o(x/\log x).$$

*Proof.* We need only show that (i) of the theorem is satisfied:

$$\begin{aligned}\frac{1}{n(k)}\log|d_k| &\leqslant \log n(k) + \sum_{p\mid d_k}\log p\\ &\ll \log k + \sum_{p\mid k}\log p\\ &\ll \log k.\end{aligned}$$

We therefore see that $\delta(S)$ exists whenever the conditions of the theorem are satisfied. If $\delta(S) > 0$, then we get an infinitude of primes which do not split completely in any $L_q$, $q \in S$. If $\delta(S) = 0$, it may happen that there are still an infinitude of such primes. Such a situation is illustrated in the following example:

Let $p_1 = 3$, and define $p_j$ to be the smallest prime satisfying $p_j \not\equiv 1 \pmod{p_i}$ for $i < j$. This sequence of primes was first discussed by Golomb [7]. Erdös [3] showed that the number of $p_j$'s $\leqslant x$ is

$$\frac{(1 + o(1))\, x}{(\log x)(\log\log x)}.$$

Thus, the set of $p_j$'s has zero density in the set of primes. If we take

$$\mathscr{F} = \{Q(\zeta_{p_i}), i = 1, 2,\dots\},$$

then any prime $q$ not splitting completely in $Q(\zeta_{p_i})$ for all $i$ must satisfy $q \not\equiv 1 \pmod{p_i}$. For some $j$, we must have $p_j < q \leqslant p_{j+1}$. Then, by our definition of $p_{j+1}$, we get $q = p_{j+1}$. This shows that the set of primes not splitting completely in any $Q(\zeta_{p_i})$ is precisely the set of $p_j$'s.

## 4. First Applications

We now derive some interesting examples from Theorem 1.

A. *Artin's Conjecture on Primitive Roots* (Hooley [10])

Let $a$ be an integer $\neq 0, \pm 1$, or a perfect square. Let $\zeta_q$ be a primitive $q$th root of unity and $q$ a rational prime. Take for $S$ the set of all rational primes and $L_q = Q(\zeta_q, a^{1/q})$, $L_1 = Q$.

We check the conditions of the corollary in this case. It is easy to see that $p \mid d_q$ only if $p = q$ or $p \mid a$. This verifies (i). Moreover, $n(k) = O(k^2)$. To verify (ii), we write

$$\begin{aligned} M(x, x^{1/2}/\log^2 x, x-1) &= M(x, x^{1/2}/\log^2 x, x^{1/2} \log x) \\ &\quad + M(x, x^{1/2} \log x, x-1) \\ &= \Sigma_1 + \Sigma_2 \end{aligned}$$

(say). We observe that

$$\Sigma_1 \leqslant \sum \pi_1(x, L_q/Q),$$

where the summation is over those $q$ satisfying

$$x^{1/2}/\log^2 x < q < x^{1/2} \log x.$$

To estimate $\Sigma_1$, we notice that $Q(\zeta_q) \subseteq Q(\zeta_q, a^{1/q})$ so that

$$\pi_1(x, L_q/Q) \leqslant \pi(x, Q(\zeta_q)/Q).$$

By the Brun–Titchmarsh theorem, there is an absolute constant $A$ such that for $q < x$,

$$\pi(x, Q(\zeta_q)/Q) \leqslant Ax/(q-1)\log(x/q).$$

We deduce

$$\Sigma_1 \ll \frac{x}{\log x} \sum{}' \frac{1}{q},$$

where the dash on the summation indicates that $q$ is in the given range for $\Sigma_1$. But for this sum, we have in turn,

$$\begin{aligned} \Sigma_1 &\ll \frac{x}{\log^2 x} \sum{}' \frac{\log q}{q} \\ &\ll x \log\log x/\log^2 x = o(x/\log x). \end{aligned}$$

To deal with $\Sigma_2$, recall that a rational prime $p$ splits completely in $L_q$ if and only if $p \nmid a$, $p \equiv 1 \pmod q$, and $a^{(p-1)/q} \equiv 1 \pmod p$. As $q > x^{1/2} \log x$ and $p \leqslant x$, we have $(p-1)/q \leqslant x^{1/2}/\log x$. Thus, such a $p$ splits completely in some $L_q$, with $q > x^{1/2} \log x$, only when it divides

$$R = \prod_{m < x^{1/2}/\log x} (a^m - 1).$$

Therefore, $\Sigma_2$ is bounded by the number of prime factors of $R$, which is trivially $O(\log R)$. But,

$$\log R \leqslant \sum_{m < x^{1/2}/\log x} m \log a \ll x/\log^2 x.$$

Therefore, $\Sigma_2 = o(x/\log x)$ and we deduce that $N_a(x)$, the number of primes $\leqslant x$ for which $a$ is a primitive root, is $\sim \delta(S)\, x/\log x$.

B. *Abelian Extensions*

If, for $q$ sufficiently large, the extensions $L_q/Q$ are Abelian, then it is possible to solve the Artin problem in certain cases. Suppose that

(a) $L_q/Q$ are abelian for $q \geqslant t$,

(b) $\sum_{q > y} (x + f_q)/n(q) = o(1/\log y)$, as $y \to \infty$. (Here, $f_q$ denotes the conductor of $L_q/Q$ for $q \geqslant t$.)

(c) $(1/n(k)) \log |d_k| = O(\log k)$.

Then, the set of primes which do not split completely in any $L_q$ has a Dirichlet density.

This result follows by applying the reciprocity law to show that (ii) of the theorem is true. We know that $p$ splits completely in $L_q$ if and only if there are residue classes $a_1, \ldots, a_t$ mod $(f_q)$ (where $f_q$ is the conductor of $L_q/Q$) such that $p \equiv a_i \pmod{f_q}$ for some $i$. Now, $t/\phi(f_q) = 1/n(q)$, and so

$$\pi_1(x, L_q/Q) \leqslant (x + f_q)/n(q),$$

giving us that

$$\sum_{q > x^{1/2}/\log^2 x} \pi_1(x, L_q/Q) = o(x/\log x)$$

as desired.

An erroneous version of the above was proved in [5].

## 5. Application to Elliptic Curves

Let $E$ be an elliptic curve over $Q$. We want to determine the number of primes $p \leqslant x$, at which $E$ has good reduction and such that $E(\mathbb{F}_p)$, the group of points (mod $p$), is cyclic.

Let us recall some facts about elliptic curves. First consider an elliptic curve $\bar{E}$ over $\bar{\mathbb{F}}_p$, algebraic closure of the finite field of $p$ elements. For any prime $q$, let

$$\bar{E}_q = \ker(\bar{E} \xrightarrow{q} \bar{E}),$$

where $q(x) = q \cdot x$. It is known that $\bar{E}_q \simeq (\mathbb{Z}/q\mathbb{Z})^2$ if $p \neq q$ and if $p = q$, $\bar{E}_q$ is isomorphic to a subgroup of $(\mathbb{Z}/p\mathbb{Z})$.

Now, let $E$ be an elliptic curve over $Q$ and $E_q$ be the $q$-division points of $E$. That is,

$$E_q = \ker(E \xrightarrow{q} E),$$

where the map is multiplication by $q$. Set $L_q = Q(E_q)$. Clearly, $L_q$ is normal over $Q$. It is known that $L_q$ is ramified only at $q$ and those primes dividing the conductor of $E$. We shall also use fact that $L_q \supseteq Q(\zeta_q)$.

Lemma 1. *Let $G$ be a finite Abelian group. Then $G$ is cyclic if and only if $G$ does not contain a $(q, q)$ group for any prime $q$.*

*Proof.* This result is clear.

Corollary. *If $E$ is an elliptic curve over $\mathbb{F}_p$, then $E(\mathbb{F}_p)$ is cyclic if and only if it does not contain a subgroup of type $(q, q)$, $q \neq p$.*

Lemma 2. *Let $p$ be a prime $\neq q$. Suppose $E$ has good reduction at $p$. Then $p$ splits completely in $L_q$ if and only if $E(\mathbb{F}_p)$ contains a $(q, q)$ group.*

*Proof.* We look at the reduced curve $\bar{E}$ over $\mathbb{F}_p$. Let $\pi_p$ be the endomorphism of $\bar{\mathbb{F}}_p$ given by $\pi_p(x) = x^p$. Then,

$$\pi_p : \bar{E} \to \bar{E}$$

is a homomorphism and $\ker(\pi_p - 1) = E(\mathbb{F}_p)$. Hence, $E(\mathbb{F}_p)$ contains a $(q, q)$ group if and only if $\pi_p$ acts trivially on $\bar{E}_q$. Hence, the decomposition group of any prime lying above $p$ is trivial if and only if $E(\mathbb{F}_p)$ contains a $(q, q)$ group. This gives the result.

Corollary. *A prime $p$ does not split completely in any $L_q$ if and only if $E(\mathbb{F}_p)$ is cyclic.*

Thus, we see that the Artin problem for the family $\mathscr{F} = \{L_q : q \text{ prime}\}$ determines the number of $p \leqslant x$, such that $E(\mathbb{F}_p)$ is cyclic. We now apply the corollary to Theorem 1 and deduce

THEOREM 2 (Serre). *Subject to the GRH, we have for any elliptic curve $E$ over $Q$,*

$$\lim_{x\to\infty} \frac{f(x, Q)}{x/\log x} = c_E,$$

*where* $f(x, Q) =$ number of $p \leqslant x$, *such that* $E(\mathbb{F}_p)$ *is cyclic.*

*Remark.* Serre has shown that the constant $c_E$ is nonzero whenever $E$ has an irrational point of order 2. If all the 2-division points are rational, then clearly $E(\mathbb{F}_p)$ is not cyclic for all primes sufficiently large.

*Proof.* It is known that there is a finite set of primes $S$ such that if $k$ is not divisible by any of the primes in $S$, then $n(k) \geqslant k^{3/2}$. In case $E$ has complex multiplication, this follows from classical results. If $E$ does not have complex multiplication, the result follows from Serre [19], who showed that $\mathrm{Gal}(L_k/Q) \simeq GL_2(\mathbb{Z}/k\mathbb{Z})$ whenever $k$ is coprime to a certain finite set of primes. In either case, we have $\sum \mu^2(k)/n(k) < \infty$.

Since $L_q$ is unramified over $Q$ except for $q$ and a finite number of primes dividing the discriminant of $E$, we see that (i) of Theorem 1 is satisfied by Hensel. If $p \leqslant x$ and $p$ splits completely in $L_q$, then $E(\mathbb{F}_p)$ contains a $(q, q)$ group and so $q^2 \mid (p + 1 - a_p)$. Therefore, $q \leqslant 2\sqrt{x}$. We need to estimate

$$\sum_{\sqrt{x}/\log^2 x < q < 2\sqrt{x}} \pi_1(x, L_q/Q).$$

Since $L_q \supseteq Q(\zeta_q)$, we use the Brun–Titchmarsh theorem and get that the above sum is

$$\ll \sum_{\sqrt{x}/\log^2 x < q < 2\sqrt{x}} \frac{x}{q \log(x/q)} \ll \frac{x}{\log x} \sum{}' \frac{1}{q},$$

where the dash on the summation indicates the range $x^{1/2}/\log^2 x < q < 2x^{1/2}$. This last sum can be estimated easily, using

$$\sum_{p<x} \frac{1}{p} = \log\log x + B + O\left(\frac{1}{\log x}\right).$$

We get

$$\sum{}' \frac{1}{q} = O\left(\frac{\log\log x}{\log x}\right).$$

Therefore,

$$\sum{}' \pi_1(x, L_q/Q) = o(x/\log x)$$

as desired. This completes the proof.

## 6. Unconditional Theorems

Let $E$ be an elliptic curve over $Q$ with complex multiplication by an order in an imaginary quadratic field $k$. Then, one can show that

$$\operatorname{card}(p \leqslant x: E(\mathbb{F}_p) \text{ is cyclic}) \sim c_E(x/\log x)$$

as $x \to \infty$, without any hypothesis. Bombieri's theorem in algebraic number fields allows us to remove the presence of GRH in our previous theorem.

Suppose $K$ is an algebraic number field and $\mathfrak{q}$ is an ideal of $O_K$. The residue classes of integers coprime to $\mathfrak{q}$ form a group under multiplication, the order of which is denoted $\phi(\mathfrak{q})$. Two ideals of $K$, $\mathfrak{a}$ and $\mathfrak{b}$, are said to be equivalent (mod $\mathfrak{q}$ and $\mathfrak{a}\mathfrak{b}^{-1} = (\alpha/\beta)$ with $\alpha \equiv \beta$ (mod* $\mathfrak{q}$), $(\alpha, \beta \in O_K)$, where this last condition means that $(\alpha - \beta) \in \mathfrak{q}$ and all the real conjugates (if any) of $\alpha/\beta$ are positive. This defines an equivalence relation and the number of equivalence classes is denoted $h(\mathfrak{q})$. The equivalence classes form an Abelian group under multiplication called the $\mathfrak{q}$-*ideal class group*. It has order

$$h(\mathfrak{q}) = h2^{r_1}\phi(\mathfrak{q})/T(\mathfrak{q}),$$

$h$ is the class number of $K$, $r_1$ is the number of real embeddings of $K$, and $T(\mathfrak{q})$ is the number of residue classes (mod* $\mathfrak{q}$) containing a unit.

The *ray class field* belonging to an ideal $\mathfrak{q}$ is the Abelian extension $L$ of $K$ such that the set of prime ideals of $K$ which split completely in $L$ are precisely those prime ideals lying in the unit class of the $\mathfrak{q}$-ideal class group; that is, those prime ideals which are principal, generated by an element $\alpha \equiv 1$ (mod* $\mathfrak{q}$).

We can now state Bombieri's theorem in algebraic number fields. Set

$$\psi(z, \mathfrak{q}, \mathfrak{a}) = \sum_{\substack{\mathfrak{P} \sim \mathfrak{a}(\mathfrak{q}) \\ N_{K/Q}(\mathfrak{p}) < z}} \log N_{K/Q}(\mathfrak{P}).$$

Lemma 3 (Wilson [22]). *For each positive constant $A$, there is a $B = B(A)$, such that if $Q = x^{1/(n+1)} \log^{-B} x$, $n = [K: Q]$, then for $x \geqslant 1$,*

$$\sum_{N_{K/Q}(\mathfrak{q}) < Q} \max_{z < x} \max_{\substack{\mathfrak{a}(\mathfrak{q}) \\ (\mathfrak{a}, \mathfrak{q}) = 1}} \frac{1}{T(\mathfrak{q})} \left| \psi(z, \mathfrak{q}, \mathfrak{a}) - \frac{z}{h(\mathfrak{q})} \right| \ll \frac{x}{\log^A x}.$$

Since $T(\mathfrak{q}) \gg 1$ for an imaginary quadratic field, we see that for such a field $K$,

$$\sum_{N_{K/Q}(\mathfrak{q}) < Q} \max_{z < x} \max_{(\mathfrak{a}, \mathfrak{q}) = 1} \left| \psi(z, \mathfrak{q}, \mathfrak{a}) - \frac{z}{h(\mathfrak{q})} \right| \ll x \log^{-A} x.$$

We shall be applying this result when $K$ is an imaginary quadratic field. Therefore $r_1 = 0$ above.

Given any elliptic curve $E$ over an algebraic number field, consider the group of endomorphisms of $E$, denoted End($E$). The addition law on $E$ gives that $\mathrm{End}(E) \supseteq \mathbb{Z}$ because each of the maps $\varphi_n(x) = nx$, $x \in E$, is an endomorphism. If $\mathrm{End}(E) \neq \mathbb{Z}$, one says that $E$ has *complex multiplication.* In this case, it is known that End($E$) must be an order in an imaginary quadratic field $k$. (An *order* is a free $\mathbb{Z}$ module of rank $[k: Q] = 2$ containing $\mathbb{Z}$.) All orders $\mathcal{O}$ of $k$ are of the form $\mathcal{O} = \mathbb{Z} + cO_k$, where $c$ is the *conductor* of $\mathcal{O}$.

Now let $E$ be an elliptic curve over $Q$ which has complex multiplication by an order of an imaginary quadratic field $k$. If $m$ is a natural number, let $E_m$ be the $m$-division points of $E$. Define $L_m = k(E_m)$. Then it is known that $L_m/k$ contains the ray class field $k_m$ of $k$ corresponding to the ideal $mO_k$. (See Lang [12, p. 216].)

LEMMA 4. *Let $E$ be an elliptic curve over $Q$ with complex multiplication by an order $\mathcal{O}$ in $k$. There is an ideal $\mathfrak{f}$ depending only on $E$ such that*

$$k_m \subseteq L_m \subseteq k_{\mathfrak{f}m},$$

*where $k_m$ and $k_{\mathfrak{f}m}$ are the ray class fields of $k$ of levels $m$ and $\mathfrak{f}m$, respectively.*

*Proof.* As $E$ has complex multiplication, $L_m/k$ is Abelian and hence is contained in a ray class field. By class field theory, it suffices to determine the subgroup $H$ of the ideal class group $k_A^\times$ such that $L_m$ is class field to $H$. That is, we determine the subgroup of $k_A^\times$ which fixes $L_m$. Let $\varphi: k_A^\times \to k$ be the homomorphism such that $\varphi(x)/x_\infty$ is the grössencharacter of $E$. Then, we know

$$\varphi(s)\, s^{-1}\mathcal{O} = \mathcal{O}.$$

The main theorem of complex multiplication (see Shimura [20, p. 211]) gives that $s \in k_A^\times$ fixes $L_m$ if and only if

$$\xi(\varphi(s)\, s^{-1}t) = \xi(t) \qquad \text{for all } t \in (1/m)\,\mathcal{O},$$

where $\xi$ is an isomorphism of $C/\mathcal{O}$ to $E$. Hence, as $\varphi(x) = x$ for all $x \in k$, we deduce that

$$\varphi(s)\, s^{-1} \in U_\varphi \cap U_{\mathcal{O}} \cap U_{m\mathcal{O}},$$

where

$$U_\varphi = \ker \varphi,$$
$$U_{\mathcal{O}} = \{s \in k_A^x : s\mathcal{O} = \mathcal{O}\},$$
$$U_{m\mathcal{O}} = \{s \in k_A^x : s \equiv 1 \ (\mathrm{mod}\ m\mathcal{O})\}.$$

Thus, $s \in k^x(U_\varphi \cap U_{\mathcal{O}} \cap U_{m\mathcal{O}})$. Conversely, if $s = \alpha r$, $\alpha \in k$, $r \in U_\varphi \cap U_{\mathcal{O}} \cap U_{m\mathcal{O}}$, then

$$\varphi(s) = \varphi(\alpha)\, \varphi(r) = \alpha,$$

and so $\varphi(s)\, s^{-1}\mathcal{O} = \mathcal{O}$, $\varphi(s)\, s^{-1} \in \ker \varphi$, and $s$ fixes $L_m$. We conclude that $L_m$ is class field to

$$H = k^x(U_\varphi \cap U\mathcal{O} \cap U_{m\mathcal{O}}).$$

But then, if $\mathfrak{f}_\varphi =$ conductor of $\varphi$ and $c$ is the conductor of $\mathcal{O}$ and we set $\mathfrak{f} = \mathrm{lcm}(\mathfrak{f}_\varphi, c)$, then we see that

$$k^x U_{m\mathcal{O}_k} \supseteq H \supseteq k^x U\mathfrak{f}_{m\mathcal{O}_k}$$

so that

$$k_m \subseteq L_m \subseteq k_{\mathfrak{f}m}$$

as desired.

This lemma allows us to deduce that if $\mathfrak{P}$ is a prime ideal of $O_k$ which splits completely in $L_m$, then $\mathfrak{P} \sim \mathfrak{a}_1$, or $\mathfrak{a}_2, \ldots$, or $\mathfrak{a}_t$ (mod $\mathfrak{f}mO_k$), with $t$ bounded because $[k_{\mathfrak{f}m} : L_m]$ is bounded.

LEMMA 5. *The number of* $\alpha \in O_k$, *with* $N_{k/Q}(\alpha) \leqslant x$, *and* $\alpha \equiv 1$ (mod $mO_k$) *is* $O(x/m^2)$.

*Proof.* Let 1, $\lambda$ be an integral basis of $O_k$. Then $\alpha = a + b\lambda$ for some $a, b \in \mathbb{Z}$. Therefore, $a - 1 = mc$, $b = md$ for some $c, d \in \mathbb{Z}$. If $k = Q(\sqrt{-D})$, we have either $a^2 + Db^2 \leqslant x$, or $(a + b/2)^2 + b^2D/4 \leqslant x$. In either case, $a = O(x^{1/2})$ and $b = O(x^{1/2})$. Since $m \mid b$, and $m \mid (a - 1)$, we get a total of $O(x/m^2)$ possibilities for $\alpha$.

We now find an asymptotic formula for a weighted sum over the prime ideals $\mathfrak{P}$ of $O_k$ such that $N_{k/Q}(\mathfrak{P}) \leqslant x$, and $\mathfrak{P}$ does not split completely in $L_q$ for all primes $q$. Set

$$\phi(x, L_m/k) = \sum_{i=1}^{t} \psi(x, \mathfrak{f}mO_k, \mathfrak{a}_i).$$

We estimate

$$T(x) = \sum_{m=1}^{\infty} \mu(m)\, \phi(x, L_m/k).$$

Let us write

$$\begin{aligned} T(x) &= \sum_{m < x^{1/6}/\log^{B/2} x} + \sum_{m > x^{1/6}/\log^{B/2} x} \\ &= \Sigma_1 + \Sigma_2 \end{aligned}$$

(say), where the constant $B$ is soon to be specified.
By Lemma 4,

$$\begin{aligned} \Sigma_2 &\ll \sum_{m > x^{1/6}/\log^{B/2} x} \phi(x, L_m/k) \\ &\ll (\log x) \sum_{m > x^{1/6}/\log^{B/2} x} x/m^2 \\ &\ll x^{5/6} (\log x)^{1+B/2}. \end{aligned}$$

In order to estimate $\Sigma_1$, we make use of Lemma 3 with $K = k$, $Q = x^{1/3} \log^{-B(A)} x$. We note that $[L_m : k] \ll h((m))$ and write

$$\Sigma_1 = \sum{}' \mu(m) \frac{x}{[L_m : k]} + \sum{}' \mu(m) \left\{ \phi(x, L_m) - \frac{x}{[L_m : k]} \right\},$$

where the dash on the summation indicates that $m < x^{1/6}/\log^{B/2} x$. On the last sum, we have to estimate

$$\sum \left| \phi(x, L_m/k) - \frac{x}{[L_m : k]} \right|.$$

If $m$ is in the specified range, then $N_{k/Q}(mO_k) \leqslant x^{1/3}/\log^B x$. Lemma 3 implies that this sum is

$$O(x/\log^A x).$$

If we choose $A=2$, then $B=B(A)$ is given by Lemma 3 and is now specified. Finally,

$$T(x)=\sum{}' \mu(m)\frac{x}{[L_m:k]}+O(x\log^{-A} x)$$

and since

$$\sum_{m>x^{1/6}/\log^{B/2}x}[L_m:k]^{-1}\ll\sum_{m>x^{1/6}/\log^{B/2}x}m^{-3/2}$$
$$=O(x^{-1/12}\log^{B/4}x),$$

we get

$$T(x)=x\sum_{m=1}^{\infty}\mu(m)[L_m:k]^{-1}+O(x\log^{-A} x)$$

for any $A>0$. Since the number of prime ideals $\mathfrak{P}$ of $k$ with degree $\geqslant 2$ and $N_{K/Q}(\mathfrak{P})\leqslant x$ is $O(x^{1/2})$, we deduce that $T(x)$ enumerates those prime ideals, with a weight of $\log N_{k/Q}(\mathfrak{P})$, which do not split completely in any $L_q$.

This settles the question over $k$. To "come down to $Q$," we need to make use of

LEMMA 6. *If $m>2$, then $k(E_m)=Q(E_m)$.*

*Proof.* If we can show $k\subseteq Q(E_m)$, then we are done. Let $\tau\in \mathrm{Gal}(\bar{Q}/Q)$; fix $Q(E_m)$. Let $k$ be identified with its normalized embedding in $\mathrm{End}_C(E)$ as in Shimura [20, p. 113]. Then, we show that $\tau$ fixes $k$ if $m$ is greater than 2, so that the result would follow by Galois theory. Suppose not. Then $\tau$ restricted to $k$ is complex conjugation. Let $\varphi_\lambda\in\mathrm{End}(E)$ be given by $\varphi_\lambda(x)=\lambda x$. For $x\in E_m$, we have $\varphi_\lambda(x)\in E_m$ so that

$$\tau(\varphi_\lambda(x))=\varphi_\lambda(x)=\lambda x.$$

On the other hand,

$$\tau(\varphi_\lambda(x))=\tau(\lambda x)=\tau(\lambda)\,\tau(x)=\bar{\lambda}x.$$

Therefore, $(\bar{\lambda}-\lambda)\,x=0$ for all $x\in E_m$. Hence,

$$2\,\mathrm{Im}(\lambda)\equiv 0 \qquad (\mathrm{mod}\ m\mathcal{O})$$

for all $\lambda\in\mathcal{O}$. In particular, $2\sqrt{-D}=mb\sqrt{-D}$ or $\sqrt{-D}=mb\sqrt{-D}/2$, so that $mb=2$ and therefore $m\mid 2$. This completes the proof.

This lemma shows that $Q_m = L_m$ for $m$ squarefree and $>2$. The sum

$$T_0(x) = \sum_{\substack{p \text{ does not} \\ \text{split completely} \\ \text{in any } Q_m/Q,\, p \leq x.}} \log p$$

can be written as

$$T_0(x) = \sum_{m=1}^{\infty} \mu(m)\, \phi_0(x, Q_m/Q),$$

where

$$\phi_0(x, Q_m/Q) = \sum_{\substack{p \text{ splits comp} \\ \text{in } Q_m,\, p \leq x}} \log p.$$

Now, $T(x)/2$ is the number of primes $\leqslant x$, weighted by $\log p$, which split completely in $k$ but not in any $L_m/Q$. Taking into account the primes which do not split in $k$, we find by using the prime number theorem for $k/Q$, that for any $A > 0$,

$$x/2 + T(x)/2 + O(x \log^{-A} x)$$

is the weighted enumeration of primes $\leqslant x$ not splitting completely in any $L_m/Q$. For $m > 2$, $L_m = Q_m$ and so

$$\begin{aligned} T_0(x) &\geqslant x/2 + T(x)/2 + \phi_0(x, L_2/Q) + \phi_0(x, Q_2/Q) + O(x \log^{-A} x) \\ &= \sum_{m=1}^{\infty} \mu(m) \frac{x}{[Q_m : Q]} + O(x \log^{-A} x), \end{aligned}$$

for any $A > 0$, by our previous calculation. Since we always have

$$\lim_{x \to \infty} T_0(x)/x \leqslant \sum_{m=1}^{\infty} \mu(m) [Q_m : Q]^{-1},$$

we deduce the asymptotic formula for $T_0(x)$.

We must relate this to $f(x, Q)$. We have

$$(\log x^{1-\delta}) \sum_{x^{1-\delta} < p < x}' 1 \leqslant \sum_{x^{1-\delta} < p < x}' \log p = T_0(x) - T_0(x^{1-\delta}),$$

where $\delta > 0$ and the dash on the summation means that we sum over those $p$ for which $E(\mathbb{F}_p)$ is cyclic.

The above shows that

$$\frac{T_0(x)}{\log x} \leqslant f(x, Q) \leqslant \frac{T_0(x) - T_0(x^{1-\delta})}{(1-\delta)\log x}$$

Choosing $\delta = 2 \log\log x/\log x$ gives

THEOREM 3. *For any elliptic curve E over Q with complex multiplication, we have*

$$\lim_{x\to\infty} \frac{f(x, Q)}{x/\log x} = \sum_{m=1}^{\infty} \mu(m)[Q_m : Q]^{-1}.$$

## ACKNOWLEDGMENTS

I would like to thank Bob Rumely and Professor H. M. Stark for their help and useful discussions.

## REFERENCES

1. E. ARTIN, "The Collected Papers of Emil Artin" (S. Lang and J. Tate, Eds.), Addison-Wesley, Reading, Mass., 1965; *Math. Rev.* **31**, #1159.
2. H. BILHARZ, Primdivisoren mit vorgegebener Primitivwurzel, *Math. Ann.* **114** (1937), 476–492.
3. P. ERDŐS, On a problem of Golomb, *J. Austral. Math. Soc.* **2** (1961), 1–8.
4. C. F. GAUSS, "Disquisitiones Arithmeticae," Yale Univ. Press, New Haven, Conn./London, 1966.
5. L. J. GOLDSTEIN, Some remarks on arithmetic density questions, *in* "Proceedings, Symposium in Pure Mathematics," St. Louis, Mo., Amer. Math. Soc., Providence, R. I., 1972.
6. L. J. GOLDSTEIN, Analogues of Artin's conjecture, *Trans. Amer. Math. Soc.* **149** (1970), 431–442.
7. S. GOLOMB, Sets of primes with intermediate density, *Math. Scand.* **3** (1956), 264–274.
8. P. HALL, The Eulerian functions of a group, *Quart. J. Math. Oxford Ser.* (2) (1936), 134–151.
9. H. HEILBRONN. See A. WESTERN AND J. MILLER, Tables of indices and primitive roots, *in* "Royal Society Mathematical Tables," Vol. 9, p. xxxviii, Cambridge, 1968.
10. C. HOOLEY, On Artin's conjecture, *J. Reine Angew. Math.* **225** (1967), 209–220.
11. J. LAGARIAS AND A. ODLYZKO, Effective versions of the Tchebotarev density theorem, *in* "Algebraic Number Fields" (A. Fröhlich, Ed.), Proceedings of the 1975 Durham Symposium, Academic Press, London/New York, 1977.
12. S. LANG, "Elliptic Functions," Addison-Wesley, Reading, Mass., 1973.
13. S. LANG AND H. TROTTER, Primitive points on elliptic curves, *Bull. Amer. Math. Soc.* **83** (1977), 289–291.

14. D. H. LEHMER AND E. LEHMER, Heuristics anyone?, *in* "Studies in Mathematical Analysis and Related Topics" (G. Szego *et al.*, Eds.), Stanford Univ. Press, Stanford, Calif., 1962.
15. H. W. LENSTRA, JR., On Artin's conjecture and Euclid's algorithm in gobal fields, *Invent. Math.* 42 (1977), 201–224.
16. G. C. ROTA, On the foundations of combinatorial theory, I. Theory of Möbius functions, *Z. Wahrsch. Verw. Gebiete* 2 (1964), 340–368.
17. J. P. SERRE, "Local Fields," Springer-Verlag, Berlin/New York, 1979.
18. J. P. SERRE, "Résumé des cours de l'année scolaire," 1977–78, Collège de France, Paris, 1979.
19. J. P. SERRE, Propriétés galoisiennes des points d'ordre fini des courbes élliptiques, *Invent. Math.* 15 (1972), 259–331.
20. G. SHIMURA, "Introduction to the Arithmetic Theory of Automorphic Functions," Iwanami Shoten, Tokyo, 1971.
21. P. J. WEINBERGER, A counterexample to an analogue of Artin's conjecture, *Proc. Amer. Math. Soc.* 35 (1972), 49–52.
22. R. J. WILSON, The large sieve in algebraic number fields, *Mathematika* 16 (1969), 189–204.

Printed by the St. Catherine Press Ltd., Tempelhof 41, Bruges, Belgium