to Weierstrass, with the totality of those functions δy of class C' which vanish at x_1 and x_2 and satisfy the relation $\delta K = 0$.

The proof of this lemma — which is an essential step in the chain of conclusions, and whose omission forms a serious gap in the older theory — constitutes the second difficulty.

Neither of these difficulties occurs in the proof which we have given above.

FREIBURG, i. B.,
November 19, 1908.

NOTES ON THE SIMPLEX THEORY OF NUMBERS.

BY PROFESSOR R. D. CARMICHAEL.

(Read before the American Mathematical Society, October 31, 1908.)

I. *Continued Product of the Terms of an Arithmetical Series.*

1. Let a and c be two relatively prime positive integers and form the arithmetical series

$$xa + c, \quad (x = 0, 1, 2, \cdots, n - 1).$$

If we inquire what is the highest power of a prime p contained in the product

$$\prod_{x=0}^{x=n-1} (xa + c), \quad a \not\equiv 0 \,(\text{mod}\, p),$$

we shall find that the general result takes an interesting form. The solution of the problem may be effected in the following manner:

Evidently there exists some number x such that $xa + c$ is divisible by p. Let i be the smallest value of x for which this division is possible, and let c_1 be the quotient thus obtained. Using the notation

$$H\{y\} \tag{1}$$

to represent the index of the highest power of p contained in y, we will show that

$$H\left\{\prod_{x=0}^{x=n-1} (xa + c)\right\} = H\left\{\prod_{x=0}^{x=e_1} (xa + c_1)\right\} + e_1 + 1, \tag{2}$$

where

$$e_1 = \left[\frac{n-1-i_1}{p}\right]$$

is the largest integer not greater than $(n-1-i_1)/p$. In order to prove (2) we have only to notice that in the product of its first member only factors of the form

$$(mp + i_1)a + c$$

contain p and that the quotient of the division is always of the form

$$ma + c_1,$$

and that e_1 is the highest possible value of m. Performing the same operation on the H-function of the second member and continuing the process, we should finally arrive at a number which is simply the index of the required power of p.

In order to write this result in a convenient form let us define a suitable notation. Let i_r be the least integer such that $i_r a + c_{r-1}$ contains p and let c_r be the quotient of this division. For uniformity, set $c = c_0$ and $n - 1 = e_0$. Further, let e_r be defined by

$$\left[\frac{e_{r-1} - i_r}{p}\right] = e_r. \tag{3}$$

Also let t be the first subscript for which

$$c_t(a + c_t)(2a + c_t) \cdots (e_t a + c_t)$$

does not contain the factor p. Then the preceding result may be written thus

$$H\left\{\prod_{x=0}^{x=n-1}(xa + c_0)\right\} = \sum_{r=1}^{r=t-1}(e_r + 1). \tag{4}$$

Since $0 \leqq i_r \leqq p - 1$, as is evident from the definition of i_r, we may deduce from (3) the following inequalities:

$$\left[\frac{e_{r-1} - (p-1)}{p}\right] \leqq e_r \leqq \left[\frac{e_{r-1}}{p}\right].$$

Hence

$$\left[\frac{e_{r-1} + 1}{p}\right] \leqq e_r + 1 \leqq \left[\frac{e_{r-1} + p}{p}\right]. \tag{5}$$

This gives

$$\left[\frac{n}{p}\right] \leqq e_1 + 1 \leqq \left[\frac{n-1}{p}\right] + 1,$$

$$\left[\frac{n}{p^2}\right] \leqq e_2 + 1 \leqq \left[\frac{n-1}{p^2}\right] + 1,$$

$$\left[\frac{n}{p^3}\right] \leqq e_3 + 1 \leqq \left[\frac{n-1}{p^3}\right] + 1,$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot$$

Taking the sum of these inequalities, we have by (4)

$$(6) \qquad \begin{aligned} \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \cdots &\leqq H\left\{\prod_{x=0}^{x=n-1}(xa + c_0)\right\} \\ &\leqq \left[\frac{n-1}{p}\right] + \left[\frac{n-1}{p^2}\right] + \cdots + R(n-1), \end{aligned}$$

where $R(n-1)$ is the index of the highest power of p not greater than $n-1$.

This result takes different forms according as n is or is not a power of p. If n is a power of p, we have evidently

$$(7) \qquad \left[\frac{n}{p^a}\right] = \left[\frac{n-1}{p^a}\right] + 1$$

for every p^a equal to or less than n. Remembering that when $n = p^h$

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \cdots = \frac{p^h - 1}{p-1},$$

and using equation (7) in connection with inequality (6), we have

$$(8) \qquad H\left\{\prod_{x=0}^{x=n-1}(xa + c_0)\right\} = \frac{n-1}{p-1}, \quad n = p^h.$$

When n is not a power of p, it is evident that

$$(9) \qquad \left[\frac{n}{p^a}\right] = \left[\frac{n-1}{p^a}\right].$$

Suppose now that

$$(10) \qquad n = \delta_h p^h + \delta_{h-1} p^{h-1} + \cdots + \delta_1 p + \delta_0, \quad \delta_h \neq 0,$$

and at least one other δ is not zero. Employing (9) and the well-known formula

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots=\frac{n-(\delta_h+\delta_{h-1}+\cdots+\delta_1+\delta_0)}{p-1},$$

we may write (6) as follows:

$$(11)\qquad \begin{aligned}\frac{n-(\delta_h+\cdots+\delta_1+\delta_0)}{p-1}\leqq H\left\{\prod_{x=0}^{x=n-1}(xa+c_0)\right\}\\ \leqq h+\frac{n-(\delta_h+\cdots+\delta_1+\delta_0)}{p-1}.\end{aligned}$$

The inequalities in (11) confine the value of H in narrow limits which are easily calculated.

2. In the series $xa+c$, it may happen that the first x for which $xa+c$ is divisible by p will give c as the quotient of this division. Then in the preceding discussion all the c's are equal; and then also all the i's. Dropping subscripts from i and c and making repeated use of equation (3), we have

$$e_1=\left[\frac{n-1-i}{p}\right],$$

$$e_2=\left[\frac{e_1-i}{p}\right]=\left[\frac{e_1p-ip}{p^2}\right]=\left[\frac{n-1-i-ip}{p^2}\right],$$

$$e_3=\left[\frac{e_2-1}{p}\right]=\left[\frac{e_2p^2-ip^2}{p^3}\right]=\left[\frac{n-1-i-ip-ip^2}{p^3}\right],$$

$$\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot\quad\cdot$$

If we add one to each member of each of these equations and take the sum of the results; then further, if we replace the resulting first member by its value taken from (4), we have

$$(12)\qquad \begin{aligned}H\left\{\prod_{x=0}^{x=n-1}(xa+c)\right\}=\left[\frac{n-1-i+p}{p}\right]\\ +\left[\frac{n-1-i-ip+p^2}{p^2}\right]+\left[\frac{n-1-i-ip-ip^2+p^3}{p^3}\right]+\cdots.\end{aligned}$$

3. If $a=c=1$, equation (12) takes a very simple form. For this case $i=p-1$. The result is the well-known theorem that the highest power of p contained in $n!$ is that whose index is

$$\left[\frac{n}{p}\right]+\left[\frac{n}{p^2}\right]+\cdots=\frac{n-(s_h+\cdots+s_1+s_0)}{p-1},$$

where

$$n = s_h p^h + s_{h-1} p^{h-1} + \cdots + s_1 p + s_0.$$

4. If $a = 2$ and $c = 1$, equation (12) takes a special form of considerable interest. The terms of $xa + c$ are the natural odd numbers in order, and p is an odd prime. It is evident that $i = \frac{1}{2}(p - 1)$. Therefore

$$\left[\frac{n - 1 - i - ip \cdots - ip^{\beta-1} + p^\beta}{p^\beta}\right]$$

$$= \left[\frac{2n-2-2i-2ip-\cdots-2ip^{\beta-1}+2p^\beta}{2p^\beta}\right] = \left[\frac{2n-1+p^\beta}{2p^\beta}\right].$$

Then (12) becomes

$$H\{1\cdot 3\cdot 5\cdots(2n-1)\} = \left[\frac{2n-1+p}{2p}\right]$$

$$+ \left[\frac{2n-1+p^2}{2p^2}\right] + \left[\frac{2n-1+p^3}{p^3}\right] + \cdots.$$

II. *An Extension of Fermat's Theorem.*

It will be shown that the congruence

$$x^{\phi(n)} \equiv 1 (\mathrm{mod}\ n),$$

where $\phi(n)$ is Euler's ϕ-function of n, is still true when the modulus is a multiple of n formed in a definite way, x being prime to the new modulus.

It has been shown * that $\phi(z) = a$ has always more than one solution. If z_1 and z_2 are two roots of $\phi(z) = a$, then z_1 and z_2 must each have a factor not common to the two except when one is an odd number and the other is twice that odd number; and hence, except in this case, their lowest common multiple is greater than either of them. Now if $z_1, z_2, \cdots, z_i$ are all the roots of $\phi(z) = a$, we have by Fermat's theorem the congruences

$$x^a \equiv 1 (\mathrm{mod}\ z_1),\ x^a \equiv 1 (\mathrm{mod}\ z_2),\ \cdots,\ x^a \equiv 1 (\mathrm{mod}\ z_i),$$

where in each case x is prime to the modulus involved. Now if L is the lowest common multiple of $z_1, z_2, \cdots, z_i$ and x is prime to L, we have

(1) $$x^a \equiv 1 (\mathrm{mod}\ L),$$

where L is greater than any number whose totient is a except

* Carmichael, BULLETIN, vol. 13, p. 241.

when the equation $\phi(z) = a$ has only the two solutions $z = L$, $z = \frac{1}{2}L$. Hence,

THEOREM. *Except when n and $\frac{1}{2}n$ are the only numbers whose totient is the same as that of n, the congruence $x^{\phi(n)} \equiv 1$ holds for a modulus which is some multiple of n.*

A working method for finding such a modulus is the following:

Set $\phi(n) = a$, for convenience. Separate a into its prime factors and find the highest power of each prime p contained in a such that $\phi(p^a)$ is equal to or is a factor of a. Suppose that the following primes are found: $p_1^{a_1}, p_2^{a_2}, \cdots, p_j^{a_j}$. Then write out all the divisors of a and take every prime q such that $q - 1$ is equal to any one of these divisors, but $q \neq$ any p; and say we have $q_1, q_2, \cdots, q_k$. Then set

$$(2) \qquad M = p_1^{a_1} p_2^{a_2} \cdots p_j^{a_j} q_1 q_2 \cdots q_k.$$

Then evidently

$$(3) \qquad X^a \equiv 1 (\text{mod } M),$$

when X is prime to M. (It should be noticed that M may be a multiple of L in congruence (1).)

As thus defined, M is a definite function of a; say $M = M(a)$. For every odd value of a, except $a = 1$, we have $M(a) = 1$, as the reader may readily verify. Some even values of a give also $M(a) = 1$. There follows a table giving the value of $M(a)$ for each a for which $M \neq 1$ up to $a = 150$.

a	$M(a)$	a	$M(a)$	a	$M(a)$
2	12	48	2 227 680	104	12 720
4	120	52	6 360	106	1 284
6	252	54	43 092	108	22 265 704 680
8	240	56	6 960	110	33 396
10	132	58	708	112	26 740 320
12	32 760	60	3 407 203 800	116	7 080
16	8 160	64	32 640	120	279 390 711 600
18	14 364	66	388 332	126	549 092 628
20	6 600	70	9 372	128	65 280
22	276	72	10 087 262 640	130	17 292
24	65 520	78	948	132	50 483 160
28	3 480	80	18 400 800	136	10 960
30	85 932	82	996	138	1 646 316
32	16 320	84	285 962 040	140	13 589 400
36	69 090 840	88	491 280	144	342 966 929 760
40	108 240	92	5 640	148	17 880
42	75 852	96	432 169 920	150	12 975 732
44	2 760	100	3 333 000		
46	564	102	25 956		

III. *The Solutions of* $\phi(z) = a$.

It is desirable to have a general method for finding all the solutions of

$$\phi(z) = a$$

for any given a. The method used in Note II for finding M in congruence (1) is suggestive, and we may formulate a rule thus:

Find M as in Note II. Evidently, *the solutions of $\phi(z) = a$ will all be factors of M. Then examine all the factors of M and retain each one whose totient is a.*

ALABAMA PRESBYTERIAN COLLEGE,
ANNISTON, ALABAMA.

THE SOLUTION OF BOUNDARY PROBLEMS OF LINEAR DIFFERENTIAL EQUATIONS OF ODD ORDER.

BY PROFESSOR W. D. A. WESTFALL.

E. SCHMIDT[1] has studied the set of linear integral equations with non-symmetric matrix

$$(1) \quad \phi_i(s) = \lambda_i \int_a^b K(s, t)\psi_i(t)dt, \qquad \psi_i(s) = \lambda_i \int_a^b K(t, s)\phi_i(t)dt,$$

and has shown that, if there can be found for a function $f(x)$ a continuous function $h(x)$, such that

$$(2) \qquad f(x) = \int_a^b K(x, t)\, h(t)dt,$$

then

$$(3) \qquad f(x) = \sum_i \frac{\phi_i(x)}{\lambda_i} \int_a^b h(t)\, \psi_i(t)dt,$$

where ϕ_i runs over a complete set of solutions of (1) which have been normalized and orthogonalized, *i. e.*,

$$(4) \qquad \int_a^b \phi_i \psi_j dx = \begin{cases} 1, & i = j, \\ 0, & i \neq j. \end{cases}$$

---

* *Math. Annalen*, vol. 63, p. 459.