COLLOQUIUM MATHEMATICUM

XVI DÉDIÉ À M. FRANCISZEK LEJA 1967

FACTORIZATION OF NATURAL NUMBERS IN SOME QUADRATIC NUMBER FIELDS

BY

W. NARKIEWICZ (WROCŁAW)

1. Let K be a quadratic extension of the rationals with class-number $h \neq 1$. For any natural number n let $f(n)$ denote the number of essentially different factorizations of n into integers irreducible in K, and let $g(n)$ denote the number of different lengths of such factorizations. (The *length* of a factorization $n = r_1 \ldots r_k$, where the $r_i'-s$ are irreducible, is equal to k.)

It was proved in [5] that for arbitrarily given M, for almost all natural numbers $f(n) \geqslant M$, and, provided $h \neq 1, 2$, $g(n) \geqslant M$. (If $h = 2$, then $g(n) = 1$ for all n [1].) Professor P. Turán asked whether it is possible to find a normal order for $f(n)$, i.e. such a function $F(n)$ that for every positive ε and almost all n the inequality

$$|f(n) - F(n)| < \varepsilon F(n)$$

holds (cf. [3], Chap. XXII, § 11). Of course, $F(n)$ should be wellbehaved in some sense, as otherwise one could simply put $F(n) = f(n)$.

In this note, we show that there is no increasing normal order $F(n)$ already for the field $Q\big((-5)^{1/2}\big)$ (and, more generally, for any quadratic field with $h = 2$). Possibly one could prove this for arbitrary fields, but we did not succeed in doing this.

Moreover, we shall prove that for quadratic fields with $h = 2$ the function $F(n) = \frac{1}{4}\log\log n \log\log\log n$ is a normal order of $\log f(n)$. Finally, we determine a normal order of $g(n)$ for quadratic fields with $h = 3$ or with $h = 4$, and with a noncyclic class-group. In the first case it is equal to $\frac{1}{9}\log\log n$, and in the second to $\frac{1}{8}\log\log n$. The method used here works for every quadratic field with a given class-group, but the necessary computations are rather involved.

2. THEOREM I. *Let K be a quadratic extension of the rationals with the class-number $h = 2$. Then there exists no non-decreasing function $F(n)$*

such that for every positive ε *and almost all* n *the inequality* $|f(n)-F(n)| < \varepsilon F(n)$ *holds, i.e.* $f(n)$ *does not possess a non-decreasing normal order.*

To the proof we need a lemma, which we state in a slightly more general form than we need to our purpose:

LEMMA 1. *Let* $\psi(n)$ *be a strongly additive function, i.e.* $\psi(m+n) = \psi(m)+\psi(n)$ *if* $(m,n)=1$ *and* $\psi(p^k)=\psi(p)$ *for all primes* p *and* $k=1,2,\ldots$ *Moreover, let*

$$A_n = \sum_{p<n} \psi(p)p^{-1}, \qquad B_n = \sum_{p<n} \psi(p)^2 p^{-1},$$

and let us assume that the following conditions are satisfied:

(i) $\psi(p)$ *is bounded independently of* p,

(ii) $\lim_{n\to\infty} B_n = \infty$,

(iii) *There exists a positive constant* β *such that* $A_n = \beta B_n + o(B_n)$,

(iv) *For every bounded function* $\varrho(n) \geqslant 1$, *and for every fixed positive* C *one has*

$$A_{n\cdot\varrho(n)} - A_n + C(B_{n\cdot\varrho(n)}^{1/2} - B_n^{1/2}) = o(B_n^{1/2}).$$

If now $H(x)$ *is an increasing function, which is positive and for every positive* B *satisfies the relation*

$$\liminf_{x\to\infty} H(x+Bx^{1/2})/H(x) > 1,$$

and $R(n)$ *is a function which for square-free* n *satisfies with some fixed* k *the inequalities* $H\big(\psi(n)\big) \leqslant R(n) \leqslant H\big(\psi(n)+k\big)$, *then* $R(n)$ *does not possess a non-decreasing normal order.*

Proof of the lemma. Choose $t_1 < 0 < t_2$ in such a way that

$$\lambda_1 = (2\pi)^{-1/2} \int_{-\infty}^{t_1} \exp(-u^2/2)\,du > 1-6/\pi^2,$$

$$\lambda_2 = (2\pi)^{-1/2} \int_{t_2}^{\infty} \exp(-u^2/2)\,du > 1-6/\pi^2.$$

(This is possible, as $2(1-6/\pi^2) < 1$.)

Let $S_1 = \{N \mid \psi(N) \leqslant A_N + t_1 B_N^{1/2}\}$ and $S_2 = \{N \mid \psi(N) \geqslant A_N + t_2 B_N^{1/2}\}$.

For any set W of natural numbers we shall denote by $W(x)$ the number of elements of the set $W \cap [0, x]$.

By a theorem of P. Erdős and M. Kac (see [2])we have

$$\lim_{x\to\infty} S_1(x)x^{-1} = \lambda_1 \quad\text{and}\quad \lim_{x\to\infty} S_2(x)x^{-1} = \lambda_2.$$

Let us now assume that there exists a non-decreasing normal order for $R(n)$, say $F(n)$. Let us fix a positive number ε and define the set $Z = \{N \mid |R(N)-F(N)| < \varepsilon F(N)\}$. By our assumption

$$\lim_{x\to\infty} Z(x)x^{-1} = 1.$$

Let Q be the set of all square-free natural numbers and let $X_1 = Z \cap Q \cap S_1$, $X_2 = Z \cap Q \cap S_2$. The sets X_1 and X_2 have both positive lower asymptotic density. Indeed, $(Z \cap Q)(x) \geqslant Q(x)-Z'(x) = (6/\pi^2)x+o(x)$ and $X_i(x) \geqslant (Z \cap Q)(x)-S_i'(x) \geqslant (6/\pi^2)x+o(x)+(\lambda_i-1)x+o(x)$ and $6/\pi^2+\lambda_i-1$ is positive.

Observe now that there exists a constant $B > 0$ and infinitely many pairs n_1, n_2 such that

(a) $n_2 < n_1 < n_2+Bn_2$,

(b) $n_1 \in X_1$, $n_2 \in X_2$.

Indeed, otherwise for every $M > 0$ and $N > \delta(M)$, $N \in X_2$ there would be no elements from X_1 in the interval $[N, N+MN]$, hence $X_1(N+MN)-X_1(N) = 0$, but for sufficiently large v we have $v \geqslant X_1(v) \geqslant cv$ with some positive c, and so

$$0 = X_1(N+NM)-X_1(N) \geqslant cN(1+M)-N,$$

which is false for $M > c^{-1}$.

For n_1 and n_2 satisfying (a) and (b) we have

$$(1+\varepsilon)F(n_2) \geqslant R(n_2) \geqslant H\big(\psi(n_2)\big) \geqslant H(A_{n_2}+t_2B_{n_2}^{1/2})$$

and

$$(1-\varepsilon)F(n_1) \leqslant R(n_1) \leqslant H\big(\psi(n_1)+k\big) \leqslant H(A_{n_1}+t_1B_{n_1}^{1/2}+k),$$

thus

$$\frac{H(A_{n_2}+t_2B_{n_2}^{1/2})}{H(A_{n_1}+t_1B_{n_1}^{1/2}+k)} \leqslant \frac{1+\varepsilon}{1-\varepsilon} \quad \text{as} \quad F(n_1) \geqslant F(n_2). \tag{1}$$

But in view of (iii) and (iv) we have

$$A_{n_1}+t_1B_{n_1}^{1/2}+k = \beta B_{n_2}+t_1B_{n_2}^{1/2}+o(B_{n_2}^{1/2})$$

and

$$A_{n_2}+t_2B_{n_2}^{1/2} = \beta B_{n_2}+t_2B_{n_2}^{1/2}+o(B_{n_2}^{1/2}).$$

Hence (1) implies

$$\liminf_{x\to\infty} H\big(x+(t_2-t_1)\beta^{-1/2}x^{1/2}\big)/H(x) \leqslant 1,$$

contrary to our assumption. The lemma is thus proved.

Proof of Theorem I. Let X be the non-principal class of ideals in K. Let P_1 be the set of all rational primes which are norms of prime ideals from X and are not ramified, and let P_2 be the set of all ramified rational primes which are norms of prime ideals from X. The set P_2 is finite, possibly void.

Consider an arbitrary square-free natural number n with the following factorization in rational primes:

$n = p_1 \dots p_r p_{r+1} \dots p_s R$, where $p_1, \dots, p_r$ belong to $P_1, p_{r+1}, \dots, p_s$ belong to P_2, and R is a natural number having no prime divisors from P_1 and P_2. Let $p_i = \mathfrak{p}_{2i-1}\mathfrak{p}_{2i}$ $(i = 1, 2, \dots, r; \mathfrak{p}_i \in X)$. Every factorization of the number $p_1 \dots p_r$ into integers irreducible in K has the form

$$p_1 \dots p_r = \prod_{k=1}^{r} (\mathfrak{p}_{i_k}\mathfrak{p}_{j_k})$$

and there are evidently $(2r)!/r!2^r$ such factorizations. Consequently $f(n) \geqslant f(p_1 \dots p_r) = (2r)!/r!2^r$. For the same reason the number $p_1 \dots p_s$ can have at most $(2s)!/s!2^s$ factorizations, consequently we have $f(n) \leqslant f(p_1 \dots p_s) = (2s)!/s!2^s$, as the number R has no influence on $f(n)$.

Let us denote by $\omega_{P_1}(n)$ the number of primes from P_1 dividing n, and let $H(x) = (2x)!/x!2^x$ for natural x. Then the above inequalities imply that for square-free n we have

$$H\big(\omega_{P_1}(n)\big) \leqslant f(n) \leqslant H\big(\omega_{P_1}(n)+k\big),$$

where k is the number of rational primes ramified in K.

To check that $\omega_{P_1}(n)$ satisfies the assumptions of Lemma 1 we use the following result, which follows by partial summation from Satz 85 of [4]:

If Y is an ideal class, then

$$\sum_{\mathfrak{p}\in Y, N\mathfrak{p}\leqslant x} N(\mathfrak{p})^{-1} = h^{-1}\log\log x + a + O\big((\log x)^{-1}\big).$$

From this the following evaluation follows immediately:

If Y is an ideal class in a quadratic number field, and P is the set of all rational primes which are norms of prime ideals from Y, then

$$\sum_{p\leqslant x, p\in P} p^{-1} = \varepsilon h^{-1}\log\log x + a + O\big((\log x)^{-1}\big), \tag{2}$$

where $\varepsilon = \frac{1}{2}$ if Y^2 is the principal class, and $\varepsilon = 1$ otherwise.

The function $\omega_{P_1}(n)$ is evidently strongly additive and $A_n = B_n = \frac{1}{4}\log\log x + a + O\big((\log x)^{-1}\big)$ by (2). (Actually P_1 is not the set of all rational primes which are norms of prime ideals from a fixed ideal class, but differs from such a set only by a finite number of primes, which does not affect (2) in principle (only the constant a will change).)

Now it is easy to see that (i)-(iv) are satisfied and, because the ratio $H(x+1)/H(x)$ tends to infinity, we can apply Lemma 1 to get the wanted result.

3. Now we consider $\log f(n)$ and prove

THEOREM II. *Let K be a quadratic extension of the rationals with the class-number $h = 2$. Then*

(i) $\sum\limits_{n\leqslant x} \log f(n) = \frac{1}{4}x(\log\log x \log\log\log x) + O(x\log\log x)$ *and*

(ii) *For every function $r(x)$ tending to infinity with x, the number of natural numbers less than x, for which*

$$|\log f(n) - \tfrac{1}{4}(\log\log x)(\log\log\log x)| \geqslant r(x)\log\log x(\log\log\log x)^{1/2}$$

holds is $o(x)$.

(This clearly implies that $\log f(n)$ has the normal order $\frac{1}{4}(\log\log n)\times$ $\times(\log\log\log n)$.)

The proof of (ii) as well as of the corresponding part of Theorem III below is based on the method used by Turán in [6] to give a simple proof of the Hardy-Ramanujan theorem.

In the sequel, let Q be the set of all rational primes which are norms of prime ideals from a fixed ideal class, and let β be the Dirichlet density of Q. As usual,

$$\omega_Q(n) = \sum_{\substack{q\mid n\\ q\in Q}} 1 \quad \text{and} \quad \Omega_Q(n) = \sum_{\substack{q\in Q\\ q^m\|n}} m.$$

LEMMA 2. *Let $h(n)$ be one of the functions $\omega_Q(n)$, $\Omega_Q(n)$. Then*

$$\text{(a)} \quad \sum_{\substack{n\leqslant x\\ d\mid n}} h(n) = \beta d^{-1}x\log\log(xd^{-1}) + O\Big(\big(1+h(d)\big)xd^{-1}\Big)$$

and

$$\text{(b)} \quad \sum_{\substack{n\leqslant x\\ d\mid n}} h^2(n) = \beta d^{-1}x\big(\log\log(xd^{-1})\big)^2 + O\Big(\big(1+h^2(d)\big)xd^{-1}\log\log(xd^{-1})\Big).$$

Proof. Clearly

$$\sum_{\substack{d\mid n\\ n\in x}} \Omega_Q(n) = \sum_{m\leqslant x/d} \Omega_Q(m) + [xd^{-1}]\,\Omega_Q(d).$$

But

$$\sum_{m\leqslant x/d}\Omega_Q(m)=\sum_{m\leqslant x/d}\sum_{\substack{q\epsilon Q\\ r\\ q^r|m}}1=\sum_{\substack{q\epsilon Q\\ q\leqslant x/d}}\sum_{\substack{r\\ q^r\leqslant x/d}}\sum_{\substack{m\leqslant x/d\\ q^r|m}}1$$

$$=\sum_{\substack{q\epsilon Q\\ q\leqslant x/d}}\sum_{\substack{r\\ q^r\leqslant x/d}}[xd^{-1}q^{-r}]=xd^{-1}\sum_{\substack{q\epsilon Q\\ r\\ q^r\leqslant x/d}}q^{-r}+O\Big(\sum_{\substack{q\epsilon Q\\ r\\ q^r\leqslant x/d}}1\Big)$$

$$=\beta xd^{-1}\log\log(xd^{-1})+O(xd^{-1}),$$

whence

$$\sum_{\substack{d|n\\ n\leqslant x}}\Omega_Q(n)=\beta xd^{-1}\log\log(xd^{-1})+O\Big(\big(1+\Omega_Q(d)\big)xd^{-1}\Big).$$

Further,

$$\sum_{\substack{d|n\\ n\leqslant x}}\omega_Q(n)=\sum_{\substack{d|n\\ n\leqslant x}}\sum_{\substack{q\epsilon Q\\ q|n}}1=\sum_{\substack{q\leqslant x\\ q\epsilon Q}}\sum_{\substack{n\leqslant x\\ d|n\\ q|n}}1=\sum_{\substack{dq\leqslant x,\, q\nmid d\\ q\epsilon Q}}[x/dq]+\sum_{\substack{q\leqslant x,\, q|d\\ q\epsilon Q}}[x/d]$$

$$=\frac{x}{d}\sum_{\substack{qd\leqslant d\\ q\epsilon Q,\, q\nmid d}}1/q+O\Big(\big(1+\omega_Q(d)\big)xd^{-1}\Big)$$

$$=\beta xd^{-1}\log\log(x/d)+O\Big(\big(1+\omega_Q(d)\big)xd^{-1}\Big)$$

and

$$\sum_{\substack{n\leqslant x\\ d|n}}\Omega_Q^2(n)=\sum_{m\leqslant x/d}\Omega_Q^2(m)+2\Omega_Q(d)\sum_{m\epsilon x/d}\Omega_Q(m)+[x/d]\,\Omega_Q^2(d).$$

But

$$\sum_{m\leqslant x/d}\Omega_Q^2(m)=\sum_{m\leqslant x/d}\sum_{\substack{q^r/n\\ q\epsilon Q}}\sum_{\substack{q_1^{r_1}/n\\ q_1\epsilon Q}}1=\sum_{\substack{q\epsilon Q\\ q^r\leqslant x/d}}\sum_{\substack{q_1\epsilon Q\\ q_1^{r_1}\leqslant x/d}}\sum_{\substack{m\leqslant x/d\\ q^r|m\\ q_1^{r_1}|m}}1$$

$$=\sum_{\substack{q\epsilon Q\\ q^r\leqslant x/d}}\sum_{\substack{q_1\epsilon Q,\, q_1\neq q\\ q_1^{r_1}\leqslant x/d}}[x/dq^r q_1^{r_1}]+O\Big(\sum_{\substack{q\epsilon Q\\ q^r\leqslant x/d}}\sum_{r_1}x/dq^{\max(r,r_1)}\Big)$$

$$=xd^{-1}\sum_{\substack{q^r\leqslant x/d\\ q\epsilon Q}}q^{-r}\sum_{\substack{q_1^{r_1}\leqslant x/d\\ q\neq q_1\epsilon Q}}q_1^{-r_1}+O\Big(\sum_{\substack{q^r\leqslant x/d\\ q\epsilon Q}}\sum_{\substack{q_1^{r_1}\leqslant x/d\\ q_1\epsilon Q\\ q\neq q_1}}1\Big)+$$

$$+O\big(xd^{-1}\log\log(xd^{-1})\big)$$

$$=\beta^2xd^{-1}\big(\log\log(xd^{-1})\big)^2+O\big(xd^{-1}\log\log(xd^{-1})\big).$$

Finally,

$$\sum_{\substack{n\leqslant x\\ d|n}} \Omega_Q^2(n) = \beta^2 xd^{-1}\big(\log\log(xd^{-1})\big)^2 + O\Big(\big(1+\Omega_Q^2(d)\big)xd^{-1}\log\log(xd^{-1})\Big),$$

and

$$\sum_{\substack{n\leqslant x\\ d|n}} \omega_Q^2(n) = \sum_{\substack{n\leqslant x\\ d|n}}\sum_{\substack{q\in Q\\ q|n}}\sum_{\substack{q_1\in Q\\ q_1|n}} 1 = \sum_{\substack{q,q_1\in Q\\ qq_1\leqslant x}}\sum_{\substack{n\leqslant x\\ d|n\\ q_1,q|n}} 1$$

$$= \sum_{\substack{q\in Q\\ q\leqslant x,\, q\nmid d}}\sum_{\substack{q_1\in Q\\ dqq_1\leqslant x\\ (q_1,qd)=1}} [x/dqq_1] +$$

$$+O\Big(\sum_{\substack{q\in Q\\ dq\leqslant x\\ q\nmid d}} x/qd + \sum_{\substack{q\in Q\\ q\leqslant x,\, q\nmid d}}\sum_{\substack{q_1\in Q\\ q_1\leqslant x\\ q_1|d}} x/qd + \sum_{\substack{q\in Q\\ q\leqslant x,\, q|d}}\sum_{\substack{q_1\in Q,\, q_1\leqslant x\\ q_1\neq q,\, q_1\nmid d}} x/dq_1 + \sum_{\substack{q\in Q,\, q\leqslant x\\ q|d}}\sum_{\substack{q_1\leqslant x,\, q_1\in Q\\ q_1|d}} x/d\Big)$$

$$= \beta^2 xd^{-1}\big(\log\log(xd^{-1})\big)^2 + O\Big(\big(1+\omega_Q^2(d)\big)x/d^{-1}\log\log x/d\Big).$$

The lemma is thus proved in all cases.

The following corollary will be useful:

For $d\leqslant x^{1/2}$ we have

$$\sum_{n\leqslant x,\, d|n}\big(h(n)-\beta\log\log x\big)^2 = O\Big(\big(1+h^2(d)\big)xd^{-1}\log\log x\Big), \tag{3}$$

where $h(n)$ is one of the functions $\omega_Q(n)$, $\Omega_Q(n)$.

LEMMA 3. *Let $h(n)$ be one of the functions $\omega_Q(n)$, $\Omega_Q(n)$. Then*

(a) $$\sum_{n\leqslant x} h(n)\log h(n) = \beta x\log\log x\log\log\log\log x + O(x\log\log x),$$

(b) $$\sum_{n\leqslant x} h^2(n)\log^2 h(n)$$
$$= \beta^2 x(\log\log x\log\log\log\log x)^2 + O\big(x(\log\log x)^2\log\log\log\log x\big).$$

(Here $h(n)\log h(n)$ should be treated as zero for $h(n)=0$).

Proof of the lemma. Split the rational integers less than x into three classes:

$$Z_1 = \{n\leqslant x|\ |h(n)-\beta\log\log x\ |\geqslant \log\log x\},$$
$$Z_2 = \{n\leqslant x|\ |h(n)-\beta\log\log x\ |\leqslant (\log\log x)^{2/3}\},$$
$$Z_3 = \{n\leqslant x\ |\ (\log\log x)^{2/3} < |\ h(n)-\beta\log\log x\ | < \log\log x\}.$$

It follows from (3) that for $d\leqslant x^{1/2}$ the number $N_1(d)$ of elements of Z_1 divisible by d is $O\Big(\big(1+h^2(d)\big)d^{-1}x(\log\log x)^{-1}\Big)$, and, similarly, the number $N_3(d)$ of elements of the set Z_3 divisible by the number d is $O\left(\left(1+h^2(d)\right)d^{-1}x(\log\log x)^{-1/3}\right)$. Moreover, the number N_2 of elements of Z_2 is equal to $x+O\left(x(\log\log x)^{-1/3}\right)$.

Now

$$\sum_{n\leqslant x} h(n)\log h(n) = \sum_{n\in Z_1} + \sum_{n\in Z_2} + \sum_{n\in Z_3}.$$

As for every $n\leqslant x$, $h(n) = O(\log x)$, thus we have

$$\sum_{n\in Z_1} h(n)\log h(n) = O\left(\log\log x \sum_{n\in Z_1} h(n)\right) = O\Big(\log\log x \sum_{p\leqslant x} \sum_{\substack{p\mid n\\ n\in Z_1}} 1\Big) + O(x\log\log x)$$

$$= O\Big(\log\log x \sum_{p\leqslant x^{1/2}} N_1(p)\Big) + O\Big(\log\log x \sum_{x^{1/2}\leqslant p\leqslant x} N_1(p)\Big) + O(x\log\log x)$$

$$= O(x\log\log x),$$

because

$$\sum_{n^{1/2}<p\leqslant x} N_1(p) = O\Big(\sum_{x^{1/2}<p\leqslant x} \frac{x}{p}\Big) = O(x).$$

Similarly, for every $n\in Z_3$ we have $h(n) = O(\log\log x)$, thus

$$\sum_{n\in Z_3} h(n)\log h(n) = O\Big(\log\log\log x \sum_{n\in Z_3} h(n)\Big)$$

$$= O\Big(\log\log\log x \sum_{p\leqslant x} \sum_{\substack{p\mid n\\ n\in Z_3}} 1\Big) + O(x\log\log\log x)$$

$$= O\Big(\log\log\log x \sum_{p\leqslant x^{1/2}} N_3(p)\Big) + O\Big(\log\log\log x \sum_{x^{1/2}<p\leqslant x} N_3(p)\Big) + O(x\log\log\log x)$$

$$= O\left(x(\log\log\log x)(\log\log x)^{2/3}\right) = O(x\log\log x).$$

For $n\in Z_2$ we have $h(n) = \beta\log\log x + O\left((\log\log x)^{2/3}\right)$ and $\log h(n) = \log\log\log x + O(1)$, thus

$$\sum_{n\in Z_2} h(n)\log h(n) = \sum_{n\in Z_2} \left(\beta\log\log x + O\left((\log\log x)^{2/3}\right)\right)\left(\log\log\log x + O(1)\right)$$

$$= N_2\beta\log\log x\log\log\log x + O(x\log\log x)$$

$$= \beta x\log\log x\log\log\log x + O(x\log\log x)$$

and so (a) is proved.

The proof of (b) follows the same line and so we leave it to the reader.

Proof of Theorem II. Let P_1 be the set of rational primes, defined in § 2. The argument used in the proof of Theorem I shows that $f(n) \geqslant H\left(\omega_{P_1}(n)\right)$ for all n, and not only for square-free n. On the other hand, a slight modification of the argument used there shows that, for all n, $f(n) \leqslant H(\Omega_{P_1}(n)+k)$. Taking into account the evaluation $\log H(n) = n\log n + O(n)$ we see that for all n

$$\omega_{P_1}(n)\log\omega_{P_1}(n)+O(\omega_{P_1}(n)) \leqslant \log f(n) \leqslant \Omega_{P_1}(n)\log\Omega_{P_1}(n)+O(\Omega_{P_1}(n))$$

and so part (i) of Theorem II follows from (1) and Lemma 3, as the Dirichlet density of P_1 is equal to $\frac{1}{4}$.

To establish part (ii) one should note only that Lemma 3 implies

$$\sum_{n\leqslant x}(\log f(n)-\tfrac{1}{4}\log\log x\log\log\log x)^2 = O\big(x(\log\log x)^2(\log\log\log x)\big)$$

and so the inequality

$$|\log f(n)-\tfrac{1}{4}\log\log x\log\log\log x| \geqslant r(x)\log\log x(\log\log\log x)^{1/2}$$

can hold for $O(x/r^2(x)) = o(x)$ numbers $n \leqslant x$.

4. Finally we consider the function $g(n)$. We shall prove the following

THEOREM III. *Let K be a quadratic field with class-number $h = 3$, or with $h = 4$, and non-cyclic class-group. Then*

(i) *we have*

$$\sum_{n\leqslant x} g(n) = \frac{1}{9}x\log\log x+O(x) \qquad (h = 3),$$

$$\sum_{n\leqslant x} g(n) = \frac{1}{8}x(\log\log x)+O\big(x(\log\log x)^{2/3}\big) \qquad (h = 4);$$

(ii) *For every function $r(x)$ tending to infinity with x, the number of natural numbers $n\leqslant x$ for which the inequality $|g(n)-C\log\log x|\geqslant r(x)(\log\log x)^a$ holds is $o(x)$. Here $C = 1/9$ if $h = 3$, $C = 1/8$ if $h = 4$, $a = 1/2$ if $h = 3$, and $a = 5/6$ if $h = 4$.*

At first we need some lemmas.

LEMMA 4. *If K is a quadratic field with $h = 3$, and X is one of the non-principal ideal classes, then $g(n) = 1+[\Omega_P(n)/3]$, where P is the set of all primes which are norms of prime ideals from X.*

Proof. Let $\Omega_P(n) = r$. The possible irreducible factors of n have one of the forms $\mathfrak{p}_i\mathfrak{q}_j$, $\mathfrak{p}_i\mathfrak{p}_j\mathfrak{p}_k$ and $\mathfrak{q}_i\mathfrak{q}_j\mathfrak{q}_k$ with $\mathfrak{p}_i \in X$, $\mathfrak{q}_i \in X^2$, and so every factorization of n must be of the form

$$n = \Big(\prod_{j=1}^{\lambda}(\mathfrak{p}_{i_j}\mathfrak{q}_{k_j})\Big)\Big(\prod_{j=1}^{\mu}(\mathfrak{p}_{r_j}\mathfrak{p}_{s_j}\mathfrak{p}_{t_j})\Big)\Big(\prod_{j=1}^{\nu}\mathfrak{q}_{a_j}\mathfrak{q}_{b_j}\mathfrak{q}_{c_j})\Big)$$

with some non-negative λ, μ, ν. (We consider only the case, when n has no factor R not divisible by any prime from P, as this restriction does not affect $g(n)$. Indeed, $g(n) = g(n/R)$.)

The length of this factorization is equal to $\lambda+\mu+\nu$ and λ, μ, ν are related to r by means of the equations

$$\lambda+3\mu = r, \qquad \lambda+3\nu = r,$$

whence $\lambda+\mu+\nu = r-\mu$. If now $\mu = \nu = 0, 1, 2, \ldots, [r/3]$, $\lambda = r-3\mu$, then we get exactly $1+[r/3]$ factorizations of n with different lengths. (Other values of μ are clearly inadmissible).

LEMMA 5. *If K is a quadratic field with class-number $h = 4$ and non-cyclic class-group $H = (E, X, Y, XY)$, then*

$$g(n) = 1+\min\big(\Omega_{P_1}(n), \Omega_{P_2}(n), \Omega_{P_3}(n)\big),$$

where

$$P_1 = \{p \mid p = N\mathfrak{p}, \mathfrak{p}\in X\}, \qquad P_2 = \{p \mid p = N\mathfrak{p}, \mathfrak{p}\in Y\},$$
$$P_3 = \{p \mid p = N\mathfrak{p}, \mathfrak{p}\in XY\}.$$

Proof. Let $n = (p_1^{a_1} \ldots p_s^{a_s})(q_1^{b_1} \ldots q_t^{b_t})(r_1^{c_1} \ldots r_u^{c_u})R$ with $p_i\in P_1$, $q_i\in P_2$, $r_i\in P_3$ and $p \nmid R$ for $p\in P_1 \cup P_2 \cup P_3$. As obviously $g(n) = g(n/R)$, we may assume that $R = 1$.

The irreducible integers in K have one of the forms $\mathfrak{p}_1\mathfrak{p}_2, \mathfrak{q}_1\mathfrak{q}_2, \mathfrak{r}_1\mathfrak{r}_2, \mathfrak{p}_1\mathfrak{q}_1\mathfrak{r}_1$ with $\mathfrak{p}_i\in X$, $\mathfrak{q}_i\in Y$ and $\mathfrak{r}_i\in XY$. Thus every factorization of n has the form

$$n = \prod_{j=1}^{\lambda}(\mathfrak{p}_j\mathfrak{p}_j')\cdot\prod_{j=1}^{\mu}(\mathfrak{q}_j\mathfrak{q}_j')\cdot\prod_{j=1}^{\nu}(\mathfrak{r}_j\mathfrak{r}_j')\cdot\prod_{j=1}^{\varrho}(\bar{\mathfrak{p}}_j\bar{\mathfrak{q}}_j\bar{\mathfrak{r}}_j),$$

where $\mathfrak{p}_i, \mathfrak{p}_i', \bar{\mathfrak{p}}_i$ are prime ideal divisors of $p_1 \ldots p_s$, and, similarly, $\mathfrak{q}_i, \mathfrak{q}_i', \bar{\mathfrak{q}}_i$ are prime ideal divisors of $q_1 \ldots q_t$, and $\mathfrak{r}_i, \mathfrak{r}_i', \bar{\mathfrak{r}}_i$ are prime ideal divisors of $r_1 \ldots r_u$.

Clearly $2\lambda+\varrho = 2\Omega_{P_1}(n)$, $2\mu+\varrho = 2\Omega_{P_2}(n)$ and $2\nu+\varrho = 2\Omega_{P_3}(n)$. The length of such a factorization is equal to

$$\lambda+\mu+\nu+\varrho = \sum_{i=1}^{3}\Omega_{P_i}(n)-\varrho/2.$$

As ϱ can assume the values $0, 2, 4, \ldots, \min\big(2\Omega_{P_1}(n), 2\Omega_{P_2}(n), 2\Omega_{P_3}(n)\big)$ only, it follows that

$$g(n) = 1+\min\big(\Omega_{P_1}(n), \Omega_{P_2}(n), \Omega_{P_3}(n)\big),$$

as asserted.

LEMMA 6. *Suppose that Q_1, Q_2, Q_3 are sets of rational primes such that each Q_i is the set of all rational primes from a fixed ideal class and assume that they all have the same Dirichlet density ϱ. Let $T(n) = \min_i \Omega_{Q_i}(n)$. Then*

$$\sum_{n\leqslant x} T(n) = \beta x \log\log x + O\left(x(\log\log x)^{2/3}\right)$$

and

$$\sum_{n\leqslant x} T^2(n) = \beta^2 x(\log\log x)^2 + O\left(x(\log\log x)^{5/3}\right).$$

Proof. Observe first that by (3) we have for $d \leqslant x^{1/2}$ the relation

$$\begin{aligned}\sum_{n\leqslant x,\, d|n} \left(\Omega_{Q_i}(n) - \Omega_{Q_j}(n)\right)^2 &= \sum_{\substack{n\leqslant x\\ d|n}} \left(\Omega_{Q_i}(n) - \beta\log\log x + \beta\log\log x - \Omega_{Q_j}(n)\right)^2 \\ &\leqslant 2\sum_{\substack{n\leqslant x\\ d|n}} \left(\Omega_{Q_i}(n) - \beta\log\log x\right)^2 + 2\sum_{\substack{n\leqslant x\\ d|n}} \left(\Omega_{Q_j}(n) - \beta\log\log x\right)^2 \\ &= O\left(\left(1+\max\left(\Omega^2_{Q_i}(d),\, \Omega^2_{Q_j}(d)\right) x d^{-1} \log\log x\right)\right).\end{aligned}$$

Now let Z_1 be the set of all natural numbers n less than or equal to x for which $|\Omega_{Q_1}(n) - \Omega_{Q_2}(n)| \geqslant (\log\log x)^{2/3}$ or $|\Omega_{Q_1}(n) - \Omega_{Q_3}(n)| \geqslant (\log\log x)^{2/3}$ holds, and let $Z_2 = [1, x] \setminus Z_1$. The estimation just proved shows that for $d \leqslant x^{1/2}$ the set $\{n \mid n \in Z_1,\, d|n\}$ has at most

$$O\left(\left(1+\max\left(\Omega^2_{Q_1}(n),\, \Omega^2_{Q_2}(n),\, \Omega^2_{Q_3}(n)\right) x d^{-1} (\log\log x\right)^{-1/3}\right)$$

elements. Thus in the same way as in the proof of Lemma 3 the estimation

$$\sum_{n\in Z_1} T(n) \leqslant \sum_{n\in Z_1} \Omega_{Q_1}(n) = O(x)$$

results and by Lemma 2 we have

$$\begin{aligned}\sum_{n\leqslant x} T(n) &= \sum_{n\in Z_2} T(n) + O(x) \\ &= \sum_{n\leqslant x} \Omega_{Q_1}(n) + O\left(\sum_{n\in Z_1} \Omega_{Q_1}(n)\right) + O(x) + O\left((x\log\log x)^{2/3}\right).\end{aligned}$$

The proof of the second part of our lemma follows the same line.

Now we can prove Theorem III. In the case of $h = 3$ it follows immediately from Lemma 4, Lemma 2 and (3). In the case of $h = 4$ it follows from Lemma 5 and Lemma 6.

Note that Lemma 6 implies that

$$\sum_{n\leqslant x}\big(T(n)-\beta\log\log x\big)^2 = O\big(x(\log\log x)^{5/3}\big).$$

REFERENCES

[1] L. Carlitz, *A characterization of algebraic number fields with class number two*, Proceedings of the American Mathematical Society 11 (1960), p. 391-392.

[2] P. Erdős and M. Kac, *The Gaussian law of errors in the theory of additive number theoretic functions*, American Journal of Mathematics 62 (1940), p. 738-742.

[3] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, IV ed., Oxford 1962.

[4] E. Landau, *Über Ideale und Primideale in Idealklassen*, Mathematische Zeitschrift 2 (1918), p. 52-154.

[5] W. Narkiewicz, *On algebraic number fields with non-unique factorization*, Colloquium Mathematicum 12 (1964), p. 59-68.

[6] P. Turán, *On a theorem of Hardy and Ramanujan*, Journal of the London Mathematical Society 9 (1934), p. 274-276.

NSTITUTE OF MATHEMATICS OF THE WROCŁAW UNIVERSITY

Reçu par la Rédaction le 30. 11. 1965