ON TWO THEOREMS OF P. ERDÖS AND A. RÉNYI

To Hans Rademacher for his birthday, April 3, 1962

BY

I. J. SCHOENBERG

Both theorems deal with additive arithmetic functions, and new proofs will be given in these pages.

1. The theorem of Erdös

In his paper [1], P. Erdös derives a number of results on additive functions from among which we single out two theorems [1, Theorem XI, page 17, and Theorem XIII, page 18] which may be stated as follows:

Let the real-valued $f(n)$ $(n = 1, 2, \cdots)$ *be such that*

$$f(mn) = f(m) + f(n) \quad \textit{whenever} \quad (m, n) = 1. \tag{1}$$

I. *If*

$$f(n + 1) \geqq f(n) \qquad (n = 1, 2, \cdots), \tag{2}$$

then

$$f(n) = C \log n \qquad (C \textit{ constant}). \tag{3}$$

II. *If*

$$\lim_{n\to\infty} (f(n + 1) - f(n)) = 0, \tag{4}$$

then again $f(n)$ *is of the form* (3).

Each of these two theorems gives a remarkable characterization of the logarithmic function $f(n) = \log n$ (up to a multiplicative constant corresponding to the arbitrary choice of the base) in terms of the weak additive property (1) and an additional condition, (2) or (4). In a recent note [6] A. Rényi gave a simple direct proof of the second theorem. We wish to do here the same for the first theorem. As a matter of fact the first theorem was rediscovered by Lambek and Moser in [4] with a short and ingenious proof. Our proof is somewhat longer and may be described as analytic in the sense that it reduces the problem to Cauchy's functional equation for continuous variables.

It suffices to establish the proposition, that (1) and (2) imply (3), for the case when the inequality (2) is replaced by the stronger condition

$$f(n + 1) > f(n) \qquad (n = 1, 2, \cdots). \tag{5}$$

For if this is already settled, and if now only (2) is assumed, then

Received December 23, 1960.

$f(n) + \delta \log n$ $(\delta > 0)$ satisfies (5); hence $f(n) + \delta \log n = C \log n$, and the general theorem is established.

We begin by extending our function to all positive rationals by the definition

$$(6) \qquad f(m/n) = f(m) - f(n) \quad \text{if} \quad (m, n) = 1.$$

We shall say that the two reduced fractions $x = m/n$ and $x' = m'/n'$ are *relatively prime* provided that

$$(7) \qquad (m, m') = (m, n') = (n, m') = (n, n') = 1,$$

and will describe this symbolically by writing

$$(x, x') = 1.$$

1. *If* $(x, x') = 1$, *then* $f(xx') = f(x) + f(x')$.

Indeed, by definition (6) and our assumptions (7) and (1) we have

$$f(x) + f(x') = f(m) - f(n) + f(m') - f(n')$$
$$= f(mm') - f(nn') = f(mm'/nn') = f(xx').$$

2. *If* $(x, x') = 1$ *and* $x < x'$, *then* $f(x) < f(x')$.

Indeed, $mn' < nm'$, $f(mn') < f(nm')$, $f(m) + f(n') < f(n) + f(m')$, and finally $f(m) - f(n) < f(m') - f(n')$, which proves the assertion in view of (6).

Our objective is to remove the assumption $(x, x') = 1$ from the statements 1 and 2. We begin by proving

3. *If* $x < x'$, *then* $f(x) < f(x')$.

It suffices to select a rational X having the properties

$$(8) \qquad (x, X) = 1, \qquad (x', X) = 1, \qquad x < X < x',$$

since now 2 gives $f(x) < f(X)$, $f(X) < f(x')$; hence $f(x) < f(x')$. Let us now exhibit a rational $X = M/N$ having the properties (8); M' and N' being natural integers, we choose

$$X = \frac{M'mm'nn' + 1}{N'mm'nn' + 1} = \frac{M}{N}, \qquad \text{where } (M, N) = 1.$$

This rational is relatively prime to $x = m/n$ and also to $x' = m'/n'$ and will moreover satisfy the inequalities in (8) for appropriate large values of M' and N'.

Thus $f(x)$ is defined for all positive rationals and is an increasing function of x. For any positive rational x we may therefore define

$$(9) \qquad \rho_x = \lim_{x' \to x-0} f(x'), \qquad \sigma_x = \lim_{x' \to x+0} f(x'),$$

and certainly $\rho_x \leqq \sigma_x$.

4. $\rho_x = f(x) + \rho_1, \quad \sigma_x = f(x) + \sigma_1.$

Let us first observe that in any left (or right) neighborhood of the rational $x = m/n$ there are rationals $x' = m'/n'$ relatively prime to x. For instance

$$x' = \frac{Mmn + 1}{Nmn + 1} = \frac{m'}{n'}, \qquad (m', n') = 1,$$

will do for appropriate M and N. It is also clear that the limits defined by (9) are not changed if we restrict the variable rational x' to be relatively prime to x. For such x' satisfying $(x, x') = 1$ we have

$$f(x') + f(1/x) = f(x'/x). \tag{10}$$

From $f(x) = f(m) - f(n)$ and $f(1/x) = f(n) - f(m)$ we conclude that $0 = f(x) + f(1/x)$, and adding this to (10) we obtain

$$f(x') = f(x) + f(x'/x). \tag{11}$$

If we assume moreover that $x' < x$ and let $x' \to x$, then $x'/x \to 1 - 0$, and (11) gives the first relation $\rho_x = f(x) + \rho_1$ to be established. Assuming $x' > x$ we likewise obtain the second.

5. $\rho_1 = \sigma_1$.

Indeed, from 4 we obtain

$$f(x + 0) - f(x - 0) = \sigma_x - \rho_x = \sigma_1 - \rho_1, \tag{12}$$

for every positive rational x. If we pick n rationals x_i such that $1 < x_1 < \cdots < x_n < 2$, then the monotonicity of $f(x)$ and (12) show that

$$\sum (f(x_i + 0) - f(x_i - 0)) = n(\sigma_1 - \rho_1) < f(2) - f(1) = f(2).$$

Thus $0 \leqq \sigma_1 - \rho_1 < f(2)/n$, and letting $n \to \infty$ we obtain our result.

6. *For a given $\eta > 0$, $f(x)$ is uniformly continuous over the rationals $x \geqq \eta$.*

Indeed, by (11) and the continuity of $f(x)$ at $x = 1$ we know that to $\varepsilon > 0$ corresponds a $\delta_1 > 0$ such that

$$f(r) < \varepsilon \quad \text{if} \quad 0 < r - 1 < \delta_1. \tag{13}$$

Choose δ such that $0 < \delta/\eta < \delta_1$, and let us assume that

$$\eta \leqq x < x' < x + \delta. \tag{14}$$

Choose a rational x'' such that $x' < x'' < x + \delta$ and $(x, x'') = 1$. But then $1 < x''/x < 1 + \delta/x \leqq 1 + \delta/\eta < 1 + \delta_1$; hence $0 < x''/x - 1 < \delta_1$. Now (11), (13), and the monotonicity of $f(x)$ show that $f(x') - f(x) < f(x'') - f(x) = f(x''/x) < \varepsilon$, so that

$$f(x') - f(x) < \varepsilon. \tag{15}$$

Thus (14) implies (15), which establishes our statement.

A proof of Erdös's theorem now follows readily. Indeed, by 5 and (12) we see that $f(x)$ is continuous over the positive rationals. On the other hand we know from 1 that

$$f(yy') = f(y) + f(y') \quad \text{if} \quad (y, y') = 1. \tag{16}$$

If x and x' is *any* given pair of positive rationals, we can find a pair y, y' with $(y, y') = 1$ such that y is as close to x, and also y' as close to x', as we wish. Indeed, the rational y may be chosen close to x at will, and then we can find y', prime to y and close to x'. For these rationals (16) holds. If we now let $y \to x$ and $y' \to x'$, then (16) goes over by continuity into

$$f(xx') = f(x) + f(x').$$

The function $f(x)$ is therefore unrestrictedly additive over the positive rationals. Because of the *uniform* continuity asserted by 6 we can now extend the definition of $f(x)$ to all positive reals preserving the continuity and the additive property. Setting $f(e^t) = g(t)$ we see that the continuous $g(t)$ satisfies Cauchy's functional equation

$$g(t + t') = g(t) + g(t').$$

We conclude that $g(t) = Ct$ $(C > 0)$. Thus $f(e^t) = Ct, f(x) = C \log x$, and in particular $f(n) = C \log n$.

2. The theorem of Rényi

For every natural integer n having the standard representation

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$$

we define an additive function $f(n)$ by setting

$$f(n) = (\alpha_1 + \alpha_2 + \cdots + \alpha_s) - s. \tag{17}$$

Rényi's theorem is as follows:

The densities

$$D\{f(n) = k\} = d_k \qquad (k = 0, 1, 2, \cdots) \tag{18}$$

exist. Moreover the power series

$$F(z) = \sum_0^\infty d_k z^k \tag{19}$$

converges in the circle $|z| < 2$ *and defines a meromorphic function* $F(z)$ *which admits in the finite plane the representation*

$$F(z) = \prod_p \left\{\left(1 - \frac{1}{p}\right)\left(1 + \frac{1}{p-z}\right)\right\}. \tag{20}$$

Proofs are due to Rényi [5] and Kac [2] (see also [3, Chap. 4, §3]). We give here a third proof of this interesting result.

As early as 1936 the writer established in [7] the following theorem:

Let $f(n)$ be an additive function, i.e., satisfying (1), *such that the infinite series*

$$\sum_p (1/p) \min (1, |f(p)|) \tag{21}$$

converges. Then $f(n)$ has an asymptotic distribution function

$$\sigma(x) = D\{f(n) \leqq x\} \qquad (-\infty < x < \infty), \tag{22}$$

having the characteristic function

$$\int_{-\infty}^{\infty} e^{itx}\, d\sigma(x) = \prod_p \left\{\left(1 - \frac{1}{p}\right)\left(1 + \frac{1}{p} e^{itf(p)} + \frac{1}{p^2} e^{itf(p^2)} + \cdots\right)\right\} \tag{23}$$

where the infinite product converges absolutely and uniformly in every finite t-interval.

In [7] can be found a number of applications of this theorem, in particular to functions having discrete distributions. However, Rényi's additive function $f(n)$, defined by (17), provides its most interesting application of this kind and the one which comes out most naturally. Indeed, since (17) implies $f(p) = 0$, the condition (21) is satisfied. Therefore the densities (18) exist, and $\sum d_k = 1$, the distribution function $\sigma(x)$, defined by (22), being a step-function having a jump of d_k at the point $x = k$. Since $f(p^n) = n - 1$ if $n \geqq 1$, (23) becomes

$$\int_{-\infty}^{\infty} e^{itx}\, d\sigma(x) = \prod_p \left\{\left(1 - \frac{1}{p}\right)\left(1 + \frac{1}{p} + \frac{1}{p^2} e^{it} + \frac{1}{p^3} e^{2it} + \cdots\right)\right\}. \tag{24}$$

If we set $z = e^{it}$, the integral on the left reduces to the power series (19), while the right side becomes the right side of (20). The representation (20) is easily shown to be valid in the finite plane and to define a meromorphic function $F(z)$ having the simple poles $z = p$ $(p \neq 3)$ and the simple zeros $z = p + 1$ $(p \neq 2)$. The power series (19) converges uniformly on $|z| = 1$ and agrees on this circumference with $F(z)$, because of (24). Since $F(z)$ is regular in $|z| < 2$, the theorem of Rényi follows as stated.

References

1. P. Erdös, *On the distribution function of additive functions*, Ann. of Math. (2), vol. 47 (1946), pp. 1–20.
2. M. Kac, *A remark on the preceding paper by A. Rényi*, Acad. Serbe Sci. Publ. Inst. Math., vol. 8 (1955), pp. 163–165.
3. ———, *Statistical independence in probability, analysis and number theory*, Carus Monograph no. 12, New York, 1959.
4. L. Moser and J. Lambek, *On monotone multiplicative functions*, Proc. Amer. Math. Soc., vol. 4 (1953), pp. 544–545.
5. A. Rényi, *On the density of certain sequences of integers*, Acad. Serbe Sci. Publ. Inst. Math., vol. 8 (1955), pp. 157–162.

6. ———, *On a theorem of P. Erdös and its application in information theory*, Mathematica (Cluj), vol. 1 (24) (1959), pp. 341–344.

7. I. J. SCHOENBERG, *On asymptotic distributions of arithmetical functions*, Trans. Amer. Math. Soc., vol. 39 (1936), pp. 315–330.

THE UNIVERSITY OF PENNSYLVANIA
PHILADELPHIA, PENNSYLVANIA