COMPOSITIO MATHEMATICA

J. P. M. DE KROON

The asymptotic behaviour of additive functions in algebraic number theory

Compositio Mathematica, tome 17 (1965-1966), p. 207-261

<http://www.numdam.org/item?id=CM_1965-1966__17__207_0>

The asymptotic behaviour of additive functions in algebraic number theory

by

J. P. M. de Kroon

CHAPTER 1

Introduction

§ 1. The problem

The aim of this paper is to prove some generalizations of a theorem of Erdös and Kac concerning the behaviour of an additive numbertheoretic function on the natural numbers [7].

The generalizations which we shall establish concern:

1. the set of the principal integral ideals of an arbitrary algebraic numberfield,
2. some sets of algebraic integers contained in an arbitrary but fixed algebraic numberfield, and
3. the ring of integral elements contained in an algebraic function-field.

We state that we shall formulate the problem in a rather general way, but only for the case where sets of algebraic integers are considered.

It may be noted that the formulation of the two other cases takes almost the same form.

Before formulating the problem in question, it is useful to make some preliminary remarks with regard to certain definitions and notations in order to make it possible to give a short and comprehensible formulation of the problem.

Let Q be the field of the rational numbers and Z the ring of the rational integers.

Let k and K be algebraic numberfields over Q such that $Q \subset k \subset K$.

Let R be the ring of integers of the field K and T the ring of integers of k.

Let $I(R)$ and $I(T)$ be the sets of ideals of R and T respectively.

Ideals of $I(R)$ are denoted by Gothic letters such as $\mathfrak{a}$, $\mathfrak{b}$ etc., accordingly prime-ideals of $I(R)$ are denoted by $\mathfrak{p}$ and $\mathfrak{q}$.

Prime-ideals of $I(T)$ are denoted by $\bar{\mathfrak{p}}$ and we assume that $\mathfrak{p} \in I(R)$ is a prime-ideal that lies above $\bar{\mathfrak{p}} \in I(T)$.

Further, let S be a function defined on T such that, for $t \in T$, $S(t) \in R$; we write: $S : T \to R$.

Let $\pi_{\mathfrak{p}}$ be the canonical operator $\pi_{\mathfrak{p}} : R \to R_{\mathfrak{p}} = R/\mathfrak{p}$ and similarly $\pi_{\bar{\mathfrak{p}}}$ the canonical operator $\pi_{\bar{\mathfrak{p}}} : T \to T_{\bar{\mathfrak{p}}} = T/\bar{\mathfrak{p}}$.

Assuming now that $S(t+v) \equiv S(t) \bmod \mathfrak{p}$, if $v \in \bar{\mathfrak{p}}$ where $\mathfrak{p}$ lies above $\bar{\mathfrak{p}}$, $S_{\mathfrak{p}}$ can be uniquely defined by $S_{\mathfrak{p}} \circ \pi_{\bar{\mathfrak{p}}} = \pi_{\mathfrak{p}} \circ S$, (Fig. 1).

$$\begin{tikzcd} T \arrow[r, "S"] \arrow[d, "\pi_{\bar{\mathfrak{p}}}"'] & R \arrow[d, "\pi_{\mathfrak{p}}"] \\ T_{\bar{\mathfrak{p}}} \arrow[r, "S_{\mathfrak{p}}"] & R_{\mathfrak{p}} \end{tikzcd}$$

Fig. 1

Let $\nu_{\mathfrak{p}}$ be the number of $t \in T_{\bar{\mathfrak{p}}}$ with $S_{\mathfrak{p}}(t) = 0$; notation: $\nu_{\mathfrak{p}} = \# \{t \in T_{\bar{\mathfrak{p}}} \mid S_{\mathfrak{p}}(t) = 0\}$.

$$\text{Analogously} \begin{cases} \nu_{\mathfrak{p}_1\mathfrak{p}_2} = \# \{t \in T_{\bar{\mathfrak{p}}} \mid S_{\mathfrak{p}_1}(t) = 0 \text{ and } S_{\mathfrak{p}_2}(t) = 0\} \text{ if} \\ \qquad\qquad \bar{\mathfrak{p}}_1 = \bar{\mathfrak{p}}_2 = \bar{\mathfrak{p}} \text{ and } \mathfrak{p}_1 \neq \mathfrak{p}_2, \\ \nu_{\mathfrak{p}_1\mathfrak{p}_2} = 0 \text{ if } \bar{\mathfrak{p}}_1 \neq \bar{\mathfrak{p}}_2 \text{ or } \mathfrak{p}_1 = \mathfrak{p}_2. \end{cases}$$

Norm. Let $\mathcal{N}_{K_1|K_2}$ be the norm defined on the ideals and integers of the numberfield K_1, relative to the numberfield K_2.

We put, by definition: $N = |\mathcal{N}_{K/\boldsymbol{Q}}|$ and $\bar{N} = |\mathcal{N}_{k|\boldsymbol{Q}}|$.

Let (r) be the principal ideal generated by r, $r \in R$. We have: $Nr = N(r)$; similarly $\bar{N}t = \bar{N}(t)$.

Let the n conjugates of an integer $r \in R$, relative to $\boldsymbol{Q}$, be denoted by $r^{(1)}, r^{(2)}, r^{(3)}, \ldots, r^{(n)}$, n being the degree of K over $\boldsymbol{Q}$.

Height. We define the height of an algebraic integer, $r \in R$, by:

$$||r|| = \max_i |r^{(i)}|.$$

Now, let $\boldsymbol{R}$ be the real field and $\mathfrak{f} : I(R) \to \boldsymbol{R}$ an additive number-theoretic function with the following properties:

$$\mathfrak{f}(\mathfrak{a} \cdot \mathfrak{b}) = \mathfrak{f}(\mathfrak{a}) + \mathfrak{f}(\mathfrak{b}) \text{ if } (\mathfrak{a}, \mathfrak{b}) = (1),$$
$$\mathfrak{f}(\mathfrak{p}^k) = \mathfrak{f}(\mathfrak{p}) \text{ for } k \in \boldsymbol{Z} \text{ with } k \geqq 1,$$
$$|\mathfrak{f}(\mathfrak{p})| \leqq 1.$$

The function $\mathfrak{f}$ is defined on R by $\mathfrak{f}(r) = \mathfrak{f}((r))$, if $r \in R$ and (r) is the principal ideal generated by r.

Further let $A : \boldsymbol{R} \to \boldsymbol{R}$ and $B : \boldsymbol{R} \to \boldsymbol{R}$ be defined by

$$A(x) = \sum_{\mathfrak{p};\, \bar{N}\mathfrak{p} \leq x} \nu_{\mathfrak{p}} \frac{\mathfrak{f}(\mathfrak{p})}{\bar{N}\mathfrak{p}},$$

$$B(x) = \left\{ \sum_{\mathfrak{p};\, \bar{N}\mathfrak{p} \leq x} \nu_{\mathfrak{p}} \frac{\mathfrak{f}^2(\mathfrak{p})}{\bar{N}\mathfrak{p}} + \sum_{\substack{\mathfrak{p};\, \bar{N}\mathfrak{p} \leq x \\ \mathfrak{q};\, \bar{N}\mathfrak{q} \leq x}} \nu_{\mathfrak{p}\mathfrak{q}} \frac{\mathfrak{f}(\mathfrak{p})\mathfrak{f}(\mathfrak{q})}{\bar{N}\mathfrak{p}} \right\}^{\frac{1}{2}}$$

respectively.

Now we wish to prove theorems of the following type:

If $\quad H(x) = \# \{t \in T \mid ||t|| \leqq x^{1/n}\}$ *and*
$G(x, u) = \# \{t \in T \mid ||t|| \leqq x^{1/n}$ *and* $\mathfrak{f}(S(t)) \leqq A(x) + uB(x)\}$,
and if $B(x) \to \infty$ *as* $x \to \infty$,

then

$$\frac{G(x, u)}{H(x)} = \Phi(u) + \varepsilon(x, u),$$

where $\Phi(u) = (2\pi)^{-\frac{1}{2}} \int_{-\infty}^{u} \exp. (-\frac{1}{2}t^2)dt$
and $|\varepsilon(x, u)| \leqq \delta(x)$ *uniformly in* $u \in \boldsymbol{R}$ *with* $\lim_{x \to \infty} \delta(x) = 0$.

In chapters 3 and 4 we shall prove such theorems. In chapter 2 we shall prove an analogous theorem, applied to the set $\mathfrak{S}_0$ of principal ideals $\in I(R)$, and in chapter 5 we shall deal with the set $\boldsymbol{F}_q[X]$ where $\boldsymbol{F}_q[X]$ is the ring of integral elements of the algebraic functionfield $\boldsymbol{F}_q(X)$ over the finite field of q elements.

For the sake of completeness we state here that in the last two mentioned cases S will be the identity and "height" is replaced by "norm" so that, instead of the condition $||t|| \leqq x^{1/n}$, we shall have $N\mathfrak{a} \leqq x$.

§ 2. Results

In subjoined table 1 we summarize the most important cases for which the problem formulated in § 1, has been solved in the litterature, while in table 2 we present the cases for which we are going to solve the problem in question.

In tables 1 and 2, Y stands for a set of integral elements and X is a subset of Y; S is a function: $X \to Y$. The symbols $o(.)$

TABLE 1: *Known Results*

Author	S	X	Y	$\mathfrak{f}$	$\delta(x)$
Erdös and Kac [7]	Identity	Z	Z	$\mathfrak{f}(p^k) = \mathfrak{f}(p)$ $\lvert\mathfrak{f}(p)\rvert \leqq 1$	$o(1)$
Kubilyus [9]	Identity	Z	Z	$\mathfrak{f}(p^k) = \mathfrak{f}(p) = 1$	$\mathcal{O}\left(\frac{\log B(x)}{B(x)}\right)$
Rényi and Turán [14]	Identity	Z	Z	$\mathfrak{f}(p^k) = k$ resp. $\mathfrak{f}(p^k) = \mathfrak{f}(p) = 1$	$\mathcal{O}\left(\frac{1}{B(x)}\right)$
Halberstam [8]	$S(t) = \sum_{j=1}^{m} a_j t^j$ $a_j \in Z$ $t \in Z$	Z	Z	$\mathfrak{f}(p^k) = \mathfrak{f}(p)$ $= o(B(\lvert p\rvert))$	$o(1)$
Rieger [15]	Identity	R	R	$\mathfrak{f}(\mathfrak{p}^k) = \mathfrak{f}(\mathfrak{p}) = 1$	$\mathcal{O}\left(\left(\frac{\log B(x)}{B(x)}\right)^{\frac12}\right)$

TABLE 2: *Results obtained in this paper*

Chapter	S	X	Y	$\mathfrak{f}$	$\delta(x)$
2	Identity	$\mathfrak{S}_0$	$\mathfrak{S}_0$	$\mathfrak{f}(\mathfrak{p}^k) = \mathfrak{f}(\mathfrak{p})$ $\lvert\mathfrak{f}(\mathfrak{p})\rvert \leqq 1$	$\mathcal{O}\left(\frac{1}{B^{\frac12}(x)}\right)$
3	$S(\xi) = \sum_{j=1}^{m} \alpha_j \xi^j$ $\alpha_j,\ \xi \in R$	R	R	$\mathfrak{f}(\mathfrak{p}^k) = \mathfrak{f}(\mathfrak{p})$ $\lvert\mathfrak{f}(\mathfrak{p})\rvert \leqq 1$	$\mathcal{O}\left(\frac{1}{B^{\frac12}(x)}\right)$
4	$S(r) = \sum_{j=1}^{m} \alpha_j r^j$ $r \in Z,\ \alpha_j \in R$	Z	R	$\mathfrak{f}(\mathfrak{p}^k) = \mathfrak{f}(\mathfrak{p})$ $\lvert\mathfrak{f}(\mathfrak{p})\rvert \leqq 1$	$\mathcal{O}\left(\frac{1}{B^{\frac12}(x)}\right)$
5	Identity	$F_q[X]$	$F_q[X]$	$\mathfrak{f}(\mathfrak{p}^k) = \mathfrak{f}(\mathfrak{p})$ $\lvert\mathfrak{f}(\mathfrak{p})\rvert \leqq 1$	$\mathcal{O}\left(\frac{\log^{\frac12} B(x)}{B(x)}\right)$

and $\mathcal{O}(.)$ are used for $x \to \infty$. The other symbols that occur in tables 1 and 2 have the same meaning as in § 1.

It should be noted that each time $B(x)$ occurs in table 1, we have: $B^2(x) = \text{loglog}\, x + \mathcal{O}(1)$.

We also make the following comments:

1. Our method of proof is analogous to that of Erdös and Kac [7].

2. Rényi and Turán [14] state that the result obtained by them, with regard to $\delta(x)$, is best possible in the sense that $\mathcal{O}(1/B(x))$ cannot be replaced by $o(1/B(x))$.
   Delange [6] gives still more information about the behaviour of $\delta(x)$ as x tends to infinity.
3. Our results are more general than those of Rieger [15], who was the first to consider the problem in question for the case of an algebraic numberfield.

The results published in this paper were achieved under the inspiring guidance of Professor Van der Blij. For this and for his stimulating criticism, I wish to express my deepest gratitude.

§ 3. Preliminaries

§ 3.1. SOME BASIC RESULTS FROM ALGEBRAIC NUMBER THEORY

Let K be an algebraic numberfield of degree n over $\boldsymbol{Q}$ and, as before, R the ring of integers of K.

It is well-known that the class-number h of the ring R is finite. From now on algebraic integers, and thus elements of R, will be denoted by Greek letters. Henceforth $x \in \boldsymbol{R}$ and $x > 0$.

We shall make use of the symbols $\mathcal{O}(.)$ and $o(.)$ of Landau and, unless otherwise stated, we shall use them for $x \to \infty$; the constants in these symbols are supposed to depend only on the field K. Now we define

$$H(x) = \#\{\mathfrak{a} \in I(R) |\, N\mathfrak{a} \leqq x\} = \sum_{N\mathfrak{a} \leqq x} 1. \tag{3.1}$$

For every class $\mathfrak{S}$ of ideals, we define

$$H(x; \mathfrak{S}) = \#\{\mathfrak{a} \in \mathfrak{S} | N\mathfrak{a} \leqq x\} = \sum_{\substack{\mathfrak{a} \in \mathfrak{S} \\ N\mathfrak{a} \leqq x}} 1. \tag{3.2}$$

Further, we define for a fixed $\gamma \in R$

$$\mathscr{A}(\mathfrak{a}; x) = \#\{\xi \in R |\; ||\xi|| \leqq x^{1/n} \text{ and } \xi \equiv \gamma \bmod \mathfrak{a}\}. \tag{3.3}$$

We have the following well-known formulae, (see [10]).

$$H(x) = \lambda h x + \mathcal{O}(x^{1-2/(n+1)}), \tag{3.4}$$

$$H(x; \mathfrak{S}) = \lambda x + \mathcal{O}(x^{1-2/(n+1)}). \tag{3.5}$$

In (3.4) and (3.5), λ and h depend only on K. We have already defined h and we note that λ is the residue of $\zeta(s; \mathfrak{S}) = \sum_{\mathfrak{a} \in \mathfrak{S}} 1/N\mathfrak{a}^s$ at $s = 1$.

Further, (see Rieger [16]),

$$\mathscr{A}(\mathfrak{a}; x) = c\,\frac{x}{N\mathfrak{a}} + \mathcal{O}\left(1 + \left(\frac{x}{N\mathfrak{a}}\right)^{1-1/n}\right), \tag{3.6}$$

where c is a constant, dependent only on K.

Now Landau [11] proved the following formula:

$$\sum_{N\mathfrak{p}\leqq x} \frac{\log N\mathfrak{p}}{N\mathfrak{p}} = \log x + \mathcal{O}(1). \tag{3.7}$$

From this we prove

$$\sum_{N\mathfrak{p}\leqq x} \frac{1}{N\mathfrak{p}} = \operatorname{loglog} x + C + \mathcal{O}\left(\frac{1}{\log x}\right), \tag{3.8}$$

where C is a constant.

Proof of (3.8).

Putting $C(x) = \sum_{N\mathfrak{p}\leqq x} (\log N\mathfrak{p})/N\mathfrak{p}$, we have

$$\sum_{N\mathfrak{p}\leqq x} \frac{1}{N\mathfrak{p}} = \sum_{N\mathfrak{p}\leqq x} \frac{\log N\mathfrak{p}}{N\mathfrak{p}} \cdot \frac{1}{\log N\mathfrak{p}}.$$

Hence

$$\sum_{N\mathfrak{p}\leqq x} \frac{1}{N\mathfrak{p}} = \frac{C(x)}{\log x} + \int_2^x \frac{C(t)}{t(\log t)^2}\,dt.$$

Now, defining $\tau(x) = C(x) - \log x$, we find

$$\begin{aligned}\sum_{N\mathfrak{p}\leqq x} \frac{1}{N\mathfrak{p}} &= 1 + \mathcal{O}\left(\frac{1}{\log x}\right) + \int_2^x \frac{dt}{t(\log t)} + \int_2^x \frac{\tau(t)dt}{t(\log t)^2}\,dt \\ &= 1 + \operatorname{loglog} x - \operatorname{loglog} 2 + \int_2^x \frac{\tau(t)dt}{t(\log t)^2} + \mathcal{O}\left(\frac{1}{\log x}\right).\end{aligned}$$

Since, clearly

$$\int_x^\infty \frac{\tau(t)dt}{t(\log t)^2} = \mathcal{O}\left(\frac{1}{\log x}\right),$$

we arrive at the required result if we put

$$C = 1 - \operatorname{loglog} 2 + \int_2^\infty \frac{\tau(t)}{t(\log t)^2}\,dt.$$

Now, starting from $\sum_{N\mathfrak{p}\leqq x} 1/N\mathfrak{p}$, we have:

$$\sum_{N\mathfrak{p}\leqq x} \frac{1}{N\mathfrak{p}} = -\sum_{N\mathfrak{p}\leqq x} \log\left(1 - \frac{1}{N\mathfrak{p}}\right) - \sum_{\mathfrak{p}} \sum_{j=2}^\infty \frac{1}{jN\mathfrak{p}^j} + \sum_{N\mathfrak{p}>x} \sum_{j=2}^\infty \frac{1}{jN\mathfrak{p}^j}.$$

Obviously

$$\sum_{N\mathfrak{p}>x}\sum_{j=2}^{\infty}\frac{1}{jN\mathfrak{p}^j}<\sum_{N\mathfrak{p}>x}\sum_{j=2}^{\infty}\frac{1}{(N\mathfrak{p})^j}<2\sum_{N\mathfrak{p}>x}\frac{1}{N\mathfrak{p}^2}=\mathcal{O}\left(\frac{1}{x}\right).$$

Applying (3.8), it follows that

$$\sum_{N\mathfrak{p}\leqq x}\log\left(1-\frac{1}{N\mathfrak{p}}\right)=-\log\log x+C'+\mathcal{O}\left(\frac{1}{\log x}\right),$$

where C' is a real constant, and therefore

$$\prod_{N\mathfrak{p}\leqq x}\left(1-\frac{1}{N\mathfrak{p}}\right)=\frac{\kappa}{\log x}\left(1+\mathcal{O}\left(\frac{1}{\log x}\right)\right), \tag{3.9}$$

where κ is a positive constant.

§ 3.2 PROBABILITY THEORY

Since, in some of the following paragraphs, we deal with notations and arguments from probability theory, we shall now briefly summarize some definitions and properties of this theory as far as we need them. Consider the set $I(R)$ of integral ideals in K which is taken here as sample-space.

On this space we consider the σ-algebra of all subsets E; on this σ-algebra is defined a completely additive, non-negative set-function P, satisfying the condition $P(I(R)) = 1$.

In this case P will be defined by

$$P(E)=\lim_{x\to\infty}\frac{\#\{\mathfrak{a}\in E\mid N\mathfrak{a}\leqq x\}}{\#\{\mathfrak{a}\in I(R)\mid N\mathfrak{a}\leqq x\}},$$

if the limit exists and $E\subset I(R)$.

Consequently, we could say that $P(E)$ is the density of the integral ideals belonging to E.

We shall also denote $P(E)$ as: the probability that $\mathfrak{a}\in E$. Analogously we could consider the ring R of the algebraic integers as the sample-space.

Then we should define the set-function P by

$$P(E)=\lim_{x\to\infty}\frac{\#\{\xi\in E\mid \|\xi\|\leqq x\}}{\#\{\xi\in R\mid \|\xi\|\leqq x\}},$$

if the limit exists and $E\subset R$.

In each chapter we shall stipulate how the set-function P is defined in that chapter.

For simplicity, we now cease considering the various cases and continue the considerations of this paragraph in terms of the sample-space $I(R)$ only.

We introduce the conditional probability by

$$P(E_1|E_2) = \lim_{x\to\infty} \frac{\#\{\mathfrak{a} \in E_1 \cap E_2 | N\mathfrak{a} \leqq x\}}{\#\{\mathfrak{a} \in E_2 | N\mathfrak{a} \leqq x\}},$$

if the limit exists and $E_1 \subset I(R)$ and $E_2 \subset I(R)$. Obviously, if $P(E_1|E_2)$ and $P(E_2)$ exist and if, moreover, $P(E_2) > 0$, we have

$$P(E_1|E_2) = \frac{P(E_1 \cap E_2)}{P(E_2)}.$$

A real-valued function defined on the sample space is called a stochastic variable or a random variable. For the sake of convenience we shall, for every stochastic variable ω and Borelset b, write

$$\{\omega(\mathfrak{a}) \in b\} \text{ instead of } \{\mathfrak{a} \in I(R)|\ \omega(\mathfrak{a}) \in b\},$$

which is defined as the set of those ideals, $\mathfrak{a} \in I(R)$, for which $\omega(\mathfrak{a}) \in b$; analogously if ω_1 and ω_2 are random variables and b_1 and b_2 Borelsets:

$$\{\omega_1(\mathfrak{a}) \in b_1 \text{ and } \omega_2(\mathfrak{a}) \in b_2\} = \{\mathfrak{a} \in I(R) | \omega_1(\mathfrak{a}) \in b_1 \text{ and }$$
$$\omega_2(\mathfrak{a}) \in b_2\} = \{\mathfrak{a} \in I(R) | \omega_1(\mathfrak{a}) \in b_1\} \cap \{\mathfrak{a} \in I(R) | \omega_2(\mathfrak{a}) \in b_2\}.$$

Two stochastic variables, ω_1 and ω_2, are said to be independent if the following multiplicative relation is satisfied for every pair of Borelsets b_1 and b_2.

$$P(\omega_1(\mathfrak{a}) \in b_1 \text{ and } \omega_2(\mathfrak{a}) \in b_2) = P(\omega_1(\mathfrak{a}) \in b_1) \cdot P(\omega_2(\mathfrak{a}) \in b_2).$$

In direct generalization, we shall say that the l random variables $\omega_1, \omega_2, \ldots, \omega_l$, are independent random variables if the multiplicative relation

$$P(\omega_1(\mathfrak{a}) \in b_1, \ldots, \omega_l(\mathfrak{a}) \in b_l) = \prod_{j=1}^{l} P(\omega_j(\mathfrak{a}) \in b_j)$$

is satisfied for any Borelsets $b_1, b_2, \ldots, b_l$. If, in a sequence $\omega_1, \omega_2, \ldots$, any set $\omega_1, \ldots, \omega_l$ of l random variables are independent, we shall briefly say that $\omega_1, \omega_2, \ldots$ form a sequence of independent variables.

If ω is a stochastic variable, then clearly for every $u \in \mathbf{R}$ it makes sense to use the expression $P(\omega(\mathfrak{a}) \leqq u)$. The function $F : \mathbf{R} \to \mathbf{R}$, defined by

$$F(u) = P(\omega(\mathfrak{a}) \leqq u)$$

is called the distribution-function of ω.

$\mathscr{E}(\omega^k) = \int_{-\infty}^{\infty} u^k dF(u)$ is called the kth moment of ω, $(k \in \boldsymbol{Z},\ k > 0)$.

$\mathscr{E}(\omega)$ is called the mean and $\mathscr{E}(\omega^2) - (\mathscr{E}(\omega))^2$ the variance of ω, which is denoted by var. (ω). The variance is sometimes denoted by σ^2; σ is then called the standard deviation.

An important theorem that we shall use is the following so-called "Central Limit Theorem", due to Liapounoff, (see Cramèr [4]).

($\mathscr{L}$) Central limit theorem of Liapounoff
(referred to as ($\mathscr{L}$)).

Let $\omega_1, \omega_2, \ldots$ be independent random variables and let μ_j and σ_j denote the mean and the standard deviation of ω_j.

Suppose that the third absolute moment, α_j, of ω_j about its mean, defined by

$$\alpha_j^3 = \mathscr{E}(|\omega_j - \mu_j|^3),$$

is finite for every j and put

$$C(r) = [\sum_{j=1}^{r} \alpha_j^3]^{\frac{1}{3}},$$

$$B(r) = [\sum_{j=1}^{r} \sigma_j^2]^{\frac{1}{2}},$$

$$A(r) = \sum_{j=1}^{r} \mu_j,$$

$$\Omega(r) = \sum_{j=1}^{r} \omega_j.$$

If

$$\lim_{r\to\infty} \frac{C(r)}{B(r)} = 0,$$

then, uniformly in u, $u \in \boldsymbol{R}$,

$$\lim_{r\to\infty} P\left(\frac{\Omega(r)(\mathfrak{a}) - A(r)}{B(r)} \leqq u\right) = \Phi(u),$$

where, as in § 1,

$$\Phi(u) = (2\pi)^{-\frac{1}{2}} \int_{-\infty}^{u} \exp.\,(-\tfrac{1}{2}t^2)dt.$$

As Uspensky [17] states, this result can be improved to the following:

($\mathscr{L}'$)

Let the same assumptions be made as in theorem ($\mathscr{L}$), then, if r is so large that

$$\tau_r = \left[\frac{C(r)}{B(r)}\right]^3 < \tfrac{1}{20},$$

$$P\left(\frac{\Omega(r)(\mathfrak{a})-A(r)}{B(r)} \leqq u\right) = \Phi(u)+\Delta(r),$$

with

$$|\Delta(r)| < \tfrac{8}{5}\tau_r\left[\left(\log\frac{1}{3\tau_r}\right)^{\frac{1}{2}}+1.1\right]+\tau_r^2\log\frac{1}{3\tau_r}+\tfrac{5}{3}\tau_r^{\frac{2}{3}}\exp.\left(\frac{-\tau_r^{-\frac{2}{3}}}{5}\right).$$

CHAPTER 2

The set $\mathfrak{S}_0$ of principal ideals

§ 4. Theorem 1

Throughout Chapter 2, $I(R)$ will be the sample-space and the set-function P will be defined by

$$P(E) = \lim_{x\to\infty}\frac{\#\{\mathfrak{a}\in E \mid N\mathfrak{a}\leqq x\}}{\#\{\mathfrak{a}\in I(R)\mid N\mathfrak{a}\leqq x\}}, \tag{4.1}$$

if the limit exists and $E\subset I(R)$.

The conditional probability will be defined by

$$P(E_1 \mid E_2) = \lim_{x\to\infty}\frac{\#\{\mathfrak{a}\in E_1\cap E_2 \mid N\mathfrak{a}\leqq x\}}{\#\{\mathfrak{a}\in E_2\mid N\mathfrak{a}\leqq x\}}, \tag{4.2}$$

if the limit exists and $E_1\subset I(R)$ and $E_2\subset I(R)$.

We recall the following definitions:

1. K is an algebraic numberfield of degree n over the rational numberfield $\boldsymbol{Q}$.
2. R is the ring of integers of K; $\boldsymbol{Z}$ is the ring of rational integers.
3. $I(R)$ is the set of ideals of R; $\mathfrak{S}_0$ is the set of the principal ideals of R.
4. N is the absolute value of the norm defined on the ideals and integers of R.

Let $\mathfrak{f}: I(R)\to \boldsymbol{R}$ be an additive number-theoretic function as defined in § 1. Hence $\mathfrak{f}$ satisfies the following conditions:

$$(4.3)\quad \begin{cases} \mathfrak{f}(\mathfrak{a}\cdot\mathfrak{b}) = \mathfrak{f}(\mathfrak{a})+\mathfrak{f}(\mathfrak{b}) \text{ if } (\mathfrak{a},\mathfrak{b}) = (1), \\ \mathfrak{f}(\mathfrak{p}^k) = \mathfrak{f}(\mathfrak{p}) \text{ for } k \in \boldsymbol{Z} \text{ with } k \geqq 1 \text{ and } \mathfrak{p} \text{ prime-ideal}, \\ |\mathfrak{f}(\mathfrak{p})| \leqq 1, \ (\mathfrak{p} \text{ prime-ideal}). \end{cases}$$

Now, for every prime-ideal $\mathfrak{p}$, we define the random variable $\rho_{\mathfrak{p}}$ by

$$(4.4)\quad \begin{cases} \rho_{\mathfrak{p}}(\mathfrak{a}) = \mathfrak{f}(\mathfrak{p}) \text{ if } \mathfrak{a} \equiv 0 \bmod \mathfrak{p}, \\ \rho_{\mathfrak{p}}(\mathfrak{a}) = 0 \text{ in all other cases.} \end{cases}$$

Obviously

$$(4.5)\quad \mathfrak{f}(\mathfrak{a}) = \sum_{\mathfrak{p}} \rho_{\mathfrak{p}}(\mathfrak{a}), \quad \mathfrak{a} \in I(R).$$

For every $x \in \boldsymbol{R}$ we introduce the function $\mathfrak{f}_x$, defined by

$$(4.6)\quad \mathfrak{f}_x(\mathfrak{a}) = \sum_{N\mathfrak{p} \leqq x} \rho_{\mathfrak{p}}(\mathfrak{a}), \quad \mathfrak{a} \in I(R).$$

According to the definitions in the introduction (§ 1), we put

$$(4.7)\quad A(x) = \sum_{N\mathfrak{p} \leqq x} \frac{\mathfrak{f}(\mathfrak{p})}{N\mathfrak{p}},$$

and

$$(4.8)\quad B(x) = \left[\sum_{N\mathfrak{p} \leqq x} \frac{\mathfrak{f}^2(\mathfrak{p})}{N\mathfrak{p}}\right]^{\frac{1}{2}}.$$

As before, $\Phi : \boldsymbol{R} \to \boldsymbol{R}$ is defined by

$$(4.9)\quad \Phi(u) = (2\pi)^{-\frac{1}{2}} \int_{-\infty}^{u} \exp.\,(-\tfrac{1}{2}t^2)dt.$$

We shall prove the following theorem:

THEOREM 1.

Let $\mathfrak{f}$, $\mathfrak{f}_x$, A, B *and* Φ *be defined by* (4.5), (4.6), (4.7), (4.8) *and* (4.9) *respectively.*

If

$$\lim_{x\to\infty} B(x) = \infty,$$

then

$$(4.10)\quad \lim_{x\to\infty} P(\mathfrak{f}_x(\mathfrak{a}) \leqq A(x)+uB(x) \mid \mathfrak{a} \in \mathfrak{S}_0) = \Phi(u)$$

uniformly in $u \in \boldsymbol{R}$, *and, in fact,*

$$(4.11)\quad P(\mathfrak{f}_x(\mathfrak{a}) \leqq A(x)+uB(x) \mid \mathfrak{a} \in \mathfrak{S}_0) = \Phi(u)+\mathcal{O}\left(\frac{(\log B(x))^{\frac{1}{2}}}{B(x)}\right)$$

uniformly in $u \in \boldsymbol{R}$.

Proof of theorem 1.

$$P(\rho_{\mathfrak{p}}(\mathfrak{a}) = \mathfrak{f}(\mathfrak{p}) \mid \mathfrak{a} \in \mathfrak{S}_0) = \lim_{x\to\infty} \frac{\#\{\mathfrak{a} \in \mathfrak{S}_0 \mid \mathfrak{a} \equiv 0 \bmod \mathfrak{p} \text{ and } N\mathfrak{a} \leqq x\}}{\#\{\mathfrak{a} \in \mathfrak{S}_0 \mid N\mathfrak{a} \leqq x\}}.$$

Now, $\mathfrak{a} \equiv 0 \bmod \mathfrak{p}$, implies $\mathfrak{a} = \mathfrak{p}\mathfrak{b}$.

The condition $\mathfrak{a} \in \mathfrak{S}_0$ is then equivalent to $\mathfrak{b} \in \mathfrak{S}$, where $\mathfrak{S}$ is one of the h classes of ideals. $\mathfrak{S}$ is uniquely determined by $\mathfrak{p}$ and $\mathfrak{S}_0$. Further, $N\mathfrak{a} \leqq x$ implies $N\mathfrak{b} \leqq x/N\mathfrak{p}$, and hence

$$P(\rho_{\mathfrak{p}}(\mathfrak{a}) = \mathfrak{f}(\mathfrak{p}) \mid \mathfrak{a} \in \mathfrak{S}_0) = \lim_{x\to\infty} \frac{H(x/N\mathfrak{p}; \mathfrak{S})}{H(x; \mathfrak{S}_0)},$$

$H(y; \mathfrak{S})$ being defined by (3.2).

Applying formula (3.5), we find

$$P(\rho_{\mathfrak{p}}(\mathfrak{a}) = \mathfrak{f}(\mathfrak{p}) \mid \mathfrak{a} \in \mathfrak{S}_0) = \frac{1}{N\mathfrak{p}}. \tag{4.12}$$

Similarly, we can show that for every pair $\mathfrak{p}$, $\mathfrak{q}$ with $\mathfrak{p} \neq \mathfrak{q}$,

$$P(\rho_{\mathfrak{p}}(\mathfrak{a}) = \mathfrak{f}(\mathfrak{p}) \text{ and } \rho_{\mathfrak{q}}(\mathfrak{a}) = \mathfrak{f}(\mathfrak{q}) \mid \mathfrak{a} \in \mathfrak{S}_0) = \frac{1}{N\mathfrak{p}\mathfrak{q}}. \tag{4.13}$$

From this it follows almost immediately that, on $\mathfrak{S}_0$, $\rho_{\mathfrak{p}}$ and $\rho_{\mathfrak{q}}$ are independent random variables if $\mathfrak{p} \neq \mathfrak{q}$. Analogously, it can be seen that the $\rho_{\mathfrak{p}}$ form a sequence of independent random variables on $\mathfrak{S}_0$. We note that on $I(R)$ the $\rho_{\mathfrak{p}}$ also form a sequence of independent random variables, but we do not require this here.

If we denote the expectation of a random variable ω on the subset E of the sample-space, by $\mathscr{E}(\omega\backslash E)$, we have

$$\begin{cases} \mathscr{E}(\rho_{\mathfrak{p}}\backslash\mathfrak{S}_0) = \dfrac{\mathfrak{f}(\mathfrak{p})}{N\mathfrak{p}}, \\ \text{var. } (\rho_{\mathfrak{p}}\backslash\mathfrak{S}_0) = \mathscr{E}(\rho_{\mathfrak{p}}^2\backslash\mathfrak{S}_0) - (\mathscr{E}(\rho_{\mathfrak{p}}\backslash\mathfrak{S}_0))^2 = \dfrac{\mathfrak{f}^2(\mathfrak{p})}{N\mathfrak{p}} - \dfrac{\mathfrak{f}^2(\mathfrak{p})}{N\mathfrak{p}^2}, \\ \text{and} \\ \mathscr{E}(|\rho_{\mathfrak{p}} - \mathscr{E}\rho_{\mathfrak{p}}|^3\backslash\mathfrak{S}_0) = \left| \dfrac{\mathfrak{f}^3(\mathfrak{p})}{N\mathfrak{p}} - 3\dfrac{\mathfrak{f}^3(\mathfrak{p})}{N\mathfrak{p}^2} + 2\dfrac{\mathfrak{f}^3(\mathfrak{p})}{N\mathfrak{p}^3} \right|. \end{cases}$$

Hence

$$\begin{cases} \mathscr{E}(\mathfrak{f}_x\backslash\mathfrak{S}_0) = \displaystyle\sum_{N\mathfrak{p}\leqq x} \frac{\mathfrak{f}(\mathfrak{p})}{N\mathfrak{p}} = A(x), \\ \text{var. } (\mathfrak{f}_x\backslash\mathfrak{S}_0) = \displaystyle\sum_{N\mathfrak{p}\leqq x} \left\{ \frac{\mathfrak{f}^2(\mathfrak{p})}{N\mathfrak{p}} - \frac{\mathfrak{f}^2(\mathfrak{p})}{N\mathfrak{p}^2} \right\} = B^2(x) - \sum_{N\mathfrak{p}\leqq x} \frac{\mathfrak{f}^2(\mathfrak{p})}{N\mathfrak{p}^2}, \\ \displaystyle\sum_{N\mathfrak{p}\leqq x} \mathscr{E}(|\rho_{\mathfrak{p}} - \mathscr{E}\rho_{\mathfrak{p}}|^3\backslash\mathfrak{S}_0) = \sum_{N\mathfrak{p}\leqq x} \left| \frac{\mathfrak{f}^3(\mathfrak{p})}{N\mathfrak{p}} - 3\frac{\mathfrak{f}^3(\mathfrak{p})}{N\mathfrak{p}^2} + 2\frac{\mathfrak{f}^3(\mathfrak{p})}{N\mathfrak{p}^3} \right|. \end{cases}$$

Now, since $B(x) \to \infty$ as $x \to \infty$ and $\sum |f(\mathfrak{p})|/N\mathfrak{p}^2$ is convergent, it can quite easily be verified that the conditions of the central limit theorem ($\mathscr{L}'$) are satisfied.

Putting

$$B_1^2(x) = B^2(x) - \sum_{N\mathfrak{p} \leqq x} \frac{\mathfrak{f}^2(\mathfrak{p})}{N\mathfrak{p}^2},$$

we conclude that

$$P\big(\mathfrak{f}_x(\mathfrak{a}) \leqq A(x) + uB_1(x) \,|\, \mathfrak{a} \in \mathfrak{S}_0\big) = \Phi(u) + \Delta(x), \tag{4.14}$$

where, obviously,

$$\Delta(x) = O\left(\frac{\log^{\frac{1}{2}} B(x)}{B(x)}\right).$$

Taking into account that $u(\exp. (-\frac{1}{2}u^2))$ is uniformly bounded in $(-\infty, \infty)$, formulae (4.10) and (4.11) follow immediately, which completes the proof of theorem 1.

§ 5. A basic lemma

As in § 4, let K be an algebraic numberfield of degree n over the rational numberfield $\boldsymbol{Q}$.

Let $\mathfrak{S}$ be a class of ideals.

We order the prime-ideals in such a way that $N\mathfrak{p}_i \leqq N\mathfrak{p}_j$ if $i < j$.

We define $\mathscr{P}(k, m)$ as the set of prime-ideals $\mathfrak{p}$ with $k < N\mathfrak{p} \leqq m$, $k \in \boldsymbol{R}$, $m \in \boldsymbol{R}$.

By $\mathscr{P}$ we denote any subset of $\mathscr{P}(1, \infty)$. As usual the function $\pi : \boldsymbol{R} \to \boldsymbol{R}$ is defined by

$$\pi(x) = \#\{\mathfrak{p} \in \mathscr{P}(1, x)\}.$$

In this paragraph x and y are always elements of $\boldsymbol{R}$. We define

$$\begin{aligned} M(\mathfrak{b}, y; \mathscr{P}) = \#\{&\mathfrak{a} \in \mathfrak{S} \,|\, N\mathfrak{a} \leqq y \\ &\text{and} \quad \mathfrak{a} \equiv 0 \bmod \mathfrak{b} \quad \text{and} \quad (\mathfrak{p} \,|\, \mathfrak{a} \to \mathfrak{p} \notin \mathscr{P})\}. \end{aligned} \tag{5.1}$$

For convenience we introduce the following abbreviations.

$$\begin{cases} M(y; \mathscr{P}) = M((1), y; \mathscr{P}), \\ M(\mathfrak{b}, y) = M(\mathfrak{b}, y; \mathscr{P}(1, 1)), \\ M(y; m) = M(y; \mathscr{P}(1, m)), \\ M(y) = M((1), y). \end{cases} \tag{5.2}$$

Obviously $M(y) = H(y; \mathfrak{S})$, which has been defined by (3.2). We shall prove the following lemma.

BASIC LEMMA (lemma 1).

Let $\psi : \boldsymbol{R} \to \boldsymbol{R}$ be a function such that

$$\lim_{y\to\infty} \psi(y) = \infty \quad \textit{and} \tag{5.3}$$

$$\lim_{y\to\infty} \frac{y}{\psi^{\gamma}(y)} = \infty \textit{ for every fixed } \gamma > 0. \tag{5.4}$$

Then

$$M(y; \psi(y)) = \lambda y \prod_{N\mathfrak{p}\leqq\psi(y)} \left(1 - \frac{1}{N\mathfrak{p}}\right) \{1+\Theta(y)\} \tag{5.5}$$

$$\textit{with } \lim_{y\to\infty} \Theta(y) = 0,$$

λ being the residue of $\zeta(s; \mathfrak{S}) = \sum_{\mathfrak{a}\in\mathfrak{S}} 1/N\mathfrak{a}^s$ at $s = 1$.

Firstly we make some comments.

Comment 1 (concerning the method of proof).

The major part of our proof will consist of applying a method, established by Brun [1] for rational integers to the case of integral ideals of class $\mathfrak{S}$. Rademacher [13] used Brun's method in order to investigate the conjecture of Goldbach in the ring of integers of an algebraic numberfield.

To achieve the aim of this chapter we could also use a method developed by Buchstab [3] and applied by De Bruijn [2].

We prefer, however, Brun's method since it does not seem possible to generalize Buchstab's method to the cases of chapters 3 and 4.

For completeness we mention that Lang [12] proves a formula which is equivalent to (5.5), using the same method as De Bruijn.

Comment 2 (concerning symmetrical functions).

For every rational integer i, $1 \leqq i \leqq t$, let a_i be a positive real number such that for at least one pair i, j, $1 \leqq i < j \leqq t$, $a_i \neq a_j$.

Furthermore, let symmetrical functions $\mathscr{S}_j$ be defined by the equality for polynomials

$$\prod_{i=1}^{t} (X-a_i) = \sum_{j=0}^{t} (-1)^j \mathscr{S}_j X^{t-j}, \qquad (t \in \boldsymbol{Z},\ t > 0). \tag{5.6}$$

It can be deduced that

$$\mathscr{S}_j < \frac{\mathscr{S}_1^j}{j!}, \qquad 1 \leqq j \leqq t, \tag{5.7}$$

and, if $\mathscr{S}_1 < 1$,

$$\mathscr{S}_j < \mathscr{S}_{j-1} < 1, \qquad 2 \leqq j \leqq t. \tag{5.8}$$

It can be proved by induction that

$$j! > \left(\frac{j}{e}\right)^j.$$

Substituting this in (5.7), we obtain

$$\mathscr{S}_j < \left(\frac{e\mathscr{S}_1}{j}\right)^j, \qquad 1 \leqq j \leqq t. \tag{5.9}$$

Comment 3.

Throughout the proof of the basic lemma, let α_0, α and α_1 be given such that

$$1 < \alpha_0 < \alpha < \alpha_1 < \sqrt{e}, \qquad \alpha_0, \alpha, \alpha_1 \in \boldsymbol{R} \tag{5.10}$$

and let β be defined by

$$\beta = \left(\frac{e \log \alpha_1}{2}\right)^2. \tag{5.11}$$

Obviously

$$\alpha_1 \beta < 1. \tag{5.12}$$

From (3.8) and (3.9), it follows that

$$\sum_{x < N\mathfrak{p} \leqq x^\alpha} \frac{1}{N\mathfrak{p}} = \log \alpha + \mathcal{O}\left(\frac{1}{\log x}\right) \tag{5.13}$$

and

$$\prod_{x < N\mathfrak{p} \leqq x^\alpha} \left(1 - \frac{1}{N\mathfrak{p}}\right) = \frac{1}{\alpha}\left(1 + \mathcal{O}\left(\frac{1}{\log x}\right)\right). \tag{5.14}$$

There exists a constant Q such that for

$$k = \max\left\{\exp. \frac{Q}{\log (\alpha/\alpha_0)}, \exp. \frac{Q}{\log (\alpha_1/\alpha)}\right\} \tag{5.15}$$

and all $x > k$ the following formulae hold.

$$\log \alpha_0 < \sum_{x < N\mathfrak{p} \leqq x^\alpha} \frac{1}{N\mathfrak{p}} < \log \alpha_1, \qquad \text{if } x > k, \tag{5.16}$$

$$\frac{1}{\alpha_1} < \prod_{x < N\mathfrak{p} \leqq x^\alpha} \left(1 - \frac{1}{N\mathfrak{p}}\right) < \frac{1}{\alpha_0}, \qquad \text{if } x > k. \tag{5.17}$$

Proof of the basic lemma.

Let k be fixed such that, for the given α_0, α and α_1, (5.16) and (5.17) hold.

Let $m \in \boldsymbol{R}$ be given and assume $m > k$.
We define

(5.18) $$v_j = m^{\alpha^{-j}}, \quad j \in \boldsymbol{Z} \quad \text{and} \quad j \geqq 0, \quad (\text{Fig. } 2).$$

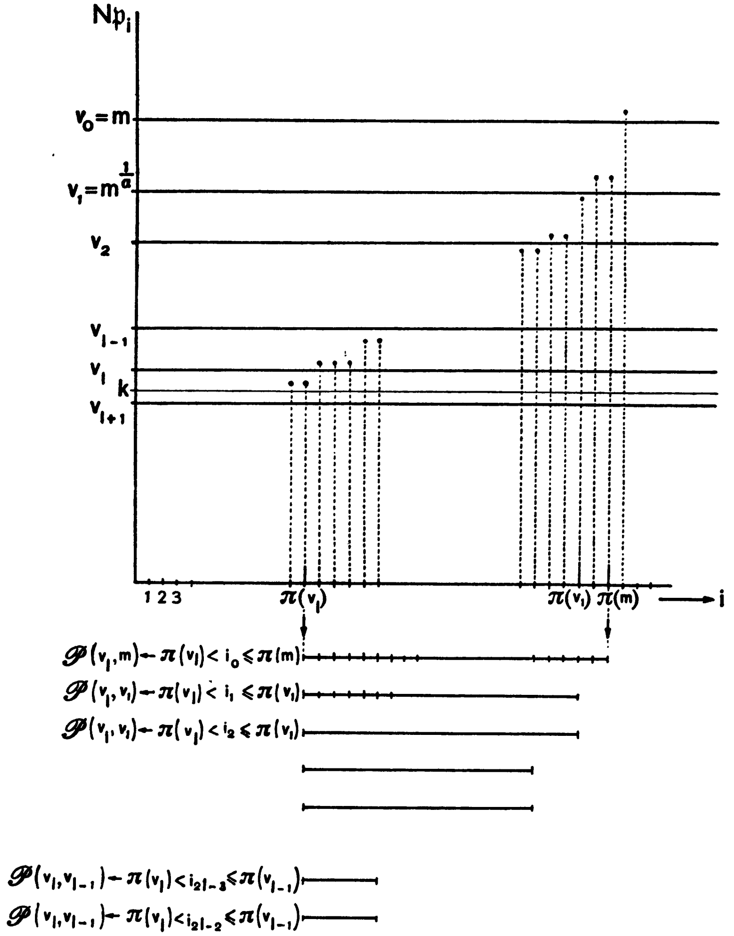

Fig. 2

Further, l is defined by

(5.19) $$v_{l+1} < k \leqq v_l, \quad l \in \boldsymbol{Z}, \quad l \geqq 0.$$

Following the sieve-method of Eratosthenes, we have

(5.20) $$M(y; \mathscr{P}(v_l, v_0)) = M(y) - \sum_{\pi(v_l) < i_0 \leqq \pi(v_0)} M(\mathfrak{p}_{i_0}, y)$$
$$+ \sum_{\pi(v_l) < i_1 < i_0 \leqq \pi(v_0)} M\Big(\mathfrak{p}_{i_0}\mathfrak{p}_{i_1}, y; \bigcup_{u=\pi(v_l)+1}^{i_1-1} \mathfrak{p}_u\Big).$$

From this it follows that

$$(5.21)\quad M(y;\mathscr{P}(v_l,v_0)) > M(y) - \sum_{\pi(v_l)<i_0\leqq\pi(v_0)} M(\mathfrak{p}_{i_0},y) + \sum_{\substack{\pi(v_l)<i_0\leqq\pi(v_0)\\ \pi(v_l)<i_1\leqq\pi(v_1)\\ i_1<i_0}} M\Big(\mathfrak{p}_{i_0}\mathfrak{p}_{i_1},y;\bigcup_{u=\pi(v_l)+1}^{i_1-1}\mathfrak{p}_u\Big).$$

For each term of the second sum on the right-hand side of (5.21), a formula analogous to (5.21) can be deduced. Before exploring formula (5.21) in this way, we give some definitions.

For $x\in \boldsymbol{R}$, we define

$$(5.22)\qquad [x] = \#\{r\in \boldsymbol{Z}\mid r>0 \text{ and } r\leqq x\}.$$

Furthermore $\Omega: I(R)\to \boldsymbol{Z}$ is defined by

$$(5.23)\qquad \Omega(\mathfrak{a}) = \sum_{d=1}^{\infty}\#\{\mathfrak{p}\in\mathscr{P}(1,\infty)\mid \mathfrak{p}^d\mid\mathfrak{a}\}.$$

We now introduce the following sets of ideals.

$$(5.24)\quad \mathfrak{A}(g) = \{\mathfrak{a}\in I(R)\mid (\mathfrak{p}\mid\mathfrak{a}\to v_g<N\mathfrak{p}\leqq v_0)\},\qquad 0\leqq g\leqq l,$$

$$(5.25)\quad \mathfrak{A}_j(g) = \{\mathfrak{a}\in\mathfrak{A}(g)\mid \Omega(\mathfrak{a}) = j\},\qquad j\in\boldsymbol{Z},\quad j>0,$$

$$(5.26)\quad \mathfrak{A}_j^*(g) = \Big\{\mathfrak{a}\in\mathfrak{A}_j(g)\mid \mathfrak{a} = \prod_{s=0}^{j-1}\mathfrak{p}_{i_s} \text{ with } \big(\pi(v_l)<i_s\leqq\pi(v_{[(s+1)/2]})\big) \text{ and } i_{j-1}<i_{j-2}<\ldots<i_1<i_0\big)\Big\},$$

$$(5.27)\quad \mathfrak{A}^*(g) = \bigcup_{j=1}^{2g-1}\mathfrak{A}_j^*(g),\qquad 0\leqq g\leqq l.$$

From (5.21) it can be proved by induction that the following formula holds.

$$(5.28)\qquad M(y;\mathscr{P}(v_l,v_0)) > \sum_{\mathfrak{a}\in\mathfrak{A}^*(l)}\mu(\mathfrak{a})M(\mathfrak{a},y),$$

μ being the Möbius-function.

From formula (3.5) we conclude:

$$M(\mathfrak{a},y) = \lambda\frac{y}{N\mathfrak{a}} + \mathcal{O}(y^{1-2/(n+1)}).$$

Defining

$$(5.29)\qquad \mathscr{R}_{m,\alpha}(y) = \sum_{\mathfrak{a}\in\mathfrak{A}^*(l)}\mu(\mathfrak{a})\left\{\frac{\lambda y}{N\mathfrak{a}} - M(\mathfrak{a},y)\right\},$$

we obtain from (5.28)

$$(5.30) \qquad M(y; \mathscr{P}(v_l, v_0)) > \lambda y \sum_{\mathfrak{a} \in \mathfrak{A}^*(l)} \frac{\mu(\mathfrak{a})}{N\mathfrak{a}} - \mathscr{R}_{m,\alpha}(y).$$

We define

$$(5.31) \qquad E(g) = \sum_{\mathfrak{a} \in \mathfrak{A}^*(g)} \frac{\mu(\mathfrak{a})}{N\mathfrak{a}},$$

which implies that (5.30) can be replaced by

$$(5.32) \qquad M(y; \mathscr{P}(v_l, v_0)) > \lambda y E(l) - \mathscr{R}_{m,\alpha}(y).$$

If we put

$$(5.33) \qquad \mathscr{S}_j^*(g) = \sum_{\mathfrak{a} \in \mathfrak{A}^*_j(g)} \frac{|\mu(\mathfrak{a})|}{N\mathfrak{a}},$$

we have

$$(5.34) \qquad E(g) = \sum_{j=0}^{2g-1} (-1)^j \mathscr{S}_j^*(g).$$

Further, $\mathscr{S}_j(g)$ and $s_j(g)$ are defined by

$$(5.35) \qquad \begin{cases} \mathscr{S}_j(g) = \displaystyle\sum_{\mathfrak{a} \in \mathfrak{A}_j(g)} \frac{|\mu(\mathfrak{a})|}{N\mathfrak{a}}, & 0 \leqq j \leqq r(g) = \pi(v_0) - \pi(v_g) \\ \text{and} & \\ s_j(g) = \displaystyle\sum_{\mathfrak{a} \in \mathfrak{B}_j(g)} \frac{|\mu(\mathfrak{a})|}{N\mathfrak{a}}, & 0 \leqq j \leqq \rho(g) = \pi(v_g) - \pi(v_{g+1}), \end{cases}$$

where $\mathfrak{B}_j(g)$ is defined by

$$\mathfrak{B}_j(g) = \{\mathfrak{a} \in I(R) \mid (\mathfrak{p}|\mathfrak{a} \to v_{g+1} < N\mathfrak{p} \leqq v_g) \text{ and } \Omega(\mathfrak{a}) = j\}.$$

Obviously $\mathscr{S}_j(g)$ and $s_j(g)$ could equally have been defined by

$$(5.36) \qquad \begin{cases} \displaystyle\prod_{v_g < N\mathfrak{p} \leqq v_0} \left(X - \frac{1}{N\mathfrak{p}}\right) = \sum_{j=0}^{r(g)} (-1)^j \mathscr{S}_j(g) X^{r(g)-j} \\ \text{and} \\ \displaystyle\prod_{v_{g+1} < N\mathfrak{p} \leqq v_g} \left(X - \frac{1}{N\mathfrak{p}}\right) = \sum_{j=0}^{\rho(g)} (-1)^j s_j(g) X^{\rho(g)-j} \end{cases}$$

respectively.

For convenience we define

$$(5.37) \qquad \begin{cases} \mathscr{S}_j^*(g) = 0 \text{ for } j > 2g-1, \\ s_j(g) = 0 \text{ for } j > \rho(g). \end{cases}$$

It is clear that

$$(5.38)\qquad \mathscr{S}_j^*(g+1) = \sum_{i=0}^{j} \mathscr{S}_{j-i}^*(g)s_i(g),$$

and consequently

$$(5.39)\qquad E(g+1) = \sum_{j=0}^{2g+1}(-1)^j \sum_{i=0}^{j} \mathscr{S}_i^*(g)s_{j-i}(g).$$

We define ϑ_g and τ_g by

$$(5.40)\qquad \vartheta_g = \prod_{v_g < N\mathfrak{p} \leqq v_{g-1}} \left(1 - \frac{1}{N\mathfrak{p}}\right)$$

and

$$(5.41)\qquad \tau_g = \sum_{v_g < N\mathfrak{p} \leqq v_{g-1}} \frac{1}{N\mathfrak{p}}$$

respectively.

We remark that, owing to (5.18), (5.19), (5.16) and (5.17), we have

$$(5.42)\qquad \frac{1}{\alpha_1} < \vartheta_g < \frac{1}{\alpha_0}, \qquad \text{if } g \leqq l,$$

$$(5.43)\qquad \log \alpha_0 < \tau_g < \log \alpha_1, \quad \text{if } g \leqq l.$$

We now consider $\vartheta_{g+1}E(g)$.

$$\begin{aligned}
\vartheta_{g+1}E(g) &= \sum_{j=0}^{\rho(g)}(-1)^j s_j(g) \sum_{i=0}^{2g-1}(-1)^i \mathscr{S}_i^*(g) \\
&= \sum_{j=0}^{\rho(g)+2g-1}(-1)^j \sum_{i=0}^{j} \mathscr{S}_i^*(g)s_{j-i}(g) \\
&= \sum_{j=0}^{2g+1}(-1)^j \sum_{i=0}^{j} \mathscr{S}_i^*(g)s_{j-i}(g) + \sum_{j=2g+2}^{\rho(g)+2g-1}(-1)^j \sum_{i=0}^{j} \mathscr{S}_i^*(g)s_{j-i}(g).
\end{aligned}$$

Combining this with (5.39), we obtain

$$(5.44)\quad \vartheta_{g+1}E(g) = E(g+1) + \sum_{j=2g+2}^{\rho(g)+2g-1}(-1)^j \sum_{i=0}^{j} \mathscr{S}_i^*(g)s_{j-i}(g).$$

The assumption concerning α_1, i.e. (5.10), now makes it clear that $\tau_{g+1} = s_1(g) < \log \alpha_1 < 1$ (if $g < l$) and hence, applying (5.8) and (5.36), we can conclude that

$$\sum_{j=2g+2}^{\rho(g)+2g-1}(-1)^j \sum_{i=0}^{j} \mathscr{S}_i^*(g)s_{j-i}(g)$$

is an alternating sum of monotonically decreasing terms since

$$\sum_{i=0}^{j+1} \mathscr{S}_i^*(g)s_{j+1-i}(g) \leqq \sum_{i=0}^{j+1} \mathscr{S}_i^*(g)s_{j-i}(g) = \sum_{i=0}^{j} \mathscr{S}_i^*(g)s_{-i}(g),$$

$s_{-1}(g)$ being an empty sum and therefore equal to 0. Hence

$$(5.45) \qquad \vartheta_{g+1}E(g) \leqq E(g+1)+\sum_{i=0}^{2g+2}\mathscr{S}_i^*(g)s_{2g+2-i}(g)$$
$$\leqq E(g+1)+\mathscr{S}^*_{2g+2}(g+1).$$

Obviously $\mathscr{S}^*_{2g+2}(g+1) < \mathscr{S}_{2g+2}(g+1)$.

Formula (5.9) can now be applied to $\mathscr{S}_{2g+2}(g+1)$. Therefore

$$\mathscr{S}_{2g+2}(g+1) < \left(\frac{e\mathscr{S}_1(g+1)}{2g+2}\right)^{2g+2} = \left(\frac{e\sum_{i=1}^{g+1}\tau_i}{2g+2}\right)^{2g+2}$$
$$< \left(\frac{e(g+1)\log\alpha_1}{2g+2}\right)^{2g+2} = \left(\frac{e\log\alpha_1}{2}\right)^{2g+2} = \beta^{g+1},$$

β being defined in (5.11).

Substituting this result in (5.45), we obtain

$$(5.46) \qquad E(g+1) > \vartheta_{g+1}E(g)-\beta^{g+1} \text{ for } g+1 \leqq l.$$

Therefore

$$E(1) = 1-\mathscr{S}_1^*(1) = 1-\tau_1 > 1-\log\alpha_1,$$
$$E(2) > \vartheta_2E(1)-\beta^2 > \vartheta_2(1-\log\alpha_1-\alpha_1\beta^2), \text{ as } \frac{1}{\vartheta_2} < \alpha_1.$$

Then, by induction,.

$$(5.47) \qquad E(g) > \left\{1-\log\alpha_1-\alpha_1\beta^2\sum_{i=0}^{g-2}(\alpha_1\beta)^i\right\}\prod_{j=2}^{g}\vartheta_j.$$

Since we assumed $\alpha_1 < \sqrt{e}$, (5.10), we have

$$(5.48) \qquad E(g) > \left(1-\log\alpha_1-\frac{\alpha_1\beta^2}{1-\alpha_1\beta}\right)\prod_{j=1}^{g}\vartheta_j, \text{ if } g \leqq l.$$

In (5.48) we used the obvious fact that $0 < \vartheta_1 < 1$. Substituting this result in (5.32), we find

$$(5.49) \quad M(y; \mathscr{P}(v_l, m)) > g(\alpha_1)\lambda y \prod_{v_l<N\mathfrak{p}\leqq m}\left(1-\frac{1}{N\mathfrak{p}}\right)-\mathscr{R}_{m,\alpha}(y),$$

where $g(\alpha_1)$ has to be defined by

$$(5.50) \qquad g(\alpha_1) = 1-\log\alpha_1-\frac{\alpha_1\beta^2}{1-\alpha_1\beta}.$$

Using the same method by which we proved (5.28), we can prove

$$M(y; \mathscr{P}(1, m)) > \sum_{\mathfrak{a} \in \mathfrak{C}} \mu(\mathfrak{a}) M(\mathfrak{a}, y), \tag{5.51}$$

where the set $\mathfrak{C}$ is defined by

$$\begin{aligned} \mathfrak{C} = \{\mathfrak{a} \in I(R) \mid \mathfrak{a} = \prod_{s=0}^{z} \mathfrak{p}_{i_s} & \\ \text{with } [1 < i_s \leqq \pi(v_{[(s+1)/2]}), & \text{ if } s \leqq 2l \\ \text{and } 1 < i_s \leqq \pi(v_l), & \text{ if } s > 2l \\ \text{and } 0 \leqq z \leqq 2l + \pi(v_l)]\}. & \end{aligned} \tag{5.52}$$

Defining

$$E'(l+1) = \sum_{\mathfrak{a} \in \mathfrak{C}} \frac{\mu(\mathfrak{a})}{N\mathfrak{a}}, \tag{5.53}$$

we find

$$M(y; \mathscr{P}(1, m)) > \lambda y E'(l+1) - \mathscr{R}'_{m,\alpha}(y), \tag{5.54}$$

where

$$\mathscr{R}'_{m,\alpha}(y) = \sum_{\mathfrak{a} \in \mathfrak{C}} \mu(\mathfrak{a}) \left(\frac{\lambda y}{N\mathfrak{a}} - M(\mathfrak{a}, y)\right). \tag{5.55}$$

It is clear that

$$E'(l+1) = E(l) \prod_{N\mathfrak{p} \leqq v_l} \left(1 - \frac{1}{N\mathfrak{p}}\right). \tag{5.56}$$

Combining (5.48) and (5.56), we obtain

$$M(y; \mathscr{P}(1, m)) > \lambda y g(\alpha_1) \prod_{N\mathfrak{p} \leqq m} \left(1 - \frac{1}{N\mathfrak{p}}\right) - \mathscr{R}'_{m,\alpha}(y). \tag{5.57}$$

Taking $m = \psi(y)$, it follows that

$$\begin{aligned} M(y; \mathscr{P}(1, \psi(y))) &= M(y; \psi(y)) \\ &> \lambda y g(\alpha_1) \prod_{N\mathfrak{p} \leqq \psi(y)} \left(1 - \frac{1}{N\mathfrak{p}}\right) - \mathscr{R}'_{\psi(y),\alpha}(y). \end{aligned} \tag{5.58}$$

The number of terms occurring in $\mathscr{R}'_{m,\alpha}(y)$ equals the number of terms occurring in $E'(l+1)$.

This number is obviously less than the number of terms occurring in the expansion of

$$D(l) = \left(1 - \sum_{v_l < N\mathfrak{p} \leqq v_0} \frac{1}{N\mathfrak{p}}\right) \prod_{j=1}^{l-1} \left(1 - \sum_{v_l < N\mathfrak{p} \leqq v_j} \frac{1}{N\mathfrak{p}}\right)^2 \prod_{N\mathfrak{p} \leqq v_l} \left(1 - \frac{1}{N\mathfrak{p}}\right).$$

As $\pi(x) < f\, x/\log x$ for some positive constant f, the number of terms occurring in the sum generated by $D(l)$ is less than

$$\left(f' \frac{m}{\log m}\right)^{1+2\sum_{j=1}^{l-1} \alpha^{-j}} \cdot 2^{v_l},$$

for some positive constant f'.

According to the special way α has been chosen, we have, owing to (5.19), $v_l = v_{l+1}^{\alpha} < k^{\alpha}$.

Therefore

$$\left(\frac{f'm}{\log m}\right)^{1+2\sum_{j=1}^{l-1} \alpha^{-j}} \cdot 2^{v_l} < 2^{k^\alpha} \cdot \left(\frac{f'm}{\log m}\right)^{(\alpha+1)/(\alpha-1)},$$

and consequently, using formula (3.5), we conclude that therc exists a constant d, such that

$$\text{(5.59)} \qquad \mathscr{R}'_{m,\alpha}(y) < d \cdot 2^{k^\alpha} \cdot \left(\frac{f'm}{\log m}\right)^{(\alpha+1)/(\alpha-1)} y^{1-2/(n+1)}.$$

We recall that n is the degree of K over $\boldsymbol{Q}$.

Owing to the assumption (5.4) in the formulation of the basic lemma, we have

$$\left(\frac{f'\psi(y)}{\log \psi(y)}\right)^{(\alpha+1)/(\alpha-1)} < C(\alpha) y^{1/(n+1)},$$

where $C(\alpha)$ is a positive constant dependent on α.

From (5.58) and (5.59) it then follows that

$$\text{(5.60)} \quad M(y; \psi(y)) > g(\alpha_1)\lambda y \prod_{N\mathfrak{p} \leq \psi(y)} \left(1 - \frac{1}{N\mathfrak{p}}\right) - C^*(\alpha) y^{1-1/(n+1)},$$

where, clearly, $C^*(\alpha)$ is a constant dependent on α.

Analogously we can deduce that

$$\text{(5.61)} \quad M(y; \psi(y)) < \alpha_1 g^*(\alpha_0)\lambda y \prod_{N\mathfrak{p} \leq \psi(y)} \left(1 - \frac{1}{N\mathfrak{p}}\right) + C_2^*(\alpha) y^{1-1/(n+1)},$$

where

$$g^*(\alpha_0) = 1 - \log \alpha_0 + \frac{\alpha_0(\frac{1}{2}e \log \alpha_0)^4}{1-(\frac{1}{2}e \log \alpha_0)^2}.$$

From (5.60) and (5.61), we conclude that

$$\text{(5.62)} \qquad g(\alpha_1) \leq \lim_{y\to\infty} \frac{M(y; \psi(y))}{\lambda y \prod_{N\mathfrak{p} \leq \psi(y)} \left(1 - \frac{1}{N\mathfrak{p}}\right)} \leq \alpha_1 g^*(\alpha_0).$$

Formula (5.62) holds for all choices of α_0, α and α_1, provided that the conditions in formula (5.10) are satisfied.

Taking $\alpha_0 = 1+\delta$, $\alpha = 1+2\delta$ and $\alpha_1 = 1+3\delta$, where $\delta > 0$ such that assumption (5.10) is satisfied, and letting $\delta \to 0$, we finally obtain

$$\lim_{y\to\infty} \frac{M(y;\psi(y))}{\lambda y \prod_{N\mathfrak{p}\leqq\psi(y)} \left(1-\frac{1}{N\mathfrak{p}}\right)} = 1, \tag{5.63}$$

which completes the proof of the basic lemma.

§ 6. Two other lemmas

Let $r: \boldsymbol{R} \to \boldsymbol{R}$ be a function such that

$$\begin{cases} r(x) > 0 \text{ for every } x \in \boldsymbol{R}, \\ \lim\limits_{x\to\infty} r(x) = 0, \\ \lim\limits_{x\to\infty} x^{r(x)} = \infty. \end{cases} \tag{6.1}$$

For every r satisfying (6.1), we define the functions $\psi: \boldsymbol{R} \to \boldsymbol{R}$ and $\Psi: \boldsymbol{R} \to \boldsymbol{R}$ by

$$\psi(x) = x^{r(x)}, \qquad x \in \boldsymbol{R} \tag{6.2}$$

and

$$\Psi(x) = x^{\sqrt{r(x)}}, \qquad x \in \boldsymbol{R}, \qquad \text{respectively.} \tag{6.3}$$

Let $\mathscr{I}[x]$ be the set of integral ideals which have no prime-factors other than those with a norm less than or equal to $\psi(x)$,

$$\mathscr{I}[x] = \{\mathfrak{a} \in I(R) \mid (\mathfrak{p} \mid \mathfrak{a} \to N\mathfrak{p} \leqq \psi(x))\}. \tag{6.4}$$

For every ideal $\mathfrak{a} \in I(R)$, we define the ideal $\mathfrak{m}(\mathfrak{a}; x)$, by the following conditions:

$$\begin{cases} \mathfrak{m}(\mathfrak{a}; x) \in \mathscr{I}[x], \\ \mathfrak{m}(\mathfrak{a}; x) \mid \mathfrak{a}, \\ \mathfrak{p} \mid \dfrac{\mathfrak{a}}{\mathfrak{m}(\mathfrak{a}; x)} \to N\mathfrak{p} > \psi(x). \end{cases} \tag{6.5}$$

Clearly, $\mathfrak{m}(\mathfrak{a}; x)$ is uniquely determined by this definition.

Let the different ideals of $\mathscr{I}[x]$ be denoted by $\mathfrak{n}_1(x)$, $\mathfrak{n}_2(x)$, $\mathfrak{n}_3(x)$, ... etc.

Let E_i be the subset of principal ideals defined by

(6.6) $E_i = \{\mathfrak{a} \in \mathfrak{S}_0 \mid \mathfrak{m}(\mathfrak{a}; x) = \mathfrak{n}_i(x) \text{ and } N\mathfrak{a} \leqq x\}, \quad i > 0,\ i \in \boldsymbol{Z}.$

LEMMA 2.

If $N\mathfrak{n}_i(x) \leqq \Psi(x)$, then —uniformly in i—

(6.7) $$P(\mathfrak{a} \in E_i \mid \mathfrak{S}_0) = \frac{1}{N\mathfrak{n}_i(x)} \prod_{N\mathfrak{p} \leqq \psi(x)} \left(1 - \frac{1}{N\mathfrak{p}}\right)(1+o(1)),$$

P being defined by (4.1) *and* (4.2).

Proof of lemma 2.

If $\mathfrak{S}$ is the inverse class of the class of $\mathfrak{n}_i(x)$, then

$$\#\{\mathfrak{a} \in E_i\} = \#\left\{\mathfrak{a} \in \mathfrak{S} \mid N\mathfrak{a} \leqq \frac{x}{N\mathfrak{n}_i(x)} \text{ and } (\mathfrak{p} \mid \mathfrak{a} \rightarrow N\mathfrak{p} > \psi(x))\right\}$$
$$= M\left(\frac{x}{N\mathfrak{n}_i(x)};\ \psi(x)\right).$$

Using the assumption $N\mathfrak{n}_i(x) \leqq \Psi(x)$, we can conclude that

$$\lim_{x\to\infty} \frac{x}{N\mathfrak{n}_i(x) \cdot (\psi(x))^\gamma} = \infty \text{ for every } \gamma \in \boldsymbol{R}.$$

Therefore the basic lemma applies, thus completing the proof of lemma 2.

LEMMA 3.

Let $L(z) = \#\{\mathfrak{a} \in I(R) \mid N\mathfrak{a} \leqq z$ and $N\mathfrak{m}(\mathfrak{a}; x) > \Psi(x)\}$. Then there exists a positive constant b such that

(6.8) $$L(z) < bz\sqrt{r(x)}.$$

Proof of lemma 3.

We have

$$(\Psi(x))^{L(z)} < \prod_{N\mathfrak{p} \leqq \psi(x)} (N\mathfrak{p})^{\sum_{j=1}^{\infty} H(z/N\mathfrak{p}^j)}.$$

Hence

$$L(z) \log \Psi(x) < \sum_{N\mathfrak{p} \leqq \psi(x)} \left(\sum_{j=1}^{\infty} H\left(\frac{z}{N\mathfrak{p}^j}\right)\right) \log N\mathfrak{p}$$
$$< b_1 z \sum_{N\mathfrak{p} \leqq \psi(x)} \frac{\log N\mathfrak{p}}{N\mathfrak{p}}$$

for some constant b_1.

Because of (3.7) there exists a constant b such that

$$L(z) \log \Psi(x) < bz \log \psi(x). \tag{6.9}$$

Substituting (6.2) and (6.3) in (6.9), we obtain

$$L(z)\sqrt{r(x)} \log x < bz\, r(x) \log x,$$

which completes the proof of lemma 3.

§ 7. Theorem 2

We shall prove the following theorem.

Theorem 2.
Let ψ be defined by (6.2).
Let $\mathfrak{f}$, $\mathfrak{f}_x$, A, B and Φ be defined as in theorem 1.
If

$$\lim_{x\to\infty} B(x) = \infty,$$

then

$$\lim_{x\to\infty} P(\mathfrak{f}_{\psi(x)}(\mathfrak{a}) \leqq A(\psi(x)) + uB(\psi(x)) \mid \mathfrak{a} \in \mathfrak{S}_0 \text{ and } N\mathfrak{a} \leqq x) = \Phi(u) \textit{ uniformly in } u \in \boldsymbol{R}. \tag{7.1}$$

Proof of theorem 2.
Let

$$W[x; u] = \{\mathfrak{a} \in \mathfrak{S}_0 \mid N\mathfrak{a} \leqq x \quad \text{and} \quad \mathfrak{f}_{\psi(x)}(\mathfrak{a}) \leqq A(\psi(x)) + uB(\psi(x))\}. \tag{7.2}$$

Because of the definition of $\mathfrak{m}(\mathfrak{a}; x)$ —see (6.5)— we have

$$\mathfrak{f}_{\psi(x)}(\mathfrak{a}) = \mathfrak{f}_{\psi(x)}(\mathfrak{m}(\mathfrak{a}; x)).$$

As before, let the set E_i, be defined by

$$E_i = \{\mathfrak{a} \in \mathfrak{S}_0 \mid \mathfrak{m}(\mathfrak{a}; x) = \mathfrak{n}_i(x) \text{ and } N\mathfrak{a} \leqq x\}, \tag{7.3}$$

it then follows that $E_i \subset W[x; u]$ or $E_i \cap W[x; u]$ is empty. We define

$$E_i^* = E_i \cap W[x; u]. \tag{7.4}$$

We note that formula (7.1), which we shall prove, is equivalent to

$$\lim_{x\to\infty} \frac{\#\{\mathfrak{a} \in W[x; u]\}}{H(x; \mathfrak{S}_0)} = \Phi(u) \text{ uniformly in } u. \tag{7.5}$$

Let Ψ be defined by (6.3).

We have

$$\#\{\mathfrak{a} \in W[x; u]\} = \sum_i \#\{\mathfrak{a} \in E_i^*\} = L_1(x)+L_2(x),$$

where

$$L_1(x) = \textstyle\sum_1 \#\{\mathfrak{a} \in E_i^*\}, \tag{7.6}$$

the sum being extended over those suffixes i, for which $N\mathfrak{n}_i(x) \leqq \Psi(x)$, and

$$L_2(x) = \textstyle\sum_2 \#\{\mathfrak{a} \in E_i^*\}, \tag{7.7}$$

the sum being extended over those suffixes i, for which $N\mathfrak{n}_i(x) > \Psi(x)$.

From lemma 3 it follows that

$$L_2(x) < bx\sqrt{r(x)},\ r \text{ satisfying conditions (6.1).}$$

Therefore

$$\lim_{x\to\infty} \frac{L_2(x)}{H(x; \mathfrak{S}_0)} = \lim_{x\to\infty} \frac{L_2(x)}{\lambda x + \mathcal{O}(x^{1-2/(n+1)})} = 0.$$

Hence, it remains to prove that

$$\lim_{x\to\infty} \frac{L_1(x)}{H(x; \mathfrak{S}_0)} = \Phi(u) \text{ uniformly in } u. \tag{7.8}$$

Applying lemma 2, we find

$$\frac{L_1(x)}{H(x; \mathfrak{S}_0)} = \left\{\sum_{N\mathfrak{n}_i(x)\leqq\Psi(x)}' \frac{1}{N\mathfrak{n}_i(x)}\right\} \prod_{N\mathfrak{p}\leqq\psi(x)} \left(1-\frac{1}{N\mathfrak{p}}\right) \{1+o(1)\}, \tag{7.9}$$

where the dash in the summation indicates that it is extended over those suffixes i for which

$$\mathfrak{f}_{\psi(x)}(\mathfrak{n}_i(x)) \leqq A(\psi(x))+uB(\psi(x)). \tag{7.10}$$

We now consider subsets F_i of $\mathfrak{S}_0$, defined by

$$F_i = \{\mathfrak{a} \in \mathfrak{S}_0 \mid \mathfrak{m}(\mathfrak{a}; x) = \mathfrak{n}_i(x)\}. \tag{7.11}$$

Applying theorem 1, we conclude that

$$P(\mathfrak{a} \in {\textstyle\bigcup}' F_i \mid \mathfrak{S}_0) = \Phi(u)+o(1) \quad \text{uniformly in } u, \text{ as } x\to\infty, \tag{7.12}$$

where the dash again indicates that the union is extended over those i which satisfy formula (7.10).

Since it follows from lemma 3 that

(7.13) $$P(\mathfrak{a} \in \bigcup'_{N\mathfrak{n}_i(x) > \Psi(x)} F_i \mid \mathfrak{S}_0) < b\sqrt{r(x)},$$

we have

(7.14) $$P(\mathfrak{a} \in \bigcup'_{N\mathfrak{n}_i(x) \leqq \Psi(x)} F_i \mid \mathfrak{S}_0) = \Phi(u) + o(1)$$
uniformly in u, as $x \to \infty$.

Further

$$P(\mathfrak{a} \in \bigcup'_{N\mathfrak{n}_i(x) \leqq \Psi(x)} F_i \mid \mathfrak{S}_0) = \sum'_{N\mathfrak{n}_i(x) \leqq \Psi(x)} P(\mathfrak{a} \in F_i \mid \mathfrak{S}_0)$$

and

$$P(\mathfrak{a} \in F_i \mid \mathfrak{S}_0) = P\left(\mathfrak{n}_i(x) \mid \mathfrak{a} \text{ and } \left(\mathfrak{p} \mid \frac{\mathfrak{a}}{\mathfrak{n}_i(x)} \to N\mathfrak{p} > \psi(x)\right) \middle| \mathfrak{a} \in \mathfrak{S}_0\right).$$

Because of the stochastical independence proved in § 4 — formulae (4.12) and (4.13) — it follows that

$$P(\mathfrak{a} \in F_i \mid \mathfrak{S}_0) = \frac{1}{N\mathfrak{n}_i(x)} \prod_{N\mathfrak{p} \leqq \psi(x)} \left(1 - \frac{1}{N\mathfrak{p}}\right)$$

and therefore

(7.15)
$$P(\mathfrak{a} \in \bigcup'_{N\mathfrak{n}_i(x) \leqq \Psi(x)} F_i \mid \mathfrak{S}_0) = \left\{\sum'_{N\mathfrak{n}_i(x) \leqq \Psi(x)} \frac{1}{N\mathfrak{n}_i(x)}\right\} \prod_{N\mathfrak{p} \leqq \psi(x)} \left(1 - \frac{1}{N\mathfrak{p}}\right),$$

where the dash still has the same meaning as in (7.12).

Combining (7.14) and (7.15), we obtain

(7.16) $$\sum'_{N\mathfrak{n}_i(x) \leqq \Psi(x)} \frac{1}{N\mathfrak{n}_i(x)} \prod_{N\mathfrak{p} \leqq \psi(x)} \left(1 - \frac{1}{N\mathfrak{p}}\right) = \Phi(u) + o(1)$$
uniformly in u,

and this, in combination with (7.9), implies that

(7.17) $$\frac{L_1(x)}{H(x; \mathfrak{S}_0)} = (\Phi(u) + o(1))(1 + o(1)) = \Phi(u) + o(1)$$
uniformly in u,

which completes the proof of theorem 2.

§ 8. Theorem 3

In the preceding sections we have made the basis on which we can now build the proof of the main theorem of this chapter.

THEOREM 3.

Let $\mathfrak{f}$: $I(R) \to \mathbf{R}$ be an additive number-theoretic function, such that

$$\mathfrak{f}(\mathfrak{a}\cdot\mathfrak{b}) = \mathfrak{f}(\mathfrak{a})+\mathfrak{f}(\mathfrak{b}) \textit{ if } (\mathfrak{a},\mathfrak{b}) = (1), \quad \mathfrak{a}\in I(R), \mathfrak{b}\in I(R),$$
$$\mathfrak{f}(\mathfrak{p}^k) = \mathfrak{f}(\mathfrak{p}) \textit{ for } k\in \boldsymbol{Z} \textit{ and } k \geqq 1 \textit{ and } \mathfrak{p} \textit{ prime-ideal,}$$
and $|\mathfrak{f}(\mathfrak{p})| \leqq 1$.

Let $A: \boldsymbol{R}\to\boldsymbol{R}$ *and* $B:\boldsymbol{R}\to\boldsymbol{R}$ *be defined by*

$$A(x) = \sum_{N\mathfrak{p}\leqq x} \frac{\mathfrak{f}(\mathfrak{p})}{N\mathfrak{p}} \quad \textit{and}$$

$$B(x) = \left[\sum_{N\mathfrak{p}\leqq x} \frac{\mathfrak{f}^2(\mathfrak{p})}{N\mathfrak{p}}\right]^{\frac{1}{2}} \quad \textit{respectively.}$$

If
$$\lim_{x\to\infty} B(x) = \infty,$$
then

$$\text{(8.1)} \quad \lim_{x\to\infty} P(\mathfrak{f}(\mathfrak{a}) \leqq A(x)+uB(x) \mid \mathfrak{a}\in\mathfrak{S}_0 \textit{ and } N\mathfrak{a}\leqq x) = \Phi(u) \quad \textit{uniformly in } u\in\boldsymbol{R},$$

P and Φ being defined by (4.2) *and* (4.9) *respectively.*

Proof of theorem 3.

Let $r: \boldsymbol{R}\to\boldsymbol{R}$ be a function such that

$$\text{(8.2)} \quad \begin{cases} r(x) > 0 \text{ for every } x\in\boldsymbol{R}, \\ \lim_{x\to\infty} r(x) = 0, \\ \lim_{x\to\infty} x^{r(x)} = \infty \text{ and} \\ \dfrac{1}{r(x)} = o(B(x)) \text{ for } x\to\infty. \end{cases}$$

Hence, r satisfies (6.1).

As before, we define $\psi: \boldsymbol{R}\to\boldsymbol{R}$ by

$$\text{(8.3)} \quad \psi(x) = x^{r(x)}.$$

If $\rho_{\mathfrak{p}}$ is defined by (4.4) and $\mathfrak{f}_x$ by (4.6) then, for every $\mathfrak{a}\in I(R)$ with $N\mathfrak{a}\leqq x$, we have

$$\text{(8.4)} \quad |\,\mathfrak{f}(\mathfrak{a})-\mathfrak{f}_{\psi(x)}(\mathfrak{a})\,| \leqq \sum_{\psi(x)<N\mathfrak{p}\leqq x} |\rho_{\mathfrak{p}}(\mathfrak{a})|$$
$$\leqq \#\{\mathfrak{p} \mid \mathfrak{a}\equiv 0 \bmod \mathfrak{p} \text{ and } N\mathfrak{p} > \psi(x) \text{ and } \mathfrak{p} \text{ prime}\}$$
$$\leqq \frac{1}{r(x)}, \text{ as } N\mathfrak{a}\leqq x.$$

Further, for $a > 1$, we can find X_0 such that, for $x > X_0$,

$$|A(x)-A(\psi(x))| < -a \log r(x) \tag{8.5}$$

and

$$|B(x)-B(\psi(x))| < -\frac{a \log r(x)}{2B(\psi(x))}. \tag{8.6}$$

(8.5) and (8.6) follow easily from

$$|\mathfrak{f}(\mathfrak{p})| \leqq 1 \text{ and } \sum_{N\mathfrak{p}\leqq x} \frac{1}{N\mathfrak{p}} = \operatorname{loglog} x + \mathcal{O}(1).$$

Because of the assumption, $1/r(x) = o(B(x))$, (8.4), (8.5) and (8.6) imply that

$$|\mathfrak{f}(\mathfrak{a})-\mathfrak{f}_{\psi(x)}(\mathfrak{a})| = o(B(x)) \text{ for } N\mathfrak{a} \leqq x, \tag{8.4'}$$

$$|A(x)-A(\psi(x))| = o(B(x)) \quad \text{and} \tag{8.5'}$$

$$|B(x)-B(\psi(x))| = o(B(x)) \tag{8.6'}$$

respectively.

Now, consider the following three sets:

$$\tag{8.7} \begin{cases} V[x] = \{\mathfrak{a} \in \mathfrak{S}_0 \mid \mathfrak{f}(\mathfrak{a}) \leqq A(x)+uB(x) \text{ and } N\mathfrak{a} \leqq x\}, \\ U_\varepsilon[x] = \{\mathfrak{a} \in \mathfrak{S}_0 \mid \mathfrak{f}_{\psi(x)}(\mathfrak{a}) \leqq A(\psi(x))+(u+u\varepsilon+\varepsilon)B(\psi(x)) \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{and } N\mathfrak{a} \leqq x\}, \\ U_{-\varepsilon}[x] = \{\mathfrak{a} \in \mathfrak{S}_0 \mid \mathfrak{f}_{\psi(x)}(\mathfrak{a}) \leqq A(\psi(x))+(u-u\varepsilon-\varepsilon)B(\psi(x)) \\ \qquad\qquad\qquad\qquad\qquad\qquad \text{and } N\mathfrak{a} \leqq x\}. \end{cases}$$

Assuming $u \geqq 0$ (if $u < 0$ the proof is analogous) we now state:

Given $\varepsilon > 0$, it is possible to find X_1 such that, for $x > X_1$

$$\cdot\ U_{-\varepsilon}[x] \subset V[x] \subset U_\varepsilon[x],$$

and hence, owing to theorem 2

$$\tag{8.8} \begin{aligned} \Phi(u-u\varepsilon-\varepsilon)-\delta(x) &\leqq P(V[x] \mid \mathfrak{a} \in \mathfrak{S}_0 \text{ and } N\mathfrak{a} \leqq x) \\ &\leqq \Phi(u+u\varepsilon+\varepsilon)+\delta(x), \end{aligned}$$

where $\delta(x) > 0$ and $\lim_{x\to\infty} \delta(x) = 0$.

Obviously

$$\Phi(u)-\Phi(u-u\varepsilon-\varepsilon) = (2\pi)^{-\frac{1}{2}} \int_{u-u\varepsilon-\varepsilon}^{u} \exp.\,(-\tfrac{1}{2}t^2)dt < \varepsilon \quad \text{uniformly in } u \in \boldsymbol{R}. \tag{8.9}$$

Similarly

$$\Phi(u+u\varepsilon+\varepsilon)-\Phi(u) < \varepsilon \text{ uniformly in } u \in \boldsymbol{R}. \tag{8.10}$$

Substituting (8.9) and (8.10) in (8.8) and then letting ε tend to 0, we finally obtain

$$\lim_{x\to\infty} P(V[x] \mid \mathfrak{a} \in \mathfrak{S}_0 \text{ and } N\mathfrak{a} \leqq x) = \Phi(u)$$

uniformly in $u \in \boldsymbol{R}$, which completes the proof of theorem 3.

§ 9. On the rate of convergence

The purpose of this section is to obtain information about the rate of convergence of the final result in the preceding section.

Therefore, we must investigate the various steps which give rise to theorem 3.

§ 9.1. CONCERNING THEOREM 1

In the course of the proof of theorem 1, we obtain the following formula, which holds under the assumptions of the theorem.

$$(4.11) \qquad P(\mathfrak{f}_x(\mathfrak{a}) \leqq A(x)+uB(x) \mid \mathfrak{a} \in \mathfrak{S}_0) = \Phi(u)+\mathcal{O}\left(\frac{\log^{\frac{1}{2}} B(x)}{B(x)}\right)$$

uniformly in $u \in \boldsymbol{R}$, as $x \to \infty$.

§ 9.2. CONCERNING THE BASIC LEMMA

Taking ψ as the function defined by (6.2), we have

(9.1)
$$M(x; \psi(x)) > \lambda x \prod_{N\mathfrak{p} \leqq \psi(x)} \left(1-\frac{1}{N\mathfrak{p}}\right)\left\{g(\alpha_1) - \frac{\mathscr{R}'_{\psi(x),\alpha}(x)}{\lambda x \prod_{N\mathfrak{p} \leqq \psi(x)} \left(1-\frac{1}{N\mathfrak{p}}\right)}\right\},$$

(see (5.58)).

We now separately consider

$$g(\alpha_1) \text{ and } \frac{\mathscr{R}'_{\psi(x),\alpha}(x)}{\lambda x \prod_{N\mathfrak{p} \leqq \psi(x)} \left(1-\frac{1}{N\mathfrak{p}}\right)}.$$

We are still to a certain extent free to choose the way in which $r(x) \to 0$ (as $x \to \infty$) and $\alpha_1 \to 1$.

We assume that δ is a function $\boldsymbol{R} \to \boldsymbol{R}$, such that $\delta(x) > 0$ and $\lim_{x\to\infty} \delta(x) = 0$ and $1+3\delta(x) < \sqrt{e}$, (see (5.10)).

We introduce:
$$\alpha_1 = 1+3\delta(x), \quad \alpha = 1+2\delta(x) \text{ and } \quad \alpha_0 = 1+\delta(x).$$

Because of the definition of $g(\alpha_1)$, see (5.50) and (5.11), we have

$$g(\alpha_1) = 1-\log \alpha_1 - \frac{\alpha_1(\frac{1}{2}e \log \alpha_1)^4}{1-\alpha_1(\frac{1}{2}e \log \alpha_1)^2},$$

and, therefore, it is clear that

$$g(1+3\delta(x)) = 1+\mathcal{O}(\delta(x)) \text{ as } x \to \infty. \tag{9.2}$$

In this case we can take instead of k in (5.15),

$$k(x) = \exp.\left(\frac{Q^*}{\delta(x)}\right), \; Q^* \text{ being some constant.}$$

From (3.9) and (5.59), it follows that there exists a constant $c_0 > 0$ and a value $X_0 \in \boldsymbol{R}$, such that, if $x > X_0$, we have

$$\frac{\mathscr{R}'_{\psi(x),\alpha}(x)}{\lambda x \prod\limits_{N\mathfrak{p} \leqq \psi(x)} \left(1-\frac{1}{N\mathfrak{p}}\right)} < \frac{c_0 \log \psi(x)}{\lambda x} 2^{k^\alpha(x)} \left\{\frac{f'\psi(x)}{\log \psi(x)}\right\}^{(\alpha+1)/(\alpha-1)} x^{1-2/(n+1)}.$$

Hence

(9.3)

$$\frac{\mathscr{R}'_{\psi(x),1+2\delta(x)}(x)}{\lambda x \prod\limits_{N\mathfrak{p} \leqq \psi(x)} \left(1-\frac{1}{N\mathfrak{p}}\right)} < \frac{c_0 r(x) \log x}{\lambda x^{2/(n+1)}} \cdot 2^{k^{1+2\delta(x)}(x)} \left\{\frac{f' x^{r(x)}}{r(x) \log x}\right\}^{1+1/\delta(x)}$$

In order to make it possible to conclude that the right-handside of this formula tends to zero, if x tends to infinity, it is clearly necessary that there exists $X_1 \in \boldsymbol{R}$, such that

$$\frac{r(x)}{\delta(x)} < \frac{2}{n+1} \text{ for } x > X_1.$$

Now, it will later become apparent that it is useful to define $r : \boldsymbol{R} \to \boldsymbol{R}$ by

$$r(x) = B^{-\frac{1}{2}}(x). \tag{9.4}$$

Therefore, we now define $\delta : \boldsymbol{R} \to \boldsymbol{R}$ by

$$(9.5) \quad \begin{cases} \delta(x) = (n+1)B^{-\frac{1}{2}}(x), \text{ if } x > X_2, \text{ where } X_2 \text{ is such that} \\ \qquad (n+1)B^{-\frac{1}{2}}(X_2) < \frac{1}{3}(\sqrt{e}-1), \\ \delta(x) = (n+1)B^{-\frac{1}{2}}(X_2), \text{ if } x \leqq X_2. \end{cases}$$

Substituting (9.4) and (9.5) in (9.2) and (9.3) respectively, we arrive at

$$g(1+3\delta(x)) = 1+\mathcal{O}(B^{-\frac{1}{2}}(x)) \tag{9.6}$$

and

$$\frac{\mathscr{R}'_{\psi(x),1+2\delta(x)}(x)}{\lambda x \prod_{N\mathfrak{p}\leqq\psi(x)} \left(1-\frac{1}{N\mathfrak{p}}\right)} = \mathcal{O}(x^{-1/2(n+1)}). \tag{9.7}$$

Hence, we may now conclude that there exists a constant c_3 such that, for every $x > X_3$ $(X_3 \in \boldsymbol{R})$,

$$M(x; \psi(x)) > \lambda x \prod_{N\mathfrak{p}\leqq\psi(x)} \left(1-\frac{1}{N\mathfrak{p}}\right) \{1-c_3 B^{-\frac{1}{2}}(x)\}. \tag{9.8}$$

Defining r and δ in the same way, similar considerations make it possible to show that, for some constant c_4 and $x > X_4$, the following also holds.

$$M(x; \psi(x)) < \lambda x \prod_{N\mathfrak{p}\leqq\psi(x)} \left(1-\frac{1}{N\mathfrak{p}}\right) \{1+c_4 B^{-\frac{1}{2}}(x)\}. \tag{9.9}$$

Combining (9.8) and (9.9) we finally obtain

$$M(x; \psi(x)) = \lambda x \prod_{N\mathfrak{p}\leqq\psi(x)} \left(1-\frac{1}{N\mathfrak{p}}\right) \{1+\mathcal{O}(B^{-\frac{1}{2}}(x))\}. \tag{9.10}$$

§ 9.3. CONCERNING LEMMA 2

We define $\Psi^* : \boldsymbol{R} \to \boldsymbol{R}$ by

$$\Psi^*(x) = x^{1/4(n+1)}. \tag{9.11}$$

As before, let E_i be defined by

$$E_i = \{\mathfrak{a} \in \mathfrak{S}_0 \,|\, \mathfrak{m}(\mathfrak{a}; x) = \mathfrak{n}_i(x) \text{ and } N\mathfrak{a} \leqq x\}, \text{ (see (6.6))},$$

$\mathfrak{n}_i(x)$ and $\mathfrak{m}(\mathfrak{a}; x)$ being defined as in § 6.

Since

$$\lim_{x\to\infty} \frac{x}{\Psi^*(x)(\psi(x))^\gamma} = \infty$$

for all real values of γ, the following result can be obtained.

If $N\mathfrak{n}_i(x) \leqq \Psi^*(x)$, then

$$P(\mathfrak{a} \in E_i \,|\, \mathfrak{S}_0) = \frac{1}{N\mathfrak{n}_i(x)} \prod_{N\mathfrak{p}\leqq\psi(x)} \left(1-\frac{1}{N\mathfrak{p}}\right) \{1+\mathcal{O}(B^{-\frac{1}{2}}(x))\} \tag{9.12}$$

uniformly in i.

This result is uniform in i, since (9.7) can be replaced in this case by

$$\frac{\mathscr{R}'_{\psi(x),1+2\delta(x)}(x)}{\lambda\dfrac{x}{N\mathfrak{n}_i(x)}\prod\limits_{N\mathfrak{p}\leqq\psi(x)}\left(1-\dfrac{1}{N\mathfrak{p}}\right)} = \mathcal{O}(x^{-1/4(n+1)}).$$

§ 9.4. CONCERNING LEMMA 3

Let we define ψ by (6.2), r by (9.4) and replace Ψ, defined by (6.3), by Ψ^*, defined by (9.11).

Let $L^*(z) = \# \{\mathfrak{a} \in I(R) \mid N\mathfrak{a} \leqq z \text{ and } N\mathfrak{m}(\mathfrak{a}; x) > \Psi^*(x)\}$, then there exists a constant b^*, such that

$$L^*(z) < b^* z B^{-\frac{1}{2}}(x). \tag{9.13}$$

The proof of formula (9.13) is analogous to that of (6.8).

§ 9.5. CONCERNING THEOREM 2

Using the results of the preceding paragraphs 9.1, 9.2, 9.3 and 9.4 it becomes clear that theorem 2 can be improved to:

THEOREM 2′.

Let $\mathfrak{f}$, $\mathfrak{f}_x$, A, B and Φ be defined as in theorem 2.

Let $\psi: \boldsymbol{R} \to \boldsymbol{R}$ be defined by $\psi(x) = x^{B^{-\frac{1}{2}}(x)}$.

If

$$\lim_{x\to\infty} B(x) = \infty,$$

then

$$P(\mathfrak{f}_{\psi(x)}(\mathfrak{a}) \leqq A(\psi(x)) + uB(\psi(x)) \mid \mathfrak{a} \in \mathfrak{S}_0 \text{ and } N\mathfrak{a} \leqq x) = \Phi(u) + \mathcal{O}(B^{-\frac{1}{2}}(x)) \text{ uniformly in } u \in \boldsymbol{R}. \tag{9.14}$$

§ 9.6. CONCERNING THEOREM 3

Again, let $r: \boldsymbol{R} \to \boldsymbol{R}$ be defined by (9.4); hence $r(x) = B^{-\frac{1}{2}}(x)$ and consequently $\psi(x) = x^{B^{-\frac{1}{2}}(x)}$. As proved in § 8, we have the following three inequalities:

$$|\mathfrak{f}(\mathfrak{a}) - \mathfrak{f}_{\psi(x)}(\mathfrak{a})| \leqq \frac{1}{r(x)}, \text{ if } N\mathfrak{a} \leqq x, \tag{8.4}$$

$$|A(x) - A(\psi(x))| < -a \log r(x) \text{ for some } a > 1, \tag{8.5}$$

$$|B(x) - B(\psi(x))| < \frac{-a \log r(x)}{2B(\psi(x))} \text{ for some } a > 1. \tag{8.6}$$

The inequality (8.4) will determine the rate of convergence.

Substituting in (8.4), (8.5) and (8.6), $r(x) = B^{-\frac{1}{2}}(x)$ and applying theorem 2′, we can obtain the following theorem in the same way as we proved theorem 3.

THEOREM 3′.

Let the same assumptions be made as in theorem 3. *Then*

(9.15) $$P(\mathfrak{f}(\mathfrak{a}) \leqq A(x)+uB(x) \mid \mathfrak{a} \in \mathfrak{S}_0 \text{ and } N\mathfrak{a} \leqq x) = \Phi(u)+\mathcal{O}(B^{-\frac{1}{2}}(x)) \text{ uniformly in } u \in \boldsymbol{R}, \text{ as } x \to \infty.$$

§ 10. Corollary

Let K be an algebraic numberfield over $\boldsymbol{Q}$, having only a finite number of units.

Let R be the ring of integers of K.

We define the probability-function P by

(10.1) $$P(E) = \lim_{x\to\infty} \frac{\# \{\xi \in E \mid N\xi \leqq x\}}{\# \{\xi \in R \mid N\xi \leqq x\}},$$

if the limit exists and $E \subset R$.

Analogously, we define the conditional probability by

(10.2) $$P(E_1 \mid E_2) = \lim_{x\to\infty} \frac{\# \{\xi \in E_1 \cap E_2 \mid N\xi \leqq x\}}{\# \{\xi \in E_2 \mid N\xi \leqq x\}},$$

if the limit exists and $E_1 \subset R$ and $E_2 \subset R$.

We define $\mathfrak{f}' : R \to \boldsymbol{R}$ by

(10.3) $\mathfrak{f}'(\xi) = \mathfrak{f}((\xi))$, where $\mathfrak{f} : I(R) \to \boldsymbol{R}$ is defined by (4.5) and (ξ) is the principal ideal generated by ξ.

As there is no question of confusion, we write $\mathfrak{f}$ instead of $\mathfrak{f}'$.

If an algebraic numberfield has only a finite number of units then the results obtained in the preceding sections, with respect to the set of principal ideals $\mathfrak{S}_0$, also hold with respect to the ring R. This is a consequence of the fact that for such an algebraic field each ideal of $\mathfrak{S}_0$ corresponds with a finite (constant) number of algebraic integers. As an example of such a field we mention the field of gaussian numbers.

Thus we can now state the following corollary.

COROLLARY.

Let K be an algebraic numberfield over $\boldsymbol{Q}$.

Let the number of units in K be finite.

Let $\mathfrak{f} : I(R) \to \boldsymbol{R}$ *be defined by* (4.5), *and* $\mathfrak{f} : R \to \boldsymbol{R}$ *by* $\mathfrak{f}(\xi) = \mathfrak{f}((\xi))$.

Let P *be defined by formulae* (10.1) *and* (10.2).

Let A, B *and* Φ *be defined as in theorem* 1.

If $\lim_{x\to\infty} B(x) = \infty$, *then*

$$(10.4)\quad P(\mathfrak{f}(\xi) \leqq A(x)+uB(x) \mid N\xi \leqq x) = \Phi(u)+\mathcal{O}(B^{-\frac{1}{2}}(x))$$
$$\text{uniformly in } u \in \boldsymbol{R}, \text{ as } x \to \infty.$$

Comment.

If in this corollary, we eliminate the assumption "The number of units in K is finite", then it no longer holds.

The difficulty which then rises is that, for fixed $x \in \boldsymbol{R}$, $\# \{\xi \in R \mid N\xi \leqq x\}$ is not finite in the case of infinity many units.

However, in the next chapter it will become apparent that it is possible to derive analogous theorems in an arbitrary algebraic numberfield if, in the definition of the probability-function P, we replace the condition, $N\xi \leqq x$, by $||\xi|| \leqq x^{1/n}$, $||\xi||$ being defined by $||\xi|| = \max_i |\xi^{(i)}|$ (see § 1, height).

If the number of units is finite, then the condition $||\xi|| \leqq x^{1/n}$, is obviously equivalent to, $N\xi \leqq x$.

CHAPTER 3

Sets of algebraic integers generated by polynomials with integral algebraic coefficients $\in R$ and the argument running through the ring R of integers of an algebraic numberfield

§ 11. Some introductory remarks and definitions

Let K be any algebraic numberfield of degree n relative to $\boldsymbol{Q}$.

Let R be the ring of integers of K and $I(R)$ the set of ideals of R, as before.

Let $G(X)$ be the polynomial

$$(11.1)\qquad G(X) = \sum_{j=0}^{m} \alpha_j X^j, \quad \alpha_j \in R, \quad \alpha_m \neq 0.$$

In this chapter R will be considered as the sample-space and the set-function P will be defined by

$$P(E) = \lim_{y\to\infty} \frac{\#\{\xi \in E \mid ||\xi|| \leqq y\}}{\#\{\xi \in R \mid ||\xi|| \leqq y\}}, \tag{11.2}$$

if the limit exists and $E \subset R$.

We recall that $||\xi||$ is the height of ξ, defined by

$$||\xi|| = \max |\xi^{(i)}|, \quad \xi \in R \text{ and } \xi^{(1)}, \ldots, \xi^{(n)} \tag{11.3}$$

are the n conjugates of ξ.

Further

$$P(E_1 \mid E_2) = \lim_{y\to\infty} \frac{\#\{\xi \in E_1 \cap E_2 \mid ||\xi|| \leqq y\}}{\#\{\xi \in E_2 \mid ||\xi|| \leqq y\}}, \tag{11.4}$$

if the limit exists and $E_1 \subset R$ and $E_2 \subset R$.

For each prime-ideal $\mathfrak{p} \in I(R)$ let $\pi_\mathfrak{p}$ be the canonical operator

$$\pi_\mathfrak{p} : R \to R_\mathfrak{p} = R/\mathfrak{p}, \tag{11.5}$$

and let $G_\mathfrak{p}$ be defined by

$$G_\mathfrak{p} \circ \pi_\mathfrak{p} = \pi_\mathfrak{p} \circ G, \quad \text{(Fig. 3)}. \tag{11.6}$$

$$\begin{tikzcd} R \arrow[r, "G"] \arrow[d, "\pi_\mathfrak{p}"'] & R \arrow[d, "\pi_\mathfrak{p}"'] \\ R_\mathfrak{p} \arrow[r, "G_\mathfrak{p}"] & R_\mathfrak{p} \end{tikzcd}$$

Fig. 3

We define

$$\nu_\mathfrak{p} = \#\{\Xi \in R_\mathfrak{p} \mid G_\mathfrak{p}(\Xi) = 0\}. \tag{11.7}$$

Obviously $\nu_\mathfrak{p}$ equals the number of mod $\mathfrak{p}$ different solutions of

$$G(\xi) \equiv 0 \bmod \mathfrak{p}, \quad \xi \in R. \tag{11.8}$$

Further we define $M : \boldsymbol{R} \to \boldsymbol{R}$ and $M_\mathfrak{p} : \boldsymbol{R} \to \boldsymbol{R}$ by

$$M(x) = \#\{\xi \in R \mid ||\xi|| \leqq x^{1/n}\} \tag{11.9}$$

and

$$M_\mathfrak{p}(x) = \#\{\xi \in R \mid G(\xi) \equiv 0 \bmod \mathfrak{p} \text{ and } ||\xi|| \leqq x^{1/n}\} \tag{11.10}$$

respectively.

Finally, we here state the following lemma.

LEMMA 4.

Let $g_1(X)$ and $g_2(X)$ be relatively prime polynomials with integral coefficients $\in R$.

Then for any prime-ideal $\mathfrak{p}$, except possibly for a finite number of prime-ideals, the two congruences $g_1(\xi) \equiv 0 \bmod \mathfrak{p}$ and $g_2(\xi) \equiv 0 \bmod \mathfrak{p}$ have no solution in common, $(\xi \in R)$.

Proof of lemma 4.

The resultant $\mathscr{R}$ of $g_1(\xi)$ and $g_2(\xi)$ is a non zero integer.

Let us suppose that the two congruences $g_1(\xi) \equiv 0 \bmod \mathfrak{p}$ and $g_2(\xi) \equiv 0 \bmod \mathfrak{p}$ have a common solution α.

Then:
$$g_1(\xi) \equiv (\xi-\alpha)\, g_1^*(\xi) \bmod \mathfrak{p}$$
and
$$g_2(\xi) \equiv (\xi-\alpha)\, g_2^*(\xi) \bmod \mathfrak{p},$$

where $g_1^*(X)$ and $g_2^*(X)$ are polynomials with integral coefficients $\in R$.

Let $\mathscr{R}^*$ be the resultant of $(\xi-\alpha)g_1^*(\xi)$ and $(\xi-\alpha)g_2^*(\xi)$, then $\mathscr{R}^* \equiv \mathscr{R} \bmod \mathfrak{p}$.

However $\mathscr{R}^*$ is obviously zero, and consequently, $\mathscr{R} \equiv 0 \bmod \mathfrak{p}$.

Thus, we see, that prime-ideals, for which $g_1(\xi) \equiv 0 \bmod \mathfrak{p}$ and $g_2(\xi) \equiv 0 \bmod \mathfrak{p}$ have a common solution, divide $\mathscr{R}$.

Hence they are finite in number, which completes the proof of lemma 4.

§ 12. Theorem 4

Let $\mathfrak{f} : I(R) \to \boldsymbol{R}$ be defined by (4.5) and $\rho_{\mathfrak{p}} : I(R) \to \boldsymbol{R}$ and $\mathfrak{f}_x : I(R) \to \boldsymbol{R}$ by (4.4) and (4.6) respectively. Throughout the chapters 3 and 4 we make the following convention.

CONVENTION.

Whenever we introduce a function $\mathfrak{f} : I(R) \to \boldsymbol{R}$, we shall also —implicitly or explicitly— introduce a function ${}_*\mathfrak{f} : R \to \boldsymbol{R}$, such that

$$(12.1) \qquad {}_*\mathfrak{f}(\xi) = \mathfrak{f}((\xi)),$$

(ξ) being the principal ideal generated by ξ.

Since R is the sample-space, ${}_*\mathfrak{f}$ is a random variable.

From the definitions of $\rho_{\mathfrak{p}}$, $\mathfrak{f}$ and $\mathfrak{f}_x$ it then follows that

$$(12.2) \qquad \begin{cases} {}_*\rho_{\mathfrak{p}}(\xi) = \mathfrak{f}(\mathfrak{p}), \text{ if } \xi \equiv 0 \bmod \mathfrak{p}, \\ {}_*\rho_{\mathfrak{p}}(\xi) = 0 \text{ in all other cases,} \end{cases}$$

$$(12.3) \qquad {}_*f = \sum_{\mathfrak{p}} {}_*\rho_{\mathfrak{p}}$$

and

$$(12.4) \qquad {}_*f_x = \sum_{N\mathfrak{p} \leqq x} {}_*\rho_{\mathfrak{p}}$$

respectively.

We define $A : \boldsymbol{R} \to \boldsymbol{R}$ and $B : \boldsymbol{R} \to \boldsymbol{R}$ by

$$(12.5) \qquad A(x) = \sum_{N\mathfrak{p} \leqq x} \nu_{\mathfrak{p}} \frac{f(\mathfrak{p})}{N\mathfrak{p}}$$

and

$$(12.6) \qquad B(x) = \left[\sum_{N\mathfrak{p} \leqq x} \nu_{\mathfrak{p}} \frac{f^2(\mathfrak{p})}{N\mathfrak{p}}\right]^{\frac{1}{2}}$$

respectively, $\nu_{\mathfrak{p}}$ being defined by (11.7).

We shall prove:

THEOREM 4.

Let ${}_*f_x$, $G(X)$, A, B *and* Φ *be defined by* (12.4), (11.1), (12.5), (12.6) *and* (4.9) *respectively.*

If $\lim_{x\to\infty} B(x) = \infty$, *then*

$$(12.7) \quad P({}_*f_x(G(\xi)) \leqq A(x)+uB(x)) = \Phi(u)+\mathcal{O}\left(\frac{\log^{\frac{1}{2}} B(x)}{B(x)}\right)$$

uniformly in $u \in \boldsymbol{R}$.

Proof of theorem 4.

Following the definition of P, formula (11.2), we have for any given prime-ideal $\mathfrak{p}$,

$$P({}_*\rho_{\mathfrak{p}}(G(\xi)) = f(\mathfrak{p})) = \lim_{y\to\infty} \frac{\#\{\xi \in R \mid G(\xi) \equiv 0 \bmod \mathfrak{p} \text{ and } ||\xi|| \leqq y\}}{\#\{\xi \in R \mid ||\xi|| \leqq y\}}.$$

Using the definitions (11.9) and (11.10), we obtain

$$P({}_*\rho_{\mathfrak{p}}(G(\xi)) = f(\mathfrak{p})) = \lim_{x\to\infty} \frac{M_{\mathfrak{p}}(x)}{M(x)}.$$

From Rieger [16], see also formula (3.6), we have

$$(12.8) \qquad M(x) = cx+\mathcal{O}(x^{1-1/n}),$$

c being a constant only dependent on the field K.

The number of prime-ideals $\mathfrak{p}$, for which the congruence $G(\xi) \equiv 0 \bmod \mathfrak{p}$ holds for every $\xi \in R$, is obviously finite.

If $\mathfrak{p}$ is a prime-ideal such that the congruence $G(\xi) \equiv 0 \bmod \mathfrak{p}$ is not true for every $\xi \in R$, then the following formula holds:

$$M_{\mathfrak{p}}(x) = c\,\frac{\nu_{\mathfrak{p}}}{N\mathfrak{p}}\,x+\mathcal{O}(x^{1-1/n}). \tag{12.9}$$

In order to prove this let $\Xi \in R_{\mathfrak{p}} = R/\mathfrak{p}$.

Take some ξ_0 with $\xi_0 \in \Xi$.

$$\#(\xi \in \Xi \mid ||\xi|| \leqq x^{1/n}\} = \#\{\xi \in R \mid \xi \equiv \xi_0 \bmod \mathfrak{p} \text{ and } ||\xi|| \leqq x^{1/n}\}$$
$$= \frac{c}{N\mathfrak{p}}\,x+\mathcal{O}(x^{1-1/n}), \text{ see formula (3.6).}$$

From this and from the definition of $\nu_{\mathfrak{p}}$, formula (12.9) immediately follows.

In the same way as we proved theorem 1, the proof of theorem 4 can now be completed.

§ 13. Some lemmas

LEMMA 5.

If the polynomial $G(X)$, *defined by* (11.1) *is irreducible in* K, *then*

$$\sum_{N\mathfrak{p}\leqq x} \nu_{\mathfrak{p}}\,\frac{\log N\mathfrak{p}}{N\mathfrak{p}} = \log x+\mathcal{O}(1), \tag{13.1}$$

$\nu_{\mathfrak{p}}$ *being defined by* (11.7).

Proof of lemma 5.

Let $K(\vartheta)$ be the algebraic field of degree m relative to K, where ϑ is a root of $G(\xi) = 0$, G being defined by (11.1) and assumed to be irreducible in K. For convenience, we put

$$\begin{cases} N = |\mathcal{N}_{K/Q}|, \\ N_{(2,1)} = |\mathcal{N}_{K(\vartheta)/K}|, \\ N_{(2,0)} = |\mathcal{N}_{K(\vartheta)/Q}|. \end{cases} \tag{13.2}$$

We recall the definition of $\mathcal{N}_{K_1/K_2}$, given in the introduction: $\mathcal{N}_{K_1/K_2}$ is the norm defined on the ideals and integers of the field K_1 relative to the field K_2.

We denote prime-ideals of $K(\vartheta)$ by $\mathfrak{P}$ and prime-ideals of K by $\mathfrak{p}$.

From formula (3.7), preliminaries, we have

$$\sum_{N_{(2,0)}\mathfrak{P}\leqq x} \frac{\log N_{(2,0)}\mathfrak{P}}{N_{(2,0)}\mathfrak{P}} = \log x+\mathcal{O}(1). \tag{13.3}$$

Let $\nu_{\mathfrak{p}}^{(r)}$, $1 \leqq r \leqq m$, be the number of prime-ideals $\mathfrak{P}$ of degree r relative to K, which divide $\mathfrak{p}$.

Prime-ideals $\mathfrak{P}$ of relative degree r will be denoted by $\mathfrak{P}_{(r)}$. Clearly

$$(13.4)\qquad \sum_{N_{(2,0)}\mathfrak{P}\leqq x} \frac{\log N_{(2,0)}\mathfrak{P}}{N_{(2,0)}\mathfrak{P}} = \sum_{r=1}^{m} \sum_{N_{(2,0)}\mathfrak{P}_{(r)}\leqq x} \frac{\log N_{(2,0)}\mathfrak{P}_{(r)}}{N_{(2,0)}\mathfrak{P}_{(r)}}.$$

Because $N_{(2,0)}\mathfrak{P}_{(r)} = N(N_{(2,1)}\mathfrak{P}_{(r)})$, we have

$$\sum_{N_{(2,0)}\mathfrak{P}\leqq x} \frac{\log N_{(2,0)}\mathfrak{P}}{N_{(2,0)}\mathfrak{P}} = \sum_{r=1}^{m} \sum_{N\mathfrak{p}\leqq x^{1/r}} \nu_{\mathfrak{p}}^{(r)} \frac{\log N\mathfrak{p}^r}{N\mathfrak{p}^r}.$$

Clearly $\nu_{\mathfrak{p}}^{(r)} \leqq m$ and hence, for $r \geqq 2$,

$$\sum_{N\mathfrak{p}\leqq x^{1/r}} \nu_{\mathfrak{p}}^{(r)} r \frac{\log N\mathfrak{p}}{N\mathfrak{p}^r}$$

is convergent, as $x \to \infty$.

Thus from (13.3) it can be concluded that

$$(13.5)\qquad \sum_{N\mathfrak{p}\leqq x} \nu_{\mathfrak{p}}^{(1)} \frac{\log N\mathfrak{p}}{N\mathfrak{p}} = \log x + \mathcal{O}(1).$$

We recall the definition of $\nu_{\mathfrak{p}}$, i.e. the number of mod $\mathfrak{p}$ different solutions of $G(\xi) \equiv 0 \bmod \mathfrak{p}$, $\xi \in R$. From Dedekind [5], it follows that $\nu_{\mathfrak{p}} = \nu_{\mathfrak{p}}^{(1)}$, as long as $\mathfrak{p}$ does not divide the relative different of the number ϑ of the field $K(\vartheta)$.

Applying this, (13.1) follows from (13.5).

Corollary.

From lemmas 4 and 5 it follows that, if $G(X)$ is the product of powers of t different in K irreducible polynomials, formula (13.1) *becomes*:

$$(13.6)\qquad \sum_{N\mathfrak{p}\leqq x} \nu_{\mathfrak{p}} \frac{\log N\mathfrak{p}}{N\mathfrak{p}} = t\log x + \mathcal{O}(1).$$

From formula (13.6) it can be deduced that also the following two formulae hold:

$$(13.7)\qquad \sum_{N\mathfrak{p}\leqq x} \frac{\nu_{\mathfrak{p}}}{N\mathfrak{p}} = t \operatorname{loglog} x + C_* + \mathcal{O}\left(\frac{1}{\log x}\right),$$

where C_* is a constant and

$$(13.8)\qquad \prod_{N\mathfrak{p}\leqq x}\left(1-\frac{\nu_{\mathfrak{p}}}{N\mathfrak{p}}\right) = \frac{\kappa}{(\log x)^t}\left(1+\mathcal{O}\left(\frac{1}{\log x}\right)\right),$$

κ being a positive constant.

We now state the following lemma.

LEMMA 6.

Let $r : \boldsymbol{R} \to \boldsymbol{R}$ *be such that*

$$\lim_{x\to\infty} r(x) = 0, \tag{13.9}$$

and let $\psi : \boldsymbol{R} \to \boldsymbol{R}$ *be defined by*

$$\psi(x) = x^{r(x)}. \tag{13.10}$$

Putting

$$M(x;m) = \#\{\xi \in R \mid ||\xi|| \leqq x^{1/n} \text{ and } (\mathfrak{p} \mid G(\xi) \to N\mathfrak{p} > m)\}, \tag{13.11}$$

then

$$M(x;\psi(x)) = M(x) \prod_{N\mathfrak{p}\leqq\psi(x)} \left(1 - \frac{\nu_{\mathfrak{p}}}{N\mathfrak{p}}\right) (1+\mathcal{O}(r(x))). \tag{13.12}$$

Formulae (13.7) and (13.8) imply that the algorithm applied in the proof of the basic lemma (§ 5), can again be applied. Taking into account the considerations concerning the rate of convergence in § 9.2, it can be seen that formula (13.12) holds indeed.

Further we can prove the following lemma in the same way as we proved lemma 3.

LEMMA 7.

Let $\psi : \boldsymbol{R} \to \boldsymbol{R}$ *be defined by* (13.10).

For every $\xi \in R$, *let the ideal* $\mathfrak{m}(\xi; x)$ *be defined by*

$$\begin{cases} \mathfrak{m}(\xi; x) \mid (\xi), \\ \mathfrak{p} \mid \mathfrak{m}(\xi; x) \to N\mathfrak{p} \leqq \psi(x), \\ \mathfrak{p} \mid \dfrac{(\xi)}{\mathfrak{m}(\xi; x)} \to N\mathfrak{p} > \psi(x). \end{cases} \tag{13.13}$$

According to § 9.3, *let* $\Psi^* : \boldsymbol{R} \to \boldsymbol{R}$ *be defined by*

$$\Psi^*(x) = x^{1/8n}. \tag{13.14}$$

Then, for some positive constant b

$$\#\{\xi \in R \mid ||\xi|| \leqq z^{1/n} \text{ and } N\mathfrak{m}(G(\xi); x) > \Psi^*(x)\} < bzr(x). \tag{13.15}$$

§ 14. Theorem 5

The preceding results now enable us to prove the following theorem.

THEOREM 5.

Let $_*\mathfrak{f}$, $G(X)$, A, B *and* Φ *be defined by* (12.3), (11.1), (12.5), (12.6) *and* (4.9) *respectively.*

If
$$\lim_{x\to\infty} B(x) = \infty,$$
then

$$(14.1)\quad P({}_*\mathfrak{f}(G(\xi)) \leqq A(x)+uB(x) \,|\, ||\xi|| \leqq x^{1/n}) = \Phi(u)+\mathcal{O}(B^{-\frac{1}{2}}(x))$$
uniformly in $u \in \boldsymbol{R}$, *as* $x \to \infty$.

Proof of theorem 5.

In the same way as we proved formula (9.14) of theorem 2′, we can prove

$$(14.2)\quad P({}_*\mathfrak{f}_{\psi(x)}(G(\xi)) \leqq A(\psi(x))+uB(\psi(x)) \,|\, ||\xi|| \leqq x^{1/n}) = \Phi(u)+\mathcal{O}\left(\frac{\log^{\frac{1}{2}} B(x)}{B(x)}\right)+\mathcal{O}(r(x))$$
uniformly in $u \in \boldsymbol{R}$, as $x \to \infty$.

Analogously to formulae (8.4), (8.5) and (8.6), we have for every $\xi \in R$ with $||\xi|| \leqq x^{1/n}$

$$(14.3)\qquad |{}_*\mathfrak{f}(G(\xi))-{}_*\mathfrak{f}_{\psi(x)}(G(\xi))| \leqq \frac{m+1}{r(x)},$$
m being the degree of $G(X)$,

$$(14.4)\qquad |A(x)-A(\psi(x))| \leqq -d\log r(x) \text{ with } d > 1$$

and

$$(14.5)\qquad |B(x)-B(\psi(x))| \leqq -\frac{d\log r(x)}{2B(\psi(x))} \text{ with } d > 1.$$

The inequality (14.3) will determine the rate of convergence.

If we put $r(x) = B^{-\frac{1}{2}}(x)$, then formula (14.1) immediately follows, completing the proof of theorem 5.

We note that the constant in the $\mathcal{O}$-term of formula (14.1) depends on the degree of $G(X)$.

CHAPTER 4

Sets of integers generated by polynomials with integral algebraic coefficients and the argument running through the ring of rational integers

§ 15. Introduction

As before, let K be an algebraic numberfield of degree n over the rational numberfield $\boldsymbol{Q}$, R the ring of algebraic integers of K, $I(R)$ the set of ideals of R and $\boldsymbol{Z}$ the ring of rational integers.

Let $G(X)$ be defined by (11.1) and the set-function P by (11.2) and (11.4), R being the sample-space. In the following two sections (§§ 16 and 17) we shall prove that for appropriate definitions of A: $\boldsymbol{R} \to \boldsymbol{R}$ and B: $\boldsymbol{R} \to \boldsymbol{R}$, theorems like theorems 4 and 5 also hold on the subset $\boldsymbol{Z}$ of R.

We shall call these theorems: theorem 6 and theorem 7 respectively.

In order to elucidate the underlying idea of this chapter we give the following comment.

Let $G(X)$ be an irreducible polynomial of degree m over $\boldsymbol{Z}$. If we consider the set of rational integers generated by this polynomial, if the argument runs through $\boldsymbol{Z}$, we could reason as follows.

Let K be the splitting-field of $G(X)$ over $\boldsymbol{Q}$.

In K, we have: $G(X) = \prod_{i=1}^{m} (X-\vartheta_i)$.

Studying the prime-divisors of $r-\vartheta_1$, if $r \in \boldsymbol{Z}$, we could hope to get information about the prime-divisors of $G(r)$, $(r \in \boldsymbol{Z})$.

However, in this chapter it will become apparent that instead of using properties of $r-\vartheta_1$ to deduce properties of $G(r)$, we want properties of $G(r)$ if we wish to prove the theorem of Erdös and Kac [6] on sets generated by $r-\vartheta_1$ $(r \in \boldsymbol{Z})$.

In order to have some idea about the type of sets on which we shall prove theorems like that of Erdös and Kac in this chapter, we consider an example.

Let K be the field of gaussian numbers; hence $K = \boldsymbol{Q}(i)$.

Let $G(X)$ be a polynomial over the ring of integers of K. We have $G(X) = G_1(X)+iG_2(X)$, where $G_1(X)$ and $G_2(X)$ are polynomials over $\boldsymbol{Z}$.

If we wish to prove the theorem of Erdös and Kac on the set generated by $G(r)$ if r runs through $\boldsymbol{Z}$, we ask for the asymptotic behaviour of the distribution of an additive function $\mathfrak{f}$ on the lattice-points in the complex plane having coordinates $G_1(r)$ and $G_2(r)$, $r \in \boldsymbol{Z}$, respectively.

§ 16. Theorem 6

We will denote arbitrary positive rational prime-numbers by p and q.

For each prime-ideal $\mathfrak{p} \in I(R)$ let $\pi_{\mathfrak{p}}$ be the canonical operator

$$(16.1) \qquad \pi_{\mathfrak{p}} : R \to R_{\mathfrak{p}} = R/\mathfrak{p}, \text{ as before}$$

and for each prime-number p let π_p be the canonical operator

$$(16.2) \qquad \pi_p : \boldsymbol{Z} \to \boldsymbol{Z}_p = \boldsymbol{Z}/p.$$

If $\mathfrak{p}$ lies above p, then $G_{\mathfrak{p}} : \boldsymbol{Z}_p \to R_{\mathfrak{p}}$ is defined by

$$(16.3) \qquad G_{\mathfrak{p}} \circ \pi_p = \pi_{\mathfrak{p}} \circ G, \text{ (Fig. 4).}$$

$$\begin{tikzcd}
Z \arrow[r, "G"] \arrow[d, "\pi_p"'] & R \arrow[d, "\pi_{\mathfrak{p}}"] \\
Z_p \arrow[r, "G_{\mathfrak{p}}"] & R_{\mathfrak{p}}
\end{tikzcd}$$

Fig. 4

Now we define $\nu_{\mathfrak{p}}$ by

$$(16.4) \qquad \nu_{\mathfrak{p}} = \# \{U \in \boldsymbol{Z}_p \mid G_{\mathfrak{p}}(U) = 0 \text{ and } \mathfrak{p} \mid p\}.$$

As before, for $y \in \boldsymbol{R}$, let

$$(16.5) \qquad [y] = \# \{r \in \boldsymbol{Z} \mid r > 0 \text{ and } r \leqq y\}.$$

Defining $h_{\mathfrak{p}} : \boldsymbol{R} \to \boldsymbol{R}$ by

$$(16.6) \qquad h_{\mathfrak{p}}(x) = \# \{r \in \boldsymbol{Z} \mid G(r) \equiv 0 \bmod \mathfrak{p} \text{ and } |r| \leqq x\},$$

it is clear that

$$(16.7) \qquad h_{\mathfrak{p}}(x) = \nu_{\mathfrak{p}} \frac{2x}{p} + \mathcal{O}(1),$$

where $\mathfrak{p}$ lies above p.

We prove the following lemma.

Lemma 8.

For each pair of prime-ideals $\mathfrak{p} \subset R$ and $\mathfrak{q} \subset R$, which lies above a pair of different rational prime-numbers p and q respectively $(p \neq q)$, the following formula holds.

$$(16.8)\qquad \# \{r \in \boldsymbol{Z} \mid G(r) \equiv 0 \bmod \mathfrak{p}\mathfrak{q} \text{ and } |r| \leqq x\} = \frac{2\nu_{\mathfrak{p}}\nu_{\mathfrak{q}}}{pq}x + \mathcal{O}(1).$$

Proof of lemma 8.

Let r_1 be a solution of $G(r) \equiv 0 \bmod \mathfrak{p}$ and r_2 be a solution of $G(r) \equiv 0 \bmod \mathfrak{q}$, with $r \in \boldsymbol{Z}$. As is well-known there exists a $r \in \boldsymbol{Z}$, which is mod pq uniquely determined such that

$$\begin{cases} r \equiv r_1 \bmod p, \\ r \equiv r_2 \bmod q. \end{cases}$$

Hence $G(r) \equiv 0 \bmod \mathfrak{p}$ and $G(r) \equiv \bmod \mathfrak{q}$, and therefore

$$G(r) \equiv 0 \bmod \mathfrak{p}\mathfrak{q}.$$

From this it follows that there are mod pq, and hence also mod $\mathfrak{p}\mathfrak{q}$, $\nu_{\mathfrak{p}}\nu_{\mathfrak{q}}$ different solutions of

$$G(r) \equiv 0 \bmod \mathfrak{p}\mathfrak{q}, \quad r \in \boldsymbol{Z}.$$

This result immediately gives rise to formula (16.8).

Comment. We draw attention to the fact that, if $p = q$ and $\mathfrak{p} \neq \mathfrak{q}$, formula (16.8) *no longer holds.*

Example: Let K be the field of gaussian numbers and let us consider the polynomial $G(X) = X-(2+i)$.

If $r \in \boldsymbol{Z}$, we have: $\begin{cases} r-(2+i) \equiv 0 \bmod (4+i) \rightarrow r \equiv -2 \bmod 17, \\ r-(2+i) \equiv 0 \bmod (4-i) \rightarrow r \equiv 6 \bmod 17. \end{cases}$

However, there is no rational solution of $r-(2+i) \equiv 0 \bmod 17$.

Let $\mathfrak{f}$ and ${}_*\mathfrak{f}$ be defined on $I(R)$ and R respectively, as in chapter 3, § 12.

Hence

$$\mathfrak{f}(\mathfrak{a}) = \sum_{\mathfrak{p} \mid \mathfrak{a}} \mathfrak{f}(\mathfrak{p}), \quad \mathfrak{a} \in I(R),$$

$$|\mathfrak{f}(\mathfrak{p})| \leqq 1 \text{ for every prime-ideal } \mathfrak{p},$$

$$\text{and} \quad {}_*\mathfrak{f}(\xi) = \mathfrak{f}((\xi)), \quad \xi \in R,$$

(ξ) being the principal ideal generated by ξ.

Further, ${}_*\rho_{\mathfrak{p}} : R \rightarrow \boldsymbol{R}$ is defined by

$$(16.9)\qquad \begin{cases} {}_*\rho_{\mathfrak{p}}(\xi) = \mathfrak{f}(\mathfrak{p}) \text{ if } \xi \equiv 0 \bmod \mathfrak{p}, \\ {}_*\rho_{\mathfrak{p}}(\xi) = 0 \text{ for all other cases.} \end{cases}$$

For every rational prime-number p we define $\Lambda_p : R \rightarrow \boldsymbol{R}$ by

(16.10) $$\Lambda_p(\xi) = \sum_{\mathfrak{p}|p} {}_*\rho_{\mathfrak{p}}(\xi).$$

Hence we have

(16.11) $$_*\mathfrak{f} = \sum_p \sum_{\mathfrak{p}|p} {}_*\rho_{\mathfrak{p}} = \sum_p \Lambda_p.$$

Now from lemma 8 it follows that, with respect to the subset $\boldsymbol{Z}$ of R the $\Lambda_p \circ G$ are mutually independent random variables.

We define

(16.12) $$_*\mathfrak{f}_x = \sum_{p \leqq x} \Lambda_p.$$

Let $\nu_{\mathfrak{p}}$ be defined by (16.4) and $\nu_{\mathfrak{p}\mathfrak{q}}$ by

(16.13) $$\begin{cases} \nu_{\mathfrak{p}\mathfrak{q}} = \# \{U \in \boldsymbol{Z}_p \mid G_{\mathfrak{p}}(U) = 0 \text{ and } G_{\mathfrak{q}}(U) = 0\}, \\ \qquad\qquad\qquad \text{if } \mathfrak{p} \neq \mathfrak{q},\ \mathfrak{p} \mid p \text{ and } \mathfrak{q} \mid p, \\ \nu_{\mathfrak{p}\mathfrak{q}} = 0 \text{ for all other cases.} \end{cases}$$

Now, it becomes apparent that

(16.14) $$\mathscr{E}(\Lambda_p \circ G \backslash \boldsymbol{Z}) = \frac{1}{p} \sum_{\mathfrak{p}|p} \nu_{\mathfrak{p}} \mathfrak{f}(\mathfrak{p})$$

and

(16.15) $$\mathscr{E}((\Lambda_p \circ G)^2 \backslash \boldsymbol{Z}) = \frac{1}{p} [\sum_{\mathfrak{p}|p} \nu_{\mathfrak{p}} \mathfrak{f}^2(\mathfrak{p}) + \sum_{\substack{\mathfrak{p}|p \\ \mathfrak{q}|p}} \nu_{\mathfrak{p}\mathfrak{q}} \mathfrak{f}(\mathfrak{p}) \mathfrak{f}(\mathfrak{q})],$$

where we denote the expectation of the stochastic variable $\Lambda_p \circ G$ on $\boldsymbol{Z}$ by $\mathscr{E}(\Lambda_p \circ G \backslash \boldsymbol{Z})$.

We now define $A : \boldsymbol{R} \to \boldsymbol{R}$ and $B : \boldsymbol{R} \to \boldsymbol{R}$ by

(16.16) $$A(x) = \sum_{p \leqq x} \sum_{\mathfrak{p}|p} \frac{\nu_{\mathfrak{p}}}{p} \mathfrak{f}(\mathfrak{p})$$

and

(16.17) $$B(x) = \left[\sum_{p \leqq x} \sum_{\mathfrak{p}|p} \frac{\nu_{\mathfrak{p}}}{p} \mathfrak{f}^2(\mathfrak{p}) + \sum_{p \leqq x} \sum_{\substack{\mathfrak{p}|p \\ \mathfrak{q}|p}} \frac{\nu_{\mathfrak{p}\mathfrak{q}}}{p} \mathfrak{f}(\mathfrak{p}) \mathfrak{f}(\mathfrak{q}) \right]^{\frac{1}{2}}.$$

Without any difficulty, it can now be verified that —with respect to the stochastic variable $_*\mathfrak{f}_x \circ G$ on $\boldsymbol{Z}$— the conditions of the central limit-theorem ($\mathscr{L}'$) are satisfied if, as before, it is assumed that $\lim_{x \to \infty} B(x) = \infty$.

Applying ($\mathscr{L}'$), we obtain:

THEOREM 6.

Let $_*\mathfrak{f}_x : R \to \boldsymbol{R}$ *be defined by* (16.12).

Let A, B, $G(X)$ and Φ be defined by (16.16), (16.17), (11.1), *and* (4.9) *respectively.*

Assume $\mathfrak{f}$ satisfies the conditions (4.3).

If $\lim_{x\to\infty} B(x) = \infty$, *then*

$$(16.18) \qquad P\left({}_*\mathfrak{f}_x(G(\xi)) \leqq A(x)+uB(x) \mid \xi \in \boldsymbol{Z}\right) = \Phi(u)+\mathcal{O}\left(\frac{\log^{\frac{1}{2}} B(x)}{B(x)}\right)$$

uniformly in $u \in \boldsymbol{R}$, as $x \to \infty$.

§ 17. Theorem 7

The aim of this section is to prove the following theorem.

THEOREM 7.

Let ${}_*\mathfrak{f}$, $G(X)$, A, B and Φ be defined by (12.3), (11.1), (16.16), (16.17) *and* (4.9) *respectively.*

If $\lim_{x\to\infty} B(x) = \infty$, *then*

$$(17.1) \qquad P\left({}_*\mathfrak{f}(G(\xi)) \leqq A(x)+uB(x) \mid \xi \in \boldsymbol{Z} \text{ and } |\xi| \leqq x\right) = \Phi(u)+\mathcal{O}\left(B^{-\frac{1}{2}}(x)\right)$$

uniformly in $u \in \boldsymbol{R}$, as $x \to \infty$.

In order to derive this theorem from theorem 6 we require lemmas similar to 1, 2 and 3, and a theorem on the lines of theorem 2.

The essential point is to realize that the reasoning of the basic lemma can again be applied.

For every rational prime-number p, we define

$$(17.2) \qquad \nu_p = \# \{U \in \boldsymbol{Z}_p \mid G_\mathfrak{p}(U) = 0 \text{ for at least one } \mathfrak{p} \text{ above } p\}.$$

Firstly, for the sake of convenience, suppose that

$$(17.3) \qquad G(X) = X - \vartheta, \quad \vartheta \in R.$$

Let

$$(17.4) \qquad J(X) = X^s + a_{s-1}X^{s-1} + \ldots + a_1 X + a_0$$

be the irreducible polynomial over $\boldsymbol{Q}$ with coefficients $a_j \in \boldsymbol{Z}$, such that $J(\vartheta) = 0$.

Define

$$(17.5) \qquad \nu_p^* = \# \{U \in \boldsymbol{Z}_p \mid J_p(U) = 0\},$$

J_p being defined by

$$J_p \circ \pi_p = \pi_p \circ J. \tag{17.6}$$

Obviously

$$\nu_p = \nu_p^*, \tag{17.7}$$

as firstly $G_{\mathfrak{p}}(U) = 0 \to J_p(U) = 0$ and
secondly $J_p(U) = 0 \to G_{\mathfrak{p}}(U) = 0$ for at least one $\mathfrak{p}$ above p.

Applying results of § 13, (formulae (13.6), (13.7) and (13.8)), we obtain

LEMMA 9.

If $G(X)$ is defined by (17.3) and ν_p by (17.2), then the following three formulae hold.

$$\sum_{p \leq x} \frac{\nu_p}{p} \log p = \log x + \mathcal{O}(1), \tag{17.8}$$

$$\sum_{p \leq x} \frac{\nu_p}{p} = \operatorname{loglog} x + D + \mathcal{O}\left(\frac{1}{\log x}\right), \tag{17.9}$$

where D is a constant,

$$\prod_{p \leq x} \left(1 - \frac{\nu_p}{p}\right) = \frac{a_0}{\log x}\left(1 + \mathcal{O}\left(\frac{1}{\log x}\right)\right), \tag{17.10}$$

where a_0 is a positive constant.

Now suppose

$$G(X) = X^m + \alpha_{m-1}X^{m-1} + \ldots + \alpha_1 X + \alpha_0 \tag{17.11}$$

is irreducible over K, $\alpha_j \in R$.

Consider then the splittingfield of $G(X)$; this field will be denoted by K_1.

In $K_1 : G(X) = \prod_{j=1}^{m} (X - \vartheta^{(j)})$, where the $\vartheta^{(j)}$ are the m conjugates.

Denoting prime-ideals of K by $\mathfrak{p}$ and prime-ideals of K_1 by $\mathfrak{P}$ we have,

$$\mathfrak{p} \mid G(r),\ r \in \mathbf{Z} \to \mathfrak{P} \mid G(r) \to \mathfrak{P} \mid r - \vartheta^{(1)}$$
$$\text{for at least one } \mathfrak{P} \text{ above } \mathfrak{p}.$$

Define

$$\nu_p' = \#\{U \in \mathbf{Z}_p \mid (r \in U \to (r - \vartheta^{(1)} \equiv 0 \bmod \mathfrak{P} \text{ for at least one } \mathfrak{P} \text{ above } \mathfrak{p}))\}. \tag{17.12}$$

Clearly, if $G(X)$ is defined by (17.11) and ν_p by (17.2) —with respect to $G(X)$ in (17.11) we have $\nu_p' = \nu_p$.

Hence formulae (17.8), (17.9) and (17.10) also hold, if $G(X)$ is defined by (17.11).

It is apparent that for these formulae, it is not essential that the coefficient of X^m in $G(X)$ equals 1.

Therefore lemma 9 can be improved to

Lemma 10.

If $G(X) = \alpha_m X^m + \alpha_{m-1} X^{m-1} + \ldots + \alpha_1 X + \alpha_0$ *is irreducible over* K, $\alpha_i \in R$, *and if* $v_p = \# \{U \in Z_p \mid G_{\mathfrak{p}}(U) = 0$ *for at least one* $\mathfrak{p}$ *above* $p\}$, *then*

$$\begin{cases} \displaystyle\sum_{p \leq x} \frac{v_p}{p} \log p = \log x + \mathcal{O}(1), \\ \displaystyle\sum_{p \leq x} \frac{v_p}{p} = \operatorname{loglog} x + D + \mathcal{O}\left(\frac{1}{\log x}\right), \\ \qquad\qquad\qquad \textit{where } D \textit{ is a constant}, \\ \displaystyle\prod_{p \leq x} \left(1 - \frac{v_p}{p}\right) = \frac{a_0}{\log x}\left(1 + \mathcal{O}\left(\frac{1}{\log x}\right)\right), \\ \qquad\qquad\qquad a_0 \textit{ being a positive constant.} \end{cases}$$

Furthermore, owing to lemma 4 (§ 11), formulae analogous to those in lemma 9 and lemma 10 (see also formulae (13.6), (13.7) and (13.8)) can be proved for an arbitrary polynomial $G(X)$, which is not necessarily irreducible.

The proof of theorem 7 is now analogous to that of theorem 3, except that we have to take some care concerning those prime-ideals $\mathfrak{p}$ that divide the discriminant of the field K or the discriminant of the polynomial $G(X)$.

We comment that the reasoning applied in § 9, concerning the rate of convergence, again holds here. This completes the proof of theorem 7.

As in the preceding chapter the $\mathcal{O}$-term of formula (17.1) depends on the degree of $G(X)$.

It can be noted that the theorems of this chapter also hold if the argument of the polynomial $G(X)$ runs through the ring T of integers of an arbitrary algebraic numberfield K_0 which is contained in K.

CHAPTER 5

The ring $F_q[X]$ of polynomials over the finite field F_q of q elements

§ 18. Introduction

The above mentioned set may be regarded as analogous to the set of rational integers.

In the subsequent paragraphs, 19 and 20, it will become apparent that the theorem of Erdös and Kac [7] also holds on the set $F_q[X]$.

One of the most interesting aspects concerning $F_q[X]$ is that — as a consequence of its simple structure — the pıoof of the basic lemma (§ 5) is quite easy and straightforward in contrast to the case of rational integers, where the proof of the basic lemma is very tedious and complicated.

Elements of $F_q[X]$ are denoted by $a(x)$, $b(x)$, etc. As is well-known every ideal of $F_q[X]$ is a principal ideal.

As before, integral ideals are denoted by Gothic letters such as $\mathfrak{a}$, $\mathfrak{b}$ etc. Since any ideal is a principal ideal we have $\mathfrak{a} = (a(x))$, where $a(x)$ is the generating polynomial of the principal ideal $(a(x))$. To each ideal $\mathfrak{a} = (a(x))$ we join the polynomial $a(x)$ whose highest coefficient is equal to 1.

Prime-ideals are denoted by $\mathfrak{p}$, $\mathfrak{q}$, etc. or by $(p(x))$, $(q(x))$ etc.

The set of all ideals of $F_q[X]$ is denoted by $\{F_q[X]\}$.

We also recall some elementary definitions and properties.

The norm $N : \{F_q[X]\} \to R$ is defined by

(18.1) $N\mathfrak{a} =$ the number of classes of residues mod $\mathfrak{a}$.

We also write: $Na(x) = N(a(x))$.

If $a(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, then

$$Na(x) = q^n. \tag{18.2}$$

We define

$$\mathcal{N}(m) = \#\{\mathfrak{a} \in \{F_q[X]\} \mid N\mathfrak{a} = q^m\}. \tag{18.3}$$

We have

$$\mathcal{N}(m) = q^m. \tag{18.4}$$

Let further

(18.5) $\mathscr{M}(m) = \#\{\mathfrak{p} \in \{F_q[X]\} \mid N\mathfrak{p} = q^m \text{ and } \mathfrak{p} \text{ prime}\}.$

We have

$$\mathscr{M}(m) = \frac{1}{m} \sum_{d \mid m} \mu\left(\frac{m}{d}\right) q^d, \tag{18.6}$$

μ being the Möbius-function.

Analogously to § 4 we introduce a set-function P on the σ-algebra of all subsets E of $\{F_q[X]\}$. P is defined by

$$P(E) = \lim_{y \to \infty} \frac{\#\{\mathfrak{a} \in E \mid N\mathfrak{a} \leqq y\}}{\#\{\mathfrak{a} \in \{F_q[X]\} \mid N\mathfrak{a} \leqq y\}}, \tag{18.7}$$

if the limit exists and $E \subset \{F_q[X]\}$.

Conditional probabilities are defined in the same way as in § 4.

§ 19. Theorem 8

Let $\mathfrak{f}$ be a real-valued function defined on $\{F_q[X]\}$, such that

$$\begin{cases} \mathfrak{f}(\mathfrak{a}) = \sum_{\mathfrak{p} \mid \mathfrak{a}} \mathfrak{f}(\mathfrak{p}), \\ |\mathfrak{f}(\mathfrak{p})| \leqq 1, \end{cases} \tag{19.1}$$

and let $\mathfrak{f}_x : \{F_q[X]\} \to \boldsymbol{R}$ be defined by

$$\mathfrak{f}_x(\mathfrak{a}) = \sum_{\substack{\mathfrak{p} \mid \mathfrak{a} \\ N\mathfrak{p} \leqq q^x}} \mathfrak{f}(\mathfrak{p}), \qquad x \in \boldsymbol{Z}. \tag{19.2}$$

Put

$$A(x) = \sum_{N\mathfrak{p} \leqq q^x} \frac{\mathfrak{f}(\mathfrak{p})}{N\mathfrak{p}}, \qquad x \in \boldsymbol{Z}, \tag{19.3}$$

and

$$B(x) = \left[\sum_{N\mathfrak{p} \leqq q^x} \frac{\mathfrak{f}^2(\mathfrak{p})}{N\mathfrak{p}}\right]^{\frac{1}{2}}, \qquad x \in \boldsymbol{Z}. \tag{19.4}$$

Now theorem 8 reads as follows.

THEOREM 8.

Let $\mathfrak{f}_x$, A, B and Φ be defined by (19.2), (19.3), (19.4) *and* (4.9) *respectively.*

If $\lim_{x \to \infty} B(x) = \infty$, *then*

$$P(\mathfrak{f}_x(\mathfrak{a}) \leqq A(x) + uB(x)) = \Phi(u) + \mathcal{O}\left(\frac{\log^{\frac{1}{2}} B(x)}{B(x)}\right) \tag{19.5}$$

uniformly in $u \in \boldsymbol{R}$, as $x \to \infty$.

Proof of theorem 8.

Define $\rho_{\mathfrak{p}} : \{F_q[X]\} \to \boldsymbol{R}$ by

$$\text{(19.6)} \qquad \begin{cases} \rho_{\mathfrak{p}}(\mathfrak{a}) = \mathfrak{f}(\mathfrak{p}) \text{ if } \mathfrak{p} \mid \mathfrak{a}, \\ \rho_{\mathfrak{p}}(\mathfrak{a}) = 0 \text{ for all other cases.} \end{cases}$$

Consequently

$$\mathfrak{f}_x(\mathfrak{a}) = \sum_{N\mathfrak{p} \leqq q^x} \rho_{\mathfrak{p}}(\mathfrak{a}).$$

As in chapter 2, it can be shown that the stochastic variables $\rho_{\mathfrak{p}}$ are mutually independent and further

$$\mathscr{E}\mathfrak{f}_x = \sum_{N\mathfrak{p} \leqq q^x} \frac{\mathfrak{f}(\mathfrak{p})}{N\mathfrak{p}},$$

$$\text{var. } (\mathfrak{f}_x) = \sum_{N\mathfrak{p} \leqq q^x} \frac{\mathfrak{f}^2(\mathfrak{p})}{N\mathfrak{p}} - \sum_{N\mathfrak{p} \leqq q^x} \frac{\mathfrak{f}^2(\mathfrak{p})}{N\mathfrak{p}^2}.$$

From $|\mathfrak{f}(\mathfrak{p})| \leqq 1$ and (18.6) it follows that

$$\sum_{N\mathfrak{p} \leqq q^x} \frac{\mathfrak{f}^2(\mathfrak{p})}{N\mathfrak{p}^2} = \mathcal{O}(1) \text{ as } x \to \infty,$$

and hence

$$\text{var. } (\mathfrak{f}_x) = B^2(x) + \mathcal{O}(1).$$

It is now apparent that all the conditions involving the central limit theorem ($\mathscr{L}'$) have been satisfied, which completes the proof.

§ 20. Lemma 11 and theorem 9

Let $H_q : \boldsymbol{R} \to \boldsymbol{R}$ be defined by

$$\text{(20.1)} \qquad H_q(x) = \#\{\mathfrak{a} \in \{F_q[X]\} \mid N\mathfrak{a} \leqq q^x\}$$

and put

$$\text{(20.2)} \quad M_q(\mathfrak{b}, x) = \#\{\mathfrak{a} \in \{F_q[X]\} \mid \mathfrak{a} \equiv 0 \bmod \mathfrak{b} \text{ and } N\mathfrak{a} \leqq q^x\}, \quad (x \in \boldsymbol{R}).$$

Taking $x \in \boldsymbol{Z}^+$ it is clear that

$$\text{(20.3)} \qquad H_q(x) = \frac{q^{x+1}-1}{q-1}$$

and

$$\text{(20.4)} \qquad M_q(\mathfrak{b}, x) = \frac{\dfrac{q^{x+1}}{N\mathfrak{b}} - 1}{q-1}.$$

Further, analogous to § 5, put

(20.5) $M_q(x;m) = \#\{\mathfrak{a} \in \{F_q[X]\} \mid N\mathfrak{a} \leqq q^x \text{ and } (\mathfrak{p} \mid \mathfrak{a} \to N\mathfrak{p} > q^m)\}$.

Using Sylvester's principle we obtain

$$(20.6) \qquad M_q(x;m) = \sum_{\mathfrak{a} \in \mathfrak{A}_0} \mu(\mathfrak{a}) M_q(\mathfrak{a}, x),$$

where the set $\mathfrak{A}_0$ is defined by

$$(20.7) \quad \mathfrak{A}_0 = \{\mathfrak{a} \in \{F_q[X]\} \mid N\mathfrak{a} \leqq q^x \text{ and } (\mathfrak{p} \mid \mathfrak{a} \to N\mathfrak{p} \leqq q^m)\}.$$

Applying (20.3) and (20.4) we can deduce

$$(20.8) \qquad M_q(x;m) = \frac{q^{x+1}}{q-1} \prod_{N\mathfrak{p} \leqq q^m} \left(1 - \frac{1}{N\mathfrak{p}}\right).$$

As an immediate consequence of this we can state the following lemma.

Lemma 11.

Let $H_q(x)$ *and* $M_q(x;m)$ *be put as in* (20.1) *and* (20.5) *respectively.*

Let ψ *be a function defined on* $\boldsymbol{R}$ *with*

$$\lim_{x\to\infty} \psi(x) = \infty \text{ and } \frac{\psi(x)}{x} \leqq 1 \text{ for every } x \in \boldsymbol{R}.$$

Then

$$(20.9) \quad M_q(x;\psi(x)) = H_q(x) \prod_{N\mathfrak{p} \leqq q^{\psi(x)}} \left(1 - \frac{1}{N\mathfrak{p}}\right)(1 + \mathcal{O}(q^{-x})),$$

as $x \to \infty$.

Without any difficulty, we can finally prove the following theorem.

Theorem 9.

Let $\mathfrak{f}$, A, B *and* Φ *be defined by* (19.1), (19.3), (19.4) *and* (4.9) *respectively.*

If $\lim_{x\to\infty} B(x) = \infty$, *then*

$$(20.10) \qquad P(\mathfrak{f}(\mathfrak{a}) \leqq A(x) + uB(x) \mid N\mathfrak{a} \leqq q^x) = \Phi(u) + \mathcal{O}\left(\frac{\log^{\frac{1}{2}} B(x)}{B(x)}\right)$$

uniformly in $u \in \boldsymbol{R}$, *as* $x \to \infty$.

REFERENCES

BRUN, V.

[1] Le crible d'Eratosthène et le théorème de Goldbach, Skrifter utgit or videnskappsels kapet I. Kristiani (1920) 1—36.

BRUIJN, N. G. DE

[2] On the number of uncancelled elements in the sieve of Eratosthenes, Proc. Ned. Akad. Wetensch. 52 (1950) 803—812; Indagationes Mathematicae, Vol. XII (1950) 247—256.

BUCHSTAB, A. A.

[3] On those numbers in an arithmetic progression all prime factors of which are small in magnitude, Doklady Akad. Nauk. SSSR (N.S.) 67 (1949) 5—8.

CRAMÈR, H.

[4] Mathematical methods of Statistics, Princeton (1958).

DEDEKIND, R.

[5] Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Congruenzen, Gesammelte mathematische Werke, Erster Band (1930) 202—232.

DELANGE, H.

[6] Sur le nombre des diviseurs premiers de n, Acta Arithmetica 7 (1962) 191—215.

ERDÖS, P. and KAC, M.

[7] The Gaussian law of errors in the theory of additive numbertheoretic functions, Am. J. of Math.s, vol. 62 (1940) 738—742.

HALBERSTAM, H.

[8] On the distribution of additive numbertheoretic functions II and III, J. London Math. Soc. vol. 31 (1956) 1—27.

KUBILYUS, I. P.

[9] Probabilistic methods in the theory of numbers, Amer. Math. Soc. Transl. 19 (1962) 47—85.

LANDAU, E.

[10] Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale, Zweite Auflage, New York (1949).

[11] Über die zu einem algebraischen Zahlkörper gehörige Zetafunktion und die Ausdehnung der Tschebyschefschen Primzahlentheorie auf den Problem der Verteilung der Primideale. J. reine und angew. Math. 125 (1903) 64—188.

LANG, S.

[12] Algebraic number theory, Reading, Mass., Palo Alto, London (1964).

RADEMACHER, H.

[13] Über die Anwendung der Viggo Brunschen Methode, Sitzungsberichte der preussischen Akademie von Wissenschaften (1923) 211—218.

RENYI, A. and TURAN, P.

[14] On a theorem of Erdös-Kac, Acta Arithmetica 4 (1958) 71—84.

RIEGER, G. J.

[15] Über die Anzahl der Primfaktoren algebraischer Zahlen und das Gauszsche Fehlergesetz, Math. Nachr. 24 (1962) 77—89.

[16] Verallgemeinerung der Siebmethode von A. Selberg auf algebraische Zahlkörper III, J. reine und angew. Math. 208 (1961) 79—90.

Uspensky, J.
[17] Introduction to mathematical probability, New York, London (1937).

(Oblatum 4-1-66)