ACTA ARITHMETICA
XXI (1972)

Primes of the type $\varphi(x, y)+A$ where φ is a quadratic form

by

H. IWANIEC (Warszawa)

In memory of W. Sierpiński

§ 1. Introduction. According to the classical theorem formulated by Dirichlet and proved by E. Schering [10] and H. Weber [12] every primitive binary quadratic form (positive if definite) with the discriminant different from a perfect square represents infinitely many primes. B. M. Bredihin [2] proved in 1965 that if a form $\varphi(\xi, \eta)$ satisfies the assumptions of the quoted theorem then for every integer $A \neq 0$ there exist infinitely many primes of the type $\varphi(\xi, \eta)+A$. Then Bredihin and Linnik [3] introduced a method of deriving the asymptotic formula for the number of solutions of the equation $\varphi(\xi, \eta)+A = p$, where p runs over primes $\leqslant N$ and where, in the case of an indefinite form, one identifies solutions obtainable one from another by an automorphism of φ. The obtained asymptotic formula does not give any direct information about the number $S(\varphi, A, N)$ of the primes $p \leqslant N$ representable as $\varphi(\xi, \eta)+A$ and even does not allow one to determine the order of magnitude of $S(\varphi, A, N)$. Recently Y. Motohashi [8] investigated the simplest case $\varphi(\xi, \eta) = \xi^2+\eta^2, A = 1$ and obtained the estimation $S(\xi^2+\eta^2, 1, N) \gg N\log^{-2}N$. He put forward the conjecture

$$S(\xi^2+\eta^2, 1, N) \sim \frac{3}{2} \prod_{p\equiv -1 \,(\mathrm{mod}\, 4)} \left(1-\frac{1}{p^2}\right)^{-1/2} \left(1-\frac{1}{p(p-1)}\right) N(\log N)^{-3/2}.$$

The aim of this paper is to prove the following theorem:

THEOREM 1. *Let* $\varphi_0(\xi, \eta) = a\xi^2+b\xi\eta+c\eta^2$, $a > 0$, $(a, b, c) = 1$, *let* $D = b^2-4ac$ *be not a perfect square,* $B \geqslant 1$, $A \neq 0$, $(A, B) = 1$, R_{φ_0} *the genus of* φ_0,

$$S_1(N, \varphi_0, B, A) = \sum_{\substack{p\leqslant N \\ p=B\varphi(\xi,\eta)+A \\ (\xi,\eta)=1,\, \varphi\in R_{\varphi_0}}} 1, \quad S_\infty(N, \varphi_0, B, A) = \sum_{\substack{p\leqslant N \\ p=B\varphi(\xi,\eta)+A \\ \varphi\in R_{\varphi_0}}} 1,$$

$$S_2(N, \varphi_0, B, A) = \sum_{\substack{p\leqslant N\\ p=B\varphi_0(\xi,\eta)+A}} 1,$$

$$\theta = \sup_{1<s<4/3}\left\{\int_1^s \frac{dt}{\sqrt{t(t-1)}} - 8s^2\sqrt{\frac{2(s-1)}{s}}\log(2s-1)\right\},$$

$$\Psi_{A,B,D} = \sqrt{\frac{2}{\pi}}\prod_{p\mid 2DA}\left(1-\frac{1}{p}\right)^{-\frac{1}{2}}\prod_{\substack{p\nmid 2DBA\\ \left(\frac{k(D)}{p}\right)=-1}}\left(1-\frac{1}{(p-1)^2}\right)\prod_{p\nmid 2DA}\left(1-\frac{1}{p}\right)^{-\frac{1}{2}\left(\frac{k(D)}{p}\right)}.$$

Then the following estimations hold:

$$\text{(1.1)}\quad \theta\Psi_{A,B,D}\Omega_{A,B,D}\frac{N}{(\log N)^{3/2}}\big(1+o(1)\big)+O(N\log^{-5}N)$$
$$< S_1(N, \varphi, B, A) < 2\Psi_{A,B,D}\Omega_{A,B,D}\frac{N}{(\log N)^{3/2}}\big(1+o(1)\big)+O(N\log^{-5}N),$$

$$\text{(1.2)}\quad \frac{N}{\varphi(B)(\log N)^{3/2}}+O(N\log^{-5}N) \ll S_\infty(N, \varphi, B, A) \ll \frac{N}{\varphi(B)(\log N)^{3/2}},$$

$$\text{(1.3)}\quad \frac{N}{\varphi(B)(\log N)^{3/2}}+O(N\log^{-5}N) \ll S_2(N, \varphi, B, A) \ll \frac{N}{\varphi(B)(\log N)^{3/2}},$$

the constant $\Omega_{A,B,D}$ is defined in § 4. The constants implicit in the symbols O, $\ll$, depend only on φ and A. Also $o(1)$ is uniform with respect to B.

Theorem 1 implies an estimation for the function $S(\xi^2+\eta^2, 1, N)$ investigated by Y. Motohashi. We shall prove the following

COROLLARY.

$$\frac{\theta}{2}\prod_{p\equiv -1 (\mathrm{mod}\, 4)}\left(1-\frac{1}{p^2}\right)^{-1/2}\left(1-\frac{1}{p(p-1)}\right)\frac{N}{(\log N)^{3/2}}\big(1+o(1)\big) < S(\xi^2+\eta^2, 1, N)$$
$$< \prod_{p\equiv -1 (\mathrm{mod}\, 4)}\left(1-\frac{1}{p^2}\right)^{-1/2}\left(1-\frac{1}{p(p-1)}\right)\frac{N}{(\log N)^{3/2}}\big(1+o(1)\big).$$

The upper bound for the function $S(\xi^2+\eta^2, 1, N)$ is less than its asymptotic value conjectured by Motohashi. An analysis of his heuristic argument shows that the factor $3/2$ occurring in the asymptotic formula should be replaced by $1/\sqrt{2}$.

Apart from few examples, sequences of integers defined in a natural way and known to contain infinitely many primes, contain $c\dfrac{N}{\log N}$ primes $\leqslant N$, where c is a positive constant. In particular $S_1(N, \varphi_0, 1, 0)$ is of order $N/\log N$. Theorem 1 implies that for $A \neq 0$, $(A, B) = 1$ the order of magnitude of $S_\delta(N, \varphi_0, B, A)$ $(\delta = 1, \infty, 2)$ is $N/(\log N)^{3/2}$. The sequence of numbers $B\varphi_0(\xi, \eta)+A$ is thus a new exception to the afore-said rule.

I wish to express here my best thanks to Professor A. Schinzel for his valuable suggestions and the assistance in the preparation of this paper. I owe to him in particular an essential simplification of the proof of Theorem 4 and the indication of the method of computing the constant $\Omega_{A,B,D}$.

§ 2. Lemmas from the theory of quadratic forms.

In this section we derive necessary and sufficient conditions for the existence of a proper representation of a given positive integer n by a genus of primitive binary quadratic forms of discriminant $D \neq 0$ (n need not be prime to D). The conditions determine the residue class of $n \bmod 8D$ and the multiplicative structure of n; its prime factors are to belong with some exceptions to a certain subgroup of index 2 of the multiplicative group of residue classes prime to a suitable modulus. We have

LEMMA 2.1. *If $\varphi(\xi, \eta)$ is a primitive non-singular quadratic form positive if definite and n is a positive integer, then n is representable properly by R_φ if and only if for every prime power p^ν the congruence*

$$\text{(2.1)}\qquad n \equiv \varphi(\xi, \eta)\ (\mathrm{mod}\ p^\nu)$$

has a solution $(\xi, \eta) \not\equiv (0, 0)\ (\mathrm{mod}\ p)$ (called primitive in the sequel).

Proof. The lemma follows at once from Theorem 51 (ii) of [11] and from the Chinese Remainder Theorem.

LEMMA 2.2. *Let $f(\xi, \eta)$ be a polynomial with integer coefficients. If $f(\xi_0, \eta_0) \equiv 0\ (\mathrm{mod}\ p)$ and $\dfrac{\partial f}{\partial \xi}(\xi_0, \eta_0) \not\equiv 0\ (\mathrm{mod}\ p)$ or $\dfrac{\partial f}{\partial \eta}(\xi_0, \eta_0) \not\equiv 0$ $(\mathrm{mod}\ p)$ then for every integer $\gamma > 0$ the congruence $f(\xi, \eta) \equiv 0\ (\mathrm{mod}\ p^\gamma)$ has a solution ξ, η such that $(\xi, \eta) \equiv (\xi_0, \eta_0)\ (\mathrm{mod}\ p)$.*

Proof. See [1], p. 62.

$\left(\dfrac{a}{b}\right)$ will denote the Kronecker symbol. For fixed $a \neq 0$ the symbol $\left(\dfrac{a}{b}\right) = \chi_{f(a)}(b)$ is a quadratic character with the conductor $f(a)$, where

$$f(a) = \begin{cases} k(a) & \text{if}\quad k(a) \equiv 1\ (\mathrm{mod}\ 4),\\ 4k(a) & \text{if}\quad k(a) \not\equiv 1\ (\mathrm{mod}\ 4)\end{cases}$$

and $k(a)$ is the square-free kernel of a.

LEMMA 2.3. *If a is different from a perfect square and $\mathscr{B}$ is the multiplicative group of residue classes prime to $f(a)$ then the condition $\chi_{f(a)}(b') = 1$, $b' \in \mathscr{B}$ determines a subgroup $\mathscr{B}'$ of index 2 in $\mathscr{B}$.*

Let d^* be the largest odd factor of d. Let $\varphi(\xi, \eta) = a\xi^2+b\xi\eta+c\eta^2$, $(a, b, c) = 1$, $a > 0$, and let $D = b^2-4ac$ be different from a perfect square.

Without loss of generality we may assume that $(a, 2D) = 1$. Let

$$D = \pm 2^{\vartheta_2} p_1^{\vartheta_{p_1}} \ldots p_r^{\vartheta_{p_r}}, \qquad D_p = p^{-\vartheta_p} D,$$
$$n = 2^{\varepsilon_2} p_1^{\varepsilon_{p_1}} \ldots p_r^{\varepsilon_{p_r}} m = dm, \qquad d_p = p^{-\vartheta_p} d,$$

where $(m, 2D) = 1$, $\vartheta_{p_i} \geqslant 1$, $\varepsilon_{p_i} \geqslant 0$ *for* $1 \leqslant i \leqslant r$.

Thus

$$D_2 = \pm D^*, \qquad d_2 = d^*.$$

THEOREM 2. *A number n is represented properly by the genus of φ if and only if the conditions given in Tables 1 and 2 are satisfied.*

Remark. The conditions (1), (3), (4), (8), (9), (10), (11), (13), (14), (15), (16), (17) and (18) given in Tables 1 and 2 (see p. 207) can be written in the form of congruences. Set

$$\mathscr{L}'_p = \left\{l;\ 0 < l < p, \left(\frac{l}{p}\right) = \left(\frac{ak(d_p)}{p}\right)\right\},$$

$$\mathscr{L}''_p = \left\{l;\ 0 < l < p, \left(\frac{l}{p}\right) = \left(\frac{-ak(d_p)k(D_p)}{p}\right)\right\},$$

$$\mathscr{L}(\varepsilon_2, \vartheta_2) = \begin{cases} \{l;\ 0 < l < 4,\ l \equiv ad^* \ (\mathrm{mod}\ 4) \text{ or } l \equiv -ad^*D^* \ (\mathrm{mod}\ 4)\} \\ \qquad\qquad \text{if } \ \varepsilon_2 = 0,\ \vartheta_2 = 2, \\ \{l;\ 0 < l < 8,\ l \equiv ad^* \ (\mathrm{mod}\ 8) \text{ or } l \equiv ad^*(1-2D^*) \ (\mathrm{mod}\ 8)\} \\ \qquad\qquad \text{if } \varepsilon_2 = 0,\ \vartheta_2 = 3, \\ \{l;\ 0 < l < 4,\ l \equiv ad^* \ (\mathrm{mod}\ 4)\} \qquad \text{if } \varepsilon_2 = 0,\ \vartheta_2 = 4, \\ \{l;\ 0 < l < 8,\ l \equiv ad^* \ (\mathrm{mod}\ 8)\} \qquad \text{if } \varepsilon_2 = 0,\ \vartheta_2 \geqslant 5, \\ \{l;\ 0 < l < 8,\ l \equiv ad^* \ (\mathrm{mod}\ 8)\} \qquad \text{if } 1 \leqslant \varepsilon_2 \leqslant \vartheta_2-5,\ 2 \mid \varepsilon_2, \\ \{l;\ 0 < l < 8,\ l \equiv 5ad^* \ (\mathrm{mod}\ 8)\} \qquad \text{if } 1 \leqslant \varepsilon_2 = \vartheta_2-4,\ 2 \mid \varepsilon_2, \\ \{l;\ 0 < l < 8,\ l \equiv ad^*(1-2D^*) \ (\mathrm{mod}\ 8)\} \\ \qquad\qquad \text{if } 1 \leqslant \varepsilon_2 = \vartheta_2-3,\ 2 \mid \varepsilon_2, \\ \{l;\ 0 < l < 4,\ l \equiv -ad^*D^* \ (\mathrm{mod}\ 4)\} \quad \text{if } 1 \leqslant \varepsilon_2 = \vartheta_2-2,\ 2 \mid \varepsilon_2, \\ \{l;\ 0 < l < 8,\ l \equiv -ad^*D^* \ (\mathrm{mod}\ 8) \text{ or } l \equiv ad^*(2-D^*) (\mathrm{mod}\ 8)\} \\ \qquad\qquad \text{if } 1 \leqslant \varepsilon_2 = \vartheta_2-2,\ 2 \nmid \varepsilon_2, \\ \{l;\ 0 < l < 4,\ l \equiv -ad^* \dfrac{D^*-1}{2} \ (\mathrm{mod}\ 4) \\ \qquad\qquad \text{if } 1 \leqslant \varepsilon_2 = \vartheta_2-1,\ 2 \nmid \varepsilon_2,\ 4 \mid D^*+1, \\ \{0\} \qquad \text{otherwise (i.e. } \varepsilon_2 \geqslant \vartheta_2). \end{cases}$$

Table 1

The relations between exponents ε, ϑ		$\varkappa$	τ	The conditions on the number m	The conditions on the numbers d and D	
$\varepsilon_{p_i} < \vartheta_{p_i}$		$\frac{p_i-1}{2}$	p_i	$\left(\frac{m}{p_i}\right) = \left(\frac{ad_{p_i}}{p_i}\right)$	$2 \mid \varepsilon_{p_i}$	(1)
$\varepsilon_{p_i} = \vartheta_{p_i}$	$2 \mid \varepsilon_{p_i}$	1	1	none	$p_i > 3$ or $p_i = 3$ and $3 \mid 1+D_3$	(2)
		1	3	$m \equiv -ad_3 \ (\mathrm{mod}\ 3)$	$p_i = 3$, $D_3 \equiv 1 \ (\mathrm{mod}\ 3)$	(3)
	$2 \nmid \varepsilon_{p_i}$	$\frac{p_i-1}{2}$	p_i	$\left(\frac{m}{p_i}\right) = \left(\frac{-ad_{p_i}D_{p_i}}{p_i}\right)$	none	(4)
$\varepsilon_{p_i} > \vartheta_{p_i}$		1	1	none	$2 \mid \vartheta_{p_i}$, $\left(\frac{D_{p_i}}{p_i}\right) = 1$	(5)
$p \mid m$, $\vartheta_p = 0$		1	1	none	$\left(\frac{D}{p}\right) = 1$	(6)

Table 2

$\varepsilon_2 = 0$	$\vartheta_2 = 0$	1	1	none	$D \equiv 1 \ (\mathrm{mod}\ 4)$	(7)
	$\vartheta_2 = 2$	1 or 2	4	$m \equiv ad^* \ (\mathrm{mod}\ 4)$ or $m \equiv -ad^*D^* (\mathrm{mod}\ 4)$	$D^* \equiv -1 \ (\mathrm{mod}\ 4)$ or $D^* \equiv 1 \ (\mathrm{mod}\ 4)$	(8)
	$\vartheta_2 = 3$	2	8	$m \equiv ad^* \ (\mathrm{mod}\ 8)$ or $m \equiv ad^*(1-2D^*) \ (\mathrm{mod}\ 8)$	none	(9)
	$\vartheta_2 = 4$	1	4	$m \equiv ad^* \ (\mathrm{mod}\ 4)$	none	(10)
	$\vartheta_2 \geqslant 5$	1	8	$m \equiv ad^* \ (\mathrm{mod}\ 8)$	none	(11)
$\varepsilon_2 \geqslant 1$,	$\vartheta_2 = 0$	1	1	none	$D \equiv 1 \ (\mathrm{mod}\ 8)$	(12)
$\varepsilon_2 \geqslant 1$, $\vartheta_2 \geqslant 1$	$\varepsilon_2 \leqslant \vartheta_2 - 5$	1	8	$m \equiv ad^* \ (\mathrm{mod}\ 8)$	$2 \mid \varepsilon_2$	(13)
	$\varepsilon_2 = \vartheta_2 - 4$	1	8	$m \equiv 5ad^* \ (\mathrm{mod}\ 8)$	$2 \mid \varepsilon_2$	(14)
	$\varepsilon_2 = \vartheta_2 - 3$	1	8	$m \equiv ad^*(1-2D^*)(\mathrm{mod}\ 8)$	$2 \mid \varepsilon_2$	(15)
	$2 \mid \varepsilon_2 = \vartheta_2 - 2$	1	4	$m \equiv -ad^*D^* \ (\mathrm{mod}\ 4)$	none	(16)
	$2 \nmid \varepsilon_2 = \vartheta_2 - 2$	2	8	$m \equiv -ad^*D^* \ (\mathrm{mod}\ 8)$ or $m \equiv ad^*(2-D^*) \ (\mathrm{mod}\ 8)$	none	(17)
	$\varepsilon_2 = \vartheta_2 - 1$	1	4	$m \equiv ad^* \frac{1-D^*}{2} \ (\mathrm{mod}\ 4)$	$2 \mid \vartheta_2$, $D^* \equiv -1 \ (\mathrm{mod}\ 4)$	(18)
	$\varepsilon_2 = \vartheta_2$	1	1	none	$2 \mid \vartheta_2$, $D^* \equiv 5 \ (\mathrm{mod}\ 8)$	(19)
	$\varepsilon_2 > \vartheta_2$	1	1	none	$2 \mid \vartheta_2$, $D^* \equiv 1 \ (\mathrm{mod}\ 8)$	(20)

The sets $\mathscr{L}'_p$ and $\mathscr{L}''_p$ have each $(p-1)/2$ elements. The set $\mathscr{L}(\varepsilon_2, \vartheta_2)$ has $\varkappa$ elements and equals $\{0\}$ if and only if $\tau = 1$. The conditions (1), (3) and (4) are equivalent to the congruence

$$m \equiv l \,(\mathrm{mod}\, p_i),$$

where l belongs to $\mathscr{L}'_{p_i}$ or $\mathscr{L}''_{p_i}$, respectively. The conditions (7)–(20) are equivalent to the congruence

$$m \equiv l \,(\mathrm{mod}\, \tau),$$

where $l \in \mathscr{L}(\varepsilon_2, \vartheta_2)$.

Proof. It suffices to verify that the conditions given in Tables 1 and 2 are necessary and sufficient for the existence of primitive solutions of the congruence

$$n \equiv \varphi(\xi_0, \eta_0) \,(\mathrm{mod}\, p^\gamma) \tag{2.2}$$

for an arbitrary integer $\gamma > 0$ and an arbitrary prime p.

Let $p \nmid 2D$, $\varepsilon_p \geqslant 1$, $p^{a_p} \| a$. Congruence (2.2) is equivalent to the congruence

$$4ap^{\varepsilon_p} n_p \equiv (2a\xi + b\eta)^2 - D\eta^2 \,(\mathrm{mod}\, p^{\gamma + a_p}).$$

If $p \nmid a$ then $p \nmid \eta$ because $p \nmid (\xi, \eta)$; hence $\left(\dfrac{D}{p}\right) = 1$.

If $p | a$ then $D = b^2 - 4ac \equiv b^2 \,(\mathrm{mod}\, p)$; hence $\left(\dfrac{D}{p}\right) = 1$.

Conversely, if $\left(\dfrac{D}{p}\right) = 1$, then (2.2) has a primitive solution for an arbitrary integer $\gamma > 0$. Indeed, there exists an integer X satisfying $X^2 \equiv D \,(\mathrm{mod}\, p)$. If $p \nmid a$ then there exists ξ_1 satisfying the congruence $2a\xi_1 + b \equiv X \,(\mathrm{mod}\, p)$, hence

$$4ap^{\varepsilon_p} n_p \equiv (2a\xi_1 + b)^2 - D \,(\mathrm{mod}\, p)$$

and if $p | a$ then $D \equiv b^2 \,(\mathrm{mod}\, p)$ and the preceding congruence also holds. It follows from Lemma 2.2 that there exist integers ξ, η such that $(\xi, \eta) \equiv (\xi_1, 1) \,(\mathrm{mod}\, p)$,

$$4ap^{\varepsilon_p} n_p \equiv (2a\xi + b\eta)^2 - D\eta^2 \,(\mathrm{mod}\, p^{\gamma + a_p}),$$

thus the congruence (2.2) has a primitive solution.

Let $p | D^*$. Then $p \nmid 4a$ and the congruence (2.2) is equivalent to the congruence

$$4an \equiv (2a\xi + b\eta)^2 - D\eta^2 \,(\mathrm{mod}\, p^\gamma),$$

which on setting $n_p = p^{-\varepsilon_p} n$, $D_p = p^{-\vartheta_p} D$ takes the form

$$4ap^{\varepsilon_p} n \equiv (2a\xi + b\eta)^2 - D\eta^2 \,(\mathrm{mod}\, p^\gamma). \tag{2.3}$$

Consider the following cases:

(i) $\varepsilon_p < \vartheta_p$. Then $2 | \varepsilon_p$, $2a\xi + b\eta = p^{\frac{1}{2}\varepsilon_p} X$,

$$4an_p \equiv X^2 - p^{\vartheta_p - \varepsilon_p} D_p \eta^2 \,(\mathrm{mod}\, p^{\gamma - \varepsilon_p}),$$

hence $\left(\dfrac{4an_p}{p}\right) = 1$ or $\left(\dfrac{k(n)}{p}\right) = \left(\dfrac{a}{p}\right)$ provided $\gamma > \varepsilon_p$. Conversely, if $\left(\dfrac{k(n)}{p}\right) = \left(\dfrac{a}{p}\right)$ then the congruence (2.3) has a primitive solution for an arbitrary positive integer γ. Indeed, there exists an integer X_1 satisfying

$$X_1^2 - p^{\vartheta_p - \varepsilon_p} D_p \equiv 4an_p \,(\mathrm{mod}\, p).$$

It follows from Lemma 2.2 that there exist integers $X \equiv X_1 \,(\mathrm{mod}\, p)$, $\eta \equiv 1 \,(\mathrm{mod}\, p)$ satisfying the congruence

$$4an_p \equiv X^2 - p^{\vartheta_p - \varepsilon_p} D_p \eta^2 \,(\mathrm{mod}\, p^{\gamma - \varepsilon_p}).$$

Since $p \nmid 2a$, so $2a\xi + b\eta \equiv p^{\frac{1}{2}\varepsilon_p} X \,(\mathrm{mod}\, p^\gamma)$ for a suitable integer ξ. It hence follows that the congruence (2.3) has a primitive solution, in fact $p \nmid \eta$.

(ii) $\varepsilon_p = \vartheta_p \equiv 1 \,(\mathrm{mod}\, 2)$. Then $2a\xi + b\eta = p^{(1+\varepsilon_p)/2} X$ and

$$4an_p \equiv pX^2 - D_p \eta^2 \,(\mathrm{mod}\, p^{\gamma - \varepsilon_p}).$$

Hence $\left(\dfrac{4an_p}{p}\right) = \left(\dfrac{-D_p}{p}\right)$ or $\left(\dfrac{n_p}{p}\right) = \left(\dfrac{-aD_p}{p}\right)$ provided $\gamma > \varepsilon_p$. The condition $\left(\dfrac{n_p}{p}\right) = \left(\dfrac{-aD_p}{p}\right)$, like in the case (i), is sufficient for the existence of a primitive solution of (2.3) for an arbitrary integer γ. The proof is analogous and will be omitted. In most of the remaining cases we also prove only the necessity of the conditions. The proofs of sufficiency can easily be obtained by an adroit application of Lemma 2.2.

(iii) $\varepsilon_p = \vartheta_p \equiv 0 \,(\mathrm{mod}\, 2)$. Then $2a\xi + b\eta = p^{\frac{1}{2}\varepsilon_p} X$ and

$$4an_p \equiv X^2 - D_p \eta^2 \,(\mathrm{mod}\, p^{\gamma - \varepsilon_p}).$$

Since $p \nmid 2a$, $p | 2a\xi + b\eta$ and $p \nmid (\xi, \eta)$ we have $p \nmid \eta$. If $p = 3$ then $\eta^2 \equiv 1 \,(\mathrm{mod}\, 3)$, $X^2 \not\equiv 2 \,(\mathrm{mod}\, 3)$ and $an_p + D_p \not\equiv 2 \,(\mathrm{mod}\, 3)$ hence either $D_p \equiv -1 \,(\mathrm{mod}\, 3)$ or $n_p \equiv -a \,(\mathrm{mod}\, 3)$. We prove that for $p > 3$ the congruence (2.3) has in any case a primitive solution. It is enough to verify that the congruence

$$4an_p \equiv X^2 - D_p \eta^2 \,(\mathrm{mod}\, p)$$

has a solution X, η with $p \nmid \eta$. For $p = 5$ one can check this considering all possible systems $4an_p$ and $D_p \bmod 5$. Therefore assume that $p \geqslant 7$. It follows from Theorem 3.2.1 of [1] that the number $N(p)$ of the solutions of the congruence

$$X^2 - D_p\eta^2 - 4an_pZ^2 \equiv 0 \pmod{p}$$

satisfies the inequality $|N(p) - p^2| \leqslant (p-1)\sqrt{p}$, and that for the congruences

$$X^2 - D_p\eta^2 \equiv 0 \pmod{p}, \qquad X^2 - 4an_pZ^2 \equiv 0 \pmod{p}$$

the respective numbers of solutions satisfy $|N_i(p) - p| \leqslant p-1$ for $i = 1, 2$. $N(p) - N_1(p) - N_2(p) + 1$ is the number of these solutions of the congruence

$$X^2 - D_p\eta^2 - 4an_pZ^2 \equiv 0 \pmod{p},$$

for which $p \nmid \eta XZ$. This completes the proof since

$$N(p) - N_1(p) - N_2(p) + 1 \geqslant p^2 - \sqrt{p}(p-1) - 2(2p-1) + 1 > 0.$$

(iv) $\varepsilon_p > \vartheta_p$. Then $2 | \vartheta_p$, $2a\xi + b\eta = p^{\frac{1}{2}\vartheta_p}X$ and

$$4ap^{\varepsilon_p - \vartheta_p}n_p \equiv X^2 - D_p\eta^2 \pmod{p^{\gamma - \vartheta_p}}.$$

Since $p | 2a\xi + b\eta$, $p \nmid 2a$, $p \nmid (\xi, \eta)$ we have $p \nmid \eta$ and $\left(\dfrac{D_p}{p}\right) = 1$.

Let $p = 2$. The congruence (2.2) is equivalent to the congruence

$$2^{2+\varepsilon_2}an^* \equiv (2a\xi + b\eta)^2 - 2^{\vartheta_2}D^*\eta^2 \pmod{2^{\gamma+2}}. \tag{2.4}$$

(v) $\varepsilon_2 = 0 = \vartheta_2$. The congruence (2.4) is solvable. Indeed, if $an^* \equiv 1 \pmod{4}$ then, by Lemma 2.2, there exist integers X and η_1 such that $2 \nmid X$ and

$$\frac{an^* - 1}{4} \equiv X(X+1) - D^*\eta_1^2 \pmod{2^{\gamma-2}}.$$

Setting $\eta = 4\eta_1$, $2a\xi + b\eta = 2(2X+1)$ we have $2 \nmid \xi$ and

$$4an^* \equiv (2a\xi + b\eta)^2 - D^*\eta^2 \pmod{2^{\gamma+2}}.$$

If $an^* \equiv -1 \pmod{4}$ then $an^* + D^* \equiv 0 \pmod{4}$. By Lemma 2.2 there exist integers η_1 and X such that

$$\frac{an^* + D^*}{4} \equiv X^2 - \eta_1(\eta_1+1)D^* \pmod{2^{\gamma-2}}.$$

Setting $\eta = 2(2\eta_1 + 1)$, $4X = 2a\xi + b\eta$ we have $2 \nmid \xi$ and

$$4an^* \equiv (2a\xi + b\eta)^2 - D^*\eta^2 \pmod{2^{\gamma+2}}.$$

(vi) $\varepsilon_2 = 0$, $\vartheta_2 \geqslant 2$. Then $b = 2b_1$ and

$$an^* \equiv (a\xi + b_1\eta)^2 - 2^{\vartheta_2 - 2}D^*\eta^2 \pmod{2^\gamma}. \tag{2.4'}$$

If $\vartheta_2 = 2$ then either $2 | \eta$ and $2 \nmid a\xi + b_1\eta$ or $2 \nmid \eta$ and $2 | a\xi + b\eta$, hence either $an^* \equiv 1 \pmod{4}$ or $an^* \equiv -D \pmod{4}$.

If $\vartheta_2 = 3$ then $a\xi + b_1\eta = 2X + 1$ and

$$\frac{an^* - 1}{2} \equiv 2X(X+1) - D^*\eta^2 \pmod{2^{\gamma-1}},$$

thus either

$$\frac{an^* - 1}{2} \equiv -D\eta^2 \pmod{4}, \qquad \frac{an^* - 1}{2} \equiv -D^* \pmod{4}$$

or

$$\frac{an^* - 1}{2} \equiv 0 \pmod{4}.$$

If $\vartheta_2 = 4$ then $a\xi + b_1\eta = 2X + 1$ and

$$\frac{an^* - 1}{2} \equiv 2X(X+1) - 2D^*\eta^2 \pmod{2^{\gamma-1}},$$

hence $an^* \equiv 1 \pmod{4}$. If $\vartheta_2 \geqslant 5$ then $a\xi + b_1\eta = 2X + 1$ and

$$\frac{an^* - 1}{2} \equiv 2X(X+1) - 2^{\vartheta_2 - 3}D^*\eta^2 \pmod{2^{\gamma-1}},$$

hence $an^* \equiv 1 \pmod{8}$.

(vii) $\varepsilon_2 \geqslant 1$, $\vartheta_2 = 0$. Then

$$4a2^{\varepsilon_2}n^* \equiv (2a\xi + b\eta)^2 - D\eta^2 \pmod{2^{\gamma+2}}$$

and *a fortiori*

$$(2a\xi + b\eta)^2 \equiv D\eta^2 \pmod{8} \quad \text{and} \quad a\xi^2 + b\xi\eta + c\eta^2 \equiv 0 \pmod{2}.$$

Since $2 \nmid a(\xi, \eta)$ it hence follows $2 \nmid \eta$, thus $D \equiv 1 \pmod{8}$.

(viii) $\varepsilon_2 \geqslant 1$, $\vartheta_2 \geqslant 2$. Then $b = 2b_1$ and

$$2^{\varepsilon_2}an^* \equiv (a\xi + b_1\eta)^2 - 2^{\vartheta_2 - 2}D^*\eta^2 \pmod{2^\gamma}.$$

If $\varepsilon_2 < \vartheta_2 - 2$ then $2 | \varepsilon_2$, $a\xi + b_1\eta = 2^{\frac{1}{2}\varepsilon_2}X$, $2 \nmid \eta$, $2 \nmid X$ and

$$an^* \equiv X^2 - 2^{\vartheta_2 - \varepsilon_2 - 2}D^*\eta^2 \pmod{2^{\gamma - \varepsilon_2}}.$$

Consider three cases:

(a) $\varepsilon_2 \leqslant \vartheta_2 - 5$. Then $an^* \equiv X^2 \equiv 1 \pmod{8}$.

(b) $\varepsilon_2 = \vartheta_2 - 4$. Then $an^* \equiv X^2 \equiv 1 \pmod{4}$.

(c) $\varepsilon_2 = \vartheta_2 - 3$. Then $an^* \equiv X^2 - 2D^* \equiv 1 - 2D^* \pmod{8}$.

If $\varepsilon_2 = \vartheta_2 - 2 \equiv 0 \pmod{2}$ then $a\xi + b_1\eta = 2^{\frac{1}{2}\varepsilon_2}X$, $2 \nmid \eta$ and

$$an^* \equiv X^2 - D^*\eta^2 \pmod{2^{\gamma - \varepsilon_2}}.$$

Hence $2 | X$ and $an^* \equiv -D^* \pmod{4}$.

If $\varepsilon_2 = \vartheta_2 - 2 \equiv 1 \pmod 2$ then $a\xi + b_1\eta = 2^{\frac{1+\varepsilon_2}{2}} X$, $2\nmid\eta$ and

$$an^* \equiv 2X^2 - D^*\eta^2 \pmod{2^{\gamma-\varepsilon_2}}.$$

Hence either $an^* \equiv -D^* \pmod 8$ or $an^* \equiv 2 - D^* \pmod 8$.

If $\varepsilon_2 \geqslant \vartheta_2 - 1$ then $2\nmid\eta$ and $2|\vartheta_2$. Indeed, $2|\eta$ implies, in view of $2\nmid(\xi, \eta)$, that $2\nmid\xi$, $2\nmid a\xi + b_1\eta$ and

$$2^{\varepsilon_2} an^* \equiv (a\xi + b_1\eta)^2 \equiv 1 \pmod 2,$$

what is incompatible with the assumption $\varepsilon_2 \geqslant 1$. If, on the other hand, $2\nmid\vartheta_2$ then

$$(a\xi + b_1\eta) = 2^{\frac{\vartheta_2-1}{2}} X \quad \text{and} \quad 2an^* \equiv 2X^2 - D^*\eta^2 \equiv 1 \pmod 2,$$

which is impossible.

Thus we have $2|\vartheta_2$, $a\xi + b_1\eta = 2^{\frac{\vartheta_2-2}{2}} X$, $2\nmid X$ and

$$2^{\varepsilon_2-\vartheta_2+2} an^* \equiv X^2 - D^*\eta^2 \pmod{2^{\gamma-\varepsilon_2+1}},$$

hence *a fortiori*

$$2^{\varepsilon_2-\vartheta_2+2} an^* \equiv 1 - D^* \pmod 8.$$

The last congruence for $\varepsilon_2 = \vartheta_2 - 1$ gives $an^* \equiv \dfrac{1-D^*}{2} \pmod 4$ and $D^* \equiv -1 \pmod 4$, for $\varepsilon_2 = \vartheta_2$ we have $D^* \equiv 5 \pmod 8$ and for $\varepsilon_2 > \vartheta_2$ we get $D^* \equiv 1 \pmod 8$.

Set

$$Q = \prod_{p|D^*} \tau(\varepsilon_p, \vartheta_p)\tau(\varepsilon_2, \vartheta_2) \quad \text{and} \quad P = \left\{p;\ \left(\frac{k(D)}{p}\right) = 1\right\}.$$

In virtue of the last remark and of the Chinese Remainder Theorem we can formulate the following theorem.

THEOREM 3. *The number $n = dm$ is representable properly by the genus R_φ if and only if d satisfies the conditions given in Tables 2 and 1, all the primes factors of m belong to P and*

$$m \equiv L \pmod Q,$$

where L is any positive integer satisfying the four conditions

$$(2.5)\qquad \begin{cases} 0 < L < Q, \\ L \equiv l \pmod\tau \text{ for some } l \in \mathscr{L}(\varepsilon_2, \vartheta_2), \\ \text{for each } p_i|Q^* \text{ such that } \varepsilon_{p_i} < \vartheta_{p_i} \text{ there exists } l \in \mathscr{L}'_{p_i} \text{ such that} \\ \qquad\qquad L \equiv l \pmod{p_i}, \\ \text{for each } p_i|Q^* \text{ such that } \varepsilon_{p_i} = \vartheta_{p_i} \text{ there exists } l \in \mathscr{L}''_{p_i} \text{ such that} \\ \qquad\qquad L \equiv l \pmod{p_i}. \end{cases}$$

The numbers L are prime to Q. The set $\mathscr{L}$ of the numbers L satisfying the conditions (2.5) has $\prod\limits_p \varkappa(\varepsilon_p, \vartheta_p)$ elements.

LEMMA 2.4. *For each $L \in \mathscr{L}$ the following conditions hold:*

$$(2.6)\qquad k(D)|Q,$$

$$(2.7)\qquad \big(L, k(D)\big) = 1,$$

$$(2.8)\qquad 2|L \Rightarrow k(D) \equiv 1 \pmod 4.$$

Proof. Clearly $Q = \tau(\varepsilon_2, \vartheta_2) \prod\limits_{\substack{p_i \\ 2\nmid\varepsilon_{p_i} < \vartheta_{p_i}}} p_i \prod\limits_{\substack{p_i \\ 2\nmid\varepsilon_{p_i} = \vartheta_{p_i}}} p_i \prod\limits_{\substack{2|\varepsilon_3 = \vartheta_3 \\ D_3 \equiv 1 \pmod 3}} 3$, thus $k(D^*)|Q$. Since $2|k(D) \Rightarrow 2\nmid\vartheta_2 \Rightarrow \mathscr{L}(\varepsilon_2, \vartheta_2) \neq \{0\} \Rightarrow \tau > 1 \Rightarrow 2|Q$, (2.6) is proved. (2.7) follows from (2.6). Since $2|L \Rightarrow 2\nmid Q \Rightarrow \tau(\varepsilon_2, \vartheta_2) = 1 \Rightarrow \mathscr{L}(\varepsilon_2, \vartheta_2) = \{0\}$ $\Rightarrow k(D) = k(D^*) \equiv D^* \equiv 1 \pmod 4$, the proof of Lemma 2.4 is complete.

THEOREM 4. *For each number $L \in \mathscr{L}$ the symbol $\left(\dfrac{k(D)}{L}\right)$ is defined and*

$$(2.9)\qquad \left(\frac{k(D)}{L}\right) = 1.$$

Proof. The first part of the assertion follows from (2.8). In order to prove (2.9) consider the number $d(L+Q+LQ)$, where L satisfies (2.5).

In virtue of Theorems 2 and 3 for every prime p and every positive integer γ the congruence

$$\varphi(x, y) \equiv d(L+Q+LQ) \pmod{p^\gamma}$$

has a primitive solution (x, y). Hence by the Chinese Remainder Theorem there exist integers ξ_0, η_0 such that $(\xi_0, \eta_0, Q) = 1$ and

$$0 < M = \varphi(\xi_0, \eta_0) \equiv d(L+Q+LQ) \pmod{2dQ}.$$

We have $M = dm$, where $m \equiv L \pmod Q$, $m \equiv 1 \pmod 2$ and $\left(\dfrac{k(D)}{m}\right) = 1$. Thus $\left(\dfrac{k(D)}{L}\right) = \left(\dfrac{k(D)}{m}\right) = 1$, since the conductor of the character $\left(\dfrac{k(D)}{a}\right)$ divides Q.

Theorem 4 plays the principal rôle in deriving the lower estimates for $S_\delta(N, \varphi_0, B, A)$ $(\delta = 1, \infty, 2)$. It implies the following

COROLLARY. *If $m \equiv L \big(\mathrm{mod}\ k(D)\big)$, $L \in \mathscr{L}$, then the number of prime factors of m not belonging to P is even. In particular, if $m \equiv L \pmod Q$, m cannot have exactly one prime factor off P.*

Let $L \in \mathscr{L}$, $(BdL+A, QBd) = 1$, $\mathscr{C} = \{p;\ |A| < p \leqslant N,\ p \equiv BdL+ +A \pmod{QBd}\}$, $\mathscr{M}' = \left\{m';\ m' = \dfrac{p-A}{Bd},\ p \in \mathscr{C}\right\}$ and $\mathscr{M} = \{m;\ m \in \mathscr{M}',\ (m, 2D) = 1\}$.

If $m' \in \mathscr{M}'$ and $m \in \mathscr{M}$ then

$$m' \equiv L \equiv m \pmod{Q}, \tag{2.10}$$

$$(m', QA) = 1, \tag{2.11}$$

$$(m, 2DA) = 1. \tag{2.12}$$

Let D_1 be the greatest divisor of $2D$ prime to QA. Then the set $\mathscr{M}$ can be written as $\mathscr{M} = \{m;\ m \in \mathscr{M}',\ (m, D_1) = 1\}$. Let $(\sigma, QA) = 1$, $\mathscr{M}'_\sigma = \{m';\ m' \in \mathscr{M}',\ \sigma | m'\}$ and $\mathscr{M}_\sigma = \{m;\ m \in \mathscr{M},\ \sigma | m\}$. There exists an integer σ_0 such that $\sigma_0 Q + L \equiv 0 \pmod{\sigma}$ and

$$\mathscr{M}'_\sigma = \left\{m;\ m = \frac{p-A}{Bd},\ p \equiv A + BdL + QBd\sigma_0 \pmod{QBd\sigma},\ |A| < p \leqslant N\right\}.$$

It can easily be verified that

$$(A+BdL+QBd\sigma_0, QBd\sigma) = 1. \tag{2.13}$$

Let $(\varrho, 2DA) = 1$ and $\varrho_1 | D_1$. Thus $(\varrho, \varrho_1) = 1$, $(\varrho\varrho_1, QA) = 1$ and

$$|\mathscr{M}_\varrho| = \sum_{\varrho_1 | D_1} |\mathscr{M}'_{\varrho\varrho_1}| \mu(\varrho_1). \tag{2.14}$$

Since

$|\mathscr{M}'_\sigma| = \pi(N, QBd\sigma, A+BdL+QBd\sigma_0) - \pi(|A|, QBd\sigma, A+BdL+QBd\sigma_0)$,

we get from (2.13)

$$\left| |\mathscr{M}'_\sigma| - \frac{\operatorname{Li} N}{\varphi(QBd\sigma)} \right| \leqslant \max_{\substack{l \\ (l, QBd\sigma)=1}} \left| \pi(N, QBd\sigma, l) - \frac{\operatorname{Li} N}{\varphi(QBd\sigma)} \right| + |A|.$$

Comparing the last inequality with the formula (2.14) where $(\varrho, 2DA) = 1$ we obtain

$$\begin{aligned} \left| |\mathscr{M}_\varrho| - \operatorname{Li} N \sum_{\varrho_1 | D_1} \frac{\mu(\varrho_1)}{\varphi(QBd\varrho\varrho_1)} \right| \\ \leqslant 2|D| \max_{\substack{l, x \\ |\varrho| \leqslant x \leqslant |2D\varrho| \\ (l, QBdx)=1}} \left| \pi(N, QBdx, l) - \frac{\operatorname{Li} N}{\varphi(QBdx)} \right| + 2|DA|. \end{aligned} \tag{2.15}$$

The function $\varphi_E(n)$ is multiplicative (see § 3), thus

$$\sum_{\varrho_1 | D_1} \frac{1}{\varphi(QBd\varrho\varrho_1)} = \prod_{p | D_1} \left(1 - \frac{1}{p}\right) \prod_{\substack{p | D_1 \\ p \nmid Bd}} \left(1 - \frac{1}{(p-1)^2}\right) \frac{1}{\varphi(QBd)\varphi_{QBd}(\varrho)}. \tag{2.16}$$

Theorem 3 gives

$$\begin{aligned} \sum_{\substack{|A| < B\varphi(\xi,\eta)+A = p \leqslant N \\ (\xi,\eta)=1, \varphi \in R_{\varphi_0}}} 1 &= \sum_d \sum_{L \in \mathscr{L}} \sum_{\substack{N \geqslant p \equiv BdL+A \pmod{QBd} \\ q \left| \frac{p-A}{Bd} \right. \Rightarrow q \in P \\ \left(\frac{p-A}{Bd}, 2D\right) = 1, p > |A|}} 1 \\ &= \sum_{\substack{d \\ 2 | ABd}} \sum_{\substack{L \in \mathscr{L} \\ (BdL+A, QBd)=1}} \sum_{\substack{m \in \mathscr{M} \\ q | m \Rightarrow q \in P}} 1 + \sum{}'. \end{aligned} \tag{2.17}$$

The summation in (2.17) runs over all positive integers satisfying the conditions given in Tables 1 and 2. For $\sum'$ we have an obvious estimation $0 \leqslant \sum' \leqslant 2|D|$.

It follows from the theorem of Bombieri on primes in arithmetical progressions that elements of the set $\mathscr{M}$ are well distributed in such progressions. For sets with this property the last sum in formula (2.17) can be estimated by the sieve method provided primes belonging to P are well distributed in the sense that

$$\sum_{\substack{p \leqslant x \\ p \in P}} \frac{\log p}{p} = h \log x + O(1). \tag{2.18}$$

In the considered case (2.18) follows from Lemma 2.3 and from Theorem 3.2.1 of [5] for $h = 1/2$.

§ 3. A $\frac{1}{2}$-dimensional sieve. This section is written with the purpose of applying the results to the proof of Theorem 1, hence it is concerned with a special case of a $\frac{1}{2}$-dimensional sieve, but small changes in the proofs of the lemmas can lead to general results.

We shall use the following notation independent of that used in the remainder of the paper.

$\mathscr{P}$ is a set of primes, E is a positive integer,

$$R(z) = \prod_{\substack{p < z \\ p \in \mathscr{P}}} \left(1 - \frac{1}{\varphi_E(p)}\right) \text{ where } \varphi_E(n) = \varphi(n) \prod_{p | (E, n)} \left(1 + \frac{1}{p-1}\right) = \frac{\varphi(En)}{\varphi(E)},$$

M is a finite set of positive integers,

$M_d = \{m \in M;\ m \equiv 0 \pmod{d}\}$,

$|M_d|$ is the number of elements of M_d,

$R_d(M) = |M_d| - \dfrac{Y}{\varphi(dE)}$,

$A(M; z) = \left|\left\{m \in M;\ \bigwedge\limits_{\substack{p < z \\ p \in \mathscr{P}}} m \not\equiv 0 \pmod{p}\right\}\right|.$

Let $y > 1$. If the range of primes $p_1, p_2, \ldots, p_i$ is clear from the context we shall use the notation $y_i = \dfrac{y}{p_1 p_2 \ldots p_i}$.

Lemma 3.1. *Let $r \geqslant 1$. For $s \geqslant 2$ and $s \geqslant 1$ we have the estimations*

$$A(M; y^{1/s}) \leqslant Y\Bigg\{\frac{1}{\varphi(E)} - \sum_{p_1 < y^{1/s}} \frac{1}{\varphi(p_1 E)} + \sum_{p_2 < p_1 < y^{1/s}} \frac{1}{\varphi(p_1 p_2 E)} - \ldots + \\ + \sum_{\substack{p_{2r} < \ldots < p_1 < y^{1/s} \\ p_{2i+1} < \sqrt{y_{2i}} \\ i=1,\ldots,r-1}} \frac{1}{\varphi(p_1 \ldots p_{2r} E)}\Bigg\} + \sum_{\substack{d<y \\ p \mid d \Rightarrow p \in \mathscr{P}}} |R_d(M)| \\ = \frac{Y}{\varphi(E)} G_{r,y}(s) + \sum_{\substack{d<y \\ p \mid d \Rightarrow p \in \mathscr{P}}} |R_d(M)|$$

and

$$A(M; y^{1/s}) \geqslant Y\Bigg\{\frac{1}{\varphi(E)} - \sum_{p_1 < y^{1/s}} \frac{1}{\varphi(p_1 E)} + \sum_{\substack{p_2 < p_1 < y^{1/s} \\ p_2 < \sqrt{y_1}}} \frac{1}{\varphi(p_1 p_2 E)} - \ldots - \\ - \sum_{\substack{p_{2r-1} < \ldots < p_1 < y^{1/s} \\ p_{2i} < \sqrt{y_{2i-1}} \\ i=1,\ldots,r-1}} \frac{1}{\varphi(p_1 \ldots p_{2r-1} E)}\Bigg\} - \sum_{\substack{d<y \\ p \mid d \Rightarrow p \in \mathscr{P}}} |R_d(M)| \\ = \frac{Y}{\varphi(E)} D_{r,y}(s) - \sum_{\substack{d<y \\ p \mid d \Rightarrow p \in \mathscr{P}}} |R_d(M)|,$$

respectively, where $p_1, \ldots, p_{2r} \in \mathscr{P}$.

Let us define the following functions:

$$d_{2,y}(s) = \sum_{\sqrt{y_1} \leqslant p_2 < p_1 < y^{1/s}} \frac{R(p_2)}{\varphi_E(p_1 p_2)} \quad (s \geqslant 1),$$

$$d_{2n+2,y}(s) = \sum_{\substack{\sqrt{y_{2n+1}} \leqslant p_{2n+2} < \ldots < y^{1/s} \\ p_{2i} < \sqrt{y_{2i-1}},\ i=1,\ldots,n}} \frac{R(p_{2n+2})}{\varphi_E(p_1 \ldots p_{2n+2})},$$

$$d_{2n+1,y}(s) = \sum_{\substack{\sqrt{y_{2n}} \leqslant p_{2n+1} < \ldots < p_1 < y^{1/s} \\ p_{2i+1} < \sqrt{y_{2i}}, i=1,\ldots,n-1}} \frac{R(p_{2n+1})}{\varphi_E(p_1 \ldots p_{2n+1})} \quad (s \geqslant 2),$$

$$d_{2n+1,y}(s) = d_{2n+1,y}(2) \quad (1 \leqslant s \leqslant 2),$$

where $p_1, \ldots, p_{2n+2} \in \mathscr{P}$ and

$$Q_{2r+1,y}(s) = \sum_{k=1}^{r} d_{2k+1,y}(s), \quad Q_{2r,y}(s) = \sum_{k=1}^{r} d_{2k,y}(s).$$

Lemma 3.2. *We have the following identities*

$$G_{r,y}(s) = R(y^{1/s}) + Q_{2r+1,y}(s) + \sum_{\substack{p_{2r+1} < \ldots < p_1 < y^{1/s} \\ p_{2i+1} < \sqrt{y_{2i}}, i=1,\ldots,r}} \frac{R(p_{2r+1})}{\varphi_E(p_1 \ldots p_{2r+1})} \quad (s \geqslant 2),$$

$$D_{r,y}(s) = R(y^{1/s}) - Q_{2r,y}(s) - \sum_{\substack{p_{2r} < \ldots < p_1 < y^{1/s} \\ p_{2i} < \sqrt{y_{2i-1}}, i=1,\ldots,r}} \frac{R(p_{2r})}{\varphi_E(p_1 \ldots p_{2r})} \quad (s \geqslant 1),$$

where $p_1, \ldots, p_{2r+1} \in \mathscr{P}$.

Lemma 3.3. *The functions $Q_{i+1,y}(s)$ can be expressed in terms of $Q_{i,y}(s)$ by the following formulae*

$$Q_{2n+1,y}(s) = \sum_{\substack{y^{1/(2n+2)} \leqslant p < y^{1/s} \\ p \in \mathscr{P}}} \frac{Q_{2n,y/p}\left(\dfrac{\log y}{\log p} - 1\right)}{\varphi_E(p)} \quad (s \geqslant 2),$$

$$Q_{2n+2,y}(s) = \sum_{\substack{y^{1/(2n+2)} \leqslant p < y^{1/s} \\ p \in \mathscr{P}}} \frac{Q_{2n+1,y/p}\left(\dfrac{\log y}{\log p} - 1\right)}{\varphi_E(p)} + d_{2,y}(s) \quad (s \geqslant 1).$$

The proofs of these lemmas are analogous to the proofs of the corresponding lemmas in [6].

Let $w(s)$ be the continuous function satisfying the following differential equation with shifted argument:

$$w(s) = \frac{1}{\sqrt{s}} \qquad (0 < s \leqslant 1),$$

$$s w'(s) = \tfrac{1}{2}\{w(s-1) - w(s)\} \qquad (s > 1).$$

For $s > 1$ we have

$$s w'(s) = -\tfrac{1}{2} \int_{s-1}^{s} w'(x)\, dx,$$

thus

$$w'(s) = O\left(\frac{1}{\sqrt{s}\, e^s}\right) \quad \text{and} \quad w(s) = w(\infty) + O\left(\frac{1}{\sqrt{s}\, e^s}\right).$$

From Lemma 1.3.2 of [4] we get $w(\infty) = \sqrt{\pi}e^{-\gamma/2}$. Set

$$W(s) = \sqrt{s}\left(1-\sqrt{\frac{e^{\gamma}}{\pi}}\, w(s)\right) = O(e^{-s}).$$

Hence

$$W(s) = \sqrt{s}-\sqrt{\frac{e^{\gamma}}{\pi}} \qquad \text{for} \quad 0 < s \leqslant 1,$$

$$W'(s) = \frac{1}{2}\,\frac{W(s-1)}{\sqrt{s(s-1)}} \qquad \text{for} \quad s > 1,$$

$$W(s) = \sqrt{s}-\sqrt{\frac{e^{\gamma}}{\pi}}\left(1+\frac{1}{2}\int_{1}^{s}\frac{dt}{\sqrt{t(t-1)}}\right) \qquad \text{for} \quad 1 \leqslant s \leqslant 2.$$

Let $M(s)$ be the continuous function satisfying the following differential equation with shifted argument:

$$M(s) = \sqrt{\frac{e^{\gamma}}{\pi}}\left(1-\frac{1}{2}\int_{1}^{s}\frac{dt}{\sqrt{t(t-1)}}\right) \qquad \text{for} \quad 1 \leqslant s \leqslant 2,$$

$$M'(s) = -\frac{1}{2}\cdot\frac{M(s-1)}{\sqrt{s(s-1)}} \qquad \text{for} \quad s > 2.$$

For $s > 2$ we have

$$(\sqrt{s}M(s))' = \frac{1}{2}\left(\frac{M(s)}{\sqrt{s}} - \frac{M(s-1)}{\sqrt{s-1}}\right),$$

thus

$$\sqrt{s}M(s) = \frac{1}{2}\int_{s-1}^{s}\frac{M(x)}{\sqrt{x}}\,dx+C, \qquad C = \text{constant}.$$

Setting $s=2$ we infer from the continuity of $M(s)$ that $C = 0$, hence $0 < M(s) = O(e^{-s})$. We introduce the functions:

$$f(s) = \frac{M(s)+W(s)}{2} \quad \text{for} \quad s \geqslant 1, \qquad F(s) = \frac{M(s)-W(s)}{2} \quad \text{for} \quad s \geqslant 2,$$

$$F(s) = F(2) = \sqrt{\frac{e^{\gamma}}{\pi}}-\frac{\sqrt{2}}{2} \qquad \text{for} \quad 0 \leqslant s \leqslant 2.$$

It is easy to show that

$$f(s) = \frac{1}{2}\sqrt{s}-\frac{1}{2}\sqrt{\frac{e^{\gamma}}{\pi}}\int_{1}^{s}\frac{dt}{\sqrt{t(t-1)}} \tag{3.1}$$

for $1 \leqslant s \leqslant 3$. It follows from the definition of $M(s)$, $W(s)$ and $F(s)$ that for $s > 2$

$$F'(s) = \frac{M'(s)-W'(s)}{2} = -\frac{1}{2}\,\frac{M(s-1)+W(s-1)}{2\sqrt{s(s-1)}}$$

$$= -\frac{f(s-1)}{2\sqrt{s(s-1)}} = O(e^{-s}),$$

thus

$$F(s) = \frac{1}{2}\int_{s}^{\infty}\frac{f(t-1)}{\sqrt{t(t-1)}}\,dt. \tag{3.2}$$

Similarly

$$f(s) = \frac{1}{2}\int_{s}^{\infty}\frac{F(t-1)}{\sqrt{t(t-1)}}\,dt \qquad \text{for} \quad s \geqslant 3.$$

If $1 \leqslant s \leqslant 3$, we get from (3.1)

$$f(s)=f(3)+f(s)-f(3) = \frac{1}{2}\int_{3}^{\infty}\frac{F(t-1)}{\sqrt{t(t-1)}}\,dt+\frac{\sqrt{s}-\sqrt{3}}{2}+\sqrt{\frac{e^{\gamma}}{\pi}}\int_{s}^{3}\frac{dt}{\sqrt{t(t-1)}}$$

$$= \frac{1}{2}\int_{s}^{\infty}\frac{F(t-1)}{\sqrt{t(t-1)}}\,dt+\frac{1}{4}\int_{s}^{3}\frac{\sqrt{2}-\sqrt{t-1}}{\sqrt{t(t-1)}}\,dt.$$

Setting

$$g_2(s) = \begin{cases} \displaystyle\int_{s}^{3}\frac{\sqrt{2}-\sqrt{t-1}}{\sqrt{t(t-1)}}\,dt & \text{for} \quad 1 \leqslant s \leqslant 3, \\ 0 & \text{for} \quad s \geqslant 3, \end{cases}$$

$$g_3(s) = \int_{s}^{\infty}\frac{g_2(t-1)}{\sqrt{t(t-1)}}\,dt \qquad \text{for} \quad s \geqslant 2$$

we can write $f(s)$ in the form

$$f(s) = \frac{1}{4}g_2(s)+\frac{1}{2}\int_{s}^{\infty}\frac{F(t-1)}{\sqrt{t(t-1)}}\,dt \qquad \text{for} \quad s \geqslant 1. \tag{3.3}$$

LEMMA 3.4. *For $s \geqslant 1$ the following inequality holds*

$$\int_{s}^{\infty}\frac{e^{-\max(t-2,1)}}{t\left(1-\frac{1}{t}\right)^{0.6}}\,dt \leqslant 4(s+1)\left(1-\frac{1}{s+1}\right)^{0.6}e^{-s}.$$

Proof of this lemma is elementary but tedious. One has to decompose the integral into two parts and estimate them separately, the ranges of integration being $\langle s, 3\rangle$ and $\langle 3, \infty\rangle$.

All the constants $1 < C_0+1 < C_1 < C_2 < \ldots$ depend only on the set $\mathscr{P}$. C_i does not depend on C_j for $1 \leqslant i < j$.

The condition

$$(*)\qquad \Bigg|\sum_{\substack{p\leqslant x\\ p\in\mathscr{P}}}\frac{\log p}{\varphi_E(p)}-\frac{1}{2}\log x\Bigg| < C_1 \quad \text{for} \quad x \geqslant 1$$

characterizes a $\frac{1}{2}$-dimensional sieve. We shall assume till the end of the present section that this condition is fulfilled.

Lemma 3.5. *For $z \geqslant 1$ and for a suitable constant C_0 we have*

$$\left|R(z)-\frac{C_0}{\sqrt{\log 3z}}\right| < \frac{C_2}{\log 3z}.$$

Lemma 3.6. *If $b(x)$ is a non-negative function, monotonous in an interval $B \leqslant x \leqslant A$, $B \geqslant 1$, we have*

$$\Bigg|\sum_{\substack{B\leqslant p\leqslant A\\ p\in\mathscr{P}}}\frac{b(p)}{\varphi_E(p)}-\frac{1}{2}\int\limits_B^A\frac{b(x)}{x\log x}\,dx\Bigg| \leqslant C_3\,\frac{b(A)+b(B)}{\log 3B}.$$

Corollary 1. *For $\beta \geqslant a \geqslant \dfrac{3-(-1)^{\vartheta}}{2}$ we have*

$$\Bigg|\sum_{\substack{y^{1/\beta}\leqslant p\leqslant y^{1/a}\\ p\in\mathscr{P}}}\frac{H_{\vartheta}\left(\dfrac{\log y}{\log p}-1\right)}{\varphi_E(p)\sqrt{\log 3\dfrac{y}{p}}}-\frac{1}{2\sqrt{\log 3y}}\int\limits_a^{\beta}\frac{H_{\vartheta}(t-1)}{\sqrt{t(t-1)}}\,dt\Bigg| < C_4\frac{\beta e^{-(a-1)}}{\log 3y},$$

where

$$H_{\vartheta}(s) = \begin{cases} f(s) & \textit{for} \quad \vartheta \equiv 0 \pmod 2,\\ F(s) & \textit{for} \quad \vartheta \equiv 1 \pmod 2.\end{cases}$$

Corollary 2. *For $\beta \geqslant a \geqslant 1$ we have*

$$\Bigg|\sum_{\substack{y^{1/\beta}\leqslant p\leqslant y^{1/a}\\ p\in\mathscr{P}}}\frac{\left(\dfrac{\log y}{\log p}-1\right)^{0.6}\left(\dfrac{\log y}{\log p}\right)^{0.4}e^{-\left(\frac{\log y}{\log p}-1\right)}}{\varphi_E(p)\left(\log 3\dfrac{y}{p}\right)^{0.6}}-\frac{1}{2(\log 3y)^{0.6}}\int\limits_a^{\beta}e^{-(t-1)}\,dt\Bigg| \leqslant C_5\frac{\beta e^{-(a-1)}}{\log 3y}.$$

Corollary 3. *For $\beta \geqslant a \geqslant 1$ we have*

$$\Bigg|\sum_{\substack{y^{1/\beta}\leqslant p\leqslant y^{1/a}\\ p\in\mathscr{P}}}\frac{e^{-\max\left(\frac{\log y}{\log p}-2,1\right)}}{\varphi_E(p)\left(\log 3\dfrac{y}{p}\right)^{0.6}}-\frac{1}{2(\log 3y)^{0.6}}\int\limits_a^{\beta}\frac{e^{-\max(t-2,1)}}{t\left(1-\dfrac{1}{t}\right)^{0.6}}\,dt\Bigg| < C_6\frac{\beta e^{-(a-1)}}{\log 3y}.$$

Corollary 4. *For $\beta \geqslant a \geqslant 1$ we have*

$$\Bigg|\sum_{\substack{y^{1/\beta}\leqslant p\leqslant y^{1/a}\\ p\in\mathscr{P}}}\frac{1}{\varphi_E(p)\sqrt{\log 3\dfrac{y}{p}}}-\frac{1}{2\sqrt{\log 3y}}\int\limits_a^{\beta}\frac{dt}{\sqrt{t(t-1)}}\Bigg| \leqslant C_7\frac{\beta}{\log 3y}.$$

Lemma 3.7. *For $a \geqslant b \geqslant 1$ we have*

$$\Bigg|\sum_{\substack{b\leqslant p\leqslant a\\ p\in\mathscr{P}}}\frac{1}{\varphi_E(p)\sqrt{\log p}}-\frac{1}{\sqrt{\log 3b}}+\frac{1}{\sqrt{\log 3a}}\Bigg| \leqslant C_8\frac{1}{\log 3b}.$$

Corollary.

$$\left|d_{2,y}(s)-\frac{C_0 g_2(s)}{2\sqrt{\log 3y}}\right| \leqslant \frac{C_9}{\log 3y} \quad \textit{for} \quad s \geqslant 1,$$

$$\left|d_{3,y}(s)-\frac{C_0 g_3(s)}{4\sqrt{\log 3y}}\right| \leqslant \frac{C_9}{\log 3y} \quad \textit{for} \quad s \geqslant 2.$$

The proofs of the above lemmas and corollaries are analogous to the proofs of the corresponding lemmas and corollaries in [6].

Theorem 5. *For $y \geqslant 1$ we have*

$$(3.4)\qquad \frac{1}{2C_0}Q_{2n,y}(s) < \frac{f(s)}{\sqrt{\log 3y}}+C_{10}\frac{(s+1)^{0.4}s^{0.6}e^{-s}2n}{(\log 3y)^{0.6}(2n+1)} \quad \textit{for} \quad s \geqslant 1,$$

$$(3.5)\qquad \frac{1}{2C_0}Q_{2n+1,y}(s) < \frac{F(s)}{\sqrt{\log 3y}}+C_{10}\frac{e^{-\max(s-1,1)}(2n+1)}{2(\log 3y)^{0.6}(2n+2)} \quad \textit{for} \quad s \geqslant 0.$$

Proof. There exists a constant C_{10} satisfying the conditions

(α) $C_{10} > \dfrac{2e^3 C_9}{C_0}$,

(β) $y > 1$ and $2m+2 > \dfrac{\sqrt[10]{\log 3y}}{\sqrt[4]{2C_5}} \Rightarrow \dfrac{1}{2C_0}\left(\dfrac{10\log\log 10y}{2m+1}\right)^{2m+1}$

$$< \frac{C_{10}}{2}\left(\frac{2m+1}{2m+2}-\frac{2m-1}{2m}\right)\frac{e^{-2m+1}}{(\log 3y)^{0.6}},$$

$$(\gamma)\ y>1 \ \text{and}\ \frac{2e^3(2m+3)C_9}{\log 3y} > \left(\frac{2m+2}{2m+3}-\frac{2m+1}{2m+2}\right)(\log 3y)^{-0.6}$$

$$\Rightarrow \frac{1}{2C_0}\left(\frac{10\log\log 10y}{2m+2}\right)^{2m+2} < C_{10}\left(\frac{2m+2}{2m+3}-\frac{2m}{2m+1}\right)\frac{e^{-(2m+3)}}{(\log 3y)^{0.6}}.$$

By the Corollary to Lemma 3.7 we obtain

$$\frac{1}{2C_0}Q_{2,y}(s) < \frac{g_2(s)}{4\sqrt{\log 3y}} + \frac{C_9}{2C_0\log 3y} < \frac{f(s)}{\sqrt{\log 3y}} + \frac{C_{10}e^{-s}}{4\log 3y},$$

$$\frac{1}{2C_0}Q_{3,y}(s) < \frac{g_3(s)}{8\sqrt{\log 3y}} + \frac{C_9}{2C_0\log 3y} < \frac{F(s)}{\sqrt{\log 3y}} + \frac{C_{10}e^{-\max(s-1,1)}}{4\log 3y}.$$

Thus the inequalites (3.4) and (3.5) are true for $n = 1$. Assume that (3.4) is true for $n = m$ and (3.5) for $n = m-1$. We shall show that (3.4) is true for $n = m+1$ and (3.5) for $n = m$.

If $s > 2m+2$ then $d_{2m+1,y}(s) = 0$ and $Q_{2m+1,y}(s) = Q_{2m-1,y}(s)$. Let $s \leqslant 2m+2$. If $2m+2 > \dfrac{\sqrt[10]{\log 3y}}{\sqrt[4]{2C_5}}$ then

$$\frac{1}{2C_0}d_{2m+1,y}(s) < \frac{1}{2C_0}\,\frac{\left(\sum\limits_{p<y}\frac{1}{p-1}\right)^{2m+1}}{(2m+1)!} < \frac{1}{2C_0}\left(\frac{10\log\log 10y}{2m+1}\right)^{2m+1}$$
$$< \frac{C_{10}}{2}\left(\frac{2m+1}{2m+2}-\frac{2m-1}{2m}\right)\frac{e^{-(s-1)}}{(\log 3y)^{0.6}},$$

hence

$$\frac{1}{2C_0}Q_{2m+1,y}(s) = \frac{1}{2C_0}Q_{2m-1,y}(s) + \frac{1}{2C_0}d_{2m+1,y}(s)$$
$$< \frac{F(s)}{\sqrt{\log 3y}} + \frac{C_{10}e^{-(s-1)}}{2(\log 3y)^{0.6}}\cdot\frac{2m+1}{2m+2}.$$

If $2 \leqslant s \leqslant 2m+2 \leqslant \dfrac{\sqrt[10]{\log 3y}}{\sqrt[4]{2C_5}}$ then

$$\frac{1}{2C_0}Q_{2m+1,y}(s) < \sum_{\substack{y^{1/(2m+2)}\leqslant p<y^{1/s}\\ p\in\mathscr{P}}} \frac{f\left(\frac{\log y}{\log p}-1\right)}{\varphi_E(p)\sqrt{\log 3\frac{y}{p}}} +$$
$$+\frac{2m}{2m+1}C_{10}\sum_{\substack{y^{1/(2m+2)}\leqslant p<y^{1/s}\\ p\in\mathscr{P}}} \frac{\left(\frac{\log y}{\log p}\right)^{0.4}\left(\frac{\log y}{\log p}-1\right)^{0.6}e^{-\left(\frac{\log y/p}{\log p}\right)}}{\varphi_E(p)\left(\log 3\frac{y}{p}\right)^{0.6}}$$

$$< \frac{F(s)}{\sqrt{\log 3y}} + \frac{2m}{2m+1}\cdot\frac{C_{10}}{2}\cdot\frac{e^{-(s-1)}}{(\log 3y)^{0.6}} + 2\,C_5C_{10}\frac{(2m+2)se^{-(s-1)}}{\log 3y}$$
$$< \frac{F(s)}{\sqrt{\log 3y}} + \frac{2m+1}{2m+2}\cdot\frac{C_{10}}{2}\cdot\frac{e^{-(s-1)}}{(\log 3y)^{0.6}}.$$

If $s > 2m+3$ then

$$d_{2m+2,y}(s) = 0 \quad \text{and} \quad Q_{2m+2,y}(s) = Q_{2m,y}(s).$$

Let $s \leqslant 2m+3$. If

$$\frac{2e^3(2m+3)C_9}{\log 3y} > \left(\frac{2m+2}{2m+3}-\frac{2m+1}{2m+2}\right)\frac{C_{10}}{(\log 3y)^{0.6}}$$

then

$$\frac{1}{2C_0}d_{2m+2,y}(s) < \frac{\left(\sum\limits_{p<y}\frac{1}{p-1}\right)^{2m+2}}{2C_0(2m+2)!} < \frac{1}{2C_0}\left(\frac{10\log\log 10y}{2m+2}\right)^{2m+2}$$
$$< C_{10}\left(\frac{2m+2}{2m+3}-\frac{2m}{2m+1}\right)\frac{e^{-(2m+3)}}{(\log 3y)^{0.6}},$$

hence

$$\frac{1}{2C_0}Q_{2m+2,y}(s) = \frac{1}{2C_0}Q_{2m,y}(s) + \frac{1}{2C_0}d_{2m+2,y}(s)$$
$$< \frac{f(s)}{\sqrt{\log 3y}} + C_{10}\frac{(s+1)^{0.4}s^{0.6}e^{-s}}{(\log 3y)^{0.6}}\cdot\frac{2m+2}{2m+3}.$$

If $1 \leqslant s \leqslant 2m+3$ and

$$2C_9\frac{(2m+3)e^3}{\log 3y} > \left(\frac{2m+2}{2m+3}-\frac{2m+1}{2m+2}\right)\frac{C_{10}}{(\log 3y)^{0.6}}$$

then

$$\frac{1}{2C_0}Q_{2m+2,y}(s) < \sum_{\substack{y^{1/(2m+3)}\leqslant p<y^{1/3}\\ p\in\mathscr{P}}} \frac{F\left(\frac{\log y}{\log p}-1\right)}{\varphi_E(p)\sqrt{\log 3\frac{y}{p}}} +$$
$$+\frac{C_{10}}{2}\cdot\frac{2m+1}{2m+2}\sum_{\substack{y^{1/(2m+3)}\leqslant p<y^{1/s}\\ p\in\mathscr{P}}} \frac{e^{-\max\left(\frac{\log y}{\log p}-2,1\right)}}{\varphi_E(p)\left(\log 3\frac{y}{p}\right)^{0.6}} + d_{2,y}(s)$$
$$\leqslant \frac{f(s)}{\sqrt{\log 3y}} + \frac{C_{10}}{4}\cdot\frac{2m+1}{2m+2}\int_s^\infty \frac{e^{-\max(t-2,1)}}{t\left(t-\frac{1}{t}\right)^{0.6}}\,dt\,(\log 3y)^{-0.6} +$$

$$+\frac{g_2(s)}{4\sqrt{\log 3y}}+2C_6\frac{(2m+3)e^{-(s-1)}}{\log 3y}+C_9\frac{\Theta(s)}{\log 3y}$$
$$<\frac{f(s)}{\log 3y}+C_{10}\frac{2m+1}{2m+2}(s+1)\left(1-\frac{1}{s+1}\right)^{0.6}e^{-s}(\log 3y)^{-0.6},$$

where $\Theta(s)=1$ for $1\leqslant s\leqslant 3$ and 0 for $s>3$.

Corollary 1.

$$Q_{\vartheta,y}(s)<\frac{2C_0H_\vartheta(s)}{\sqrt{\log 3y}}\left(1+C_{11}(\log 3y)^{-1/10}\right).$$

Corollary 2. *If the condition* $(*)$ *is satisfied and* $y\geqslant 1$ *then for* $s\geqslant 2$ *and* $s\geqslant 1$ *we have the estimations*

$$A(M;y^{1/s})\leqslant\frac{YC_0}{\varphi(E)\sqrt{\log 3y}}\left\{\sqrt{s}+2F(s)+\frac{C_{12}}{(\log 3y)^{1/10}}\right\}+\sum_{\substack{d<y\\ p|d\Rightarrow p\in\mathscr{P}}}|R_d(M)|,$$
$$A(M;y^{1/s})\geqslant\frac{YC_0}{\varphi(E)\sqrt{\log 3y}}\left\{\sqrt{s}-2f(s)-\frac{C_{12}}{(\log 3y)^{1/10}}\right\}-\sum_{\substack{d<y\\ p|d\Rightarrow p\in\mathscr{P}}}|R_d(M)|,$$

respectively.

Proof. It follows from Corollary 1 to Theorem 5 and from Lemmas 3.2 and 3.5 that for $r\gg\log 3y$

$$G_{r,y}(s)=R(y^{1/s})+Q_{2r+1,y}(s)\leqslant\frac{C_0\sqrt{s}}{\sqrt{\log 3y}}+\frac{2C_0F(s)}{\sqrt{\log 3y}}+\frac{C_{12}}{(\log 3y)^{0.6}},$$
$$D_{r,y}(s)=R(y^{1/s})-Q_{2r,y}(s)\geqslant\frac{C_0\sqrt{s}}{\sqrt{\log 3y}}-\frac{2C_0f(s)}{\sqrt{\log 3y}}-\frac{C_{12}}{(\log 3y)^{0.6}}$$

which proves the assertion.

In particular we get

Corollary 3. *If the condition* $(*)$ *is satisfied and* $1\leqslant s\leqslant 3$ *then*

(3.6) $A(M;y^{1/s})$
$$\leqslant 2\sqrt{\frac{e^\gamma}{\pi}}\cdot\frac{C_0Y}{\varphi(E)\sqrt{\log 3y}}\left\{1+\frac{C_{13}}{(\log 3y)^{1/10}}\right\}+\sum_{\substack{d<y\\ p|d\Rightarrow p\in\mathscr{P}}}|R_d(M)|,$$

(3.7) $A(M;y^{1/s})$
$$\geqslant\sqrt{\frac{e^\gamma}{\pi}}\cdot\frac{C_0Y}{\varphi(E)\sqrt{\log 3y}}\left\{\int_1^s\frac{dt}{\sqrt{t(t-1)}}-\frac{C_{13}}{(\log 3y)^{1/10}}\right\}-\sum_{\substack{d<y\\ p|d\Rightarrow p\in\mathscr{P}}}|R_d(M)|.$$

Remark. The constant C_{13} depends only on the constants C_0, C_1.

§ 4. Proof of Theorem 1.

We shall use the following lemmas:

Lemma 4.1 (Bombieri). *There exists an absolute constant* U *such that*

$$\sum_{k<\frac{\sqrt{x}}{(\ln x)^U}}\max_{\substack{l\\ (l,k)=1}}\left|\pi(x,k,l)-\frac{\mathrm{Li}\,x}{\varphi(k)}\right|\ll\frac{x}{(\log x)^{20}}$$

(see e.g. [7]).

Lemma 4.2. *If* $f(n)$ *is a multiplicative function,*

$$f(n)\geqslant 0,\quad f(p^\vartheta)\leqslant\frac{\gamma_1\gamma_2^\vartheta}{p^\vartheta},\quad \gamma_2<2\leqslant\vartheta$$

and

$$\sum_{p<x}f(p)\log p\sim\tau\log x \tag{4.1}$$

then

$$\sum_{n\leqslant X}f(n)\sim\frac{1}{\Gamma(\tau+1)}\prod_p\left(1+f(p)+f(p^2)+\ldots\right)\left(1-\frac{1}{p}\right)^\tau(\log x)^\tau \tag{4.2}$$

(see e.g. [13]).

Lemma 4.3. *Let* $(a,\beta)=1$, $a\geqslant 1$, $2\,|\,a\beta$, $(l,k)=1$, $(al+\beta,k)=1$, $2a+\beta<N$, $k<\log^{15}N$. *Then*

$$\sum_{\substack{ap_1+\beta=p_2\leqslant N\\ p_1\equiv l(\mathrm{mod}\,k)}}1\leqslant\frac{8}{a\varphi(k)}\prod_{p>2}\left(1-\frac{1}{(p-1)^2}\right)\prod_{2<p|a\beta k}\left(1+\frac{1}{p-2}\right)\times$$
$$\times\frac{N-\beta}{\log^2\frac{N-\beta}{a}}\left(1+\frac{\log\log\frac{N-\beta}{a}}{\log\frac{N-\beta}{a}}O(1)\right).$$

The constant in the symbol $O(1)$ is absolute.

The proof of this lemma can be obtained with use of Lemma 4.1 and the linear sieve (see [9]).

Let $\mathscr{P}$ be the set of primes not dividing $2DA$ such that $\left(\frac{k(D)}{p}\right)=-1$.

It follows from (2.18) that the condition $(*)$ is fulfilled. The constant C_1 depends only on D and A. Let $E=QBd$, $M=\mathscr{M}$,

$$Y=\prod_{p|D_1}\left(1-\frac{1}{p}\right)\prod_{\substack{p|D_1\\ p\nmid Bd}}\left(1-\frac{1}{(p-1)^2}\right)LiN,\quad y=\sqrt{N}/|QBdD|(\log N)^U,$$

$|QBd| < \log^{15} N$ and $1 \leqslant s \leqslant 3$. If N is large enough $(\sqrt{N}\log^{-U-15} N > e^{C_1})$, the assumptions of Theorem 5 are satisfied and we get the estimate

$$(4.3)\qquad A(\mathscr{M}; y^{1/s}) \leqslant \frac{2\sqrt{2\frac{e^{\gamma}}{\pi}C_0}}{\varphi(QBd)} \prod_{p|D_1}\left(1-\frac{1}{p}\right)\prod_{\substack{p|D_1\\ p\nmid Bd}}\left(1-\frac{1}{(p-1)^2}\right)\times$$
$$\times\frac{N}{(\log N)^{3/2}}\big(1+o(1)\big)+O(N\log^{-20}N),$$

$$(4.4)\qquad A(\mathscr{M}; y^{1/s}) \geqslant \frac{\sqrt{2\frac{e^{\gamma}}{\pi}C_0}}{\varphi(QBd)} \prod_{p|D_1}\left(1-\frac{1}{p}\right)\prod_{\substack{p|D_1\\ p\nmid Bd}}\left(1-\frac{1}{(p-1)^2}\right)\times$$
$$\times\frac{N}{(\log N)^{3/2}}\left\{\int_1^s\frac{dt}{\sqrt{t(t-1)}}+o(1)\right\}+O(N\log^{-20}N).$$

The constants implicit in the symbols $O(N\log^{-20}N)$ depend only on D, A and C_0. Also $o(1)$ is uniform with respect to B. The estimation of the remainder term follows from (2.15) and Lemma 4.1. Note that

$$C_0 = \lim_{z\to\infty}\prod_{\substack{p<z\\ p\in\mathscr{P}}}\left(1-\frac{1}{\varphi_E(p)}\right)\sqrt{\log z} = \lim_{z\to\infty}\prod_{\substack{p<z\\ p\in\mathscr{P}\\ p|QBd}}\left(1-\frac{1}{p}\right)\prod_{\substack{p<z\\ p\in\mathscr{P}\\ p\nmid QBd}}\left(1-\frac{1}{p-1}\right)\sqrt{\log z}$$
$$= \lim_{z\to\infty}\prod_{\substack{p<z\\ p\in\mathscr{P}\\ p\nmid B}}\frac{\left(1-\frac{1}{p-1}\right)}{\left(1-\frac{1}{p}\right)}\prod_{\substack{p<z\\ p\in\mathscr{P}}}\left(1-\frac{1}{p}\right)\sqrt{\log z}$$
$$= \prod_{\substack{p\nmid 2DBA\\ \left(\frac{k(D)}{p}\right)=-1}}\left(1-\frac{1}{(p-1)^2}\right)\lim_{z\to\infty}\prod_{\substack{p<z\\ p\nmid 2DA\\ \left(\frac{k(D)}{p}\right)=-1}}\left(1-\frac{1}{p}\right)\sqrt{\log z}$$
$$= e^{-\gamma/2}\prod_{\substack{p\nmid 2DBA\\ \left(\frac{k(D)}{p}\right)=-1}}\left(1-\frac{1}{(p-1)^2}\right)\prod_{p|2DA}\left(1-\frac{1}{p}\right)^{-1/2}\prod_{p\nmid 2DA}\left(1-\frac{1}{p}\right)^{-\frac{1}{2}\cdot\left(\frac{k(D)}{p}\right)}.$$

In particular, hence follows the estimation $1 \ll C_0 \ll 1$, where the constants implicit in the symbol $\ll$ depend only on D and A.

Thus the constants implicit in the symbols $O(N\log^{-20}N)$ occurring in the formulae (4.3) and (4.4) depend also only on D and A, also $o(1)$ is uniform with respect to B.

The inequalities (4.3) and (4.4) allow us to estimate $\sum\limits_{\substack{m\in\mathscr{M}\\ q|m\Rightarrow q\in P}} 1$. By (2.12) and the definition of $A(M; y^{1/s})$ we obtain

$$A(\mathscr{M}; y^{1/s}) = \sum_{\substack{m\in\mathscr{M}\\ \left.\begin{smallmatrix}q|m\\ q<y^{1/s}\end{smallmatrix}\right\}\Rightarrow q\in P}} 1,$$

whence, in virtue of the Corollary to Theorem 4, it follows that for $1 < s < \frac{4}{3}$ and sufficiently large N (such that $(N^{1/2}\log^{-15-U}N)^{1/s} > N^{1/3}$)

$$(4.5)\qquad A(\mathscr{M}; y^{1/s}) = \sum_{\substack{m\in\mathscr{M}\\ q|m\Rightarrow q\in P}} 1 + \sum_{\substack{p_1p_2m\in\mathscr{M}\\ q|m\Rightarrow q\in P\\ y^{1/s}\leqslant p_1,p_2\in\mathscr{P}}} 1.$$

Lemma 4.4. *Let $|QBd| < (\log N)^{15}$ and $s > 1$. Then*

$$\sum_{\substack{p_1p_2m\in\mathscr{M}\\ q|m\Rightarrow q\in P\\ y^{1/s}\leqslant p_1,p_2\in\mathscr{P}}} 1 < \frac{4e^{\gamma/2}C_0\sqrt{s-1}}{\sqrt{\pi}\varphi(QBd)\sqrt{s}}\log(2s-1)\frac{4s^2N}{(\log N)^{3/2}}\big(1+o(1)\big),$$

where $o(1)$ is uniform with respect to B.

Proof. Applying Lemma 4.3 we obtain

$$\sum_{\substack{p_1p_2m\in\mathscr{M}\\ q|m\Rightarrow q\in P\\ y^{1/s}\leqslant p_1,p_2\in\mathscr{P}}} 1 = \sum_{\substack{mp_1p_2Bd+A=p\equiv BdL+A\,(\mathrm{mod}\,QBd)\\ q|m\Rightarrow q\in P,\,y^{1/s}\leqslant p_1,p_2\in\mathscr{P},\,p\leqslant N}} 1 \leqslant \sum_{\substack{m<\frac{N}{Bdy^{2/s}}\\ q|m\Rightarrow q\in P\\ (m,2DA)=1}}\ \sum_{\substack{y^{1/s}\leqslant p_1,p_2\in\mathscr{P}\\ mp_1p_2Bd+A=p\leqslant N\\ p_1p_2\equiv\frac{L}{m}(\mathrm{mod}\,Q)}} 1$$
$$\leqslant \sum_{\substack{m<\frac{N}{Bdy^{2/s}}\\ q|m\Rightarrow q\in P\\ (m,2DA)=1}}\ \sum_{\substack{y^{1/s}\leqslant p_1<\frac{N}{mBdy^{1/s}}\\ p_1\in\mathscr{P}}}\ \sum_{\substack{y^{1/s}\leqslant p_2<\frac{N}{mBdp_1}\\ mp_1p_2Bd+A=p\leqslant N\\ p_2\equiv\frac{L}{mp_1}(\mathrm{mod}\,Q)}} 1$$
$$< \sum_{\substack{m<N^{\frac{s-1}{s}}\log^{2U}N\\ q|m\Rightarrow q\in P\\ (m,2DA)=1}}\ \sum_{\substack{N^{\frac{1}{2s}}\log^{-U-15}N\leqslant p_1\leqslant\frac{N^{\frac{2s-1}{2s}}\log^U N}{Bdm}\\ p_1\in\mathscr{P}}}\times$$
$$\times\frac{8\prod\limits_{p>2}\left(1-\frac{1}{(p-1)^2}\right)}{Bdp_1\varphi(Q)}\,\frac{\prod\limits_{p>2,\,p|QBdAm}\left(1+\frac{1}{p-2}\right)N}{m\log^2 N/mp_1Bd}\big(1+o(1)\big).$$

If m is prime to $2DA$ then

$$\prod_{2<p|QBdAm}\left(1+\frac{1}{p-2}\right) = \prod_{2<p|QBdA}\left(1+\frac{1}{p-2}\right)\prod_{\substack{p|m\\ p\nmid B}}\left(1+\frac{1}{p-2}\right).$$

The function $\lambda(m)$ defined by the formula

$$\lambda(m)=\begin{cases}\dfrac{1}{m}\prod\limits_{p|m,\,p\nmid B}\left(1+\dfrac{1}{p-2}\right) & \text{if}\quad (m,2DA)=1,\ q|m\Rightarrow q\epsilon P,\\ 0 & \text{otherwise}\end{cases}$$

is multiplicative. Moreover,

$$\lambda(p^{\vartheta})=\begin{cases}p^{-\vartheta}\left(1+\dfrac{1}{p-2}\right) & \text{if}\quad p\nmid 2BDA,\ \left(\dfrac{k(D)}{p}\right)=1,\\ p^{-\vartheta} & \text{if}\quad p|B,\,p\nmid 2DA,\left(\dfrac{k(D)}{p}\right)=1,\\ 0 & \text{otherwise,}\end{cases}$$

thus

$$\prod_{p}\left(1+\lambda(p)+\lambda(p^2)+\ldots\right)\left(1-\frac{1}{p}\right)^{1/2}$$
$$=\prod_{p|2DA}\left(1-\frac{1}{p}\right)^{1/2}\prod_{p\nmid 2DA}\left(1-\frac{1}{p}\right)^{-\frac{1}{2}\left(\frac{k(D)}{p}\right)}\prod_{\substack{p\nmid 2DBA\\ \left(\frac{k(D)}{p}\right)=1}}\left(1+\frac{1}{p(p-2)}\right).$$

Applying now Lemma 4.2 we get the estimation

$$\sum_{\substack{p_1p_2m\epsilon\mathscr{M}\\ q|m\Rightarrow q\epsilon P\\ y^{1/s}\leqslant p_1,p_2\epsilon\mathscr{P}}}1\leqslant\frac{4\prod\limits_{p>2}\left(1-\frac{1}{(p-1)^2}\right)}{\varphi(Q)Bd}\prod_{2<p|QBdA}\left(1+\frac{1}{p-2}\right)\log(2s-1)\frac{4s^2N}{\log^2N}\times$$
$$\times\sum_{m<N^{\frac{2s-1}{2s}}\log^{U}N}\lambda(m)\left(1+o(1)\right)$$
$$\leqslant\frac{4\prod\limits_{p\neq 2}\left(1-\frac{1}{(p-1)^2}\right)}{\Gamma(\frac{3}{2})\varphi(Q)Bd}\prod_{2<p|QBdA}\left(1+\frac{1}{p-2}\right)\frac{4s^2N}{\log^2N}\log(2s-1)\sqrt{\frac{2s-1}{s}\log N}\times$$
$$\times\prod_{p|2DA}\left(1-\frac{1}{p}\right)^{1/2}\prod_{\substack{p\nmid 2DBA\\ \left(\frac{k(D)}{p}\right)=1}}\left(1+\frac{1}{p(p-2)}\right)\prod_{p\nmid 2DA}\left(1-\frac{1}{p}\right)^{-\frac{1}{2}\left(\frac{k(D)}{p}\right)}\left(1+o(1)\right)$$
$$=4\prod_{p|2DA}\left(1-\frac{1}{p}\right)^{-1/2}\prod_{\substack{p\nmid 2DBA\\ \left(\frac{k(D)}{p}\right)=-1}}\left(1-\frac{1}{(p-1)^2}\right)\times$$

$$\times\prod_{p\nmid 2DA}\left(1-\frac{1}{p}\right)^{-\frac{1}{2}\left(\frac{k(D)}{p}\right)}\frac{\sqrt{\frac{s-1}{s}}\log(2s-1)}{\sqrt{\pi}\,\varphi(QBd)}\cdot\frac{4s^2N}{(\log N)^{3/2}}\left(1+o(1)\right),$$

and the proof of the lemma is complete.

Putting together the results of Lemma 4.4, the identity (4.5) and the estimates (4.3) and (4.4) we get for $1<s<\frac{4}{3}$, $|QBd|<\log^{15}N$,

$$(4.6)\qquad \sum_{\substack{m\epsilon\mathscr{M}\\ q|m\Rightarrow q\epsilon P}}1\leqslant 2\sqrt{\frac{2e^{\gamma}}{\pi}}\cdot\frac{C_0}{\varphi(QBd)}\prod_{p|D_1}\left(1-\frac{1}{p}\right)\prod_{\substack{p|D_1\\ p\nmid Bd}}\left(1-\frac{1}{(p-1)^2}\right)\times$$
$$\times\frac{N}{(\log N)^{3/2}}\left(1+o(1)\right)+O(N\log^{-20}N),$$

$$(4.7)\qquad \sum_{\substack{m\epsilon\mathscr{M}\\ q|m\Rightarrow q\epsilon P}}1\geqslant\sqrt{\frac{2e^{\gamma}}{\pi}}\cdot\frac{C_0}{\varphi(QBd)}\prod_{p|D_1}\left(1-\frac{1}{p}\right)\prod_{\substack{p|D_1\\ p\nmid Bd}}\left(1-\frac{1}{(p-1)^2}\right)\times$$
$$\times\frac{N}{(\log N)^{3/2}}\left\{\int_1^s\frac{dt}{\sqrt{t(t-1)}}-8s^2\sqrt{2\frac{s-1}{s}}\log(2s-1)+o(1)\right\}+O(N\log^{-20}N).$$

The constants implicit in the symbol $O(N\log^{-20}N)$ depend only on D and A, also $o(1)$ is uniform with respect to B.

Proof of Theorem 1. Set

$$(4.8)\qquad \Omega_{A,B,D}=\sum_{\substack{d\\ 2|ABd}}\ \sum_{\substack{L\epsilon\mathscr{L}\\ (BdL+A,QBd)=1}}\frac{1}{\varphi(QBd)}\prod_{p|D_1}\left(1-\frac{1}{p}\right)\prod_{\substack{p|D_1\\ p\nmid Bd}}\left(1-\frac{1}{(p-1)^2}\right),$$

where d runs over all positive integers satisfying the conditions given in Tables 1 and 2 and $\mathscr{L}=\mathscr{L}(d)$ for fixed A and D.

Define further

$$\tilde{\Omega}_{A,B,D}=\sum_{\substack{d\\ 2|ABd\\ |QBd|\leqslant\log^{15}N}}\ \sum_{\substack{L\epsilon\mathscr{L}\\ (BdL+A,QBd)=1}}\frac{1}{\varphi(QBd)}\prod_{p|D_1}\left(1-\frac{1}{p}\right)\prod_{\substack{p|D_1\\ p\nmid Bd}}\left(1-\frac{1}{(p-1)^2}\right),$$

whence

$$|\Omega_{A,B,D}-\tilde{\Omega}_{A,B,D}|\leqslant\sum_{\substack{d\\ QBd>\log^{15}N\\ p|d\Rightarrow p|2D}}\frac{Q}{\varphi(QBd)}<\frac{|8D|}{\log^5N}\sum_{p|d\Rightarrow p|2D}\frac{1}{\sqrt{\varphi(d)}}<\frac{|8D|^3}{\log^5N}.$$

By (4.7) and (2.17) we get

$$S_1(N,\varphi,B,A)\geqslant\theta\sqrt{\frac{2e^{\gamma}}{\pi}}\,C_0\tilde{\Omega}_{A,B,D}\frac{N}{(\log N)^{3/2}}\big(1+o(1)\big)+$$
$$+O(N\log^{-20}N)\sum_{d\leqslant\log^{15}N}Q(d)-|A|$$
$$=\theta\Psi_{A,B,D}\Omega_{A,B,D}\frac{N}{(\log N)^{3/2}}\big(1+o(1)\big)+O(N\log^{-5}N)$$

and

$$S_1(N,\varphi,B,A)\leqslant 2\sqrt{\frac{2e^{\gamma}}{\pi}}\,C_0\tilde{\Omega}_{A,B,D}\frac{N}{(\log N)^{3/2}}\big(1+o(1)\big)+$$
$$+\sum_{\substack{d\\ 2|ABd\\ QBd>\log^{15}N}}\ \sum_{\substack{L\epsilon\mathscr{L}\\ (BdL+A,QBd)=1}}\ \sum_{\substack{m\epsilon\mathscr{M}\\ q|m\Rightarrow q\epsilon P}}1+O(N\log^{-5}N)$$
$$\leqslant 2\Psi_{A,B,D}\Omega_{A,B,D}\frac{N}{(\log N)^{3/2}}\big(1+o(1)\big)+\sum_{\substack{d\\ QBd>\log^{15}N\\ p|d\Rightarrow p|2D}}\ \sum_{L\epsilon\mathscr{L}}\ \sum_{m\leqslant\frac{N+|A|}{Bd}}1+O(N\log^{-5}N)$$
$$\leqslant 2\Psi_{A,B,D}\Omega_{A,B,D}\frac{N}{(\log N)^{3/2}}\big(1+o(1)\big)+\sum_{\substack{d\\ QBd>\log^{15}N\\ p|d\Rightarrow p|2D}}\frac{Q(N+|A|)}{Bd}+O(N\log^{-5}N)$$
$$\leqslant 2\Psi_{A,B,D}\Omega_{A,B,D}\frac{N}{(\log N)^{3/2}}\big(1+o(1)\big)+\frac{(8D)^4(N+|A|)}{\log^5N}+O(N\log^{-5}N).$$

Thus the proof of (1.1) is complete.

It follows from (4.8) that

$$\frac{1}{\varphi(B)}\ll\Omega_{A,B,D}\ll\frac{1}{\varphi(B)};$$

thus we get

$$S_\infty(N,\varphi,B,A)\leqslant\sum_{\substack{B_0=1\\ (B_0,A)=1}}^{\infty}S_1(N,\varphi,BB_0^2,A)=\sum_{B_0\leqslant\log^2N}+\sum_{B_0>\log^2N}$$
$$\ll\sum_{B_0\leqslant\log^2N}\Big\{\frac{N}{\varphi(BB_0^2)(\log N)^{3/2}}+O(N\log^{-5}N)\Big\}+\sum_{B_0>\log^2N}\frac{N+|A|}{BB_0^2}$$
$$\ll\frac{N}{\varphi(B)(\log N)^{3/2}}.$$

Since

$$S_\infty(N,\varphi,B,A)\geqslant S_1(N,\varphi,B,A)\gg\frac{N}{\varphi(B)(\log N)^{3/2}}+O(N\log^{-5}N),$$

(1.2) is proved.

It remains to prove (1.3). Let $\varphi_1=\varphi_0,\varphi_2,\ldots,\varphi_t$ represent all classes of the genus R_{φ_0}. There exists an integer r prime to A and integer matrices T_i $(i=1,\ldots,t)$ such that

$$\varphi_0=\varphi_iS_i,\qquad S_i=\frac{T_i}{r}=\begin{pmatrix}\alpha_i&\beta_i\\ \gamma_i&\delta_i\end{pmatrix},\qquad\det S_i=1\qquad(1\leqslant i\leqslant t).$$

If $m=\varphi_i(\xi,\eta)$ for some i and some integers ξ,η then

$$m=\varphi_0(\alpha_i\xi+\beta_i\eta,\ \gamma_i\xi+\delta_i\eta).$$

The number $mr^2=\varphi_0(\alpha_i\xi r+\beta_i\eta r,\ \gamma_i\xi r+\delta_i\eta r)$ is representable by φ_0. Moreover, if $(\xi,\eta)=1$ then $(\alpha_i\xi r+\beta_i\eta r,\ \gamma_i\xi r+\delta_i\eta r)|r^2$, thus

$$S_2(N,\varphi,B,A)\geqslant S_1(N,\varphi,Br^2,A)\gg\frac{N}{\varphi(Br^2)(\log N)^{3/2}}+O(N\log^{-5}N).$$

The proof of Theorem 1 is complete.

Proof of the Corollary. Set $\varphi_0=\xi^2+\eta^2$, $A=1$. The genus of φ_0 contains only one class, besides, there for every value φ_0 is representable uniquely in the form B^2n, where n is representable properly by φ_0 and B has no prime factors $\equiv 1\pmod 4$

$$S(\xi^2+\eta^2,1,N)=\sum_{\substack{B=1\\ p|B\Rightarrow p\not\equiv 1(\mathrm{mod}\,4)}}^{\infty}S_1(N,\xi^2+\eta^2,B^2,1).$$

Since $D=-4$,

$$\Psi_{A,B,D}$$
$$=\frac{2}{\sqrt{\pi}}\prod_{p>2}\Big(1-\frac{1}{p}\Big)^{-\frac{1}{2}\left(\frac{-1}{p}\right)}\prod_{p\equiv-1(\mathrm{mod}\,4)}\Big(1-\frac{1}{(p-1)^2}\Big)\prod_{\substack{p\equiv-1(\mathrm{mod}\,4)\\ p|B^*}}\Big(1-\frac{1}{(p-1)^2}\Big)^{-1}.$$

It follows from the representation of L-series in a product form and from Dirichlet's class number formula that

$$\prod_{p>2}\Big(1-\Big(\frac{-1}{p}\Big)p^{-1}\Big)=\frac{4}{\pi},$$

hence

$$\Psi_{A,B,D}=\prod_{p\equiv-1(\mathrm{mod}\,4)}\Big(1-\frac{1}{(p-1)^2}\Big)\Big(1-\frac{1}{p^2}\Big)^{1/2}\prod_{\substack{p|B\\ p\equiv-1(\mathrm{mod}\,4)}}\Big(1-\frac{1}{(p-1)^2}\Big)^{-1}.$$

Let us compute the constant $\Omega_{A,B,D}$. Since $D = -4$, we have $\vartheta_2 = 2$, $d = 2^{\varepsilon_2}$. Table 2 gives $\varepsilon_2 = 0$, $\tau = 4$, $\varkappa = 1$ or $\varepsilon_2 = 1$, $\tau = 4$, $\varkappa = 1$, thus $Q = \tau(\varepsilon_2, \nu_2) = 4$, $D_1 = 1$ and

$$\Omega_{A,B,D} = \sum_{2|B} \sum_{\substack{L\in\mathscr{L}\\(BL+1,4B)=1}} \frac{1}{\varphi(4B)} + \sum_{\substack{L\in\mathscr{L}\\(2BL+1,8B)=1}} \frac{1}{\varphi(8B)} = \sum_{2|B} \frac{\varkappa(0,2)}{\varphi(4B)} + \frac{\varkappa(1,2)}{\varphi(8B)}$$

$$= \sum_{2|B} \frac{1}{\varphi(4B)} + \frac{1}{\varphi(8B)} = \frac{\varepsilon_B^*}{4\varphi(B)},$$

where we have set $\varepsilon_B^* = 1$ if $2\nmid B$ and $3/2$ if $2|B$.

The function

$$A(B) = \frac{\varepsilon_B^*}{\varphi(B) \displaystyle\prod_{\substack{p|B\\ p\equiv -1(\mathrm{mod}\,4)}} \left(1 - \frac{1}{(p-1)^2}\right)}$$

is multiplicative, thus

$$\sum_{\substack{B=1\\ p|B \Rightarrow p\not\equiv 1(\mathrm{mod}\,4)}}^{\infty} A(B^2) = \prod_p \left(1 + A(p^2) + A(p^4) + \ldots\right)$$

$$= 2 \prod_{p\equiv -1(\mathrm{mod}\,4)} \left(1 + \frac{1}{(p-2)(p+1)}\right).$$

Therefore

$$\sum_{\substack{B=1\\ p|B \Rightarrow p\not\equiv 1(\mathrm{mod}\,4)}}^{\infty} \Omega_{A,B^2,D} \Psi_{A,B^2,D} = \frac{1}{2} \prod_{p\equiv -1(\mathrm{mod}\,4)} \left(1 - \frac{1}{p^2}\right)^{-1/2} \left(1 - \frac{1}{p(p-1)}\right).$$

The corollary follows easily from this and from (1.1).

Set

$$J(D) = \begin{cases} 0 & \text{if} \quad \vartheta_2 = 0, \\ \frac{1}{2} & \text{if} \quad \vartheta_2 = 2,\ D^* \equiv -1\ (\mathrm{mod}\ 4) \ \text{or}\ \vartheta_2 = 3, \\ \frac{1}{4} & \text{if} \quad \vartheta_2 = 2,\ D^* \equiv 1\ (\mathrm{mod}\ 4), \\ \frac{3}{8} & \text{if} \quad \vartheta_2 = 4, \\ \frac{1}{3} + \frac{5}{3} 2^{2-\vartheta_2} & \text{if} \quad \vartheta_2 \geqslant 5,\ 2|\vartheta_2, \\ \frac{1}{3} + \frac{1}{3} 2^{4-\vartheta_2} & \text{if} \quad \vartheta_2 \geqslant 5,\ 2\nmid\vartheta_2, \end{cases}$$

$$\Phi(D, B)$$

$$= \prod_{2|B} 2 \begin{cases} \displaystyle\prod_{2\nmid A} \tfrac{1}{2} \prod_{2\nmid B} \tfrac{1}{2} & \text{if} \quad \vartheta_2 = 0, \\ \frac{1}{2} & \text{if} \quad \vartheta_2 = 2,\ D^* \equiv 1\ (\mathrm{mod}\ 4), \\ \frac{1}{4} & \text{if} \quad \vartheta_2 = 2,\ D^* \equiv -1\ (\mathrm{mod}\ 4) \ \text{or}\ \vartheta_2 = 3 \ \text{or}\ \vartheta_2 = 4, \\ \frac{1}{8} & \text{if} \quad \vartheta_2 \geqslant 5. \end{cases}$$

Using this notation we can write the constant $\Omega_{A,B,D}$ in the following compact form

$$\Omega_{A,B,D} = \frac{\Phi(D, B)}{B \displaystyle\prod_{\substack{p|B\\ p\nmid D^*}} \left(1 - \frac{1}{p}\right) \prod_{p|D^*} 2} \prod_{\substack{p|D^*\\ p\nmid AB}} \left(1 - \frac{\left|\left(\frac{a}{p}\right) + \left(\frac{-AB}{p}\right)\right|}{p-1}\right) \times$$

$$\times \prod_{\substack{p|D^*, 2|\vartheta_p, p\nmid 2A\\ p\neq 3 \text{ or } k(D)\not\equiv 1(\mathrm{mod}\,3)}} \left\{ 1 + \frac{\dfrac{1-p^{-\vartheta_p}}{p+1} + \left(1 + \left(\dfrac{k(D)}{p}\right)\right) p^{-\vartheta_p}}{(p-1) \displaystyle\prod_{p\nmid B} \left(1 - \frac{\left|\left(\frac{a}{p}\right) + \left(\frac{-AB}{p}\right)\right|}{p-1}\right)} \right\} \times$$

$$\times \prod_{\substack{3\nmid A\\ 3|D, k(D)\equiv 1(\mathrm{mod}\,3)}} \left\{ 1 + \frac{1 + 15\cdot 3^{-\vartheta_3}}{8 \displaystyle\prod_{3\nmid B} \left(1 - \frac{\left|\left(\frac{a}{3}\right) + \left(\frac{-AB}{3}\right)\right|}{2}\right)} \right\} \times$$

$$\times \prod_{\substack{p|D^*\\ p\nmid 2A\\ 2\nmid\vartheta_p}} \left\{ 1 - \frac{\dfrac{1-p^{-\vartheta_p}}{p^2-1} + p^{-\vartheta_p}}{\displaystyle\prod_{p\nmid B} \left(1 - \frac{\left|\left(\frac{a}{p}\right) + \left(\frac{-AB}{p}\right)\right|}{p-1}\right)} \right\} \times$$

$$\times \begin{cases} 1 & \text{if} \quad 2|A, \\ \displaystyle\sum_{2|B} 1 + \sum_{2\nmid B} 2 & \text{if} \quad 2\nmid A,\ D^* \equiv 1\ (\mathrm{mod}\ 8) \ \text{and}\ \vartheta_2 = 0, \\ \displaystyle\sum_{2|B} 1 + J(D) & \text{if} \quad 2\nmid A,\ D^* \not\equiv 1\ (\mathrm{mod}\ 8) \ \text{or}\ \vartheta_2 \neq 0. \end{cases}$$

References

[1] З. И. Боревич, И. Р. Шафаревич, *Теория чисел*, Москва 1964.

[2] Б. М. Бредихин, *Дисперсионный метод и бинарные аддитивные проблемы определенного типа*, Uspehi Mat. Nauk 20 (1965), no. 2 (122), pp. 89–130.

[3] Б. М. Бредихин, Ю. В. Линник, *Асимптотика и эргодические свойства решений обобщенного уравнения Гарди-Литтлвуда*, Мат. сб. 71 (113) (1966), pp. 145–161.

[4] Б. В. Левин, А. С. Файнлейб, *Применение некоторых интегральных уравнений к вопросам теории чисел*, Uspehi Mat. Nauk 27 (1967), no. 3 (135), pp. 119–197.

[5] А. О. Гельфонд, Ю. В. Линник, *Элементарные методы в аналитической теории чисел*, Москва 1962.

[6] H. Iwaniec, *On the error term in the linear sieve*, Acta Arith. 19 (1971), pp. 29–58.

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

[8] Y. Motohashi, *On the distribution of prime numbers which are of the form* x^2+y^2+1, Acta Arith. 16 (1970), pp. 351–363.

[9] H.-E. Richert, *Selberg's sieve with weights*, Proc. Symposia Pure Math. 20 (1971), pp. 287–310.

[10] E. Schering, *Beweis des Dirichletschen Satzes*, Ges. Werke, Bd. II, 1909, pp. 357–365.

[11] G. L. Watson, *Integral quadratic forms*, Cambridge 1960.

[12] H. Weber, *Beweis des Satzes, dass usw.*, Math. Ann. 20 (1882), pp. 301–329.

[13] E. Wirsing, *Das asymptotische Verhalten von Summen über multiplicative Funktionen*, Math. Ann. 143 (1961), pp. 75–102.

Received on 24. 7. 1971 (193)

ACTA ARITHMETICA
XXI (1972)

Количественная форма задачи Бореля

Л. П. Постникова (Москва)

Понятие нормального числа в g-ичной шкале, т.е. вещественного числа α, для которого дробные доли $\{\alpha g^x\}$, $x = 1, 2, \ldots$, равномерно распределены на отрезке $[0, 1]$, было впервые введено Э. Борелем [2], стр. 197–199. Будем говорить, что некоторое число α *явно конструируется*, если указано разложение числа α в g-ичную дробь. Э. Борель [2], стр. 198–199, дал набросок явной конструкции нормальных чисел. Таким образом, задача о построении нормальных чисел восходит к Э. Борелю. Начиная с работ Мизеса [8] и Чемпернуона [13], было предложено множество конструкций нормальных чисел и более общих конструкций, библиографические сведения по этому вопросу можно найти в книге А. Г. Постникова [9].

Обозначим через $N_\gamma(P)$ количество дробных долей функции αg^x, попадающих на полуинтервал $[0, \gamma)$, $0 < \gamma \leqslant 1$, когда x пробегает значения $x = 1, 2, \ldots, P$. Свойство равномерного распределения означает, что при любом γ

$$N_\gamma(P) = \gamma P + o(P). \tag{1}$$

Естественно придать проблеме более определенный характер: под этим мы понимаем задачу о построении таких чисел α, для которых понижение в остаточном члене формулы (1) имело бы как можно меньший порядок. Инициатором такой постановки вопроса явился Н. М. Коробов; в работе [5] Н. М. Коробов явно сконструировал числа α, для которых при любом заданном γ выполняется соотношение

$$N_\gamma(P) = \gamma P + O(P^{1/2}). \tag{2}$$

В работах А. Г. Постникова [10] и М. Ф. Куликовой [7] были построены числа α, для которых в соотношении (2) остаточный член понижается на некоторую степень логарифма P, именно в работе [7] для любого целого $g \geqslant 2$ строится число α такое, что при любом $\varepsilon > 0$

$$N_\gamma(P) = \gamma P + O\left(\frac{P^{1/2}}{(\ln P)^{1/4-\varepsilon}}\right).$$