Table des matières du tome XII, fascicule 1

La revue est consacrée à toutes les branches de *l'Arithmétique et de la Théorie des Nombers*, ainsi qu'aux *fonctions ayant de l'importance dans ces domaines.*

Prière d'adresser les textes dactylographiés à l'un des redacteurs de la revue ou bien à la Rédaction de

ACTA ARITHMETICA

Warszawa 1 (Pologne) ul. Śniadeckich 8.

La même adresse est valable pour toute correspondance concernant l'échange de Acta Arithmetica.

Les volumes IV et suivants de ACTA ARITHMETICA sont à obtenir chez

Ars Polona, Warszawa 5 (Pologne), Krakowskie Przedmieście 7.

Prix de ce fascicule 3.00 $.

Les volumes I-III (reédits) sont à obtenir chez

Johnson Reprint Corp., 111 Fifth Ave., New York, N. Y.

PRINTED IN POLAND

W R O C Ł A W S K A D R U K A R N I A N A U K O W A

ACTA ARITHMETICA
XII (1966)

On natural numbers having unique factorization in a quadratic number field

by

W. Narkiewicz (Wrocław)

1. Let K be a quadratic extension of the rationals with the class-number h and class-group H. Let $C_{h_1} \times \ldots \times C_{h_r}$ be a factorization of H into cyclic groups. (It is obviously not unique, but we shall choose and fix one of them.) Let F be the set of all natural numbers which have a unique factorization into integers irreducible in K (apart of unit factors, of course). Similarly, let G be the set of all natural numbers whose all factorizations into integers irreducible in K have the same length. This means that in every factorization of a given number from G there occurs the same number of irreducible factors. (Note that if $h = 2$ then all natural numbers are in G as proved by L. Carlitz in [1].) Let us now define:

$$F(x) = N(n \leqslant x \mid n \in F),$$

$$G(x) = N(n \leqslant x \mid n \in G),$$

$$F_{k,l}(x) = N\big(n \leqslant x \mid n \in F,\ n \equiv l \pmod{k}\big),$$

$$G_{k,l}(x) = N\big(n \leqslant x \mid n \in G,\ n \equiv l \pmod{k}\big),$$

where by $N(n \leqslant x \mid \mathrm{W})$ we understand the number of natural numbers not larger than x, having the property W.

E. Fogels proved in [3] that in the case $K = R(i5^{1/2})$ one has

$$F(x) = O\big(x(\log\log x)^{4/5}(\log x)^{-1/5}\big)$$

and it was proved in [6] that for any normal (not necessarily quadratic) extension of the rationals with $h \neq 1$ one has

$$F(x) = O\big(x(\log\log x)^{a}(\log x)^{-b}\big)$$

with some constants a, b (b positive) depending on the field. A similar result for the function $G(x)$ (with the obvious assumption $h \neq 1, 2$) was obtained in [7].

In this paper we give an asymptotic evaluation of $F(x)$ and $G(x)$ in the quadratic case and prove

$$F(x) \approx C_1 x(\log\log x)^M (\log x)^{(1-h)/2h},$$
$$G(x) \approx C_2 x(\log\log x)^N (\log x)^{(1+g-h)/2h}.$$

Here g denotes the number of even invariants of H, i.e. the number of even integers among the h_i—s and the meaning of C_1, C_2, M and N will be described in the sequel. The notation $A(x) \approx B(x)$ means $\lim_{x\to\infty}(A(x)/B(x)) = 1$.

We shall get similar evaluations for $F_{k,l}(x)$ and $G_{k,l}(x)$ when k is relatively prime to the discriminant of K, restricting ourselves in the first case to $(k, l) = 1$. The results obtained here were announced without proof in [8], where unfortunately the condition on k was omitted.

The author is grateful to Professor E. Fogels for pointing out some obscurities in the earlier draft of this paper and for suggesting some improvements in the presentation of the results.

2. We shall start with a characterization of the natural numbers belonging to F and G.

Note that if we treat the Galois group C_2 as a transformation group acting on H then the orbit of $X \in H$ is evidently (X, X^{-1}). Let $h_1, \dots, h_r$ be the orders of cyclic factors in a decomposition of H into product of cyclic groups (which decomposition will be regarded as fixed in sequel). For a given integer a and $i = 1, 2, \dots, r$ let $[a]_i = h_i - a$ if $a \neq 0$, and let $[a]_i = 0$ if $a = 0$. Now we have a one-to-one correspondence between the orbits $\mathcal{O} = (X, X^{-1})$ and r-tuples of nonnegative rational integers $(a_1, \dots, a_r)$ satisfying the following conditions:

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

(ii) $a_1 \leqslant [a_1]_1$, and if $a_i = [a_i]_i$ for $i = 1, 2, \dots, t-1$ with some t, then $a_t \leqslant [a_t]_t$.

Indeed, let X_i be the generator of C_{h_i} treated as a subgroup of H. Then every $X \in H$ can be represented uniquely in the form $X = X_1^{a_1} \dots X_r^{a_r}$ with $0 \leqslant a_i < h_i$ $(i = 1, 2, \dots, r)$. If now $\mathcal{O} = (X, X^{-1})$ then exactly one of the r-tuples $(a_1, \dots, a_r), ([a_1]_1, \dots, [a_r]_r)$ satisfies (i) and (ii). We shall say this r-tuple corresponds to the orbit $\mathcal{O}$. Conversely, every r-tuple $(a_1, \dots, a_r)$ satisfying (i) and (ii) determines a unique orbit, namely the orbit containing $X_1^{a_1} \dots X_r^{a_r}$.

Given an orbit $\mathcal{O} = (X, X^{-1})$ we shall say that a rational prime p *belongs to* $\mathcal{O}$, and write $p \sim \mathcal{O}$ if $p = \mathfrak{p}_1\mathfrak{p}_2$ $(\mathfrak{p}_1 \in X, \mathfrak{p}_2 \in X^{-1})$.

By a *complex* we shall understand any system $(Z_1, \dots, Z_s)$ of (not necessarily distinct) elements of H such that $Z_1 \dots Z_s = E$, the unit element of H. The number s will be called the *length of the complex*. By a *minimal complex* we shall understand any complex which does not contain a proper subcomplex. By a *factorization of a complex* Z we shall understand any partition of Z into minimal subcomplexes. These subcomplexes we shall call the *factors* of Z.

Let us say, a set of r-tuples $(a_1^{(j)}, \dots, a_r^{(j)})$ $(j = 1, 2, \dots, n)$ is *F-admissible* if every r-tuple from this set satisfies (i) and (ii) and moreover the following condition is satisfied:

(iii) For every two different sequences $(\varepsilon_1, \dots, \varepsilon_n)$, $(\eta_1, \dots, \eta_n)$ with $\varepsilon_i, \eta_i = 0, 1$,

$$\Big(\sum_{k=1}^{n} \varepsilon_k a_1^{(k)}, \dots, \sum_{k=1}^{n} \varepsilon_k a_r^{(k)}\Big) \not\equiv \Big(\sum_{k=1}^{n} \eta_k a_1^{(k)}, \dots, \sum_{k=1}^{n} \eta_k a_r^{(k)}\Big) \pmod{\langle h_1, \dots, h_r\rangle}$$

(where by $(a_1, \dots, a_r) \equiv (b_1, \dots, b_r) \pmod{\langle h_1, \dots, h_r\rangle}$ we mean $a_i \equiv b_i \pmod{h_i}$ for $i = 1, 2, \dots, r$).

(Note that the r-tuple $(0, 0, \dots, 0)$ is not contained in any F-admissible set.)

The reason for introducing this definition becomes clear from the following

LEMMA 1. *Suppose that $\mathcal{O}_1, \dots, \mathcal{O}_s$ are distinct orbits $(\mathcal{O}_i \neq (E, E))$ and $a^{(i)} = (a_1^{(i)}, \dots, a_r^{(i)})$ $(i = 1, 2, \dots, s)$ are the corresponding r-tuples satisfying* (i) *and* (ii). *Let $m = p_1 \dots p_s$ with $p_i \sim \mathcal{O}_i$ for $i = 1, 2, \dots, s$.*

Then m has a unique factorization in K (i.e. $m \in F$) if and only if the set $\{a^{(1)}, \dots, a^{(s)}\}$ is F-admissible.

Proof. With every integer β in K we can associate a complex in the following way: factorize the principal ideal (β) generated by β into prime ideals, $(\beta) = \mathfrak{p}_1^{a_1} \dots \mathfrak{p}_t^{a_t}$ with $\mathfrak{p}_i \in Z_i$, say, and take the complex $(Z_1, \dots, Z_1, \dots, Z_s, \dots, Z_s)$, where every Z_i appears a_i times. Every factorization of β into integers irreducible in K induces in an evident way a factorization of the associated complex and conversely.

From our assumptions follows that the following complex is associated with m:

$$(1) \qquad (\{X_1^{a_1^{(i)}} \dots X_r^{a_r^{(i)}}\}_{i=1}^{s}, \{X_1^{h_1 - a_1^{(i)}}, \dots, X_r^{h_r - a_r^{(i)}}\}_{i=1}^{s}).$$

The number m will have a unique factorization if and only if all factors of the complex (1) will be of the form

$$(2) \qquad \{X_1^{a_1^{(i)}} \dots X_r^{a_r^{(i)}}, X_1^{h_1 - a_1^{(i)}} \dots X_r^{h_r - a_r^{(i)}}\}.$$

Indeed, $m = p_1 \dots p_s$ is a factorization into integers irreducible in K (because no p_i belongs to the orbit (E, E)) and the factorization of the complex (1) induced by it has all factors of the form (2).

Consequently, if m has two different factorizations, then among the factors of (1) it must occur a factor having the form

$$(\{X_1^{a_i^{(\alpha_i)}} \dots X_r^{a_r^{(\alpha_i)}}\}_{i=1}^{s_1}, \{X_1^{h_1-a_1^{(\beta_j)}} \dots X_r^{h_r-a_r^{(\beta_j)}}\}_{j=1}^{s_2})$$

with

$$\langle a_1^{(\alpha_i)}, \dots, a_r^{(\alpha_i)}\rangle \neq \langle a_1^{(\beta_j)}, \dots, a_r^{(\beta_j)}\rangle$$

for all $1 \leqslant i \leqslant s_1, 1 \leqslant j \leqslant s_2$, thus for $j = 1, 2, \dots, r$ we have

$$a_j^{(\alpha_1)} + \dots + a_j^{(\alpha_{s_1})} \equiv a_j^{(\beta_1)} + \dots + a_j^{(\beta_{s_2})} \pmod{h_j}$$

and so the set $\{a^{(1)}, \dots, a^{(s)}\}$ is not F-admissible.

Suppose now that $\{a^{(1)}, \dots, a^{(s)}\}$ is not F-admissible. Then there exist indices $i_1, \dots, i_t, j_1, \dots, j_u$ such that

$$\langle a_1^{(i_\alpha)}, \dots, a_r^{(i_\alpha)}\rangle \neq \langle a_1^{(j_\beta)}, \dots, a_r^{(j_\beta)}\rangle$$

for $1 \leqslant \alpha \leqslant t$, $1 \leqslant \beta \leqslant u$, and

$$a_v^{(i_1)} + \dots + a_v^{(i_t)} \equiv a_v^{(j_1)} + \dots + a_v^{(j_u)} \pmod{h_v}$$

for $v = 1, 2, \dots, r$.

Thus the system

$$(\{X_1^{a_1^{(i_\alpha)}} \dots X_r^{a_r^{(i_\alpha)}}\}_{\alpha=1}^{t}, \{X_1^{h_1-a_1^{(j_\beta)}} \dots X_r^{h_r-a_r^{(j_\beta)}}\}_{\beta=1}^{v})$$

forms a complex, which is clearly a subcomplex of the complex (1) and cannot have a factor of the form (2), consequently m must have a non-unique factorization.

LEMMA 2. *If $m = p_1 \dots p_s$, all primes p_i belong to the same orbit $\mathcal{O} = (X, X^{-1}) \neq (E, E)$ and m has a unique factorization in K, then $p_1 = p_2 = \dots = p_s$ and either p_1 is ramified, or s is at most equal to $r(\mathcal{O})-1$, where by $r(\mathcal{O})$ we denote the least natural number r such that $X^r = E$.*

Proof. If $p_i \neq p_j$ for a pair i, j, then $p_i = \mathfrak{p}\mathfrak{q}$, $p_j = \mathfrak{p}'\mathfrak{q}'$ with $\mathfrak{p}, \mathfrak{p}' \in X$, $\mathfrak{q}, \mathfrak{q}' \in X^{-1}$, thus the number $p_i p_j$ has two factorizations into irreducible integers, given by $p_i p_j = (\mathfrak{p}\mathfrak{q})(\mathfrak{p}'\mathfrak{q}') = (\mathfrak{p}\mathfrak{q}')(\mathfrak{p}'\mathfrak{q})$. As $p_i p_j$ divides m it follows that m does not have a unique factorization.

Thus $p_1 = p_2 = \dots = p_s = \mathfrak{p}\mathfrak{q}$ with $\mathfrak{p} \in X, \mathfrak{q} \in X^{-1}$. If $s \geqslant r(\mathcal{O})$, then $p_1^{r(\mathcal{O})} = (\mathfrak{p}\mathfrak{q})^{r(\mathcal{O})} = \mathfrak{p}^{r(\mathcal{O})}\mathfrak{q}^{r(\mathcal{O})}$. If p_1 is not ramified then $\mathfrak{p} \neq \mathfrak{q}$, hence $p_1^{r(\mathcal{O})}$ has at least two factorizations, and the same follows for m. The lemma is thus proved.

To get similar results for natural numbers with all factorizations of the same length we must introduce a modified notion of admissibility. Suppose $a^{(i)} = (a_1^{(i)}, \dots, a_r^{(i)})$ $(i = 1, 2, \dots, n)$ are given r-tuples of non-negative rational integers satisfying the conditions (i) and (ii) and such that $a_1^{(i)} + \dots + a_r^{(i)} > 0$. Suppose moreover that the r-tuples $a^{(1)}, \dots, a_s$ $(0 \leqslant s \leqslant n)$ correspond to orbits $\mathcal{O}$ with $r(\mathcal{O}) = 2$, i.e. $2a_j^{(i)} \equiv 0 \pmod{h_j}$ for $i = 1, 2, \dots, s$ and $j = 1, 2, \dots, r$ and the other r-tuples $a^{(s+1)}, \dots, a^{(n)}$ correspond to orbits $\mathcal{O}$ with $r(\mathcal{O}) \neq 2$. Finally let $A_{s+1}, \dots, A_n$ be given positive rational integers. We shall say the system $S = (a^{(1)}, \dots, a^{(n)}; A_{s+1}, \dots, A_n)$ is *G-admissible* if and only if it satisfies the condition

(iv) For every two different sequences $(\varepsilon_1, \dots, \varepsilon_n)$, $(\eta_1, \dots, \eta_n)$ with $0 \leqslant \varepsilon_i, \eta_i \leqslant 1$ for $i = 1, 2, \dots, s$ and $0 \leqslant \varepsilon_i, \eta_i \leqslant A_i$ for $i = s+1, \dots, n$,

$$\Big(\sum_{k=1}^{n} \varepsilon_k a_1^{(k)}, \dots, \sum_{k=1}^{n} \varepsilon_k a_r^{(k)}\Big) \not\equiv \Big(\sum_{k=1}^{n} \eta_k a_1^{(k)}, \dots, \sum_{k=1}^{n} \eta_k a_r^{(k)}\Big) \pmod{\langle h_1, \dots, h_r\rangle}.$$

If Q is a set of rational primes, then by $\omega_Q(n)$ we shall denote the number of distinct primes from Q dividing n, and by $\Omega_Q(n)$ we shall denote the number of primes from Q dividing n, each counted accordingly to its multiplicity.

Suppose $a^{(1)}, \dots, a^{(t)}$ are given non-zero r-tuples of nonnegative rational integers satisfying (i) and (ii) and let $\mathcal{O}_1, \dots, \mathcal{O}_t$ be the corresponding orbits. We shall assume that they are numbered in such way that $r(\mathcal{O}_i) = 2$ for $i = 1, 2, \dots, s$ (possibly $s = 0$), and $r(\mathcal{O}_i) \neq 2$ for $i = s+1, \dots, t$. Let m be a natural number with the following decomposition into rational primes:

$$m = \prod_{j=1}^{t} (p_{j,1}^{v_{j,1}} \dots p_{j,s_j}^{v_{j,s_j}}) \qquad (v_{j,k} > 0), \tag{3}$$

where $p_{j,k} \sim \mathcal{O}_j$ for $k = 1, 2, \dots, s_j$ and $j = 1, 2, \dots, t$. Then we have

LEMMA 3. *The number m with the decomposition (3) into rational primes belongs to the set G if and only if the system*

$$S = \big(a^{(1)}, \dots, a^{(t)}; \Omega_{Q_{1+s}}(m), \dots, \Omega_{Q_t}(m)\big)$$

is G-admissible. (Q_i is the set of all rational primes, belonging to $\mathcal{O}_i$.)

Proof. Let $a^{(i)} = (a_1^{(i)}, \dots, a_r^{(i)})$ for $i = 1, 2, \dots, t$ and consider the complex

$$\{T_1, \dots, T_1, \dots, T_t, \dots, T_t, T_1^{-1}, \dots, T_1^{-1}, \dots, T_t^{-1}, \dots, T_t^{-1}\}, \tag{4}$$

where $T_i = X_1^{a_i^{(1)}} \dots X_r^{a_i^{(r)}}$ $(i = 1, 2, \dots, t)$ and T_i, T_i^{-1} occur $\Omega_{Q_i}(m)$ times.

Clearly (4) is the complex associated with m in the way explained in the proof of Lemma 1. Note that every factorization of m in K has the same length, i.e. $m \in G$ if and only if every factor of the complex (4) has the length 2.

Suppose now that the system S is not G-admissible and m has all its factorizations of the same length. With suitable $\varepsilon_1, \dots, \varepsilon_t, \eta_1, \dots, \eta_t$ satisfying

$$(\varepsilon_1, \dots, \varepsilon_t) \neq (\eta_1, \dots, \eta_t),$$
$$0 \leqslant \varepsilon_i, \eta_i \leqslant 1 \quad \text{for} \quad i = 1, 2, \dots, s,$$
$$0 \leqslant \varepsilon_i, \eta_i \leqslant \Omega_{Q_i}(m) \quad \text{for} \quad i = s+1, \dots, t,$$

we have

$$\sum_{i=1}^{t} \varepsilon_i a_j^{(i)} \equiv \sum_{i=1}^{t} \eta_i a_j^{(i)} \pmod{h_j} \tag{5}$$

for $j = 1, 2, \dots, r$.

Consider now the system

$$\{T_1, \dots, T_1, \dots, T_t, \dots, T_t, T_1^{-1}, \dots, T_1^{-1}, \dots, T_t^{-1}, \dots, T_t^{-1}\} \tag{6}$$

where T_i and T_i^{-1} appear ε_i respectively η_i times.

In view of (5) this is a complex, which is a subcomplex of (4) and so every factor of (6) must be of the length two. It follows that every factor of (6) has one of the following forms: $\{T_i, T_j\}$, $\{T_i, T_j^{-1}\}$, $\{T_i^{-1}, T_j^{-1}\}$. Suppose that for some i, j, $\{T_i, T_j\}$ is a factor. Then $T_i T_j = E$ hence T_i and T_j represent the same orbit thus $i = j \leqslant s$. But in this case $0 \leqslant \varepsilon_i + \eta_i \leqslant 1$ and so T_i can appear at most once in (6). It follows that $\{T_i, T_i\}$ is not a subcomplex of (6). In the same way it follows that $\{T_i^{-1}, T_j^{-1}\}$ is not a factor of (6) and consequently every factor of (6) must be of the form $\{T_i, T_j^{-1}\}$. As $T_i \neq T_j$ for $i \neq j$ it results $i = j$ because $T_i T_j^{-1} = E$. We found thus that every factorization of (6) has the form

$$\{(T_1, T_1^{-1}), (T_1, T_1^{-1}), \dots, (T_t, T_t^{-1})\}$$

hence for every i, T_i and T_i^{-1} must occur the same number of times in (6), i.e. $\varepsilon_i = \eta_i$ for $i = 1, 2, \dots, t$, a contradiction. We proved thus that if all factorizations of m have the same length then the system S is G-admissible.

Now let us assume that m has factorizations with different lengths. Then the complex (4) must have a factor of the length at least three, say

$$\{T_1, \dots, T_1, \dots, T_t, \dots, T_t, T_1^{-1}, \dots, T_1^{-1}, \dots, T_t^{-1}, \dots, T_t^{-1}\} \tag{7}$$

where T_i appears ε_i times, and T_i^{-1} appears η_i times. Moreover $0 \leqslant \varepsilon_i, \eta_i \leqslant \Omega_{Q_i}(m)$ and $\varepsilon_i \eta_i = 0$ for $i = 1, 2, \dots t$ as (7) is a factor and so cannot have subcomplexes of the form $\{T_i, T_i^{-1}\}$ and is not of this form itself because its length is $\neq 2$. By the same reason for $i = 1, 2, \dots, s$ ε_i and η_i can assume the values 0 and 1 only, as otherwise (7) would have a subcomplex $\{T_i, T_i\}$ respectively $\{T_i^{-1}, T_i^{-1}\}$.

From $T_1^{\varepsilon_1} \dots T_t^{\varepsilon_t} T_1^{-\eta_1} \dots T_t^{-\eta_t} = E$ it results

$$\sum_{j=1}^{t} \varepsilon_j a_k^{(j)} \equiv \sum_{j=1}^{t} \eta_j a_k^{(j)} \pmod{h_k}$$

for $k = 1, 2, \dots, r$ and so the system S is not G-admissible. The lemma is thus proved.

Now let $a = (a^{(1)}, \dots, a^{(t)})$ be a F-admissible set of r-tuples, let for $i = 1, 2, \dots, t$ $\mathcal{O}_i$ be the orbit corresponding to the r-tuple $a^{(i)}$ and let Q_i be the set of all rational primes belonging to the orbit $\mathcal{O}_i$. Let us now define

$$S_a = \{n \mid n = p_1 \dots p_t,\ p_i \in Q_i\ (i = 1, 2, \dots, t)\},$$
$$S'_a = \{n \mid n = p_1^{a_1} \dots p_t^{a_t},\ p_i \in Q_i,\ a_i \geqslant 1\ (i = 1, 2, \dots, t)\}$$

and $S = \bigcup_a S_a$, $S' = \bigcup_a S'_a$ where the sums are taken over all F-admissible sets of r-tuples. Finally let Z be the set of all natural numbers all prime factors of which are either products of two principal prime ideals in K or generate prime ideals in K.

Then we have

LEMMA 4. *For every k, l*

$$N\{n \leqslant x \mid n \equiv l \pmod{k},\ n = n_1 n_2,\ n_1 \in Z,\ n_2 \in S\} \leqslant F_{k,l}(x)$$
$$\leqslant N\{n \leqslant x \mid n \equiv l \pmod{k},\ n = n_1 n_2,\ n_1 \in Z,\ n_2 \in S'\}.$$

Proof. Observe first that if a natural number m has unique factorization in K, then $m = m_1 m_2$ where $m_1 \in Z$ and $m_2 \in S'$. Indeed, if after dividing m by its maximal divisor from Z we are left with, say $m_2 = p_1^{v_1} \dots p_u^{v_u}$ then $p_1 \dots p_u$ must have unique factorization in K, and from Lemmas 1 and 2 it follows that either $u = 1$ and in this case $m_2 = p_1^{v_1} \in S'$ (because every set a satisfying (i) and (ii) and consisting of exactly one non-zero r-tuple is evidently F-admissible) or else $p_1 \dots p_s \in S$, hence $p_1^{v_1} \dots p_u^{v_u} = m_2 \in S'$.

Conversely, from Lemma 1 follows that every number $m = m_1 m_2$ ($m_1 \in Z$, $m_2 \in S$) has a unique factorization. The lemma is thus proved.

Let $V = (a^{(1)}, \dots, a^{(s)}, \dots, a^{(t)}; A_{1+s}, \dots, A_t)$ be a G-admissible system (ordered in the same way as stated before Lemma 3), let for $i = 1, 2, \dots, t$ $\mathcal{O}_i$ be the orbit corresponding to the r-tuple $a^{(i)}$, and let Q_i be the set of all rational primes belonging to the orbit $\mathcal{O}_i$. Finally let $\bar{Q}_V$ be the set of all primes belonging to orbits different from $\mathcal{O}_1, \dots, \mathcal{O}_t$, (E, E), i.e. $\bar{Q}_V = P \setminus (Q_0 \cup Q_1 \cup \dots \cup Q_t)$ where P is the set of all rational primes and Q_0 is the set of all primes contained in Z.

Let k, l be given natural numbers with the greatest common divisor $(k, l) = D$. We shall say the system V is *D-G-admissible* if for $i = 1+s, \dots, t$, $\Omega_{Q_i}(D) \leqslant A_i$ and $\Omega_{\bar{Q}_V}(D) = 0$.

Let

$$R_V^{(k,l)} = \{n \mid n \equiv l \pmod k,\ \Omega_{Q_i}(n) \geqslant 1\ (i = 1, 2, \ldots, s),\ \Omega_{Q_i}(n) = A_i\ (i = 1+s, \ldots, t),\ \Omega_{\bar{Q}_V}(n) = 0\}.$$

(Note that for different systems V the corresponding sets $R_V^{(k,l)}$ are disjoint.)

Lemma 3 implies immediately the following

LEMMA 5.

$$\{n \mid n \equiv l \pmod k,\ n \in G\} = \bigcup_V R_V^{(k,l)}$$

where the sum is taken over all D-G-admissible systems V.

3. We shall use a tauberian theorem of H. Delange (see [2], theorem b) which we state as

LEMMA 6. *Suppose that β is a real number, which is not zero or a negative integer, q is a positive integer and A is a set of natural numbers such that for $\operatorname{re} s > 1$ the following equality holds:*

$$\sum_{n \in A} n^{-s} = (s-1)^{-\beta} \sum_{j=0}^{q} a_j(s) \left(\log \frac{1}{s-1}\right)^j + b(s)$$

with $a_1(s), \ldots, a_q(s), b(s)$ regular for $\operatorname{re} s \geqslant 1$, and $a_q(1) \neq 0$. Then

$$N(n \leqslant x \mid n \in A) \approx a_q(1)\Gamma^{-1}(\beta) x (\log x)^{\beta-1} (\log\log x)^q.$$

We shall say that a set Q of rational primes is *regular* (cf. [2]) if there exists a nonnegative number β and a function $g(s)$ regular in the closed halfplane $\operatorname{re} s \geqslant 1$ such that

$$\sum_{p \in Q} p^{-s} = \beta \log \frac{1}{s-1} + g(s)$$

holds for $\operatorname{re} s > 1$.

(We shall in sequel denote by the same symbol $g(s)$, with or without indices, a function regular in the closed halfplane $\operatorname{re} s \geqslant 1$, not always the same.)

The number β occurring in the definition of a regular set is called the *density* of this set. Following H. Delange ([2]) we shall associate with every regular set of primes Q with a positive density β a constant $\mathscr{K}_Q$ defined by

$$\mathscr{K}_Q^{-1} = \Gamma(\beta) e^{C\beta} \lim_{x \to \infty} \left\{(\log x)^\beta \prod_{\substack{p \leqslant x \\ p \in Q}} (1-p^{-1})\right\}$$

where C is Euler's constant.

We shall need the following lemmas:

LEMMA 7. (For the case $t = 1$, see [2], theorems 36 and 41. In the general case no essential changes in the proof are needed.) *Suppose $Q_1, \ldots, Q_t$ are disjoint regular sets of rational primes with positive densities $a_1, \ldots, a_t$ respectively satisfying $a_1 + \ldots + a_t < 1$. Suppose that $q_1, \ldots, q_t$ are given nonnegative rational integers, not all of them equal to zero. Then*

$$\begin{aligned} &N\{n \leqslant x \mid \Omega_{Q_i}(n) = q_i \text{ for } i = 1, 2, \ldots, t\} \\ &\quad \approx N\{n \leqslant x \mid \omega_{Q_i}(n) = q_i \text{ for } i = 1, 2, \ldots, t\} \\ &\quad \approx \mathscr{K}_Q a_1^{q_1} \ldots a_t^{q_t} \{(q_1)! \ldots (q_t)!\}^{-1} x (\log\log x)^{q_1+\ldots+q_t} (\log x)^{-(a_1+\ldots+a_t)}, \end{aligned}$$

where Q is the set of all rational primes which do not belong to the sum $Q_1 \cup \ldots \cup Q_t$.

In the course of proving this lemma one arrives at the following identities holding for $\operatorname{re} s > 1$ and $|z_i| < 1$ $(i = 1, 2, \ldots, t)$:

$$(8)\quad \sum_{n=1}^{\infty} \frac{z_1^{\Omega_1(n)} \ldots z_t^{\Omega_t(n)}}{n^s} = H(s)(s-1)^{a_1+\ldots+a_t-1} \prod_{i=1}^{t} \sum_{k=0}^{\infty} \sum_{j=0}^{k} a_i^j f_{k-j,k}^{(i)}(s) z_i^k \left(\log \frac{1}{s-1}\right)^j (j!)^{-1};$$

$$(9)\quad \sum_{n=1}^{\infty} \frac{z_1^{\omega_1(n)} \ldots z_t^{\omega_t(n)}}{n^s} = \bar{H}(s)(s-1)^{a_1+\ldots+a_t-1} \prod_{i=1}^{t} \sum_{k=0}^{\infty} \sum_{j=0}^{k} a_i^j \bar{f}_{k-j,k}^{(i)}(s) z_i^k \left(\log \frac{1}{s-1}\right)^j (j!)^{-1},$$

where $H(s)$, $\bar{H}(s)$, $f_{j,k}^{(i)}(s)$, $\bar{f}_{j,k}^{(i)}(s)$ $(i = 1, 2, \ldots, t;\ j = 0, 1, \ldots, k;\ k = 0, 1, 2, \ldots)$ are regular for $\operatorname{re} s \geqslant 1$, $\Omega_i(n)$ respectively $\omega_i(n)$ stand for $\Omega_{Q_i}(n)$, $\omega_{Q_i}(n)$ and $H(1)\bar{H}(1) f_{0,k}^{(1)}(1) \ldots f_{0,k}^{(t)}(1) \bar{f}_{0,k}^{(1)}(1) \ldots \bar{f}_{0,k}^{(t)}(1) \neq 0$ for $k = 0, 1, 2, \ldots$

LEMMA 8. *Suppose that $Q_1, \ldots, Q_t$ and $q_1, \ldots, q_t$ are the same as in Lemma 7. Let moreover k be a given natural number. Then*

$$\begin{aligned} &N\{n \leqslant x \mid \Omega_{Q_i}(n) = q_i\ (i = 1, \ldots, t),\ (k, n) = 1\} \\ &\quad \approx N\{n \leqslant x \mid \omega_{Q_i}(n) = q_i\ (i = 1, \ldots, t),\ (k, n) = 1\} \\ &\quad \approx \prod_{\substack{p \mid k \\ p \in Q}} (1-p^{-1}) N\{n \leqslant x \mid \Omega_{Q_i}(n) = q_i\ (i = 1, \ldots, t)\}, \end{aligned}$$

where Q has the same meaning as in Lemma 7.

Proof. We use the method of H. Delange ([2]). Let $|z_i| < 1$ for $i = 1, 2, \ldots, t$. Then for $\mathrm{re}\, s > 1$ we have

$$\Phi(s, z_1, \ldots, z_t) = \sum_{\substack{n \\ (n,k)=1}} z_1^{\Omega_1(n)} \ldots z_t^{\Omega_t(n)} n^{-s} = \prod_{p \nmid k} (1 - z_1^{\Omega_1(p)} \ldots z_t^{\Omega_t(p)} p^{-s})^{-1}$$

$$= \prod_{p|k} (1 - z_1^{\Omega_1(p)} \ldots z_t^{\Omega_t(p)} p^{-s}) \sum_{n=1}^{\infty} z_1^{\Omega_1(n)} \ldots z_t^{\Omega_t(n)} n^{-s},$$

(here $\Omega_i(n)$ stands for $\Omega_{Q_i}(n)$) and using (8) we get

$$\Phi(s, z_1, \ldots, z_t) = \prod_{p|k} (1 - z_1^{\Omega_1(p)} \ldots z_t^{\Omega_t(p)} p^{-s}) H(s) (s-1)^{a_1+\ldots+a_t-1} \times$$

$$\times \prod_{i=1}^{t} \sum_{k=0}^{\infty} \sum_{j=0}^{k} a_j^i f_{k-j,k}^{(i)}(s) z_i^k \left(\log \frac{1}{s-1}\right)^j (j!)^{-1}.$$

Now,

$$\prod_{p|k} (1 - z_1^{\Omega_1(p)} \ldots z_t^{\Omega_t(p)} p^{-s})$$

$$= \prod_{\substack{p|k \\ p \in Q}} (1-p^{-s}) \prod_{i=1}^{t} \prod_{\substack{p|k \\ p \in Q_i}} (1 - z_i p^{-s}) = \prod_{\substack{p|k \\ p \in Q}} (1-p^{-s}) \prod_{i=1}^{t} \left\{ \sum_{j=0}^{r_i} z_i^j \Big(\sum_{\substack{d|D_i \\ \Omega_i(d)=j}} \mu(d) d^{-s} \Big) \right\}$$

where r_i is the number of rational primes dividing k and belonging to Q_i, and D_i is their product. Finally we get

$$\Phi(s, z_1, \ldots, z_t) = H(s)(s-1)^{a_1+\ldots+a_t-1} \prod_{\substack{p|k \\ p \in Q}} (1-p^{-s}) \times$$

$$\times \prod_{i=1}^{t} \left\{ \sum_{\nu=0}^{\infty} z_i^{\nu} \left(\sum_{j=0}^{\nu_i} \sum_{\substack{d|D_i \\ \Omega_i(d)=j}} \sum_{l=0}^{\nu-j} \mu(d) \left(\log \frac{1}{s-1}\right)^l a_i^l f_{\nu-j-l,\nu-j}^{(i)}(s) (l!)^{-1} d^{-s} \right) \right\},$$

where $\nu_i = \min(\nu, r_i)$.

It follows by equating coefficients that

$$\sum_{\substack{n \\ (n,k)=1 \\ \Omega_i(n)=q_i}} n^{-s} = H(s)(s-1)^{a_1+\ldots+a_t-1} \prod_{\substack{p|k \\ p \in Q}} (1-p^{-s}) \times$$

$$\times \prod_{i=1}^{t} \left\{ \sum_{j=0}^{\lambda_i} \sum_{\substack{d|D_i \\ \Omega_i(d)=j}} \sum_{l=0}^{q_i-j} \mu(d) \left(\log \frac{1}{s-1}\right)^l a_i^l f_{q_i-l-j,q_i-j}^{(i)}(s) (l!)^{-1} d^{-s} \right\}$$

with $\lambda_i = \min\{r_i, q_i\}$, and it results finally

$$\sum_{\substack{n \\ (n,k)=1 \\ \Omega_i(n)=q_i}} n^{-s}$$

$$= H(s)(s-1)^{a_1+\ldots+a_t-1} \prod_{\substack{p|k \\ p \in Q}} (1-p^{-s}) \left\{ \frac{f_{0,q_1}^{(1)}(s) \ldots f_{0,q_t}^{(t)}(s)}{q_1! \ldots q_t!} a_1^{q_1} \ldots a_t^{q_t} \times \right.$$

$$\left. \times \left(\log \frac{1}{s-1} \right)^{a_1+\ldots+a_t} + g_1(s) \left(\log \frac{1}{s-1} \right)^{a_1+\ldots+a_t-1} + \ldots + g_{a_1+\ldots+a_t}(s) \right\}.$$

By Lemma 6, we get

$$N\{n \leqslant x \mid \Omega_i(n) = q_i \ (i = 1, \ldots, t), \ (k, n) = 1\}$$

$$\approx \prod_{\substack{p|k \\ p \in Q}} \left(1 - \frac{1}{p}\right) H(1) \frac{f_{0,q_1}^{(1)}(1) \ldots f_{0,q_t}^{(t)}(1)}{q_1! \ldots q_t! \Gamma(1-(a_1+\ldots+a_t))} \cdot \frac{x (\log\log x)^{a_1+\ldots+a_t}}{(\log x)^{a_1+\ldots+a_t}}.$$

But from (8), we get

$$\sum_{\substack{n \\ \Omega_i(n)=q_i}} n^{-s} = H(s)(s-1)^{a_1+\ldots+a_t-1} \left\{ \frac{f_{0,q_1}^{(1)}(s) \ldots f_{0,q_t}^{(t)}(s)}{q_1! \ldots q_t!} a_1^{q_1} \ldots a_t^{q_t} \times \right.$$

$$\left. \times \left(\log \frac{1}{s-1} \right)^{a_1+\ldots+a_t} + g_1(s) \left(\log \frac{1}{s-1} \right)^{a_1+\ldots+a_t-1} + \ldots + g_{a_1+\ldots+a_t}(s) \right\}$$

and after applying Lemma 6 and comparing the obtained result with (11) one finishes the proof of the first part of our lemma. The second part, concerning $\omega_{Q_i}(n)$, can be dealt with in a similar way using (9) in place of (8).

LEMMA 9. (See e.g. [4]). *If K is a quadratic number field and $\mathcal{O} = (X, X^{-1}) \neq (E, E)$ is an orbit of H, then the set $Q_{\mathcal{O}}$ of all rational primes belonging to the orbit $\mathcal{O}$ is regular and has the density $1/h\varepsilon(X)$, where $\varepsilon(X) = 2$ if $X^2 = E$, and $\varepsilon(X) = 1$ otherwise. Moreover the set Q_0 of all rational primes belonging to the set Z (occurring in Lemma 4) is regular and has the density $(h+1)/2h$.* (In sequel we shall use the notation Q_0 for this set of primes only.)

LEMMA 10. (See [4], [5]). *Let $\mathfrak{f}$ be an ideal in K and W let be an ideal class* (mod $\mathfrak{f}$) *in the narrow sense. Then the following equality holds for* $\mathrm{re}\, s > 1$:

$$\sum_{\mathfrak{p} \in W} (N\mathfrak{p})^{-s} = \frac{1}{h(\mathfrak{f})} \log \frac{1}{s-1} + g(s)$$

where the sum is taken over all prime ideals in W and $h(\mathfrak{f})$ is the number of classes (mod $\mathfrak{f}$).

(Two ideals $\mathfrak{a}, \mathfrak{b}$ relatively prime to $\mathfrak{f}$ *belong to the same class* (mod $\mathfrak{f}$) if and only if there exist in K two totally positive integers x and y both congruent to 1 (mod $\mathfrak{f}$) and such that $\mathfrak{a}(x) = \mathfrak{b}(y)$, where (t) denotes the principal ideal generated by t. Clearly $\mathfrak{a}$ and $\mathfrak{b}$ must belong to the same absolute ideal-class.)

LEMMA 11. *Let K be a quadratic number field. Suppose that $X_1, \dots, X_t$ are ideal-classes belonging to disjoint orbits, and such that $\varepsilon^{-1}(X_1) + \dots + \varepsilon^{-1}(X_t) < h$. Let Q_i be the set of rational primes belonging to the orbit (X_i, X_i^{-1}) $(i = 1, 2, \dots, t)$, and let $A_1, \dots, A_t$ are given nonnegative rational integers, not all of them equal to zero. Finally let k be a given natural number, relatively prime to the discriminant of K, and let $\chi(n)$ be a non-principal character* (mod k). *Let f stand for one of the functions ω, Ω. Then the series*

$$\sum \chi(n) n^{-s} = H_\chi^{(f)}(s)$$

(where the sum is taken over all n which are relatively prime to k, and for which $f_{Q_i}(n) = A_i$ $(i = 1, 2, \dots, t)$) defines for $\operatorname{res} > 1$ *a function $H_\chi^{(f)}(s)$ which can be continued to a function regular in the closed halfplane* $\operatorname{res} \geqslant 1$. *For the principal character χ_0 this series defines a function $H_{\chi_0}^{(f)}(s)$ regular for* $\operatorname{res} > 1$.

Proof. Only the possibility of continuation needs a verification. Consider a division of ideals relatively prime to (k) into classes defined as follows: two ideals *belong to the same class* if and only if they belong to the same absolute class and their norms are congruent (mod k). It is easy to see that the classes so defined form a group under multiplication. Let us denote it by J, and let $J_1, \dots, J_w$ be the elements of J.

Clearly two ideals belonging to the same class (mod (k)) belong to the same class J_i. Moreover the number of classes (mod (k)) forming a class J_i is independent of i. Indeed, let $W_1, \dots, W_z$ be classes (mod (k)) forming a class J_i and let $U_1, \dots, U_y$ be classes (mod (k)) forming the class J_1 = consisting of all principal ideals whose norms are congruent to 1 (mod k). Let $w_i \in W_i$ $(i = 1, 2, \dots, z)$, let J_i^{-1} be the class inverse to J_i in the group J and let $x \in J_i^{-1}$. Then xw_i $(i = 1, \dots, z)$ all belong to J_1 (which is the unit of J) and are inequivalent (mod (k)). Thus $z \leqslant y$. Now take $u_i \in U_i$ $(i = 1, \dots, y)$ and consider $u_i w_1$. These ideals belong to J_i and are clearly inequivalent (mod (k)), hence $y \leqslant z$ and the equality $y = z$ follows, as asserted.

Let us denote by $C(k)$ the number of classes (mod (k)) forming a class J_i.

Now let X be an absolute ideal-class, j a norm-residue (mod k), relatively prime to k and let $U_1, \dots, U_{C(k)}$ be classes (mod (k)) contained in the class $K = \{\mathfrak{a} \mid \mathfrak{a} \in X, N\mathfrak{a} \equiv j \pmod k\}$. Finally let $P_j(X)$ be the set of all rational primes congruent to j (mod k) which are norms of prime ideals from the class X. From Lemma 10 we get for $\operatorname{res} > 1$

$$\sum_{p \in P_j(X)} p^{-s} = \sum_{m=1}^{C(k)} \sum_{\substack{p = Np \\ \mathfrak{p} \in U_m}} p^{-s} = C(k) h^{-1}\big((k)\big) \varepsilon^{-1}(X) \log \frac{1}{s-1} + g(s).$$

As k has no ramified prime divisors, the set of all principal ideals $\mathfrak{a}$ with $N(\mathfrak{a}) \equiv j \pmod k$ (with an arbitrarily given j, relatively prime to k) is not void. It follows easily that the set of all ideals $\mathfrak{a}$ belonging to the class X and satisfying $N(\mathfrak{a}) \equiv j \pmod k$ is not void. This set contains a class (mod (k)) and so, by the theorem of Hecke (see [4]) it contains infinitely many prime ideals of the first degree.

It follows that for every character $\chi \pmod k$ and $\operatorname{res} > 1$ we have

$$\sum_{\substack{p = Np \\ \mathfrak{p} \in X}} \chi(p) p^{-s} = S(k) h^{-1}\big((k)\big) \varepsilon^{-1}(X) \sum_{\substack{1 \leqslant j \leqslant k \\ (j,k)=1}} \chi(j) \log \frac{1}{s-1} + g(s).$$

For non-principal χ this implies obviously

$$\sum_{\substack{p = Np \\ \mathfrak{p} \in X}} \chi(p) p^{-s} = g(s) \tag{12}$$

for $\operatorname{res} > 1$.

Let first $f = \Omega$. Let $z_1, \dots, z_t$ be arbitrary complex numbers inside the unit circle. Then for $\operatorname{res} > 1$ we have (writing shortly $\Omega_i(n)$ for $\Omega_{Q_i}(n)$)

$$\begin{aligned}
\sum_{(n,k)=1} z_1^{\Omega_1(n)} \dots z_t^{\Omega_t(n)} \chi(n) n^{-s} &= \prod_{p \nmid k} \big(1 - z_1^{\Omega_1(p)} \dots z_t^{\Omega_t(p)} \chi(p) p^{-s}\big)^{-1} \\
&= \prod_{i=1}^{t} \prod_{\substack{p \nmid k \\ p \in Q_i}} \big(1 - z_i \chi(p) p^{-s}\big)^{-1} \prod_{\substack{p \nmid k \\ \mathfrak{p} \notin \bigcup_{i=1}^{t} Q_i}} \big(1 - \chi(p) p^{-s}\big)^{-1} \\
&= \prod_{i=1}^{t} \Big\{ H_i(s, z_i) \exp\Big\{ z_i \sum_{\substack{p \nmid k \\ p \in Q_i}} \chi(p) p^{-s} \Big\} \Big\} \exp \sum_{\substack{p \nmid k \\ \mathfrak{p} \notin \bigcup_{i=1}^{t} Q_i}} \chi(p) p^{-s} \\
&= \prod_{i=1}^{t} \big\{ H_i(s, z_i) \exp\big\{ z_i g_i(s) \big\} \big\} \exp \sum_{\substack{p \nmid k \\ \mathfrak{p} \notin \bigcup_{i=1}^{t} Q_i}} \chi(p) p^{-s}
\end{aligned}$$

by (12). Here $H_1(s, z_1), \dots, H_t(s, z_t)$ are regular for $\operatorname{re} s \geqslant 1$ and $|z_i| < 1$ and not vanishing there, by Lemma 4 of [2].

Moreover for $\operatorname{re} s > 1$ we have

$$\sum_{\substack{p \nmid k \\ p \neq \bigcup_{i=1}^{t} Q_i}} \chi(p) p^{-s} = \sum_{p \nmid k} \chi(p) p^{-s} - \sum_{i=1}^{t} \sum_{\substack{p \in Q_i \\ p \nmid k}} \chi(p) p^{-s} = \log L(s, \chi) + g(s) = g(s).$$

It follows that

$$\sum_{\substack{n \\ (n,k)=1}} z_1^{\Omega_1(n)} \dots z_t^{\Omega_t(n)} \chi(n) n^{-s} = H_1(s, z_1) \dots H_t(s, z_t) g(s) \exp\Big\{\sum_{i=1}^{t} z_i h_i(s)\Big\}$$

with $H_1(1, z_1) \dots H_t(1, z_t) g(1) \neq 0$.

After expanding the right-hand side in a power series and equating coefficients on both sides we obtain the required result for $f = \Omega$:

In the case $f = \omega$ one shall start with the following identities valid for $\operatorname{re} s > 1$ and $|z_i| < 1$:

$$\begin{aligned}
\sum_{\substack{n \\ (n,k)=1}} z_1^{\omega_1(n)} \dots z_t^{\omega_t(n)} \chi(n) n^{-s} &= \prod_{p \nmid k} \Big(1 + \frac{z_1^{\omega_1(p)} \dots z_t^{\omega_t(p)} \chi(p)}{p^s - \chi(p)}\Big) \\
&= \prod_{i=1}^{t} \prod_{\substack{p \nmid k \\ p \in Q_i}} \Big(1 + \frac{z_i \chi(p)}{p^s - \chi(p)}\Big) \prod_{\substack{p \nmid k \\ p \neq \bigcup_{i=1}^{t} Q_i}} \Big(1 + \frac{\chi(p)}{p^s - \chi(p)}\Big) \\
&= \prod_{i=1}^{t} \bar{H}_i(s, z_i) \exp\Big\{z_i \sum_{\substack{p \in Q_i \\ p \nmid k}} \chi(p) p^{-s}\Big\} \bar{H}(s) \exp\Big\{\sum_{\substack{p \nmid k \\ p \neq \bigcup_{i=1}^{t} Q_i}} \chi(p) p^{-s}\Big\}
\end{aligned}$$

with $\bar{H}_1(s, z_1), \dots, \bar{H}_t(s, z_t)$ and $\bar{H}(s)$ not vanishing for $\operatorname{re} s \geqslant 1$ by lemma 4 of [2], and then proceed as above.

LEMMA 12. *The assumptions are as in Lemma 11. Moreover let* $(k, l) = 1$. *Then*

$$\begin{aligned}
&N\{n \leqslant x \mid n \equiv l \pmod k,\ \Omega_{Q_i}(n) = A_i\ (i = 1, 2, \dots, t)\} \\
&\quad \approx N\{n \leqslant x \mid n \equiv l \pmod k,\ \omega_{Q_i}(n) = A_i\ (i = 1, 2, \dots, t)\} \\
&\quad \approx \varphi^{-1}(k) N\{n \leqslant x \mid (n, k) = 1,\ \Omega_{Q_i}(n) = A_i\ (i = 1, 2, \dots, t)\}.
\end{aligned}$$

Proof. Let $F_m(s) = \sum_n n^{-s}$ where the sum is taken over all natural numbers congruent to $m \pmod k$ and for which $\Omega_{Q_i}(n) = A_i\ (i = 1, 2, \dots, t)$.

Then for the function $H_\chi^{(\Omega)}(s)$ (as defined in Lemma 11) we have

$$H_\chi^{(\Omega)}(s) = \sum_{\substack{1 \leqslant m \leqslant k \\ (k,m)=1}} \chi(m) F_m(s) \qquad (\operatorname{re} s > 1)$$

and it follows by Lemma 11

$$F_l(s) = \varphi^{-1}(k) \sum_\chi \overline{\chi(l)} H_\chi^{(\Omega)}(s) = \varphi^{-1}(k) H_{\chi_0}^{(\Omega)}(s) + g(s) \qquad (\operatorname{re} s > 1).$$

As

$$H_{\chi_0}^{(\Omega)}(s) = \sum_{\substack{n \\ (n,k)=1 \\ \Omega_{Q_i}(n) = A_i}} n^{-s}$$

thus by (10) and Lemma 6 the desired evaluation follows in the case of Ω. In the case of ω instead of Ω the argument is the same (instead of (10) one has to use its analogue for ω which is easy provable along the same lines).

LEMMA 13. *The assumptions are as in Lemma 11. Moreover let* $(k, l) = D$.

If for some i, $A_i < \Omega_{Q_i}(D)$, *then*

$$N\{n \leqslant x \mid n \equiv l \pmod k,\ \Omega_{Q_i}(n) = A_i\ (i = 1, \dots, t)\} = 0 \quad \text{for all } x.$$

If for $i = 1, 2, \dots, t$, $A_i \geqslant \Omega_{Q_i}(D)$ *then*

$$\begin{aligned}
&N\{n \leqslant x \mid n \equiv l \pmod k,\ \Omega_{Q_i}(n) = A_i\ (i = 1, 2, \dots, t)\} \\
&\approx \varphi^{-1}(k_1) \prod_{\substack{p \mid k_1 \\ p \in Q}} (1 - p^{-1}) N\{n \leqslant x/D \mid \Omega_{Q_i}(n) = A_i - \Omega_{Q_i}(D)\ (i = 1, 2, \dots, t)\} \\
&\approx \varphi^{-1}(k_1) \Big(\prod_{\substack{p \mid k_1 \\ p \in Q}} (1 - p^{-1})\Big) \mathscr{K}_Q h^{-\mu} \Big(\prod_{i=1}^{t} \varepsilon(X_i)^{-m_i} (m_i!)^{-1}\Big) x D^{-1} (\log\log x)^{\mu} (\log x)^{-\nu},
\end{aligned}$$

where $k_1 = k/D$, $m_i = A_i - \Omega_{Q_i}(D)$, $m_1 + \dots + m_t = \mu$, $\big(\varepsilon(X_1)^{-1} + \dots + \varepsilon(X_t)^{-1}\big) h^{-1} = \nu$, Q *is the set of all rational primes not included in the set* $Q_1 \cup \dots \cup Q_t$ *and* h *is the class number of* K. *The constant* $\mathscr{K}_Q$ *is defined before Lemma 7.*

Proof. The first part is trivial. To establish the second part observe that the functions $\Omega_{Q_i}(n)$ are completely additive and so

$$\begin{aligned}
&N\{n \leqslant x \mid n \equiv l \pmod k,\ \Omega_{Q_i}(n) = A_i\ (i = 1, 2, \dots, t)\} \\
&= N\{n \leqslant x/D \mid n \equiv l/D \pmod{k_1},\ \Omega_{Q_i}(n) = A_i - \Omega_{Q_i}(D)\ (i = 1, 2, \dots, t)\}.
\end{aligned}$$

The lemma follows now from Lemmas 7, 8, 9 and 12.

4. Now we can find the asymptotic evaluations of the functions $F_{k,l}(x)$ and $G_{k,l}(x)$. Let us start with $F_{k,l}(x)$. In this case we assume that k and l have no common divisor larger than 1. By Lemma 4 the problem is reduced to the evaluation of the number of elements $\leqslant x$ in following sets:

$$S_a^{(k,l)} = \{n \mid n \equiv l \pmod k),\ n = mp_1 \dots p_t,\ p_i \in Q_i,\ m \in Z\},$$
$$\overline{S}_a^{(k,l)} = \{n \mid n \equiv l \pmod k),\ n = mp_1^{a_1} \dots p_t^{a_t},\ p_i \in Q_i,\ a_i \geqslant 1,\ m \in Z\},$$

where $a = (a^{(1)}, \dots, a^{(t)})$ is a F-admissible set of r-tuples, Q_i is the set of all rational primes belonging to the orbit $\mathcal{O}_i$, which corresponds to the r-tuple $a^{(i)}$, and Z is, as before, the set of all natural numbers all prime factors of which are either products of two principal ideals in K or generate prime ideals in K.

We can write the sets $S_a^{(k,l)}$ and $\overline{S}_a^{(k,l)}$ in the following form:

$$S_a^{(k,l)} = \{n \mid n \equiv l \pmod k),\ \Omega_{Q_i}(n) = 1\ (i = 1, \dots, t),$$
$$\Omega_{Q_i}(n) = 0\ (i = 1+t, \dots, v)\},$$
$$\overline{S}_a^{(k,l)} = \{n \mid n \equiv l \pmod k),\ \omega_{Q_i}(n) = 1\ (i = 1, \dots, t),$$
$$\omega_{Q_i}(n) = 0\ (i = 1+t, \dots, v)\},$$

where $Q_{t+1}, \dots, Q_v$ are the sets of all rational primes belonging to the remaining orbits $\mathcal{O}_{t+1}, \dots, \mathcal{O}_v \neq (E, E)$. From the Lemmas 7, 8, 9 and 12 we obtain

$$(13)\quad N\{n \leqslant x \mid n \in S_a^{(k,l)}\} \approx N\{n \leqslant x \mid n \in \overline{S}_a^{(k,l)}\}$$
$$\approx \varphi^{-1}(k) \prod_{\substack{p \mid k \\ p \in Q_0}} (1-p^{-1}) \cdot \mathcal{K}_{Q_0} h^{-t} \Big(\prod_{i=1}^{t} \varepsilon(X_i)^{-1} \Big) x (\log\log x)^t (\log x)^{-\nu}$$

where ν is the density of the set $Q_1 \cup \dots \cup Q_v$.

Observe now that $Q_0 \cup Q_1 \cup \dots \cup Q_v$ is the set of all rational primes, and so the density of Q_0 (which is equal to $(h+1)/2h$ by Lemma 9) equals $1-\nu$. It follows finally that $\nu = (h-1)/2h$.

It is clear that for different F-admissible sets a and b the corresponding sets $S_a^{(k,l)}$ and $S_b^{(k,l)}$ are disjoint, and the same holds for the sets $\overline{S}_a^{(k,l)}$ and $\overline{S}_b^{(k,l)}$.

Let now

$$S^{(k,l)} = \bigcup_a S_a^{(k,l)} \quad \text{and} \quad \overline{S}^{(k,l)} = \bigcup_a \overline{S}_a^{(k,l)}$$

where the sums are taken over all F-admissible sets a of r-tuples. (Note that there is only a finite number of these sets.) By Lemma 4 we have

$$N\{n \leqslant x \mid n \in S^{(k,l)}\} \leqslant F_{k,l}(x) \leqslant N\{n \leqslant x \mid n \in \overline{S}^{(k,l)}\}.$$

From (13) we infer that

$$F_{k,l}(x) \approx N\{n \leqslant x \mid n \in S^{(k,l)}\} = \sum_a N\{n \leqslant x \mid n \in S_a^{(k,l)}\}.$$

As every summand of the last sum is asymptotically equal to $C_a x (\log\log x)^t (\log x)^{(1-h)/2h}$ (with a suitable positive constant C_a), we can restrict ourselves in this sum only to such F-admissible sets a which have the largest possible value of t, i.e. which contain the largest possible number of r-tuples. Let us call such sets *maximal F-admissible sets* and let M be the number of r-tuples in such a maximal set. Let moreover for any maximal F-admissible set a, $\beta(a)$ be the number of r-tuples $(a_1, \dots, a_r)$ contained in a, with the property $2a_i \equiv 0 \pmod{h_i}$ for $i = 1, 2, \dots, r$, or, which means the same, the number of orbits (X, X^{-1}) with $X^2 = E$ corresponding to r-tuples contained in a.

Then from (13) we obtain the following

THEOREM I. *Let K be a quadratic number field with the class-number $h \neq 1$ and let k and l are natural numbers with $(k, l) = 1$. Assume moreover that k is relatively prime to the discriminant of the field. Then*

$$F_{k,l}(x) \approx \varphi(k)^{-1} \prod_{\substack{p \mid k \\ p \in Q_0}} (1-p^{-1}) h^{-M} \mathcal{K}_{Q_0} \Big(\sum_a 2^{-\beta(a)} \Big) x (\log\log x)^M (\log x)^{(1-h)/2h},$$

where Q_0 is the set of all rational primes which are either products of two principal ideals or generate prime ideals in K, M is the number of r-tuples in a F-admissible maximal set, $\beta(a)$ is defined above, and the sum is taken over all maximal F-admissible sets a.

As a special case ($k = l = 1$) we obtain

THEOREM II. *Let K be a quadratic field with the class-number $h \neq 1$. Then*

$$F(x) \approx \Big(\mathcal{K}_{Q_0} \sum_a 2^{-\beta(a)} \Big) \frac{x (\log\log x)^M}{(\log x)^{(h-1)/2h}}.$$

Observe now that the number M depends on the structure of the class-group H only. To evaluate M the following result is useful:

LEMMA 14. *Let $H = C_{h_1} \times \dots \times C_{h_r}$ be a factorization of the class-group H into cyclic factors. Then*

$$\sum_{j=1}^{r} [\log h_j / \log 2] \leqslant M \leqslant [\log h / \log 2].$$

Proof. The number of possible sequences $\{\varepsilon_i\}_{i=1}^t$ (with $\varepsilon_i = 0, 1$) is 2^t and the number of r-tuples pairwise incongruent mod $\langle h_1, \dots, h_r \rangle$ is evidently $h_1 \dots h_r = h$, thus $2^t \leqslant h$. On the other hand if we put

$n_i = [\log h_i/\log 2]-1$ for $i = 1, 2, \ldots, r$ and define

$$a_k^{(j)} = \begin{cases} 2^{j-(n_1+\ldots+n_{k-1}+k-1)} & \text{for } n_1+\ldots+n_{k-1}+k-1 < j \\ & \leqslant n_1+\ldots+n_{k-1}+n_k+k, \\ 0 & \text{otherwise} \end{cases}$$

$$(k = 1, 2, \ldots, r;\ j = 1, 2, \ldots, n_1+n_2+\ldots+n_r+r),$$

then the obtained set $\{(a_1^{(j)}, \ldots, a_r^{(j)})\}$ is clearly F-admissible and has $n_1+\ldots+n_r+r$ elements, which proves the first part of the inequality.

COROLLARY. *If H is cyclic, then $M = [\log h/\log 2]$. In particular for the field $R(\sqrt{-5})$ considered by E. Fogels ([3]) we get*

$$F(x) \approx \mathscr{K}_{Q_0} x \log\log x (\log x)^{-1/4}.$$

5. Now we shall find the asymptotic evaluation of the functions $G_{k,l}(x)$. We assume throughout that k is relatively prime to the discriminant of the field K. By Lemma 5 and by the observation that for different sets V the corresponding sets $R_V^{(k,l)}$ (as defined on p. 8) are disjoint we get

$$G_{k,l}(x) = \sum_V N\{n \leqslant x \mid n \in R_V^{(k,l)}\} \tag{14}$$

where the sum is taken over all D-G-admissible systems V.

Let $V = (a^{(1)}, \ldots, a^{(s)}, \ldots, a^{(t)}; A_{1+s}, \ldots, A_t)$ (where $a^{(1)}, \ldots, a^{(s)}$ correspond to orbits $\mathcal{O}$ with $r(\mathcal{O}) = 2$) be a D-G-admissible system and let, as in section 2, Q_i be the set of all rational primes belonging to the orbit $\mathcal{O}_i$ corresponding to the r-tuple $a^{(i)}$, finally let $Q_{t+1}, \ldots, Q_v$ be sets of all rational primes belonging respectively to the orbits $\mathcal{O}_{t+1}, \ldots, \mathcal{O}_v$ distinct from $\mathcal{O}_1, \ldots, \mathcal{O}_t$ and (E, E). The condition of D-G-admissibility, we recall, runs as follows: for $i = 1+s, \ldots, t$, $\Omega_{Q_i}(D) \leqslant A_i$ and for $i = 1+t, \ldots, v$, $\Omega_{Q_i}(D) = 0$, and V is G-admissible.

From the definition of $R_V^{(k,l)}$ it follows that

$$N\{n \leqslant x \mid n \in R_V^{(k,l)}\} = N\{n \leqslant x \mid n \equiv l \pmod k,\ \Omega_{Q_i}(n) = A_i$$
$$(i = 1+s, \ldots, t),\ \Omega_{Q_i}(n) \geqslant 1\ (i = 1, \ldots, s),\ \Omega_{Q_i}(n) = 0\ (i = 1+t, \ldots, v)\}$$

and this is clearly equal to

$$\sum_{j=0}^{s} (-1)^j \sum_{1 \leqslant i_1 < \ldots < i_j \leqslant s} N\{n \leqslant x \mid n \equiv l \pmod k,\ \Omega_{Q_i}(n) = A_i \tag{15}$$
$$(i = 1+s, \ldots, t),\ \Omega_{Q_i}(n) = 0\ (i = 1+t, \ldots, v),\ \Omega_{Q_i}(n) = 0\ (i = i_1, \ldots, i_j)\}$$
$$= N\{n \leqslant x \mid n \equiv l \pmod k,\ \Omega_{Q_i}(n) = A_i\ (i = 1+s, \ldots, t),$$
$$\Omega_{Q_i}(n) = 0\ (i = 1+t, \ldots, v)\} + \sum_{j=1}^{s} (-1)^j \sum_{1 \leqslant i_1 < \ldots < i_j \leqslant s} N(i_1, \ldots, i_j).$$

By Lemma 13 the first summand is asymptotically equal to

$$\varphi^{-1}(k_1) \prod_{\substack{p \mid k_1 \\ p \in P_V}} (1-p^{-1}) K_{P_V} h^{-\mu} \prod_{i=1+s}^{t} (m_i!)^{-1} D^{-1} x (\log\log x)^{\mu} (\log x)^{\sigma-1} \tag{16}$$

where $k_1 = k/D$, $m_i = A_i - \Omega_{Q_i}(D)$ $(i = 1+s, \ldots, t)$, $\mu = m_1+\ldots+m_t$, $P_V = Q_0 \cup Q_1 \ldots \cup Q_s$, and σ is the density of P_V, which according to Lemma 9 is equal to $(h+1)/2h+s/2h$, thus $\sigma-1 = (1+s-h)/2h$.

By the same Lemma 13 we get that $N(i_1, \ldots, i_j)$ is either zero, or is $O\left(x(\log\log x)^a (\log x)^{(s-h)/2h}\right)$ with some fixed a, hence from (15) and (16) we get that $N\{n \leqslant x \mid n \in R_V^{(k,l)}\}$ is asymptotically equal to $C_V x (\log\log x)^{\mu} \times (\log x)^{(1+s-h)/2h}$ with a suitable positive constant C_V.

In view of this we may restrict the summation in the sum appearing in (14) to such systems V, for which s assumes the largest possible value. We shall now determine this maximal value in the case $D = 1$ and get some evaluation of it in the general case.

LEMMA 15. *If $D \notin G$ then there are no D-G-admissible systems at all. If $D = 1$ then there exist D-G-admissible systems having g r-tuples corresponding to orbits $\mathcal{O}$ with $r(\mathcal{O}) = 2$. (We recall that g is the number of even invariants of the class-group H.) On the other hand every G-admissible (and a fortiori every D-G-admissible) system can contain at most g such r-tuples.*

Proof. If $D \notin G$ then there are no integers n congruent to $l \pmod k$ in G and from Lemma 5 it follows that for every D-G-admissible set V the corresponding set $R_V^{(k,l)}$ is void, but every such set contains D *ex definitione*, and so there are no D-G-admissible sets at all.

Now we prove that every G-admissible system has at most g r-tuples corresponding to orbits $\mathcal{O}$ with $r(\mathcal{O}) = 2$, i.e. that $s \leqslant g$. Note first that if the system $(a^{(1)}, \ldots, a^{(s)}, \ldots, a^{(t)}; A_{1+s}, \ldots, A_t)$ is G-admissible, then the system $(a^{(1)}, \ldots, a^{(s)})$ is G-admissible too. Indeed, otherwise one could find $\{\varepsilon_1, \ldots, \varepsilon_s\} \neq \{\bar{\varepsilon}_1, \ldots, \bar{\varepsilon}_s\}$ with $0 \leqslant \varepsilon_i, \bar{\varepsilon}_i \leqslant 1$ such that

$$\sum_{i=1}^{s} \varepsilon_i a_k^{(i)} \equiv \sum_{i=1}^{s} \bar{\varepsilon}_i a_k^{(i)} \pmod{h_k} \qquad (k = 1, \ldots, r)$$

(where $\langle a_1^{(i)}, \ldots, a_r^{(i)} \rangle = a^{(i)}$), and if we define $\varepsilon_i = \bar{\varepsilon}_i = 0$ for $i = 1+s, \ldots, t$ then

$$\sum_{i=1}^{t} \varepsilon_i a_k^{(i)} \equiv \sum_{i=1}^{t} \bar{\varepsilon}_i a_k^{(i)} \pmod{h_k} \qquad (k = 1, \ldots, r)$$

in contradiction to G-admissibility of $(a^{(1)}, \ldots, a^{(t)}; A_{s+1}, \ldots, A_t)$.

Hence looking for the maximal value of s we may confine ourselves to the case $s = t$. Without restriction we may assume that $h_1, \ldots, h_g$

are even and $h_{g+1}, \dots, h_r$ are odd. Every orbit $\mathcal{O}$ with $r(\mathcal{O}) = 2$ has thus the form

$$(X_1^{\eta_1 h_1/2} \dots X_g^{\eta_g h_g/2}, X_1^{\eta_1 h_1/2} \dots X_g^{\eta_g h_g/2})$$

where $\eta_i = 0$ or 1. Let $V = (a^{(1)}, \dots, a^{(s)})$ be an G-admissible set of r-tuples corresponding to such orbits and let for $i = 1, 2, \dots, s$

$$a^{(i)} = \langle \eta_1^{(i)} h_1/2, \dots, \eta_g^{(i)} h_g/2, 0, 0, \dots, 0 \rangle$$

with $\eta_j^{(i)} = 0$ or 1. From the definition of G-admissibility it follows that all g-tuples of the form

$$\Big(\sum_{i=1}^{s} \varepsilon_i \eta_1^{(i)}, \dots, \sum_{i=1}^{s} \varepsilon_i \eta_g^{(i)}\Big)$$

with $\varepsilon_i = 0, 1$ must be incongruent (mod $\langle 2, 2, \dots, 2 \rangle$), or what means the same, the system of vectors

$$\langle (\eta_1^{(1)}, \dots, \eta_g^{(1)}), \dots, (\eta_1^{(s)}, \dots, \eta_g^{(s)}) \rangle$$

must be linearly independent in the g-dimensional vector space over GF(2). But clearly there are at most g linearly independent vectors in this space, and so $s \leqslant g$ results.

Now let $D = 1$. In this case D-G-admissibility and G-admissibility mean the same thing. Take $a^{(i)} = (\delta_1^{(i)} h_1/2, \dots, \delta_g^{(i)} h_g/2, 0, \dots, 0)$ where δ_j^i is the symbol of Kronecker, and observe that the system $(a^{(1)}, \dots, a^{(g)})$ is G-admissible. The lemma is thus proved.

Note that this lemma does not give any information about the largest possible value of s in the case $D \neq 1$, except the inequality $s \leqslant g$. It can be conjectured that in this case also it is equal to g, but we are unable to settle this. In any case let us define $S(D) = \max s$, where the maximum is taken over all D-G-admissible systems.

Now let $\mathscr{W}$ be the set of all D-G-admissible systems for which $s = S(D)$. With the notation used above, let N be the largest possible value of $m_1 + \dots + m_t$ for systems in the set $\mathscr{W}$. Let finally $\mathscr{W}_0$ be the set of all those systems in $\mathscr{W}$ for which N is attained. Now by (16) and the remarks before Lemma 15 we get the following

THEOREM III. *Let K be a quadratic number field with $h \neq 1, 2$, and let k, l are natural numbers with $(k, l) = D$. Assume moreover that k is relatively prime to the discriminant of the field. Then*

$$G_{k,l}(x) \approx \varphi^{-1}(k_1) D^{-1} h^{-N} \sum_{V \in \mathscr{W}_0} \Big\{ \prod_{\substack{p \mid k_1 \\ p \notin P_V}} (1 - p^{-1}) \mathscr{K}_{P_V} \prod_{i=1+S(D)}^{t} (m_i!)^{-1} \Big\} \times$$

$$\times x (\log\log x)^N (\log x)^{(1+S(D)-h)/2h}, \quad \text{if } D \in G,$$

$$G_{k,l}(x) = 0 \quad \text{if} \quad D \notin G,$$

where the summation is extended over all $V = (a^{(1)}, \dots, a^{(S(D))}, \dots, a^{(t)}; A_{1+S(D)}, \dots, A_t) \in \mathscr{W}_0$, $k_1 = k/D$, $m_i = A_i - \Omega_{Q_i}(D)$, Q_i is the set of all rational primes belonging to the orbit corresponding to $a^{(i)}$,

$$N = \max_{V \in \mathscr{W}} (m_{1+S(D)} + \dots + m_t) \quad \text{and} \quad P_V = Q_0 \cup Q_1 \cup \dots \cup Q_{S(D)}.$$

As a special case ($k = l = 1$) we get with the use of Lemma 15 the following

THEOREM IV. *Let K be a quadratic number field with $h \neq 1, 2$. Then*

$$G(x) \approx h^{-N} \sum_{V \in \mathscr{W}_0} \Big\{ \mathscr{K}_{P_V} \prod_{i=1+g}^{t} (A_i!)^{-1} \Big\} x (\log\log x)^N (\log x)^{(1+g-h)/2h}$$

where the summation is extended over all systems $V = (a^{(1)}, \dots, a^{(t)}; A_{1+g}, \dots, A_t) \in \mathscr{W}_0$, $N = \max_{V \in \mathscr{W}} (A_{1+g} + \dots + A_t)$ and $P_V = Q_0 \cup Q_1 \dots \cup Q_g$ (where Q_i is the set of all rational primes belonging to the orbit corresponding to $a^{(i)}$).

In the case of cyclic class-group we get the following corollaries:

COROLLARY 1. *If the quadratic number field K has a cyclic class-group and h is odd, then with a suitable, positive C*

$$G(x) \approx Cx (\log\log x)^{h-1} (\log x)^{(1-h)/2h}.$$

Indeed, the system $\{\langle 1 \rangle; h-1\}$ is G-admissible and for every G-admissible system $(a^{(1)}, \dots, a^{(t)}; A_{1+g}, \dots, A_t)$ one has $\prod_{i=1+g}^{t} (1 + A_i) \leqslant h$ whence $N = \max(A_{1+g} + \dots + A_t) \leqslant h-1$.

COROLLARY 2. *If the quadratic number field K has a cyclic class-group and h is even, then with a suitable, positive C*

$$G(x) \approx Cx (\log\log x)^{(h-2)/2} (\log x)^{(2-h)/2h}.$$

Indeed, the system $\{\langle h/2 \rangle, \langle 1 \rangle; (h-2)/2\}$ is G-admissible and the inequality $N \leqslant (h-2)/2$ follows as above.

References

[1] L. Carlitz, *A characterization of algebraic number fields with class number two*, Proc. Amer. Math. Soc. 11 (1960), pp. 391-392.

[2] H. Delange, *Sur la distribution des entiers ayant certaines propriétés*, Ann. Sci. de l'École Norm. Sup. 73 (1956), pp. 15-74.

[3] E. Fogels, *Zur Arithmetik quadratischer Zahlenkörper*, Univ. Riga, Wiss. Abh. kl. Math. Abt. 1 (1943), pp. 23-47.

[4] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, T. I. Jber. Dtsch. Math. Ver. 35 (1926), pp. 1-55.

[5] E. Landau, *Über Ideale und Primideale in Idealklassen*, Math. Zeitschr. 2 (1918), pp. 52-154.

[6] W. Narkiewicz, *On algebraic number fields with nonunique factorization*, Coll. Math. 12 (1964), pp. 59-68.

[7] — *On algebraic number fields with nonunique factorization II*, Colloq. Math. 15 (1966), pp. 49-58.

[8] — *On natural numbers having unique factorization in a quadratic number field*, Bull. Acad. Pol. Sci. 14 (1966), pp. 17-18.

MATHEMATICAL INSTITUTE OF THE WROCŁAW UNIVERSITY

Reçu par la Rédaction le 9. 9. 1965

ACTA ARITHMETICA
XII (1966)

The representation of primes by cubic polynomials

by

P. A. B. Pleasants (Cambridge)

1. Introduction. Let

$$\phi(x_1, \ldots, x_n) = \phi(\boldsymbol{x}) = C(\boldsymbol{x}) + Q(\boldsymbol{x}) + L(\boldsymbol{x}) + N \tag{1}$$

be a cubic polynomial with integral coefficients, where $C(\boldsymbol{x})$ denotes the cubic part of ϕ, $Q(\boldsymbol{x})$ the quadratic part, and so on. An obvious necessary condition for $\phi(\boldsymbol{x})$ to represent infinitely many primes is that for any given integer $m > 1$ there is some integer point $\boldsymbol{x}$ for which $\phi(\boldsymbol{x})$ is not divisible by m. The object of the present paper is to prove that in certain circumstances of reasonable generality, this necessary condition is also sufficient.

The investigation is based on the Hardy-Littlewood method, as modified by Davenport in his treatment of homogeneous cubic equations ([1] and [2]). Let $\mathscr{P}$ be any parallelepiped of suitable shape (that is, with bounding hyperplanes parallel to certain particular hyperplanes) in n dimensional space, such that $C(\boldsymbol{x})$ is positive in and on the boundary of $\mathscr{P}$. Let P be a large positive number. Then the number of integer points $\boldsymbol{x}$ in the expanded parallelepiped $P\mathscr{P}$ is asymptotic to VP^n, where V is the volume of $\mathscr{P}$, and the values of $\phi(\boldsymbol{x})$ at these points lie between fixed positive multiples of P^3. Let $\mathscr{M}(P)$ denote the number of these integer points for which the value of $\phi(\boldsymbol{x})$ is a prime. It is reasonable to expect that $\mathscr{M}(P)$ should be approximately proportional to $VP^n/\log P^3$ for large P, subject to the above necessary condition.

In the present paper we shall prove, subject to a further condition, that

$$\mathscr{M}(P) \sim \frac{VP^n}{\log P^3}\mathfrak{S} \quad \text{as} \quad P \to \infty, \tag{2}$$

where $\mathfrak{S}$ is a positive constant (the 'singular series' for the problem) depending only on $\phi(\boldsymbol{x})$. Following Davenport and Lewis [4] we define the invariant $h = h(C)$ to be the least positive integer for which $C(\boldsymbol{x})$