A FUNCTIONAL EQUATION IN ARITHMETIC*

BY

E. T. BELL

1. Possible theories of arithmetical composition. The functional equation to be discussed is that of associativity,

$$\phi(x, \phi(y, z)) = \phi(\phi(x, y), z),$$

which occurs in all theories of numerical functions hitherto considered. The two most highly developed theories of this kind are those in which multiplication in the ring of all numerical functions is abstractly identical with C (Cauchy) or D (Dirichlet) multiplication of infinite series.†

Lehmer's five postulates are sufficient for the development of a theory of inversion as exemplified in the cases of C, D multiplication, without requiring, as is the fact in those cases, that the function $\phi(x, y)$ (his $\psi(x, y)$) of composition be a polynomial. For C multiplication, $\phi(x, y) \equiv x+y-1$, instead of the usual $x+y$, as a change in notation justifies; for D multiplication, $\phi(x, y) \equiv xy$.

But these are not the only $\phi(x, y)$ which give an arithmetical theory of composition (as in the papers cited); to mention only three further instances, there is von Sterneck's "L.C.M. calculus," quoted by Lehmer, in addition to the well known compositions $\phi(x, y) \equiv M(x, y)$, where M is either "max" or "min."

It is of considerable interest then to see precisely what position is occupied in the general theory of composition developed in the paper (B) by the classical theories in which multiplication is abstractly identical with either C or D. We shall prove that *if $\phi(x, y)$ is a polynomial in x, y, then, in order that the composition $\phi(x, y) = n$, where n is an arbitrary constant integer >0 and x, y are variable integers >0, shall lead to an arithmetical theory of composition, it is necessary and sufficient that $\phi(x, y)$ be either $x+y-1$ or xy, namely, that multiplication in the ring of all numerical functions be either C or D.*

* Presented to the Society, November 30, 1935; received by the editors October 29, 1935.

† See the following papers in vol. 33 (1931) of these Transactions, where further references (especially in (A), (B)) are given.

(A) R. Vaidyanathaswamy, *The theory of multiplicative numerical functions*, pp. 579–662.

(B) E. T. Bell, *Arithmetical composition and inversion of functions over classes*, pp. 897–933.

(C) D. H. Lehmer, *Arithmetic of double series*, pp. 945–957.

The essential points for the arithmetical theory are the existence of a "unit function" and "inverses." Lehmer gives a postulational treatment.

2. **Associativity.** Although only I, III, IV of Lehmer's five postulates are required when $\phi(x, y)$ is a polynomial, we shall give the full set to indicate the content of the theory. For the purposes of the arithmetical theory it suffices to restrict $x, y, z, \cdots, n, \cdots$ to be integers >0; when this is not assumed, $x, y, z, \cdots$ are arbitrary elements of a field. Lehmer's postulates are as follows.

POSTULATE I. *For each integer $n>0$, $\phi(x, y)=n$ has only a finite number of integer solutions (x, y), $x>0$, $y>0$.*

POSTULATE II. *For all integers $x, y>0$, $\phi(x, y)=\phi(y, x)$.*

POSTULATE III. *For all integers $x, y, z>0$, $\phi(x, \phi(y, z))=\phi(\phi(x, y), z)$.*

POSTULATE IV. *If n, x are integers >0, $\phi(x, 1)=n$ implies $x=n$.*

POSTULATE V. *If n is an integer >0, and $d(n)$ denotes the greatest value >0 of x (or of y) for which $\phi(x, y)=n$, then, for each integer $m>0$, the equation $d(n)=m$ has a unique solution n, and $d(1)=1$.*

Having obtained the general polynomial solution of the functional equation in Postulate III in which, first, x, y, z are complex numbers, we shall then show that when x, y, z are restricted to be integers >0, Postulate II is superfluous (for polynomial solutions) when Postulate I is assumed, and that Postulate IV then suffices to isolate either Cauchy or Dirichlet multiplication as the composition $\phi(x, y)$, so that, in the case of $\phi(x, y)$ a polynomial, Postulate V is superfluous. We shall prove first

THEOREM 1. *The only polynomial solutions of*

$$\phi(x, \phi(y, z)) = \phi(\phi(x, y), z) \tag{1}$$

in the domain of complex numbers are the unsymmetric solutions*

$$\phi(x, y) \equiv x, \qquad \phi(x, y) \equiv y, \tag{2}$$

and the symmetric solution

$$\phi(x, y) \equiv a + b(x + y) + cxy, \tag{3}$$

in which a, b, c are any constants such that

$$b^2 - b - ac = 0. \tag{4}$$

Note that Postulate I, which is necessary for the arithmetical theory, excludes the solutions (2), also the solution $\phi(x, y)\equiv a$, included in (3), which appears in (7) below as one of two possibilities consequent on the assumption that $\phi(x, y)$ is a polynomial.

* This can be extended to any domain of integrity. For the interpretation of the solutions (2), see Lehmer, loc. cit., p. 946.

Let $\phi(x, y)$ be a polynomial of degree $r \geqq 0$ in the complex variables x, y with constant term c. Then we may take

$$\phi(x, 0) \equiv c + a_1x + \cdots + a_rx^r, \qquad \phi(0, y) \equiv c + b_1y + \cdots + b_ry^r. \tag{5}$$

In (1) take $x=y=0$. Then

$$\phi(0, \phi(0, z)) \equiv \phi(c, z), \tag{6}$$

identically in z. By (5) the right of (6) is of degree r in z; the left is of degree r^2, and the coefficient of z^{r^2} is b_r^{r+1}. Hence, unless $r^2 \leqq r$, it follows that $b_r=0$. But $r^2<r$ is impossible, r being an integer $\geqq 0$. Thus $r=0$ or 1. Hence either

$$\phi(x, y) \equiv c, \tag{7}$$

where c is an arbitrary constant, or

$$\phi(x, y) \equiv a + bx + ky + pxy, \tag{8}$$

where the constants a, b, k, p are to be conditioned so that this $\phi(x, y)$ satisfies (1). A short reduction of the result of substituting $\phi(x, y)$ as in (8) into (1) gives (4) as a necessary and sufficient condition that (8) be a solution of (1).

COROLLARY. *If $\phi(x, y)$ is a polynomial in x, y, Postulates* I, III *imply Postulate* II.

3. **Exclusion of all but C, D multiplication.** Everything will be proved as stated for polynomial composition $\phi(x, y)$ satisfying Postulates I–V when we prove

THEOREM 2. *The only $\phi(x, y)$ as in* (3), (4) *satisfying Postulate* IV *are*

$$\phi(x, y) \equiv \dot{x} + y - 1, \qquad \phi(x, y) \equiv xy. \tag{9}$$

For Postulate I rejected the solutions (2); the Corollary in §2 rendered Postulate II superfluous when $\phi(x, y)$ is a polynomial; and if either of (9) holds, Postulate V is automatically satisfied.

To prove Theorem 2, we note that if, in accordance with Postulate IV, $\phi(x, y)$ as in (3) satisfies the condition that $\phi(x, 1)=n$ implies $x=n$ for all integers $n>0$, then

$$a + b = n(1 - b - c),$$

for all integers $n>0$, and hence $a+b=0$, $b+c=1$. (Otherwise: take $n=1, 2, 3$, and get the same conditions.) Thus $a=-b$, $c=1-b$, and these values of a, c satisfy (4). Hence

$$\phi(x, y) \equiv - b + b(x + y) + (1 - b)xy, \tag{10}$$

in which the constant b is to be determined. By the definition of composition and the postulates, $\phi(x, y)$ is to be an integer >0 for all integers $x, y>0$. The condition is satisfied if $b=0$ or 1, giving

$$\phi(x, y) \equiv x + y - 1, \qquad \phi(x, y) \equiv xy. \tag{11}$$

To see that no solutions other than (11) are possible, let $b=1+h$, $h>0$. Then, from (10),

$$\phi(x, y) \equiv (1 + h)(x + y - 1) - hxy,$$

which is negative $(h=1)$ if $xy>2(x+y-1)$. This inequality is obviously satisfied for an infinity of pairs of integers $x, y>0$.

California Institute of Technology,
Pasadena, Calif.