[3] O. Perron, *Grundlagen für eine Theorie des Jacobischen Kettenbruchalgorithmus*, Math. Ann. 64 (1907), S. 1-76.

[4] C. Ryll-Nardzewski, *On the ergodic theorems (II)*, Studia Math. 12 (1951), S. 74-79.

[5] S. Saks and St. Banach, *Theory of the Integral*, Warszawa 1937.

[6] F. Schweiger, *Geometrische und elementare metrische Sätze über den Jacobischen Algorithmus*, Sitzungsber. Öst. Akad. Wiss., Mathem.=naturw. Klasse, Abt. II, 173 (1964), S. 59-92.

[7] — *Metrische Sätze über den Jacobischen Algorithmus*, Monatshefte Math. 69 (1965), S. 243-255.

Reçu par la Rédaction le 27. 10. 1965

ACTA ARITHMETICA
XI (1966)

The expression of a polynomial as a sum of three irreducibles*

by

D. R. Hayes (Tennessee)

1. Introduction. Let k be a finite field of q elements, and let $k[x]$ denote its polynomial ring. The leading coefficient of a polynomial M in $k[x]$ is denoted by sgn M. If sgn $M = 1$, the polynomial is said to be *primary*. The "absolute value" of a polynomial A in $k[x]$ is defined by

$$|A| = q^{\deg A}. \tag{1.1}$$

A polynomial A is *even* if it is divisible by an irreducible P such that $|P| = 2$; otherwise, A is *odd*. It is clear that even polynomials can occur only over the finite field of two elements.

According to a famous theorem of Vinogradov, every sufficiently large odd integer can be epxressed as a sum of three primes. In this paper, we prove the following analog of Vinogradov's theorem for the polynomial domain $k[x]$.

Theorem 1.1. *Let M be an odd polynomial in $k[x]$ of sufficiently high degree r (i.e., r is greater than a fixed positive constant which depends only on k). Suppose α, β, and γ are any three non-zero elements of k such that $\alpha+\beta+\gamma = \operatorname{sgn} M$. Then there exist primary irreducibles P_1, P_2, and P_3 in $k[x]$, each of degree r, such that*

$$\alpha P_1+\beta P_2+\gamma P_3 = M. \tag{1.2}$$

The restriction that M be odd is necessary. Consider, for example, the even polynomial $M = x^r$ over the finite field of two elements. We must choose $\alpha = \beta = \gamma = 1$ since there is no other non-zero element of the field. If we were to have $x^r = P_1+P_2+P_3$, then we would have $P_1(0)+P_2(0)+P_3(0) = 0$ upon substituting $x = 0$. Now for $r > 1$, $P_1(0) \neq 0$ since otherwise P_1 would not be irreducible. Hence, $P_1(0) = 1$ and $P_1(0)+P_2(0)+P_3(0) = 1+1+1 = 1 \neq 0$, a contradiction. Thus,

* Supported in part by NSF Grant GP-1632.

there are even polynomials of arbitrarily high degree which cannot be expressed as a sum of three irreducibles of the same degree.

Theorem 1.1 is proved by first deriving an asymptotic formula for the number of representations of a polynomial M in the form (1.2). The asymptotic formula is then used to show that the number of representations becomes infinite as r tends to infinity. One can also let q tend to infinity in this asymptotic formula, obtaining the following result:

THEOREM 1.2. *Suppose k is a finite field with a sufficiently large number of elements (i.e., q is greater than a fixed absolute constant). Then for any odd polynomial M in $k[x]$ and any non-zero field elements α, β, and γ such that $\alpha+\beta+\gamma = \operatorname{sgn} M$, there are primary irreducibles P_1, P_2, and P_3 having the same degree as M such that (1.2) holds.*

There are in the literature two lines of attack upon Vinogradov's theorem. The first line of attack, due to Hardy-Littlewood ([6]) is technically less complicated than the second, which is due to Vinogradov ([11]). However, the Hardy-Littlewood line of attack requires the validity of an as yet unproved hypothesis concerning the location of the zeros of the Dirichlet L-functions. The Vinogradov method is based upon the same idea as that of Hardy-Littlewood but avoids the above mentioned unproved hypothesis by means of a highly ingenious estimate for a certain exponential sum. Both these methods rest heavily on analytic techniques; and the Hardy-Littlewood approach requires in addition the so-called Farey dissection of the unit interval. Excellent expositions of these two lines of attack can be found in [9] and [5] respectively.

The method used in this paper to prove Theorems 1.1 and 1.2 uses a polynomial version of the Hardy-Littlewood line of attack. The rational function field $K = k(x)$ is completed with respect to an appropriate valuation to a field $K_{1/x}$ which, as a complete valued field, provides a suitable analog of the real numbers. The "unit interval" of $K_{1/x}$, i.e., the open ball of radius 1 about 0, turns out to be a compact additive group. Using the Haar integral on this group, one can parallel the Hardy-Littlewood proof rather closely until an analog is required for the Farey dissection. The Farey dissection depends upon the order properties of the real numbers, for which there appears to be no satisfactory analog in the field $K_{1/x}$. Fortunately, there is a "natural dissection" of the unit interval of $K_{1/x}$ which can be used in the proof. However, since this dissection is based upon a different principal (namely that $K_{1/x}$ is rather badly disconnected as a topological space) than is the Farey dissection, the analogy with the Hardy-Littlewood proof breaks down to a certain extent. One finds that, in order to make proper use of this dissection, a more general class of L-functions is required than the strict polynomial analog of the Dirichlet L-functions. (These L-functions are described in Section 5.) For Theorem 1.1, one must have for these L-functions exactly the same hypothesis which is required in the Hardy-Littlewood proof for the Dirichlet L-functions. Thanks to the work of A. Weil, one has at hand even a Riemann hypothesis for these L-functions, which is more than is required. For Theorem 1.2, one must have a somewhat stronger hypothesis than that required for Theorem 1.1; but the full strength of the Riemann hypothesis is still not needed.

It is probable that one could also devise a proof of Theorem 1.1 using the Vinogradov line of attack. Such a proof would presumably avoid the Riemann hypothesis and also the analog of the Farey dissection. However, the use of the Riemann hypothesis in the Hardy-Littlewood method almost certainly leads to a better error term in the asymptotic formula for the number of representations than could be obtained without it. Also, it does not seem likely that the Vinogradov line of attack would lead to a proof of Theorem 1.2.

One might conjecture that every odd polynomial over a finite field can be expressed as a sum of three irreducibles. Theorems 1.1 and 1.2 reduce this conjecture to a finite calculation. Some preliminary investigations seem to indicate that the constants in the asymptotic formula are not so large as to place this calculation beyond the practical limitations of a modern electronic computer.

The author wishes to acknowledge his debt to two papers of Carlitz ([1], [2]) in which a general method for attacking additive problems in the arithmetic of polynomials is developed. This method is essentially equivalent to the method used here. Carlitz second paper contains the idea which led to the "natural dissection" of the unit interval of $K_{1/x}$.

2. Preliminaries. Let $K = k(x)$, the field of rational functions over the finite field k. Elements of k will be denoted usually by lower case Greek letters, and polynomials in $k[x]$ will be denoted by capital Roman letters. On K one has the valuation ν associated with the "infinite prime" of K and defined by

$$\nu(0) = \infty \quad \text{and} \quad \nu(A/B) = \deg B - \deg A \tag{2.1}$$

for every non-zero rational function A/B. The valuation ν has the following easily established properties:

$$\nu(ab) = \nu(a)+\nu(b), \tag{2.2}$$

$$\nu(a+b) \geqslant \min\{\nu(a), \nu(b)\}, \tag{2.3}$$

$$\nu(a) = \infty \text{ if and only if } a = 0 \tag{2.4}$$

for all $a, b \in K$.

Let $K_{1/x}$ denote the completion of K with respect to the valuation v. Then every $a \in K_{1/x}$ can be expanded in a unique way in a convergent "Laurent series" in $1/x$, i.e., in an infinite series of the form

$$a = \sum_{s=-\infty}^{\infty} a_s \left(\frac{1}{x}\right)^s \qquad (a_s \in k) \tag{2.5}$$

where all but a finite number of the coefficients a_s with $s < 0$ are zero. Addition and multiplication of elements of $K_{1/x}$ when written as infinite series are formal. The field $K_{1/x}$, of course, contains K as a subfield. In terms of the representation (2.5), K is just the field of quotients in $K_{1/x}$ of the ring $k[x]$, which is identified in the obvious way with the set of all those elements of $K_{1/x}$ whose Laurent series (2.5) have $a_s = 0$ for all $s > 0$. The extension of the valuation v to $K_{1/x}$ can also be determined in terms of the representation (2.5). If $a \neq 0$, and a has the Laurent expansion (2.5), then

$$v(a) = \text{the smallest } s \text{ such that } a_s \neq 0. \tag{2.6}$$

The properties (2.2)-(2.4) also hold, of course, for the extended valuation. A discussion of completions together with proofs for the assertions of this paragraph can be found in [12], § 1.9.

Given $a \in K_{1/x}$, the "absolute value" of a is defined by

$$|a| = q^{-v(a)}. \tag{2.7}$$

With respect to the metric δ defined by

$$\delta(a, b) = |a-b| \tag{2.8}$$

for all $a, b \in K_{1/x}$, the field $K_{1/x}$ becomes a metric space, which is of course complete by construction. It follows from (2.2) and (2.3) that $K_{1/x}$ is a topological field in the topology induced by this metric. The metric δ is actually an *ultrametric* in the sense of Dieudonné ([4], § 3.8, Ex. 4). Thus if any two open balls in $K_{1/x}$ have a non-vacuous intersection, then one must be contained in the other. From this it follows that any open ball in $K_{1/x}$ is both open and closed in the metric topology. It is easily verified that the set $\mathscr{V}_n(a)$ defined for a given $a \in K_{1/x}$ and a given natural number n by

$$\mathscr{V}_n(a) = \{t \in K_{1/x} \mid v(t-a) > n\} \tag{2.9}$$

is an open ball with center a. Further, the family $\{\mathscr{V}_n(a)\}_{n=0}^{\infty}$ is a base for the family of neighborhoods of a.

Consider now the "unit interval" of $K_{1/x}$; i.e., the set $\mathscr{P}$ defined by

$$\mathscr{P} = \{t \in K_{1/x} \mid v(t) > 0\}. \tag{2.10}$$

The set $\mathscr{P}$ is just the open ball of radius 1 about 0 or, alternatively, the set of all Laurent series (2.5) with $a_s = 0$ for $s < 1$. It is clear from (2.3) that $\mathscr{P}$ is an additive group. Further $\mathscr{P}$ is compact in the relative metric topology and hence is a compact topological group. This result is well known. A proof can be found, for example, in [12], § 1.9. Alternatively, the reader can verify that $\mathscr{P}$ is a closed and totally bounded subset of the complete metric space $K_{1/x}$.

3. The Haar integral and the character E on $\mathscr{P}$. In this section, some calculations are performed which will be used throughout the remainder of the paper. These calculations involve the Haar measure and the Haar integral for the compact additive group $\mathscr{P}$. A rather complete account of the Haar integral can be found in Nachbin ([10]). Actually, for our purposes, little more is required than the existence of a translation invariant (positive) integral for the continuous complex valued functions on $\mathscr{P}$.

DEFINITION 3.1. Let ϱ denote the Haar measure on $\mathscr{P}$ normalized so that $\varrho(\mathscr{P}) = 1$.

DEFINITION 3.2. For a given non-negative integer j, let $\mathscr{P}_j$ denote the set defined by

$$\mathscr{P}_j = \{t \in \mathscr{P} \mid v(t) > j\}. \tag{3.1}$$

In particular, $\mathscr{P}_0 = \mathscr{P}$.

THEOREM 3.1. *For every non-negative j, $\mathscr{P}_j$ is a subgroup of $\mathscr{P}$. Further, each $\mathscr{P}_j$ is open in $\mathscr{P}$, and*

$$\varrho(\mathscr{P}_j) = q^{-j}. \tag{3.2}$$

Proof. Each $\mathscr{P}_j$ is a subgroup by (2.3), and each is open by (2.9). For a given polynomial A of degree less than j, let

$$\mathscr{B}_A = (A/x^j) + \mathscr{P}_j.$$

Then since $\mathscr{B}_A$ is just a translate of $\mathscr{P}_j$, $\mathscr{B}_A$ is open and hence measurable. Further, by the invariance of the Haar measure

$$\varrho(\mathscr{B}_A) = \varrho(\mathscr{P}_j) \tag{3.3}$$

for every such A. We now show that the sets $\{\mathscr{B}_A\}$, where A runs through the polynomials of degree less than j, form a disjoint cover of $\mathscr{P}$. First, disjointness: Suppose $\mathscr{B}_{A_1} \cap \mathscr{B}_{A_2} \neq \emptyset$. Then $(A_1/x^j)+t_1 = (A_2/x^j)+t_2$ for some t_1 and $t_2 \in \mathscr{P}_j$, and hence $(A_1-A_2)/x^j = t_2-t_1 \in \mathscr{P}_j$. From this it follows that $v\big((A_1-A_2)/x^j\big) > j$. But $v\big((A_1-A_2)/x^j\big) = j - \deg(A_1-A_2)$ so that we must have $\deg(A_1-A_2) < 0$ or $A_1 = A_2$.

To show that the sets $\mathscr{B}_A$ cover, we pick an arbitrary $a \in \mathscr{P}$ and write it as a Laurent series (2.5). If we take $A = a_1 x^{j-1} + a_2 x^{j-2} + \ldots + a_j$,

where the a_s's are the coefficients of the Laurent series, then it is clear that $a-(A/x^j)\in\mathscr{P}_j$. Thus $a\in\mathscr{B}_A$ for this A.

Now, since the sets $\{\mathscr{B}_A\}$ constitute a finite disjoint cover of $\mathscr{P}$, we have, by the additivity of the measure, that

$$1=\varrho(\mathscr{P})=\sum_A\varrho(\mathscr{B}_A)=\sum_A\varrho(\mathscr{P}_j)=q^j\varrho(\mathscr{P}_j)$$

by (3.3), as there are exactly q^j polynomials in $k[x]$ of degree less than j. Equation (3.2) follows immediately from this last equality.

COROLLARY 3.2. *Given $a\in\mathscr{P}$, let $\mathscr{B}$ be the open ball about a defined by*

$$\mathscr{B}=\{t\in\mathscr{P}\mid v(t-a)>j\}$$

for a given non-negative integer j. Then

$$\varrho(\mathscr{B})=q^{-j}. \tag{3.4}$$

Proof. It is immediate from the definition that $\mathscr{B}=a+\mathscr{P}_j$. Thus, by the preceding theorem and the invariance of the measure, we have $\varrho(\mathscr{B})=\varrho(\mathscr{P}_j)=q^{-j}$. This completes the proof.

DEFINITION 3.3. Let λ be a fixed non-principal character (into the complex numbers) of the additive group of the finite field k. For every $a\in K_{1/x}$ define $E(a)=E_\lambda(a)$ by

$$E(a)=\lambda(a_1) \tag{3.5}$$

where a_1 is the coefficient of $1/x$ in the Laurent expansion (2.5) of a.

THEOREM 3.3. *The function E is a character of the additive topological group $K_{1/x}$.*

Proof. We must show that E has the homomorphism property

$$E(a+b)=E(a)E(b) \tag{3.6}$$

and that E maps $K_{1/x}$ in a continuous manner onto a subset of the complex numbers. The homomorphism property (3.6) follows from the definition. For the continuity of E, it suffices to show that $E^{-1}(z)$ is open for every complex z in the range of E. Therefore, let z be a fixed element of the range of E, and suppose $a\in E^{-1}(z)$. Then the set $\mathscr{V}=\{t\in K_{1/x}\mid v(t-a)>1\}$ is a neighborhood of a. From the definitions, it is clear that the coefficients of $1/x$ in the Laurent expansions of t and a are equal if $t\in\mathscr{V}$. Thus $E(t)=E(a)=z$ for every $t\in\mathscr{V}$ by the definition of E; and hence $\mathscr{V}\subseteq E^{-1}(z)$. Since, therefore, $E^{-1}(z)$ contains a neighborhood of each of its points, $E^{-1}(z)$ is open. This completes the proof.

THEOREM 3.4. *For every A, B and H in $k[x]$, we have*

$$E(A)=1 \tag{3.7}$$

and

$$E(A/H)=E(B/H) \quad \text{if} \quad A\equiv B\ (\mathrm{mod}\ H). \tag{3.8}$$

Proof. Since the coefficient of $1/x$ in the Laurent expansion of A is zero, $E(A)=\lambda(0)=1$. If $A\equiv B\ (\mathrm{mod}\ H)$, then $A=B+RH$ for some $R\in k[x]$. Thus

$$E(A/H)=E\big((B+RH)/H\big)=E\big((B/H)+R\big)=E(B/H)E(R)=E(B/H).$$

This completes the proof.

If $\mathscr{B}$ is a ϱ-measurable subset of $\mathscr{P}$ and if $X_{\mathscr{B}}$ is the characteristic function of $\mathscr{B}$, then we define

$$\int_{\mathscr{B}}f(t)\,d\varrho=\int f(t)X_{\mathscr{B}}(t)\,d\varrho, \tag{3.9}$$

for every continuous function f on $\mathscr{B}$. Of course, the integral on the right is the Haar integral on $\mathscr{P}$.

THEOREM 3.5. *Let $a\in K_{1/x}$. Then*

$$\int_{\mathscr{P}_j}E(at)\,d\varrho=\begin{cases}q^{-j} & \text{if} \quad v(a)>-j,\\ 0 & \text{otherwise.}\end{cases} \tag{3.10}$$

Proof. If $v(a)>-j$, then $v(at)=v(a)+v(t)\geqslant v(a)+j+1>-j+j+1=1$ for every $t\in\mathscr{P}_j$. Hence, the coefficient of $1/x$ in the Laurent expansion of at is zero; and therefore $E(at)=1$, for all $t\in\mathscr{P}_j$. Thus

$$\int_{\mathscr{P}_j}E(at)\,d\varrho=\int X_{\mathscr{P}_j}(t)\,d\varrho=\varrho(\mathscr{P}_j)=q^{-j}$$

by Theorem 3.1. If $v(a)\leqslant -j$, then $-v(a)\geqslant j$. Let β be the coefficient of $(1/x)^{v(a)}$ in the Laurent expansion of a. Then β is non-zero by (2.6). If $d=-v(a)$, then $d+1\geqslant j+1>j$ so that $x^{-d-1}\in\mathscr{P}_j$. Therefore, we have

$$\begin{aligned}\int_{\mathscr{P}_j}E(at)\,d\varrho&=\int E(at)X_{\mathscr{P}_j}(t)\,d\varrho=\int E\big(a(t+\alpha x^{-d-1})\big)X_{\mathscr{P}_j}(t+\alpha x^{-d-1})\,d\varrho\\&=\int\lambda(\alpha\beta)E(at)X_{\mathscr{P}_j}(t)\,d\varrho=\lambda(\alpha\beta)\int_{\mathscr{P}_j}E(at)\,d\varrho\end{aligned}$$

for every $\alpha\in k$. Here we have used the invariance of the Haar integral, the fact that $\mathscr{P}_j$ is a subgroup, and the definition of $E=E_\lambda$. Thus,

$$\big(1-\lambda(\alpha\beta)\big)\int_{\mathscr{P}_j}E(at)\,d\varrho=0$$

for every $a \in k$. But, since λ is non-principal and $\beta \neq 0$, $\lambda(a\beta) \neq 1$ for some $a \in k$. Hence, the value of the integral must be zero.

THEOREM 3.6. *Let* $\mathscr{B} = \{t \in \mathscr{P} \mid \nu(t-b) > j\}$, *where* $b \in \mathscr{P}$, *and* j *is a non-negative integer. Then for any* $a \in K_{1/x}$, *we have*

$$\int_{\mathscr{B}} E(at)\,d\varrho = \begin{cases} q^{-j}E(ab) & \text{if} \quad \nu(a) > -j, \\ 0 & \text{otherwise.} \end{cases} \tag{3.11}$$

Proof. We have

$$\int_{\mathscr{B}} E(at)\,d\varrho = \int E(at)X_{\mathscr{B}}(t)\,d\varrho = \int E\big(a(t+b)\big)X_{\mathscr{B}}(t+b)\,d\varrho$$

$$= \int E(at)E(ab)X_{\mathscr{P}_j}(t)\,d\varrho = E(ab)\int_{\mathscr{P}_j} E(at)\,d\varrho,$$

since clearly $\mathscr{P}_j = b + \mathscr{B}$ and by the invariance of the integral. The result now follows from Theorem 3.5.

We adopt the following convention: Whenever the symbol $\sum'$ is used in a summation over polynomials, it is understood that only primary polynomials appear in the summation. For example, the summation in the following theorem is over all primary polynomials of degree s.

THEOREM 3.7. *Suppose* $a \in \mathscr{P}$. *Then for every positive integer* s, *we have*

$$\sum_{\deg B = s}{}' E(Ba) = \begin{cases} q^{s}E(x^{s}a) & \text{if} \quad \nu(a) > s, \\ 0 & \text{otherwise.} \end{cases} \tag{3.12}$$

Proof. Since $\nu(x^{s+1}a) = \nu(x^{s+1}) + \nu(a) = -(s+1) + \nu(a) > -(s+1)$, we know by Theorem 3.6 that

$$E(Ba) = q^{s+1}\int_{\mathscr{B}} E(x^{s+1}at)\,d\varrho,$$

where $\mathscr{B} = \{t \in \mathscr{P} \mid \nu\big(t-(B/x^{s+1})\big) > s+1\}$. As in the proof of Theorem 3.1, one can show that the sets $\mathscr{B}$ defined by the various primary polynomials B of degree s are pairwise disjoint and cover the set $\mathscr{V} = \{t \in \mathscr{P} \mid \nu(t-x^{-1}) > 1\}$. Thus,

$$\sum_{\deg B = s}{}' E(Ba) = q^{s+1}\sum_{\deg B = s}{}' \int_{\mathscr{B}} E(x^{s+1}at)\,d\varrho = q^{s+1}\int_{\mathscr{V}} E(x^{s+1}at)\,d\varrho.$$

If $\nu(a) > s$, then $\nu(x^{s+1}a) > -1$; and so the last integral above has the value $q^{-1}E(x^{s}a)$ by Theorem 3.6. If $\nu(a)$ is not greater than s, then this last integral has the value 0, again by Theorem 3.6. Thus, the value of the sum in question is given by (3.12).

4. Dissection of the "unit interval" $\mathscr{P}$. Theorem 3.5 of the preceding section allows one to write down a useful formula for the number of representations of a polynomial M in the form (1.2). For the remainder of the paper, M is a fixed odd polynomial of degree r, and α, β, and γ are fixed non-zero elements of k such that $\alpha+\beta+\gamma = \operatorname{sgn} M$.

DEFINITION 4.1. Let $\boldsymbol{N}(M)$ denote the number of triples of primary irreducibles P_1, P_2, and P_3, each of degree r, such that $\alpha P_1 + \beta P_2 + \gamma P_3 = M$.

DEFINITION 4.2. For all $t \in \mathscr{P}$, let

$$f(t) = \sum_{\deg P = r}{}' E(Pt), \tag{4.1}$$

where the summation is over the primary irreducibles in $k[x]$ of degree r.

THEOREM 4.1. *We have*

$$\boldsymbol{N}(M) = \int f(at)f(\beta t)f(\gamma t)E(-Mt)\,d\varrho. \tag{4.2}$$

Proof. From the above definitions,

$$f(at)f(\beta t)f(\gamma t) = \sum_{P_1,P_2,P_3}{}' E\big((\alpha P_1 + \beta P_2 + \gamma P_3)t\big),$$

where P_1, P_2, and P_3 run independently over the primary irreducibles of degree r. Hence,

$$\int f(at)f(\beta t)f(\gamma t)E(-Mt)\,d\varrho = \int \sum_{P_1,P_2,P_3}{}' E\big((\alpha P_1 + \beta P_2 + \gamma P_3 - M)t\big)\,d\varrho$$

$$= \sum_{P_1,P_2,P_3}{}' \int E\big((\alpha P_1 + \beta P_2 + \gamma P_3 - M)t\big)\,d\varrho$$

$$= \sum_{\substack{P_1,P_2,P_3 \\ \alpha P_1 + \beta P_2 + \gamma P_3 = M}}{}' 1 = \boldsymbol{N}(M)$$

by Theorem 3.5, since $\nu(\alpha P_1 + \beta P_2 + \gamma P_3 - M) > 0$ if and only if $\alpha P_1 + \beta P_2 + \gamma P_3 - M = 0$. This completes the proof.

In the Hardy-Littlewood line of attack on the number-theoretic version of Theorem 1.1, the function corresponding to $f(t)$ is estimated on certain subarcs of a circle in the complex plane. These subarcs are determined by the so-called Farey dissection of the unit interval. Following Hardy-Littlewood, we will attempt to dissect the "unit interval" $\mathscr{P}$ into a collection of disjoint open sets on each of which a good "analytic" estimate for $f(t)$ can be obtained. The remainder of this section is devoted to a description of such a dissection of $\mathscr{P}$.

DEFINITION 4.3. A rational function G/H in $k(x)$ is called *primordial* (relative to r), if it satisfies the following conditions:

1) $G/H \in \mathscr{P}$; i.e., $\deg G < \deg H$.

2) G/H is in reduced form, i.e., $(G, H) = 1$.

3) H is primary.

4) $\deg H \leqslant r/2$.

DEFINITION 4.4. We set $w = [r/2]$, the greatest integer which is less than or equal to $r/2$.

We shall need the following lemma, which is due to Carlitz ([2], Eq. (3.11)).

LEMMA 4.2. *Suppose $0 \leqslant h \leqslant w$. Then the number N_h of primordial rational functions G/H such that $\deg H = h$ is given by*

$$N_h = \begin{cases} 1 & \text{if} \quad h = 0, \\ q^{2h} - q^{2h-1} & \text{otherwise.} \end{cases} \tag{4.3}$$

DEFINITION 4.5. If G/H is primordial, then we set

$$\mathscr{U}_{G/H} = \{t \in \mathscr{P} \mid v(t - (G/H)) > h + w\} \tag{4.4}$$

where $h = \deg H$. We call $\mathscr{U}_{G/H}$ a *primordial subset of* $\mathscr{P}$.

THEOREM 4.3. *The collection $\{\mathscr{U}_{G/H}\}$ of primordial subsets of $\mathscr{P}$ forms a disjoint open cover of $\mathscr{P}$.*

Proof. We show first that the sets $\mathscr{U}_{G/H}$ are pairwise disjoint. Suppose that $\mathscr{U}_{G/H}$ and $\mathscr{U}_{G'/H'}$ have a non-void intersection, where of course both G/H and G'/H' are primordial. Then, since both these sets are open balls in $\mathscr{P}$ by (2.9), one must be contained in the other as $\mathscr{P}$ is an ultra-metric space. We may suppose that $\mathscr{U}_{G'/H'} \subseteq \mathscr{U}_{G/H}$. Then in particular $G'/H' \in \mathscr{U}_{G/H}$, and hence by definition 4.5,

$$v\left(\frac{G'}{H'} - \frac{G}{H}\right) > h + w,$$

where $h = \deg H$. Thus, $h + w < v((G'H - GH')/HH') = \deg(HH') - \deg(G'H - GH') = h + \deg H' - \deg(G'H - GH')$, or

$$\deg(G'H - GH') < \deg H' - w. \tag{4.5}$$

But $\deg H' \leqslant w$ since G'/H' is primordial, and hence from (4.5) we learn that $\deg(G'H - GH') < 0$. Thus, $G'H - GH' = 0$, or $G'/H' = G/H$. It follows that the sets are pairwise disjoint.

Now let $\mathscr{V} = \bigcup \{\mathscr{U}_{G/H}\}$. We wish to show that $\mathscr{V} = \mathscr{P}$. By Corollary 3.2, $\varrho(\mathscr{U}_{G/H}) = q^{-h-w}$ for every primordial G/H. Therefore, since the sets $\mathscr{U}_{G/H}$ are pairwise disjoint, we have

$$\begin{aligned} \varrho(\mathscr{V}) &= \sum_{G/H} \varrho(\mathscr{U}_{G/H}) = \sum_{h=0}^{w} \Big(\sum_{\substack{G/H \\ \deg H = h}} \varrho(\mathscr{U}_{G/H}) \Big) \\ &= \sum_{h=0}^{w} N_h q^{-w-h} = q^{-w} + \sum_{h=1}^{w} (q^{2h} - q^{2h-1}) q^{-w-h} \\ &= q^{-w} + q^{-w} \sum_{h=1}^{w} (q^h - q^{h-1}) = q^{-w} + q^{-w}(q^w - 1) = 1, \end{aligned}$$

where the first summation above is over all primordial G/H. We have, of course, used the value of N_h given by (4.3). From the preceding calculation, it follows that $\mathscr{P} \setminus \mathscr{V}$ is a null-set. But, each $\mathscr{U}_{G/H}$ is closed in $\mathscr{P}$ since $\mathscr{P}$ is an ultrametric space, and hence $\mathscr{P} \setminus \mathscr{V}$ is open. If $\mathscr{P} \setminus \mathscr{V}$ were not empty, then it would contain an open ball and hence would have positive measure by Corollary 3.2. Since it has measure zero, it must be empty, and thus $\mathscr{P} = \mathscr{V}$. This completes the proof.

5. Estimate for $f(t)$ on $\mathscr{U}_{G/H}$. Our principal aim in this section is to derive the estimate (5.7) below, which gives a reasonably good, "analytic" approximation to the function $f(t)$ on any one of the sets $\mathscr{U}_{G/H}$.

DEFINITION 5.1. Let $\boldsymbol{M}$ denote the multiplicative semigroup of all primary polynomials in $k[x]$.

DEFINITION 5.2. Let $B = x^m + \beta_1 x^{m-1} + \ldots + \beta_m$ be a polynomial in $\boldsymbol{M}$, and let s be a non-negative integer. The sequence of field elements $\beta_1, \ldots, \beta_s$ is called the first s coefficients of B, it being understood that $\beta_i = 0$ if $i > m$.

DEFINITION 5.3. Given a non-negative integer s and a polynomial $H \in k[x]$, we define an equivalence relation $\mathscr{R}_{(s)H}$ on $\boldsymbol{M}$ as follows: polynomials A and B in $\boldsymbol{M}$ fall in the same equivalence class of $\mathscr{R}_{(s)H}$ if 1) A and B have the same first s coefficients and 2) $A \equiv B \pmod{H}$.

In [7], § 8, it is shown that each relation $\mathscr{R}_{(s)H}$ is a finite congruence relation on $\boldsymbol{M}$, i.e., a relation which is compatible with the semigroup structure of $\boldsymbol{M}$ and which partitions $\boldsymbol{M}$ into a finite number of equivalence classes. Further, with each character χ of $\mathscr{R}_{(s)H}$ ([7], § 4), we have the associated L-function ([7], § 7), which is a function of a complex variable defined and meromorphic in the whole complex plane ([7], § 8 and 9).

DEFINITION 5.4. Let Θ^* denote the least upper bound of the real parts of the zeros of all the L-functions associated with the relations of the form $\mathscr{R}_{(s)H}$; and let $\Theta = \max\{1/2, \Theta^*\}$.

For the remainder of this section, H is a fixed polynomial in $\boldsymbol{M}$ such that $h = \deg H \leqslant r/2$. The value of s is fixed by $s = r-w-h$. For notational convenience, we introduce the abbreviation $\mathscr{R} = \mathscr{R}_{(s)H}$.

THEOREM 5.1. *If χ is a non-principal character of $\mathscr{R}$, then*

$$\left|\sum_{\deg P=r}{}' \chi(P)\right| < q^{\Theta r}, \tag{5.1}$$

where P runs through the primary irreducibles of degree r.

Proof. By [7], Theorem 2.3, we have

$$\sum_{d|r} d \sum_{\deg P=d}{}' \chi(P^{r/d}) = \sum_{a\epsilon k^{(r)}} \chi^{(r)}(x+a), \tag{5.2}$$

where $k^{(r)}$ is an algebraic extension of k of degree r, $\chi^{(r)}$ is a character of the induced relation ([7], § 5), and P is irreducible. As in the proof ([7], Theorem 9.3), we have

$$\left|\sum_{a} \chi^{(r)}(x+a)\right| \leqslant (s+h-1)q^{\Theta r} < (r/2)q^{\Theta r} \tag{5.3}$$

since $s+h-1 = r-w-1 < r/2$. It is well known that the number of primary irreducibles of degree d in $k[x]$ is less than or equal to q^d/d. Therefore,

$$\left|\sum_{\substack{d|r\\ d<r}} d \sum_{\deg P=d}{}' \chi(P)\right| \leqslant \sum_{\substack{d|r\\ d<r}} d \sum_{\deg P=d}{}' 1 \leqslant \sum_{\substack{d|r\\ d<r}} q^d \leqslant (r/2)q^{r/2}. \tag{5.4}$$

Using the estimates (5.3) and (5.4) in (5.2), we arrive at (5.1). This completes the proof.

LEMMA 5.2. *Suppose $t \epsilon \mathscr{U}_{G/H}$ for some G such that G/H is primordial. If A and B are polynomials of degree r in $\boldsymbol{M}$ such that $A \equiv B \pmod{\mathscr{R}}$, then*

$$E(At) = E(Bt). \tag{5.5}$$

Proof. It suffices to show that $E\big((A-B)t\big) = 1$. Since $A \equiv B \pmod{H}$, $E\big((A-B)G/H\big) = 1$. Therefore,

$$E\big((A-B)t\big) = E\big((A-B)(t-G/H)\big)\, E\big((A-B)G/H\big) = E\big((A-B)(t-G/H)\big).$$

Now $\deg(A-B) \leqslant r-s-1$ since A and B have the same first s coefficients. Hence, $\nu(A-B) = -\deg(A-B) \geqslant s+1-r$. Also, $\nu(t-G/H) > > h+w$ as $t \epsilon \mathscr{U}_{G/H}$. Thus, we have $\nu\big((A-B)(t-G/H)\big) = \nu(A-B)+ +\nu(t-G/H) > (s+1-r)+(w+h) = 1$ since $s = r-w-h$. But this implies that the coefficient of $1/x$ in the Laurent expansion of $(A-B)(t-G/H)$ is 0, which means that $E\big((A-B)(t-G/H)\big) = \lambda(0) = 1$. This completes the proof.

By a representative set (reduced representative set) modulo $\mathscr{R}$ we mean a set of polynomials in $\boldsymbol{M}$ which contains exactly one polynomial from each equivalence class (invertible equivalence class ([7], § 3)) of $\mathscr{R}$. Since $r \geqslant s+h = r-w$, it follows from [7], Lemma 8.2, that a representative set (reduced representative set) can be chosen from among the primary polynomials of degree r. This justifies the following definition.

DEFINITION 5.5. Let $\mathscr{W}_H = \bigcup_G \mathscr{U}_{G/H}$, where G runs through all those polynomials such that G/H is primordial. Then for every $t \epsilon \mathscr{W}_H$, we set

$$T_H(t) = \sum_{A}{}' E(At) \tag{5.6}$$

where A runs through a reduced representative set modulo $\mathscr{R}$ chosen from among the primary polynomials of degree r. By Lemma 5.2 above, the value of $T_H(t)$ is independent of the particular reduced representative set used to define it.

THEOREM 5.3. *If $t \epsilon \mathscr{W}_H$, then*

$$\left|f(t) - \frac{1}{q^s \Phi(H)} \cdot \frac{q^r}{r} \cdot T_H(t)\right| < 2q^{1/4}\, q^{(1/4+\Theta)r}, \tag{5.7}$$

where $\Phi(H)$ is the number of polynomials in a reduced residue system modulo H.

Proof. Let A run through a particular reduced representative set modulo $\mathscr{R}$ chosen from among the primary polynomials of degree r. Since $h \leqslant w < r$, every irreducible of degree r is invertible modulo $\mathscr{R}$ by the last paragraph of [7], § 8. From this it follows that every irreducible P of degree r is congruent to some one of the polynomials A modulo $\mathscr{R}$. Thus, we have

$$f(t) = \sum_{\deg P=r}{}' E(Pt) = \sum_{A}{}' \sum_{P \equiv A \pmod{\mathscr{R}}}{}' E(Pt) = \sum_{A}{}' E(At) \sum_{P \equiv A \pmod{\mathscr{R}}}{}' 1, \tag{5.8}$$

using Lemma 5.2 to obtain the last equality. According to [7], § 4 and the last paragraph of [7], § 8, for every P we have

$$\big(1/q^s \Phi(H)\big) \sum_{\chi} \bar{\chi}(A)\chi(P) = \begin{cases} 1 & \text{if} \quad P \equiv A \pmod{\mathscr{R}}, \\ 0 & \text{otherwise}, \end{cases} \tag{5.9}$$

where χ runs through the characters of $\mathscr{R}$. Thus, (5.8) implies that

$$\begin{aligned} f(t) &= \sum_{A}{}' E(At) \sum_{P}{}' \big(1/q^s \Phi(H)\big) \sum_{\chi} \bar{\chi}(A)\chi(P) \\ &= \big(1/q^s \Phi(H)\big) \sum_{\chi} \Big(\sum_{A}{}' \bar{\chi}(A) E(At)\Big) \Big(\sum_{P}{}' \chi(P)\Big), \end{aligned} \tag{5.10}$$

where P runs through the primary irreducibles of degree r. If $\psi(r)$ denotes the total number of irreducibles in $\boldsymbol{M}$ of degree r, then since every such irreducible is invertible modulo $\mathscr{R}$, we have

$$\psi(r) = \sum_{\deg P = r}{}' \chi_0(P), \tag{5.11}$$

where χ_0 is the principal character of $\mathscr{R}$. Thus, (5.10) implies that

$$f(t) = \big(\psi(r)/q^s\Phi(H)\big)\sum_{A}{}' \chi_0(A)E(At) + \\ + \big(1/q^s\Phi(H)\big)\sum_{\chi\neq\chi_0}\Big(\sum_{A}{}'\bar{\chi}(A)E(At)\Big)\Big(\sum_{P}{}'\chi(P)\Big).$$

The first summation on the right above is $T_H(t)$ by definition 5.5. Therefore, if we transpose the first term on the right above and take the absolute value of both sides, we obtain

$$|f(t)-\big(\psi(r)/q^s\Phi(H)\big)T_H(t)| \\ \leqslant \big(1/q^s\Phi(H)\big)\sum_{\chi\neq\chi_0}\Big|\sum_{A}{}'\bar{\chi}(A)E(At)\Big|\Big|\sum_{P}{}'\chi(P)\Big| \\ \leqslant \big(q^{\Theta r}/q^s\Phi(H)\big)\sum_{\chi\neq\chi_0}\Big|\sum_{A}{}'\bar{\chi}(A)E(At)\Big| \tag{5.12}$$

by Theorem 5.1. Now, by the Cauchy inequality

$$\sum_{\chi\neq\chi_0}\Big|\sum_{A}{}'\bar{\chi}(A)E(At)\Big| \leqslant \sum_{\chi}\Big|\sum_{A}{}'\bar{\chi}(A)E(At)\Big| \\ \leqslant \Big[\Big(\sum_{\chi}1\Big)\Big(\sum_{\chi}\Big|\sum_{A}{}'\bar{\chi}(A)E(At)\Big|^2\Big)\Big]^{1/2}. \tag{5.13}$$

Also, $\sum_{\chi}1 = q^s\Phi(H)$ as there are exactly $q^s\Phi(H)$ characters of $\mathscr{R}$. Further, if A_1 and A_2 run independently over the same reduced representative set modulo $\mathscr{R}$ as does A, then

$$\sum_{\chi}\Big|\sum_{A}{}'\bar{\chi}(A)E(At)\Big|^2 \\ = \sum_{\chi}\Big(\sum_{A_1}{}'\bar{\chi}(A_1)E(A_1t)\Big)\Big(\sum_{A_2}{}'\chi(A_2)E(-A_2t)\Big) \\ = \sum_{A_1,A_2}{}'E\big((A_1-A_2)t\big)\sum_{\chi}\bar{\chi}(A_1)\chi(A_2) \\ = q^s\Phi(H)\sum_{A_1\equiv A_2(\mathrm{mod}\,\mathscr{R})}{}'E\big((A_1-A_2)t\big) \\ = q^s\Phi(H)\sum_{A_1\equiv A_2(\mathrm{mod}\,\mathscr{R})}{}'1 = \big(q^s\Phi(H)\big)^2$$

by (5.9) and since $A_1 \equiv A_2 \pmod{\mathscr{R}}$ only if $A_1 = A_2$, as a reduced representative set modulo $\mathscr{R}$ contains exactly one polynomial from each of the $q^s\Phi(H)$ invertible equivalence classes of $\mathscr{R}$. Using these results in (5.13), one finds that

$$\sum_{\chi\neq\chi_0}\Big|\sum_{A}{}'\bar{\chi}(A)E(At)\Big| \leqslant \big(q^s\Phi(H)\big)^{3/2},$$

which together with (5.12) yields

$$|f(t)-\big(\psi(r)/q^s\Phi(H)\big)T_H(t)| \leqslant q^{\Theta r}\big(q^s\Phi(H)\big)^{1/2}. \tag{5.14}$$

Since clearly $\Phi(H) < q^h$, we have $q^s\Phi(H) < q^{s+h} = q^{r-w} \leqslant q^{r-(r/2)+(1/2)} = q^{1/2}q^{r/2}$. Using this bound in (5.14), we obtain

$$|f(t)-\big(\psi(r)/q^s\Phi(H)\big)T_H(t)| < q^{1/4}q^{(1/4+\Theta)r}. \tag{5.15}$$

Now, as is well known, $|\psi(r)-q^r/r| \leqslant q^{r/2}$. Thus,

$$\big|\big(\psi(r)/q^s\Phi(H)\big)T_H(t)-\big(q^r/rq^s\Phi(H)\big)T_H(t)\big| \\ = \big(1/q^s\Phi(H)\big)|T_H(t)||\psi(r)-q^r/r| \leqslant q^{r/2} \leqslant q^{\Theta r} < q^{1/4}q^{(1/4+\Theta)r}$$

since trivially $|T_H(t)| \leqslant q^s\Phi(H)$. This last estimate together with (5.15) yields (5.7), and the proof is complete.

6. The singular series. In this section, we investigate the polynomial analog of the Hardy-Littlewood "singular series". Our treatment follows closely that of Landau ([9], Kap. 4) for the number theoretic singular series.

DEFINITION 6.1. For given H and L in $k[x]$, we set

$$D_H(L) = \sum_{G}E(GL/H), \tag{6.1}$$

where G runs through a reduced residue system modulo H. By (3.8), the value of $D_H(L)$ is independent of the particular reduced residue system used to define it.

DEFINITION 6.2. The polynomial Möbius function μ is defined as follows: $\mu(A) = 0$ if A is divisible by the square of an irreducible; otherwise, $\mu(A) = (-1)^j$, where j is the number of primary irreducibles which divide H.

THEOREM 6.1. *We have*

$$D_H(L) = \sum_{E|H;\,E|L}{}'|E|\mu(H/E). \tag{6.2}$$

Proof. Set

$$C_H(L) = \sum_{B}E(BL/H), \tag{6.3}$$

where B runs through a complete residue system modulo H. Let L^* be the remainder left after dividing L by H. Then $\deg L^* < \deg H$ so that $\nu(L^*/H) > 0$, or $L^*/H \epsilon \mathscr{P}$. Further, from (3.8) we have $C_H(L) = C_H(L^*)$. A particular complete residue system modulo H is furnished by the primary polynomials of degree $h = \deg H$. If we let B run through this particular complete residue system in (6.3), then

$$C_H(L) = C_H(L^*) = \begin{cases} q^h E(x^h L^*/H) & \text{if} \quad \nu(L^*/H) > h, \\ 0 & \text{otherwise} \end{cases}$$

by Theorem 3.7. But $\nu(L^*/H) = h - \deg(L^*) > h$ if and only if $\deg(L^*) < 0$, i.e., if and only if $L^* = 0$. Thus we have

$$C_H(L) = \begin{cases} q^h = |H| & \text{if} \quad H \mid L, \\ 0 & \text{otherwise.} \end{cases} \tag{6.4}$$

Now, as in Landau ([9], Satz 220),

$$C_H(L) = \sum_{E \mid H}{}' D_E(L).$$

Applying Möbius inversion to this last inequality and using (6.4) as in Landau, we arrive at (6.2). This completes the proof.

LEMMA 6.2. *For every odd* $H \epsilon k[x]$

$$\Phi(H) \geqslant |H|^{1/2}, \tag{6.5}$$

where $\Phi(H)$ *is the polynomial analog of the Euler totient function, i.e., the number of polynomials in a reduced residue system modulo* H.

Proof. Both sides of the inequality (6.5) are multiplicative functions of H, so it suffices to verify (6.5) for $H = P^e$, where P is an odd irreducible. Setting $c = |P|$, we have

$$\begin{aligned} \Phi(H) &= |P|^e - |P|^{e-1} = c^e - c^{e-1} \\ &= c^{e-1}(c-1) = c^{(e-1)/2}(c^{1/2} - c^{-1/2})c^{e/2}. \end{aligned} \tag{6.6}$$

The function $g(z) = z - z^{-1}$ has derivative $1 + z^{-2}$ and is, therefore, an increasing function. Since $g(\sqrt{3}) = 2/\sqrt{3} > 1$, $g(z) > 1$ for all $z \geqslant \sqrt{3}$. Since P is odd $c = |P| \geqslant 3$, and hence $g(\sqrt{c}) > 1$. Using this estimate in (6.6), we deduce that

$$\Phi(H) \geqslant c^{e/2} = |P|^{e/2} = |P^e|^{1/2} = |H|^{1/2}.$$

This completes the proof.

LEMMA 6.3. *For every* $H \epsilon k[x]$,

$$\Phi(H) \geqslant |H|^{1/2}/4. \tag{6.7}$$

Proof. If H is odd, then (6.7) follows from (6.5). Therefore, we may suppose that $|H|$ is even, which implies that $q = 2$ and that H is divisible by one or both of the polynomials x and $x+1$. Thus, we have

$$H = x^{e_1}(x+1)^{e_2} H_1,$$

where H_1 is odd, and so

$$\Phi(H) = \Phi(x^{e_1})\Phi\big((x+1)^{e_2}\big)\Phi(H_1) \geqslant \Phi(x^{e_1})\Phi\big((x+1)^{e_2}\big)|H_1|^{1/2}$$

by Lemma 6.2. But

$$\Phi(x^{e_1}) = 2^{e_1} - 2^{e_1-1} = 2^{e_1-1} = 2^{-1}|x^{e_1}|^{1/2},$$

and similarly

$$\Phi\big((x+1)^{e_2}\big) \geqslant 2^{-1}|(x+1)^{e_2}|^{1/2}.$$

Thus,

$$\Phi(H) \geqslant 2^{-1}|x^{e_1}|^{1/2}2^{-1}|(x+1)^{e_2}|^{1/2}|H_1|^{1/2} = |x^{e_1}(x+1)^{e_2}H_1|^{1/2}/4 = |H|^{1/2}/4.$$

This completes the proof.

LEMMA 6.4. *For every non-negative* h,

$$\sum_{\deg H = h}{}' \frac{1}{\Phi(H)} \leqslant h+1. \tag{6.8}$$

Proof. We have

$$\Phi(H) = |H| \prod_{P \mid H} \left(1 - \frac{1}{|P|}\right) \geqslant |H| \prod_{P \mid H} \frac{1}{2},$$

where P runs through the primary irreducible divisors of H. Now $\prod_{P \mid H} 2$ is just the number of primary square-free divisors of H and hence is less than or equal to $\tau(H)$, the number of primary divisors of H. Thus,

$$\sum_{\deg H = h}{}' \frac{1}{\Phi(H)} \leqslant \sum_{\deg H = h}{}' \frac{\tau(H)}{|H|} = q^{-h} \sum_{\deg H = h}{}' \tau(H).$$

The last summation above was found by Carlitz ([3], § 4) to have the value $(h+1)q^h$. This completes the proof.

LEMMA 6.5. *For every non-negative* h,

$$\sum_{\deg H = h}{}' \frac{1}{\Phi^2(H)} \leqslant 4(h+1)q^{-h/2}. \tag{6.9}$$

Proof. By (6.7) we have $1/\Phi(H) \leqslant 4|H|^{-1/2}$. Therefore,

$$\sum_{\deg H=h}{}' \frac{1}{\Phi^2(H)} \leqslant \sum_{\deg H=h}{}' \frac{4|H|^{-1/2}}{\Phi(H)} = 4q^{-h/2} \sum_{\deg H=h}{}' \frac{1}{\Phi(H)} \leqslant 4(h+1)q^{-h/2}$$

by (6.8). This completes the proof.

THEOREM 6.6. *The "singular series"*

$$S(N) = \sum_{H}{}' \frac{\mu(H)}{\Phi^3(H)} D_H(-N), \tag{6.10}$$

where the summation is over all primary H in $k[x]$, is absolutely convergent for every $N \in k[x]$.

Proof. Trivially, $|D_H(-N)| \leqslant \Phi(H)$. Therefore,

$$\sum_{H}{}' \left|\frac{\mu(H)}{\Phi^3(H)}\right| |D_H(-N)| \leqslant \sum_{H}{}' \frac{1}{\Phi^2(H)} = \sum_{h=0}^{\infty} \sum_{\deg H=h}{}' \frac{1}{\Phi^2(H)}$$

$$\leqslant \sum_{h=0}^{\infty} 4(h+1)q^{-h/2} < \infty,$$

by Lemma 6.5. The singular series is thus absolutely convergent by comparison. This completes the proof.

THEOREM 6.7. *For every $N \in k[x]$,*

$$S(N) = \prod_{P} \left(1 + \frac{1}{(|P|-1)^3}\right) \prod_{P|N} \left(1 - \frac{1}{|P|^2 - 3|P| + 3}\right), \tag{6.11}$$

where in the first product P runs through all the primary irreducibles in $k[x]$ and in the second through the primary irreducible divisors of N.

Proof. The proof follows Landau ([9], Satz 247) in every detail.

THEOREM 6.8. *There is an absolute positive constant d (independent of q!) such that $S(N) \geqslant d$ for every odd polynomial N in $k[x]$.*

Proof. It suffices by Theorem 6.7 to show that the second factor in (6.11) is bounded below by an absolute positive constant d, since the first factor is clearly greater than 1. Since N is odd, we have

$$\prod_{P|N} \left(1 - \frac{1}{|P|^2 - 3|P| + 3}\right) \geqslant \prod_{\substack{P \\ P \text{ odd}}} \left(1 - \frac{1}{|P|^2 - 3|P| + 3}\right) \tag{6.12}$$

$$\geqslant 1 - \sum_{P \text{ odd}}{}' \frac{1}{|P|^2 - 3|P| + 3}.$$

Now $z^2 - 3z + 3 = (z^2/4) + 3(z/2-1)^2 \geqslant z^2/4$ for every real z. Therefore, the summation on the right in (6.12) is bounded above by

$$\sum_{H \neq 1}{}' \frac{4}{|H|^2} = 4 \sum_{h=1}^{\infty} q^{-2h} \sum_{\deg H=h}{}' 1 = 4 \sum_{h=1}^{\infty} q^{-h} = \frac{4}{(q-1)}.$$

In particular, the infinite product in (6.12) is convergent and hence different from zero, since as one easily verifies, a factor of the product can vanish only if $|P| = 2$, which does not occur. Further, if $q \geqslant 7$, then $1 - 4/(q-1) \geqslant 1/3$, so that this infinite product is bounded below by $1/3$. Thus, one can take for d the minimum of $1/3$ and the positive values of the infinite product in (6.12) for $q = 2$, 3, 4 and 5. This completes the proof.

7. Coup de grace. In this section, we derive an asymptotic formula for $\boldsymbol{N}(M)$ and prove Theorems 1.1 and 1.2.

LEMMA 7.1. *If G/H is primordial, then for any $t \in \mathcal{U}_{G/H}$ and any non-zero $\delta \in k$, we have*

$$T_H(\delta t) = \begin{cases} \mu(H) q^s E\big(\delta x^r (t - G/H)\big) & \text{if} \quad \nu(t - G/H) > r, \\ 0 \quad \text{otherwise}, \end{cases} \tag{7.1}$$

where $s = r - w - h$ and $h = \deg H$.

Proof. Let B run through the primary polynomials of degree s, and let C run through the polynomials of degree less than h which are prime to H. We claim that then the polynomials $A = x^w HB + C$ run through a reduced representative set modulo $\mathscr{R} = \mathscr{R}_{(s)H}$ taken from among the primary polynomials of degree r. Clearly each polynomial A is primary and has degree r. Further, each is invertible modulo $\mathscr{R}$ by the last paragraph of [7], § 8, since $(A, H) = (C, H) = 1$. Also, there are formally at least $q^s \Phi(H)$ of the polynomials A, which is the number of polynomials in a reduced representative set modulo $\mathscr{R}$. Thus, it remains only to show that the polynomials A are pair-wise distinct modulo $\mathscr{R}$. Suppose that $x^w HB_1 + C_1 \equiv x^w HB_2 + C_2 \pmod{\mathscr{R}}$. Then in particular, these polynomials are congruent modulo H, which shows that $C_1 \equiv C_2 \pmod{H}$ or that $C_1 = C_2$, since each polynomial C has degree less than h. As $\deg C < h$, the first s coefficients of A are determined by the summand $x^w HB$. Thus, $x^w HB_1$ and $x^w HB_2$ have the same first s coefficients. But this occurs if and only if B_1 and B_2 have the same first s coefficients ([7], pp. 117, 118), i.e., if and only if $B_1 = B_2$, as $\deg B_1 = \deg B_2 = s$. It follows that the polynomials A are distinct modulo $\mathscr{R}$ and hence that they constitute a reduced representative set modulo $\mathscr{R}$.

In definition 5.5, let A run through the particular reduced representative set defined above. Then

$$T_H(\delta t) = \sum_A{}' E(A\delta t) = \sum_A{}' E\big(A\delta(t-G/H)\big)E(A\delta G/H). \tag{7.2}$$

Now, $E(A\delta G/H) = E\big((x^w HB+C)\delta G/H\big) = E(\delta CG/H)$ by (3.8). Also, since

$$\begin{aligned}\nu\big(\delta(A-x^w HB)(t-G/H)\big) &= \nu\big(\delta C(t-G/H)\big) = \nu(C)+\nu(t-G/H)\\ &= \nu(t-G/H)-\deg C > w+h-(h-1) = w+1 \geqslant 1\end{aligned}$$

as $t\in\mathscr{U}_{G/H}$, we have

$$E\big(\delta(A-x^w HB)(t-G/H)\big) = 1 \quad\text{or}\quad E\big(\delta A(t-G/H)\big) = E\big(\delta x^w HB(t-G/H)\big).$$

Therefore, from (7.2)

$$\begin{aligned}T_H(\delta t) &= \sum_B{}' E\big(\delta x^w HB(t-G/H)\big)\sum_C E(\delta CG/H)\\ &= \Big(\sum_B{}' E\big(\delta x^w HB(t-G/H)\big)\Big)\,D_H(\delta G)\\ &= \mu(H)\sum_B{}' E\big(\delta x^w HB(t-G/H)\big)\end{aligned} \tag{7.3}$$

by Theorem 6.1. Since

$$\begin{aligned}\nu\big(\delta x^w H(t-G/H)\big) &= \nu(t-G/H)-\deg(x^w H)\\ &= \nu(t-G/H)-(w+h) > (w+h)-(w+h) = 0,\end{aligned}$$

Theorem 3.7 shows that the last summation in (7.3) has the value

$$\begin{cases} q^s E\big(\delta x^{s+w} H(t-G/H)\big) & \text{if} \quad \nu\big(x^w H(t-G/H)\big) > s,\\ 0 \quad \text{otherwise.}\end{cases}$$

But $\nu\big(x^w H(t-G/H)\big) = \nu(t-G/H)-w-h$ is greater than s if and only if $\nu(t-G/H) > s+w+h = r$. And if $\nu(t-G/H) > r$, then

$$\begin{aligned}\nu\big(\delta x^{s+w}(H-x^h)(t-G/H)\big) &= \nu(t-G/H)-w-s-\deg(H-x^h)\\ &> r-w-s-(h-1) = 1,\end{aligned}$$

as H is primary and of degree h. Thus,

$$E\big(\delta x^{s+w}(H-x^h)(t-G/H)\big) = 1$$

or

$$E\big(\delta x^{s+w} H(t-G/H)\big) = E\big(\delta x^{s+w+h}(t-G/H)\big) = E\big(\delta x^r(t-G/H)\big).$$

Using these results in (7.3), we arrive at (7.1). This completes the proof.

THEOREM 7.2. *The number of representations $N(M)$ of M in the form* (1.2) (see definition 4.1) *is estimated by*

$$N(M) = \frac{q^{2r}}{r^3}\,S(M) + O\big(q^{1/4}q^{(5/4+\Theta)r}\big), \tag{7.4}$$

where $S(M)$ is the singular series (6.10) *and $r = \deg M$. Further, the constant implied in the O-notation is independent of both M and q.*

Proof. According to Theorem 4.1,

$$\begin{aligned}N(M) &= \int f(\alpha t)f(\beta t)f(\gamma t)E(-Mt)\,d\varrho\\ &= \sum_{G/H}\int_{\mathscr{U}_{G/H}} f(\alpha t)f(\beta t)f(\gamma t)E(-Mt)\,d\varrho,\end{aligned} \tag{7.5}$$

where $f(t)$ is defined by (4.1) and where the summation is over all primordial G/H. For given primary H such that $\deg H = h \leqslant w$, we set

$$g(t) = g_H(t) = \frac{1}{q^s\Phi(H)}\cdot\frac{q^r}{r}\,T_H(t) \tag{7.6}$$

for every $t\in\mathscr{W}_H$ (see definition 5.5).

Step 1: We first estimate the absolute value of

$$I = \int f(\alpha t)f(\beta t)f(\gamma t)E(-Mt)\,d\varrho - \sum_{G/H}\int_{\mathscr{U}_{G/H}} g(\alpha t)g(\beta t)g(\gamma t)E(-Mt)\,d\varrho, \tag{7.7}$$

where G/H runs through all primordial G/H. We have

$$|I| \leqslant \sum_{G/H}\int_{\mathscr{U}_{G/H}} |f(\alpha t)f(\beta t)f(\gamma t)-g(\alpha t)g(\beta t)g(\gamma t)|\,d\varrho. \tag{7.8}$$

Now for every $t\in\mathscr{U}_{G/H}$,

$$\begin{aligned}&f(\alpha t)f(\beta t)f(\gamma t)-g(\alpha t)g(\beta t)g(\gamma t)\\ &= \big(f(\alpha t)-g(\alpha t)\big)f(\beta t)f(\gamma t)+\big(f(\beta t)-g(\beta t)\big)g(\alpha t)f(\gamma t)+\big(f(\gamma t)-g(\gamma t)\big)g(\alpha t)g(\beta t).\end{aligned}$$

Therefore, on $\mathscr{U}_{G/H}$ we have

$$\begin{aligned}&|f(\alpha t)f(\beta t)f(\gamma t)-g(\alpha t)g(\beta t)g(\gamma t)|\\ &\leqslant |f(\alpha t)-g(\alpha t)|\,|f(\beta t)|\,|f(\gamma t)|+|f(\beta t)-g(\beta t)|\,|g(\alpha t)|\,|f(\gamma t)|+\\ &\qquad +|f(\gamma t)-g(\gamma t)|\,|g(\alpha t)|\,|g(\beta t)|\\ &\leqslant 2q^{1/4}q^{(1/4+\Theta)r}\big(|f(\beta t)|\,|f(\gamma t)|+|g(\alpha t)|\,|f(\gamma t)|+|g(\alpha t)|\,|g(\beta t)|\big)\end{aligned} \tag{7.9}$$

by Theorem 5.3. Now

$$|g(\alpha t)|\,|f(\gamma t)| \leqslant \big(|g(\alpha t)|^2+|f(\gamma t)|^2\big)/2,$$

so that (7.9) implies that

$$|f(\alpha t)f(\beta t)f(\gamma t)-g(\alpha t)g(\beta t)g(\gamma t)| \leqslant 2q^{1/4}q^{(1/4+\Theta)r}\big(|f(\beta t)|\,|f(\gamma t)|+\tfrac{1}{2}|f(\gamma t)|^2\big)+ + 2q^{1/4}q^{(1/4+\Theta)r}\big(|g(\alpha t)|\,|g(\beta t)|+\tfrac{1}{2}|g(\alpha t)|^2\big)$$

for every $t\in\mathscr{U}_{G/H}$. Using this estimate in (7.8), we find that

$$|I| \leqslant 2q^{1/4}q^{(1/4+\Theta)r}(I_1+I_2) \tag{7.10}$$

where

$$I_1=\sum_{G/H}\int_{\mathscr{U}_{G/H}}\big(|f(\beta t)|\,|f(\gamma t)|+\tfrac{1}{2}|f(\gamma t)|^2\big)\,d\varrho \tag{7.11}$$

and

$$I_2=\sum_{G/H}\int_{\mathscr{U}_{G/H}}\big(|g(\alpha t)|\,|g(\beta t)|+\tfrac{1}{2}|g(\alpha t)|^2\big)\,d\varrho\,. \tag{7.12}$$

Now since the sets $\mathscr{U}_{G/H}$ form a partition of $\mathscr{P}$,

$$I_1=\int|f(\beta t)|\,|f(\gamma t)|\,d\varrho+\tfrac{1}{2}\int|f(\gamma t)|^2\,d\varrho\,. \tag{7.13}$$

And

$$\int|f(\gamma t)|^2\,d\varrho=\int f(\gamma t)\overline{f(\gamma t)}\,d\varrho=\int\sum_{P_1,P_2}{}'E\big(\gamma(P_1-P_2)t\big)\,d\varrho = \sum_{P_1,P_2}{}'\int E\big(\gamma(P_1-P_2)t\big)\,d\varrho=\sum_{\substack{P_1,P_2\\P_1=P_2}}{}'1=\psi(r)\leqslant q^r \tag{7.14}$$

where P_1 and P_2 run through the primary irreducibles of degree r and where $\psi(r)$ is the number of primary irreducibles of degree r. Here we have applied Theorem 3.5. Also, since

$$\langle h_1(t),h_2(t)\rangle=\int h_1(t)\overline{h_2(t)}\,d\varrho$$

is an inner product on the vector space of all continuous functions on $\mathscr{P}$, the Schwarz inequality yields

$$\langle|f(\beta t)|,|f(\gamma t)|\rangle\leqslant\langle|f(\beta t)|,|f(\beta t)|\rangle^{1/2}\cdot\langle|f(\gamma t)|,|f(\gamma t)|\rangle^{1/2} =\big(\psi(r)\big)^{1/2}\big(\psi(r)\big)^{1/2}=\psi(r)\leqslant q^r$$

as in (7.14). Using these estimates in (7.13), we find that

$$I_1\leqslant\tfrac{3}{2}q^r\leqslant 3q^r. \tag{7.15}$$

We turn now to I_2. If $\mathscr{B}_{G/H}=\{t\in\mathscr{P}\mid v(t-G/H)>r\}$, then by Lemma 7.1, Corollary 3.2 and (7.6),

$$I_2=\sum_{G/H}\frac{q^{2r}/r^2}{q^{2s}\Phi^2(H)}\int_{\mathscr{U}_{G/H}}\big(|T_H(\alpha t)||T_H(\beta t)|+\tfrac{1}{2}|T_H(\alpha t)|^2\big)\,d\varrho \tag{7.16}$$

$$\leqslant(q^{2r}/r^2)\sum_{G/H}\frac{1}{q^{2s}\Phi^2(H)}\int_{\mathscr{B}_{G/H}}(q^{2s}+\tfrac{1}{2}q^{2s})\,d\varrho$$

$$=(q^{2r}/r^2)\sum_{G/H}\frac{3}{2\Phi^2(H)}\varrho(\mathscr{B}_{G/H})$$

$$=(3q^{2r}/2r^2)\sum_{G/H}\frac{1}{\Phi^2(H)}q^{-r}$$

$$=(3q^r/2r^2)\sum_{\deg H\leqslant w}{}'\frac{1}{\Phi^2(H)}\sum_{\substack{G\\(G,H)=1}}1$$

$$=(3q^r/2r^2)\sum_{\deg H\leqslant w}{}'\frac{1}{\Phi(H)},$$

as G/H runs through the primordial rational functions. For the last summation above, we have by Lemma 6.4 that

$$\sum_{\deg H\leqslant w}{}'\frac{1}{\Phi(H)}=\sum_{h=0}^{w}\sum_{\deg H=h}{}'\frac{1}{\Phi(H)}\leqslant\sum_{h=0}^{w}(h+1)=\frac{(w+1)(w+2)}{2} \leqslant\frac{1}{2}\left(\frac{r}{2}+1\right)\left(\frac{r}{2}+2\right)=\frac{r^2}{8}+\frac{3r}{4}+1.$$

Using this bound in (7.16), we find that

$$I_2\leqslant(3q^r/2)\left(\frac{1}{8}+\frac{3}{4r}+\frac{1}{r^2}\right)\leqslant\frac{45}{16}q^r\leqslant 3q^r. \tag{7.17}$$

Finally (7.17), (7.15) and (7.10) show that

$$|I|\leqslant 12q^{\frac{1}{4}}q^{\left(\frac{5}{4}+\Theta\right)r}. \tag{7.18}$$

We have, therefore, by Theorem 4.1 that

$$\Big|N(M)-\sum_{G/H}\int_{\mathscr{U}_{G/H}}g(\alpha t)g(\beta t)g(\gamma t)E(-Mt)\,d\varrho\Big|=|I|\leqslant 12q^{\frac{1}{4}}q^{\left(\frac{5}{4}+\Theta\right)r}. \tag{7.19}$$

Step 2: We have now to evaluate the integral

$$I_{G|H} = \int_{\mathscr{U}_{G|H}} g(\alpha t)\, g(\beta t)\, g(\gamma t)\, E(-Mt)\, d\varrho,$$

which by (7.6) and Lemma 7.1 has the value

$$\frac{q^{3r}/r^3}{q^{3s}\Phi^3(H)} \int_{\mathscr{U}_{G|H}} T_H(\alpha t) T_H(\beta t) T_H(\gamma t) E(-Mt)\, d\varrho$$

$$= \frac{q^{3r}/r^3}{q^{3s}\Phi^3(H)} \int_{\mathscr{B}_{G|H}} \mu^3(H) q^{3s} E\big((\alpha+\beta+\gamma)x^r(t-G/H)\big) E(-Mt)\, d\varrho$$

$$= \left(\frac{q^{3r}}{r^3}\right)\left(\frac{\mu^3(H)}{\Phi^3(H)}\right) E(-GM/H) \int_{\mathscr{B}_{G|H}} E\Big(\big((\alpha+\beta+\gamma)x^r - M\big)(t-G/H)\Big)\, d\varrho$$

where $\mathscr{B}_{G|H} = \{t \in P \mid \nu(t-G/H) > r\}$. By the invariance of the Haar integral, the last integral above has the value

$$\int_{\mathscr{B}_r} E\Big(\big((\alpha+\beta+\gamma)x^r - M\big)t\Big)\, d\varrho = q^{-r}$$

by Theorem 3.5 as $\nu\big((\alpha+\beta+\gamma)x^r - M\big) = -\deg\big((\alpha+\beta+\gamma)x^r - M\big) > -r$, since $\deg M = r$ and $\alpha+\beta+\gamma = \operatorname{sgn} M$ by hypothesis. Thus,

$$I_{G|H} = \left(\frac{q^{2r}}{r^3}\right)\left(\frac{\mu(H)}{\Phi^3(H)}\right) E(-GM/H).$$

Step 3: We have from step 2 that

$$\sum_{G|H} I_{G|H} = \sum_{G|H}\left(\frac{q^{2r}}{r^3}\right)\left(\frac{\mu(H)}{\Phi^3(H)}\right) E(-MG/H)$$

$$= (q^{2r}/r^3) \sum_{\deg H \leqslant w}{}' \frac{\mu(H)}{\Phi^3(H)} \sum_{\substack{G \\ (G,H)=1}} E(-MG/H)$$

$$= (q^{2r}/r^3) \sum_{\deg H \leqslant w}{}' \frac{\mu(H)}{\Phi^3(H)} D_H(-M).$$

Thus, (7.19) implies that

$$\left| N(M) - (q^{2r}/r^3) \sum_{\deg H \leqslant w}{}' \frac{\mu(H)}{\Phi^3(H)} D_H(-M) \right| \leqslant 12 q^{\frac{1}{4}} q^{\left(\frac{5}{4}+\Theta\right)r}. \tag{7.20}$$

Step 4: Now let

$$I_3 = \left| S(M) - \sum_{\deg H \leqslant w}{}' \frac{\mu(H)}{\Phi^3(H)} D_H(-M) \right|.$$

Then since trivially $|D_H(-M)| \leqslant \Phi(H)$,

$$I_3 \leqslant \sum_{\deg H > w}{}' \left|\frac{\mu(H)}{\Phi^3(H)}\right| |D_H(-M)| \leqslant \sum_{\deg H > w}{}' \frac{1}{\Phi^2(H)} \tag{7.21}$$

$$= \sum_{h=w+1}^{\infty} \sum_{\deg H = h}{}' \frac{1}{\Phi^2(H)} \leqslant \sum_{h=w+1}^{\infty} 4(h+1) q^{-h/2}$$

by Lemma 6.5. Now

$$\sum_{h=w+1}^{\infty} z^{h+1} = z^{w+2}/(1-z)$$

for every z such that $|z| < 1$. Differentiating this equality, we get

$$\sum_{h=w+1}^{\infty} (h+1) z^h = \frac{z^{w+1}}{(1-z)^2}\big(w+2-(w+1)z\big) \leqslant (w+2) z^{w+1}(1-z)^{-2}$$

if $0 < z < 1$. If $z = q^{-1/2}$, then we get

$$\sum_{h=w+1}^{\infty} 4(h+1) q^{-h/2} \leqslant 4(w+2) q^{-(w+1)/2}(1-q^{-1/2})^{-2} \leqslant 56(w+2) q^{-(w+1)/2}$$

since $(1-q^{-1/2})^{-2} \leqslant (1-2^{-1/2})^{-2} = 6+4\sqrt{2} < 14$, as $q \geqslant 2$. Using this result in (7.21), we find that

$$I_3 \leqslant 56(w+2) q^{-(w+1)/2} \leqslant 56\left(\frac{r}{2}+2\right) q^{-r/4}.$$

Thus,

$$(q^{2r}/r^3) I_3 \leqslant 56\left(\frac{1}{2r^2} + \frac{2}{r^3}\right) q^{\frac{7}{4}r} \leqslant 168 q^{\frac{7}{4}r} \leqslant 168 q^{1/4} q^{\left(\frac{5}{4}+\Theta\right)r}$$

as $r \geqslant 1$ and $\Theta \geqslant 1/2$. This last estimate together with (7.20) shows that

$$|N(M) - (q^{2r}/r^3) S(M)| \leqslant 180 q^{\frac{1}{4}} q^{\left(\frac{5}{4}+\Theta\right)r}.$$

This completes the proof.

COROLLARY 7.3. *There is an absolute positive constant c_3 such that $N(M) > 0$ (M odd) provided that*

$$3 - 4\Theta - \frac{1}{r} > 0 \tag{7.22}$$

and

$$r^{1/4}\left(3 - 4\Theta - \frac{1}{r}\right) > \frac{c_3}{\log q}. \tag{7.23}$$

Proof. If follows from Theorem 7.2 that

$$N(M) \geqslant \frac{q^{2r}}{r^3}|S(M)| - c_1\sigma(q,r)$$

for some absolute positive constant c_1, where $\sigma(q,r) = q^{1/4}q^{(\frac{5}{4}+\Theta)r}$. By Theorem 6.8, $S(M) \geqslant d > 0$ since M is odd, where d is also an absolute positive constant. Therefore,

$$\frac{N(M)}{\sigma(q,r)} \geqslant \frac{d}{r^3}q^{(\frac{3}{4}-\Theta)r-\frac{1}{4}} - c_1.$$

Now $\left(\frac{3}{4}-\Theta\right)r-\frac{1}{4} = \frac{r}{4}\left(3-4\Theta-\frac{1}{r}\right) > 0$ by (7.22), and hence

$$q^{(\frac{3}{4}-\Theta)r-\frac{1}{4}} = \sum_{n=0}^{\infty}\frac{(\log q)^n}{n!}\left(\frac{r}{4}\left(3-4\Theta-\frac{1}{r}\right)\right)^n \geqslant \frac{(\log q)^4}{4!}\cdot\frac{r^4}{4^4}\left(3-4\Theta-\frac{1}{r}\right)^4.$$

Thus

$$\frac{N(M)}{\sigma(q,r)} \geqslant \frac{d(\log q)^4}{4!4^4}\left[r\left(3-4\Theta-\frac{1}{r}\right)^4 - \frac{c_2}{(\log q)^4}\right]$$

where $c_2 = 4!\,4^4 c_1/d$. Therefore, $N(M) > 0$ provided that the second factor on the right above is positive, i.e., provided that (7.23) holds with $c_3 = c_2^{1/4}$. This completes the proof.

We are now in a position to prove Theorems 1.1 and 1.2. It is clear hat, for fixed q, both (7.22) and (7.23) will hold for r sufficiently large f $3-4\Theta > 0$, i.e., if $\Theta < 3/4$. Thus, by the above corollary, we have:

Theorem 1.1 *is proved if* $\Theta < 3/4$.

Also, if $r \geqslant 2$, then

$$r^{1/4}\left(3-4\Theta-\frac{1}{r}\right) \geqslant 2^{1/4}\left(3-4\Theta-\frac{1}{2}\right);$$

and, therefore, both (7.22) and (7.23) hold for all $r \geqslant 2$ provided that $3-4\Theta-\frac{1}{2} > 0$ (i.e., $\Theta < 5/8$) and provided that q is chosen sufficiently large. Now any polynomial of degree 1 has trivially a representation in the form (1.2) since all first degree polynomials are irreducible. Thus, by Corollary 7.3, we have:

Theorem 1.2 *is proved if* $\Theta < 5/8$.

From the Riemann hypothesis for function fields proved by A. Weil, it follows that actually $\Theta = 1/2$ (see [8]). Thus, the proofs of Theorems 1.1 and 1.2 are complete.

If we put $\Theta = 1/2$ and use Theorem 6.7 in (7.4), we obtain the following asymptotic formula for $N(M)$:

$$N(M) = c\frac{q^{2r}}{r^3}\prod_{P\mid M}\left(1-\frac{1}{|P|^2-3|P|+3}\right) + O\left(q^{1/4}q^{\frac{7}{4}r}\right),$$

where

$$c = \prod_{P}\left(1+\frac{1}{(|P|-1)^3}\right)$$

and where the constant implied by the O-notation is absolute.

Postscript: If one examines the above proofs, he will find that it is nowhere actually required that deg $M = r$, except in step 2 of the proof of Theorem 7.2 where deg $M < r$ and $\alpha+\beta+\gamma = 0$ would also suffice. Therefore, if one wishes, he can fix M and let r tend to infinity independently of M, provided only that $\alpha+\beta+\gamma = 0$. In this way one can show that *any* odd M can be represented in the form (1.2) with perhaps $\deg P_1 = \deg P_2 = \deg P_3 = r$ greater than deg M and $\alpha+\beta+\gamma = 0$. In doing this, one is perhaps "not playing the game" since a good deal of cancellation occurs in the addition of the higher order terms in the polynomials P_1, P_2, and P_3. In the number theoretic case, of course, no cancellation can occur. Therefore, one should probably view Theorem 1.1 as the "correct" analog of Vinogradov's theorem.

References

[1] L. Carlitz, *Representation of Arithmetic Functions in GF[p^n, x]*, Duke Math. Journ. 14 (1947), pp. 1121-1137.

[2] — *Representation of Arithmetic Functions in GF[p^n, x], II*, Duke Math. Journ. 15 (1948), pp. 795-801.

[3] — *The Arithmetic of Polynomials in a Galois Field*, Amer. Journ Math. 54 (1932), pp. 39-50.

[4] J. Dieudonné, *Foundations of Modern Analysis*, New York 1960.

[5] T. Estermann, *Introduction to Modern Prime Number Theory*, Cambridge University Press 1952.

[6] G. H. Hardy and J. E. Littlewood, *Some Problems of 'Partitio Numerorum': On the expression of a number as a sum of primes*, Acta Math. (Stockholm), 44 (1923), pp. 1-70.

[7] D. R. Hayes, *The Distribution of Irreducibles in GF[q, x]*, Trans. Amer. Math. Soc. 117 (1965), pp. 101-127.

[8] — *A General Character Sum*, to appear.

[9] E. Landau, *Vorlesungen über Zahlentheorie*, Band 1, Teil 5, New York 1947.

[10] L. Nachbin, *The Haar Integral*, Princeton 1965.

[11] I. M. Vinogradov, *Representation of an Odd Number as a Sum of Three Primes*, Comptes Rendus (Doklady) de l'Académie des Sciences de l'URSS, 15 (1937), pp. 191-294.

[12] E. Weiss, *Algebraic Number Theory*, New York 1963.

THE UNIVERSITY OF TENNESSEE

Reçu par la Rédaction le 7. 12. 1965

ACTA ARITHMETICA
XI (1966)

Correction to the paper "Binomial coefficients in an algebraic number field"

by

L. Carlitz (Durham, N. C.)

Mr. William Leahey has kindly drawn the writer's attention to an error in the statement of Theorem 1 of the paper [1]. The theorem should read as follows:

Theorem 1. *The binomial coefficients* $\binom{a}{m}$ *are integral* $(\mathrm{mod}\,\mathfrak{p})$ *for all* $a \in K\mathfrak{p}$ *and all* $m \geqslant 1$ *if and only if* $\mathfrak{p}$ *is a prime ideal of the first degree and moreover* $\mathfrak{p}^2$ *does not divide* p.

The former proof applies with very minor changes. If the field K is normal the original statement of the theorem is correct.

Reference

[1] L. Carlitz, *Binomial coefficients in an algebraic field*, Acta Arith. 7 (1962), pp. 381-388.

Reçu par la Rédaction le 3. 8. 1965