NOTE ON A CERTAIN RING-CONGRUENCE

BY H. S. VANDIVER

1. *Introduction.* Consider the functions

$$\alpha_1 a_1^n + \alpha_2 a_2^n + \cdots + \alpha_k a_k^n = f_n(\alpha_1, \cdots, \alpha_k),$$

where the a's are rational integers and the α's belong to a ring R including the rational integers. Further, for any a_i prime to m, let

$$a_i^d \equiv 1 \pmod{m}, \qquad (i = 1, 2, \cdots, k).$$

Now we set up the function

$$\alpha_1 a_1^n x^{a_1^d} + \alpha_2 a_2^n x^{a_2^d} + \cdots + \alpha_k a_k^n x^{a_k^d} = f_n(x) = f_n(x, \alpha_1, \cdots, \alpha_k).$$

Consider the operation of differentiating $f_n(x)$ with respect to x and then multiplying the result by x. We shall call this operation $E(f)$. Similarly we shall call $E^{(j)}(f)$ the result of carrying out this operation j times on f. Hence

$$E^{(j)} f_n(x) = f_{n+jd}(x), \tag{1}$$

and

$$[E^{(j)} f_n(x)]_{x=1} = f_{n+jd}(\alpha_0, \alpha_1, \cdots, \alpha_k). \tag{2}$$

Now consider any function of the form

$$H(x) = \sum_h \gamma_h x^h,$$

where the γ's are in R and the summation ranges over any finite number of rational integers, h. If u_1 and u_2 are functions of this type, then it may easily be shown by induction that

$$E^{(j)}(u_1 u_2) = (u_1 + u_2)^j,$$

where on the right we expand by the binomial theorem and replace $(u_1)^t$ by $u_1^{(t)}$ with $u_1^{(t)} = E^{(t)}(u_1)$ and similarly for $(u_2)^s$, with $(u_1)^0 = u_1$; $(u_2)^0 = u_2$. In fact, this scheme corresponds to setting $x = e^v$, where e is the Napierian base, and differentiating $u_1 u_2$, j times with respect to v, if we should assume that R contains the field of all real numbers. More generally we have

(3) $$E^{(j)}(u_1u_2\cdots u_s) = (u_1+u_2+\cdots+u_s)^j,$$

where, in the expression on the right, we expand by the multinomial theorem and replace u_i^r by $u_i^{(r)}$ with $u_i^{(r)}=E^{(r)}(u_i)$; the latter theorem is written in the form

(4) $$(u_1+u_2+\cdots+u_s)^j = \sum \frac{j!}{c_1!c_2!\cdots c_s!} u_1^{c_1}u_2^{c_2}\cdots u_s^{c_s},$$

the summation ranging independently over each set of positive or zero c's satisfying

$$c_1+c_2+\cdots+c_s = j,$$

and further $u_i^0=u_i$.

2. *The Main Theorem.* Write

(5) $$f_{n_i}^{(i)}(x) = \sum_{r=1}^{k_i} \alpha_{ri}a_{ri}^{n_i}x^{a_{ri}^d}.$$

If $(b_1, b_2, \cdots, b_v)$ is the greatest common divisor of $b_1, b_2, \cdots, b_v$, consider the $a_{ri}^{n_i}$'s in (5) which have factors in common with m and let l_i be the greatest common divisor of all such. Consider the product

(6) $$f_{n_1}^{(1)}(x^{\beta_1})f_{n_2}^{(2)}(x^{\beta_2})\cdots f_{n_s}^{(s)}(x^{\beta_s}) = F,$$

where the β's are integers such that

(6a) $$\beta_1+\beta_2+\cdots+\beta_s \equiv 0 \pmod{m}.$$

We now proceed to carry out in two different ways the operation $E^{(j)}(F)$ and finally set $x=1$ in each result. Employing (2) and (3), we find

$$[E^{(j)}(F)]_{x=1} = (f_{n_1}+f_{n_2}+\cdots+f_{n_s})^j,$$

where, after expansion of the right-hand member following (3), we set

$$f_{n_i}^t = \beta^t f_{n_i+td}^{(i)}(\alpha_1, \alpha_2, \cdots, \alpha_{k_i}).$$

Consider a term in $f_{n_i}^{(i)}(x^{\beta_i})$ in which a_{gi} is prime to m,

$$\alpha_{gi}a_{gi}^{n_i}x^{a_{gi}^d\beta_i}.$$

Set $a_{gi}^d = 1 + mq(a_{gi})$; then the above becomes

$$\alpha_{gi} a_{gi}^{n_i} x^{\beta_i + \beta_i mq(a_{gi})}.$$

The terms in our f in which the a_{gi}'s are prime to m may then be written

$$G_i \equiv x^{\beta_i} \sum_g \alpha_{gi} a_{gi}^{n_i} x^{\beta_i mq(a_{gi})},$$

so that

$$f_{n_i}^{(i)}(x^{\beta_i}) = G_i + l_i C(x),$$

where $C(x)$ is a function of the same type as $H(x)$. Since

$$\beta_1 + \beta_2 + \cdots + \beta_s \equiv 0 \pmod{l},$$

then

$$\prod_{i=1}^{s} G_i$$

can be expressed as the sum of terms of the form $Ax^{m\gamma}$, where A belongs to R. Hence we may write

$$F \equiv \sum A_\gamma x^m + LD(x),$$

where $L = (l_1, l_2, \cdots, l_s)$; $D(x)$ is of the same type as $H(x)$, and then

$$E^{(j)}[Ax^{m\gamma}]_{x=1} \equiv 0 \pmod{m^j},$$

and also, if we write (mod L, m^j) for (mod (L, m^j)),

$$[E^{(j)}(F)]_{x=1} \equiv 0 \pmod{L, m^j}.$$

THEOREM. *Let R be a ring containing the ring of rational integers. Put*

$$f_{n_i}^{(i)}(\alpha_1, \alpha_2, \cdots, \alpha_{k_i}) = \sum_{r=1}^{k_i} \alpha_{ri} a_{ri}^{n_i},$$

where the a's are rational integers and the α's belong to R. Further, let

$$a_{ri}^d \equiv 1 \pmod{m}, \qquad (i = 1, 2, \cdots, k);$$

let l_i be the greatest common divisor of all the a_{ri}^n in the above which *have factors in common with m; and let $\beta_1, \beta_2, \cdots, \beta_s$ be rational integers such that*

$$\beta_1 + \beta_2 + \cdots + \beta_s \equiv 0 \pmod{m}.$$

Then

$$(7) \qquad (f_{n_1} + f_{n_2} + \cdots + f_{n_s})^j \equiv 0 \; (\text{mod } m^j, l_1, l_2, \cdots, l_s),$$

where we expand the left-hand member, employing (4), *and set*

$$\overset{t}{f}_{n_i} = \overset{t}{\beta} \overset{t\,(i)}{f}_{n_i+td}(\alpha_1, \alpha_2, \cdots, \alpha_{k_i}), \qquad (i = 1, 2, \cdots, s).$$

3. *Applications of the Theorem.* The above general theorem has many applications, some of which will be considered here. Kummer* gave a result which may be expressed as follows:

$$(8) \; h^n(h^{p-1} - 1)^j \equiv 0 \pmod{p^j}, \; (n - 1 \geqq j; n \not\equiv 0 \; (\text{mod } \overline{p-1})),$$

where p is an odd prime; the left-hand member is expanded in full, then b_t/t is substituted for h^t, and the b's are defined by the recursion formula

$$(b + 1)^n = b_n, \qquad (n > 1),$$

in which we expand the left-hand member by the binomial theorem and substitute b_k for b^k. The latter formula gives the Bernoulli numbers.

To apply the main theorem in the present paper to Bernoulli numbers, we employ the known formula

$$S_i(p^k) = 1^i + 2^i + \cdots + (p^k - 1)^i \equiv p^k b_i \pmod{p^{2k}},$$

where i is even and $p > 3$. We also employ the formula

$$\frac{(n^i - 1)S_i(p^\alpha)}{p^\alpha} = \sum_{a=1}^{p\alpha-1} \sum_{s=1}^{i} a^i C_{s,i} \left(\frac{\nu_a}{a}\right)^s p^{\alpha(s-1)},$$

where n is prime to p and

$$y_a \equiv -\frac{a}{p} \pmod{n}, \qquad (0 \leqq y_a < n).$$

These give

$$\frac{n^{2i} - 1}{2i} b_{2i} \equiv \sum_{a=1}^{p\alpha-1} y_a a^{2i-1} \pmod{p^\alpha},$$

---

* Journal für Mathematik, vol. 41 (1851), pp. 368–372.

which we immediately connect up with the f-functions treated in our theorem, and the latter gives

$$h_1^{n_1}h_2^{n_2}\cdots h_s^{n_s}(\beta_1 h_1^{p-1}+\beta_2 h_2^{p-1}+\cdots+\beta_s h_s^{p-1})^j$$
$$\equiv 0 \pmod{p^j, p^{n_1-1}, p^{n_2-1}, \cdots, p^{n_s-1}},$$
$$(n_i \not\equiv 0 \pmod{\overline{p-1}};\ i = 1, 2, \cdots, s),$$

where the left-hand member is expanded in full and b_t/t substituted for $h_i{}^t$ in the result, $(i=1, 2, \cdots, s)$. To obtain (8) from (7), set $s=2$, and

$$f_{n_1} = \sum_{a=1}^{p^j-1} y_a a^{n-1}, \qquad f_{n_2} = 1, \beta_1 = 1, \beta_2 = -1,$$

and the result follows.

Frobenius* gave the relation

$$(10) \qquad H^a(1 - H^b)^c \equiv 0 \pmod{(p^a, p^{ec})},$$

where p is a prime, b is a multiple of $p^{e-1}(p-1)$, and the left-hand member is expanded in full and H^t is replaced by H_t. Further, H_t is defined by the recursion formula

$$(H + 1)^n = xH^n, \qquad (n > 0),$$

where the left-hand member is expanded by the binomial theorem and H^t is replaced by H_t. This gives H as the quotient of two polynomials in x with rational integral coefficients. If these fractions are expressed in their lowest terms, the numerators are called Euler polynomials. Each denominator is a power of $(x-1)$. The relation (10) can be obtained from (7) if we take R as the polynomial ring obtained by adjoining the indeterminate x to the rational ring and extending the result given by Frobenius† so that we have the congruence mod p^j which is analogous to the one he gives mod p. The $R_n(x)$ referred to in this formula is defined by

* Berliner Mathematische Gesellschaft, Sitzungsberichte, 1910, p. 826 and p. 841.

† Loc. cit., p. 843, relation (1).

$$H^n(x) = \frac{R_n(x)}{(x-1)^n}.$$

The relation (7) gives many generalizations of (9). For example we can take $m = p^e$ in lieu of $m = p$. Further details I hope to give in another paper on Bernoulli numbers and Euler polynomials.

UNIVERSITY OF TEXAS

A THEOREM ON MEAN RULED SURFACES

BY MALCOLM FOSTER

Consider the ruled surface formed by the normals to a surface S along some curve C on S. We ask: What are the curves C for which the line of striction of the ruled surface is the locus of the centers of mean curvature corresponding to C?

On S we take the lines of curvature parametric. Referred to the moving trihedral of S, the direction-cosines of the normal are (0, 0, 1), and the variations in these are given by*

$$dX = qdu, \qquad dY = -p_1dv, \qquad dZ = 0.$$

Now the displacement of the central point on each generator of the ruled surface is orthogonal both to the normal and to its neighboring position. Hence we have

$$\delta z = 0, \qquad qdu\delta x - p_1dv\delta y + \delta z = 0,$$

which reduce to

$$(1) \qquad qdu(\xi du + zqdu) - p_1dv(\eta_1dv - zp_1dv) = 0.$$

If in (1) we assign a value to the ratio dv/du, this equation will determine the distance z to the line of striction on the ruled surface defined by this ratio; and if to z we assign a given value, equation (1) will determine the curves, (though not necessarily real), for which this assigned value of z is the distance to the lines of striction.

From (1) we have for the problem at hand,

* Eisenhart, *Differential Geometry of Curves and Surfaces*, pp. 166–174.