

**Average Values of Number-Theoretic Functions**  
**Addendum to a Lecture at UMass, Amherst, 4/26/00**  
**Michael Rosen, Brown University**

In the lecture, it was explained how the notion of statistical independence can be used to evaluate number-theoretic averages. However, time did not allow for the proof, due to Mark Kac, of a beautiful theorem of A. Renyi. The point of the present note is to give an outline of the proof and a more detailed discussion of the consequences.

To begin with we recall a few definitions. Let  $f : \mathbb{Z}^+ \rightarrow \mathbb{R}$  be a real valued function on the positive integers. Define

$$M(f) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N f(n) ,$$

provided that the limit exists.  $M(f)$  is called the average value of  $f$ , or, alternatively, the mean value of  $f$ .

If  $S \subset \mathbb{Z}^+$ , let  $\chi_S(n)$  be the characteristic function of  $S$ . The mean value of  $\chi_S$  is denoted by  $\mu(S)$ . It is interpreted as the probability that a positive integer lies in  $S$ .

There are three main properties associated with the notion of the mean value of a function.

- a) If  $f$  and  $g$  are functions and  $\alpha$  and  $\beta$  are constants, then  $M(\alpha f + \beta g) = \alpha M(f) + \beta M(g)$ .
- b) Let  $k$  run through the possible values of  $f$ . Then,

$$M(f) = \sum_k k \mu(\{n \mid f(n) = k\}) .$$

- c) Suppose  $f$  and  $g$  are independent functions (to be explained below). Then,  $M(fg) = M(f)M(g)$ .

Two functions,  $f$  and  $g$ , are said to be independent if the following condition holds; for all possible values  $k$  of  $f$  and  $l$  of  $g$  we have

$$\mu(\{n \mid f(n) = k \text{ and } g(n) = l\}) = \mu(\{n \mid f(n) = k\}) \times \mu(\{n \mid g(n) = l\}) .$$

From this description, the generalization to finitely many functions is clear, as is the generalization of property c).

For each prime  $p$  define the function  $\epsilon_p(n)$  to be 1 if  $p$  divides  $n$  and 0 otherwise. It is easy to check that if  $q$  is another prime  $\epsilon_p(n)$  and  $\epsilon_q(n)$  are independent. This easily extends to finitely many primes.

We now introduce a few more number-theoretic functions. Let

$$n = p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t} ,$$

be the usual prime decomposition of the integer  $n$ . Define  $\omega(n) = e_1 + e_2 + \dots + e_t$  and  $\nu(n) = t$ .  $\omega(n)$  is the total number of prime divisors of  $n$  (with multiplicities allowed), whereas  $\nu(n)$  is the number of distinct prime divisors of  $n$ . Our task will be to understand as closely as we can the probabilities

$$d_k = \mu(\{n \mid \omega(n) - \nu(n) = k\}) .$$

The number  $d_0$  is just the probability that an integer be square-free. In the earlier part of the lecture this was shown to be  $6/\pi^2$ . It will turn out that all the  $d_k$  are finite and non-zero. We will find a formula for  $d_1$  and give an asymptotic estimate for  $d_k$  when  $k$  is large.

As a first step we note that  $\nu(n) = \sum_p \epsilon_p(n)$ , the sum being over all positive prime numbers. This is clear from the definition. It is desirable to have a similar expression for  $\omega(n)$ . To this end we introduce the function  $\text{ord}_p(n)$ . For each non-negative integer  $k$  we set  $\text{ord}_p(n) = k$  if  $p^k$  divides  $n$  and  $p^{k+1}$  does not divide  $n$ . In other words,  $\text{ord}_p(n) = k$  when  $p^k$  is the highest power of  $p$  dividing  $n$ . It is easy to check that if  $q$  is another prime that  $\text{ord}_p(n)$  and  $\text{ord}_q(n)$  are independent functions and, in fact, this extends to finitely many primes. We also have the following two facts

$$\omega(n) = \sum_p \text{ord}_p(n) \quad \text{and}$$

$$\mu(\{n \mid \text{ord}_p(n) = k\}) = \frac{1}{p^k} - \frac{1}{p^{k+1}} .$$

Our approach to an understanding of the numbers  $d_k$  begins by characterizing them in a new way using the following elementary formula. Let  $m$  be an integer. Then,

$$\frac{1}{2\pi} \int_0^{2\pi} e^{imx} dx = 1 \text{ if } m = 0, \text{ and } 0 \text{ otherwise .}$$

Using this we see that the integral

$$\frac{1}{2\pi} \int_0^{2\pi} \left( \sum_{n=1}^N e^{i(\omega(n) - \nu(n) - k)x} \right) dx ,$$

is the number of integers between 1 and  $N$  such that  $\omega(n) - \nu(n) = k$ . Thus, dividing by  $N$  and passing to the limit as  $N \rightarrow \infty$  we find

$$d_k = \frac{1}{2\pi} \int_0^{2\pi} e^{-ikx} g(x) dx , \tag{1}$$

where

$$g(x) = M(e^{i(\omega(n) - \nu(n))x}) = \lim_{N \rightarrow \infty} \frac{1}{N} \sum_{n=1}^N e^{i(\omega(n) - \nu(n))x} .$$

A number of things here need justification, especially the interchange of taking a limit and integration. All this is not hard to provide, but we shall not do so here. Let's assume it is OK and pass on.

Since  $\omega(n) - \nu(n) = \sum_p \text{ord}_p(n) - \epsilon_p(n)$ , we have

$$e^{i(\omega(n)-\nu(n))x} = \prod_p e^{i(\text{ord}_p(n)-\epsilon_p(n))x} .$$

Since the functions  $\text{ord}_p(n)$  and  $\epsilon_p(n)$  are independent over finite sets of primes, so are the functions

$$e^{i(\text{ord}_p(n)-\epsilon_p(n))x} .$$

We want to evaluate the function  $g(x)$  defined above. To do so we will use property *c*) of mean values. That property, which holds for finitely many independent functions, will be taken to apply to infinitely many "independent" functions. This needs justification and the justification is not so easy (in spite of Kac's statement to the contrary). The interested reader can consult pages 166-168 of his book [2]. It is plausible however, so, in the spirit of Euler (see the fascinating book about Euler [1]), we ignore niceties and calculate

$$g(x) = M(e^{i(\omega(x)-\nu(x))x}) = M\left(\prod_p e^{i(\text{ord}_p(n)-\epsilon_p(n))x}\right) = \prod_p M(e^{i(\text{ord}_p(n)-\epsilon_p(n))x}) .$$

The calculation of the mean value of the function  $e^{i(\text{ord}_p(n)-\epsilon_p(n))x}$  is made possible by property *b*) of mean values. The possible values of this function are  $1, e^{ix}, e^{2ix}, \dots$ . The value 1 is assumed if either  $p$  does not divide  $n$  or if  $p$  divides  $n$  exactly. The probability  $p$  doesn't divide  $n$  is  $1 - \frac{1}{p}$  and that it divides  $n$  exactly is  $\frac{1}{p} - \frac{1}{p^2}$ . If  $k \geq 1$  and  $\text{ord}_p(n) = k$  then the value of the function is  $e^{i(k-1)x}$  and this happens with probability  $\frac{1}{p^k} - \frac{1}{p^{k+1}}$ . Thus,

$$\begin{aligned} M(e^{i(\text{ord}_p(n)-\epsilon_p(n))x}) &= 1 - \frac{1}{p} + \sum_{k=1}^{\infty} e^{i(k-1)x} \left( \frac{1}{p^k} - \frac{1}{p^{k+1}} \right) \\ &= \left(1 - \frac{1}{p}\right) \left(1 + e^{-ix} \sum_{k=1}^{\infty} \frac{e^{ikx}}{p^k}\right) = \left(1 - \frac{1}{p}\right) \left(1 + \frac{1}{p - e^{ix}}\right) . \end{aligned}$$

We have thus derived the following formula for  $g(x)$

$$g(x) = \prod_p \left(1 - \frac{1}{p}\right) \left(1 + \frac{1}{p - e^{ix}}\right) . \quad (2)$$

This product is easily seen to converge uniformly in  $x$  by using the fact that  $\prod_p \left(1 - \frac{1}{p^2}\right)$  is a convergent product. However, even more is true. Define  $f(z)$  by the infinite product

$$f(z) = \prod_p \left(1 - \frac{1}{p}\right) \left(1 + \frac{1}{p - z}\right) . \quad (3)$$

If we draw a little disc around each prime in the complex plane it is easy to see that the product converges uniformly on the complement of the union of the discs. One can then prove that  $f(z)$  is meromorphic on the whole plane and has simple poles precisely at the positive primes. Since the first pole is at  $p = 2$ ,  $f(z)$  can be expressed as a convergent power series in the open disc about the origin of radius 2.

**Theorem.** (A. Renyi) For all complex numbers  $z$  with  $|z| < 2$  we have

$$f(z) = \prod_p \left(1 - \frac{1}{p}\right) \left(1 + \frac{1}{p-z}\right) = \sum_{k=0}^{\infty} d_k z^k .$$

**Proof.** In the power series expansion of  $f(z)$  around the origin, the coefficient of  $z^k$  is given by

$$\frac{1}{2\pi i} \int_C \frac{f(z)}{z^{k+1}} dz .$$

Here,  $C$  is any circle about the origin of radius less than 2. This is just the Cauchy integral formula. Take for  $C$  the unit circle about the origin parametrized by  $e^{ix}$  with  $1 \leq x \leq 2\pi$ . Then this integral reduces to

$$\frac{1}{2\pi} \int_0^{2\pi} e^{-ikx} f(e^{ix}) dx = \frac{1}{2\pi} \int_0^{2\pi} e^{-ikx} g(x) dx = d_k .$$

We have used equations 1), 2), and 3) given above. This completes the proof!

Setting  $z = 0$  we find, once again, that  $d_0$ , the probability that an integer is square-free, is given by  $\prod_p \left(1 - \frac{1}{p^2}\right)$ . Setting  $z = 1$  we derive the equation  $1 = \sum_{k=0}^{\infty} d_k$ . This is not surprising, but since our set function  $\mu$  is not countably additive (give a counter-example) it cannot be said to just follow from general principles.

To evaluate  $d_1$  one has to calculate the coefficient of  $z$  in the infinite product for  $f(x)$ . This was done in the lecture. The answer is

$$d_1 = \frac{6}{\pi^2} \sum_p \frac{1}{p(p+1)} .$$

A more substantial corollary of the theorem is to calculate the asymptotic behavior of  $d_k$  as  $k$  gets large. We will need some basic facts from complex variable theory. The result is

**Corollary.** Let  $A$  denote the convergent product

$$A = \prod_{p \neq 2} \left(1 - \frac{1}{p}\right) \left(1 + \frac{1}{p-2}\right).$$

Then,

$$d_k \sim \frac{A}{2^{k+1}}.$$

More precisely,  $\lim_{k \rightarrow \infty} 2^{k+1} d_k = A$ .

**Proof.** Using the definition of  $f(z)$  given in equation 3) we see that it has a simple pole at  $z = 2$  and that the residue there is  $-A$ . Thus,

$$f(z) + \frac{A}{z-2} \tag{4}$$

is holomorphic in the open disc of radius 3 about the origin. Let  $\sum_{k=0}^{\infty} c_k z^k$  be its power series expansion. Since the lim sup of the sequence  $\{\sqrt[k]{|c_k|}\}$  is  $1/3$  we see that for all but finitely many  $k$  we have  $|c_k| < (\frac{1.1}{3})^k$  (instead of 1.1 we can use any number  $\alpha$  such that  $1 < \alpha < 1.5$ ). If we now use the series expansion

$$\frac{A}{z-2} = - \sum_{k=0}^{\infty} \frac{A}{2^{k+1}} z^k,$$

which is valid for  $|z| < 2$  we see that for all but finitely many  $k$

$$\left| d_k - \frac{A}{2^{k+1}} \right| = |c_k| < \left(\frac{1.1}{3}\right)^k.$$

The conclusion follows immediately from these inequalities.

### Bibliography

1. Dunham, W. *Euler, the Master of Us All*, MAA Publications, 1999.
2. Kac, M. *Statistical Independence in Probability, Analysis, and Number Theory*, Carus Math. Monograph Nu. 9, MAA Publications, 1959.