ACTA ARITHMETICA
116.4 (2005)

Shifted B-numbers as a set of uniqueness for additive and multiplicative functions

by

KARL-HEINZ INDLEKOFER (Paderborn) and
NIKOLAI M. TIMOFEEV

1. Introduction and results. A function $f:\mathbb{N}\to\mathbb{C}$ is called *additive* if

(1) $$f(mn)=f(m)+f(n)$$

for all coprime $m,n\in\mathbb{N}$. If (1) holds for all pairs of integers $m,n\in\mathbb{N}$, we say that f is *completely additive*. A function $g:\mathbb{N}\to\mathbb{C}$ is called *multiplicative* (resp. *completely multiplicative*) if

(2) $$g(mn)=g(m)g(n)$$

for all coprime $m,n\in\mathbb{N}$ (resp. for all $m,n\in\mathbb{N}$).

Because of the canonical representation

(3) $$n=\prod_{p\,\mathrm{prime}} p^{\alpha_p}\quad \text{with } p^{\alpha_p}\,\|\,n$$

of $n\in\mathbb{N}$ we have $f(n)=\sum_{p\,\mathrm{prime}} f(p^{\alpha_p})$ (resp. $g(n)=\prod_{p\,\mathrm{prime}} g(p^{\alpha_p})$).

An additive f can be extended uniquely to an "additive" function $f^*:\mathbb{Q}^+\to\mathbb{C}$, where $\mathbb{Q}^+=\{a/b:(a,b)=1;\ a,b\in\mathbb{N}\}$, by $f^*(a/b)=f(a)-f(b)$. In a similar manner we get an extension g^* of a multiplicative function g by $g^*(a/b)=g(a)/g(b)$ in case $g(b)\neq 0$ for all $b\in\mathbb{N}$. In the following we denote by $\mathcal{A}$ the set of all additive $f:\mathbb{Q}^+\to\mathbb{C}$ and by $\mathcal{M}$ the set of all multiplicative $g:\mathbb{Q}^+\to\mathbb{C}$ with $g(b)\neq 0$ for all $b\in\mathbb{N}$. We write $\mathcal{A}_0$ (resp. $\mathcal{M}_0$) for the subsets of completely additive (resp. completely multiplicative) functions in $\mathcal{A}$ (resp. $\mathcal{M}$).

2000 *Mathematics Subject Classification*: 11E25, 11M25, 11M36, 11M37.

Key words and phrases: sums of two squares, sets of uniqueness, lower sieve estimates, binary quadratic forms, additive and multiplicative functions.

Research of the first author supported by the DFG (Deutsche Forschungsgemeinschaft).

Research of the second author supported by the DFG (Deutsche Forschungsgemeinschaft) and by the grant no. 99-01-00070 from the Russian Foundation for Basic Research.

DEFINITIONS. Let $A = \{a_n\} \subset \mathbb{Q}^+$. We say that A is a

(a) *U-set for* $\mathcal{A}$ in case $f \in \mathcal{A}$, $f(A) = \{0\}$ implies $f = 0$,
(b) *U-set for* $\mathcal{M}$ in case $g \in \mathcal{M}$, $g(A) = \{1\}$ implies $g = 1$,
(c) *C-set for* $\mathcal{A}$ in case $f \in \mathcal{A}$, $\lim_{n\to\infty} f(a_n) = 0$ implies $f = 0$,
(d) *C-set for* $\mathcal{M}$ in case $g \in \mathcal{M}$, $\lim_{n\to\infty} g(a_n) = 1$ implies $g = 1$.

In an obvious manner U-sets and C-sets are defined for $\mathcal{A}_0$ (resp. $\mathcal{M}_0$).

Wolke [18], Dress and Volkmann [1] and Indlekofer [8] (see also [4]) showed: In order that the set $A = \{a_n\}$ should be a U-set for $\mathcal{A}_0$, it is both necessary and sufficient that every positive integer n has a representation

$$n = \prod_{i=1}^{l} a_i^{\alpha_i} \quad \text{where } \alpha_i \in \mathbb{Q} \ (i = 1, \dots, l).$$

On the other hand, to the subset $A \subset \mathbb{Q}^+$ there corresponds the subgroup $\Gamma = \langle A \rangle$ of $\mathbb{Q}^+$ generated by A. From this observation Indlekofer ([8, Theorem 2]) deduced the following:

Let $A = \{a_n\} \subset \mathbb{Q}^+$. Then the following two assertions are equivalent:

(I) *A is a U-set for $\mathcal{M}_0$.*
(II) *Every positive integer n has a representation*

$$n = \prod_{i=1}^{l} a_i^{\varepsilon_i} \quad \textit{where } \varepsilon_i \in \{-1, 1\} \ (i = 1, \dots, l) \textit{ and } l = l(n).$$

Obviously this is equivalent to $\mathbb{Q}^+/\Gamma = \{1\}$.

Kátai introduced the notion of U-sets for $\mathcal{A}$ in his paper [12] and showed that the set A containing the prime divisors of k and the arithmetic progression $\{l + jk : j = 0, 1, \dots\}$ is a U-set for $\mathcal{A}_0$. Further examples may be found in [13], [6] and [8].

In [13] Kátai proved that the set $\{p + 1\}$ of shifted primes is a set of "quasiuniqueness", i.e. the union of $\{p + 1\}$ and some finite set is a U-set for $\mathcal{A}_0$. In 1974 Elliott [2] showed that $\{p + 1\}$ is in fact a U-set for $\mathcal{A}_0$.

It is still unknown whether $\{p+1\}$ is a U-set for $\mathcal{M}_0$. If $\Gamma = \langle\{p+1\}\rangle$ then Elliott [3] proved $|\mathbb{Q}^+/\Gamma| \le 3$. This means that $f \in \mathcal{M}_0$ and $f(p+1) = 1$ for all primes p implies the existence of an integer $0 < k \le 3$ such that $f^k = 1$. A famous conjecture of Schinzel implies that every positive integer n can be written as

$$n = \frac{p+1}{q+1} \quad (p, q \text{ prime})$$

and, in addition, there are infinitely many such representations of n. The case $n = 2$ corresponds to the existence of infinitely many Sophie Germain primes p and $q = 2p + 1$ (see also Indlekofer and Járai [10]).

In this paper we deal with the set $B \subset \mathbb{N}$ of natural numbers which can be represented as a sum of two squares of integers.

It is well known (see, for example, [9], [14]) that $n \in B$ if and only if n has the form

$$n = 2^s n_1 n_3^2 \tag{4}$$

where $s \geq 0$ and all prime divisors of n_1 and n_3 are $\equiv 1 \bmod 4$ and $\equiv 3 \bmod 4$, respectively.

For such B-numbers Landau [14] showed ($c > 0$)

$$\sum_{\substack{n \leq x \\ n \in B}} 1 \sim c \frac{x}{\sqrt{\log x}},$$

and it turns out that some conjectured properties for primes are valid for B-numbers. For example, it is known that there are infinitely many B-twins and, moreover, the estimates

$$\sum_{\substack{n \leq x \\ n \in B,\, n+1 \in B}} 1 \asymp \frac{x}{\log x}$$

hold true (Indlekofer [7]). Further, here we prove that the set $B+1 = \{b+1 : b \in B\}$ of shifted B-numbers is a U-set for $\mathcal{M}_0$. In addition we give the exact lower bound of the number of factors which are needed in the representation

$$n = \prod_{i=1}^{l} (b_i + 1)^{\varepsilon_i}, \qquad \varepsilon_i = \pm 1,\ b_i \in B\ (i = 1, \dots, l), \tag{5}$$

and prove that there are infinitely many representations (5) for every n. In particular, there are infinitely many representations

$$n = \frac{a+1}{b+1}, \qquad a, b \in B,$$

if n is odd or $n = 2m$ and m is odd.

Remark 1. Kátai [13] showed that $\{p : p \equiv 3 \bmod 4 \text{ prime}\} \cup \{n^2 + 1 : n \in \mathbb{N}\}$ is a U-set for $\mathcal{A}_0$. Using an idea of his paper Fehér, Indlekofer and Timofeev [5] proved that the sets $B + 1$ and $\{n^2 + 2m^2 + 1 : m, n \in \mathbb{Z}\}$ are also U-sets for $\mathcal{A}_0$.

The key result of this paper is a lower sieve estimate contained in

Theorem 1. *Let c be a non-zero integer and $a, b \in \mathbb{N}$ such that $(a, b) = 1$ and $(ab, 2c) = 1$. Further, let*

$$S(x) := \sharp\{n : n \leq x,\ a(n + c) = b(m + c),\ (a, n + c) = 1,\ n, m \in B\}.$$

Then there exists a positive constant $\vartheta = \vartheta(a, b, c)$ such that

$$S(x) \geq \vartheta \frac{x}{\log x} \tag{6}$$

for $x \geq x_0 = x_0(a, b, c)$.

Remark 2. We have two possibilities to prove the lower estimate (6). One is to apply the linear sieve in a similar way to what has been done in [7], but here we shall use the half-dimensional sieve details of which are given in [11]. The upper bound result $S(x) \ll x/\log x$ follows immediately from standard (upper) sieve estimates.

Applying Theorem 1 we prove

Theorem 2. *Let c be a non-zero integer. Then $B+c$ is a C-set for $\mathcal{M}_0$. In particular, $B+c$ is a U-set for $\mathcal{M}_0$.*

This implies the following:

Corollary 1. *Let c be a non-zero integer. Then $\mathbb{Q}^+ = \langle B+c \rangle$. Further, for each $n \in \mathbb{N}$ there exists $\kappa = \kappa(n)$ such that n can be expressed as a product*

$$n = \prod_{i=1}^{k} (n_i + c)^{\varepsilon_i}, \qquad \varepsilon_i = \pm 1,\, n_i \in B \ (i = 1, \dots, k),$$

infinitely often where $k \le \kappa$.

Directly from Theorem 1 follows

Corollary 2. *Let c be a non-zero integer. Then*

$$B + c \,\cup \{p^r : p \,|\, 2c,\ r = 1, 2, \dots\}$$

is a U-set for $\mathcal{A}$ and $\mathcal{M}$.

Let us now consider the special case $c = 1$. Theorem 1 yields infinitely many representations

$$\frac{a}{b} = \frac{m+1}{n+1}, \qquad \text{where } m, n \in B,$$

for natural numbers a and b which are odd and coprime. Now, we shall show that the equation

$$\frac{2a}{b} = \frac{m+1}{2n+1}$$

holds true infinitely often in case $(2, ab) = (a, b) = 1$ with suitable $m, 2n \in B$. This result is a consequence of

Theorem 3. *Let $a, b \in \mathbb{N}$ be odd with $(a, b) = 1$, and define $\widetilde{S}(x)$ by*

$$\widetilde{S}(x) := \sharp\{n : n \le x,\ 2a(2n+1) = b(m+1),\ n, m \in B\}.$$

Then there exists a positive constant $\vartheta = \vartheta(a, b)$ such that

$$\widetilde{S}(x) \ge \vartheta \, \frac{x}{\log x}$$

for $x \ge x_0 = x_0(a, b)$.

Since $2 = 1^2 + 0^2 + 1$, Corollary 2 implies

Corollary 3. *$B + 1 \cup \{2^r : r = 2, 3, \dots\}$ is a U-set for $\mathcal{A}$ and $\mathcal{M}$.*

Every $a \in \mathbb{N}$ can be represented as a finite product

$$a = (n_1 + 1)^{\varepsilon_1} \cdots (n_s + 1)^{\varepsilon_s} \tag{7}$$

where $\varepsilon_i = \pm 1$, $n_i \in B$ $(i = 1, \dots, s)$. Defining $s(a)$ as the smallest s such that (7) holds we shall prove

THEOREM 4. *Let $a = 2^r b$ where $0 \le r$ and $(2, b) = 1$.*

(i) *If $0 \le r \le 1$ then*

$$s(a) = \begin{cases} 1 & \textit{if } a - 1 \in B, \\ 2 & \textit{otherwise}, \end{cases}$$

and there are infinitely many representations (7) *of a with $s = 2$.*

(ii) *If $r \ge 2$ then $s(a) = r$ or $s(a) = r + 1$, and both cases occur. Further, there are infinitely many representations* (7) *of a with $s = r + 1$.*

REMARK 3. Let $f(x, y) = ax^2 + bxy + cy^2$, where $a, b, c \in \mathbb{Z}$, $(a, b, c) = 1$, be a primitive, positive-definite binary quadratic form with discriminant $D = b - 4ac$. We believe that results similar to Theorems 1, 2 and Corollaries 1, 2 are true for the set $B_f + d$, where $B_f := \{n : n = f(x, y),\ x, y \in \mathbb{Z}\}$ and d is a non-zero integer.

The discriminant $D = -4$ corresponds to the representation as a sum of two squares. We now describe, as an example, how our method works in the case $D = -8$, i.e. $f(x, y) = x^2 + 2y^2$. Putting

$$B(2) := \{n : n = x^2 + 2y^2,\ x, y \in \mathbb{Z}\}$$

we prove

THEOREM 5. *Let c be a non-zero integer. Let $a, b \in \mathbb{N}$ such that $(a, b) = 1$ and $(ab, 2c) = 1$. Further, let*

$$\tilde{\tilde{S}}(x) := \sharp\{n : n \le x,\ a(n + c) = b(m + c),\ (n + c, a) = 1,\ m, n \in B(2)\}.$$

Then there exists a positive constant $\vartheta = \vartheta(a, b, c)$ such that

$$\tilde{\tilde{S}}(x) \ge \vartheta \frac{x}{\log x}$$

for $x \ge x_0 = x_0(a, b, c)$.

An immediate application of Theorem 5 yields

THEOREM 6. *Let c be a non-zero integer. Then $B(2) + c$ is a C-set for $\mathcal{M}_0$. In particular, $B(2) + c$ is a U-set for $\mathcal{M}_0$.*

This, together with Theorem 5, gives

COROLLARY 4. *Let c be a non-zero integer. Then $\mathbb{Q}^+ = \langle |B(2) + c| \rangle$. Further, for each $n \in \mathbb{N}$ there exists $\kappa = \kappa(n)$ such that n can be expressed* *as a product*

$$n = \prod_{i=1}^{k} (n_i + c)^{\varepsilon_i}, \qquad \varepsilon_i = \pm 1,\, n_i \in B(2)\ (i = 1, \ldots, k),$$

infinitely often where $k \le \kappa$.

Theorem 5 implies

Corollary 5. *Let* c *be a non-zero integer. Then*

$$B(2) + c \cup \{p^r : p \,|\, 2c,\ r = 1, 2, \ldots\}$$

is a U*-set for* $\mathcal{A}$ *and* $\mathcal{M}$.

2. Proofs of Theorem 2 and Corollaries 1, 2. We assume that g is completely multiplicative with $\lim_{i\to\infty} g(n_i + c) = 1$ where n_i runs through the set B.

If p is prime, $p \nmid 2c$, then, by Theorem 1,

$$p = \frac{m + c}{n + c} \quad \text{for infinitely many } m, n \in B,$$

and thus $g(p) = 1$.

Next we show $g(2) = 1$. Assume that $c = 2^r c_1$ where $r \ge 0$ and $(c_1, 2) = 1$. First suppose $c_1 \equiv 1 \bmod 4$. We choose a prime $p \equiv 1 \bmod 4$ such that $p \nmid c$. Since $2^r p \in B$ we conclude

$$2^r p + c = 2^r (p + c_1) = 2^{r+1} a \quad \text{where } (a, 2c) = 1.$$

Thus $g(2^{r+1}) = g(2^r p + c)$, and choosing p large enough leads to

$$g(2^{r+1}) = 1. \tag{8}$$

If $r > 0$ we let p be as before and obtain, since $2^{r+2} p \in B$,

$$2^{r+2} p + c = 2^r (4p + c_1) \quad \text{with } (4p + c_1, 2c) = 1,$$

which implies

$$g(2^r) = 1. \tag{9}$$

Now, (8) and (9) prove $g(2) = 1$ if $c_1 \equiv 1 \bmod 4$.

If $c_1 \equiv -1 \bmod 4$ we choose large primes p_1 and p_2 by

$$p_1 \equiv -c_1 + 4 \bmod 8, \quad p_2 \equiv -c_1 + 8 \bmod 16$$

and obtain

$$2^r p_1 + c = 2^r (p_1 + c_1) = 2^{r+2} a_1 \quad \text{with } (a_1, 2c) = 1,$$
$$2^r p_2 + c = 2^r (p_2 + c_1) = 2^{r+3} a_2 \quad \text{with } (a_2, 2c) = 1.$$

This implies

$$g(2^{r+2}) = g(2^{r+3}) = 1,$$

and thus $g(2) = 1$.

Now, let p be a prime divisor of c different from 2, and put $c = 2^s p^r c_1$ with $(c_1, 2p) = 1$, where $s \geq 0$ and $r \geq 1$.

If r is odd choose an arbitrary prime $p_1 \equiv 1 \bmod 4$, $p_1 \nmid c$. Then $2^{s+1}p^{r+1}p_1 \in B$ and

$$2^{s+1}p^{r+1}p_1 + c = 2^s p^r(2pp_1 + c_1) \quad \text{where } (2pp_1 + c_1, 2c) = 1,$$

which shows

$$g(p^r) = 1 \quad \text{if } r \text{ is odd.}$$

Let now r be even. Then, if $c_1 \equiv l \bmod 4p$ with $(l, 2p) = 1$, choose a prime $p_1 \equiv 1 \bmod 4$, $p_1 \nmid c$, satisfying

$$p_1 \equiv 1 + 4l_1 \bmod 4p,$$

where l_1 is taken such that

$$1 + 4l_1 + l \not\equiv 0 \bmod p.$$

For example, if $p \nmid (1+l)$ put $l_1 = p$. If $p \mid (1+l)$ and $p \neq 5$ put $l_1 = 1$, and if $p = 5$ and $p \mid (1+l)$ let $l_1 = -1$. Then $2^s p^r p_1 \in B$ and

$$2^s p^r p_1 + c = 2^s p^r(p_1 + c_1) = 2^{s'} p^r a \quad \text{with } (a, 2c) = 1.$$

Thus

$$g(p^r) = 1 \quad \text{if } r \text{ is even.}$$

In the next step we show $g(p^{r-1}) = 1$ if r is odd and $g(p^{r+1}) = 1$ if r is even. Let r be odd and $r \geq 3$. Then $2^s p^{r-1} p_1$ with $p_1 \equiv 1 \bmod 4$, $p_1 \nmid c$, is an element of B, and thus in the same way as above

$$g(p^{r-1}) = 1 \quad \text{if } r \text{ is odd.}$$

In the other case let the prime $p_1 \equiv 1 \bmod 4$ $(p_1 \nmid c)$ satisfy

$$p_1 + c_1 \equiv 0 \bmod p, \qquad p_1 + c_1 \not\equiv 0 \bmod p^2. \tag{10}$$

This choice is possible. For, if $c_1 = l + 4p^2 k$, $(l, 2p) = 1$, let $p_1 \equiv 1 + 4l_1 \bmod 4p^2$ such that $1 + 4l_1 + l \equiv 0 \bmod p$ but $1 + 4l_1 + l \not\equiv 0 \bmod p^2$. If $c_1 = l + 4pk$, $(p, k) = 1$, choose $p_1 \equiv 1 + 4l_1 \bmod 4p^2$, where $1 + 4l_1 + l \equiv 0 \bmod p^2$. Thus, by (10),

$$2^s p^r p_1 + c = 2^{s''} p^{r+1} a' \quad \text{with } (a', 2c) = 1,$$

which gives

$$g(p^{r+1}) = 1 \quad \text{if } r \text{ is even.}$$

This ends the proof of Theorem 2.

The first part of Corollary 1 holds since $B + c$ is a U-set for $\mathcal{M}_0$. Next, each $n \in \mathbb{N}$ can be written in the form $n = n'a$, where $(a, 2c) = 1$ and all prime divisors of n' divide $2c$. Applying Theorem 1 to a gives the second assertion of Corollary 1.

Corollary 2 follows directly from Theorem 1, since if $(a, 2c) = 1$, then $f(B+c) = \{0\}$ $(f \in \mathcal{A})$ and $g(B+c) = \{1\}$ $(g \in \mathcal{M})$ implies $f(a) = 0$ and $g(a) = 1$, respectively.

3. The half-dimensional sieve. First we recollect the notations and some facts on the half-dimensional sieve. For details see [11].

Let $\mathcal{A}$ be a finite set of positive integers and let $\mathcal{P}$ be a set of primes. The *sieve problem* is to *sift* a certain sequence $\mathcal{A}$ by a truncation (at z) of $\mathcal{P}$, that is, to estimate the *sifting function*

$$S(\mathcal{A}, \mathcal{P}, z) := \sharp\{a : a \in \mathcal{A},\ (a, P(z)) = 1\}$$

with

$$P(z) := \prod_{\substack{p<z \\ p \in \mathcal{P}}} p.$$

Let ϱ be a multiplicative function such that

$$0 \le \varrho(p) < p \quad \text{and} \quad \varrho(p) = 0 \quad \text{for } p \notin \mathcal{P}, \tag{11}$$

and, for some positive constant K,

$$\left| \sum_{\substack{p \le z \\ p \in \mathcal{P}}} \frac{\varrho(p)}{p - \varrho(p)} \log p - \frac{1}{2} \log z \right| \le K \tag{12}$$

for any real number $z \ge 2$. Further, we put

$$V(z) := \prod_{p<z} \left(1 - \frac{\varrho(p)}{p}\right)$$

and, for squarefree numbers d,

$$\mathcal{A}_d := \{a \in \mathcal{A} : a \equiv 0 \bmod d\}, \qquad R(\mathcal{A}, d) := \sharp\mathcal{A}_d - \frac{\varrho(d)}{d} X$$

where $X \ge 1$ is a good approximation to $\sharp\mathcal{A}$. Thus we have (cf. [11, Theorem 1])

Lemma 1. *Let $\mathcal{A}$ be a finite sequence of integers, ϱ be a multiplicative function such that* (11) *and* (12) *are satisfied. Then for all $z \ge 2$, $y \ge 2$ we have*

$$S(\mathcal{A}, \mathcal{P}, z) \le XV(z)\{F(s) + O(\log^{-1/5} y)\} + \sum_{\substack{d<y \\ d|P(z)}} |R(\mathcal{A}, d)|, \tag{13}$$

$$S(\mathcal{A}, \mathcal{P}, z) \ge XV(z)\{f(s) + O(\log^{-1/5} y)\} - \sum_{\substack{d<y \\ d|P(z)}} |R(\mathcal{A}, d)|, \tag{14}$$

where $s = \log y/\log z$ *and the functions* $f(s), F(s)$ *are the continuous solutions of the system of differential-difference equations*

$$f(s) = 0, \quad F(s) = 2\left(\frac{e^\gamma}{\pi s}\right)^{1/2} \quad \text{for } 0 < s \le 1, \tag{15}$$

$$2s^{1/2}(s^{1/2}f(s))' = F(s-1), \quad 2s^{1/2}(s^{1/2}F(s))' = f(s-1) \quad \text{for } s > 1, \tag{16}$$

with γ *denoting Euler's constant. For* $s > 1$ *we have*

$$0 < f(s) < 1 < F(s), \qquad F'(s) < 0 < f'(s),$$

and, *for* $1 \le s \le 2$,

$$f(s) = \sqrt{\frac{e^\gamma}{\pi}}\,\frac{1}{\sqrt{s}}\int_1^s \frac{dt}{\sqrt{t(t-1)}}, \qquad F(s) = 2\sqrt{\frac{e^\gamma}{\pi}}\,\frac{1}{\sqrt{s}}. \tag{17}$$

To estimate the error terms of the sieve we shall apply the results of [15]. There the following notations have been used:

$$\sum(x,f,k,s) = \sum_{\substack{n\le x\\ n\equiv s \bmod k}} f(n) - \frac{1}{\varphi(k)}\sum_{\substack{n\le x\\ (n,k)=1}} f(n),$$

$$\delta(x,f,k) = \max_{(s,k)=1}\max_{y\le x}\Big|\sum(y,f,k,s)\Big|, \qquad \Delta(Q,f,E) = \sum_{\substack{k\le Q\\ k\in E}} \delta(x,f,k),$$

$$\Delta_1(Q,f,E) = \sum_{\substack{k\le Q\\ k\in E}} \max_{(s,k)=1}\max_{y\le x}\Bigg|\sum_{\substack{p\le y\\ p\equiv s \bmod k}} f(p)\log p - \frac{1}{\varphi(k)}\sum_{\substack{p\le y\\ p\nmid k}} f(p)\log p\Bigg|.$$

We shall deal with multiplicative functions described in the following

Definition. A multiplicative function f belongs to $\mathcal{M}_\alpha(\mathcal{D})$ if

$$\sum_{n\le x} |f(n)|^4 \ll x\log^{4\alpha} x, \qquad \alpha \ge 0,$$

and if for all primitive characters χ_d^* mod d, where $d \in \mathcal{D}$, $d \le \log^{c_1} x$, we have

$$\sum_{z<p\le y} \chi_d^*(p) f(p)\log p \ll y\log^{-B} x, \tag{18}$$

where

$$\log z = (\log x)^{\Theta}, \qquad \Theta = 1 - \frac{\log\log\log x}{\log\log x}, \qquad y \le x,$$

c_1 and B are arbitrary constants, and $\mathcal{D}$ is a subset of the natural numbers.

Then the following holds true.

Lemma 2 (see [15, Theorem 4]). *If* $f \in \mathcal{M}_\alpha(\mathcal{D})$ *and* $\Delta_1(Q,f,E) \ll x\log^{-3B} x$, *where* E *is a set of natural number whose divisors belong to* $\mathcal{D}$, *then*

$$\Delta(Q_1, f, E) \ll x(\log x)^{-B+5/6+4\alpha/3}(\log\log x)^{2+\alpha},$$

with $Q_1 = \min(Q(x), \sqrt{x}\,(\log x)^{-3B-3/2-2\alpha}(\log\log x)^{-5/4})$.

Using the theorem of Vinogradov–Bombieri we prove

LEMMA 3. *Let f be a completely multiplicative function such that $f(p)=1$ for $p \equiv 1 \bmod 4$ and $f(p) = 0$ otherwise. Then for any $A > 0$ there exists $B = B(A)$ such that*

$$\sum_{\substack{d\le\sqrt{x}\log^{-B} x\\ (d,2)=1}} \max_{(s,d)=1} \max_{y\le x} \Bigg| \sum_{\substack{n\le y\\ n\equiv s \bmod d}} f(n) - \frac{1}{\varphi(d)} \sum_{\substack{n\le y\\ (n,d)=1}} f(n) \Bigg| \ll x\log^{-A} x.$$

Proof. It is easy to see that $f \in \mathcal{M}_0(E)$, where E is the set of odd numbers. To verify condition (18) we use the theorem of Siegel–Walfisz (see, for example, [16, Chapter IV, Theorem 8.3]) for characters of the form $\chi_4\chi_d^*$, where $d \in E$. Then

$$\begin{aligned}\Delta_1(Q, f, E) = &\sum_{\substack{k\le Q\\ (k,2)=1}} \max_{(s,k)=1} \max_{y\le x} \Bigg| \sum_{\substack{p\le y\\ p\equiv 1 \bmod 4\\ p\equiv s \bmod k}} \log p - \frac{1}{\varphi(k)} \sum_{\substack{p\le y\\ p\equiv 1 \bmod 4\\ p\nmid k}} \log p\Bigg| \\ &\le \sum_{\substack{k\le Q\\ (k,2)=1}} \max_{(s,2k)=1} \max_{y\le x} \left|\psi(y,4k,s) - \frac{y}{\varphi(4k)}\right| \\ &\quad + \sum_{k\le Q} \frac{1}{\varphi(k)} \max_{y\le x} \left|\psi(y,4,1) - \frac{y}{2}\right| + \sum_{k\le Q} \frac{\log k}{\varphi(k)}.\end{aligned}$$

By Vinogradov–Bombieri's theorem we conclude that

$$\Delta_1\left(\frac{\sqrt{x}}{\log^B x}, f, E\right) \ll \frac{x}{\log^A x}.$$

Applying Lemma 2 finishes the proof.

The next result is due to E. Landau ([14, §183]).

LEMMA 4. *Let $\lambda(x)$ be the number of odd integers n with $1 \le n \le x$ which do not have any prime factors of the form $4n + 3$. Then*

$$\lambda(x) = \frac{cx}{\sqrt{\log x}} + O\left(\frac{x}{\log x}\right)$$

with some $c > 0$.

For the proof see, for example, [17, pp. 183–185].

4. Proof of Theorem 1. Let us assume that $c = 2^r c_1$, $(c_1, 2) = 1$. Put $n = 2^r n_1$, $m = 2^r m_1$, where $n, m, n_1, m_1 \in B$. Then

$$\begin{aligned} S(x) &= \sharp\{n : n \le x,\ a(n+c) = b(m+c),\ (a, n+c) = 1,\ n, m \in B\} \\ &\ge \sharp\{n_1 : n_1 \le x/2^r,\ a(n_1+c_1) = b(m_1+c_1), \\ &\qquad (a, n_1+c_1) = 1,\ n_1, m_1 \in B\}, \end{aligned}$$

and obviously it is enough to prove (6) in the case when c is an odd number.

Let $\mathcal{P} := \{2\} \cup \{p : p \equiv 3 \bmod 4\}$. For a real number $x > 1$ let $P(x) := \prod_{p<x,\, p\in\mathcal{P}} p$. We know that $n \in B$ if and only if $n = 2^\alpha p_1^{\alpha_1} \cdots p_t^{\alpha_t}$, where α_i is an even number in case $p_i \equiv 3 \bmod 4$. Hence

$$\begin{aligned} S(x) \ge S_1(x) := \sharp\Big\{n : n \le x,\ n \equiv -c \bmod b,\ (a, n+c) = 1, \\ (n, P(x)) = 1, \big(\tfrac{a}{b}(n+c) - c, P(Y)\big) = 1\Big\}, \end{aligned} \tag{19}$$

where $Y = \frac{a}{b}(x+c) - c$. Let α be a real number, $1/3 < \alpha < 1/2$. Then we can show that

$$S_1(x) \ge S_2(x) - S_3(x) + O(x^{1-\alpha}), \tag{20}$$

where

$$\begin{aligned} S_2(x) &:= \sharp\Big\{n : n \le x,\ n \equiv -c \bmod b,\ (a, n+c) = 1,\ (n, P(x)) = 1, \\ &\qquad \big(\tfrac{a}{b}(n+c) - c, P(Y^\alpha)\big) = 1\Big\}, \\ S_3(x) &:= \sharp\Big\{n : n \le x,\ n \equiv -c \bmod b,\ (a, n+c) = 1,\ (n, P(x)) = 1, \\ &\qquad \tfrac{a}{b}(n+c) - c = p_1 p_2 m,\ Y^\alpha \le p_1 < p_2 \le Y^{1-\alpha},\ p_1 \equiv 3 \bmod 4, \\ &\qquad p_2 \equiv 3 \bmod 4,\ (m, P(Y)) = 1\Big\}. \end{aligned}$$

Indeed, it is easy to see that

$$S_1(x) = S_2(x) - S_3(x) - S_4(x) + O\bigg(\sum_{p > Y^\alpha} \frac{x}{p^2}\bigg),$$

where

$$\begin{aligned} S_4(x) &:= \sharp\Big\{n : n \le x,\ n \equiv -c \bmod b,\ (a, n+c) = 1,\ (n, P(x)) = 1, \\ &\qquad \tfrac{a}{b}(n+c) - c = pm,\ Y^\alpha \le p,\ p \equiv 3 \bmod 4,\ (m, P(Y)) = 1\Big\}. \end{aligned}$$

Since $(abc, 2) = 1$ and $(n, P(x)) = 1$, $(m, P(Y)) = 1$ we get $n \equiv 1 \bmod 4$, $m \equiv 1 \bmod 4$, $\frac{a}{b}(n+c) - c \equiv (1+c) - c \equiv 1 \bmod 4$ or $\frac{a}{b}(n+c) - c \equiv 3(1+c) - c \equiv 1 \bmod 4$. Therefore $S_4(x) = 0$ and (20) holds.

Using Lemma 1 we shall prove lower bounds for $S_2(x)$. We choose

$$X = X_1 := \sharp\{n : n \le x,\ n \equiv -c \bmod b,\ (a, n+c) = 1,\ (n, P(x)) = 1\},$$

$$z = Y^\alpha, \qquad y = \frac{\sqrt{x}}{\log^B x}$$

and

$$\frac{\varrho(d)}{d} = \begin{cases} \dfrac{\varphi(b)}{\varphi(bd)} & \text{if } d \mid P(z),\ (d, ac(a-b)) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

Hence $\varrho(p)/p = 0$ if $p \mid ac(a-b)$ or $p \equiv 1 \bmod 4$, $\varrho(p)/p = 1/(p-1)$ if $p \equiv 3 \bmod 4$, $p \nmid b$ and $\varrho(p)/p = 1/p$ if $p \equiv 3 \bmod 4$, $p \mid b$. So conditions (11), (12) are fulfilled. We have

$$\frac{\log y}{\log Y^\alpha} = \frac{1}{2\alpha} + O\Big(\frac{\log\log x}{\log x}\Big).$$

So, by Lemma 1,

$$S_2(x) \geq \prod_{\substack{p<Y^\alpha \\ p\equiv 3 \bmod 4 \\ p\nmid ac(a-b)}} \Big(1 - \frac{\varphi(b)}{\varphi(bp)}\Big) X_1 \Big\{ f\Big(\frac{1}{2\alpha}\Big) + O(\log^{-1/5} x) \Big\}$$
$$- \sum_{\substack{d \leq \sqrt{x}/\log^B x \\ d \mid P(Y^\alpha) \\ (d,ac(a-b))=1}} \Big| \sharp\{n : n \leq x,\ (a, n+c) = 1,\ (n, P(x)) = 1,\ n \equiv -c + ca^* b \bmod db\} - \frac{\varphi(b)}{\varphi(bd)} X_1 \Big|,$$

where $a^* a \equiv 1 \bmod db$. Since $(a,b) = 1$ we see that

$$S_2(x) \geq \frac{1}{\varphi(b)} \prod_{\substack{p<Y^\alpha \\ p\equiv 3 \bmod 4 \\ p\nmid ac(a-b)}} \Big(1 - \frac{\varphi(b)}{\varphi(bp)}\Big) \sum_{\nu \mid a} \frac{\mu(\nu)}{\varphi(\nu)} \sharp\{n : n \leq x,\ (n, \nu b P(x)) = 1\}$$
$$\times \Big(f\Big(\frac{1}{2\alpha}\Big) + O(\log^{-1/5} x) \Big)$$
$$+ O\Big(\sum_{\substack{\nu d \leq a\sqrt{x}/\log^B x \\ \nu\mid a,\, d\mid P(Y^\alpha) \\ (d,ac(a-b))=1}} \Big| \sharp\{n : n \leq x,\ (n, P(x)) = 1,\ n \equiv -c + ca^*\nu^* b\nu \bmod db\nu\}$$
$$- \frac{1}{\varphi(d\nu b)} \sharp\{n : n \leq x,\ (n, \nu b P(x)) = 1\} \Big| \Big),$$

where $\nu^* \nu \equiv a \bmod db$. Because of $(n, P(x)) = 1$ and $d \mid P(Y^\alpha)$ we have $(n,d) = 1$. By Lemma 3,

$$S_2(x) \geq \frac{f(1/2\alpha)}{\varphi(b)} \sum_{\nu \mid a} \frac{\mu(\nu)}{\varphi(\nu)} \sharp\{n : n \leq x,\ (n, \nu b P(x)) = 1\} \times \prod_{\substack{p<Y^\alpha \\ p\equiv 3 \bmod 4 \\ p\nmid ac(a-b)}} \Big(1 - \frac{\varphi(b)}{\varphi(bp)}\Big) + O(x \log^{-6/5} x). \tag{21}$$

Concerning the sum $S_3(x)$ we have

$$\begin{aligned}
S_3(x) \le S_5(x) := \sharp\big\{mp_1p_2 : mp_1p_2 \le Y,\ (m, P(Y)) = 1,\ p_1 \equiv 3 \bmod 4, \\
p_2 \equiv 3 \bmod 4,\ Y^\alpha \le p_1 < p_2 \le Y^{1-\alpha},\ mp_1p_2 \equiv c \bmod a, \\
\big(\tfrac{b}{a}(mp_1p_2 + c) - c, P(Y^{\alpha/3})\big) = 1\big\} \\
\le \prod_{\substack{p<Y^\alpha \\ p\equiv 3 \bmod 4 \\ p\nmid ac(a-b)}} \left(1 - \frac{\varphi(b)}{\varphi(bp)}\right) \frac{1}{\varphi(a)} \sharp\{mp_1p_2 : mp_1p_2 \le Y,\ (m, P(Y)) = 1, \\
Y^\alpha \le p_1 < p_2 \le Y^{1-\alpha},\ p_1 \equiv p_2 \equiv 3 \bmod 4\} \\
\times (F(1) + O(\log^{-1/5} x)) \\
+ \sum_{\substack{d\le Y^{\alpha/3} \\ d\mid P(Y^{\alpha/3}) \\ (d,bc(a-b))=1}} \Big| \sharp\{mp_1p_2 : mp_1p_2 \le Y,\ (m, P(Y)) = 1, \\
Y^\alpha \le p_1 < p_2 \le Y^{1-\alpha},\ p_1 \equiv p_2 \equiv 3 \bmod 4, \\
mp_1p_2 \equiv -c + cb^*a \bmod da\} \\
- \frac{1}{\varphi(da)} \sharp\{mp_1p_2 : mp_1p_2 \le Y,\ (m, aP(Y)) = 1, \\
Y^\alpha \le p_1 < p_2 \le Y^{1-\alpha},\ p_1 \equiv p_2 \equiv 3 \bmod 4\}\Big|,
\end{aligned}$$

where $b^*b \equiv 1 \bmod da$. Since $p_1 > Y^\alpha$ and $d \le Y^{\alpha/3}$ we can apply the Vinogradov–Bombieri theorem to the sum on the right hand side. Thus for any $A > 0$ we obtain

$$\begin{aligned}
S_3(x) \le \sqrt{\frac{e^\gamma}{\pi}} \frac{2}{\varphi(a)} \prod_{\substack{p<Y^{\alpha/3} \\ p\nmid bc(a-b)}} \left(1 - \frac{\varphi(a)}{\varphi(ap)}\right) \\
\times \sharp\{mp_1p_2 : mp_1p_2 \le Y,\ (m, P(Y)) = 1, \\
Y^\alpha \le p_1 < p_2 \le Y^{1-\alpha},\ p_1 \equiv p_2 \equiv 3 \bmod 4\} \\
+ O(x \log^{-A} x).
\end{aligned}$$

Hence (21), (20) and (19) yield

$$\begin{aligned}
S(x) \ge \sqrt{\frac{e^\gamma}{\pi}} \prod_{\substack{p<Y^{\alpha/3} \\ p\nmid bc(a-b) \\ p\equiv 3 \bmod 4}} \left(1 - \frac{1}{p}\right) \bigg\{ \frac{\sqrt{3}}{\varphi(b)} \sqrt{2\alpha} \int_1^{1/2\alpha} \frac{dt}{\sqrt{t(t-1)}} \\
\times \sum_{\nu\mid a} \frac{\mu(\nu)}{\varphi(\nu)} \sharp\{n : n \le x,\ (n, \nu bP(x)) = 1\} \prod_{\substack{p\mid b \\ p\equiv 3 \bmod 4}} \left(1 - \frac{1}{p-1}\right)
\end{aligned}$$

$$-\frac{1}{\varphi(a)}\prod_{\substack{p|a\\ p\equiv 3 \bmod 4}}\Big(1-\frac{1}{p-1}\Big)\sharp\Big\{mp_1p_2 : mp_1p_2\le Y,\ (m,P(Y))=1,\ Y^\alpha\le p_1<p_2\le Y^{1-\alpha}\}\Big\}+O(x\log^{-6/5}x).$$

By Lemma 4 we have

$$\sum_{\nu|a}\frac{\mu(\nu)}{\varphi(\nu)}\sharp\{n : n\le x,\ (n,\nu bP(x))=1\} = \sum_{\nu|a}\frac{\mu(\nu)}{\varphi(\nu)}\prod_{\substack{p|\nu b\\ p\equiv 1 \bmod 4}}\Big(1-\frac{1}{p}\Big)c\,\frac{x}{\sqrt{\log x}}+O\Big(\frac{x}{\log x}\Big).$$

Since $p_2>Y^\alpha$ the inequalities $mp_1\le Y^{1-\alpha}$ and $m\le Y^{1-2\alpha}$ hold. Hence

$$\sharp\{mp_1p_2 : mp_1p_2\le Y,\ (m,P(Y))=1,\ Y^\alpha\le p_1<p_2\le Y^{1-\alpha}\}$$
$$\le\sum_{\substack{m\le Y^{1-2\alpha}\\ (m,P(Y))=1}}\ \sum_{Y^\alpha\le p_1\le\sqrt{Y}}\frac{2Y}{mp_1\log Y^\alpha}\ll\frac{x}{\log x}\exp\Big(\sum_{\substack{m\le Y^{1-2\alpha}\\ p\equiv 1 \bmod 4}}\frac{1}{p}\Big)\log\frac{1}{2\alpha}$$
$$\ll\frac{x}{\sqrt{\log x}}\sqrt{1-2\alpha}\log\Big(1+\frac{1-2\alpha}{2\alpha}\Big).$$

From this we conclude that

$$S(x)\ge c_1\frac{x}{\log x}\big(\sqrt{1-2\alpha}-c_2\sqrt{1-2\alpha}\,(1-2\alpha)\big),$$

where c_1,c_2 are positive constants depending only on a,b,c. Choosing a suitable real number $1/3<\alpha<1/2$ gives

$$\sqrt{1-2\alpha}-c_2\sqrt{1-2\alpha}\,(1-2\alpha)\ge c_3>0.$$

This ends the proof of Theorem 1.

5. Proof of Theorem 3. As in the proof of Theorem 1 we start with the obvious lower estimate

$$\widetilde{S}(x):=\sharp\{n : n\le x,\ 2a(2n+1)=b(m+1),\ m,n\in B\}$$
$$\ge\widetilde{S}_1(x):=\sharp\Big\{n : n\le x,\ (n,P(x))=1,\ 2n+1\equiv 0 \bmod b,\ \big(\tfrac{2a}{b}(2n+1)-1,\ P(Y)\big)=1\Big\}$$

with $Y=\frac{2a}{b}(2x+1)$. Since $(ab,2)=1$ and $(n,P(x))=1$ we obtain $n\equiv 1 \bmod 4$ and $\frac{2a}{b}(2n+1)-1\equiv 1 \bmod 4$. Therefore, in the same way as before we have

$$\widetilde{S}(x)\ge\widetilde{S}_2(x)-\widetilde{S}_3(x)+O(x^{1-\alpha})$$

where $1/3<\alpha<1/2$ and

$$\begin{aligned}\widetilde{S}_2(x) &:= \sharp\big\{n : n \le x,\ 2n+1 \equiv 0 \bmod b,\ (n, P(x)) = 1,\\ &\qquad \big(\tfrac{2a}{b}(2n+1)-1, P(Y)\big) = 1\big\},\\ \widetilde{S}_3(x) &:= \sharp\big\{n : n \le x,\ 2n+1 \equiv 0 \bmod b,\ (n, P(x)) = 1,\\ &\qquad \tfrac{2a}{b}(2n+1)-1 = mp_1p_2,\ Y^\alpha \le p_1 < p_2 \le Y^{1-\alpha},\\ &\qquad p_1 \equiv p_2 \equiv 3 \bmod 4,\ (m, P(Y)) = 1\big\}.\end{aligned}$$

Using Lemmas 1 and 3 we get the lower estimate

$$\begin{aligned}\widetilde{S}_2(x) \ge \frac{1}{\varphi(b)}\, f\left(\frac{1}{2\alpha}\right)&\sharp\{n : n \le x,\ (n, P(x)) = 1\}\\ &\times \prod_{\substack{p<Y^\alpha\\ p\equiv 3 \bmod 4\\ p\nmid 2a(2a-b)}} \left(1 - \frac{\varphi(b)}{\varphi(bp)}\right) + O(x \log^{-6/5} x)\end{aligned}$$

and the upper estimates

$$\begin{aligned}\widetilde{S}_3(x) &\le \sharp\big\{mp_1p_2 : mp_1p_2 \le Y,\ (m, P(Y)) = 1,\ p_1 \equiv p_2 \equiv 3 \bmod 4,\\ &\qquad Y^\alpha \le p_1 < p_2 \le Y^{1-\alpha},\ mp_1p_2 + 1 \equiv 0 \bmod 2a,\\ &\qquad \big(\tfrac{1}{2}\big(\tfrac{b}{2a}(mp_1p_2+1)-1\big), P(Y^{\alpha/3})\big) = 1\big\}\\ &\le \prod_{\substack{p<Y^{\alpha/3}\\ p\in\mathcal{P}\\ p\nmid b(2a-b)}} \left(1 - \frac{\varphi(2a)}{\varphi(2ap)}\right)\frac{1}{\varphi(2a)}\sharp\{mp_1p_2 : mp_1p_2 \le Y,\ (m, P(Y)) = 1,\\ &\qquad Y^\alpha \le p_1 < p_2 \le Y^{1-\alpha},\ p_1 \equiv p_2 \equiv 3 \bmod 4\}\\ &\quad \times (F(1) + O(\log^{-1/5} x))\\ &\quad + \sum_{\substack{d\le Y^{\alpha/3}\\ d\mid P(Y^{\alpha/3})\\ (d,b(2a-b))=1}} \bigg|\sharp\{mp_1p_2 : mp_1p_2 \le y,\ (m, P(Y)) = 1,\\ &\qquad Y^\alpha \le p_1 < p_2 \le Y^{1-\alpha},\\ &\qquad p_1 \equiv p_2 \equiv 3 \bmod 4,\ bmp_1p_2 \equiv 2a - b \bmod 4ad\}\\ &\qquad - \frac{1}{\varphi(4ad)}\sharp\{mp_1p_2 : mp_1p_2 \le Y,\ (m, P(Y)) = 1,\\ &\qquad Y^\alpha \le p_1 < p_2 \le Y^{1-\alpha},\ p_1 \equiv p_2 \equiv 3 \bmod 4\}\bigg|.\end{aligned}$$

Collecting the estimates yields, as in the proof of Theorem 1,

$$\widetilde{S}_2(x) \ge c_1\sqrt{1-2\alpha}\,\frac{x}{\log x}, \qquad \widetilde{S}_3(x) \le c_2(1-2\alpha)^{3/2}\,\frac{x}{\log x},$$

where $c_1 > 0$ and $1/3 < \alpha < 1/2$. This leads to

$$\widetilde{S}(x) \ge \vartheta\,\frac{x}{\log x},$$

which ends the proof of Theorem 3.

6. Proof of Theorem 4. Let $a = 2^r b$ where b is odd, and let $s(a)$ be the smallest s such that the representation (7) holds.

If $0 \le r \le 1$ then, by Theorems 2 and 3, $s(a) = 1$ or 2, and $s(a) = 1$ holds if and only if $a - 1 \in B$.

Suppose now $r \ge 2$. By the representation (4) every $n \in B$ is either an even number or $n \equiv 1 \bmod 4$, and therefore $n+1$ is odd or $n+1 = 2(2k+1)$. Hence $s(2^r b) \ge r$.

Assume that $s(2^r b) = r$, i.e.

$$2^r b = (n_1 + 1) \cdots (n_r + 1) \qquad (n_i \in B,\ i = 1, \ldots, r).$$

Obviously this is equivalent to the existence of odd numbers $b_1, \ldots, b_r$ such that

(i) $b = b_1 \cdots b_r$,
(ii) $2b_i - 1 \in B$, $i = 1, \ldots, r$.

If these conditions do not hold then $s(2^r b) \ge r + 1$. On the other hand, by Theorem 3,

$$2^r b = (1^2 + 0^2 + 1)^{r-1} \cdot \frac{m+1}{n+1} \qquad \text{with } m, n \in B,$$

and thus $s(2^r b) = r + 1$.

As an example consider $a = 2^r \cdot 29$, $r \ge 2$. We have $2 \cdot 29 - 1 = 3 \cdot 19 \notin B$. Therefore $s(2^r \cdot 29) > r$ and

$$2^r \cdot 29 = (1^2 + 0^2 + 1)^{r-1} \cdot \frac{15^2 + 8^2 + 1}{2^2 + 0^2 + 1},$$

i.e. $s(2^r \cdot 29) = r + 1$. This proves Theorem 4.

7. Proofs of Theorems 5 and 6. It is well known that $n \in B(2)$ if and only if

$$n = 2^s n_1 n_2^2,$$

where $s \ge 0$ and all prime divisors of n_1 and n_2 are $\equiv 1$ or $3 \bmod 8$ and $\equiv 5$ or $7 \bmod 8$, respectively.

The proof of Theorem 5 follows the same lines as that of Theorem 1. Therefore we indicate only the necessary modifications.

Let

$$\mathcal{P}_1 := \{2\} \cup \{p : p \text{ prime}, p \equiv 5 \text{ or } 7 \bmod 8\}, \qquad P_1(x) := \prod_{\substack{p \le x \\ p \in \mathcal{P}_1}} p.$$

As before we may assume that c is an odd integer. We have

$$\begin{aligned}\widetilde{\widetilde{S}}(x) \ge S_4(x) := \sharp\big\{n : n \le x,\ n \equiv -c \bmod b,\ n \equiv \delta(c) \bmod 8,\ (n+c, a) = 1,\\ (n, P_1(x)) = 1,\ \big(\tfrac{a}{b}(n+c) - c, P_1(Y)\big) = 1\big\}\end{aligned}$$

where $\delta(c) = 1$ or 3 and $\delta(c) \equiv -c \bmod 4$, $Y = (a/b)(x+c) - c$. If $n \equiv \delta(c) \bmod 8$ then

$$\frac{a}{b}\,(n+c) - c \equiv \frac{a}{b}\,(\delta(c)+c) - c \equiv \delta(c) \bmod 8.$$

Hence, if $1/3 < \alpha < 1/2$,

$$\widetilde{\widetilde{S}}(x) \geq S_5(x) - S_6(x) + O(x^{1-\alpha})$$

where

$$\begin{aligned} S_5(x) := \sharp\big\{n : n \leq x,\ n \equiv -c \bmod b,\ n \equiv \delta(c) \bmod 8,& \\ (n+c,a) = 1,\ (n, P_1(x)) = 1,\ \big(\tfrac{a}{b}(n+c) - c, P_1(Y^\alpha)\big) = 1\big\},& \\ S_6(x) := \sharp\big\{n : n \leq x,\ n \equiv -c \bmod b,\ (n, P_1(x)) = 1,& \\ \tfrac{a}{b}(n+c) - c = mp_1p_2,\ Y^\alpha \leq p_1 < p_2 \leq Y^{1-\alpha},& \\ p_1 \equiv 5 \text{ or } 7 \text{ and } p_2 \equiv 5 \text{ or } 7 \bmod 8,\ (m, P_1(Y)) = 1\big\}.& \end{aligned}$$

Using Lemmata 1, 3 and 4 and the Vinogradov–Bombieri theorem we prove as before

$$S_5(x) \geq c_3(1-2\alpha)^{1/2}\,\frac{x}{\log x}, \qquad S_6(x) \leq c_4(1-2\alpha)^{3/2}\,\frac{x}{\log x}$$

with some positive constant c_3. Choosing α close to $1/2$ and such that $c_3 - c_4(1-2\alpha) > 0$ gives the assertion of Theorem 5.

For the proof of Theorem 6 we proceed in the same manner as in §2. We assume that g is completely multiplicative with $\lim_{i\to\infty} g(n_i + c) = 1$, where n_i runs through the set $B(2)$.

If p is prime, $p \nmid 2c$, then, by Theorem 5,

$$p = \frac{m+c}{n+c} \quad \text{for infinitely many } m, n \in B(2),$$

which implies $g(p) = 1$.

Thus we only have to show that $g(2) = 1$ and $g(p) = 1$ for all primes $p \mid c$.

We leave the case $p = 2$ to the reader and outline the proof for odd prime divisors p of c.

Assume $g(2) = 1$ and suppose $c = 2^s p^r c_1$, $s \geq 0$, $r \geq 1$ and $(c_1, 2p) = 1$. If r is even define l by $c_1 = l + 4pk$, $(l, 2p) = 1$. Choose $m, n \in \mathbb{Z}$ such that $m^2 + 2n^2 = 2^s p^r p_1$ where p_1 is prime, $p_1 \nmid 2c$ and $p_1 = 1 + 8l_1 + 8pt$ with $p \nmid (1 + 8l_1 + l)$. This choice is possible: if $p \nmid (1+l)$ put $l_1 = p$; if $p \mid (1+l)$ and $p \neq 3$ let $l_1 = 1$, and if $p = 3 \mid (1+l)$ let $l_1 = -1$.

Thus we obtain $m^2 + 2n^2 + c = 2^s p^r (p_1 + c_1) = 2^{s'} p^r c_2$ with $(c_2, 2c) = 1$. Then choosing p_1 large enough leads to

$$g(p^r) = 1.$$

Next we show $g(p^{r+1}) = 1$, which implies $g(p) = 1$. For this let $m, n \in \mathbb{Z}$ satisfy $m^2 + 2n^2 = 2^s p^r p_2$ where the prime p_2 is chosen such that $p_2 \equiv 1 \bmod 8$, $p_2 \nmid 2c$, $p_2 + c_1 \equiv 0 \bmod p$ and $p^2 \nmid (p_2 + c_1)$. Again, this choice is possible: if $c_1 = l + 4p^2 k$, $(l, 2p) = 1$, we put $p_2 = 1 + 8l_1 + 8p^2 t$, where $1 + 8l_1 + l \equiv 0 \bmod p$ and $1 + 8l_1 + l \not\equiv 0 \bmod p^2$; if $c_1 = l + 4kp$, $(k, p) = 1$ we let $p_2 = 1 + 8l_1 + 8p^2 t$, where $1 + 8l_1 + l \equiv 0 \bmod p^2$.

Now $m^2 + n^2 + c = 2^{s_1} p^{r+1} c_2$ with $(c_2, 2c) = 1$. Hence $g(2^{s_1} c_2) = 1$ and again, since p_2 can be chosen arbitrarily large,

$$g(p^{r+1}) = 1.$$

The case of r odd can be handled in a similar way, and this proves Theorem 6.

References

[1] F. Dress et B. Volkmann, *Ensembles d'unicité pour les fonctions arithmétiques additives ou multiplicatives*, C. R. Acad. Sci. Paris Sér. A 287 (1978), 43–46.

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

[3] —, *The multiplicative group of rationals generated by the shifted primes*, *I*, J. Reine Angew. Math. 463 (1995), 169–216.

[4] J. Fehér, K.-H. Indlekofer and L. L. Stachó, *On sets of uniqueness for completely additive arithmetic functions*, Analysis 16 (1996), 405–415.

[5] J. Fehér, K.-H. Indlekofer and N. M. Timofeev, *A set of uniqueness for completely additive arithmetic functions*, Ann. Univ. Sci. Budapest Sect. Comput. 21 (2002), 57–67.

[6] K.-H. Indlekofer, *On sets characterizing additive arithmetical functions*, Math. Z. 146 (1976), 285–290.

[7] —, *Scharfe untere Abschätzung für die Anzahlfunktion der B-Zwillinge*, Acta Arith. 26 (1974), 207–212.

[8] —, *On sets characterizing additive and multiplicative arithmetical functions*, Illinois J. Math. 25 (1981), 251–257.

[9] —, *Zahlentheorie: Eine Einführung*, Birkhäuser, Basel, 1978.

[10] K.-H. Indlekofer and A. Járai, *Largest known twin primes and Sophie Germain primes*, Math. Comp. 68 (1999), 1317–1324.

[11] H. Iwaniec, *The half-dimensional sieve*, Acta Arith. 29 (1976), 69–95.

[12] I. Kátai, *On sets characterizing number-theoretical functions*, ibid. 13 (1968), 315–320.

[13] —, *On sets characterizing number-theoretical functions* (*II*). (*The set of "prime plus one" 's is a set of quasi-uniqueness*), ibid. 16 (1969), 1–4.

[14] E. Landau, *Handbuch der Lehre von der Verteilung der Primzahlen*, 2. Bd., Teubner, Leipzig, 1909.

[15] B. V. Levin and N. M. Timofeev, *Distribution of arithmetic functions in the mean over progressions* (*theorems of the Vinogradov–Bombieri type*), Math. USSR-Sb. 53 (1986), 563–579.

[16] K. Prachar, *Primzahlverteilung*, Grundlehren Math. Wiss. 91, Springer, Berlin, 1957.

[17] A. Selberg, *Lectures on sieves*, in: Collected Papers, Vol. II, Springer, 1991.

[18] D. Wolke, *Bemerkungen über Eindeutigkeitsmengen additiver Funktionen*, Elem. Math. 33 (1978), 14–16.

Faculty of Computer Science,
Electrical Engineering and Mathematics
University of Paderborn
Warburger Straße 100
33098 Paderborn, Germany
E-mail: k-heinz@math.uni-paderborn.de

Received on 18.3.2003 (4490)