Conspectus materiae tomi XXXIX, fasciculi 1

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

ISBN 83-01-01337-0 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
XXXIX (1981)

Another proof of Iwasawa's class number formula

by

LADISLAV SKULA (Brno)

1. Introduction. K. Iwasawa ([3]) has proved that the first class number factor of the p^{n+1}th cyclotomic field F_n (p is an odd prime and $n \geqslant 0$) is equal to the group index $[\mathfrak{R}^-:\mathfrak{I}^-]$, were $\mathfrak{R}^-$ and $\mathfrak{I}^-$ are certain subgroups of the additive group of the group ring $\boldsymbol{Z}[G_n]$ of the group G_n over the ring of rational integers $\boldsymbol{Z}$. The group G_n denotes the Galois group of F_n over the rational field $\boldsymbol{Q}$.

Iwasawa's proof is based on the representations of a semi-simple algebra. In the present paper, we shall give another proof of this Iwasawa's formula based on the presentation of a special basis of $\mathfrak{I}^-$. By the calculation of the determinant of the transition matrix from a certain basis of $\mathfrak{R}^-$ to this basis of $\mathfrak{I}^-$ we obtain Iwasawa's class number formula or the p^{n+1}th cyclotomic field.

2. Notation. In this paper the following symbols are used:

p an odd prime,

n a non-negative integer,

h_n^- the first factor of the class number of the cyclotomic field generated by p^{n+1}th roots of unity over the rational field,

$\boldsymbol{Z}$ the ring of integers,

$q = p^{n+1}$,

$M = p^n(p-1)$,

$N = M/2$,

r a primitive root modulo q,

r_j the integer ($j \in \boldsymbol{Z}$), $0 < r_j < q$,

$$r_j \equiv r^j \pmod q \quad \text{for} \quad j \geqslant 0,$$

$$r_j r^{-j} \equiv 1 \pmod q \quad \text{for} \quad j < 0,$$

$\sum_j \delta_j = \sum_{j=0}^{M-1} \delta_j$ for suitable symbols δ_j,

$F(X) = \sum_j r_j X^j$ polynomial over the complex field,

θ a primitive Mth root of unity,
G a cyclic group of order M (written multiplicatively),
s a generator of G; thus $G = \{1, s, s^2, \ldots, s^{M-1}\}$,
$\mathfrak{R} = \boldsymbol{Z}[G]$ the group ring of G over $\boldsymbol{Z}$; thus

$$\mathfrak{R} = \Big\{\sum_j a_j s^j:\ a_j \in \boldsymbol{Z}\Big\},$$

$\omega_0 = \sum_j r_{-j} s^j$,
$\mathfrak{I} = \{\alpha \in \mathfrak{R}:\ \exists \varrho \in \mathfrak{R},\ \varrho\omega_0 = q\alpha\}$,
$\mathfrak{R}^- = \{\alpha \in \mathfrak{R}:\ (1+s^N)\alpha = 0\}$,
$\mathfrak{I}^- = \mathfrak{I} \cap \mathfrak{R}^-$.

3. The expressing of h_n^- as a determinant. From [2] we obtain the following formula:

$$h_n^- = \frac{1}{(2q)^{N-1}}\,|F(\theta)F(\theta^3)\ldots F(\theta)^{M-1}|. \tag{1}$$

For and odd k we get

$$F(\theta^k) = \sum_i r_i \theta^{ik} = \sum_{i=0}^{N-1} (r_i - r_{N+i})\,\theta^{ik},$$

therefore

$$F(\theta^k) = \sum_{i=0}^{N-1} (r_{i+j} - r_{N+i+j})\,\theta^{(i+j)k}$$

for each $0 \leqslant j \leqslant N-1$.

Put

$$C = (\theta^{(2l+1)i})_{0\leqslant l,i\leqslant N-1}, \qquad A = (r_{N+i+j} - r_{i+j})_{0\leqslant i,j\leqslant N-1},$$

$$D = C\cdot A = (d_{lj})_{0\leqslant l,j\leqslant N-1}.$$

Then

$$d_{lj} = -\sum_{i=0}^{N-1} (r_{i+j} - r_{N+i+j})\,\theta^{(2l+1)(i+j)}\theta^{-(2l+1)j} = -\theta^{-(2l+1)j}F(\theta^{2l+1}),$$

hence

$$|\det D| = |F(\theta)F(\theta^3)\ldots F(\theta^{M-1})|\cdot|\det C| = |\det C|\cdot|\det A|.$$

It follows from (1)

$$h_n^- = \frac{1}{2q^{N-1}}\,|\det(r_{N+i+j} - r_{i+j})_{0\leqslant i,j\leqslant N-1}|. \tag{2}$$

For $n = 0$ this formula is given in the exercise 5, § 5, Chapter V of [1].

Let us put as for $n = 0$ in [4]

$$b_{00} = q-2,$$
$$b_{0j} = 1 - r_j, \quad 1 \leqslant j \leqslant N-1,$$
$$b_{i0} = 1 - r_i, \quad 1 \leqslant i \leqslant N-1,$$
$$b_{ij} = \frac{1}{q}(r_i r_j - r_{r+j}), \quad 1 \leqslant i,\ j \leqslant N-1,$$
$$B = (b_{ij})_{0\leqslant i,j\leqslant N-1}.$$

By the same way as for $n = 0$ in [4] $(A = (q - 2r_{i+j})_{0\leqslant i,j\leqslant N-1}$, subtraction of the row 0 of A from every other row, removing of the factor 2 from the last $N-1$ rows, subtraction of r_j times the column 0 from the column j $(1 \leqslant j \leqslant N-1)$ and removing of the factor q from the last $N-1$ columns) we obtain from (2)

$$h_n^- = |\det B|. \tag{3}$$

4. The basis $\{\alpha_i:\ i \in \mathcal{O}\}$ of $\mathfrak{I}^-$. If $\alpha = \sum_j a_j s^j \in \mathfrak{I}$, then there exists $\varrho = \sum_t x_t s^t \in \mathfrak{R}$ $(a_j, x_t \in \boldsymbol{Z})$ such that $\varrho\cdot\omega_0 = q\cdot\alpha$. Hence $q\alpha = \sum_k r_{-k}s^k \sum_t x_t s^t = \sum_j s^j \sum_t x_t r_{-j+t}$ and it follows $a_j = \frac{1}{q}\sum_t x_t r_{-j+t}$ for each $0 \leqslant j \leqslant M-1$.

Let conversely $x_t \in \boldsymbol{Z}$ $(0 \leqslant t \leqslant M-1)$, $\sum_t x_t r_t \equiv 0 \pmod q$ and $a_j = \frac{1}{q}\sum_t x_t r_{-j+t}$ $(0 \leqslant j \leqslant M-1)$. Then $a_j \in \boldsymbol{Z}$ and $\alpha = \sum_j a_j s^j \in \mathfrak{R}$. Put $\varrho = \sum_t x_t s^t$. Then

$$\varrho \in \mathfrak{R} \quad\text{and}\quad \varrho\cdot\omega_0 = \sum_t x_t s^t \sum_k r_{-k}s^k = \sum_j s^j \sum_t x_t r_{-j+t} = q\alpha.$$

Therefore we have

$$\mathfrak{I} = \Big\{\alpha = \sum_j a_j s^j:\ a_j = \frac{1}{q}\sum_t x_t r_{-j+t},\ x_t \in \boldsymbol{Z},\ \sum_t x_t r_t \equiv 0 \pmod q\Big\}. \tag{4}$$

It is easy to see that it holds

$$\mathfrak{R}^- = \Big\{\alpha = \sum_j a_j s^j:\ a_j \in \boldsymbol{Z},\ a_j + a_{j+N} = 0,\ 0 \leqslant j \leqslant N-1\Big\},$$

$$\mathfrak{I}^- = \Big\{\alpha = \sum_j a_j s^j:\ a_j = \frac{1}{q}\sum_t x_t r_{-j+t},\ x_t \in \boldsymbol{Z},\ \sum_t x_t r_t \equiv 0 \pmod q,\ \sum_t x_t = 0\Big\}. \tag{5}$$

Put $\mathcal{O} = \{i \in \mathbf{Z}:\ 0 \leqslant i < M,\ r_i \text{ odd}\}$ and for $0 \leqslant j \leqslant M-1$, $i \in \mathcal{O}$ put

$$a_{ij} = \frac{r_{-j}r_i - r_{-j+i}}{q} + \frac{1-r_i}{2}, \quad i \neq 0, \tag{6}$$

$$a_{0j} = 2r_{-j} - q.$$

Further put for $i \in \mathcal{O}$

$$a_i = \sum_j a_{ij} s^j. \tag{7}$$

Suppose that $i \in \mathcal{O}$, $i \neq 0$. If we put

$$x_t = \begin{cases} (1+r_i)/2 & \text{for} \quad t = 0, \\ -1 & \text{for} \quad t = i, \\ (1-r_i)/2 & \text{for} \quad t = N \\ 0 & \text{for} \quad 0 \leqslant t \leqslant M-1,\ t \neq 0, i, N, \end{cases}$$

we get $\sum_t x_t = 0$, $\sum_t x_t r_t \equiv 0 \pmod q$ and $\sum_t x_t r_{-j+t} = q a_{ij}$ for each $0 \leqslant j \leqslant M-1$. Hence $a_i \in \mathfrak{J}^-$.

If we put

$$x_t = \begin{cases} q & \text{for} \quad t = 0, \\ -q & \text{for} \quad t = N, \\ 0 & \text{for} \quad 0 \leqslant t \leqslant M-1,\ t \neq 0, N, \end{cases}$$

we get $\sum_t x_t = 0$, $\sum_t x_t r_t \equiv 0 \pmod q$ and $\sum_t x_t r_{-j+t} = q a_{0j}$ for each $0 \leqslant j \leqslant M-1$. Hence $a_0 \in \mathfrak{J}^-$.

Then we have

$$a_i \in \mathfrak{J}^- \quad \text{for each } i \in \mathcal{O}. \tag{8}$$

Let $\beta = \sum_j b_j s^j \in \mathfrak{J}^-$. According to (5) there exists $x_t \in \mathbf{Z}$ $(0 \leqslant t \leqslant M-1)$ such that $\sum_t x_t r_t \equiv 0 \pmod q$, $\sum_t x_t = 0$ and $b_j = \frac{1}{q}\sum_t x_t r_{-j+t}$ $(0 \leqslant j \leqslant M-1)$.

Put $y_t = x_t - x_{t'}$ for $t \in \mathcal{O}$, where $0 \leqslant t' < M-1$, $t' \equiv t+N \pmod M$. Further put $c = \sum_{t \in \mathcal{O}} y_t r_t$. Since $r_t \equiv 1 \pmod 2$ $(t \in \mathcal{O})$ and $\sum_t x_t = 0$ we have $c \equiv 0 \pmod 2$. Since $r_t \equiv -r_{t+N} \pmod q$ for each $t \in \mathbf{Z}$ and $\sum_t x_t r_t \equiv 0 \pmod q$ it holds $c \equiv 0 \pmod q$. Therefore there exists $d \in \mathbf{Z}$ such that $c = 2qd$. By computation we obtain

$$b_j = -\sum_{\substack{t \in \mathcal{O} \\ t \neq 0}} y_t a_{tj} + d(2r_{-j} - q) \qquad (0 \leqslant j \leqslant M-1).$$

It follows that

$$\beta = -\sum_{\substack{t \in \mathcal{O} \\ t \neq 0}} y_t a_t + d a_0,$$

therefore

(9) *$\{a_i:\ i \in \mathcal{O}\}$ is a system of generators of the additive group $\mathfrak{J}^-$.*

The additive group $\mathfrak{R}^-$ has a basis $s^j(1-s^N)$, $0 \leqslant j < N$. The determinant Δ of the transition matrix from this basis to the system of generators $\{a_i:\ i \in \mathcal{O}\}$ is equal to $\det(a_{ij})_{i \in \mathcal{O}, 0 \leqslant j \leqslant N-1}$.

If we subtract the column 0 from every other column, we obtain

$$\Delta = \begin{vmatrix} 2-q & \dots & 2(r_{-j}-1) & \dots \\ \vdots & & \vdots & \\ \frac{1-r_i}{2} & \dots & \frac{r_{-j}r_i - r_{-j+i}}{q} & \dots \\ \vdots & & \vdots & \end{vmatrix} = -\begin{vmatrix} q-2 & \dots & 1-r_{-j} & \dots \\ \vdots & & \vdots & \\ 1-r_i & \dots & \frac{r_{-j}r_i - r_{-j+i}}{q} & \dots \\ \vdots & & \vdots & \end{vmatrix}.$$

Since $r_{-j} = r_{M-j}$ we have

$$|\Delta| = \left\|\begin{matrix} q-2 & \dots & 1-r_{j+N} & \dots \\ \vdots & & \vdots & \\ 1-r_i & \dots & \frac{r_{j+N}r_i - r_{j+i+N}}{q} & \dots \\ \vdots & & \vdots & \end{matrix}\right\|_{\substack{i \in \mathcal{O}, i \neq 0 \\ 1 \leqslant j < N}}.$$

If we add the column 0 to every other column, we obtain, according to $r_{j+N} = q - r_j$

$$|\Delta| = \left\|\begin{matrix} q-2 & \dots & 1-r_j & \dots \\ \vdots & & \vdots & \\ 1-r_i & \dots & \frac{r_i r_j - r_{i+j}}{q} & \dots \\ \vdots & & \vdots & \end{matrix}\right\|_{\substack{i \in \mathcal{O}, i \neq 0 \\ 1 \leqslant j < N}}.$$

If we add the row 0 to the ith row for each $i \geqslant N$, we get, according to $r_i + r_{i-N} = q$ and (3),

$$h_n^- = |\Delta|. \tag{10}$$

From the results we obtain the following theorem.

THEOREM. *The system $\{a_i:\ i \in \mathcal{O}\}$ is a basis of the additive group $\mathfrak{J}^-$ and for the determinant Δ of the transition matrix from the basis $s^j(1-s^N)$, $0 \leqslant j < N$ of the additive group $\mathfrak{R}^-$ to the basis $\{a_i:\ i \in \mathcal{O}\}$ of the additive group $\mathfrak{J}^-$ there holds*

$$h_n^- = |\Delta|.$$

Therefore $h_n^- = [\mathfrak{R}^- : \mathfrak{J}^-]$.

References

[1] Z. I. Borevič and I. R. Šafarevič, *Number theory*, New York 1966.
[2] H. Hasse, *Über die Klassenzahl abelscher Zahlkörper*, Berlin 1952.
[3] K. Iwasawa, *A class number formula for cyclotomic fields*, Ann. of Math. 76 (1) (1962), pp. 171–179.
[4] M. Newman, *A table of the first factor for prime cyclotomic fields*, Math. Comp. 24 (109) (1970), pp. 215–219.

Received on 25. 11. 1977 (1004)

ACTA ARITHMETICA
XXXIX (1981)

The primality of certain integers of the form $2Ar^n-1$

by

H. C. WILLIAMS (Winnipeg)

1. Introduction. In [6] Lucas presented conditions which are sufficient for integers of the form Br^n-1 $(B < r^n)$ $r = 2, 3, 5$, to be prime. Lehmer [4], Riesel [7] and Stechkin [8] have given criteria which are both necessary and sufficient for the primality of $A2^n-1$ $(A < 2^n)$ and Williams [10], [12] has given necessary and sufficient conditions for the primality of $2A3^n-1$ $(A < 3^n)$ and $A2^n3^m-1$ $(A < 2^{n+1}3^m)$. All of these tests make use of Lucas functions or functions similar to the Lucas functions. In this paper we present, using the Lucas functions together with the generalized Lehmer functions of [11], a necessary and sufficient criterion for the primality of certain numbers of the form $N = 2Ar^n-1$ $(A < r^n)$ when r and s are odd primes, $r = 2s+1$, and $2A-1$ is a primitive root of s.

We define the Lucas functions

$$V_n(P, Q) = \alpha^n+\beta^n, \qquad U_n(P, Q) = (\alpha^n-\beta^n)/(\alpha-\beta),$$

where α, β are the roots of the auxiliary quadratic

$$x^2-Px+Q = 0$$

and P, Q are coprime integers. (While it is usual to insist that $(P, Q) = 1$, it is sufficient in dealing with the functions modulo N to have $(N, Q) = 1$.) The usual test for the primality of $N = Br^n-1$ $(B < r^n)$ (see, for example, Brillhart, Lehmer, Selfridge [1]) involves attempting to find P, Q such that $(Q, N) = 1$ and

$$N \mid U_{N+1}(P, Q), \tag{1.1}$$

$$\big(N,\ U_{(N+1)/r}(P, Q)\big) = 1. \tag{1.2}$$

If such a pair P, Q can be found, N is a prime. The determination of this pair is done by trial, subject to the constraint that the Jacobi symbol $(P^2-4Q \mid N) = -1$. Under this constraint, if (1.1) is not satisfied, N is composite.