ACTA ARITHMETICA
XI (1966)

On the abstract theory of primes III

by

E. Fogels (Riga)

Introduction

1. In the previous papers ([10], [11] and [12], §§ 14-18) we have been dealing with an infinite semigroup $\mathfrak{G}$ on a countable number of generators $\mathfrak{b}$, the elements of $\mathfrak{G}$ generally being denoted by $\mathfrak{a}$. We have supposed the following:

(i) The elements $\mathfrak{a} \in \mathfrak{G}$ are distributed into classes H_j $(1 \leqslant j \leqslant h)$ forming an Abelian group Γ, and the number of classes satisfies

$$1 \leqslant h \leqslant D \tag{1}$$

where D is a parameter $\geqslant D_0 > 2$ which may increase indefinitely.

(ii) There is a homomorphism N of $\mathfrak{G}$ into the multiplicative semigroup of real numbers $\geqslant 1$ such that the images $a = N\mathfrak{a}$ for all $x \geqslant 1$ satisfy

$$\sum_{\substack{\mathfrak{a} \in H_j \\ a \leqslant x}} 1 = \varkappa x + O(D^{c_1} x^{1-\vartheta}), \qquad \varkappa = D^l \tag{2}$$

where the constants l, c_1, ϑ do not depend on j $(0 \leqq l \ll 1, 0 \leqslant c_1 \ll 1$, $0 < \vartheta \leqslant 1)$.

(iii) If in (2) $\vartheta \leqslant \frac{1}{2}$, then for a suitable constant $c_2 > 0$ we have[1]

$$\lim_{x \to \infty} \left(\sum_{\substack{\mathfrak{a} \in \Gamma' \\ a \leqslant x}} \frac{1}{a} - \sum_{\substack{\mathfrak{a} \notin \Gamma' \\ a \leqslant x}} \frac{1}{a} \right) > D^{-c_2} \tag{3}$$

where Γ' denotes any subgroup of the group Γ with the index 2.

---

[1] By the sum over all $\mathfrak{a} \in \Gamma'$ in (3) we actually mean a double sum over all $\mathfrak{a} \in H$ with H running through all the classes $H_j \in \Gamma'$. A similar remark concerns the sum over all $\mathfrak{a} \notin \Gamma'$.

(iv) There is a homomorphism I of $\mathfrak{G}$ into a multiplicative semigroup of complex numbers such that the images

$$I\mathfrak{a} = \sqrt{a}\, e^{2\pi i a} \qquad (a = N\mathfrak{a} \geqslant 1,\ 0 \leqslant \alpha < 1)$$

of the elements $\mathfrak{a} \in \mathfrak{G}$ next to (1) and (2) satisfy

$$\sum_{\substack{\mathfrak{a} \in H_j \\ a \leqslant x, 0 \leqslant \alpha < \varphi}} 1 = \varkappa \varphi x + O(D^{c_1} x^{1-\vartheta'}), \qquad 0 \leqslant \vartheta' \leqslant \vartheta \tag{4}$$

(with ϑ' independent of j) uniformly in $0 < \varphi \leqslant 1$.

Using (i), (ii) and (iii) in [10] we proved the existence of a generator $\mathfrak{b} \in H$ with $N\mathfrak{b} \in (x, xD^{c_3})$ for any class H and any $x \geqslant 1$, $c_3 = c_3(c_1, c_2, \vartheta, l)$ being a suitable positive constant. After adding condition (iv), we proved in [11] the existence of $\mathfrak{b} \in H$ with $I\mathfrak{b}$ in the region

$$x < N\mathfrak{b} < xD^{c_3}, \qquad \alpha_1 \leqslant \alpha < \alpha_2 (\mathrm{mod}\, 1).$$

In [12], §§ 14-18 we proved similar results with smaller intervals for $N\mathfrak{b}$ and α.

In the present paper we shall consider some particular semigroups $\mathfrak{G}$ for which conditions (i)-(iv) are satisfied.

The most important example is given by the arithmetical progressions $Du+r$ $(u = 0, 1, \ldots)$ of natural numbers prime with respect to D. Evidently they form a group Γ and satisfy (2) with $\vartheta = 1$, $c_1 = 1$.

From this example we arrive by generalization at classes $\mathfrak{H} \bmod \mathfrak{f}$ of ideals in the algebraic field K_n of degree n and discriminant Δ. These classes form a group (cf. [18], Satz XXX) and the number h of classes satisfy (1) with $D = |\Delta| N\mathfrak{f}$, where $N\mathfrak{f}$ is the norm of the ideal $\mathfrak{f}$ (cf. [8], Lemma 2). Using Landau's method in § 2 we shall prove for any $x \geqslant 1$ the estimate

$$\sum_{\substack{\mathfrak{a} \in \mathfrak{H} \\ N\mathfrak{a} \leqslant x}} 1 = \varkappa x + O(D^{17/12} x^{(n-1)/(n+1)}), \tag{5}$$

where

$$\varkappa = h^{-1} D^{o(1)} \qquad (D \to \infty). \tag{6}$$

Thus for the classes $\mathfrak{H}$ condition (ii) is satisfied with $\vartheta = 2/(n+1)$.

If $n = 2$ (the quadratic field), then $\vartheta > \frac{1}{2}$, whence in this case (iii) is superfluous. For any $n \geqslant 1$, the left-hand side of (3) being the value $\zeta(1, \chi)$ of the Hecke L-function with a real non-principal character χ (cf. [10], § 19), the inequality is satisfied by [6], p. 105.

Thus (iii) holds for any K_n (independently of $\vartheta > \frac{1}{2}$ or $\leqslant \frac{1}{2}$) and instead of (5) we could do with [7], (8) which is a weaker result. Nevertheless we shall go through a brief sketch of the proof of (5), since the result may be interesting in itself as providing a non-trivial example of a semigroup $\mathfrak{G}$ (namely that of the ideals in any quadratic field) for which (iii) is superfluous because of $\vartheta > \frac{1}{2}$.

In the further part of the present paper we shall confine ourselves to the case $n = 2$. Following Hecke [14] we shall replace ideals by a homomorphic system of ideal numbers. In this way we establish the homomorphism I on which relation (iv) rests.

In §§ 3-6 we shall prove that the estimate

$$\sum_{\substack{\mathfrak{a} \in \mathfrak{H}, N\mathfrak{a} \leqslant x \\ \alpha_1 \leqslant \alpha < \alpha_1 + \varphi (\mathrm{mod}\, 1)}} 1 = \varkappa \varphi x + O(D^{2/3} x^{\theta}) \tag{7}$$

with any fixed $\theta > \frac{2}{3}$ holds for all $x \geqslant 1$ uniformly in $0 \leqslant \alpha_1 \leqslant 1$, $0 < \varphi \leqslant 1$. Hence for the ideals in any quadratic field K_2 condition (iv) is satisfied. Conditions (i)-(iii) being satisfied as well (by what was said before), we deduce that the two-dimensional distribution theorems of [11] and [12], §§ 15-18 hold for the ideal primes over K_2.

In §§ 7-10 we shall deal with primitive binary quadratic forms

$$F(x_1, x_2) = ax_1^2 + bx_1x_2 + cx_2^2$$

where the coefficients and variables are rational integers, the discriminant being

$$D = b^2 - 4ac = \Delta Q^2$$

(Δ — fundamental discriminant). It has been shown by Hecke ([14], § 8), that to any representation $p = |F(x_1, x_2)|$ of a rational prime p in the field K_2 generated by $\sqrt{\Delta}$ corresponds a representation of an ideal prime $\hat{\pi}$ by a linear form $\hat{\alpha}_1 x_1 + \hat{\alpha}_2 x_2$. And all the ideal integers representable by the latter form are $\equiv r\hat{\varrho} \,(\mathrm{mod}\, Q)$ where $\hat{\varrho}$ is a fixed ideal integer and r runs through the rational integers. In a metric associated with the form F for any two rays Ol and Ol' drawn from the origin O we shall define (after Hecke) a non-Euclidean measure φ of the angle lOl'. Then from the result of [12], § 18, we deduce the following

THEOREM. *For appropriate absolute constants c', c, θ $(0 < \theta < 1)$ and for all $x \geqslant |D|^{c'}$ in the region*

$$x < |F(x_1, x_2)| < x + x^{\theta}$$

in the x_1x_2-plane between any two straight lines starting from the origin and forming an angle with the non-Euclidean measure $\varphi \geqslant x^{-c}$ there is a lattice point (x_1, x_2) at which $|F(x_1, x_2)|$ represents a prime.

A simple interpretation of the non-Euclidean angle φ by a Euclidean area will be given in the Appendix, § 21.

COROLLARY. *Let q be any natural number, prime with respect to D, and let $x \geqslant |Dq|^{c'}$. Then for any number r of the reduced set of residues* mod q *in the domain defined by the theorem there is a lattice point (x_1, x_2) at which $|F(x_1, x_2)|$ represents a prime $\equiv r \pmod q$.*

The proof will be given in § 10.

In §§ 11-15 we shall prove an estimate for the least prime representable by a primitive ternary quadratic form $f(x_1, x_2, x_3)$ with the condition that the point (x_1, x_2, x_3) is in a given cone having its apex at the origin.

As another application of the general theory in § 16 we shall prove an estimate for the least pair of primes representable by two given linear forms in two variables.

In § 17 it will be shown that from the theorem of [10] we can deduce results about irreducible polynomials of the form

$$g(x) = r(x)+Qf(x)$$

where $r(x)$ and $f(x)$ are any given polynomials with rational integer coefficients of absolute value $\leqslant A$ ($A \geqslant 2$) and with no common polynomial divisor. It will be proved that for a suitable natural integer $Q \leqslant A^c$ (where the constant c depends merely on the degrees of r and f) the polynomial $g(x)$ is irreducible in K_1. This is an analogue of Linnik's theorem (about the smallest prime $\equiv r \pmod D$) for irreducible polynomials $\equiv r(x) \pmod{f(x)}$.

In § 19 we shall prove the corresponding theorem for the general algebraic field K_n (which in particular for $n = 1$ coincides with the previous result). The proof is given in full for $n = 2$ and outlined for larger n (see the end of § 18). An analogous theorem for polynomials over a finite field of coefficients will be proved in § 20.

Since almost all polynomials over the ring of rational integers are irreducible in K_1 (cf. [21], p. 161), it seems probable that one could easily find some shorter proof for the irreducibility of $g(x)$ than that given in the present paper, in which our aim has been to give various applications of the general theorems (proved in [10] and [11]) about the distribution of generators in a semigroup. Reducible polynomials being very scarce, it might seem more natural to prove that there is one of the form $r(x)+Qf(x)$ (Q rational integer). However, such a theorem is not true. If for example $r(x) = x^2+4x+1$ and $f(x) = 4x^2+4x+4$, then $r(x)+Qf(x)$ is irreducible in K_1, since $(4Q+4)^2-4(4Q+1)^2$ is never a rational square.

Proof of the estimate (5)

2. Let $D = |\Delta|N\mathfrak{f}$, where Δ denotes the discriminant of the algebraic field K of degree $n \geqslant 2$ and $N\mathfrak{f}$ the norm of the ideal $\mathfrak{f}$, and let $\mathfrak{H}$ be any class of ideals mod $\mathfrak{f}$. For $D \leqslant 1$ and $x \geqslant 1$ Landau (see [18], Satz XCVI, and [19], Satz 210) has proved the estimate

$$\sum_{\substack{\mathfrak{a}\in\mathfrak{H}\\ N\mathfrak{a}\leqslant x}} 1 = \varkappa x+O(x^{1-2/(n+1)}),$$

where the constant $\varkappa = \varkappa(K, \mathfrak{f})$ does not depend on $\mathfrak{H}$. By the same method one can prove (5), which is the corresponding result for $D \to \infty$.

Denoting by $\zeta(s, \chi)$ the L-functions of Hecke on the field K with characters $\chi \bmod \mathfrak{f}$ and writing

$$f(s; \chi) = \zeta(s, \chi)/\zeta(1-s, \bar{\chi})$$

we have

$$f(s; \chi) = (-i)^q W(\chi) N\mathfrak{f}^{1/2-s}\left(\frac{\cos\frac{1}{2}\pi s}{\sin\frac{1}{2}\pi s}\right)^q f(s), \tag{8}$$

where

$$f(s) = \left(\Gamma(s)\right)^{-n}(\sin\tfrac{1}{2}\pi s)^{-r_2}(\cos\tfrac{1}{2}\pi s)^{-(r_1+r_2)}|\Delta|^{1/2-s}2^{-n}(2\pi)^{ns}, \tag{9}$$

r_1 denotes the number of real conjugate fields, $r_1+2r_2 = n$, $|W(\chi)| = 1$ and q stands for a rational integer $\in[0, r_1]$ (cf. [18], pp. 105, 89 and 99).

Let $F(m)$ denote the number of ideals $\mathfrak{a}$, prime with respect to $\mathfrak{f}$, with $N\mathfrak{a} = m$. Then for all $x \geqslant 1$

$$\sum_{m\leqslant x}\frac{F(m)}{m^\vartheta} \ll D^{2/3}x^{1-\vartheta} \quad \text{if} \quad 0 < \vartheta < 1, \tag{10}$$

$$\sum_{m>x}\frac{F(m)}{m^\vartheta} \ll D^{2/3}x^{1-\vartheta} \quad \text{if} \quad \vartheta > 1. \tag{11}$$

The constants implied in the notation in these and further formulae may depend on the degree of K, but not on D, x or other parameters.

(10) and (11) may be deduced from the estimate

$$\sum_{m\leqslant x}F(m) = \lambda x+O(D^{2/3}x^{1-2/(n+3)}), \qquad \lambda = D^{o(1)} \quad (D \to \infty)$$

(see [7], (9) and [6], (13)) by means of Abel's identity (see for example [22], p. 371).

For any $w > 0$ let

$$L(w) = \int_{3/2-i\infty}^{3/2+i\infty} f(s; \chi)\,\frac{w^{s+n}}{s(s+1)\ldots(s+n)}\,ds \tag{12}$$

and let $R(w)$ denote the sum of residues of the integrand at $s = 1$ and $s = 0$. Writing

$$K(w) = L(w) - 2\pi i R(w)$$

and following Landau's arguments (see [19], Satz 207, and [18], p. 119) we can prove that

$$K(w) \ll D^{1+1/2n} w^{n-1/2-1/2n}, \qquad K^{(n)}(w) \ll D^{1/2} w^{1/2-1/2n}. \tag{13}$$

In the proof we use the expansion

$$f(s;\chi) = A_0 t^{n(1/2-\sigma)} e^{-nti(\log t - A)}\left(1+O\left(\frac{1}{t}\right)\right) \qquad (s = \sigma+it,\ \sigma \ll 1,\ t \geqslant 1),$$

where

$$A_0 \ll D^{1/2-\sigma} \quad \text{and} \quad A \text{ (which is real)}$$

do not depend on t (cf. (8), (9) and [19], Satz 166). We use the fact that in (12) the integrand has a simple pole at $s = 0$ with residue $\frac{1}{n!} w^n f(0;\chi)$ where by (8) and (9) $f(0;\chi) \ll D^{1/2}$.

Writing

$$\Delta_v K(w) = \sum_{0 \leqslant l \leqslant n} (-1)^{n-l} \binom{n}{l} K(w+lv)$$

and using (13), by the arguments of [19], Satz 208, we can prove that for $w > 1$ and $0 < v < w$

$$\Delta_v K(w) \ll \begin{cases} D^{1+1/2n} w^{n-1/2-1/2n}, \\ D^{1/2} v^n w^{1/2-1/2n}. \end{cases} \tag{14}$$

Having these estimates we can follow the proof of [19], Satz 210 (cf. also [18], Satz XCV), except that dealing with $\Delta_z T(x)$ we divide the sum $\sum_m$ into two parts, $\sum_1$ and $\sum_2$, corresponding to $m < m_0$ and $m \geqslant m_0$, respectively, where

$$m_0 = zD^{1/2+1/2n}, \qquad z = x^{(n-1)/(n+1)}.$$

In estimating $\sum_1$ and $\sum_2$ we use (10), (11) and the two inequalities (14) (the first one for $\sum_2$ and the second one for $\sum_1$). Proceeding as in [19] we first deduce that for a primitive principal character $\chi = \chi_0$

$$\sum_{\substack{\mathfrak{a} \\ N\mathfrak{a} \leqslant x}} \chi(\mathfrak{a}) = c(\chi)x + O(D^{17/12-(2n)^{-2}} x^{(n-1)/(n+1)}), \qquad c(\chi_0) > 0. \tag{15}$$

By means of this result we can prove (15) (but with $c(\chi) = 0$) for any primitive character $\chi \neq \chi_0$ (cf. [18], p. 121). Let us denote the left-hand side of (15) by $H(x;\chi)$.

For any non-primitive χ there is a primitive character X such that

$$H(x;\chi) = \sum_{\mathfrak{b} \mid \mathfrak{f}} \mu(\mathfrak{b}) X(\mathfrak{b}) H\left(\frac{x}{N\mathfrak{b}}, X\right),$$

$\mu(\mathfrak{b})$ being the Möbius function of ideals. From this and (15) we deduce that for any χ (primitive or not)

$$H(x;\chi) = c_1(\chi)x + O(D^{17/12} x^{(n-1)/(n+1)}),$$

where $c_1(\chi) = 0$ if $\chi \neq \chi_0$. Now proceeding as in [18], Satz XCVI, we get (5).

By [18], Satz XCVI, the constant $\varkappa$ in (5) is the same for all classes $\mathfrak{H} \bmod \mathfrak{f}$. By a theorem of R. Brauer

$$h\varkappa = \operatorname*{Res}_{s=1} \zeta(s, \chi_0) = D^{o(1)} \qquad \text{as} \qquad D \to \infty$$

(cf. [6], (13)), which is equivalent to (6).

The exponent of D in the remaining term in (5) could be improved, but it is of no importance in the present paper.

Proof of the estimate (7)

3. We begin by a short description of the system $\mathfrak{Z}$ of 'ideal' numbers $\hat{\mu}$ as introduced by Hecke [14].

Let $\mathfrak{R}$ denote the ordinary classes of ideals $\mathfrak{a}$ in a given algebraic field K of degree n, and let $\mathfrak{R}_1, \ldots, \mathfrak{R}_l$ be a basis of the group of classes $\mathfrak{R}$. Having chosen fixed ideals $\mathfrak{b}_1 \in \mathfrak{R}_1, \ldots, \mathfrak{b}_l \in \mathfrak{R}_l$, we can represent any ideal in K as

$$\mathfrak{a} = \varrho \mathfrak{b}_1^{a_1} \ldots \mathfrak{b}_l^{a_l} \tag{16}$$

where ϱ is a number in K and the exponents a_j $(1 \leqslant j \leqslant l)$ are rational integers. Each a_j is unique except for additive multiples of the least natural number h_j such that $\mathfrak{b}_j^{h_j}$ is a principal ideal:

$$\mathfrak{b}_j^{h_j} = (\beta_j). \tag{17}$$

The number $\beta_j \in K$ in (17) is unique except for a factor η which runs through the unities of K.

Introducing the numbers

$$\hat{\beta}_j = \sqrt[h_j]{\beta_j} \tag{18}$$

(with some arbitrarily fixed values of the surds) we may replace the ideals (16) by the isomorphic system $\mathfrak{Z}$ of complex numbers

$$\hat{\mu} = \varrho \hat{\beta}_1^{a_1} \ldots \hat{\beta}_l^{a_l} \tag{19}$$

with a unique factorization. Then to every ideal $\mathfrak{a} \in K$ corresponds a principal ideal $(\hat{\mu})$ such that $(\hat{\mu}) = (\hat{\mu}_1)$ if and only if $\hat{\mu}$ and $\hat{\mu}_1$ are associate numbers, i.e. if $\hat{\mu}_1 = \eta\hat{\mu}$ (where η is a unity in K) and vice versa. Generally the numbers $\hat{\mu} \in \mathfrak{Z}$ are not in K.

The numbers $\hat{\mu} \in \mathfrak{Z}$ can be distributed into $h = h_1 \dots h_l$ classes $\hat{\mathfrak{R}}$ such that the sums and the differences of numbers of the same class $\hat{\mathfrak{R}}$ are again in $\hat{\mathfrak{R}}$. If in the set of the conjugate fields of K there are complex conjugate fields K and K'(say), then the values of the surds in (18) are chosen in such a manner that $\hat{\beta}_j$ and $\hat{\beta}'_j$ are conjugate complex numbers.

Denoting by $\hat{\mu}^{(q)}$ $(q = 1, \dots, n)$ the ideal numbers corresponding to conjugate fields, we define the norm

$$N\hat{\mu} = \hat{\mu}^{(1)} \dots \hat{\mu}^{(n)}. \tag{20}$$

If $\mathfrak{a}$ denotes the ideal corresponding to $\hat{\mu}$, then from (16)-(20) we deduce that $N\hat{\mu}$ is in modulus $= N\mathfrak{a}$.

4. In this section our aim is the proof of condition (7) for the semigroup of numbers representable by binary quadratic forms of discriminant $d = \Delta Q^2$ (Δ — fundamental discriminant). In the proof we shall use the Hecke zeta-functions with Grössencharaktere on the quadratic field K generated by $\sqrt{\Delta}$. Using the system $\mathfrak{Z}$ of complex numbers $\hat{\mu} = N\mathfrak{a}e^{2\pi i\alpha}$ Hecke gets a representation of the ideals by two-dimensional vectors.

In the following let $\chi((\hat{\mu}))$ denote the group characters of the ideal classes $\mathfrak{H} \bmod \mathfrak{f}$ (see [18], p. 67).

First let us consider the case of $d < 0$ or that of an imaginary K. Then the Grössencharaktere are (cf. [14], § 9)

$$X(\hat{\mu}) = \left(\frac{\hat{\mu}}{|\hat{\mu}|}\right)^{gm} \chi((\hat{\mu})) \tag{21}$$

where g denotes the number of units $\bmod \mathfrak{f}$ (in general $g = 1$) and m is any rational integer. The function

$$\zeta(s, X) = \frac{1}{g'} \sum_{\hat{\mu}} \frac{X(\hat{\mu})}{|N\hat{\mu}|^s} \qquad (\sigma > 1) \tag{22}$$

(where g' denotes the number of units in K and $\hat{\mu}$ runs through all ideal integers $\neq 0$) admits of analytic continuation over the whole plane, except for a simple pole at $s = 1$ with residue $\mu_0 > 0$ in the case where

$$X(\hat{\mu}) = X_0(\hat{\mu}) = \begin{cases} 1 & \text{if } \hat{\mu}, \mathfrak{f} \text{ are prime to one another,} \\ 0 & \text{otherwise.} \end{cases}$$

In the case of a primitive character χ the function $\zeta(s, X)$ satisfies the functional equation

$$\zeta(s, X) = W(X)A^{1-2s} \frac{\Gamma(1-s+\frac{1}{2}g|m|)}{\Gamma(s+\frac{1}{2}g|m|)} \zeta(1-s, \bar{X}), \tag{23}$$

where

$$|W(X)| = 1, \qquad A = \frac{1}{2\pi}|\sqrt{\Delta N\mathfrak{f}}|$$

(see [14], pp. 34, 44). The Dedekind zeta-function of the field K, $\zeta_K(s)$, being a product $L_0(s)L_1(s)$ of Dirichlet L-functions with the principal character and, respectively, a non-principal real character modulo $D = |\Delta|N\mathfrak{f}$, we have in $\sigma > 1$

$$\zeta(\sigma+it, X) \ll \zeta_K(\sigma) = L_0(\sigma)L_1(\sigma) \leqslant \zeta(\sigma)L_1(\sigma) \ll (\sigma-1)^{-1}\log D \tag{24}$$

(cf. [20] I, p. 83; III Satz 882 and [24], p. 31). By the identity $\Gamma(s+1) = s\Gamma(s)$ and the asymptotic estimate

$$\Gamma(\sigma+it) = \sqrt{2\pi}\, e^{-|t|\pi/2}|t|^{\sigma-1/2}\{1+O(|t|^{-1})\} \qquad (\sigma \ll 1,\ |t| \to \infty)$$

([22], p. 395) for any even $g|m| = 2k$ and $s = -\delta+it$ $(0 < \delta < \frac{1}{2})$ we have

$$\frac{\Gamma(1-s+\frac{1}{2}g|m|)}{\Gamma(s+\frac{1}{2}g|m|)} = \frac{k+\delta-it}{k-1-\delta+it} \cdot \frac{k-1+\delta-it}{k-2-\delta+it} \cdots \frac{2+\delta-it}{1-\delta+it} \cdot \frac{\Gamma(2+\delta-it)}{\Gamma(1-\delta+it)}$$

$$\ll \frac{k+\delta}{k-1-\delta} \cdot \frac{k-1+\delta}{k-2-\delta} \cdots \frac{2+\delta}{1-\delta} (1+|t|)^{1+2\delta}$$

$$\ll k \frac{1+\delta/(k-1)}{1-\delta/(k-1)} \cdot \frac{1+\delta/(k-2)}{1-\delta/(k-2)} \cdots \frac{1+\delta/2}{1-\delta/2} (1+|t|)^{1+2\delta}$$

$$\ll k(1+|t|)^{1+2\delta} \exp\left(\sum_{j=1}^{k-2} \log \frac{1+\delta/(k-j)}{1-\delta/(k-j)}\right)$$

$$\ll k(1+|t|)^{1+2\delta} \exp\left(2\delta \sum_{j=1}^{k} \frac{1}{j} + c_3\right) \ll k^{1+2\delta}(1+|t|)^{1+2\delta} \ll \{(1+|m|)(1+|t|)\}^{1+2\delta}.$$

In the case of an odd $g|m|$ we use the same reduction in the Γ factor until we arrive at

$$\Gamma(\tfrac{3}{2}+\delta-it)/\Gamma(\tfrac{1}{2}-\delta+it) \ll (1+|t|)^{1+2\delta}$$

and get the same estimate. Hence, by (23) and (24)

$$\zeta(-\delta+it, X) \ll D^{1/2+\delta}\{(1+|m|)(1+|t|)\}^{1+2\delta}\delta^{-1}\log D. \tag{25}$$

Arguing as in [6], p. 91, we can prove that (25) holds as well for any non-primitive χ.

From (23) and a theorem of Doetsch (see [22], p. 400) we can deduce that in $-\frac{1}{2} \leqslant \sigma \leqslant \frac{3}{2}$

$$|\zeta(s, X)| < c_4(D, m)\exp(e^{c_5|t|}).$$

Hence, by (24) and (25), we have

$$\zeta(\sigma+it, X) \ll \delta^{-1}D^{(1-\sigma)/2}\{(1+|m|)(1+|t|)\}^{1+\delta-\sigma}\log D \tag{26}$$

uniformly in $-\delta \leqslant \sigma \leqslant 1+\delta$ $(0 < \delta \leqslant 1/\log D < \frac{1}{2})$. For the principal character X_0 this is true with the restriction $|s-1| > \frac{1}{8}$ (cf. [6], p. 93).

5. Let $\mathfrak{a}$ be that ideal in K which corresponds to the number $\hat{\mu}$ in (22). Then, by § 3, $N\mathfrak{a} = |N\hat{\mu}|$ and writing $X(\mathfrak{a})$ in place of $X(\hat{\mu})$, we have

$$\zeta(s, X) = \sum_{\mathfrak{a}} \frac{X(\mathfrak{a})}{N\mathfrak{a}^s} \quad (\sigma > 1). \tag{27}$$

Hence, by a generalization of Landau's formula (cf. [22], p. 376),

$$\sum_{\substack{\mathfrak{a} \\ N\mathfrak{a} \leqslant x}} X(\mathfrak{a}) - \frac{1}{2\pi i}\int_{\eta-iT}^{\eta+iT} \frac{x^s}{s}\zeta(s, X)\,ds \ll \frac{x^\eta}{T(\eta-1)^2} + \frac{x^{1+\varepsilon}}{T} + x^\varepsilon,$$

where $x > 1$, $T > 1$, $1 < \eta < 2$, $\varepsilon > 0$ stands for an arbitrarily small constant, and the constant implied in the notation depends on ε. Writing

$$X(\mathfrak{a}) = \chi(\mathfrak{a})e^{2\pi i m\alpha}, \quad \alpha = \alpha(\mathfrak{a}),$$

we deduce

$$\sum_{\substack{\mathfrak{a} \in \mathfrak{H} \\ N\mathfrak{a} \leqslant x}} e^{2\pi i m\alpha} - \frac{h^{-1}}{2\pi i}\sum_{\chi}\overline{\chi}(\mathfrak{H})\int_{\eta-iT}^{\eta+iT}\frac{x^s}{s}\zeta(s, X)\,ds \ll \frac{x^\eta}{T(\eta-1)^2} + \frac{x^{1+\varepsilon}}{T} + x^\varepsilon. \tag{28}$$

Now let

$$x \geqslant D > e, \quad 1+|m| \leqslant x^{1/3}, \quad \eta = 1+1/\log x, \quad (1+|m|)T = x^{2/3}.$$

We replace the path of integration by straight lines L_1, L_2, L_3 joining successively the points $\eta-iT$, $1/\log D x-iT$, $1/\log D x+iT$, $\eta+iT$. By (26)

$$\int_{L_2}\frac{x^s}{s}\zeta(s, X)\,ds \ll D^{1/2}(1+|m|)T\log D x\log D\log x \ll D^{2/3}x^{2/3+\varepsilon},$$

$$\int_{L_1L_3} \ll \max\{D^{1/2}(1+|m|)\log D\log D x,\ xT^{-1}\log D\log x\} \ll D^{2/3}x^{2/3+\varepsilon}.$$

Since $T \geqslant x^{1/3}$, the right-hand side of (28) is $\ll x^{2/3+\varepsilon}$. The function $\zeta(s, X_0)$ (corresponding to $\chi = \chi_0$, $m = 0$) has a simple pole at $s = 1$ with residue

$$\mu_0 = \operatorname*{Res}_{s=1}\zeta(s, X_0) \leqslant L_1(1) \ll \log D$$

(cf. (24)). Hence, by (27),

$$\sum_{\substack{\mathfrak{a} \in \mathfrak{H} \\ N\mathfrak{a} \leqslant x}} e^{2\pi i m\alpha} = \lambda_m x + O(D^{2/3}x^{2/3+\varepsilon}), \tag{29}$$

where $\lambda_m = h^{-1}\mu_0$ if $m = 0$, and $\lambda_m = 0$ otherwise.

If $1 \leqslant x < D$, then (29) holds trivially by the estimate

$$\sum_{\substack{\mathfrak{a} \in \mathfrak{H} \\ N\mathfrak{a} \leqslant x}} 1 = \lambda_0 x + O(D^{2/3}x^{3/5})$$

(see [7], (8)), which has been proved for any $x \geqslant 1$.

By I. M. Vinogradov's lemma there is a periodic function $f(\alpha)$ with the period 1 such that

$f(\alpha) = 1$ in a given interval $[\alpha_1, \alpha_2](\mathrm{mod}\,1)$ of the length $\varphi = \alpha_2 - \alpha_1$ $(0 < \varphi < 1)$;

$0 \leqslant f \leqslant 1$ in the intervals $[\alpha_1-\Delta, \alpha_1]$ and $[\alpha_2, \alpha_2+\Delta]$ (where $0 < \Delta < \frac{1}{2}(1-\varphi)$);

$f = 0$ for other α,

and such that the coefficients in the Fourier-expansion

$$f(\alpha) = \sum_{m=-\infty}^{\infty} d_m e^{2\pi i m\alpha}$$

satisfy

$$d_m \ll \min\{|m|^{-1}, |m|^{-1}|\Delta m|^{-r}\} \quad (m \neq 0), \qquad d_0 = \varphi+\Delta, \tag{30}$$

where r denotes any natural number (the coefficients implied in the notation depending on r. Cf. [11], § 11). Taking $\Delta = x^{-1/3+\varepsilon}$ we deduce

$$f(\alpha) = \sum_{|m| \leqslant x^{1/3}} d_m e^{2\pi i m\alpha} + O\Big(\sum_{m > x^{1/3}} m^{-1-3r\varepsilon}\Big).$$

For $r \geqslant 1/\varepsilon$ the latter sum being $\ll x^{-1}$, we have

$$\sum_{\substack{\mathfrak{a} \in \mathfrak{H} \\ N\mathfrak{a} \leqslant x}} f(\alpha) = \sum_{\substack{\mathfrak{a} \in \mathfrak{H} \\ N\mathfrak{a} \leqslant x}}\Big(\sum_{|m| \leqslant x^{1/3}} d_m e^{2\pi i m\alpha} + O(x^{-1})\Big) \tag{31}$$

$$= \sum_{\substack{\mathfrak{a} \in \mathfrak{H} \\ N\mathfrak{a} \leqslant x}}\sum_{|m| \leqslant x^{1/3}} d_m e^{2\pi i m\alpha} + O(h^{-1}\mu_0 + D^{2/3}x^{-2/5}).$$

By (29) and (30)

$$\sum_{\substack{\mathfrak{a}\in\mathfrak{P}\\ N\mathfrak{a}\leqslant x}}\sum_{|m|\leqslant x^{1/3}} d_m e^{2\pi i m\alpha} = \sum_{|m|\leqslant x^{1/3}} d_m\{\lambda_m x+O(D^{2/3}x^{2/3+\varepsilon})\}$$
$$= d_0\lambda_0 x+O(D^{2/3}x^{2/3+\varepsilon}\log x) = \lambda_0\varphi x+O(D^{2/3}x^{2/3+\varepsilon}\log x),$$

whence by (31)

$$\sum_{\substack{\mathfrak{a}\in\mathfrak{P}\\ N\mathfrak{a}\leqslant x}} f(\alpha) = \lambda_0\varphi x+O(D^{2/3}x^{\theta}) \tag{32}$$

for any $\theta > \frac{2}{3}+\varepsilon$ (with the constant implied in the notation depending on θ). Taking $\varphi = \Delta$ from (32) we deduce that each of the sums

$$\sum_{\substack{\mathfrak{a}\in\mathfrak{P},N\mathfrak{a}\leqslant x\\ a_1-\Delta\leqslant a\leqslant a_1 \,(\mathrm{mod}\,1)}} 1, \qquad \sum_{\substack{\mathfrak{a}\in\mathfrak{P},N\mathfrak{a}\leqslant x\\ a_2\leqslant a\leqslant a_2+\Delta \,(\mathrm{mod}\,1)}} 1$$

is $\ll D^{2/3}x^{\theta}$. Hence the sum

$$\sum_{\substack{\mathfrak{a}\in\mathfrak{P},N\mathfrak{a}\leqslant x\\ a_1\leqslant a\leqslant a_2 \,(\mathrm{mod}\,1)}} 1$$

differs from that of (32) by at most $\ll D^{2/3}x^{\theta}$. This proves estimate (7) with $\varkappa = \mu_0/h$ for any imaginary quadratic field.

6. For the real quadratic field K the characters X (cf. [14], § 10) are

$$X(\hat{\mu}) = \left(\frac{\hat{\mu}}{|\hat{\mu}|}\right)^{a_1}\left(\frac{\hat{\mu}'}{|\hat{\mu}'|}\right)^{a_2}\chi((\hat{\mu}))e^{2\pi i m\alpha}, \qquad \alpha = \alpha(\hat{\mu}) = \frac{1}{2\log\eta}\log\left|\frac{\hat{\mu}}{\hat{\mu}'}\right|,$$

where η denotes the fundamental unit modulo $\mathfrak{f}$ ($\eta > 1$), the logarithm has its principal value and a_1, a_2 have the values 0 or 1. Supposing χ to be a primitive character, the function (27) satisfies the functional equation

$$\zeta(s, X) = W(X)A^{1-2s}\frac{\Gamma\left(\frac{1-s+a_1}{2}+\frac{\pi i m}{2\log\eta}\right)\Gamma\left(\frac{1-s+a_2}{2}-\frac{\pi i m}{2\log\eta}\right)}{\Gamma\left(\frac{s+a_1}{2}+\frac{\pi i m}{2\log\eta}\right)\Gamma\left(\frac{s+a_2}{2}-\frac{\pi i m}{2\log\eta}\right)}\zeta(1-s, \bar{X}),$$

where

$$|W(X)| = 1, \qquad A = \frac{1}{\pi}|\sqrt{\Delta N\mathfrak{f}}| = \frac{1}{\pi}D^{1/2}.$$

For $s = -\delta+it$ ($0 < \delta < \frac{1}{8}$) the term with the Γ factors satisfy

$$\frac{\Gamma\left(\frac{1+\delta+a_1}{2}+i\left(\frac{\pi m}{2\log\eta}-\frac{t}{2}\right)\right)\Gamma\left(\frac{1+\delta+a_2}{2}-i\left(\frac{\pi m}{2\log\eta}+\frac{t}{2}\right)\right)}{\Gamma\left(\frac{-\delta+a_1}{2}+i\left(\frac{\pi m}{2\log\eta}+\frac{t}{2}\right)\right)\Gamma\left(\frac{-\delta+a_2}{2}-i\left(\frac{\pi m}{2\log\eta}-\frac{t}{2}\right)\right)}$$
$$\leqslant\left(1+\left|\frac{\pi m}{2\log\eta}-\frac{t}{2}\right|\right)^{\frac{1+\delta+a_1}{2}+\frac{\delta-a_2}{2}}\left(1+\left|\frac{\pi m}{2\log\eta}+\frac{t}{2}\right|\right)^{\frac{1+\delta+a_2}{2}+\frac{\delta-a_1}{2}}$$
$$=\left(1+\left|\frac{\pi m}{2\log\eta}-\frac{t}{2}\right|\right)^{1/2+\delta+(a_1-a_2)/2}\left(1+\left|\frac{\pi m}{2\log\eta}+\frac{t}{2}\right|\right)^{1/2+\delta+(a_2-a_1)/2}$$
$$\ll (1+|m|)^{1+2\delta}(1+|t|)^{1+2\delta}.$$

Hence (25) follows for the real quadratic field and (since (24) holds also in this case) we may proceed as before. At the end we deduce that (7) holds as well for the real quadratic field.

On primes representable by binary quadratic forms

7. Let K be the quadratic field generated by $\sqrt{\Delta}$ (Δ — fundamental discriminant) and let $\hat{a}_1$, $\hat{a}_2$ be ideal integers of the same class $\hat{\mathfrak{R}}$ (as defined in § 3), prime to one another. The linear form $L(x_1, x_2) = \hat{a}_1 x_1 + \hat{a}_2 x_2$, where x_1 and x_2 run through the rational integers, will be called a primitive one if the equality $L = 0$ implies $x_1 = x_2 = 0$. In the present paragraph we shall merely quote some results from Hecke [14], § 8.

(i) For any primitive quadratic form $F(x_1, x_2) = ax_1^2+bx_1x_2+cx_2^2$ with rational integer coefficients and discriminant $b^2-4ac = \Delta Q^2$ (where Q is a natural integer and $a > 0$ if $\Delta < 0$) there is a primitive linear form $L(x_1, x_2) = \hat{a}_1x_1+\hat{a}_2x_2$ such that if $\hat{\omega}$ denotes any fixed number representable by $L(x_1, x_2)$ and $\hat{\omega}'$ denotes the corresponding number for the conjugate field, then we have identically

$$ax_1^2+bx_1x_2+cx_2^2 = \frac{|\hat{\omega}\hat{\omega}'|}{\hat{\omega}\hat{\omega}'}(\hat{a}_1x_1+\hat{a}_2x_2)(\hat{a}_1'x_1+\hat{a}_2'x_2). \tag{33}$$

(ii) For any primitive linear form $L(x_1, x_2)$ there is a quadratic form $F(x_1, x_2)$ with the properties mentioned above. In the case of $\Delta < 0$ (the imaginary field) the quadratic form is unique. If $\Delta > 0$ (the real field), then the linear form L gives rise to two quadratic forms with coefficients a, b, c and $-a$, $-b$, $-c$, respectively.

(iii) There is an ideal integer $\hat{\varrho}\in\hat{\mathfrak{R}}$ such that the set of numbers $\hat{\omega}$ representable by the primitive linear form $L(x_1, x_2)$ is identical to that of the numbers $\equiv r\hat{\varrho}\,(\mathrm{mod}\,Q)$ where r runs through the rational integers.

8. Let us consider first the case $\Delta < 0$. Then the term $|\hat{\omega}\hat{\omega}'|(\hat{\omega}\hat{\omega}')^{-1}$ in (33) is 1, and denoting by m the natural numbers representable by the given quadratic form F, we have

$$m = N\hat{\mu}, \quad \hat{\mu} \equiv r\hat{\varrho} \pmod{Q}. \tag{34}$$

To any pair of rational integers x_1, x_2 with $F(x_1, x_2) = m$ there is a unique $\hat{\mu} = \hat{\alpha}_1 x_1 + \hat{\alpha}_2 x_2$ satisfying (34) and vice versa (see [14], § 9). The pairs x_1, x_2 and y_1, y_2 are said to be associate mod$Q$ if such are the numbers $\hat{\mu} = L(x_1, x_2)$ and $\hat{\nu} = L(y_1, y_2)$.

The exponent α in the factor

$$\left(\frac{\hat{\mu}}{|\hat{\mu}|}\right)^g = e^{2\pi i a} \tag{35}$$

in (21) is evidently a function of the place in the x_1x_2-plane. We may suppose that α has the same value at all points of any fixed ray l starting from the origin (since for all $t > 0$ we have $t\hat{\mu}/|t\hat{\mu}| = \hat{\mu}/|\hat{\mu}|$). At any two rays l and l' which are associate mod$Q$ function (35) has the same value, whence the values of α differ by a rational integer. There are g rays $l = l_j$ $(0 \leqslant j \leqslant g-1$; l_j corresponding to the numbers $\hat{\mu}e^{2\pi i j/g}$ with $\hat{\mu} > 0)$ along which $\alpha \equiv 0 \pmod{1}$.

In the x_1x_2-plane with a 'cut' along the ray l_0 we can define a single-valued and continuous function α which has the value j at the points of l_j $(0 \leqslant j \leqslant g-1)$; further, let α be that particular function. Then for any two different rays l, l' starting from the origin the values of α differ by a number φ $(0 < \varphi < g)$, which is called the non-Euclidean measure of the angle (l, l'). In the Appendix (§ 21) we shall prove that for an appropriate constant λ_0 (which depends on the discriminant, but not on the particular form F)

$$\varphi = \lambda_0 A(x)/x, \tag{36}$$

where $A(x)$ denotes the Euclidean area of the sector between l, l' and the curve $F(x_1, x_2) = x$.

In the field K generated by $\sqrt{\Delta}$ the ideal integers $\hat{\mu}$ prime to Q, if divided into classes $\mathfrak{H} \bmod Q$:

$$\hat{\mu} \equiv r\hat{\varrho} \pmod{Q} \quad (r \text{ and } \hat{\varrho} \text{ fixed, depending on } \mathfrak{H})$$

and if mod$Q$ associate numbers $\hat{\mu}$ are considered as identical, by § 1 (with $\mathfrak{f} = [Q]$) evidently satisfy the conditions of the two-dimensional distribution theorem. Hence in any class $\mathfrak{H}$ there is an ideal prime number $\hat{\pi}$ such that $N\hat{\pi} = p$ (a rational prime) and $\hat{\pi}$ is in the given sector. Summing over the $\varphi(Q)$ different classes $\mathfrak{H}$ which correspond to a fixed $\hat{\varrho}$ and a variable r running through the reduced set of residues mod$Q$ (cf. [8], § 3), and using the isomorphisms considered in §§ 7 and 1, we deduce

the result stated in the theorem of § 1 for primes representable by a positive definite binary quadratic form(2).

9. Now let $F(x_1, x_2)$ be a primitive indefinite form with the discriminant $\Delta Q^2 > 0$. Then the pair of lines $F(x_1, x_2) = 0$ divides the x_1x_2-plane into four angular regions $\mathscr{A}_1, \ldots, \mathscr{A}_4$ such that in two of them $F(x_1, x_2) = |\hat{\omega}\hat{\omega}'|(\hat{\omega}\hat{\omega}')^{-1}LL'$ is positive and in the other two negative. Let us consider for example one of such regions $\mathscr{A}$, in which (cf. (33))

$$\hat{\mu}\hat{\mu}' > 0, \quad \hat{\mu} = L(x_1, x_2) = \hat{\alpha}_1 x_1 + \hat{\alpha}_2 x_2.$$

Then (34) is true again and we may proceed as in § 8, except that now

$$a = a(\hat{\mu}) = \frac{1}{2\log|\eta|} \log\left|\frac{\hat{\mu}}{\hat{\mu}'}\right|$$

(η — fundamental unit mod$Q$) is a single-valued continuous function of the ray l starting from the origin. To each l there is an infinite sequence $\ldots l, l', \ldots$ of associated ones such that for any two consecutive rays of the sequence the values of a differ by unity. If $l \in \mathscr{A}$ turns about the origin in a proper sense, then a changes monotonously from $-\infty$ to ∞.

Other conclusions remain as in § 8.

By the definition of Δ (cf. [20] I, p. 172) the quadratic form $F(x_1, x_2)$ with $D = Q^2$ has so far been excluded from our considerations. Since in this case the form F is a product of two linear forms with rational integer coefficients, the points (x_1, x_2) at which $|F|$ represent primes are distributed along four straight lines (cf. [8], p. 268) and the theorem of § 1 is no longer true.

10. In the present paragraph let $F(x_1, x_2)$ be a primitive quadratic form with the discriminant $D = \Delta Q^2 \gtrless 0$ (Δ — fundamental discriminant) and let q be any natural number, prime with respect to D. Then for any number r of the reduced set of residues mod$q$ there are rational integers r_1, r_2 such that $F(r_1, r_2) \equiv r \pmod{q}$ (see § 23). Hence for all rational integers x_1, x_2

$$F(r_1 + qx_1, r_2 + qx_2) \equiv r \pmod{q}.$$

Let $L(x_1, x_2)$ be the linear form which by (33) corresponds to F, and let

$$\hat{\mu} = L(r_1 + qx_1, r_2 + qx_2). \tag{37}$$

(2) Vaitkevičius [25] tries to prove that in any class $\mathfrak{H}$ of ideals in the imaginary quadratic field there is an ideal $\mathfrak{p}$ which belongs to a given sector with the non-Euclidean angle φ and such that the norm $N\mathfrak{p}$ is a prime $< (D/\varphi)^c$ (where c stands for a suitable absolute constant). The theorem is true and some parts of the proof are correct. However, in the proof of the main auxiliary theorem (p. 32) there are two capital errors which destroy the result.

Then

$$\hat{\mu} = q(\hat{\alpha}_1 x_1 + \hat{\alpha}_2 x_2) + (\hat{\alpha}_1 r_1 + \hat{\alpha}_2 r_2) = qL(x_1, x_2) + \hat{\mu}_0$$

(say). Since, by § 7, $L(x_1, x_2) \equiv r\hat{\varrho} \pmod{Q}$, we have $\hat{\mu} \equiv \hat{\mu}_0 + qr\hat{\varrho} \pmod{qQ}$, $\hat{\mu}_0 \equiv r_0\hat{\varrho} \pmod{Q}$. In order that the numbers $\hat{\mu}_0 + qr\hat{\varrho}$ and qQ be prime to one another, it is necessary and sufficient that

$$(38) \qquad (\hat{\mu}_0, q) = 1 \quad \text{and} \quad (r_0 + qr, Q) = 1.$$

The first of the conditions (38) is satisfied, since for an appropriate sign $\pm$ we have

$$\hat{\mu}_0\hat{\mu}_0' = \pm F(r_1, r_2) \equiv \pm r \pmod{q}.$$

Considering that $(q, Q) = 1$ we deduce that in any class mod q there are numbers r for which the second condition (38) holds.

By §§ 8 and 9 for any fixed r satisfying (38) in the set of numbers

$$\hat{\mu} \equiv \hat{\mu}_0 + qr\hat{\varrho} \pmod{qQ}$$

there are ideal primes such that the corresponding point (x_1, x_2) in (37) lies in a fixed region as given in the theorem of § 1. This proves the Corollary.

On primes representable by a ternary quadratic form (3)

11. In this section we shall deal with the form

$$(39) \qquad f(x_1, x_2, x_3) = a_{11}x_1^2 + a_{22}x_2^2 + a_{33}x_3^2 + 2a_{12}x_1x_2 + 2a_{13}x_1x_3 + 2a_{23}x_2x_3,$$

where the coefficients $a_{11}, \ldots, 2a_{23}$ are rational integers having no common divisor. Then the determinant

$$D = D(f) = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix} \qquad (\text{where } a_{ij} = a_{ji};\ i, j = 1, 2, 3)$$

is a rational number with the denominator 4. Of all the definite forms we shall consider merely those who represent non-negative numbers, which implies $D \geqslant 0$. Since $D(-f) = -D(f)$, we may confine ourselves to forms with $D \geqslant 0$. Leaving out only a finite number of form classes we shall suppose in the sequel that $D \geqslant D_0 \geqslant 2$ (4).

(3) Having met professor Turán during the mathematical conference in Leningrad 1961, I was for some time in correspondence with him. He was kind enough to suggest to me (in 1962) some problems associated with my paper [9]. The result of the work following these suggestions is embodied in § 11-15 and 17-20 of the present paper. Cf. also [10], footnote (4).

(4) We could, in fact, merely suppose that $D > 0$ (which means that $D \geqslant \frac{1}{4}$). But then in the estimate $p_1 < D^c$ of the least prime representable by the form, and elsewhere, we must replace D by $8D$ or by some larger multiple of D.

Using the fact that for any binary quadratic form of the discriminant $d \neq 0$ there is an equivalent form $ax^2 + bxy + cy^2$ with $|b| \leqslant |a| \leqslant |\frac{1}{3}d|^{1/2}$ ($d = b^2 - 4ac$; cf. [20] I, p. 135), by the arguments of [2], § 101, we first prove that for any form (39) there is an equivalent form $a_{11}'x_1'^2 + \ldots$ such that

$$|a_{11}'| \leqslant |\tfrac{4}{3}A_{33}|^{1/2}, \quad \text{where} \quad A_{33} = a_{11}a_{22} - a_{12}^2,$$

and $A_{33}' = A_{33}$, etc. Finally we deduce that there is an equivalent form whose coefficients are all in absolute value $< (10D)^4$. In what follows we take for granted that this restriction on the coefficients is satisfied already for the form (39).

Further, let c_0 denote an arbitrarily large fixed constant and let $\mathscr{K}$ be the region inside a right circular cone with the angle D^{-c_0} at the vertex which is at the origin, the axis l or $\mathscr{K}$ being any fixed ray. It is our aim to prove the existence of an absolute constant $c = c(c_0)$ such that *for any primitive form* (39) *with determinant* $D \geqslant 2$ *there is a lattice point* $(x_1, x_2, x_3) \in \mathscr{K}$ *at which* $|f|$ *represents a prime* $< D^c$.

In the case $D = 0$, if f is a product of two linear forms L_1, L_2, it may happen that they have rational integer coefficients (5). In that case all the lattice points at which $|f|$ represent primes are evidently situated in four planes and no such point may be in $\mathscr{K}$.

In the proof we shall use a suitable section of the surface $f(x_1, x_2, x_3) = \text{const}$, which reduces the problem to the corresponding one for binary quadratic form $\Phi(u, v)$, solved by the theorem of § 1. In the case of a definite f we shall have merely to prove that for an appropriate choice of the parameters the form $\Phi(u, v)$ will be a primitive one. For indefinite f we shall have to prove moreover that the discriminant of Φ will not be a square (cf. the end of § 9).

12. In this paragraph we shall be concerned with the question of the primitivity of the form Φ.

Let us first prove that by a suitable unimodular substitution

$$S = \begin{bmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{bmatrix}$$

we can ensure that in (39) $a_{11}a_{22}a_{33} \neq 0$ without violating the condition that all the coefficients are not too large ($\ll D^4$, say).

(5) In this case the system of equations

$$\alpha\alpha_1 = a_{11}, \quad \beta\beta_1 = a_{22}, \quad \gamma\gamma_1 = a_{33},$$
$$\alpha\beta_1 + \alpha_1\beta = 2a_{12}, \quad \alpha\gamma_1 + \alpha_1\gamma = 2a_{13}, \quad \beta\gamma_1 + \beta_1\gamma = 2a_{23}$$

has rational integer solutions $\alpha, \alpha_1, \beta, \beta_1, \gamma, \gamma_1$ (and vice versa) and one can find them by a finite number of trials.

Suppose that f is transformed by S into $f_1 = a'_{11}x_1'^2+\ldots$; then $a'_{11} = f(\alpha, \alpha', \alpha'')$, $a'_{22} = f(\beta, \beta', \beta'')$ and $a'_{33} = f(\gamma, \gamma', \gamma'')$. We can evidently choose two sets of coprime rational integers α, α', α'' and β, β', β'' in such a manner that $a'_{11} \neq 0$ and $a'_{22} \neq 0$. Then the Diophantine equation

$$\begin{vmatrix} \alpha & \beta & \gamma \\ \alpha' & \beta' & \gamma' \\ \alpha'' & \beta'' & \gamma'' \end{vmatrix} = 1$$

has a solution

$$\gamma = Au+Bv+C, \quad \gamma' = A'u+B'v+C', \quad \gamma'' = A''u+B''v+C'',$$

where all the coefficients $A, B, \ldots, C''$ are $\leqslant 1$ and u, v denote independent integer variables.

The case $D = 0$ being excluded, the surface $f = 0$ is either a cone with the vertex at the origin or (in the case of a definite f) the origin itself. With the plane

$$(40) \qquad x_1 = Au+Bv+C, \quad x_2 = A'u+B'v+C', \quad x_3 = A''u+B''v+C''$$

it has at most a line $\mathscr{L}$ in common. There is a lattice point $(\gamma, \gamma', \gamma'')$ which is in the plane (40) but not on the line $\mathscr{L}$, and is such that γ, γ', $\gamma'' \leqslant 1$. Then $a'_{33} = f(\gamma, \gamma', \gamma'') \neq 0$, and all the coefficients of f_1 are evidently $\leqslant D^4$.

Further, we suppose that form (39) already has these properties, i.e. that all the coefficients in (39) are $\leqslant D^4$ and $a_{11}a_{22}a_{33} \neq 0$.

Putting

$$(41) \qquad x_1 = \alpha t, \quad x_2 = \beta t \quad (\alpha \text{ and } \beta \text{ rational integers})$$

we get the binary form

$$(42) \quad \Phi(t, x_3) = f(\alpha t, \beta t, x_3)$$
$$= (a_{11}\alpha^2+2a_{12}\alpha\beta+a_{22}\beta^2)t^2+(2a_{13}\alpha+2a_{23}\beta)tx_3+a_{33}x_3^2,$$

which is certainly primitive if $|a_{33}| = 1$.

In what follows we suppose that $|a_{33}| > 1$ and we denote by p any prime dividing a_{33}. (39) being a primitive form, at least one of its other coefficients is not divisible by p. If one of the coefficients $2a_{13}$, $2a_{23}$ possesses this property, then for a suitable choice of α and β from the set of numbers $\equiv 0, 1 \pmod p$ the coefficient $2a_{13}\alpha+2a_{23}\beta = B$ (say) is not divisible by p. Considering separately the cases where exactly one or two or none of the coefficients a_{11}, $2a_{12}$, a_{22} are divisible by p, we secure in the same manner that $a_{11}\alpha^2+2a_{12}\alpha\beta+a_{22}\beta^2 = A$ (say) is not divisible by p.

Now suppose that p runs through all the different prime divisors of a_{33} and that for each of them we have fixed values of $\alpha, \beta \pmod p$ such that one or the other of the numbers A and B is not divisible by p. Then solving a system of linear congruences we can find values of α and $\beta \bmod P$ (where $P \leqslant |a_{33}|$ is the product of all different primes dividing a_{33}) for which (42) is a primitive form.

13. We suppose that the axis l of $\mathscr{K}$ forms an angle $\geqslant \frac{1}{4}\pi$ with the axis x_3 (otherwise we change the rôles of the axes x_1, x_2, x_3). Projecting $\mathscr{K}$ on the plane x_1x_2 we get an angular region $\mathscr{A}$ between two straight lines starting from the origin and forming an angle $\varphi \geqslant D^{-c_0}$ bisected by the projection l_0 of l. Let $\mathscr{A}'$ be that part of $\mathscr{A}$ which lies between the trisectors of $\mathscr{A}$.

Choosing a large constant c_3 (which will be specified later on) we denote by A_0 that point of l_0 which is at the distance D^{c_3} from the origin. Let R be a square with sides $= |a_{33}|$ running parallel to the axes x_1, x_2 and having a vertex at A_0. Taking $c_3 = c_3(c_0)$ large enough we ensure that R lies entirely in $\mathscr{A}'$. According to § 12 there is in R a lattice point $x_1 = \alpha$, $x_2 = \beta$ such that the form (42) is a primitive one. Denoting by d its discriminant and considering the restrictions imposed on the coefficients $a_{11}, \ldots, 2a_{23}$ in § 12, we deduce that $|d| \leqslant D^{c_4}$ for appropriate $c_4 \leqslant 1$.

In the present paragraph let us confine ourselves to the case of a definite form f. Then so is the form (42), whence $d < 0$. To the section of $\mathscr{K}$ by the plane (41) corresponds an angular region $\mathscr{S}$ in the plane tx_3 between two straight lines starting from the origin and forming an angle $\varphi_1 > \frac{1}{8}D^{-c_0-c_3}$. By the theorem of § 1 there is in $\mathscr{S}$ a lattice point $(t = t_0, x_3 = u_0)$ at which the form $\Phi(t, x_3)$ represents a prime

$$p_0 < |d|^c \leqslant D^{cc_4}.$$

Since, by (42), $p_0 = f(\alpha t_0, \beta t_0, u_0)$ and the lattice point $(\alpha t_0, \beta t_0, u_0)$ is in $\mathscr{K}$, the statement of § 11 follows for the definite forms.

14. In what follows we suppose the form (39) to be an indefinite one. The discriminant of the form (42), viz.

$$(43) \qquad d = (2a_{13}\alpha+2a_{23}\beta)^2-4a_{33}(a_{11}\alpha^2+2a_{12}\alpha\beta+a_{22}\beta^2) = \Psi(\alpha, \beta)$$

is itself a quadratic form in α and β. In the present paragraph we take for granted that $\Psi(\alpha, \beta)$ is not the square of a linear form with rational integer coefficients.

Let $\mathscr{A}''$ be the part of $\mathscr{A}'$ (as defined in § 13) between two circles with a common centre at the origin, the radii being respectively D^{c_3} and $2D^{c_3}$. Covering $\mathscr{A}''$ by a lattice of the squares R (with the length of the

side $= |a_{33}|$) we denote by N the number of those R which lie entirely in $\mathscr{A}''$. If c_3 is large enough, then using [20] II, (675), we deduce that

$$N > \tfrac{1}{4}D^{-c_0}D^{2c_3}|a_{33}|^{-2}.$$

By § 12 there are in $\mathscr{A}''$ at least N lattice points (α, β) at which the form (42) is a primitive one. It remains to show that the number N_1 (say) of lattice points $\in \mathscr{A}''$ at which the form $\Psi(\alpha, \beta)$ represent squares is less than N.

Any number n representable by $\Psi(\alpha, \beta)$ at some point $(\alpha, \beta) \in \mathscr{A}''$ is evidently $\ll D^{2c_3+8}$, the number of representations being $\ll n^{1/8}\log D$. Hence

$$N_1 \ll \{(1^2)^{1/8}+(2^2)^{1/8}+\ldots+(m^2)^{1/8}\}\log D, \quad \text{where} \quad m \ll D^{c_3+4},$$

and thus

$$N_1 \ll D^{c_3+4}D^{(2c_3+8)/8}\log D < D^{(5/4)c_3+6}.$$

This proves that for all large $c_3 \ll 1$ we have $N_1 < N$, i.e. the desired result.

15. In this paragraph we shall discuss the case where $\Psi(\alpha, \beta)$ is the square of a linear form $a\alpha+b\beta$ with rational integer coefficients a, b which by (43) are $\ll D^{c_4}$.

If we choose the values of α and β as in § 12, the form $f(at, \beta t, x_3)$ is a primitive one. Its discriminant being a square, we have

$$f(at, \beta t, z) = (a_1 t+b_1 z)(a_2 t+b_2 z), \tag{44}$$

where a_1, b_1, a_2, b_2 are rational integers $\ll D^{c_5}$ with the greatest common divisor

$$(a_1, b_1) = (a_2, b_2) = 1. \tag{45}$$

If for some integer values of t and z $|f|$ is a prime p, then we may suppose that the first factor in (44) is 1 (or -1) and the second one represents p. The first equality, being a linear Diophantine equation, is satisfied for

$$t = t_0-b_1 u, \quad z = z_0+a_1 u \quad (u = 0, \pm 1, \ldots),$$

where $t_0, z_0 \ll D^{c_5}$ and

$$a_1 t_0+b_1 z_0 = 1 \text{ (or } -1). \tag{46}$$

Substituting into $p = a_2 t+b_2 z$ we obtain

$$p = A+Bu,$$

where

$$A = a_2 t_0+b_2 z_0 \quad \text{and} \quad B = a_1 b_2-a_2 b_1$$

in absolute value do not exceed D^{c_6}. If there is a prime p_1 dividing both A and B, then multiplying the first of the relations

$$a_2 t_0+b_2 z_0 \equiv 0 (\mathrm{mod} p_1), \quad a_1 b_2-a_2 b_1 \equiv 0 (\mathrm{mod} p_1) \tag{47}$$

by b_1 and using the second one and (46), we deduce that $p_1 | b_2$. Hence from the second relation (47) and (45) if follows that $p_1 | b_1$ and from (45) it follows, by the first relation (47), that $p_1 | t_0$. Now from (46) we get the relation $p_1 | 1$, which proves that $(A, B) = 1$.

If $B = 0$, then $f(at, \beta t, z)$ (or $-f$) is a square of a linear form in t and z. The discriminant d being a square $= (a\alpha+b\beta)^2$, we deduce that $d = 0$. To secure that B does not disappear, in the case of $a^2+b^2 > 0$ we have only to discard the lattice points (α, β) along the line $a\alpha+b\beta = 0$. In the opposite case when $a^2+b^2 = 0$ we deduce from (43) that the first minors $A_{11}, A_{22}, A_{12}, A_{21}$ of the determinant D disappear. Now we arrive at our aim by means of the form $f(x_1, \alpha t, \beta t)$ for which a similar case cannot occur (otherwise $A_{32} = 0$ whence $D = 0$).

Hence there are infinitely many primes $p = A+Bu$. It remains to prove that there is a prime $p = A+Bu = D^{O(1)}$ $(D \to \infty)$ such that the point (x_1, x_2, x_3), where

$$x_1 = at = \alpha(t_0-b_1 u), \quad x_2 = \beta t = \beta(t_0-b_1 u), \quad x_3 = z = z_0+a_1 u,$$

is in $\mathscr{K}$.

In [12], § 13, we have proved that for some constant $\theta < 1$ and for any $x \geqslant |2B|^{c_7}$ $(c_7 = c_7(\theta))$ there is a prime $p = A+Bu$ in the interval $x, x+x^{\theta}$. Hence for any c_8 there is a prime $p = A+Bu$ with u lying in an interval $\mathscr{I} = (u_1, u_1+D^{-c_8}u_1)$, where $u_1 = D^{c_9}$ with appropriate $c_9 = c_9(c_8)$.

If the lattice point $(x_1 = at, x_2 = \beta t, x_3)$ (with fixed α, β) is in $\mathscr{K}$, then by § 13 the coordinate $x_3 = z$ lies in an interval $(z_1, z_1+\frac{1}{2}D^{-c_0}\sqrt{\alpha^2+\beta^2}t)$, where $z_1 \ll \sqrt{\alpha^2+\beta^2}|t|$. Since $z = z_0+a_1 u$, we deduce that for all large $t = D^{O(1)}$ $(D \to \infty)$ u lies in an interval of the type $\mathscr{I}$ (as defined above), and vice versa. This completes the proof.

Note on a problem of Loo-Keng Hua

16. Most of the results of the present paper are different generalizations or analogies of Linnik's estimate $p_1 = D^{O(1)}$ $(D \to \infty)$ for the least prime $p_1 = p_1(D, l)$ representable by the linear form $Dx+l$. Considering a pair of linear forms

$$L(x, y) = ax+by+c, \quad L_1(x, y) = a_1 x+b_1 y+c_1 \tag{48}$$

one can naturally ask for an estimate for the 'least' pair(6) of primes p_0, p_1 such that

$$p_0 = L(x, y) \quad \text{and} \quad p_1 = L_1(x, y).$$

We suppose that the coefficients and the variables of L, L_1 are rational integers.

In 1947 Loo-Keng Hua ([15], p. 170) asked whether the system (48) represents an infinity of prime pairs.

Writing

$$D = \begin{vmatrix} a & b \\ a_1 & b_1 \end{vmatrix}$$

we may suppose that $D \geqslant 0$(7). In the case of $D = 0$ the problem of Hua is (in another form) the question whether there are infinitely many primes p, p_1 satisfying the linear Diophantine equation

$$a_1 p - a p_1 = C \qquad (C = a_1 c - a c_1).$$

If $C \neq 0$ and the equation is not evidently impossible(8), no method is known for the solution of this problem.

The case $D \neq 0$, which is much easier, has been studied by N. Dūma [5] and A. I. Vinogradov [26]. For special values of the coefficients (e.g. if a, b and c are divisible by 4) the system of forms L, L_1 does not represent any pair of primes. In the present note we shall confine ourselves to the proof of the following result.

Let $D \geqslant 2$ and let the linear forms L, L_1 represent a pair of primes p_0, p_1, at least one of which does not divide D. Then there is an infinity of prime pairs representable by the given forms, among them a pair (p, p') such that

$$p \leqslant D^{c_2}, \quad p' \leqslant D^{c_2} \tag{49}$$

where c_2 denotes a suitable absolute constants $\geqslant 2$.

In proving this we take for granted that there are integers x_0, y_0 such that

$$a x_0 + b y_0 + c = p_0, \qquad a_1 x_0 + b_1 y_0 + c_1 = p_1$$

and p_0 does not divide D. Then for any integer t and $x = x_0 + b_1 t$, $y = y_0 - a_1 t$ we have

$$a_1 x + b_1 y + c_1 = p_1, \qquad a x + b y + c = D t + p_0.$$

Hence by Dirichlet's theorem there is an infinite set of primes $p = L(x, y)$, which proves the first part of the statement.

(6) E.g. with the least sum $p_0 + p_1$.

(7) This may be attained by changing (if necessary) the rôles of L an L_1.

(8) That is to say, if the greatest common divisor of a and a_1 does not divide C.

By the theorem of [10] there is a prime $p = Dt + p_0 = L(x, y)$ in the interval (D, D^{c_2}). If $p_1 \leqslant D^{c_2}$, then (49) holds with $p' = p_1$. If, on the contrary, $p_1 > D^{c_2}$, then p_1 does not divide D and arguing as before we deduce that there is a pair of primes $p = L(x, y)$ and $p_1' = L_1(x, y)$ neither of which exceeds D^{c_2}.

We have excluded the case $D = 1$ where any pair p_0, p_1 is representable by the system L, L_1, but (49) does not hold, the least prime being > 1.

On irreducible polynomials

17. In the present paragraph let $f(x)$ and $r(x)$ denote polynomials of degrees $n \geqslant 2$ and $\leqslant n$, respectively, with rational integer coefficients, the absolute value of which does not exceed $A \geqslant 2$. The coefficient of x^n in f is supposed to be > 0. Next we suppose that f and r have no common polynomial divisor. Then by the method of Euclid's algorithm we can find polynomials $U(x)$ and $V(x)$ over the field of rationals and a rational number $m > 0$ such that for all x

$$f(x)U(x) + r(x)V(x) = m. \tag{50}$$

After multiplying through by a suitable integer we may suppose that m and the coefficients in U and V are integers. Then for any integer $x = x_0$ the integer m in (50) is divisible by the highest common divisor $d_0 = (f(x_0), r(x_0))$. Let d_0 be the maximal divisor of m for which there is an integer x_0 such that $(f(x_0), r(x_0)) = d_0$ and let $x_0 \equiv a \pmod{d_0}$ where $0 \leqslant a < d_0$. Then for any number $x_1 \equiv a \pmod{d_0}$ we have $d_0 = (f(x_1), r(x_1))$. Hence, writing $U_1(t) = U(d_0 t + a)$, $V_1(t) = V(d_0 t + a)$,

$$f_1(t) = d_0^{-1} f(d_0 t + a), \qquad r_1(t) = d_0^{-1} r(d_0 t + a), \qquad m_1 = d_0^{-1} m, \tag{51}$$

we have, by (50),

$$f_1(t)U_1(t) + r_1(t)V_1(t) = m_1$$

and for any integer t

$$(f_1(t), r_1(t)) = 1. \tag{52}$$

The algorithm leading to (50) consists of $\leqslant n$ divisions, the first of them being the division of $f(x)$ by $r(x) = b_0 x^m + \ldots + b_m$. If instead of $f(x)$ we divide $b_0^{n-m+1} f(x)$ by $r(x)$, then the coefficients in the remainder are integers. Proceeding in the same manner we can prove that the integer m in (50) satisfies $m < A^{c_1}$, where $c_1 = c_1(n)$ stands for a positive constant which does not depend on A. Hence

$$d_0 < A^{c_1}. \tag{53}$$

Now let us denote by $\|g(x)\|$ the height (i.e. the maximal modulus of the coefficients) of a polynomial $g(x)$ and let us write

$$F(t) = f(d_0 t + a), \qquad R(t) = r(d_0 t + a). \tag{54}$$

Using the binomial expansions and considering that for $k = 0, 1, \ldots, n$ $\binom{n}{k} < 2^n$, we deduce that

$$\left.\begin{matrix} \|F(t)\| \\ \|R(t)\| \end{matrix}\right\} \leqslant (n+1)A(2d_0)^n. \tag{55}$$

LEMMA 1. *If the coefficients in the polynomial $g(z)$ of degree n are rational integers* (9), *then all the zeros of $g(z)$ lie in the circle $|z| = (n+1)\|g\|$.*

Proof. Outside the circle we have

$$|g(z)| \geqslant |z|^n\left(1 - \frac{n\|g\|}{|z|}\right) \geqslant |z|^n\left(1 - \frac{n}{n+1}\right) \geqslant (n+1)^n - n(n+1)^{n-1} \geqslant 3.$$

LEMMA 2. *Let $g(z)$ be a polynomial with rational integer coefficients such that all the zeros of $g(z)$ are in $|z| < \lambda$ $(\lambda \geqslant 1)$. If for some integer $x_1 \geqslant 2\lambda d_1$ $(d_1 \geqslant 1)$ we have*

$$g(x_1) = dp, \tag{56}$$

where p is a prime and $|d|$ integer $\leqslant d_1$, then $g(z)$ is irreducible in the field of rationals (Cf. [3], p. 326).

Proof. In the case of reducible $g(z)$ we have $g(z) = g_1(z)g_2(z)$, where by a theorem of Gauss g_1 and g_2 are polynomials of degrees $\geqslant 1$ with integer coefficients. Then, by (56), $g_1(x_1) = d'p$ where $d' | d$, and

$$g_2(x_1) = d'', \qquad |d''| \leqslant d_1.$$

For appropriate integer a_0 and a set of zeros z_j $(1 \leqslant j \leqslant k)$ lying in the circle $|z| < \lambda \leqslant \frac{1}{2}x_1$ we have $g_2(z) = a_0(z - z_1)\ldots(z - z_k)$, whence

$$g_2(x_1) \geqslant |x_1 - z_1|\ldots|x_1 - z_k| > (\tfrac{1}{2}x_1)^k \geqslant d_1.$$

Thus we have arrived at a contradiction, which proves the lemma.

THEOREM. *Let $f(x)$ and $r(x)$ denote polynomials of degrees $n \geqslant 2$ and $\leqslant n$, respectively, with rational integer coefficients. If f and r have no common polynomial divisor, then there is a positive constant $c \geqslant 1$, depending merely on n, such that for appropriate positive integer $Q < A^c$ with $A = 1 + \max(\|f\|, \|r\|)$ the polynomial*

$$\varphi(x) = r(x) + Qf(x)$$

is irreducible in the field of rationals.

(9) Actually we need only the highest coefficient to be in modulus > 1.

Evidently $\varphi \equiv r \pmod f$ and the height of φ satisfies

$$\|\varphi\| < \{1 + \max(\|f\|, \|r\|)\}^{c+1}.$$

Proof. Let $F(t)$ and $R(t)$ be the polynomials (54) and let

$$g(z) = R(z) + QF(z), \tag{57}$$

where Q stands for an integer such that

$$Q > Q_0 = E\|R(t)\| \tag{58}$$

with appropriate constant $E = E(n) > 1$. By (54) and Lemma 1 all the zeros of $F(z)$ are in the circle $|z| < 2(n+1)A$. For a sufficiently large E the coefficients in $Q^{-1}g(z)$ differ from those in $F(z)$ by less than an arbitrarily small constant. The zeros of polynomial being continuous functions of the coefficients, we deduce that all the zeros of $g(z)$ lie in the circle

$$|z| < 4(n+1)A.$$

By the theorem of [10] for any $x \geqslant 1$ and any integer $D \geqslant 2$ in the interval (x, xD^{c_0}) (where c_0 denotes an absolute constant > 1) there is a prime $p \equiv l \pmod D$, if $(D, l) = 1$.

Supposing that the leading term in $f(x)$ has a positive coefficient, for any integer $t_1 > 2(n+1)A$ we have $f_1(t_1) > 3$. Therefore using (52) we deduce that for any $x \geqslant 1$ there is a prime

$$p = f_1(t_1)Q + r_1(t_1) \in [x, xf_1(t_1)^{c_0}]. \tag{59}$$

Hence, by (51), (54) and (57),

$$pd_0 = F(t_1)Q + R(t_1) = g(t_1).$$

We may suppose that the integer t_1 satisfies

$$t_1 \geqslant 8(n+1)A^{c_1+1}, \tag{60}$$

c_1 being the constant in (53). Hence

$$t_1 > 2 \cdot 4(n+1)Ad_0.$$

If inequality (58) holds, then by Lemma 2 (with $\lambda = 4(n+1)A$, $d_1 = d_0$) $g(t)$ is irreducible in the field of rationals. Hence, by (57) and (54), the polynomial

$$Qf(d_0 t + a) + r(d_0 t + a)$$

is irreducible and so is the polynomial

$$Qf(z) + r(z) = \varphi(z),$$

since the linear transformation $z = d_0 t + a$ does not affect the reducibility.

Now let us take

$$x = \{f_1(t_1)+|r_1(t_1)|\}2^n(n+1)A^{c_1n+1}E.$$

Then by (59), (55), (53) and the definition of Q_0 (cf. (58))

$$Q > (n+1)2^nA^{c_1n+1}E > Q_0$$

and thus inequality (58) holds. Now by (59) and (60) $Q < A^c$, which completes the proof of the theorem.

18. In the subsequent two paragraphs we shall deal with an analogous theorem in an algebraic field K of degree $k > 1$. We begin by proving a lemma analogous to Gauss's theorem which we used in the proof of Lemma 2.

We suppose that the coefficients in any polynomial $f(x)$ we shall deal with are ideal numbers of the same class $\mathfrak{R} = \mathfrak{R}_f$ (in the ordinary sense; cf. § 3). If they are ideal integers, then the greatest common divisor $\hat{\delta}$ [10] will be called the divisor of $f(x)$; polynomials with $\hat{\delta} = 1$ will be called primitive ones. Any polynomial $f(x)$, whose coefficients are ideal integers of the same class $\mathfrak{R}$, admits of the representation

$$f(x) = \hat{\delta}f_1(x),$$

where $f_1(x)$ is a primitive polynomial.

LEMMA 3. *If f and g are primitive polynomials, so is the product fg.*

Proof. Let the coefficients in the polynomials

$$f(x) = \hat{\alpha}_0x^n+\hat{\alpha}_1x^{n-1}+\ldots+\hat{\alpha}_n, \quad \text{and} \quad g(x) = \hat{\beta}_0x^m+\hat{\beta}_1x^{m-1}+\ldots+\hat{\beta}_m$$

be ideal integers of the classes $\mathfrak{R}_f$ and $\mathfrak{R}_g$, respectively, with the greatest common divisor $(\hat{\alpha}_0, \hat{\alpha}_1, \ldots, \hat{\alpha}_n) = (\hat{\beta}_0, \hat{\beta}_1, \ldots, \hat{\beta}_m) = 1$. Then the coefficients

$$\hat{\gamma}_0 = \alpha_0\hat{\beta}_0, \ \hat{\gamma}_1 = \hat{\alpha}_0\hat{\beta}_1+\hat{\alpha}_1\hat{\beta}_0, \ \ldots$$

in the polynomial

$$F(x) = f(x)g(x) = \hat{\gamma}_0x^{m+n}+\hat{\gamma}_1x^{m+n-1}+\ldots+\hat{\gamma}_{m+n}$$

are ideal integers of the same class $\mathfrak{R} = \mathfrak{R}_f\mathfrak{R}_g$. If F is not a primitive polynomial, then there is an ideal prime $\hat{\pi}$ which divides all the coefficients $\hat{\gamma}_l$ $(0 \leqslant l \leqslant m+n)$. Since $\hat{\pi}|\hat{\alpha}_0\hat{\beta}_0$, we may suppose that $\hat{\pi}|\hat{\alpha}_0$. Then for an appropriate index j $(0 \leqslant j < n)$ we have

$$\hat{\pi}|\hat{\alpha}_0, \ \hat{\pi}|\hat{\alpha}_1, \ \ldots, \ \hat{\pi}|\hat{\alpha}_j, \ \hat{\pi}\nmid\hat{\alpha}_{j+1}. \tag{61}$$

[10] I.e. the divisor $\hat{\delta}$ with the greatest $|N\hat{\delta}|$. It is unique if the associate numbers $\hat{\delta}$ and $\varepsilon\hat{\delta}$ (where ε denotes any unity in K) are considered as identical.

Let $r \geqslant 0$ be the least index such that

$$\hat{\pi}\nmid\hat{\beta}_r, \ \hat{\pi}|\hat{\beta}_{r-1}, \ \hat{\pi}|\hat{\beta}_{r-2}, \ \ldots, \ \hat{\pi}|\beta_0. \tag{62}$$

Then

$$\begin{aligned}\hat{\gamma}_{j+r+1} &= \hat{\alpha}_0\hat{\beta}_{j+r+1}+\ldots+\hat{\alpha}_j\hat{\beta}_{r+1}+\hat{\alpha}_{j+1}\hat{\beta}_r+\hat{\alpha}_{j+2}\hat{\beta}_{r-1}+\ldots+\hat{\alpha}_{j+r+1}\hat{\beta}_0\\ &= \hat{\alpha}_{j+1}\hat{\beta}_r+\hat{\gamma},\end{aligned}$$

say. By (61) and (62) $\hat{\pi}$ divides $\hat{\gamma}$, but it does not divide $\hat{\alpha}_{j+1}\hat{\beta}_r$. Therefore $\hat{\pi}\nmid\hat{\gamma}_{j+r+1}$. We have thus arrived at a contradiction, which proves the lemma.

LEMMA 4. *Let the coefficients in the polynomial*

$$F(x) = a_0x^n+a_1x^{n-1}+\ldots+a_n$$

be integers in the algebraic field K. If $F(x)$ is reducible in K, then there is a factorization

$$F(x) = f(x)g(x), \tag{63}$$

where the coefficients in f and g are ideal integers of classes $\mathfrak{R}$ and $\mathfrak{R}^{-1}$, respectively [11].

Proof. According to the lemma there is a factorization

$$F(x) = F_1(x)F_2(x), \tag{64}$$

where F_1 and F_2 are polynomials over K. Then there are integers α_1, $\alpha_2 \in K$ such that the coefficients in the polynomials $f_1(x) = \alpha_1F_1(x)$ and $g_1(x) = \alpha_2F_2(x)$ are integers in K. By (64)

$$\alpha_1\alpha_2F(x) = f_1(x)g_1(x). \tag{65}$$

Let $\hat{\delta}$, $\hat{\delta}_1$, $\hat{\delta}_2$ be the divisors of the polynomials F, f_1, g_1, respectively. Then there are primitive polynomials F_0, f_2, g_2 such that

$$F(x) = \hat{\delta}F_0(x), \quad f_1(x) = \hat{\delta}_1f_2(x), \quad g_1(x) = \hat{\delta}_2g_2(x).$$

By (65)

$$\alpha_1\alpha_2\hat{\delta}F_0(x) = \hat{\delta}_1\hat{\delta}_2f_2(x)g_2(x), \tag{66}$$

whence, by Lemma 3,

$$\alpha_1\alpha_2\hat{\delta} = \hat{\delta}_1\hat{\delta}_2\varepsilon,$$

where ε is a unity in K. Now by (66)

$$F(x) = \varepsilon^{-1}\hat{\delta}f_2(x)g_2(x),$$

whence (63) follows.

[11] If $a_0 = 1$, then one can prove that the coefficients in f and g are integers in the field. Cf. [13], p. 341.

LEMMA 5. *Let α and β be any fixed integers in the algebraic field K of the degree $k>1$ and discriminant Δ, and let*

$$\xi = \alpha+\beta\tau, \tag{67}$$

where τ runs through all integers of the field. Then for any $x \geqslant 1$ and for appropriate $\tau = \tau(x)$ we have $\xi = \hat{\delta}\hat{\pi}$ where $\hat{\delta}$ is the greatest common divisor of α and β, and $|N\hat{\pi}|$ is a prime p such that

$$x < p < x|\Delta N\beta|^c, \quad c = c(k). \tag{68}$$

Proof. Writing

$$\alpha = \hat{\delta}\hat{\alpha}_1, \quad \beta = \hat{\delta}\hat{\beta}_1, \quad \xi = \hat{\delta}\hat{\xi}_1$$

we have, by (67),

$$\hat{\xi}_1 = \hat{\alpha}_1+\hat{\beta}_1\tau, \quad \text{i.e.} \quad \hat{\xi}_1 \equiv \hat{\alpha}_1 (\mathrm{mod}\,\hat{\beta}_1).$$

$\hat{\alpha}_1$ and $\hat{\beta}_1$ being prime to one another, by the theorem of [10] there is an ideal prime $\hat{\pi}$ such that

$$\hat{\pi} \equiv \hat{\alpha}_1 (\mathrm{mod}\,\hat{\beta}_1) \tag{69}$$

and $|N\hat{\pi}|$ is a rational prime $\epsilon(x, x|\Delta N\hat{\beta}_1|^c)$. From (69) we deduce (67) with $\hat{\xi} = \hat{\delta}\hat{\pi}$ and, since $|N\hat{\beta}_1| \leqslant |N\beta|$, (68) follows.

LEMMA 6. *Let all the conjugates of α and β be in modulus $\leqslant M$ and let $D = |\Delta|M$. Then for any constant $c_2 > 0$ there is a corresponding $c_3 > 0$ with the following property: If $x \geqslant D^{c_3}$, then in the previous lemma all the conjugates of the number $\tau(x)$ are in modulus $> D^{c_2}$.*

Proof. First let K be the real quadratic field generated by $\sqrt{\Delta}$ ($\Delta > 0$) and let $\tau = x_1+x_2\sqrt{\Delta}$ be any number ϵK. If we cut out the rectangle $R(|x_1| \leqslant D^{c_4}, \ |x_2| \leqslant \Delta^{-1/2}D^{c_4})$ and two the angular regions $|x_2/\Delta^{-1/2}x_1-1| \leqslant \frac{1}{2}$, $|x_2/\Delta^{-1/2}x_1+1| \leqslant \frac{1}{2}$, then in the remaining part T (say) of the τ-plane $|\tau|$ and $|\tau'|$ are both $> \frac{1}{8}D^{c_4}$. Having performed the affine transformation $\xi = \alpha+\beta\tau$, we get in the ξ-plane the corresponding region $\mathfrak{T}$, whose boundary polygone is the map of the boundary of T. The rectangle R goes into a parallelogram with the centre at $\alpha = y_1+y_2\sqrt{\Delta}$ ($|y_1| \leqslant M$, $|y_2| \leqslant \Delta^{-1/2}M$) and with the length of sides $\ll MD^{c_4}$. In various ways we can choose in the ξ-plane two straight lines $\mathscr{L}$ and $\mathscr{L}'$ starting from the origin and forming an angle with the non-Euclidean measure $\varphi > \frac{1}{8}$ (cf. § 9), such that the region G between $\mathscr{L}$, $\mathscr{L}'$ and the curves $|N\xi| = x|N\hat{\delta}|$, $|N\xi| = x|N\hat{\delta}||\Delta N\beta|^c$ (where $\hat{\delta}$ has the same meaning as in Lemma 5) lies entirely in $\mathfrak{T}$. By § 9 there is in G a lattice point ξ such that the linear form $\hat{\alpha}_1+\hat{\beta}_1\tau$ (cf. the previous proof) represents an ideal prime $\hat{\pi}$ having the desired properties.

In the imaginary quadratic field the proof is much simpler, since now for any τ we have $|\tau| = |\tau'| = (N\tau)^{1/2}$.

In the general algebraic field the proof is similar and it rests on the estimate for the number N (say) of ideal primes $\hat{\pi} \equiv \hat{\alpha}_1 (\mathrm{mod}\,\hat{\beta}_1)$ in a many-dimensional sector. An asymptotic formula for N was first proved by Hecke [14], § 7. His result was improved by Kubilius ([17], § 11), who gave an estimate for the remaining term. In those papers the discriminant of the field remains fixed ($\Delta \ll 1$). By the method of [11] and [12], § 18, it is possible to prove a satisfactory estimate for N if $|\Delta| \to \infty$ and $|N\hat{\pi}|$ does not exceed $|\Delta N\hat{\beta}_1|^{O(1)}$ ([12]). This is what we need for the proof of the lemma in the general case.

19. In the present paragraph we suppose that $f(z)$ and $r(z)$ are polynomials of degrees $n \geqslant 2$ and $\leqslant n$, respectively, the coefficients being integers in the field K of degree k and discriminant Δ. Denoting by A ($A \geqslant 1$) the maximal modulus of all conjugates of the coefficients, we deduce that any of the coefficients is in modulus $\geqslant A^{-(k-1)}$ and so are the conjugates.

Next we suppose that f and r have no common polynomial divisor.

Let $f_j(z)$ and $r_j(z)$ ($1 \leqslant j \leqslant k$) be the corresponding polynomials over the conjugate fields $K^{(j)}$. Then the polynomials

$$F(z) = \prod_j f_j(z) \quad \text{and} \quad R(z) = \prod_j r_j(z)$$

have rational integer coefficients in absolute value $\leqslant (n+1)^k A^k$ and F and R have no common polynomial divisor. By the arguments of § 17 we can find rational integers d_0, a,

$$0 \leqslant a < d_0 < (nA)^{c_1} \quad (c_1 = c_1(n, k))$$

such that for any rational integer $t \geqslant 0$ the greatest common divisor of $F(d_0t+a)$ and $R(d_0t+a)$ is d_0. Further, we shall use a fixed integer

$$x_1 = d_0t+a = (nA)^{c_0}, \tag{70}$$

where c_0 denotes a sufficiently large positive constant, subject to later restriction. Writing

$$\alpha = r(x_1), \quad \beta = f(x_1), \quad \hat{\delta} = (\alpha, \beta) \tag{71}$$

we have

$$|N\hat{\delta}| = d_0 < (nA)^{c_1}. \tag{72}$$

By Lemma 1 all the zeros of the polynomials $F(z)$ and $R(z)$ are in the circle $|z| \leqslant (kn+1)(n+1)^k A^k$ and so are the zeros of any $f_j(z)$ and $r_j(z)$.

([12]) I hope to return to this problem in some later paper.

Writing

$$M = (n+1)A(nA)^{c_0 n}, \qquad D = |\Delta| M,$$

we deduce, by Lemma 6, that for any $c_2 > 0$ there is an integer $\tau \in K$ such that all the conjugates of τ are in modulus $> D^{c_2}$ and are such that

$$\alpha + \beta\tau = \hat{\delta}\hat{\pi}, \qquad \text{where} \qquad |N\hat{\pi}| = p \tag{73}$$

is a rational prime. For a sufficiently large $c_2 \ll 1$ all zeros of the polynomial

$$g(z) = r(z) + \tau f(z)$$

are in the circle

$$|z| \leqslant 2(kn+1)^{k+1} A^k \tag{74}$$

(cf. § 17), and so are the zeros of any conjugate of $g(z)$.

If the polynomial $g(z)$ is reducible in K, then by Lemma 4

$$g(z) = \varphi(z)\psi(z),$$

where φ and ψ are polynomials of degrees $\geqslant 1$ with ideal integer coefficients. Since by (71), (72) and (73) $|Ng(x_1)| = d_0 p$, one of the rational integers $N\varphi(x_1)$ and $N\psi(x_1)$ is in absolute value $\leqslant d_0$. We may suppose that

$$|N\varphi(x_1)| \leqslant d_0 < (nA)^{c_1}. \tag{75}$$

Let

$$\varphi(z) = \hat{\gamma}_0 z^l + \ldots + \hat{\gamma}_l = \hat{\gamma}_0 (z - z_1)\ldots(z - z_l),$$

where $\hat{\gamma}_0, \ldots, \hat{\gamma}_l$ are ideal integers of the same class $\mathfrak{R}$ and $z_1, \ldots, z_l$ are in the circle (74). So are the zeros $z_1^{(j)}, \ldots, z_l^{(j)}$ (say) of the conjugate polynomials $\varphi_j(z)$ $(1 \leqslant j \leqslant k)$. We have

$$|N\varphi(x_1)| = |N\hat{\gamma}_0| \prod_j |x_1 - z_1^{(j)}| \ldots |x_1 - z_l^{(j)}|, \tag{76}$$

where $|N\hat{\gamma}_0| \geqslant 1$. If x_1 is large enough, e.g. if in (70)

$$c_0 \geqslant c_1 + 2(k+1)\log 4(kn+1),$$

then (76) contradicts (75). Hence $g(z)$ is not reducible in K.

We can prove that for appropriate constant $c_5 = c_5(n, k)$ all the conjugates of the number τ in (73) are in modulus $\leqslant D^{c_5}$. If in fact $|\tau| > D^{c_5}$ for any c_5 (when D runs to infinity over a suitable sequence of numbers), then on the one hand

$$|N(\alpha + \beta\tau)| \geqslant D^{c_2(k-1)} D^{c_5} \tag{77}$$

(since for a sufficiently large c_0 all the conjugates of $\beta = f(x_1)$ are in modulus > 2, but those of $\alpha = r(x_1)$ and τ are $\leqslant M$ and $> D^{c_2}$, respectively). On the other hand, by (68) and Lemma 6,

$$|N(\alpha + \beta\tau)| = d_0 p < (nA)^{c_1} x |\Delta N\beta|^c = (nA)^{c_1} D^{c_3 + kc},$$

where c_1, c_3 and c do not depend on c_5. If c_5 is large enough, this contradicts (77).

Thus we have proved *the existence of an integer $\tau \in K$ all the conjugates of which satisfy the inequalities*

$$|2A\Delta|^{c_6} < |\tau^{(j)}| < |2A\Delta|^{c_7}$$

with appropriate positive constants c_6 and c_7 (depending merely on k and n), and such that the polynomial

$$g(z) = r(z) + \tau f(z)$$

is irreducible in K[13].

If in particular K is the field of rationals, then $k = 1$, $\Delta = 1$ and we get the theorem of § 17.

20. In this paragraph we shall deal with polynomials $f(t)$ whose coefficients are the residue classes of a fixed prime q. If t^n is the highest power of t whose coefficient $a_0 \not\equiv 0 \pmod q$, then q^n will be called the *norm* of f and denoted by $[f]$. The polynomials with the highest coefficient $a_0 \equiv 1 \pmod q$ will be called primitive ones. Evidently there are q^n different primitive polynomials of the degree n.

Choosing a fixed primitive polynomial $M(t)$ of the degree $m \geqslant 1$ we divide the polynomials $f(t)$ into classes $\bmod M$. In the same class $H = H_R$ are all the polynomials

$$f \equiv R \pmod M,$$

where R is any fixed polynomial. If R and M have no common polynomial divisor, then the class H_R will be called a reduced one. If we write

$$D = q^m = [M],$$

the number h of the reduced classes satisfies $1 \leqslant h \leqslant D$.

In 1914 Kornblum [16] proved that in any reduced class $\bmod M$ there are infinitely many irreducible polynomials. As an application of the theorem of [10] we shall show the existence of an absolute constant c such that *in any reduced class* $\bmod M$ *there is a primitive irreducible polynomial of the degree $n \leqslant cm$ (m being the degree of M).*

The reduced classes $H \bmod M$ form a group and in any class the number of primitive polynomials f with $[f] = q^n$, $n \geqslant m$, is $q^{n-m} = D^{-1} q^n$ (see [16], pp. 100-102). Hence, if $x = 1, q, q^2, \ldots$, then

$$\sum_{\substack{f \in H \\ [f] = x}} 1 = D^{-1} x + O(D).$$

---

[13] Asserting in [10], p. 140, that this result follows from the theorem of that paper I had overlooked some arguments by which we ensure that no zeros of the polynomial $g(z)$ and neither those of the conjugate polynomials, are too large in modulus.

Thus the conditions of [10], Theorem (i) (with $q>1$, $\vartheta=1$, $c_1=1$, $l=-1-\log(1-q^{-1})/\log D$) are satisfied. Hence for an appropriate $c\ll 1$ there is a primitive irreducible $p(t)\in H$ with $[p]\leqslant D^c=q^{mc}$. This implies the result stated.

We could still impose the restriction $n\equiv r(\mathrm{mod}\,k)$ (r and k — arbitrarily fixed integers, $k\geqslant 1$; cf. [16], § 2) for the degree n of f, but then the constant c would depend on k.

The general theory of algebraic functions over a finite field of coefficients was developped by E. Artin [1], F. K. Schmidt [23] and other writers. It procures many other applications of our theorem (with $q>1$), but they are of little interest, since sharper results follow from the Riemann hypothesis, which A. Weil ([27], p. 82) proved for the corresponding L-functions. Including in [10] the case $q>1$ (which made the paper very intricate) we aimed at getting a possibly general theorem.

Appendix

21. In this paragraph our aim is the proof of the relation (36). All the premises and the notation remain the same as in §§ 7-9. The quadratic form F being primitive, we deduce that the numbers $\hat{\varrho}$ and Q are prime to one another. By $\lambda_0, \lambda_1, \ldots$ we shall denote positive constants which may depend on the discriminant D, but not on the particular form F. First we shall consider the case $D<0$, $x>0$.

Let $A_1(x,\mathscr{I})$ be the number of ideal numbers $\hat{\mu}\equiv r\hat{\varrho}(\mathrm{mod}\,Q)$ with a fixed r, prime to Q, such that $|N\hat{\mu}|\leqslant x$ and $\alpha(\hat{\mu})$ is in a given angle $\mathscr{I}(l_0,l_1)$ with the non-Euclidean measure φ. Then by (7) for any fixed $\vartheta<\frac{1}{3}$ and all $x\geqslant 1$

$$A_1(x,\mathscr{I})=\lambda_1\varphi x+O(D^{2/3}x^{1-\vartheta}). \tag{78}$$

Summing $A_1(x,\mathscr{I})$ over the reduced set of residues $r\,\mathrm{mod}\,Q$ we get an estimate for the number of such representations $m=F(x_1,x_2)$ where the points (x_1,x_2) belong to the sector S ($\mathscr{I}$, $m\leqslant x$) and the greatest common divisor (m,Q) is 1. It is also the number of representations by the linear form $\hat{\mu}=\hat{a}_1x_1+\hat{a}_2x_2$ with $(\hat{\mu},Q)=1$ (since $N\hat{\mu}=m$).

Now let $A_d(x,\mathscr{I})$ (for any natural integer $d|Q$) be the number of lattice points $(x_1,x_2)\in S$ such that in the representation

$$\hat{\mu}\equiv r\hat{\varrho}(\mathrm{mod}\,Q)\qquad (r \text{ fixed rational integer})$$

of the number $\hat{\mu}=\hat{a}_1x_1+\hat{a}_2x_2$ we have $(r,Q)=d$. Dividing through by d and writing

$$\frac{r}{d}=r_1,\qquad \frac{Q}{d}=Q_1,\qquad \frac{\hat{\mu}}{d}=\hat{\mu}_1,$$

we deduce

$$\hat{\mu}_1\equiv r_1\hat{\varrho}(\mathrm{mod}\,Q_1),\qquad (r_1,Q_1)=1.$$

Since $N\hat{\mu}\leqslant x$, we have

$$N\hat{\mu}_1=N\frac{\hat{\mu}}{d}=\frac{1}{d^2}N\hat{\mu}\leqslant\frac{x}{d^2}.$$

If $\hat{\mu}$ belongs to the angle $\mathscr{I}$, so does $\hat{\mu}_1$, since division by a positive number d does not change the value of α in (35). Hence, by (78),

$$A_d(x,\mathscr{I})=\lambda_1\varphi\frac{x}{d^2}+O\left\{\left(\frac{|D|}{d^2}\right)^{2/3}\left(\frac{x}{d^2}\right)^{1-\vartheta}\right\}. \tag{79}$$

Let N be the number of lattice points in S. Summing (79) over the reduced set of residues $r_1\,\mathrm{mod}\,Q/d$ and summing the results over all $d|Q$ we deduce

$$N=\lambda\varphi x+O(|D|^{7/6}x^{1-\vartheta}). \tag{80}$$

If $F(x_1,x_2)=ax_1^2+bx_1x_2+cx_2^2$ is a reduced quadratic form, then (cf. [20] I, p. 135) $|b|\leqslant a<\frac{1}{3}D^{1/2}$, whence for any fixed $x\geqslant 1$ the curve $F(x_1,x_2)=x$ is in the rectangle $|x_1|\leqslant 2|D|^{1/4}\sqrt{x}$, $|x_2|\leqslant 2|D|^{-1/4}\sqrt{x}$. Therefore the perimeter L of the sector S does not exceed $O(|D|^{1/4}x^{1/2})$.

Denoting by $A(x)$ the Euclidean area of S, we have (cf. [20] II, (675))

$$N=A(x)+O(L)=A(x)+O(|D|^{1/4}x^{1/2}). \tag{81}$$

Comparing with (80) we deduce that

$$\varphi=\lambda_0\frac{A(x)}{x}+O(|D|^{7/6}x^{-\vartheta}),\qquad \lambda_0=\lambda^{-1}. \tag{82}$$

Keeping the angle $\mathscr{I}(l_0,l_1)$ fixed but increasing x, we can see by geometrical consideration that the area $A(x)$ increases in the same ratio as x, whence $\lambda_0A(x)/x$ is a constant. According to (82) (with $x\to\infty$) it differs from φ by less than an arbitrarily small constant. Hence equality (36) follows.

If F is not a reduced form, then the remaining term in (82) is $\ll|D|^{7/6}x^{-\vartheta}+Ex^{-1/2}$, where E may be arbitrarily large, but independent of x, whence (36) follows again.

The same method may be used in the case $D>0$. Supposing $a\geqslant 1$ we consider that the perimeter of the sector $S(l_0,l_1;|F(x_1,x_2)|\leqslant x)$ between the positive x_1-axis l_0 (say) and the nearest ray l_1 with $\varphi=1$ does not exceed $O(\eta\sqrt{x})$, where $\eta=\eta(D)=T+U\sqrt{D}$ and T, U denote the least natural integers satisfying Pell's equation $t^2-Du^2=4$. The same estimate of the perimeter L holds evidently for any smaller angle

$\mathcal{S}(l_0, l_2)$ with $\varphi < 1$. Arguing as before we prove an analogous relation (82), where appears an extra term $O(\eta x^{-1/2})$ corresponding to the remaining term $O(L)$ in (81). This is in general the worst term, since from the formula

$$\overline{\lim_{D\to\infty}} \frac{\log\log\eta}{\log D} = \frac{1}{2},$$

due to I. Schur ([24], § 5), we deduce that for any constant $\varepsilon > 0$ there is a sequence of discriminants $D \to \infty$ such that

$$\eta(D) > \exp(D^{1/2-\varepsilon}). \tag{83}$$

In ordinary cases, however, $\eta(D)$ does not exceed some power of D. If for example $D = 4n^2+1$ ($n = 1, 2, \ldots$), then the equation $t^2 - Du^2 = 4$ has the solution $t = 16n^2+2$, $u = 8n$, whence $\eta \leqslant t+u\sqrt{D} < 8D$. A great many other examples were given by Euler and later writers (cf. [4], Ch. XII).

22. Using an elementary geometrical method in some cases we can improve the remaining term in (7).

Let $F(x_1, x_2) = ax_1^2+bx_1x_2+cx_2^2$ be a primitive quadratic form with $a > 0$ and the discriminant $D = \Delta Q^2 < 0$. Choosing any fixed sector $S(l_0, l_1; F(x_1, x_2) \leqslant x)$ we denote respectively by $A(x)$, L and N the area, the perimeter and the number of lattice points $(x_1, x_2) \in S$ such that $F(x_1, x_2)$ and Q are prime to one another (N is also the sum over appropriate classes $\mathfrak{H} \bmod Q$ of the left-hand sides in (7); cf. the end of § 8). Let us cover the sector S by a lattice of squares R having their sides of the length Q parallel to the coordinate axes and let us consider merely those R which have at least one point in common with S. Any such square will be called an inner one or a peripherial one according to whether all its points are or are not in S. The total number of lattice points in the peripherial squares is evidently $\ll Q^2L \leqslant |D|L$.

Further we consider that whenever the lattice points (x_1, x_2) and (r_1, r_2) are congruent $\bmod Q$ (by which we mean that $x_1 \equiv r_1$ and $x_2 \equiv r_2 (\bmod Q)$), then $F(x_1, x_2) \equiv F(r_1, r_2) (\bmod Q)$. Hence the greatest common divisor $d = (Q, m)$ of Q and numbers m representable by F is the same at all congruent points. F being a primitive form, in any inner square R there is at least one lattice point (r_1, r_2) with $d = 1$. Hence the number of lattice points with $d = 1$ is the same for all inner R; denoting it by λ, we have $1 \leqslant \lambda \leqslant Q^2$.

If I denotes the number of inner squares R, then by (81)

$$I = \frac{A(x)}{Q^2} + O\left(\frac{L}{Q}\right),$$

whence

$$N = \lambda I + O(|D|L) = \lambda_0 A(x) + O(|D|L).$$

Supposing F to be a reduced form, we have $L \ll |D|^{1/4}x^{1/2}$ (cf. § 21) and thus

$$N = \lambda_0 A(x) + O(|D|^{5/4}x^{1/2}), \tag{84}$$

which is the desired result.

An analogous result can be proved as well for primitive forms with a positive discriminant. But now, the estimate $L \ll \eta\sqrt{x}$ being worse (cf. (83)), the exponent of D in the remaining term in (84) may exceed any fixed constant. This makes the formula useless for our applications (cf. § 1)([14]).

23. In the subsequent §§ 23-25 we shall prove the following lemma, which we have used in § 10 (the result may be known, but I cannot give any reference).

LEMMA 7. *Let $F(x, y) = ax^2+bxy+cy^2$ be a primitive form with the discriminant $D = b^2-4ac \neq 0$ and let q be any natural number with the greatest common divisor $(q, D) = 1$. Then for any number l of the reduced set of residues* mod q *there are rational integers x, y such that $F(x, y) \equiv l (\bmod q)$.*

Note. The condition $(q, D) = 1$ cannot be replaced by the weaker one

$$(q, Q) = 1, \tag{85}$$

([14]) The estimate (7) actually holds for any constant $\theta > \frac{1}{2}$ and it can be proved by the following improvements in the arguments of §§ 4-6.

(i) Considering separately the cases $|t| < k$ and $|t| > k$ one can prove the estimate $\ll 1+|m|+(1+|t|)^{1+2\delta}$ ($0 < \delta \leqslant 1/\log(1+|m|)$) for the Γ-factor of § 4. It holds also for the Γ-factor of § 6.

(ii) If in [6], Lemma 3, we have $F(\alpha+it) \ll U+(1+|t|)^\nu$ (the other conditions remaining as before), then

$$F(\sigma+it) \ll (U+|t|^\nu)^{(\beta-\sigma)/(\beta-\alpha)} V^{(\sigma-\alpha)/(\beta-\alpha)} \qquad (\alpha < \sigma < \beta).$$

This can be proved by the method of [6], § 6, if in the definition of $g(s)$ we replace α and β everywhere (except in the exponent) respectively by α/U_1 and β/U_1 where $U_1 = U^{1/\nu}$. And in the definition of $f(s)$ we take $g(s/U_1)$ instead of $g(s)$.

By means of (i) and (ii) we get the following improvement of (26):

$$\zeta(\sigma+it, X) \ll \{1+|m|+|t|\}^{1+\delta-\sigma\delta^{-1}} D^{(1-\sigma)/2} \log D \qquad (-\delta < \sigma < 1+\delta)$$

for any positive $\delta < 1/\log D(1+|m|)$. Using this in (28) and taking $T = x^{1/2}$, $|m| < x^{1/2+\varepsilon}$ (where ε denotes any positive constant) we get for the remaining term in (29) the estimate $\ll D^{4/5}x^{1/2+\varepsilon}$. Now using $\Delta = x^{-1/2+\varepsilon}$ and estimating separately the contribution of the terms with $|m| > x^{1/2}$ by the arguments of § 5 we prove that the remaining term in (7) does not exceed $\ll D^{4/5}x^{1/2+\varepsilon}$. The example considered in [11], ([1]), shows that (7) cannot hold for $\theta < \frac{1}{2}$ (*Added 17th May* 1965).

where Q^2 is the factor in the representation $D = \Delta Q^2$ (Δ fundamental discriminant). If for example $F = x^2+y^2$, then $Q = 1$ (cf. [20] I, p. 172) and (85) imposes no restriction on q. However, F does not represent numbers $\equiv 3 \pmod 4$.

And, since the same form does not represent numbers $\equiv 3 \pmod 9$, we conclude that also the restriction $(l, q) = 1$ is necessary.

Proof. In the present paragraph we shall consider the case $q = 2^k$ (k integer $\geqslant 1$), l any odd integer. Since $(D, q) = 1$, we deduce that b is odd.

First let $k = 1$. Since

$$(\mathrm{mod}\,2)F(x,y) \equiv \begin{cases} ax+xy+cy & \text{if} \quad ac \text{ is odd}, \\ ax+xy & \text{if} \quad c \text{ is even}, \\ xy & \text{if} \quad a \text{ and } c \text{ are even}, \end{cases}$$

in the first and third case taking odd values for x and y we get an odd $F(x, y)$. In the second case we get an odd $F(x, y)$ by taking xy odd, if a is even; otherwise we take x odd and y even. This proves the lemma in the case $q = 2^k$, $k = 1$.

Using the method of induction we suppose that for a fixed $k \geqslant 1$ and any odd l there are integers x_1, y_1 such that

$$F(x_1, y_1) \equiv l \pmod{2^k}, \tag{86}$$

whence for any integer u, v

$$F(x_1+2^k u, y_1+2^k v) \equiv l \pmod{2^k}.$$

Now we are going to prove that for appropriate u, v

$$F(x_1+2^k u, y_1+2^k v) \equiv l \pmod{2^{k+1}},$$

i.e.

$$a(x_1+2^k u)^2+b(x_1+2^k u)(y_1+2^k v)+c(y_1+2^k v)^2-l = 2^k t \quad (t \text{ even}). \tag{87}$$

Since by (86) $ax_1^2+bx_1y_1+cy_1^2 = l+2^k t_0$ (t_0 — integer), the left-hand side of (87) is evidently

$$\equiv b(2^k y_1 u+2^k x_1 v)+2^k t_0 \pmod{2^{k+1}}$$

Hence t is even if

$$b(2^k y_1 u+2^k x_1 v)+2^k t_0 \equiv 0 \pmod{2^{k+1}}.$$

This is equivalent to the condition

$$y_1 u+x_1 v \equiv t_0 \pmod 2,$$

which evidently can be satisfied, since x_1, y_1 are not both even (otherwise in (86) l would be even). If t_0 is even, then we take even values of u and v. In the case of an odd t_0 we take one of the variables u, v odd (that one which has an odd coefficient) and the other even.

In a similar way we can prove that there are also values of u and v such that

$$F(x_1+2^k u, y_1+2^k v) \equiv l+2^k \pmod{2^{k+1}}.$$

Since for l running through the reduced set of residues $\bmod 2^k$ the numbers l and $l+2^k$ represent the reduced set of residues $\bmod 2^{k+1}$, we have proved the lemma for $q = 2^k$.

24. In the present paragraph we shall prove the lemma for $q = p^k$, where p denotes a fixed prime $\geqslant 3$ and k is any natural number.

Being a primitive form, $F(x, y) = ax^2+bxy+cy^2$ represents a number which is not a multiple of p: If $p \nmid a$ or $p \nmid c$, then $F(1, 0)$ or $F(0, 1)$ possesses the required property; if $p \mid a$ and $p \mid c$, then $p \nmid b$, whence $F(1, 1) \equiv b \not\equiv 0 \pmod p$. Replacing F (if necessary) by an equivalent form we may suppose that $p \nmid a$. Since $4aF(x, y) = (2ax+by)^2-Dy^2$, writing $F(x, y) \equiv l \pmod q$ we deduce

$$4al \equiv (2ax+by)^2-Dy^2 \pmod q. \tag{88}$$

First let us consider the case where $-D$ is not a quadratic residue $\bmod q$. Then the right-hand side of (88) with $y = 0$ and a variable x represents all the quadratic residues $\bmod q$. Since for any fixed y there is an $x = x_y$ such that $2ax+by \equiv 0 \pmod q$, the right-hand side of (88) (with a variable y and $x = x_y$) evidently represents all the quadratic non-residues. Hence $4al$ (and simultaneously l) for appropriate x, y represent any number of the reduced set of residues $\bmod q$.

Now let us suppose that $-D$ is a quadratic residue $\bmod q$. Then we consider the following cases (i) and (ii) separately.

(i) There are numbers x_1 and y_1 ($p \nmid y_1$) such that for $x = x_1$ and $y = y_1$ the right-hand side of (88) represents a number n which is not a quadratic residue $\bmod q$ but is in the reduced set of residues. Multiplying by t^2 where t runs through the reduced set of residues $\bmod q$, we deduce that the right-hand side of (88) represents all the quadratic non-residues $\bmod q$. Since (with $y = 0$ and a variable x) it also represents all the quadratic residues, we deduce that l represents any number of the reduced set of residues $\bmod q$.

(ii) If (i) is impossible, then for any x, y the right-hand side of (88) either is divisible by p or represents a quadratic residue $\bmod q$. Writing $-D \equiv e^2 \pmod q$ we can find an integer e_1 such that $ee_1 \equiv 1 \pmod q$. By the assumptions of the case we are dealing with, $(2ax+be_1)^2+1$

is either a quadratic residue mod q or a multiple of p. For appropriate x_1 we have $2ax_1+be_1 \equiv 1 (\mathrm{mod}\, q)$, whence $(2ax_1+be_1)^2+1 \equiv 2 (\mathrm{mod}\, q)$ is a quadratic residue mod q (since $p \nmid 2$). Now for appropriate x_2 we have $(2ax_2+be_1)^2 \equiv 2 (\mathrm{mod}\, q)$, whence $(2ax_2+be_1)^2+1 \equiv 3 (\mathrm{mod}\, q)$ is a quadratic residue mod q (if $p \nmid 3$), etc. Proceeding in this way we deduce that all the numbers $1, 2, \ldots, p-1$ are quadratic residues mod q. Simultaneously they are quadratic residues mod p, which, being impossible, disproves the case. This proves the lemma for $q = p^k$.

25. In the general case (where q is not a power of a prime) there is a representation $q = q_1 q_2$, where $q_1 > 1$ and $q_2 > 1$ are prime to one another. Let us suppose that for q_1 and q_2 the lemma has been proved. Then for any l with $(l, q_1 q_2) = 1$ there are integers x_1, y_1 and x_2, y_2 satisfying

$$F(x_1, y_1) \equiv l (\mathrm{mod}\, q_1) \quad \text{and} \quad F(x_2, y_2) \equiv l (\mathrm{mod}\, q_2). \tag{89}$$

Since $(q_1, q_2) = 1$, there are integers x, y such that

$$\begin{cases} x \equiv x_1 (\mathrm{mod}\, q_1), \\ x \equiv x_2 (\mathrm{mod}\, q_2), \end{cases} \qquad \begin{cases} y \equiv y_1 (\mathrm{mod}\, q_1), \\ y \equiv y_2 (\mathrm{mod}\, q_2), \end{cases}$$

whence, by (89),

$$F(x, y) \equiv l (\mathrm{mod}\, q_1), \qquad F(x, y) \equiv l (\mathrm{mod}\, q_2)$$

and thus $F(x, y) \equiv l (\mathrm{mod}\, q)$. This completes the proof of the lemma

References

[1] E. Artin, *Quadratische Körper im Gebiete der höheren Kongruencen I, II*, Math. Zeitschr. 19 (1924), pp. 153-206; 207-246.

[2] L. Bianchi, *Lezioni sulla teoria aritmetica delle forme quadratiche binarie e ternarie*, Pisa 1912.

[3] Z. Chládek, *Nouvelle méthode pour décomposer les polynômes réductibles à une variable*, Časopis pro pěst. mat. a fys. 51 (1922), pp. 326-327.

[4] L. E. Dickson, *History of the Theory of Numbers II*, New York 1934.

[5] N. Dūma (Н. Дума), *Об одной проблеме Хуа Ло-кен*, Latvijas PSR Zinātnu Akad. Vēstis 1 (66), (1953), pp. 159-162.

[6] E. Fogels, *On the zeros of Hecke's L-functions I*, Acta Arith. 7 (1962), pp. 87-106.

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

[8] — *On the distribution of prime ideals*, ibid., pp. 255-269.

[9] — *О распределении аналогов простых чисел*, Doklady Akad. Nauk SSSR 146 (1962), pp. 318-321.

[10] — *On the abstract theory of primes I*, Acta Arith. 10 (1964), pp. 137-182.

[11] — *On the abstract theory of primes II*, ibid., pp. 333-358.

[12] — *On the zeros of L-functions*, Acta Arith. 11 (1965), pp. 67-96.

[13] H. Hasse, *Zahlentheorie*, Berlin 1963.

[14] E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen*, Math. Zeitschr. 6 (1920), pp. 11-51.

[15] Hua, Loo-Keng (Хуа Ло-кен), *Аддитивная теория простых чисел* Trudy Mat. Inst. Steklova 22 (1947).

[16] H. Kornblum, *Über die Primfunktionen in einer arithmetischen Progression*, Math. Zeitschr. 5 (1919), pp. 100-111.

[17] J. Kubilius (И. П. Кубилюс), *О некоторых задачах геометрии простых чисел*, Mat. Sb. N. S. 31 (73), (1952), pp. 507-542.

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

[19] — *Einführung in die elementare und analytische Theorie der algebraischen Zahlen und der Ideale*, Leipzig und Berlin 1927.

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

[21] G. Pólya und G. Szegö, *Aufgaben und Lehrsätze aus der Analysis II*, Berlin 1925.

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

[23] F. K. Schmidt, *Analytische Zahlentheorie in Körpern der Charakteristik p*, Math. Zeitschr. 33 (1931), pp. 1-32.

[24] I. Schur, *Einige Bemerkungen zu der vorstehenden Arbeit des Herrn G. Pólya: Über die Verteilung der quadratischen Reste und Nichtreste*, Göttinger Nachrichten (1918), pp. 30-36.

[25] J. Vaitkevičius (И. Вайткявичус), *О распределении простых чисел мнимого квадратичного поля в секторах*, Litovsk. mat. sb. III N. 2 (1963), pp. 17-52.

[26] A. I. Vinogradov (А. И. Виноградов), *Об одной проблеме Хуа Ло-кена*, Doklady Akad. Nauk SSSR 151 (1963), pp. 255-257.

[27] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités scient. et ind. 1041, Paris 1948.

Reçu par la Rédaction le 15. 1. 1965