NOTE ON A NEW NUMBER THEORY FUNCTION.

BY MR. R. D. CARMICHAEL.

(Read before the American Mathematical Society, September 13, 1909.)

THE present note deals with the properties of a number theory function defined by means of Euler's ϕ-function in the following way:

$\lambda(p^a) = \phi(p^a)$ when p is an odd prime;
$\lambda(2^a) = \phi(2^a)$ if $a = 0$, 1, or 2; $\lambda(2^a) = \frac{1}{2}\phi(2^a)$ if $a > 2$;*
$\lambda(2^a p_1^{a_1} \cdots p_i^{a_i}) =$ the lowest common multiple of $\lambda(2^a)$, $\lambda(p_1^{a_1})$, $\cdots$, $\lambda(p_i^{a_i})$, p_1, $\cdots$, p_i being different odd primes.

Throughout, in a congruence such as

$$x^a \equiv 1 \pmod{n}$$

it will be assumed that x is prime to n. Then we have the theorem

(1) $$x^{\lambda(p^a)} \equiv 1 \pmod{p^a}$$

for every prime p and integer a. For, by Fermat's theorem, (1) is true when p is an odd prime and also when $p = 2$ and $a = 1$ or 2, in view of the definition of λ. Then we have to examine only the case where $p = 2$ and $a > 2$.

Now by Fermat's theorem we have

$$x^{\phi(2^a)} \equiv 1 \pmod{2^a}, \quad (a > 2).$$

But it is known that the foregoing congruence has no primitive root; that is, for any odd x the congruence is true when $\phi(2^a)$ is replaced by some factor of $\phi(2^a)$ less than the number itself. But $\frac{1}{2}\phi(2^a) = \lambda(2^a)$ is the largest factor of $\phi(2^a)$ less than itself and contains all other such factors. Then

$$x^{\frac{1}{2}\phi(2^a)} \equiv 1 \pmod{2^a}, \quad (a > 2).$$

Hence the theorem of congruence (1) is proved.

This result may be employed to obtain a simple demonstration of the following analog of Fermat's general theorem:

* It is in respect to this part of the definition alone that $\lambda(n)$ differs from $\psi(n)$ defined by Bachmann, Niedere Zahlentheorie, I, p. 157.

I. *For any given n the congruence*

$$x^{\lambda(n)} \equiv 1 \pmod{n}$$

is satisfied by every x prime to n.

For suppose

$$n = 2^{\alpha} p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_i^{\alpha_i}$$

and let β be any number prime to n. Then since $\lambda(n)$ is a multiple of every $\lambda(p^{\alpha})$, $p = 2, p_1, \cdots, p_i$, we have

$$\beta^{\lambda(n)} \equiv 1 \pmod{2^{\alpha}}, \qquad \beta^{\lambda(n)} \equiv 1 \pmod{p_1^{\alpha_1}},$$

$$\cdots, \beta^{\lambda(n)} \equiv 1 \pmod{p_i^{\alpha_i}}.$$

From these congruences the theorem follows.

If $a^{\lambda(n)}$ is the first power of a congruent to 1 modulo n, we may say that a is a primitive λ-root (mod n). To distinguish, we may speak of the usual primitive root as a primitive ϕ-root (mod n). It follows immediately from the theory of primitive ϕ-roots that primitive λ-roots always exist when n is the power of any prime; for this is but another statement of well-known results for the modulus p^{α}. The λ-function introduces a simplification and allows the principal theory of the existence of primitive roots to be summarized into the following theorem:

II. *In every congruence*

$$x^{\lambda(n)} \equiv 1 \pmod{n} \tag{2}$$

a solution g exists which is a primitive λ-root, and for any such solution g there are $\phi\{\lambda(n)\}$ primitive roots congruent to powers of g.

If any primitive root g exists, g^{α} is or is not a primitive root according as α is or is not prime to $\lambda(n)$; and therefore the number of primitive λ-roots which are congruent to powers of any such root g is $\phi\{\lambda(n)\}$.

The existence of a primitive λ-root in every case is easily shown by induction. If n is a power of a prime the theorem has already been established. We will suppose that it has been established when n is the product of powers of r different primes and show that the theorem still remains true when n is the product of powers of $r + 1$ different primes; and from this follows the theorem in general.

Put

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r} p_{r+1}^{a_{r+1}},$$

and let h be a primitive λ-root of

$$x^{\lambda(p_1^{a_1} \cdots p_r^{a_r})} \equiv 1 \pmod{p_1^{a_1} \cdots p_r^{a_r}}; \tag{3}$$

whence $h + p_1^{a_1} \cdots p_r^{a_r} x$ is another form of the same root if x is any integer. Likewise, if c is any primitive root of

$$x^{\lambda(p_{r+1}^{a_{r+1}})} \equiv 1 \pmod{p_{r+1}^{a_{r+1}}}, \tag{4}$$

another form of the root is $c + p_{r+1}^{a_{r+1}} y$, where y is any integer. If x and y can be so chosen that

$$h + p_1^{a_1} \cdots p_r^{a_r} x = c + p_{r+1}^{a_{r+1}} y,$$

either member of this equation will be a common primitive root of congruences (3) and (4); that is, a common primitive root of the two congruences may always be obtained provided that the equation

$$p_1^{a_1} \cdots p_r^{a_r} x - p_{r+1}^{a_{r+1}} y = c - h$$

has always a solution in which x and y are integers. But since the coefficients of x and y are relatively prime, the equation has always a solution in integers.

Now let g be the common primitive λ-root of congruences (3) and (4) and write

$$g^{\alpha} \equiv 1 \pmod{n},$$

where α is to be the smallest integer for which the congruence is true. Since g is a primitive λ-root of (3), α is a multiple of $\lambda(p_1^{a_1} \cdots p_r^{a_r})$. In the same way it is a multiple of $\lambda(p_{r+1}^{a_{r+1}})$. But $\lambda(n)$ is the lowest common multiple of $\lambda(p_1^{a_1} \cdots p_r^{a_r})$ and $\lambda(p_{r+1}^{a_{r+1}})$; therefore α is a multiple of $\lambda(n)$, and hence $\alpha = \lambda(n)$ in view of the analogue of Fermat's theorem already demonstrated; for $g = h + p_1^{a_1} \cdots p_r^{a_r} x = c + p_{r+1}^{a_{r+1}} y$ is evidently prime to n. Therefore g is a primitive λ-root of

$$x^{\lambda(n)} \equiv 1 \pmod{n}.$$

The theorem announced follows by simple induction.

There is nothing in the preceding argument to indicate that the primitive λ-roots of (2) are all in a single set obtained by taking the powers of some root g; in fact this is not even usually

so when n contains more than one prime factor. By taking powers of a primitive root g a set of primitive roots is obtained which evidently is identical with the set obtained by taking powers of any other root belonging to the set. We may say then that the set thus obtained is the set belonging to g. Then

III. *If* $\lambda(n) > 2$, *the product of the primitive roots in the set belonging to any* g *is congruent to* 1 (mod n).

These primitive roots are

$$g,\ g^{c_1},\ g^{c_2},\ \cdots,\ g^{c_\nu},$$

where $1, c_1, c_2, \cdots, c_\nu$ are the integers less than $\lambda(n)$ and prime to it. If any one of these is c, another is $\lambda(n) - c$ when $\lambda(n) > 2$. Hence

$$1 + c_1 + c_2 + \cdots + c_\nu \equiv 0 \quad [\text{mod } \lambda(n)].$$

Therefore

$$g^{1 + c_1 + c_2 + \cdots + c_\nu} \equiv 1 \quad (\text{mod } n).$$

Hence the theorem.

COROLLARY. *The product of all the primitive* λ*-roots of* $x^{\lambda(n)} \equiv 1$ (mod n) *is congruent to* 1 (mod n) *when* $\lambda(n) > 2$.

When n is given it is of course a very easy matter to find $\lambda(n)$. But the inverse problem, to find every x such that

$$\lambda(x) = a \quad \text{or} \quad \lambda^{-1}(a) = x, \tag{5}$$

is more difficult. We construct a method for solving this problem.

IV. *If* x_1 *is the largest value of* x *satisfying* (5), *any other solution* x_2 *is a factor of* x_1.

Suppose that p^α is the highest power of any prime p such that $\lambda(p^\alpha)$ is a factor of a. Then evidently p^α is a factor of x_1; but no higher power of p is a factor of x_2, and therefore the theorem follows. Hence the following method for solving the problem in consideration:

Obtain the largest solution x_1 *of* (2); *examine every divisor* d *of* x_1 *and retain those* d*'s for which* $\lambda(d) = a$. *These are all the solutions of* (5).

To make the rule effective we require a means of computing x_1. It is evident that the following method leads to the desired result: Separate a into its prime factors and find the highest power p^α of each prime p contained in a such that $\lambda(p^\alpha)$ is equal to or is a factor of a. Suppose that the following prime powers are found: $p_1^{\alpha_1}, p_2^{\alpha_2}, \cdots, p_i^{\alpha_i}$. 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 is not eqnal to any p; and say we have q_1, $q_2, \cdots, q_k$. Then

$$x_1 = p_1^{a_1} p_2^{a_2} \cdots p_i^{a_i} q_1 q_2 \cdots q_k. \tag{6}$$

V. COROLLARY. *If y_1 and x_1 respectively are the largest solutions of the equations*

$$\lambda^{-1}(ma) = y, \quad \lambda^{-1}(a) = x, \tag{5a}$$

where m is any integer > 1, then $y_1 > x_1$.

(It is to be observed that in equations (5) and (5a), a and ma are assumed to be numbers such that each equation has at least one solution.)

By aid of theorem IV and the rule based on it I have constructed the following table containing every n for each $\lambda(n) > 1$ and $\leqq 24$. It is interesting to notice that $\lambda(x) = 12$ has 84 solutions.

$\lambda(n)$	n
2	3, 4, 6, 8, 12, 24.
4	5, 10, 15, 16, 20, 30, 40, 48, 60, 80, 120, 240.
6	7, 9, 14, 18, 21, 28, 36, 42, 56, 63, 72, 84, 136, 168, 252, 504.
8	32, 96, 160, 480.
10	11, 22, 33, 44, 66, 88, 132, 264.
12	13, 26, 35, 39, 45, 52, 65, 70, 78, 90, 91, 104, 105, 112, 117, 130, 140, 144, 156, 180, 182, 195, 208, 210, 234, 260, 273, 280, 312, 315, 336, 360, 364, 390, 420, 455, 468, 520, 546, 560, 585, 624, 630, 720, 728, 780, 819, 840, 910, 936, 1008, 1040, 1092, 1170, 1260, 1365, 1456, 1560, 1638, 1680, 1820, 1872, 2184, 2340, 2520, 2730, 3120, 3276, 3640, 4095, 4368, 4680, 5040, 5460, 6552, 7280, 8190, 9360, 10920, 13104, 16380, 21840, 32760, 65520.
16	17, 34, 51, 64, 68, 85, 102, 136, 170, 192, 204, 255, 272, 320, 340, 408, 510, 544, 680, 816, 960, 1020, 1088, 1360, 1632, 2040, 2720, 3264, 4080, 5440, 8160, 16320.
18	19, 27, 38, 54, 57, 76, 108, 114, 133, 152, 171, 189, 216, 228, 266, 342, 378, 399, 456, 513, 532, 684, 756, 798, 1026, 1064, 1197, 1368, 1512, 1596, 2052, 2394, 3192, 3591, 4104, 4788, 7182, 9576, 14364, 28728.
20	25, 50, 55, 75, 100, 110, 150, 165, 176, 200, 220, 275, 300, 330, 400, 440, 550, 600, 660, 825, 880, 1100, 1200, 1320, 1650, 2200, 2640, 3300, 4400, 6600, 13200.
22	23, 46, 69, 92, 138, 184, 276, 552.
24	224, 288, 416, 672, 1120, 1248, 1440, 2016, 2080, 2912, 3360, 3744, 6240, 8736, 10080, 14560, 18720, 26208, 43680, 131040.

VI. *Let a be that divisor of α for which $\lambda^{-1}(a) = x$ has a greatest solution x_1 greater than such a solution when for a any other divisor of α is taken. Then x_1 is the largest divisor of $z^\alpha - 1$ for every z prime to the divisor.*

That x_1 divides $z^\alpha - 1$ follows from Theorem I. Let y_1 be any number greater than x_1. Then in view of the conditions in the proposition $\lambda(y_1)$ is not a divisor of α. Hence, from the foregoing theory of primitive roots, it follows that there is some number z such that $z^\alpha - 1$ is not divisible by y_1. Hence the theorem. (From V. it is seen that $a = \alpha$ when $\lambda^{-1}(a) = x$ has a solution.)

In a previous paper * I tabulated a function $M(a)$ for possible values of a up to $a = 150$. A reference to the definition of $M(a)$ there given will show that $2M(a)$ is identical with our present x_1, the largest solution of $\lambda^{-1}(a) = x$, provided this equation has a solution. That table will therefore serve for determining x_1 for $a \leqq 150$. Thus it is seen that the largest divisor of $z^{144} - 1$ for every z which is prime to the divisor is 685,933,859,520. Further, the table for $M(a)$ may also be used in continuing the table of the present paper.

Professor J. H. Jeans † and more recently Mr. E. B. Escott ‡ have discussed the converse of Fermat's theorem, showing that the relation

$$e^{n-1} \equiv 1 \pmod{n}, \tag{7}$$

which is always true, when n is prime, for any value of e prime to n, is for any particular value of e true for values of n which are not prime. This result will be extended by proving the theorem that *there are values of composite n for which relation (7) is true when e is any number prime to n.* In view of the foregoing theory of the congruence

$$e^{\lambda(n)} \equiv 1 \pmod{n},$$

it is evidently necessary and sufficient for this result that n has the property

$$n - 1 \equiv 0 \quad [\text{mod } \lambda(n)]. \tag{8}$$

When $n > 2$, $\lambda(n)$ is even; and therefore (8) can be true for composite n only when n is odd. Further, since $\lambda(n)$ is prime

* BULLETIN, ser. 2, vol. 15, no. 5 (February, 1909), p. 222.
† *Messenger of Mathematics*, vol. 27, p. 174.
‡ *Messenger of Mathematics*, vol. 36, p. 175.

to n it follows that n contains no repeated prime factor; and hence *n is a product of odd primes no one of which is repeated.*

That n is not the product of two odd primes is easily shown. Suppose $n = p_1 p_2$, $p_2 > p_1$. Then

$$\frac{p_1 p_2 - 1}{p_2 - 1} = p_1 + \frac{p_1 - 1}{p_2 - 1} \neq \text{integer}.$$

But $\lambda(n)$ contains the factor $p_2 - 1$ and is therefore not a divisor of $n - 1 = p_1 p_2 - 1$.

On the other hand it is easy to find values of $n = p_1 p_2 p_3$, satisfying relation (8). It is necessary and sufficient that

$$\frac{p_i p_j p_k - 1}{p_i - 1} \equiv \frac{p_j p_k (p_i - 1) + p_j p_k - 1}{p_i - 1} = \text{integer},$$
$$(i, j, k = 1, 2, 3 \text{ in some order});$$

that is, that $(p_j p_k - 1)/(p_i - 1) = \text{integer}$. The following values of n have been found by inspection using this relation:

$$3 \cdot 11 \cdot 17, \quad 5 \cdot 13 \cdot 17, \quad 7 \cdot 13 \cdot 31, \quad 7 \cdot 31 \cdot 73.$$

By a similar method one may seek values of n for which n is the product of four or more primes; but the work will not be carried out here.

An example given by Lucas,* illustrating the failure of the converse of Fermat's theorem, belongs to a different class of exceptions. He shows that

$$2^{n-1} \equiv 1 \pmod{n}, \text{ when } n = 73 \cdot 37.$$

Here $\lambda(n) = 72$ while $n - 1 = 36 \cdot 75$; or $n - 1$ is a multiple of $\frac{1}{2}\lambda(n)$. Then we can easily find other values than 2 and its powers for which the preceding congruence is true. In fact every number prime to n belongs to some index which is a divisor of $\lambda(n)$. But every divisor of $\lambda(n) = 72$ except 8, 24, 72 is a divisor of $n - 1$. Hence the congruence $a^{n-1} \equiv 1 \pmod{n}$ is true for any integer a prime to n and not belonging to the index 8, 24, or 72 (mod n). Most of the examples given by Escott in the paper already referred to are similar to this one. These, however, are not so interesting as those for which congruence (7) is true for any e prime to n.

* Théorie des nombres, p. 422.