References

[1] W. Burnside, *On simply transitive groups of prime degree*, Quart. J. Math. 37 (1906), pp. 215–221.
[2] L. R. Ford, *Automorphic Functions*, New York 1951.
[3] M. Fried, *Arithmetical properties of value sets of polynomials (I)*, Acta Arith. 15 (1969), pp. 91–125.
[4] — *On a conjecture of Schur*, Mich. Math. J. 17 (1970), pp. 41–55.
[5] — *The field of definition of function fields and a problem in the reducibility of polynomials in two variables*, Illinois J. Math. 17 (1973), pp. 128–146.
[6] — *On a theorem of Ritt*, to appear in Crelle's J., June 1974.
[7] — *Naive class field theory for local function fields over finite fields*, in preparation.
[8] — *On a theorem of MacCluer*, Acta Arith. 25 (1974), pp. 121–125.
[9] — (with R. E. MacRae), *On the invariance of chains of fields*, Illinois J. Math. 13 (1969), pp. 165–171.
[10] R. Lidl and C. Wells, *Chebychev polynomials in several variables*, Crelle 1972.
[11] J. F. Ritt, *Prime and composite polynomials*, Trans. Amer. Math. Soc. 23 (1922), pp. 51–66.
[12] — *Permutable rational functions*, Trans. Amer. Math. Soc. 25 (1923), pp. 399–448.
[13] — *On algebraic functions which can be expressed in terms of radicals*, Trans. Amer. Math. Soc. 24 (1922).
[14] G. Springer, *Introduction to Riemann Surfaces*, Reading, Mass., 1957.
[15] C. Wells (with the aid of W. Nöbauer), *Bibliography of Literature on Representable Mappings of an Algebraic Structure Into Itself*, Dept. of Math, Case Western Reserve University.

Added in References

[16] M. Fried and D. J. Lewis, *Solution spaces to diophantine problems*, Bull. Amer. Math. Soc., to appear.
[17] M. Fried, *On Hilbert's Irreducibility Theorem*, Journal of Number Theory, to appear June 1973.
[18] S. Cohen, *The distribution of polynomials over finite fields*, Acta Arith. 17 (1970), pp. 259–273.

Received on 12. 6. 1970 (312)

ACTA ARITHMETICA
XXV (1974)

On the limiting distribution of $f(p+1)$ for non-negative additive functions

by

P. D. T. A. Elliott (Boulder, Colo.)

Let $f(n)$ be an additive function. Thus for coprime integers a and b it satisfies the relation $f(ab) = f(a)+f(b)$.

For each set E, and real number $x \geqslant 2$ we define frequencies

$$\nu_x(p;\ p\in E) = \big(\pi(x)\big)^{-1}\sum_{p\leqslant x}{}' 1,$$

where $'$ denotes that summation is restricted to those primes p which belong to the set E, and $\pi(x)$ denotes the total number of primes not exceeding x.

It was proved by Katai [3] that if the three series

$$\sum_{|f(p)|>1}\frac{1}{p},\qquad \sum_{|f(p)|\leqslant 1}\frac{f(p)}{p},\qquad \sum_{|f(p)|\leqslant 1}\frac{f^2(p)}{p}$$

converge, then the frequencies

$$\nu_x\big(p;\ f(p+1)\leqslant z\big)\qquad (x\to\infty),$$

possess a limiting distribution. We here show that if $f(p)\geqslant 0$ holds for every prime p then these conditions are also necessary.

Theorem. *Let $f(n)$ be a non-negative strongly additive function. Then a limiting distribution exists for the frequencies*

$$\nu_x\big(p;\ f(p+1)\leqslant z\big)\qquad (x\to\infty)$$

if and only if the series

$$\sum_{|f(p)|>1}\frac{1}{p},\qquad \sum_{|f(p)|\leqslant 1}\frac{f(p)}{p}$$

converge.

Remarks

(i) Since $f(p) \geqslant 0$ the convergence of the second of these two series implies the convergence of the series

$$\sum_{|f(p)|\leqslant 1} \frac{f^2(p)}{p}.$$

(ii) The conditions of Katai are necessary if f may assume negative values but $f(p)\to 0$ as $p\to\infty$. This could (for example) be proved by modifying the present argument.

(iii) The necessity of similar conditions for non-negative functions when $p+1$ is replaced by $g(n)$ or $g(p)$ for a polynomial g with integral coefficients, can be proved in the manner of the present theorem.

(iv) By operating on the primes for which $p+1$ is squarefree one can prove the theorem under the weaker assumption that f is additive.

An essential rôle in the proof will be played by the following result of Barban, which generalizes an earlier result of Kubilius.

LEMMA 1. (See Barban [1], Lemma 7.4.) *Let $g(x)$ be a polynomial with integer coefficients, $L(p)$ the number of solutions of the congruence* $g(x) \equiv 0 \pmod p$, $K = \prod_{p\leqslant r} p$, $\mathscr{K} \subseteq \{k;\ k\,|\,K\}$, $E(d) = \{g(d);\ d\leqslant x,\ g(d) \equiv 0 \pmod d\}$. *For every* $k\in\mathscr{K}$ *let*

$$Q_k = \bigcap_{p|k} E(p) \cap \bigcap_{\substack{p\nmid k\\ p\leqslant r}} \bar{E}(p) = \{g(p);\ p\leqslant x,\ k\,|\,g(p),\ (g(p), K/k) = 1\}.$$

Then there exists a positive constant c so that

$$\nu_x\Big(p;\ g(p)\in \bigcup_{k\in\mathscr{K}} Q_k\Big) = \sum_{k\in\mathscr{K}} \prod_{p|k} \frac{L(p)}{\varphi(p)} \prod_{p|K/k} \left(1-\frac{L(p)}{\varphi(p)}\right) + O\big(e^{-\frac{c\log x}{\log r}}\big) + O\big((\log x)^{-1}\big)$$

uniformly with respect to $\mathscr{K}$.

We shall need the following consequence of Lemma 1.

LEMMA 2. *Define independent random variables X_p, one for each prime $p\geqslant 2$, by*

$$X_p = \begin{cases} f(p) & \text{with probability } \dfrac{1}{p-1},\\[2mm] 0 & \text{with probability } 1-\dfrac{1}{p-1}.\end{cases}$$

Then there are positive absolute constants c_3 and c_4 so that if ε is a real number in the interval $0<\varepsilon<c_3$, then

$$\nu_x\Big(p;\ \sum_{q|(p+1),\, q\leqslant x^{\varepsilon}} f(q)\leqslant z\Big) = P\Big(\sum_{p\leqslant x^{\varepsilon}} X_p \leqslant z\Big) + O\big(\exp(-c_4\varepsilon^{-1})\big).$$

Proof. In Lemma 1 set $g(x) = x+1$, $r = x^{\varepsilon}$, and $\mathscr{K} = \{k;\ k\,|\,K,\ f(k)\leqslant z\}$. Then $L(p) = 1$ and

$$\nu_x\Big(p;\ p+1\in\bigcup_{k\in\mathscr{K}} Q_k\Big) = \sum_{k\in\mathscr{K}} \prod_{p|k} \frac{1}{p-1} \prod_{p|K/k}\left(1-\frac{1}{p-1}\right) + O(e^{-c/\varepsilon}) + O\big((\log x)^{-1}\big)$$
$$= \sum_{k\in\mathscr{K}} + O(e^{-c_4\varepsilon^{-1}}).$$

Since $f(n)$ is strongly additive

$$\nu_x\Big(p;\ \sum_{q|(p+1),\, q\leqslant r} f(q)\leqslant z\Big) = \nu_x\Big(p;\ p+1\in\bigcup_{k\in\mathscr{K}} Q_k\Big).$$

On the other hand, since the random variables X_p are independent and have a discrete distribution, we have

$$P\Big(\sum_{p\leqslant r} X_p\leqslant z\Big) = \sum_{\substack{x_p = 0 \text{ or } f(p)\\ \sum_{p\leqslant r} x_p\leqslant z}} \prod_{p\leqslant r} P(X_p = x_p) = \sum_{k\in\mathscr{K}} \prod_{p|k}\frac{1}{p-1}\prod_{p|K/k}\left(1-\frac{1}{p-1}\right).$$

This completes the proof of Lemma 2.

Proof of the theorem. We give a proof of the necessity part only, since the proof of sufficiency is included in the result of Katai [3].

Let ε_1 be a real number in the interval $0<\varepsilon_1<1$. Assuming that the function $f(p+1)$ has a limiting distribution we can find a real number z_1 so that for all sufficiently large values of x:

$$\nu_x\big(p;\ f(p-1)\leqslant z_1\big) > 1-\varepsilon_1.$$

Let q_j run through those odd primes q for which $f(q)>z_1$. Then it follows that

$$\nu_x\big(p;\ p\not\equiv -1 \,(\operatorname{mod} q_j)\ \forall j\geqslant 1\big) > 1-\varepsilon_1.$$

We first choose an integer $r\geqslant 1$. A simple application of the sieve of Eratosthenes, together with Dirichlet's theorem on primes in arithmetic progression, shows that the number of primes in the interval $2\leqslant p\leqslant x$ for which $q_j\nmid(p+1)$ $(j = 1,\ldots,r)$, does not exceed

$$\big(1+o(1)\big)\frac{x}{\log x}\prod_{j=1}^{r}\left(1-\frac{1}{q_j-1}\right) \qquad (x\to\infty).$$

By letting first x and then $r\to\infty$ we arrive at the inequality

$$1-\varepsilon_1\leqslant \prod_{j=1}^{\infty}\left(1-\frac{1}{q_j-1}\right)$$

so that the series $\sum (q_j-1)^{-1}$ converges.

Let ε be a further real number in the interval $0<\varepsilon<1$. Then for any positive real numbers y and z set

$$F(y, z) = P\Big(\sum_{p\leqslant y} X_p \leqslant z\Big).$$

Since f is non-negative we have

$$\nu_x\big(p;\, f(p+1)\leqslant z\big) \leqslant \nu_x\Big(p;\, \sum_{q\mid p+1,\, q\leqslant x^\varepsilon} \leqslant z\Big)$$

which by Lemma 2 does not exceed

$$F(x^\varepsilon, z) + O\big(\exp(-c_4\varepsilon^{-1}) + (\log x)^{-1}\big).$$

Let u be a further positive real number, then

$$F(x^\varepsilon, z) \leqslant F(x, z+u) + P\Big(\sum_{x^\varepsilon<p\leqslant x} X_p > u\Big).$$

Define new independent random variables by

$$X'_p = \begin{cases} X_p & \text{if} \quad X_p \leqslant z_1, \\ 0 & \text{if} \quad X_p > z_1. \end{cases}$$

Then

$$P\Big(\sum_{x^\varepsilon<p\leqslant x} X_p > u\Big) \leqslant \sum_{x^\varepsilon<p\leqslant x} P(X_p > z_1) + P\Big(\sum_{x^\varepsilon<p\leqslant x} X'_p > u\Big).$$

The first sum which appears on the right hand side here is

$$\sum_{x^\varepsilon<q_j\leqslant x} \frac{1}{q_j-1} = o(1) \qquad (x\to\infty),$$

whatever the value of u. Moreover, since the variables X'_p are independent

$$\operatorname{Var}\Big(\sum_{x^\varepsilon<p\leqslant x} X'_p\Big)^2 = \sum_{x^\varepsilon<p\leqslant x} \operatorname{Var}(X'_p)^2 \leqslant \sum_{\substack{x^\varepsilon<p\leqslant x\\ 0\leqslant f(p)\leqslant z_1}} \frac{f^2(p)}{p-1} + \Big(\sum_{\substack{x^\varepsilon<p\leqslant x\\ 0\leqslant f(p)\leqslant z_1}} \frac{f(p)}{p-1}\Big)^2$$

$$\leqslant z_1^2\Big(\log\frac{1}{\varepsilon} + O(1)\Big)^2 \qquad (x\to\infty).$$

Hence

$$P\Big(\sum_{x^\varepsilon<p\leqslant x} X'_p > u\Big) \leqslant u^{-2} z_1^2 \Big(\log\frac{1}{\varepsilon} + O(1)\Big)^2$$

so that as $x\to\infty$:

$$\nu_x\big(p;\, f(p+1)\leqslant z\big) \leqslant F(x, z+u) + O\big(\exp(-c_4\varepsilon^{-1})\big) + O\Big(u^{-2} z_1^2 \log\frac{1}{\varepsilon}\Big) + o(1).$$

We now prove that the sequence of distribution functions $F(n, z)$ ($n = 1, 2, \ldots$), is compact in the sense of P. Lévy. By the Helly selection principle there exists a subsequence n_j ($j = 1, 2, \ldots$) so that $F(n_j, z)\to H(z)$ at the points of continuity of $H(z)$. We need only prove that the total variation of $H(z)$ is 1.

Let δ be a real number in the interval $0<\delta<1$. We first choose z_1 so large as to obtain $\varepsilon_1 < \delta/4$. We next choose ε so small that the term $O\big(\exp(-c_4\varepsilon^{-1})\big)$ is $<\delta/4$. With z_1 and ε fixed we choose u so large that the term $O(-u^{-2}z_1^2\log\varepsilon)$ is $<\delta/4$. Finally, for all sufficiently large values of n the term $o(1)$ does not exceed $\delta/4$, and we have thus exhibited a value $z_2 = z_1+u$ so that $H(z_2)-H(-z_2) > 1-\delta$. In view of the fact that we may allow $\delta\to 0+$ we have proved that $H(z)$ is a distribution function.

Let $\varphi_j(t)$, $\varphi(t)$ be the characteristic functions of the distributions $F_{n_j}(z)$ ($j = 1, 2, \ldots$), $H(z)$ respectively. Then $|\varphi_j(t)|\to|\varphi(t)|$ whatever the (temporarily fixed) value of t. By direct calculation it follows readily that

$$w(t) = \lim_{j\to\infty} \sum_{p\leqslant n_j} \frac{1}{p} \sin^2\frac{tf(p)}{2}$$

exists. Then for any $z>0$

$$\sum_{f(p)>z} \frac{1}{p} \leqslant \frac{z}{2}\int_{-4/z}^{4/z} w(t)\,dt < \infty$$

so that for any $\varepsilon>0$, $z_1>0$,

$$\sum_{\substack{x^\varepsilon<p\leqslant x\\ f(p)>z_1}} \frac{1}{p} \to 0 \qquad (x\to\infty).$$

Our inequality involving $\nu_x\big(p; f(p+1)\leqslant z\big)$ therefore holds for any $z_1>0$. A similar inequality holds in the other direction, but with u replaced by $-u$.

Let $G(z)$ denote the limiting distribution for $f(p+1)$, and let z be a point of continuity of $G(z)$. Then if u is chosen such that $z\pm u$ are also continuity points of $G(z)$ we can assert that $x\to\infty$

$$\limsup_{x\to\infty} F(x, z) - \liminf_{x\to\infty} F(x, z)$$

$$\leqslant G(z+u) - G(z-u) + O\big(\exp(-c_4\varepsilon^{-1})\big) + O\Big(\Big\{u^{-1}z_1\log\frac{1}{\varepsilon}\Big\}^2\Big).$$

We let $z_1\to 0+$, $\varepsilon\to 0+$, and then $u\to 0+$ to deduce that the series

$$\sum_q X_q$$

converges in distribution, and also in probability. Hence by Kolmogorov's three series criterion (see for example Doob [2], Theorem 2.5, pp. 111–114) we deduce that the following series are convergent:

$$\sum_{|f(p)|>1} \frac{1}{p-1}, \qquad \sum_{|f(p)|\leqslant 1} \frac{f(p)}{p-1}, \qquad \sum_{|f(p)|\leqslant 1} \frac{f^2(p)}{p-1}.$$

This completes the proof of the theorem.

References

[1] M. B. Barban, *The 'Large Sieve' method and its applications in the theory of numbers*, Uspehi Mat. Nauk. 21 (1) (1966), pp. 49–103.

[2] J. L. Doob, *Stochastic Processes*, New York 1953.

[3] I. Katai, *On the distribution of arithmetical functions on the set of primes plus one*, Compositio Math. 19 (1968), pp. 278–289.

Received on 15. 6. 1972 (294)

ACTA ARITHMETICA
XXV (1974)

Odd perfect numbers are divisible by at least seven distinct primes

by

CARL POMERANCE* (Athens, Ga.)

If n is a positive integer, we let $\sigma(n)$ be the sum of the positive divisors of n. n is said to be *perfect* if $\sigma(n) = 2n$. It is well-known that if 2^k-1 is prime, then $2^{k-1}(2^k-1)$ is perfect and that all even perfect numbers are of this form. No odd perfect numbers are known, but neither has any proof of their non-existence ever been discovered.

If n is a positive integer and if $p_1^{a_1}p_2^{a_2}\dots p_k^{a_k}$ is the unique prime factorization of n, we shall call $p_1^{a_1}, p_2^{a_2}, \dots, p_k^{a_k}$ the *components* of n.

The modern work on the subject was begun by Sylvester. He proved that an odd perfect number (o.p.n.) has at least five components [16] (also proved by Dickson [4] and Kanold [11]) and that an o.p.n. not divisible by 3 has at least eight components [17]. Sylvester claimed he could prove that an o.p.n. has at least six components [18]. Sylvester [18] and Kanold [9] have been the only researchers on the subject aware of 1.8. However, Sylvester's proof of 1.8 is incorrect. A neat proof of this much-proved theorem may be found in Artin [1]. 1.8 is originally due to Bang [2], Birkhoff–Vandiver [3], and Zsigmondy [21].

Gradstein [6], Kühnel [12], and Webber [20] have each independently proved that an o.p.n. has at least six components. Kanold [10] proved that an o.p.n. not divisible by 3 has at least nine components. Tuckerman [19] proved that any o.p.n. is greater than 10^{36}. Hagis [7] proved that any o.p.n. is greater than 10^{50}. Recently Stubblefield [15] announced he could prove any o.p.n. is greater than 10^{100}.

In this paper, I will prove that any o.p.n. has at least seven components. In light of the result mentioned above by Gradstein, Kühnel, and Webber, all I need prove is that every odd number with exactly six components is not perfect.

* This paper is the author's doctoral dissertation which was submitted in June 1972 and directed by Dr. John Tate of Harvard University.