THE DISTRIBUTION OF IRREDUCIBLES IN GF[q,x][1]

BY
DAVID R. HAYES

1. **Introduction.** In 1924 Artin [1, pp. 242–246] proved for the ring of polynomials over a finite field the following analog of the prime number theorem for arithmetic progressions:

THEOREM 1.1 (ARTIN). *Let H be a polynomial over a finite field of q elements, and let A be a polynomial prime to H. If $\pi(r; H, A)$ denotes the number of primary irreducibles of degree r which are congruent to A modulo H, then*

$$\pi(r;H,A) = \frac{1}{\Phi(H)} \cdot \frac{q^r}{r} + O\left(\frac{q^{rv}}{r}\right) \tag{1.1}$$

for some $v < 1$.

A primary polynomial is one whose first coefficient is 1, and $\Phi(H)$ is the number of polynomials in a reduced residue system modulo H.

Let M denote the multiplicative semigroup consisting of the primary polynomials in the ring GF[q,x] of polynomials over the finite field of q elements, q being a prime power. An equivalence relation on M is said to be a *congruence relation* if it is compatible with the semigroup structure of M. If $\mathcal{R}_H$ denotes the restriction to M of the relation "congruence modulo H" on GF[q,x], then it is clear that $\mathcal{R}_H$ is a congruence relation on M for every H in GF[q,x]. Our aim in this paper is to establish a result similar to Theorem 1.1 for a wider class of congruence relations on M than those of the special form $\mathcal{R}_H$. To this end, we have extracted the relevant properties of the relations $\mathcal{R}_H$ and used these properties to define a class of congruence relations on M which we call the *arithmetically distributed relations*. The precise definition is given in §8. Theorem 8.1 of that section states a result for arithmetically distributed relations which is analogous to that stated in Theorem 1.1 for the relations $\mathcal{R}_H$. It includes Theorem 1.1 as a special case. The proof given for Theorem 8.1 is similar to that given by Artin for Theorem 1.1 in that certain analytic functions, the L-functions, are introduced and in that the crucial step of the proof lies in showing that these L-functions do not vanish on the line Real(z) = 1. However, the proof differs from that of Artin in

Presented to the Society, August 29, 1963, under the title *The distribution of irreducibles in the ring of polynomials over a finite field*; received by the editors September 3, 1963.

[1] Supported in part by NSF grant G-16485.

several respects and might be thought to be somewhat more natural. The most radical departures involve the use of Theorems 6.2 and 9.2.

Among the corollaries of Theorem 8.1 is Theorem 1.2 below which can be thought of as an extension of Theorem 1.1. Before stating this theorem, we require a definition.

DEFINITION 1.1. Let $B = x^m + \beta_1 x^{m-1} + \cdots + \beta_m$ be a polynomial in M and let s and t be positive integers. The field elements $\beta_1, \cdots, \beta_s$ are called the first s coefficients of B, it being understood that $\beta_i = 0$ if $i > m$. The field elements $\beta_{m-t+1}, \beta_{m-t+2}, \cdots, \beta_m$ are called the last t coefficients of B, it being understood that $\beta_0 = 1$ and that $\beta_i = 0$ if $i < 0$.

THEOREM 1.2. *Let s be a non-negative integer, and let a sequence of s field elements be given. Let H be a polynomial in* GF$[q,x]$, *and let A be a polynomial prime to H. If $\pi(r)$ denotes the number of primary irreducibles in* GF$[q,x]$ *of degree r which* (1) *are congruent to A modulo H and* (2) *have as first s coefficients the given field elements, then*

$$\pi(r) = \frac{1}{q^s\Phi(H)} \cdot \frac{q^r}{r} + O\left(\frac{q^{rv}}{r}\right) \tag{1.2}$$

for some $v < 1$.

In a later paper it will be shown that if $x^q - x$ does not divide H, then (1.2) is valid with $v = \frac{1}{2}$. If in Theorem 1.2 we take $H = x^t$; t being a positive integer, then we obtain the following improvement of a theorem of Uchiyama.

THEOREM 1.3. *Let s first coefficients and t last coefficients be given, and let $\pi(r;s,t)$ be the number of primary irreducibles in* GF$[q,x]$ *of degree r with these first s and last t coefficients. Then if the last coefficient is not zero,*

$$\pi(r;s,t) = \frac{1}{q^{s+t-1}(q-1)} \cdot \frac{q^r}{r} + O\left(\frac{q^{rv}}{r}\right) \tag{1.3}$$

for some $v < 1$.

This theorem was proved by Uchiyama in [7] with the added hypothesis that $p > \max\{s, t-1\}$, p being the prime characteristic of the underlying finite field. We note what appears to be a slight error in Uchiyama's asymptotic formula for $\pi(r; s,t)$. He gives $q^{-(s+t)}(q^r/r)$ instead of $(q^{s+t-1}(q-1))^{-1}(q^r/r)$ as the major term. Previous to Uchiyama's work Carlitz [2] considered the case $s = t = 1$ and proved (falling into the same error as Uchiyama in his statement of the major term) that

$$\pi(r;1,1) = \frac{1}{q(q-1)} \cdot \frac{q^r}{r} + O\left(\frac{q^{r/2}}{r}\right). \tag{1.4}$$

Carlitz's proof involves the introduction of certain L-functions. In §6, we show how (1.4) can be derived in an elementary manner.

§§2–7 introduce the basic definitions and some of the machinery necessary to define arithmetically distributed relations and to prove Theorem 8.1. The definition and some examples of arithmetically distributed relations are given in §8. The remaining sections complete the proof of Theorem 8.1.

2. **Preliminaries.** We begin by recalling several well-known facts concerning the relationship between the finite field of q elements GF(q) and the finite field of q^r elements GF(q^r), r being a positive integer. Lower case Greek letters are used for field elements and capital Roman letters for polynomials.

The finite field GF(q^r) contains one and only one subfield which is isomorphic with GF(q), this subfield being defined as the set of all elements α in GF(q^r) such that $\alpha^q - \alpha = 0$. If GF(q) is identified with this subfield, then GF(q^r) becomes a Galois extension field of GF(q) of degree r. The Galois group of GF(q^r) relative to GF(q) is cyclic and is generated by the automorphism $\sigma: \alpha \rightarrow \alpha^q$. The trace $t^{(r)}(\alpha)$ and the norm $n^{(r)}(\alpha)$ relative to GF(q) of an element α in GF(q^r) may be defined, therefore, by

$$t^{(r)}(\alpha) = \sum_{i=1}^{r} \sigma^i(\alpha) \tag{2.1}$$

and

$$n^{(r)}(\alpha) = \prod_{i=1}^{r} \sigma^i(\alpha), \tag{2.2}$$

respectively. Both of the functions $t^{(r)}$ and $n^{(r)}$ are onto GF(q).

Since GF(q) is a subfield of GF(q^r), the ring GF[q,x] is a subring of the ring GF[q^r,x], and the semigroup M is a subsemigroup of $M^{(r)}$, the semigroup of all primary polynomials in GF[q^r,x]. Every irreducible A in GF[q^r,x] divides a unique primary irreducible in GF[q,x], the division taking place within the structure of the ring GF[q^r,x]. Furthermore [4, p. 33],

THEOREM 2.1. *A primary irreducible P in* GF[q,x] *is the product of g distinct primary irreducibles Q in* GF[q^r,x], *where $g = (r, \deg P)$. The degree of each such irreducible Q is* $\deg P/g$.

DEFINITION 2.1. The automorphism σ of GF(q^r) may be extended to an automorphism of the ring GF[q^r,x] by defining for $A = \alpha_0 x^m + \alpha_1 x^{m-1} + \cdots + \alpha_m$

$$\sigma(A) = \sigma(\alpha_0)x^m + \sigma(\alpha_1)x^{m-1} + \cdots + \sigma(\alpha_m). \tag{2.3}$$

For every A in GF[q^r,x], the polynomial

$$N^{(r)}(A) = \prod_{i=1}^{r} \sigma^i(A) \tag{2.4}$$

is called the *norm* of A relative to $\mathrm{GF}[q,x]$.

THEOREM 2.2. *For every A and B in* $\mathrm{GF}[q^r,x]$, *we have*:
1°. *$N^{(r)}(A)$ is a polynomial in* $\mathrm{GF}[q,x]$.
2°. $N^{(r)}(AB) = N^{(r)}(A) \cdot N^{(r)}(B)$.
3°. *$N^{(r)}(A) = A^r$ if A is in* $\mathrm{GF}[q,x]$.
4°. *If A is irreducible, then $N^{(r)}(A) = n^{(r)}(\alpha) \cdot P^f$, where α is the leading coefficient of A, P is the unique primary irreducible in* $\mathrm{GF}[q,x]$ *which A divides, and $f = r/(r, \deg P)$.*

Proof. The proofs of 1°–3° are straightforward. For the proof of 4°, let $P = A \cdot R$. Then for every integer i,

$$P = \sigma^i(P) = \sigma^i(A \cdot R) = \sigma^i(A) \cdot \sigma^i(R),$$

which shows that $\sigma^i(A)$ divides P in $\mathrm{GF}[q^r,x]$. It follows that $N^{(r)}(A) = \beta P^f$ for some positive integer f and some field element β. It is clear from the definitions that $\beta = n^{(r)}(\alpha)$, where α is the leading coefficient of A. Since $\deg N^{(r)}(A) = r \deg A$ and since by Theorem 2.1 $\deg A = \deg P/(r, \deg P)$, we see that $f = r/(r, \deg P)$. This completes the proof.

THEOREM 2.3. *As α runs through the elements of the field* $\mathrm{GF}(q^r)$, *$N^{(r)}(x + \alpha)$ runs through all those polynomials in $\mathbf{M}$ of the form $P^{r/d}$, where d is a positive integer dividing r and P is an irreducible in $\mathbf{M}$ of degree d. Further, for every irreducible P in $\mathbf{M}$ of degree d dividing r, there are exactly d elements α of the field* $\mathrm{GF}(q^r)$ *for which $N^{(r)}(x + \alpha) = P^{r/d}$.*

Proof. Given α in $\mathrm{GF}(q^r)$, let P be the unique primary irreducible in $\mathrm{GF}[q,x]$ which $x + \alpha$ divides. Let $\deg P = d$. Since a root of P generates a subfield of $\mathrm{GF}(q^r)$ of degree d over $\mathrm{GF}(q)$, d divides r and so $(r, \deg P) = d$. By part 4° of Theorem 2.2, it follows that $N^{(r)}(x + \alpha) = P^{r/d}$.

Given an irreducible P in $\mathbf{M}$ of degree d dividing r, let $-\alpha$ be a root of P in $\mathrm{GF}(q^r)$. Then by part 4° of Theorem 2.2, $N^{(r)}(x + \alpha) = P^{r/d}$. The distinct field elements

$$-\alpha^{q^i} \qquad (0 \leqq i < d) \tag{2.5}$$

are all roots of P in $\mathrm{GF}(q^r)$ so that also $N^{(r)}(x + \alpha^{q^i}) = P^{r/d}$ for these d values of i. Now if $N^{(r)}(x + \beta) = P^{r/d}$, then $x + \beta$ divides P in $\mathrm{GF}[q^r, x]$, and therefore $-\beta$ must be one of the elements (2.5). This completes the proof.

A character Ψ of the multiplicative group $\mathrm{GF}(q)^*$ of the field $\mathrm{GF}(q)$ may be extended as a multiplicative function to the whole field by defining $\Psi(0) = 0$.

Such a multiplicative function is called a *multiplicative character* of GF(q). If Ψ is a multiplicative character of GF(q) and if λ is a character of the additive group of GF(q), then the sum

$$\tau(\Psi,\lambda) = \sum_{\alpha \in \mathrm{GF}(q)} \Psi(\alpha)\lambda(\alpha)$$

is called a *Gauss sum* on GF(q). If both Ψ and λ are principal, then clearly $\tau(\Psi,\lambda) = q - 1$. If one of Ψ and λ is not principal, then we have the well-known elementary bound [3, p. 152]

$$| \tau(\Psi,\lambda) | \leqq q^{1/2}. \tag{2.6}$$

3. **Congruence relations on M.** If two polynomials A and B in M fall in the same equivalence class of a congruence relation $\mathscr{R}$ on M, then we say that A and B are congruent modulo $\mathscr{R}$ and write $A \equiv B \pmod{\mathscr{R}}$. In this notation, the defining property of a congruence relation becomes: If $A \equiv B \pmod{\mathscr{R}}$ then $AC \equiv BC \pmod{\mathscr{R}}$ for every C in M.

DEFINITION 3.1. A polynomial A in M is said to be *invertible modulo* a congruence relation $\mathscr{R}$ if there is a polynomial B in M such that $AB \equiv 1 \pmod{\mathscr{R}}$.

The following properties of invertible polynomials are easily established:

(3.1) If A is invertible modulo $\mathscr{R}$ and if $A \equiv B \pmod{\mathscr{R}}$, then B is invertible modulo $\mathscr{R}$.

(3.2) The product of two invertible polynomials is invertible.

(3.3) If one of A and D is not invertible, then AD is not invertible.

If $A = x^m + \alpha_1 x^{m-1} + \cdots + \alpha_m$ is a polynomial in M, then α_1 and α_m are called, respectively, the first coefficient and the last coefficient of A. When deg $A = 0$, the first coefficient of A is defined to be zero. When deg $A = 1$, the first and last coefficients of A coincide. We define an equivalence relation $\mathscr{C}$ on M as follows: Two polynomials A and B fall in the same equivalence class of $\mathscr{C}$ if and only if A and B both have the same first and the same last coefficient. We shall show that $\mathscr{C}$ is a congruence relation and that the invertible polynomials modulo $\mathscr{C}$ are just those with nonzero last coefficient. Let A, B and C be three polynomials in M with first coefficients α, β, and γ and last coefficients α', β' and γ', respectively. The first coefficient of AC is $\alpha + \gamma$ and that of BC is $\beta + \gamma$, and the last coefficient of AC is $\alpha'\gamma'$ while that of BC is $\beta'\gamma'$. When $\alpha = \beta$ and $\alpha' = \beta'$, therefore, the first and last coefficients of AC and BC are the same. It follows that whenever $A \equiv B \pmod{\mathscr{C}}$ then also $AC \equiv BC \pmod{\mathscr{C}}$. This shows that $\mathscr{C}$ is a congruence relation.

To determine the invertible polynomials modulo $\mathscr{C}$, we observe first that the equivalence class of 1 consists of all those polynomials in M with first coefficient 0 and last coefficient 1. Let A have first coefficient α and last coefficient β. If $\beta \neq 0$ and if $B = x^2 - \alpha x + \beta^{-1}$, then $AB \equiv 1 \pmod{\mathscr{C}}$, which shows that A is invertible modulo $\mathscr{C}$. If $\beta = 0$, then the last coefficient of AB is zero for every polynomial B, so that A cannot be invertible modulo $\mathscr{C}$. This shows that the invertible polynomials modulo $\mathscr{C}$ are just those with nonzero last coefficient.

If $\mathscr{R}$ is a congruence relation on M, then a composition can be defined on $M/\mathscr{R}$, the set of equivalence classes of $\mathscr{R}$, in the familiar way making $M/\mathscr{R}$ a commutative semigroup having as identity element the equivalence class of the polynomial 1. The set $G(\mathscr{R})$ of equivalence classes of the invertible polynomials modulo $\mathscr{R}$ is by (3.1) and (3.2) a subsemigroup of $M/\mathscr{R}$. Since, as is evident from the definitions, every element of $G(\mathscr{R})$ is invertible for the composition induced from $M/\mathscr{R}$, we see that $G(\mathscr{R})$ is a commutative group.

Definition 3.2. When $G(\mathscr{R})$ is finite, we denote its order by $g(\mathscr{R})$.

Definition 3.3. A congruence relation which partitions M into a finite number of equivalence classes is called a *finite* congruence relation.

The group $G(\mathscr{R})$ associated with a finite congruence relation is finite also. We shall show in §6 that when $\mathscr{R}$ is finite, then the characters of $G(\mathscr{R})$ enable us to write down a useful formula for the number of irreducibles of a given degree in a given equivalence class of $\mathscr{R}$.

The relation $\mathscr{C}$ defined above is finite. In fact, since there are exactly q^2 ways of choosing a first and last coefficient for a polynomial, $\mathscr{C}$ partitions M into exactly q^2 equivalence classes. The group $G(\mathscr{C})$ associated with $\mathscr{C}$ is easily seen to be isomorphic with the group consisting of all ordered pairs (α,β) with $\beta \neq 0$ of elements of $\mathrm{GF}(q)$ under the composition $(\alpha,\beta)(\gamma,\delta) = (\alpha + \gamma, \beta\delta)$. Since the order of $G(\mathscr{C})$ is $q(q-1)$, we write $g(\mathscr{C}) = q(q-1)$.

4. **Characters.** Throughout this section, the reader is assumed to be familiar with the theory of the characters of a finite commutative group. An account of this theory may be found, for example, in [5, pp. 33–38].

Definition 4.1. Let $\mathscr{R}$ be a finite congruence relation on M. For every character χ of $G(\mathscr{R})$, we define $\chi^\dagger$ with domain M as follows: If A is invertible modulo $\mathscr{R}$ and if $\mathfrak{c}$ is the equivalence class of A, then $\chi^\dagger(A) = \chi(\mathfrak{c})$; if A is not invertible, then $\chi^\dagger(A) = 0$.

The set of functions $\chi^\dagger$ defined in this way are called the *characters of the relation* $\mathscr{R}$. Since we shall have no occasion in the sequel to use the characters of $G(\mathscr{R})$ directly, we shall for notational convenience abuse language somewhat and write χ instead of $\chi^\dagger$ to indicate the character of the *relation* $\mathscr{R}$ derived from the character χ of the group $G(\mathscr{R})$. Thus we write χ_0 for the character of $\mathscr{R}$ which has the value 1 when A is invertible and the value 0 otherwise.

A character χ of $\mathscr{R}$ has the multiplicative property

$$\chi(AB) = \chi(A)\chi(B) \tag{4.1}$$

for all A and B in M. This is immediate if A and B are invertible modulo $\mathscr{R}$. Otherwise, it follows from (3.3). A character χ of $\mathscr{R}$ also satisfies:

$$\chi(A) = \chi(B) \qquad \text{if } A \equiv B \pmod{\mathscr{R}}; \tag{4.2}$$

$$\chi(1) = 1; \tag{4.3}$$

$$\chi(A) = 0 \qquad \text{if } A \text{ is not invertible modulo } \mathscr{R}. \tag{4.4}$$

Conversely, any complex-valued function χ defined on M which satisfies (4.1)–(4.4) is a character of $\mathscr{R}$. For any such function may be used to define a character of the group $G(\mathscr{R})$ of which it is the associated character of $\mathscr{R}$.

If χ_1 and χ_2 are characters of $\mathscr{R}$, then the function χ defined by $\chi(A) = \chi_1(A)\chi_2(A)$ for A in M satisfies (4.1)–(4.4) and is therefore a character of $\mathscr{R}$. It is easy to verify that the characters of $\mathscr{R}$ with multiplication defined in this way form a group isomorphic to the character group of $G(\mathscr{R})$ and therefore isomorphic to $G(\mathscr{R})$ itself. In particular, there are exactly $g(\mathscr{R})$ characters of $\mathscr{R}$.

DEFINITION 4.2. A set of polynomials in M is called a *representative set modulo* $\mathscr{R}$ if the set contains one and only one polynomial from each equivalence class of $\mathscr{R}$ and a *reduced representative set* if it contains one and only one polynomial from each equivalence class in $G(\mathscr{R})$.

If χ is a character of $\mathscr{R}$, then

$$\frac{1}{g(\mathscr{R})} \sum_F \chi(F) = \begin{cases} 0 & \text{if } \chi \neq \chi_0, \\ 1 & \text{if } \chi = \chi_0, \end{cases} \tag{4.5}$$

F running through either a representative set or a reduced representative set modulo $\mathscr{R}$. We have also, if one of A and B is invertible modulo $\mathscr{R}$,

$$\frac{1}{g(\mathscr{R})} \sum_\chi \chi(A)\bar{\chi}(B) = \begin{cases} 1 & \text{if } A \equiv B \pmod{\mathscr{R}}, \\ 0 & \text{otherwise,} \end{cases} \tag{4.6}$$

χ running through the characters of $\mathscr{R}$. The bar indicates the complex conjugate. Both (4.5) and (4.6) follow immediately from the corresponding properties of the characters of $G(\mathscr{R})$.

The group $G(\mathscr{C})$, as we saw before, is isomorphic with the direct product of the additive group GF(q) with the multiplicative group GF$(q)^*$. Every character χ of $G(\mathscr{C})$, therefore, may be represented as the product of an additive character λ of GF(q) and a multiplicative character Ψ of GF(q). The corresponding character χ of $\mathscr{C}$ is defined as follows: For

$$A = x^m + \alpha_1 x^{m-1} + \cdots + \alpha_m, \qquad \chi(A) = \Psi(\alpha_m)\lambda(\alpha_1).$$

When deg $A = 1$, the first and last coefficients of A coincide. Thus

$$\sum_{\deg A = 1} \chi(A) = \sum_{\alpha \in \mathrm{GF}(q)} \Psi(\alpha)\lambda(\alpha),$$

which we note is a Gauss sum.

5. **Induced relations.** A finite congruence relation on M induces in a natural way a finite congruence relation on $M^{(r)}$.

DEFINITION 5.1. Let $\mathscr{R}$ be a finite congruence relation on M. We define a relation $\mathscr{R}^{(r)}$ on $M^{(r)}$ as follows: For every A and B in $M^{(r)}$, A and B stand in the relation $\mathscr{R}^{(r)}$ if and only if $N^{(r)}(A) \equiv N^{(r)}(B) \pmod{\mathscr{R}}$. The relation $\mathscr{R}^{(r)}$ is said to be the relation *induced* by $\mathscr{R}$ on $M^{(r)}$.

THEOREM 5.1. *The relation $\mathscr{R}^{(r)}$ is a finite congruence relation on $M^{(r)}$. A polynomial A in $M^{(r)}$ is invertible modulo $\mathscr{R}^{(r)}$ if and only if $N^{(r)}(A)$ is invertible modulo $\mathscr{R}$.*

Proof. Suppose $N^{(r)}(A) \equiv N^{(r)}(B) \pmod{\mathscr{R}}$. Then for any C in $M^{(r)}$, $N^{(r)}(A)N^{(r)}(C) \equiv N^{(r)}(B)N^{(r)}(C) \pmod{\mathscr{R}}$, and hence $N^{(r)}(AC) \equiv N^{(r)}(BC) \pmod{\mathscr{R}}$. This proves that $\mathscr{R}^{(r)}$ is a congruence relation. Since for any A in $M^{(r)}$, $N^{(r)}(A)$ falls in one of a finite number of equivalence classes of $\mathscr{R}$, $\mathscr{R}^{(r)}$ is finite, and, in fact, partitions $M^{(r)}$ into a number of equivalence classes which is less than or equal to the number of equivalence classes into which $\mathscr{R}$ partitions M.

To prove the second assertion of the theorem, suppose first that A is invertible modulo $\mathscr{R}^{(r)}$. Choose B so that $AB \equiv 1 \pmod{\mathscr{R}^{(r)}}$. Then $N^{(r)}(A)N^{(r)}(B) = N^{(r)}(AB) \equiv 1 \pmod{\mathscr{R}}$, so that $N^{(r)}(A)$ is invertible modulo $\mathscr{R}$. Suppose next that $N^{(r)}(A)$ is invertible modulo $\mathscr{R}$. Then each of the following congruences implies its successor:

$$\begin{aligned} AB &\equiv AC \pmod{\mathscr{R}^{(r)}}; \quad N^{(r)}(AB) \equiv N^{(r)}(AC) \pmod{\mathscr{R}}; \\ N^{(r)}(A)N^{(r)}(B) &\equiv N^{(r)}(A)N^{(r)}(C) \pmod{\mathscr{R}}; \\ N^{(r)}(B) &\equiv N^{(r)}(C) \pmod{\mathscr{R}}; \quad B \equiv C \pmod{\mathscr{R}^{(r)}}. \end{aligned}$$

It follows from this that AB runs through a representative set modulo $\mathscr{R}^{(r)}$ when B does. Therefore, there is some B such that $AB \equiv 1 \pmod{\mathscr{R}^{(r)}}$. This completes the proof.

DEFINITION 5.2. If χ is a character of the finite congruence relation $\mathscr{R}$, then for every A in $M^{(r)}$, we define $\chi^{(r)}(A) = \chi(N^{(r)}(A))$.

THEOREM 5.2. *For every character χ of $\mathscr{R}$, $\chi^{(r)}$ is a character of $\mathscr{R}^{(r)}$. The map $\chi \to \chi^{(r)}$ is a homomorphism from the character group of $\mathscr{R}$ into the character group of $\mathscr{R}^{(r)}$.*

Proof. To show that $\chi^{(r)}$ is a character of $\mathscr{R}^{(r)}$, we have only to verify properties (4.1)–(4.4). The verification of (4.1)–(4.3) is immediate. To verify (4.4), we observe from Theorem 5.1 that whenever A is not invertible modulo $\mathscr{R}^{(r)}$, then $N^{(r)}(A)$ is not invertible modulo $\mathscr{R}$. Therefore, if A is not invertible modulo $\mathscr{R}^{(r)}$, then $\chi^{(r)}(A) = \chi(N^{(r)}(A)) = 0$. The proof of the homomorphism property is a simple exercise.

6. **A basic formula.** The proof of the main theorem, Theorem 8.1, is based upon formula (6.2) below which expresses the number of irreducibles of a given degree in a given equivalence class of a finite congruence relation $\mathscr{R}$ on $\boldsymbol{M}$ asymptotically as a sum involving the characters of $\mathscr{R}$.

DEFINITION 6.1. Let $\mathscr{R}$ be a finite congruence relation on $\boldsymbol{M}$ and let $A \in \boldsymbol{M}$. Given positive integers r and d such that $d \mid r$, we denote by $\pi(A; r, d)$ the number of irreducibles P in $\boldsymbol{M}$ such that 1° $\deg P = d$ and 2° $P^{r/d} \equiv A \pmod{\mathscr{R}}$.

THEOREM 6.1. *Let A be a polynomial which is invertible modulo the finite congruence relation $\mathscr{R}$ on $\boldsymbol{M}$. Then*

$$\sum_{d \mid r} d \cdot \pi(A; r, d) = \frac{1}{g(\mathscr{R})} \sum_{\chi} \bar{\chi}(A) \sum_{\alpha} \chi^{(r)}(x+\alpha), \tag{6.1}$$

where χ runs through the characters of $\mathscr{R}$ and α runs through the elements of the field GF(q^r).

Proof. By (4.6), for any $K \in \boldsymbol{M}$,

$$\frac{1}{g(\mathscr{R})} \sum_{\chi} \chi(K)\bar{\chi}(A) = \begin{cases} 1 & \text{if } K \equiv A \pmod{\mathscr{R}}, \\ 0 & \text{otherwise.} \end{cases}$$

Therefore, by Theorem 2.3 we have

$$\begin{aligned} \sum_{d \mid r} d \cdot \pi(A; r, d) &= \sum_{d \mid r} d \sum_{\deg P = d} \frac{1}{g(\mathscr{R})} \sum_{\chi} \chi(P^{r/d})\bar{\chi}(A) \\ &= \sum_{\alpha} \frac{1}{g(\mathscr{R})} \sum_{\chi} \chi(N^{(r)}(x+\alpha))\bar{\chi}(A) \\ &= \frac{1}{g(\mathscr{R})} \sum_{\chi} \bar{\chi}(A) \sum_{\alpha} \chi^{(r)}(x+\alpha), \end{aligned}$$

where the polynomials P are primary and irreducible. The formula (6.1) is thus proved.

DEFINITION 6.2. Let $\pi(r; \mathscr{R}, A)$ denote the number of primary irreducibles of degree r which are congruent to A in $\boldsymbol{M}$ modulo the finite congruence relation $\mathscr{R}$.

THEOREM 6.2. *If A is invertible modulo the finite congruence relation $\mathscr{R}$, then*

$$\pi(r; \mathscr{R}, A) = \frac{1}{r \cdot g(\mathscr{R})} \sum_{\chi} \bar{\chi}(A) \sum_{\alpha} \chi^{(r)}(x+\alpha) + O\left(\frac{q^{r/2}}{r}\right), \tag{6.2}$$

where χ runs through the characters of $\mathscr{R}$ and α runs through the elements of GF(q^r).

Proof. We observe first from the definitions that $\pi(r; \mathscr{R}, A) = \pi(A; r, r)$. Secondly, we observe that

$$\sum_{d|r;d<r} d\cdot \pi(A;r,d) = \sum_{d|r;d<r} d\cdot O\left(\frac{q^d}{d}\right) = O\left(\sum_{d|r;d<r} q^d\right) = O\left(q^{r/2} + \sum_{d\leqq r/3} q^d\right)$$

$$= O(q^{r/2}) + O(rq^{r/3}) = O(q^{r/2}).$$

Here we have used the well-known fact that the *total* number of primary irreducibles of degree d in $\mathrm{GF}[q,x]$ is $O(q^d/d)$. The asymptotic formula (6.2) follows from these two observations and (6.1).

If we apply Theorem 6.2 to the relation $\mathscr{C}$ defined in §3, we obtain an asymptotic formula for the number $\pi(r;\gamma,\delta)$ of primary irreducibles of degree r which have for first and last coefficients, respectively, the fixed field elements γ and δ, δ being different from 0. Left in the form (6.2), this formula is not particularly enlightening. We proceed to show how Theorem 6.2 may be used to derive an asymptotic formula for $\pi(r;\gamma,\delta)$ which gives more insight into the nature of this function. This formula was first derived in a different way by Carlitz [2].

First, an estimate is required for the absolute value of the sum

$$\sum_{\alpha\in \mathrm{GF}(q^r)} \chi^{(r)}(x+\alpha), \tag{6.3}$$

when χ is a nonprincipal character of $\mathscr{C}$. From our previous discussion, we know that if $A = x^m + \alpha_1 x^{m-1} + \cdots + \alpha_m$, then $\chi(A) = \Psi(\alpha_m)\lambda(\alpha_1)$ for some multiplicative character Ψ and some additive character λ of $\mathrm{GF}(q)$. Since χ is nonprincipal, at least one of Ψ and λ is nonprincipal. From (2.4) it is evident that the last coefficient of $N^{(r)}(x+\alpha)$ is $n^{(r)}(\alpha)$ and the first coefficient is $t^{(r)}(\alpha)$. Therefore $\chi^{(r)}(x+\alpha) = \Psi(n^{(r)}(\alpha))\cdot\lambda(t^{(r)}(\alpha))$. If we set $\Psi^{(r)}(\alpha) = \Psi(n^{(r)}(\alpha))$ and $\lambda^{(r)}(\alpha) = \lambda(t^{(r)}(\alpha))$, then $\Psi^{(r)}$ is a multiplicative and $\lambda^{(r)}$ is an additive character of $\mathrm{GF}(q^r)$. It follows that (6.3) is a Gauss sum defined on $\mathrm{GF}(q^r)$. Since one of Ψ and λ is nonprincipal and since both $t^{(r)}$ and $n^{(r)}$ are onto, one of $\Psi^{(r)}$ and $\lambda^{(r)}$ is nonprincipal. From the estimate (2.6), therefore, we conclude that

$$\left|\sum_{\alpha\in \mathrm{GF}(q^r)} \chi^{(r)}(x+\alpha)\right| \leqq q^{r/2}. \tag{6.4}$$

Now let $A = x^2 + \gamma x + \delta$. Since $\delta \neq 0$, A is invertible modulo $\mathscr{C}$. By Theorem 6.2 and the estimate (6.4), therefore,

$$\pi(r;\gamma,\delta) = \pi(r;\mathscr{C},A) = \frac{1}{r\cdot g(\mathscr{C})}\sum_{\chi}\bar{\chi}(A)\sum_{\alpha}\chi^{(r)}(x+\alpha) + O\left(\frac{q^{r/2}}{r}\right)$$

$$= \frac{1}{rq(q-1)}\left[\sum_{\alpha}\chi_0^{(r)}(x+\alpha) + \sum_{\chi\neq\chi_0}\bar{\chi}(A)\sum_{\alpha}\chi^{(r)}(x+\alpha)\right] + O\left(\frac{q^{r/2}}{r}\right)$$

$$= \frac{1}{rq(q-1)}\left[q^r - 1 + \sum_{\chi\neq\chi_0} O(q^{r/2})\right] + O\left(\frac{q^{r/2}}{r}\right)$$

$$= \frac{1}{q(q-1)}\cdot\frac{q^r}{r} + O\left(\frac{q^{r/2}}{r}\right).$$

This is the asymptotic formula derived by Carlitz in [2].

7. *L*-functions.

In this and succeeding sections, whenever the symbol $\sum'$ is used in a summation over polynomials, then it is understood that only primary polynomials appear in the summation.

DEFINITION 7.1. The "absolute value" of a polynomial F is defined by

$$|F| = q^{\deg F}. \tag{7.1}$$

The absolute value clearly satisfies the multiplicative property

$$|FG| = |F| \cdot |G| \tag{7.2}$$

for every F and G in $\mathrm{GF}[q,x]$.

DEFINITION 7.2. A complex-valued function χ defined on $\boldsymbol{M}$ is said to be *multiplicative* if

1°. $|\chi(A)|$ is either 0 or 1 for all A in $\boldsymbol{M}$ and

2°. $\chi(AB) = \chi(A)\chi(B)$ for all A and B in $\boldsymbol{M}$.

If χ is a multiplicative function on $\boldsymbol{M}$, then for all complex values s where the series is convergent, we define

$$L(s,\chi) = \sum_{d=0}^{\infty} S_d(\chi) \cdot q^{-ds} \tag{7.3}$$

where

$$S_d(\chi) = \sum_{F;\deg F = d}' \chi(F). \tag{7.4}$$

The function $L(s,\chi)$ is called the L-function associated with χ. Observing the tradition in number theory, we write $s = \sigma + it$, where σ is the real part and t the imaginary part of s. Since clearly

$$|S_d(\chi)| \leqq \sum_{F;\deg F = d}' |\chi(F)| \leqq \sum_{F;\deg F = d}' 1 = q^d, \tag{7.5}$$

we see that the series (7.3) is absolutely convergent when $\sigma > 1$ and uniformly convergent in the half plane $\sigma > 1 + \delta$ for every positive δ. The function $L(s,\chi)$ is therefore defined and analytic in the half plane $\sigma > 1$.

Since

$$\sum_{F;\deg F \leqq r}' \frac{\chi(F)}{|F|^s} = \sum_{d=0}^{r} S_d(\chi) \cdot q^{-ds}, \tag{7.6}$$

the infinite series

$$\sum_F' \frac{\chi(F)}{|F|^s}$$

is absolutely convergent for $\sigma > 1$ when the polynomials F in M are arranged in a sequence by degree. When $\sigma > 1$, therefore, it is immaterial what sequence the polynomials F run through, and we may write without ambiguity

$$L(s,\chi) = \sum_F{}' \frac{\chi(F)}{|F|^s}. \tag{7.7}$$

The infinite product

$$\prod_P \left(1 - \frac{\chi(P)}{|P|^s}\right)^{-1}, \tag{7.8}$$

the product extending over the irreducibles in M, is absolutely convergent in the half plane $\sigma > 1$. Furthermore,

$$L(s,\chi) = \prod_P \left(1 - \frac{\chi(P)}{|P|^s}\right)^{-1} \tag{7.9}$$

for every s in that half plane. The product (7.8) is called the *Euler factorization* of $L(s,\chi)$. The reader who is familiar with the elementary properties of the Riemann-Zeta function will have no difficulty in seeing how the proofs go for the assertions of this paragraph. We therefore omit the details.

We note from the definition (7.3) that the function $L(s,\chi)$ is periodic with period $2\pi i/\log q$.

DEFINITION 7.3. If r is a positive integer and ζ is a complex rth root of unity, we define a complex-valued function η on M as follows:

$$\eta(A) = \zeta^{\deg A}$$

for all A in M.

It is easily verified that such a function η is multiplicative.

For fixed r, there are exactly r different functions η corresponding to the r different rth roots of unity. Under the "pointwise" product, the functions η form a group isomorphic with the group of rth roots of unity. In fact, the map which assigns to each rth root of unity ζ the function η defined by ζ is an isomorphism of these two algebraic structures.

THEOREM 7.1. *If χ is a character of the finite congruence relation $\mathcal{R}$ and if r is a positive integer, then for $\sigma > 1$*

$$L(s,\chi^{(r)}) = \prod_\eta L(s,\eta\chi), \tag{7.10}$$

where in the product η runs through the functions of Definition 7.3.

Proof. By the Euler factorization (7.9), we have for $\sigma > 1$

$$\tag{7.11} \begin{aligned} \prod_{\eta} L(s,\eta\chi) &= \prod_{\eta} \prod_{P} \left(1 - \frac{\eta\chi(P)}{|P|^s}\right)^{-1} \\ &= \prod_{P} \left[\prod_{\eta} \left(1 - \frac{\eta(P)\chi(P)}{|P|^s}\right)\right]^{-1}. \end{aligned}$$

For fixed P, the map $\eta \to \eta(P)$ is a homomorphism from the group of the functions η into the group of rth roots of unity. The image of this map will be the group of fth roots of unity for some f dividing r, and each fth root of unity will be $\eta(P)$ for $g = r/f$ functions η. Thus

$$\begin{aligned} \prod_{\eta} \left(1 - \eta(P)\frac{\chi(P)}{|P|^s}\right) &= \left[\prod_{\zeta} \left(1 - \zeta \frac{\chi(P)}{|P|^s}\right)\right]^g \\ &= \left[1 - \left(\frac{\chi(P)}{|P|^s}\right)^f\right]^g \\ &= \left[1 - \frac{\chi(P^f)}{|P^f|^s}\right]^g, \end{aligned}$$

where in the product, ζ runs through the fth roots of unity. Using this last relation in (7.11), we find that

$$\tag{7.12} \begin{aligned} \prod_{\eta} L(s,\eta\chi) &= \prod_{P} \left(1 - \frac{\chi(P^f)}{|P^f|^s}\right)^{-g} \\ &= \prod_{P} \left(1 - \frac{\chi(P^f)}{q^{fs \cdot \deg P}}\right)^{-g}. \end{aligned}$$

Now, as is evident from the definition of the functions η, the values of f and g associated with a fixed P are given by $f = r/(r, \deg P)$ and $g = (r, \deg P)$. Therefore, by Theorems 2.1 and 2.2,

$$\tag{7.13} \begin{aligned} \prod_{\eta} L(s,\eta\chi) &= \prod_{Q} \left(1 - \frac{\chi(N^{(r)}(Q))}{(q^r)^{s \cdot \deg P/g}}\right)^{-1} \\ &= \prod_{Q} \left(1 - \frac{\chi^{(r)}(Q)}{|Q|^s}\right)^{-1}, \end{aligned}$$

where Q runs through the irrreducibles in $M^{(r)}$. The product on the right in (7.13) is the Euler factorization of $L(s,\chi^{(r)})$. Substituting $L(s,\chi^{(r)})$ for this product, we obtain (7.10). This completes the proof.

8. **Arithmetically distributed relations.** In this section we define the class of finite congruence relations on M which we call the *arithmetically distributed*

relations. The importance of these relations stems from the following theorem, the proof of which we must delay until §10.

THEOREM 8.1. *If $\mathscr{R}$ is arithmetically distributed on M and if A is invertible modulo $\mathscr{R}$, then*

$$\pi(r;\mathscr{R},A) = \frac{1}{g(\mathscr{R})}\cdot\frac{q^r}{r} + O\left(\frac{q^{r\nu}}{r}\right) \tag{8.1}$$

for some $\nu < 1$.

Since there are approximately q^r/r irreducibles of degree r in M, Theorem 8.1 asserts that these irreducibles are "ultimately uniformly divided" among the equivalence classes in $G(\mathscr{R})$. Axioms sufficient to insure this uniform distribution of irreducibles are stated in the following definition.

DEFINITION 8.1. A finite congruence relation $\mathscr{R}$ on M is said to be arithmetically distributed if:

(AD1) Only finitely many irreducibles in M are not invertible modulo $\mathscr{R}$.

(AD2) There is an integer m depending only on $\mathscr{R}$ such that if $r > m$, then the number of primary polynomials of degree r in any one equivalence class of $G(\mathscr{R})$ is the same as the number in any other equivalence class of $G(\mathscr{R})$.

DEFINITION 8.2. Let $\mathscr{R}$ be arithmetically distributed. Then we define $m(\mathscr{R})$ to be the smallest of those non-negative integers m for which the condition of (AD2) holds for $\mathscr{R}$.

The finite congruence relation $\mathscr{C}$ is arithmetically distributed. Every polynomial which is not invertible modulo $\mathscr{C}$ has last coefficient 0 and therefore is divisible by the polynomial x. The only irreducible which is not invertible moduo $\mathscr{C}$ is therefore x itself. To verify that $\mathscr{C}$ satisfies (AD2), we observe that having chosen a first and last coefficient for a polynomial of degree $r \geqq 2$, we may fill in the $r-2$ remaining coefficients in exactly q^{r-2} different ways without altering the equivalence class to which the polynomial belongs modulo $\mathscr{C}$. Thus, if $r > 1$, then each equivalence class modulo $\mathscr{C}$ contains exactly q^{r-2} polynomials of degree r. Since the condition of (AD2) clearly does not hold for $m = 0$ and $\mathscr{R} = \mathscr{C}$, it follows that $m(\mathscr{C}) = 1$.

We proceed now to describe some further examples of arithmetically distributed relations on M. We require the following lemma.

LEMMA 8.2. *Let a polynomial H and a non-negative integer s be given. If $\deg H = h$ and if $r \geqq h + s$, then for any polynomial K and any field elements $\alpha_1,\cdots,\alpha_s$, there are exactly q^{r-h-s} primary polynomials A of degree r such that*

(1) *The first s coefficients of A are respectively $\alpha_1,\cdots,\alpha_s$ and*

(2) *$A \equiv K \pmod{H}$.*

Proof. For the purposes of this proof, a polynomial is said to be *regular* if it is primary and of degree r, has first s coefficients $\alpha_1, \cdots, \alpha_s$ and is congruent to K modulo H. If A is regular, then the polynomials of the form $A + HR$ where $\deg R < r - h - s$ are regular also. Conversely any regular polynomial is necessarily of that form; for such a polynomial is congruent to A modulo H and has the same first s coefficients as A. Thus if there is any regular polynomial at all, then there are exactly q^{r-h-s} regular polynomials. But since every polynomial is congruent modulo H to a polynomial of degree less than h and since $r \geqq h + s$, regular polynomials clearly exist. This completes the proof.

For a fixed polynomial H in $\mathrm{GF}[q,x]$ the relation $\mathscr{R}_H$ ("congruence modulo H") is a finite congruence relation on $\mathbf{M}$. This relation is also arithmetically distributed and provides us with an important example of this class of relations. The polynomials which are not invertible modulo H are those which have a common factor with H. Therefore, an irreducible which is not invertible modulo H is necessarily one of the irreducible divisors of H. Since there are only finitely many such divisors, we have verified (AD1) for this relation. That (AD2) holds is an immediate consequence of Lemma 8.2 with $s = 0$.

DEFINITION 8.3. Given a nonzero polynomial A in $\mathrm{GF}[q,x]$ of degree m, let A^* be the polynomial defined by

$$A^*(x) = x^m \cdot A\left(\frac{1}{x}\right). \tag{8.2}$$

The polynomial A^* is called the *conjugate* of A, and the function which associates with each polynomial its conjugate is called *conjugation.* In order that a conjugate be defined for every polynomial in $\mathrm{GF}[q,x]$, we set $0^* = 0$.

We list below several easily proved properties of the conjugation function.

1°. For every positive integer m, $(x^m)^* = 1$.

2°. If the constant term of A is not zero, then $A^{**} = A$. Further, A^{**} divides A for every A in $\mathrm{GF}[q,x]$.

3°. Conjugation maps $\mathrm{GF}[q,x]$ onto the set of all polynomials in $\mathrm{GF}[q,x]$ with nonzero last coefficient together with the zero polynomial.

4°. For all A and B in $\mathrm{GF}[q,x]$, $(AB)^* = A^*B^*$.

5°. If $\deg A = \deg B$ and if $\omega = \deg A - \deg(A + B)$, then $x^\omega(A + B)^* = A^* + B^*$, and $x^{\omega+1}$ does not divide $A^* + B^*$.

6°. Let H be a polynomial in $\mathrm{GF}[q,x]$ which is not divisible by x. Then for every K in $\mathrm{GF}[q,x]$, H divides K^* if and only if H^* divides K.

DEFINITION 8.4. Given H in $\mathrm{GF}[q,x]$, let $\mathscr{R}_H^*$ be the relation on $\mathbf{M}$ defined as follows: polynomials A and B in $\mathbf{M}$ fall in the same equivalence class of $\mathscr{R}_H^*$ if and only if $A^* \equiv B^* (\operatorname{mod} H)$.

THEOREM 8.3. *For every polynomial H in* $\mathrm{GF}[q,x]$, *$\mathscr{R}_H^*$ is arithmetically distributed.*

Proof. We show first that $\mathscr{R}_H^*$ is a finite congruence relation. Suppose A and B fall in the same equivalence class modulo $\mathscr{R}_H^*$. Then for any C in $\boldsymbol{M}$, we have, since $A^* \equiv B^* \pmod{H}$ that $(CA)^* = C^*A^* \equiv C^*B^* = (CB)^* \pmod{H}$. In other words, for any C in $\boldsymbol{M}$ the polynomials CA and CB fall in the same equivalence class modulo $\mathscr{R}_H^*$. Thus $\mathscr{R}_H^*$ is a congruence relation. Since for any A, A^* falls in one of a finite number of residue classes modulo H, $\mathscr{R}_H^*$ is finite.

Next, we verify (AD1). Suppose A is an irreducible in $\boldsymbol{M}$ which is not invertible modulo $\mathscr{R}_H^*$. Since $AB \equiv 1 \pmod{\mathscr{R}_H^*}$ for no B in $\boldsymbol{M}$, as B runs through a representative set modulo $\mathscr{R}_H^*$, AB does not. Therefore, there are polynomials B and C in $\boldsymbol{M}$ such that $AB \equiv AC \pmod{\mathscr{R}_H^*}$ but $B \not\equiv C \pmod{\mathscr{R}_H^*}$. That is, there are polynomials B and C in $\boldsymbol{M}$ such that $A^*B^* \equiv A^*C^* \pmod{H}$ but $B^* \not\equiv C^*$ $(\bmod H)$. This can happen only when there is a primary irreducible P which divides both A^* and H. Since x does not divide A^*, $P \neq x$. Therefore, by Property 6° of the conjugation function, P^* divides A. Since A is irreducible, therefore, $A = \alpha P^*$ for some field element α. Since only finitely many irreducibles divide H, only finitely many irreducibles are not invertible modulo $\mathscr{R}_H^*$.

Finally, we verify (AD2) for $\mathscr{R}_H^*$. Let $H = x^s H_1$ where s is a non-negative integer and x does not divide H_1. Suppose A and B are polynomials in $\boldsymbol{M}$, each of degree $r \geqq \deg H$. Let $\omega = r - \deg(A-B)$. Then we have, making use of the properties of conjugation listed above, $A \equiv B \pmod{\mathscr{R}_H^*} \leftrightarrow A^* \equiv B^* \pmod{H}$ $\leftrightarrow H \mid (A^* - B^*) \leftrightarrow H \mid x^\omega (A-B)^* \leftrightarrow x^s H_1 \mid x^\omega (A-B)^* \leftrightarrow s \leqq \omega$ and $H_1^* \mid (A-B)$ $\leftrightarrow A$ and B have the same first $s-1$ coefficients and $A \equiv B \pmod{H_1^*}$. If $s = 0$ or 1, this last statement is to be interpreted to mean just $A \equiv B \pmod{H_1^*}$. Now $r \geqq \deg H = \deg H_1 + s = \deg H_1^* + s$. It follows from Lemma 8.2, therefore, that the number of polynomials of degree r which fall in any one equivalence class of $\mathscr{R}_H^*$ is exactly $q^{r - \deg H_1 - s + 1} = q^{r - \deg H + 1}$ if $s \geqq 1$ or exactly $q^{r - \deg H}$ if $s = 0$. These numbers being independent of the equivalence class, we see that (AD2) holds for $\mathscr{R}_H^*$. This completes the proof.

THEOREM 8.4. *Let H in* GF$[q,x]$ *be given. The polynomial A in $\boldsymbol{M}$ is invertible modulo $\mathscr{R}_H^*$ if and only if $(A^*, H) = 1$.*

Proof. Suppose first that $(A^*, H) = 1$. If $AB \equiv AC \pmod{\mathscr{R}_H^*}$, then we have successively: $(AB)^* \equiv (AC)^* \pmod{H}$; $A^*B^* \equiv A^*C^* \pmod{H}$; $B^* \equiv C^* \pmod{H}$; $B \equiv C \pmod{\mathscr{R}_H^*}$. We conclude that AB runs through a representative set modulo $\mathscr{R}_H^*$ when B does. Therefore, there is a polynomial B in $\boldsymbol{M}$ such that $AB \equiv 1 \pmod{\mathscr{R}_H^*}$.

Now suppose that A is invertible modulo $\mathscr{R}_H^*$; that is, suppose there is a B such that $A^*B^* \equiv 1 \pmod{H}$. This clearly implies that $(A^*, H) = 1$. The proof is complete.

Given a positive integer s, we define a relation $\mathscr{R}_{(s)}$ on $\boldsymbol{M}$ as follows: Two polynomials A and B in $\boldsymbol{M}$ fall in the same equivalence class of $\mathscr{R}_{(s)}$ if and only if A and B have the same first s coefficients. If $A = x^m + \alpha_1 x^{m-1} + \cdots + \alpha_m$, then $A^* = 1 + \alpha_1 x + \alpha_2 x^2 + \cdots + \alpha_i x^i$, where i is the last subscript such that $\alpha_i \neq 0$. Hence, if we choose $H = x^{s+1}$, then we have evidently $\mathscr{R}_{(s)} = \mathscr{R}_H^*$. It follows from the previous two theorems, therefore, that $\mathscr{R}_{(s)}$ is arithmetically distributed and that every polynomial is invertible modulo $\mathscr{R}_{(s)}$. The total number of equivalence classes modulo $\mathscr{R}_{(s)}$ is clearly q^s, so that we have $g(\mathscr{R}_{(s)}) = q^s$.

We now investigate the possibility of forming a third arithmetically distributed relation from two given ones.

DEFINITION 8.5. Let $\mathscr{R}_1$ and $\mathscr{R}_2$ be congruence relations on $\boldsymbol{M}$. A new relation $\mathscr{R}$ is defined on $\boldsymbol{M}$ as follows: For all A and B in $\boldsymbol{M}$, A and B fall in the same equivalence class of $\mathscr{R}$ if and only if both $A \equiv B (\operatorname{mod} \mathscr{R}_1)$ and $A \equiv B (\operatorname{mod} \mathscr{R}_2)$. The relation so defined is called the *intersection* of $\mathscr{R}_1$ and $\mathscr{R}_2$.

THEOREM 8.5. *The intersection $\mathscr{R}$ of two congruence relations $\mathscr{R}_1$ and $\mathscr{R}_2$ on $\boldsymbol{M}$ is again a congruence relation on $\boldsymbol{M}$. The set of equivalence classes of $\mathscr{R}$ consists of all nonvacuous intersections of the form $\mathfrak{c} \cap \mathfrak{d}$ where $\mathfrak{c}$ is an equivalence class of $\mathscr{R}_1$ and $\mathfrak{d}$ is an equivalence class of $\mathscr{R}_2$. If $\mathscr{R}_1$ and $\mathscr{R}_2$ are finite and f A in $\boldsymbol{M}$ is invertible modulo both $\mathscr{R}_1$ and $\mathscr{R}_2$, then A is also invertible modulo $\mathscr{R}$.*

The proof is straightforward. We note that Theorem 8.5 implies that the intersection of two finite congruence relations on $\boldsymbol{M}$ is finite also.

DEFINITION 8.6. Two congruence relations $\mathscr{R}_1$ and $\mathscr{R}_2$ are said to be *independent* if for all polynomials B and C in $\boldsymbol{M}$, there is a polynomial A such that $A \equiv B (\operatorname{mod} \mathscr{R}_1)$ and $A \equiv C (\operatorname{mod} \mathscr{R}_2)$. In other words, $\mathscr{R}_1$ and $\mathscr{R}_2$ are independent if an equivalence class of $\mathscr{R}_1$ and an equivalence class of $\mathscr{R}_2$ always have a nonvacuous intersection.

THEOREM 8.6. *Let $\mathscr{R}_1$ and $\mathscr{R}_2$ be independent finite congruence relations on $\boldsymbol{M}$, and let $\mathscr{R}$ be their intersection. Then*:

1°. *$G(\mathscr{R})$ is isomorphic to the direct product of $G(\mathscr{R}_1)$ and $G(\mathscr{R}_2)$.*

2°. *A is invertible modulo $\mathscr{R}$ if and only if A is invertible modulo both $\mathscr{R}_1$ and $\mathscr{R}_2$.*

3°. *The characters of $\mathscr{R}$ are exactly the functions of the form $\chi_1\chi_2$, where χ_1 is a character of R_1 and χ_2 is a character of $\mathscr{R}_2$.*

Proof. The map f: $(\mathfrak{c},\mathfrak{d}) \to \mathfrak{c} \cap \mathfrak{d}$ is by Theorem 8.5 a bijection from the set of ordered pairs $(\mathfrak{c},\mathfrak{d})$, where $\mathfrak{c}$ is an equivalence class of $\mathscr{R}_1$ and $\mathfrak{d}$ is an equivalence class of $\mathscr{R}_2$, onto the equivalence classes of $\mathscr{R}$. We show first that f is also a homomorphism of the semigroup which is the direct product of $\boldsymbol{M}/\mathscr{R}_1$ and $\boldsymbol{M}/\mathscr{R}_2$ and the semigroup $\boldsymbol{M}/\mathscr{R}$. Let $(\mathfrak{c}_1,\mathfrak{d}_1)$ and $(\mathfrak{c}_2,\mathfrak{d}_2)$ be given and choose $A \in \mathfrak{c}_1 \cap \mathfrak{d}_1$ and $B \in \mathfrak{c}_2 \cap \mathfrak{d}_2$. Then

$$\begin{aligned}(\mathfrak{c}_1,\mathfrak{d}_1)\cdot(\mathfrak{c}_2,\mathfrak{d}_2) &= (\mathfrak{c}_1\mathfrak{c}_2,\mathfrak{d}_1\mathfrak{d}_2) = ((AB:\mathscr{R}_1), (AB:\mathscr{R}_2))\\ &\to (AB:\mathscr{R}_1)\cap(AB:\mathscr{R}_2) = (AB:\mathscr{R})\\ &= (A:\mathscr{R})\cdot(B:\mathscr{R}) = (\mathfrak{c}_1\cap\mathfrak{d}_1)\cdot(\mathfrak{c}_2\cap\mathfrak{d}_2),\end{aligned}$$

where $(A:\mathscr{R})$ denotes the equivalence class of A modulo $\mathscr{R}$. The map f is thus an isomorphism of the two semigroups. We note also that the identity element of the direct product semigroup is carried into the equivalence class of $\mathscr{R}$ which contains 1 and therefore into the identity element of $M/\mathscr{R}$.

Let h denote the restriction of f to the subgroup $G(\mathscr{R}_1) \times G(\mathscr{R}_2)$ of $M/\mathscr{R}_1 \times M/\mathscr{R}_2$. Since f is an isomorphism which carries the identity element of the one semigroup into the identity element of the other, the range of h is a subgroup of $G(\mathscr{R})$. On the other hand, for the same reason, if $f(\mathfrak{c},\mathfrak{d})$ is invertible, then so is $(\mathfrak{c},\mathfrak{d})$, i.e., both $\mathfrak{c}$ and $\mathfrak{d}$ are invertible in $M/\mathscr{R}_1$ and $M/\mathscr{R}_2$, respectively. Thus, h is onto $G(\mathscr{R})$, which proves 1°. Both 2° and 3° are easy corollaries of 1°. This completes the proof.

If $\mathscr{R}_1$ and $\mathscr{R}_2$ are arithmetically distributed, then their intersection $\mathscr{R}$ satisfies (AD1). For let $\mathfrak{c}$ be an equivalence class modulo $\mathscr{R}$ which consists of polynomials not invertible modulo $\mathscr{R}$. Choose $\mathfrak{c}_1$ and $\mathfrak{c}_2$, equivalence classes of $\mathscr{R}_1$ and $\mathscr{R}_2$, respectively, such that $\mathfrak{c} = \mathfrak{c}_1 \cap \mathfrak{c}_2$. By the last sentence of Theorem 8.5, one of $\mathfrak{c}_1$ and $\mathfrak{c}_2$ consists of polynomials which are not invertible modulo one of $\mathscr{R}_1$ and $\mathscr{R}_2$. Thus one of $\mathfrak{c}_1$ and $\mathfrak{c}_2$ contains only finitely many irreducibles so that their intersection $\mathfrak{c}$ contains only finitely many irreducibles also. In order to decide whether or not the intersection of two arithmetically distributed relations is arithmetically distributed, therefore, one has only to verify (AD2).

We are now in a position to prove Theorem 1.2. Given a positive integer s and a polynomial H in GF$[q,x]$, let $\mathscr{R}_{(s)H}$ be the intersection of the arithmetically distributed relations $\mathscr{R}_{(s)}$ and $\mathscr{R}_H$. It follows from Lemma 8.2 that $\mathscr{R}_{(s)H}$ satisfies (AD2) and also that the relations $\mathscr{R}_{(s)}$ and $\mathscr{R}_H$ are independent. Since $g(\mathscr{R}_{(s)}) = q^s$ and $g(\mathscr{R}_H) = \Phi(H)$, we see from Theorem 8.6 that $g(\mathscr{R}_{(s)H}) = q^s\Phi(H)$. It follows also from Theorem 8.6 that the invertible polynomials modulo $\mathscr{R}_{(s)H}$ are just those which have no common divisor with H. If we take $\mathscr{R} = \mathscr{R}_{(s)H}$ in Theorem 8.1, therefore, we obtain Theorem 1.2.

9. ***L*-functions of arithmetically distributed relations.** Let $\mathscr{R}$ be arithmetically distributed on M, and let χ be a nonprincipal character of $\mathscr{R}$. By (AD2) the polynomials of degree $d > m(\mathscr{R})$ consist of several copies of a reduced representative set modulo $\mathscr{R}$ together with a few odd noninvertible polynomials. By (4.5), therefore, $S_d(\chi) = 0$ for every $d > m(\mathscr{R})$. We observe from this and the definition (7.3) that when $\chi \neq \chi_0$, then $L(s,\chi)$ is a polynomial function of q^{-s}. It follows at once that $L(s,\chi)$ is defined and analytic in the whole complex plane.

The function $L(s,\chi_0)$ also has a simple form. It follows from (7.9) that for $\sigma > 1$,

$$(9.1) \qquad L(s,\chi_0) = \prod_{Q} \left(1 - \frac{1}{|Q|^s}\right)^{-1},$$

where Q runs through the irreducibles in M which are invertible modulo $\mathscr{R}$. Since by (AD1) only finitely many irreducibles are not invertible modulo $\mathscr{R}$, we conclude from (9.1) that for $\sigma > 1$

$$L(s,\chi_0) = \prod_T \left(1 - \frac{1}{|T|^s}\right) \cdot \prod_P \left(1 - \frac{1}{|P|^s}\right)^{-1},$$

where T runs through the finitely many irreducibles in M which are not invertible modulo $\mathscr{R}$ and P runs through the set of all irreducibles in M. Now, since the function on M which is identically 1 is multiplicative, the Euler factorization of the associated L-function gives

$$\prod_P \left(1 - \frac{1}{|P|^s}\right)^{-1} = \sum_F{}' \frac{1}{|F|^s} = \sum_{d=0}^{\infty} q^{-ds} \sum_{F;\deg F = d}{}' 1 = \sum_{d=0}^{\infty} q^{d(1-s)} = (1 - q^{(1-s)})^{-1}.$$

Therefore, for $\sigma > 1$

$$L(s,\chi_0) = \prod_T \left(1 - \frac{1}{|T|^s}\right) \cdot (1 - q^{(1-s)})^{-1}. \tag{9.2}$$

Since the product over T is finite, (9.2) shows that $L(s,\chi_0)$ can be continued to a function which is meromorphic in the whole complex plane with poles of order 1 at the points

$$s = 1 + 2\pi i r/\log q, \qquad r = 0, \pm 1, \pm 2, \cdots. \tag{9.3}$$

THEOREM 9.1. *If $\mathscr{R}$ is arithmetically distributed on M, then $\mathscr{R}^{(r)}$ is arithmetically distributed on $M^{(r)}$, and $m(\mathscr{R}^{(r)}) = m(\mathscr{R})$. The map $\chi \to \chi^{(r)}$ is an isomorphism of the character group of $\mathscr{R}$ onto the character group of $\mathscr{R}^{(r)}$. Further, the number of irreducibles which are not invertible modulo $\mathscr{R}^{(r)}$ is $O(1)$ as $r \to \infty$.*

Proof. If Q is an irreducible in $M^{(r)}$, then by Theorem 2.2, $N^{(r)}(Q) = P^f$, where P is the unique irreducible of M which is divisible by Q in the ring $\mathrm{GF}[q^r, x]$ and $f = r/(r, \deg P)$. If Q is not invertible modulo $\mathscr{R}^{(r)}$, then P is not invertible modulo $\mathscr{R}$. Otherwise, $N^{(r)}(Q) = P^f$ would be invertible modulo $\mathscr{R}$ in contradiction to Theorem 5.1. Since the number of noninvertible irreducibles in M is finite, the number of divisors of these polynomials in $M^{(r)}$ is finite; and in fact the sum of the degrees of these polynomials is an upper bound for this number. Therefore, we have established (AD1) for $\mathscr{R}^{(r)}$ and also proved the last assertion of the theorem.

If χ is any nonprincipal character of $\mathscr{R}$, then $L(s,\eta\chi)$ is a polynomial in q^{-s} of degree less than or equal to $m(\mathscr{R})$ for every function η (see §7). This follows since

$$S_d(\eta\chi) = \sum_{F;\deg F = d}{}' \eta(F)\chi(F) = \zeta^d S_d(\chi) = 0 \tag{9.4}$$

if $d > m(\mathscr{R})$, for some rth root of unity ζ. The function $L(s, \chi^{(r)})$, being by (7.10) a product of r polynomials in q^{-s} of degree less than or equal to $m(\mathscr{R})$, is itself a polynomial in q^{-s} of degree less than or equal to $r \cdot m(\mathscr{R})$. Comparing coefficients in (7.3), we find that

$$S_d(\chi^{(r)}) = 0 \quad \text{for } d > m(\mathscr{R}). \tag{9.5}$$

If $\chi^{(r)}$ were the principal character of $\mathscr{R}^{(r)}$ for some nonprincipal character χ of $\mathscr{R}$, then (9.5) would imply that every polynomial of degree $d > m(\mathscr{R})$ is not invertible modulo $\mathscr{R}^{(r)}$. But since $\mathscr{R}^{(r)}$ satisfies (AD1), there are infinitely many irreducibles which are invertible modulo $\mathscr{R}^{(r)}$, and therefore there are invertible polynomials of arbitrarily high degree. It follows that $\chi^{(r)}$ is nonprincipal whenever χ is.

Now by Theorem 5.2, the map $\chi \to \chi^{(r)}$ is a homomorphism of the character group of $\mathscr{R}$ into the character group of $\mathscr{R}^{(r)}$. We have just seen in effect that the kernel of this homomorphism consists of χ_0 alone. Since the order of $G(\mathscr{R}^{(r)})$ is less than or equal to that of $G(\mathscr{R})$, it follows that the map $\chi \to \chi^{(r)}$ is onto. Every character of $\mathscr{R}^{(r)}$ is, therefore, $\chi^{(r)}$ for some character χ of $\mathscr{R}$ and $\chi \to \chi^{(r)}$ is an isomorphism.

The verification of (AD2) for $\mathscr{R}^{(r)}$ is now easy. If A is invertible modulo $\mathscr{R}^{(r)}$, then the number of polynomials of degree d in $M^{(r)}$ which are congruent to A modulo $\mathscr{R}^{(r)}$ is, by (4.6) and what we have just proved, equal to

$$\sum_{F \in M^{(r)}; \deg F = d} \frac{1}{g(\mathscr{R}^{(r)})} \sum_{\chi} \bar{\chi}^{(r)}(A) \chi^{(r)}(F), \tag{9.6}$$

where χ runs through the characters of $\mathscr{R}$. Interchanging the summations in (9.6), we find that the number of polynomials in $M^{(r)}$ of degree d and congruent to A modulo $\mathscr{R}$ is

$$\frac{1}{g(\mathscr{R}^{(r)})} \sum_{\chi} \bar{\chi}^{(r)}(A) \cdot S_d(\chi^{(r)}).$$

If $d > m(\mathscr{R})$, then by (9.5) this sum becomes

$$\frac{1}{g(\mathscr{R}^{(r)})} \cdot S_d(\chi_0),$$

which is independent of A. It is evident, therefore, that (AD2) holds for $\mathscr{R}^{(r)}$ and that in fact $m(\mathscr{R}^{(r)}) \leqq m(\mathscr{R})$.

To prove $m(\mathscr{R}) = m(\mathscr{R}^{(r)})$, we note first that we may assume $g(\mathscr{R}) > 1$ since otherwise we have trivially $m(\mathscr{R}) = 0 = m(\mathscr{R}^{(r)})$. When $g(\mathscr{R}) > 1$, there is always a nonprincipal character χ of $\mathscr{R}$ for which

$$S_{m(\mathscr{R})}(\chi) \neq 0. \tag{9.7}$$

When $m(\mathscr{R}) = 0$, this is trivial. If $m(\mathscr{R}) \geqq 1$, the assumption that (9.7) is false for every nonprincipal character of $\mathscr{R}$ leads via the argument of the preceding paragraph to the conclusion that the condition of (AD2) holds with $m = m(\mathscr{R}) - 1$, contradicting the defining property of $m(\mathscr{R})$. Letting χ be a nonprincipal character for which (9.7) holds, therefore, we observe from (9.4) that the r functions $L(s,\eta\chi)$ are all polynomials of degree $m(\mathscr{R})$ in q^{-s}. Therefore, by (7.10) $L(s,\chi^{(r)})$ is a polynomial of degree $r \cdot m(\mathscr{R})$ in q^{-s}, from which we deduce that

$$(9.8) \qquad S_{m(\mathscr{R})}(\chi^{(r)}) \neq 0.$$

This implies that $m(\mathscr{R}^{(r)}) \geqq m(\mathscr{R})$. Combining this inequality with the inequality at the end of the preceding paragraph, we find that $m(\mathscr{R}) = m(\mathscr{R}^{(r)})$. This completes the proof.

Definition 9.1. For every nonprincipal character χ of the arithmetically distributed relation $\mathscr{R}$, set

$$(9.9) \qquad \xi_\chi(z) = \sum_{d=0}^{m(\mathscr{R})} S_d(\chi) \cdot z^{m(\mathscr{R})-d}$$

so that ξ_χ is a polynomial function of z.

Let a run through the $m(\mathscr{R})$ complex roots of ξ_χ so that

$$(9.10) \qquad \xi_\chi(z) = \prod_a (z - a).$$

Then we have, setting $m = m(\mathscr{R})$,

$$(9.11) \qquad L(s,\chi) = \sum_{d=0}^{m} S_d(\chi) \cdot q^{-ds} = q^{-ms} \cdot \xi_\chi(q^s) = \prod_a (1 - a \cdot q^{-s}).$$

Theorem 9.2. *Let $\mathscr{R}$ be arithmetically distributed on* **M**, *and let χ be a nonprincipal character of $\mathscr{R}$. Then for every positive integer r, the roots of $\xi_{\chi^{(r)}}$ are just the rth powers of the roots of ξ_χ.*

Proof. Let $m = m(\mathscr{R}) = m(\mathscr{R}^{(r)})$. We have for every function η

$$L(s,\eta\chi) = \sum_{d=0}^{\infty} S_d(\eta\chi) \cdot q^{-ds} = \sum_{d=0}^{\infty} \zeta^d \cdot S_d(\chi) \cdot q^{-ds}$$

$$= \sum_{d=0}^{m} S_d(\chi) \cdot (\zeta^{-1} q^s)^{-d} = (\zeta q^{-s})^m \cdot \xi_\chi(\zeta^{-1} q^s)$$

for some rth root of unity ζ. Using this result and (9.11) to substitute for $L(s,\chi^{(r)})$ and $L(s,\eta\chi)$ in (7.10), one obtains for $\sigma > 1$

$$(9.12) \qquad q^{-rms} \cdot \xi_{\chi^{(r)}}(q^{rs}) = \prod_\zeta (\zeta q^{-s})^m \xi_\chi(\zeta^{-1} q^s),$$

where ζ runs through the rth roots of unity. Cancelling the factor q^{-rms} from both sides of (9.12), we get for $\sigma > 1$

$$\xi_{\chi^{(r)}}(q^{rs}) = \prod_{\zeta} \zeta^m \cdot \xi_\chi(\zeta^{-1}q^s). \tag{9.13}$$

Since both sides of this equation are polynomials in q^s, and since equality holds for infinitely many values of q^s, we find, replacing q^s by z, that

$$\xi_{\chi^{(r)}}(z^r) = \prod_{\zeta} \zeta^m \cdot \xi_\chi(\zeta^{-1}z) \tag{9.14}$$

for every complex z. Now from (9.10),

$$\prod_{\zeta} \zeta^m \cdot \xi_\chi(\zeta^{-1}z) = \prod_{\zeta} \zeta^m \cdot \prod_{a} (\zeta^{-1}z - a)$$
$$= \prod_{a} \prod_{\zeta} (z - \zeta a) = \prod_{a}(z^r - a^r),$$

where a runs through the m complex roots of ξ_χ. Substituting from this last relation in (9.14) and changing z^r to z, we find that

$$\xi_{\chi^{(r)}}(z) = \prod_{a}(z - a^r),$$

which is what was to be proved.

Definition 9.2. For a given arithmetically distributed relation $\mathcal{R}$ on M, let $a(\mathcal{R})$ denote the set of complex roots of all the L-functions associated with the characters of $\mathcal{R}$, and let $\theta(\mathcal{R})$ denote the least upper bound of the real parts of the numbers in $a(\mathcal{R})$.

Theorem 9.3. *If $\mathcal{R}$ is arithmetically distributed on M and if A is invertible modulo $\mathcal{R}$, then*

$$\pi(r;\mathcal{R},A) = \frac{1}{g(\mathcal{R})} \cdot \frac{q^r}{r} + O\left(\frac{q^{rv}}{r}\right), \tag{9.15}$$

where $v = \max\{\frac{1}{2}, \theta(\mathcal{R})\}$.

Proof. Put $\theta = \theta(\mathcal{R})$ and $m = m(\mathcal{R})$. Let χ be a nonprincipal character modulo $\mathcal{R}$ and for every nonzero root a of ξ_χ, choose $s_0 = \sigma_0 + it_0$ so that $q^{s_0} = a$. Then from (9.11) it is evident that s_0 is a root of $L(s,\chi)$. Therefore, $|a| = |q^{s_0}| = q^{\sigma_0} \leqq q^\theta$ from the definition of $\theta = \theta(\mathcal{R})$. The coefficient $S_1(\chi^{(r)})$ of $\xi_{\chi^{(r)}}$ is the negative of the sum of the roots of $\xi_{\chi(r)}$. Therefore, by Theorem 9.2

$$|S_1(\chi^{(r)})| = \left|\sum_a a^r\right| \leqq \sum_a |a^r| \leqq \sum_a q^{r\theta} = mq^{r\theta}, \tag{9.16}$$

where a runs through the roots of ξ_χ. By Theorem 6.2 and (9.16), we have

$$
\begin{aligned}
\pi(r;\mathscr{R},A) &= \frac{1}{r\cdot g(\mathscr{R})}\left[S_1(\chi_0^{(r)}) + \sum_{\chi;\chi\neq\chi_0} S_1(\chi^{(r)})\right] + O\left(\frac{q^{r/2}}{r}\right) \\
&= \frac{S_1(\chi_0^{(r)})}{r\cdot g(\mathscr{R})} + \sum_{\chi\neq\chi_0} O\left(\frac{q^{r\theta}}{r}\right) + O\left(\frac{q^{r/2}}{r}\right) \qquad (9.17) \\
&= \frac{S_1(\chi_0^{(r)})}{r\cdot g(\mathscr{R})} + O\left(\frac{q^{r\nu}}{r}\right).
\end{aligned}
$$

The number of noninvertible irreducibles in $M^{(r)}$ is by Theorem 9.1 less than a fixed positive constant. Therefore, since first-degree polynomials are irreducible, $S_1(\chi_0^{(r)}) = q^r + O(1)$. Substituting this estimate in (9.17), we arrive at (9.15). This completes the proof.

10. **Nonvanishing of the L-functions on the line $\sigma = 1$.** That the L-functions associated with the characters of a given arithmetically distributed relation $\mathscr{R}$ do not vanish in the half plane $\sigma > 1$ is a simple consequence of the Euler factorization (7.9). We arrive rather easily therefore at the estimate $\theta(\mathscr{R}) \leqq 1$. Unfortunately, this upper bound for $\theta(\mathscr{R})$ is not sufficient to ensure that the asymptotic formula (9.15) gives a meaningful estimate for the function $\pi(r;\mathscr{R},A)$. In this section, the estimate $\theta(\mathscr{R}) \leqq 1$ is improved to $\theta(\mathscr{R}) < 1$, thus providing a proof of Theorem 8.1. The method used is essentially that used in classical number theory in the analytic proof of the prime number theorem for arithmetic progressions. This method was first adapted for use in the arithmetic of polynomials by Kornblum [6] and Artin [1].

THEOREM 10.1 (LANDAU). *For $0 < u < 1$ and any real v,*

$$(1-u)^3|1-ue^{vi}|^4|1-ue^{2vi}|^2 < 1. \qquad (10.1)$$

Proof. Note first that

$$2\cos v + \cos 2v = 2\cos v + 2\cos^2 v - 1 = 2\left(\cos v + \frac{1}{2}\right)^2 - \frac{3}{2} \geqq -\frac{3}{2}.$$

Therefore, since the geometric mean of three positive numbers is less than or equal to their arithmetic mean,

$$
\begin{aligned}
|1-ue^{vi}|^4|1-ue^{2vi}|^2 &= (1-2u\cos v+u^2)^2(1-2u\cos 2v+u^2) \\
&\leqq (1-(2/3)u(2\cos v+\cos 2v)+u^2)^3 \\
&\leqq (1+u+u^2)^3 \\
&< \left(\frac{1}{1-u}\right)^3,
\end{aligned}
$$

which was to be proved.

THEOREM 10.2. *If $\mathcal{R}$ is arithmetically distributed on M and if χ is a character of $\mathcal{R}$, then for $\sigma > 1$ and any real t*

$$L(\sigma,\chi_0)^3|L(\sigma+it,\chi)|^4|L(\sigma+2it,\chi^2)|^2 \geqq 1. \tag{10.2}$$

Proof. In Theorem 10.1 take $u = |P|^{-\sigma}$, where P is a fixed invertible irreducible modulo $\mathcal{R}$ in M. Choose v so that $e^{iv} = \chi(P)\cdot|P|^{-it}$. Then from (10.1)

$$\left(1-\frac{\chi_0(P)}{|P|^{\sigma}}\right)^3\left|1-\frac{\chi(P)}{|P|^{\sigma+it}}\right|^4\left|1-\frac{\chi^2(P)}{|P|^{\sigma+2it}}\right|^2 \leqq 1.$$

This inequality clearly holds also when P is not invertible modulo $\mathcal{R}$. Taking the product of the inverse of the left-hand side of this inequality over all irreducibles P in M, we observe from the Euler factorization (7.9) that

$$(L(\sigma,\chi_0))^3|L(\sigma+it,\chi)|^4|L(\sigma+2it,\chi^2)|^2 \geqq 1,$$

which is what we set out to prove.

THEOREM 10.3. *If either $\chi^2 \neq \chi_0$ or $\chi = \chi_0$, then $L(s,\chi)$ does not vanish on the line $\sigma = 1$. If $\chi^2 = \chi_0$, then $L(s,\chi)$ does not vanish on the line $\sigma = 1$ except possibly at one of the points $s = 1 + k\pi i/\log q$, $k = 0, \pm 1, \pm 2, \cdots$.*

Proof. If $\chi = \chi_0$, then it is evident from (9.2) that any zero of $L(s,\chi)$ must lie on the line $\sigma = 0$. We may assume, therefore, that $\chi \neq \chi_0$. By Theorem 10.2

$$((\sigma-1)L(\sigma,\chi_0))^3\left|\frac{L(\sigma+it,\chi)}{\sigma-1}\right|^4\left|L(\sigma+2it,\chi^2)\right|^2 \geqq \frac{1}{\sigma-1} \tag{10.3}$$

for $\sigma > 1$ and all real values of t. Suppose for a certain value of t that $L(1+it,\chi) = 0$. Letting $\sigma \to 1$ on the left-hand side of (10.3), we find that:

1°. $(\sigma-1)L(\sigma,\chi_0)$ approaches a finite limit since $L(s,\chi_0)$ has a pole of order 1 at the point $s = 1$.

2°. $L(\sigma+it,\chi)/(\sigma-1)$ approaches the finite limit $L'(1+it,\chi)$, $L(s,\chi)$ being analytic in the whole plane.

3°. $L(\sigma+2it,\chi^2)$ approaches a finite limit if $1+2it$ is not a pole of χ^2, i.e., if either $\chi^2 \neq \chi_0$ or else $1+2it$ is not one of the points (9.3). This follows since $L(s,\chi^2)$ is a meromorphic function.

The hypotheses of the theorem, therefore, are enough to ensure that the left-hand side of (10.3) approaches a limiting value as $\sigma \to 1$. The right-hand side of (10.3), however, is clearly unbounded as $\sigma \to 1$. This contradiction establishes the theorem.

THEOREM 10.4. *If $\chi^2 = \chi_0$ but $\chi \neq \chi_0$, then $L(1,\chi) \neq 0$.*

Proof. Consider the complex-valued function f on M defined by

$$f(A) = \sum_{D|A}{}' \chi(D) \tag{10.4}$$

for all A in $\boldsymbol{M}$. If $(A,B) = 1$, then

$$\begin{aligned} f(AB) &= \sum_{D|AB}{}' \chi(D) = \sum_{D_1|A;|D_2|B}{}' \chi(D_1D_2) = \sum_{D_1|A;\,D_2|B}{}' \chi(D_1)\chi(D_2) \\ &= \Big(\sum_{D_1|A}{}' \chi(D_1)\Big)\Big(\sum_{D_2|B}{}'\chi(D_2)\Big) = f(A)\cdot f(B). \end{aligned} \tag{10.5}$$

If P is an irreducible in $\boldsymbol{M}$ and if e is a positive integer, then

$$f(P^e) = \sum_{i=0}^{e} \chi(P^i) = \sum_{i=0}^{e} (\chi(P))^i = \begin{cases} 1 & \text{if } \chi(P) = 0 \\ e+1 & \text{if } \chi(P) = 1 \\ \dfrac{1+(-1)^e}{2} & \text{if } \chi(P) = -1. \end{cases}$$

It follows from (10.5) therefore that $f(A) \geqq 0$ for every A in $\boldsymbol{M}$. Further, if $A = B^2$ so that the exponent of every irreducible in the canonical factorization of A is even, then $f(A) \geqq 1$. Let

$$g(k) = \sum_{A;\deg A = 2k}{}' f(A)$$

for every non-negative integer k. Then

$$g(k) \geqq \sum_{B;\deg B = k}{}' f(B^2) \geqq q^k. \tag{10.6}$$

On the other hand,

$$\begin{aligned} g(k) &= \sum_{A;\deg A = 2k}{}' \sum_{D|A}{}' \chi(D) = \sum_{B,D;\deg BD = 2k}{}' \chi(D) \\ &= \sum_{D;\deg D \leqq 2k}{}' \chi(D) \sum_{B;\deg B = 2k - \deg D}{}' 1 = \sum_{D;\deg D \leqq 2k}{}' \chi(D) q^{2k - \deg D} \\ &= q^{2k} \sum_{d=0}^{2k} q^{-d} \sum_{D;\deg D = d}{}' \chi(D) = q^{2k} \sum_{d=0}^{2k} S_d(\chi) q^{-d} = q^{2k} L(1,\chi) \end{aligned}$$

if $2k \geqq m(\mathscr{R})$. From (10.6), therefore, $L(1,\chi) \geqq q^{-k} > 0$ for $2k \geqq m(\mathscr{R})$. This completes the proof.

THEOREM 10.5. *If $\chi^2 = \chi_0$ but $\chi \neq \chi_0$, then*

$$L(1 - i\pi/\log q, \chi) \neq 0.$$

Proof. Consider the complex-valued function f on $\boldsymbol{M}$ defined by

$$f(A) = \sum_{D|A}{}' (-1)^{\deg D} \chi(D).$$

As in the previous theorem if $(A,B) = 1$, then

$$f(AB) = f(A) f(B). \tag{10.7}$$

If P is an irreducible in M and if e is a positive integer, then

$$f(P^e) = \sum_{i=0}^{e}(-1)^{i\deg P}\chi(P^i) = \sum_{i=0}^{e}((-1)^{\deg P}\chi(P))^i$$

$$= \begin{cases} 1 & \text{if } \chi(P) = 0 \\ e+1 & \text{if } (-1)^{\deg P}\chi(P) = 1 \\ \dfrac{1+(-1)^e}{2} & \text{if } (-1)^{\deg P}\chi(P) = -1. \end{cases}$$

As in the previous theorem, we observe from this and (10.7) that $f(A) \geqq 0$ for all A in M and that $f(A) \geqq 1$ if $A = B^2$. Let

$$g(k) = \sum_{A;\deg A = 2k}{}' f(A)$$

for every non-negative integer k. Then

$$g(k) \geqq \sum_{B\cdot \deg B = k}{}' f(B^2) \geqq q^k. \tag{10.8}$$

On the other hand,

$$g(k) = \sum_{A;\deg A = 2k}{}' \sum_{D|A}{}'(-1)^{\deg D}\chi(D) = \sum_{B,D;\deg BD = 2k}{}' (-1)^{\deg D}\chi(D)$$

$$= \sum_{D;\deg D \leqq 2k}{}' (-1)^{\deg D}\chi(D) \sum_{B;\deg B = 2k - \deg D}{}' 1$$

$$= \sum_{D;\ \deg D \leqq 2k}{}' (-1)^{\deg D}\chi(D)q^{2k-\deg D}$$

$$= q^{2k}\sum_{d=0}^{2k}(-1)^d q^{-d} \sum_{D;\deg D = d}{}' \chi(D) = q^{2k}\sum_{d=0}^{2k} S_d(\chi)q^{-(1-\pi i/\log q)d}$$

$$= q^{2k}L(1-\pi i/\log q, \chi)$$

if $2k \geqq m(\mathscr{R})$. From (10.8) therefore $L(1-\pi i/\log q, \chi) \geqq q^{-k} > 0$ for $2k \geqq m(\mathscr{R})$. This completes the proof.

THEOREM 10.6. *If χ is a character of the arithmetically distributed relation $\mathscr{R}$ on M, then $L(s,\chi) \neq 0$ for any point s on the line $\sigma = 1$.*

Proof. By Theorem 10.3, we may assume that $\chi \neq \chi_0$, that $\chi^2 = \chi_0$, and that $s = 1 + k\pi i/\log q$ for some integer k. Since $L(1,\chi) \neq 0$ by Theorem 10.4 and since $L(s,\chi)$ is periodic with period $2\pi i/\log q$, $L(s,\chi)$ is not zero if k is even. Similarly, since by Theorem 10.5, $L(1-\pi i/\log q, \chi) \neq 0$, $L(s,\chi)$ is not zero when k is odd. Therefore, $L(s,\chi)$ is not zero, and the proof is complete.

THEOREM 10.7. *If $\mathscr{R}$ is arithmetically distributed on $\boldsymbol{M}$, then $\theta(\mathscr{R}) < 1$.*

Proof. If χ is a character of $\mathscr{R}$, then the zeros of $L(s,\chi)$ all lie on a certain finite number of vertical lines in the plane. When $\chi = \chi_0$, this follows from (9.2). When $\chi \neq \chi_0$, it follows from (9.11). The numbers in $a(\mathscr{R})$, therefore, also lie on a certain finite number of vertical lines. We know from the remarks at the beginning of this section and from Theorem 10.6 that all these lines lie to the left of the line $\sigma = 1$. Therefore, since $\theta(\mathscr{R})$ is just the abscissa of that one of these lines which lies farthest to the right, $\theta(\mathscr{R}) < 1$. This completes the proof.

Theorem 8.1 follows readily from this estimate for $\theta(\mathscr{R})$ and Theorem 9.3.

REFERENCES

1. E. Artin, *Quadratische Körper im Gebiete der höheren Kongruenzen.* II, Math. Z. **19** (1924), 207–246.
2. L. Carlitz, *Theorem of Dickson on irreducible polynomials*, Proc. Amer. Math. Soc. **3** (1952), 693–700.
3. H. Davenport and H. Hasse, *Die Nullstellen der Kongruenz zeta funktionen in gewissen zyklischen Fällen*, J. Reine Angew. Math. **172** (1934), 151–182.
4. L. E. Dickson, *Linear groups*, Dover, New York, 1958.
5. E. Hecke, *Vorlesungen über die Theorie der algebraischen Zahlen*, Akademische Verlag, Leipzig, 1923.
6. H. Kornblum, *Über die Primfunktionen in einer arithmetische Progression*, Math. Z. **5** (1919), 100–111.
7. S. Uchiyama, *Sur les polynomes irréductibles dans un corps fini.* II, Proc. Japan Acad. **31** (1955), 267–269.

UNIVERSITY OF TENNESSEE,
KNOXVILLE, TENNESSEE
DUKE UNIVERSITY,
DURHAM, NORTH CAROLINA