length 12:

24584	37973	93149	119366	74846
59399	180515	39020	59324	63473
26093	67100			(2)

length 22:

9045	63198	99837	167916	91410
60075	27708	66414	17601	24585
40074	18855	71787	83190	92061
66858	84213	34068	41811	33795
79467	101463			(3)

length 28:

70225	19996	184924	93898	183877
99394	178414	51625	14059	63199
126118	40579	80005	35893	95428
95998	21304	1300	244	2080
32800	33043	1753	20176	24616
16609	74602	25639		(7)

The numbers with brackets denote first natural numbers appeared as cyclic parts.

Therefore we have 15 cyclic parts: five cyclic parts with length 1, three cyclic parts with length 2, one cyclic part with length 4, one cyclic part with length 6, two cyclic parts with length 10, one cyclic part with length 12, one cyclic part with length 22, and one cyclic part with length 28.

References

[1] K. Chikawa, K. Iséki and T. Kusakabe, *On a problem by H. Steinhaus*, Acta Arith. this volume, pp. 251-252.

[2] K. Iséki, *Necessary results for computation of cyclic parts in Steinhaus problem*, Proc. of Japan Academy 36 (1960), pp. 650-651.

O. R. DEPT. YAMAMURA GLASS COMPANY,
KÔBE UNIVERSITY AND
FACOM COMPUTING CENTER, YULIN ELECTRIC COMPANY

Reçu par la Rédaction le 30. 8. 1961

ACTA ARITHMETICA
VII (1962)

On the distribution of prime ideals

by

E. Fogels (Riga)

Introduction

1. In 1944 Linnik (see [13]) proved the existence of an absolute constant $c > 0$ such that the least prime in any arithmetical progression $Du+l[(D, l) = 1, u = 0, 1, \ldots]$ does not exceed D^c. In 1954 Rodosskiĭ [15] gave a shorter proof of the same theorem. In 1955 I proved [3] the existence of an absolute constant $c > 0$ such that there is at least one prime $p \equiv l \pmod D$ with $(D, l) = 1$ in the interval (x, xD^c) for any $x \geqslant 1$ (1). It is the aim of the present paper to prove an analogous result for an algebraic field as stated in the following

Theorem. *Let K, $\mathfrak{f}$, $\mathfrak{H}$ denote respectively any algebraic field of degree $n \geqslant 1$, any ideal in K and any class of ideals modulo $\mathfrak{f}$. Further let*

$$D = |\Delta| \cdot N\mathfrak{f} > 1 ,$$

where Δ denotes the discriminant of the field and $N\mathfrak{f}$ the norm of $\mathfrak{f}$. Then there is a positive constant c (which depends on n only) such that for all $x \geqslant 1$ in the interval (x, xD^c) there is at least one prime $\mathfrak{p}$ representing the norm of a prime ideal $\mathfrak{p} \in \mathfrak{H}$.

In particular for $n = 1$, $\mathfrak{f} = [D]$ we get the result concerning primes $p \equiv l \pmod D$ as stated above. Taking $n > 1$, $x = 1$, $\mathfrak{f} = \mathfrak{o}$ (the unit ideal) we deduce that *in any class of ideals* (in the usual sense) *there is a prime ideal* $\mathfrak{p}$ *with the norm* $\leqslant |\Delta|^c$.

Taking $n = 2$, $\mathfrak{f} = [k]$ (k any natural number $\geqslant 1$) we deduce the existence of a prime $p_\psi \in (x, xD^c)$ *representable by the prescribed primitive binary quadratic form* ψ with the discriminant Δk^2, where Δ is a fundamental discriminant and $D = |\Delta| k^2$. For $\Delta < 0$ only positive forms are considered. See further §§ 3 and 6-8, where the statement will be improved for intervals (x, xD^ε) $(0 < \varepsilon \leqslant c,\ D \geqslant D_0(\varepsilon),\ x \geqslant D^{c' \log (c/\varepsilon)})$.

---

(1) In 1960 I improved (see [4]) this theorem for intervals (x, xD^ε), $0 < \varepsilon \leqslant c$, $D \geqslant D_0(\varepsilon)$, $x \geqslant D^{c' \log (c/\varepsilon)}$.

COROLLARY 1. *Let* $\pi_{\mathfrak{H}}(x)$ *denote the number of primes* $p \leqslant x$ *with* $p = N\mathfrak{p}$, $\mathfrak{p} \in \mathfrak{H}$; *then for all* $D \geqslant D_0 > 1$, $x \geqslant D^c$

$$\pi_{\mathfrak{H}}(x) > x/D^{2n+3c/2}\log x\,.$$

COROLLARY 2. *Let* q *be any natural number* > 1 *and* l *any rational integer, prime with respect to* q, *such that there is an ideal* $\mathfrak{a} \in \mathfrak{H}$ *with* $N\mathfrak{a} \equiv l \pmod q$. *If* D *is replaced by* $|\Delta| q^n N\mathfrak{f}$, *then the theorem still holds for primes* $p \equiv l \pmod q$.

The method used in the proof of the theorem is essentially the same as that employed by Rodosskiĭ (see [15], pp. 351-355 or [14] X § 4), the necessary properties of the Hecke-Landau function $\zeta(s, \chi)$ being proved by [5], [6], [7]. The notation used in those papers will be generally retained here.

We shall prove the theorem for a fixed $n \leqslant 1$ and for all $D \geqslant D_0$ with a sufficiently large $D_0 > 1$. For a finite number of exceptional cases (2) with $2 \leqslant D < D_0$ the truth of the theorem (if c is large enough) follows from the asymptotical distribution formula for prime ideals in classes $\mathfrak{H}$ (see [11], Satz LXXXV).

On the classes of ideals

2. There are different definitions of classes of ideals in the field K. According to the usual definition the ideals $\mathfrak{a}$, $\mathfrak{b}$ are equivalent or belong to the same class $\mathfrak{K}$ if there are integers $\alpha, \beta \in K$ such that

$$\mathfrak{a}[\alpha] = \mathfrak{b}[\beta]\,. \tag{1}$$

The number of classes $\mathfrak{K}$ will be denoted by h_0.

The ideals $\mathfrak{a}$, $\mathfrak{b}$ are *equivalent modulo* $\mathfrak{f}$ if $(\mathfrak{a}, \mathfrak{f}) = (\mathfrak{b}, \mathfrak{f}) = \mathfrak{o}$ and (1) holds for some integers α, β satisfying the conditions

$$\alpha \equiv \beta \equiv 1 \pmod{\mathfrak{f}} \tag{2}$$

and

$$\alpha \succ 0\,, \quad \beta \succ 0\,, \tag{3}$$

where $\xi \succ 0$ is an abbreviation for "all the real conjugates (if any) of $\xi \in K$ are positive numbers". The classes of ideals modulo $\mathfrak{f}$ and the number of classes will be denoted by $\mathfrak{H}$ and h respectively. The notation $\mathfrak{a} \sim \mathfrak{b}$ means that $\mathfrak{a}$ and $\mathfrak{b}$ are equivalent modulo $\mathfrak{f}$.

LEMMA 1. *Let* S *and* S' *be two sets of conditions for the equivalence of ideals in the field* K *such that* $S \subset S'$ *and let the corresponding classes*

(2) Consider that (i) there is only a finite number of fields K of degree n with the discriminant Δ and (ii) there is only a finite number of ideals $\mathfrak{f}$ in K with a given norm. For these theorems see, for example [1], p. 341 and [12], Satz 818.

be $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$ *and* $\mathfrak{B}_1, \ldots, \mathfrak{B}_{k'}$ *respectively. Then each class* $\mathfrak{A}$ *is the sum of the same number* $j \geqslant 1$ *of classes* $\mathfrak{B}$.

Proof. Suppose that the principal class $\mathfrak{A}_1$ of S is divided up by S' into the classes $\mathfrak{B}_1, \ldots, \mathfrak{B}_j$, evidently forming a group. Let $\mathfrak{B}_i', \mathfrak{B}_i''$ be any two of the classes (not excluding $\mathfrak{B}_i' = \mathfrak{B}_i''$) into which $\mathfrak{A}_i$ is divided up by S'. Since $\mathfrak{B}_i', \mathfrak{B}_i'' \subset \mathfrak{A}_i$, we have

$$\mathfrak{B}_i'/\mathfrak{B}_i'' \subset \mathfrak{A}_1$$

(in the sense of class composition). Hence for appropriate $\nu = \nu(i)$ $(1 \leqslant \nu \leqslant j)$

$$\mathfrak{B}_i'/\mathfrak{B}_i'' = \mathfrak{B}_\nu \quad \text{or} \quad \mathfrak{B}_i' = \mathfrak{B}_i''\mathfrak{B}_\nu\,.$$

Thus $\mathfrak{B}_i'$ is one of the classes $\mathfrak{B}_i''\mathfrak{B}_1, \ldots, \mathfrak{B}_i''\mathfrak{B}_j$. This proves that by S' any of the classes $\mathfrak{A}_1, \ldots, \mathfrak{A}_k$ is divided up into j classes $\mathfrak{B}$.

LEMMA 2. *If* h *and* h_0 *denote the numbers of classes* $\mathfrak{H}$ *and* $\mathfrak{K}$, *respectively, then*

$$h \ll h_0 N\mathfrak{f} \ll (|\Delta|^{1/2}\log^{n-1}|\Delta|)\,N\mathfrak{f} \ll D\,. \tag{4}$$

Proof. Let α, β be any integers in K satisfying the conditions

$$\alpha \equiv \beta \pmod{\mathfrak{f}}\,, \quad ([\alpha], \mathfrak{f}) = ([\beta], \mathfrak{f}) = \mathfrak{o}\,. \tag{5}$$

Then there is an integer ξ in K such that $\alpha\xi \equiv 1 \pmod{\mathfrak{f}}$ (see [11] Satz XV). Multiplying $[\alpha][\beta] = [\beta][\alpha]$ by $[\xi]$ and writing $\alpha\xi = \beta_1$, $\beta\xi = \alpha_1$, we obtain

$$[\alpha][\alpha_1] = [\beta][\beta_1]\,, \quad \alpha_1 \equiv \beta_1 \equiv 1 \pmod{\mathfrak{f}}\,.$$

This proves that for any α, β satisfying (5) the principal ideals $[\alpha]$, $[\beta]$ are equivalent in the sence (1)+(2). Hence the class $\mathfrak{K}_1$ containing all the principal ideals of the field is divided, by condition (2), into $j \leqslant N\mathfrak{f}$ classes $\mathfrak{B}$ corresponding to (1)+(2) (cf. the definition of $N\mathfrak{f}$ as given in [12] III, p. 112). By (3) each of these classes $\mathfrak{B}$ is divided into $\leqslant 2^n$ classes $\mathfrak{H}$, whence $h \leqslant h_0 N\mathfrak{f} \cdot 2^n \ll h_0 N\mathfrak{f}$. Since $h_0 \ll |\Delta|^{1/2}\log^{n-1}|\Delta|$ (see [10], § 3), this proves (4) (3).

3. In this paragraph we shall consider an example of forming classes of ideals which play an important rôle in the theory of binary quadratic forms. (The corresponding classes $\mathfrak{C}$ will be used further in §§ 6-8). Now let K be the quadratic field generated by $\sqrt{\Delta}$, where Δ is a fundamental discriminant (cf. [12] Satz 873; I, p. 172), and let k be a fixed natural number $\geqslant 1$. We deal exclusively with ideals $\mathfrak{a}$, $\mathfrak{b}$, ... prime with respect

(3) Hecke ([9]) considered his L-functions in a real cubic field having imaginary conjugates. He did not use the equivalence condition (3), which was introduced by Landau ([11]); hence Hecke's L-functions are in the set of Landau functions $\zeta(s, \chi)$ with possibly imprimitive characters.

to $[k]$. Such ideals belong, by definition, to the same class $\mathfrak{C}$, if we have in (1):

(6) *α and β are congruent* mod$[k]$ *to rational integers prime with respect to k*

and

$$N\alpha \cdot N\beta > 0 \,. \tag{7}$$

Let $\mathfrak{O}_k$ denote the ring of all integers in K which are congruent mod$[k]$ to rational integers. We choose a fixed *primitive* $\mathfrak{a} \in \mathfrak{C}$ (i.e., the largest natural number l dividing all the numbers $\xi \in \mathfrak{a}$ is $l = 1$. For any $\mathfrak{a} \in \mathfrak{C}$ there is a primitive ideal $\mathfrak{b} \in \mathfrak{C}$ and a natural number l such that $\mathfrak{a} = [l]\mathfrak{b}$; if $l > 1$, then we use $\mathfrak{b}$ instead of $\mathfrak{a}$). Let $\mathfrak{a}_k$ denote the ring of all the numbers common to $\mathfrak{O}_k$ and $\mathfrak{a}$ (a similar definition for $\mathfrak{b}_k$). If α_1, α_2 is a basis of $\mathfrak{a}_k$ and ξ any number $\in \mathfrak{a}_k$, then there are rational integers x, y such that

$$\xi = \alpha_1 x + \alpha_2 y \,,$$

whence

$$N\xi = \alpha_1\alpha_1' x^2 + (\alpha_1\alpha_2' + \alpha_2\alpha_1')xy + \alpha_2\alpha_2' y^2$$

(α' denoting the conjugate of α). Let $\mathfrak{a}'$ be the ideal formed by the numbers conjugate to those of $\mathfrak{a}$. Then we have $\mathfrak{a}\mathfrak{a}' = N\mathfrak{a}$ (see [16] p. 353). Since $\alpha_1\alpha_1'$, $\alpha_1\alpha_2' + \alpha_2\alpha_1'$, $\alpha_2\alpha_2'$ are rational integers belonging to the latter ideal, there are other rational integers a, b, c such that

$$\alpha_1\alpha_1' = aN\mathfrak{a} \,, \quad \alpha_1\alpha_2' + \alpha_2\alpha_1' = bN\mathfrak{a} \,, \quad \alpha_2\alpha_2' = cN\mathfrak{a} \,,$$

$$ax^2 + bxy + cy^2 = N\xi/N\mathfrak{a} \,. \tag{8}$$

It can be proved that (8) is a primitive quadratic form with the discriminant $d = \Delta k^2$ (see [8], pp. 277-279, where the proof does not depend on the sign of d; cf. also [17], pp. 123-124).

Take any ideal $\mathfrak{b}$ belonging to the same class $\mathfrak{C}$ as $\mathfrak{a}'$. Then there are numbers α, β, satisfying (6), (7), such that $\mathfrak{a}'[\alpha] = \mathfrak{b}[\beta]$, whence $\mathfrak{a}\mathfrak{b} = [\xi]$ with $\xi = (\alpha/\beta)N\mathfrak{a}$ belonging to the group formed by the quotients of the numbers (6). Being an integer (since $[\xi] = \mathfrak{a}\mathfrak{b}$) ξ is in the ring $\mathfrak{O}_k$ and simultaneously in $\mathfrak{a}$ (since $\mathfrak{a}$ divides ξ); hence $\xi \in \mathfrak{a}_k$. Consequently there are rational integers x, y such that $\xi = \alpha_1 x + \alpha_2 y$ and, by (8),

$$ax^2 + bxy + cy^2 = N\xi/N\mathfrak{a} = N\mathfrak{b} \,,$$

since $\mathfrak{a}\mathfrak{b} = [\xi]$, $N\xi > 0$. This proves that *for any class $\mathfrak{C}$ of ideals there is a quadratic form representing norms of the ideals $\mathfrak{b} \in \mathfrak{C}$.*

To verify the converse correspondence, let $ax^2 + bxy + cy^2$ be a primitive quadratic form having the discriminant $d = b^2 - 4ac = \Delta k^2$, where Δ is a fundamental discriminant and k a natural number $\geqslant 1$ (cf. [12] I, p. 172 and Satz 873). Being interested only in positive numbers representable by the form we may suppose $a > 0$ and $(a, d) = 1$ (cf. [12] Satz 206, 201).

Then it can be proved (see [16] § 97, Satz 6) that in the quadratic field generated by $\sqrt{\Delta}$ there is an ideal

$$\mathfrak{a} = \left(a, \tfrac{1}{2}(b + \sqrt{d})\right)$$

having the norm a, which is representable by the form (with $x = 1, y = 0$).

Now let us suppose that the theorem of § 1 is proved. Then for any class $\mathfrak{H}$ of ideals mod$[k]$ and any $x \geqslant 1$ there is a prime p such that $p = N\mathfrak{p} \in (x, x|\Delta k^2|^c)$, $\mathfrak{p} \in \mathfrak{H}$. By Lemma 1 each class $\mathfrak{C}$ is a sum of the same number $j \geqslant 1$ of the classes $\mathfrak{H}$, since the set of conditions (6)+(7) is included in that of (2)+(3). Hence the theorem holds for classes $\mathfrak{C}$ as well and consequently there is a prime $p \in (x, x|d|^c)$ representable by the binary quadratic form with the discriminant d.

Applying the same argument to the principal class $\mathfrak{K}_1$ (now in any field K) we can deduce for any integer $\alpha \in K$, prime with respect to $\mathfrak{f}$ and to any $x \geqslant 1$, the existence of an integer $\pi \in K$ such that $|N\pi| = p \in (x, xD^c)$, $\pi \equiv a \,(\mathrm{mod}\,\mathfrak{f})$.

4. In this paragraph let q be a fixed natural number > 1 and let H be the classes modulo $\mathfrak{f}[q]$ in general.

If $\mathfrak{a}, \mathfrak{b}$ are ideals of the same class H, then, by § 2, there are integers $\alpha, \beta \in K$ such that $\mathfrak{a}[\alpha] = \mathfrak{b}[\beta]$, $\alpha \succ 0$, $\beta \succ 0$ and $\alpha \equiv \beta \equiv 1 \,(\mathrm{mod}\,\mathfrak{f}[q])$. Hence $\alpha = 1 + q\gamma$ where γ is an integer $\in K$. Multiplying by the associate numbers $\alpha' = 1 + q\gamma'$, $\alpha'' = 1 + q\gamma''$, ... and considering that the elementary symmetrical functions of $\gamma, \gamma', \gamma'', \ldots$ are rational integers, we deduce that $N\alpha \equiv 1 \,(\mathrm{mod}\,q)$ and, in a similar way, that $N\beta \equiv 1 \,(\mathrm{mod}\,q)$. Now we have, by (1), (3), $N\mathfrak{a} \cdot N\alpha = N\mathfrak{b} \cdot N\beta$, whence $N\mathfrak{a} \equiv N\mathfrak{b} \,(\mathrm{mod}\,q)$ and

$$\chi_q(N\mathfrak{a}) = \chi_q(N\mathfrak{b})$$

for any Dirichlet character χ_q modulo q. Hence we may define

$$\chi_q(H) = \chi_q(N\mathfrak{a}) \quad \text{with} \quad \mathfrak{a} \in H$$

and consider the function of mixed characters [4]

$$\zeta(s, \chi_q, \chi) = \sum_H \chi_q(H)\chi(H)\zeta(s, H) = \sum_{\mathfrak{a}} \frac{\chi_q(N\mathfrak{a})\chi(\mathfrak{a})}{N\mathfrak{a}^s} \qquad (\sigma > 1) \,, \tag{9}$$

where

$$\zeta(s, H) = \sum_{\mathfrak{a} \in H} N\mathfrak{a}^{-s} \,.$$

Since $\chi_q(H)\chi(H)$ is some character modulo $\mathfrak{f}[q]$, $= \chi'(H)$ (say), we have

$$\zeta(s, \chi_q, \chi) = \zeta(s, \chi') \,. \tag{10}$$

[4] For the idea of mixed characters I am indebted to professor Linnik.

Let us call a "$\mathfrak{H}$ norm-residue" any integer $l \in [1, q-1]$ prime with respect to q if there is an $\mathfrak{a} \in \mathfrak{H}$ with $N\mathfrak{a} \equiv l \pmod q$. The number of such l's will be denoted by $\nu(\mathfrak{H})$.

Let $\mathfrak{H}_1$ be the principal class and let

$$\mathfrak{H}_1 = H_1 + \ldots + H_j \tag{11}$$

be its representation by a sum of classes H; then the classes $H_1, \ldots, H_j$ form a group. Consider that there is exactly one norm residue in each H. Hence there is a subgroup $\mathfrak{G} = H_1 + \ldots + H_{j_1}$ $(j_1 = \nu(\mathfrak{H}_1))$ in (11) corresponding to the set of the $\nu(\mathfrak{H}_1)$ different "$\mathfrak{H}_1$ norm-residues" and $\mathfrak{H}_1$ may be represented by a sum of sets

$$\mathfrak{H}_1 = H_1\mathfrak{G} + H_2\mathfrak{G} + \ldots + H_r\mathfrak{G} \quad (H_1\mathfrak{G} = \mathfrak{G}) .$$

All the norm-residues of any set $H_i\mathfrak{G}$ $(1 \leqslant i \leqslant r)$, being different and belonging to $\mathfrak{H}_1$, must coincide with those of $\mathfrak{G}$. This proves that any "$\mathfrak{H}_1$ norm-residue" is represented by (11) the same number of times. And the corresponding thing is true for all the other classes $\mathfrak{H}_2, \ldots$ as well, since

$$\mathfrak{H}_2 = H'H_1 + \ldots + H'H_j , \qquad \mathfrak{H}_3 = H''H_1 + \ldots + H''H_j ,$$

etc. This proves that $\nu(\mathfrak{H}_1) = \nu(\mathfrak{H}_2) = \ldots = \nu(\mathfrak{H}_h)$.

If l is a "$\mathfrak{H}$ norm-residue", then, by (9) and [7] (3),

$$\sum_{\substack{\mathfrak{a} \in \mathfrak{H} \\ N\mathfrak{a} \equiv l \pmod q}} N\mathfrak{a}^{-s} = \frac{1}{h\varphi(q)} \sum_{\chi_q} \overline{\chi}_q(l) \sum_{\chi'} \overline{\chi}'(\mathfrak{H}) \zeta(s, \chi_q, \chi') \qquad (\sigma > 1) , \tag{12}$$

where χ' runs through all characters of classes $\mathfrak{H}$ (they are imprimitive characters of classes H as well).

Using the function $\zeta(s, \chi_q, \chi)$ instead of $\zeta(s, \chi)$ we can prove results concerning the distribution of ideals or prime ideals in any class $\mathfrak{H} \bmod \mathfrak{f}$ having the prescribed norm-residue $\bmod q$ (cf. (12)); this accounts for Corollary 2. However, we need not deal further with the functions $\zeta(s, \chi_q, \chi)$ since, by (10), they are in the set of functions $\zeta(s, \chi)$ with exchanged $\mathfrak{f}$.

Proof of the theorem

5. The proof consists of going through a sequence of deductions similar to those used for $n = 1$ in [4], pp. 299-308. For $n > 1$ and a large x the theorem is a weaker one than that for $n = 1$, since the analogue of Siegel's theorem for Hecke's L-functions is not at our disposal (5). Some

(5) But that analogue can be proved by the method of Estermann (see [14], IV, § 8) for any fixed field K with $\Delta \ll 1$.

parts of the proof become simpler in detail and for this reason we shall revise it.

By the use of [5] (11) and [7] (1), by the analogue of [4] (14),

$$h \sum_{\substack{\mathfrak{p}^m \in \mathfrak{H} \\ m \geqslant 1}} \exp\left(\frac{-\log^2 N\mathfrak{p}/x}{4y}\right) N\mathfrak{p}^{m/2} \log N\mathfrak{p} = 2\sqrt{\pi y}\, x^{3/2} e^{9y/4} \{1 - e_1 x^{-\delta'} \chi'(\mathfrak{H}) e^{-\delta'(3-\delta')y} - S\} + O(D^{3/2}) \tag{13}$$

where $x > 0$, $y > 0$,

$$S = \sum_{\chi} \overline{\chi}(\mathfrak{H}) \sum_{\varrho_\chi (\neq \beta')} x^{-\delta} e^{(-\delta(3-\delta) - \tau^2 + i\tau(3-2\delta))y + i\tau \log x} , \tag{14}$$

$\varrho_\chi = \varrho = 1 - \delta + i\tau$ runs through the zeros of $\zeta(s, \chi)$ with $0 < \delta \leqslant 1$; $e_1 = 1$ if the exceptional zero $\beta' = 1 - \delta'$ exists and $e_1 = 0$ otherwise. The remaining term is obtained by the use of (4) and the estimate

$$\zeta'/\zeta(-\tfrac{1}{2} + it, \chi) \ll \log D(1 + |t|) ,$$

which is a simple consequence of [5] (41), [5] (36) and the fact that there are no zeros of $\zeta(s, \chi)$ in the strip $-1 < \sigma < 0$.

Write

$$x = D^{\xi} , \qquad \xi \geqslant 0; \qquad y = \eta \log D , \qquad \eta \geqslant \eta_0 > 2 .$$

Let $\Phi(x, y, \mathfrak{H})$ be the left-hand side of (13) and let I_B denote the integration repeated B times with respect to η, the range of integration being $(\eta, \eta + 1)$. By (13), (14)

$$I_B \frac{\Phi(x, y, \mathfrak{H})}{2\sqrt{\pi y}\, x^{3/2} e^{9y/4}} \geqslant 1 - x^{\delta'} e^{-2\eta_0 \delta' \log D} - I_B S - c_1 D^{3/2 - 9\eta_0/4} , \tag{15}$$

$$I_B S \leqslant \left(\frac{2}{\log D}\right)^B \sum_{\varrho} x^{-\delta} \frac{\exp\{-\eta_0(2\delta + \tau^2)\log D\}}{|2\delta + i\tau|^B} = T_1 + T_2 + T_3 . \tag{16}$$

The sum in (16) extends over all the zeros $\varrho \neq \beta'$ of $Z(s) = \prod_{\chi} \zeta(s, z)$ in the strip $0 \leqslant \sigma \leqslant 1$, which is cut into the regions G_1, G_2, G_3 (as defined below) and T_1, T_2, T_3 denote the corresponding parts of $I_B S$.

Let G_1 be the region $|t| > 1$. By (16), (4), [5] (6), [5] (36),

$$\begin{aligned} T_1 &\ll \sum_{\varrho \in G_1} e^{-\eta_0 \tau^2 \log D} \ll h \int_1^{\infty} e^{-\eta_0 t^2 \log D} \cdot t^2 \log D \cdot \log D(1 + t)\, dt \\ &< h \log^2 D \int_1^{\infty} e^{-\eta_0 t^2 \log D} t^2 \log(1 + t)\, dt < h \log^2 D \int_1^{\infty} e^{-(\eta_0 - 1) t \log D} dt \\ &\ll h D^{1 - \eta_0} \log D \ll D^{2 - \eta_0} \log D . \end{aligned} \tag{17}$$

Let G_2 be the region of the points $s = 1-\lambda/\log D + i\gamma/\log D$ with

$$\lambda_0 \leqslant \lambda \leqslant \log D\,, \qquad |\gamma| \leqslant \gamma_1 = \gamma_1(\lambda) = \min(e^\lambda, \log D)\,,$$

λ_0 being defined as in [6], and let us write the zeros $\varrho \notin G_1$ as follows:

$$\varrho = 1-\lambda/\log D + i\gamma/\log D\,, \qquad \lambda = \lambda_\varrho\,,\ \gamma = \gamma_\varrho\,.$$

Then, by (16), [5] (6), [7]

$$(18)\qquad T_2 \ll \sum_{\varrho\,\epsilon\,G_2} e^{-\lambda\xi-2\eta_0\lambda}/\lambda^B \ll \sum_{\lambda_0<\lambda\leqslant\log D} e^{-(\xi+2\eta_0)\lambda} \ll \int_{\lambda_0}^{\log D} (\xi+2\eta_0)\, e^{-(\xi+2\eta_0-C)\lambda}\,d\lambda \ll e^{-(\xi+\eta_0)\lambda_0}\,,$$

provided that (6) $\eta_0 > C$.

Let G_3 be the remaining part of the rectangle $0 \leqslant \sigma \leqslant 1$, $|t| < 1$. Supposing $\lambda_0 < \log\log D$, $B \geqslant C+1$ we have, by (16), [5] (6), [7],

$$(19)\qquad T_3 \ll \sum_{\varrho\,\epsilon\,G_3} e^{-(\xi+2\eta_0)\lambda}|\gamma|^{-B} \ll e^{-(\xi+2\eta_0)\lambda_0} \sum_{\varrho\,\epsilon\,G_3} |\gamma|^{-B} \ll e^{-(\xi+2\eta_0)\lambda_0} \int_{\lambda_0}^{\log\log D} e^{-(B-C)\lambda}\,d\lambda \ll e^{-(\xi+2\eta_0+B-C)\lambda_0} \ll e^{-(\xi+\eta_0)\lambda_0}\,.$$

If U denotes the left-hand side of (15), then, by (15), (16), (17), (18), (19),

$$(20)\qquad U \geqslant 1 - x^{\delta'} e^{-2\eta_0\delta'\log D} - c_2 e^{-(\xi+\eta_0)\lambda_0} - c_3 D^{2-\eta_0}\log D\,.$$

Considering that, by [6], $\delta' \geqslant \delta_0$, we have for (6) $\eta_0 \geqslant 1/2A$

$$(21)\qquad 1 - x^{\delta'} e^{-2\eta_0\delta'\log D} \geqslant 1 - e^{-2\eta_0\delta_0\log D} \geqslant 1 - e^{-(\delta_0/A)\log D} \geqslant (\delta_0/2A)\log D$$

(since $1-e^{-\theta} \geqslant \frac{1}{2}\theta$ for $0 \leqslant \theta \leqslant 1$). We may suppose that

$$\eta_0 \geqslant 1/A\,, \qquad c_2 e^{-A\eta_0} < \tfrac{1}{8}\,, \qquad c_3 D^{2-\eta_0}\log D < (\delta_0/8A)\log D$$

(since, by [6], [5], $\delta_0 \geqslant D^{-2n}$); then, by [6],

$$c_2 e^{-(\xi+\eta_0)\lambda_0} \leqslant c_2 e^{-\eta_0\lambda_0} = c_2 \exp\left\{-\eta_0 A \log\frac{eA}{\delta_0\log D}\right\} = \left(\frac{\delta_0\log D}{A}\right)^{A\eta_0} c_2 e^{-A\eta_0} \leqslant \frac{1}{8A}\,\delta_0\log D\,.$$

Hence, by (21), (22),

$$U > (\delta_0/4A)\log D\,.$$

Introducing the number $z = xe^{4y}$, we must divide the sum

$$\Phi(x, y, \mathfrak{H}) = h \sum_{\substack{\mathfrak{p},\,m\\ \mathfrak{p}^m\,\epsilon\,\mathfrak{H}\\ m\geqslant 1}} \exp\left(-\frac{\log^2 N\mathfrak{p}/x}{4y}\right) N\mathfrak{p}^{m/2}\log N\mathfrak{p}$$

(6) The constants C and A are those defined by the theorems of [7] and [6] respectively.

into five partial sums $S_0, hS', S_1, hS_2, hS_3$ (say) corresponding to the restrictions

$$\mathfrak{p}\,\epsilon\,\mathfrak{H}\,,\ N\mathfrak{p} \leqslant x;\ \mathfrak{p}\,\epsilon\,\mathfrak{H}\,,\ x < N\mathfrak{p} = p < z;\ \mathfrak{p}^m\,\epsilon\,\mathfrak{H}\,,\ m \geqslant 1\,,\ N\mathfrak{p}^m \geqslant z;$$
$$\mathfrak{p}^m\,\epsilon\,\mathfrak{H}\,,\ m \geqslant 2\,,\ N\mathfrak{p}^m < z;\ \mathfrak{p}\,\epsilon\,\mathfrak{H}\,,\ x < N\mathfrak{p} = p^f < z\,,\ 2 \leqslant f \leqslant n\,,$$

respectively. We can show that

$$S_0 \ll x^{3/2}e^{2y}\,, \qquad S_3 \ll xe^{3y/2} + \exp\left(\log z - \frac{\log^2 z/x}{4y}\right)$$

and

$$S_2 + S_3 \ll (4+\xi/\eta_0)\,xy\,e^{3y/2}$$

(cf. [4] (54), (51), (52), (53)). Proving the estimate $S_1 \ll x^{3/2}e^{2y}$ we make use of [7] (44), which is justified if $\eta_0 \ll 1$ is large enough. Writing

$$V = I_B[2\sqrt{\pi y}\,x^{3/2}e^{9y/4}]^{-1}h \sum_{\substack{\mathfrak{p}\,\epsilon\,\mathfrak{H}\\ x<N\mathfrak{p}=p<z}} \exp\left(-\frac{\log^2 p/x}{4y}\right)\sqrt{p}\,\log p$$

we get the inequality

$$(22)\qquad V > (\delta_0/4A)\log D - c_4 e^{-(\eta_0/4)\log D}\,.$$

For a sufficiently large η_0 the right-hand side of (22) is > 0 (since $\delta_0 > D^{-2n}$, by [5]), whence the theorem.

If η_0 is large enough, then we have, by (22)

$$\sum_{\substack{\mathfrak{p}\,\epsilon\,\mathfrak{H}\\ x<N\mathfrak{p}=p<z}} p^{1/2}\log p > c_5 x^{3/2}\delta_0\log D > c_6 x^{3/2}D^{-2n}\log D\,,$$

whence

$$\pi_{\mathfrak{H}}(z)\,z^{1/2}\log z > c_6(zD^{-c})^{3/2}D^{-2n}\log D\,, \qquad \pi_{\mathfrak{H}}(z) > z/D^{2n+3c/2}\log z\,.$$

This proves Corollary 1. For the Corollary 2 see § 4.

On primes representable by binary quadratic forms (7)

6. The statement of § 1 concerning the quadratic form is a consequence of the theorem and § 3. In the following paragraphs, 6-8, we shall improve that result for intervals (x, xD^ε) with $0 < \varepsilon \leqslant c$, $D \geqslant D_0(\varepsilon)$, $x \geqslant D^{c'\log(c/\varepsilon)}$.

(7) In the present exposition the deductions of the paragraphs 6 and 8 are ultimately based on the functional equation of $\zeta(s, \chi)$ proved by Landau for the general algebraic field. If the reader is interested only in quadratic forms, it is a nuisance to go through the complicate proof (extended to nearly 50 pages) of that equation. For this reason I have worked out more direct proofs of the necessary properties of the function $\zeta(s, X)$ (see (24)) and I hope to publish them as soon as an opportunity presents itself.

Let $\Delta, K, k, \mathfrak{C}$ be defined as in § 3, $d = \Delta k^2$, $D = |d|$, $\mathfrak{H}$ denote classes of ideals modulo $[k]$, $X(\mathfrak{C})$ the characters of classes $\mathfrak{C}$ and let

$$X(\mathfrak{a}) = \begin{cases} X(\mathfrak{C}) & \text{if} \quad \mathfrak{a} \in \mathfrak{C}, \\ 0 & \text{if} \quad \mathfrak{a} \text{ is not prime with respect to } k. \end{cases}$$

The principal character will be denoted by X_0.

Further let h_1 denote the number of classes $\mathfrak{C}$; by § 3 and [12] Satz 209

$$h_1 \ll D^{1/2}\log D \tag{23}$$

(since $\sum_m \left(\frac{d}{m}\right)\frac{1}{m} \ll \log|d|$ by [12] I, p. 83 and (72) with $s=1$, $u=|d|$, $v\to\infty$). We introduce the functions

$$\begin{aligned} \zeta(s, \mathfrak{C}) &= \sum_{\mathfrak{a}\in\mathfrak{C}} N\mathfrak{a}^{-s}, \\ \zeta(s, X) &= \sum_{\mathfrak{C}} X(\mathfrak{C})\zeta(s, \mathfrak{C}) = \sum_{\mathfrak{a}} X(\mathfrak{a}) N\mathfrak{a}^{-s} = \prod_{\substack{\mathfrak{p} \\ N\mathfrak{p}\nmid k}} \frac{1}{1 - X(\mathfrak{p}) N\mathfrak{p}^{-s}} \end{aligned} \tag{24}$$

$$(\sigma > 1).$$

Denoting characters of classes $\mathfrak{H}$ by χ, we have, by [5] (14) (with $n=2$), for any positive $\eta \ll 1$

$$|\zeta(1+\eta+it, X)| \leqslant \zeta(1+\eta, X_0) = \zeta(1+\eta, \chi_0) \ll \eta^{-2}.$$

According to §§ 2, 3 each class $\mathfrak{C}$ is the sum of $j \leqslant h$ classes $\mathfrak{H}$. By (24) and [7] (3) for $\sigma > 1$

$$\begin{aligned} \zeta(s, \mathfrak{C}) &= \sum_{\mathfrak{H}\subset\mathfrak{C}} \zeta(s, \mathfrak{H}) = h^{-1} \sum_{\mathfrak{H}\subset\mathfrak{C}} \sum_{\chi} \overline{\chi}(\mathfrak{H})\zeta(s, \chi), \\ \zeta(s, X) &= h^{-1} \sum_{\mathfrak{C}} X(\mathfrak{C}) \sum_{\mathfrak{H}\subset\mathfrak{C}} \sum_{\chi} \overline{\chi}(\mathfrak{H})\zeta(s, \chi). \end{aligned} \tag{25}$$

Hence the functions $\zeta(s, \mathfrak{C})$ and $\zeta(s, X_0)$ are regular in the whole plane, except for a simple pole at $s=1$; the other $\zeta(s, X)$ $(X \neq X_0)$ are integral functions (since $\operatorname{Res}_{s=1}\zeta(s, \mathfrak{C}) = jh^{-1}\operatorname{Res}_{s=1}\zeta(s, \chi_0)$ does not depend on $\mathfrak{C}$ and $\sum_{\mathfrak{C}} X(\mathfrak{C}) = 0$).

By (25) and [5] (15), [5] (16) for any positive $\eta \ll 1$

$$\begin{aligned} \zeta(-\eta+it, X) &\ll h\eta^{-2}D^{1/2+\eta}(1+|t|)^{1+2\eta}, \\ |\zeta(\sigma+it, X)| &\leqslant c(\eta, D)e^{2|t|} \qquad (-\eta \leqslant \sigma \leqslant 1+\eta, \ |t| \geqslant 1). \end{aligned} \tag{26}$$

Using these estimates we can repeat all the deductions of [5], [6], [7] ([8]) with $n=2$ and X instead to χ, taking into account the changes induced

([8]) Although some of them are now superfluous and some may be simplified or improved by means of identity (30) and adequate properties of Dirichlet L-functions.

by the factor $h \ll D$ in (26). Thus we now have uniformly in $-\delta \leqslant \sigma \leqslant 1+\delta$ $(0 < \delta \leqslant 1/\log D < \frac{1}{2})$

$$\zeta(s, X) \ll \delta^{-2} D^{\frac{3}{2}(1-\sigma)}(1+|t|)^{1+\delta-\sigma},$$

provided that $|s-1| > \frac{1}{8}$ when $X = X_0$ (cf. [5] (32)). This estimate holds also for the function $\zeta(s, \mathfrak{C}) = h_1^{-1}\sum_{X} \overline{X}(\mathfrak{C})\zeta(s, X)$.

By the arguments of [7] § 2 we obtain for $x \geqslant 1$

$$\sum_{\substack{\mathfrak{a}\in\mathfrak{C} \\ N\mathfrak{a}\leqslant x}} 1 = \mu x + O(D^{3/2}x^{2/3}), \qquad \sum_{\substack{\mathfrak{a} \\ N\mathfrak{a}\leqslant x \\ (N\mathfrak{a}, k)=1}} 1 = h_1\mu x + O(D^{3/2}x^{2/3}),$$

where $\mu = h_1^{-1}\operatorname{Res}_{s=1}\zeta(s, \chi_0)$. We have

$$\begin{aligned} &\sum_{\substack{\mathfrak{p}\in\mathfrak{C} \\ N\mathfrak{p}\leqslant x}} 1 \ll x/h_1\log x \qquad (x \geqslant D^{24}, \ D \geqslant D_0), \\ &\sum_{\substack{\mathfrak{p}^m\in\mathfrak{C} \\ N\mathfrak{p}^m\leqslant x, m\geqslant 1}} \log N\mathfrak{p} \ll x/h_1 \quad \text{for} \quad x \geqslant D^{25}, \ D \geqslant D_0 \end{aligned} \tag{27}$$

(cf. [7] § 6), etc. By the method of [5] Lemma 5 we prove the estimate

$$N_X(t) \ll \log D(1+|t|), \tag{28}$$

where $N_X(T)$ denotes the number of zeros of $\zeta(s, X)$ in the rectangle $-2 \leqslant \sigma \leqslant 1$, $|t-T| \leqslant 1$ (the presence of critical zeros in $\sigma < 0$ not being excluded).

7. By an ambiguous class we denote any class $\mathfrak{C}$ for which $\mathfrak{C}^2$ is the principal class $\mathfrak{C}_1$. If $\mathfrak{C}$ is an ambiguous class, then all the characters $X(\mathfrak{C})$ are real and vice versa.

It has been proved (see e.g. [2], p. 34 and [16], p. 373) that the number of the ambiguous classes is $A = 2^{\nu-1}$, where

$$\nu = \begin{cases} \lambda & \text{if} \quad d \text{ is odd or } \ d \equiv 4 \pmod{16}, \\ \lambda+2 & \text{if} \quad d \equiv 0 \pmod{32}, \\ \lambda+1 & \text{otherwise} \end{cases}$$

and λ denotes the number of the different odd prime divisors of d.

According to [2], pp. 20-28 there are $2^{\nu-1}$ real and different Dirichlet characters $\chi_D(m)$ modulo $D = |d|$ having the same values (1 or -1) for all $m > 0$, prime with respect to D, which are representable by the primitive quadratic form

$$\psi(x, y) = ax^2 + bxy + cy^2 \qquad (d = b^2 - 4ac; \ a > 0 \text{ if } d < 0).$$

Since, by § 3, these m are norms of ideals $\mathfrak{b}$ of an appropriate class $\mathfrak{C}$, we may define 2^{r-1} real and different characters of the classes $\mathfrak{C}$ putting

$$X(\mathfrak{C}) = X(\mathfrak{b}) = \chi_D(N\mathfrak{b}) \quad \text{with} \quad \mathfrak{b} \in \mathfrak{C}. \tag{29}$$

(Consider that by (29) and the multiplicative property of χ_D we have

$$X(\mathfrak{ab}) = \chi_D(N\mathfrak{ab}) = \chi_D(N\mathfrak{a} \cdot N\mathfrak{b}) = \chi_D(N\mathfrak{a})\chi_D(N\mathfrak{b}) = X(\mathfrak{a})X(\mathfrak{b});$$

cf. [12] I, p. 83 and Satz 804).

Let $\mathfrak{G}$ denote the group of the classes $\mathfrak{C}$, $\mathfrak{G}_1$ the group of all characters $X(\mathfrak{C})$ and A_1 the number of the real characters $X(\mathfrak{C})$. Since the real characters X are the elements of second degree in $\mathfrak{G}_1$ (i.e. $XX = X_0$) and the ambiguous classes are the elements of second degree in $\mathfrak{G}$, we have $A_1 = A = 2^{r-1}$ by the isomorphism of $\mathfrak{G}$ on $\mathfrak{G}_1$. This proves

LEMMA 3. *For any real character $X(\mathfrak{C})$ there is a Dirichlet character χ_D modulo D satisfying* (29).

LEMMA 4. *For any real character $X(\mathfrak{C})$ the function $\zeta(s, X)$ satisfies*

$$\prod_{\substack{\mathfrak{p} \\ N\mathfrak{p}\mid A \\ N\mathfrak{p}\nmid k}} (1 - X(\mathfrak{p})N\mathfrak{p}^{-s})\zeta(s, X) = \sum_{m=1}^{\infty} \chi_D(m)m^{-s} \cdot \sum_{m=1}^{\infty} \chi'_D(m)m^{-s} \qquad (\sigma > 1), \tag{30}$$

where χ_D, χ'_D are Dirichlet characters modulo $D = |\Delta|k^2$ and $\chi'_D(m) = \chi_D(m)(\Delta/m)$.

Proof. Let p, q denote primes, not dividing D, such that

$$\left(\frac{\Delta}{p}\right) = 1, \quad \left(\frac{\Delta}{q}\right) = -1. \tag{31}$$

In the field K generated by $\sqrt{\Delta}$ $[q]$ is a prime ideal with the norm q^2 whereas $[p] = \mathfrak{p} \cdot \mathfrak{p}'$, $N\mathfrak{p} = N\mathfrak{p}' = p$ (see [12] Satz 881, 812). Hence, by (24), (31) and Lemma 3, the left-hand side of (30) is

$$= \prod_{\substack{\mathfrak{p} \\ \mathfrak{p}\nmid D}} \frac{1}{1 - X(\mathfrak{p})N\mathfrak{p}^{-s}} = \prod_q \frac{1}{1 - \chi_D(q^2)q^{-2s}} \left(\prod_p \frac{1}{1 - \chi_D(p)p^{-s}}\right)^2$$

$$= \prod_q \frac{1}{1 - \chi_D(q)q^{-s}} \cdot \frac{1}{1 + \chi_D(q)q^{-s}} \left(\prod_p \frac{1}{1 - \chi_D(p)p^{-s}}\right)^2$$

$$= \prod_{p,q} \frac{1}{1 - \chi_D(p)p^{-s}} \cdot \frac{1}{1 - \chi_D(q)q^{-s}} \prod_{p,q} \frac{1}{1 - \chi_D(p)p^{-s}} \cdot \frac{1}{1 + \chi_D(q)q^{-s}}$$

$$= \prod_{p,q} \frac{1}{1 - \chi_D(p)p^{-s}} \cdot \frac{1}{1 - \chi_D(q)q^{-s}} \prod_{p,q} \frac{1}{1 - \chi_D(p)\left(\frac{\Delta}{p}\right)p^{-s}} \cdot \frac{1}{1 - \chi_D(q)\left(\frac{\Delta}{q}\right)q^{-s}}$$

$$= \prod_r \frac{1}{1 - \chi_D(r)r^{-s}} \prod_r \frac{1}{1 - \chi'_D(r)r^{-s}},$$

where r runs through all primes not dividing D. Kronecker's symbol (Δ/m) being a real character modulo $|\Delta|$ (see [12] I, p. 83) is also one modulo D, the lemma follows.

By identity (30) the problem about the distribution of the zeros near the line $\sigma = 1$ of $\zeta(s, X)$ for a real character $X(\mathfrak{C})$ is reduced to the same problem for Dirichlet functions $L(s, \chi_D)$. Now using [14] IV Satz 5.8, 6.8, 6.1, 8.2 we get the following

LEMMA 5. *For an appropriate absolute constant $c_1 > 0$ in the region*

$$\sigma \geqslant 1 - c_1/\log D(1 + |t|)$$

there is at most one zero $1 - \delta$ of at most one function $\zeta(s, X)$ with a real character $X(\mathfrak{C})$; δ is real and for any $\varepsilon > 0$

$$\delta > c_2(\varepsilon)D^{-\varepsilon}, \tag{32}$$

where $c_2(\varepsilon) > 0$ does not depend on D.

(32) is the analogue of Siegel's theorem for functions $\zeta(s, X)$.

8. In the previous paragraphs 3, 6, 7 we have proved or sketched proofs of everything that is necessary to adjust the deductions of [4] to the functions $\zeta'/\zeta(s, X)$. It remains only to remove the obstacle connected with the probable existence of zeros of $\zeta(s, X)$ in the strip $-1 < \sigma < 0$. Using (28) we shall prove that there is a line L in the strip $-\frac{1}{2} - 2D^{-1/2} \leqslant \sigma \leqslant -\frac{1}{2}$ such that

(i) the distance between any point $\sigma + it \in L$ and the nearest zero of the function

$$Z(s) = \prod_X \zeta(s, X)$$

for $D > D_0$ is $> 1/D^{4/3}\log(2 + |t|)$ and

(ii) the length of the piece of L between any two of its points $\sigma_1 + it$, $\sigma_2 + i(t+1)$ is < 2.

In order to construct the line L let us first cut the strip $-\frac{1}{2} - 2D^{-1/2} \leqslant \sigma \leqslant -\frac{1}{2}$ into the rectangles R_g $(g - \frac{3}{4} \leqslant t \leqslant g + \frac{3}{4})$ $(g = 0, \pm 1, \ldots)$. By (28) the number of zeros of $Z(s)$ in R_g is $< N = c_3 h_1 \log D(1 + |g|)$ for an appropriate constant c_3. By vertical lines (i.e. runing parallel to the imaginary axis) we cut R_g into N equal strips; in at least one of them there is no zero of $Z(s)$. Let l_g denote the vertical line halving that strip. The distance between any point $\sigma + it$ of l_g (with $|t - g| \leqslant \frac{2}{3}$) and the nearest zero of $Z(s)$ is evidently $> 1/ND^{1/2}$. In a similar way we deduce the existence of a horizontal segment l'_g in

$$(g + \tfrac{1}{2} \leqslant t \leqslant g + \tfrac{1}{2} + 2D^{-1/2}, \quad -\tfrac{1}{2} - 2D^{-1/2} + 1/ND^{1/2} \leqslant \sigma \leqslant -\tfrac{1}{2} - 1/ND^{1/2})$$

such that the distance between any point of l'_g and the nearest zero of $Z(s)$ is $> 1/ND^{1/2}$. Now the broken line L which is built up by the segments

of l_g between l'_{g-1} and l'_g together with the segments of l'_g between l_g and l_{g+1} ($g = 0, \pm 1, \ldots$) evidently has the required properties (i), (ii) (see (23)).

In the formula corresponding to [4] (15) integrating along the line L and using (23), (28) and [5] (42) (with X instead of χ) we get the remaining term $O(D^3)$ and may proceed as in [4], except that the sum

$$\Phi(x, y, \mathfrak{C}) = h_1 \sum_{\substack{\mathfrak{p}, m \\ \mathfrak{p}^m \in \mathfrak{C} \\ m \geqslant 1}} \exp\left(-\frac{\log^2 N\mathfrak{p}/x}{4y}\right) N\mathfrak{p}^{m/2} \log N\mathfrak{p}$$

(with

$$x = D^{\xi},\ \xi \geqslant 0; \qquad y = (\eta/\nu)\log D,$$
$$1 < \eta_0 \leqslant \eta \leqslant \eta_0 + B, \qquad 1 \leqslant \nu \leqslant \min(e^{\alpha\xi}, \log D),$$

where η_0, B and $1/\alpha$ are sufficiently large absolute constants) is to be divided into five partial sums as in § 5. Proving the estimate $S_1 \ll x^{3/2}e^{2\nu}$ for the part of that sum with $\mathfrak{p}^m \in \mathfrak{C}$, $m \geqslant 1$, $N\mathfrak{p} \geqslant z = xe^{4\nu}$, we make use of (27) which is justified if $z \geqslant D^{25}$; consider that for $\xi \leqslant 25$ we have

$$y \geqslant \eta_0 e^{-25\alpha} \log D$$

whence

$$z \geqslant e^{4\nu} > D^{25},$$

provided that η_0 is large enough. In this way we come to the following result: *There are positive absolute constants c, c' such that for any positive $\varepsilon \leqslant c$, $D \geqslant D_0(\varepsilon)$, $x \geqslant D^{c' \log(c/\varepsilon)}$ and any fixed primitive binary quadratic form ψ with the discriminant d ($\neq k^2$) in absolute value $= D$ there is a prime*

$$p \in (x, xD^{\varepsilon})$$

representable by ψ. The number of primes $p \leqslant x$ representable by the form ψ is

$$\pi(x, \psi) > x/h_1 D^{2\varepsilon} \log x \quad \text{for} \quad x \geqslant D^{c' \log(c/\varepsilon) + \varepsilon}.$$

These statements hold for $d = k^2$ as well and may be proved as follows. Supposing $d = k^2$ we deduce $\psi = (\alpha u + \beta v)(\gamma u + \delta v)$, where u, v are variables and α, β, γ, δ rational integers with $(\alpha, \beta) = 1$, $(\gamma, \delta) = 1$ and $(\alpha\delta + \beta\gamma)^2 - 4\alpha\gamma\beta\delta = d$ or $(\alpha\delta - \beta\gamma)^2 = k^2$. If a prime p is representable by the form ψ, then the linear factors of ψ have the values 1, p (or -1, $-p$), respectively. We may suppose

$$\alpha u + \beta v = 1, \qquad \gamma u + \delta v = p \tag{33}$$

(otherwise change the rôles of $\alpha, \beta, \gamma, \delta$ or change u, v to $-u$, $-v$). From the first equation (33)

$$u = u_0 - \beta t, \qquad v = v_0 + \alpha t,$$

where u_0, v_0 is a particular solution and $t = 0, \pm 1, \ldots$ Now by the second equation (33)

$$(\alpha\delta - \beta\gamma)t + (\gamma u_0 + \delta v_0) = p$$

or

$$kt + l = p, \quad \text{where} \quad k = \alpha\delta - \beta\gamma, \quad l = \gamma u_0 + \delta v_0 \tag{34}$$

and $(k, l) = 1$. (If k and l have a common divisor $j > 1$, then from

$$ku_0 = \delta - \beta l, \qquad kv_0 = \alpha l - \gamma,$$

which is a consequence of $\alpha u_0 + \beta v_0 = 1$, $\gamma u_0 + \delta v_0 = l$, we deduce that δ and γ are divisible by j, whence ψ is not a primitive form.) Conversely from (34) and $\alpha u_0 + \beta v_0 = 1$ we deduce (33). Hence the primes representable by the form ψ with $d = k^2$ are $\equiv l \pmod k$ and the desired result follows from the theorem proved in [4].

References

[1] P. Bachmann *Allgemeine Arithmetik der Zahlenkörper*, Leipzig 1905.

[2] P. Bernays, *Über die Darstellung von positiven ganzen Zahlen durch die primitiven binären quadratischen Formen einer nicht-quadratischen Diskriminante*. Dissertation. Göttingen 1912.

[3] E. Fogels (Э. К. Фогелс), *О простых числах в начале арифметической прогрессии* (in Russian), Dokl. Akad. Nauk SSSR 102 (1955), pp. 455-456.

[4] — *On the existence of primes in short arithmetical progressions*, Acta Arith. 6 (1961), pp. 295-311.

[5] — *On the zeros of Hecke's L-functions I*, Acta Arith. 7 (1961), pp. 87-106.

[6] — *On the zeros of Hecke's L-functions II*, ibid. pp. 131-147.

[7] — *On the zeros of Hecke's L-functions III*, ibid. pp. 225-240

[8] R. Fricke, *Lehrbuch der Algebra III*, Braunschweig 1928.

[9] E. Hecke, *Über die L-Funktionen und den Dirichletschen Primzahlsatz für einen beliebigen Zahlkörper*, Göttinger Nachrichten, Math. ph. Klasse 1917, pp. 299-318.

[10] E. Landau, *Abschätzungen von Charaktersummen, Einheiten und Klassenzahlen*, Göttinger Nachrichten, Math. ph. Klasse 1918, pp. 79-97.

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

[12] — *Vorlesungen über Zahlentheorie I, III*, Leipzig 1927.

[13] Yu. V. Linnik, *On the least prime in arithmetical progression. I. The basic theorem; II. The Deuring-Heilbronn's phenomenon*, Mat. Sb. N. S. 15 (57) (1944), pp. 139-178; 347-367.

[14] K. Prachar, *Primzahlverteilung*, Berlin 1957.

[15] K. Rodosskiĭ (К. А. Родосский), *О наименьшем простом числе в арифметической прогрессии* (in Russian), Mat. Sb. N. S. 34 (76) (1954), pp. 331-356.

[16] H. Weber, *Lehrbuch der Algebra III*, Braunschweig 1908.

[17] W. Weber, *Bemerkungen zur arithmetischen Theorie der binären quadratischen Formen*, Nachr. Gesellschaft Wiss. Göttingen, Math. ph. Klasse 1929, pp. 116-130.

Reçu par la Rédaction le 25. 4. 1961