so folgt aus (94), (124), (91) und (92)

$$A_{r,s+1}(\nu) = \pi^r \Gamma^{-2}\left(\frac{r}{2}+s\right) d^{\frac{1-r}{2}} (2h \log \eta)^{-s} \mathfrak{S}_{r,s}(\nu)$$

$$+ o\left(N\nu^{\frac{r}{2}+s-1} \log^{-s} N\nu\right) \sum_{\omega<\nu,\, \omega'<\nu'} 1$$

$$= \pi^r \Gamma^{-2}\left(\frac{r}{2}+s+1\right) d^{\frac{1-r}{2}} (2h \log \eta)^{-s-1} N\nu^{\frac{r}{2}+s} \log^{-s-1} N\nu \,.\, \mathfrak{S}_{r,s+1}(\nu)$$

$$+ o\left(N\nu^{\frac{r}{2}} \log^{-s-1} N\nu\right),$$

d. h. es gilt (125) mit $s+1$ statt s. Also ist auch (93) mit $s+1$ richtig, w. z. b. w.

Radość, den 24. November 1934.

(Eingegangen am 24. November 1934.)

Congruences involving only e-th powers.

By

L. E. Dickson (Chicago).

1. A. Hurwitz[1]) proved that if e is an odd prime,

$$ax^e + by^e + cz^e \equiv 0 \pmod{p}, \quad abc \neq 0,$$

has solutions prime to p for every prime p exceeding a specified limit. He also gave recursion formulas for the number N of solutions of the analogous congruence in any number of variables. We shall show that these formulas, in a more convenient form, serve to express N in terms of the cyclotomic constants (k, h). Nor can the latter be avoided in spite of Hurwitz's explicit exclusion of the theory of cyclotomy.

Moreover we remove the restriction that e is a prime.

2. Let g be a primitive root of the prime $p = ef + 1$. For given integers a_i, Hurwitz defined the symbol $[a_1, \ldots, a_r]$ so that its product by f denotes the number of sets $t_1, \ldots, t_r$ of integers each chosen from $0, 1, \ldots, f-1$ which satisfy

$$\sum_{i=1}^{r} g^{et_i + a_i} \equiv 0 \pmod{p}. \tag{1}$$

We may also permit t_i to range over any complete set of residues modulo f, since the replacement of t_i by $t_i + nf$ inserts in the i-th term of (1) the factor $g^{nef} \equiv 1 \pmod{p}$. For a fixed integer k, $t_i + k$ ranges with t_i over a complete set of residues modulo f. Hence $[a_1, \ldots, a_r]$ is unaltered when we replace a_i by $a_i + ke$. The

[1]) *Jour. für Mathematik*, vol. 136 (1909), p. 272. Case $a = b = c = 1$ by Dickson, *ibid.*, vol. 135, by cyclotomy.

symbol is also unaltered if we add the same integer c to each a_i, since (1) is then multiplied by g^c. The case $c=-a_r$ gives

(2) $$[a_1, \ldots, a_{r-1}, a_r] = [a_1 - a_r, \ldots, a_{r-1} - a_r, 0].$$

Call two sets $(t_1, \ldots, t_r)$ and $(T_1, \ldots, T_r)$ congruent modulo f if and only if $t_1 \equiv T_1, \ldots, t_r \equiv T_r \pmod f$. When as above, each t_i ranges independently over a complete set of residues modulo f, we obtain from $(t_1, \ldots, t_r)$ a complete system of f^r incongruent sets modulo f. The latter is evidently obtained also from $(t_1 + t_r, \ldots, t_{r-1} + t_r, t_r)$. After making this replacement in (1), we may remove the common factor g^{et_r}. Since t_r has f values, we obtain

THEOREM 1. *The symbol* $[a_1, \ldots, a_r]$ *denotes the number of sets* $t_1, \ldots, t_{r-1}$ *each chosen from any complete set of residues modulo* f *which satisfy*

(3) $$g^{a_r} + \sum_{i=1}^{r-1} g^{et_i + a_i} \equiv 0 \pmod p.$$

In particular, $[k, h, 0]$ is the number of sets t, T each from a complete set of residues modulo f which satisfy

(4) $$1 + g^{et+k} + g^{eT+h} \equiv 0 \pmod p.$$

3. Theory when f is even. Then

(5) $$p-1 = 2e \cdot \frac{1}{2} f, \quad -1 \equiv g^{\frac{1}{2}(p-1)} = g^{e \cdot \frac{1}{2} f} \pmod p,$$

and (4) may be written as

(6) $$1 + g^{et+k} \equiv g^{ez+h} \pmod p,$$

where $z = T + f$. In the standard notation of cyclotomy, (k, h) denotes the number of sets t, z chosen from $0, 1, \ldots, f-1$ which satisfy (6). Thus

(7) $$[k, h, 0] = (k, h) \quad (f \text{ even}).$$

As a generalization, let $(a_1, \ldots, a_m)$ be the number of sets $t_1, \ldots, t_m$ each chosen from any complete set of residues modulo f which satisfy

(8) $$1 + \sum_{i=1}^{m} g^{et_i + a_i} \equiv 0 \pmod p.$$

For $m=2$, the symbol is that of cyclotomy. By Theorem 1,

(9) $$[a_1, \ldots, a_m, 0] = (a_1, \ldots, a_m).$$

For $m=1$, we see at once from (5) that

(10) $$(a) = 1 \textit{ if } a \equiv 0 \pmod e, \quad (a) = 0 \textit{ if } a \not\equiv 0 \pmod e.$$

The symbol $(a_1, \ldots, a_m)$ is unaltered if we permute the a_i in any way. If we multiply (8) by the reciprocal of its last term, we see that

(11) $$(a_1, \ldots, a_m) = (a_1 - a_m, \ldots, a_{m-1} - a_m, -a_m).$$

Although the results by Hurwitz, pp. 280-6, were stated only for the case in which e is an odd prime, the proofs are valid also when e is composite, provided always that f be even. By (2), his symbol can be replaced by (9). Without loss of generality we may take $\beta_s = 0$ and replace s by $m+1$. Then

(12) $$(a_2, \ldots, a_r, b_1, \ldots, b_m) = f(a_1 - a_r, \ldots, a_{r-1} - a_r)\,(b_1, \ldots, b_m) + \sum_{j=0}^{e-1} (a_1 + j, \ldots, a_r + j)\,(b_1 + j, \ldots, b_m + j, j),$$

$$\sum_{j=0}^{e-1} (a_1 + j, \ldots, a_r + j, b_1, \ldots, b_m) =$$

(13) $$\{p-1\}\,(a_1 - a_r, \ldots, a_{r-1} - a_r)\,(b_1, \ldots, b_m) + \{f^{r-1} - (a_1 - a_r, \ldots, a_{r-1} - a_r)\}\,\{f^m - (b_1, \ldots, b_m)\}.$$

Since (12) is trivial if $m=0$ or if $r=1$ by (11), the first case of interest is given by $m=1$, $r=2$:

(14) $$(a_1, a_2, b) = f\,(a_1 - a_2)\,(b) + \sum_{j=0}^{e-1} (a_1 + j, a_2 + j)\,(b + j, j),$$

which expresses (a_1, a_2, b) in terms of the cyclotomic constants (k, h). For $r=1$, $m=2$, (13) becomes

(15) $$\sum_{j=0}^{e-1} (a_1 + j, b_1, b_2) = f^2 - (b_1 b_2).$$

But for $r=2$, $m=1$, (13) gives a relation free of the cyclotomic numbers (k, h). Since we may take $a_2 + j$ as a new summation index, the result is not more general than the case $a_2 = 0$:

(16) $$\sum_{j=0}^{e-1}(a+j,\ j,\ b)=\{p-1\}\ (a)\ (b)+\{f-(a)\}\ \{f-(b)\}.$$

4. **Case** $e=3$. By (11), $11=02,\ 22=01$, and

$$111=002,\ 112=122=012,\ 022=011,\ 222=001.$$

The theory of cyclotomy [2]) gives

$$18(00)=2p-16+2L,\quad 18(01)=2p-4-L+9M,$$
$$18(12)=2p+2\ +2L,\quad 18(02)=2p\ -4-L-9M,$$

where $4p=L^2+27M^2$, $L\equiv 1\pmod 3$. Then (14) gives

$$27(000)=p^2+3p+15-4L,\quad 54(001)=2p^2-12p+12+L-27M,$$
$$27(011)=p^2+3\ +2L,\qquad 54(002)=2p^2-12p+12+L+27M,$$
$$27(012)=p^2-3p+\ L.$$

These satisfy the following relations, to which (16) reduce:

$$(011)+2(012)=f^2,\quad (000)+2(011)=f^2+f+1,$$
$$(001)+(002)+(012)=f^2-f.$$

5. **Case** $e=4$, f **even.** By (11),

$$11=\ 03,\quad 13=\ 12,\quad 22=\ 02,\quad 23=\ 12,\quad 33=01,$$
$$111=003,\quad 112=013,\quad 113=122=023,\quad 222=002,$$
$$223=133=012,\quad 033=011,\quad 233=013,\quad 333=001.$$

By the theory of cyclotomy (cf. D),

$$16(00)=p-11\ -6x,\ 16(02)=h=p-3+2x,\ 16(01)=h+8y,$$
$$16(03)=h-8y,\quad 16(12)=p+1-2x,\quad p=x^2+4y,\ x\equiv 1\pmod 4).$$

Then (14) gives

$$64(000)=p^2+14p+21+24x+4x^2,$$
$$64(001)=p^2-10p+9-8y(x+3),$$
$$64(002)=p^2-6p\ +9\ -4x^2,$$
$$64(003)=p^2-10p+9+8y(x+3),$$
$$64(011)=p^2+6p\ +5\ -8x-4x^2,$$

[2]) Dickson, *American Jour. Math.*, vol. 57 (1935). Cited as D.

$$64(012)=p^2-2p\ +1,$$
$$64(022)=p^2-2p\ +5\ -8x+4x^2,$$
$$64(013)=p^2-6p\ +1+4x^2,$$
$$64(023)=p^2-2p\ +1\ +8y(1-x),$$
$$64(123)=p^2-2p\ -3+8x-4x^2.$$

These satisfy the following relations, to which (16) reduce:

$$(002)+(013)=\frac{1}{2}(f^2-f),\quad (011)+2(013)+(123)=f^2,$$

$$(001)+(003)=\frac{1}{2}f^2-f,\quad (000)+2(011)+(022)=(f+1)^2,$$

$$(012)+(023)=\frac{1}{2}f^2,\qquad (022)+\ (123)=\frac{1}{2}f^2.$$

6. **Theory when** f **is odd.** Let $\{a_1,\dots,a_m\}$ denote the number of sets $t_1,\dots,t_m$ modulo f which satisfy (8). By Theorem 1,

(17) $$[a_1,\dots,a_m,\ 0]=\{a_1,\dots,a_m\},$$

(18) $$\{a\}=1\ \text{if}\ a\equiv\frac{1}{2}e\ (\mathrm{mod}\ e),\ \{a\}=0\ \text{if}\ a\not\equiv\frac{1}{2}e\ (\mathrm{mod}\ e).$$

By the definition in § 3 of the cyclotomic number $(k,\ h)$,

(19) $$\{k,\ h\}=\left(k,\ h+\frac{1}{2}e\right)\quad (f\ \text{odd}),$$

since, by (5), (4) becomes

$$1+g^{el+k}\equiv g^n\ (\mathrm{mod}\ p),\quad n=e\left[T+\frac{1}{2}(f-1)\right]+h+\frac{1}{2}e.$$

By modifying the discussion by Hurwitz, we now get

(20) $$[a_1,\dots,a_r,\ b_1,\dots,b_s]=f[a_1,\dots,a_r]\ b_1,\dots,b_s] + \sum_{j=0}^{e-1}\left|a_1,\dots,a_r,\ j+\frac{1}{2}e\right]\ [b_1,\dots,b_s,\ j].$$

His (27) and (28) hold also if f is odd. Also (29), if we replace

$\alpha_1 \equiv \alpha_2$ by $\alpha_1 \equiv \alpha_2 + \frac{1}{2} e$ (mod e). In (20) take $r = s = 2$, $b_2 = 0$, replace j by $-j$, and in the symbols of Σ make the final arguments zero by (2). We get

$$\{a_1 a_2 b\} = f\{a_1 - a_2\}\{b\} + \sum_{j=0}^{e-1}\left\{a_1 + j - \frac{1}{2}e, a_2 + j - \frac{1}{2}e\right\}\{b+j, j\},$$

From our modification of Hurwitz's (29) for $s = 2$, $\alpha_2 = \beta_2 = 0$,

$$(22) \qquad \sum_{j=0}^{e-1}\{a+j, j, b\} = \begin{cases} f^2 - f\{b\} & \text{if } a \not\equiv \frac{1}{2}e \pmod{e}, \\ (f-1)f + (p-f)\{b\} & \text{if } a \equiv \frac{1}{2}e \pmod{e}. \end{cases}$$

7. Case $e = 4$, f odd. By cyclotomy (see D),

$$(22) = (20) = (00),\ (32) = (13) = (01),\ (12) = (31) = (03),$$
$$(33) = (23) = (30) = (21) = (11) = (10),$$
$$16\,(01) = k - 8y,\quad 16\,(03) = k + 8y,\quad k = p + 1 + 2x,$$
$$16\,(00) = k - 8,\quad 16\,(02) = p + 1 - 6x,\ 16\,(10) = p - 3 - 2x,$$

where $p = x^2 + 4y^2$, $x \equiv 1$ (mod 4). We get the $\{k, h\}$ by (19). By (21),

$$64\,\{000\} = p^2 - 10p - 3 + 24x + 4x^2,$$
$$64\,\{001\} = p^2 + 2p - 3 - 8y(x+3),$$
$$64\,\{002\} = p^2 - 6p + 9 - 4x^2,$$
$$64\,\{003\} = p^2 + 2p - 3 + 8y(x+3),$$
$$64\,\{011\} = p^2 - 2p - 3 - 8x - 4x^2,$$
$$64\,\{012\} = p^2 - 6p + 5 + 8y(x-1),$$
$$64\,\{013\} = p^2 - 6p + 1 + 4x^2$$
$$64\,\{023\} = p^2 - 6p + 5 - 8y(x-1),$$
$$64\,\{022\} = p^2 + 6p + 13 - 8x + 4x^2,$$
$$64\,\{123\} = p^2 + 6p + 5 + 8x - 4x^2.$$

The remaining $\{abc\}$ are equal to these as in §5. The displayed $\{abc\}$ satisfy the following relations, to which (22) reduce:

$$\{002\} + \{013\} = \frac{1}{2}(f^2 - f), \qquad \{011\} + 2\{013\} + \{123\} = f^2,$$
$$\{001\} + \{003\} = \frac{1}{2}(f^2 + f), \qquad \{000\} + 2\{011\} + \{022\} = f^2,$$
$$\{012\} + \{023\} = \frac{1}{2}(f^2 - f), \qquad \{022\} + \{123\} = \frac{1}{2}(f+1)^2.$$

8. Number of solutions of the congruence.

$$(23) \qquad d + \sum_{i=1}^{r} c_i x_i^e \equiv 0, \text{ each } c_i \not\equiv 0 \pmod{p}.$$

We may write $c_i \equiv g^{a_i}$ (mod p). It is readily proved (in D) that the number N of solutions all prime to p of (23) is e^r times the number of sets of values of $t_1, \ldots, t_r$ each chosen from $0, 1, \ldots, f-1$ which satisfy

$$(24) \qquad d + \sum_{i=1}^{r} g^{et_i + a_i} \equiv 0 \pmod{p}.$$

If $d \equiv 0$ (mod p), (24) becomes (1), whence $N = e^r f[a_1, \ldots, a_r]$. But if $d \not\equiv 0$, $d \equiv g^{a_{r+1}}$ (mod p) and Theorem 1 gives

$$N = e^r [a_1, \ldots, a_{r+1}].$$

We readily deduce the total number T of all solutions of (23) by using the number of solutions in which a single x_i is a multiple of p, the number of solutions in which just two variables are multiples of p, etc.

The case $d \not\equiv 0$ reduces by multiplication to the case $d \equiv 1$ (mod p). The total number T of solutions of

$$(25) \qquad 1 + c_1 x_1^e + c_2 x_2^e + c_3 x_3^e \equiv 0,\ c_i \equiv g^{a_i} \pmod{p}$$

is therefore

$$T = e^3[a_1 a_2 a_3 0] + e^2[a_2 a_3 0] + e^2[a_1 a_3 0] + e^2[a_1 a_2 0] + e[a_3 0] + e[a_2 0] + e[a_1 0].$$

For example, if each $c_i = 1$, and f is even,

$$(26) \qquad T = e^3(000) + 3e^2(00) + 3e.$$

When $e = 3$ or 4, T is respectively

$$p^2 + 6p - L, \qquad p^2 + 17p + 6x + 4x^2.$$

(Received 13 January, 1935.)