For other $p$ it is equivalent to the system

$$
(70) \
\begin{align*}
&x \text{ind}2 + y \text{ind}3 = 0 \mod p - 1, \\
&y \text{ind}2 + z \text{ind}3 = 2 \text{ind}2 \mod p - 1,
\end{align*}
$$

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

Now

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

Hence

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

and the equation

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

is soluble in integers. The numbers $x = -\frac{\text{ind}3}{(\text{ind}2, \text{ind}3)}$, $y = \frac{\text{ind}2}{(\text{ind}2, \text{ind}3)}$

and $z$ satisfy the system $(70)$ and hence also $(69)$.

References


Received on 11. 11. 1973

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

by

HENRYK IWANIEC (Warszawa)

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
numeralorum". Having introduced in the analytic theory of numbers a new
and powerful circle method the authors derived with its help many asympto-

tic 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

$$
(HL) \sum_{p+p^2+p^3=n} 1
$$

and conjectured its validity (the first half of Conjecture J). In the fifth
paper of the series [3] they expressed the opinion that the generalised
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 $n$ is ternary one
and nowadays it can be easily solved without the generalised Riemann
hypothesis by using Vinogradov's estimates for trigonometric sums with
primes, which supplement the circle method in an essential way.
The generalized Hardy-Littlewood's problem

where \( F(x, y) = ax^2 + bxy + cy^2 + dx + ey + g \) 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

\[
\partial^2[F(x, y) - g] + G(r, s) = G(dx + r, dy + s),
\]

where \( r = bf - 2ac, s = be - 2af \) allows one to reduce to problem of representing \( m \) by \( F \) to that of representing \( m - g \) by \( G \) by 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 Bredhlin'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 \( 2^{r-1} \), where \( r \) 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 \( \mathfrak{O} \) of discriminant \( d \), in which there is no uniqueness of factorization into prime ideals. For this reason we give up the ideals in \( \mathfrak{O} \). Ordinary classes of ideals in \( (\mathfrak{d} \mathfrak{d}) \) being inadequate we introduce finer classes (their group is isomorphic to the group of classes of similar modules belonging to \( \mathfrak{O} \)). 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

\[
\sum_{\substack{p \leq x = \theta \log n \log \log n}} 1 = 2 \frac{b_2}{b_1} L(1, \chi) \prod_{p(D - d_0)} \left( \frac{1 - x(p)}{p} \right) \prod_{p(D - d_0)} \left( 1 + \frac{x(p)}{p(p - 1)} \right)^n \log n \log \log n.
\]
In the above formula $p$ runs over the primes $\leq n$; $\sum^e$ means that
the pairs $(x, y)$ and $(x', y')$ differing by an automorphism of $F$ are
identified; $\chi$ is the character of the field $Q(V \delta)$; $h_\delta$ is the order of
group $I^g : I^g_1$ (definition see part I, § 1). The constant in $\Theta$ 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
$\sum^e$, 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 $\sum^e_d$.

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 $\mathcal{N}[F = n]$

§ 1. Notations, definitions and selected facts from the theory of quadratic
fields. Let $K = Q(V \delta)$ be a quadratic field with discriminant $\Delta$, $\Sigma$
be the ring of integers of $K$ and $\Sigma_\Delta = \{ a : \Delta = 0 \}$ the order of
index $f$ and discriminant $d = \Delta f^2$. In the group $I$ of fractional ideals and
in the group $\sigma^+$ of units (of $K$) we can distinguish subgroups arranged in
the following diagrams

\[
\begin{array}{ccc}
I^d & \rightarrow & I^f \\
\uparrow & & \uparrow \\
I_d^f & \leftarrow & I^f_1 \\
\end{array}
\]

Here

\[
I^f = \{(\gamma) \in I ; \gamma > 0\}
\]

is the group of totally positive principal ideals
(i.e. ideals generated by totally positive elements),

\[
I^f = \{ a \epsilon I ; a = a \}$
\]

= 1 for all $\epsilon$

the group of ideals of the principal genus,

\[
I^f = \{(\gamma) \epsilon I^f ; \gamma = 1 \}$
\]

\[
I^f = \{(\gamma) \epsilon I^f ; \gamma \in \Sigma\}
\]

$\sigma^+$ = { $\gamma \epsilon \sigma^+ ; \gamma = 0 \}$ the group of totally positive units,

$\sigma_1^e$ = { $\gamma \epsilon \sigma^+ ; \gamma = 1 \}$ (mod $\Delta$).

The arrows in the diagrams denote inclusion.

Let $p_1, p_2, \ldots, p_t$ be the ramified ideals of $K$, i.e. the prime factors
of $\Delta$ and let us set $b = p_1 p_2 \ldots p_t$. Then

\[
I^f = \text{the group of genera}; \{ I^f : I^f \} = 2^{f-1},
\]

\[
I^f = \{ \gamma \epsilon I^f ; \gamma = \text{the group of classes in the principal genus}; \}
\]

\[
I^f = \{ \gamma \epsilon I^f ; \gamma = \text{the class group}; \}
\]

$\sigma^+$ = { $\gamma \epsilon \sigma^+ ; \gamma = 0 \}$ the group of ambiguous classes.

Each ambiguous class contains exactly two ideals dividing $b$. There exist
$2^{f-1}$ ambiguous classes. An ideal $a$ is called ambiguous if $a = \bar{a}$.
Every ambiguous ideal $a$ can be uniquely represented in the form
$a = (\gamma)b_1$, where $\gamma \epsilon Q^\times$, $b_1 \epsilon b$.

PROPOSITION 1. We have

\[
\sigma^+ = \{ \eta \gamma^{-1} ; \eta \epsilon b \}.
\]

Proof. For $\eta \epsilon b$ the ideal $(\eta)$ is ambiguous hence $\epsilon = \eta \gamma^{-1}$ is a unit. Clearly
\[
\epsilon > 0 \text{ thus } \eta \gamma^{-1} = \sigma^+.
\]

For $\epsilon \epsilon \sigma^+$ we get from Hilbert's theorem 90 that $\epsilon = \eta \gamma^{-1}$,
where $\eta \epsilon K^\times$ (hence the ideal $(\eta)$ is ambiguous and $\gamma = \gamma_\eta$,
where $r \epsilon Q^\times$, $\eta \epsilon b$. Clearly $\eta = \eta \gamma^{-1}$, thus \[
\sigma^+ = \{ \eta \gamma^{-1} ; \eta \epsilon b \}.
\]

PROPOSITION 2. We have

\[
I^f_1 = \{ a \epsilon I^f ; a \epsilon \gamma^{-1} \}
\]

Proof. The inclusion $I^f_1 = \{ a \epsilon I^f ; a \epsilon \gamma^{-1} \}$ is clear. Assume that
$a \epsilon I^f ; a \epsilon \gamma^{-1} = (\gamma)$, where $\gamma > 0$, $\gamma = 1 \mod \Delta$. Hence it follows in particular
that the ideal $a$ belongs to an ambiguous class, thus there exist
$q \epsilon b$ and $\varphi > 0$ such that $qa = (\varphi)$. Hence $a \epsilon \gamma^{-1} = (\varphi \varphi^{-1}) = (\gamma)$ and for a
certain $\epsilon \epsilon \sigma^+$ we have $\varphi \varphi^{-1} = \gamma$. By Proposition 1 there exists an
integer $q \epsilon b$ such that $a = \gamma \varphi^{-1}$. Putting $\varphi = \varphi \varphi^{-1} = 1 \mod \Delta$ we get $\varphi \varphi^{-1} = 1 \mod \Delta$. The ideal $(\gamma \varphi^{-1})$ can be uniquely represented in the form $b_1/b_2$,
where $b_1, b_2 \epsilon b$. Hence

\[
(\psi b_1/b_2, (\psi b_1/b_2) = 1, \varphi \epsilon 1 \mod b_2), \psi \epsilon \varphi \mod b_2, \varphi \psi = 0 \mod b_2.
\]

Since the number $(\psi - \varphi)/\Delta$ is rational, the last congruence can be strenghtened to
$(\psi - \varphi)/\Delta = 0 \mod b_2$, which implies that $(\psi - \varphi)/\Delta = 0 \mod b_2$.
On the other hand, the number $(\psi + \psi)/3$ is also rational, thus

\[
\psi = (\psi + \psi)/2 + (\psi - \varphi)/2 = 0 \mod b_2.
\]
which is possible only if \( b_1 = (1) \). Similarly one can prove that \( b_2 = (1) \). Therefore \( q = (q) \) and \( a = (q) \in \mathbb{P}_a^1 \), which completes the proof.

**Remark 1.** Proposition 2 can be worded as follows: \( \mathbb{P}_a^1/I_1^a \) is the group of the invariant classes of \( \mathbb{P}/I_1 \), i.e.

\[
I_1^a/I_1^a = \{ C \in \mathbb{P}/I_1^a ; \ C \in \mathcal{O} \}.
\]

**Proposition 3.** Let \( (e, d) = 1 \), \( Ne = 1 \pmod{d} \). Then there exists \( \eta \in \mathbb{K}^\times \) such that

\[
e = \bar{\eta}^{-1} (\mod d/(2, d)).
\]

Proof. Using the Chinese remainder theorem (for the field \( \mathbb{K} \)) it is easy to reduce the proof to the case of \( d \) being a prime power. It follows from the congruence \( es = 1 \pmod{d} \) that the ideals \( (e \pm 1, d) \) are ambiguous. Hence \( (e \pm 1, d)/2, d) \) or \( (e \pm 1, d)/(2, d) \). Setting

\[
\eta = \begin{cases} e+1 & \text{if } (e+1, d) | 2, \\ (e-1)^2 & \text{if } (e-1, d) | 2,
\end{cases}
\]

we get \( e = \bar{\eta}^{-1} (\mod d/(2, d)) \), which completes the proof.

**Remark 2.** Proposition 2 can be improved in the following way: Let \( d \) be a positive integer, \( e \in \mathbb{K}^\times \), \( (e, d) = 1 \). Then

\[
Ne = 1 (\mod d) \Rightarrow 0 = \bar{e} \equiv \eta^{-1} n (\mod d/(2, d, d)).
\]

Let \( G(x, y) = ax^2 + bxy + cy^2 \) be a primitive quadratic form of discriminant \( d = b^2 - 4ac \). Then the ideal \( a = (a, b+Vd)/2 \) is prime to \( a \) and has a norm \( Na = |a| \).

**Proposition 4.** Let us set \( M = aZ + b+Vd/2 Z \). Then \( M = a \cap \mathbb{O} \).

Proof. The inclusion \( M = a \cap \mathbb{O} \) is clear. For \( \xi \in a \cap \mathbb{O} \) we have

\[
y = (\xi - \bar{\xi})/Vd \in Q \cap \mathbb{O} = Z.
\]

and

\[
\xi - \frac{b+Vd}{2} y = \frac{\xi + \bar{\xi}}{2} - \frac{b(\xi - \bar{\xi})}{2Vd} e \in Q \cap \mathbb{O} = a \cap Z = aZ.
\]

Hence

\[
x = \left( \xi - \frac{b+Vd}{2} y \right) a^{-1} e Z \quad \text{and} \quad \xi = ax + \frac{b+Vd}{2} y e M,
\]

which completes the proof.

**Remark 3.** The group \( a/M \) is cyclic of order \( f \), thus the numbers

\[
a_2 \left( \frac{b+y^d}{2} \right)
\]

form a basis for the ideal \( a \) only if \( d \) is a fundamental discriminant.

**§ 2. Automorphs of the polynomial \( F(x, y) \).** The form \( aF \) and the polynomial \( a(D - dF) \) are in the field \( K \) the norm of a linear form \( \xi_{a, y} = ax + \frac{b+Vd}{2} y \) and of a linear polynomial \( \mu_{a, y} = \xi_{a, y} + \xi_{a, e} \), respectively:

\[
\begin{align*}
(1) \quad & aG(x, y) = N\xi_{a, y}, \\
(2) \quad & a(D - dF(x, y)) = N\mu_{a, y}.
\end{align*}
\]

Let us set \( \tau = \xi_{a, y} = \mu_{a, y} \). Then \( \tau = 0 (\mod a) \) and \( N\tau = a(D - dy) \). For integers \( x, y \in \mathbb{Z} \) we have

\[
(3) \quad \xi_{a, y} = 0 (\mod a); \quad \mu_{a, y} = \tau (\mod aVd) ; \quad N\mu_{a, y} = N\tau (\mod |ad|).
\]

Affine transformations

\[
\lambda(x, y) = (x', y') = (ax + by + \varphi, y + d + \psi),
\]

where

\[
\varphi, \psi, a, b, \gamma, \delta \in \mathbb{Z} ; \quad |ad - \beta y| = 1
\]

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

**Lemma 1.** The group \( \Lambda_F \) of automorphs of the form \( \lambda F \) is isomorphic to \( \mathbb{Z} \cap \mathbb{O} \). The isomorphism is defined by the formula

\[
\lambda_{\lambda F} \left( \lambda F \right) = \lambda \mathbb{O} \mathbb{F}.
\]

We shall prove

**Proposition 5.** If the discriminants of \( F \) are coprime then its group of automorphs \( \Lambda_F \) is isomorphic to \( \mathbb{Z} \). The isomorphism is defined by the formula

\[
\lambda_{\lambda F} \left( \lambda F \right) = \lambda \mathbb{O} \mathbb{F}.
\]

Proof. Since \( (d, D) = 1 \) the form \( G \) is primitive and \( (\tau^{-1}, d) = 1 \). Let \( \lambda(x, y) = (x', y') \) be an automorphism of \( F \). Then \( \lambda(x, y) - \lambda(0, 0) \) is an automorphism of \( G \), thus there exists \( e \in \mathbb{Z} \) such that \( \mu_{a, y} - \mu_{a, e} = e(\mu_{a, y} - \tau) \).

We have from (2) \( N\mu_{a, y} = N\mu_{a, e} \), hence for any \( m \in \mathbb{Z} \) we get

\[
\left| \mu_{a, y} \right| = \left| \mu_{a, e} \right| = \left| \mu_{a, y} - e \tau \right|.
\]
Since for suitable integers \( x, y \in \mathbb{Z} \) the number \( \mu_{x, y} \) has arbitrarily large divisors \( m \in \mathbb{Z} \) it follows that \( \tau = \mu_{x', y'} = \tau \) (mod \( v \tilde{d} \)). Hence \( \tau = 1 \) (mod \( v \tilde{d} \)) and \( \mu_{x', y'} = \tau \cdot \mu_{x, y} \).

Let \( \varepsilon = 1 \), and let \( x, y, x', y' \) be a solution in rationals of the equation \( \mu_{x, y} = \varepsilon \cdot \mu_{x', y'} \). Hence from (2) we get \( F(x', y') = F(x, y) \) and \( \mu_{x', y'} = \varepsilon \cdot \mu_{x, y} \) (mod \( \tilde{v} \tilde{d} \)). Therefore \( \xi_{x', y'} = \xi \). Hence and again from (2) we obtain

\[
N_{\tau} = N_{\xi_{x', y'}} = N_{\xi_{x, y}} = N_{\xi_{x, y}} \tilde{v} \tilde{d} + \tau
\]

Since \( \tau = 1 \) (mod \( v \tilde{d} \)) we have \( \xi_{x, y} = \xi_{x', y'} \) (mod \( v \tilde{d} \)), i.e., \( \xi_{x', y'} \in \mathfrak{O} \). It follows from Proposition 4 that the numbers \( x', y' \) are integers, thus \( \lambda(x, y) = (x', y') \) is an automorphism of \( \mathfrak{F} \).

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

\[ F(x, y) = n. \]

We say that two solutions \((x, y), (x', y')\) of (4) are equivalent, if \((x', y') = \lambda(x, y) \) for a certain \( \lambda \in \mathfrak{A} \). 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 \( (\mu) \in \mathfrak{O} \), such that

\[
N_{\mu} = a(D - d)n;
\]

\[
\mu = \tau \text{ (mod } v \tilde{d}).
\]

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 \( \varepsilon \in \mathfrak{O} \) we have \( \mu_{x, y} = \varepsilon \cdot \mu_{x, y} \). Since \( \mu_{x, y} = \mu_{x, y} = \tau \) (mod \( v \tilde{d} \)) it follows that \( \varepsilon = 1 \) (mod \( v \tilde{d} \)), 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

\[
N_{\tau} = N_{\mu} = N_{\xi} \tilde{v} \tilde{d} + \tau = (\tau \xi \tau \xi) \tilde{v} \tilde{d} + N_{\tau} \text{ (mod } |\tilde{a}|).\]

Since \( \tau = 1 \) (mod \( v \tilde{d} \)) we have \( \xi = \xi \) (mod \( v \tilde{d} \)), i.e., \( \xi \in \mathfrak{O} \). It follows from Proposition 4 that there exist integers \( x, y \in \mathbb{Z} \) 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 \( L_2 \) into a direct sum of cyclic groups

\[
L_2 = \bigoplus_{i=1}^{R} G_i,
\]

where \( G_i \) is generated by a class \( H_i \) of order \( h_i \), and let us introduce the following notation

\[
m = D - d n; \quad n' = a n; \quad l_i = \left\lfloor \frac{1}{\varepsilon_{n', a n'} \text{deg } - 1} \right\rfloor; \quad e_r = (h_r - 1) \cos \pi h_r \eta \pi.
\]

\[
N[F = n] \text{ the number of inequivalent solutions of the equation (4).}
\]

Theorem 1. If

(i) \( n' > 0 \) for \( d < 0 \),
(ii) \( (d, D) = 1 \),
(iii) \( h_r > 2 h_r \),
then there exist numbers \( h_r \) such that \(-1 \leq \theta \leq 1\) and

\[
N[F = n] = \frac{1}{h_r} \prod_{i=1}^{R} (1 + \theta, e_r) \sum_{l_m} \chi(l).
\]

Corollary. If \( L_2 = Z_2 \times \ldots \times Z_2 \), then we have under the assumption of Theorem 1

\[
N[F = n] = \frac{1}{h_r} \sum_{l_m} \chi(l).
\]

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

Lemma 2. For any integer \( m \neq 0 \) we have

\[
\sum_{\alpha = 0 \text{ or } \alpha = m} 1 = \sum_{l_m} \chi(l).
\]

Proof. see [8], Satz 882.

Lemma 3. For any positive integers \( L \) and \( h \) we have

\[
\sum_{\alpha \in \mathfrak{A}} \left( \frac{T_1}{L} \right) = h^{-1} 2L \sum_{l_m} \cos \left( \frac{(L - 2a) \pi r}{h} \right) \cos \pi \eta (h / L)
\]

where \(-1 \leq \theta \leq 1\).
Proof. Since
\[ \sum_{r=0}^{h-1} \frac{2^{2ir}-1}{h} = \begin{cases} h & \text{if } l \equiv a \pmod{h}, \\ 0 & \text{if } l \not\equiv a \pmod{h}, \end{cases} \]
we get
\[ h \sum_{l=1}^{h-1} \binom{L}{l} = \sum_{r=0}^{h-1} \sum_{0 \leq l \leq 2r \leq h} \binom{L}{l} e^{2\pi ir L/h} = \sum_{r=0}^{h-1} e^{-2\pi ir L/h} \left( 2 \cos \frac{\pi r}{h} \right)^L = 2^L \sum_{r=1}^{h-1} \cos \frac{(L-2)a + v}{p} \left( \cos \frac{a}{p} \right)^L \]
which completes the proof.

Proof of Theorem 1. By Proposition 6 the number \( N[F = \pi] \) is equal to the number of principal ideals of \( \mathcal{O} \) generated by elements satisfying the conditions (3) and (6). Hence if \( \pi' \) is not the norm of an ideal, \( N[F = \pi] = 0 \) and the formula (7) is trivial. Thus let us assume
\[ (8) \quad \pi' \text{ is the norm of an ideal (i.e. } \varepsilon_\pi(\pi') = \left( \frac{\pi'}{p} \right) = 1 \text{ for } p \mid A. \]
By the assumption (iii) there exist distinct and pairwise non-conjugate prime ideals \( p_{r,l} \in R \), \( 1 \leq r \leq L, \ 1 \leq l \leq L \), such that
\[ \chi(p_{r,l}) = 1 \text{ and } p_{r,l} \mid m. \]
Let us put
\[ s = \prod_{r=1}^{h} \prod_{l=1}^{L} p_{r,l} \]
and fix an integral ideal \( \mathcal{C} \) of the norm \( N \mathcal{C} = |m| N \mathcal{C}^{-1} \). Each integral ideal of the norm \( |m'| \) and divisible by \( \mathcal{C} \) can be uniquely represented in the form
\[ b_\pi = a \mathcal{C} q \mathcal{C}^{-1}, \]
where \( q \mid p \). We shall prove

**Lemma 4.** For each integral ideal \( \mathcal{C} \) of the norm \( |m| N \mathcal{C}^{-1} \) there exists a class \( \mathcal{C} \in I^2/I^2_0 \) such that an ideal \( b_\pi \) satisfies the conditions (5) and (6) if and only if \( \varepsilon_\mathcal{C} \mid \mathcal{C} \).

Proof. Ideals \( b_\pi \) have the norm \( N b_\pi = |m'| \), hence they belong to the same genus determined by the invariants
\[ \varepsilon_\pi(\pi') = \left( \frac{\pi'}{p} \right) \text{ for } p \mid A. \]
Let us remark, that for \( p \mid A \) we have
\[ \varepsilon_\pi(\pi') = \left( \frac{\pi'}{p} \right) = \left( \frac{a \pi, \pi'}{p} \right) = \left( \frac{D - dn, \pi'}{p} \right) = \left( \frac{\pi, \pi'}{p} \right) = 1 \]
whence for
\[ v = \begin{cases} 1 & \text{if } \pi' > 0, \\ \sqrt{\mathcal{A}} & \text{if } \pi' < 0, \end{cases} \]
we get
\[ \varepsilon_\pi(\pi') = \left( \frac{1}{p} \right) = 1 = \varepsilon_\pi(\pi') = \varepsilon_\pi(\pi') \quad \text{if } \pi' > 0. \]
and
\[ \varepsilon_\pi(\pi') = \left( \frac{\pi, \pi'}{p} \right) = \left( \frac{-1, \pi'}{p} \right) = \varepsilon_\pi(-\pi') = \varepsilon_\pi(\pi') \quad \text{if } \pi' < 0. \]
In view of the above, the principal ideal \( (\pi) \) belongs to the same genus as the ideals \( b_\pi \). In particular \( (\pi^{-1})b_\pi \mathcal{C} \mathcal{C}^{-1} \), i.e. there exists a number \( a \mid p \) and an ideal \( \mathcal{C} \) such that
\[ b_\pi = (a\mathcal{C}) \mathcal{C}^{-1} \mathcal{C}^{-1}. \]
It is easy to see, that for \( x \) one can take an ideal from \( \mathcal{I}^2 \), since each class of ideals contains an ideal prime to \( \mathcal{A} \).

If \( q \) runs over the divisors of the ideal \( \prod_{r=1}^{h} \prod_{l=1}^{L} p_{r,l} \), then its class \( I^2 \) runs through the whole group \( I^2/I^2_0 \), hence exactly one ideal \( q_1 \) is equivalent to \( x \) mod \( I^2_0 \), i.e. there exists \( \eta \in I^2_0 \) such that
\[ q_1 = \eta x. \]
If \( \eta \eta^{-1} = (y_1) \), \( y_1 \not\equiv 0 \) by putting \( \xi_1 = a\mathcal{C} N \mathcal{C}^{-1} \), we get
\[ b_\eta = b_{\eta_1} b_{\eta_1}^{-1} = (a\mathcal{C} N \mathcal{C}^{-1})^{-1} \]
and moreover
\[ N \xi_1 = \pi' \equiv N \mathcal{C} (\text{mod } |a\mathcal{C}|). \]
Hence for \( e = \xi_1 \) we have \( (e, \mathcal{C}) = 1 \) and \( N \mathcal{C} = 1 \) (mod \(|a\mathcal{C}|\)). By Proposition 3 there exists a number \( n \) such that \( e = n \eta^{-1} \) (mod \( \mathcal{A} \)). The ideal \( n = (1, \eta \eta^{-1})^{-1} \) belongs to \( I^2 \).
If \( q_2 \) runs over the divisors of the ideal \( \prod_{r=1}^{h} \prod_{l=1}^{L} p_{r,l} \) then its class runs through the whole group \( I^2/I^2_0 \) hence exactly one ideal \( q_2 \) is equivalent
mod $I_1^2$ to $\eta$, i.e. there exists $\eta_2 \in I_1^2$ such that $\bar{\eta}_2 \eta_2^{-1} = (y_2)$, $y_2 \equiv 0$, $y_2 = 1 \pmod{\sqrt{d}}$ and
\[ q_2 = \eta_2 \eta. \]
Putting
\[ \bar{\xi} = \xi_1 y_2 \bar{\eta} \eta^{-1} \]
we get
\[ N \bar{\xi} = N \bar{\xi}_1 = \eta \]
and
\[ \xi = \xi_1 \bar{\eta} \eta^{-1} = \bar{\xi}_1 \xi = \tau \pmod{\sqrt{d}}. \]
Moreover
\[ b_{n \eta} = \bar{q}_2 q_2^{-1} b_1 = \eta \eta^{-1} (\xi_1 y_2) = (\xi). \]
Thus we have proved that the ideal $b_{n \eta}$ satisfies the conditions (5) and (6).

It follows easily from Proposition 2 that the class $G \equiv I^2_1 I^2_1$ of the ideal $q_2 q_2^{-1}$ satisfies the conditions of Lemma 4 which completes its proof.

Let us put
\[ C = \prod_{r=1}^{R} 1_{\eta_0^r}, \quad 1 \leq \alpha_r \leq h_r. \]
By Lemma 2, 3 and 4 we get
\[ N[F = n] = \sum_{e_1 = 1}^{h_1} \sum_{\eta_0 = 1}^{h_0 \eta_0^{-1}} 1 = \sum_{e_1 = 1}^{h_1} \prod_{r=1}^{R} \left( \frac{1}{1 + \Theta_r(h_r - 1) \cos \pi h_r} \right) \]
\[ = h_1^{-1} \prod_{r=1}^{R} (1 + \Theta_r \xi_r) \sum_{m \in \mathcal{O}, m \equiv e_1} 1 = h_1^{-1} \prod_{r=1}^{R} (1 + \Theta_r \xi_r) \sum_{l \equiv e_1} \chi(l), \]
where $-1 \leq \Theta_r \leq 1$ (the numbers $\Theta_r$ occurring in different places need not be equal). This completes the proof of Theorem 1.

Remark 4. The order $h_r$ of the group $G \equiv I^2_1 I^2_1$ is given by the formula
\[ h_r = \frac{\Phi(f)}{e_r f} h = \frac{f h}{e_r} \prod_{l \nmid \Delta(f)} (1 - \frac{\chi(l)}{l}). \]
where $h$ is the absolute class number, $\Phi(f)$ the number of residue classes of $\mathcal{O}$ mod $f$, $e_r$ the index of the group of units belonging to $\mathcal{O}$, in $\mathfrak{f}$. 

Part II (Analytic)

An asymptotic formula for the sum $\sum_{p \leq x} \sum_{d \leq L} \chi(l)$

§ 1. Lemmata from elementary and analytic number theory. Thelemmata 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
\[ d_k(m) = \sum_{d_1 \cdots d_k = m} 1; \quad l_k(m) = \sum_{d \leq m} d^{-1} (1 + \log d)^k; \]
\[ d(m; y) = \sum_{d \leq m, d \leq y} 1; \quad \sigma_{-1}(m; y) = \sum_{d \leq m, d \leq y} d; \]
\[ d(m) = \sum_{d \leq m} 1; \quad \sigma_{-1}(m) = \sum_{d \leq m} d^{-1}. \]

**Lemma 1.** If $1 \leq \alpha \leq \beta \leq y$, we have
\[ d(m; y) \leq d(m; y) d(n; y), \]
\[ \sigma_{-1}(m; y) \leq \sigma_{-1}(m) \sigma_{-1}(n; y) + d(m) d(n; y) y^{-1}, \]
\[ \sum_{1 \leq k \leq \beta} l_{-1}(2^{k})(1 + \log y/\alpha), \]
\[ \sum_{1 \leq k \leq \beta} l_{-1}(k ; 1) (1 + \log \xi/\alpha), \]
\[ \sum_{1 \leq k \leq \beta} l_{-1}(m ; 1) (1 + \log y/\alpha), \]
\[ \sum_{1 \leq k \leq \beta} d(m ; y)^2 (1 + \log y/\alpha), \]
\[ \sum_{1 \leq k \leq \beta} l_{-1}(m ; 1) (1 + \log y/\alpha), \]
\[ l_{-1}(m) \leq k ! (1 + \log 3 m)^{\beta + 1}. \]

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

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

Then
\[ \sum_{l \leq \alpha, l \nmid (m,a)} \frac{\chi(l)}{l} \prod_{p \mid l \nmid (m,a)} \left( 1 - \frac{1}{p} \right), \]
\[ = \frac{L(1, \chi)}{\prod_{p \mid m} \left( 1 - \frac{1}{p} \right)} \prod_{p \mid m} \left( 1 + \frac{\chi(p)}{p(p-1)} \right) + O(R(m; a)). \]

The constant in the symbol $O$ depends only on $\Delta$. 

28 — Acta Arithmetica XXVII.
Proof. First, we compute the following sum
\[ \sum_{\ell \leq s} \frac{1}{\ell} \sum_{\ell \leq s} \frac{1}{\ell} = \sum_{\ell \leq s} \mu(\ell) \frac{\chi(\ell)}{\ell} \sum_{\ell \leq s} \frac{1}{\ell} = \sum_{\ell \leq s} \mu(\ell) \left( \frac{\chi(\ell)}{\ell} \sum_{\ell \leq s} \frac{1}{\ell} \right) \]
\[ = \sum_{\ell \leq s} \mu(\ell) \left( \frac{\chi(\ell)}{\ell} \sum_{\ell \leq s} \frac{1}{\ell} \right) \]
\[ = \frac{1}{\ell} \left( 1 - \frac{\chi(\ell)}{\ell} \sum_{\ell \leq s} \frac{1}{\ell} \right) + O(\sigma_1(m; a)) \]
\[ = \frac{1}{\ell} \left( 1 - \frac{\chi(\ell)}{\ell} \sum_{\ell \leq s} \frac{1}{\ell} \right) + O(\sigma_1(m; a)) \]

Next, we remark that for
\[ \mu_n(d) = \begin{cases} \mu(d) & \text{if } (d, n) = 1, \\ 0 & \text{if } (d, n) > 1, \end{cases} \]
we have
\[ \prod_{p \mid n} \left( 1 - \frac{1}{p} \right) = \prod_{p \mid n} \left( 1 - \frac{1}{p} \right) = \prod_{p \mid d} \frac{|\mu_n(d)|}{\phi(d)}. \]

Hence we get
\[ \sum_{\ell \leq s} \frac{1}{\ell} \prod_{p \mid \ell} \left( 1 - \frac{1}{p} \right) = \sum_{\ell \leq s} \frac{1}{\ell} \prod_{p \mid \ell} \left( 1 - \frac{1}{p} \right) = \sum_{\ell \leq s} \frac{1}{\ell} \prod_{p \mid \ell} \left( 1 - \frac{1}{p} \right) + O \left( \sigma_1(m; a) + O(\sigma_1(m; a)) \right) \]
\[ = \frac{1}{\ell} \left( 1 - \frac{\chi(\ell)}{\ell} \sum_{\ell \leq s} \frac{1}{\ell} \right) + O \left( \sigma_1(m; a) + O(\sigma_1(m; a)) \right) \]
\[ = \frac{1}{\ell} \left( 1 - \frac{\chi(\ell)}{\ell} \sum_{\ell \leq s} \frac{1}{\ell} \right) + O \left( \sigma_1(m; a) + O(\sigma_1(m; a)) \right) \]
\[ = \frac{1}{\ell} \left( 1 - \frac{\chi(\ell)}{\ell} \sum_{\ell \leq s} \frac{1}{\ell} \right) + O \left( \sigma_1(m; a) + O(\sigma_1(m; a)) \right) \]

which completes the proof.

Lemma 3. If \( 1 \leq \omega \leq \varepsilon \leq y \) we have
\[ \sum_{r \in \mathbb{N}} \frac{1}{r} \sum_{\omega \leq r < \varepsilon} R \left( \left| \frac{\omega}{r} \right| \right) \leq \int_{\omega}^x \frac{\ln x}{x} \left( 1 + \ln \frac{x}{r} \right) \left( 1 + \ln \frac{x}{r} \right). \]

Proof. From Lemma 1 we get successively
\[ R \left( \left| \frac{\omega}{r} \right| \right) \leq \sigma_1 \left( \frac{\omega}{r} \right) \left( 1 + \ln \frac{x}{r} \right) \left( 1 + \ln \frac{x}{r} \right) \]
\[ \leq \sigma_1 \left( \frac{\omega}{r} \right) \left( 1 + \ln \frac{x}{r} \right) \left( 1 + \ln \frac{x}{r} \right) \]
\[ \leq (1 + \ln \frac{x}{r}) \left( 1 + \ln \frac{x}{r} \right). \]

and the proof is complete.
LEMMA 4. If $1 \leq x \leq z$ we have

$$\sum_{l \leq x} \frac{1}{l} R \left( w; \frac{x}{l} \right) \ll H(w).$$

Proof. Since

$$R(w; s/l) \ll \sigma_{-1}(w) s/x + \sigma_{-1}(w) w/l + d(w; s/l) (1 + \log s/l) l/s \leq \frac{x}{l}$$

we get from Lemma 1

$$\sum_{l \leq x} \frac{1}{l} R \left( w; \frac{x}{l} \right) \ll \frac{\sigma_{-1}(w)}{x} \frac{x}{l} + \sum_{l \leq x} \frac{1}{l} \sigma_{-1}(w) \frac{x}{l} + \frac{1}{l} \sum_{l \leq x} \frac{1}{l} \left( 1 + \log \frac{s}{l} \right) \frac{x}{l}.$$

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

LEMMA 5 (A. I. Vinogradov). Let $\Phi(x, z)$ be the number of positive integers with all prime factors $\leq z$. Then for $x \leq z \leq x^{1/2}$

$$\Phi(x, z) \ll \left( \frac{z}{\log z} \right)^{2/3},$$

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

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

LEMMA 6. If $2l \leq n$ we have

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

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

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

$$\sum_{n = \max \left| d(D - d_m) \right|}^{\min \left| d(D - d_m) \right|} e^{-\frac{n}{m} \log \frac{n}{m}} \ll \log \frac{n}{m}.$$}

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

LEMMA 8 (Bombieri–Montgomery).

$$\sum_{n \leq x} \max_{l \leq n \leq x} \left( \frac{\pi(x, l, a)}{\varphi(l)} \right) \ll \log^{-1} n.$$}

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

LEMMA 9 (C. Hooley). Put

$$P(n) = \prod_{p \leq \log \log \log n} \left( 1 - \frac{1}{p} \right) \sim \frac{1}{\log \log n},$$

$$B(n) = \prod_{p \leq \log \log \log n} \left( 1 - \frac{1}{p} \right) \sim \frac{1}{\log \log n},$$

$$f(v) = \begin{cases} 1 & \text{if } \nu, P(n) = 1, \\ 0 & \text{otherwise}. \end{cases}$$

Then for $n \leq n$ and $k \leq n^{1/4}$ we have

$$\sum_{l \leq n, (l, k) = 1} f(v) \frac{B(n) y}{\varphi(k)} + 0 \left( \frac{n}{\log \log n} \right)$$

if $(l, k, P(n)) = 1$,

$$0 \left( \frac{n}{\log \log n} \right) \quad \text{if } (l, k, P(n)) > 1.$$

Proof, see [6], Lemma 4.

LEMMA 10. If $1/2 < \gamma < \delta < 1, \varepsilon < \varepsilon < M$, then

$$\sum_{\substack{\sigma_{-1}(n) \leq \log n \leq \log n \leq 1 + \delta, \log \log n \leq 1}} e^{-\frac{n}{\log \log n} \log \log n} \ll (\log M)^{1 - \delta}.$$}

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

§ 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

$$\sum_{\substack{\sigma_{-1}(n) \leq \log n \leq \log n \leq 1 + \delta, \log \log n \leq 1}} \chi(l) = 2L(1, \chi) \prod_{p \leq \log \log n} \left( 1 - \frac{\chi(p)}{p} \right) \prod_{p \leq \log \log n} \left( 1 + \frac{\chi(p)}{p (p - 1)} \right) \frac{n}{\log \log n} + O \left( \frac{n}{\log \log n} \log \log n \right),$$

where $\delta = \frac{1}{4} (3 - \log 2) > 1/35$ (Hooley's constant). The constant in the symbol $O$ depends only on $\Delta$.

Let $a = \frac{d(D - d_m)}{m} = D - d(n - v)$ and $v(l)$ be a solution of the congruence

$$m \equiv 0 \pmod{l} \quad \text{for } (d, l) = 1.$$
Let 
\[ \mathcal{M} = \{m_p; p \leq n\}; \quad M = \max_{m \in \mathcal{M}} |m|. \]

Hence
\[ n < M = |d(n-2) - D| < n \log n. \]

Our sum can be represented in the following way
\[
\sum_{x \geq 1} \sum_{l \geq 2} \chi(l) = \sum_{l \in \mathcal{M}} \sum_{\substack{n \leq x \leq \frac{x}{l}}} \chi(l) = \sum_{l \in \mathcal{M}} \left( \sum_{n \leq x \leq \frac{x}{l}} \chi(l) \right) + \sum_{l \in \mathcal{M}} \sum_{n_1 \leq l < n_2} \chi(l) = \Sigma_D + \Sigma_P + \Sigma_C,
\]
where \( n_1 = \sqrt{n \log^{-14} n}, n_2 = \sqrt{n \log^{-1.5} n}. \)

§ 3. An asymptotic formula for \( \Sigma_D. \) From Lemma 8 and Corollary to Lemma 2 we get
\[
\Sigma_D = \sum_{l \in \mathcal{M}} \chi(l) \pi(n, l, \nu(l)) = \sum_{l \in \mathcal{M}} \chi(l) \pi(n, l, l, \nu(l)) + O(n_2)
\]
\[= \sum_{l \in \mathcal{M}} \frac{\chi(l)}{l} \ln + O(n \log^{-2} n) \]
\[= L(1, \chi) \prod_{p \in \mathcal{M}} \left( 1 - \frac{\chi(p)}{p} \right) \prod_{p \in \mathcal{M}} \left( 1 + \frac{\chi(p)}{p(p-1)} \right) \ln + O(n \log^{-2} n) + \left( \frac{\log n}{n} \right) \ln \]
\[= L(1, \chi) \prod_{p \in \mathcal{M}} \left( 1 - \frac{\chi(p)}{p} \right) \prod_{p \in \mathcal{M}} \left( 1 + \frac{\chi(p)}{p(p-1)} \right) \ln + O(n \log^{-2} n) .
\]

§ 4. An asymptotic formula for \( \Sigma_C. \) If \( |D| < n \leq M \) the equation \( |m| = n \) has exactly one solution \( \nu(n) = n - |d|^{-1} - D \) contained in the interval \( 2 \leq \nu \leq n. \) Since for \( m \in \mathcal{M} \) we have
\[ \chi(m) = \chi(D) = 1 \]
hence and from Lemma 8 we get
\[
\Sigma_C = \sum_{m \in \mathcal{M}} \sum_{l \leq m \leq n_2} \chi(l) = \sum_{l \leq \frac{n}{\sqrt{n \log n}}} \chi(l) \sum_{\nu = \frac{n}{l}}^{\frac{n}{l+1}} 1
\]
\[= \sum_{l \leq \frac{n}{\sqrt{n \log n}}} \frac{\chi(l)}{\nu(l)} \ln + O(n \log^{-2} n) + O(M/n_2).
\]

To the last sum we shall apply partial summation. To this end we set
\[
S(x) = \sum_{l \geq 1} \frac{\chi(l)}{\nu(l)}
\]
and remark that if \( 2 \leq l \leq M/n_2 \) we have
\[
|\mathcal{L}(\nu(n_2) - \mathcal{L}(\nu(l-1)n_2)| = \sum_{n_2}^{n_2} \log^{-1} n \ln v < r[(l-1)n_2] - r[ln_2] = \frac{n_2}{|d|} \]
\[|\mathcal{L}n - \mathcal{L}v[n_2]| < |n - v[n_2]| < \frac{|D| + n_2}{|d|}.
\]

Partial summation and Corollary to Lemma 2 give
\[
\sum_{l \leq M/n_2} \frac{\chi(l)}{\nu(l)} \ln + O(n \log^{-2} n) = S(1) \ln + O(n \log^{-2} n) + \sum_{l \leq M/n_2} S(l) \ln + O(n \log^{-2} n)
\]
\[= S(1) \ln + O\left( \frac{1}{\log n} \right) + \sum_{l \leq M/n_2} S(l) \ln + O(n \log^{-2} n).
\]

Hence
\[
\Sigma_C = L(1, \chi) \prod_{p \in \mathcal{M}} \left( 1 - \frac{\chi(p)}{p} \right) \prod_{p \in \mathcal{M}} \left( 1 + \frac{\chi(p)}{p(p-1)} \right) \ln + O(n \log^{-2} n). \]

§ 5. An inequality for \( \Sigma_P. \) Let
\[
D(m) = \sum_{m \leq \nu \leq n} 1; \quad F(m) = \sum_{m \leq \nu \leq n} \chi(l).
\]
From Cauchy–Schwartz inequality we get
\[
\Sigma_P \leq \left( \sum_{m \leq |D(m)|} \right) \left( \sum_{m \leq |D(m)|} F(m) \right) = \Sigma_D \Sigma_D.
\]

§ 6. Estimation of \( \Sigma_D. \) We have
\[
\Sigma_D \leq n \log^{-2} n + \sum_{m \in \mathcal{M}} D(m) + \sum_{m \in \mathcal{M}} \log \log |D(m)|
\]
\[= \sum_{m \in \mathcal{M}} \log \log |D(m)| + \log \log |D(m)|
\]
For the divisors \( l \) of numbers \( m \) involved in the summation of \( \Sigma_D \) we have
\[4 \mathcal{O}(l) \leq \log \log M \quad \text{or} \quad \mathcal{O}(l') \leq \log \log M; \]
\[n_1 < l < n_2; \quad M_1 < n < l < n'< M_2;
\]
\[n_2 < l + n_1; \quad M_1 < n < l < n'_2; \quad M_2.
\]
where \( U = \{ |m| \} \), \( n' = V n \log^{-2} n \), \( n'' = V n \log^{-2} n \), \( M_1 = V M \log^{-2} M \), \( M_2 = V M \log^{-2} M \). Hence and from Lemma 6 and 10 we get

\[
\Sigma_{D_1} \leq \sum_{l < M_1} \sum_{n \ll \log M} \sum_{l' \ll \log M} \pi(n, l, \nu(l)) \leq \frac{n}{\log n} \sum_{l \ll \log M} \sum_{m \ll \log M} \frac{1}{\varphi(l)} \ll n(\log n)^{-2} \log^2 \log n.
\]

From Lemma 5, 7 and 10 we obtain

\[
\Sigma_{D_2} \leq \Phi(M; M \log^{-2} M) + \sum_{\log \log M} \sum_{m \ll \log M} \sum_{l \ll \log M} \sum_{l' \ll \log M} \sum_{m \ll \log M} \sum_{l \ll \log M} \frac{1}{\varphi(l)} \ll \frac{n \log^2 n + n \log \log n + \log^2 \log \log n + \log^2 \log^2 \log n}{\log \log M}
\]

Finally

\[
\Sigma_D \ll n(\log n)^{-2} \log^2 \log n.
\]

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

\[
\Sigma_E = \sum_{m \ll M} f_1(m) = \sum_{m \ll M} f(M) \sum_{m \ll M} \frac{1}{\varphi(l)} \ll \log \log n \sum_{\nu_1 < \nu_2 \ll \log \log n} \frac{1}{\nu_1 \nu_2} \ll \log \log n.
\]

By Lemma 2 the inner sum is \( \ll R \left( \frac{1}{\nu_1 \nu_2} \right) \), which by Lemma 3 implies

\[
\sum_{\nu_1 < \nu_2 \ll \log \log n} \frac{1}{\nu_1 \nu_2} \ll \log \log n.
\]

Finally

\[
\Sigma_E \ll n \log \log n + O(n \log^{-2} n) \ll \frac{n \log \log n}{\log n}.
\]

§ 8. Estimation of \( \Sigma_{E_1} \). In the range of summation of \( \Sigma_{E_1} \) we have

\[
r_1 l_2 < n_1^2/r \ll n^{3/2} \log^2 n.
\]

Hence and from Lemma 9 on quasiprimes we get

\[
\Sigma_{E_1} = \sum_{n_1 \ll \log n} \sum_{l_1 \ll \log n} \chi(l_1, l_2) \sum_{r_1 \ll \log n} \sum_{r_2 \ll \log n} f(v) \ll \frac{n \log n}{\log \log n} \sum_{\nu_1 < \nu_2 \ll \log \log n} \frac{1}{\nu_1 \nu_2} \ll n \log \log n + O(n \log^{-2} n),
\]

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

For \( n_1 < \nu < n_2 \) we have the trivial estimate

\[
\sum_{n_1 < \nu < n_2} \ll \log \log n \sum_{n_1 < \nu < n_2} \frac{1}{\nu_1 \nu_2} \ll \log \log n.
\]

Since if \( l_1, l_2 = 1 \), then \( \varphi(\nu_1 \nu_2) = \varphi(\nu_1) \nu_2 \prod_{\nu_1 \nu_2} \left( 1 - \frac{1}{\nu} \right) \) it follows

\[
\sum_{\nu_1 < \nu_2 \ll \log \log n} \frac{1}{\nu_1 \nu_2} \ll \log \log n \sum_{\nu_1 < \nu_2 \ll \log \log n} \frac{1}{\nu_1 \nu_2} \ll \log \log n \sum_{\nu_1 < \nu_2 \ll \log \log n} \frac{1}{\nu_1 \nu_2} \ll \log \log n.
\]

By Lemma 2 the inner sum is \( \ll \log \log \log \log n \), which by Lemma 3 implies

\[
\sum_{\nu_1 < \nu_2 \ll \log \log n} \frac{1}{\nu_1 \nu_2} \ll \log \log n.
\]

Finally

\[
\Sigma_{E_1} \ll nB(n \log \log n + O(n \log^{-2} n) \ll \frac{n \log \log n}{\log n}.
\]
we have
\[ \sum_{\nu < \alpha < s} \nu \sum_{s = \alpha + \beta} f(\nu) = \sum_{s = \alpha} + \sum_{s > \alpha}. \]

For the sum \( \sum_{s = \alpha} \) we have the trivial estimate
\[ \sum_{s = \alpha} \leq \sum_{s = \alpha} \sum_{\nu < s} 1 < \sum_{s = \alpha} \sum_{\nu < s} s \log^2 \nu \leq s^{-2} M \log^2 M \leq \log^{-2} n. \]

Since \( \chi(m) = \chi(D) = 1 \), we have
\[ \sum_{s = \alpha} \leq \sum_{s = \alpha} \sum_{\nu < s} \chi(\nu) \cdot f(\nu). \]

Let us remark that for the numbers \( l_1, m, r, s \) involved in the summation of \( \sum_{s = \alpha} \) we have \( l_1 m s^2 \leq M s / n \leq n^3 \log^2 \nu \), hence the inner sum can be estimated by means of Lemma 3. Thus we get
\[ \sum_{s = \alpha} \leq B(n) \sum_{s = \alpha} \sum_{\nu < s} \chi(\nu) \cdot f(\nu) = B(n) \log^{-2} n. \]

Let us remark that for the numbers \( l_1, m, n, r, s \) involved in the summation of \( \sum_{s = \alpha} \) we have \( l_1 m s^2 \leq M s / n \leq n^3 \log^2 \nu \), hence the inner sum can be estimated by means of Lemma 3. Thus we get
\[ \sum_{s = \alpha} \leq B(n) \sum_{s = \alpha} \sum_{\nu < s} \chi(\nu) \cdot f(\nu) = B(n) \log^{-2} n. \]

Finally,
\[ \sum_{s = \alpha} \leq B(n) \log^{-2} n. \]

Putting together the results of §§ 8–9 we get
\[ \sum_{s = \alpha} \leq B(n) \log^{-2} n. \]

which completes the proof of Theorem 2.

Part III

Proof of the Main Theorem

§ 1. Estimation of \( \sum_{s = \alpha} \sum \chi(l) \). For a given positive integer \( L \) and a class \( C \in T^2 \), we set
\[ \mathcal{M}_{G,L} = \left\{ m, n : \sum_{l \in \mathcal{L}(m,n)} \chi(l) \leq L \right\} , \]
We shall prove

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

$$\sum_{m \in \mathcal{O}_L, \lim n} \sum_{l|m, \lim n} \chi(l) \leq \frac{n}{\log^{1+\log M}} \left( A \log \log n \right)^a \frac{1}{L},$$

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

In the proof we shall use the following

**Lemma.** For $a \geq 3$ we have

$$\prod_{p \in C, \lim n} (1 + Np^{-1}) \ll (\log n)^{-1/4}.$$

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

**Proof.** Let $\mathcal{A}$ be any class of $I^d/I^d_1$. By Theorem 2.4, Chapter VIII of [3], we have

$$\sum_{p \in C, \lim n} 1 \sim \frac{1}{[I^d_1/I^d]} \log x.$$

Since $C$ is a union of finite number of classes from $I^d/I^d_1$, we get

$$\sum_{p \in C, \lim n} 1 \sim \frac{1}{h_1} \log x$$

which implies the lemma.

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

$$\sum_{m \in \mathcal{O}_L, \lim n} \sum_{l|m, \lim n} \chi(l) \leq \sum_{m \in \mathcal{M}, \lim n} d(m) + \sum_{m \in \mathcal{M}, \lim n} d(m) + \sum_{m \in \mathcal{O}_L, \lim n} \sum_{l|m, \lim n} \chi(l)$$

$$= \Sigma_1 + \Sigma_2 + \Sigma_3.$$

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

$$\Sigma_1 \ll \Phi(M ; x) \sum_{m \in \mathcal{M}} d^2(m) \ll n \log^{-1} \log n,$$

$$\Sigma_2 \ll \left( \sum_{m \in \mathcal{M}} \left( \sum_{p > m} p \right) \right) \ll M^2 \log^2 M \sum_{p > M} p^{-2} \ll n^2 \log^{-1} \log n.$$

Let us set

$$\mathcal{A}'_C = \{ \mathfrak{a} \in \mathcal{L}_C ; (\mathfrak{a}, \mathfrak{d}) = 1 \}, \sum_{p \in \mathcal{O}_C, \lim n} 1 \leq L.$$

Then

$$\Sigma_3 \leq \sum_{p \in \mathcal{C}_M} \sum_{n \in \mathcal{O}_C} \left( \sum_{1 \leq n' < n} 1 \right) \leq 1 \leq A \log \log n$$

Let us set further

$$\mathcal{A}_1 = \{ \mathfrak{a}_1, \mathfrak{d} \leq \mathcal{C} \cap I^d \},$$

$$\mathcal{A}_2 = \{ \mathfrak{a}_2, \mathfrak{d} = p^2 \mathfrak{b}, \chi(p) = 1 \} \cap I^d \cap C,$$

$$\mathcal{A}_3 = \{ \mathfrak{a}_3, \mathfrak{d} = p^2 \mathfrak{b}, \chi(p) = 1, \chi(p) \cap I^d \},$$

$$\mathcal{A}_4 = \{ p_1 \cdots p_r ; r \leq L, \chi(p_i) = 1, p_i \notin I^d \}$$

for $i \neq j$.

Then

$$\Sigma_3 \ll \sum_{p \in \mathcal{C}_M} \sum_{n \in \mathcal{O}_C} \left( \sum_{p \in \mathcal{C}_M} \left( \sum_{n' < n} \mathfrak{a}_1 \mathfrak{a}_2 \mathfrak{a}_3 \mathfrak{a}_4 \right) \right) = \Sigma_1 \Sigma_2 \Sigma_3 \Sigma_4.$$

We have the obvious estimates

$$\Sigma_1 \ll \sum_{p \in \mathcal{C}_M} \left( \sum_{n \in \mathcal{O}_C} \mathfrak{a}_1 \right) \ll 1,$$

$$\Sigma_2 \ll \sum_{p \in \mathcal{C}_M} \left( \sum_{n \in \mathcal{O}_C} \mathfrak{a}_2 \right) \ll 1,$$

$$\Sigma_3 \ll \prod_{p \in \mathcal{C}_M} (1 + Np^{-1}) \ll (\log n)^{-1/4},$$

for sufficiently large constant $A > 5$. Hence

$$\Sigma_4 \ll \sum_{i \ll L} \left( \sum_{n \in \mathcal{O}_C} 1 \right) \ll \sum_{r \ll L} \left( \frac{A \log \log n}{r} \right)^r \ll \left( \frac{A}{L} \log \log n \right)^{L},$$

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

\[
\sum_{n \leq \varepsilon_1} N[F = n - p] = (\frac{L}{\log L} + O(\varepsilon_1^2)) \sum_{m \leq L} \sum_{\lambda \leq m} \chi(\lambda) + O \left( \sum_{m \leq L} \sum_{\lambda \leq m} \sum_{\mu \leq D} \sum_{\kappa} \chi(\lambda) \right).
\]

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

\[
\sum_{n \leq \varepsilon_0} - \frac{2}{\log n} \log n = \frac{1}{\log n} \log \log n + \frac{1}{\log n} \log \log n + \frac{1}{\log n} \log \log n = \frac{1}{\log n} \log \log n.
\]

On putting \( L = \frac{1}{\Delta n} \log \log n \) we get the required estimate.

References


Received on 18.12.1973 (503)