TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 149, June 1970

ANALOGUES OF ARTIN'S CONJECTURE

BY
LARRY JOEL GOLDSTEIN(1)

Abstract. Based on heuristic, a general conjecture is made, which contains Artin's primitive root conjecture as a special case. Special cases of the general conjecture are verified using the generalized Siegel-Walfisz theorem. It is shown that the general conjecture can be considered as an infinite-dimensional analogue of the Tchebotarev density theorem.

1. **Introduction.** In 1927, Artin conjectured that the set A of rational primes p for which a given rational integer a is a primitive root has a Dirichlet density $A(a)$. It is easily seen that if $a=\pm 1$ or $=$a square, then this density exists and has the value zero. Artin conjectured that for all other a, the density has a strictly positive value. It is known (Hasse [5], Hooley [6]), that a is a primitive root modulo p if and only if p does not split completely in each of the extensions

$$L_q = Q(\zeta_q, a^{1/q}),$$

where q is a rational prime and ζ_q is a primitive qth root of unity. If k is a positive, square-free integer, and if we set $L_k=Q(\zeta_k, a^{1/k})$, $n(k)=\deg(L_k/Q)$, then the quantitative part of Artin's conjecture (Hooley [6]) states that

$$A(a) = \sum_k \mu(k)/n(k) \tag{1.1}$$

where μ denotes the Möbius function and the sum runs over all integers, $n(1)$ being equal to 1.

Recently, Hooley [6] has shown that Artin's conjecture would follow if one assumes the Riemann hypothesis for the Dedekind zeta function of each of the fields L_k. In fact, the Riemann hypothesis implies the existence of the corresponding natural density. Hooley's proof is accomplished by showing that the Riemann hypothesis implies a "uniform prime number theorem"—that is, a formula for the number of prime ideals of norm at most x in L_k such that the error term in the formula is small and the dependence of the error on k is explicit.

Received by the editors December 11, 1968 and, in revised form, September 6, 1969.

AMS Subject Classifications. Primary 1250; Secondary 1041.

Key Words and Phrases. Number field, zeta function, Riemann hypothesis, primitive root, density of primes, Tchebotarev's theorem, locally compact group, Haar measure, equidistribution.

(1) Research partially supported by Air Force Office of Scientific Research Grant No. Sar/F- 44620-67.

The same heuristics which lead to Artin's conjecture suggest the following:

CONJECTURE. Let S be a set of rational primes. For each $q \in S$, let L_q be an algebraic number field. Let k denote either 1 or a positive, square-free integer. For $k>1$, define L_k to be the composite of all L_q for $q|k$; set $L_1=Q$. Denote $n(k)=\deg(L_k/Q)$, and assume that $\sum(1/n(k))$ converges, where the sum is over all those k for which $n(k)$ is defined. Then the natural density of the set $\mathscr{A}$ of primes p which do not split completely in each L_q exists and has the value $\sum_k \mu(k)/n(k)$.

If S is a finite set, then the conjecture is easily established using the prime ideal theorem. If $S=\{\text{all rational primes}\}$ and $L_q=Q(\zeta_q, a^{1/q})$, $a \in Z$, then the conjecture is equivalent to Artin's conjecture. If $S=\{\text{all rational primes}\}$ and $L_q=Q(\zeta_{q^r})$, $r \geqq 2$, then the conjecture has been proved by Knobloch [7] (only for Dirichlet densities and for $r=2$) and by Mirsky [8].

In the present paper, we will prove certain special cases of the above conjecture. Although we cannot prove the Artin conjecture, we will be able to treat the case $L_q=Q(\zeta_{q^2}, a^{1/q})$, $a \in Z$. Our main theorem can be interpreted as a Tchebotarev-type density theorem for certain infinite, normal extensions of Q.

The author owes a great debt to many people who have inspired and given helpful advice during the preparation of this paper. Especially, he would like to thank Dr. Oscar Goldman, in whose course on algebraic number theory the author first learned of Artin's conjecture. Thanks also go to Drs. Tamagawa, Schacher, Randol, and Steinberg, who patiently attended my seminar at Yale University and listened to the paper in a nascent state.

Some of our results were announced in [3].

2. **Statement of results.** Let S be a set of rational primes. For $q \in S$, let L_q be a finite, normal, algebraic number field. Throughout, let k be either 1 or a positive, square-free integer, divisible only by primes in S. For $k>1$, let $L_k=$the composite of all L_q for which $q|k$; let $L_1=Q$. Let $G_k=$the Galois group of L_k/Q, $n(k)=\deg(L_k/Q)$. Let

$$\mathscr{A} = \mathscr{A}(\{L_q\}, S) = \{p \text{ a rational prime} \mid p \text{ does not split completely in } L_q,\ q \in S\}.$$

We will prove

THEOREM 1. *Assume that $L_q \supset Q(\zeta_{q^2})$ for almost all q. Then $\mathscr{A}$ has a natural density $d(\mathscr{A})$, given by*

$$d(\mathscr{A}) = \sum_k \frac{\mu(k)}{n(k)}.$$

Therefore, the conjecture is true if $L_q \supset Q(\zeta_{q^2})$ for almost all q, and L_q/Q is normal for all q.

THEOREM 2. *Let $S=\{\text{all rational primes}\}$, $L_q=Q(\zeta_{q^2}, a^{1/q})$, $a \in Z$. Then $d(\mathscr{A}) \neq 0$, if $a \neq$ a square.*

The situation of Artin's conjecture is an example where $L_q \not\supset Q(\zeta_{q^2})$ for almost all q. However, by assuming the Riemann hypothesis for the Dedekind zeta functions of the fields L_k, one can prove a generalization of Hooley's theorem, namely

THEOREM 3. *Assume the Riemann hypothesis for the Dedekind zeta function of L_k. Then the conjecture is true if $L_q \supset Q(\zeta_q, a^{1/q})$, $a \in Z$, for almost all q.*

Let $\pi(x, \mathscr{A}) =$ the number of $p \in \mathscr{A}$ such that $p \leqq x$. Then we will prove

THEOREM 4. *Let the family of algebraic number fields $\{L_q\}$ be as above. Then*

$$\limsup_{x \to \infty} \frac{\pi(x, \mathscr{A})}{x/\log x} \leqq \sum_k \frac{\mu(k)}{n(k)}.$$

The fundamental tool in the proof of these theorems is our generalization of the Siegel-Walfisz theorem [4, Main Theorem], hereafter referred to as [SW]:

THEOREM [SW]. *Let L be an algebraic number field, $\pi(x, L) =$ the number of primes φ of L such that $N\varphi \leqq x$, and let $\varepsilon > 0$. Then there exist constants $b = b(\varepsilon)$, $c = c(\varepsilon)$, not depending on L, such that*

$$|\pi(x, L) - li(x)| \leqq Dx \log^2 x \exp\{-bn(\log x)^{1/2}/D\},$$

where

$$li(x) = \int_2^x \frac{dy}{\log y}, \qquad n = \deg(L/Q),$$

$$d = \text{the discriminant of } L/Q, \qquad D = n^3 |d|^{\varepsilon} c^n.$$

3. **Proofs of Theorems 1 and 3.** This section will be mainly devoted to proving Theorem 1. The proof of Theorem 3 is similar, so that we will only indicate the role that the extended Riemann hypothesis plays in the proof of Theorem 3.

Our object, then, is to show that if $L_q \supset Q(\zeta_{q^2})$ for almost all q, then

$$\pi(x, \mathscr{A}) = d(\mathscr{A}) li(x) + o(x/\log x), \qquad x \to \infty,$$

where $d(\mathscr{A}) = \sum_k (\mu(k)/n(k))$. If $L_q = Q$ for some q, then $\mathscr{A}$ is empty and $d(\mathscr{A}) = 0$ by a simple computation. Therefore, without loss of generality, we will assume that $L_q \neq Q$ for all q. Let $S_0 = \{q \in S \mid L_q \not\supset Q(\zeta_{q^2})\}$. Let us make the following definitions:

$N(x, \xi) =$ the number of primes $p \leqq x$ which do not split completely in L_q, $q \leqq \xi$, $q \in S$,

$P(x, k) =$ the number of primes $p \leqq x$ which split completely in L_k/Q (by convention, $L_1 = Q$, so that $P(x, 1) =$ the number of $p \leqq x$),

$M(x, \xi_1, \xi_2) =$ the number of primes $p \leqq x$ which split completely in some L_q, $\xi_1 < q \leqq \xi_2 \leqq x$.

If $p \leqq x$ splits completely in $Q(\zeta_{q^2})$, then $p \equiv 1 \pmod{q^2} \Rightarrow q \leqq x^{1/2}$. Therefore, if $p \leqq x$ splits completely in L_q, either $q \in S_0$ or $q \leqq x^{1/2} \Rightarrow \pi(x, \mathscr{A}) = N(x, x^{1/2})$ for x sufficiently large.

As in [6], we see that for $\xi_1 < \xi_2 \leqq x^{1/2}$,

$$\pi(x, \mathscr{A}) = N(x, \xi_1) + O(M(x, \xi_1, \xi_2)) + O(M(x, \xi_2, x^{1/2})), \qquad x \to \infty, \tag{3.1}$$

where the O-term constants do not depend on x, ξ_1, ξ_2. Set $\xi_2 = (\log x)^2$. Choose $\xi_1 = \xi_1(x)$ so that

$$\sup_{k \leqq \exp(2\xi_1)} \log |d_k| \leqq \log x, \tag{3.2}$$

$$\sup_{k \leqq \exp(2\xi_1)} n(k) \leqq A \log\log x, \tag{3.3}$$

$$\xi_1(x) \to \infty \quad \text{as } x \to \infty, \tag{3.4}$$

$$\exp(2\xi_1) \leqq \log x, \tag{3.5}$$

where d_k = the discriminant of L_k/Q, and A is a constant to be fixed later, subject only to the condition that it be sufficiently small.

Let us first show that with the above choice of ξ_1 and ξ_2, the O-terms of (3.1) are $o(x/\log x)$. We trivially have

$$M(x, \xi_1, \xi_2) \leqq \sum_{\xi_1 < q \leqq \xi_2} P(x, q), \tag{3.6}$$

$$M(x, \xi_2, x^{1/2}) \leqq \sum_{\xi_2 < q \leqq x^{1/2}} P(x, q), \tag{3.7}$$

$$P(x, q) \leqq \sum_{p \equiv 1 \pmod{q^2}} 1. \tag{3.8}$$

But,

$$\begin{aligned} \sum_{\xi_2 < q \leqq x^{1/2}} \sum_{p \equiv 1 \pmod{q^2};\, p \leqq x} 1 &\leqq \sum_{a^2 b \leqq x;\, \xi_2 < a} 1 \\ &\leqq x \sum_{\xi_2 < a \leqq x^{1/2}} a^{-2} \\ &\leqq Bx/\xi_2 = o(x/\log x), \qquad x \to \infty, \end{aligned} \tag{3.9}$$

for some constant B. Thus, $M(x, \xi_2, x^{1/2}) = o(x/\log x)$, $x \to \infty$. By the Brun-Selberg sieve [9, p. 44], the sum of (3.8) is at most $Cx/\varphi(q^2)\log(x/q^2)$ for C a positive constant not depending on x or q, and where φ = Euler's totient function. Thus, for x sufficiently large,

$$\begin{aligned} M(x, \xi_1, \xi_2) &\leqq Cx \sum_{\xi_1 < q \leqq \xi_2} [\varphi(q^2)\log(x/q^2)]^{-1} \\ &\leqq \frac{Cx}{\log(x/\xi_2)} \sum_{\xi_1 < q \leqq \xi_2} \varphi(q^2)^{-1} \\ &= o(x/\log x), \qquad x \to \infty, \end{aligned} \tag{3.10}$$

since $\xi_1 \to \infty$, and since $\sum_q \varphi(q^2)^{-1}$ converges. Therefore, by (3.11), (3.9) and (3.10), we obtain

$$\pi(x, \mathscr{A}) = N(x, \xi_1) + o(x/\log x), \qquad x \to \infty. \tag{3.11}$$

It remains for us to study $N(x, \xi_1)$. One easily sees that

$$N(x, \xi_1) = \sum_k^* \mu(k)P(x, k), \tag{3.12}$$

where the summation is over all k whose prime factors are $\leqq \xi_1$.

We will write $\pi(x, k)$ instead of $\pi(x, L_k)$ in what follows. Let $\pi'(x, k)$ = the number of primes φ of L_k such that $N\varphi \leqq x$ and such that φ is of absolute degree 1 and unramified in L_k/Q. Set $\pi''(x, k) = \pi(x, k) - \pi'(x, k)$. Note that $\pi'(x, k) = n(k)P(x, k)$. The primes counted in $\pi'(x, k)$ either ramify in L_k/Q or are of degree >1. Thus, since the ramified primes divide d_k,

$$\pi''(x, k) \leqq 2 \log |d_k| + n(k) \sum_{p^2 \leqq x} 1 \leqq 2 \log |d_k| + n(k)x^{1/2}. \tag{3.13}$$

Denoting $\vartheta(y) = \sum_{p \leqq y} \log p$, a classical theorem of Tchebycheff asserts that $\vartheta(y) \leqq 2y$. But, in the sum of (3.12), we consider only square-free k whose prime factors are $\leqq \xi_1$. Thus, for any k present in (3.12), we have

$$k \leqq \exp(\theta(\xi_1)) \leqq \exp(2\xi_1).$$

Therefore, by (3.2), (3.3), and (3.5), for k appearing in (3.12), $\pi''(x, k) \leqq 2x^{1/2} \log x$. Therefore, for k appearing in (3.12),

$$\pi(x, k) = n(k)P(x, k) + O(x^{1/2} \log x), \qquad x \to \infty,$$

and

$$\begin{aligned} N(x, \xi_1) &= \sum_k^* \mu(k)\left[\frac{\pi(x, k)}{n(k)} + O\left(\frac{x^{1/2} \log x}{n(k)}\right)\right] \\ &= \sum_k^* \frac{\mu(k)\pi(x, k)}{n(k)} + O(x^{1/2} \log x) \end{aligned}$$

since $\sum_k n(k)^{-1}$ converges. But, by (3.11),

$$\pi(x, \mathscr{A}) = \sum_k^* \frac{\mu(k)\pi(x, k)}{n(k)} + o(x/\log x), \qquad x \to \infty. \tag{3.14}$$

Let $\varepsilon > 0$ be given. Then, by [SW], there exist constants $b = b(\varepsilon)$, $c = c(\varepsilon)$, independent of k, such that

$$|\pi(x, k) - li(x)| \leqq Dx \log^2 x \exp\{-bn(\log x)^{1/2}/D\}, \qquad D = n(k)^3 |d_k|^{\varepsilon} c^{n(k)}.$$

Without loss of generality, assume $c > 1$. If $k \leqq \exp(2\xi_1)$, then equations (3.2)–(3.5) imply that

$$D \leqq (\log x)^{\varepsilon}(A \log \log x)^3 (\log x)^{A \log c}. \tag{3.15}$$

Choose A so that $A \log c < \varepsilon$. Then $k \leqq \exp(2\xi_1)$ implies that

$$|\pi(x, k) - li(x)| \leqq c_1 x (\log x)^{2+3\varepsilon} \exp(-c_2 (\log x)^{1/2 - 3\varepsilon}) \tag{3.16}$$

where c_i $(i=1, 2)$ are independent of k. Setting $\varepsilon=1/12$ and inserting the estimate (3.16) in (3.14), we get

$$\begin{aligned}\pi(x, \mathscr{A}) &= \sum_k{}^* \frac{\mu(k)}{n(k)} [li(x)+O(x \exp(-c_2(\log x)^{1/4}))]+o(x/\log x)\\ &= li(x) \sum_k{}^* \frac{\mu(k)}{n(k)}+O(x \exp(-c_2(\log x)^{1/4}))+o(x/\log x)\\ &= li(x) \sum_k{}^* \frac{\mu(k)}{n(k)}+o(x/\log x), \qquad x \to \infty,\end{aligned}$$

since $\sum_k n(k)^{-1}$ converges. But $\sum_k^*$ certainly includes all terms for which $k \leqq \xi_1$. The terms for which $k > \xi_1$ give an error of $o(x/\log x)$ since $\sum_k n(k)^{-1}$ converges and $\xi_1 \to \infty$ as $x \to \infty$. Thus,

$$\pi(x, \mathscr{A}) = li(x) \sum_{k \leqq \xi_1} \frac{\mu(k)}{n(k)}+o(x/\log x) = li(x)d(\mathscr{A})+o(x/\log x),$$

which proves Theorem 1.

Let us now sketch the proof of Theorem 3. Let notations be as above. Then, $\pi(x, \mathscr{A})=N(x, x)$. If $\xi_1<\xi_2<\xi_3 \leqq x$, then

$$\pi(x, \mathscr{A}) = N(x, \xi_1)+O(M(x, \xi_1, \xi_2))+O(M(x, \xi_2, \xi_3))+O(M(x, \xi_3, x)),$$

where the O-term constants do not depend on x or ξ_i $(i=1, 2, 3)$. Let ξ_1 be defined by (3.2)–(3.5). Set $\xi_2=x^{1/2} \log^{-2} x$, $\xi_3=x^{1/2} \log^2 x$. Using the same reasoning as [6, pp. 211–212], we see that $M(x, \xi_2, \xi_3)=o(x/\log x)$, $M(x, \xi_3, x)=o(x/\log x)$. By the extended Riemann hypothesis [6, p. 218]

$$\pi(x, k) = li(x)+O(n(k)x^{1/2} \log^2 x),$$

where the O-term constant does not depend on k. Therefore,

$$\begin{aligned}M(x, \xi_1, \xi_2) &\leqq \sum_{\xi_1 < q \leqq \xi_2} \frac{\pi(x, q)}{n(q)}\\ &= li(x) \sum_{\xi_1 < q \leqq \xi_2} n(q)^{-1}+O(x^{1/2} \log^2 x\, P(\xi_2, 1))\\ &= o(x/\log x).\end{aligned}$$

Therefore, $\pi(x, \mathscr{A})=N(x, \xi_1)+o(x/\log x)$. From this point the reasoning proceeds as in the proof of Theorem 1.

4. **Proof of Theorem 2.** Our proof of Theorem 2 is modelled on the calculations in [6, §6]. Since $L_q=Q(\zeta_{q^2}, a^{1/q})$, we clearly have $L_k=Q(\zeta_{k^2}, a^{1/k})$. Let us compute $n(k)$. Let $M_k=Q(\zeta_{k^2})$, $r=$ the largest integer such that a is an rth power, $k_1=k/(k, r)$. Then

$$\deg(M_k/Q) = \varphi(k^2), \tag{4.1}$$

$$\deg(L_k/M_k) | k_1. \tag{4.2}$$

Set $k_1 = m \deg (L_k/M_k)$, where m is square-free. For q prime, $q|k$, $s_q = \deg (M_k(a^{1/q})/M_k)$ is either 1 or q and $s_q|(k_1/m)$. Therefore, if $q|m$, $s_q = 1 \Rightarrow a^{1/q} \in M_k \Rightarrow q = 2$ since M_k/Q is abelian $\Rightarrow m = 1$ or 2. If k is odd, then $m = 1$. Assume that k is even and let $a = a_1 a_2^2$, with a_1 square-free. Then $m = 2 \Leftrightarrow a_1^{1/2} \in M_k$.

LEMMA 4.1. $a_1^{1/2} \in M_k \Leftrightarrow a_1|k$.

Proof. If $a_1|k$, then $Q((\pm a_1)^{1/2}) \subset M_k$ for some choice of sign. But k is even, so that $(-1)^{1/2} \in M_k$. Therefore, $Q(a_1^{1/2}) \subset M_k$. If $a_1^{1/2} \in M_k$, and $q|a_1$, then q ramifies in the extension M_k/Q, so that $q|k$. Since a_1 is square-free, $a_1|k$. Therefore,

LEMMA 4.2.

$$\begin{aligned} \deg (L_k/M_k) &= k_1/2 \quad \textit{if } k \textit{ even, } a_1|k, \\ &= k_1 \quad \textit{otherwise.} \end{aligned}$$

Using equation (4.1) and Lemma 4.2, we see that

PROPOSITION 4.3.

$$\begin{aligned} n(k) &= k\varphi(k^2)/2(r, k) \quad \textit{if } k \textit{ is even, } a_1|k, \\ &= k\varphi(k^2)/(r, k) \quad \textit{otherwise.} \end{aligned}$$

By Theorem 1, $d(\mathscr{A}) = \sum_k (\mu(k)/n(k))$. Let us break the computation of $d(\mathscr{A})$ up into two cases. Assume that $a \neq a$ square.

Case 1. a_1 odd. In this case, the first case of Proposition 4.3 holds $\Leftrightarrow k \equiv 0 \pmod{2a_1}$. Therefore,

$$\begin{aligned} d(\mathscr{A}) &= \sum_{k \equiv 0 \,(\mathrm{mod}\, 2a_1)} \frac{2\mu(k)(r, k)}{k\varphi(k^2)} + \sum_{k \not\equiv 0 \,(\mathrm{mod}\, 2a_1)} \frac{\mu(k)(r, k)}{k\varphi(k^2)} \\ &= \sum_{k \equiv 0 \,(\mathrm{mod}\, 2a_1)} \frac{\mu(k)(r, k)}{k\varphi(k^2)} + \sum_k \frac{\mu(k)(r, k)}{k\varphi(k^2)}. \end{aligned}$$

The second sum can be written

$$\prod_{q|r} \left[1 - \frac{1}{q(q-1)}\right] \prod_{q \nmid r} \left[1 - \frac{1}{q^2(q-1)}\right].$$

In the first sum, let $k = 2|a_1|j$, j square-free. Then the first sum equals

$$\begin{aligned} &\frac{\mu(2|a_1|)(r, 2a_1)}{2|a_1|\varphi(4|a_1|^2)} \sum_{j;(j, 2a_1)=1} \frac{\mu(j)(r, j)}{j\varphi(j^2)} \\ &\qquad = \frac{\mu(2|a_1|)(r, 2a_1)}{2|a_1|\varphi(4|a_1|^2)} \sum_{q \nmid 2a_1;\, q \nmid r} \left[1 - \frac{1}{q^2(q-1)}\right] \prod_{q \nmid 2a_1;\, q|r} \left[1 - \frac{1}{q(q-1)}\right]. \end{aligned}$$

An easy calculation now shows that

$$d(\mathscr{A}) = C(a) \prod_{q \nmid 2a_1;\, q \nmid r} \left[1 - \frac{1}{q^2(q-1)}\right] \prod_{q \nmid 2a_1;\, q|r} \left[1 - \frac{1}{q(q-1)}\right] \tag{4.3}$$

where

$$C(a) = \left[\prod_{q|2a_1;\, q|r} q(q-1) \prod_{q|2a_1;\, q\nmid r} q^2(q-1)\right]^{-1} \times \left[\mu(2|a_1|) + \prod_{q|2a_1;\, q|r} (q^2-q-1) \prod_{q|2a_1;\, q\nmid r} (q^3-q^2-1)\right]. \tag{4.4}$$

It is easy to see that $C(a)\neq 0$, so that Theorem 2 is verified in case $a\equiv 0, 1, 3 \pmod 4$.

Case 2. a_2 even. In this case, the first case of Proposition 4.3 holds $\Leftrightarrow k\equiv 0 \pmod{|a_1|}$. Reasoning as in Case 1, we see that

$$d(\mathscr{A}) = C'(a) \prod_{q\nmid 2a_1;\, q\nmid r} \left[1-\frac{1}{q^2(q-1)}\right] \prod_{q|2a_1;\, q|r} \left[1-\frac{1}{q(q-1)}\right] \tag{4.5}$$

where

$$C'(a) = \left[\prod_{q|a_1;\, q|r} q(q-1) \prod_{q|a_1;\, q\nmid r} q^2(q-1)\right]^{-1} \times \left[\mu(|a_1|) + \prod_{q|a_1;\, q|r} (q^2-q-1) \prod_{q|a_1;\, q\nmid r} (q^3-q^2-1)\right]. \tag{4.6}$$

Again one verifies that $C'(a)\neq 0$ and hence that $d(\mathscr{A})\neq 0$. This completes the proof of Theorem 2.

5. **Connection with Serre's theory.** In the following paragraph, we will demonstrate the connection between our main theorem and some recent work of Serre [10, I-19–I-29] on Tchebotarev's density theorem. It will turn out that Theorem 1 is a "Tchebotarev-type" density theorem for a certain infinite, Galois extension of Q. Let us first summarize Serre's theory.

Let X be a compact topological space, μ' a Radon measure on X. Let $x_1, x_2, \ldots$ be a sequence of points of X. We say that the sequence is *μ'-equidistributed* if, for each continuous function f having compact support on X, we have

$$\mu'(f) = \lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} f(x_i).$$

PROPOSITION 5.1 (SERRE [10, p. I-19]). *Suppose that the sequence $\{x_n\}$ is μ'-equidistributed. Let $U\subset X$ be such that boundary (U) has μ' measure 0. Denote by $\pi(x, U)$ the number of $x_i \in U$, $i\leqq x$. Then*

$$\lim_{x\to\infty} \frac{\pi(x, U)}{x} = \mu'(U).$$

If U is only μ'-measurable, then

$$\limsup_{x\to\infty} \frac{\pi(x, U)}{x} \leqq \mu'(U).$$

Let G be a compact group and let X be the space of conjugacy classes of G. Topologize X with the strongest topology such that the projection map $G \xrightarrow{\pi} X$

is continuous. Let μ be the Haar measure on G such that $\mu(G)=1$. Let μ' be the measure on X induced by μ. Then, for $V\subset X$, $\mu'(V)=\mu(\eta^{-1}(V))$. A simple test for equidistribution of a sequence on X is given by

PROPOSITION 5.2 (SERRE [10, p. I-20]). *A sequence $\eta(x_1), \eta(x_2), \ldots$ of elements of X is μ'-equidistributed $\Leftrightarrow$ for every nontrivial, irreducible character χ of G, we have*

$$\lim_{n\to\infty} \frac{1}{n} \sum_{i=1}^{n} \chi(x_i) = 0.$$

Let L be a (finite or infinite) Galois extension of the algebraic number field K. Then $G=\mathrm{Gal}\,(L/K)$ is a compact, totally-disconnected group. Let μ be the Haar measure on G such that $\mu(G)=1$. Assume that only finitely many primes $\mathfrak{p}$ of K ramify in L. Then, for almost all $\mathfrak{p}$, the Artin symbol $((L/K)/\mathfrak{p})$ is defined. If $C\subset G$, denote by $\pi(x, C)$ the number of $\mathfrak{p}$ such that $N\mathfrak{p}\leqq x$, $((L/K)/\mathfrak{p})\in C$. Then, from Propositions 5.1 and 5.2, one can deduce

THEOREM 5.3 (TCHEBOTAREV-SERRE [10, I-8]). *Let $C\subset G$ be invariant under inner automorphisms of G and assume that Boundary (C) has μ-measure 0. Then*

$$\lim_{x\to\infty} \frac{\pi(x, C)}{x/\log x} = \int_C d\mu.$$

In what follows, we will show that Theorem 1 is essentially a statement of Theorem 5.3 for particular C and G with the following two differences: (1) In our situation, L/K will be ramified at every prime, so that $((L/K)/\varphi)$ may not be well defined. (2) Boundary (C) will not generally have μ-measure 0. The first difficulty is easily remedied by redefining the Artin symbol so that it is always defined. The second difficulty is not superficial, however. For, if the above theorem were true without the condition on Boundary (C), then one could trivially establish the Artin conjecture. Actually, very little is known about the situation where Boundary (C) has positive measure. Theorem 5.3 is proven by showing that the sequence $\{\sigma_\varphi\}$, $\sigma_\varphi=\eta(((L/K)/\mathfrak{p}))$ is μ'-equidistributed on X. One then appeals to Proposition 5.1 to get the conclusion. If, in Proposition 5.1, one removes the condition on Boundary (U), then the conclusion is, in general, false. For example, one can construct a Cantor set C of positive measure on R/Z and a sequence $\{z_n\}$ which is equidistributed on R/Z such that $z_n\notin C$ for all n[2]. It appears that any characterization of the sets C for which Theorem 5.3 holds (using a suitable generalization of the Artin symbol) would be of great consequence in analytic number theory.

Let us now interpret Theorem 1 as a "Tchebotarev-type" density theorem. Let us consider a family of fields $\{L_q\}_{q\in S}$, satisfying

(1) $L_q\neq Q$, $q\in S$,

(2) $\sum_k 1/n(k)$ converges,

(3) L_q/Q a normal extension.

---

[2] This example was pointed out to me by Burton Randol.

Let L be the composite of all L_q. Then L is a Galois extension of Q, having a compact, totally disconnected Galois group G. Let X, μ, μ' have the same meanings as above. Let $H_k \subset G$ be the open subgroup corresponding to L_k, i.e. $G/H_k = G_k = \mathrm{Gal}(L_k/Q)$. Let $C = G - \bigcup_q H_q$. Then C is a compact subset of G, invariant under conjugation by elements of G. Set $\bar{C} = \eta(C)$.

LEMMA 5.4. $\int_{\bar{C}} d\mu' = \sum_k \mu(k)/n(k)$.

Proof. Since C is invariant under conjugation by elements of G, $\eta^{-1}(\bar{C}) = C$. Therefore, $\int_{\bar{C}} d\mu' = \int_C d\mu$. Let r be a positive integer. Elementary combinatorial reasoning shows that

$$\left| \mu(C) - \left\{ \mu(G) - \sum_q \mu(H_q) + \sum_{q_1,2q;\, q_i \text{ distinct}} \mu(H_{q_1 q_2}) - \cdots + (-1)^r \sum_{q_1,\ldots,q_r;\, q_i \text{ distinct}} \mu(H_{q_1 \ldots q_r}) \right\} \right| \leqq \sum_{q_1,\ldots,q_{r+1};\, q_i \text{ distinct}} \mu(H_{q_1 \ldots q_{r+1}}).$$

Since μ is translation-invariant, and since $G/H_k = G_k$ has order $n(k)$, one sees that $\mu(H_k) = 1/n(k)$. Inserting this value in the above inequality, and letting $r \to \infty$, we see that the right-hand side tends to 0, which proves the lemma.

Let us now define the Artin symbol for ramified primes. Let M and N be finite, algebraic number fields, N/M Galois. Let φ be a prime of M and $\wp$ any extension of φ to N. Then we have the exact sequence

$$(1) \longrightarrow I(\wp) \longrightarrow D(\wp) \xrightarrow{\theta} \mathrm{Gal}(\bar{N}/\bar{M}) \longrightarrow (1),$$

where

$I(\wp)$ = the inertia group at $\wp$,

$D(\wp)$ = the decomposition group at $\wp$,

$\bar{M}$ (resp. $\bar{N}$) = the residue class field of M (resp. N) at φ (resp. $\wp$),

θ = reduction mod $\wp$.

Let $\pi \in \mathrm{Gal}(\bar{N}/\bar{M})$ be the Frobenius map: $\pi(x) = x^{N\mathfrak{p}}$.

DEFINITION. The generalized Artin symbol $((N/M)/\mathfrak{p})$ is the smallest union of conjugacy classes in $H = \mathrm{Gal}(N/M)$, containing $I(\wp)\theta^{-1}(\pi)$.

It is trivial to verify the following properties of the symbol $((N/M)/\mathfrak{p})$:

LEMMA 5.5. (1) $((N/M)/\mathfrak{p})$ *does not depend on the choice of* $\wp$. *If* $\mathfrak{p}$ *is unramified in* N/M, *then* $((N/M)/\mathfrak{p})$ *coincides with the usual Artin symbol.*

(2) *If* $K \subset M \subset N$, *with* N/K *and* M/K *Galois, then the restrictions of the element, of* $((N/K)/\mathfrak{p})$ *to* M *are precisely the elements of* $((M/K)/\mathfrak{p})$.

(3) $\mathfrak{p}$ *splits completely in* $N \Leftrightarrow ((N/M)/\mathfrak{p})$ *consists only of the identity of* H.

If L is an infinite, Galois extension of K, with Galois group G, and if $\mathfrak{p}$ is a prime of K, then the Artin symbol $((L/K)/\mathfrak{p})$ is defined as the set of $\sigma \in G$ such that for

every field M such that $K \subset M \subset L$, M/K finite and Galois, one has $\sigma|_M \in ((M/K)/\mathfrak{p})$.

Returning to our particular field L, let us choose for each rational prime p, and element σ_p contained in $((L/Q)/p)$. Throughout the remainder of this discussion hold the sequence $\{\sigma_p\}$ fixed.

LEMMA 5.6. *Let $\bar{\sigma}_p$ be the image of σ_p in X. Then the sequence $\{\bar{\sigma}_p\}$ is μ'-equidistributed.*

Proof. By Proposition 5.2, it suffices to show that for χ a nontrivial, irreducible character of G, we have

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p \leqq x} \chi(\sigma_p) = 0,$$

where $\pi(x)$ = the number of rational primes $\leqq x$. It is well known that χ is a finite-dimensional character of G. Let ρ be a representation of G having character χ. The kernel H of ρ is an open subgroup of G; let L_0 be the fixed field of H. Then L_0 is a finite, Galois extension of Q, with Galois group $G_0 = G/H$. Let $\hat{\chi}$ be the character induced by χ on G_0. If p does not ramify in L_0/Q, then

$$\chi(\sigma_p) = \hat{\chi}(((L_0/Q)/p)).$$

Therefore, for all but a finite number of primes p, $\chi(\sigma_p)$ coincides with the value $\chi_0(p)$ of the Artin character $\hat{\chi}(((L_0/Q)/p))$. It is easy to see that χ_0 is nontrivial. Therefore,

$$\lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p \leqq x} \chi(\sigma_p) = \lim_{x\to\infty} \frac{1}{\pi(x)} \sum_{p \leqq x;\ p \text{ unramified in } L_0/Q} \chi_0(p) = 0$$

by a well-known theorem of Artin [1, p. 121]. Therefore, $\{\bar{\sigma}_p\}$ is μ'-equidistributed.

Let $\mathscr{A}$ denote the set of primes p which do not split completely in L_q for all $q \in S$.

LEMMA 5.7. $p \in \mathscr{A} \Leftrightarrow \bar{\sigma}_p \in \bar{C}$.

Proof. $p \in \mathscr{A} \Leftrightarrow ((L_q/Q)/p) \neq \{e_q\}$, e_q = identity of G_q, $q \in S \Leftrightarrow \sigma_p \notin H_q$, $q \in S$ $\Leftrightarrow \sigma_p \in C \Leftrightarrow \bar{\sigma}_p \in \bar{C}$.

Combining Theorem 1, and Lemmas 5.4 and 5.7, we finally arrive at the main theorem of this paragraph:

THEOREM 5.8. *Assume that $L_q \supset Q(\zeta_{q^2})$ for almost all $q \in S$. Then*

$$\lim_{x\to\infty} \frac{\pi(x, \mathscr{A})}{x/\log x} = \lim_{x\to\infty} \frac{\pi(x, C)}{x/\log x} = \int_C d\mu.$$

Using the second assertion of Proposition 5.1 and Lemmas 5.4, 5.6, and 5.7, we can easily establish Theorem 4. (One can also give a direct proof.)

BIBLIOGRAPHY

1. S. Lang and J. T. Tate (editors), *Collected papers of Emil Artin*, Addison-Wesley, Reading, Mass., 1965. MR 31 #1159.

2. H. Bilharz, *Primdivisoren mit vorgegebenen Primitivwurzel*, Math. Ann. **114** (1937), 476–492.

3. L. Goldstein, *Analogues of Artin's conjecture*, Bull. Amer. Math. Soc. **74** (1968), 517–519. MR **36** #6376.

4. ———, *A generalization of the Siegel-Walfisz theorem*, Trans. Amer. Math. Soc. **149** (1970), 417–429.

5. H. Hasse, *Über die Artinsche Vermutung und verwandte Dichtefragen*, Ann. Acad. Sci. Fenn. Ser. A I. Math.-Phys. no. 116 (1952). MR **14**, 538.

6. C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220. MR **34** #7445.

7. W. Knobloch, *Über Primzahlreihen nebst Anwendung auf ein elementares Dichteproblem*. Abh. Math. Sem. Univ. Hamburg **19** (1954), no. 1–2, 1–13. MR **16**, 16.

8. L. Mirsky, *The number of representations of an integer as the sum of a prime and a k-free integer*, Amer. Math. Monthly **56** (1949), 17–19. MR **10**, 431.

9. K. Prachar, *Primzahlverteilung*, Springer-Verlag, Berlin and New York, 1957. MR **19**, 393.

10. J.-P. Serre, *Abelian l-adic representations and elliptic curves*, Benjamin, New York, 1968.

YALE UNIVERSITY,
NEW HAVEN, CONNECTICUT 06520