Цитированная литература

[1] Kraitchik, *Théorie des nombres*, tome II, стр. 133-143 (1926).

[2] D. H. Lehmer, *On the converse of Fermat's theorem*, Amer. Math. Monthly 43 (1936), стр. 347-354.

[3] — *A factorization theorem applied to a test for primality*, Bull. Amer. Math. Soc. 45 (1939), стр. 132-137.

[4] R. M. Robinson, *The converse of Fermat's theorem*, Amer. Math. Monthly 64. 10 (1957), стр. 703-710.

Reçu par la Rédaction le 18. 8. 1966

ACTA ARITHMETICA
XII (1967)

On certain additive functions

by

P. D. T. A. Elliott (Nottingham)

Towards the end of chapter 9 in his book [9] on the applications of probability to number theory, J. Kubilius proves a result which includes the following:

Let $\nu(m)$ denote the number of distinct prime divisors of a positive integer m. Let $\varepsilon_x \to 0$ as $x \to \infty$. Then for a constant $c_1 > 0$,

$$\sum_{\substack{m \leqslant x \\ |\nu(m) - \log\log x| > \varepsilon_x \log\log x}} 1 < x \exp(-c_1 \varepsilon_x^2 \log\log x). \tag{1}$$

Obviously we can rewrite this as follows:

Let $0 < a_1 < a_2 < \dots$ be a sequence of integers which in the usual notation [1] satisfies $A(x) > x\exp(-\varepsilon_x \log\log x)$. Then $\nu(a_i)$ is normally $\log\log a_i$.

This result is, in a certain sense, best possible as can be seen by taking $a_i = p_i$, the ith rational prime. This shows that we cannot replace $\varepsilon_x \to 0$ by $\varepsilon_x = 1$; in fact, it is not difficult to construct sequences A satisfying $A(x) > c_2 x (\log x)^{-\alpha}$ for any given α with $0 < \alpha < 1$, for which $\nu(a_i)$ has no normal value. We give such an example later.

Broadly speaking, the accuracy of (1) is obtained by considering the appropriate Dirichlet series and evaluating, for an appropriate range of z, the sum

$$\sum_{m \leqslant x} z^{\nu(m)}. \tag{2}$$

The evaluation of this sum was first carried out in detail by A. Selberg [13]. In this respect $\nu(m)$ enjoys distinct advantages over other functions. Essentially this is because the value of $\nu(p^\alpha)$ is the same for all powers of primes p and so can be interpreted in terms of counting functions [2].

In this present note we seek to generalise (1) to cover more general additive functions. In particular, we consider $\nu(m)$ when m runs through

[1] $A(x)$ denotes the number of $a_i \leqslant x$.

[2] Cf. the remarks near the beginning of the proof of Theorem 2.

the values of a polynomial. To estimate sums of type (2) we have however to truncate our functions and this introduces a weak but additional restriction on their generality. We first state the result concerning $\nu(m)$.

THEOREM 1. *Let $g(t)$ be a polynomial in t with integer coefficients which is primitive and irreducible. Let $0 < a_1 < \dots$ be a sequence of integers satisfying $A(x) > x\exp(-\varepsilon_x \log\log x)$. Then, for any integer $k > 0$,*

$$\sum_{a_i \leqslant x} \nu^k(g(a_i)) \sim A(x)(\log\log x)^k \quad \text{as} \quad x \to \infty.$$

Really this is a corollary of our second result. However, we give it as a separate theorem since it is the most interesting case and we shall later consider $\nu(m)$ in more detail. Clearly, by taking $k = 1$ and 2 we see that $\nu(g(a_i))$ is normally $\log\log a_i$. By an earlier remark the result is best possible. For convenience only we assume that $g(t) > 0$ for all integers $t \geqslant 1$. Then we prove more generally the following

THEOREM 2. *Let $f(m)$ be a non-negative additive function. Let $\varrho(u)$ denote the number of residue classes r satisfying $g(r) \equiv 0 \pmod u$. Let*

$$S_x = \sum_{p^\alpha \leqslant x} \varrho(p^\alpha) f(p^\alpha) p^{-\alpha} \quad \text{and} \quad \mu_x = \max_{p^\alpha \leqslant x} f(p^\alpha).$$

Suppose that

$$S_x^{-1} \mu_x \log\log\log x \to 0 \quad \text{as} \quad x \to \infty. \tag{3}$$

Let A be a sequence of positive integers satisfying $A(x) > x\exp(-\varepsilon_x S_x \mu_x^{-1})$. Then, for any integer $k > 0$,

$$\sum_{a_i \leqslant x} f^k(g(a_i)) \sim A(x) S_x^k. \tag{4}$$

Naturally, one would expect that the condition (4) could be replaced by $S_x^{-1}\mu_x \to 0$. If we allow $f(m)$ to take negative values the problem appears to be more difficult to handle. One would then expect conditions on

$$\sum_{p^\alpha \leqslant x} f^2(p^\alpha) p^{-\alpha}.$$

Taking $f(m) = \nu(m)$ in Theorem 2 we get Theorem 1. For, by the prime ideal theorem (see, for example, Erdös [3], Lemma 7),

$$S_x = \sum_{p \leqslant x} \varrho(p) p^{-1} + O(1) \sim \log\log x.$$

We have used here the well-known fact that $\varrho(p^\alpha) < c_3$ for some c_3 depending only upon $g(t)$. In particular, Nagell [11] showed that if the degree and discriminant of $g(t)$ are respectively l and D one may take $c_3 = lD^2$.

Although we do not go into details it is easy to see that the following results can, without difficulty, be extended to cover sequences of the Σ_R-distributed type considered by Barban [1]. We need various lemmas, and, when no confusion is possible, we renumber constants occuring in them. We denote these by $c_1, c_2, \dots, C$ and they will always be positive. We use sometimes the Vinogradov notation $\ll$.

Before we begin the proof we note that we may assume that $f(m)$ satisfies $0 \leqslant f(p^\alpha) < 1$ and $S_x \to \infty$ with x. For instead of $f(m)$ we consider the additive function $f^*(m)$ defined by

$$f^*(p^\alpha) = f(p^\alpha)/2\mu_x \quad \text{if} \quad p^\alpha \leqslant x$$

and zero for other prime powers. Let a suffix 1 denote for the time being that we count only prime powers $p^\alpha \leqslant x$ in evaluating an additive function. Then if we prove Theorem 2 for $f^*(m)$ it is easily seen that

$$\sum_{a_i \leqslant x} f^k(g(a_i)) \sim \sum_{a_i \leqslant x} f_1^k(g(a_i)) \sim (2\mu_x)^k \sum_{a_i \leqslant x} \{f^*(g(a_i))\}^k$$
$$\sim (2\mu_x)^k A(x)(S_x/2\mu_x)^k = A(x) S_x^k.$$

Thus the general result will hold. Corresponding to this restriction on $f(m)$, our condition on $A(x)$ becomes $A(x) > x\exp(-\varepsilon_x S_x)$.

LEMMA 1. *$\varrho(u)$ is a multiplicative function of u and satisfies, for all prime powers p^α, $\varrho(p^\alpha) < c_3$.*

LEMMA 2. *Let $\log y = \log x/(\log\log x)^2 > 3$. If the exact power of p dividing m is k we write $p^k \| m$. The number of integers $m < x$ for which*

$$\prod_{p^\alpha \| g(m), p \leqslant y} p^\alpha > x^{1/2}$$

is $O_C(x(\log x)^{-C})$ for any fixed $C > 0$.

Proof. This is Lemma 6 of Erdös [3], with trivial modifications.

For convenience, we use N_x to denote the set of integers not exceeding x for which Lemma 2 is false; also let B_x denote the set of prime powers p^α satisfying $p \leqslant y$, $p^\alpha \leqslant x^{1/2}$. We now define

$$h(p^\alpha) = \begin{cases} f(p^\alpha) & \text{if} \quad p^\alpha \in B_x, \\ 0 & \text{otherwise.} \end{cases}$$

LEMMA 3. *Let*

$$F(s, x) = \prod_{p \leqslant x^{1/2}} \Big(1 + \sum_{p^\alpha \in B_x} \varrho(p^\alpha) H(p^\alpha) p^{-\alpha(1+s)}\Big),$$

where $H(m)$ is the multiplicative function of m defined by $H(p^\alpha) = z^{h(p^\alpha)} - z^{h(p^{\alpha-1})}$. Then, if $\operatorname{re} s \geqslant -1/2\log y$, $|z| < c_5$, we have

$$|F(s, x)| < c_6 \log y.$$

Proof. Clearly, $|H(p^a)| < c_7$. Hence by Lemma 1, for any $p_0 > 0$

$$\sum_{a\geqslant 2} \varrho(p^a) H(p^a) p^{-a(1+s)} \ll \sum_a p^{-a(1-1/(2\log y))} \ll p^{-2(1-1/(2\log y))}.$$

Thus, for a large enough but fixed value of p_0 which ensures that no individual term of the product is zero,

$$\begin{aligned}\operatorname{re}\log \prod_{p_0<p\leqslant x^{1/2}} \Big(1+\sum_{\substack{a\\ p^a\in B_x}} \varrho(p^a) H(p^a) p^{-a(1+s)}\Big) &\\ \ll \sum_{p_0<p\leqslant y} p^{-(1-1/(2\log y))} + p^{-2(1-1/(2\log y))} &\\ \ll \sum_{p\leqslant y} p^{-1}\exp\big(\log p/2\log y\big)+1 \ll \sum_{p\leqslant y} p^{-1} \ll \log\log y &\end{aligned}$$

by well-known estimates and the fact that $0 < \log p/(2\log y) \leqslant \frac{1}{2}$. The lemma is now clear.

Lemma 4. *Let*

$$r(m) = \sum_{p^a \| m} h(p^a).$$

Then, if z is real and $0 \leqslant z \leqslant 2$,

$$\sum_{m\leqslant x} z^{r(g(m))} \leqslant c_7 \exp\big((z-1) S_y^*\big),$$

where

$$S_y^* = \sum_{p^a\in B_x} h(p^a)\varrho(p^a)p^{-a}.$$

Proof. We have

$$\sum_{v\mid n} H(v) = \prod_{p^a\| n} (1+z^{h(p^a)}-1+z^{h(p^2)}-z^{h(p)}+\ldots+z^{h(p^a)}-z^{h(p^{a-1})}) = z^{r(n)}.$$

In other words $H(v)$ is the Möbius inverse of $z^{r(n)}$. Hence

$$T = \sum_{\substack{m\leqslant x\\ m\in N_x}} z^{r(g(m))} = \sum_{u\leqslant x^{1/2}} H(u) \sum_{\substack{g(m)\equiv 0 \pmod u\\ m\leqslant x,\ m\in N_x}} 1.$$

For $H(u) = 0$ unless the primes p dividing $g(m)$ do not exceed y and, by Lemma 2, since $m \in N_x$, we must then have that $u \leqslant x^{1/2}$. Thus the inner sum is

$$\frac{x}{u}\varrho(u) + \vartheta\varrho(u) + \sum_{\substack{m\leqslant x\\ u\mid g(m)\ m\notin N_x}} 1, \quad |\vartheta| \leqslant 1.$$

Hence

$$\begin{aligned} T &= x\sum_{u\leqslant x^{1/2}} \frac{\varrho(u)}{u} H(u) + O\Big(\sum_{u\leqslant x^{1/2}} \varrho(u) c^{r(u)}\Big) + \sum_{\substack{m\notin N_x\\ m\leqslant x}} \sum_{\substack{u\mid g(m)\\ u\leqslant x^{1/2}}} H(u) \\ &= \Sigma_1 + \Sigma_2 + \Sigma_3, \end{aligned}$$

say. For any $\varepsilon > 0$, Σ_2 clearly does not exceed

$$c_1(\varepsilon) x^{\varepsilon} \sum_{u\leqslant x^{1/2}} 1 \leqslant c_1(\varepsilon) x^{1/2+\varepsilon}.$$

Moreover, by the Cauchy-Schwarz inequality,

$$|\Sigma_3|^2 \leqslant \sum_{\substack{m\notin N_x\\ m\leqslant x}} 1 \cdot \sum_{m\leqslant x} \Big|\sum_{\substack{u\mid g(m)\\ u\leqslant x^{1/2}}} H(u)\Big|^2.$$

The second of these sums is at most [3]

$$\sum_{m\leqslant x} c^{r(u)} \sum_{u\mid g(m)} 1 < \sum_{m\leqslant x} \tau^{\Delta}\big(g(m)\big) < c_8 x (\log x)^{C(\Delta)},$$

by a well-known result of van der Corput [2]. Note that $C(\Delta)$ is independent of N_x.

Since

$$\sum_{\substack{m\notin N_x\\ m\leqslant x}} 1 < c_9(\Delta) x (\log x)^{-\Delta-C} \quad \text{for} \quad x \geqslant x_0(\Delta, C)$$

from Lemma 2, we see that

$$|\Sigma_3| \leqslant c_{10}(C) x (\log x)^{-C}$$

for any fixed $C > 0$.

Similarly,

$$\Big|\sum_{\substack{m\leqslant x\\ m\notin N_x}} z^{r(g(m))}\Big| < c_{11}(C) x (\log x)^{-C}$$

for any fixed $C > 0$. Thus

$$\sum_{m\leqslant x} z^{r(g(m))} = x\sum_{u\leqslant x^{1/2}} u^{-1}\varrho(u)H(u) + O_C\big(x(\log x)^{-C}\big).$$

We note that a result of this type occurs in Barban [1], Lemma 4. In that paper he considered sums of the type

$$\sum_{a_i\leqslant x} t\big(g(a_i)\big),$$

---

[3] τ denotes, as usual, the divisor function. Δ denotes a positive constant depending at most on c and the coefficients of g.

where a_i runs over well distributed sequences and $t(m)$ is a multiplicative function of m satisfying $t(p^{\alpha+1}) \geqslant t(p^\alpha)$, $\alpha = 0, 1, \ldots$ He gets upper and lower inequalities for these, generalising a result of Erdös. However, he needs $t(p) \geqslant 1$ and, in our case, since we intend to apply our result for values of $z < 1$, the corresponding condition is clearly not satisfied. We therefore use the following standard technique to evaluate Σ_1.

Consider $F(s, x)$ expanded as a Dirichlet series:

$$F(s, x) = \sum_{n=1}^{\infty} a_n n^{-s}.$$

Clearly if $n \leqslant x^{1/2}$, $a_n = n^{-1}\varrho(n)H(n)$ whilst if $n > x^{1/2}$, $|a_n| \leqslant c_{12}^{r(n)}$ for a certain constant $c_{12} > 0$. By a standard method of Perron (see, for example, Titchmarsh [14], Lemma 3.12) we see that for any fixed $\varepsilon > 0$ and $T \geqslant 2$,

$$\sum_{u \leqslant x^{1/2}} u^{-1}\varrho(u)H(u) = \frac{1}{2\pi i}\int_{\varepsilon-iT}^{\varepsilon+iT} F(s, x)\frac{x^{s/2}}{s}\,ds + O_\varepsilon(T^{-1}x^{2\varepsilon}).$$

Moving the contour over the simple pole at $s = 0$ where the residue is $F(0, x)$, we introduce further terms

$$\frac{1}{2\pi i}\Big(\int_{\varepsilon-iT}^{-1/2\log y-iT} + \int_{-1/2\log y-iT}^{-1/2\log y+iT} + \int_{-1/2\log y+iT}^{\varepsilon+iT}\Big) F(s, x)\frac{x^{s/2}}{s}\,ds.$$

Clearly the first and third of these are, by Lemma 3, $O_\varepsilon(x^\varepsilon T^{-1})$, whilst for the second

$$\Big|\int_{-1/2\log y-iT}^{-1/2\log y+iT} F(s, x)\frac{x^{s/2}}{s}\,ds\Big| \leqslant c_{13}x^{-1/4\log y}\int_0^T \frac{dt}{\sqrt{t^2+1/4(\log y)^2}} \log x.$$

Here

$$\int_0^T \frac{dt}{\sqrt{t^2+1/4(\log y)^2}} \leqslant \int_0^{(\log y)^{-1}} 2\log y\cdot\frac{dt}{2} + \int_{(\log y)^{-1}}^T \frac{dt}{t} \leqslant 2+\log(T\log y).$$

Choosing $\varepsilon = 1/2$, $T = x^2$ we see that

$$\sum_{u \leqslant x^{1/2}} u^{-1}\varrho(u)H(u) - F(0, x) = O(x^{-1}) + O\{\exp(2\log\log x - c_{14}(\log\log x)^2)\}$$
$$= O_C\big((\log x)^{-C}\big)$$

for any fixed $C > 0$. Now

$$F(0, x) = \prod_{p \leqslant x^{1/2}} \Big(1+p^{-1}\varrho(p)H(p) + \sum_{\alpha \geqslant 2} p^{-\alpha}\varrho(p^\alpha)H(p^\alpha)\Big).$$

By Lemma 1 and the fact that $|H(p^\alpha)| \leqslant c_7$ we obtain

$$F(0, x) \ll \prod_{p \leqslant x^{1/2}} \big(1+p^{-1}\varrho(p)H(p)\big) \ll \exp\Big(\sum_{p \leqslant x^{1/2}} p^{-1}\varrho(p)H(p)\Big).$$

Now

$$\sum_{p \leqslant x^{1/2}} p^{-1}\varrho(p)H(p) = \sum_{p \leqslant y} p^{-1}\varrho(p)\{z^{h(p)}-1\}.$$

In this sum we write $z = (1+z-1)$ and apply the mean-value theorem for $|z-1| \leqslant 1$ to obtain for it the estimate

$$\sum_{p \leqslant y} p^{-1}\varrho(p)\{(z-1)h(p) + \tfrac{1}{2}(z-1)^2 h(p)\big(h(p)-1\big)(1+\vartheta)^{h(p)-2}\},$$

where $|\vartheta| < 1$. Now $h(p)\big(h(p)-1\big) \leqslant 0$, so that

$$\sum_{p \leqslant x^{1/2}} p^{-1}\varrho(p)H(p) \leqslant (z-1)\sum_{p \leqslant y} p^{-1}\varrho(p)h(p) = (z-1)S_y^* + O(1).$$

Putting these results together we obtain the result stated in the lemma.

We define $r^*(m) = r_g^*(m) = r\big(g(m)\big) - S_y^*$.

LEMMA 5.

$$\sum_{r^*(m) > \varepsilon_x^{1/3} S_y^*} \big(r^*(m)\big)^{2k} \ll x\exp(-c_1\varepsilon_x^{2/3}S_x).$$

Proof. If $0 < 2\sigma < 1$,

$$\frac{1}{(2k+2l)!}\sum_{m \leqslant x}\big(r^*(m)\big)^{2k+2l} = \frac{1}{2\pi i}\int_{|\zeta|=0}\sum_{m \leqslant x} e^{\zeta r^*(m)}\zeta^{-(2k+2l+1)}d\zeta.$$

Now $0 < e^{\mathrm{re}\,\zeta} < e^{1/2} < 2$, so that by Lemma 4,

$$\Big|\sum_{m \leqslant x} e^{\zeta r^*(m)}\Big| \leqslant \sum_{m \leqslant x} e^{\mathrm{re}\,\zeta r^*(m)} \ll \exp\big((e^{\mathrm{re}\,\zeta}-1-\mathrm{re}\,\zeta)S_y^*\big).$$

Moreover

$$|e^{\mathrm{re}\,\zeta}-1-\mathrm{re}\,\zeta| \leqslant \sum_{j=2}^{\infty}\frac{1}{j!}|\mathrm{re}\,\zeta|^j \leqslant \tfrac{1}{2}\sum_{j=2}^{\infty}\sigma^j \leqslant \sigma^2.$$

Thus

$$\sum_{|r^*(m)| > \varepsilon_x^{1/3}S_x}\big(r^*(m)\big)^{2k} \ll \frac{(2k+2l)!}{(\varepsilon_x^{1/3}S_x)^{2l}}\,x\exp(\sigma^2 S_y^*)\sigma^{-(2k+2l+1)}.$$

Hence, by applying Stirling's formula to $(2k+2l)!$ we have, for the right-hand side, the upper bound

$$c_2 x\exp\big(2(k+l)\{\log(2k+2l)-1\} + c_3\log(2k+2l) + \ldots$$
$$\ldots - 2l\log(\sigma\varepsilon_x^{1/3}S_x) + \sigma^2 S_x - (2k+1)\log\sigma\big),$$

since $S_y^* \leqslant S_x$.

Now this holds uniformly for any integers l, k such that $l+k \geqslant 1$. With k fixed, choose $l = [\frac{1}{2}\sigma\varepsilon_x^{1/3} S_x] - k$. If $\sigma \geqslant 2(k+1)\varepsilon_x^{-1/3} S_x^{-1}$, then $l > 0$ and so our upper bound is less than

$$c_4 x \exp\left(-\tfrac{1}{4}\sigma\varepsilon_x^{1/3} S_x + \sigma^2 S_x + 2k\log(S_x\varepsilon_x^{1/3}) + c_5 \log \sigma S_x \varepsilon_x^{1/3}\right).$$

Choosing $4\sigma = \varepsilon_x^{1/3}$ we see that the exponent here does not exceed

$$-\frac{3}{16}\varepsilon_x^{2/3} S_x + c_6(k)\log S_x^2 \varepsilon_x^{2/3}\cdot\varepsilon_x^{1/3} < -\frac{1}{8}\varepsilon_x^{2/3} S_x,$$

since, without loss of generality, we may assume that $\varepsilon_x^{-1} \ll S_x$. Collecting results we see that we have proved the lemma with c_1, c_2 depending upon k.

LEMMA 6. *Let $0 < a_1 < a_2 \dots$ be a sequence of integers satisfying the conditions of Theorem 2. Then for any fixed $k > 0$,*

$$\sum_{a_i \leqslant x} r^k(g(a_i)) \sim A(x) S_x^k.$$

Proof. We split the sum into two parts according as $|r(g(a_i)) - S_y^*| > \varepsilon_x^{1/3} S_x$ or not. For the first of these sums $\sum_1$, when $k > 0$,

$$\sum_{a_i \leqslant x}{}_1 r^k(g(a_i)) = \sum_{a_i \leqslant x} \{r(g(a_i)) - S_y^* + S_y^*\}^k = \sum_{s=0}^{k} \binom{k}{s} \sum_{a_i \leqslant x}{}_1 \{r(g(a_i)) - S_y^*\}^s (S_y^*)^{k-s}.$$

If $t > 0$

$$\sum_{a_i \leqslant x}{}_1 |\{r(g(a_i)) - S_y^*\}^t| \ll x\exp(-c_1\varepsilon_x^{2/3} S_x) = o(A(x) S_x^t),$$

by Lemma 5 and the Cauchy-Schwarz inequality.

Hence

$$\sum_{a_i \leqslant x}{}_1 r^k(g(a_i)) = o(A(x) S_x^k).$$

Note that if $k = 0$ or $t = 0$ in the above, we apply Lemma 5 with $k = 0$, which states that all but $o(A(x))$ of the terms in A are counted in Σ_2.

Moreover, writing

$$\sum_{a_i \leqslant x}{}_2 r^k(g(a_i)) = \sum_{s=0}^{k} \binom{k}{s} \sum_{a_i \leqslant x}{}_2 \{r(g(a_i)) - S_y^*\}^s (S_y^*)^{k-s},$$

we see that for any fixed $s > 0$,

$$\Big|\sum_{a_i \leqslant x}{}_2 \{r(g(a_i)) - S_y^*\}^s (S_y^*)^{k-s}\Big| \leqslant S_x^k \varepsilon_x^{1/3s} \sum_{a_i \leqslant x}{}_2 1 = o(A(x) S_x^k).$$

Hence we obtain the result stated in the lemma with S_y^* in place of S_x. Finally, we can, however, replace S_y^* by S_x since

$$|S_x - S_y^*| \leqslant c_1 + c_2 \sum_{y < p \leqslant x} p^{-1} \ll \log\left(\frac{\log x}{\log y}\right) = o(S_x),$$

by the hypotheses of Theorem 2.

This completes the proof of the lemma.

It remains now only to show that we can remove the truncation in the definition of $r(m)$ with a small error. For

$$\sum_{a_i \leqslant x} \Big(\sum_{\substack{p^\alpha \| g(a_i) \\ p^\alpha \in B_x}} f(p^\alpha)\Big)^k \sim \sum_{a_i \leqslant x} r^k(g(a_i)) \sim A(x) S_x^k.$$

Indeed, it is now that we need the fact that $f(m) \geqslant 0$, which we have not used yet in a vital context.

LEMMA 7. *Let P_s be a set of at most $k-s$ prime powers such that*

(i) *no prime occurs with more than one power,*

(ii) *if λ is the greatest member of P_s, then $\lambda^{k+1} \leqslant x$.*

Let π be the product of all members of P_s, and $\pi = 1$ if P_s is empty. Define

$$F_{P_s}(m) = \sum_{\substack{p^\alpha \| m \\ p^{\alpha(k+1)} \leqslant x, p \nmid \pi}} f(p^\alpha).$$

Then, for a fixed integer $k > 0$, and any integer s, $0 \leqslant s \leqslant k$,

$$\sum_{\substack{m \leqslant x \\ g(m) \equiv 0 \pmod{\pi}}} F_{P_s}^s(g(m)) \leqslant \frac{x\varrho(\pi)}{\pi}(S_x + s)^s.$$

Proof. We prove this by induction on s for all P_s, for all $x \geqslant 1$. For $s = 0$ the result is trivial. When $s = 1$ we have

$$\sum_{\substack{m \leqslant x \\ g(m) \equiv 0 \pmod{\pi}}} F_{P_1}(g(m)) = \sum_{p^\alpha \pi \leqslant x} \sum_{\pi p^\alpha \| g(m)} f(p^\alpha).$$

Now $p^\alpha \pi \leqslant x$. Thus, interchanging the order of summation, we see that the sum we wish to estimate is not more than

$$\sum_{p^\alpha \leqslant x} f(p^\alpha) \sum_{\substack{m \leqslant x \\ g(m) \equiv 0 \pmod{p^\alpha \pi}}} 1 \leqslant \frac{\varrho(\pi)}{\pi} \sum_{p^\alpha \leqslant x} p^{-\alpha}\varrho(p^\alpha) f(p^\alpha).$$

Suppose now that the result holds for $s = 0, 1, \dots, r-1$. Then

$$\sum_{m \leqslant x} F_{P_r}^r(g(m)) = \sum_{m \leqslant x} F_{P_r}^{r-1}(g(m)) \sum_{p^\alpha \| g(m)}{}' f(p^\alpha),$$

where $\sum'$ indicates that p^a satisfies the conditions stated in the definition of $F_{P_r}(m)$ in the statement of the lemma. Our double sum is then

$$\sum_{p^a\leqslant x}{}' f(p^a) \sum_{\substack{m\leqslant x\\ g(m)\equiv 0(\mathrm{mod}\, p^a)}} \{f(p^a)+F_{P_r}(p^{-a}g(m))\}^{r-1}$$

$$= \sum_{p^a\leqslant x}{}' f(p^a) \sum_{s=0}^{r-1}\binom{r-1}{s}(f(p^a))^{r-1-s} \sum_{\substack{m\leqslant x\\ g(m)\equiv 0(\mathrm{mod}\, p^a)}} \{F_{P_r}(p^{-a}g(m))\}^s$$

$$\leqslant \sum_{p^a\leqslant x}{}' f(p^a) \sum_{s=0}^{r-1}\binom{r-1}{s} \sum_{\substack{m\leqslant x\\ g(m)\equiv 0(\mathrm{mod}\, p^a)}} \{F_{P_r}(p^{-a}g(m))\}^s,$$

where we have used the fact that $f(p^a)<1$. Now

$$F_{P_r}(p^{-a}g(m)) = F_{P_{r-1}}(g(m)), \quad \text{where} \quad P_{r-1} = P_r \cup \{p^a\}.$$

Note that p does not occur in P_r by definition of $F_{P_r}(g(m))$. Further if λ_1 is the greatest member of P_{r-1} then

$$\lambda_1^{k+1} \leqslant \mathrm{Max}(\lambda^{k+1}, p^{a(k+1)}) \leqslant x.$$

Clearly each P_r is a P_s if $s<r$.

Thus we can apply our induction hypothesis to the inner sums $(0\leqslant s\leqslant r-1)$ and obtain

$$\sum_{m\leqslant x}\{F_{P_r}(p^{-a}g(m))\}^s \leqslant \frac{x\varrho(\pi)}{\pi}\cdot\frac{\varrho(p^a)}{p^a}(S_x+(r-1))^s.$$

Hence

$$\sum_{m\leqslant x, g(m)\equiv 0(\mathrm{mod}\,\pi)}\{F_{P_r}(g(m))\}^r \leqslant \frac{x\varrho(\pi)}{\pi}\sum_{p^a\leqslant x}p^{-a}\varrho(p^a)f(p^a)(S_x+(r-1)+1)^{r-1}.$$

This completes our induction step and the lemma therefore holds.

LEMMA 8. *Let A be a sequence of positive integers satisfying $A(x) > x\exp(-\varepsilon_x S_x)$. Let $S_x^{-1}\log\log\log x\to\infty$. Then*

$$\sum_{a_i\leqslant x}\{f(g(a_i))-r(g(a_i))\}^k = o(A(x)S_x^k).$$

Proof. Let

$$j(p^a) = \begin{cases} f(p^a) & \text{if} \quad p^a\leqslant \exp(S_x^{-1}\varepsilon_x^{-1/2}\log x) \text{ and } p>y,\\ 0 & \text{otherwise.}\end{cases}$$

Define $j(m)$ additively. Then by Lemma 7 (with P_0 empty so that $\pi^{-1}\varrho(\pi)=1$), we see that if $(1+t)\varepsilon_x^{-1/2}S_x^{-1}\leqslant 1$,

$$\sum_{m\leqslant x} j^t(g(m)) \leqslant x(S_x^{**}+t)^t,$$

where

$$S_x^{**} = \sum_{p^a\leqslant x} p^{-a}\varrho(p^a)j(p^a).$$

Thus, taking $t=kl$ we see from Hölder's inequality that

$$\{A(x)\}^{-1}\sum_{a_i\leqslant x} j^k(g(a_i)) \leqslant \Big(\{A(x)\}^{-1}\sum_{a_i\leqslant x} j^{kl}(g(a_i))\Big)^{1/l}$$

$$\leqslant (x/A(x))^{1/l}\Big(x^{-1}\sum_{m\leqslant x} j^{kl}(g(m))\Big)^{1/l},$$

which does not exceed

$$\{x/A(x)\}^{1/l}(S_x+kl)^k.$$

For any fixed k, let $l=l(k)=[(\varepsilon_x^{1/2}S_x-1)/k]\geqslant 1$. Clearly this is an admissible value of l if x is sufficiently large. Then

$$\{x/A(x)\}^{1/l} \leqslant \exp(l^{-1}\varepsilon_x S_x) \leqslant \exp(c_1\varepsilon_x^{-1/2}S_x^{-1}\varepsilon_x S_x) \ll 1.$$

Also $kl \ll \varepsilon_x^{1/2}S_x = o(S_x)$, so that

$$\{A(x)\}^{-1}\sum_{a_i\leqslant x} j^k(g(a_i)) \ll o(S_x^k)+(S_x^{**})^k.$$

Now

$$S_x^{**} \ll \sum_{y<p\leqslant x}\frac{1}{p} \ll \log\log\log x = o(S_x).$$

Moreover

$$|f(g(a_i))-r(g(a_i))-j(g(a_i))|$$

$$\leqslant \Big|\sum_{\substack{p^a\| g(a_i)\\ p^a>\mathrm{Max}(y,\exp(\varepsilon_x^{-1/2}S_x^{-1}\log x))} f(p^a)\Big| + \Big|\sum_{\substack{p^a\| g(a_i), p\leqslant y\\ p^a>x^{1/2}}} f(p^a)\Big|$$

$$\leqslant \sum_{\substack{p^a\| g(a_i)\\ p^a>\exp(\varepsilon_x^{-1/2}S_x^{-1}\log x)}} 1 \leqslant \varepsilon_x^{1/2}S_x = o(S_x).$$

Hence, as in Lemma 6,

$$\sum_{a_i\leqslant x}\{f(g(a_i))-r(g(a_i))\}^k = \sum_{a_i\leqslant x} j^k(g(a_i)) + o(A(x)S_x^k) = o(A(x)S_x^k).$$

This completes the proof of the lemma.

Proof of Theorem 2. We have

$$\sum_{a_i\leqslant x} f^k(g(a_i)) = \sum_{s=0}^{k}\binom{k}{s}\sum_{a_i\leqslant x}\{f(g(a_i))-r(g(a_i))\}^s\{r(g(a_i))\}^{k-s}$$

$$= \sum_{a_i\leqslant x}\{r(g(a_i))\}^k + \sum_{s=1}^{k}\binom{k}{s}\sum_{a_i\leqslant x}\{f(g(a_i))-r(g(a_i))\}^s\{r(g(a_i))\}^{k-s}.$$

By Lemmas 6, 8 and the inequality of Cauchy-Schwarz the double sum does not exceed

$$\sum_{s=1}^{k}\binom{k}{s}\Big\{\sum_{a_i\leqslant x}[r(g(a_i))]^{2k-2s}\Big\}^{1/2}\Big\{\sum_{a_i\leqslant x}[f(g(a_i))-r(g(a_i))]^{2s}\Big\}^{1/2}=o\big(A(x)S_x^k\big).$$

Moreover

$$\sum_{a_i\leqslant x} r^k(g(a_i))\sim A(x)S_x^k,$$

and this completes the proof of Theorem 2.

The special case $\nu(g(m))$ can be considered differently, as we have already mentioned. Indeed, one can use the ideas of Hardy and Ramanujan as used by Halberstam [6] combined with some of the ideas above in order to obtain Theorem 1. For example, Hardy and Ramanujan [7] showed that

$$\sum_{\substack{m\leqslant x\\ \nu(m)=k}} 1<\frac{c_1x}{\log x}\cdot\frac{(\log\log x+c_2)^{k-1}}{(k-1)!}$$

(and obtained an effectively similar result about the values of $\Omega(m)$, the total number of prime divisors of m). We can generalise these results to estimate, for example,

$$\sum_{\substack{m\leqslant x\\ \bar\nu(g(m))=k}} 1,$$

where $\bar\nu(m)$ is a truncated form of $\nu(m)$. If $0<z<c_3$, we arrive at an analogue to

$$\sum_{m\leqslant x} z^{\nu(m)}=\sum_{k=1}^{\infty}z^k\sum_{\substack{m\leqslant x\\ \nu(m)=k}}1<c_2\frac{x}{\log x}\sum_{k=1}^{\infty}\frac{1}{(k-1)!}(z\log\log x+c_4)^{k-1}$$

$$<c_5x(\log x)^{z-1}.$$

We then link up with the above analysis at the end of Lemma 4. In order to use this approach we must use a sieve process, as for example, A. Selberg's method.

Hooley [8] had occasion to introduce the integer sequence $Q_j=\{m;\ e^{j-1}<m<e^j,\ p\,|\,m\Rightarrow p>e^{j^\alpha}\}$, where $0<\alpha<1$ is a constant. We call these 'quasi primes' with exclusion up to e^{j^α}. We now use Q_j to construct the example mentioned earlier which will give a limitation on Theorem 1. For convenience, we denote summation over integers m having no prime factors $p\leqslant e^{j^\alpha}$ by $\sum'$.

Now

$$\sum_{m\in Q_j}\nu(m)=\sum_{e^{j^\alpha}<p\leqslant e^j}\ \sum_{m\equiv 0(\mathrm{mod}\,p)}{}'\ 1.$$

Following the lines of Lemma 4 of Hooley [8] we see that, for a constant $d>0$ and any fixed $\varepsilon>0$, the inner sum is

$$d(p-1)^{-1}(1-e^{-1})j^{-\alpha}e^j\big(1+O_\varepsilon(j^{-\alpha+\varepsilon})\big)\quad\text{as}\quad j\to\infty.$$

Thus

$$\begin{aligned}\sum_{m\in Q_j}\nu(m)&=d(1-e^{-1})j^{-\alpha}e^j\big(1+O_\varepsilon(j^{-\alpha+\varepsilon})\big)\sum_p{}'\frac{1}{p-1}\\&=d(1-e^{-1})j^{-\alpha}e^j\big(1+O_\varepsilon(j^{-\alpha+\varepsilon})\big)\big(\log j/j^\alpha+O(1)\big)\\&=\{d(1-e^{-1})j^{-\alpha}e^j(1-\alpha)\log j\}\Big\{1+O\Big(\frac{1}{\log j}\Big)\Big\},\end{aligned}$$

and it follows that

$$\begin{aligned}\sum_{j\leqslant N}\sum_{m\in Q_j}\nu(m)&\sim d(1-e^{-1})(1-\alpha)\sum_{j\leqslant N}j^{-\alpha}e^j\log j\\&\sim d(1-e^{-1})(1-\alpha)\log N\sum_{j\leqslant N}j^{-\alpha}e^j\\&\sim(1-\alpha)\log N\sum_{j\leqslant N}\sum_{m\in Q_j}1\quad\text{as}\quad N\to\infty.\end{aligned}$$

Here we have left out some easy calculations, it being necessary only to consider values of $j\leqslant\frac12 N$ and $\frac12 N<j\leqslant N$ separately.

Varying the values of j clearly gives rise to disjoint sets Q_j, so that if $Q=\bigcup_{j=1}^{\infty}Q_j$, we have with the obvious definitions

$$\sum_{\substack{m\leqslant x\\ m\in Q}}\nu(m)\sim(1-\alpha)Q(x)\log\log x$$

as $x\to\infty$ through integer multiples of e.

Equally we can prove that

$$\sum_{\substack{m\leqslant x\\ m\in Q}}\nu^2(m)\sim(1-\alpha)^2Q(x)(\log\log x)^2.$$

From these results we clearly obtain

$$\sum_{\substack{m\leqslant x\\ m\in Q}}\big(\nu(m)-(1-\alpha)\log\log x\big)^2=o\big(Q(x)(\log\log x)^2\big).$$

Now let $Q^{(1)}=\{m;\ m-1\in Q\}$. Then it is easy to check that results corresponding to the above hold with Q replaced by $Q^{(1)}$ and $1-\alpha$ by 1.

The calculations make use of the good distribution of quasi-primes in arithmetic progressions with large differences. Thus as $x \to \infty$ through integral powers of e we obtain

$$\sum_{\substack{m \leqslant x \\ m \in Q^{(1)}}} \nu(m) \sim Q^{(1)}(x) \log\log x \sim Q(x) \log\log x$$

and

$$\sum_{\substack{m \leqslant x \\ m \in Q^{(1)}}} \big(\nu(m) - \log\log x\big)^2 = o\big(Q(x)(\log\log x)^2\big).$$

Finally let us take $Q^{(2)} = Q \cup Q^{(1)}$.

It is not difficult to check that infinitely often $Q^{(2)}(x) \sim cx(\log x)^{-a}$. Moreover, we see from the above results that in a certain sense $\nu(m)$ behaves like $(1-a)\log\log m$ in Q and $\log\log m$ in $Q^{(1)}$. It is evident therefore that $\nu(m)$ cannot have a normal value in $Q^{(2)}$. More general examples can be given, related to Theorem 2, but the details are complicated and the result no more enlightening. It is true that $Q^{(2)}(x) \sim cx(\log x)^{-a}$ has only been proved to hold infinitely often but this is nevertheless a true restriction to Theorem 1 since we need only prove that theorem for x running through the members of some infinite sequence.

An interesting result which follows from the above construction is that $\nu(m)$ is generally too small rather than too big. Indeed to find a sequence A in which $\nu(m)$ is always large demands that one should make A very thin, say consisting of $a_i = \prod_{j \leqslant i} p_j$, the product of the first i rational primes. Clearly, for such an A,

$$e^{c_1 j} < a_j < e^{c_2 j}$$

and

$$\sum_{a_i \leqslant x} \nu(a_i) > c_3\big(A(x)\big)^2 > c_4 A(x) \log x.$$

Actually from the prime number theorem $a_j \sim e^j$, and we can find an asymptotic estimate for the left hand sum.

In view of these facts, we make the following

CONJECTURE (1). *There is an absolute constant $0 < c < 1$ so that for any sequence A whatsoever*

$$\sum_{a_i \leqslant x} \nu(a_i) \leqslant \big(1+o(1)\big) A(x) \log\log x + O(x^c).$$

Similarly for $\sum_{a_i \leqslant x} \nu^k(a_i)$. Indeed perhaps we can replace $O(x^c)$ by $O_\varepsilon(x^\varepsilon)$ for any $\varepsilon > 0$. Let us, for example, consider the following model for

(1) Note added in proof: Prof. Erdös has informed me of a result which shows this to be false.

generating random sequences of integers used by Erdös [4] and Erdös and Rényi [5](4).

Let Ω be the cartesian product of a denumerable number of copies of the set $\{0, 1\}$. We define on the jth copy a measure which has value μ_j on $\{1\}$, and $1-\mu_j$ on $\{0\}$, where $\mu_j \to 0$ as $j \to \infty$. This induces a measure on S in a natural way. We now map the set of all sequences of integers $1 < a_1 < a_2 \ldots$ into Ω by taking $(a_1, a_2, \ldots)$ into the point with 1 as the a_1th, a_2th, ... coordinates and zeros elsewhere. Thus we have a measure on the space of all sequences of integers. Speaking probabilistically (as we shall for convenience) we have independent random variables $\xi_1, \xi_2, \ldots$ assuming the values 0, 1 with probabilities $1-\mu_j, \mu_j$ for ξ_j, $j = 1, 2, \ldots$, respectively. We denote $\sum_{i \leqslant n} \mu_i$ by $M(n)$.

We can now prove various results.

THEOREM 3. (i) *Let*

$$\frac{c_1}{q} M(n) < \sum_{\substack{j \leqslant n \\ q \mid j}} \mu_j < \frac{c_2}{q} M(n)$$

hold for all $n \geqslant 1$ and $q < \big(M(n)\big)^{c_3}$ (for some $c_3 > 0$). Then almost all sequences A (in the above measure sense) satisfy

$$\sum_{a_i \leqslant x} \nu^k(a_i) \leqslant \big(1+o(1)\big) A(x) (\log\log x)^k.$$

(ii) *If in addition we assume that, uniformly for $q \leqslant \big(M(n)\big)^{c_4}$, and some $c_5 > 0$,*

$$\sum_{\substack{j \leqslant n \\ q \mid j}} \mu_j = \frac{M(n)}{q}\Big(1+O\big\{\big(M(n)\big)^{-c_5}\big\}\Big),$$

then almost all sequences A satisfy

$$\sum_{a_i \leqslant x} \nu^k(a_i) \sim A(x) (\log\log x)^k.$$

In both cases we assume that

$$M(n) > \exp(\lambda_n \log n / \log\log n), \qquad \lambda_n \to \infty.$$

COROLLARY. *Given $0 < \alpha < 1$ we can find a sequence of integers A satisfying*

(i) $$A(x) \sim \alpha^{-1} x^\alpha,$$

(ii) $$\sum_{a_i \leqslant x} \nu^k(a_i) \sim A(x) (\log\log x)^k.$$

(4) For a detailed account, see *Sequences* by H. Halberstam and K. F. Roth (Oxford 1966).

The proof of these results rests upon the following lemma which is perhaps of independent interest.

LEMMA 9. *Let $\{\mu_i\}$ be a sequence of non-negative real numbers with $M(n) = \sum_{i\leqslant n} \mu_i$. Let*

$$\sum_{i\leqslant n/q} \mu_{iq} = \frac{1}{q}\{M(n)+O(M(n))^{c_6}\}$$

uniformly for $q < (M(n))^{c_7}$, $0 < c_6, c_7 < 1$. Let $M(n) > (\log n)^{c(c_6,c_7)}$ hold. Then we can find a sequence of integers A satisfying

(i) $$A(x) = M(x)\{1+O(\varepsilon_{x,1}^{1/3})\},$$

(ii) $$\sum_{\substack{a_i\leqslant x\\ a_i\equiv 0 \pmod q}} 1 = \frac{A(x)}{q}\{1+O(\varepsilon_{x,q}^{1/3})\},$$

uniformly for $q < (M(x))^{c_8}$. Here q can be restricted (for the μ_i and a_j simultaneously) to a class of integers if desired. We may take

$$\varepsilon_{x,q} = \operatorname{Max}\Big((M(x))^{-c_9}, \sum_{\nu\leqslant x/q}\mu_{\nu q}^2 \Big/ \sum_{\nu\leqslant x/q}\mu_{\nu q}\Big).$$

Actually the proof can be made to give errors involving $O_\varepsilon(\varepsilon_{x,q}^{1-\varepsilon})$ for any fixed $\varepsilon > 0$. We do not do this however since the result as stated allows us to quote one of our previous lemmas.

Proof of Lemma 9. Let $\mu(\ldots)$ denote the probability that the event ... in brackets occurs. Then if $k \leqslant n/q$,

$$\begin{aligned}\mu\Big(\sum_{\substack{a_i\leqslant n\\ a_i\equiv 0 \pmod q}} 1 = k\Big) &= \sum_{1\leqslant j_1<j_2<\ldots<j_k\leqslant n/q}\ \prod_{i=1}^{k}\mu_{j_i q}\prod_{\substack{r\leqslant n/q\\ r\neq j_i}}(1-\mu_{rq})\\ &= \prod_{r\leqslant n/q}(1-\mu_{rq})\sum_{1\leqslant j_1<j_2<\ldots<j_k\leqslant n/q}\ \prod_{i=1}^{k}\mu_{j_i q}(1-\mu_{j_i q})^{-1}\\ &\leqslant \prod_{r\leqslant n/q}(1-\mu_{rq})\cdot(k!)^{-1}\Big(\sum_{j\leqslant n/q}\mu_{jq}(1-\mu_{jq})^{-1}\Big)^k.\end{aligned}$$

Hence if z is real and non-negative

$$\sum_{k=0}^{\infty} z^k \mu\Big(\sum_{\substack{a_i\leqslant n\\ a_i\equiv 0 \pmod q}} 1 = k\Big) \leqslant \prod_{r\leqslant n/q}(1-\mu_{rq})\exp\Big(z\sum_{j\leqslant n/q}\mu_{jq}(1-\mu_{jq})^{-1}\Big).$$

Note that

$$\sum_{j\leqslant n/q}\mu_{jq}(1-\mu_{jq})^{-1} \geqslant \sum_{j\leqslant n/q}\mu_{jq} > q^{-1}\big(M(n)-c(M(n))^{c_6}\big) > (M(n))^{c_{10}}$$

provided

$$q \leqslant (M(n))^{c_{11}}.$$

Taking $\varepsilon_{n,q} = \operatorname{Min}\big(M(n)^{-c_9}, \sum_{\nu\leqslant n/q}\mu_{\nu q}^2 / \sum_{\nu\leqslant n/q}\mu_{\nu q}\big)$ in Lemma 5 we see that, with trivial alterations, the proof shows that

$$\begin{aligned}\mu\Big(\Big|\sum_{\substack{a_i\leqslant n\\ a_i\equiv 0 \pmod q}} 1 - M_q(n)\Big| > \varepsilon_{n,q}^{1/3} M_q(n)\Big)&\\ \leqslant c_{12}\prod_{r\leqslant n/q}(1-\mu_{rq})\exp\Big(\Big\{1-\frac{1}{8}\varepsilon_{n,q}^{2/3}\Big\}M_q(n)\Big),&\end{aligned}$$

where $M_q(n)$ denotes $\sum_{r\leqslant n/q}\mu_{rq}(1-\mu_{rq})^{-1}$.

We note that $\mu_j \to 0$ as $j\to\infty$; hence given $\varepsilon > 0$ we can find $C(\varepsilon) > 0$ so that $\mu_j < \varepsilon$ if $j > C(\varepsilon)$. Thus, *uniformly* for all q under consideration,

$$\sum_{\nu\leqslant n/q}\mu_{\nu q}^3 \leqslant \sum_{\nu\leqslant C(\varepsilon)}\mu_\nu^2 + \varepsilon\sum_{\nu\leqslant n/q}\mu_{\nu q},$$

and so $\sum_{\nu\leqslant n/q}\mu_{\nu q}^2 / \sum_{\nu\leqslant n/q}\mu_{\nu q} \to 0$ *uniformly* for all $q = q(n)$ satisfying $1 < q < (M(n))^{c_{11}}$. Now

$$\prod_{r\leqslant n/q}(1-\mu_{rq})\exp\big(M_q(n)\big) < c_{13}\exp\Big(\sum_{\nu\leqslant n/q}\mu_{\nu q}^2\Big) = c_{13}\exp\big(o\{\varepsilon_{n,q}^{2/3}M_q(n)\}\big).$$

Hence the probability $\mathfrak{p}_n$ that $\big|\sum_{\substack{a_i\leqslant n\\ q\mid a_i}} 1 - M_q(n)\big| > \varepsilon_{n,q}^{1/3}M_q(n)$ should hold for *any* $q \leqslant (M(n))^{c_{14}}$ does not exceed

$$\begin{aligned}c_{15}\sum_{q\leqslant (M(n))^{c_{14}}}\exp\big(-\varepsilon_{n,q}^{2/3}M_q(n)/16\big) &< c_{15}\sum_{q\leqslant (M(n))^{c_{14}}}\exp\big(-(M(n))^{c_{16}}\big)\\ &< \exp\big(-(M(n))^{c_{16}}/2\big)\\ &< \exp(-2\log n) = n^{-2},\end{aligned}$$

provided that c_{14} is sufficiently small. For if this holds

$$\varepsilon_{n,q}^{2/3}M_q(n)/16 > \big(M_q(n)\big)^{c_{17}} \geqslant \big(M(n)/q\big)^{c_{17}} > (M(n))^{c_{18}} > 4\log n.$$

Hence $\sum_{n=1}^{\infty}\mathfrak{p}_n < \infty$ and by the Borel-Cantelli lemma (see [10] for example) we have that with probability 1,

$$\Big|\sum_{\substack{a_i\leqslant n\\ a_i\equiv 0 \pmod q}} 1 - M_q(n)\Big| \leqslant \varepsilon_{n,q}^{1/3}M_q(n) \qquad (n > n_0)$$

uniformly for $q < (M(n))^{c_8}$. Taking $q = 1$ we obtain (i) and using this for other values of q we obtain (ii). Note that even if we restrict q to a class of integers the result concerning $\sum_{\nu\leqslant n/q}\mu_{\nu q}$ holds trivially with $q = 1$, so that (i) holds always. This completes the proof of the lemma.

Proof of Theorem 3 (ii). We prove the case $k=1$ for simplicity, the higher powers being reached with only slightly more complication. We have

$$\sum_{a_i\leqslant n}\nu(a_i)=\sum_{a_i\leqslant n}\Big(\sum_{\substack{p\mid a_i\\ p\leqslant\exp(\lambda_n^{1/2}\log n/\log\log n)}}1+\sum_{\substack{p\mid a_i\\ p>\exp(\lambda_n^{1/2}\log n/\log\log n)}}1\Big)=\Sigma_1+\Sigma_2,$$

say. Using our Lemma 9, we see that with probability 1,

$$\begin{aligned}\Sigma_1&=\sum_{p\leqslant\exp(\lambda_n^{1/2}\log n/\log\log n)}\ \sum_{\substack{a_i\leqslant n\\ a_i\equiv 0\,(\mathrm{mod}\,p)}}1\\&=\sum_{p\leqslant\exp(\lambda_n^{1/2}\log n/\log\log n)}p^{-1}A(n)\{1+O(\operatorname*{Min}_p\varepsilon_{n,p}^{1/3})\}\\&=\big(1+o(1)\big)A(n)\{\log(\lambda_n^{1/2}\log n/\log\log n)+O(1)\}\sim A(n)\log\log n,\end{aligned}$$

since $\varepsilon_{n,p}^{1/3}\to 0$ uniformly for the primes indicated by $\sum_p$, namely those not exceeding $\exp(\lambda_n^{1/2}\log n/\log\log n)<\big(M(n)\big)^{c_{14}}$ if $n>n_0(c_{14})$.

Moreover, the number of prime factors of a_i which exceed $\exp(\lambda_n^{1/2}\log n/\log\log n)$ is clearly $\leqslant\lambda_n^{1/2}\log\log n$, so that $\Sigma_2=o\big(A(n)\log\log n\big)$.

The result (ii) is now clear.

Proof of Theorem 3 (i). This can be proved using a method on the lines of Lemma 9. We adjust that proof to show that with probability 1 we have, uniformly for $q<\big(M(n)\big)^{c_{19}}$,

$$\Big|\sum_{\substack{a_i\leqslant n\\ a_i\equiv 0\,(\mathrm{mod}\,q)}}1-M_q(n)\Big|<c_{20}M_q(n)\qquad(n>n_0)$$

where $c_{20}>0$ is absolute. Then by modifying Lemma 7, we see that, for each such sequence A,

$$\sum_{a_i\leqslant x}\nu_1^k(a_i)<c_{21}A(x)(\log\log x+c_{22}k)^k,$$

where $\nu_1(m)$ indicates that we count only those prime divisors of m not exceeding $x^{1/(k+1)}$. Hence we see, by using Hölder's inequality with a high exponent as in Lemma 8, that

$$\sum_{a_i\leqslant x}\Big(\sum_{\substack{p\mid a_i\\ p\leqslant\exp(\lambda_n^{1/2}\log n/\log\log n)}}1\Big)^k\leqslant\big(1+o(1)\big)A(x)(\log\log x)^k.$$

Clearly we can remove this restriction on p since this introduces sums which are typically

$$\lambda_n^{1/2}\sum_{a_i\leqslant x}(\log\log x)^k=o\big(A(x)(\log\log x)^k\big),\qquad k\geqslant 1.$$

The practical value of (i) is that it is likely to be quite difficult to find a $\{\mu_i\}$ which will satisfy the conditions of Theorem 3 (ii). In this connection we note that if we weaken the hypothesis of Lemma 9 we can still obtain asymptotic estimates of (i) and (ii)-type. If we aim only for $A(n)\sim M(n)$ and similar results, we can replace the condition on $\sum_{\nu\leqslant n/q}\mu_{\nu q}$ by $\sim M(n)/q$ uniformly for q.

Proof of Corollary. We take $\mu_i=i^{a-1}$. Then

$$\begin{aligned}\sum_{i\leqslant n/q}\mu_{iq}&=q^{a-1}\sum_{i\leqslant n/q}i^{a-1}=q^{a-1}\big(a^{-1}(n/q)+O(1)\big)\\&=(aq)^{-1}n^a+O(q^{-1+a})=(aq)^{-1}n^a\big(1+O(n^{-\delta})\big),\end{aligned}$$

provided $q<n^{c(a,\delta)}<\big(M(n)\big)^{c_{12}}$. We can then apply Theorem 3 (ii). Indeed if $2a>1$ here, our $\varepsilon_{n,q}$ is not more than

$$q^{2a-2}\sum_{i\leqslant n/q}i^{2a-2}/c_3q^{-1}n^a\sim c_4q^{2a-2}(q^{-1}n)^{2a-1}/n^aq^{-1}=c_4n^{a-1}$$

if $q<n^{c_5}$.

We note that by modifying Lemma 9 (in the manner just indicated) we can obtain for a given δ with $0<\delta<1$ a sequence A for which

$$\sum_{a_i\leqslant x}\nu^k(a_i)\sim A(x)(\log\log x)^k,\qquad k=1,2,\ldots,$$

and

$$A(x)\sim\exp\big(\log x(\log\log x)^{-1+\delta}\big)\qquad\text{as}\qquad x\to\infty.$$

We are prevented from weakening our lower bound on $M(n)$ by the fact that we have to consider a truncated $\nu(m)$ at some stage. However, since $\exp(\lambda_n\log n/\log\log n)$ is $O_\varepsilon(n^\varepsilon)$ for any fixed $\varepsilon>0$ provided $\lambda_n=o(\log\log n)$, the results are in accord with the more general conjecture, and the method used here would appear not to shed any light on the behaviour of $\sum_{a_i\leqslant x}\nu(a_i)$ for very thin sequences A.

Note that we have that in the sense of Theorem 3 (ii) almost all sequences are well Σ_H-distributed in the sense of Barban [1]. Hence, we can apply a variant of the sieve of Eratosthenes as used by Hooley [8], Lemma 4 and show for example that if $P=\prod p$, where p runs over the rational primes which satisfy $p\leqslant\exp\big((\log n)^\beta\big)$ for a fixed β, $0<\beta<1$ then

$$\sum_{\substack{a_i\leqslant n\\ (a_i,P)=1}}1=A(n)\prod_{p\mid P}(1-p^{-1})+O_C\big(A(n)(\log n)^{-C}\big),$$

for any fixed $C>0$. Then if $M(n)>(\log n)^{\Delta(\beta)}$ where $\Delta(\beta)$ is a certain

constant depending upon β, this and similar estimates show that we can construct a subsequence B of A which satisfies, for an infinity of values of x,

(i) $B(n) \sim Cn^{\alpha}(\log n)^{-\beta} \sim CA(n)(\log n)^{-\beta}$,

(ii) $\sum_{b_i \leqslant n} \nu^k(b_i) \sim (1-\beta)^k B(n)(\log\log n)^k$,

as $x \to \infty$ through integral powers of e.

We do this by analogy with the earlier limiting example. Thus, we can find such a subsequence of almost all sequences A. Clearly the set of sequences B has measure zero with respect to the measure induced by the μ_i corresponding to $M(n)$.

References

[1] М. Б. Барбан, *Мультипликативные функции от Σ_R-равнораспределенных последовательностей*, Известия Акад. Наук. Узбек., Серил физ.-мат. наук 6 (1964), pp. 13-19.

[2] T. G. van der Corput, *Une inégalité relative au nombre des diviseurs*, Proc. K. Neder. Akad. van. Wet. Amsterdam 42 (1939), pp. 547-553.

[3] P. Erdös, *On the sum* $\sum_{k=1}^{x} d(f(k))$, J.Lond. Math. Soc. 27 (1952), pp. 7-15.

[4] — *Problems and results in additive number theory*, Colloque sur la théorie des nombres, Bruxelles 1955, pp. 127-137.

[5] P. Erdös and A. Rényi, *Additive properties of random sequences of positive integers*, Acta Arith. 6 (1960), pp. 83-110.

[6] H. Halberstam, *On the distribution of additive number-theoretic functions I-III*, J. Lond. Math. Soc. 30 (1955), pp. 43-53; 31 (1956), pp. 1-14; pp. 15-28.

[7] G. H. Hardy and S. Ramanujan, *The normal number of prime factors of a number n*, Quart. J. Math. 48 (1917), pp. 76-92.

[8] C. Hooley, *On the representation of numbers as the sum of two squares and a prime*, Acta Math. 97 (1957), pp. 189-210.

[9] J. Kubilius, *Probabilistic methods in the theory of numbers*, A. M. S. Translations no. 11, 1964.

[10] A. Kolmogoroff, *Grundbegriffe der Wahrscheinlichkeitsrechnung*, Berlin 1933.

[11] T. Nagell, *Généralisation d'un théorème de Tchebycheff*, Journ. de Math. 8 Série, 4 (1921), pp. 343-356.

[12] K. Prachar, *Primzahlverteilung*, Berlin 1957.

[13] A. Selberg, *Note on a paper of L. G. Sathe*, J. Indian Math. Soc. N. S. 18 (1954), pp. 83-87.

[14] E. C. Titchmarsh, *The theory of the Riemann zeta function*, Oxford 1951.

UNIVERSITY OF NOTTINGHAM

Reçu par la Rédaction le 20. 8. 1966

ACTA ARITHMETICA
XII (1967)

The cyclotomy of Kloosterman sums

by

D. H. and Emma Lehmer (Berkeley, Calif.)

1. Introduction. Historically the Kloosterman sum arose as a coefficient in the expansion of certain series giving the number of representations of integers by various quadratic forms. Thus it was that questions of the order of magnitude of the Kloosterman sums were uppermost in the minds of writers of the many papers on these sums. In this paper we try to indicate that Kloosterman sums have rather interesting intrinsic properties not depending on their estimated magnitude. In particular we show that there is a complete theory, parallel to the classical theory of cyclotomy, in which the Kloosterman sums now play the role of the roots of unity.

To be more precise some notation will be needed to which we adhere throughout the paper.

Let p be an odd prime and let

$$\varepsilon(\nu) = \exp\{2\pi i\nu/p\}. \tag{1.0}$$

The ordinary Kloosterman sum will be denoted as usual by

$$S(h) = \sum_{x=1}^{p-1} \varepsilon(x+h\bar{x}) \qquad (x\bar{x} \equiv 1 \pmod p) \tag{1.1}$$

so that

$$S(0) = \sum_{x=1}^{p-1} \varepsilon(x) = -1. \tag{1.2}$$

In § 3 we investigate sums of products of Kloosterman sums extending the early results of Salié [10]. The methods used here apply equally well to the more general Kloosterman sum

$$S_k(h) = \sum_{x=1}^{p-1} \varepsilon(x+hx^k) \tag{1.3}$$