FUNCTIONAL EQUATIONS FOR TOTIENTS*

BY E. T. BELL

1. *Totient Functions.* Let $p_1, \cdots, p_a$ be the distinct prime factors of n. The number of different sets of k equal or distinct positive integers less than or equal to n whose G. C. D. is prime to n is the Jordan totient $\phi_k(n)$ of order k, and

$$\phi_k(n) \equiv n^k(1 - p_1^{-k}) \cdots (1 - p_a^{-k}). \tag{1}$$

If k is complex, $\phi_k(n)$ is defined by (1). The special case $k=1$ gives Euler's $\phi(n)$. The case $k=0$ is trivial and will be ignored.

We say that the numerical function $f \equiv f(n)$ is *factorable* if $f(1)=1$ (which is adjoined to the definition of $f(n)$ if $f(n)$ is defined arithmetically for $n>1$ but not for $n=1$), and if $f(mn) = f(m)\,f(n)$ for all pairs of coprime integers m, n.

Factorability is distinct from separability, which we define as follows. Let α denote a variable integer >0 and p a fixed but arbitrary prime. Write $p^\alpha \equiv y$, $p \equiv x$, and regard x, y as independent variables. Then the factorable numerical function f is *separable* if there exist numerical functions g, h such that $f(p^\alpha) \equiv g(x)\,h(y)$. For example, ϕ_k is separable; σ_k, where $\sigma_k(n)$ is the sum of the kth powers of all the divisors of n, is not.

If f is separable, say $f(p^\alpha) \equiv g(x)\,h(y)$, and if further $h(y)$ is of the form $\sum_{i=1}^{s} (a_i y^i + b_i y^{-i})$, where the a_i, b_i are constants and $a_s b_s \neq 0$, we say that f is *simply* separable of *extent* s. Thus ϕ_k is simply separable of extent 1. *Regarding $f(p^\alpha)$ as a function of x and y, we shall write $f(p^\alpha) \equiv f(x, y)$.*

It is well known that ϕ_k is the unique solution f of the functional equation

$$\sum_{d|n} f(d) = n^k, \qquad (n = 1, 2, \cdots). \tag{2}$$

Although a proof of this will not be required, we give one to contrast the algebra involved with another, which will be used.

* Presented to the Society, November 29, 1930.

Write $u_r(n) \equiv n^r$ for all integers $n > 0$. Then* (2) is $u_0 f = u_k$, which is linear in f and hence has the unique solution $f = u_k u_0^{-1} = u_k \mu$ ($\mu \equiv$ Möbius' function). Hence, by (1), $f = \phi_k$ is the unique solution of (2).

When k is a positive rational integer, (2) can be obtained at once from the arithmetical definition of $\phi_k(n)$, and in fact one of the usual ways of deriving the properties of Euler's $\phi(n)$ ($k = 1$) is by first proving (2) directly from the definition of $\phi(n)$. Another functional equation for ϕ_k, stated in (3), of which ϕ_k is again the unique solution, conceals some more recondite arithmetical property of totients. In itself it is remarkable enough to merit independent notice. It also gives an example in a new algebra, devised by D. H. Lehmer, which is isomorphic with common algebra (the theory of an abstract infinite field), and which reveals interesting new aspects of numerical functions radically different from those depending ultimately upon Dirichlet multiplication, as was the case with the algebra cited in the preceding footnote. In this algebra, since it is isomorphic with a field, multiplication has a unique inverse and a unique identity element; multiplication and division are the operations of greatest arithmetical interest. Applied to simply separable functions the new multiplication gives the second characteristic equation (3) for ϕ_k. A third characteristic equation is given in §3.

All that will be required of Lehmer's algebra is the definition of multiplication. Let m, n, r be positive integers. The number of sets (m, n) such that the L. C. M. of m, n has the constant value r is finite. Let f, g be numerical functions, and let the summation refer to all of the pairs (m, n) just defined. Then $\sum f(m)g(n)$ is a numerical function of r, say $h(r)$, and

$$\sum f(m)g(n) = h(r), \qquad (r = 1, 2, \cdots),$$

is written $(fg) = h$, which defines the *product* (fg). As stated, the multiplication (fg) is associative and commutative, and has a unique inverse. The last implies that if f is any numerical function other than the identically zero function, there exists

* For the algebra (symbolic method) used, see *Outline of a theory*, etc., Journal Indian Mathematical Society, vol. 17 (1928), where references to previous papers are given. If f, g are numerical functions, $f = g$ means that $f(n) = g(n)$, $(n = 1, 2, \cdots)$.

a *unique* numerical function u (the same for all f) such that $(fg)=u$ has a unique solution g.

We write $(ff)\equiv(f^2)$, $(f^2)(n)\equiv f^2(n)$. If f is separable, say $f(p^\alpha)\equiv f(x, y)\equiv g(x)\,h(y)$, and if $n=p_1^{\alpha_1}\cdots p_a^{\alpha_a}$, where $p_1, \cdots, p_a$ are distinct primes, then

$$f(n) = f(p_1^{\alpha_1})\cdots f(p_a^{\alpha_a}) \equiv g(x_1)\cdots g(x_a)h(y_1)\cdots h(y_a),$$

where $x_j\equiv p_j$, $y_j\equiv p_j^{\alpha_j}$. Hence it is sufficient to discuss the equation $f(x, y)=g(x)\,h(y)$.

If f is separable, f^2 in general is not separable. In §2 we determine all simply separable f such that f^2 is separable. The problem of determining *all* separable f (not merely *simply* separable f) such that f^2 is separable, leads to a functional equation which appears to be quite intractable. When f is simply separable and f^2 is separable, we shall see that f^2 also is simply separable.

If both f, f^2 are separable, say

$$f(x, y) \equiv g(x)h(y),\quad f^2(x, y) \equiv G(x)H(y),$$

then also (k is any complex number $\neq 0$),

$$f(x^k, y^k) \equiv g(x^k)h(y^k),\quad f^2(x^k, y^k) \equiv G(x^k)H(y^k),$$

and conversely this implies the preceding. It is sufficient therefore to consider the case $k=1$. The second characteristic equation of ϕ_k is given by the next theorem.

THEOREM 1. *The unique simply separable solution $f(x, y)$ of*

$$f^2(x, y) = f(x^2, y^2) \tag{3}$$

is $f=\phi_k$, where k is an arbitrary complex number $\neq 0$.

This theorem, proved in §2, end, originated in an attempt to relate the following astonishing property of $(\phi_k\phi_l)$ to Jordan's original definition when k, l are positive integers: if k, l are any complex numbers other than zero, $(\phi_k\phi_l)=\phi_{k+l}$. This is due to von Sterneck.* It is shown in §3 that this property gives a third functional equation for totients.

2. *Simply Separable f and f^2.* As in §1, write $p\equiv x$, $p^\alpha\equiv y$ (p

* Monatshefte für Mathematik, vol. 5 (1894), pp. 255–266.

prime, α an arbitrary positive integer), and define $Q, \cdots, T_j$ by

$$Q(y) \equiv \sum_{j=1}^{s}(a_j y^j + b_j y^{-j}), \qquad a_s b_s \neq 0;$$

$$A(x) \equiv \prod_{j=1}^{s}(x^j - 1), \quad A_j(x) \equiv A(x)/(x^j - 1);$$

$$R_j(x) \equiv -b_{s-j}(x^{s-j} + 1)A_{s-j}(x), \quad (j = 0, 1, \cdots, s-1);$$

$$S(x) \equiv A(x) + P(x)\sum_{j=1}^{s}(b_j - a_j x^j)A_j(x);$$

$$T_j(x) \equiv a_j(x^j + 1)A_j(x), \qquad (j = 1, \cdots, s).$$

Then, if the function $f(x, y)$ is simply separable of extent s, and $f(x, y) \equiv P(x)Q(y)$, we have

$$f^2(x, y) = \frac{P(x)Q(y)}{A(x)y^s}\left[P(x)\sum_{j=0}^{s-1}R_j(x)y^j + 2S(x)y^s + P(x)\sum_{j=1}^{s}T_j(x)y^{s+j}\right].$$

For, from the definition of Lehmer's product (hg) in terms of L. C. M., where h, g are any numerical functions,

$$(hg)(p^\alpha) = h(p^\alpha)\left[1 + \sum_{j=1}^{\alpha}g(p^j)\right] + g(p^\alpha)\left[1 + \sum_{j=1}^{\alpha}h(p^j)\right] - h(p^\alpha)g(p^\alpha).$$

In this take $h = g = f$, $f(x, y) \equiv P(x)\,Q(y)$. Then, by a short reduction,

$$f^2(x, y) \equiv P(x)Q(y)\left[2 + P(x)\sum_{j=1}^{s}\{b_j t_j(x, y) + a_j t_j(x^{-1}, y^{-1})\}\right],$$

$$t_j(x, y) \equiv y^{-j}(1 + x^j - 2y^j)/(1 - x^j).$$

Reducing this to a common denominator we find the form stated.

In order that $f^2(x, y)$ be separable it is therefore necessary and sufficient that

$$P(x)\sum_{j=0}^{s-1}R_j(x)y^j + 2S(x)y^s + P(x)\sum_{j=1}^{s}T_j(x)y^{s+j} \equiv L(x)M(y),$$

identically in x and y, where $L(x)$, $M(y)$ are functions of x and of y alone respectively. The trivial cases where one of $P(x)$, $L(x)$, $M(y)$ is identically zero are excluded. Hence it is necessary and sufficient that

$$P(x)R_j(x) \equiv \alpha_j L(x), \quad (j = 0, \cdots, s-1);$$
$$S(x) \equiv \beta L(x);$$
$$P(x)T_i(x) \equiv \gamma_i L(x), \qquad (i = 1, \cdots, s),$$

where the α, β, γ are constants not all zero. The first and third of these are

$$-b_{s-j}(x^{s-j}+1)A_{s-j}(x)P(x) \equiv \alpha_j L(x), \quad (j = 0, \cdots, s-1);$$
$$a_i(x^i+1)A_i(x)P(x) \equiv \gamma_i L(x), \qquad (i = 1, \cdots, s).$$

By a simple contradiction it is seen from the first that either all the b's are zero or precisely one is not zero. For, since $j<s$, the first identity gives for some j

$$(x^{s-j}+1)/(x^{s-j}-1) \equiv \delta_j L(x)P(x)/A(x),$$

where δ_j is a constant. If $\delta_j = 0$, $(j=0, \cdots, s-1)$, then $b_{s-j}=0$, $(j=0, \cdots, s-1)$. Suppose next that $\delta_j \neq 0$ when $j=j_1$, $j=j_2$, $j_1 \neq j_2$. Then the corresponding left members can differ only by a constant factor $\delta \neq 0$, and we have

$$(x^{s-j_1}+1)(x^{s-j_2}-1) \equiv \delta(x^{s-j_1}-1)(x^{s-j_2}+1).$$

Now $2s-j_1-j_2 \neq 0$, since $j_1<s$, $j_2<s$. Moreover, $s-j_1 \neq s-j_2$ since $j_1 \neq j_2$; $s-j_1 \neq 2s-j_1-j_2$; $s-j_2 \neq 2s-j_1-j_2$; $(s-j_1)(s-j_2) \neq 0$. Thus we may equate coefficients and get $\delta=1$; whence $x^{s-j_1}=x^{s-j_2}$, and we have the contradiction $j_1=j_2$.

Similarly for the second identity and the a's. There are thus four possibilities, of which one is trivial; the remaining three are as follows.

All b's and α's are zero, and all but one a are zero.

All but one of the b's are zero, and all the a's and γ's are zero.

All but one of the b's and all but one of the a's are zero.

Obviously the first two are identical on a suitable change of notation. We shall consider only the third in detail, as a similar argument shows that the conclusion reached includes the other possibilities as limiting cases.

Let then $b_{s-j}a_i \neq 0$ for a particular j and i. Write $-b_{s-j} \equiv c_{s-j}$.

Then from the two identities we have, on comparing the values which they give for $P(x)$,

$$\alpha_j a_i(x^{s-j+i} + x^{s-j} - x^i - 1) \equiv \gamma_i c_{s-j}(x^{s-j+i} - x^{s-j} + x^i - 1).$$

Now $0 \leqq j < s$, $0 < i \leqq s$. Hence $i(s-j)(s-j+i) \neq 0$, and therefore the apparent constant terms in the above are the actual constant terms, so that $\alpha_j a_i = \gamma_i c_{s-j}$. It follows thence from the last identity that $s-j=i$.

To find $L(x)$ and hence $P(x)$ apply this conclusion to $S(x)$. We find thus

$$L(x) \equiv \frac{A(x)(x^i+1)}{x^i(\beta+\gamma_i)+(\beta+\alpha_j)},$$

$$P(x) \equiv \frac{\gamma_i(x^i-1)}{a_i[x^i(\beta+\gamma_i)+(\beta+\alpha_j)]}.$$

Combining all results we have the following result.

THEOREM 2. *The unique simply separable $f(x, y)$ such that $f^2(x, y)$ is separable, is*

$$f(x, y) \equiv \frac{x^r-1}{(a+b)x^r+(b+c)}(ay^r - cy^{-r}),$$

where r is an arbitrary constant integer $\neq 0$, and a, b, c are constants not all zero; $f^2(x, y)$ is also simply separable,

$$f^2(x, y) \equiv \frac{x^{2r}-1}{[(a+b)x^r+(b+c)]^2}(ay^r - cy^{-r})(ay^r + 2b + cy^{-r}).$$

If the further condition (3) be imposed we find immediately Theorem 1.

3. *Third Functional Equation for ϕ_k.* Let t, k, l be constants, $tkl \neq 0$. With x, y as in preceding sections, let f be a numerical function and define the numerical functions $f_k, f_{k,l}$ by

$$f_k(x, y) \equiv y^k f(x^k), \quad (f_k f_l) \equiv f_{k,l}.$$

Then by a shorter argument similar to that of §2, we find the following theorem.

THEOREM. *If $f_{k,l}(x, y) = y^t F(x^t)$, then necessarily $t = k+l$, $F = f$ and $f(x) = 1 - x^{-r}$, where r is an arbitrary constant $\neq 0$. Hence $f_k = \phi_k$ is the unique solution of the functional equation.*

CALIFORNIA INSTITUTE OF TECHNOLOGY