Conspectus materiae tomi XXXVIII, fasciculi 4

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de la Rédaction et de l'échange
Address of the Editorial Board and of the exchange
Die Adresse der Schriftleitung und des Austausches
Адрес редакции и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статей редакция просит предлагать в двух экземплярах

© Copyright by Państwowe Wydawnictwo Naukowe, Warszawa 1981

ISBN 83-01-01336-2 ISSN 0065-1036

PRINTED IN POLAND

W R O C Ł A W S K A D R U K A R N I A N A U K O W A

ACTA ARITHMETICA
XXXVIII (1981)

Norms from certain extensions of $F_q(T)$

by

Sudesh K. Gogia and Indar S. Luthar (Chandigarh, India)

In 1908 Landau [2] gave an asymptotic formula for the number $B(x)$ of integers $\leqslant x$ which are representable as sums of two squares of integers. The number $B(x)$ may be interpreted as the number of integers $\leqslant x$ which are norms of (totally positive) elements of $Q(\sqrt{-1})$. In this form the result was generalized by Luthar [3] to arbitrary quadratic extensions of Q.

In this paper we consider the analogous problems for certain types of extensions of $F_q(T)$, F_q being the finite field with q elements and T an indeterminate. In § 1, we determine the number of non-zero polynomials in $F_q[T]$ of degree $\leqslant n$ which are representable as norms (of polynomials) from a constant field extension $F_{q'}(T)$ of $F_q(T)$. In § 2 we consider the number of non-zero polynomials of $F_q[T]$ of degree $\leqslant n$ which are norms of elements of a quadratic extension $F_q(T, \sqrt{D(T)})$ of $F_q(T)$, $D(T)$ being a non-constant square free polynomial in $F_q[T]$. These results are deduced from the following theorem.

Theorem 1. *Let z be a complex number of absolute value >1 and let λ be a positive real number <1. Let $\psi(u)$ be any holomorphic function of u in $|u| < |z|^{-1/2}$ with $\psi(z^{-1}) \neq 0$. For $|u| < |z|^{-1}$, write*

$$(1-zu)^{-\lambda}\psi(u) = \sum_{\nu=0}^{\infty} b_\nu u^\nu$$

where the power series expansion of $(1-zu)^{-\lambda}$ around $u=0$ begins with 1. Then

$$\sum_{\nu=0}^{n} b_\nu = \frac{bz^n}{n^{1-\lambda}}\left[1+\frac{c}{n}+O\left(\frac{\log n}{n^2}\right)\right]$$

with

$$b = \frac{1}{\Gamma(\lambda)}\frac{z}{z-1}\psi(z^{-1}), \quad c = (1-\lambda)\frac{1}{z}\left[\frac{\psi'}{\psi}(z^{-1}) - z\left(\frac{\lambda}{2}-\frac{1}{z-1}\right)\right].$$

The proof of this result will be given in § 3.

1. Norms from constant field extensions. Let $k' = F_{q'}(T)$ be a constant field extension of $k = F_q(T)$ of degree l, so that $q' = q^l$; here l is any integer $\geqslant 2$. If $\pi(T)$ is a monic irreducible polynomial in $F_q[T]$ and if

$$\pi(T) = \pi_1(T)\ldots\pi_g(T)$$

is its factorization into monic irreducible polynomials in $F_{q'}[T]$, then all the $\pi_i(T)$ are distinct; moreover they are conjugates of each other with respect to the extension k'/k. We put

$$N_{k'/k}(\pi_i(T)) = \pi(T)^f$$

so that

$$fg = l.$$

When we wish to be more explicit, we shall denote the integers f and g by f_π and g_π respectively. The product

$$\prod_\pi (1-q^{-ls\deg\pi/g_\pi})^{-l+g_\pi}$$

extended over all monic irreducible polynomials $\pi(T)$ in $F_q[T]$, represents a holomorphic function of s in $\sigma > \frac{1}{2}$ which is never zero there. Putting

$$u = q^{-ls}$$

we see that the function

$$G(u) = \prod_\pi (1-u^{\deg\pi/g_\pi})^{-l+g_\pi} \tag{1}$$

is holomorphic and never zero in $|u| < q^{-l/2}$. Consequently there is a unique function $\psi(u)$ satisfying

$$\psi(u) = 1+au+\ldots, \tag{2}$$

and

$$\psi(u)^l = G(u). \tag{3}$$

With the above notations, we have

THEOREM 2. *The number $B(n)$ of non-zero polynomials in $F_q[T]$ of degree $\leqslant n$, which appear as norms from k' to k of elements of $F_{q'}[T]$, is given by*

$$B(ln+r) = \frac{(q-1)bq'^n}{n^{1-1/l}}\left[1+\frac{c}{n}+O\left(\frac{\log n}{n^2}\right)\right] \quad (n\geqslant 0,\ 0\leqslant r<l) \tag{4}$$

where

$$b = \frac{1}{\Gamma(1/l)}\frac{q'}{q'-1}\psi\left(\frac{1}{q'}\right),\quad c = \left(1-\frac{1}{l}\right)\frac{1}{q'}\left[\frac{\psi'}{\psi}\left(\frac{1}{q'}\right)-q'\left(\frac{1}{2l}-\frac{1}{q'-1}\right)\right] \tag{5}$$

and ψ is defined by (2) *and* (3).

Call $C(n)$ the number of monic polynomials in $F_q[T]$ of degree $\leqslant n$ which appear as norms from k' to k of elements of $F_{q'}[T]$. As each element of F_q is a norm from $F_{q'}$ to F_q and hence a norm from k' to k, we see that

$$C(n) = \frac{1}{q-1}B(n);$$

hence (4) is equivalent to

$$C(ln+r) = \frac{bq'^n}{n^{1-1/l}}\left[1+\frac{c}{n}+O\left(\frac{\log n}{n^2}\right)\right] \quad (0\leqslant r<l). \tag{4'}$$

If $h'(T)$ is a polynomial in $F_{q'}[T]$, then $N_{k'/k}(h'(T))$ has its degree a multiple of l. It follows that for $0\leqslant r<l$

$$C(ln) = C(ln+r);$$

consequently to prove Theorem 2, it suffices to prove (4′) with $r=0$.

For a monic polynomial $h(T)$ in $F_q(T)$, define b_h to be 1 or 0 according as $h(T)$ is or is not the norm of some polynomial in $F_{q'}[T]$. It is clear that

$$C(ln) = \sum b_h$$

where the summation is extended over all monic polynomials $h(T)$ in $F_q[T]$ of degree $\leqslant ln$. The series

$$\varphi(s) = \sum_h b_h q^{-s\deg h}$$

extended over all monic polynomials $h(T)$ in $F_q(T)$ of degree $\geqslant 0$ represents a holomorphic function in $\sigma>1$. Since $b_h = 0$ if degree of $h(T)$ is not a multiple of l, it follows that φ is a function of

$$u = q^{-ls} = q'^{-s};$$

we shall write $\varphi(u)$ for $\varphi(s)$. Thus, for $|q'u|<1$,

$$\varphi(u) = \sum_h b_h u^{\deg h/l} = \sum_{n=0}^{\infty} b_n u^n; \tag{6}$$

where

$$b_n = \sum_h b_h,$$

h running over all monic polynomials of degree ln, so that

(7) $$C(ln) = \sum_{\nu=0}^{n} b_\nu.$$

One verifies easily that for relatively prime polynomials $g(T)$ and $h(T)$ n $F_q[T]$

$$b_{gh} = b_g b_h;$$

it follows that for $\sigma > 1$,

$$\varphi(s) = \prod_\pi (1-q^{-sf_\pi \deg \pi})^{-1}$$

where the product is extended over all monic irreducible polynomials $\pi(T)$ of $F_q[T]$. Since $f_\pi g_\pi = l$, for $|q'u| < 1$, $\varphi(u)$ can be written as

$$\varphi(u) = \prod_\pi (1-u^{\deg \pi/g_\pi})^{-1}.$$

If $\zeta_{k'}(s)$ denotes the Dedekind zeta function of k', then we have for $|q'u| < 1$

$$(1-u)^{-1}(1-q'u)^{-1} = \zeta_{k'}(s) = (1-u)^{-1}\prod_\pi (1-u^{\deg\pi/g_\pi})^{-g_\pi},$$

so that

$$\varphi(u)^l = (1-q'u)^{-1}G(u),$$

where $G(u)$ is as in (1). Taking lth roots, we get for $|q'u| < 1$,

(8) $$\varphi(u) = (1-q'u)^{-1/l}\psi(u)$$

where the power-series expansion of $(1-q'u)^{-1/l}$ around $u = 0$ begins with 1.

In view of (6), (7) and (8) the desired result (4′) with $r = 0$ follows at once on taking $z = q'$ and $\lambda = 1/l$ in Theorem 1.

2. Norms from quadratic extensions. Let $k' = k(\sqrt{D(T)})$ be a quadratic extension of $k = F_q(T)$ with $D(T)$ a non-constant square free polynomial in $F_q[T]$. If F_q is of characteristic 2, then one easily proves that the number $B(n)$ of non-zero polynomials in $F_q[T]$ of degree $\leqslant n$ which are norms from k' to k of elements of k' is given by

$$B(n) = q^{n+1}-1.$$

Throughout the rest of this section, we shall assume that the characteristic of F_q is different from 2. We shall first find a formula for the number $C(n)$ of monic polynomials $h(T)$ in $F_q[T]$ of degree $\leqslant n$ such that $c\cdot h(T)$ is a norm from k' for some $c \neq 0$ in F_q. The estimate for $B(n)$ will then result from the obvious relation

(9) $$B(n) = \nu_0 C(n)$$

where ν_0 is the number of non-zero elements of F_q which are norms from k'; we shall determine the number ν_0 explicitly.

Let $\mathfrak{o}' = F_q[T, \sqrt{D(T)}]$ be the integral closure in k' of $F_q[T]$, and let I and I' denote respectively the group of (fractional) ideals of k and k'. Let H' be the subgroup of I' consisting of all principal ideals and let G' be the subgroup of I' consisting of all ideals $\mathfrak{a}'$ of k' such that for some $\xi' \neq 0$ in k'

$$N_{k'/k}(\mathfrak{a}') = (N_{k'/k}(\xi')).$$

One verifies at once that an ideal $\mathfrak{a}'$ of k' is in G' if and only if the class of $\mathfrak{a}'$ is a square. It is also clear that for an element $h(T) \neq 0$ of $F_q[T]$, $c\cdot h(T)$ is a norm from k' for some $c \neq 0$ in F_q if and only if there exists $\mathfrak{a}'$ in G' such that

$$N_{k'/k}(\mathfrak{a}') = (h(T)).$$

For a character χ of I' trivial on G', and for a monic polynomial $h(T)$ in $F_q[T]$, we define $b(h,\chi)$ to be $\chi(\mathfrak{a}')$ or 0 according as $(h(T)) = N_{k'/k}(\mathfrak{a}')$ for some $\mathfrak{a}'$ in I' or not; it is trivial to check that $b(h,\chi)$ is well-defined and that the sum

$$\sum_\chi b(h,\chi)$$

extended over all characters χ of I' trivial on G' equals the number of characters of I'/G' or 0 according as some non-zero constant multiple of $h(T)$ is or is not the norm of an element of k'. Thus

(10) $$\sum_{\deg h \leqslant n}\sum_\chi b(h,\chi) = rC(n)$$

where r is the number of characters of I'/G'. This number is determined elsewhere.

The series

(11) $$\varphi(s,\chi) = \sum_h b(h,\chi) q^{-s\deg h}$$

extended over all monic polynomials $h(T)$ in $F_q[T]$ represents a holomorphic function of s in $\sigma > 1$. If $\mathfrak{p}'$ and $\mathfrak{p}''$ are two distinct prime ideals of k' lying above the same prime ideal $(\pi(T))$ of k, then $\mathfrak{p}'/\mathfrak{p}''$ is in G' and hence $\chi(\mathfrak{p}') = \chi(\mathfrak{p}'')$. Thus for any monic irreducible polynomial $\pi(T)$ of $F_q[T]$ we may define $\chi(\pi)$ as $\chi(\mathfrak{p}')$ where $\mathfrak{p}'$ is any prime ideal of k' above $\pi(T)$; if

$$h(T) = \pi_1(T)^{l_1}\ldots\pi_m(T)^{l_m}$$

is any monic polynomial, we define

$$\chi(h) = \chi(\pi_1)^{l_1}\ldots\chi(\pi_m)^{l_m}.$$

Let f_π denote the modular degree of any prime ideal $\mathfrak{p}'$ of k' lying above the prime ideal $(\pi(T))$ of k, so that

$$N_{k'/k}(\mathfrak{p}') = (\pi(T)^{f_\pi}).$$

Clearly $b(\pi_1^{l_1}\ldots\pi_m^{l_m}, \chi) \neq 0$, if and only if, $f_i = f_{\pi_i}$ divides l_i for $1 \leqslant i \leqslant m$; when that is so,

$$b(\pi_1^{a_1 f_1}\ldots\pi_m^{a_m f_m}, \chi) = \chi(\pi_1^{a_1}\ldots\pi_m^{a_m}).$$

It follows that for $\sigma > 1$,

$$(12)\qquad \varphi(s,\chi) = \prod_{\pi}\left(1-\chi(\pi)q^{-sf_\pi \deg\pi}\right)^{-1}$$
$$= \prod_{\pi|D}\left(1-\chi(\pi)q^{-s\deg\pi}\right)^{-1}\prod_{\left(\frac{D}{\pi}\right)=+1}\left(1-\chi(\pi)q^{-s\deg\pi}\right)^{-1}\prod_{\left(\frac{D}{\pi}\right)=-1}\left(1-\chi(\pi)q^{-2s\deg\pi}\right)^{-1},$$

where $\pi = \pi(T)$ runs over monic irreducible polynomials of $F_q[T]$ and where the symbol $\left(\frac{D(T)}{\pi(T)}\right)$ has a meaning similar to the Legendre symbol.

Let ∞ denote the place of k characterized by $|T^{-1}|_\infty < 1$; we put

$$\Omega' = \prod_{v'|\infty} k_{v'}'^{\times}\prod_{v'\nmid\infty} r_{v'}'^{\times}$$

where v' runs over the places of k' and where $r_{v'}'^{\times}$ denotes the group of units of the maximal compact subring $r'_{v'}$ of the completion $k'_{v'}$ of k' at the place v'. The canonical map

$$i\colon k_A'^{\times} \to I'$$

induces an isomorphism of $k_A'^{\times}/k'^{\times}\Omega'$ with the group $\mathscr{C}' = I'/H'$ of ideal classes of $\mathfrak{o}'$. As $G'/H' = \mathscr{C}'^2$, it follows that

$$\chi \to \chi\circ i$$

is an isomorphism of the group of characters of $I'/G' = \mathscr{C}'/\mathscr{C}'^2$ with the group of real characters of $k_A'^{\times}/k'^{\times}\Omega'$. We shall write χ for $\chi\circ i$ and denote by $L(s,\chi)$ the L-function of the field k' with respect to the character $\chi = \chi\circ i$ of $k_A'^{\times}$ trivial on $k'^{\times}\Omega'$. Then for $\sigma > 1$, we have (with usual notations)

$$L(s,\chi) = \prod_{v'|\infty}(1-q_{v'}^{-s})^{-1}\prod_{\pi|D}\left(1-\chi(\pi)q^{-s\deg\pi}\right)^{-1}\prod_{\left(\frac{D}{\pi}\right)=+1}\left(1-\chi(\pi)q^{-s\deg\pi}\right)^{-2}\times$$
$$\times\prod_{\left(\frac{D}{\pi}\right)=-1}\left(1-\chi(\pi)q^{-2s\deg\pi}\right)^{-1},$$

so that by (12)

$$\varphi^2(s,\chi) = A(s)L(s,\chi)\prod_{\pi|D}\left(1-\chi(\pi)q^{-s\deg\pi}\right)^{-1}\prod_{\left(\frac{D}{\pi}\right)=-1}\left(1-\chi(\pi)q^{-2s\deg\pi}\right)^{-1},$$

where

$$A(s) = \prod_{v'|\infty}(1-q_{v'}^{-s}).$$

We put

$$u = q^{-s},$$

and

$$\varphi(u,\chi) = \varphi(s,\chi),\qquad L(u,\chi) = L(s,\chi),\qquad A(u) = A(s);$$

then for $|u| < q^{-1}$,

$$(13)\quad \varphi^2(u,\chi) = A(u)L(u,\chi)\prod_{\pi|D}\left(1-\chi(\pi)u^{\deg\pi}\right)^{-1}\prod_{\left(\frac{D}{\pi}\right)=-1}\left(1-\chi(\pi)u^{2\deg\pi}\right)^{-1}$$

Also $\varphi(u,\chi)$, in view of (11), is given by

$$(14)\qquad \varphi(u,\chi) = \sum_h b(h,\chi)u^{\deg h} = \sum_{\nu=0}^{\infty} b_\nu(\chi)u^\nu$$

with

$$b_\nu(\chi) = \sum_{\deg h=\nu} b(h,\chi),$$

so that by (10) we have

$$(15)\qquad rC(n) = \sum_\chi\sum_{\nu=0}^{n} b_\nu(\chi)$$

where χ runs over the characters of I'/G', i.e., over the real characters of $k_A'^{\times}/k'^{\times}\Omega'$ and where r is the number of these characters. Thus, to estimate the number $C(n)$, it suffices to estimate the sum $\sum_{\nu=0}^{n} b_\nu(\chi)$ for each χ. To do this, we distinguish three cases:

I. χ does not lie in the principal sheet.

II. χ is a non-trivial character lying in the principal sheet.

III. χ is the trivial character.

Estimates in Case I. As before, let χ be a character of I'/G'; suppose that χ, regarded as a character of $k_A'^{\times}/k'^{\times}\Omega'$, does not lie in the principal sheet. Then $L(u,\chi)$ is a polynomial in u ([4], Chapter 7) and has no zeros in $|u| \leqslant q^{-1}$ ([4], Chapter 13); consequently it has no zeros in a slightly bigger disc. Also the product $\prod_{(D/\pi)=-1}\left(1-\chi(\pi)u^{2\deg\pi}\right)^{-1}$ is holomorphic and never zero in $|u| < q^{-1/2}$. On separating one of the factors in the finite product $\prod_{\pi|D}(1-\chi(\pi)u^{\deg\pi})^{-1}$ corresponding to a prime divisor, say $\pi_0(T)$, of $D(T)$, it now follows from (13) that for $|u| < q^{-1}$,

$$\varphi^2(u,\chi) = (1-\delta u^l)^{-1}G(u,\chi) \qquad (l = \text{degree of } \pi_0(T),\ \delta = \chi(\pi_0))$$

where $G(u,\chi)$ is holomorphic and never zero in $|u| < q^{a-1}$ for some $a > 0$. Taking square roots, we have

(16) $$\varphi(u,\chi) = (1-\delta u^l)^{-1/2}\psi(u,\chi)$$

where the expansions around $u = 0$ of $(1-\delta u^l)^{-1/2}$ and of $\psi(u,\chi)$ begin with 1. We write

$$(1-\delta u^l)^{-1/2} = 1 + \sum_{m=1}^{\infty}\frac{(2m)!}{(m!)^2}\frac{\delta^m}{2^{2m}}u^{lm} = \sum_{\nu=0}^{\infty}a_\nu u^\nu,$$

$$S_n = \sum_{\nu=0}^{n}a_\nu,$$

and

$$\psi(u,\chi) = \sum_{\nu=0}^{\infty}c_\nu u^\nu \qquad (|u| < q^{a-1})$$

so that by (14) and (16) we have

(17) $$\sum_{\nu=0}^{n}b_\nu(\chi) = \sum_{\nu=0}^{n}c_\nu S_{n-\nu}.$$

Since $|a_{lj}/a_{l(j+1)}| \leqslant 2$, we have, by Stirling's formula, on putting $m = [n/l]$

(18) $$S_n = S_{lm} \ll 2^n|a_{lm}| \sim \frac{2^n}{\sqrt{\pi m}} \ll \frac{2^n}{\sqrt{n}} \ll \frac{q^n}{n^3}.$$

We put

$$N = \left[\frac{6}{a}\log n\right]+1$$

and write (17) as

(a) $$\sum_{\nu=0}^{n}b_\nu(\chi) = \sum_{\nu=0}^{N-1}c_\nu S_{n-\nu} + \sum_{\nu=N}^{n}c_\nu S_{n-\nu} = X+Y.$$

In view of (18) we have

(b) $$Y \ll \sum_{\nu=N}^{n}|c_\nu|q^{n-\nu} \leqslant \frac{q^n}{n^3}\sum_{\nu=N}^{n}{}'|c_\nu|q^{\frac{a}{2}\nu-\nu} \ll q^n/n^3.$$

Similarly

(c) $$X \ll \sum_{\nu=0}^{N-1}|c_\nu|q^{n-\nu}(n-\nu)^{-3} \ll q^n/n^3\sum_{\nu=0}^{N-1}|c_\nu|q^{-\nu} \ll q^n/n^3.$$

Combining (a), (b) and (c), we obtain:

(19) $$\sum_{\nu=0}^{n}b_\nu(\chi) \ll q^n/n^3.$$

Estimates in Case III. We shall denote the trivial character by χ_0 and the Dedekind zeta function of k' by $\zeta_{k'}(s)$. As before, we put $u = q^{-s}$, so that

$$L(u,\chi_0) = \zeta_{k'}(u) = P(u)/(1-u)(1-qu)$$

where $P(u)$ is a polynomial in u all whose zeros lie on the circle $|u| = q^{-1/2}$ ([5], Chapter II). One easily proves that in the present case relation (13) gives:

(20) $$\sum_{\nu=0}^{\infty}b_\nu(\chi)u^\nu = \varphi(u,\chi_0) = (1-qu)^{-1/2}\psi_0(u) \qquad (|u| < q^{-1})$$

where $\psi_0(u)$ is holomorphic and never zero in $|u| < q^{-1/2}$, $\psi_0(0) = 1$ and

(20′) $$\psi_0^2(u) = \frac{A(u)}{1-u}P(u)\prod_{\pi|D}(1-u^{\deg\pi})^{-1}\prod_{(D/\pi)=-1}(1-u^{2\deg\pi})^{-1}.$$

Applying Theorem 1 to the function $\varphi(u,\chi_0)$ (with $z = q$ and $\lambda = 1/2$), we get

(21) $$\sum_{\nu=0}^{n}b_\nu(\chi_0) = \frac{bq^n}{\sqrt{n}}\left[1+\frac{c}{n}+O\left(\frac{\log n}{n^2}\right)\right]$$

where

(22) $$b = \frac{1}{\sqrt{\pi}}\frac{q}{q-1}\psi_0(q^{-1}), \qquad c = \frac{1}{2q}\left[\frac{\psi_0'}{\psi_0}(q^{-1})+\frac{q(5-q)}{4(q-1)}\right].$$

Estimates in Case II. In this case χ is a non-trivial character of $k_A'^\times$ and lies in the principal sheet, so that it is of the form

$$\chi(z) = |z|_A^{i\vartheta} \qquad (z \text{ in } k_A'^\times).$$

Since the group $\{|z|_A\colon z \in k_A'^\times\}$ is generated by q, therefore ϑ is an odd integral multiple of $\pi/\log q$ and hence

(23) $$\chi(z) = |z|_A^{i\pi/\log q} = |z|_A^{i\pi}$$

where $\tau = \pi/\log q$. It follows that a non-trivial real character of $k_A'^{\times}/k'^{\times}\Omega'$ which lies in the principal sheet, if it exists, is unique and it is given by (23). The necessary and sufficient conditions for the existence of such a χ are given in the following lemma; the proof is easy and is therefore omitted.

LEMMA 1. *The following conditions are equivalent.*

(i) *There exists a non-trivial real character of $k_A'^{\times}/k'^{\times}\Omega'$ which lies in the principal sheet.*

(ii) *If w is a place of k' lying above the place ∞ of k, then the modular degree f_w of k'_w/k_∞ is 2.*

(iii) *$D(T)$ is an even degree polynomial with its leading coefficient a non-square in F_q.*

Let χ be as in (23) and let $L(s,\chi)$ be the corresponding L-function of k'. Then (in view of $f_w = 2$), we have

$$L(s,\chi) = \zeta_{k'}(s+i\tau)$$

firstly for $\sigma > 1$, and then, by analytic continuation, for all s. We put $u = q^{-s}$ so that

$$L(u,\chi) = \zeta_{k'}(-u) = P(-u)/(1+u)(1+qu)$$

where $P(u)$ is a polynomial in u with all its zeros lying on the circle $|u| = q^{-1/2}$. One easily verifies that in the present case, relation (13) gives:

$$(24)\qquad \sum_{\nu=0}^{\infty} b_\nu(\chi)u^\nu = \varphi(u,\chi) = (1+qu)^{-1/2}\psi(u) \qquad (|u| < q^{-1})$$

where $\psi(u)$ is holomorphic and never zero in $|u| < q^{-1/2}$, and the power series expansions of $(1+qu)^{-1/2}$ and of $\psi(u)$ around $u = 0$ begin with 1. Therefore Theorem 1 is applicable to the function $\varphi(u,\chi)$ (with $z = -q$ and $\lambda = 1/2$); so that

$$(25)\qquad \sum_{\nu=0}^{n} b_\nu(\chi) = b'\frac{(-q)^n}{\sqrt{n}}\left[1+\frac{c'}{n}+O\left(\frac{\log n}{n^2}\right)\right]$$

where

$$(26)\quad b' = \frac{1}{\sqrt{\pi}}\,\frac{q}{q+1}\,\psi(-q^{-1}), \qquad c' = \frac{-1}{2q}\left[\frac{\psi'}{\psi}(-q^{-1}) + \frac{q(5+q)}{4(1+q)}\right].$$

In view of (13), (20′) and (24), it is easy to verify that for $|u| < q^{-1/2}$,

$$\psi_0^2(u) = \psi^2(-u);$$

Since $\psi_0(0) = \psi(0) = 1$, it follows that for $|u| < q^{-1/2}$,

$$\psi_0(u) = \psi(-u).$$

Therefore b' and c' are given by

$$(26')\qquad b' = \frac{1}{\sqrt{\pi}}\,\frac{q}{q+1}\,\psi_0(q^{-1}), \qquad c' = \frac{1}{2q}\left[\frac{\psi_0'}{\psi_0}(q^{-1}) - \frac{q(5+q)}{4(1+q)}\right].$$

The number ν_0 and the number $B(n)$. The following lemma determines the number ν_0 of non-zero elements of F_q which are norms from k' to k.

LEMMA 2. *The number ν_0 equals $(q-1)/2$ or $q-1$ according as $D(T)$ has or has not an irreducible factor of odd degree.*

Proof. Suppose first that $D(T)$ has an irreducible factor, say $h(T)$ of odd degree l (say). If a non-square α in F_q appears as a norm from k' to k, then we have

$$(*)\qquad \alpha c^2(T) = a^2(T) - D(T)b^2(T)$$

for some polynomials $a(T)$, $b(T)$ and $c(T)$ in $F_q[T]$ having the g.c.d. 1. The polynomials $c(T)$ and $D(T)$ are then co-prime. Reading $(*)$ mod $h(T)$, we see that α is a square in the field $F_q[T]/(h(T)) = F_{q^l}$ which is impossible because l is odd. Hence an element of F_q is a norm if and only if it is a square in F_q; therefore $\nu_0 = (q-1)/2$.

Suppose now that each irreducible factor of $D(T)$ is of even degree. We have to prove that $\nu_0 = q-1$. In view of the Hasse Norm Theorem ([1], Chapter 7), it suffices to prove that for each place v of k and for each place v' of k' above v, all elements of F_q are norms from $k'_{v'}$ to k_v. For this, suppose first that v' lies above the place $v = v_\pi$ of k corresponding to a monic irreducible polynomial $\pi(T)$ of $F_q[T]$. If $\pi(T)$ does not divide $D(T)$, then $k'_{v'}$ is an unramified extension of k_v. Hence every unit of the maximal compact subring r_v of k_v appears as a norm from $k'_{v'}$ to k_v; in particular all non-zero elements of F_q do so. If $\pi(T)$ divides $D(T)$, then the module of k_v, being $q^{\deg\pi}$, is a power of q^2, and hence F_{q^2} is contained in k_v; consequently

$$F_q \subset (F_{q^2})^2 \subset N_{k'_{v'}/k_v}(k'_{v'}).$$

Finally suppose that v' lies above the place ∞ of k. Since $D(T)$ is of even degree, it is either a square in $k_\infty = F_q((T^{-1}))$ in which case $k'_{v'} = k_\infty(\sqrt{D(T)}) = k_\infty$, or $k'_{v'}$ is an unramified extension of k_∞ (by Lemma 1). In either case each non-zero element of F_q appears as a norm from $k'_{v'}$ to k_∞.

We are now in a position to estimate the number $B(n)$. Combining relations (9), (15), (19), (21) and (25) with Lemmas 1 and 2, we get

THEOREM 3. *Suppose that the characteristic of $k = F_q(T)$ is not equal to 2. Let $D(T)$ be a non-constant square-free polynomial in $F_q[T]$ and let $\mathfrak{o}'$ be the integral closure in $k' = k(\sqrt{D(T)})$ of $F_q[T]$. Then the number $B(n)$*

of non-zero polynomials in $F_q[T]$ of degree $\leqslant n$ which appear as norms from k' to k is given by:

$$\frac{r}{\nu_0} B(n) = \frac{bq^n}{\sqrt{n}}\left[1+\frac{c}{n}+O\left(\frac{\log n}{n^2}\right)\right]$$

in all cases except when $D(T)$ is an even degree polynomial with its leading coefficient a non-square in F_q, in which case

$$\frac{r}{\nu_0} B(n) = \frac{q^n}{\sqrt{n}}\left[b+(-1)^n b'+\frac{bc+(-1)^n b'c'}{n}+O\left(\frac{\log n}{n^2}\right)\right];$$

here $\nu_0 = (q-1)/2$ or $q-1$ according as $D(T)$ has or has not an irreducible factor of odd degree; r is the number of real characters of the group of ideal classes of the Dedekind domain $\mathfrak{o}'$; b, c and b', c' are given by (22) *and* (26′) *respectively.*

3. Proof of Theorem 1. For the proof of this theorem, we need a few results.

LEMMA 3. *Let z be a non-zero complex number and let λ be any positive real number. Let $a_0 = 1$, $a_1, \ldots$, denote the coefficients of the power series expansion of $(1-zu)^{-\lambda}$ around $u = 0$; then*

$$a_n = \frac{\lambda(\lambda+1)\ldots(\lambda+n-1)}{n!} z^n = \frac{z^n n^{\lambda-1}}{\Gamma(\lambda)}\left[1+\frac{1}{2n}(\lambda^2-\lambda)+O\left(\frac{1}{n^2}\right)\right].$$

Proof. This follows by applying Euler–Maclaurin summation formula to the function $\log(\lambda+x)$ on the interval $[0, n]$ and then applying Stirling's formula.

LEMMA 4. *Let z be a complex number of absolute value >1 and let ϱ be any positive real number. Then*

$$\sigma_n = \sum_{\nu=1}^{n} \frac{z^\nu}{\nu^\varrho} = \frac{z}{z-1}\frac{z^n}{n^\varrho}\left[1+\frac{\varrho}{z-1}\frac{1}{n}+O\left(\frac{\log n}{n^2}\right)\right].$$

Proof. Since $|z^n n^{-\varrho}/z^{n+1}(n+1)^{-\varrho}|$ approaches the limit $|1/z| < 1$, therefore

$$\sigma_n \ll |z|^n/n^\varrho.$$

We put

$$N = \left[\frac{(\varrho+2)\log n}{\log|z|}\right]+1, \qquad n' = n-N+1;$$

since

$$\sigma_{n-N} \ll |z|^{n-N} \leqslant |z|^n/n^{\varrho+2},$$

therefore it suffices to show that

(a) $$\sum_{\nu=n'}^{n} \frac{z^\nu}{\nu^\varrho} = \frac{z}{z-1}\frac{z^n}{n^\varrho}\left[1+\frac{\varrho}{z-1}\frac{1}{n}+O\left(\frac{\log n}{n^2}\right)\right].$$

We write the left-hand side of (a) as $S+T$, where

(b) $$S = \frac{1}{n^\varrho}\sum_{\nu=n'}^{n} z^\nu = \frac{z}{z-1}\frac{z^n}{n^\varrho}+O\left(\frac{|z|^n}{n^{2\varrho+2}}\right)$$

and

(c) $$T = \sum_{\nu=n'}^{n} \frac{z^\nu}{\nu^\varrho}\left(1-\left(\frac{\nu}{n}\right)^\varrho\right) = \sum_{\nu=n'}^{n} \frac{z^\nu}{\nu^\varrho}\left[\varrho\frac{n-\nu}{n}+O\left(\frac{n-\nu}{n}\right)^2\right]$$

$$= \varrho U+O(V),$$

with

$$U = \sum_{\nu=n'}^{n} \frac{z^\nu}{\nu^\varrho}\frac{n-\nu}{n}, \qquad V = \sum_{\nu=n'}^{n} \frac{|z|^\nu}{\nu^\varrho}\left(\frac{n-\nu}{n}\right)^2.$$

Since $n' \leqslant \nu \leqslant n$, we see that

(d) $$V \ll \frac{\log n}{n^{\varrho+2}}\sum_{\nu=n'}^{n} |z|^\nu(n-\nu) \ll \frac{\log n}{n^{\varrho+2}}|z|^n.$$

Next

$$U = \sum_{\nu=n'}^{n} \frac{z^\nu}{n^\varrho}\left(\frac{n-\nu}{n}\right)+\sum_{\nu=n'}^{n} z^\nu\frac{n-\nu}{n}\left(\frac{1}{\nu^\varrho}-\frac{1}{n^\varrho}\right);$$

the first term on the right-hand side of U is

$$\frac{z}{(z-1)^2}\frac{z^n}{n^{\varrho+1}}+O\left(\frac{\log n}{n^{2\varrho+3}}|z|^n\right),$$

and the second sum on the right-hand side of U is

$$\sum_{\nu=n'}^{n} \frac{z^\nu}{\nu^\varrho}\frac{n-\nu}{n}\left(1-\left(\frac{\nu}{n}\right)^\varrho\right) \ll \sum_{\nu=n'}^{n} \frac{|z|^\nu}{\nu^\varrho}\left(\frac{n-\nu}{n}\right)^2 = V \ll \frac{\log n}{n^{\varrho+2}}|z|^n.$$

Thus

(e) $$U = \frac{z}{(z-1)^2}\frac{z^n}{n^{\varrho+1}}+O\left(\frac{\log n}{n^{\varrho+2}}|z|^n.\right)$$

Combining (b), (c), (d) and (e), we obtain the desired relation (a).

The following corollary follows immediately from Lemmas 3 and 4.

COROLLARY. *Let z be a complex number with $|z|>1$ and let λ be any positive real number <1. Let $a_0 = 1$, $a_1, \ldots$ denote the coefficients of the* *power series expansion of* $(1-zu)^{-\lambda}$ *around* $u=0$, *then*

$$S_n = a_0+\ldots+a_n = \beta\frac{z^n}{n^{1-\lambda}}\left[1+\frac{\gamma}{n}+O\left(\frac{\log n}{n^2}\right)\right],$$

where

(27) $$\beta = \frac{1}{\Gamma(\lambda)}\left(\frac{z}{z-1}\right), \quad \gamma = (1-\lambda)\left[\frac{1}{z-1}-\frac{\lambda}{2}\right].$$

We are now in a position to prove Theorem 1. Write

$$\psi(u) = \sum_{\nu=0}^{\infty} c_\nu u^\nu \quad (|u|<|z|^{-1/2}),$$

and as in the above corollary, write

$$(1-zu)^{-\lambda} = \sum_{\nu=0}^{\infty} a_\nu u^\nu \quad (|u|<|z|^{-1}),$$

$$S_n = \sum_{\nu=0}^{n} a_\nu .$$

Then

$$\sum_{\nu=0}^{n} b_\nu = \sum_{\nu=0}^{n} c_\nu S_{n-\nu} = X+Y,$$

where

$$X = \sum_{\nu=0}^{N-1} c_\nu S_{n-\nu}, \qquad Y = \sum_{\nu=N}^{n} c_\nu S_{n-\nu},$$

with

$$N = \left[\frac{8\log n}{\log|z|}\right]+1.$$

It is an immediate consequence of the corollary to Lemma 4 that

$$S_n \ll |z|^n/n^{1-\lambda} \ll |z|^n,$$

and hence

$$Y \ll \sum_{\nu=N}^{n} |c_\nu|\,|z|^{n-\nu} \ll \frac{|z|^n}{n^3}\sum_{\nu=N}^{\infty}|c_\nu|\,|z|^{-5\nu/8} \ll \frac{|z|^n}{n^3};$$

thus to prove Theorem 1, it will suffice to show that

(28) $$X = \frac{bz^n}{n^{1-\lambda}}\left[1+\frac{c}{n}+O\left(\frac{\log n}{n^2}\right)\right].$$

By applying the corollary to Lemma 4, we see that

(29) $$X = \beta z^n\left(X'+\gamma X''+O(X''')\right)$$

where β and γ are as in (27) and where

(29′) $$X' = \sum_{\nu=0}^{N-1} c_\nu z^{-\nu}(n-\nu)^{\lambda-1},$$

(29″) $$X'' = \sum_{\nu=0}^{N-1} c_\nu z^{-\nu}(n-\nu)^{\lambda-2},$$

(29‴) $$X''' = \sum_{\nu=0}^{N-1} |c_\nu|\,|z|^{-\nu}(n-\nu)^{\lambda-3}\log(n-\nu).$$

Write

$$X' = \frac{1}{n^{1-\lambda}}\sum_{\nu=0}^{N-1} c_\nu z^{-\nu}+\sum_{\nu=0}^{N-1} c_\nu z^{-\nu}\left(\frac{1}{(n-\nu)^{1-\lambda}}-\frac{1}{n^{1-\lambda}}\right)$$

$$= \psi(z^{-1})\frac{1}{n^{1-\lambda}}-\frac{1}{n^{1-\lambda}}\sum_{\nu=N}^{\infty} c_\nu z^{-\nu}+\sum_{\nu=0}^{N-1}\frac{c_\nu z^{-\nu}}{(n-\nu)^{1-\lambda}}\left(1-\left(1-\frac{\nu}{n}\right)^{1-\lambda}\right)$$

$$= \psi(z^{-1})\frac{1}{n^{1-\lambda}}-S+T \text{ (say)};$$

now

(a) $$S \ll \frac{1}{n^{4-\lambda}}\sum_{\nu=N}^{\infty}|c_\nu|\,|z|^{-5\nu/8} \ll \frac{1}{n^{4-\lambda}},$$

and

$$T = \sum_{\nu=0}^{N-1}\frac{c_\nu z^{-\nu}}{(n-\nu)^{1-\lambda}}\left[(1-\lambda)\frac{\nu}{n}+O\left(\frac{\nu^2}{n^2}\right)\right] = \frac{1-\lambda}{n}T'+O(T''),$$

where

$$T'' = \sum_{\nu=0}^{N-1}\frac{|c_\nu|\,|z|^{-\nu}}{(n-\nu)^{1-\lambda}}\frac{\nu^2}{n^2} \ll \frac{\log n}{n^{3-\lambda}}\sum_{\nu=0}^{N-1}\nu|c_\nu|\,|z|^{-\nu} \ll \frac{\log n}{n^{3-\lambda}},$$

and

$$T' = \sum_{\nu=0}^{N-1}\frac{\nu c_\nu z^{-\nu}}{(n-\nu)^{1-\lambda}} = \frac{1}{n^{1-\lambda}}\sum_{\nu=0}^{N-1}\nu c_\nu z^{-\nu}+\sum_{\nu=0}^{N-1}\nu c_\nu z^{-\nu}\left(\frac{1}{(n-\nu)^{1-\lambda}}-\frac{1}{n^{1-\lambda}}\right)$$

$$= \frac{\psi'(z^{-1})}{z}\frac{1}{n^{1-\lambda}}-\frac{1}{n^{1-\lambda}}\sum_{\nu=N}^{\infty}\nu c_\nu z^{-\nu}+O\left(\sum_{\nu=0}^{N-1}\frac{\nu^2}{n}\frac{|c_\nu|\,|z|^{-\nu}}{(n-\nu)^{1-\lambda}}\right)$$

$$= \frac{\psi'(z^{-1})}{z}\frac{1}{n^{1-\lambda}}+O\left(\frac{1}{n^{4-\lambda}}\sum_{\nu=N}^{\infty}\nu|c_\nu|\,|z|^{-5\nu/8}\right)+O\left(\frac{\log n}{n^{2-\lambda}}\right)$$

$$= \frac{\psi'(z^{-1})}{z}\frac{1}{n^{1-\lambda}}+O\left(\frac{\log n}{n^{2-\lambda}}\right).$$

Thus

(b) $$T = (1-\lambda)\frac{\psi'(z^{-1})}{z}\frac{1}{n^{2-\lambda}} + O\left(\frac{\log n}{n^{3-\lambda}}\right).$$

Combining (a) and (b) we see that

(30) $$X' = \psi(z^{-1})\frac{1}{n^{1-\lambda}} + \frac{(1-\lambda)\psi'(z^{-1})}{z}\frac{1}{n^{2-\lambda}} + O\left(\frac{\log n}{n^{3-\lambda}}\right).$$

Similar (and easier) calculations give

(31) $$X'' = \psi(z^{-1})\frac{1}{n^{2-\lambda}} + O\left(\frac{1}{n^{3-\lambda}}\right),$$

(32) $$X''' = O\left(\frac{\log n}{n^{3-\lambda}}\right).$$

Relation (29) combined with relations (30), (31) and (32) gives the desired relation (28) and hence completes the proof of Theorem 1.

References

[1] J. W. S. Cassels and A. Fröhlich, *Algebraic number theory*, Academic Press, London and New York 1967.
[2] E. Landau, *Über die Einteilung der positive ganzen Zahlen in vier Klassen nach der Minderzahl der zu ihrer additiven Zusammensetzung erfordlichen Quadrate*, Archiv der Math. und Physik (3), 13 (1908), pp. 305–312.
[3] I. S. Luthar, *A generalization of a theorem of Landau*, Acta Arith. 12 (1967), pp. 223–228.
[4] A. Weil, *Basic number theory*, 2nd ed., Springer-Verlag, 1973.
[5] — *Courbes algebriques et variétés abeliennes*, Hermann, Paris 1971.

DEPARTMENT OF MATHEMATICS
PANJAB UNIVERSITY
Chandigarh, India

Received on 18. 3. 1977
and in revised form on 4. 5. 1978 (927)

ACTA ARITHMETICA
XXXVIII (1981)

On an extension of a theorem of S. Chowla

by

TADASHIGE OKADA (Hachinohe, Japan)

1. Introduction. In [4] S. Chowla proved that if p is an odd prime, then the $(p-1)/2$ real numbers $\cot(2\pi a/p)$, $a = 1, 2, \ldots, (p-1)/2$ are linearly independent over the field Q of rational numbers. Other proofs were given by H. Hasse [5], R. Ayoub [1], [2] and T. Okada [8].

The purpose of this note is to show the following theorem, which is an extension of S. Chowla's theorem mentioned above.

THEOREM. *Let k and q be integers with $k > 0$ and $q > 2$. Let T be a set of $\varphi(q)/2$ representatives* mod q *such that the union $\{T, -T\}$ is a complete set of residues prime to q. Then the real numbers $D^{k-1}(\cot\pi z)|_{z=a/q}$, $a \in T$ are linearly independent over Q, where φ is the Euler totient function and $D = d/dz$.*

In the case $k = 2$, this corresponds to the result of H. Jager and H. W. Lenstra, Jr. [6].

2. Preliminary results. We put

$$F_k(z) = \begin{cases} \dfrac{k}{(-2\pi i)^k} D^{k-1}(\pi\cot\pi z) & \text{if } z \text{ is not an integer,} \\ 0 & \text{if } z \text{ is an integer and } k \text{ is odd,} \\ B_k & \text{if } z \text{ is an integer and } k \text{ is even,} \end{cases}$$

where B_k is the kth Bernoulli number. Then we have the following partial fraction decomposition of $F_k(z)$:

(1) $$F_k(z) = -\frac{k!}{(2\pi i)^k}\sum_{n=-\infty}^{\infty}{}' \frac{1}{(z+n)^k},$$

where the dash $'$ means that the term with $n = -z$ is omitted if z is an integer. (If $k = 1$, we interpret the sum as grouping the corresponding positive and negative terms together.)