COLLOQUIUM MATHEMATICUM

VOL. XLV 1981 FASC. 1

NUMBERS WITH ALL FACTORIZATIONS OF THE SAME LENGTH IN A QUADRATIC NUMBER FIELD

BY

W. NARKIEWICZ (WROCŁAW)

1. Let K be a quadratic number field and denote by $G(x)$ the number of positive rational integers not exceeding x which have all their factorizations into irreducibles in K of the same length. In [1] it was shown that for x tending to infinity one has

$$G(x) = \big(C_K + o(1)\big)x\frac{(\log\log x)^N}{(\log x)^{1/2-1/2h-g/2h}}, \tag{1}$$

where h denotes the class number of K, g is the number of even invariants of the class group H of K, C_K is a positive constant depending on K, and $N = N(H)$ is a nonnegative integer which depends only on H.

In this note we shall obtain bounds for $N(H)$ and in the case when H is a p-group we shall express $N(H)$ in terms of Davenport's constant. (Let us recall that *Davenport's constant* $D(A)$ is defined for a given abelian group A as the minimal number s with the property that from every sequence of s elements of A one can extract a subsequence with vanishing sum.)

We prove the following result:

THEOREM. *Let H_0 denote the subgroup of H generated by elements of order* 2. *If*

$$H/H_0 \simeq \bigoplus_{i=1}^{M} Z/n_iZ,$$

then

$$\sum_{i=1}^{M}(n_i-1) \leqslant N(H) \leqslant D(H/H_0)-1.$$

Note that the sum on the left-hand side attains its maximal value in the case of the canonical factorization of H/H_0, i.e. in case where $n_1|n_2|\ldots|n_M$.

COROLLARY 1. *If H/H_0 is a p-group,*

$$H/H_0 = \bigoplus_{i=1}^{M} Z/p^{n_i}Z,$$

then

$$N(H) = D(H/H_0)-1 = \sum_{i=1}^{M}(p^{n_i}-1).$$

COROLLARY 2. *$N(H)$ is positive except when $H = C_2^N$ for a certain N.*

2. We recall the description of $N(H)$ given in [1]. Write $H = \bigoplus Z/h_iZ$, where $h_1, \ldots, h_g$ are even and $h_{g+1}, \ldots, h_r$ are odd, and consider r-tuples $\langle a_1, \ldots, a_r\rangle$ of nonnegative rational integers satisfying the following conditions:

(i) $a_1+ \ldots +a_r > 0$,

(ii) $0 \leqslant a_i \leqslant h_i-1$ $(i = 1, 2, \ldots, r)$,

(iii) $a_1 \leqslant h_1/2$ and if for a certain s we have either $a_i = 0$ or $a_i = h_i/2$ for all $i = 1, 2, \ldots, s-1$, then $a_s \leqslant h_s/2$.

Let now $a^{(j)} = \langle a_1^{(j)}, \ldots, a_r^{(j)}\rangle$ $(j = 1, 2, \ldots, n)$ be such r-tuples and assume that for $j = 1, 2, \ldots, g$ we have $2a_i^{(j)} \equiv 0 \pmod{h_i}$ $(i = 1, 2, \ldots, r)$. Moreover, let $A_{g+1}, \ldots, A_r$ be given positive integers. The system

$$\langle a^{(1)}, \ldots, a^{(n)};\ A_{g+1}, \ldots, A_r\rangle$$

is called ***admissible*** provided for any two different sequences $(\varepsilon_1, \ldots, \varepsilon_n)$ and $(\eta_1, \ldots, \eta_n)$ satisfying

$$(2)\qquad \begin{aligned} &0 \leqslant \varepsilon_i, \eta_i \leqslant 1 \quad (i = 1, 2, \ldots, g),\\ &0 \leqslant \varepsilon_i, \eta_i \leqslant A_i \quad (i = 1+g, \ldots, n)\end{aligned}$$

there is an index k such that

$$\sum_{i=1}^{n} \varepsilon_i a_k^{(i)} \not\equiv \sum_{i=1}^{n} \eta_i a_k^{(i)} \pmod{h_k}.$$

It was established in [1] that $N(H)$ equals the maximal value of $A_{g+1}+ \ldots +A_n$ for admissible systems.

LEMMA. *Let $x_1, \ldots, x_g$ be a basis of $H_0 \simeq (Z/2Z)^g$ and let $N_0(H)$ be equal to the maximal possible value of the sum $B_1+ \ldots +B_m$ such that there exist elements $y_1, \ldots, y_m$ in H with the property that all sums*

$$(3)\qquad \sum_{i=1}^{g} a_i x_i + \sum_{j=1}^{m} \beta_j y_j$$

$$(0 \leqslant a_i \leqslant 1\ (i = 1, 2, \ldots, g),\ 0 \leqslant \beta_j \in B_j\ (j = 1, 2, \ldots, m))$$

are distinct. Then $N(H) = N_0(H)$.

Proof. If the maximal value of $N_0(H)$ is realized by $y_1, \ldots, y_m$ and $B_1, \ldots, B_m$ so that sums (3) are distinct and $N_0(H) = B_1 + \ldots + B_m$, then we construct an admissible system as follows: Let $t_1, \ldots, t_r$ be independent generators of H. For $j = 1, 2, \ldots, m$ write

$$y_j = \sum_{i=1}^{r} \gamma_j^{(i)} t_i \qquad (0 \leqslant \gamma_j^{(i)} < h_i).$$

Then, clearly,

$$-y_j = \sum_{i=1}^{r} \hat{\gamma}_j^{(i)} t_i$$

with

$$\hat{\gamma}_j^{(i)} = \begin{cases} h_i - \gamma_j^{(i)} & \text{if } \gamma_j^{(i)} \neq 0, \\ 0 & \text{if } \gamma_j^{(i)} = 0, \end{cases}$$

and we see that at least one of the r-tuples $\langle \gamma_j^{(1)}, \ldots, \gamma_j^{(r)} \rangle$, $\langle \hat{\gamma}_j^{(1)}, \ldots, \hat{\gamma}_j^{(r)} \rangle$ satisfies (i), (ii) and (iii). Denote it by

$$a^{(g+j)} = \langle a_1^{(g+j)}, \ldots, a_r^{(g+j)} \rangle.$$

Note that with $s(j) = 0$ or 1 we have

$$\sum_{k=1}^{r} a_k^{(j)} t_k = (-1)^{s(j)} y_j. \tag{4}$$

Moreover, for $j = 1, 2, \ldots, g$ put

$$a^{(j)} = \left\langle \delta_1^j \frac{h_j}{2}, \ldots, \delta_r^j \frac{h_j}{2} \right\rangle$$

and let $A_{g+j} = B_j$ for $j = 1, 2, \ldots, m$. We claim that the system

$$\langle a^{(1)}, \ldots, a^{(m+g)}; A_{1+g}, \ldots, A_{m+g} \rangle \tag{5}$$

is admissible. Indeed, otherwise we could find distinct sequences $(\varepsilon_1, \ldots, \varepsilon_{m+g})$ and $(\eta_1, \ldots, \eta_{m+g})$ satisfying (2) and

$$\sum_{j=1}^{m+g} \varepsilon_j a_k^{(j)} \equiv \sum_{j=1}^{m+g} \eta_j a_k^{(j)} \pmod{h_k} \qquad (k = 1, 2, \ldots, r).$$

Summing over k and using (4) and the equality

$$\sum_{k=1}^{r} a_k^{(j)} t_k = x_j \qquad (j = 1, 2, \ldots, g),$$

we arrive at equality of two sums of form (3). This contradiction shows that system (5) is admissible, thus $N(H) \geqslant N_0(H)$. To obtain the converse inequality it is sufficient to observe that every r-tuple satisfying (i), (ii) and (iii) induces an element of H by

$$\langle a_1, \ldots, a_r\rangle \mapsto \sum_{i=1}^{r} a_i t_i$$

and one sees immediately that in this way admissible systems induce subsets of H which satisfy the condition concerning sums (3).

COROLLARY. *The number $N(H)$ is the maximal value of $A_1 + \ldots + A_m$ for which there are elements $y_1, \ldots, y_m$ in H such that all sums*

$$\sum_{i=1}^{m} \varepsilon_i y_i \quad (0 \leqslant \varepsilon_i \leqslant A_i)$$

are distinct $(\operatorname{mod} H_0)$.

For the proof it suffices to note that

$$H_0 = \Big\{\sum_{i=1}^{g} a_i x_i\colon\ a_i = 0, 1\Big\}.$$

To obtain now the upper bound for $N(H)$ observe that if the elements $y_1, \ldots, y_m$ have the property stated in the corollary, and $\bar{y}_i = y_i + H_0$, then the sequence

$$\{\underbrace{\bar{y}_1, \ldots, \bar{y}_1}_{A_1 \text{ times}}, \ldots, \underbrace{\bar{y}_m, \ldots, \bar{y}_m}_{A_m \text{ times}}\}$$

has no subsequence with vanishing sum, thus $N(H) \leqslant D(H/H_0) - 1$. The lower bound results from taking y_i to be equal to the generator of $Z/n_i Z$ and $A_i = n_i - 1$.

Corollary 1 follows now from the formula for $D(A)$ when A is a p-group, due to Olson [2], and corollary 2 is immediate.

REFERENCES

[1] W. Narkiewicz, *On natural numbers having unique factorization in a quadratic number field*, Acta Arithmetica 12 (1966), p. 1-22.

[2] J. E. Olson, *A combinatorial problem on finite abelian groups*, Journal of Number Theory 1 (1969), p. 8-10.

INSTITUTE OF MATHEMATICS
WROCŁAW UNIVERSITY

Reçu par la Rédaction le 11. 10. 1978