ACTA ARITHMETICA
XXXVII (1980)

Additive functions with restricted growth on the numbers of the form $p+1$

by

E. WIRSING (Ulm)

1. In 1974 Elliott [3], elaborating on his earlier paper [2] and thereby solving a problem of Kátai [6], proved the existence of constants A, B, C, such that for every completely additive function f and every $n \geqslant C$ the following inequality holds:

$$|f(n)| \leqslant A \max_{p\in P, p\leqslant n^B} |f(p+1)|. \tag{1}$$

Here P is the set of all primes and a function $f\colon N \to C$ is called completely additive if $f(ab) = f(a)+f(b)$ for all a, b. This inequality implies in particular, that a completely additive function f must vanish identically if $f(p+1) = o(\log p)$.

In the more general case of additive functions, that is if $f(ab) = f(a)+ +f(b)$ for $(a, b) = 1$, he has a weaker result:

$$|f(n)| \leqslant A \max_{p\leqslant n^B} |f(p+1)| + A \max_{m\leqslant \log^B n} |f(m)|.$$

In this paper we shall prove (1), and actually a little more, for all additive functions.

THEOREM 1. *There are constants A, B such that for all additive functions f and all $n \in N$ the inequality*

$$|f(n)| \leqslant A \max_{\substack{n\leqslant p+1\leqslant n^B \\ p\in P}} |f(p+1)| \tag{2}$$

holds.

Except for the lower bound $p+1 \geqslant n$ this is again a conjecture of Kátai's [7]. We could even increase this bound to become $p > n^c$ at the cost of larger $A = A(c)$, $B = B(c)$.

Uniqueness statements for additive functions are usually related to, if not equivalent with, statements on multiplicative representations of numbers, see Wolke [10]. We give here a theorem which renders Theorem 1 obvious as far as completely additive functions are concerned.

THEOREM 2. *There are constants c_1, c_2 such that for every $n \in N$ there is a representation*

$$n^a = \prod_{i=1}^{b} (p_i+1)^{\varepsilon_i}, \quad p_i \in \boldsymbol{P},$$

where $a \leqslant c_1$, $b \leqslant c_1$, $\varepsilon_i \in \{+1, -1\}$, $n \leqslant p_i+1 \leqslant n^{c_2}$.

Very likely this theorem is true with small values of a and b. The case $a=1$, $b=2$, $\varepsilon_1 = 1$, $\varepsilon_2 = -1$ is a generalized prime-twin conjecture for which there is presently little hope of resolution. But $a = 1$, $b=3$ may just be accessible for modern sieve theory.

As an obvious corollary we may mention that for multiplicative functions $f(n) = O(\log^a n)$ and $f(p+1) = O(\log^a(p+1))$ are equivalent. This is still true if $a < 0$ but it is rather a weak statement then. Actually, by Theorem 1 $f(p+1) \to 0$ and $f(n) \to 0$ are equivalent but the only additive function with this property is the null function: Let n be arbitrary and let m tend to infinity while $(m,n) = 1$; then $f(n) = f(mn) - -f(m) \to 0$, whence $f(n) = 0$. So we have

COROLLARY 1. *If f is additive and $f(p+1) \to 0$, then $f = 0$ identically.*

The case $a = 0$ corresponds to the statement that '$f(p+1) = O(1)$' and '$f(n) = O(1)$' are equivalent. This again allows for a refinement out of itself, so to speak.

COROLLARY 2. *Let f be additive, real valued and suppose that $|f(p+1)|$ is bounded. Then*

$$\overline{\lim} f(2n) = \overline{\lim} f(p+1), \quad \underline{\lim} f(2n) = \underline{\lim} f(p+1).$$

This is essentially due to J. Meyer [8] who uses results from Elliott [2] and lower sieve estimates for his deduction. Corollary 2 of course includes Corollary 1.

Proof. By Theorem 1 we know that $f(n)$ is bounded. Therefore

$$\sum_p \sup_\nu |f(p^\nu)|$$

converges, otherwise an $n = \prod p_i^{\nu_i}$ with arbitrarily large $f(n)$ could be found. Choose x and m so that

$$\sum_{p \geqslant x} \sup_\nu |f(p^\nu)| \leqslant \varepsilon,$$

$$f(2m) \geqslant \overline{\lim} f(2n) - \varepsilon$$

and let

$$2m = \prod_{i=1}^{k} p_i^{\nu_i}.$$

By Dirichlet's Theorem there are infinitely many primes p such that

$$p+1 \equiv 2m \bmod \Big(\prod_{i=1}^{k} p_i^{\nu_i+1}\Big)$$

and

$$p+1 \not\equiv 0 \bmod p' \quad \text{for all } p' \leqslant x,\ p' \notin \{p_1, \ldots, p_k\}.$$

Then $p+1 = 2mq$, where $(q, 2m) = 1$ and no prime divisor of q is $\leqslant x$. Hence $f(q) \geqslant -\varepsilon$, $f(p+1) \geqslant f(2m) - \varepsilon \geqslant \overline{\lim} f(2m) - 2\varepsilon$.

2. Sketch of the proofs. We define a relation

$$k \sim m :\Leftrightarrow km-1 \in \boldsymbol{P}, \quad (k, m) = 1$$

and call such numbers k and m *relatives of first degree*. Numbers k, l are called relatives of *second degree* if there is an m such that $k \sim m \sim l$.

Let f be additive and $|f(p+1)|$ 'small' for all $p \in \boldsymbol{P}$. If $k \sim m$, then $km = p+1$, $f(k)+f(m) = f(p+1)$, hence $f(k) \approx -f(m)$. Therefore, if k and l are relatives of second degree, $f(k) \approx f(l)$. For fixed k and large y there are $\gg \dfrac{y}{\log y}$ relatives of first degree $m \leqslant y$, and therefore $\gg \dfrac{xy}{\log x \log y}$ relatives of second degree $l \leqslant x$ (x large compared to y) where only $m \leqslant y$ are allowed to mediate and every l is counted with the number of mediating m as its multiplicity.

Given k and l this multiplicity is the number of a certain type of prime twins and therefore accessible to a good upper estimate by the sieve method. Together these estimates imply that each k has at least γx relatives $l \leqslant x$ of second degree ($\gamma = \text{const} > 0$), now counted without multiplicity. For all these l, as we have seen, $f(l)$ approximates $f(k)$. If we have $k_1, \ldots, k_N$ such that $f(k_1), \ldots, f(k_N)$ are 'essentially different' then the corresponding sets of relatives must be disjoint, whence $N \leqslant \gamma^{-1}$. In the case of completely additive f it is enough to have one k with a 'big' value of $f(k)$, then for $k_i = k^i$ the $f(k_i) = if(k)$ are essentially different for $i \leqslant N$ and arbitrary N so that we gain a contradiction from the assumption of a big value $f(k)$.

In the case of (not completely) additive f we use Linnik's Theorem on the smallest prime in a progression to construct k_i with similar properties.

The main difficulty in carrying through the sketched proof arises from the fact that in view of our proposition we are not allowed to use a y greater than some fixed power of k. Fortunately, by the work of Fogels [4] (see Elliott [3]) or more conveniently Gallagher [5], lower estimates for $\pi(y; k, r)$ with such a small y have become available.

There are many parallels between Elliott's method and ours. The main differences seem to be that we measure sets of integers by their cardinality rather than the sum of reciprocals, and our use of Linnik's Theorem.

3. Proofs. We begin with a list of notations:

P : the set of rational primes,

$\pi(x; k, r)$: the number of primes $p \leqslant x$, $p \equiv r \bmod k$,

$E(x, k) := \max\limits_{y\leqslant x, (r,k)=1} \left|\pi(y; k, r) - \frac{1}{\varphi(k)} \operatorname{li} y\right|$,

$k \sim m : \Leftrightarrow km-1 \in P$, $(k, m) = 1$,

$M_k := \{m; m \sim k\}$,

$S_{kl} := M_k \cap M_l$,

$M_k(x)$, $S_{kl}(x)$: the corresponding counting functions,

$L_k(x, y)$: the number of $l \leqslant x$ with $S_{kl}(y) > 0$,

x_ν, c_ν : positive constants that may be enlarged without affecting the defining inequality,

γ_ν : positive constants that may be diminished without affecting the defining inequality.

Voluminous summation conditions will be given following the sum and enclosed in $\{\ldots\}$.

Lemma 1. *There are x_0 and γ_1 such that*

$$\pi(x; k, r) \geqslant \frac{x}{4\varphi(k)\log x} \tag{3}$$

for all $x \geqslant x_0$, $k \leqslant x^{\gamma_1}$, $(r, k) = 1$ with the possible exception of the multiples k of a number $q_1(x)$. We have $q_1(x) \geqslant 2$ and $q_1(x') = q_1(x)$ if $x \leqslant x' \leqslant x^2$ provided both q_1 exist.

Proof. According to Gallagher [5], Theorem 7, there are γ_2, γ_3 such that

$$\Big|\sum_x^{x+h} \log p - h\Big| + \sum_{\substack{2\leqslant q\leqslant Q\\ q\neq q_1}} \sum_\chi^* \Big|\sum_x^{x+h} \chi(p)\log p\Big| = O\big(xe^{-\gamma_3\frac{\log x}{\log Q}}\big) \tag{4}$$

if

$$\sqrt{\log x} \leqslant \log Q \leqslant \gamma_2 \log x, \quad x/Q \leqslant h \leqslant x.$$

Here as usual $\sum^*$ denotes summation over all primitive characters mod q and q_1 is the possibly existing "exceptional modulus" $q_1 \leqslant Q$ for which there is a primitive character χ_1 with a zero

$$\sigma_1 > 1 - \frac{\delta}{\log Q} \tag{5}$$

of $L(s, \chi_1)$. The positive constant δ can be given any small value, it determines γ_2, γ_3, the O-constant in (4) and the notion of exceptionality.

If we take $h = x$ and $Q = (2x)^{\gamma_1}$ the right hand side of (4) becomes $O(xe^{-\gamma_3/\gamma_1})$ and therefore $\leqslant \frac{1}{2}x$ if γ_1 is chosen small enough. Now by the usual argument one finds

$$\Big|\sum_{\substack{x\\ p\equiv r \bmod k}}^{2x} \log p - \frac{x}{\varphi(k)}\Big| \leqslant \frac{1}{\varphi(k)}\Big(\Big|\sum_x^{2x}\log p - x\Big| + \sum_{\substack{q|k\\ q>1}} \sum_\chi^* \Big|\sum_x^{2x}\chi(p)\log p\Big|\Big) \leqslant \frac{x}{2\varphi(k)},$$

$$\pi(2x; k, r) \geqslant \frac{x}{2\varphi(k)\log 2x},$$

provided $q_1 \nmid k$ and $k \leqslant Q$. Replacing $2x$ by x and redefining $Q := x^{\gamma_1}$ we obtain (3).

As is well known (Landau) there is at most one primitive character χ_1 with modulus $q_1 \leqslant Q$ and with a zero σ of $L(s, \chi_1)$ satisfying (5), if $\delta \leqslant \gamma_4$, say. Consequently, if $\delta := \frac{1}{2}\gamma_4$ then exceptional moduli $q_1 \leqslant Q$ and $q_1' \leqslant Q'$ will coincide for $Q \leqslant Q' \leqslant Q^2$. Because of $Q = x^{\gamma_1}$ this corresponds to saying $x \leqslant x' \leqslant x^2$. Obviously $q_1 \geqslant 2$ since $\zeta(s) \neq 0$ in $0 < s < 1$.

Lemma 2. *Let $x \geqslant x_0+1$, $k \leqslant x^{\gamma_1/2}$, $q_1 \nmid k^2$. Then*

$$M_k(x) \geqslant \frac{x}{5\log x},$$

where q_1 is the possibly existing $q_1(x')$ for $x-1 \leqslant x' \leqslant (x-1)^2$.

Proof.

$$M_k(x) = \sum_{m\leqslant x} 1 \qquad \{mk-1 \in P, (m, k) = 1\}$$

$$= \sum_{p\leqslant kx-1} 1 \qquad \Big\{p \in P, p \equiv -1 \bmod k, \Big(\frac{p+1}{k}, k\Big) = 1\Big\}$$

$$= \sum_{r \bmod k^2} \pi(kx-1; k^2, r) \qquad \{(r+1, k^2) = k\}.$$

Because of $kx-1 \geqslant x_0$, $k^2 \leqslant x^{\gamma_1}$ and $x-1 \leqslant kx-1 \leqslant (x-1)^2$ Lemma 1 applies to each term in the last sum, always with the same — if any —

exceptional modulus:

$$M_k(x) \geqslant \frac{kx-1}{4\varphi(k^2)\log(kx-1)} \sum_{s \bmod k^2} 1 \qquad \{(s, k^2) = k\}$$

$$= \frac{kx-1}{4k\log(kx-1)} \geqslant \frac{x-1}{4\log kx} \geqslant \frac{1-1/x}{1+\gamma_1/2}\,\frac{x}{4\log x}.$$

If x_0 is taken big and γ_1 small enough our proposition follows.

Lemma 3. *Let $x \geqslant x_1$, x_1 sufficiently large, and $y = x^{1/4}$. Then for all $k \leqslant x^{\gamma_1/8}$ with $q_1 \nmid k^2$ one has*

$$\sum_{\substack{l \leqslant x \\ l \neq k}} S_{kl}(y) \geqslant \frac{xy}{2\log^2 x}.$$

Proof. Firstly

$$M_m(x) = \sum_{l \leqslant x} 1 \qquad \{lm-1 \in \boldsymbol{P}, (l, m) = 1\}$$

$$= \sum_{d|m} \mu(d) \sum_{l \leqslant x} 1 \qquad \{lm-1 \in \boldsymbol{P}, d|l\}$$

$$= \sum_{d|m} \mu(d)\, \pi(mx-1; md, -1)$$

$$\geqslant \sum_{d|m} \left(\frac{\mu(d)}{\varphi(md)} \operatorname{li}(mx-1) - |\mu(d)|\, E(mx, md)\right).$$

Here $\sum_{d|m} \mu(d)/\varphi(md) = 1/m$ because of $\varphi(md) = d\varphi(m)$ and $\sum \mu(d)/d = \varphi(m)/m$. Furthermore for large x

$$\frac{1}{m} \operatorname{li}(mx-1) \geqslant (1-\varepsilon)\frac{x}{\log(mx)},$$

therefore

$$M_m(x) \geqslant \frac{5}{6}\,\frac{x}{\log(mx)} - \sum_{d|m} |\mu(d)|\, E(mx, md) \tag{6}$$

if $x \geqslant x_1$.

Secondly

$$\sum_{l \leqslant x} S_{kl}(y) = \sum_{l,m} 1 \qquad \{l \leqslant x, m \leqslant y, k \sim m \sim l\}$$

$$= \sum_{m \leqslant y, m \sim k} \; \sum_{l \leqslant x, l \sim m} 1 = \sum_{m \leqslant y, m \sim k} M_m(x).$$

Using (6) and $y = x^{1/4}$ we see that

$$\sum_{l \leqslant x} S_{kl}(x) \geqslant \sum_{\substack{m \leqslant y \\ m \sim k}} \frac{2x}{3\log x} - \sum_{\substack{m \leqslant y \\ d|m}} |\mu(d)|\, E(xy, md) \tag{7}$$

$$= \frac{2x}{3\log x} M_k(y) - \sum_{n \leqslant y^2} \psi(n)\, E(xy, n),$$

where

$$\psi(n) := \sum_{\substack{md=n \\ d|m}} |\mu(d)| = \sum_{d^2|n} |\mu(d)|$$

is a multiplicative function. Since $\psi(p) = 1$, $\psi(p^\nu) = 2$ for $\nu \geqslant 2$ one finds

$$\sum_{n \leqslant y^2} \frac{\psi^2(n)}{n} \leqslant \prod_{p \leqslant y^2} \left(1 + \frac{1}{p} + \frac{4}{p^2} + \frac{4}{p^3} + \ldots\right)$$

$$\leqslant \prod_{p \leqslant y^2} \left(1 - \frac{1}{p}\right)^{-1} \prod_{p} \left(1 + \frac{3}{p^2}\right) \ll \log x.$$

Therefore

$$\sum_{n \leqslant y^2} \psi(n)\, E(xy, n) \leqslant \left(\sum_{n \leqslant y^2} \frac{\psi^2(n)}{n}\right)^{1/2} \left(\sum_{n \leqslant y^2} n E^2(xy, n)\right)^{1/2} \tag{8}$$

$$\ll \left(\log x \sum_{n \leqslant y^2} n E^2(xy, n)\right)^{1/2}.$$

With the trivial estimate $E(z, n) \ll z/n$ for $z \geqslant n$ and the deep Bombieri–Vinogradov Theorem, see [1], of which the weakened version

$$\sum_{n \leqslant z^{2/5}} E(z, n) \ll \frac{z}{\log^7 z}$$

suffices for us, (8) turns into

$$\sum_{n \leqslant y^2} \psi(n)\, E(xy, n) \ll \frac{xy}{\log^3 x}$$

(note that $y^2 = (xy)^{2/5}$).

Since, by assumption, $q_1 \nmid k^2$ and $k \leqslant x^{\gamma_1/8} = y^{\gamma_1/2}$ we may apply Lemma 2 to $M_k(y)$ in (7). Thereby

$$\sum_{l \leqslant x} S_{kl}(y) \geqslant \frac{2xy}{15\log x \log y} - O\left(\frac{xy}{\log^3 x}\right) = \frac{8xy}{15\log^2 x} - O\left(\frac{xy}{\log^3 x}\right).$$

Now, obviously, $S_{kk}(y) \leqslant y$ and the proposition follows for sufficiently large x_1.

LEMMA 4. *If* $y \geqslant 2$ *and* $k \neq l$ *then*

$$S_{kl}(y) \ll \frac{|k-l|}{\varphi(|k-l|)} \cdot \frac{y}{\log^2 y},$$

uniformly in k *and* l.

This lemma can be deduced with any one of the standard sieve methods (Brun, Selberg, Montgomery). For every prime p the set

$$S_{kl} = \{m;\ mk-1 \in \boldsymbol{P},\ ml-1 \in \boldsymbol{P},\ (m, kl) = 1\}$$

contains no $m \equiv 0 \bmod p$ if $p|k$, and at most one $m \equiv \frac{1}{k} \bmod p$ if $p \nmid k$; similarly no $m \equiv 0 \bmod p$ if $p|l$ and at most one $m \equiv \frac{1}{l} \bmod p$ if $p \nmid l$. Given k, l and p these two forbidden classes coincide if and only if $k \equiv l \bmod p$. If all elements of all these residue classes for all $p \leqslant \sqrt{y}$ are cancelled from the intervall $[1, y]$ the number of the remaining integers is

$$\ll y \prod_{\substack{p \leqslant \sqrt{y} \\ k \equiv l \bmod p}} \left(1-\frac{1}{p}\right) \prod_{\substack{p \leqslant \sqrt{y} \\ k \not\equiv l \bmod p}} \left(1-\frac{1}{p}\right)^2$$

$$< y \prod_{p|(k-l)} \left(1-\frac{1}{p}\right)^{-1} \prod_{p \leqslant \sqrt{y}} \left(1-\frac{1}{p}\right)^2 \ll \frac{|k-l|}{\varphi(|k-l|)} \cdot \frac{y}{\log^2 y}.$$

Unjustly cancelled are only those numbers of the form $\frac{p+1}{k}$ or $\frac{p+1}{l}$ with $p \leqslant \sqrt{y}$, less than $\sqrt{y}$ of them altogether.

LEMMA 5. *There are* γ_5, γ_6 *such that for all* $x \geqslant x_1$ *and* $k \leqslant x^{\gamma_5}$ *(except if* $q_1|k^2$*)*

$$L_k(x, y) \geqslant \gamma_6 x \qquad (y := x^{1/4}).$$

Proof. Elementary calculations or general theorems (see Wirsing [9]) yield

$$\sum_{n \leqslant x} \frac{n^2}{\varphi^2(n)} \ll x.$$

Thereby we infer from Lemma 4 for every $k \leqslant x$

$$\sum_{\substack{l \leqslant x \\ l \neq k}} S_{kl}^2(x) \ll \frac{y^2}{\log^4 y} \sum_{\substack{-k \leqslant n \leqslant x-k \\ n \neq 0}} \frac{n^2}{\varphi^2(|n|)}$$

$$\ll \frac{xy^2}{\log^4 y} \ll \frac{xy^2}{\log^4 x}.$$

For those k that are admitted in Lemma 3 one has therefore

$$\left(\frac{xy}{2\log^2 x}\right)^2 \leqslant \Big(\sum_{\substack{l \leqslant x \\ l \neq k}} S_{kl}(y)\Big)^2 \leqslant L_k(x, y) \sum_{\substack{l \leqslant x \\ l \neq k}} S_{kl}^2(y) \ll \frac{xy^2}{\log^4 x} L_k(x, y),$$

whence $L_k(x, y) \gg x$.

Proof of Theorem 2. Let c denote Linnik's constant. Then for any $n \geqslant 2$ there is a prime

$$p \equiv n-1 \bmod n^2, \quad p \leqslant n^{2c}.$$

Writing $p+1 = nn'$ we have $n' = (p+1)/n \equiv 1 \bmod n$ and therefore $(n, n') = 1$. We assume $n' \geqslant 2$ since otherwise by $n = p+1$ we have already found the desired representation. Choose N so big that

$$N\gamma_6 > 1 \quad \text{and} \quad 2^{2cN} \geqslant x_1^{\gamma_5}.$$

Then we may apply Lemma 5 to all $k = n^i$ $(i = 1, \ldots, N)$ or to all $k = (n')^i$ and $x = n^{2cN/\gamma_5}$. With these parameters, on the one hand $k \leqslant n^{2cN} \leqslant x^{\gamma_5}$, on the other $x \geqslant 4^{cN/\gamma_5} \geqslant x_1$, and not for both choices n and n' can $q_1|k^2$ since $q_1 \geqslant 2$ and $(n, n') = 1$.

Let us first assume that n is admissible. For each $i \leqslant N$ the lemma guarantees the existence of at least $\gamma_6 x$ integers $l \leqslant x$ and for each l an $m \leqslant y$ such that

(9) $$lm = p'+1, \quad km = p''+1, \quad p', p'' \in \boldsymbol{P},$$

which implies a representation

(10) $$l = \frac{p'+1}{p''+1} k = \frac{p'+1}{p''+1} n^i.$$

There are altogether at least $N\gamma_6 x > x$ such representations. Hence, there is an l that can be represented in the form (10) with two different exponents i and j, say:

$$\frac{p^{(1)}+1}{p^{(2)}+1} n^i = \frac{p^{(3)}+1}{p^{(4)}+1} n^j.$$

Assuming $i-j =: a > 0$ we find

(11) $$n^a = \frac{(p^{(2)}+1)(p^{(3)}+1)}{(p^{(1)}+1)(p^{(4)}+1)}.$$

As for the size of these primes, (9) implies

$$p'+1 = lm \leqslant xy < x^2 = n^{c_3} \qquad (c_3 := 4cN\gamma_5^{-1})$$

and

$$p''+1 = km \leqslant xy < n^{c_3}.$$

To obtain a lower bound for p', p'' we have to use a slight sharpening of Lemma 5. The definition of $L_k(x, y)$ may obviously be modified so as to count only l that are $\geqslant \sqrt{x}$, say, and the loss can be compensated by a reduction of γ_6. After this change we may infer from (9)

$$p'+1 \geqslant l \geqslant x^{1/2} = n^{cN/\gamma_5} \geqslant n.$$

Concerning p'' we have $p''+1 \geqslant k \geqslant n$ anyway.

There remains the case where n is not admissible because of $q_1|n^{2i}$ for some i. Here we have a representation of type (11) with n' instead of n, which combines with $nn' = p+1$ into

$$n^a = (p+1)^a \frac{(p^{(1)}+1)(p^{(4)}+1)}{(p^{(2)}+1)(p^{(3)}+1)}.$$

For p we know already that $p \leqslant n^{2c}$, and $p+1 \geqslant n$ follows from $p+1 \equiv n \bmod n^2$. Actually in the present case we have $n \neq p+1$, therefore $nn' \geqslant n^2+n$, $n' > n$.

Consequently $p^{(i)}+1 \geqslant n' > n$. In the other direction

$$p^{(i)} < (n')^{c_3} \leqslant n^{2cc_3}$$

follows. A possible choice for N is $[\gamma_6^{-1}+1]$; so Theorem 2 is valid with $c_1 := N+4 = [\gamma_6^{-1}+5]$ and $c_2 := 2cc_3$.

Though the proof of Theorem 1, where the completeness of additivity is dropped, follows the same line, the coprimality condition necessitates some extra care which gives our last lemma a somewhat technical appearance.

Lemma 6. *There are constants c_4, c_5, such that for every even $n \in N$ the following conditions can be satisfied with natural numbers a, b, $h_1, \ldots, h_b$, m_a, m_b and l:*

$$(12) \qquad 1 \leqslant b < a \leqslant c_4,$$

$$(13) \qquad h_i \sim n \quad \textit{for} \quad 1 \leqslant i \leqslant a,$$

$$(14) \qquad (h_i, h_j) = 1 \quad \textit{for} \quad i \neq j,$$

$$(15) \qquad n \leqslant h_i \leqslant n^{c_5},$$

$$(16) \qquad l \sim m_a \sim h_1 h_2 \ldots h_a, \quad l \sim m_b \sim h_1 h_2 \ldots h_b,$$

$$(17) \qquad n \leqslant l \leqslant n^{c_5}, \quad m_a \leqslant n^{c_5}, \quad m_b \leqslant n^{c_5}.$$

Proof. For $n = 2$ an explicit solution is $a = 2$, $b = 1$, $h_1 = 3$, $h_2 = 7$, $m_a = m_b = 2$, $l = 3$. Indeed $2\cdot 3-1 \in P$, $2\cdot 7-1 \in P$ and $2\cdot 3\cdot 7-1 \in P$.

Now we can assume $n > 2$. We fix N so big that

$$(18) \qquad (N-2)\tfrac{1}{2}\gamma_6 > 1.$$

We consider primes p_i $(i = 1, 2, \ldots, N)$ fulfilling

$$(19) \qquad p_i \equiv -n-1 \bmod n^2.$$

Then

$$h_i := \frac{p_i+1}{n} \equiv -1 \bmod n,$$

hence $h_i \geqslant n-1$ and $(h_i, n) = 1$. The h_i are odd, since $2|n$. Choosing the p_i (or h_i) successively we may demand

$$(20) \qquad p_i \equiv 1 \bmod (h_1 h_2 \ldots h_{i-1})$$

along with (19). This implies

$$(nh_i, h_1 h_2 \ldots h_{i-1}) = (2, h_1 h_2 \ldots h_{i-1}) = 1$$

and in particular (14). Linnik's Theorem guarantees the existence of p_i according to (19) and (20) such that

$$h_i < p_i \leqslant (n^2 h_1 h_2 \ldots h_{i-1})^c.$$

After a little calculation this yields

$$h_i \leqslant n^{2c(1+c)^{i-1}} \leqslant n^{c_6} \quad \text{for} \quad i \leqslant N,$$

if

$$c_6 := 2c(1+c)^{N-1}.$$

Since the h_i are coprime and $\geqslant n-1 > 1$ they differ from each other. Should one of them equal $n-1$ we cancel it and renumber the remaining ones into $h_1, \ldots, h_{N-1}$.

Now choose

$$c_5 :\geqslant \frac{c_6}{\gamma_5} N, \quad x := n^{c_5}$$

and apply Lemma 5 to $k_i := h_1 h_2 \ldots h_i$. Then $k_i \leqslant n^{c_6 N} = x^{\gamma_5}$ and, provided c_5 is big enough,

$$x \geqslant 4^{c_5} \geqslant x_1.$$

Should $q_1|(h_1 \ldots h_{N-2})^2$ then because of (14) it will suffice to cancel a suitable one of $h_1, \ldots, h_{N-1}$ (and to renumber the remaining ones) in order to ensure

$$q_1 \nmid k_i^2 \quad \text{for all } i = 1, \ldots, N-2.$$

By the lemma each of these k_i possesses no less than $\gamma_6 x$ relatives $l \leqslant x$. At least $\tfrac{1}{2}\gamma_6 x$ of them are $\geqslant \tfrac{1}{2}\gamma_6 x$. For these l

$$l \geqslant \tfrac{1}{2}\gamma_6 n^{c_5} \geqslant \tfrac{1}{2}\gamma_6 \cdot 4^{c_5-1} \cdot n \geqslant n$$

if c_5 is made large enough. The total number of $l \leqslant x$ thus represented is $\geqslant (N-2)\gamma_6 \frac{1}{2} x > x$; so two of them must coincide. Explicitly: There are a, b, m_a, m_b and l such that (12) (with $c_4 := N-2$) and (16) hold. The upper bounds (17) derive from m_a, $m_b \leqslant y < x = n^{c_5}$ and $l \leqslant x$. For the sake of simplicity also $h_i \leqslant n^{c_6}$ is weakened into $h_i \leqslant n^{c_5}$; quite apparently $c_5 > c_6$.

Proof of Theorem 1. In the first instance consider even n. Then with the notations of Lemma 6

$$\begin{aligned} nh_i &= p_i+1, & (n, h_i) &= 1, \\ m_a h_1 \dots h_a &= p'_a+1, & (m_a, h_1 \dots h_a) &= 1, \\ m_b h_1 \dots h_b &= p'_b+1, & (m_b, h_1 \dots h_b) &= 1, \\ m_a l &= p''_a+1, & (m_a, l) &= 1, \\ m_b l &= p''_b+1, & (m_b, l) &= 1. \end{aligned}$$

Using also (14) we infer

$$f(n) = f(p_i+1) - f(h_i),$$

$$(a-b)f(n) = \sum_{b+1}^{a} f(p_i+1) - f(m_a h_1 \dots h_a) + f(m_a l) + f(m_b h_1 \dots h_b) - f(m_b l),$$

(21)

$$(a-b)f(n) = \sum_{b+1}^{a} f(p_i+1) - f(p'_a+1) + f(p''_a+1) + f(p'_b+1) - f(p''_b+1).$$

Bounds for the primes concerned are derived from (15) and (17):

$$\begin{aligned} & n \leqslant nh_i = p_i+1 \leqslant n^{1+c_5}, \\ (22) \qquad & n \leqslant h_1 \leqslant p'_a+1 \leqslant (n^{c_5})^{a+1} \leqslant n^{c_5(c_4+1)}, \\ & n \leqslant l \leqslant p''_a+1 \leqslant n^{2c_5}, \end{aligned}$$

and similarly for p'_b and p''_b.

For even n Theorem 1 follows immediately from (21) and (22) and the initial remark on $n = 2$. For odd n we write

$$f(n) = f(2^s n) - f(2^s).$$

If s is chosen according to

$$n < 2^s \leqslant 2n \qquad (\leqslant n^2)$$

and the section of the theorem so far proved is applied to both terms Theorem 1 is obtained in full.

Remark (added in proof). Lemma 3 is more easily seen by another application of Lemma 2 to the individual $M_m(x)$ rather than estimating them *via* Bombieri's Theorem: Instead of $y = x^{1/4}$ take $y := x^{\gamma_1/2}$. Then we have $M_m(x) \gg x/\log x$ for all $m \leqslant y$ but those with $q_2 | m^2$. By Siegel's Theorem $q_2 \gg \log^4 y$, say; so the condition $q_2 \nmid m^2$ excludes no more than $y/\sqrt{q_2} \ll y/\log^2 y$ of the $M_k(y)$ $(\gg y/\log y)$ numbers $m \leqslant y$ with $m \sim k$. Hence

$$\sum_{l \leqslant x} S_{kl}(x) = \sum_{\substack{m \leqslant y \\ m \sim k}} M_m(x) \gg \frac{xy}{\log x \log y} \gg \frac{xy}{\log^2 x}.$$

References

[1] E. Bombieri, *Le grand crible dans la théorie analytique des nombres*, Asterisque 18, Soc. Math. de France, 1974.

[2] P. D. T. A. Elliott, *A conjecture of Kátai*, Acta Arith. 26 (1974), pp. 11–20.

[3] – *On two conjectures of Kátai*, ibid. 30 (1976), pp. 341–365.

[4] E. Fogels, *On the zeros of L-functions*, ibid. 11 (1965), pp. 67–96.

[5] P. X. Gallagher, *A large sieve density estimate near* $\sigma = 1$, Inventiones Math. 11 (1970), pp. 329–339.

[6] I. Kátai, *Some remarks on additive arithmetic functions*, Litovsk. Mat. Sb. 9 (1969), pp. 515–518.

[7] – *Számelméleti Problémak I*, Mat. Lapok 19 (1968), pp. 317–325.

[8] J. Meyer, *Sur les fonctions additives bornées sur les nombres de la forme* $p+1$, *avec* p *premier*, Preprint, Paris (1977).

[9] E. Wirsing, *Das asymptotische Verhalten von Summen über multiplikative Funktionen*, Math. Ann. 143 (1961), pp. 75–102.

[10] D. Wolke, *Bemerkungen über Eindentigkeitsmengen additiver Funktionen*, Elemente d. Math. 33 (1978), pp. 14–16.

Received on 6. 2. 1978 (1041)