A Congruence Theorem relating to Eulerian Numbers and other Coefficients. By J. W. L. Glaisher.

Read May 10th, 1900. Received May 28th, 1900.

1. In the *Comptes Rendus* for 1861* Sylvester gave without proof the theorem that, if $(p-1)p^i$ is a factor of $2n$, then, if p is a prime of the form $4k+1$, p^{i+1} will be a factor of E_n, and, if p is of the form $4k-1$, p^{i+1} will be a factor of $(-1)^{n-1}2+E_n$, where E_n is the n^{th} Eulerian number.

The principal object of this paper is to prove two general theorems, from either of which Sylvester's results in the case $i=0$ may be deduced, as well as corresponding results relating to the I-numbers and other coefficients.

In the latter portion of the paper (§§ 39–65) these general theorems are applied to obtain the residues, mod p, of various systems of series containing $\frac{1}{2}(p-3)$ terms.

I. *Residues of the Bernoullian Functions with Uneven Suffixes, and Applications* (§§ 2–38).

2. Let p be any uneven prime, and let A_r denote the sum of the products of the numbers $1, 2, \ldots, p-1$ taken r together. Then we have evidently

$$x^{p-1}+A_1x^{p-2}+A_2x^{p-3}+\ldots+A_{p-2}x+A_{p-1} = (x+1)(x+2)\ldots(x+p-1).$$

In a recent paper in the *Quarterly Journal*† it has been shown that, if r is even and $<p-1$, A_r is divisible by p, and that, if r is uneven and >1, A_r is divisible by p^2, and that the residues of the quotients are

$$\frac{A_{2t}}{p} \equiv (-1)^t\frac{B_t}{2t}, \bmod p \ \left(t<\frac{p-1}{2}\right),$$

$$\frac{A_{2t+1}}{p^2} \equiv (-1)^{t+1}\frac{(2t+1)B_t}{4t}, \bmod p \ (t>0).$$

---

* Vol. LII., p. 163.

† "On the Residues of the Sums of Products of the first $p-1$ Numbers and their Products to Modulus p^2 or p^3," Vol. XXXI., pp. 321–353. The formulæ quoted occur on pp. 326, 327.

It was also shown that

$$\frac{A_{p-1}+1}{p} \equiv J, \text{ mod } p,$$

where B_t is the t^{th} Bernoullian number and

$$J = -1 + (-1)^{\frac{1}{2}(p+1)} B_{\frac{1}{2}(p-1)} + \frac{1}{p}.$$

The value of A_1 is $\frac{1}{2}p(p-1)$, so that it is divisible by p only.

3. Multiplying the equation in § 2 by x and dividing by p, we therefore find

$$\frac{x^p}{p} - \tfrac{1}{2}x^{p-1} - \frac{B_1}{2}x^{p-2} + \frac{B_2}{4}x^{p-4} - \dots + (-1)^{\frac{1}{2}(p-3)}\frac{B_{\frac{1}{2}(p-3)}}{p-3}x^3 + \frac{A_{p-1}}{p}x$$

$$\equiv \frac{x(x+1)\dots(x+p-1)}{p}, \text{ mod } p.$$

Now the Bernoullian function $B_n(x)$, n being uneven, is defined by the equation

$$B_n(x) = \frac{x^n}{n} - \tfrac{1}{2}x^{n-1} + \frac{n-1}{2!}B_1 x^{n-2} - \frac{(n-1)(n-2)(n-3)}{4!}B_2 x^{n-4} + \dots$$

$$\dots + (-1)^{\frac{1}{2}(n+1)} B_{\frac{1}{2}(n-1)} x,$$

and therefore

$$B_p(x) \equiv \frac{x^p}{p} - \tfrac{1}{2}x^{p-1} - \frac{B_1}{2}x^{p-2} + \frac{B_2}{4}x^{p-4} - \dots + (-1)^{\frac{1}{2}(p+1)} B_{\frac{1}{2}(p-1)} x, \text{ mod } p.$$

Substituting in the preceding congruence, we find

$$B_p(x) + (-1)^{\frac{1}{2}(p-1)} B_{\frac{1}{2}(p-1)} x + \frac{A_{p-1}}{p} x \equiv \frac{x(x+1)\dots(x+p-1)}{p}, \text{ mod } p.$$

Now

$$(-1)^{\frac{1}{2}(p-1)} B_{\frac{1}{2}(p-1)} + \frac{A_{p-1}}{p}$$

$$\equiv (-1)^{\frac{1}{2}(p-1)} B_{\frac{1}{2}(p-1)} + J - \frac{1}{p}, \quad \text{mod } p,$$

$$\equiv (-1)^{\frac{1}{2}(p-1)} B_{\frac{1}{2}(p-1)} - 1 + (-1)^{\frac{1}{2}(p+1)} B_{\frac{1}{2}(p-1)}, \text{ mod } p,$$

$$\equiv -1, \text{ mod } p;$$

so that the congruence becomes

$$B_p(x) - x \equiv \frac{x(x+1)\dots(x+p-1)}{p}, \quad \text{mod } p.$$

4. When x is a positive integer prime to p, one of the p consecutive numbers $x, x+1, \ldots, x+p-1$ must be divisible by p, and the other $p-1$ numbers must have residues $1, 2, 3, \ldots, p-1$ with respect to p.

If therefore $x = kp+t$, t being $<p$, the formula gives

$$B_p(x)-x \equiv -(k+1), \quad \text{mod } p,$$

and in particular, if x be any number $<p$,

$$B_p(x) \equiv x-1, \quad \text{mod } p.$$

5. These formulæ can be readily verified, for, when x is a positive integer,

$$B_p(x) = 1^{p-1}+2^{p-1}+3^{p-1}+\ldots+(x-1)^{p-1};$$

and therefore, since $r^{p-1} \equiv 1$, mod p, unless r is a multiple of p, we have, if $x<p$,

$$B_p(x) \equiv x-1, \quad \text{mod } p,$$

and, if $x = kp+t$,

$$B_p(x) \equiv x-1-k, \quad \text{mod } p,$$

since the k terms $p^{p-1}, (2p)^{p-1}, \ldots, (kp)^{p-1}$ are $\equiv 0$, not 1, mod p.

6. Now let $x = \dfrac{1}{r}$, where r is a positive integer prime to p.

The general formula

$$B_p(x) \equiv x+\frac{x(x+1)\ldots(x+p-1)}{p}, \quad \text{mod } p,$$

then becomes

$$r^pB_p\left(\frac{1}{r}\right) \equiv r^{p-1}+\frac{(r+1)(2r+1)\ldots\{(p-1)r+1\}}{p}, \quad \text{mod } p,$$

whence $$r^pB_p\left(\frac{1}{r}\right) \equiv 1+\frac{(r+1)(2r+1)\ldots\{(p-1)r+1\}}{p}, \quad \text{mod } p.$$

7. Since r is prime to p, the numbers $r, 2r, \ldots, (p-1)r$ have to mod p the system of residues $1, 2, \ldots, p-1$; and therefore the numbers $r+1, 2r+1, \ldots, (p-1)r+1$ have the system of residues $2, 3, \ldots, p-1, p$; that is to say, one of the numbers $r+1, 2r+1, \ldots, (p-1)r+1$ is divisible by p, and the other numbers give the residues $2, 3, \ldots, p-1$.

To determine which is the factor divisible by p, we notice that, if

$\lambda r+1$ is this factor, we must have $\lambda r+1=qp$, where $q<r$ and $\equiv \frac{1}{p}$, mod r. The product of the factors 2, 3, ..., $p-1\equiv -1$, mod p, and therefore we have the formula

$$r^p B_p\left(\frac{1}{r}\right) \equiv 1-q, \quad \text{mod } p,$$

where q is the least positive residue of $\frac{1}{p}$, mod r.

8. We may conveniently express the least positive residue of any quantity a, mod r, by $[a]_r$.

Using this notation, the result just obtained may be written

$$r^p B_p\left(\frac{1}{r}\right) \equiv 1-\left[\frac{1}{p}\right]_r, \quad \text{mod } p.$$

9. This formula enables us to assign the residue of $r^p B_p\left(\frac{1}{r}\right)$, mod p, for all values of r and all (prime) values of p.

In general, if $p=kr+s$, where $s<r$ and is necessarily prime to r, since p is prime,

$$\left[\frac{1}{p}\right]_r = \left[\frac{1}{s}\right]_r.$$

Thus the number of residues of $r^p B_p\left(\frac{1}{r}\right)$ is equal to the number of admissible values of s, that is, to the number of numbers less than r and prime to it.

10. The residue of $r^p B_p\left(\frac{l}{r}\right)$ may be expressed in an exactly similar manner; for, putting $x=\frac{l}{r}$ in § 6, l being prime to r, we have

$$r^p B_p\left(\frac{l}{r}\right) \equiv lr^{p-1}+\frac{l(r+l)(2r+l)\dots\{(p-1)r+l\}}{p}, \text{ mod } p,$$

$$\equiv l+\frac{l(r+l)(2r+l)\dots\{(p-1)r+l\}}{p}, \text{ mod } p.$$

Now, of the p numbers l, $r+l$, $2r+l$, ... $\{(p-1)r+l\}$, one, say $\lambda r+l$, is divisible by p, and the others $\equiv 2, 3, \dots, p-1$, mod p, so that we find

$$r^p B_p\left(\frac{l}{r}\right) \equiv l-q_l, \text{ mod } p,$$

where q_l is the least root of the congruence $px \equiv l$, mod r; or, using the notation of § 8,

$$r^p B_p\left(\frac{l}{r}\right) \equiv l - \left[\frac{l}{p}\right]_r, \quad \text{mod } p.^*$$

11. It is known that

$$B_n \equiv B_{n-k(p-1)}(x), \quad \text{mod } p,\dagger$$

and therefore
$$r^{k(p-1)+p} B_{k(p-1)+p}(x) \equiv r^p B_p(x), \quad \text{mod } p.$$

Putting $x = \frac{l}{r}$, and replacing k by $k-1$ in this formula, we have

$$r^{k(p-1)+1} B_{k(p-1)+1}\left(\frac{l}{r}\right) \equiv r^p B_p\left(\frac{l}{r}\right) \equiv l - \left[\frac{l}{p}\right]_r, \quad \text{mod } p.$$

It has thus been shown that, if p be an uneven prime, and $p-1$ be a divisor of $2n$, then, if $l<p+r$,

$$r^{2n+1} B_{2n+1}\left(\frac{l}{r}\right) \equiv l - \left[\frac{l}{p}\right]_r, \quad \text{mod } p.$$

If $l \geqq p+r$, the formula requires modification in the manner indicated in the note to the last section.

12. As special values of $r^{2n+1} B_{2n+1}\left(\frac{1}{r}\right)$, we have‡

$$4^{2n+1} B_{2n+1}\left(\tfrac{1}{4}\right) = (-1)^{n+1} E_n,$$
$$3^{2n+1} B_{2n+1}\left(\tfrac{1}{3}\right) = (-1)^{n+1} I_n,$$
$$6^{2n+1} B_{2n+1}\left(\tfrac{1}{6}\right) = (-1)^{n+1} J_n,$$

---

* This congruence holds good so long as $l<p+r$, but for greater values of l it requires modification, q_l not being then, necessarily, the least root of the congruence $px \equiv l$, mod r. In general it can be shown that, if $l = kp+t$, where $t>0$ and $<p$, then

$$r^p B_p\left(\frac{l}{r}\right) \equiv l - q_l, \text{ mod } p,$$

where q_l is not x_1, the least root of the congruence $px \equiv l$, mod r, but x_1+mr, mr being such a multiple of r as will bring x_1+mr within the range of numbers $k+1$, $k+2$, ..., $k+r$, *i.e.*, q_l is that root of the congruence $px \equiv l$, mod r, which lies between $k+1$ and $k+r$ both inclusive. The value of q_l may be expressed in terms of k and t by $k+\left[\frac{t}{p}\right]_r$.

In most of the applications of the theorem l is, or can be so chosen as to be, $<p+r$; the principal exceptions in this paper occur in §§ 33–38 and 60–65.

[The residue of $\dfrac{l(r+l)(2r+l)\ldots\{(p-1)r+l\}}{p}$, mod p, that is, the value of q_l, forms the subject of the first part of a paper "Residue of the Product of p Numbers in Arithmetical Progression, mod p^2 and p^3" (*Messenger of Mathematics*, Vol. xxx., pp. 71–92), which has been written since this paper was communicated to the Society.]

† *Proc. Lond. Math. Soc.*, Vol. xxxi., p. 206.

‡ *Quarterly Journal*, Vol. xxix., pp. 31, 35, 44, or *Messenger*, Vol. xxvi., p. 179.

where E_n is the n^{th} Eulerian number, and I_n and J_n are the numbers so denoted in Vol. XXXI., pp. 216, 228 of the *Proceedings*, viz., E_n, I_n, J_n are the coefficients in the expansions

$$\frac{1}{\cos x} = E_0 + \frac{E_1}{2!}x^2 + \frac{E_2}{4!}x^4 + \frac{E_3}{6!}x^6 + \&c.,$$

$$\frac{1}{2\cos x+1} = \tfrac{2}{3}\left\{I_0 + \frac{I_1}{2!}x^2 + \frac{I_2}{4!}x^4 + \frac{I_3}{6!}x^6 + \&c.\right\},$$

$$\frac{2\cos x}{2\cos 2x+1} = \tfrac{1}{3}\left\{J_0 + \frac{J_1}{2!}x^2 + \frac{J_2}{4!}x^4 + \frac{J_3}{6!}x^6 + \&c.\right\}.$$

13. It is convenient to call the admissible values of p the *Staudt factors* for n, *i.e.*, the Staudt factors for n are those values of p for which $p-1$ is a divisor of $2n$. Thus a number p is a Staudt factor for n, if (i.) p is prime, (ii.) $p-1$ is a divisor of $2n$.*

14. Using the formula

$$r^p B_p\left(\frac{1}{r}\right) \equiv 1 - \left[\frac{1}{p}\right]_r, \text{ mod } p,$$

and taking the case $r = 4$, we have

$$\left[\frac{1}{p}\right]_4 = [1]_4 = 1, \text{ if } p \text{ is of the form } 4k+1,$$

and $$= [\tfrac{1}{3}]_4 = 3, \quad\text{,,}\quad\text{,,}\quad 4k+3.$$

Thus, p being any uneven Staudt factor for n,

$$E_n \equiv 0 \text{ or } (-1)^n 2, \text{ mod } p,$$

according as p is of the form $4k+1$ or $4k+3$.

This is the case $i = 0$ of Sylvester's theorem referred to in § 1.

15. For $r = 3$, we have

$$\left[\frac{1}{p}\right]_3 = [1]_3 = 1, \text{ if } p \text{ is of the form } 3k+1,$$

and $$= [\tfrac{1}{2}]_3 = 2, \quad\text{,,}\quad\text{,,}\quad 3k+2,$$

* In previous papers (*Messenger*, Vol. XXIX., pp. 49, 129; *Quarterly Journal*, Vol. XXXI., p. 261) I have called values of p which satisfy these conditions *Staudt factors of* B_n. As the connexion is solely between the numbers p and n, it seems unnecessary to introduce B_n. The Staudt factors for n are the prime factors whose product forms the denominator of B_n.

so that, p being any uneven Staudt factor for n,

$$I_n \equiv 0 \text{ or } (-1)^n, \text{ mod } p,$$

according as p is of the form $3k+1$ or $3k+2$.

16. The quantities I_n formed the subject of a paper in the last volume of the *Proceedings.** That paper contains a table of the first thirteen I's, by means of which I have verified the theorem up to $n = 13$.

The numbers 2 and 3 are Staudt factors for all values of n. The number 2 is excluded, as the modulus is always supposed to be an uneven prime. The number 3 is excluded in this case, as $r = 3$ and r must be prime to p. The residues given by the theorem with respect to the other Staudt factors are as follows:—

$$I_2 \equiv 1, \text{ mod } 5,$$
$$I_3 \equiv 0, \text{ mod } 7,$$
$$I_4 \equiv 1, \text{ mod } 5,$$
$$I_5 \equiv -1, \text{ mod } 11,$$
$$I_6 \equiv 0, \text{ mods } 7, 13, \equiv 1, \text{ mod } 5,$$
$$I_7 \text{ (no admissible Staudt factor)},$$
$$I_8 \equiv 1, \text{ mods } 5, 17,$$
$$I_9 \equiv 0, \text{ mods } 7, 19,$$
$$I_{10} \equiv 1, \text{ mods } 5, 11,$$
$$I_{11} \equiv -1, \text{ mod } 23,$$
$$I_{12} \equiv 0, \text{ mods } 7, 13, \equiv 1, \text{ mod } 5,$$
$$I_{13} \text{ (no admissible Staudt factor)}.$$

These residues agree with those obtained from the table of I_n.

17. For $r = 6$ we have

$$\left[\frac{1}{p}\right]_6 = [1]_6 = 1, \text{ if } p \text{ is of the form } 6k+1,$$

and $$= [\tfrac{1}{5}]_6 = 5, \quad ,, \quad ,, \quad 6k+5;$$

* "On a Set of Coefficients analogous to the Eulerian Numbers," Vol. XXXI., pp. 216–235.

so that $$J_n \equiv 0 \text{ or } (-1)^n 4, \text{ mod } p,$$

according as p is of the form $6k+1$ or $6k+5$.

This result may be derived from § 15 by means of the formula

$$J_n = (2^{2n+1}+2)\, I_n,$$

for, when $p-1$ is a divisor of $2n$, $2^{2n} \equiv 1$, mod p, and therefore

$$J_n \equiv 4I_n, \text{ mod } p.$$

18. The Bernoullian function $A'_n(x)$, when n is uneven, may be defined by the equation

$$A'_n(x) = B_n(x) - 2^n B_n(\tfrac{1}{2}x).*$$

Thus we derive from § 6

$$r^p A'_p\left(\frac{1}{r}\right) \equiv \frac{(r+1)(2r+1)\dots\{(p-1)r+1\}}{p} - \frac{(2r+1)(4r+1)\dots\{2(p-1)r+1\}}{p}, \text{ mod } p,$$

and therefore $$r^p A'_p\left(\frac{1}{r}\right) \equiv q'-q, \text{ mod } p,$$

where q, q' are the least residues given by the congruences

$$px \equiv 1, \text{ mod } r,$$

$$px \equiv 1, \text{ mod } 2r,$$

respectively.

This result may be expressed by the formula

$$r^p A'_p\left(\frac{1}{r}\right) \equiv \left[\frac{1}{p}\right]_{2r} - \left[\frac{1}{p}\right]_r, \text{ mod } p.$$

19. More generally we have in the same manner

$$r^p A'_p\left(\frac{l}{r}\right) \equiv \frac{l(r+l)(2r+l)\dots\{(p-1)r+l\}}{p} - \frac{l(2r+l)(4r+l)\dots\{2(p-1)r+l\}}{p}, \text{ mod } p;$$

whence we find $$r^p A'_p\left(\frac{l}{r}\right) \equiv \left[\frac{l}{p}\right]_{2r} - \left[\frac{l}{p}\right]_r, \text{ mod } p.\dagger$$

---

* The expression for $A'_n(x)$ in powers of x was given in *Proc. Lond. Math. Soc.*, Vol. XXXI., p. 203.

† In this formula l must be $< p+r$; otherwise a modification is requisite of the same kind as that stated in the note to § 10.

20. It is not necessary that l should be prime to $2r$, but, if l be even, $= 2l'$, then

$$\frac{l(2r+l)(4r+l)\ \ldots\ \{2(p-1)r+l\}}{p}$$

$$= 2^p \frac{l'(r+l')(2r+l')\ \ldots\ \{(p-1)r+l'\}}{p} \equiv 2\left[\frac{l'}{p}\right]_r, \quad \text{mod } p;\text{*}$$

so that in this case the formula may be written

$$r^p A'_p\left(\frac{l}{r}\right) \equiv 2\left[\frac{l'}{p}\right]_r - \left[\frac{l}{p}\right], \quad \text{mod } p.$$

21. The expression $\left[\frac{l}{p}\right]_{2r} - \left[\frac{l}{p}\right]_r$

can only have the values zero and r; for the expression is $\alpha-\beta$, where α is the least root of the congruence

$$px \equiv l, \quad \text{mod } 2r,$$

and β is the least root of the congruence

$$px \equiv l, \quad \text{mod } r.$$

Now, if $\alpha < r$, it is clear that β must $= \alpha$, and, if $\alpha > r$, we must have $\beta = \alpha - r$. Thus $\alpha-\beta$ has the value 0 or r according as the least root of the congruence $px \equiv l$, mod $2r$, is $<$ or $>$ r.†

---

* This reasoning is general and shows that, if $l = ml'$, then

$$\left[\frac{l}{p}\right]_{mr} = m\left[\frac{l'}{p}\right]_r.$$

We may easily prove this formula directly, for $\left[\frac{l}{p}\right]_{mr}$ is the least value of x given by the congruence $px \equiv l$, mod mr, and, if $l = ml'$, the congruence becomes $p\frac{x}{m} \equiv l'$, mod r, from which the least value of x is $m\left[\frac{l'}{p}\right]_r$.

† If the least root of the congruence $px \equiv l$, mod $2r$, is $= r$, we must have $pr \equiv l$, mod $2r$, and therefore l must be an uneven multiple of r, $= mr$ say, m being uneven, in which case

$$\alpha-\beta = \left[\frac{mr}{p}\right]_{2r} - \left[\frac{mr}{p}\right]_r = r\left[\frac{m}{p}\right]_2 - r\left[\frac{m}{p}\right]_1 = 0.$$

22. The result obtained in § 19 therefore shows that

$$r^p A'_p\left(\frac{l}{r}\right) \equiv 0 \text{ or } r, \quad \text{mod } p,$$

according as the least root of the congruence

$$px \equiv l, \quad \text{mod } 2r,$$

is $< r$ or $> r$. The residue is zero if the root is equal to r.

23. If we put $$\left(\frac{l}{p}\right)_{2r} = \left[\frac{l}{p}\right]_{2r} - \left[\frac{l}{p}\right]_r,$$

then the symbol $\left(\frac{l}{p}\right)_{2r}$ denotes 0 if the least root of the congruence

$$px \equiv l, \quad \text{mod } 2r,$$

is $< r$ or $= r$, and denotes r if the least root $> r$. We may therefore express the result of § 19 in the convenient form

$$r^p A'_p\left(\frac{l}{r}\right) \equiv \left(\frac{l}{p}\right)_{2r}, \quad \text{mod } p.$$

24. Since $$A'_n(x) \equiv A'_{n-k(p-1)}, \quad \text{mod } p,\text{*}$$

we can, by proceeding as in § 11, apply the results obtained in §§ 19 and 22 to show that, if p is any uneven prime, and $p-1$ is a divisor of $2n$ (that is, if p is an uneven Staudt factor for n), then

$$r^{2n+1} A'_{2n+1}\left(\frac{l}{r}\right) \equiv \left[\frac{l}{p}\right]_{2r} - \left[\frac{l}{p}\right]_r, \quad \text{mod } p,$$

$$\equiv \left(\frac{l}{p}\right)_{2r}, \quad \text{mod } p,$$

the expression on the right-hand side being zero or r according as $\left[\frac{l}{p}\right]_{2r} \leqq$ or $> r$.

If l is not $< p+r$, the formula requires modification in the manner indicated in the note to § 19.

* *Proc. Lond. Math. Soc.*, Vol. XXXI., p. 204.

25. As special values of $r^{2n+1}A'_{2n+1}\left(\frac{1}{r}\right)$, we have*

$$2^{2n+1}A'_{2n+1}(\tfrac{1}{2}) = (-1)^n E_n,$$
$$4^{2n+1}A'_{2n+1}(\tfrac{1}{4}) = (-1)^n 2P_n,$$
$$3^{2n+1}A'_{2n+1}(\tfrac{1}{3}) = (-1)^n H_n,$$
$$6^{2n+1}A'_{2n+1}(\tfrac{1}{6}) = (-1)^n \frac{3^{2n+1}+3}{2} E_n,$$

where P_n and H_n are defined as coefficients in the expansions

$$\frac{\cos x}{\cos 2x} = P_0 + \frac{P_1}{2!}x^2 + \frac{P_2}{4!}x^4 + \frac{P_3}{6!}x^6 + \&c.,$$

$$\frac{1}{2\cos x - 1} = \tfrac{2}{3}\left\{ H_0 + \frac{H_1}{2!}x^2 + \frac{H_2}{4!}x^4 + \frac{H_3}{6!}x^6 + \&c. \right\}.$$

26. We thus have, p being any uneven Staudt factor for n,

$$E_n \equiv (-1)^n \left(\frac{1}{p}\right)_4, \quad \text{mod } p,$$

$$2P_n \equiv (-1)^n \left(\frac{1}{p}\right)_8 \quad \text{,,}$$

$$H_n \equiv (-1)^n \left(\frac{1}{p}\right)_6 \quad \text{,,}$$

$$\frac{3^{2n+1}+3}{2}E_n \equiv (-1)^n \left(\frac{1}{p}\right)_{12} \quad \text{,,}$$

27. If $p = 4k+1$, $\qquad \left(\frac{1}{p}\right)_4 = 0,$

for the least root of $x \equiv 1$, mod 4, is $x = 1$, which < 2, and, if $p = 4k+3$,

$$\left(\frac{1}{p}\right)_4 = 2,$$

for the least root of $3x \equiv 1$, mod 4, is $x = 3$, which > 2.

The first congruence in § 26 therefore gives $E_n \equiv 0$ or $(-1)^n 2$, mod p, according as p is of the form $4k+1$ or $4k+3$ (§ 14).

---

* *Quarterly Journal*, Vol. XXIX., p. 107; and *Messenger*, Vol. XXVI., p. 178.

28. Taking now the last of the four congruences in § 26, we have

$$\left(\frac{1}{p}\right)_{12} = 0, \quad \text{if} \quad p = 12k+1 \text{ or } 12k+5,$$

and $$= 6, \quad \text{if} \quad p = 12k+7 \text{ or } 12k+11,$$

for the least roots of the congruences

$$x \equiv 1, \quad 5x \equiv 1, \quad 7x \equiv 1, \quad 11x \equiv 1, \quad \text{mod } 12,$$

are 1, 5, 7, 11 respectively, of which the first two < 6, and the last two > 6.

Thus the right-hand side of the congruence is 0 or $(-1)^n 6$ according as n is of the form $4k+1$ or $4k+3$.

This result agrees with § 14, for, if p is a Staudt factor for n,

$$\frac{3^{2n+1}+3}{2} \equiv \frac{3+3}{2} \equiv 3, \quad \text{mod } p.$$

29. The third congruence of § 26 gives

$$H_n = 0 \text{ or } (-1)^n 3, \quad \text{mod } p,$$

according as p is of the form $6k+1$ or $6k+5$.

This result agrees with § 15, for

$$H_n = (2^{2n+1}+1)\, I_n;$$

so that, p being any uneven Staudt factor for n,

$$H_n \equiv 3I_n, \quad \text{mod } p.$$

30. Considering now the second congruence in § 26, we have

$$\left(\frac{1}{p}\right)_{8} = 0, \quad \text{if} \quad p = 8k+1 \text{ or } 8k+3,$$

and $$= 4, \quad \text{if} \quad p = 8k+5 \text{ or } 8k+7,$$

for the least roots of the congruences

$$x \equiv 1, \quad 3x \equiv 1, \quad 5x \equiv 1, \quad 7x \equiv 1, \quad \text{mod } 8,$$

are respectively 1, 3, 5, 7.

Thus we find that

$$P_n \equiv 0 \text{ or } (-1)^n 2, \quad \text{mod } p,$$

according as p is of the forms $8k+1$ and $8k+3$, or of the forms $8k+5$ and $8k+7$.

31. Since 3 is a Staudt factor for all values of n, this theorem shows that all the P's must be divisible by 3. With respect to the other Staudt factors, it shows that

$$P_2 \equiv 2, \quad \text{mod } 5,$$
$$P_3 \equiv -2, \quad \text{mod } 7,$$
$$P_4 \equiv 2, \quad \text{mod } 5,$$
$$P_5 \equiv 0, \quad \text{mod } 11,$$
$$P_6 \equiv 2, \quad \text{mods } 5, 7, 13.$$

These results I have verified. The values of the first five P's were given in the *Quarterly Journal*, Vol. XXIX., p. 63.* The value of P_6 (viz., $P_6 = 7828053417$) was calculated for the purpose of this verification.

32. The principal formulæ which have been established in this paper are

$$\text{(i.)} \quad r^p B_p \left(\frac{l}{r}\right) \equiv l - \left[\frac{l}{p}\right]_r, \quad \text{mod } p \quad (\S\,10),$$

$$\text{(ii.)} \quad r^p A'_p \left(\frac{l}{r}\right) \equiv \left(\frac{l}{p}\right)_{2r}, \quad \text{mod } p \quad (\S\,23).$$

These results combined with those obtained in a previous paper have enabled us to assign the residues of $r^{2n+1} B_{2n+1}\left(\frac{l}{r}\right)$ and $r^{2n+1} A_{2n+1}\left(\frac{l}{r}\right)$ for any uneven Staudt factor for n as modulus (§§ 11, 24).

The principal particular cases of the formulæ (i.) and (ii.) are

$$(1) \quad E_{\frac{1}{2}(p-1)} \equiv 0 \text{ or } -2, \quad \text{mod } p,$$

according as p is of the form $4k+1$ or $4k+3$ (§ 14).

$$(2) \quad I_{\frac{1}{2}(p-1)} \equiv 0 \text{ or } (-1)^{\frac{1}{2}(p-1)}, \quad \text{mod } p,$$

according as p is of the form $3k+1$ or $3k+2$ (§ 15).

$$(3) \quad P_{\frac{1}{2}(p-1)} \equiv 0 \text{ or } (-1)^{\frac{1}{2}(p-1)}\, 2, \quad \text{mod } p,$$

according as p is of the forms $8k+1$ and $8k+3$, or of the forms $8k+5$ and $8k+7$ (§ 30).

* They are $P_1 = 3$, $P_2 = 57$, $P_3 = 2763$, $P_4 = 250737$, $P_5 = 36581523$.

33. I now proceed to consider the expansions in which the quantities $a^{2n+1}B_{2n+1}\left(\frac{b}{a}\right)$ and $a^{2n+1}A'_{2n+1}\left(\frac{b}{a}\right)$ are the coefficients, in order to determine the most general expansions in which the residues of the coefficients can be assigned by the formulæ (i.) and (ii.). We know that

$$\frac{a}{2}\,\frac{\sin(2b-a)x}{\sin ax} = \frac{2b-a}{2} - a^3B_3\left(\frac{b}{a}\right)\frac{(2x)^2}{2!} + a^5B_5\left(\frac{b}{a}\right)\frac{(2x)^4}{4!} - \&c.^*$$

Putting $2b-a=c$, so that $b=\frac{1}{2}(c+a)$, we have

$$\frac{a}{2}\,\frac{\sin cx}{\sin ax} = \frac{c}{2} - a^3B_3\left(\frac{a+c}{2a}\right)\frac{(2x)^2}{2!} + a^5B_5\left(\frac{a+c}{2a}\right)\frac{(2x)^4}{4!} - \&c.$$

Similarly, we have

$$\frac{a}{2}\,\frac{\cos(2b-a)x}{\cos ax} = aA'_1\left(\frac{b}{a}\right) - a^3A'_3\left(\frac{b}{a}\right)\frac{(2x)^2}{2!} + a^5A'_5\left(\frac{b}{a}\right)\frac{(2x)^4}{4!} - \&c.,\dagger$$

giving

$$\frac{a}{2}\,\frac{\cos cx}{\cos ax} = \frac{a}{2} - a^3A'_3\left(\frac{a+c}{2a}\right)\frac{(2x)^2}{2!} + a^5A'_5\left(\frac{a+c}{2a}\right)\frac{(2x)^4}{4!} - \&c.$$

We thus find, a and c being unrestricted,

$$\frac{a}{2}\,\frac{\sin cx}{\sin ax} = \frac{c}{2} - \Delta_1\frac{(2x)^2}{2!} + \Delta_2\frac{(2x)^4}{4!} - \&c.,$$

$$\frac{a}{2}\,\frac{\cos cx}{\cos ax} = \frac{a}{2} - \Theta_1\frac{(2x)^2}{2!} + \Theta_3\frac{(2x)^4}{4!} - \&c.,$$

where $$\Delta_n = a^{2n+1}B_{2n+1}\left(\frac{a+c}{2a}\right),$$

$$\Theta_n = a^{2n+1}A'_{2n+1}\left(\frac{a+c}{2a}\right).$$

Since $$B_{2n+1}(1-x) = -B_{2n+1}(x),$$

and $$A'_{2n+1}(1-x) = A'_{2n+1}(x),$$

we have also $$\Delta_n = -a^{2n+1}B_{2n+1}\left(\frac{a-c}{2a}\right),$$

$$\Theta_n = a^{2n+1}A'_{2n+1}\left(\frac{a-c}{2a}\right).$$

---

* *Proc. Lond. Math. Soc.*, Vol. XXXI., p. 207.

† *Ib.*, p. 206.

34. If a and c are both even integers or both uneven integers, so that $\frac{1}{2}(a+c)$ is an integer, the residues of $\Delta_{\frac{1}{2}(p-1)}$ and $\Theta_{\frac{1}{2}(p-1)}$ are given directly by (i.) and (ii.), viz.,

$$\Delta_{\frac{1}{2}(p-1)} \equiv \tfrac{1}{2}(a+c) - \left[\frac{\frac{1}{2}(a+c)}{p}\right]_a, \quad \text{mod } p,$$

$$\Theta_{\frac{1}{2}(p-1)} \equiv \left(\frac{\frac{1}{2}(a+c)}{p}\right)_{2a}, \quad \text{mod } p;$$

but, if a and c are one even and one uneven, we have to use the ormulæ (i.) and (ii.) in a slightly modified form.

35. To obtain this modified form, put $r = ma$, $l = b$ in (i.) and (ii.) of § 32. We thus find

$$m^p a^p B_p\left(\frac{b}{ma}\right) \equiv b - \left[\frac{b}{p}\right]_{ma}, \quad \text{mod } p,$$

$$m^p a^p A'_p\left(\frac{b}{ma}\right) \equiv \left(\frac{b}{p}\right)_{2ma}, \quad \text{mod } p,$$

whence

$$\text{(i.)}\quad a^p B_p\left(\frac{b}{ma}\right) \equiv \frac{1}{m}\left\{b - \left[\frac{b}{p}\right]_{ma}\right\}, \quad \text{mod } p,$$

$$\text{(ii.)}\quad a^p A'_p\left(\frac{b}{ma}\right) \equiv \frac{1}{m}\left(\frac{b}{p}\right)_{2ma}, \quad \text{mod } p.$$

36. Applying these formulæ to the case when a and c are one even and one uneven, we have

$$\Delta_{\frac{1}{2}(p-1)} \equiv \tfrac{1}{2}\left\{a+c - \left[\frac{a+c}{p}\right]_{2a}\right\}, \quad \text{mod } p,$$

$$\Theta_{\frac{1}{2}(p-1)} \equiv \tfrac{1}{2}\left(\frac{a+c}{p}\right)_{4a}, \quad \text{mod } p.$$

These formulæ also include the case of $a+c$ even (§ 34), for, if b is divisible by any number m, $= m\beta$ say, then, by §§ 19 and 23,

$$\frac{1}{m}\left[\frac{b}{p}\right]_{ma} = \left[\frac{\beta}{p}\right]_a,$$

$$\frac{1}{m}\left(\frac{b}{p}\right)_{2ma} = \left[\frac{\beta}{p}\right]_{2a}.$$

37. In general, therefore, if p be any uneven Staudt factor for n,

$$\Delta_n \equiv \tfrac{1}{2}\left\{a+c-\left[\frac{a+c}{p}\right]\right\}_{2a}, \quad \text{mod } p,$$

whether $a+c$ be even or uneven. If $a+c$ is even, we may replace $\left[\frac{a+c}{p}\right]_{2a}$ by $2\left[\frac{\frac{1}{2}(a+c)}{p}\right]_a$.

38. Similarly, if p be any uneven Staudt factor for n,

$$\Theta_n \equiv \tfrac{1}{2}\left(\frac{a+c}{p}\right)_{4a}, \quad \text{mod } p,$$

whether $a+c$ be even or uneven. If $a+c$ is even, the congruence may be written

$$\Theta_n \equiv \left(\frac{\frac{1}{2}(a+c)}{p}\right)_{2a}, \quad \text{mod } p.$$

Thus the residue of Θ_n, mod p, can only have the values 0 and a; and it has the former or latter of these values according as $\left[\frac{a+c}{p}\right]_{4a} \overline{\overline{<}}$ or $> 2a$.*

II. *Residues of certain Series containing* $\frac{1}{2}(p-3)$ *terms* (§§ 39–65).

39. In Vol. XXXI., p. 214, of the *Proceedings*, a general congruence theorem was given connecting the first $\frac{1}{2}(p-1)$ coefficients in a general expansion formula; and the two following formulæ were given as particular cases:—

$$\text{(i.)}\ E_0-E_1+E_2-\ldots+(-1)^{\frac{1}{2}(p-1)}E_{\frac{1}{2}(p-1)} \equiv 0, \quad \text{mod } p,$$

$$\text{(ii.)}\ I_0-I_1+I_2-\ldots+(-1)^{\frac{1}{2}(p-1)}\tfrac{3}{2}I_{\frac{1}{2}(p-1)} \equiv 0, \quad \text{mod } p,$$

the last term in the second series having the coefficient $\frac{3}{2}$. The values to be assigned to E_0 and I_0 are respectively 1 and $\frac{1}{2}$.

Since $E_{\frac{1}{2}(p-1)} \equiv 0$ or -2, mod p, according as p is of the form $4k+1$ or $4k+3$ (§ 14) and $I_{\frac{1}{2}(p-1)} \equiv 0$ or $(-1)^{\frac{1}{2}(p-1)}$, mod p, according as p is

---

* The formulæ for the residues of the Δ's and Θ's require modification, if $p \overline{\overline{<}} c-a$ (see notes to §§ 10, 19).

of the form $3k+1$ or $3k+2$ (§ 15), these formulæ show that

$$\text{(i.)}\quad E_0-E_1+E_2-\ldots+(-1)^{\frac{1}{2}(p-3)}E_{\frac{1}{2}(p-3)}\equiv 0 \text{ or } -2, \text{ mod } p,$$

according as p is of the form $4k+1$ or $4k+3$, and

$$\text{(ii.)}\quad I_0-I_1+I_2-\ldots+(-1)^{\frac{1}{2}(p-3)}I_{\frac{1}{2}(p-3)}\equiv 0 \text{ or } -\tfrac{3}{2}, \text{ mod } p,$$

according as p is of the form $3k+1$ or $3k+2$.

40. These results may be generalised by means of the formulæ (i.) and (ii.) of § 32, so that we may obtain the residues of similar expressions in which the coefficients of the expansion are multiplied by successive even powers of any number m; *e.g.*, we may assign the residue, mod p, of

$$E_0-m^2E_1+m^4E_2-\ldots+(-1)^{\frac{1}{2}(p-3)}m^{p-3}E_{\frac{1}{2}(p-3)}.$$

41. To obtain these general results we start with the formula

$$\tfrac{1}{2}\left\{r^pB_p\left(\frac{rx+1}{r}\right)-r^pB_p\left(\frac{rx+r-1}{r}\right)\right\}$$

$$=r^pB_p\left(\frac{1}{r}\right)+(p-1)_2(rx)^2r^{p-2}B_{p-2}\left(\frac{1}{r}\right)$$

$$+(p-1)_4(rx)^4r^{p-4}B_{p-4}\left(\frac{1}{r}\right)+\&\text{c.},$$

where $(p-1)_t$ denotes the number of combinations of $p-1$ things taken t together.*

Since $(p-1)_t\equiv 1$, mod p, we find, by transposing to the left-hand side the first term on the right-hand side, and writing the terms on the right-hand side in the reverse order,

$$\tfrac{1}{2}\left\{r^pB_p\left(\frac{rx+1}{r}\right)-r^pB_p\left(\frac{rx+r-1}{r}\right)\right\}-r^pB_p\left(\frac{1}{r}\right)$$

$$\equiv(rx)^{p-1}rB_1\left(\frac{1}{r}\right)+(rx)^{p-3}r^3B_3\left(\frac{1}{r}\right)+\ldots+(rx)^2r^{p-2}B_{p-2}\left(\frac{1}{r}\right), \text{ mod } p.$$

---

* This formula may be derived from the first formula on p. 155 of Vol. XXIX. of the *Quarterly Journal* by putting $n=p$, using the relation

$$V_{2n+1}(x)=(2n+1)B_{2n+1}(x)$$

to replace V's by B's, and dividing throughout by p.

Putting $rx = \frac{1}{m}$, and noticing that $m^{p-1} \equiv 1$, mod p, we obtain the formula

$$rB_1\left(\frac{1}{r}\right) + m^2r^3B_3\left(\frac{1}{r}\right) + m^4r^5B_5\left(\frac{1}{r}\right) + \ldots + m^{p-3}r^{p-2}B_{p-r}\left(\frac{1}{r}\right)$$
$$\equiv \tfrac{1}{2}\left\{ r^pB_p\left(\frac{m+1}{rm}\right) - r^pB_p\left(\frac{(r-1)\,m+1}{rm}\right)\right\} - r^pB_p\left(\frac{1}{r}\right), \text{ mod } p.$$

42. Now, by § 32, the right-hand side

$$\equiv \frac{1}{2m}\left\{ m+1-\left[\frac{m+1}{p}\right]_{rm} - (r-1)\,m-1+\left[\frac{(r-1)\,m+1}{p}\right]_{rm}\right\}$$
$$-1+\left[\frac{1}{p}\right]_r, \quad \text{mod } p,$$
$$\equiv \frac{1}{2m}\left\{\left[\frac{(r-1)\,m+1}{p}\right]_{rm} - \left[\frac{m+1}{p}\right]_{rm} - rm\right\} + \left[\frac{1}{p}\right]_r, \quad \text{mod } p;$$

and we thus obtain the formula

$$rB_1\left(\frac{1}{r}\right) + m^2r^3B_3\left(\frac{1}{r}\right) + m^4r^5B_5\left(\frac{1}{r}\right) + \ldots + m^{p-3}r^{p-2}B_{p-2}\left(\frac{1}{r}\right)$$
$$\equiv -\frac{r}{2} + \frac{1}{2m}\left\{\left[\frac{(r-1)\,m+1}{p}\right]_{rm} - \left[\frac{m+1}{p}\right]_{rm}\right\} + \left[\frac{1}{p}\right]_r, \quad \text{mod } p.$$

Thus the residue of the series depends upon r and m and upon the residue of p, mod rm.

43. Since $2^{2n+1}B_{2n+1}(\frac{1}{2}) = 0$, the left-hand side is zero when $r = 2$; and it is easy to see that the right-hand side also is equal to zero.

44. Since $$4^{2n+1}B_{2n+1}(\tfrac{1}{4}) = (-1)^{n+1}E_n, \quad (\S\ 12),$$

we find, by putting $r = 4$,

$$E_0 - m^2E_1 + m^4E_2 - \ldots + (-1)^{\frac{1}{2}(p-3)}E_{\frac{1}{2}(p-3)}$$
$$\equiv 2 + \frac{1}{2m}\left\{\left[\frac{m+1}{p}\right]_{4m} - \left[\frac{3m+1}{p}\right]_{4m}\right\} - \left[\frac{1}{p}\right]_4, \quad \text{mod } p,$$

which gives the residue of

$$E_0 - m^2E_1 + m^4E_2 - \ldots + (-1)^{\frac{1}{2}(p-3)}m^{p-3}E_{\frac{1}{2}(p-3)}$$

for all integral values of m.

45. For $m = 1$ the right-hand side of the congruence

$$= 2+\tfrac{1}{2}\left\{\left[\frac{2}{p}\right]_4-\left[\frac{4}{p}\right]_4\right\}-\left[\frac{1}{p}\right]_4$$

$$= 2+\tfrac{1}{2}\left\{2\left[\frac{1}{p}\right]_2-4\left[\frac{1}{p}\right]_1\right\}-\left[\frac{1}{p}\right]_4$$

$$= \left[\frac{1}{p}\right]_2-\left[\frac{1}{p}\right]_4.$$

Now $\left[\frac{1}{p}\right]_2$ always $= 1$, and $\left[\frac{1}{p}\right]_4 = 1$ or 3, according as p is of the form $4k+1$ or $4k+3$. Therefore

$$E_0-E_1+E_2-\ldots+(-1)^{\frac{1}{2}(p-3)}E_{\frac{1}{2}(p-3)} \equiv 0 \text{ or } -2, \text{ mod } p,$$

according as p is of the form $4k+1$ or $4k+3$. This formula was given in § 39.

46. Putting $m = 2$ in § 44, we have

$$E_0-2^2E_1+2^4E_2-\ldots+(-1)^{\frac{1}{2}(p-3)}2^{p-3}E_{\frac{1}{2}(p-3)}$$

$$\equiv 2+\tfrac{1}{4}\left\{\left[\frac{3}{p}\right]_8-\left[\frac{7}{p}\right]_8\right\}-\left[\frac{1}{p}\right]_4, \text{ mod } p.$$

The residue $\left[\frac{1}{p}\right]_4 = 1$ or 3, according as p is of the form $4k+1$ or $4k+3$. The other residues are given for the different forms of p by the following congruences :—

if $p = 8k+1$, $x \equiv 3$, mod 8, giving $x_1 = 3$,*
„ „ $x \equiv 7$, „ „ $x_1 = 7$;
if $p = 8k+3$, $3x \equiv 3$, mod 8, giving $x_1 = 1$,
„ „ $3x \equiv 7$, „ „ $x_1 = 5$;
if $p = 8k+5$, $5x \equiv 3$, mod 8, giving $x_1 = 7$,
„ „ $5x \equiv 7$, „ „ $x_1 = 3$;
if $p = 8k+7$, $7x \equiv 3$, mod 8, giving $x_1 = 5$,
„ „ $7x \equiv 7$, „ „ $x_1 = 1$.

* x_1 will always be used to denote the least root of the congruence in question.

The residue of the series is therefore, in the four cases,

$$2+\tfrac{1}{4}(3-7)-1=0,$$
$$2+\tfrac{1}{4}(1-5)-3=-2,$$
$$2+\tfrac{1}{4}(7-3)-1=2,$$
$$2+\tfrac{1}{4}(5-1)-3=0,$$

respectively. Therefore

$$E_0-2^2E_1+2^4E_2-\ldots+(-1)^{\frac{1}{2}(p-3)}2^{p-3}E_{\frac{1}{2}(p-3)}\equiv 0,\,-2,\,2,\,0,\ \text{mod}\ p,$$

according as $p\equiv 1, 3, 5, 7$, mod 8.

47. Putting $m=3$, we have

$$E_0-3^2E_1+3^4E_2-\ldots+(-1)^{\frac{1}{2}(p-3)}3^{p-2}E_{\frac{1}{2}(p-3)}$$
$$\equiv 2+\tfrac{1}{3}\left\{2\left[\frac{1}{p}\right]_3-\left[\frac{5}{p}\right]_6\right\}-\left[\frac{1}{p}\right]_4,\ \text{mod}\ p.$$

The congruences giving the first two residues are

if $p=12k+1$,	$x\equiv 1$, mod 3,	giving	$x_1=1$,
,, ,,	$x\equiv 5$, mod 6,	,,	$x_1=5$;
if $p=12k+5$,	$5x\equiv 1$, mod 3,	giving	$x_1=2$,
,, ,,	$5x\equiv 5$, mod 6,	,,	$x_1=1$;
if $p=12k+7$,	$7x\equiv 1$, mod 3,	giving	$x_1=1$,
,, ,,	$7x\equiv 5$, mod 6,	,,	$x_1=5$;
if $p=12k+11$,	$11x\equiv 1$, mod 3,	giving	$x_1=2$,
,, ,,	$11x\equiv 5$, mod 6,	,,	$x_1=1$.

Thus in the four cases the residue of the series $=0, 2, -2, 0$, respectively; and therefore

$$E_0-3^2E_1+3^4E_2-\ldots+(-1)^{\frac{1}{2}(p-3)}3^{p-3}E_{\frac{1}{2}(p-3)}\equiv 0,\,2,\,-2,\,0,\ \text{mod}\ p,$$

according as $p\equiv 1, 5, 7, 11$, mod 12.

48. Similarly, putting $m=4$,

$$E_0-4^2E_1+4^4E_2-\ldots+(-1)^{\frac{1}{2}(p-3)}4^{p-2}E_{\frac{1}{2}(p-3)}$$
$$\equiv 2+\tfrac{1}{8}\left\{\left[\frac{5}{p}\right]_{16}-\left[\frac{13}{p}\right]_{16}\right\}-\left[\frac{1}{p}\right]_4,\ \text{mod}\ p.$$

By considering as in the two preceding sections the values of the residues according to the different forms of p, we find that

$$E_0-4^2E_1+4^4E_2-\ldots+(-1)^{\frac{1}{2}(p-3)}4^{p-3}E_{\frac{1}{2}(p-3)}$$
$$\equiv 0,\ -2,\ 0,\ -2,\ 2,\ 0,\ 2,\ 0,\ \text{mod } p,$$

according as $p \equiv 1, 3, 5, 7, 9, 11, 13, 15$, mod 16.

49. Putting now $r=3$ in the general congruence of § 42, and using the formula

$$3^{2n+1}B_{2n+1}(\tfrac{1}{3}) = (-1)^n I_n \ (\S\ 12),$$

we find

$$I_0-m^2I_1+m^4I_2-\ldots+(-1)^{\frac{1}{2}(p-3)}m^{p-2}I_{\frac{1}{2}(p-3)}$$
$$\equiv \tfrac{3}{2}+\frac{1}{2m}\left\{\left[\frac{m+1}{p}\right]_{3m}-\left[\frac{2m+1}{p}\right]_{3m}\right\}-\left[\frac{1}{p}\right]_3,\ \text{mod } p.$$

50. By putting $m=1, 2, 3, 4$, and determining the separate residues exactly as in the case of $r=4$, we obtain the following results:—

(i.) $I_0-I_1+I_2-\ldots+(-1)^{\frac{1}{2}(p-3)}I_{\frac{1}{2}(p-3)} \equiv 0$ or $-\tfrac{3}{2}$, mod p,

according as p is of the form $3k+1$ or $3k+2$. This formula has been already given in § 39.

(ii.) $I_0-2^2I_1+2^4I_2-\ldots+(-1)^{\frac{1}{2}(p-3)}2^{p-3}I_{\frac{1}{2}(p-3)} \equiv 0$, mod p,

for all values of p.

(iii.) $I_0-3^2I_1+3^4I_2-\ldots+(-1)^{\frac{1}{2}(p-3)}3^{p-3}I_{\frac{1}{2}(p-3)}$
$$\equiv 0,\ -\tfrac{3}{2},\ 0,\ 0,\ \tfrac{3}{2},\ 0,\ \text{mod } p,$$

according as $p \equiv 1, 2, 4, 5, 7, 8$, mod 9.

(iv.) $I_0-4^2I_1+4^4I_2-\ldots+(-1)^{\frac{1}{2}(p-3)}4^{p-3}I_{\frac{1}{2}(p-3)}$
$$\equiv 0,\ -\tfrac{3}{2},\ \tfrac{3}{2},\ 0,\ \text{mod } p,$$

according as $p \equiv 1, 5, 7, 11$, mod 12.

51. It may be remarked that in general, if p is of the form $krm+1$,

$$rB_1\left(\frac{1}{r}\right)+m^2r^3B_3\left(\frac{1}{r}\right)+m^4r^5B_5\left(\frac{1}{r}\right)+\ldots$$
$$\ldots+m^{p-3}r^{p-2}B_{p-2}\left(\frac{1}{r}\right) \equiv 0,\ \text{mod } p;$$

for in this case the value of the right-hand side of the formula in § 42

$$=-\frac{r}{2}+\frac{1}{2m}\{(r-1)m+1-(m+1)\}+1=0.$$

52. The A'-formula corresponding to the B-formula of § 41 is

$$\tfrac{1}{2}\left\{r^pA'_p\left(\frac{rx+1}{r}\right)+r^pA'_p\left(\frac{rx+r-1}{r}\right)\right\}-r^pA'_p\left(\frac{1}{r}\right)$$

$$\equiv (rx)^{p-1}rA'_1\left(\frac{1}{r}\right)+(rx)^{p-3}r^3A'_3\left(\frac{1}{r}\right)+\ldots+(rx)^2r^{p-2}A'_{p-2}\left(\frac{1}{r}\right), \text{ mod } p,$$

whence, putting $rx=\dfrac{1}{m}$,

$$rA'_1\left(\frac{1}{r}\right)+m^2r^3A'_3\left(\frac{1}{r}\right)+m^4r^5A'_5\left(\frac{1}{r}\right)+\ldots+m^{p-3}r^{p-2}A'_{p-2}\left(\frac{1}{r}\right)$$

$$\equiv\tfrac{1}{2}\left\{r^pA'_p\left(\frac{m+1}{rm}\right)+r^pA'_p\left(\frac{(r-1)m+1}{r}\right)\right\}-r^pA'_p\left(\frac{1}{r}\right), \text{ mod } p.$$

53. By § 35 the right-hand side

$$\equiv\frac{1}{2m}\left\{\left(\frac{m+1}{p}\right)_{2rm}+\left(\frac{(r-1)m+1}{p}\right)_{2rm}\right\}-\left(\frac{1}{p}\right)_{2r}, \text{ mod } p;$$

and therefore we find that

$$rA'_1\left(\frac{1}{r}\right)+m^2r^3A'_3\left(\frac{1}{r}\right)+m^4r^5A'_5\left(\frac{1}{r}\right)+\ldots+m^{p-3}r^{p-2}A'_{p-2}\left(\frac{1}{r}\right)$$

$$\equiv\frac{A+B}{2m}-C, \text{ mod } p,$$

where $A=0$ or rm according as the least root of $px\equiv m+1$, mod $2rm$, is $\overline{\underset{<}{=}}$ or $> rm$; $B=0$ or rm, according as the least root of $px\equiv(r-1)m+1$, mod $2rm$, is $\overline{\underset{<}{=}}$ or $> rm$; and $c=0$ or r, according as the least root of $px\equiv 1$, mod $2r$, is $\overline{\underset{<}{=}}$ or $> r$.

54. Since $\qquad 2^{2n+1}A'_{2n+1}(\tfrac{1}{2})=(-1)^nE_n$ (§ 25),

the formula becomes, by putting $r=2$,

$$E_0-m^2E_1+m^4E_2-\ldots+(-1)^{\frac{1}{2}(p-3)}m^{p-3}E_{\frac{1}{2}(p-3)}\equiv\frac{A}{m}-C, \text{ mod } p,$$

where $A = 0$ or $2m$ according as $\left[\frac{m+1}{p}\right]_{4m} <$ or $> 2m$,

$C = 0$ or 2 „ „ $\left[\frac{1}{p}\right]_4 <$ or > 2.

Thus $C = 0$ or 2, according as p is of the form $4k+1$ or $4k+3$.

55. When $m = 1$, $A = \left(\frac{2}{p}\right)_4 = 0$, and therefore the series $\equiv 0$ or -2, mod p, according as p is of the form $4k+1$ or $4k+3$.

When $m = 2$, $A = \left(\frac{3}{p}\right)_8$, which $= 0, 0, 4, 4$, according as $p \equiv 1, 3, 5, 7$, mod 8. Therefore the series $\equiv 0, -2, 2, 0$, mod p, according as $p \equiv 1, 3, 5, 7$, mod 8.

When $m = 3$, $A = \left(\frac{4}{p}\right)_{12} = 0$ or 6, according as p is of the form $3k+1$ or $3k+2$. Therefore the series $\equiv 0, 2, -2, 0$, mod p, according as $p \equiv 1, 5, 7, 11$, mod 12.

When $m = 4$, $A = \left(\frac{5}{p}\right)_{16}$, which $= 0$ if $p \equiv 1, 3, 5, 7$, mod 16, and $= 8$ if $p = 9, 11, 13, 15$, mod 16. Therefore the series $\equiv 0, -2, 0, -2, 2, 0, 2, 0$, mod p, according as $p \equiv 1, 3, 5, 7, 9, 11, 13, 15$, mod 16.

These results agree with those already obtained in §§ 45–48. It will be seen that the second formula (§ 53) is simpler than the first* (§ 44).

---

* Comparing the two formulæ of §§ 44 and 53, we find that they lead to the equation

$$\left[\frac{m+1}{p}\right]_{4m} + \left[\frac{3m+1}{p}\right]_{4m} = \left[\frac{2m+2}{p}\right]_{4m} + 2m.$$

This relation may be proved independently; for, if $p = 4km+h$, h being $< 4m$ and prime to it, and if a_1, b_1, c_1 be the least roots of the respective congruences

$$hx \equiv m+1, \quad hx \equiv 3m+1, \quad hx \equiv 2m+2, \quad \text{mod } 4m,$$

then
$$h(a_1+b_1-c_1) = 2m+\lambda.4m,$$

whence
$$a_1+b_1-c_1 = \frac{2\lambda+1}{h}2m = \nu.2m,$$

ν being an uneven integer. Now it is obvious that ν cannot be > 1, for a_1, b_1, c_1 are all $\leqq 4m$, so that $a_1+b_1-c_1$ cannot exceed $8m$, and therefore we must have $\nu = 1$.

56. Since $$4^{2n+1}A'_{2n+1}(\tfrac{1}{4}) = (-1)^n 2P_n \ (\S\ 25),$$
we find, by putting $r = 4$,

$$P_0 - m^2P_1 + m^4P_2 - \dots + (-1)^{\frac{1}{2}(p-3)} m^{p-3} P_{\frac{1}{2}(p-3)}\text{*}$$
$$= \frac{1}{4m}\left\{\left(\frac{m+1}{p}\right)_{8m} + \left(\frac{3m+1}{p}\right)_{8m}\right\} - \tfrac{1}{2}\left(\frac{1}{p}\right)_8, \bmod p,$$
$$= \frac{A+B}{4m} - C, \bmod p,$$

where $A = 0$ or $4m$, according as $\left[\frac{m+1}{p}\right]_{8m} <$ or $> 4m$,

$B = 0$ or $4m$, „ „ $\left[\frac{3m+1}{p}\right]_{8m} <$ or $> 4m$,

$C = 0$ or 4, „ „ $\left[\frac{1}{p}\right]_8 <$ or > 4.

As particular cases we find

(i.) $P_0 - P_1 + P_2 - \dots + (-1)^{\frac{1}{2}(p-3)} P_{\frac{1}{2}(p-3)} \equiv 0, 1, -2, -1, \bmod p$,
according as $p \equiv 1, 3, 5, 7, \bmod 8$.

(ii.) $P_0 - 2^2P_1 + 2^4P_2 - \dots + (-1)^{\frac{1}{2}(p-3)} 2^{p-3} P_{\frac{1}{2}(p-3)}$
$\equiv 0, 1, -1, -2, 2, 1, -1, 0, \bmod p$,
according as $p \equiv 1, 3, 5, 7, 9, 11, 13, 15, \bmod 16$.

(iii.) $P_0 - 3^2P_1 + 3^4P_2 - \dots + (-1)^{\frac{1}{2}(p-3)} 3^{p-3} P_{\frac{1}{2}(p-3)}$
$\equiv 0, -1, -1, 2, -2, 1, 1, 0, \bmod p$,
according as $p \equiv 1, 5, 7, 11, 13, 17, 19, 23, \bmod 24$.

57. For $r = 3$ the formula of § 55 gives

$$H_0 - m^2H_1 + m^4H_2 - \dots + (-1)^{\frac{1}{2}(p-3)} m^{p-3} H_{\frac{1}{2}(p-3)}\dagger$$
$$\equiv \frac{1}{2m}\left\{\left(\frac{m+1}{p}\right)_{6m} + \left(\frac{2m+1}{p}\right)_{6m}\right\} - \left(\frac{1}{p}\right)_6, \bmod p,$$

from which we obtain the particular cases:

(i.) $H_0 - H_1 + H_2 - \dots + (-1)^{\frac{1}{2}(p-3)} H_{\frac{1}{2}(p-3)} \equiv 0$ or $-\tfrac{3}{2}$, mod p,
according as p is of the form $3k+1$ or $3k+2$.

---

* The value of P_0 is 1 (§ 25).
† The value of H_0 is $\frac{3}{2}$ (§ 25). The values of H_n up to $n = 13$ were given in *Proc. Lond. Math. Soc.*, Vol. XXXI., p. 229.

(ii.) $H_0 - 2^2H_1 + 2^4H_2 - \ldots + (-1)^{\frac{1}{2}(p-3)} 2^{p-3} H_{\frac{1}{2}(p-3)}$

$$\equiv 0,\ -3,\ 3,\ 0,\ \text{mod}\ p,$$

according as $p \equiv 1, 5, 7, 11$, mod 12.

(iii.) $H_0 - 3^2H_1 + 3^4H_2 - \ldots + (-1)^{\frac{1}{2}(p-3)} 3^{p-3} H_{\frac{1}{2}(p-3)}$

$$\equiv 0,\ -3,\ \tfrac{3}{2},\ -\tfrac{3}{2},\ 3,\ 0,\ \text{mod}\ p,$$

according as $p \equiv 1, 5, 7, 11, 13, 17$, mod 18.

58. If p is of the form $2krm+1$, the right-hand member of the general formula is zero, for in this case each of the quantities A, B, C (§ 53) is zero, so that we have

$$rA_1'\left(\frac{1}{r}\right) + m^2r^3A_3'\left(\frac{1}{r}\right) + m^4r^5A_5'\left(\frac{1}{r}\right) + \ldots + m^{p-3}A_{p-2}'\left(\frac{1}{r}\right) \equiv 0,\ \text{mod}\ p.$$

The corresponding B-formula was given in § 51.

59. I have verified numerically all the formulæ involving E's, I's, P's, and H's in §§ 45–50 and §§ 55–57 for the values 5, 7, 11, 13 of p.

60. If in §§ 41 and 52 we put $rx = m$ $\left(\text{instead of } \frac{1}{m}\right)$, we obtain similar series, but in which the coefficients are descending powers of m^2, viz., m^{p-1}, m^{p-3}, m^{p-5}, ..., m^2. Since $m^{p-1} \equiv 1$, mod p, we may also write these coefficients $1, \frac{1}{m^2}, \frac{1}{m^4}, \ldots, \frac{1}{m^{p-3}}$.

We thus find

$$rB_1\left(\frac{1}{r}\right) + \frac{1}{m^2}r^3B_3\left(\frac{1}{r}\right) + \frac{1}{m^4}r^5B_5\left(\frac{1}{r}\right) + \ldots + \frac{1}{m^{p-3}}r^{p-2}B_{p-2}\left(\frac{1}{r}\right)$$

$$\equiv \tfrac{1}{2}\left\{r^pB_p\left(\frac{m+1}{r}\right) - r^pB_p\left(\frac{m+r-1}{r}\right)\right\} - r^pB_p\left(\frac{1}{r}\right),\ \text{mod}\ p,$$

$$rA_1'\left(\frac{1}{r}\right) + \frac{1}{m^2}r^3A_3'\left(\frac{1}{r}\right) + \frac{1}{m^4}r^5A_5'\left(\frac{1}{r}\right) + \ldots + \frac{1}{m^{p-3}}r^{p-2}A_{p-2}'\left(\frac{1}{r}\right)$$

$$\equiv \tfrac{1}{2}\left\{r^pA_p'\left(\frac{m+1}{r}\right) + r^pA_p'\left(\frac{m+r-1}{r}\right)\right\} - r^pA_p'\left(\frac{1}{r}\right),\ \text{mod}\ p;$$

whence, by § 32,

$$\text{(i.)}\quad rB_1\left(\frac{1}{r}\right)+\frac{1}{m^2}r^3B_3\left(\frac{1}{r}\right)+\frac{1}{m^4}r^5B_5\left(\frac{1}{r}\right)+\ldots+\frac{1}{m^{p-3}}r^{p-2}B_{p-2}\left(\frac{1}{r}\right)$$

$$\equiv -\frac{r}{2}+\tfrac{1}{2}\left\{\left[\frac{m+r-1}{p}\right]_r-\left[\frac{m+1}{p}\right]_r\right\}+\left[\frac{1}{p}\right]_r,\ \text{mod}\ p,$$

$$\text{(ii.)}\quad rA_1'\left(\frac{1}{r}\right)+\frac{1}{m^2}r^3A_3'\left(\frac{1}{r}\right)+\frac{1}{m^4}r^5A_5'\left(\frac{1}{r}\right)+\ldots+\frac{1}{m^{p-3}}r^{p-2}A_{p-2}'\left(\frac{1}{r}\right)$$

$$\equiv \tfrac{1}{2}\left\{\left(\frac{m+1}{p}\right)_{2r}+\left(\frac{m+r-1}{p}\right)_{2r}\right\}-\left(\frac{1}{p}\right)_{2r},\ \text{mod}\ p.$$

61. It will be seen that in the formulæ (i.) and (ii.) the classification of p is much simpler than in the corresponding formulæ of §§ 42 and 53, viz., the different cases depend upon the residue of p, mod r or mod $2r$, instead of upon the residue of p, mod mr or mod $2mr$. Thus the number of cases is only $\phi(r)$ or $\phi(2r)$ instead of $\phi(mr)$ or $\phi(2mr)$, where $\phi(n)$ denotes the number of numbers less than n and prime to it. Not only therefore is the number of cases smaller, but the cases themselves are independent of m; so that for any given values of p and m the residue of the series, mod p, depends only upon the residues of p and m, mod r or mod $2r$.

62. Putting $r=4$ in (i.), we have

$$E_0-\frac{1}{m^2}E_1+\frac{1}{m^4}E_2-\ldots+(-1)^{\frac{1}{2}(p-3)}\frac{1}{m^{p-3}}E_{\frac{1}{2}(p-3)}$$

$$\equiv 2+\tfrac{1}{2}\left\{\left[\frac{m+1}{p}\right]_4-\left[\frac{m+3}{p}\right]_4\right\}-\left[\frac{1}{p}\right]_4,\ \text{mod}\ p.$$

Denoting the right-hand side by R, we find, by putting successively $m=1, 2, 3, 4$, that, if $p=4k+1$, then

$$R=0,\ 2,\ 2,\ 0,\ \text{according as}\ m\equiv 1,\ 2,\ 3,\ 4,\ \text{mod}\ 4,$$

and that, if $p=4k+3$, then

$$R=-2,\ -2,\ 0,\ 0,\ \text{according as}\ m\equiv 1,\ 2,\ 3,\ 4,\ \text{mod}\ 4.$$

Thus the residue of

$$E_0-\frac{1}{m^2}E_1+\frac{1}{m^4}E_2-\ldots+(-1)^{\frac{1}{2}(p-3)}\frac{1}{m^{p-3}}E_{\frac{1}{2}(p-3)}$$

is given by the following table:—

	$m \equiv 1$	$m \equiv 2$	$m \equiv 3$	$m \equiv 4$
$p \equiv 1$	0	2	2	0
$p \equiv 1$	−2	−2	0	0

n which the headings of the columns are the residues of m, mod 4, and the arguments of the lines are the residues of p, mod 4.

Thus, for example, since $7 \equiv 3$, mod 4, the table shows that

$$E_0 - \frac{1}{7^2}E_1 + \frac{1}{7^4}E_2 - \dots + (-1)^{\frac{1}{2}(p-3)}\frac{1}{7^{p-3}}E_{\frac{1}{2}(p-3)} \equiv 2 \text{ or } 0, \text{ mod } p,$$

according as p is of the form $4k+1$ or $4k+3$.

63. It is to be noticed that p must not be equal to m, and that the formula and the results given by the table require modification if $p < m$. For in § 10 it was necessary that l should be $< p+r$, which in this case gives $m+3 < p+4$, that is, $p > m-1$.

64. Putting $r = 2$, the formula (ii.) of § 60 gives

$$E_0 - \frac{1}{m^2}E_1 + \frac{1}{m^4}E_2 - \dots + (-1)^{\frac{1}{2}(p-3)}\frac{1}{m^{p-3}}E_{\frac{1}{2}(p-3)}$$

$$\equiv \left(\frac{m+1}{p}\right)_4 - \left(\frac{1}{p}\right)_4, \quad \text{mod } p,$$

from which we may derive, and in a simpler manner, the results given in § 62.*

I have verified these results numerically for the values 1, 2, 3, 4, 5, 6, 7 of m, and the values 5, 7, 11, 13 of p.

---

* Comparing the two formulæ, we obtain the relation

$$\left[\frac{m+1}{p}\right]_4 + \left[\frac{m+3}{p}\right]_4 = \left[\frac{2m+2}{p}\right]_4 + 2,$$

which may be proved independently by the same reasoning as that employed to prove the similar theorem in the note to § 55.

65. Putting $r=3$ in (i.) of § 60, we have

$$I_0-\frac{1}{m^2}I_1+\frac{1}{m^4}I_2-\dots+(-1)^{\frac{1}{2}(p-3)}\frac{1}{m^{p-3}}I_{\frac{1}{2}(p-3)}$$

$$\equiv \tfrac{3}{2}+\tfrac{1}{2}\left\{\left[\frac{m+1}{p}\right]_3-\left[\frac{m+2}{p}\right]_3\right\}-\left[\frac{1}{p}\right]_3, \text{ mod } p.$$

From this formula we obtain the following table giving the residue of the series according to the residues of m and p, mod 3:—

	$m\equiv 1$	$m\equiv 2$	$m\equiv 3$
$p\equiv 1$	0	$\frac{3}{2}$	0
$p\equiv 2$	$-\frac{3}{2}$	0	0

Thus, for example, for $m=5$, which $\equiv 2$, mod 3, we have

$$I_0-\frac{1}{5^2}I_1+\frac{1}{5^4}I_2-\dots+(-1)^{\frac{1}{2}(p-3)}\frac{1}{m^{p-3}}I_{\frac{1}{2}(p-3)}\equiv\tfrac{3}{2}\text{ or } 0, \text{ mod } p,$$

according as p is of the form $3k+1$ or $3k+2$.

I have verified the table for $m=1, 2, 3, 4, 5$ and $p=5, 7, 11, 13$. The results require modification if $p<m$.

66. In this paper I have restricted myself to the consideration of the Bernoullian functions $B_n(x)$ and $A_n'(x)$, when the suffix n is uneven. I have obtained also the residues of these functions in the case when n is even, but the results are more complicated, and I reserve their consideration for a separate paper.