THEOREM. *A necessary and sufficient condition that a non-singular matrix, M, shall be expressible as the product of two skew-symmetric matrices, viz., $M = S_1S_2$, is that every even invariant factor of the linear λ-matrix, $M - \lambda I$, shall be equal to the preceding odd invariant factor.**

UNIVERSITY OF TEXAS.

ON THE FIRST FACTOR OF THE CLASS NUMBER OF A CYCLOTOMIC FIELD.

BY MR. H. S. VANDIVER.

(Read before the American Mathematical Society April 27, 1918.)

LET l be an odd prime rational integer and consider the cyclotomic field defined by $e^{2i\pi/l}$. A number of questions connected with this field depend on the divisibility of its class number by l and its powers. This class number can be expressed as the product of two integral factors one of which (generally referred to as the first factor) is

$$h = \frac{f(Z)f(Z^3)\cdots f(Z^{l-2})}{(2l)^{\frac{1}{2}(l-3)}}, \tag{1}$$

where

$$f(x) = r_0 + r_1x + r_2x^2 + \cdots + r_{l-2}x^{l-2},$$

$Z = e^{2i\pi/l-1}$, r is a primitive root of l, and r_i is the least positive residue of r^i, modulo l.

Kummer† proved that the necessary and sufficient condition that h be divisible by l is that one of the numbers of Bernoulli, B_s, $[s = 1, 2, \cdots, (l-3)/2]$ is divisible by l, a B being termed divisible by an integer i when its denominator is prime to i and its numerator is divisible by i. Kronecker‡ gave another proof which was reproduced by Hilbert.§

* Otherwise expressed, the condition is that the number of integers within parentheses in the characteristic shall always be even, and these alike in pairs. Thus [(2, 2); (3, 3, 1, 1); (1, 1)] is possible, while [(2, 1); (2, 1)]; [2], and [1, 1] are impossible.

† *Journal für die Mathematik*, vol. 40 (1850.)

‡ *Werke*, vol. 1, p. 93.

§ Die Theorie der algebraischen Zahlkörper, Bericht, p. 429.

In the present paper I give an expression for the residue of h modulo l^n, where n is arbitrary, from which it is possible to give necessary and sufficient conditions that h be divisible by a given power of l in terms of Bernoulli numbers. The argument used is a bit different from those employed by Kummer and Kronecker for the special case $n = 1$.

The decomposition of l into ideal prime factors in the field $\Omega(Z)$ shows that one of these prime factors is

$$\mathfrak{P} = (Z - r, l),$$

whence

$$Z \equiv r \pmod{\mathfrak{P}}$$

and

$$Z^{kl^{a'}} \equiv r^{kl^{a'}} \pmod{\mathfrak{P}^{a'+1}}, \qquad a' > \frac{l-3}{2}, \tag{2}$$

where k is an integer. The right-hand member of (1) is unaltered by the substitution $(Z^{l^{a'}}/Z)$; hence from (1) and (2)

$$(2l)^{\frac{1}{2}(l-3)} h \equiv \prod_s f(r^{sl^{a'}}) \pmod{\mathfrak{P}^{a'+1}},$$

where $s = 1, 3, \cdots, l-2$. Since h and $f(r)$ are rational integers and l is not divisible by $\mathfrak{P}^2$, we then obtain, if $a = a' - \frac{1}{2}(l-3)$

$$h \equiv \frac{\prod_s f(r^{sl^{a'}})}{(2l)^{\frac{1}{2}(l-3)}} \pmod{l^{a+1}}. \tag{3}$$

We also have

$$r_i \equiv r^i \pmod{l}, \quad r^{isl^{a'}} \equiv r_i^{sl^{a'}} \pmod{l^{a'+1}}$$

and this gives

$$\frac{f(r^{sl^{a'}})}{l} \equiv \sum_{n=1}^{l-1} \frac{n^{sl^{a'}+1}}{l} \pmod{l^{a'}}. \tag{3a}$$

But since

$$n^{l^a(l^{a'-a}-1)} \equiv 1 \pmod{l^{a+1}},$$

then

$$\sum_{n=1}^{l-1} \frac{n^{sl^{a'}+1}}{l} \equiv \frac{\sum_{n=1}^{l-1} n^{sl^a+1}}{l} \pmod{l^a},$$

and (3) and (3a) give

$$h \equiv \frac{\prod_{s} \sum_{n=1}^{l-1} n^{sl^a+1}}{(2l)^{\frac{1}{2}(l-3)}} \pmod{l^a}. \tag{4}$$

We shall now show that, for s odd,

$$\sum_{n=1}^{l-1} n^{sl^a+1} \equiv (-1)^{(sl^a-1)/2} l B_{(sl^a+1)/2} \pmod{l^{a+1}}. \tag{5}$$

By the Bernouilli summation formula we have if $b_1 = -1/2$, $b_{2a+1} = 0$, and $b_{2a} = (-1)^{a+1}B_a$, where $B_1 = 1/6$, $B_2 = 1/30$, etc., $b_s = b^s$,

$$\sum_{n=1}^{l} n^k = lb^k + l\frac{k}{2} lb^{k-1} + l^2 \frac{k(k-1)}{2\cdot 3} lb^{k-2} + \cdots + \frac{l^r}{r+1}\left(\frac{k}{r}\right) lb^{k-r} + \cdots. \tag{6}$$

By the Staudt-Clausen theorem lb^a is an integer or a fraction whose denominator is prime to l. All the coefficients of lb^a in the right-hand member of (6), commencing with the third, are divisible by l^{a+1}. To prove this, we observe that

$$(b+l)^l \equiv b^l + l^2 b^{l-1} \pmod{l^3}$$

and

$$(b+l)^{sl^a} \equiv b^{sl^a} + sl^{a+1} b^{sl^a-1} \pmod{l^{a+2}},$$

whence

$$(b+l)^{sl^a+2} \equiv b^{sl^a+2} + (sl^a+2) lb^{sl^a+1} + b^{sl^a} l^2 \pmod{l^{a+2}},$$

and

$$\frac{(b+l)^{sl^a+2} - b^{sl^a+2}}{sl^a+2} \equiv lb^{sl^a+1} + \frac{b^{sl^a} l^2}{2} \pmod{l^{a+2}}. \tag{7}$$

The left-hand member of this relation is precisely the right-hand member of (6) if we expand and set $k = sl^a + 1$. Setting b_a for b^a in (7), noting that $b_{sl^a} = 0$ for s odd, and comparing (6) with the new (7), the relation (5) is obtained. We then deduce from (3) and (4)

$$h \equiv \frac{\prod_{s} l(-1)^{(sl^a-1)/2} B_{(sl^a+1)/2}}{2^{\frac{1}{2}(l-3)}} \pmod{l^a}, \tag{8}$$

$s = 1, 3, \cdots, l-2$.

Kummer* has shown that

$$\frac{B_a}{a} \equiv (-1)^{k\mu} \frac{B_{a+k\mu}}{a+k\mu} \pmod{l},$$

where k is an integer and a is not a multiple of $\mu = (l-1)/2$. This gives

$$(-1)^{s\mu} \frac{B_{(sl+1)/2}}{s(l+1)/2} \equiv \frac{B_{(s+1)/2}}{(s+1)/2} \pmod{l},$$

and applying the latter relation to (8) for $a = 1$, we obtain Kummer's result to the effect that the necessary and sufficient condition that h be divisible by l is that one of the Bernoulli numbers B_s, $(s = 1, 2, \cdots, \frac{1}{2}(l-3))$ is divisible by l.

BALA, PA.,
November, 1918.

CORRECTIONS AND NOTE TO THE CAMBRIDGE COLLOQUIUM OF SEPTEMBER, 1916.

BY PROFESSOR G. C. EVANS.

1. *Corrections.* On page 35 in equation (9′) change γ to α. In all the formulas and equations following on page 35 change γ to β and β to α.

On page 37 in equation (12) change γ to β and β to α.

On page 39 in the second equation there should be an i as a factor of each of the last two terms of the integrand.

2. *Note to Art. 27, the Analogue of Green's Theorem.* The approach to the analogue of Green's theorem is clearer if made in the following way, and bears more relation to the development with which we are familiar in calculus. The meaning of equations (17) to (20) is perhaps not clear, as the equations stand. But the invariant $H_{\Phi_1\Phi_1'}$, defined by

$$(V_1 \times V_2) H_{\Phi_1\phi_1'} = W_1 \times W_2', \tag{21}$$

which may be rewritten in the new forms

$$\begin{aligned} H_{\Phi_1\Phi_1'} &= (\beta \cdot W_1)(\beta \cdot W_1') + (\alpha \cdot W_1)(\alpha \cdot W_1') \\ &= -(\beta \cdot W_1)(\alpha \cdot W_2') + (\alpha \cdot W_1)(\beta \cdot W_2'), \end{aligned}$$

* L. c., vol. 41, p. 368.