PUBLICATIONS DE L'INSTITUT MATHÉMATIQUE
Nouvelle série, tome 77(91) (2005), 71–78

ON THE DISTRIBUTION OF M-TUPLES OF B-NUMBERS

Werner Georg Nowak

Communicated by Aleksandar Ivić

ABSTRACT. In the classical sense, the set B consists of all integers which can be written as a sum of two perfect squares. In other words, these are the values attained by norms of integral ideals over the Gaussian field $\mathbb{Q}(i)$. G. J. Rieger (1965) and T. Cochrane, R. E. Dressler (1987) established bounds for the number of pairs $(n, n+h)$, resp., triples $(n, n+1, n+2)$ of B-numbers up to a large real parameter x. The present article generalizes these investigations into two directions: The result obtained deals with arbitrary M-tuples of arithmetic progressions of positive integers, excluding the trivial case that one of them is a constant multiple of one of the others. Furthermore, the estimate applies to the case of an arbitrary normal extension K of the rational field instead of $\mathbb{Q}(i)$.

1. Introduction. Already E. Landau's in his classic monograph [4] provided a proof of the result that the set B of all positive integers which can be written as a sum of two squares of integers is distributed fairly regularly: It satisfies the asymptotic formula

$$\sum_{1 \leqslant n \leqslant x,\ n \in B} 1 \sim \frac{c\,x}{\sqrt{\log x}} \qquad (c > 0)\,. \tag{1.1}$$

Almost six decades later, G. J. Rieger [9] was the first to deal with the question of "B-twins": How frequently does it happen that both n and $n+1$ belong to the

2000 *Mathematics Subject Classification.* Primary 11P05, 11N35.

Key words and phrases. B-numbers; Selberg sieve; norms of ideals in number fields.

The author gratefully acknowledges support from the Austrian Science Fund (FWF) under project Nr. P18079-N12.

set B? A bit more general, he was able to show that, for any positive integer h and large real x,

$$\sum_{\substack{1\leqslant n\leqslant x\\ n\in B,\ n+h\in B}} 1 \ll \prod_{\substack{p\mid h\\ p\equiv 3 \pmod 4}} \left(1+\frac{1}{p}\right)\frac{x}{\log x}\,. \tag{1.2}$$

Later on, C. Hooley [2] and K.-H. Indlekofer [3], independently and at about the same time, showed that this bound is essentially best possible. In 1987, T. Cochrane and R. E. Dressler [1] extended the question to triples of B-numbers. Replacing Rieger's sieve technique by a more recent variant of Selberg's method, they succeeded in proving that

$$\sum_{\substack{1\leqslant n\leqslant x\\ n\in B,\, n+1\in B,\, n+2\in B}} 1 \ll \frac{x}{(\log x)^{3/2}}\,. \tag{1.3}$$

2. Statement of result. In this article we intend to generalize these estimates in two different directions: Firstly, instead of pairs or triples we consider M-tuples of arithmetic progressions $(a_m n+b_m)$, $m=1,\dots,M\geqslant 2$, where $a_m\in\mathbb{Z}^+$, $b_m\in\mathbb{Z}$ throughout. Secondly, we deal with an arbitrary number field K which is supposed to be a normal extension of the rationals of degree $[K:\mathbb{Q}]=N\geqslant 2$. Denoting by $\mathcal{O}_K$ the ring of algebraic integers in K, we put

$$\boldsymbol{b}_K(n) := \begin{cases} 1 & \text{if there exists an integral ideal } \mathfrak{A} \text{ in } \mathcal{O}_K \text{ of norm } \mathcal{N}(\mathfrak{A})=n,\\ 0 & \text{else.}\end{cases}$$

Our target is then the estimation of the sum

$$S(x)=S(a_1,b_1,\dots,a_M,b_M;\,x) := \sum_{1\leqslant n\leqslant x}\prod_{m=1}^{M}\boldsymbol{b}_K(a_m n+b_m)\,. \tag{2.1}$$

Of course, the classic case reported in section 1 is contained in this, by the special choice $K=\mathbb{Q}(i)$, the Gaussian field.

Theorem. *Suppose that $(a_m,b_m)\in\mathbb{Z}^+\times\mathbb{Z}$ for $m=1,\dots,M$, and, furthermore,*

$$\prod_{\substack{m,k=1\\ m\neq k}}^{M}(a_m b_k - a_k b_m) \neq 0\,.$$

Then, for large real x,

$$S(a_1,b_1,\dots,a_M,b_M;\,x) \ll \gamma(a_1,b_1,\dots,a_M,b_M)\,\frac{x}{(\log x)^{M(1-1/N)}}\,,$$

with

$$\gamma(a_1,b_1,\dots,a_M,b_M)=\prod_{p\in\mathbb{P}'}\left(1+\frac{M}{p}\right),$$

the finite set of primes $\mathbb{P}'=\mathbb{P}'(a_1,b_1,\dots,a_M,b_M)$ to be defined below in (4.6). The $\ll$-constant depends on M and the field K, but not on $a_1,b_1,\dots,a_M,b_M$.

3. Some auxiliary results. *Notation.* Variables of summation automatically range over all integers satisfying the conditions indicated. p denotes rational primes throughout, and $\mathbb{P}$ is the set of all rational primes. $\mathfrak{P}$ stands for prime ideals in $\mathcal{O}_K$. For any subset $\mathbb{P}^\circ \subseteq \mathbb{P}$, we denote by $\mathcal{D}(\mathbb{P}^\circ)$ the set of all positive integers whose prime divisors all belong to $\mathbb{P}^\circ$. The constants implied in the symbols $O(\cdot)$, $\ll$, $\gg$, etc., may depend throughout on the field K and on M, but not on $a_1, b_1, \dots, a_M, b_M$.

LEMMA 1. *For each prime power p^α, $\alpha \geqslant 1$, let $\overline{\Omega}(p^\alpha)$ be a set of distinct residue classes $\bar{\mathfrak{c}}$ modulo p^α. Define further*

$$\Omega(p^\alpha) = \left\{ n \in \mathbb{Z}^+ : n \in \bigcup_{\bar{\mathfrak{c}} \in \overline{\Omega}(p^\alpha)} \bar{\mathfrak{c}} \right\},$$

and let

$$\theta(p^\alpha) := 1 - \sum_{j=1}^{\alpha} \frac{\#\overline{\Omega}(p^j)}{p^j} > 0\,, \qquad \theta(1) := 1\,.$$

Suppose that $\Omega(p^\alpha) \cap \Omega(p^{\alpha'}) = \emptyset$ for all primes p and positive integers $\alpha \neq \alpha'$. For real $x > 0$, let finally

$$A(x) = \left\{ n \in \mathbb{Z}^+ : n \leqslant x \ \ \& \ \ n \notin \bigcup_{p \in \mathbb{P},\, \alpha \in \mathbb{Z}^+} \Omega(p^\alpha) \right\}.$$

Then, for arbitrary real $Y > 1$,

$$\#A(x) \leqslant \frac{x + Y^2}{V_Y}\,,$$

where

$$V_Y := \sum_{0<d<Y} \ \prod_{p^\alpha \,\|\, d} \left(\frac{1}{\theta(p^\alpha)} - \frac{1}{\theta(p^{\alpha-1})} \right).$$

Proof. This is a deep sieve theorem due to A. Selberg [10]. It can be found in Y. Motohashi [5, p. 11], and also in T. Cochrane and R. E. Dressler [1].

LEMMA 2. *Let $(c_n)_{n \in \mathbb{Z}^+}$ be a sequence of nonnegative reals, and suppose that the Dirichlet series*

$$f(s) = \sum_{n=1}^{\infty} c_n\, n^{-s}$$

converges for $\mathrm{Re}(s) > 1$. *Assume further that, for some real constants A and $\beta > 0$,*

$$f(s) = (A + o(1))(s-1)^{-\beta}\,,$$

as $s \to 1+$. Then, for $x \to \infty$,

$$\sum_{1 \leqslant n \leqslant x} \frac{c_n}{n} \ = \ \left(\frac{A}{\Gamma(1+\beta)} + o(1) \right) (\log x)^\beta\,.$$

Proof. This is a standard Tauberian theorem. For the present formulation, cf. Cochrane and Dressler [1, Lemma B].

4. Proof of the Theorem. We recall the decomposition laws in a normal extension K over $\mathbb{Q}$ of degree $N \geqslant 2$ (cf. W. Narkiewicz [6, Theorem 7.10]): Every rational prime p which does not divide the field discriminant $\mathrm{disc}(K)$ belongs to one of the classes

$$\mathbb{P}_r = \left\{p \in \mathbb{P} : (p) = \mathfrak{P}_1 \cdots \mathfrak{P}_{N/r},\ \mathcal{N}(\mathfrak{P}_1) = \cdots = \mathcal{N}(\mathfrak{P}_{N/r}) = p^r\right\},$$

where r ranges over the divisors of N, and $\mathfrak{P}_1, \ldots, \mathfrak{P}_{N/r}$ are distinct. As an easy consequence, if $p \in \mathbb{P}_r$, $\alpha \in \mathbb{Z}^+$,

$$\boldsymbol{b}_K(p^\alpha) = \begin{cases} 1, & \text{if } r|\alpha, \\ 0, & \text{else.} \end{cases} \tag{4.1}$$

In order to apply Lemma 1, we need a bit of preparation. Let

$$\mathbb{P}_r^* = \left\{p \in \mathbb{P}_r : p \nmid \prod_{m=1}^{M} a_m \prod_{\substack{m,k=1 \\ m \neq k}}^{M} (a_m b_k - a_k b_m),\ p \neq M-1\right\},$$
$$\mathbb{P}^* = \bigcup_{r|N,\, r>1} \mathbb{P}_r^*.$$

Then we choose

$$\overline{\Omega}(p^\alpha) := \bigcup_{m=1}^{M} \left\{\overline{a_m}^{\,(-1)}\overline{(jp^{\alpha-1} - b_m)} : j = 1, \ldots, p-1\right\},$$

if $p \in \mathbb{P}_r^*$ and $r \nmid (\alpha-1)$, while $\overline{\Omega}(p^\alpha) := \emptyset$ in all other cases. Here $\overline{\cdot}$ denotes residue classes modulo p^α, in particular $\overline{a_m}^{\,(-1)}$ is the class which satisfies $\overline{a_m}\ \overline{a_m}^{\,(-1)} = \overline{1}$ mod p^α. We summarize the relevant properties of these sets $\overline{\Omega}(p^\alpha)$, and of the corresponding sets $\Omega(p^\alpha)$ (see Lemma 1), as follows.

PROPOSITION. *Suppose throughout that $p \in \mathbb{P}^*$ and $\alpha \in \mathbb{Z}^+$.*

(i) *If $p \in \mathbb{P}_r^*$, $r \nmid (\alpha-1)$, then $\overline{\Omega}(p^\alpha)$ contains exactly $M(p-1)$ elements.*

(ii) *If a positive integer k lies in some $\Omega(p^\alpha)$, it follows that there exists an $m \in \{1, \ldots, M\}$ such that $p^{\alpha-1} \parallel (a_m k + b_m)$.*

(iii) *It is impossible that there exist $m, n \in \{1, \ldots, M\}$, $m \neq n$, and a positive integer k, such that some $p \in \mathbb{P}^*$ divides both $a_m k + b_m$ and $a_n k + b_n$.*

(iv) *If $k \in \Omega(p^\alpha)$, it follows that*

$$p^{\alpha-1} \parallel \prod_{m=1}^{M} (a_m\, k + b_m).$$

Consequently, $\Omega(p^\alpha) \cap \Omega(p^{\alpha'}) = \emptyset$ for any positive integers $\alpha \neq \alpha'$.

(v) *If* $k \in \Omega(p^\alpha)$, *then*

$$\prod_{m=1}^{M} \boldsymbol{b}_K(a_m\, k + b_m) = 0\,.$$

As a consequence,

$$S(x) \leqslant \#A(x)\,,$$

where $S(x)$ *and* $A(x)$ *have been defined in* (2.1) *and Lemma 1, respectively.*

Proof of the Proposition. (i) Assume that two of these residue classes would be equal, say, $\overline{a_m}^{(-1)}\overline{(u\,p^{\alpha-1} - b_m)}$ and $\overline{a_n}^{(-1)}\overline{(v\,p^{\alpha-1} - b_n)}$, where $u, v \in \{1, \ldots, p-1\}$, $m, n \in \{1, \ldots, M\}$. Multiplying by $\overline{a_m}\,\overline{a_n}$, we could conclude that

$$a_n(u\,p^{\alpha-1} - b_m) \equiv a_m(v\,p^{\alpha-1} - b_n) \qquad \bmod\ p^\alpha\,,$$

or, equivalently, that

$$(a_n\,u - a_m\,v)p^{\alpha-1} \equiv a_n\,b_m - a_m\,b_n \qquad \bmod\ p^\alpha\,. \tag{4.2}$$

Hence $p\,|(a_n\,b_m - a_m\,b_n)$, which is only possible if $m = n$. This in turn simplifies (4.2) to

$$a_m(u - v)p^{\alpha-1} \equiv 0 \qquad \bmod\ p^\alpha\,,$$

thus also $u = v$. □

(ii) If $k \in \Omega(p^\alpha)$, there exist $j \in \{1, \ldots, p-1\}$, $m \in \{1, \ldots, M\}$, and an integer q, such that

$$a_m\,k = j\,p^{\alpha-1} - b_m + q\,p^\alpha\,.$$

From this the assertion is obvious. □

(iii) Assuming the contrary, we would infer that p divides

$$(a_m\,k + b_m)b_n - (a_n\,k + b_n)b_m = (a_m\,b_n - a_n\,b_m)k\,,$$

hence $p\,|k$, thus p divides also b_m and b_n, which contradicts $p \in \mathbb{P}^*$. □

(iv) This is immediate from (ii) and (iii). □

(v) By (ii), $p^{\alpha-1} \parallel (a_m\,k + b_m)$ for some $m \in \{1, \ldots, M\}$. Recalling that $r \nmid (\alpha-1)$ (otherwise $\Omega(p^\alpha)$ would be empty), along with (4.1) and the multiplicativity of $\boldsymbol{b}_K(\cdot)$, it is clear that $\boldsymbol{b}_K(a_m k + b_m) = 0$. The last inequality is obvious from the relevant definitions. □

We are now ready to apply Lemma 1. Choosing $Y = \sqrt{x}$ and appealing to part (v) of the Proposition, we see that

$$S(x) \leqslant \frac{2x}{V_Y}\,. \tag{4.3}$$

To derive a lower bound for V_Y, observe that $\overline{\Omega}(p) = \emptyset$ for every prime p, and $\#\overline{\Omega}(p^2) = M(p-1)$ for each $p \in \mathbb{P}^*$. Further, if $p \notin \mathbb{P}^*$, then $\overline{\Omega}(p^j) = \emptyset$ throughout. Therefore, if $p \in \mathbb{P}^*$, then $\theta(p) = 1$ and

$$\theta(p^2) = 1 - \frac{1}{p^2}\,\#\overline{\Omega}(p^2) = 1 - \frac{M(p-1)}{p^2}\,,$$

hence

$$\frac{1}{\theta(p^2)} - \frac{1}{\theta(p)} = \frac{M(p-1)}{p^2 - M(p-1)} \geqslant \frac{M}{p}\,. \tag{4.4}$$

Furthermore, for any $\alpha > 2$,

$$\theta(p^\alpha) \geqslant 1 - M(p-1) \sum_{2 \leqslant j \leqslant \alpha} p^{-j} > 1 - \frac{M}{p} \geqslant 0\,,$$

since $M(p-1) \leqslant p^2 - 1$ according to clause (i) of the Proposition, and $M = p+1$ is impossible for $p \in \mathbb{P}^*$. Thus actually $\theta(p^\alpha) > 0$ for all primes p and all $\alpha \in \mathbb{Z}^+$. Thus all the terms in the sum V_Y are nonnegative, and restricting the summation to the set

$$Q := \left\{ d = d_1^2 :\ d_1 \in \mathbb{Z}^+,\ \mu(d_1) \neq 0,\ d_1 \in \mathcal{D}(\mathbb{P}^*) \right\}\,,$$

we conclude by (4.4) that

$$\begin{aligned} V_Y &\geqslant \sum_{0<d<Y,\, d \in Q} \prod_{p \mid d} \left(\frac{1}{\theta(p^2)} - \frac{1}{\theta(p)} \right) \geqslant \sum_{0<d_1<\sqrt{Y},\, d_1 \in \mathcal{D}(\mathbb{P}^*)} \mu^2(d_1) \prod_{p \mid d_1} \frac{M}{p} = \\ &= \sum_{0<d_1<\sqrt{Y},\, d_1 \in \mathcal{D}(\mathbb{P}^*)} \mu^2(d_1)\, \frac{M^{\omega(d_1)}}{d_1}\,, \end{aligned} \tag{4.5}$$

where $\omega(d_1)$ denotes the number of primes dividing d_1. Our next step is to take care of the primes excluded in the construction of $\mathbb{P}^*$. We define

(4.6)

$$\mathbb{P}' = \mathbb{P}'(a_1, b_1, \dots, a_M, b_M) := \left\{ p \in \bigcup_{\substack{r \mid N \\ r>1}} \mathbb{P}_r : p \mid \prod_{m=1}^{M} a_m \prod_{\substack{m,k=1 \\ m \neq k}}^{M} (a_m b_k - a_k b_m) \right\}$$

and

$$\gamma = \gamma(a_1, b_1, \dots, a_M, b_M) := \prod_{p \in \mathbb{P}'} \left(1 + \frac{M}{p} \right) = \sum_{k_1 \in \mathcal{D}(\mathbb{P}')} \mu^2(k_1)\, \frac{M^{\omega(k_1)}}{k_1}\,. \tag{4.7}$$

Putting finally

$$\mathbb{P}_\cup := \bigcup_{r \mid N,\, r>1} \mathbb{P}_r\,,$$

we readily infer from (4.5) and (4.7) that

$$\gamma V_Y \gg \sum_{k<\sqrt{Y},\, k\in\mathcal{D}(\mathbb{P}_\cup)} \mu^2(k)\,\frac{M^{\omega(k)}}{k}\,. \tag{4.8}$$

We shall estimate this latter sum by the corresponding generating function

$$f(s) := \sum_{k\in\mathcal{D}(\mathbb{P}_\cup)} \mu^2(k)\,\frac{M^{\omega(k)}}{k^s} = \prod_{p\in\mathbb{P}_\cup}\Big(1+\frac{M}{p^s}\Big) \qquad (\mathrm{Re}(s)>1)\,,$$

applying Lemma 2. By $h_1(s), h_2(s), \ldots$ we will denote functions which are holomorphic and bounded, both from above and away from zero, in every half-plane $\mathrm{Re}(s) \geqslant \sigma_0 > 1/2$. We first observe that

$$f(s) = h_1(s)\prod_{p\in\mathbb{P}_\cup}\big(1-p^{-s}\big)^{-M} \qquad (\mathrm{Re}(s)>1)\,. \tag{4.9}$$

This follows by a standard argument which can be found exposed neatly in G. Tenenbaum [11, p. 200]. The next step is to consider the Euler product of the Dedekind zeta-function $\zeta_K(s)$: For $\mathrm{Re}(s)>1$,

$$\begin{aligned}\zeta_K(s) &= \prod_{\mathfrak{P}}\big(1-\mathcal{N}(\mathfrak{P})^{-s}\big)^{-1} = h_2(s)\prod_{r|N}\Bigg(\prod_{p\in\mathbb{P}_r}\big(1-p^{-rs}\big)^{-N/r}\Bigg) = \\ &= h_3(s)\prod_{p\in\mathbb{P}_1}\big(1-p^{-s}\big)^{-N}\,.\end{aligned}$$

Therefore,

$$\frac{\big(\zeta(s)\big)^M}{\big(\zeta_K(s)\big)^{M/N}} = h_4(s)\prod_{p\in\mathbb{P}_\cup}\big(1-p^{-s}\big)^{-M} \qquad (\mathrm{Re}(s)>1)\,.$$

Comparing this with (4.9), we arrive at

$$f(s) = h_5(s)\,\frac{\big(\zeta(s)\big)^M}{\big(\zeta_K(s)\big)^{M/N}}\,.$$

From this it is evident that, as $s\to 1+$,

$$f(s) \sim h_5(1)\,\rho_K^{-M/N}\,(s-1)^{-M+M/N}\,,$$

where ρ_K denotes the residue of $\zeta_K(s)$ at $s=1$. Lemma 2 now immediately implies that

$$\sum_{k<\sqrt{Y},\, k\in\mathcal{D}(\mathbb{P}_\cup)} \mu^2(k)\,\frac{M^{\omega(k)}}{k} \gg (\log Y)^{M-M/N} \gg (\log x)^{M-M/N}\,,$$

in view of our earlier choice $Y=\sqrt{x}$. Combing this with (4.3) and (4.8), we complete the proof of our Theorem. □

5. Concluding remarks. 1. Taking more care and imposing special conditions on the numbers $a_1, b_1, \ldots, a_M, b_M$, one could improve slightly on the factor γ in our estimate. (Observe that Rieger's bound (1.2) is in fact a bit sharper than our general result.) But it is easy to see that γ is rather small anyway: By elementary facts about the Euler totient function (see K. Prachar [8, p. 24–28]),

$$\gamma(a_1, b_1, \ldots, a_M, b_M) \ll \prod_{p \in \mathbb{P}'} \left(1 - \frac{1}{p}\right)^{-M} \ll (\log\log x)^M ,$$

under the very mild restriction that, for some constant $c > 0$,

$$\max_{m=1,\ldots,M} \bigl(a_m, |b_m|\bigr) \ll \exp((\log x)^c) .$$

2. As far as the asymptotics (1.1) is concerned, the generalization to an arbitrary normal extension K of $\mathbb{Q}$ can be found in W. Narkiewicz' monograph [6, p. 361, Prop. 7.11], where it is attributed to E. Wirsing. For this question, the case of non-normal extensions K has been dealt with by R. W. K. Odoni [7]. It may be interesting to extend our present problem to the non-normal case as well. We might return to this at a later occasion.

References

[1] T. Cochrane and R. E. Dressler, *Consecutive triples of sums of two squares,* Arch. Math. (Basel) 49 (1987), 301–304.

[2] C. Hooley, *On the intervals between numbers that are sums of two squares, III*, J. Reine Angew. Math. 267 (1974), 207–218.

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

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

[5] Y. Motohashi, *Lectures on Sieve Methods and Prime Number Theory*, Tata Institute of Fund. Research, Bombay, 1983.

[6] W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, 2nd ed., Springer & PWN, Berlin, 1990.

[7] R. W. K. Odoni, *On the norms of algebraic integers*, Mathematika 22 (1975), 71–80.

[8] K. Prachar, *Primzahlverteilung*, Springer, Berlin–Göttingen–Heidelberg, 1957.

[9] G. J. Rieger, *Aufeinanderfolgende Zahlen als Summen von zwei Quadraten*, Indag. Math. 27 (1965), 208–220.

[10] A. Selberg, *Remarks on multiplicative functions*, Number Theory Day, Proc. Conf., New York, 1976, Lecture Notes in Math. 626 (1977), 232–241.

[11] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, Cambridge University Press, 1995.

Institute of Mathematics
Department of Integrative Biology
Universität für Bodenkultur Wien
Gregor Mendel-Straße 33
1180 Wien, Austria

nowak@mail.boku.ac.at
http://www.boku.ac.at/math/nth.html

(Received 05 10 2004)