Density Questions in Algebraic Number Theory

L. J. Goldstein

The American Mathematical Monthly, Vol. 78, No. 4. (Apr., 1971), pp. 342-351.

Stable URL:
http://links.jstor.org/sici?sici=0002-9890%28197104%2978%3A4%3C342%3ADQIANT%3E2.0.CO%3B2-J

The American Mathematical Monthly is currently published by Mathematical Association of America.

Supplementary References

At the suggestion of the referee some additional general references have been added. The most relevant pages in each of the cited works are indicated in parentheses after the citation.

J. Dieudonné, Foundations of Modern Analysis, Academic Press, New York, 1960 (pp. 308–311; 319–323; 329–351).

T. Kato, Perturbation Theory for Linear Operators, Springer Verlag, Berlin and Heidelberg, 1966 (pp. 364–426).

M. A. Naimark, Normed Rings, Nordhoff, Groningen, 1959 (pp. 65–66; 82–83; 173–175; 192–195; 202–207).

K. Yosida, Functional Analysis, Springer Verlag, Berlin and Heidelberg, 1965 (pp. 209–212; 225–231).

A. C. Zaanen, Linear Analysis, North Holland Publishing Co., Amsterdam, 1953 (pp. 344–350; 462–495; 500–509).

DENSITY QUESTIONS IN ALGEBRAIC NUMBER THEORY

L. J. GOLDSTEIN, University of Maryland

Very often, the number theorist bases conjectures on empirical investigations. Even before the invention of the electronic computer, number theorists spent much time doing calculations, the results of which suggested possibly true statements. After the empirical stage of his investigation is completed, the number theorist then tries to supply proofs for his conjectures. It is here where the number theorist applies a formidable armada of high-powered machinery, ranging from analytic function theory to algebraic geometry. It is most surprising that even the most innocently conceived conjecture may lead into a vast jungle of very difficult and technical mathematics. But such is the nature of number theory. In this lecture, I should like to discuss a set of conjectures which typify the process of number-theoretic creation as we have described it: These conjectures originate out of empirical investigation and those few that we are able to prove seem to lead us far afield for their proofs.

1. Gauss' conjecture. Let us denote by Z the rational integers, p an odd prime, a an arbitrary integer, and $Z_p^\times$ the group of nonzero residue classes mod p. Since $Z_p^\times$ is the multiplicative group of a finite field, a well-known result asserts that $Z_p^\times$ is cyclic of order $p-1$. We say that a is a *primitive root* modulo p if $(a, p)=1$ and if its residue class $\bar{a}$ in $Z_p^\times$ is a generator of $Z_p^\times$.

LEMMA 1.1. *The number a is a primitive root modulo p if and only if* $(a, p)=1$ *and* $a^\nu \not\equiv 1 \pmod{p}$ *for* $\nu=1, 2, \cdots, p-1$.

Larry Goldstein received his Princeton PhD under G. Shimura in 1967. He was a Gibbs lecturer at Yale for two years before his present associate professorship at Maryland. His main research is in analytic and algebraic number theory, and his book, *Analytic Number Theory*, is scheduled to appear. *Editor.*

Note that by Fermat's Little Theorem, if $(a, p)=1$, then

$$a^{p-1} \equiv 1 \pmod{p}.$$

From now on, let us fix a, and let us define

$$\mathcal{A}(a) = \{p \mid p \text{ is prime and } a \text{ is a primitive root modulo } p\}.$$

It may be that $\mathcal{A}(a)$ is empty. For example, if a is a perfect square, say x^2, with $(p, a)=1$, then

$$x^{p-1} \equiv 1 \pmod{p}$$

by Fermat's Little Theorem, so that

$$a^{(p-1)/2} \equiv 1 \pmod{p}.$$

Therefore, if $p \nmid x$, p odd, then $p \notin \mathcal{A}(a)$. However, if $p \mid x$, then it is certainly true that $p \notin \mathcal{A}(a)$. Therefore, we have shown that $\mathcal{A}(a)=\varnothing$ if a is a perfect square. Moreover, since $(-1)^2=+1$, we see that $p \notin \mathcal{A}(-1)$ if $p-1>2$. Therefore, since -1 is a primitive root modulo 3, we have proved that $\mathcal{A}(-1)=\{3\}$.

By means of laborious calculations, Gauss investigated the case $a=10$ and arrived at the following conjecture, which is stated in Article 303 of his *Disquisitiones Arithmeticae*:

CONJECTURE A: $\mathcal{A}(10)$ *is infinite.*

In the next sections, we shall present some heuristic evidence for this conjecture, as well as some more general conjectures which seem to be true.

2. Artin's conjecture. In a conversation with Hasse in 1927, Artin made the following conjecture:

CONJECTURE B: *Suppose that a is not* -1 *and not a perfect square. Then* $\mathcal{A}(a)$ *is infinite.*

This conjecture was not just a wild guess, but followed from a very compelling probabilistic argument which Artin advanced. In order to trace Artin's line of thought, we must first define a few notions.

Let $\mathcal{S}$ be a set of primes (finite or infinite), and let x be a positive real number. Let $\pi(x)$ denote the number of primes $\leqq x$, and let $\pi(x, \mathcal{S})$ denote the number of primes in $\mathcal{S}$ which are $\leqq x$. We say that $\mathcal{S}$ has a *(natural) density* if

$$\lim_{x\to\infty} \pi(x, \mathcal{S})/\pi(x)$$

exists. The value of the limit is called the *density of* $\mathcal{S}$ and is denoted $d(\mathcal{S})$. We clearly have

$$0 \leqq d(\mathcal{S}) \leqq 1.$$

Moreover, if $d(\mathcal{S})>0$, then $\mathcal{S}$ is infinite since $\pi(x)\to\infty$ as $x\to\infty$. In a few moments we shall reformulate Conjecture B in the form of a statement about densities. But first we must state some preliminary information about algebraic number theory.

Let K be an algebraic number field, that is, a finite, algebraic extension of $\boldsymbol{Q}$. Let $\mathfrak{O}$ be the ring of integers of K, that is, the integral closure of $\boldsymbol{Z}$ in K. If p is an ordinary prime, then $p\mathfrak{O}$ is an ideal of $\mathfrak{O}$, but is usually no longer a prime ideal. However, $p\mathfrak{O}$ can be written as a product of powers of prime ideals of $\mathfrak{O}$ (since $\mathfrak{O}$ is a Dedekind domain):

$$p\mathfrak{O} = \mathfrak{P}_1^{e_1} \cdots \mathfrak{P}_g^{e_g}.$$

It is a general fact from algebraic number theory that $g \leqq \deg(K/\boldsymbol{Q})$. We say that p *splits completely* in K if $g = \deg(K/\boldsymbol{Q})$. Here is a basic theorem which one meets in the analytical portion of algebraic number theory.

THEOREM 2.1 (Dirichlet). *Let $n = \deg(K/\boldsymbol{Q})$ and let $\mathcal{S}$ denote the set of all primes which split completely in K. Then $\mathcal{S}$ has a density and*

$$d(\mathcal{S}) = 1/n.$$

Let q be a prime and let L_q denote the splitting field over $\boldsymbol{Q}$ of the polynomial $X^q - a$. We get L_q from $\boldsymbol{Q}$ in two steps. First we adjoin to $\boldsymbol{Q}$ a primitive qth root of unity ζ_q. Then we adjoin to $\boldsymbol{Q}(\zeta_q)$ any qth root of a, say the real value of $a^{1/q}$. Then,

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

$L_q/\boldsymbol{Q}(\zeta_q)$ is a Galois extension of degree either 1 or q with cyclic Galois group. (The extension is a so-called Kummer extension.) Also, $\boldsymbol{Q}(\zeta_q)/\boldsymbol{Q}$ is a Galois extension of degree $q-1$ with cyclic Galois group. Thus, $L_q/\boldsymbol{Q}$ is a Galois extension with solvable Galois group and

$$\deg(L_q/\boldsymbol{Q}) = q - 1 \quad \text{or} \quad q(q-1), \tag{2}$$

depending on the value of a.

From the tool box of the algebraic number theorist, we quote the following result:

THEOREM 2.2. *p splits completely in $L_q \Leftrightarrow p \equiv 1 \pmod{q}$ and*

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

Combined with Lemma 1.1, this yields the following:

THEOREM 2.3. *a is a primitive root modulo p if and only if for each prime q, the prime p does not split completely in L_q.*

For K an algebraic number field, let $\mathrm{Spl}(K)$ denote the set of all primes which split completely in K; let $\mathcal{P}$ denote the set of all primes. Then, by Theorem 2.3, we can assert the following:

COROLLARY 2.4. $\mathcal{A}(a)=\bigcap_q (\mathcal{P}-\mathrm{Spl}(L_q))$.

Now for Artin's probabilistic argument: By Dirichlet's theorem, $\mathrm{Spl}(L_q)$ has a density and $d(\mathrm{Spl}(L_q))=1/\deg(L_q/Q)$. Therefore, $\mathcal{P}-\mathrm{Spl}(L_q)$ has a density and

$$d(\mathcal{P}-\mathrm{Spl}(L_q)) = 1 - 1/\deg(L_q/Q).$$

Therefore, from Corollary 2.4, we might guess that $\mathcal{A}(a)$ has a density and that

$$(*) \qquad d(\mathcal{A}(a)) = \prod_q (1 - 1/n(q)), \qquad n(q) = \deg(L_q/Q).$$

Let us see how (*) fits in with Conjecture B. First of all, it is easy to check that if $a\neq -1$ then $n(q)=q(q-1)$ for all but a finite number of q. Therefore, the product converges for $a\neq -1$. For $a=-1$, the product diverges to 0. Thus, if $a\neq -1$, the product can converge to 0 if and only if one of the factors$=0$, and this in turn if and only if $n(q)=1$ for some q. But it is trivial to check that $n(q)\geqq q-1>1$ if $q>2$. Therefore, the product$=0$ if and only if $n(2)=1$. But $L_2=Q(a^{1/2})$, so that $n(2)=1$ if and only if a is a perfect square. Therefore, we conclude that if $a\neq -1$ and $a\neq b^2$, then the product is positive, so that $d(\mathcal{A}(a))>0$, which implies Conjecture B.

Thus, the heuristic arguments of Artin seemed to fit the facts such as they were known at the time. However, experimental calculations by D. H. Lehmer cast a serious doubt as to whether the true value of the density of $\mathcal{A}(a)$ was given by (*). In the face of this disagreement between conjecture and evidence, it was necessary to reexamine the reasoning which led to (*). Let us consider the probabilistic event "a randomly chosen prime belongs to $\mathcal{P}-\mathrm{Spl}(L_q)$." Dirichlet's Theorem may be interpreted as saying that the probability of this event is $1/n(q)$. We then get the probability that a randomly chosen prime belongs to the intersection of all $\mathcal{P}-\mathrm{Spl}(L_q)$ by multiplying the corresponding probabilities. This is valid, as every student of probability knows, only when the events are pairwise independent. Therefore, what probably goes wrong is that something analogous to probabilistic independence is violated. Of course, all of our analogies with probability theory are only of heuristic value. But they seem to lead somewhere in this case! For, upon close inspection, we see that the fields L_q are not "independent" of one another, that is, it is not true that $L_q\cap L_{q'}=Q$ for $q\neq q'$. Therefore, if we wish to make a statement like (*), it is necessary to somehow take into account this dependence.

By Corollary 2.4,

$$\mathcal{A}(a) = \mathcal{P} - \bigcup_q \mathrm{Spl}(L_q).$$

Note, however, that the primes which split completely in two fields L_{q_1} and L_{q_2} are subtracted twice on the right hand side of (3). In an attempt to count each prime in $\mathcal{A}(a)$ once and only once, let us add back in those primes which were removed twice to get

$$\mathcal{A}(a) = \mathcal{P} - \bigcup_q \mathrm{Spl}(L_q) + \bigcup_{\substack{q_1, q_2 \\ q_1\neq q_2}} \mathrm{Spl}(L_{q_1}) \cap \mathrm{Spl}(L_{q_2}).$$

In adding the last term, however, we have counted twice the primes which split completely in three fields L_{q_1}, L_{q_2}, L_{q_3}. Therefore, let us correct this by writing

$$\mathfrak{A}(a) = \mathcal{P} - \bigcup_{q} \mathrm{Spl}(L_q) + \bigcup_{\substack{q_1, q_2 \\ q_1 \neq q_2}} \mathrm{Spl}(L_{q_1}) \cap \mathrm{Spl}(L_{q_2})$$
$$- \bigcup_{\substack{q_1, q_2, q_3 \\ q_i \text{ distinct}}} \mathrm{Spl}(L_{q_1}) \cap \mathrm{Spl}(L_{q_2}) \cap \mathrm{Spl}(L_{q_3}).$$

But now the primes which split completely in four fields have been subtracted twice, so we must add them back in, and the process continues. Eventually, we arrive at a formula for $\mathfrak{A}(a)$ in which each prime is counted exactly once. If $q_1, q_2, \cdots, q_r$ are distinct primes, $k = q_1 \cdots q_r$, let us define L_k to be the composite

$$L_k = L_{q_1} \cdot \cdots \cdot L_{q_r}.$$

Then

$$\mathrm{Spl}(L_{q_1}) \cap \cdots \cap \mathrm{Spl}(L_{q_r}) = \mathrm{Spl}(L_k).$$

Therefore, we may write our formula for $\mathfrak{A}(a)$ in the form

$$\mathfrak{A}(a) = \mathcal{P} - \bigcup_{q} \mathrm{Spl}(L_q) + \bigcup_{\substack{q_1, q_2 \\ q_i \text{ distinct}}} \mathrm{Spl}(L_{q_1 q_2})$$
$$(3) \qquad - \bigcup_{\substack{q_1, q_2, q_3 \\ q_i \text{ distinct}}} \mathrm{Spl}(L_{q_1 q_2 q_3}) + \cdots.$$

We have defined L_k for each positive, square-free integer. Let $n(k) = \deg(L_k/Q)$. Then by Dirichlet's Theorem and (3), we can conjecture that

$$(4) \qquad d(\mathfrak{A}(a)) = 1 - \sum_{q} n(q)^{-1} + \sum_{\substack{q_1, q_2 \\ q_i \text{ distinct}}} n(q_1 q_2)^{-1} - \cdots.$$

By rewriting the right hand side of (4), we derive the following conjecture:

CONJECTURE C: *$\mathfrak{A}(a)$ has a natural density, and*

$$d(\mathfrak{A}(a)) = \sum_{k} \mu(k)/n(k), \qquad n(1) = 1,$$

where $\mu(k)$ denotes the Möbius function and the sum runs over all positive square-free integers k (including 1).

It is Conjecture C that agrees with the experimental evidence. Note, however, that from the form of the sum in Conjecture C, it is no longer evident that $d(\mathfrak{A}(a)) > 0$ if $a \neq -1$ and $a \neq b^2$. Also, it must be checked that the series converges. Both points are answered by the following theorem.

THEOREM 2.5 (Hooley [3]). *Let k be a positive square-free integer, let h denote the largest positive integer such that a is an h-th power, and let*

$$\begin{aligned} k_1 &= k/(h, k), \\ a_1 &= \textit{the square-free part of } a, \\ \epsilon(k) &= \begin{cases} 2 & \textit{if } k \textit{ is divisible by } 2a_1 \textit{ and } a_1 \equiv 1 \pmod 4 \\ 1 & \textit{otherwise.} \end{cases} \end{aligned}$$

Then $n(k) = k_1\phi(k)/\epsilon(k)$, where $\phi(k)$ denotes Euler's function.

As an immediate consequence of Hooley's theorem, we deduce two corollaries.

COROLLARY 2.6. *The sum $\sum_k \mu(k)/n(k)$ converges absolutely.*

COROLLARY 2.7. *If k and a are relatively prime, then*

$$n(k) = k\phi(k).$$

Using Hooley's theorem, we can write the sum of Conjecture C as a product, so that we may revise Conjecture C as follows:

CONJECTURE D: *$\mathfrak{A}(a)$ has a natural density and*

$$d(\mathfrak{A}(a)) = \begin{cases} C(k), & a_1 \not\equiv 1 \pmod 4 \\ C(k)\cdot\left[1 - \mu(|a_1|) \prod\limits_{\substack{q|h \\ q|a_1}} (q-2)^{-1} \prod\limits_{\substack{q\nmid h \\ q|a_1}} (q^2 - q - 1)^{-1}\right], & a_1 \equiv 1 \pmod 4, \end{cases}$$

where

$$C(k) = \prod_{q|h} (1 - (q-1)^{-1}) \prod_{q\nmid h} (1 - \phi(q^2)^{-1}).$$

This is our final form of Artin's conjecture. Implicit in the statement of Conjecture D is the statement that if $a \neq -1$ and a is not a perfect square, then $d(\mathfrak{A}(a)) > 0$. For then $|a_1| \neq 1$. Since $C(k) > 0$, we see that (mod Conjecture D)

$$d(\mathfrak{A}(a)) = 0 \Leftrightarrow a_1 \equiv 1 \pmod 4 \quad \text{and} \quad \mu(|a_1|) = 1$$

and

$$\prod_{\substack{q|h \\ q|a_1}} (q-2)^{-1} \prod_{\substack{q\nmid h \\ q|a_1}} (q^2 - q - 1)^{-1} = 1.$$

The last of the three conditions on the right can be satisfied only when $|a_1| = 1$, 2, or 3. But of these three possibilities only $|a_1| = 1$ is consistent with the remaining two conditions. Therefore Conjecture D implies

$$\begin{aligned} d(\mathfrak{A}(a)) &= 0 \Leftrightarrow |a_1| = 1 \\ &\Leftrightarrow a = -1 \quad \text{or} \quad a = b^2. \end{aligned} \tag{5}$$

3. Bilharz's Theorem. Let k be a finite field with q elements, $k[t]$ the ring of polynomials over k in an indeterminate t, and $K=k(t)$ the field of rational functions in t with coefficients in K. The field K is the simplest example of an algebraic function in one variable. The arithmetic properties of such fields parallel the arithmetic of Q, with $k[t]$ playing the role of the rational integers. In many ways, the arithmetic of K is even simpler than that of Z, so that often number theorists use function fields as a testing ground for conjectures about the rational integers. This testing process consists of reformulating a problem about Q or Z into an analogous problem about K or $k[t]$, respectively, and then solving the analogous problem.

In 1935, Bilharz [1], a student of Hasse, formulated and proved the analogue of Artin's conjecture. The role of the rational primes is played by the monic, irreducible polynomials $P\in k[t]$. If P is such a polynomial, then the *norm of P*, denoted NP, is defined by

$$NP = q^r, \qquad r = \deg(P).$$

The quotient ring

$$K_P = k[t]/Pk[t], \qquad P \text{ monic, irreducible,}$$

is a finite field with NP elements. The multiplicative group $K_P^\times$ of K_P is cyclic. Suppose that $A\in K$ is not divisible by P. We say that A is a *primitive root modulo P* if A mod $Pk[t]$ generates $K_P^\times$. Given $A\in K$, we can define

$$\mathfrak{A}(A) = \{P \mid A \text{ is a primitive root modulo } P\}.$$

It is easy to check that if A is an *r-th* power for some r dividing $q-1$, then $\mathfrak{A}(A)=\varnothing$. In analogy with the situation in Q, we can formulate a conjecture.

CONJECTURE A′: *If A is not an r-th power for any prime r dividing $q-1$, then $\mathfrak{A}(A)$ is infinite.*

Conjecture A' was proved in the cited work of Bilharz. The most interesting feature of Bilharz's paper is that he proves Conjecture A′ only by assuming a deep result, at the time conjectured but not proved, known as the "Riemann hypothesis for function fields over finite fields." The conjecture was settled by André Weil in 1941 [4], so that the gap in Bilharz's argument was filled.

Let $\mathcal{S}_0$ be the set of all monic, irreducible polynomials in $k[t]$, and let $x\geqq 0$. For $\mathcal{S}\subseteq\mathcal{S}_0$, define

$$\pi_K(x, \mathcal{S}) = \sum_{\substack{P\in\mathcal{S}\\ NP\leqq x}} 1, \qquad \pi_K(x) = \pi_K(x, \mathcal{S}_0).$$

We say that $\mathcal{S}$ has a *natural density* if

$$\lim_{x\to\infty} \frac{\pi_K(x, \mathcal{S})}{\pi_K(x)}$$

exists. We can formulate the analogues of the density conjectures in the function field case. However, the situation here is very much different from the preceding case. The set $\mathfrak{A}(A)$ usually does not have a natural density. However, it is possible to define a new concept of density (Dirichlet density) with respect to which the analogues of the density conjectures are true. The proofs of these results are contained in Bilharz's paper.

4. Hooley's Theorem. Let L be an algebraic number field. If $\mathfrak{A}$ is an ideal of the ring of integers $\mathfrak{O}_L$, the *norm of* $\mathfrak{A}$ denoted $N\mathfrak{A}$, is the number of elements in the (finite) ring $\mathfrak{O}_L/\mathfrak{A}$. The *Dedekind zeta function* of L is defined by

$$\zeta_L(s) = \sum_{\mathfrak{A}} N\mathfrak{A}^{-s},$$

where $\mathfrak{A}$ runs over all ideals of $\mathfrak{O}_K$ and s is a complex variable. The series on the right converges absolutely for $\mathrm{Re}(s) > 1$. Moreover, for s in this half-plane,

$$\zeta_L(s) = \prod_{\mathfrak{p}} (1 - N\mathfrak{p}^{-s})^{-1}, \tag{6}$$

where $\mathfrak{p}$ runs over all prime ideals of $\mathfrak{O}_L$. The product of (6) converges absolutely for $\mathrm{Re}(s) > 1$. Therefore,

$$\zeta_L(s) \neq 0 \qquad (\mathrm{Re}(s) > 1). \tag{7}$$

It is possible to show that $\zeta_L(s)$ can be analytically continued to a meromorphic function on the whole s-plane. The continued function (also denoted $\zeta_L(s)$) has only one pole, a simple pole at $s = 1$ with residue 1. Moreover, $\zeta_L(s)$ satisfies a functional equation connecting its behavior at s with its behavior at $1 - s$. One consequence of this functional equation is that the zeros of $\zeta_L(s)$ in the half-plane $\mathrm{Re}(s) < 0$ are known. These zeros are called *trivial zeros*. By (7), all nontrivial zeros of $\zeta_L(s)$ lie in the strip

$$0 \leqq \mathrm{Re}(s) \leqq 1.$$

There is strong evidence in favor of the following conjecture.

CONJECTURE (Riemann Hypothesis): *All nontrivial zeros of* $\zeta_L(s)$ *lie on the line* $\mathrm{Re}(s) = 1/2$.

The special case $L = Q$ of this celebrated conjecture was first stated by Riemann in 1860. Although the Riemann hypothesis has received the attention of many of the greatest mathematicians of the last 100 years, it remains unproved, and is one of the most significant unsolved problems of contemporary mathematics.

There is a link between the Riemann hypothesis and Conjecture C (the most general form of Artin's conjecture)—namely, Hooley [3], has proved the analogue of Bilharz's theorem:

THEOREM 4.1. *Assume that the Riemann hypothesis is true for each of the fields* L_k. *Then Conjecture* C *is true.*

5. Analogues of Artin's conjecture. It is possible to generalize the heuristic argument which gave rise to Conjecture C: Suppose that $\mathcal{S}$ is a set of rational primes, and suppose that for each $q \in \mathcal{S}$ there is given a number field L_q. Let $\mathcal{A} = \mathcal{A}(\mathcal{S}, \{L_q\})$ denote the set of rational primes which do not split completely in each L_q for $q \in \mathcal{S}$. Let us make a conjecture about the natural density of $\mathcal{A}$.

For $k = q_1 \cdots q_r$, $q_i \in \mathcal{S}$, set

$$L_k = L_{q_1} \cdots L_{q_r},$$

$$n(k) = \deg(L_k/Q).$$

Define $L_1 = Q$, so that $n(1) = 1$. Using the same arguments as in Paragraph 2, we can formulate another conjecture.

CONJECTURE E: *Suppose that*

$$\sum_k n(k)^{-1}$$

converges, where the sum runs over all k for which n(k) is defined. Then $\mathcal{A}$ *has a natural density*

$$d(\mathcal{A}) = \sum_k \mu(k) n(k)^{-1}.$$

Conjecture E clearly contains Conjecture C as a special case, namely for $\mathcal{S} = \{\text{all rational primes}\}$, $L_q = Q(\zeta_q, a^{1/q})$ $(q \in \mathcal{S})$. There are only two special cases for which Conjecture E has been verified. When $\mathcal{S}$ is finite, Conjecture E can be easily checked using Dirichlet's theorem. When $\mathcal{S}$ is infinite, however, Conjecture E is very difficult. The only case known is now given.

THEOREM 5.1 (Goldstein [2]). *Suppose that*

$$L_q \supseteq Q(\zeta_{q^2})$$

holds for all but a finite number of $q \in \mathcal{S}$. *Then Conjecture* E *is true. In particular, Conjecture* E *is true if* $\mathcal{S} = \{$*all rational primes*$\}$ *and*

$$L_q = Q(\zeta_{q^2}, a^{1/q}) \qquad (a \in Z, q \in \mathcal{S}).$$

Theorem 5.1 is tantalizingly close to Artin's conjecture. One might hope that the methods used to prove Theorem 5.1 could be appropriately generalized to prove Artin's conjecture. However, it appears that Conjecture E is of a much higher order of difficulty and any hopes in that direction are overly optimistic.

6. Conclusion. In this talk I have tried to indicate how a number theorist comes by his conjectures. In some sense, the combination of intuition, deduction, and heuristic arguments by means of which we have arrived at our conjectures, is a typical way in which many mathematicians work. There is much that we have been forced to omit. For example, it is possible to formulate Conjecture E as a conjecture about Haar measure on a certain compact topological group. In this formulation Conjecture E can be thought of as a generalization of Dirichlet's theorem to infinite-dimensional extensions L of Q. For an exposition of this theory, the reader is referred to [2]. If I have said little about methods of proof, it is because there are only a few theorems now proved in the subject. I hope that this talk will generate enough interest to remedy this appalling situation.

This paper is the text of an invited address delivered by the author under the title "On a Conjecture of Artin" at the Northeastern Sectional Meeting on June 20, 1969.

Research supported by NSF Grant GP-13872.

References

1. H. Bilharz, Primdivisoren mit vorgegebener Primitivwürzel, Math. Ann., 114 (1937) 476–492.
2. L. Goldstein, Analogues of Artin's conjecture, Trans. Amer. Math. Soc., (to appear).
3. C. Hooley, On Artin's conjecture, J. Reine Angew. Math., 225 (1967) 209–220.
4. A. Weil, Sur les Courbes Algébriques et les Variétés qui s'en Déduisent, Hermann, Paris, 1948.

MUSIMATICS or THE NUN'S FIDDLE*

A. L. LEIGH SILVER, Fellow of the Institute of Musical Instrument Technology, England

1. The divine ratio. "*Abominandum!*" said Cicero as he went a purler over a hidden obstacle—"*quid est quod?*"—and scrabbling in the undergrowth he uncovered an ancient monument. The lettering was illegible but the design—a cylinder circumscribing a sphere—was clearly that which Archimedes, who was killed in the fall of Syracuse 212 B.C., had charged his friends to inscribe on his tombstone. Since Cicero made this discovery about 75 B.C., the tomb has again been lost, probably forever.

Archimedes transformed empirical knowledge into theoretical science and developed the integral calculus which he said would be used by mathematicians "as yet unborn." In keeping with Aristotle's dictum that "it is proper to consider the similar even in things far distant from each other," he considered it highly significant that the cylinder and inscribed sphere, as regards surface

* A symbolic title with Chaucerian overtones. This one-stringed instrument, better known as the 'Marine Trumpet', has clarion qualities well suited for trans-Atlantic communication.

A. L. Leigh Silver writes that he is a 3M man: medicine, music, and maths. Son of a professional organist, he is an Oxford and London educated physician and presently is employed by the 7520 U.S.A.F. Hospital. He is a fellow of the British Medical Association, Fellow of the Inst. of Musical Instrument Technology, and Hon. Fellow Mercator Music Foundation. *Editor.*