For other p it is equivalent to the system

$$(70)\qquad \begin{aligned} x\,\mathrm{ind}\,2+y\,\mathrm{ind}\,3 &\equiv 0 \bmod p-1,\\ y\,\mathrm{ind}\,2+z\,\mathrm{ind}\,3 &\equiv 2\,\mathrm{ind}\,2 \bmod p-1,\end{aligned}$$

where indices are taken with respect to a fixed primitive root mod p. Now

$$\big((\mathrm{ind}\,2)^2, (\mathrm{ind}\,3)^2\big)\,|\,\mathrm{ind}\,2\,\mathrm{ind}\,3.$$

Hence

$$\left(\frac{(\mathrm{ind}\,2)^2}{(\mathrm{ind}\,2, \mathrm{ind}\,3)}, \mathrm{ind}\,3\right)\Big|\,\mathrm{ind}\,2$$

and the equation

$$t\frac{(\mathrm{ind}\,2)^2}{(\mathrm{ind}\,2, \mathrm{ind}\,3)}+z\,\mathrm{ind}\,3 = 2\,\mathrm{ind}\,2$$

is soluble in integers. The numbers $x = \dfrac{-t\,\mathrm{ind}\,3}{(\mathrm{ind}\,2, \mathrm{ind}\,3)}$, $y = \dfrac{t\,\mathrm{ind}\,2}{(\mathrm{ind}\,2, \mathrm{ind}\,3)}$ and z satisfy the system (70) and hence also (69).

References

[1] H. Flanders, *Generalization of a theorem of Ankeny and Rogers*, Ann. of Math. 57 (1953), pp. 392–400.
[2] I. Gerst, *On the theory of nth power residues and a conjecture of Kronecker*, Acta Arith. 17 (1970), pp. 121–139.
[3] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil II, 1930; reprint Würzburg–Wien 1965.
[4] — *Zum Existenzsatz von Grunwald in der Klassenkörpertheorie*, J. Reine Angew. Math. 188 (1950), pp. 40–64.
[5] H. B. Mann, *Introduction to Algebraic Number Theory*, Columbus, Ohio 1955.
[6] A. Schinzel, *A refinement of a theorem of Gerst on power residues*, Acta Arith. 17 (1970), pp. 161–168.
[7] Th. Skolem, *Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen*, Vid. akad. Avh. Oslo I 1937 nr 12.
[8] — *Diophantische Gleichungen*, Berlin 1938.
[9] — *On the existence of a multiplicative basis for an arbitrary algebraic field*, Norske Vid. Selsk. Forh. (Trondheim) 20 (1947) nr 2.

Received on 11. 12. 1973 (502)

ACTA ARITHMETICA
XXVII (1975)

The generalized Hardy-Littlewood's problem involving a quadratic polynomial with coprime discriminants

by

HENRYK IWANIEC (Warszawa)

Dedicated to the memory of Yu. V. Linnik

Introduction
(History of the problem and the principal ideas)

The problem to be treated in this paper has its origin in the third pape [4] of Hardy and Littlewood's famous series "*Some problems of partitio numerorum*". Having introduced in the analytic theory of numbers a new and powerful circle method the authors derived with its help many asymptotic formulae for the number of representation of a given positive integer as the sum of a fixed number of summands taken from prescribed sequences (prime numbers, squares and higher powers of positive integers). The method is applicable to problems involving a large number summands. Nevertheless Hardy and Littlewood using it in a formal way derived the asymptotic formula

$$(\mathrm{HL})\qquad \sum_{p+x^2+y^2=n} 1$$
$$\sim\pi\prod_{p>2}\left(1+\frac{\chi(p)}{p(p-1)}\right)\prod_{\substack{p\mid n\\ p\equiv 1 \,(\mathrm{mod}\, 4)}}\left(1-\frac{p}{p^2-p+1}\right)\prod_{\substack{p\mid n\\ p\equiv 3\,(\mathrm{mod}\, 4)}}\left(1+\frac{p}{p^2-p-1}\right)\frac{n}{\log n}$$

and conjectured its validity (the first half of Conjecture J). In the fifth paper of the series [5] they expressed the opinion that the generalized Riemann hypothesis (GRH) implies the formula (HL) for almost all positive integers n. The implication was proved by Miss Stanley in 1928 ([12]). The problem of the validity of (HL) for almost all n unlike that for all n is ternary one and nowadays it can be easily solved without the generalized Riemann hypothesis by using Vinogradov's estimates for trigonometric sums with primes, which supplement the circle method in an essential way.

A new turn to the study of Hardy–Littlewood's problem has been given by C. Hooley in his very important paper of 1957 [6], where he deduced from GRH the formula (HL) itself. An important feature of the paper is the introducing of a new concept of "quasiprimes" useful nowadays also in other problems. The ultimate goal was achieved in 1960 by Linnik [9] who by his dispersion method eliminated GRH from Hooley's proof. In this way Hardy–Littlewood's problem was finally solved on having stimulated many fruitful ideas in the analytic number theory. Soon afterwards it proved possible to replace the formidable Linnik's method by Bombieri's mean value theorem.

The problem has been generalized in many different ways but the name of the generalized Hardy–Littlewood's problem was given by Linnik to that in which the form x^2+y^2 is replaced by an arbitrary quadratic form $\varphi(x, y)$. The principal difficulties involved in the new problem are purely algebraic. Generally speaking the number of solutions of the equation $\varphi(x, y) = m$ is known only if φ runs over all the inequivalent forms of a genus which as a rule are many. Nevertheless for the numbers m being a multiple of a suitable integer depending on φ one can estimate the number of solutions of $\varphi(x, y) = m$ with a fixed φ by a bound which exceeds a certain fixed fraction of the true value. Thus without essential difficulty one can show the existence of solutions of the equation $p+\varphi(x, y) = m$ and determine the order of their number N as the function of m ([1]). (When the discriminant of φ is negative we assume that φ is positive definite and when it is positive we identify the pairs (x, y) and (x', y') differing by an automorph of φ.) The above method gives no chance to obtain an asymptotic formula for N.

The new idea came again from Linnik and has been developed to almost final form by Linnik and Bredihin [2]. Let us assume that discriminant d of φ is fundamental. An ideal $\mathfrak{a}$ of $Q(\sqrt{d})$ is called by Linnik an ideal with good trajectory if it is divisible by sufficiently many prime ideals from each class. The points of a trajectory are all the ideals with norm $N\mathfrak{a}$. Linnik remarks that for $n-p$ being the norm of an ideal with good trajectory the number of solutions of the equation $p+\varphi(x, y) = n$ is large and asymptotically equal to a fixed fraction of the number of solutions of the equation $p+\varphi(x, y) = n$, where φ runs over inequivalent forms of the genus of φ. Moreover there are only few integers $n-p$ not being the norm of an ideal with good trajectory (i.e. having few factors from some class). These notions have been used in [2], where the generalized Hardy–Littlewood's problem is solved for all positive definite binary quadratic forms with fundamental discriminant.

The object of the present paper is the equation

$$p+F(x, y) = n,$$

where $F(x, y) = ax^2+bxy+cy^2+ex+fy+g \in Z[x, y]$. The numbers $d = b^2-4ac$, $D = af^2-bef+ce^2+dg$ and the form $G(x, y) = ax^2+bxy+cy^2$ are called the small, the large discriminant and the quadratic form of $F(x, y)$ respectively. We assume that d is different from a perfect square and is prime to D. The identity

$$d^2\big(F(x, y)-g\big)+G(r, s) = G(dx+r,\ dy+s),$$

where $r = bf-2ce$, $s = be-2af$ allows one to reduce to problem of representing m by F to that of representing $d^2(m-g)+G(r, s)$ by the form $G(X, Y)$ for integers X, Y with prescribed residues mod $|d|$. If d is a fundamental discriminant it turns out that Linnik's idea about good trajectories is applicable also in the new situation. A particular role is played by the ambiguous classes. In Linnik and Bredihin's terminology (which will not be used in the sequel) one can say that the good trajectories stay in each class of ideals for approximately the same time and during their stay in a given class (i.e. when the points of the trajectory differ from each other by ideal factors belonging to ambiguous classes) the solutions X, Y of the equation are uniformly distributed in the residue classes mod $|d|$ (the number of admissible residue classes is equal to the number of ambiguous classes and equals 2^{t-1}, where t is the number of distinct prime factors of d). This line of argument has been used in [7].

The situation changes completely if d is not a fundamental discriminant. An attempt to apply the above argument requires use of the arithmetic of ideals in a non-maximal order $\mathfrak{O}_f$ of discriminant d, in which there is no uniqueness of factorization into prime ideals. For this reason we give up the ideals in $\mathfrak{O}_f$. Ordinary classes of ideals in $Q(\sqrt{d})$ being inadequate we introduce finer classes (their group is isomorphic to the group of classes of similar modules belonging to $\mathfrak{O}_f$). The group in question does not admit an ergodic interpretation in the spirit of Linnik's trajectories and for this purpose has to be replaced by another one (see the remark after Proposition 2 below).

The goal of the paper is the following

Main Theorem. *If the discriminants d, D of F are coprime and its quadratic form is positive definite for $d<0$ then there exists a positive constant $\varepsilon = \varepsilon(d, D)$ such that*

$$\sum_{p+F(x,y)=n}^{*} 1 = \frac{2}{h_f} L(1, \chi) \prod_{p \mid d(D-dn)} \left(1-\frac{\chi(p)}{p}\right) \prod_{p \nmid d(D-dn)} \left(1+\frac{\chi(p)}{p(p-1)}\right) \frac{n}{\log n} + O\left(\frac{n}{\log^{1+\varepsilon} n}\right).$$

In the above formula p runs over the primes $\leqslant n$; $\sum^*$ means that the pairs (x, y) and (x', y') differing by an automorph of F are identified; χ is the character of the field $Q(\sqrt{d})$; h_f is the order of group I^d/I_1^d (definition see part I, § 1). The constant in O depends only on d and D.

Remark. The right hand side of the asymptotic formula depends only on the discriminants d and D, which are pairwise equal for polynomials equivalent by an unimodular affine transformation but do not form a complete system of invariants for such equivalence.

The analytic part of the proof is almost mechanically transferred from Hooley's paper, GRH being replaced by Bombieri's theorem. Some differences between the two papers occur in the estimation of the sum $\sum_C$, which in Hooley's case is of smaller order than the main term, but in our case contributes to the main term as much as the sum $\sum_\Delta$.

I conclude this introduction by expressing my thanks to Docent Marceli Stark for his valuable help and criticism concerning the display of the subsequent text.

Part I (Algebraic)

The formula for $N[F = n]$

§ 1. Notations, definitions and selected facts from the theory of quadratic fields. Let $K = Q(\sqrt{\Delta})$ be a quadratic field with discriminant Δ, $\mathfrak{O}$ be the ring of integers of K and $\mathfrak{O}_f = \{\alpha \in \mathfrak{O};\ \alpha \equiv \bar{\alpha} (\operatorname{mod} \sqrt{d})\}$ the order of index f and discriminant $d = \Delta f^2$. In the group I of fractional ideals and in the group $\mathscr{E}$ of units (of K) we can distinguish subgroups arranged in the following diagrams

$$\begin{array}{ccccc} I^d & \longrightarrow & I & \longleftarrow & I^R \\ \uparrow & & & & \uparrow \\ I_1^d & \longleftarrow & I_1^+ & \longrightarrow & I^+ \end{array} \qquad \mathscr{E}_1 \longrightarrow \mathscr{E}^+ \cap \mathfrak{O}_f \longrightarrow \mathscr{E}^+ \longrightarrow \mathscr{E}.$$

Here

$I^+ = \{(\gamma) \in I;\ \gamma \gg 0\}$ is the group of totally positive principal ideals (i.e. ideals generated by totally positive elements),

$$I^R = \{\mathfrak{a} \in I;\ N\mathfrak{a} = N\gamma;\ \gamma \in K^\times\} = \{\mathfrak{a}\mathfrak{b}^2;\ \mathfrak{a} \in I^+,\ \mathfrak{b} \in I\} = \left\{\mathfrak{a} \in I;\ \left(\frac{N\mathfrak{a}, \Delta}{p}\right) = 1 \text{ for all } p\right\}$$ the group of ideals of the principal genus,

$I_1^+ = \{(\gamma) \in I^+;\ \gamma \equiv 1 \ (\operatorname{mod} \sqrt{d})\}$,

$I^d = \{\mathfrak{a} \in I;\ (\mathfrak{a}, d) = 1\}$,

$I_1^d = \{(\gamma) \in I^d;\ \gamma \in \mathfrak{O}_f\}$,

$\mathscr{E}^+ = \{\varepsilon \in \mathscr{E};\ N\varepsilon = 1\}$ the group of totally positive units,

$\mathscr{E}_1 = \{\varepsilon \in \mathscr{E};\ \varepsilon \equiv 1 \ (\operatorname{mod} \sqrt{d})\}$.

The arrows in the diagrams denote inclusion.

Let $\mathfrak{p}_1, \mathfrak{p}_2, \ldots, \mathfrak{p}_t$ be the ramified ideals of K, i.e. the prime factors of Δ and let us set $\mathfrak{d} = \mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_t$. Then

I/I^R is the group of genera; $[I : I^R] = 2^{t-1}$,

$I^R/I^+ = \{C^2;\ C \in I/I^+\}$ the group of classes in the principal genus; $[I^R : I^+] = h^+/2^{t-1}$,

I/I^+ is the class group; $[I : I^+] = h^+$,

$\mathscr{A} = \{C \in I/I^+;\ C = \bar{C}\} = \{C \in I/I^+;\ C^2 = I^+\}$ the group of ambiguous classes.

Each ambiguous class contains exactly two ideals dividing $\mathfrak{d}$. There exist 2^{t-1} ambiguous classes. An ideal $\mathfrak{a}$ is called ambiguous if $\mathfrak{a} = \bar{\mathfrak{a}}$. Every ambiguous ideal $\mathfrak{a}$ can be uniquely represented in the form $\mathfrak{a} = (r)\mathfrak{d}_1$, where $r \in Q^\times$, $\mathfrak{d}_1 | \mathfrak{d}$.

PROPOSITION 1. *We have*

$$\mathscr{E}^+ = \{\bar{\eta}\eta^{-1};\ \eta | \mathfrak{d}\}.$$

Proof. For $\eta | \mathfrak{d}$ the ideal (η) is ambiguous hence $\varepsilon = \bar{\eta}\eta^{-1}$ is a unit. Clearly $\varepsilon \gg 0$ thus $\{\bar{\eta}\eta^{-1};\ \eta | \mathfrak{d}\} \subset \mathscr{E}^+$.

For $\varepsilon \in \mathscr{E}^+$ we get from Hilbert's theorem 90 that $\varepsilon = \bar{\eta}_1\eta_1^{-1}$ where $\eta_1 \in K^\times$. Hence the ideal (η_1) is ambiguous and $\eta_1 = r\eta$, where $r \in Q^\times$, $\eta | \mathfrak{d}$. Clearly $\varepsilon = \bar{\eta}\eta^{-1}$, thus $\mathscr{E}^+ \subset \{\bar{\eta}\eta^{-1};\ \eta | \mathfrak{d}\}$.

PROPOSITION 2. *We have*

$$I_1^d = \{\mathfrak{a} \in I^d;\ \bar{\mathfrak{a}}\mathfrak{a}^{-1} \in I_1^+\}.$$

Proof. The inclusion $I_1^d \subset \{\mathfrak{a} \in I^d;\ \bar{\mathfrak{a}}\mathfrak{a}^{-1} \in I_1^+\}$ is clear. Assume that $\mathfrak{a} \in I^d;\ \bar{\mathfrak{a}}\mathfrak{a}^{-1} = (\gamma)$, where $\gamma \gg 0$, $\gamma \equiv 1 \ (\operatorname{mod} \sqrt{d})$. Hence it follows in particular that the ideal $\mathfrak{a}$ belongs to an ambiguous class, thus there exist $\mathfrak{q} | \mathfrak{d}$ and $\varphi \gg 0$ such that $\mathfrak{q}\mathfrak{a} = (\varphi)$. Hence $\bar{\mathfrak{a}}\mathfrak{a}^{-1} = (\bar{\varphi}\varphi^{-1}) = (\gamma)$ and for a certain $\varepsilon \in \mathscr{E}^+$ we have $\bar{\varphi}\varphi^{-1} = \varepsilon\gamma$. By Proposition 1 there exists an integer $\eta | \mathfrak{d}$ such that $\varepsilon = \bar{\eta}\eta^{-1}$. Putting $\psi = \varphi\eta^{-1}$ we get $\bar{\psi}\psi^{-1} = \gamma \equiv 1$ $(\operatorname{mod} \sqrt{d})$. The ideal $(\eta^{-1})\mathfrak{q}$ can be uniquely represented in the form $\mathfrak{d}_1/\mathfrak{d}_2$ where $\mathfrak{d}_1\mathfrak{d}_2 | \mathfrak{d}$. Hence

$$\mathfrak{d}_1 | \psi, \quad (\psi\mathfrak{d}_1^{-1}, \mathfrak{d}_1) = 1, \quad \psi \equiv \bar{\psi} (\operatorname{mod} \mathfrak{d}_1\sqrt{d}), \quad \frac{\psi - \bar{\psi}}{\sqrt{\Delta}} \equiv 0 \ (\operatorname{mod} \mathfrak{d}_1).$$

Since the number $(\psi - \bar{\psi})/\sqrt{\Delta}$ is rational, the last congruence can be strenghtened to $(\psi - \bar{\psi})/\sqrt{\Delta} \equiv 0 \ (\operatorname{mod} \mathfrak{d}_1^2)$, which implies that $(\psi - \bar{\psi})/2 \equiv 0 \ (\operatorname{mod} \mathfrak{d}_1^2)$. On the other hand, the number $(\psi + \bar{\psi})/2$ is also rational, thus

$$\psi = \frac{\psi + \bar{\psi}}{2} + \frac{\psi - \bar{\psi}}{2} \equiv 0 \ (\operatorname{mod} \mathfrak{d}_1^2),$$

which is possible only if $\mathfrak{d}_1 = (1)$. Similarly one can prove that $\mathfrak{d}_2 = (1)$. Therefore $\mathfrak{q} = (\eta)$ and $\mathfrak{a} = (\psi) \in I_1^d$, which completes the proof.

Remark 1. Proposition 2 can be worded as follows: I_1^d/I_1^+ is the group of the invariant classes of I^d/I_1, i.e.

$$I_1^d/I_1^+ = \{C \in I^d/I_1^+;\ C = \bar{C}\}.$$

Proposition 3. *Let* $(\varepsilon, d) = 1$, $N\varepsilon \equiv 1 \pmod d$. *Then there exists* $\eta \in K^\times$ *such that*

$$\varepsilon \equiv \bar{\eta}\eta^{-1} \left(\bmod\ d/(2, d)\right).$$

Proof. Using the Chinese remainder theorem (for the field K) it is easy to reduce the proof to the case of d being a prime power. It follows from the congruence $\varepsilon\bar{\varepsilon} \equiv 1 \pmod d$ that the ideals $(\varepsilon \pm 1, d)$ are ambiguous. Hence $(\varepsilon+1, d) \mid (2, d)$ or $(\varepsilon-1, d) \mid (2, d)$. Setting

$$\bar{\eta} = \begin{cases} \varepsilon+1 & \text{if} \quad (\varepsilon+1, d) \mid 2, \\ (\varepsilon-1)\sqrt{d} & \text{if} \quad (\varepsilon+1, d) \nmid 2, \end{cases}$$

we get $\varepsilon \equiv \bar{\eta}\eta^{-1} \left(\bmod\ d/(2, d)\right)$, which completes the proof.

Remark 2. Proposition 2 can be improved in the following way: Let d be a positive integer, $\varepsilon \in K^\times$, $(\varepsilon, d) = 1$. Then

$$N\varepsilon \equiv 1 \pmod d \Leftrightarrow \varepsilon \equiv \bar{\eta}\eta^{-1} \left(\bmod\ d/(2, d, \Delta)\right).$$

Let $G(x, y) = ax^2 + bxy + cy^2$ be a primitive quadratic form of discriminant $d = b^2 - 4ac$. Then the ideal $\mathfrak{a} = \left(a, \dfrac{b+\sqrt{d}}{2}\right)$ is prime to $\mathfrak{a}$ and has a norm $N\mathfrak{a} = |a|$.

Proposition 4. *Let us set* $M = aZ + \dfrac{b+\sqrt{d}}{2}Z$. *Then* $M = \mathfrak{a} \cap \mathfrak{O}_f$.

Proof. The inclusion $M \subset \mathfrak{a} \cap \mathfrak{O}_f$ is clear. For $\xi \in \mathfrak{a} \cap \mathfrak{O}_f$ we have

$$y = (\xi - \bar{\xi})/\sqrt{d} \in Q \cap \mathfrak{O} = Z$$

and

$$\xi - \frac{b+\sqrt{d}}{2} y = \frac{\xi + \bar{\xi}}{2} - \frac{b(\xi - \bar{\xi})}{2\sqrt{d}} \in \mathfrak{a} \cap Q = \mathfrak{a} \cap Z = aZ.$$

Hence

$$x = \left(\xi - \frac{b+\sqrt{d}}{2} y\right) a^{-1} \in Z \quad \text{and} \quad \xi = ax + \frac{b+\sqrt{d}}{2} y \in M,$$

which completes the proof.

Remark 3. The group $\mathfrak{a}/M$ is cyclic of order f, thus the numbers a, $\dfrac{b+\sqrt{d}}{2}$ form a basis for the ideal $\mathfrak{a}$ only if d is a fundamental discriminant.

§ 2. Automorphs of the polynomial $F(x, y)$. The form aG and the polynomial $a(D - dF)$ are in the field K the norm of a linear form $\xi_{x,y} = ax + \dfrac{b+\sqrt{d}}{2} y$ and of a linear polynomial $\mu_{x,y} = \xi_{x,y}\sqrt{d} + \xi_{-f,e}$, respectively:

$$(1) \qquad aG(x, y) = N\xi_{x,y},$$

$$(2) \qquad a\left(D - dF(x, y)\right) = N\mu_{x,y}.$$

Let us set $\tau = \xi_{-f,e} = \mu_{0,0}$. Then $\tau \equiv 0 \pmod{\mathfrak{a}}$ and $N\tau = a(D - dg)$. For integers $x, y \in Z$ we have

$$(3) \quad \xi_{x,y} \equiv 0 \pmod{\mathfrak{a}}; \quad \mu_{x,y} \equiv \tau \pmod{\mathfrak{a}\sqrt{d}}; \quad N\mu_{x,y} \equiv N\tau \pmod{|ad|}.$$

Affine transformations

$$\lambda(x, y) = (x', y') = (\alpha x + \beta y + \varphi, \gamma x + \delta y + \psi),$$

where

$$\varphi, \psi, \alpha, \beta, \gamma, \delta \in Z; \quad |\alpha\delta - \beta\gamma| = 1$$

are called unimodular. They form a group Λ. Polynomials $F_\lambda(x, y) = F\left(\lambda(x, y)\right)$, where $\lambda \in \Lambda$ called equivalent have the discriminants pairwise equal. The subgroup $\Lambda_F = \{\lambda \in \Lambda;\ F_\lambda = F\}$ is called the group of automorphs of F. The group of automorphs of F_λ is $\lambda \Lambda_F \lambda^{-1}$ thus equivalent polynomials have isomorphic groups of automorphs. We have the well known

Lemma 1. *The group* Λ_G *of automorphs of the form* G *is isomorphic to* $\mathscr{E}^+ \cap \mathfrak{O}_f$. *The isomorphism is defined by the formula*

$$\lambda \xrightarrow[\xi_{x',y'} = \varepsilon \xi_{x,y}]{} \varepsilon.$$

We shall prove

Proposition 5. *If the discriminants of* F *are coprime then its group of automorphs* Λ_F *is isomorphic to* $\mathscr{E}_1$. *The isomorphism is defined by the formula*

$$\lambda \xrightarrow[\mu_{x',y'} = \varepsilon \mu_{x,y}]{} \varepsilon.$$

Proof. Since $(d, D) = 1$ the form G is primitive and $(\tau\mathfrak{a}^{-1}, d) = 1$.

Let $\lambda(x, y) = (x', y')$ be an automorph of F. Then $\lambda(x, y) - \lambda(0, 0)$ is an automorph of G, thus there exists $\varepsilon \in \mathscr{E}^+$ such that $\mu_{x',y'} - \mu_{0',0'} = \varepsilon(\mu_{x,y} - \tau)$. We have from (2) $N\mu_{x',y'} = N\mu_{x,y}$ hence for any $m \in Z$ we get

$$m \mid \mu_{x,y} \Rightarrow m \mid \mu_{x',y'} \Rightarrow m \mid \mu_{0',0'} - \varepsilon\tau.$$

Since for suitable integers $x, y \in Z$ the number $\mu_{x,y}$ has arbitrarily large divisors $m \in Z$ it follows that $\varepsilon\tau = \mu_{0',0'} \equiv \tau \pmod{\mathfrak{a}\sqrt{d}}$. Hence $\varepsilon \equiv 1 \pmod{\sqrt{d}}$ and $\mu_{x',y'} = \varepsilon\mu_{x,y}$.

Let $\varepsilon \in \mathscr{E}_1$ and for $x, y \in Z$ let $\lambda(x, y) = (x', y')$ be a solution in rationals of the equation $\mu_{x',y'} = \varepsilon\mu_{x,y}$. Hence and from (2) we get $F(x', y') = F(x, y)$ and $\mu_{x',y'} \equiv \varepsilon\tau \equiv \tau \pmod{\mathfrak{a}\sqrt{d}}$. Therefore $\xi_{x',y'} \in \mathfrak{a}$. Hence and again from (2) we obtain

$$\begin{aligned} N\tau \equiv N\mu_{x,y} = N\mu_{x',y'} &= N(\xi_{x',y'}\sqrt{d}+\tau) \\ &\equiv (\bar{\tau}\xi_{x',y'} - \tau\bar{\xi}_{x',y'})\sqrt{d} + N\tau \pmod{|ad|}. \end{aligned}$$

Since $\tau \equiv \bar{\tau} \pmod{\sqrt{d}}$ we have $\xi_{x',y'} \equiv \bar{\xi}_{x',y'} \pmod{\sqrt{d}}$, i.e. $\xi_{x',y'} \in \mathfrak{O}_f$. It follows from Proposition 4 that the numbers x', y' are integers, thus $\lambda(x, y) = (x', y')$ is an automorph of F.

§ 3. Representation of integers by F and ideals of $\mathfrak{O}$. Let us fix an integer n and consider the equation

$$F(x, y) = n. \tag{4}$$

We say that two solutions (x, y), (x', y') of (4) are *equivalent*, if $(x', y') = \lambda(x, y)$ for a certain $\lambda \in \Lambda_F$. Such solutions will be identified. The class of equivalent solutions of (4) containing (x, y) will be denoted by $[x, y]$.

PROPOSITION 6. *If the discriminants of F are coprime then there exists a one-to-one correspondence between the classes $[x, y]$ of equivalent solutions of (4) and the principal ideals $(\mu) \subset \mathfrak{O}$ such that*

$$N\mu = a(D - dn), \tag{5}$$

$$\mu \equiv \tau \pmod{\mathfrak{a}\sqrt{d}}. \tag{6}$$

The correspondence is given by formula $[x, y] \mapsto (\mu_{x,y})$.

Proof. Clearly the mapping $[x, y] \mapsto (\mu_{x,y})$ is well defined.

Suppose that $(\mu_{x,y}) = (\mu_{X,Y})$, where (x, y), (X, Y) are solutions of (4). Then for a certain $\varepsilon \in \mathscr{E}$ we have $\mu_{x,y} = \varepsilon\mu_{X,Y}$. Since $\mu_{x,y} \equiv \mu_{X,Y} \equiv \tau \pmod{\mathfrak{a}\sqrt{d}}$ it follows that $\varepsilon \equiv 1 \pmod{\sqrt{d}}$, which together with Proposition 5 implies that the solutions (x, y), (X, Y) are equivalent. Thus we have proved that the mapping $[x, y] \mapsto (\mu_{x,y})$ is a monomorphism.

Suppose that a number $\mu \in \mathfrak{O}$ satisfies (5) and (6). Then we get from (6) $\xi = (\mu - \tau)/\sqrt{d} \in \mathfrak{a}$ and from (5)

$$N\tau \equiv N\mu = N(\xi\sqrt{d}+\tau) \equiv (\bar{\tau}\xi - \tau\bar{\xi})\sqrt{d} + N\tau \pmod{|ad|}.$$

Since $\tau \equiv \bar{\tau} \pmod{\sqrt{d}}$ we have $\xi \equiv \bar{\xi} \pmod{\sqrt{d}}$, i.e. $\xi \in \mathfrak{O}_f$. It follows from Proposition 4 that there exist integers $x, y \in Z$ such that $\mu = \mu_{x,y}$. By (2) and (5) (x, y) is a solution of (4). This completes the proof.

§ 4. Proof of Theorem 1. Let us decompose the group I^d/I_1^d into a direct sum of cyclic groups

$$I^d/I_1^d = \prod_{r=1}^{R} G_r,$$

where G_r is generated by a class H_r of order h_r and let us introduce the following notation

$$m = D - dn; \quad n' = am; \quad l_r = \Big[\sum_{\mathfrak{p}\| m,\, \mathfrak{p}\in H_r,\, \deg \mathfrak{p}=1} \tfrac{1}{2}\Big];$$

$$\varepsilon_r = (h_r - 1)(\cos \pi/h_r)^{l_r};$$

$N[F = n]$ the number of inequivalent solutions of the equation (4).

THEOREM 1. *If*

(i) $n' > 0$ *for* $d < 0$,

(ii) $(d, D) = 1$,

(iii) $l_r \geqslant 2h_r$

then there exist numbers θ_r such that $-1 \leqslant \theta_r \leqslant 1$ and

$$N[F = n] = \frac{1}{h_f}\prod_{r=1}^{R}(1+\theta_r\varepsilon_r)\sum_{l|m}\chi(l). \tag{7}$$

COROLLARY. *If $I^d/I_1^d = Z_2 \times \ldots \times Z_2$ then we have under the assumption of Theorem 1*

$$N[F = n] = \frac{1}{h_f}\sum_{l|m}\chi(l).$$

In the proof of Theorem 1 we shall use the following two lemmata:

LEMMA 2. *For any integer $m \neq 0$ we have*

$$\sum_{\mathfrak{a}\subset\mathfrak{O},\, N\mathfrak{a}=|m|} 1 = \sum_{l|m}\chi(l).$$

Proof, see [8], Satz 882.

LEMMA 3. *For any positive integers L and h we have*

$$\begin{aligned} \sum_{\substack{0\leqslant l\leqslant L \\ l\equiv a \,(\mathrm{mod}\, h)}} \binom{L}{l} &= h^{-1}2^L \sum_{|r|<h/2} \cos\frac{(L-2a)\pi r}{h}(\cos \pi r/h)^L \\ &= h^{-1}2^L\Big\{1+\theta(h-1)\cos^L\frac{\pi}{h}\Big\} \end{aligned}$$

where $-1 \leqslant \theta \leqslant 1$.

Proof. Since

$$\sum_{r=0}^{h-1} e^{\frac{2\pi i(l-a)r}{h}} = \begin{cases} h & \text{if} \quad l \equiv a \pmod{h}, \\ 0 & \text{if} \quad l \not\equiv a \pmod{h}, \end{cases}$$

we get

$$h \sum_{\substack{0\leqslant l\leqslant L\\ l\equiv a \pmod h}} \binom{L}{l} = \sum_{r=0}^{h-1} e^{-\frac{2\pi iar}{h}} \sum_{0\leqslant l\leqslant L} \binom{L}{l} e^{\frac{2\pi ilr}{h}}$$

$$= \sum_{r=0}^{h-1} e^{-\frac{2\pi iar}{h}} \left(1+e^{\frac{2\pi ir}{h}}\right)^L = \sum_{r=0}^{h-1} e^{-\frac{2\pi iar}{h}} \left(2\cos\frac{\pi r}{h} e^{\frac{\pi ir}{h}}\right)^L$$

$$= 2^L \sum_{|r|<h/2} \cos\frac{(L-2a)\pi r}{h} \left(\cos\frac{\pi r}{h}\right)^L$$

which completes the proof.

Proof of Theorem 1. By Proposition 6 the number $N[F=n]$ is equal to the number of principal ideals of $\mathfrak{O}$ generated by elements satisfying the conditions (5) and (6). Hence if $|n'|$ is not the norm of an ideal, $N[F=n]=0$ and the formula (7) is trivial. Thus let us assume

(8) $|n'|$ is the norm of an ideal (i.e. $e_p(|n'|) = \left(\frac{|n'|,\Delta}{p}\right) = 1$ for $p\nmid\Delta$).

By the assumption (iii) there exist distinct and pairwise non-conjugate prime ideals $\mathfrak{p}_{r,l}\in H_r$, $1\leqslant r\leqslant R$, $1\leqslant l\leqslant l_r$ such that

$$\chi(\mathfrak{p}_{r,l}) = 1 \quad\text{and}\quad \mathfrak{p}_{r,l}\,\|\,m.$$

Let us put

$$\mathfrak{g} = \prod_{r=1}^{R}\prod_{l=1}^{l_r} \mathfrak{p}_{r,l}$$

and fix an integral ideal $\mathfrak{c}$ of the norm $N\mathfrak{c} = |m|N\mathfrak{g}^{-1}$. Each integral ideal of the norm $|n'|$ and divisible by $\mathfrak{a}\mathfrak{c}$ can be uniquely represented in the form

$$\mathfrak{b}_{\mathfrak{q}} = \mathfrak{a}\mathfrak{c}\mathfrak{g}\bar{\mathfrak{q}}\mathfrak{q}^{-1},$$

where $\mathfrak{q}\,|\,\mathfrak{g}$. We shall prove

Lemma 4. *For each integral ideal $\mathfrak{c}$ of the norm $|m|N\mathfrak{g}^{-1}$ there exists a class $C\in I^d/I_1^d$ such that an ideal $\mathfrak{b}_{\mathfrak{q}}$ satisfies the conditions* (5) *and* (6) *if and only if $\mathfrak{q}\in C$.*

Proof. Ideals $\mathfrak{b}_{\mathfrak{q}}$ have the norm $N\mathfrak{b}_{\mathfrak{q}} = |n'|$, hence they belong to the same genus determined by the invariants

$$e_p(|n'|) = \left(\frac{|n'|,\Delta}{p}\right) \quad\text{for}\quad p\,|\,\Delta.$$

Let us remark, that for $p\,|\,\Delta$ we have

$$e_p(n') = \left(\frac{n',\Delta}{p}\right) = \left(\frac{a,\Delta}{p}\right)\cdot\left(\frac{D-dn,\Delta}{p}\right)$$

$$= \left(\frac{a,\Delta}{p}\right)\cdot\left(\frac{D-dg,\Delta}{p}\right) = \left(\frac{N\tau,\Delta}{p}\right) = 1$$

whence for

$$\nu = \begin{cases} 1 & \text{if} \quad n'>0, \\ \sqrt{\Delta} & \text{if} \quad n'<0, \end{cases}$$

we get

$$e_p(|N\nu|) = \left(\frac{1,\Delta}{p}\right) = 1 = e_p(n') = e_p(|n'|) \quad \text{if} \quad n'>0$$

and

$$e_p(|N\nu|) = \left(\frac{\Delta,\Delta}{p}\right) = \left(\frac{-1,\Delta}{p}\right) = e_p(-n') = e_p(|n'|) \quad \text{if} \quad n'<0.$$

In view of the above, the principal ideal (ν) belongs to the same genus as the ideals $\mathfrak{b}_{\mathfrak{q}}$. In particular $(\nu^{-1})\mathfrak{b}_1\in I^R$, i.e. there exists a number $a\gg 0$ and an ideal $\mathfrak{x}$ such that

$$\mathfrak{b}_1 = (a\nu)\mathfrak{x}^2.$$

It is easy to see, that for $\mathfrak{x}$ one can take an ideal from I^d, since each class of ideals contains an ideal prime to d.

If $\mathfrak{q}$ runs over the divisors of the ideal $\prod_{r=1}^{R}\prod_{l=1}^{h_r}\mathfrak{p}_{r,l}$ then its class mod I_1^d runs through the whole group I^d/I_1^d, hence exactly one ideal $\mathfrak{q}_1$ is equivalent to $\mathfrak{x}$ mod I_1^d, i.e. there exists $\mathfrak{y}_1\in I_1^d$ such that

$$\mathfrak{q}_1 = \mathfrak{y}_1\mathfrak{x}.$$

If $\bar{\mathfrak{y}}_1\mathfrak{y}_1^{-1} = (y_1)$, $y_1\gg 0$ by putting $\xi_1 = a\nu y_1 N\mathfrak{x}$ we get

$$\mathfrak{b}_{\mathfrak{q}_1} = \mathfrak{b}_1\bar{\mathfrak{q}}_1\mathfrak{q}_1^{-1} = (a\nu)\mathfrak{x}\bar{\mathfrak{x}}\bar{\mathfrak{y}}_1\mathfrak{y}_1^{-1} = (\xi_1)$$

and moreover

$$N\xi_1 = n' \equiv N\tau \pmod{|ad|}.$$

Hence for $\varepsilon = \tau\xi_1^{-1}$ we have $(\varepsilon, d) = 1$ and $N\varepsilon \equiv 1 \pmod{|d|}$. By Proposition 3 there exists a number η such that $\varepsilon \equiv \bar{\eta}\eta^{-1} \pmod{\sqrt{d}}$. The ideal $\mathfrak{n} = (1, \bar{\eta}\eta^{-1})^{-1}$ belongs to I^d.

If $\mathfrak{q}_2$ runs over the divisors of the ideal $\prod_{r=1}^{R}\prod_{l=h_r+1}^{2h_r}\mathfrak{p}_{r,l}$ then its class runs through the whole group I^d/I_1^d hence exactly one ideal $\mathfrak{q}_2$ is equivalent mod I_1^d to $\mathfrak{n}$, i.e. there exists $\mathfrak{y}_2 \in I_1^d$ such that $\bar{\mathfrak{y}}_2 \mathfrak{y}_2^{-1} = (y_2)$, $y_2 \geqslant 0$, $y_2 \equiv 1 \pmod{\sqrt{d}}$ and

$$\mathfrak{q}_2 = \mathfrak{y}_2 \mathfrak{n}.$$

Putting

$$\xi = \xi_1 y_2 \bar{\eta}\eta^{-1}$$

we get

$$N\xi = N\xi_1 = n'$$

and

$$\xi = \xi_1 \bar{\eta}\eta^{-1} \equiv \xi_1 \varepsilon = \tau (\operatorname{mod} \mathfrak{a}\sqrt{d}).$$

Moreover

$$\mathfrak{b}_{\mathfrak{q}_1\mathfrak{q}_2} = \bar{\mathfrak{q}}_2 \mathfrak{q}_2^{-1} \mathfrak{b}_{\mathfrak{q}_1} = \bar{\mathfrak{n}}\mathfrak{n}^{-1}(\xi_1 y_2) = (\xi).$$

Thus we have proved that the ideal $\mathfrak{b}_{\mathfrak{q}_1\mathfrak{q}_2}$ satisfies the conditions (5) and (6). It follows easily from Proposition 2 that the class $C \in I^d/I_1^d$ of the ideal $\mathfrak{q}_1\mathfrak{q}_2$ satisfies the conditions of Lemma 4 which completes its proof.

Let us put

$$C = \prod_{r=1}^{R} H_r^{a_r}, \quad 1 \leqslant a_r \leqslant h_r.$$

By Lemmata 2, 3 and 4 we get

$$N[F = n] = \sum_{\substack{\mathfrak{c} \subset \mathfrak{O} \\ N\mathfrak{c} = |m|N\mathfrak{g}^{-1}}} \sum_{\mathfrak{q}|\mathfrak{g}, \mathfrak{q} \in C} 1 = \sum_{\substack{\mathfrak{c} \subset \mathfrak{O} \\ N\mathfrak{c} = |m|N\mathfrak{g}^{-1}}} \prod_{r=1}^{R} \sum_{\substack{1 \leqslant l \leqslant l_r \\ l \equiv a_r (\operatorname{mod} h_r)}} \binom{l_r}{l}$$

$$= \sum_{\substack{\mathfrak{c} \subset \mathfrak{O} \\ N\mathfrak{c} = |m|N\mathfrak{g}^{-1}}} \prod_{r=1}^{R} h_r^{-1} 2^{l_r} \left\{1 + \theta_r (h_r - 1) \cos^{l_r} \frac{\pi}{h_r}\right\}$$

$$= h_f^{-1} \prod_{r=1}^{R} (1 + \theta_r \varepsilon_r) \sum_{\mathfrak{m} \subset \mathfrak{O}, N\mathfrak{m} = |m|} 1 = h_f^{-1} \prod_{r=1}^{R} (1 + \theta_r \varepsilon_r) \sum_{l|m} \chi(l),$$

where $-1 \leqslant \theta_r \leqslant 1$ (the numbers θ_r occurring in different places need not be equal). This completes the proof of Theorem 1.

Remark 4. The order h_f of the group I^d/I_1^d is given by the formula

$$h_f = \frac{\Phi(f)}{e_f \varphi(f)} h = \frac{fh}{e_f} \prod_{p|f} \left(1 - \frac{\chi(p)}{p}\right),$$

where h is the absolute class number, $\Phi(f)$ the number of residue classes of $\mathfrak{O} \bmod f$, prime to f, e_f the index of the group of units belonging to $\mathfrak{O}_f$ in $\mathscr{E}$.

Part II (Analytic)

An asymptotic formula for the sum $\sum_{p \leqslant n} \sum_{l|D-d(n-p)} \chi(l)$

§ 1. Lemmata from elementary and analytic number theory. The lemmata given below are mostly versions of those used by Hooley [6], suitable for a little different situation. The proofs that are simple or well known will be omitted.

Let us put

$$d_k(m) = \sum_{d_1 \ldots d_k = m} 1; \quad l_k(m) = \sum_{d|m} d^{-1}(1 + \log d)^k,$$

$$d(m; y) = \sum_{d|m, d \leqslant y} 1; \quad \sigma_{-1}(m; y) = \sum_{d|m, d > y} d^{-1},$$

$$d(m) = \sum_{d|m} 1; \quad \sigma_{-1}(m) = \sum_{d|m} d^{-1}.$$

LEMMA 1. *If* $1 \leqslant x \leqslant z \leqslant y$ *we have*

$$d(mn; y) \leqslant d(m; y) d(n; y),$$

$$\sigma_{-1}(mn; y) \leqslant \sigma_{-1}(m)\sigma_{-1}(n; y) + d(m) d(n; y) y^{-1},$$

$$\sum_{x \leqslant l \leqslant y} l^{-1} \sigma_{-1}(l) \leqslant \zeta(2)(1 + \log y/x),$$

$$\sum_{x \leqslant l \leqslant y} l^{-1} d(l; z) \leqslant (1 + \log z)(1 + \log y/x),$$

$$\sum_{l \leqslant z} l^{-1} \sigma_{-1}(m; z/l) \leqslant l_1(m),$$

$$\sum_{l \leqslant z} d(m; z/l)(1 + \log z/l)^k \leqslant k! z \sum_{i=0}^{k} \frac{l_i(m)}{i!},$$

$$l_k(m) \leqslant k!(\log\log 3m)^{k+1}.$$

Proof. All these formulae are given explicitly or implicitly in [6], sometimes in a slightly weaker version.

LEMMA 2. *Let* $R(m; x) = \sigma_{-1}(m) x^{-1} + \sigma_{-1}(m; x) + d(m; x) \dfrac{1 + \log x}{x}$. *Then*

$$\sum_{l \leqslant x, (l,m)=1} \frac{\chi(l)}{l} \prod_{p|l, p \nmid n} \left(1 - \frac{1}{p}\right)^{-1}$$

$$= L(1, \chi) \prod_{p|m} \left(1 - \frac{\chi(p)}{p}\right) \prod_{p \nmid mn} \left(1 + \frac{\chi(p)}{p(p-1)}\right) + O(R(m; x)).$$

The constant in the symbol O depends only on Δ.

Proof. First, we compute the following sum

$$\sum_{\substack{l\leqslant x\\(l,m)=1}}\frac{\chi(l)}{l}=\sum_{r|m}\mu(r)\frac{\chi(r)}{r}\sum_{l\leqslant x/r}\frac{\chi(l)}{l}$$

$$=\sum_{\substack{r|m\\r\leqslant x}}\mu(r)\frac{\chi(r)}{r}\left(L(1,\chi)+O\left(\frac{r}{x}\right)\right)$$

$$=L(1,\chi)\prod_{p|m}\left(1-\frac{\chi(p)}{p}\right)+O\left(\sigma_{-1}(m;x)+d(m;x)x^{-1}\right).$$

Next, we remark that for

$$\mu_n(d)=\begin{cases}\mu(d) & \text{if}\quad (d,n)=1,\\ 0 & \text{if}\quad (d,n)>1,\end{cases}$$

we have

$$\prod_{\substack{p|l\\p\nmid n}}\left(1-\frac{1}{p}\right)^{-1}=\prod_{\substack{p|l\\p\nmid n}}\left(1+\frac{1}{p-1}\right)=\sum_{d|l}\frac{|\mu_n(d)|}{\varphi(d)}.$$

Hence we get

$$\sum_{\substack{l\leqslant x\\(l,m)=1}}\frac{\chi(l)}{l}\prod_{\substack{p|l\\p\nmid n}}\left(1-\frac{1}{p}\right)^{-1}=\sum_{\substack{d\leqslant x\\(d,m)=1}}|\mu_n(d)|\frac{\chi(d)}{d\varphi(d)}\sum_{\substack{(l,m)=1\\l\leqslant x/d}}\frac{\chi(l)}{l}$$

$$=L(1,\chi)\prod_{p|m}\left(1-\frac{\chi(p)}{p}\right)\prod_{p\nmid mn}\left(1+\frac{\chi(p)}{p(p-1)}\right)+$$

$$+O\left(L(1,\chi)\prod_{p|m}\left(1-\frac{\chi(p)}{p}\right)\sum_{d>x}\frac{1}{d\varphi(d)}\right)+$$

$$+O\left(\sum_{d\leqslant x}\frac{1}{x\varphi(d)}d(m;x/d)\right)+O\left(\sum_{d\leqslant x}\frac{1}{d\varphi(d)}\sigma_{-1}(m;x/d)\right)$$

which by the formulae

$$\sum_{d>x}\frac{1}{d\varphi(d)}\ll x^{-1};\qquad \prod_{p|m}\left(1-\frac{\chi(p)}{p}\right)\leqslant\frac{m}{\varphi(m)}\ll\sigma_{-1}(m);$$

$$\sum_{d\leqslant x}\frac{1}{\varphi(d)}d(m;x/d)\leqslant d(m;x)\sum_{d\leqslant x}\frac{1}{\varphi(d)}\ll d(m;x)(1+\log x);$$

$$\sum_{d\leqslant x}\frac{1}{d\varphi(d)}\sigma_{-1}(m;x/d)$$

$$=\sum_{\substack{l|m\\l\leqslant x}}\frac{1}{l}\sum_{x/l<d\leqslant x}\frac{1}{d\varphi(d)}+\sum_{d\leqslant x}\frac{1}{d\varphi(d)}\sum_{\substack{l|m\\l>x}}\frac{1}{l}\ll d(m;x)x^{-1}+\sigma_{-1}(m;x)$$

implies the assertion of Lemma 2.

Substituting in Lemma 2 $n=1$ we get the following

COROLLARY.

$$\sum_{\substack{l\leqslant x\\(l,m)=1}}\frac{\chi(l)}{\varphi(l)}=L(1,\chi)\prod_{p|m}\left(1-\frac{\chi(p)}{p}\right)\prod_{p\nmid m}\left(1+\frac{\chi(p)}{p(p-1)}\right)+O\left(m^{1/10}(1+\log x)x^{-1}\right).$$

Proof. We have the obvious estimates

$$\sigma_{-1}(m)\leqslant d(m);\qquad \sigma_{-1}(m;x)\leqslant d(m)x^{-1};\qquad d(m;x)\leqslant d(m).$$

We have also $d(m)\ll m^{1/10}$. Hence

$$R(m;x)\leqslant\frac{3+\log x}{x}d(m)\ll m^{1/10}(1+\log x)x^{-1}$$

which completes the proof.

LEMMA 3. *If* $1\leqslant x\leqslant z\leqslant y$ *we have*

$$\sum_{r\leqslant x}\frac{1}{r}\sum_{x/r\leqslant l\leqslant y/r}\frac{1}{l}R\left(lw;\frac{z}{r}\right)\ll\left(l_2(w)+l_0(w)\log y/z\right)(1+\log y/x).$$

Proof. From Lemma 1 we get successively

$$R\left(lw;\frac{z}{r}\right)$$

$$\leqslant\sigma_{-1}(l)\left[\frac{r}{x}\sigma_{-1}(w)+\sigma_{-1}\left(w;\frac{x}{r}\right)\right]+\left[d(l)+d\left(l;\frac{z}{r}\right)\left(1+\log\frac{z}{r}\right)\right]\frac{r}{z}d\left(w;\frac{z}{r}\right),$$

$$\sum_{x/r\leqslant l\leqslant y/r}\frac{1}{l}R\left(lw;\frac{z}{r}\right)$$

$$\ll(1+\log y/x)\left[\sigma_{-1}(w)\frac{r}{x}+\sigma_{-1}\left(w;\frac{x}{r}\right)+\left(1+\log\frac{y}{r}+\log^2\frac{z}{r}\right)\frac{r}{z}d\left(w;\frac{z}{r}\right)\right],$$

$$\sum_{r\leqslant x}\frac{1}{r}\sum_{x/r\leqslant l\leqslant y/r}\frac{1}{l}R\left(lw;\frac{z}{r}\right)\ll(1+\log y/x)\left[l_2(w)+l_1(w)+l_0(w)\log y/z\right]$$

and the proof is complete.

LEMMA 4. *If $1 \leqslant x \leqslant z$ we have*

$$\sum_{ls\leqslant x}\frac{1}{ls^2}R\left(w;\frac{z}{ls}\right) \ll l_1(w).$$

Proof. Since

$$R(w; z/ls) \leqslant \sigma_{-1}(w)ls/x+\sigma_{-1}(w; x/ls)+d(w; z/ls)(1+\log z/ls)ls/z$$

we get from Lemma 1

$$\sum_{ls\leqslant x}\frac{1}{ls^2}R\left(w;\frac{z}{ls}\right)$$

$$\leqslant\frac{\sigma_{-1}(w)}{x}\sum_{ls\leqslant x}\frac{1}{s}+\sum_{ls\leqslant x}\frac{1}{ls^2}\sigma_{-1}\left(w;\frac{x}{ls}\right)+\frac{1}{z}\sum_{ls\leqslant z}s^{-1}d\left(w;\frac{z}{ls}\right)\left(1+\log\frac{z}{ls}\right)$$

$$\ll \sigma_{-1}(w)+l_1(w)+l_1(w) \ll l_1(w).$$

LEMMA 5 (A. I. Vinogradov). *Let $\Phi(x, z)$ be the number of positive integers with all prime factors $\leqslant z$. Then for $\log x\leqslant z\leqslant x^{1/e}$*

$$\Phi(x, z) \ll \left(\frac{e^3}{s\log s}\right)^s x,$$

where $s = \log x/\log z$. The constant in the symbol $\ll$ is absolute.

Proof, see [13], Theorem 1, part 1.

LEMMA 6. *If $2l < n$ we have*

$$\pi(n, l, a) \ll \frac{n}{\varphi(l)}\log^{-1}n/l.$$

This is Theorem 4.1 of Chapter II in [11].

LEMMA 7. *If $2m < n$ we have*

$$\sum_{\substack{p\leqslant n\\ |D-d(n-p)|=mp'}} 1 \ll \sigma_{-1}\big(d(D-dn)m\big)\frac{n}{m}\log^{-2}\frac{n}{m}.$$

This is a simple consequence of Theorem 4.2 of Chapter II in [11].

LEMMA 8 (Bombieri–Montgomery).

$$\sum_{l<\sqrt{n}\log^{-15}n}\max_{(a,l)=1}\max_{y\leqslant n}\left|\pi(y, l, a)-\frac{\mathrm{Li}\,y}{\varphi(l)}\right| \ll n\log^{-2}n.$$

This is a simple consequence of Theorem 15.1 of [10].

LEMMA 9 (C. Hooley). *Put*

$$P(n) = \prod_{\log x\leqslant\log n/\log^2\log n} p;\qquad B(n) = \prod_{p|P(n)}\left(1-\frac{1}{p}\right)\sim\frac{e^{-\gamma}\log^2\log n}{\log n},$$

$$f(\nu) = \begin{cases}1 & \text{if} \quad (\nu, P(n)) = 1,\\ 1 & \text{if} \quad \nu \text{ is a prime factor of } P(n),\\ 0 & \text{otherwise.}\end{cases}$$

Then for $y\leqslant n$ and $k\leqslant n^{9/10}$ we have

$$\sum_{\substack{\nu\leqslant y\\ \nu\equiv l\,(\mathrm{mod}\,k)}} f(\nu) = \begin{cases}B(n)y/\varphi(k)+O\left(\dfrac{n}{k\log^5 n}\right) & \text{if} \quad (l, k, P(n)) = 1,\\ O\left(\dfrac{n}{k\log^5 n}\right) & \text{if} \quad (l, k, P(n)) > 1.\end{cases}$$

Proof, see [6], Lemma 4.

LEMMA 10. *If $\frac{1}{2}\leqslant\alpha<1<\beta\leqslant\frac{3}{2}$, $e^3<c^3<M$, then*

$$\sum_{\substack{c^{-1}\sqrt{M}<l<c\sqrt{M}\\ \Omega(l)\leqslant\alpha\log\log M}} l^{-1} \ll (\log M)^{\alpha-1-\alpha\log\alpha}\log c,$$

$$\sum_{\substack{l\leqslant M\\ 1+\Omega(l)\geqslant\beta\log\log M}} l^{-1} \ll (\log M)^{\beta-\beta\log\beta}.$$

For $c = \log^3 M$ this is Lemma 7 of [6]. Hooley's proof can be easily extended to any c satisfying $e^3<c^3<M$.

§ 2. Formulation of Theorem 2. After these preparations we can proceed to the proof of the following

THEOREM 2. *For $n>\exp(|d|+|D|)$ we have*

$$\sum_{p\leqslant n}\sum_{l|D-d(n-p)}\chi(l) = 2L(1, \chi)\prod_{p|d(D-dn)}\left(1-\frac{\chi(p)}{p}\right)\prod_{p\nmid d(D-dn)}\left(1+\frac{\chi(p)}{p(p-1)}\right)\frac{n}{\log n}+$$

$$+O\left(\frac{n}{\log^{1+\delta}n}\log^5\log n\right),$$

where $\delta = \frac{1}{4}(2-e\log 2)>1/35$ (Hooley's constant). The constant in the symbol O depends only on Δ.

Let $\omega = d(D-dn)$, $m_\nu = D-d(n-\nu)$ and $\nu(l)$ be a solution of the congruence

$$m_\nu\equiv 0\ (\mathrm{mod}\ l)\quad\text{for}\quad (d, l) = 1.$$

Let

$$\mathcal{M} = \{m_p;\, p \leqslant n\}; \qquad M = \max_{m\in\mathcal{M}} |m|.$$

Hence

$$n < M = |d(n-2) - D| < n\log n.$$

Our sum can be represented in the following way

$$\sum_{p\leqslant n}\sum_{l|D-d(n-p)} \chi(l) = \sum_{m\in\mathcal{M}}\sum_{l|m}\chi(l)$$
$$= \sum_{m\in\mathcal{M}}\Big(\sum_{\substack{l|m\\ l\leqslant n_1}}\chi(l) + \sum_{\substack{l|m\\ n_1<l<n_2}}\chi(l) + \sum_{\substack{l|m\\ l\geqslant n_2}}\chi(l)\Big) = \Sigma_A + \Sigma_B + \Sigma_C,$$

where $n_1 = \sqrt{n}\log^{-16}n$, $n_2 = \sqrt{n}\log^{16}n$.

§ 3. An asymptotic formula for Σ_A. From Lemma 8 and Corollary to Lemma 2 we get

$$\Sigma_A = \sum_{\substack{l\leqslant n_1\\ (l,d)=1}}\chi(l)\pi\big(n, l, \nu(l)\big) = \sum_{\substack{l\leqslant n_1\\ (l,\omega)=1}}\chi(l)\pi\big(n, l, \nu(l)\big) + O(n_1)$$
$$= \sum_{\substack{l\leqslant n_1\\ (l,\omega)=1}}\frac{\chi(l)}{l}\,\mathrm{Li}\,n + O(n\log^{-2}n)$$
$$= L(1,\chi)\prod_{p|\omega}\Big(1-\frac{\chi(p)}{p}\Big)\prod_{p\nmid\omega}\Big(1+\frac{\chi(p)}{p(p-1)}\Big)\mathrm{Li}\,n + O(n\log^{-2}n) +$$
$$+\,O\Big(\frac{|\omega|^{1/10}\log n_1}{n_1}\,\mathrm{Li}\,n\Big)$$
$$= L(1,\chi)\prod_{p|\omega}\Big(1-\frac{\chi(p)}{p}\Big)\prod_{p\nmid\omega}\Big(1+\frac{\chi(p)}{p(p-1)}\Big)\mathrm{Li}\,n + O(n\log^{-2}n).$$

§ 4. An asymptotic formula for Σ_C. If $|D| < x \leqslant M$ the equation $|m_\nu| = x$ has exactly one solution $\nu[x] = n - x|d|^{-1} - Dd^{-1}$ contained in the interval $2 \leqslant \nu \leqslant n$. Since for $m\in\mathcal{M}$ we have

$$\chi(m) = \chi(D) = 1$$

hence and from Lemma 8 we get

$$\Sigma_C = \sum_{m\in\mathcal{M}}\sum_{\substack{l|m\\ l\leqslant|m|/n_2}}\chi(l) = \sum_{\substack{l\leqslant M/n_2\\ (l,d)=1}}\chi(l)\sum_{\substack{p\leqslant\nu[ln_2]\\ p\equiv\nu(l)\,(\mathrm{mod}\,l)}}1$$
$$= \sum_{\substack{l\leqslant M/n_2\\ (l,\omega)=1}}\frac{\chi(l)}{\varphi(l)}\,\mathrm{Li}\,\nu[ln_2] + O(n\log^{-2}n) + O(M/n_2).$$

To the last sum we shall apply partial summation. To this end we set

$$S(x) = \sum_{\substack{l\geqslant x\\ (l,\omega)=1}}\frac{\chi(l)}{\varphi(l)}$$

and remark that if $2\leqslant l\leqslant M/n_2$ we have

$$|\mathrm{Li}\,\nu[ln_2] - \mathrm{Li}\,\nu[(l-1)n_2]| = \int_{\nu[ln_2]}^{\nu[(l-1)n_2]}\log^{-1}u\,du < \nu[(l-1)n_2] - \nu[ln_2] = \frac{n_2}{|d|},$$
$$|\mathrm{Li}\,n - \mathrm{Li}\,\nu[n_2]| < |n-\nu[n_2]| < \frac{|D|+n_2}{|d|}.$$

Partial summation and Corollary to Lemma 2 give

$$\sum_{\substack{l\leqslant M/n_2\\ (l,\omega)=1}}\frac{\chi(l)}{\varphi(l)}\,\mathrm{Li}\,\nu[ln_2] = S(1)\,\mathrm{Li}\,\nu[n_2] - S([M/n_2]+1)\,\mathrm{Li}[M/n_2] +$$
$$+ \sum_{2\leqslant l\leqslant M/n_2} S(l)\big(\mathrm{Li}\,\nu[ln_2] - \mathrm{Li}\,\nu[(l-1)n_2]\big)$$
$$= S(1)\,\mathrm{Li}\,n + O\Big(|\omega|^{1/10}\frac{n_2}{|d|}\sum_{l\leqslant M/n_2} l^{-1}\log l\Big).$$

Hence

$$\Sigma_C = L(1,\chi)\prod_{p|\omega}\Big(1-\frac{\chi(p)}{p}\Big)\prod_{p\nmid\omega}\Big(1+\frac{\chi(p)}{p(p-1)}\Big)\mathrm{Li}\,n + O(n\log^{-2}n).$$

§ 5. An inequality for Σ_B. Let

$$D(m) = \sum_{\substack{l|m\\ n_1<l<n_2}} 1; \qquad F(m) = \sum_{\substack{l|m\\ n_1<l<n_2}}\chi(l).$$

From Cauchy–Schwartz inequality we get

$$\Sigma_B^2 \leqslant \Big(\sum_{\substack{m\in\mathcal{M}\\ D(m)\neq 0}} 1\Big)\Big(\sum_{m\in\mathcal{M}} F^2(m)\Big) = \Sigma_D\Sigma_E.$$

§ 6. Estimation of Σ_D. We have

$$\Sigma_D \leqslant n\log^{-2}n + \sum_{\substack{m\in\mathcal{M},\,|m|>n\log^{-2}n\\ 2\Omega(m)\leqslant e\log\log M}} D(m) + \sum_{\substack{m\in\mathcal{M}\\ 2\Omega(m)>e\log\log M}} 1 = n\log^{-2}n + \Sigma_{D1} + \Sigma_{D2}.$$

For the divisors l of numbers m involved in the summation of Σ_{D1} we have

$$4\Omega(l) \leqslant e\log\log M \quad \text{or} \quad 4\Omega(l') \leqslant e\log\log M;$$
$$n_1 < l < n_2; \qquad M_1 < n' < l' < n'' < M_2,$$

where $ll' = |m|$, $n' = \sqrt{n}\log^{-18}n$, $n'' = \sqrt{n}\log^{18}n$, $M_1 = \sqrt{M}\log^{-20}M$, $M_2 = \sqrt{M}\log^{20}M$. Hence and from Lemmata 6 and 10 we get

$$\Sigma_{D1} \leqslant \sum_{m\in\mathcal{M}} \sum_{\substack{l|m,\, n'<l<n'' \\ 4\Omega(l)\leqslant e\log\log M}} 1 = \sum_{\substack{n'<l<n'',\,(l,d)=1 \\ 4\Omega(l)\leqslant e\log\log M}} \pi\big(n, l, \nu(l)\big)$$

$$\ll \frac{n}{\log n'} \sum_{\substack{M_1<l<M_2 \\ 4\Omega(l)\leqslant e\log\log M}} \frac{1}{\varphi(l)} \ll n(\log n)^{\frac{e\log 2-4}{2}}\log^2\log n.$$

From Lemmata 5, 7 and 10 we obtain

$$\Sigma_{D2} \leqslant \Phi(M;\, M^{1/\log\log M}) + \sum_{M^{1/\log\log M}\leqslant p'\leqslant M} \sum_{\substack{m\in\mathcal{M},\, p'|m \\ 2\Omega(m)>e\log\log M}} 1$$

$$\ll n\log^{-2}n + \sum_{\substack{m\leqslant M^{1-1/\log\log M} \\ 2+2\Omega(m)>e\log\log M}} \sum_{|m_p|=mp'} 1$$

$$\ll n\log^{-2}n + n\log\log n \sum_{\substack{m<M^{1-1/\log\log M} \\ 2+2\Omega(m)>e\log\log M}} (m\log^2 n/m)^{-1}$$

$$\ll n\log^{-2}n + n\log^{-2}n\log^3\log n \sum_{\substack{m\leqslant M \\ 2+2\Omega(m)>e\log\log M}} m^{-1}$$

$$\ll n(\log n)^{\frac{e\log 2-4}{2}}\log^3\log n.$$

Finally

$$\Sigma_D \ll n(\log n)^{\frac{e\log 2-4}{2}}\log^3\log n.$$

§ 7. An inequality for Σ_E with quasiprimes. Let $f(\nu)$ be the function defined in Lemma 9, i.e. the characteristic function of the set of quasiprimes. Then

$$\Sigma_E = \sum_{m\in\mathcal{M}} F^2(m) \leqslant \sum_{\nu\leqslant n} f(\nu)F^2(m_\nu) = \sum_{\nu\leqslant n} f(\nu) \sum_{\substack{n_1<l',l''<n_2 \\ l'|m_\nu,\, l''|m_\nu}} \chi(l'l'')$$

$$= \sum_{\substack{r<n_2 \\ \nu\leqslant n_2}} f(\nu) \sum_{\substack{\frac{n_1}{r}<l_1,l_2<\frac{n_2}{r} \\ (l_1,l_2)=1,\, rl_1l_2|m_\nu}} \chi(l_1l_2) = \sum_{r\geqslant n^{1/8}} + \sum_{r<n^{1/8}} = \Sigma_{E1} + \Sigma_{E2}.$$

§ 8. Estimation of Σ_{E1}. In the range of summation of Σ_{E1} we have

$$rl_1l_2 < n_2^2/r \leqslant n^{7/8}\log^{32}n.$$

Hence and from Lemma 9 on quasiprimes we get

$$\Sigma_{E1} = \sum_{\substack{n^{1/8}\leqslant r<n_2,\, \frac{n_1}{r}<l_1,l_2<\frac{n_2}{r} \\ (l_1,l_2)=1,\,(rl_1l_2,d)=1}} \chi(l_1l_2) \sum_{\substack{\nu\leqslant n \\ \nu\equiv\nu(rl_1l_2)(\mathrm{mod}\, rl_1l_2)}} f(\nu)$$

$$= nB(n) \sum_{\substack{n^{1/8}\leqslant r<n_2,\, \frac{n_1}{r}<l_1,l_2<\frac{n_2}{r} \\ (l_1,l_2)=1,\,(rl_1l_2,w)=1}} \chi(l_1l_2)\varphi^{-1}(rl_1l_2) + O\Big(\frac{n}{\log^5 n}\sum_{r,l_1,l_2<n}\frac{1}{rl_1l_2}\Big)$$

$$= nB(n)\Big(\sum_{n^{1/8}\leqslant r\leqslant n_1} + \sum_{n_1<r<n_2}\Big) + O(n\log^{-2}n),$$

where $w = \big(\omega, P(n)\big)$.

For $\sum_{n_1<r<n_2}$ we have the trivial estimate

$$\sum_{n_1<r<n_2} \ll \log\log n \sum_{\substack{n_1<r<n_2 \\ \frac{n_1}{r}<l_1,l_2<\frac{n_2}{r}}} \frac{1}{rl_1l_2} \ll \log^4\log n.$$

Since if $(l_1, l_2) = 1$, then $\varphi(rl_1l_2) = \varphi(rl_1)l_2 \prod_{p|l_2,\, p\nmid r}\Big(1-\frac{1}{p}\Big)$ it follows

$$\sum_{n^{1/8}\leqslant r\leqslant n_1} = \sum_{\substack{n^{1/8}\leqslant r\leqslant n_1,\,(rl_1,w)=1 \\ n_1/r<l_1<n_2/r}} \frac{\chi(l_1)}{\varphi(rl_1)} \sum_{\substack{\frac{n_1}{r}<l_2<\frac{n_2}{r} \\ (l_2,l_1w)=1}} \frac{\chi(l_2)}{l_2} \prod_{p|l_2,\, p\nmid r}\Big(1-\frac{1}{p}\Big)^{-1}$$

$$\ll \log\log n \sum_{r\leqslant n_1<rl_1<n_2} \frac{1}{rl_1}\Bigg|\sum_{\substack{(l,l_1w)=1 \\ \frac{n_1}{r}<l<\frac{n_2}{r}}} \frac{\chi(l)}{l} \prod_{p|l,\, p\nmid r}\Big(1-\frac{1}{p}\Big)^{-1}\Bigg|.$$

By Lemma 2 the inner sum is $\ll R\Big(l_1w;\frac{n_1}{r}\Big) + R\Big(l_1w;\frac{n_2}{r}\Big)$, which by Lemma 3 implies

$$\sum_{n^{1/8}\leqslant r\leqslant n_1} \ll \big(l_2(w) + l_0(w)\log n_2/n_1\big)\log n_2/n_1\log\log n \ll \log^5\log n.$$

Finally

$$\Sigma_{E1} \ll nB(n)\log^5\log n + O(n\log^{-2}n) \ll \frac{n}{\log n}\log^7\log n.$$

§ 9. Estimation of Σ_{E2}. Since

$$\sum_{s|l_1,\, s|l_2} \mu(s) = \begin{cases} 1 & \text{if} \quad (l_1, l_2) = 1, \\ 0 & \text{if} \quad (l_1, l_2) > 1, \end{cases}$$

we have

$$\Sigma_{E2} = \sum_{\substack{r<n^{1/8}, rs<n_2 \\ \frac{n_1}{rs}<l_1, l_2<\frac{n_2}{rs}}} \chi(l_1 l_2) \sum_{\substack{\nu\leqslant n \\ l_1 l_2 mrs^2 = |m_\nu|}} f(\nu) = \sum_{s<n^{1/8}} + \sum_{s\geqslant n^{1/8}}.$$

For the sum $\sum_{s\geqslant n^{1/8}}$ we have the trivial estimate

$$\Big|\sum_{s\geqslant n^{1/8}}\Big| \leqslant \sum_{n^{1/8}\leqslant s, l_1 l_2 mrs^2\leqslant M} 1 \leqslant \sum_{s\geqslant n^{1/8}} \sum_{\mu\leqslant Ms^{-2}} d_4(\mu)$$
$$\ll \sum_{s\geqslant n^{1/8}} s^{-2} M \log^3 M \ll n\log^{-2} n.$$

Since $\chi(m_\nu) = \chi(D) = 1$, we have

$$\sum_{s<n^{1/8}} = \pm \sum_{\substack{r,s<n^{1/8}, n_1<rsl_1<n_2 \\ m\leqslant M/l_1 n_1 s, (l_1 mrs, d)=1}} \chi(mr) \sum_{\substack{mn_1 l_1 s<|m_\nu|<mn_2 l_1 s, \nu\leqslant n \\ \nu\equiv\nu(l_1 mrs^2)(\mathrm{mod}\, l_1 mrs^2)}} f(\nu).$$

Let us remark that for the numbers l_1, m, r, s involved in the summation of $\sum_{s>n^{1/8}}$ we have $l_1 mrs^2 \leqslant Mrs/n_1 < n^{3/4}\log^{17} n$, hence the inner sum can be estimated by means of Lemma 9. Thus we get

$$\sum_{s<n^{1/8}} \ll \sum_{\substack{r,s<n^{1/8}, n_1<rsl_1<n_2 \\ l_1 n_1 ms\leqslant M, (l_1 mrs, w)=1}} \chi(mr) \frac{\nu_2-\nu_1}{\varphi(l_1 mrs^2)} B(n) + \frac{n}{\log^5 n} \sum_{l_1, m, r, s<n} (l_1 mrs^2)^{-1}$$
$$\ll B(n) \sum_{\substack{s<n^{1/8}, l_1 n_1 ms\leqslant M \\ n^{-1/8} n_1 < sl_1 < n_2}} \frac{\nu_2-\nu_1}{\varphi(l_1 ms^2)} \Big| \sum_{\substack{r<n^{1/8}, (r,w)=1 \\ n_1<l_1 rs<n_2}} \frac{\chi(r)}{r} \prod_{p|r, p\nmid l_1 ms} \Big(1-\frac{1}{p}\Big)^{-1}\Big| + n\log^{-2} n,$$

where

$$\nu_2 = \nu[mn_1 l_1 s] = n - mn_1 l_1 s|d|^{-1} - Dd^{-1},$$
$$\nu_1 = \nu[\min(M, mn_2 l_1 s)] = \max(2, n - mn_2 l_1 s|d|^{-1} - Dd^{-1})$$

and hence

$$\nu_2 - \nu_1 \leqslant \min\big(l_1 ms(n_2-n_1)|d|^{-1}, n\big) \leqslant l_1 msn_2 |d|^{-1} \min\Big(1, \frac{|d|n_1}{l_1 ms}\Big).$$

From Lemma 3 applied to the inner sum we get the estimate

$$\Big|\sum_r\Big| \leqslant \sum_{r<n_2/n_1} \varphi^{-1}(r) \ll \log n_2/n_1 = \lambda(sl_1) \quad \text{if} \quad n_1 < sl_1 < n_2,$$
$$\Big|\sum_r\Big| \ll R(w; n_1/sl_1) + R(w; n_2/sl_1) = \lambda(sl_1) \quad \text{if} \quad n^{-1/8} n_2 \leqslant sl_1 \leqslant n_1,$$
$$\Big|\sum_r\Big| \ll R(w; n_1/sl_1) + R(w; n^{1/8}) = \lambda(sl_1) \quad \text{if} \quad n^{-1/8} n_1 < sl_1 < n^{-1/8} n_2.$$

Let us remark that

$$\sum_{m\leqslant M/sl_1 n_1} \min\Big(1, \frac{|d|n_1}{l_1 ms}\Big) = \sum_{m<\frac{|d|n_1}{sl_1}} 1 + \sum_{\frac{|d|n_1}{sl_1}\leqslant m\leqslant \frac{M}{sl_1 n_1}} \frac{|d|n_1}{l_1 ms} \ll \frac{|d|n_1}{sl_1} \log\log n.$$

Hence and from Lemma 4 the sum $\sum_{s<n^{1/8}}$ can be estimated as follows

$$\sum_{s<n^{1/8}} \ll B(n)\log\log n \sum_{\substack{n^{-1/8} n_1 < sl_1 < n_2 \\ s<n^{1/8}, m<M/l_1 n_1 s}} \lambda(sl_1) \frac{\nu_2-\nu_1}{l_1 ms^2} + n\log^{-2} n$$
$$\ll B(n)\log\log n \frac{n_2}{|d|} \sum_{\substack{n^{-1/8} n_1 < sl_1 < n_2 \\ s<n^{1/8}, m<M/l_1 n_1 s}} s^{-1}\lambda(sl_1)\min\Big(1, \frac{|d|n_1}{l_1 ms}\Big) + n\log^{-2} n$$
$$\ll B(n) n\log^2\log n \sum_{\substack{s<n^{1/8} \\ n^{-1/8} n_1 < sl_1 < n_2}} \frac{\lambda(sl_1)}{l_1 s^2}$$
$$\ll B(n) n\log^2\log n \Big\{\log^2\frac{n_2}{n_1} + R(w; n^{1/8})\log\frac{n_2}{n_1} +$$
$$+ \sum_{sl_1<n_1} \frac{1}{l_1 s^2}\Big(R\Big(w; \frac{n_1}{sl_1}\Big) + R\Big(w; \frac{n_2}{sl_1}\Big)\Big)\Big\}$$
$$\ll B(n) n\log^4\log n \ll \frac{n}{\log n}\log^6\log n.$$

Finally,

$$\Sigma_{E2} \ll \frac{n}{\log n}\log^6\log n.$$

Putting together the resuts of §§ 5–9 we get

$$\Sigma_B \ll \frac{n}{\log^{1+\delta} n}\log^5\log n$$

which completes the proof of Theorem 2.

Part III

Proof of the Main Theorem

§ 1. Estimation of $\sum_{m\in\mathscr{M}_{C,L}} \sum_{l|m} \chi(l)$. For a given positive integer L and a class $C\in I^d/I_1^d$ we set

$$\mathscr{M}_{C,L} = \Big\{m\in\mathscr{M};\ \sum_{\mathfrak{p}\|m, \mathfrak{p}\in C, \deg\mathfrak{p}=1} 1 \leqslant L\Big\}.$$

We shall prove

THEOREM 3. *There exists an absolute constant $A > 5$ such that*

$$\sum_{m\in\mathcal{M}_{C,L}}\sum_{l|m}\chi(l) \ll \frac{n}{\log^{1+1/h_f} n}\left(\frac{A\log\log n}{L}\right)^L$$

for $L < \log\log n$. The constant in the symbol $\ll$ is absolute.

In the proof we shall use the following

LEMMA. *For $x \geqslant 3$ we have*

$$\prod_{\mathfrak{p}\notin C,\, N\mathfrak{p}\leqslant x}(1+N\mathfrak{p}^{-1}) \ll (\log x)^{1-\frac{1}{h_f}}.$$

The constant in the symbol $\ll$ depends only on d.

Proof. Let $\mathscr{A}$ be any class of I^d/I_1^+. By Theorem 2.4, Chapter VIII of [3], we have

$$\sum_{\mathfrak{p}\in\mathscr{A},\, N\mathfrak{p}\leqslant x} 1 \sim \frac{1}{[I^d : I_1^+]}\,\frac{x}{\log x}.$$

Since C is a union of finite number of classes from I^d/I_1^+, we get

$$\sum_{\mathfrak{p}\in C,\, N\mathfrak{p}\leqslant x} 1 \sim \frac{1}{h_f}\,\frac{x}{\log x}$$

which implies the lemma.

Proof of Theorem 3. The sum in question can be decomposed into three sums in the following way

$$\sum_{m\in\mathcal{M}_{C,L}}\sum_{l|m}\chi(l) \leqslant \sum_{\substack{m\leqslant M\\ p|m\Rightarrow p\leqslant z}} d(m) + \sum_{\substack{m\leqslant M\\ \exists\, p^2|m\\ p>z}} d(m) + \sum_{\substack{m\in\mathcal{M}_{C,L}\\ \exists\, p\|m\\ p>z}}\sum_{l|m}\chi(l)$$
$$= \Sigma_F + \Sigma_G + \Sigma_H.$$

Putting $\log z = \log M/\log\log M$ we get from Vinogradov's lemma and Cauchy–Schwartz inequality

$$\Sigma_F^2 \leqslant \Phi(M; z)\sum_{m\leqslant M} d^2(m) \ll n^2\log^{-4} n,$$

$$\Sigma_G^2 \leqslant \Big(\sum_{\substack{m\leqslant M\\ \exists\, p^2|m\\ p>z}} 1\Big)\Big(\sum_{m\leqslant M} d^2(m)\Big) \ll M^2\log^3 M\sum_{p>z} p^{-2} \ll n^2\log^{-4} n.$$

Let us set

$$\mathscr{A}_{C,L} = \Big\{\mathfrak{a}\subset\mathfrak{O};\, (\mathfrak{a}, d) = 1,\ \sum_{\substack{\mathfrak{p}\|\mathfrak{a},\, \mathfrak{p}\in C\\ \deg\mathfrak{p}=1}} 1 \leqslant L\Big\}.$$

Then

$$\Sigma_H \leqslant 2\sum_{p\leqslant n}\sum_{p'>z}\sum_{\substack{\mathfrak{a}\in\mathscr{A}_{C,L}\\ |m_p|=p'N\mathfrak{a}}} 1 \leqslant 2\sum_{\substack{\mathfrak{a}\in\mathscr{A}_{C,L}\\ N\mathfrak{a}<M/z}}\sum_{\substack{p\leqslant n\\ |m_p|=p'N\mathfrak{a}}} 1$$
$$\ll \sum_{\substack{\mathfrak{a}\in\mathscr{A}_{C,L}\\ N\mathfrak{a}\leqslant M/z}}\frac{n\log\log n}{N\mathfrak{a}\log^2(nN\mathfrak{a}^{-1})} \leqslant \frac{n\log\log n}{\log^2(nz/M)}\sum_{\substack{\mathfrak{a}\in\mathscr{A}_{C,L}\\ N\mathfrak{a}\leqslant M}} N\mathfrak{a}^{-1}.$$

Let us set further

$$\mathscr{A}_1 = \{\mathfrak{b}^2;\, \mathfrak{b}\subset\mathfrak{O}\}\cap I^d,$$
$$\mathscr{A}_2 = \{\mathfrak{b};\, \mathfrak{p}|\mathfrak{b}\Rightarrow\mathfrak{p}^2\nmid\mathfrak{b},\ \chi(\mathfrak{p}) = -1\}\cap I^d,$$
$$\mathscr{A}_3 = \{\mathfrak{b};\, \mathfrak{p}|\mathfrak{b}\Rightarrow\mathfrak{p}^2\nmid\mathfrak{b},\ \chi(\mathfrak{p}) = 1,\ \mathfrak{p}\notin C\}\cap I^d,$$
$$\mathscr{A}_4 = \{\mathfrak{p}_1\ldots\mathfrak{p}_r;\, r\leqslant L,\ \chi(\mathfrak{p}_i) = 1,\ \mathfrak{p}_i\in C,\ \mathfrak{p}_i\neq\mathfrak{p}_j \text{ for } i\neq j\}.$$

Then

$$\mathscr{A}_{C,L} = \{\mathfrak{a}_1\mathfrak{a}_2\mathfrak{a}_3\mathfrak{a}_4;\, \mathfrak{a}_i\in\mathscr{A}_i,\ i = 1, 2, 3, 4\},$$

whence

$$\sum_{\substack{\mathfrak{a}\in\mathscr{A}_{C,L}\\ N\mathfrak{a}\leqslant M}} N\mathfrak{a}^{-1} \leqslant \Big(\sum_{\mathfrak{a}\in\mathscr{A}_1} N\mathfrak{a}^{-1}\Big)\Big(\sum_{\mathfrak{a}\in\mathscr{A}_2} N\mathfrak{a}^{-1}\Big)\Big(\sum_{\substack{\mathfrak{a}\in\mathscr{A}_3\\ N\mathfrak{a}\leqslant M}} N\mathfrak{a}^{-1}\Big)\Big(\sum_{\substack{\mathfrak{a}\in\mathscr{A}_4\\ N\mathfrak{a}\leqslant M}} N\mathfrak{a}^{-1}\Big) = \Sigma_1\Sigma_2\Sigma_3\Sigma_4.$$

We have the obvious estimates

$$\Sigma_1 \leqslant \sum_{\mathfrak{b}\subset\mathfrak{O}} N\mathfrak{b}^{-2} \ll 1,$$
$$\Sigma_2 \leqslant \sum_{(m,d)=1} |\mu(m)|\, m^{-2} \ll 1,$$
$$\Sigma_3 \leqslant \prod_{\mathfrak{p}\notin C,\, N\mathfrak{p}\leqslant M}(1+N\mathfrak{p}^{-1}) \ll (\log n)^{1-1/h_f}.$$

We have also

$$\sum_{N\mathfrak{p}\leqslant M} N\mathfrak{p}^{-1} \leqslant 2\sum_{p\leqslant M} p^{-1} \leqslant e^{-1}A\log\log n$$

for sufficiently large constant $A > 5$. Hence

$$\Sigma_4 \leqslant \sum_{r\leqslant L}\frac{1}{r!}\Big(\sum_{N\mathfrak{p}\leqslant M} N\mathfrak{p}^{-1}\Big)^r \leqslant \sum_{r\leqslant L}\Big(\frac{A}{r}\log\log n\Big)^r \ll \Big(\frac{A}{L}\log\log n\Big)^L$$

and the proof of Theorem 3 is complete.

§ 2. Proof of the Main Theorem. By Theorem 1 there exist positive real numbers $\varepsilon_0 = \varepsilon_0(d, D) < 1$, $L_0 = L_0(d, D)$ such that for $L > L_0$ we have

$$\begin{aligned}\Sigma^* &= \sum_{p\leqslant n} N[F = n-p]\\ &= \big(h_f^{-1} + O(\varepsilon_0^L)\big)\sum_{m\in\mathscr{M}}\sum_{l|m}\chi(l) + O\Big(\sum_{C\in I^d/I_1^d}\ \sum_{m\in\mathscr{M}_{C,L}}\ \sum_{l|m}\chi(l)\Big).\end{aligned}$$

Hence for $L_0 < L < \log\log n$ we obtain from Theorem 2 and 3

$$\Sigma^* - \frac{2}{h_f}L(1,\chi)\prod_{p|d(D-dn)}\Big(1-\frac{\chi(p)}{p}\Big)\prod_{p\nmid d(D-dn)}\Big(1+\frac{\chi(p)}{p(p-1)}\Big)\frac{n}{\log n}$$
$$\ll \varepsilon_0^L\frac{n}{\log n}\log\log n + \frac{n}{\log^{1+\delta} n}\log^5\log n + \frac{n}{\log^{1+1/h_f} n}\Big(\frac{A}{L}\log\log n\Big)^L.$$

On putting $L = \dfrac{1}{Ah_f^2}\log\log n$ we get the required estimate.

References

[1] Б. М. Бредихин, *Дисперсионный метод и бинарные аддитивные проблемы определенного типа*, Успехи мат. наук 20:2 (1965), pp. 89–130.

[2] Б. М. Бредихин и Ю. В. Линник, *Асимптотика и эргодические свойства решений обобщенного уравнения Гарди–Литтльвуда*, Мат. сб. 71 (1966), pp. 145–161.

[3] J. W. S. Cassels and A. Fröhlich, *Algebraic Number Theory*, London and New York 1967.

[4] G. H. Hardy and J. E. Littlewood, *Some Problems of 'Partitio Numerorum'. III: On the expression of a number as a sum of primes*, Acta Math. 44 (1923), pp. 1–70.

[5] — — *Some Problems of 'Partitio Numerorum'. V: A further contribution to the study of Goldbach's problems*, Proc. London Math. Soc. 22 (1924), pp. 46–56.

[6] C. Hooley, *On the representation of a number as the sum of two squares and a prime*, Acta Math. 97 (1957), pp. 189–210.

[7] H. Iwaniec, *Primes represented by quadratic polynomials in two variables*, Bull. Acad. Polon. Sci., Sér. Sci. Math. Astronom. Phys. 20 (1972), pp. 195–202.

[8] E. Landau, *Vorlesungen über Zahlentheorie III*, Leipzig 1927, reprint by Chelsea 1947.

[9] Ю. В. Линник, *Асимптотическая формула в аддитивной проблеме Гарди–Литтльвуда*, Изв. АН СССР, сер. мат. 24 (1960), pp. 629–706.

[10] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Berlin–Heidelberg–New York 1971.

[11] K. Prachar, *Primzahlverteilung*, Berlin–Göttingen–Heidelberg 1957.

[12] G. K. Stanley, *On the representation of a number as a sum of squares and primes*, Proc. London Math. Soc. 29 (1928), pp. 122–144.

[13] А. И. Виноградов, *О числах с малыми простыми делителями*, Докл. АН СССР 109 (1956), pp. 683–686.

Received on 18. 12. 1973 (503)

ACTA ARITHMETICA
XXVII (1975)

The proof of Minkowski's conjecture concerning the critical determinant of the region $|x|^p+|y|^p<1$ for $p\geqslant 6$

by

A. V. Malyshev and A. B. Voronetsky (Leningrad)

1. Introduction. Let $p>1$ be a real number, $\mathscr{D}_p$ be the convex region

$$|x|^p+|y|^p<1$$

and $\Delta(\mathscr{D}_p)$ be the critical determinant of $\mathscr{D}_p$ (for definition of the necessary notions from the geometry of numbers see Cassels [1]). Let us consider two $\mathscr{D}_p$-admissible lattices $\Lambda_p^{(0)}$ and $\Lambda_p^{(1)}$. $\Lambda_p^{(0)}$ as well as $\Lambda_p^{(1)}$ has six points on the boundary of $\mathscr{D}_p$ and $(1,0)\in\Lambda_p^{(0)}$, $(-2^{-1/p}, 2^{-1/p})\in\Lambda_p^{(1)}$. (The lattices $\Lambda_p^{(0)}$, $\Lambda_p^{(1)}$ are defined uniquely under those conditions.) We write $\Delta_p^{(0)}$, $\Delta_p^{(1)}$ for $d(\Lambda_p^{(0)})$, $d(\Lambda_p^{(1)})$. Minkowski [4] had conjectured that

$$\Delta(\mathscr{D}_p) = \min(\Delta_p^{(0)}, \Delta_p^{(1)}), \tag{1}$$

all critical lattices of $\mathscr{D}_p$ being contained among the lattices $\Lambda_p^{(0)}$, $\Lambda_p^{(1)}$ and among those which are symmetrical to $\Lambda_p^{(0)}$, $\Lambda_p^{(1)}$ with respect to lines $x=0$, $y=0$, $x=y$, $x=-y$.

Papers [2], [3], [5]–[9] are devoted to this conjecture. Watson [6] has proved that there exists a constant p_0, with $2.57<p_0<2.58$, such that

$$\Delta_{p_0}^{(0)} = \Delta_{p_0}^{(1)} \tag{2}$$

and

$$\begin{aligned}&\Delta_p^{(1)}<\Delta_p^{(0)} \quad\text{for}\quad 1<p<2,\ p>p_0,\\ &\Delta_p^{(0)}<\Delta_p^{(1)} \quad\text{for}\quad 2<p<p_0.\end{aligned} \tag{3}$$

Therefore the conjectural equality (1) can be written as

$$\Delta(\mathscr{D}_p) = \begin{cases}\Delta_p^{(1)} & \text{for}\quad 1\leqslant p\leqslant 2,\ p\geqslant p_0,\\ \Delta_p^{(0)} & \text{for}\quad 2\leqslant p\leqslant p_0.\end{cases} \tag{4}$$