[6] C. L. Siegel, *Über die Diskriminante total reeller Körper*, Gott. Nachr. (1922), p. 17-24.
[7] — *Neuer Beweis des Satzes von Minkowski über lineare Formen*, Math. Annalen 87 (1922), p. 36-38.
[8] — *Über Gitterpunkte in konvexen Körpern und ein damit zusammenhängendes extremal Problem*, Acta Math. 65 (1935), p. 307-323.
[9] — *Über die analytische Theorie der quadratischen Formen*, Annals of Math. 36 (1935), p. 527-606.
[10] — *Discontinuous groups*, ibid. 44 (1943), p. 674-689.
[11] — *Quadratic forms*, Tata Institute of Fundamental Research, Bombay 1957.

TATA INSTITUTE OF FUNDAMENTAL RESEARCH, BOMBAY

Reçu par la Rédaction le 27. 12. 1958

Added in proof (5 August 1959). Professor Carl Siegel informs me (23 July 1959) that the theorem on splitting of rational quaternion algebras, which is deduced in § 6 as a consequence of formula (21), has been proved already by E. Witt (*Über ein Gegenbeispiel zum Normensatz*, Math. Zeit. 39 (1935), p. 467) by using number geometric methods.

ACTA ARITHMETICA
V (1959)

Note on a theorem of S. Uchiyama

by

L. CARLITZ (Durham, North Carolina)

Let $Z(m, n)$ denote the number of systems of complex numbers $(z_1, z_2, \ldots, z_n)$ satisfying the system of equations

$$s_{m+1} = s_{m+2} = \ldots = s_{m+n-1} = 0,$$

where

$$s_k = z_1^k + z_2^k + \ldots + z_n^k$$

and m is an integer $\geqslant 0$. Two systems $(z_1, z_2, \ldots, z_n)$ and $z_1', z_2', \ldots, z_n'$ are *equivalent* in $Z(m, n)$ if there exists a complex number $\lambda \neq 0$ such that

$$f(x; z_1, z_2, \ldots, z_n) = f(x; \lambda z_1', \lambda z_2', \ldots, \lambda z_n'),$$

where

$$f(x; z_1, z_2, \ldots, z_n) = \prod_{j=1}^{n} (x - z_j).$$

Let $B(m, n)$ denote the number of classes of non-trivial sets relative to this equivalence relation. In a recent paper [1], Uchiyama has proved that

$$\sum_{d|(m,n)} a(d) B\left(\frac{m}{d}, \frac{n}{d}\right) = \frac{(m+n-1)!}{m!\, n!}, \tag{1}$$

where

$$a(1) = 1 \quad \text{and} \quad a(n) = n^{-1} \prod_{p|n} (1-p),$$

the product extending over all distinct prime divisors of n. A consequence of (1) is the elegant reciprocity relation

$$B(m, n) = B(n, m), \tag{2}$$

as noted by Uchiyama.

We should like to point out that (1) implies the explicit result

$$B(m,n)=\sum_{d\mid(m,n)}\frac{\varphi(d)}{d}\,C\left(\frac{m}{d},\frac{n}{d}\right), \tag{3}$$

where $\varphi(d)$ is the Euler φ-function and

$$C(m,n)=\frac{(m+n-1)!}{m!\,n!}.$$

Indeed, $B(m,n)$ is uniquely determined by (1). Thus it will suffice to verify that the value of $B(m,n)$ furnished by (3) does satisfy (1).

We have

$$\sum_{d\mid(m,n)}a(d)\,B\left(\frac{m}{d},\frac{n}{d}\right)=\sum_{d\mid(m,n)}a(d)\sum_{\delta\mid\left(\frac{m}{d},\frac{n}{d}\right)}\frac{\varphi(\delta)}{\delta}\,C\left(\frac{m}{d\delta},\frac{n}{d\delta}\right)$$

$$=\sum_{t\mid(m,n)}C\left(\frac{m}{t},\frac{n}{t}\right)\sum_{d\delta=t}\frac{a(d)\,\varphi(\delta)}{\delta}.$$

Thus it is only necessary to show that

$$\sum_{d\delta=t}\frac{a(d)\varphi(\delta)}{\delta}=\begin{cases}1 & \text{for } t=1,\\ 0 & \text{for } t>1.\end{cases} \tag{4}$$

Since both $a(d)$ and $\varphi(\delta)/\delta$ are factorable and the Dirichlet product of factorable functions is again factorable, it suffices to prove (4) when $t=p^r$. In this case the left member of (4) reduces to

$$\sum_{d\delta=p^r}\frac{a(d)\varphi(\delta)}{\delta}=\varphi(1)a(p^r)+\frac{\varphi(p)}{p}a(p^{r-1})+\ldots+\frac{\varphi(p^r)}{p^r}a(1)$$

$$=\frac{1-p}{p^r}+\frac{p-1}{p}\cdot\frac{1-p}{p^{r-1}}+\frac{p(p-1)}{p^2}\cdot\frac{1-p}{p^{r-2}}+\ldots$$

$$+\frac{p^{r-2}(p-1)}{p^{r-1}}\cdot\frac{1-p}{p}+\frac{p^{r-1}(p-1)}{p^r}$$

$$=\frac{1-p}{p^r}\{1+(p-1)+p(p-1)+\ldots+p^{r-2}(p-1)\}+\frac{p-1}{p}$$

$$=\frac{1-p}{p^r}p^{r-1}+\frac{p-1}{p}=0$$

for $r>0$. For $r=0$, the result is obvious. Thus (4) is proved.

In a letter to the writer, Uchiyama has asked whether one can show directly that the right member of (3) is integral. This can be done as follows. Define $B(m,n)$ by means of (3). Also put

$$k=(m,n),$$
$$m=m'k,$$
$$n=n'k;$$

then (3) becomes

$$mB(m,n)=\sum_{dt=k}\varphi(d)\binom{(m'+n')t-1}{m't-1}$$

$$=\sum_{rst=k}r\mu(s)\binom{(m'+n')t-1}{m't-1}$$

$$=\sum_{ru=k}r\sum_{st=u}\mu(s)\binom{(m'+n')t-1}{m't-1}.$$

We have

$$\sum_{st=u}\mu(s)\binom{(m'+n')t-1}{m't-1}\equiv 0\pmod{u}. \tag{5}$$

This result is evidently a consequence of

$$\binom{ap^e-1}{bp^e-1}\equiv\binom{ap^{e-1}-1}{bp^{e-1}-1}\pmod{p^e}, \tag{6}$$

where p is prime. To prove (6), let

$$H_e=\binom{ap^e-1}{bp^e-1}.$$

Then it is clear that

$$H_e=H_{e-1}\prod_{\substack{j=1\\ p\nmid j}}^{bp^e}\frac{ap^e-j}{bp^e-j}.$$

Clearly the product on the right $\equiv 1\pmod{p^e}$ and (6) follows at once. (A stronger result can be obtained easily but this is unnecessary for our purpose.)

In view of (5) we have

$$mB(m,n)\equiv 0\pmod{k};$$

in the same way

$$nB(m, n) \equiv 0 \pmod{k}.$$

Hence if $k = mm_1 + nn_1$, we get

$$kB(m, n) \equiv 0 \pmod{k},$$

and therefore $B(m, n)$ is integral.

Reference

[1] S. Uchiyama, *Sur un problème posé par M. Paul Turán*, Acta Arithmetica 4 (1958), p. 240-246.

DUKE UNIVERSITY

Reçu par la Rédaction le 27. 12. 1958

ACTA ARITHMETICA
V (1959)

Some cyclotomic matrices

by

L. Carlitz (Durham, North Carolina)

1. Introduction. In a recent paper [5] Lehmer remarks that for relatively few matrices M can one give explicit formulas for the determinant, characteristic roots and inverse of A as well as the general element of M^r. He then considers two classes of matrices whose elements involve the Legendre symbol for which these problems are solved explicitly.

Let $\chi(r)$ denote the Legendre symbol (r/p), where p is an odd prime. The first class of matrices is of the type

$$(1.1)\qquad \big(a+b\chi(r)+c\chi(s)+d\chi(rs)\big) \qquad (r, s = 1, \ldots, p-1),$$

where a, b, c, d are constants. The second is of the type

$$(1.2)\qquad \big(c+\chi(a+r+s)\big) \qquad (r, s = 1, \ldots, p-1),$$

where c is arbitrary but a is an integer.

In the present paper we consider some additional classes of matrices for which at least the characteristic roots can be computed. We discuss first the matrix

$$(1.3)\qquad (\varepsilon^{rs}) \qquad (r, s = 0, 1, \ldots, n-1),$$

where $\varepsilon = e^{2\pi i/n}$. This matrix is familiar in connection with Schur's derivation of the value of Gauss's sum ([4], vol. 1, p. 162). By means of his method it is easy to determine the characteristic roots of (1.3) for arbitrary n.

Next if $\chi(r)$ is an arbitrary character $(\mathrm{mod}\, n)$ we consider the matrix of order $\varphi(n)$

$$(1.4)\qquad A = \big(a+b\chi(r)+c\bar{\chi}(s)+d\chi(r)\bar{\chi}(s)\big),$$

where r, s run through the numbers of a reduced residue system $(\mathrm{mod}\, n)$ in some prescribed order. This evidently generalizes (1.1). Similarly the matrix

$$(1.5)\qquad \big(c+\chi(a+r+s)\big) \qquad (r, s = 1, \ldots, p-1)$$