ERDŐS THEOREMS ON THE CHARACTERIZATION OF THE LOGARITHM

Notes for NUT classes November 26 & 27

An arithmetical function f is called *additive*, if the functional equation

$$(1) \qquad f(nm) = f(n) + f(m) \qquad (\forall n, m \in \mathbb{N},\ (n,m) = 1)\ )$$

holds true. Moreover, if this is valid for all m and n, then f is called *completely* or *totally* additive.

Theorem 1 (Erdős) . *Suppose that the arithmetical function f is additive and monotone. Then $f(n) = c \log n$ with some constant c.*

Proof. Since f is additive, $f(1) = 0$. Now either f, or $-f$ is non-decreasing, hence without loss of generality we may assume that f is non-decreasing and hence also $f \geq 0$. Consider the case when there exists any integer $n \geq 2$ with $f(n) = 0$. Monotonicity implies $f(1) = f(2) = \cdots = f(n) = 0$, hence at least $f(2) = 0$. Moreover, let $f(3) = a$. Then by additivity $f(6) = f(3) + f(2) = a + 0 = a$, hence $f(3) = f(4) = f(5) = f(6) = a$ by monotonicity; and the same way we can prove that f is constant a from $k_1 := 5$ to $2k_1 = 10$, ... , from $2k_{m+1} = 2k_m - 1$ to $2k_{m+1}$, etc. So by induction we obtain $f(n) = a$ for all $n \geq 3$. But then the additive equation $a = f(15) = f(3) + f(5) = a + a = 2a$ proves $a = 0$, that is, $f \equiv 0$ and the assertion holds with $c := 0$.

Now assume that $f \neq 0$. First we prove the assertion for the special case when f is completely additive, too. Denote $c := f(2)/\log 2$, and choose any $k > 2$. For any (large) n there is a unique m so that $k^m \leq 2^n < k^{m+1}$. In view of monotonicity and total additivity, $mf(k) \leq nf(2) \leq (m+1)f(k)$, that is, since $f > 0$,

$$\frac{m}{n} \leq \frac{f(2)}{f(k)} < \frac{m+1}{n}.$$

However, also the logarithm function is completely additive and increasing, hence the same is valid for $\log n$, too. Comparing these two estimates we are led to

$$\left|\frac{f(2)}{f(k)} - \frac{\log 2}{logk}\right| \leq \frac{1}{n},$$

and, since n can be arbitrarily large, we conclude that $f(2)/f(k) = \log 2/\log k$, that is,

$$f(k) = \frac{f(2)}{\log 2}\log k = c\log k,$$

as needed.

Turning to the general case, first we deduce $f(n) = o(n)$. Consider now the sequence $a_0 = 2, a_1 = 5, a_2 = 14, ..., a_k = 3^{k+1} - 3^k - ... - 1 = (3^k + 1)/2$. Using again both monotonicity and additivity we get

$$f(a_k) \leq f(a_{k+1} = f(3(3^k + 1)/2) = f(3) + f(a_{k-1}),$$

and repeating this estimation procedure k times yields

$$f(a_k) \leq kf(3) + f(2) \leq (k+1)f(3). \tag{2}$$

Since $a_k \to \infty$ strictly increasingly, every integer n lies in a unique interval $[a_k, a_{k+1})$. In fact, this occurs exactly when $3^{k+1}/2 < n < 3^{k+2}/2$. Thus monotonicity and (2) entail

$$\frac{f(n)}{n} < \frac{f(a_{k+1})}{3^{k+1}/2} \leq \frac{2(k+2)}{3^{k+1}}f(3)\,,$$

and, as the right hand side tends to 0, we obtain $f(n) = o(n)$.

Next we show

$$a := \liminf_{n\to\infty} f(n+1) - f(n) = 0, \tag{3}$$

and, moreover, that for any given $m \in \mathbb{N}$ and $\epsilon > 0$ there exists $n \in \mathbb{N}$ so that $(n, m) = 1$ and

$$f(n+m) - f(n) < \epsilon \tag{4}$$

This can be obtained by simple averaging. For let

$$\mu := \mu_m(N) := \min\{ f(n+m) - f(n) \,:\, 1 \le n \le N,\, (n,m)=1\}.$$

Then we obviously have

$$\mu\varphi(m)\left[\frac{N}{m}\right] \le \sum_{\substack{n=1\\(n,m)=1}}^{N} \mu \le \sum_{\substack{n=1\\(n,m)=1}}^{N} f(n+m) - f(n) \le \sum_{n=1}^{N} f(n+m) - f(n)$$

$$= f(N+m) + \cdots + f(N+1) - f(m) \cdots - f(1) < mf(N+m),$$

and thus

$$\mu \le \frac{m}{\varphi(m)} \frac{N+m}{[N/m]} \frac{f(N+m)}{N+m}.$$

Let now $N \ge 3m$ be a large integer. We obtain

$$\mu(N) \le \frac{m^2}{\varphi(m)} \frac{N+m}{N-m} \frac{f(N+m)}{N+m} \le \frac{2m^2}{\varphi(m)} \frac{f(N+m)}{N+m}.$$

In view of $f(n) = o(n)$, the right hand side will be $< \epsilon$ for N sufficiently large. Hence also $\mu_m(N)$ is less than ϵ for N sufficiently large, and (4) follows.

Finally we show that f is necessarily totally additive. Choose now any integer $m \ge 2$ and let $k \ge 1$ be arbitrary. We want to prove

$$f(m^{k+1}) = f(m^k) + f(m). \tag{5}$$

Let now n be any natural number coprime to m. In view of (1)

$$f(nm^{k+1}) = f(m^{k+1}) + f(n). \tag{6}$$

Now since $(n,m)=1$, we also have $(n \pm m, m) = (n,m) = 1$ and $(mn \pm 1, m) = 1$ and so by (1) and monotonicity we infer

$$f(nm^{k+1}) \le f(m^k(nm+1)) = f(m^k) + f(mn+1) \tag{7}$$

$$\le f(m^k) + f(nm+m^2) = f(m^k) + f(m) + f(n+m),$$

and similarly

$$f(nm^{k+1}) \ge f(m^k(nm-11)) = f(m^k) + f(mn-1) \tag{8}$$

$$\ge f(m^k) + f(nm-m^2) = f(m^k) + f(m) + f(n-m).$$

On combining (6), (7) and (8) we obtain

$$\left|f(m^{k+1}) - f(m^k) - f(m)\right| \le f(n+m) - f(n-m). \tag{9}$$

Here we can apply the above (4) (with $2m$ in place of m and $n-m$ in place of n) to get further from (9)

$$\left|f(m^{k+1}) - f(m^k) - f(m)\right| \le \epsilon. \tag{10}$$

Since (10) is valid for arbitrary ϵ, we obtain (5), which, in turn, leads to

$$f(m^k) = kf(m) \qquad (k, m \in \mathbb{N})$$

by simple induction. Application of this for prime powers will imply complete additivity under the condition (1) of ("simple") additivity. Thus the proof is complete.

Comment. There are many proofs of Erdős' Theorem, some of them being even shorter than the above. The nice feature of the topic is that each approach shed light to some new aspects of the question, while ignoring others. That also explains why we know so many extensions and relatives of this simple and fundamental result. One of the most well-known, also due to Erdős, is the following.

Theorem 2 (Erdős) . *Suppose that the arithmetical function f is additive and satisfies $f(n+1) - f(n) \to 0$ $(n \to \infty)$. Then $f(n) = c \log n$ with some constant c.*

The above Theorems 1 and 2 can be proved through a common generalization.

Theorem 3 (Erdős) . *Let the additive arithmetical function f satisfy*

$$\liminf_{n\to\infty} f(n+1) - f(n) \ge 0.$$

Then with some appropriate constant c we have $f(n) = c \log n$.

A GLIMPSE AT PROBABILISTIC NUMBER THEORY

Notes for NUT classes November 26 & 27

The Hardy–Ramanujan theorem can be generalized for many additive functions. A general form of this is the following.

Theorem 4 (Turán – Kubilius) . *Let f be an additive arithmetical function, and let*

$$A := A(f,x) := \sum_{p^k \le x} \frac{f(p^k)}{p^k}(1-\frac{1}{p})$$

be the "average", and

$$D := D(f,x) := \sum_{p^k \le x} \frac{f(p^k)^2}{p^k}$$

be the "dispersion". Then we have

$$S := S(f,x) := \sum_{n \le x} (f(n)-A)^2 \le CxD.$$

This theorem expresses an arithmetical interpretation of Chebyshev's inequality. It can be used to prove upper estimates on the number of integers below x which have f-values deviating at least a certain extent from the average. Eg. the Hardy-Ramanujan Theorem follows immediately.

However, for the particular function $\omega(n)$ (and, in fact, for a large class of additive arithmetical functions) we even have so-called limit distribution theorems. This is a more refined formulation, directly analogous to limit distributions in probability theory. The underlying idea is that independent random variables sum up to a normally distributed random variable, hence the value distribution must have a Gauss density.

Namely, let us choose a large integer x, and consider the interval $[1,x]$ with a uniform probability distribution as our probability space. If we interpret $f(n) \sim \sum_{p|n} f(p)$ as the sum of the "random variables" $X_p(n)$, where $X_p(n)$ is $f(p)$ or 0 according to whether $p|n$ or not, then these random variables are approximately totally independent. That is, any given set of primes have joint probability $P(p_j|n,\ j = 1,\dots,n)$ almost precisely equal to the product of the individual probabilities. Thus the underlying idea is that closely following the standard proof of the central limit theorem, we are to obtain a proof of an analogous value distribution result for our additive arithmetical function.

In the case of $\omega(n)$ that is expressed by the following by now classical result.

Theorem 5 (Erdős – Kac) .

$$N\left(n \leq x : \frac{\omega(n) - \log\log x}{\sqrt{\log\log x}} \leq y\right) \to \Phi(y) := \frac{1}{\sqrt{2\pi}} \int_{-\infty}^{y} e^{-u^2/2} du.$$

Here the left hand side stands for the number of integers up to x satisfying the inside inequality, and $\Phi(y)$ is the standard normal (or Gauss-) distribution.

That means, that below x the values of ω are situated around the average value $\log\log x$ and the density of integers with values deviating only a (large) constant times $\sqrt{\log\log x}$ must have a comparatively small density. Hence eg. it follows that for almost all integers n the value $\omega(n)$ is between $0.99 \log\log x$ and $1.01 \log\log x$. You can try various deviation values like $(\log\log x)^\alpha$ etc. to compare what the Erdős-Kac Theorem and the Hardy-Ramanujan Theorem gives.

One important area of number theory is the use of probabilistic methods and ideas in the analysis of additive and multiplicative functions. From creation to present day research, Hungarian researchers like Paul Erdős, Paul Turán and Gábor Halász have made significant contributions to this area.