Conspectus materiae tomi XXIV, fasciculi 5

La revue est consacrée à la Théorie des Nombres
The journal publishes papers on the Theory of Numbers
Die Zeitschrift veröffentlicht Arbeiten aus der Zahlentheorie
Журнал посвящен теории чисел

L'adresse de
la Rédaction
et de l'échange

Address of the
Editorial Board
and of the exchange

Die Adresse der
Schriftleitung und
des Austausches

Адрес редакции
и книгообмена

ACTA ARITHMETICA
ul. Śniadeckich 8, 00-950 Warszawa

Les auteurs sont priés d'envoyer leurs manuscrits en deux exemplaires
The authors are requested to submit papers in two copies
Die Autoren sind gebeten um Zusendung von 2 Exemplaren jeder Arbeit
Рукописи статьей редакция просит предлагать в двух экземплярах

PRINTED IN POLAND

WROCŁAWSKA DRUKARNIA NAUKOWA

ACTA ARITHMETICA
XXIV (1974)

Primes represented by quadratic polynomials in two variables

by

H. Iwaniec (Warszawa)

Dedicated to C. L. Siegel

Introduction. Let $P(x, y) = ax^2+bxy+cy^2+ex+fy+g$ be a primitive quadratic polynomial with integer coefficients. If $P(x, y)$ is reducible in $Q(x, y)$ the question whether it represents infinitely many primes can be settled easily using Dirichlet's theorem on arithmetic progression. If $P(x, y)$ is irreducible in $Q[x, y]$ an obvious necessary condition is that P should represent arbitrarily large odd integers. The aim of this paper is to show that if P depends essentially on two variables (i.e. $\partial P/\partial x$ and $\partial P/\partial y$ are linearly independent) the above condition is also sufficient. We prove

Theorem 1. *Let*

$$P(x, y) = ax^2+bxy+cy^2+ex+fy+g \in Z[x, y],$$

$\deg P = 2$, $(a, b, c, e, f, g) = 1$, *$P(x, y)$ be irreducible in $Q[x, y]$, represent arbitrarily large odd numbers and depend essentially on two variables. Then*

(i) $$N\log^{-1}N \ll \sum_{\substack{p\leqslant N\\ p=P(x,y)}} 1 \quad \textit{if } D = af^2-bef+ce^2+(b^2-4ac)g = 0 \textit{ or } \Delta = b^2-4ac \textit{ is a perfect square},$$

(ii) $$N\log^{-3/2}N \ll \sum_{\substack{p\leqslant N\\ p=P(x,y)}} 1 \ll N\log^{-3/2}N \quad \textit{if } D \neq 0 \textit{ and } \Delta \textit{ is different from a perfect square.}$$

The estimation (ii) has been proved in [4] for $e = f = 0$.

A proof of (ii) for the case, where Δ is a fundamental discriminant has been outlined in [3]. The proof of (i) is based mainly on the theorem on arithmetic progression for the fields Q and $Q(\sqrt{\Delta})$. The proof of (ii) involves in an essential manner the method of $\frac{1}{2}$-dimensional sieve, Bombieri's mean value theorem and also Lemma 12 which allows one to reduce the problem of representation of integers from suitable arithmetic progressions by $P(x, y)$ to the problem of representation of certain other integers by the quadratic form $ax^2+bxy+cy^2$. The difficulties in obtaining an asymptotic formula are of two kinds. First, Lemma 12 allows one to count only primes p represented by $P(x,y)$ belonging to special arithmetic progressions. This difficulty could be overcome by using the arithmetic of ideals in $Z[\sqrt{\Delta}]$ as in [3] and besides the method of Bredihin and Linnik [1]. The other difficulty, much more serious consists in the incapability of the $\frac{1}{2}$-dimensional sieve to give the asymptotic value of the estimated quantity. Therefore it does not seem possible to obtain on the present lines the asymptotic formula in (ii).

On the other hand an asymptotic formula in (i) can be obtained by improving Lemma 11 on the lines indicated by E. Hecke [2]. In the case of $\Delta < 0$ he has actually formulated in [2], p. 48, the statement which easily implies Lemma 11 with an asymptotic formula in place of the inequality.

Let $F(\boldsymbol{x}) = G(\boldsymbol{x})+L(\boldsymbol{x})+g \in Q[x_1,\dots,x_n]$ and $\deg F = 2$, where $G(\boldsymbol{x})$ and $L(\boldsymbol{x})$ are a quadratic and linear form, respectively. We say that $F(\boldsymbol{x})$ depends essentially on at least two variables if there exists no affine transformation $E\colon R^n \to R^n$ which transforms F into a polynomial in one variable. Theorem 1 implies the following extension of Theorem 1 of [6].

Theorem 2. *Let $F(\boldsymbol{x})$ be a quadratic polynomial, integer valued (i.e. taking integer values in integer points) and irreducible in $Q[x_1,\dots,x_n]$. Let $F(\boldsymbol{x})$ assume positive values prime to an arbitrary given non-zero integer. Then if $F(\boldsymbol{x})$ depends essentially on at least two variables, it represents infinitely many primes.*

Proof. By Lemma 1 from [6] the coefficients of $2F(\boldsymbol{x})$ are integers. Let $E \in \mathrm{GL}(n,Q)$ transform G to a diagonal form. Let $R \neq 0$ be an integer such that the elements of RE are integers. By the assumption there exists an integer vector $\boldsymbol{a}$ such that $\big(F(\boldsymbol{a}), 2R^n|E|C(2G)\big) = 1$, where $C(2G)$ is the content of $2G$, thus we can assume that $\big(g, 2R^n|E|C(2G)\big) = 1$. Let r be the rank of G and put $\boldsymbol{x} = 2RE\boldsymbol{y}$. Thus the polynomial

$$F_1(\boldsymbol{y}) \overset{\mathrm{df}}{=} F(\boldsymbol{x}) = a_1y_1^2+\dots+a_ly_l^2-a_{l+1}y_{l+1}^2-\dots-a_ry_r^2+\sum_{i=1}^{n} b_iy_i+g$$

is irreducible with integer coefficients, $(g, 2a_1, 2a_2, \dots, 2a_r) = 1$ and $F_1(\boldsymbol{y})$ assumes arbitrarily large values. By Lemma 2 from [6] it follows that $F_1(\boldsymbol{y})$ assumes integer values prime to an arbitrary given non-zero integer. Since polynomials equivalent by an affine transformation depend essentially on the same number of variables, $F_1(\boldsymbol{y})$ depends essentially on at least two variables. Clearly every integer represented by $F_1(\boldsymbol{y})$ is represented by $F(\boldsymbol{x})$. Therefore, it is enough to prove that there exist infinitely many primes represented by $F_1(\boldsymbol{y})$. We distinguish the following two cases:

a) There exists an $i > r$, $i \leqslant n$ such that $b_i \neq 0$.

Let $\boldsymbol{c} = (c_1,\dots,c_n)$ be an integer vector such that $\big(F_1(\boldsymbol{c}), b_i\big) = 1$. Then

$$\sum_{\substack{p\leqslant N\\ p=F_1(\boldsymbol{y})}} 1 \geqslant \sum_{\substack{p\leqslant N\\ p=F_1(c_1,\dots,c_{i-1},x+c_i,c_{i+1},\dots,c_n)}} 1 = \pi\big(N, |b_i|, F_1(\boldsymbol{c})\big) \geqslant N\log^{-1}N.$$

b) For each $i > r$, $i \leqslant n$ we have $b_i = 0$.

Since $F_1(\boldsymbol{y})$ assumes arbitrarily large values, we have $l \geqslant 1$. Since $F_1(\boldsymbol{y})$ depend essentially on at least two variables we have $r \geqslant 2$. If $r = 2$, the polynomial $F_1(\boldsymbol{y})$ satisfies all the assumptions of Theorem 1. Hence it represents infinitely many primes. If $r > 2$ then at least one of the polynomials $P_i(x,y) = F_1(x,y; 2ia_1a_2, 0,\dots,0)$ $(i = 0,1)$ satisfies all the assumptions of Theorem 1. Hence it represents infinitely many primes.

As pointed out by P. A. B. Pleasants (written communication) Theorem 2 combined with the method of his paper [6] gives the following improvement of the result of that paper: *If $\phi(x_1,\dots,x_n)$ is a non-degenerate, irreducible cubic polynomial in n variables with $n \geqslant 9$ and if for every integer $m > 1$ there is an integer point $\boldsymbol{x}$ for which $\phi(\boldsymbol{x}) \not\equiv 0 \pmod{m}$, then ϕ represents infinitely many positive prime numbers for integer values of the variables.*

I conclude by expressing my thanks to Professor A. Schinzel for reading and criticism of the manuscript. I owe to him Lemma 11 and some valuable suggestions.

§ 1. Some remarks about quadratic polynomials.

Let $P(x,y) = ax^2+bxy+cy^2+ex+fy+g$ and $P'(x,y) = a'x^2+b'xy+c'y^2+e'x+f'y+g'$ be polynomials with integer coefficients. We shall say that P' is *represented by P* if there exists an affine transformation $\tau(x,y) = (a_1x+a_2y+a_3, b_1x+b_2y+b_3)$ such that $P\big(\tau(x,y)\big) = P'(x,y)$ (the numbers $a_1, a_2, a_3, b_1, b_2, b_3$, are integers). Clearly, every integer represented by P' is represented by P. Set $\Delta = b^2-4ac$ (small discriminant), $D = af^2-bef+ce^2+\Delta g$ (large discriminant), $\alpha = bf-2ce$, $\beta = be-2af$. Easy calculations show that

(1) $$a' = aa_1^2+ba_1b_1+cb_1^2,$$

(2) $$b' = 2aa_1a_2+b(a_1b_2+a_2b_1)+2cb_1b_2,$$

(3) $$c' = aa_2^2+ba_2b_2+cb_2^2,$$

(4) $$e' = 2aa_1a_3+b(a_1b_3+a_3b_1)+2cb_1b_3+ea_1+fb_1,$$

(5) $$f' = 2aa_2a_3+b(a_2b_3+a_3b_2)+2cb_2b_3+ea_2+fb_2,$$

(6) $$g' = P(a_3, b_3),$$

$$\Delta' = (a_1b_2-a_2b_1)^2\Delta, \tag{7}$$

$$D' = (a_1b_2-a_2b_1)^2D, \tag{8}$$

$$\alpha' = (a_1b_2-a_2b_1)\big((a_3b_2-a_2b_3)\Delta+\alpha b_2-\beta a_2\big), \tag{9}$$

$$\beta' = (a_2b_1-a_1b_2)\big((a_3b_1-a_1b_3)\Delta+\alpha b_1-\beta a_1\big). \tag{10}$$

We shall say that a polynomial P is *equivalent to* P' if P is represented by P' and conversely. Hence P is equivalent to P if and only if $P\big(\tau(x, y)\big) = P'(x, y)$, where $\tau(x, y)$ is a unimodular affine transformation. The formulae (7)–(10) show that equivalent polynomials have the same both discriminants and also the same parameters $\varkappa = (\alpha, \beta, \Delta)$. Every integer represented by P is a constant term of a suitable polynomial P' equivalent to P, in fact obtained from P by translation.

Let $G_P(x, y)$ be the homogeneous part of P, i.e. $G_P(x, y) = ax^2+ +bxy+cy^2$. We have

$$\Delta^2P(x, y) = G_P(\Delta x+\alpha, \Delta y+\beta)+\Delta D, \tag{11}$$

which implies the following identities

$$2a\alpha+b\beta = \Delta e, \tag{12}$$

$$2c\beta+b\alpha = \Delta f, \tag{13}$$

$$G_P(\alpha, \beta) = -\Delta G_P(f, -e), \tag{14}$$

$$g\Delta^2-G_P(\alpha, \beta) = \Delta D. \tag{15}$$

Lemma 1. *$\partial P/\partial x$ and $\partial P/\partial y$ are linearly dependent if and only if $\Delta = \alpha = \beta = 0$.*

Proof (due to A. Schinzel). If $\partial P/\partial x = c_1L(x, y)$, $\partial P/\partial y = c_2L(x, y)$, where $L(x, y)$ is a linear form, then for a suitable c_3, $P(x, y)-c_3L^2(x, y)$ has both partial derivatives 0, hence it is constant and it follows from (7)–(10) that $\Delta = \alpha = \beta = 0$. If $\Delta = \alpha = \beta = 0$ then $P(x, y)$ is equivalent to polynomial $P'(x, y) = a'x^2+e'x+f'y+g'$, where $\alpha' = \beta' = 0$. Hence $a'\cdot f' = 0$ and either $f' = 0$, $\partial P'/\partial y = 0$ or $a' = 0$, $f'\partial P'/\partial x - -e'\partial P'/\partial y = 0$. It follows that $\partial P/\partial x$, $\partial P/\partial y$ are linearly dependent.

We shall say that a polynomial $P(x, y)$ *belongs to the class* $\mathscr{H}$ if for every integer $\Delta \neq 0$ P represents an integer prime to Δ.

Lemma 2. *A polynomial $P(x, y) = ax^2+bxy+cy^2+ex+fy+g$ belongs to $\mathscr{H}$ if and only if*

$$(a, b, c, e, f, g) = 1, \tag{16}$$

$$[a, c, b, g] \not\equiv [e, f, 0, 0] (\mathrm{mod}\, 2). \tag{17}$$

Proof. This lemma follows from Lemma 2 of [6].

Lemma 3. *If $P'(x, y) \in \mathscr{H}$ and $\Delta' \neq 0$ then $P'(x, y)$ represents a polynomial $P(x, y) = ax^2+bxy+cy^2+ex+fy+g \in \mathscr{H}$ such that*

$$\Delta = (a, b, c)^2\Delta', \quad (\alpha, \beta) = \varkappa,$$
$$D = (a, b, c)^2D', \quad (g, \Delta) = 1,$$
$$(ac, \Delta) = (a, b, c)^2, \quad (a, b, c)\,|\,(e, f).$$

Proof. Since $P'(x, y)$ represents integer prime to Δ', P' is equivalent to a polynomial $P''(x, y) = a''x^2+b''xy+c''y^2+e''x+f''y+g''$, where $g'' \neq D'/\Delta'$ and $(g'', \Delta') = 1$. Hence by (14) and (15) we obtain $G_{P''}(f'', -e'') \neq 0$, thus $|e''|+|f''| \neq 0$. Let u and v be a solution of the equation $uf''+ve'' = (e'', f'')$. The unimodular transformation

$$\tau(x, y) = \big(f''/(e'', f'')x+vy,\ -e''/(e'', f'')x+uy\big)$$

transforms $P''(x, y)$ into the polynomial

$$P'''(x, y) = P''\big(\tau(x, y)\big) = a'''x^2+b'''xy+c'''y^2+(e'', f'')y+g'',$$

where $a''' = G_{P''}(f'', -e'')/(e'', f'')^2 = (D'-\Delta'g'')/(e'', f'')^2$. Put $a''' = UW$, where $(U, a''', b''', c''') = 1$, $p\,|\,W \Rightarrow p\,|\,(a''', b''', c''')$. The transformation $\sigma(x, y) = (x, yW)$ transforms $P'''(x, y)$ into the polynomial $P^{\mathrm{IV}}(x, y) = W\big((a'''/W)x^2+b'''xy+c'''Wy^2+(e'', f'')y\big)+g''$. Clearly $(a'''/W,\ b''',\ c'''W) = 1$. It follows from (7) and (8) that the small and the large discriminant of $P^{\mathrm{IV}}(x, y)$ are equal $\Delta^{\mathrm{IV}} = W^2\Delta'$ and $D^{\mathrm{IV}} = W^2D'$ respectively. Since the form $G_{P^{\mathrm{IV}}}(x, y)/W$ is primitive, P^{IV} is equivalent to a polynomial $P^{\mathrm{V}}(x, y) = ax^2+bxy+cy^2+e^{\mathrm{V}}x+f^{\mathrm{V}}y+g$, where $(a, b, c) = W$, $(ac, \Delta^{\mathrm{V}}) = W^2$, $W\,|\,(e^{\mathrm{V}}, f^{\mathrm{V}})$. Set $|\Delta^{\mathrm{V}}| = \prod p^{\vartheta_p}$, $(\alpha^{\mathrm{V}}, \beta^{\mathrm{V}}) = \prod p^{\mu_p}$ and solve the system of congruences

$$[\bar{a}_3, \bar{b}_3] \equiv \begin{cases} [0, 0]\ (\mathrm{mod}\ p) & \text{if} \quad \nu_p > \mu_p, \\ [-2\alpha^{\mathrm{V}}/\Delta^{\mathrm{V}},\ -2\beta^{\mathrm{V}}/\Delta^{\mathrm{V}}] (\mathrm{mod}\, p) & \text{if} \quad \mu_p = \nu_p > 0, \\ [-b/2a, 1]\ (\mathrm{mod}\, p) & \text{if} \quad \mu_p > \nu_p > 0,\ p \neq 2, \\ [1, 1]\ (\mathrm{mod}\ p) & \text{if} \quad \mu_p > \nu_p > 0,\ p = 2. \end{cases}$$

Hence $p^{\min(\mu_p, \nu_p)}\,\|\,(\alpha^{\mathrm{V}}+\bar{a}_3\Delta^{\mathrm{V}}, \beta^{\mathrm{V}}+\bar{b}_3\Delta^{\mathrm{V}})$ for $p\,|\,\Delta^{\mathrm{V}}$. It follows that there exist integers $\bar{\bar{a}}_3, \bar{\bar{b}}_3$ such that $\big(\alpha^{\mathrm{V}}+(\bar{a}_3+\bar{\bar{a}}_3\Delta^{\mathrm{V}})\Delta^{\mathrm{V}}, \beta^{\mathrm{V}}+(\bar{b}_3+\bar{\bar{b}}_3\Delta^{\mathrm{V}})\Delta^{\mathrm{V}}\big)\,|\,\Delta^{\mathrm{V}}$. Let $a_3 = \bar{a}_3+\bar{\bar{a}}_3\Delta^{\mathrm{V}}$, $b_3 = \bar{b}_3+\bar{\bar{b}}_3\Delta^{\mathrm{V}}$. Hence $P^{\mathrm{V}}(a_3, b_3) \equiv P^{\mathrm{V}}(\bar{a}_3, \bar{b}_3) \equiv g''\big(\mathrm{mod} \prod_{p|\Delta^{\mathrm{V}}} p\big)$. The translation $\varrho(x, y) = (x+a_3, y+b_3)$ transforms P^{V} into a polynomial $P(x, y) = ax^2+bxy+cy^2+ex+fy+g$, where $\Delta = \Delta^{\mathrm{IV}} = \Delta'W^2$, $D = D^{\mathrm{IV}} = D'W^2$, $(ac, \Delta) = (a, b, c)^2$, $(a, b, c)\,|\,(e, f)$, $g = P^{\mathrm{V}}(a_3, b_3)$. By (9) and (10) we get $\alpha = \alpha^{\mathrm{V}}+a_3\Delta^{\mathrm{V}}$, $\beta = \beta^{\mathrm{V}}+b_3\Delta^{\mathrm{V}}$. Hence $(\alpha, \beta)\,|\,\Delta$, $(g, \Delta) = 1$, $P(x, y) \in \mathscr{H}$.

§ 2. Integers represented by quadratic forms. Let $\varphi(x, y) = ax^2+ +bxy+cy^2$ be a primitive quadratic form with the discriminant $\delta = b^2-4ac$ different from a perfect square, $a > 0$, $(a, \delta) = 1$. Put $|\delta| = \prod p^{\vartheta_p}$

($\vartheta_p = 0$ for almost all p), $k(\delta) = \operatorname{sgn}\delta \prod_{2\nmid\vartheta_p} p$ — the square-free kernel of δ. Thus $k(\delta) \neq 1$, $\delta \equiv 0$ or $1 \pmod 4$. Let

$$\mathscr{P} = \left\{p \nmid k(\delta);\ \left(\frac{k(\delta)}{p}\right) = 1\right\},$$

$$\Gamma = \Big\{d;\ d = \prod_{\substack{p\mid\delta\\ p\neq 2,\, \varepsilon_p<\vartheta_p \Rightarrow 2\mid\varepsilon_p\\ p\neq 2,\, \varepsilon_p>\vartheta_p \Rightarrow p\in\mathscr{P}\\ \varepsilon_2+2<\vartheta_2 \Rightarrow 2\mid\varepsilon_2\\ e_2+1=\vartheta_2 \Rightarrow k(\delta)\equiv 3 \,(\mathrm{mod}\, 4)\\ e_2=\vartheta_2 \Rightarrow k(\delta)\equiv 5 \,(\mathrm{mod}\, 8)\\ \varepsilon_2>\vartheta_2 \Rightarrow k(\delta)\equiv 1 \,(\mathrm{mod}\, 8)}} p^{e_p}\Big\}.$$

Then for $d \in \Gamma$ we have $k(d) = \prod_{\vartheta_p\leqslant e_p+1+(-1)^p\equiv 1 \,(\mathrm{mod}\, 2)} p$ and $\varepsilon_p+1+(-1)^p \neq \vartheta_p \Rightarrow \min(\varepsilon_p+1+(-1)^p, \nu_p) \equiv 0 \pmod 2$. Let us set for $d \in \Gamma$

$$\mathscr{L}_d = \{0 < L < |\delta|;\ (L, \delta) = 1\}$$

$$\begin{array}{l} p\neq 2,\, \varepsilon_p<\vartheta_p \Rightarrow \left(\frac{ak(\delta)L}{p}\right) = 1\\ \left.\begin{array}{l} p\neq 2,\, e_p=\vartheta_p\equiv 1 \,(\mathrm{mod}\, 2) \text{ or}\\ p=3,\, 3\mid k(\delta)-1,\, 0<\varepsilon_3=\nu_3\equiv 0 \,(\mathrm{mod}\, 2)\end{array}\right\} \Rightarrow \left(\frac{-ak(\delta d)L}{p}\right) = 1\\ \varepsilon_2=0,\, \vartheta_2=2,\, 4\mid k(\delta)+1 \Rightarrow ak(d)L\equiv 1 \,(\mathrm{mod}\, 4)\\ \varepsilon_2=0,\, \vartheta_2=3 \Rightarrow ak(d)L\equiv 1 \text{ or } 1-k(\delta) \,(\mathrm{mod}\, 8)\\ \varepsilon_2=0,\, \vartheta_2=4 \Rightarrow ak(d)L\equiv 1 \,(\mathrm{mod}\, 4)\\ \varepsilon_2\leqslant\vartheta_2-5 \Rightarrow ak(d)L\equiv 1 \,(\mathrm{mod}\, 8)\\ 0<\varepsilon_2=\vartheta_2-4 \Rightarrow ak(d)L\equiv 5 \,(\mathrm{mod}\, 8)\\ 0<\varepsilon_2=\vartheta_2-3 \Rightarrow ak(d)L\equiv 1-k(\delta) \,(\mathrm{mod}\, 8)\\ 0<\varepsilon_2=\vartheta_2-2\equiv 0 \,(\mathrm{mod}\, 2) \Rightarrow ak(d)L\equiv -k(\delta) \,(\mathrm{mod}\, 4)\\ 0<\varepsilon_2=\vartheta_2-2\equiv 1 \,(\mathrm{mod}\, 2) \Rightarrow ak(d)L\equiv -1 \text{ or } k(\delta)-1 \,(\mathrm{mod}\, 8)\\ 0<\varepsilon_2=\vartheta_2-1 \Rightarrow \tfrac{1}{2}ak(d)L\equiv \tfrac{1}{2}(1-k(\delta)) \,(\mathrm{mod}\, 4).\end{array}$$

LEMMA 4. *For each $L \in \mathscr{L}_d$ the Kronecker symbol $\left(\frac{k(\delta)}{L}\right)$ is defined and equals* 1.

Proof see [4], Theorem 4.

Let R_φ be the genus of φ. The numbers $\psi(x, y)$, where $\psi \in R_\varphi$, $(x, y) = 1$ will be called *represented properly* by the genus of φ.

LEMMA 5. *Let $n = dm > 0$, where $m \equiv L \pmod{|\delta|}$, $(L, \delta) = 1$, $p \mid d \Rightarrow p \mid \delta$. Then n is represented properly by the genus of R_φ if and only if*

$$d \in \Gamma, \tag{18}$$

$$L \in \mathscr{L}_d, \tag{19}$$

$$p \mid m \Rightarrow p \in \mathscr{P}. \tag{20}$$

Proof see [4], Theorem 3.

LEMMA 6. *Let A be an arbitrary integer $\neq 0$. There exists an integer R prime to A such that if n is represented properly by the genus R_φ then $R^2 n = \varphi(x_0, y_0)$, where $(x_0, y_0) \mid R$.*

Proof see [4], p. 231.

§ 3. Lemmata from the analytic number theory.

LEMMA 7 (Bombieri's mean value theorem).

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

Proof see [5].

LEMMA 8 (The $\frac{1}{2}$-dimensional sieve). *Let $\mathscr{M}$ be a finite set of integers, $\mathscr{M}_\lambda = \{m \in \mathscr{M};\ \lambda \mid m\}$, $|\mathscr{M}_\lambda|$ the number of elements of $\mathscr{M}_\lambda$, T a positive integer, Y a real number, $\eta(\lambda, \mathscr{M}) = |\mathscr{M}_\lambda| - Y/\varphi(\lambda T)$, P a set of primes with Dirichlet's density $1/2$, $\mathscr{A}(\mathscr{M};\ z) = \Big|\Big\{m \in \mathscr{M};\ \Big(m, \prod_{\substack{p<z\\ p\in P}} p\Big) = 1\Big\}\Big|$. Let*

$$\sum_{\substack{p\leqslant x\\ p\in P}} p^{-1}\log p = \tfrac{1}{2}\log x + O(1). \tag{21}$$

Then for $1 \leqslant s \leqslant 3 \leqslant y$ we have

$$\mathscr{A}(\mathscr{M};\ y^{1/s}) < 2\sqrt{\frac{e^\gamma}{\pi}}\,\frac{\mathscr{C}}{\varphi(T)}\,Y\log^{-1/2}y + O(Y\log^{-3/5}y) + \sum_{\substack{\lambda<y\\ p\mid\lambda\Rightarrow p\in P}} |\eta(\lambda, \mathscr{M})|,$$

$$\mathscr{A}(\mathscr{M};\ y^{1/s}) > \sqrt{\frac{e^\gamma}{\pi}}\,\frac{\mathscr{C}}{\varphi(T)} \int_1^s \frac{dt}{\big(t(t-1)\big)^{1/2}}\,Y\log^{-1/2}y + O(Y\log^{-3/5}y) - \sum_{\substack{\lambda<y\\ p\mid\lambda\Rightarrow p\in P}} |\eta(\lambda, \mathscr{M})|,$$

where $\mathscr{C} = \lim_{z\to\infty} \prod_{\substack{p<z\\ p\in P}} \left(1 - \frac{\varphi(T)}{\varphi(pT)}\right)\log^{1/2}z$. The constant in O is independent of s, y and Y.

Proof see [4], Corollary 3, p 224.

LEMMA 9. *Let $0 \neq a_1 \neq \pm a_2 \neq 0$, $b_1 \neq \pm b_2$, $(a_i, b_i) = 1$ for $i = 1, 2$, $E = a_1 a_2(a_1 b_2 - a_2 b_1)$ and $w(p)$ be the number of solutions of the congruence*

$$(a_1 x + b_1)(a_2 x + b_2) \equiv 0 \pmod p.$$

Then, if $w(p) < p$ we have for $N \geqslant 2$

$$\sum_{\substack{x\leqslant N\\ |a_i x+b_i|\text{-primes for } i=1,2}} 1 \ll \prod_{p\mid E} \left(1 - \frac{1}{p}\right)^{w(p)-2} N\log^{-2}N,$$

where the constant in the symbol $\ll$ is absolute.

Proof see [7], Theorem 4.2.

LEMMA 10. *If an integer $\Delta \equiv 0, 1 \pmod 4$ is different from a perfect square then there exists a constant $c = c(\Delta)$ such that for all $x > 2$*

$$\sum_{\substack{m \leqslant x \\ q|m \Rightarrow \left(\frac{\Delta}{q}\right)=1}} m^{-1}\log^{-2}\left(3+\frac{x}{m}\right)\prod_{q|m}\left(1-\frac{1}{q}\right)^{-2} < c\log^{-3/2}x.$$

Proof. The lemma follows easily by partial summation from the estimation

$$\sum_{\substack{m \leqslant x \\ q|m \Rightarrow \left(\frac{\Delta}{q}\right)=1}} \prod_{q|m}\left(1-\frac{1}{q}\right)^{2} m^{-1} \leqslant \prod_{\substack{p \leqslant x \\ \left(\frac{\Delta}{p}\right)=1}}\left(1+\frac{1}{p}-\frac{1}{p^2}\right) < \prod_{\substack{p \leqslant x \\ \left(\frac{\Delta}{p}\right)=1}}\left(1-\frac{1}{p}\right)^{-1} \ll \log^{1/2}x.$$

LEMMA 11. *Let $F(x, y) = ax^2+bxy+cy^2$ be an irreducible quadratic form, $a > 0$, $mn \neq 0$. If $F(mx+r, ny+s) \in \mathscr{H}$ then*

$$\sum_{\substack{p \leqslant N \\ p=F(mx+r,\, ny+s)}} 1 \gg N\log^{-1}N.$$

Proof (due to A. Schinzel). Let $\Delta = b^2-4ac = k^2\cdot\Delta_0$, where Δ_0 is a fundamental discriminant. Adding if necessary to r and s suitable multiples of m and n we can assume that $\left(F(r, s), 2akmn\right) = 1$, $F(r, s) > 0$. Then the ideal $\mathfrak{a} = \left(ar+(b+\sqrt{\Delta})s/2\right)\left(a, \dfrac{b+\sqrt{\Delta}}{2}\right)^{-1}$ is prime to $2akmn$. By the theorem on arithmetic progression for the field $Q(\sqrt{\Delta})$ we have

$$\sum_{\substack{\mathfrak{p} \subset Q(\sqrt{\Delta}) \\ N\mathfrak{p}<N,\ \mathfrak{p} \text{ prime of degree } 1 \\ \mathfrak{p}\mathfrak{a}^{-1}=(e),\ e \gg 0 \\ e\equiv 1 \pmod{2akmn}}} 1 \gg N\log^{-1}N,$$

where $N\mathfrak{p}$ denotes the norm. Set $e\left(ar+\dfrac{b+\sqrt{\Delta}}{2}s\right) = (x+y\sqrt{\Delta_0})/2$. Since $e \gg 0$, $x^2-\Delta_0y^2 = 4F(r, s)\cdot Ne > 0$. Hence $x^2-\Delta_0y^2 = 4N\left(\mathfrak{p}\left(a, \dfrac{b+\sqrt{\Delta}}{2}\right)\right)$ $= 4aN\mathfrak{p}$ and the number $\dfrac{x^2-\Delta_0y^2}{4a}$ is a prime. On the other hand, since $e \equiv 1 \pmod{2akmn}$ we have

$$x+\sqrt{\Delta_0}y = 2ar+(b+\sqrt{\Delta})s+2akmn(t+u\sqrt{\Delta_0})$$

where t, u are integers. It can easily be verified that

$$\frac{x^2-\Delta_0y^2}{4a} = F\left(mn(kt-bu)+r,\ 2amnu+s\right),$$

which completes the proof.

§ 4. Proof of (i). In this section we consider polynomials with the small discriminant being a perfect square or the large discriminant being zero. Dirichlet's density of primes represented by these polynomials is positive.

PROPOSITION 1. *Let $P(x, y)$ be an irreducible quadratic polynomial with integer coefficients and the small discriminant being a perfect square* $\neq 0$. *If $P(x, y) \in \mathscr{H}$ then*

$$\sum_{\substack{p \leqslant N \\ p=P(x,y)}} 1 \gg N\log^{-1}N.$$

Proof. See [6] proof of Lemma 16, where the qualitative form of Dirichlet's theorem is to be replaced by the quantitative.

PROPOSITION 2. *Let $P(x, y)$ be a quadratic polynomial with integer coefficients and the small discriminant equal to zero. If $P(x, y) \in \mathscr{H}$ and $P(x, y)$ depends essentially on two variables then*

$$\sum_{\substack{p \leqslant N \\ p=P(x,y)}} 1 \gg N\log^{-1}N.$$

Proof. Since the small discriminant of $P(x, y)$ equals zero, $P(x, y)$ is equivalent to a polynomial $P'(x, y) = a'x^2+e'x+f'y+g'$, $2\nmid g'$. It follows from Lemma 1 that $\beta' = -2a'f' \neq 0$. Since $P'(x, y)$ is primitive there exists an integer x_0 such that $(a'x_0^2+e'x_0+g', f') = 1$. Hence

$$\sum_{\substack{p \leqslant N \\ p=P(x,y)}} 1 = \sum_{\substack{p \leqslant N \\ p=P'(x,y)}} 1 \geqslant \sum_{\substack{p \leqslant N \\ p=P'(x_0,y)}} 1 = \pi(N, |f'|, a'x_0^2+e'x_0+g') \gg N\log^{-1}N,$$

which completes the proof.

PROPOSITION 3. *Let $P(x, y)$ be a quadratic polynomial with integer coefficients, the small discriminant different from a perfect square and the large discriminant equal to zero. If $P(x, y) \in \mathscr{H}$ and P represents a positive integer then*

$$\sum_{\substack{p \leqslant N \\ p=P(x,y)}} 1 \gg N\log^{-1}N.$$

Proof. $P(x, y)$ is equivalent to a polynomial $P'(x, y) = a'x^2+b'xy+$ $+c'y^2+e'x+f'y+g'$, where $g' > 0$, $(g', \Delta') = 1$, $\beta' = b'e'-2a'f' = 0$. Since $D = D' = a'f'^2-b'e'f'+c'e'^2+\Delta'g' = 0$ we have $|e'|+|f'| \neq 0$.

Hence $\alpha' \neq 0$ and $a' = \frac{G_{P'}(\alpha', 0)}{\alpha'^2} = \frac{-\Delta G_{P'}(f', -e')}{\alpha'^2} = \frac{\Delta^2 g'}{\alpha'^2}$. Since a' is an integer and $(g', \Delta) = 1$ we have $\big(\alpha'/(\alpha', \Delta), \Delta\big) = 1$ and $\frac{\alpha'^2}{(\alpha', \Delta)^2} \,|\, g'$. Hence $\Delta \,|\, b'(\alpha', \Delta)$ for $b'\alpha' = \Delta f'$. Proposition 3 follows now from Lemma 11 and the identity

$$P'(x, y) = \frac{g'(\alpha', \Delta)^2}{\alpha'^2}\left(\frac{\Delta}{(\alpha', \Delta)}x + \frac{\alpha'}{(\alpha', \Delta)}\right)^2 + \\ + \frac{b'(\alpha', \Delta')}{\Delta}\left(\frac{\Delta}{(\alpha', \Delta)}x + \frac{\alpha'}{(\alpha', \Delta)}\right)y + c'y^2.$$

§ 5. Reduction of the problem of representation of integers by quadratic polynomials to that of representation by forms. Let $G(x, y) = ax^2 + bxy + cy^2$, $\Delta = b^2 - 4ac \neq 0$, $(ac, \Delta) = 1$, $F(x, y) = G(x, y) + ex + fy$, $\alpha = bf - 2ce$, $\beta = be - 2af$. Since $2a\alpha + b\beta = \Delta e$, $2c\beta + b\alpha = \Delta f$ we have $(2\alpha, \Delta) = (2\beta, \Delta)$. Hence $(\beta, \Delta)\,|\,(\alpha, \Delta)$ or $(\alpha, \Delta)\,|\,(\beta, \Delta)$. Assume that $(\beta, \Delta)\,|\,(\alpha, \Delta)$ and set $\alpha_1 = \alpha/(\beta, \Delta)$, $\beta_1 = \beta/(\beta, \Delta)$, $\Delta_1 = \Delta/(\beta, \Delta)$.

It follows from the identity

$$4aF(x, y) + e^2 = (2ax + by + e)^2 - \Delta y^2 - 2\beta y$$

and from the formulae (11) and (15) that if n is represented by $F(x, y)$ then $4an + e^2$ is a quadratic residue $\operatorname{mod}(2\beta, \Delta)$ and n satisfies the system of equations

$$(22)\qquad \begin{cases} \Delta_1^2 n + G(\alpha_1, \beta_1) = G(x, y), \\ (y, \Delta_1) = 1. \end{cases}$$

For each $d\,|\,\Delta$ and $A \neq 0$ we set

$$r_d = (4d, \Delta/d), \qquad q_{d\gamma} = \frac{4d}{r_d}\gamma^2 - \frac{\Delta}{dr_d} \quad \text{and} \quad Z(A) = \prod_{\substack{d|\Delta \\ d>0}} \prod_{\substack{0<\gamma<|A\Delta| \\ (q_{d\gamma}, A\Delta)=1}} |q_{d\gamma}|.$$

We shall prove

Lemma 12. *Let A be an arbitrary integer $\neq 0$, $Q \equiv 1 \big(\operatorname{mod} (A\Delta)^2\big)$ and $Q \equiv 0 \big(\operatorname{mod} Z(A)\big)$. Then if the number $4an + e^2$ is a quadratic residue* $\operatorname{mod}(2\beta, \Delta)$ *and n is solution of the system of equations*

$$(23)\qquad \begin{cases} \Delta_1^2 n + G(\alpha_1, \beta_1) = Q^2 G(x, y), \\ (y, \Delta_1) = 1 \end{cases}$$

then n is represented by F.

Corollary 1. *Let A and Q be such as in Lemma 12. Then if the number $4an + e^2$ is a quadratic residue* $\operatorname{mod}(2\beta, \Delta)$ *and n is a solution of the system of equations*

$$(24)\qquad \begin{cases} \Delta_1^2 n + G(\alpha_1, \beta_1) = Q^2 G\left(\frac{3 + (-1)^{(\alpha_1, \Delta_1)}}{2} X, Y\right), \\ (X, Y, \Delta_1) = 1 \end{cases}$$

then n is represented by F.

Proof of Corollary 1. We have from (24_1) $\Delta_1^2(4an + e^2) - \Delta\beta_1^2 = Q^2\Big(\big(\big(3 + (-1)^{(\alpha_1, \Delta_1)}\big)aX + bY\big)^2 - \Delta Y^2\Big)$, whence for $p > 2$ we get $p \nmid (Y, \Delta_1)$, since otherwise $p\,|\,X$ contrary to the assumption (24_2). Similarly for $p = 2$ we have $2 \nmid (Y, \Delta_1)$ since otherwise we get from (24_1)

$$\alpha_1 + 1 \equiv G(\alpha_1, \beta_1) \equiv G\left(\frac{3 + (-1)^{\alpha_1}}{2} X, 0\right) \equiv \frac{3 + (-1)^{\alpha_1}}{2} X \pmod 2$$

whence $2 \nmid \alpha_1$, $2\,|\,X$ against the assumption (24_2). Thus $(y, \Delta_1) = 1$ and the numbers $x = \frac{3 + (-1)^{(\alpha_1, \Delta_1)}}{2} X$, $y = Y$ satisfy the system (23).

Corollary 2. *Let us set $\varphi(x, y) = G\left(\frac{3 + (-1)^{(\alpha_1, \Delta_1)}}{2}x, y\right)$, $H(x, y) = WF(x; y) + g$, $\delta = \left(\frac{3 + (-1)^{(\alpha_1, \Delta_1)}}{2}\right)^2 \Delta$-discriminant of the form φ, $\Delta_H = W^2\Delta$ small discriminant of the $H(x, y)$. Let us assume that $W > 0$, $(g, \Delta_H) = 1$, $(\alpha, \beta)\,|\,\Delta$ and φ is positive define if $\delta < 0$. If $n \equiv g \pmod W$, $4a(n - g)/W + e^2$ is a quadratic residue* $\operatorname{mod}(2\beta, \Delta)$ *and moreover the equation $\Delta_1^2 \frac{n - g}{W} + G(\alpha_1, \beta_1) = Q^2\varphi(x, y)$ has a solution x, y such that $(x, y, \Delta_1) = 1$ then n is represented by the polynomial $H(x, y)$.*

Proof of Lemma 12. Consider first the simple case $y = \pm\beta_1$. By (12) and (23_1) we get

$$\Delta_1^2(4an + e^2) - \Delta\beta_1^2 = Q^2\big((2ax + by)^2 - \Delta y^2\big) \equiv (2ax \pm \beta_1 b)^2 - \Delta\beta_1^2 \pmod{\Delta^2}$$

which implies

$$2ax \pm b\beta_1 \equiv \Delta_1 e\left(\operatorname{mod} \frac{3 + (-1)^{\Delta_1}}{2}\,|\Delta_1|\right).$$

Hence using again (12) we have

$$2a(x \mp \alpha_1) = 2ax \pm b\beta_1 - \Delta_1 e \equiv 0\left(\operatorname{mod} \frac{3 + (-1)^{\Delta_1}}{2}|\Delta_1|\right),$$

whence $x \equiv \pm a_1 \pmod{|\Delta_1|}$. Thus the numbers $x = \big(\pm Q(\beta, \Delta)X - a\big)/\Delta$, $y = \big(\pm Q(\beta, \Delta)Y - \beta\big)/\Delta$ are integers and as it can easily be seen, satisfy $n = F(x, y)$ which completes the proof for this case. Assume therefore that $y^2 \neq \beta_1^2$.

Let $4an + e^2 \equiv S^2 \big(\mathrm{mod}\,(2\beta, \Delta)\big)$. Then we get from (23_1)

$$(2ax+by)^2 - \Delta(y^2 - \beta_1^2) \equiv (\Delta_1 S)^2 \left(\mathrm{mod}\, \frac{3+(-1)^{\Delta_1}}{2} \Delta\Delta_1\right). \tag{25}$$

Set $|\Delta| = \prod p^{\varepsilon_p}$, $\bar{\varepsilon}_p = \varepsilon_p - (-1)^p - 1$, $|\Delta_1| = \prod p^{\eta_p}$, $|y - \beta_1| = \prod p^{\varkappa_p}$, $|y+\beta_1| = \prod p^{\lambda_p}$, $|2ax+by| = \prod p^{\nu_p}$ ($\nu_p = \infty$ if $2ax+by = 0$). Hence if $\eta_p > 0$ we have

$$\begin{cases} \varkappa_p \lambda_p = 0, \text{ if } p > 2, \\ \eta_p < \varepsilon_p, 2 \nmid \beta_1 y, (\varkappa_2 > 1 = \lambda_2) \vee (\varkappa_2 = 1 < \lambda_2), \text{ if } p = 2. \end{cases}$$

We divide the set of all primes into six classes

$$\begin{aligned}
A &= \{p;\ \eta_p > 0,\ \varkappa_p \geqslant \eta_p\},\\
B &= \{p;\ \eta_p > 0,\ \varkappa_p < \eta_p,\ \lambda_p \geqslant \eta_p\},\\
C &= \{p;\ \eta_p > 0,\ \varkappa_p < \eta_p,\ \lambda_p < \eta_p,\ 2\nu_p \geqslant \bar{\varepsilon}_p + \varkappa_p + \lambda_p\},\\
D &= \{p;\ \eta_p > 0,\ \varkappa_p < \eta_p,\ \lambda_p < \eta_p,\ 2\nu_p < \bar{\varepsilon}_p + \varkappa_p + \lambda_p,\ \lambda_p \leqslant \varkappa_p\},\\
E &= \{p;\ \eta_p > 0,\ \varkappa_p < \eta_p,\ \lambda_p < \eta_p,\ 2\nu_p < \bar{\varepsilon}_p + \varkappa_p + \lambda_p,\ \varkappa_p < \lambda_p\},\\
F &= \{p;\ \eta_p = 0\} = \{p;\ p \nmid \Delta_1\}.
\end{aligned}$$

By (25) we get

$$\begin{aligned} \eta_p &\leqslant \vartheta_p \quad \text{if} \quad p \in A \cup B \cup D \cup E,\\ 2\vartheta_p &\geqslant \varepsilon_p + \varkappa_p + \lambda_p \equiv 0 \ (\mathrm{mod}\ 2) \quad \text{if} \quad p \in C. \end{aligned}$$

The proof of the lemma will be performed in 4 steps.

I. Construction of the number d. Put

$$\delta_p = \begin{cases} 0, & \text{if} \quad p \in A \cup F,\\ \bar{\varepsilon}_p, & \text{if} \quad p \in B,\\ (\bar{\varepsilon}_p - \varkappa_p + \lambda_p)/2, & \text{if} \quad p \in C,\\ \vartheta_p - \varkappa_p, & \text{if} \quad p \in D,\\ \bar{\varepsilon}_p + \lambda_p - \vartheta_p, & \text{if} \quad p \in E, \end{cases}$$

$$\mu_p = \begin{cases} 0, & \text{if} \quad p \in A \cup B \cup F,\\ (\varepsilon_p - \varkappa_p - \lambda_p)/2, & \text{if} \quad p \in C,\\ \vartheta_p - \varkappa_p + \lambda_p + \dfrac{1+(-1)^p}{2}, & \text{if} \quad p \in D \cup E, \end{cases}$$

$$d = \prod p^{\delta_p}, \qquad r_d = \left(4d, \frac{\Delta}{d}\right).$$

Thus the numbers δ_p, μ_p are integers and it can easily be seen that

$$\begin{gathered} 0 \leqslant \delta_p \leqslant \varepsilon_p, \qquad d \mid \Delta,\\ 0 \leqslant \mu_p \leqslant \vartheta_p, \qquad r_d = (4, \Delta) \prod p^{\mu_p} \mid 4(2ax+by). \end{gathered}$$

II. Construction of the number γ. Let

$$\gamma^{\pm} = -\frac{2ax+by \pm \Delta_1 S}{2d(y-\beta_1)}, \qquad \gamma_{\pm} = -\frac{2d(2ax+by \pm \Delta_1 S)}{\Delta(y+\beta_1)}.$$

It follows from (25) that for $p \in D \cup E$, $p^{\nu_p} \| \Delta_1 S$ thus the numbers $\gamma^{\pm}, \gamma_{\pm}$ are p-adic integers and one of the numbers $\gamma^+\gamma_+, \gamma^+\gamma_-, \gamma^-\gamma_+, \gamma^-\gamma_-$ is not divisible by p (for $p = 2$ exactly one). Similarly for $p \in C$ we have from (25) $p^{(\varepsilon_p + \varkappa_p + \lambda_p)/2} \mid \Delta_1 S$ thus numbers $\gamma^{\pm}, \gamma_{\pm}$ are p-adic integers. For every prime p we define auxiliary numbers γ_p:

$$\gamma_p = \begin{cases} 0, & \text{if} \quad p \in A \cup B \cup F, p = 2 = \varepsilon_2,\\ 1, & \text{if} \quad p \in A \cup B \cup F, (p \neq 2) \vee (\varepsilon_p \neq 2); \end{cases}$$

$$\gamma_p = \begin{cases} \gamma^+, & \text{if} \quad p \in D, p \nmid \gamma^+,\\ \gamma^-, & \text{if} \quad p \in D, p \mid \gamma^+; \end{cases}$$

$$\gamma_p = \begin{cases} \gamma^+, & \text{if} \quad p \in C, p \nmid q_{d\gamma^+},\\ \gamma^-, & \text{if} \quad p \in C, p \mid q_{d\gamma^+}; \end{cases}$$

$$\gamma_p = \begin{cases} 1/\gamma_+, & \text{if} \quad p \in E, p \nmid \gamma_+,\\ 1/\gamma_-, & \text{if} \quad p \in E, p \mid \gamma_+. \end{cases}$$

Hence for $p \in D \cup E$ we have $p \nmid \gamma_p$. Since γ_p are p-adic integers there exists a positive integer $\gamma < |A\Delta|$ satisfying the system of congruences

$$\begin{aligned} \gamma &\equiv \gamma_p \ (\mathrm{mod}\ p^{\varepsilon_p}) \quad &&\text{for} \quad p \mid \Delta,\\ \gamma &\equiv 0 \ (\mathrm{mod}\ p) &&\text{for} \quad p \mid A, p \nmid \Delta. \end{aligned}$$

III. Proof of the formula $(q_{d\gamma}, A\Delta) = 1$. It is enough to show that for $p \mid \Delta$ we have

$$p \nmid q_{d\gamma_p}. \tag{26}$$

If $p \in A \cup B \cup F$, $(p \neq 2) \vee (\varepsilon_p \neq 2)$ then

$$q_{d\gamma_p} = \frac{4d}{r_d} - \frac{\Delta}{dr_d} \equiv \frac{4d}{r_d} \not\equiv 0 \ (\mathrm{mod}\ p).$$

If $p \in A \cup B \cup F$, $p = 2 = \varepsilon_2$ then

$$q_{d\gamma_p} = -\frac{\Delta}{dr_d} \equiv 1 \ (\mathrm{mod}\ 2).$$

If $p \in C$ then the number $\omega = \dfrac{2(y-\beta_1)\Delta}{dr_d(y-\beta_1)^2}$ is a p-adic unit. We get from (25)

$$q_{d\gamma\pm} = \frac{2(2ax+by)(2ax+by\pm\Delta_1 S)-2y(y-\beta_1)\Delta}{dr_d(y-\beta_1)^2} - \frac{[(2ax+by)^2-\Delta(y^2-\beta_1^2)-(\Delta_1 S)^2]}{dr_d(y-\beta_1)^2}$$
$$\equiv \frac{2(2ax+by)(2ax+by\pm\Delta_1 S)}{dr_d(y-\beta_1)^2} - \omega y \pmod{p^{\eta_p-\varkappa_p}},$$

$$\frac{1}{2}\left(1+\frac{\Delta_1 S}{2ax+by}\right)q_{d\gamma+} + \frac{1}{2}\left(1-\frac{\Delta_1 S}{2ax+by}\right)q_{d\gamma-}$$
$$= \frac{2\beta_1(y-\beta_1)\Delta+[(2ax+by)^2-\Delta(y^2-\beta_1^2)-(\Delta_1 S)^2]}{dr_d(y-\beta_1)^2} \equiv \omega\beta_1 \pmod{p^{\eta_p-\varkappa_p}}.$$

Hence if $2\nu_p > \varepsilon_p+\varkappa_p+\lambda_p$ or $2\nu_p = \varepsilon_p+\varkappa_p+\lambda_p$, $p = 2$ the first congruence gives $q_{d\gamma\pm} \equiv -\omega y \not\equiv 0 \pmod{p}$ and if $2\nu_p = \varepsilon_p+\varkappa_p+\lambda_p$, $p \neq 2$ the second congruence implies that one of the numbers $q_{d\gamma\pm}$ is not divisible by p. This proves (26).

If $p \in D$ then $\delta_p < \bar{\varepsilon}_p/2$ thus

$$q_{d\gamma_p} \equiv \frac{4d}{r_d}\gamma_p^2 \not\equiv 0 \pmod{p}.$$

If $p \in E$ then $\delta_p > \bar{\varepsilon}_p/2$ thus

$$q_{d\gamma_p} \equiv -\frac{\Delta}{dr_d} \not\equiv 0 \pmod{p}.$$

IV. Conclusion of the proof. Put

$$X' = \left(\frac{4d}{r_d}\gamma^2+\frac{\Delta}{dr_d}\right)x - \frac{4(2cy+bx)}{r_d}\gamma, \tag{27}$$

$$Y' = \left(\frac{4d}{r_d}\gamma^2+\frac{\Delta}{dr_d}\right)y + \frac{4(2ax+by)}{r_d}\gamma. \tag{28}$$

It is easy to verify the identity

$$G(X', Y') = q^2 G(x, y) \qquad (q = q_{d\gamma}). \tag{29}$$

The number Y' is an integer since $r_d \mid 4(2ax+by)$. Since $r_d \mid \Delta$ and $(a, \Delta) = 1$ it follows from (29) that X' is also an integer. We shall prove the congruences

$$X' \equiv q\alpha_1 \pmod{|\Delta_1|}, \tag{30}$$

$$Y' \equiv q\beta_1 \pmod{|\Delta_1|}. \tag{31}$$

Let $p \in A$. Then

$$Y'-q\beta_1 = q(y-\beta_1)+\frac{2\Delta}{dr_d}y+\frac{4(2ax+by)}{r_d}\gamma \equiv 0+0+0 \equiv 0 \pmod{p^{\eta_p}}.$$

Let $p \in B$. Then

$$Y'-q\beta_1 = -q(y+\beta_1)+\frac{8d}{r_d}y\gamma^2+\frac{4(2ax+by)}{r_d}\gamma \equiv 0+0+0 \equiv 0 \pmod{p^{\eta_p}}.$$

Let $p \in C \cup D$. Then

$$dr_d(y-\beta_1)(Y'-q\beta_1) = \big(2d(y-\beta_1)\gamma+2ax+by\big)^2-(2ax+by)^2+\Delta(y^2-\beta_1^2)$$
$$\equiv \big(2d(y-\beta_1)\gamma_p+2ax+by\big)^2-(2ax+by)^2+\Delta(y^2-\beta_1^2)$$
$$= (\Delta_1 S)^2-(2ax+by)^2+\Delta(y^2-\beta_1^2) \pmod{p^{\varepsilon_p+\min(\varepsilon_p+\varkappa_p+\lambda_p,2\nu_p)}}.$$

Hence by (25) we get

$$dr_d(y-\beta_1)(Y'-q\beta_1) \equiv 0 \pmod{p^{\varepsilon_p+\eta_p+\frac{1+(-1)^p}{2}}}. \tag{32}$$

Since $p^{\varepsilon_p+\frac{1+(-1)^p}{2}} \| dr_d(y-\beta_1)$ we have

$$Y'-q\beta_1 \equiv 0 \pmod{p^{\eta_p}}.$$

Let $p \in E$. Then

$$\frac{\Delta}{d}r_d(y+\beta_1)(Y'-q\beta_1) \tag{33}$$
$$= 4\gamma^2\left[\left(\frac{\Delta}{2d\gamma}(y+\beta_1)+2ax+by\right)^2-(2ax+by)^2+\Delta(y^2-\beta_1^2)\right]$$
$$\equiv 4\gamma^2\left[\left(\frac{\Delta}{2d\gamma_p}(y+\beta_1)+2ax+by\right)^2-(2ax+by)^2+\Delta(y^2-\beta_1^2)\right]$$
$$= 4\gamma^2[(\Delta_1 S)^2-(2ax+by)^2+\Delta(y^2-\beta_1^2)] \pmod{p^{\varepsilon_p+2\nu_p+1+(-1)^p}}.$$

Hence by (25) we get

$$\frac{\Delta}{d}r_d(y+\beta_1)(Y'-q\beta_1) \equiv 0 \pmod{p^{\varepsilon_p+\eta_p+1+(-1)^p}}.$$

Since $p^{2(\nu_p+1+(-1)^p)-\lambda_p} \| \frac{\Delta}{d}r_d(y+\beta_1)$ and $2(\nu_p+1+(-1)^p)-\lambda_p \leqslant \varepsilon_p+1+(-1)^p$ we have $Y'-q\beta_1 \equiv 0 \pmod{p^{\eta_p}}$. This completes the proof of (31).

It follows from (23_1) and the identity (29) that

$$G(X', Y') = q^2 G(x, y) \equiv q^2 Q^2 G(x, y)$$
$$\equiv q^2\big(\Delta_1^2 n+G(\alpha_1, \beta_1)\big) \equiv q^2 G(\alpha_1, \beta_1) \pmod{\Delta_1^2},$$

whence

$$(2aX'+bY')^2-\Delta Y'^2 \equiv q^2\big((\Delta_1 e)^2-\Delta\beta_1^2\big) \pmod{(2\Delta_1)^2}.$$

Hence by (31) we have

$$2aX'+bY' \equiv \Delta_1 e\left(\operatorname{mod}\frac{3+(-1)^{\Delta_1}}{2}|\Delta_1|\right),\quad bY' \equiv bq\beta_1\left(\operatorname{mod}\frac{3+(-1)^{\Delta_1}}{2}|\Delta_1|\right).$$

Since $2a\alpha_1+b\beta_1 = \Delta_1 e$ and $(a, \Delta_1) = 1$ it follows that $X' \equiv q\alpha_1 \pmod{|\Delta_1|}$.

We have proved in III that $q|Q$ thus the numbers $X = (\beta, \Delta)QX'/q$, $Y = (\beta, \Delta)QY'/q$ are integers and it is easy to verify that

$$X \equiv (\beta, \Delta)Q/q\cdot q\alpha_1 = Q\alpha \equiv \alpha \pmod{|\Delta|},$$
$$Y \equiv (\beta, \Delta)Q/q\cdot q\beta_1 = Q\beta \equiv \beta \pmod{|\Delta|},$$
$$G(X, Y) = \big((\beta, \Delta)Q/q\big)^2 G(X', Y') = \big((\beta, \Delta)Q\big)^2 G(x, y)$$
$$= (\beta, \Delta)\big(\Delta_1^2 n+G(\alpha_1, \beta_1)\big) = \Delta^2 n+G(\alpha, \beta).$$

Hence $n = F\left(\dfrac{X-\alpha}{\Delta}, \dfrac{Y-\beta}{\Delta}\right)$.

§ 6. Primes represented by a polynomial $H(x, y)$. The main lemma in the proof of part (ii) of Theorem 1 is the following

LEMMA 13. *If the small discriminant of a polynomial $H(x, y)$ is different from a perfect square and the large discriminant is different from zero then under the assumption of Corollary 2 to Lemma 12 we have the inequality*

$$\sum_{\substack{p\leqslant N\\ p=H(x,y)}} 1 \gg N\log^{-3/2}N.$$

Proof. Let R and Q be integers defined in Lemmata 6 and 12 respectively for the number $A = \Delta_H D_H = W^4\big(g\Delta^2-WG(\alpha, \beta)\big)$, where D_H is the large discriminant of $H(x, y)$. Then $(C, \Delta_H D_H) = 1$, where $C = \dfrac{3-(-1)^{\Delta D_H}}{2}QR$. Since $(\alpha, \beta)|\Delta$ we have $(\alpha_1, \beta_1) = 1$. Hence the number $G(\alpha_1, \beta_1)$ is represented properly by the form $\varphi(x, y)$. Let d be the greatest divisor of $G(\alpha_1, \beta_1)$ all prime factors of which divide δ and define L by the congruence $C^2L \equiv G(\alpha_1, \beta_1)/d \pmod{|\delta|}$, $0 < L < |\delta|$. Then $d\in\Gamma$ and $L\in\mathscr{L}_d$. It follows hence by Lemmata 6 and 7 that numbers C^2dm, where $m \equiv L \pmod{|\delta|}$, $p|m \Rightarrow p\in\mathscr{P}$ are of the form $Q^2\varphi(x, y)$, where $(x, y)|R$ and *a fortiori* $(x, y, \Delta_1) = 1$.

Since $4aG(\alpha_1, \beta_1) = \Delta_1^2 e^2-\Delta\beta_1^2$ we have $(\Delta_1^2, \Delta)|(4, \Delta)d$. Hence $(2\beta, \Delta)\Delta_1^2|4d\delta$. From the definition of d and L we get $C^2dL \equiv G(\alpha_1, \beta_1) \pmod{|\delta d|}$ thus

$$4a\frac{C^2dL-G(\alpha_1, \beta_1)}{\Delta_1^2} \equiv \big(\operatorname{mod}(2\beta, \Delta)\big). \tag{34}$$

Let $T = C^2W\dfrac{|d\delta|}{\Delta_1^2}$ and $l = W\dfrac{C^2dL-G(\alpha_1, \beta_1)}{\Delta_1^2}+g$. It follows from (34) that for $n \equiv l \pmod{T}$ the number $4a(n-g)/W+e^2$ is a quadratic residue $\big(\operatorname{mod}(2\beta, \Delta)\big)$ and $n \equiv g \pmod{W}$. Put

$$\mathscr{M} = \{m;\ \Delta_1^2(p-g)/W+G(\alpha_1, \beta_1) = C^2dm,\ p \equiv l \pmod{T},\ |A| < p \leqslant N\}.$$

For $m\in\mathscr{M}$ we have $m \equiv L(\operatorname{mod}|\delta|)$. Hence by Corollary 2 to Lemma 12 we get

$$\sum_{\substack{p\leqslant N\\ p=H(x,y)}} 1 \geqslant \sum_{\substack{m\in\mathscr{M}\\ p|m\Rightarrow p\in\mathscr{P}}} 1. \tag{35}$$

The sum $\sum_{\substack{m\in\mathscr{M}\\ p|m\Rightarrow p\in\mathscr{P}}} 1$ will be estimated by the method of the $\frac{1}{2}$-dimensional sieve. For $m\in\mathscr{M}$ we have

$$(m, \Delta D_H/W^2) = 1. \tag{36}$$

Let

$$(\lambda, \Delta D_H/W^2) = 1,\qquad L_\lambda \equiv \begin{cases} L \pmod{|\delta|},\\ 0 \pmod{|\lambda|}\end{cases}$$

and put

$$l_\lambda = W\frac{C^2dL_\lambda-G(\alpha_1, \beta_1)}{\Delta_1^2}+g.$$

Hence

$$(l_\lambda, \lambda T) = 1. \tag{37}$$

Let $\mathscr{M}_\lambda = \{m\in\mathscr{M};\ \lambda|m\}$. By the definition of l_λ we get

$$\mathscr{M}_\lambda = \{m;\ \Delta_1^2(p-g)/W+G(\alpha_1, \beta_1) = C^2dm,\ p \equiv l_\lambda \pmod{\lambda T},\ |A| < p \leqslant N\}.$$

Hence the number of elements of $\mathscr{M}_\lambda$ equals

$$|\mathscr{M}_\lambda| = \pi(N, \lambda T, l_\lambda)-\pi(|A|, \lambda T, l_\lambda). \tag{38}$$

Put in Lemma 8

$$Y = \operatorname{Li}N,\quad y = \sqrt{N}/T\log^{15}N,\quad P = \left\{p\nmid \Delta D_H/W^2;\ \left(\frac{k(\delta)}{p}\right) = -1\right\}.$$

Since $k(\delta) \neq 1$ P has the property (21). If $(\lambda, \Delta D_H/W^2) = 1$ we get from (38)

$$\eta(\lambda, \mathscr{M}) = \pi(N, \lambda T, l_\lambda)-\pi(|A|, \lambda T, l_\lambda)-\operatorname{Li}N/\varphi(\lambda T).$$

Hence by (37) and Lemma 7 we have the estimation

$$\sum_{\substack{\lambda<y\\ p|\lambda\Rightarrow p\in P}} |\eta(\lambda, \mathscr{M})| \ll N\log^{-2}N.$$

It follows by Lemma 8

(39)
$$\mathscr{A}(\mathscr{M};\ N^{1/2s}) \geqslant \sqrt{\frac{2e^{\gamma}}{\pi}}\,\frac{\mathscr{C}}{\varphi(T)}\int\limits_{1}^{s}\frac{dt}{\sqrt{t(t-1)}}\,N\log^{-3/2}N + O(N\log^{-8/5}N),$$

where

$$\mathscr{C} = \lim_{z\to\infty}\prod_{\substack{p<z\\ p\nmid \Delta D_H/W^2\\ (\delta/p)=-1}}\left(1-\frac{\varphi(T)}{\varphi(pT)}\right)\sqrt{\log z}$$

$$= e^{-\gamma/2}\prod_{\substack{p\nmid T\Delta D_H/W^2\\ (\Delta/p)=-1}}\left(1-\frac{1}{(p-1)^2}\right)\prod_{p\nmid \Delta D_H/W^2}\left(1-\frac{1}{p}\right)^{-\left(\frac{\Delta}{p}\right)/2}\prod_{p\mid \Delta D_H/W^2}\left(1-\frac{1}{p}\right)^{-1/2} > 0.$$

Since $|\delta|$ is the conductor of the character $\left(\frac{k(\delta)}{\cdot}\right)$ we have by Lemma 4 for $m\in\mathscr{M}$ the equality $\left(\frac{k(\delta)}{m}\right) = \left(\frac{k(\delta)}{L}\right) = 1$. Thus the number of the prime factors of m not belonging to $\mathscr{P}$ is even. In particular if $1\leqslant s<2$ and N is large enough we have

(40)
$$\sum_{\substack{m\in\mathscr{M}\\ p\mid m\Rightarrow p\in\mathscr{P}}} 1 = \mathscr{A}(\mathscr{M};\ N^{1/2s}) - \sum_{\substack{N^{1/2s}\leqslant p_1\leqslant p_2\\ p_1,p_2\in P}}\mathscr{A}(\mathscr{M}_{p_1p_2};\ N^{1/2s}).$$

Put $M = \big(\Delta_1^2(N-g)+WG(\alpha_1,\beta_1)\big)/WC^2d$. Then for $m\in\mathscr{M}$ we have $m\leqslant M$ hence

(41)
$$\sum_{\substack{N^{1/2s}\leqslant p_1<p_2\\ p_1,p_2\in P}}\mathscr{A}(\mathscr{M}_{p_1p_2};\ N^{1/2s})$$
$$\leqslant \sum_{\substack{m\leqslant MN^{-1/s}\\ q\mid m\Rightarrow q\in\mathscr{P}}}\ \sum_{\substack{N^{1/2s}\leqslant p_1\leqslant\sqrt{M}\\ p_1\in P}}\ \sum_{\substack{p\leqslant N\\ p\equiv l_{p_1m}\,(\mathrm{mod}\,p_1mT)\\ \Delta_1^2(p-g)+WG(\alpha_1,\beta_1)=WC^2d_{p_1p_2m}}} 1 = \Sigma\Sigma\Sigma_1.$$

The inner sum can be written in the form

(42)
$$\Sigma_1 = \sum_{\substack{x\leqslant N/p_1mT\\ p_1mTx+l_{p_1m}\ \text{prime}\\ |\delta|x+\frac{\Delta_1^2l_{p_1m}+WG(\alpha_1,\beta_1)-\Delta_1^2g}{WC^2dp_1m}\ \text{prime}}} 1.$$

Put in Lemma 9

$$a_1 = p_1mT,\quad b_1 = l_{p_1m},\quad a_2 = |\delta|,\quad b_2 = \frac{\Delta_1^2l_{p_1m}+WG(\alpha_1,\beta_1)-\Delta_1^2g}{WC^2dp_1m}.$$

Then $E = p_1mTD_H\delta^2/\Delta W^2 = p_1mE_0$. Let us remark that for $p\mid m$ we have $w(p)=1$. Hence by Lemma 9 we get

(43)
$$\Sigma_1 \ll \frac{N}{p_1mT\log^2(N/p_1mT)}\prod_{\substack{p\mid m\\ p\nmid E_0}}\left(1-\frac{1}{p}\right)^{-1}\prod_{p\mid E_0}\left(1-\frac{1}{p}\right)^{w(p)-2},$$

where the constant in the symbol $\ll$ is absolute. We get from (41) and (43)

(44)
$$\sum_{\substack{N^{1/2s}\leqslant p_1<p_2\\ p_1,p_2\in P}}\mathscr{A}(\mathscr{M}_{p_1p_2};\ N^{1/2s})$$
$$\ll \prod_{p\mid E_0}\left(1-\frac{1}{p}\right)^{w(p)-2}\frac{N}{T\log^2N}\sum_{\substack{m<N^{1-1/s}\\ q\mid m\Rightarrow q\in\mathscr{P}}}\frac{1}{m}\prod_{\substack{p\mid m\\ p\nmid E_0}}\left(1-\frac{1}{p}\right)^{-1}\sum_{\substack{N^{1/2s}<p<N^{1/2}\\ p\in P}}p^{-1}$$
$$< c(\Delta, D_H, \delta, W, d, C)\sqrt{\frac{s-1}{s}}\log s\ N\log^{-3/2}N.$$

Since $\int\limits_1^s\frac{dt}{(t(t-1))^{1/2}} > 2\sqrt{\frac{s-1}{s}}$ it follows from (39)–(41) and (44) that for a sufficiently small number $s-1 = s(\Delta, D, \delta, W, d, C)$ we get $\sum\limits_{\substack{m\in\mathscr{M}\\ p\mid m\Rightarrow p\in\mathscr{P}}} 1 \gg N\log^{-3/2}N$ which completes the proof of Lemma 13.

§ 7. Proof of the part (ii) of Theorem 1.

We have to prove

PROPOSITION 4. *Let $P(x,y)$ be a polynomial of degree 2 with integral coefficients, the little discriminant different from a perfect square and the great discriminant different from zero. If $P(x,y)\in\mathscr{H}$ and P represents arbitrarily large positive integers then*

$$N\log^{-3/2}N \ll \sum_{\substack{p\leqslant N\\ p=P(x,y)}} 1 \ll N\log^{-3/2}N.$$

Proof. By Lemmata 4 and 13 we get

$$\sum_{\substack{p\leqslant N\\ p=P(x,y)}} 1 \gg \sum_{\substack{p\leqslant N\\ p=P(x,y)}} 1 \gg N\log^{-3/2}N.$$

On the other hand by (15)

$$\sum_{\substack{p\leqslant N\\ p=P(x,y)}} 1 = \sum_{\substack{p\leqslant N\\ \Delta^2p-\Delta D=G_P(\Delta x+\alpha,\Delta y+\beta)}} 1 \leqslant \sum_{\substack{p\leqslant N\\ \left.\begin{array}{l} q^{2k+1}\|\Delta p-D\\ q\nmid\Delta\end{array}\right\}\Rightarrow\left(\frac{\Delta}{q}\right)=1}} 1$$
$$= \sum_{\substack{0<d\leqslant M\\ q\mid d\Rightarrow q\mid\Delta\\ (d,\Delta D/(\Delta,D)^2)=1}}\ \sum_{\substack{0<r\leqslant\sqrt{M/d}\\ (r,\Delta)=1}}\ \sum_{\substack{0<m<M/dr^2\\ |\mu(m)|=1,\,q\mid m\Rightarrow\left(\frac{\Delta}{q}\right)=1}}\ \sum_{\substack{p\leqslant N\\ \Delta p-D=(\Delta,D)dr^2mp'}} 1 = \Sigma\Sigma\Sigma\Sigma_2$$

where $M = |\Delta N - D|/(\Delta, D)$. Let l be a solution of the congruence $(\Delta, D)dr^2ml \equiv -D \pmod{|\Delta|}$ and set in Lemma 9 $a_1 = \Delta/(\Delta, D)$, $b_1 = l$, $a_2 = dr^2m$, $b_2 = \big((\Delta, D)dr^2ml + D\big)/\Delta$. Hence $E = a_1a_2(a_1b_2 - a_2b_1) = \Delta D/(\Delta, D)^2dr^2m$ and we get from the said lemma

$$\Sigma_2 = \sum_{\substack{0 < x \leqslant \frac{(M/dr^2m - l)(\Delta, D)}{|\Delta|} \\ |a_ix+b_i| \text{ primes for } i=1,2}} 1 \ll \frac{M(\Delta, D)}{dr^2m|\Delta|}\log^{-2}\left(\frac{M(\Delta, D)}{dr^2m|\Delta|} + 3\right) \times$$

$$\times \prod_{p \mid \frac{\Delta D dr^2m}{(\Delta, D)^2}} \left(1 - \frac{1}{p}\right)^{w(p)-2} \ll \frac{M}{dr^2m}\log^{-2}\left(\frac{M}{dr^2m} + 3\right) \prod_{p \mid drm} \left(1 - \frac{1}{p}\right)^{-2}.$$

The constant in the symbol $\ll$ is absolute. Hence by Lemma 10 we get

$$\sum_{\substack{p \leqslant N \\ p = P(x,y)}} 1 \ll \sum_d \sideset{}{^*}\sum_r \frac{M}{dr^2}\log^{-3/2}\left(\frac{M}{dr^2} + 3\right) \ll M\log^{-3/2}M \ll N\log^{-3/2}N$$

and the proof is complete.

Note concerning paper [3]. [3] contains an outline of the proof of (ii) for the case where the small discriminant of $P(x, y)$ is fundamental. The proof given there is based on the estimation

$$N\log^{-3/2}N \ll \sum_{\substack{p \leqslant N \\ Ap+B = C\varphi(x,y)}} 1 \ll N\log^{-3/2}N,$$

where φ is a primitive quadratic form with the discriminant Δ different from a perfect square and the constants A, B, C different from zero satisfy suitable arithmetic conditions. Some of those conditions have been omitted in [3] and as a result the necessary (and obvious) condition that P should represent odd integer is missing in the formulation of the theorem. Generalizing the considerations of § 6 of the present paper we shall show

THEOREM 3. *Let φ be a primitive quadratic form with discriminant Δ different from a perfect square, positive definite if $\Delta < 0$ and let $A > 0$, $B \neq 0$, $C > 0$. If there exist integer g, t_1, t_2 such that*

$$Ag + B = C\varphi(t_1, t_2),$$

$$\big(g, 2B\Delta/(A, \Delta B)\big) = 1$$

then

$$N\log^{-3/2}N \ll \sum_{\substack{p \leqslant N \\ Ap+B = C\varphi(x,y)}} 1 \ll N\log^{-3/2}N.$$

Put $r = (t_1, t_2)R$, $\varphi(t_1, t_2) = (t_1, t_2)^2dL$. It follows from Lemmata 5 and 6 that

$$\sum_{\substack{p \leqslant N \\ Ap+B = C\varphi(x,y)}} 1 \geqslant \sum_{\substack{p \leqslant N \\ Ap+B = CR^2\psi(x,y) \\ \psi \in R_\varphi}} 1 \geqslant \sum_{\substack{p \leqslant N \\ Ap+B = Cr^2dm \\ m \equiv L \,(\mathrm{mod}\, |\Delta|) \\ q|m \Rightarrow \left(\frac{\Delta}{q}\right) = 1}} 1 = \Sigma_3. \tag{45}$$

The sum Σ_3 is estimated as in § 6 using the method of $\frac{1}{2}$-dimensional sieve.

Let us consider the system of conditions

$$\begin{cases} Ag + B = Cr^2dm, \\ m \equiv L \pmod{|\Delta|}, \\ q \mid m \Rightarrow \left(\dfrac{\Delta}{q}\right) = 1. \end{cases} \tag{46}$$

It implies that $(A, B)/(A, B, Cr^2d) \mid m$, hence

$$q \mid (A, B)/(A, B, Cr^2d) \Rightarrow \left(\frac{\Delta}{q}\right) = 1, \tag{47}$$

$$\big(Cr^2d/(A, B, Cr^2d),\ AB/(A, B)^2\big) = 1 \tag{48}$$

since g is prime to $B/(A, B)$. Let L_1 be a solution of the congruence $(A, B)L_1/(A, B, Cr^2d) \equiv L \pmod{|\Delta|}$ and put $m_1 = m(A, B, Cr^2d)/(A, B)$. We get from (46)

$$\begin{aligned} \frac{A}{(A, B)}g &= \frac{Cr^2d}{(A, B, Cr^2d)}m_1 - \frac{B}{(A, B)} \\ &\equiv \frac{Cr^2dL_1}{(A, B, Cr^2d)} - \frac{B}{(A, B)} \left(\mathrm{mod}\ \frac{Cr^2d|\Delta|}{(A, B, Cr^2d)}\right). \end{aligned} \tag{49}$$

Put $T = \dfrac{Cr^2d}{(A, B, Cr^2d)}\dfrac{\Delta(A, B)}{(A, \Delta B)}$. Since $\left(g, \dfrac{\Delta(A, B)}{(A, \Delta B)}\right) = 1$ we get from (49)

$$\left(\frac{Cr^2dL_1}{(A, B, Cr^2d)} - \frac{B}{(A, B)}, \frac{(A, \Delta B)}{(A, B)}T\right) = \frac{(A, \Delta B)}{(A, B)}. \tag{50}$$

(46) implies also the condition

$$\Delta \equiv 5 \pmod 8 \Rightarrow 2 \mid \frac{Cr^2d}{(A, B, Cr^2d)}\frac{AB}{(A, B)^2} \tag{51}$$

since $2 \nmid g$. We shall prove

LEMMA 14. *We have $\Sigma_3 \geqslant N\log^{-3/2}N$.*

Proof of Lemma 14. Let l be a solution of the congruence

$$\frac{A}{(A,B)}\,l \equiv \left(\frac{Cr^2dL_1}{(A,B,Cr^2d)} - \frac{B}{(A,B)}\right)\frac{(A,B)}{(A,\Delta B)} \pmod{T}.$$

By (50) we have $(l,T) = 1$. Put

$$\mathcal{M} = \Big\{m_1;\ \frac{A}{(A,B)}p + \frac{B}{(A,B)} = \frac{Cr^2d}{(A,B,Cr^2d)}m_1;\ p \equiv l \,(\mathrm{mod}\, T),\ |AB| < p \leqslant N\Big\}.$$

Then for $m_1 \in \mathcal{M}$ we have

$$m_1 \equiv L_1 \,(\mathrm{mod}\,|\Delta|), \tag{52}$$

$$\big(m_1,\ \Delta AB/(A,B)^2\big) = 1. \tag{53}$$

Let $\big(\lambda, \Delta AB/(A,B)^2\big) = 1$, $\lambda > 0$, $\mathcal{M}_\lambda = \{m_1 \in \mathcal{M};\ \lambda \mid m_1\}$. The system of congruences

$$\begin{aligned} l_\lambda &\equiv l \,(\mathrm{mod}\, T),\\ \frac{A}{(A,B)}l_\lambda &\equiv \frac{-B}{(A,B)}\left(\mathrm{mod}\ \frac{Cr^2d}{(A,B,Cr^2d)}\lambda\right) \end{aligned} \tag{54}$$

is consistent and has a solution l_λ determined uniquely modulo λT. Clearly

$$(l_\lambda, \lambda T) = 1. \tag{55}$$

It is easy to see that

$$\mathcal{M}_\lambda = \Big\{m_1 \in \mathcal{M};\ \frac{A}{(A,B)}p + \frac{B}{(A,B)} = \frac{Cr^2d}{(A,B,Cr^2d)}m_1;\ p \equiv l_\lambda (\mathrm{mod}\ \lambda T),\ |AB| < p \leqslant N\Big\}.$$

Hence

$$|\mathcal{M}_\lambda| = \pi(N, \lambda T, l_\lambda) - \pi(|AB|, \lambda T, l_\lambda).$$

By (47) and (52) we have

$$\left(\frac{k(\Delta)}{m_1}\right) = \left(\frac{k(\Delta)}{L_1}\right) = \left(\frac{k(\Delta)}{\dfrac{(A,B)L_1}{(A,B,Cr^2d)}}\right) = \left(\frac{k(\Delta)}{L}\right) = 1.$$

It follows that the number of prime factors $p \notin \mathcal{P} = \left\{p \nmid \frac{\Delta AB}{(A,B)^2};\ \left(\frac{\Delta}{p}\right) = 1\right\}$ of m_1 is even. Hence, as in § 6 we get for $s \in (1, 2)$ and N large enough

$$\Sigma_3 = \mathcal{A}(\mathcal{M}; N^{1/2s}) - \sum_{\substack{p_2 \geqslant p_1 \geqslant N^{1/2s}\\ p_1, p_2 \notin \mathcal{P}}} \mathcal{A}(\mathcal{M}_{p_1p_2}; N^{1/2s}). \tag{56}$$

In order to estimate $\mathcal{A}(\mathcal{M}; N^{1/2s})$ we shall use Lemma 9. We set in the said lemma

$$Y = \mathrm{Li}\,N, \quad y = \sqrt{N}/T\log^{15}N, \quad P = \left\{p \nmid \frac{\Delta AB}{(A,B)^2};\ \left(\frac{\Delta}{p}\right) = -1\right\}.$$

Since Δ is not a perfect square P has property (21). If $\left(\lambda, \frac{\Delta AB}{(A,B)^2}\right) = 1$ we have

$$\eta(\lambda, \mathcal{M}) = \pi(N, \lambda T, l_\lambda) - \pi(|AB|, \lambda T, l_\lambda) - \mathrm{Li}\,N/\varphi(\lambda T)$$

thus by (55) and Lemma 8 we get

$$\sum_{\substack{\lambda < y\\ p\mid\lambda \Rightarrow p \in P}} |\eta(\lambda, \mathcal{M})| \ll N\log^{-2}N.$$

Therefore, by Lemma 9

$$\mathcal{A}(\mathcal{M}; N^{1/2s}) \geqslant \sqrt{\frac{2e^\gamma}{\pi}}\,\frac{\mathcal{C}}{\varphi(T)}\int_1^s \frac{dt}{\sqrt{t(t-1)}}\,N\log^{-3/2}N + O(N\log^{-8/5}N), \tag{57}$$

where

$$\mathcal{C} = \lim_{z\to\infty} \prod_{\substack{p<z\\ p\nmid \Delta AB(A,B)^{-2},\ \left(\frac{\Delta}{p}\right) = -1}} \left(1 - \frac{\varphi(T)}{\varphi(pT)}\right)\log^{1/2}z.$$

It follows from (51) that $\mathcal{C} > 0$. It remains to estimate $\sum \mathcal{A}(\mathcal{M}_{p_1p_2}; N^{1/2s})$. Put $M = (AN+B)(A,B,Cr^2d)/(A,B)Cr^2d$. Thus for $m_1 \in \mathcal{M}$ we have $0 < m_1 \leqslant M$, hence

$$\begin{aligned} &\sum_{\substack{p_2 \geqslant p_1 \geqslant N^{1/2s}\\ p_1, p_2 \notin \mathcal{P}}} \mathcal{A}(\mathcal{M}_{p_1p_2}; N^{1/2s})\\ &\qquad \leqslant \sum_{\substack{m_1 \leqslant MN^{-1/s}\\ q\mid m_1 \Rightarrow q \in \mathcal{P}}}\ \sum_{\substack{N^{1/2s} \leqslant p_1 < \sqrt{M}\\ \left(\frac{\Delta}{p_1}\right) = -1}}\ \sum_{\substack{p \leqslant N,\ p \equiv l_{p_1m_1} (\mathrm{mod}\ p_1m_1T)\\ \frac{A}{(A,B)}p + \frac{B}{(A,B)} = \frac{Cr^2d}{(A,B,Cr^2d)}p_1p_2m_1}} 1 = \Sigma\Sigma\Sigma_4. \end{aligned} \tag{58}$$

The inner sum can be written in the form $\Sigma_4 = \sum_{\substack{x \leqslant N/p_1 m_1 T \\ |a_i x + b_i| \text{ primes for } i=1,2}} 1$, where

$$a_1 = p_1 m_1 T,\ \ b_1 = l_{p_1 m_1},\ \ a_2 = \frac{A(A,B,Cr^2d)T}{(A,B)Cr^2d},\ \ b_2 = \frac{(B - Al_{p_1 m_1})}{(A,B)Cr^2 d p_1 m_1} \times$$

$\times (A, B, Cr^2d)$ hence $E = a_1 a_2 (a_1 b_2 - a_2 b_1) = \frac{AB\Delta^2}{(A, \Delta B)^2} p_1 m_1$. It follows from Lemma 9 that

(59)
$$\Sigma_4 \ll \frac{N}{p_1 m_1 T \log^2 (N/p_1 m_1 T)} \prod_{p \mid \frac{AB\Delta^2}{(A,\Delta B)^2}} \left(1 - \frac{1}{p}\right)^{w(p)-2} \prod_{\substack{p \mid m_1 \\ p \nmid \frac{AB\Delta^2}{(A,\Delta B)^2}}} \left(1 - \frac{1}{p}\right)^{w(p)-2},$$

where the constant in the symbol $\ll$ is absolute. From (58) and (59) we get

$$\sum_{\substack{p_2 \geqslant p_1 \geqslant N^{1/2s} \\ p_1, p_2 \in \mathscr{P}}} \mathscr{A}(\mathscr{M}_{p_1 p_2}; N^{1/2s})$$
$$< c_1 N \log^{-2} N \sum_{\substack{m < N^{1-1/s} \\ q \mid m \Rightarrow \left(\frac{\Delta}{q}\right) = 1}} \frac{1}{m} \prod_{p \mid m} \left(1 - \frac{1}{p}\right)^{-2} \sum_{N^{1/2s} < p < \sqrt{N}} p^{-1}$$
$$< c_2 \sqrt{s-1} \log s\, N \log^{-3/2} N$$

where the constants c_1, c_2 are independent on s, N. This completes the proof of the lemma since $\sup_{1<s<2} \left\{ \sqrt{\frac{2e^{\gamma}}{\pi}} \frac{\mathscr{C}}{\varrho(T)} \int_1^s \frac{dt}{\sqrt{t(t-1)}} - c_2 \sqrt{s-1} \log s \right\} > 0$.

Proof of Theorem 3. The lower estimate follows from (45) and Lemma 14. On the other hand

$$\sum_{\substack{p \leqslant N \\ Ap+B = C\varphi(x,y)}} 1 \leqslant \sum_{\substack{p \leqslant N \\ \left.\begin{array}{l} q^{2k+1} \| Ap+B \\ q \nmid \Delta C \end{array}\right\} \Rightarrow \left(\frac{\Delta}{q}\right) = 1}} 1$$
$$\leqslant \sum_{\substack{d \\ q \mid d \Rightarrow q \mid \Delta}} \sum_{\substack{r \\ \left(\frac{AB}{(A,B)^2}, \frac{Cr^2d}{(A,B,Cr^2d)}\right) = 1}} \sum_{\substack{p \leqslant N \\ \frac{A}{(A,B)}p + \frac{B}{(A,B)} = \frac{Cr^2d}{(A,B,Cr^2d)} m_1}} 1$$
$$= \sum_d \sum_r \sum_{\substack{m_2 < M \\ \left(m_2, \frac{AB}{(A,B)^2}\right) = 1 \\ q \mid m_2 \Rightarrow \left(\frac{\Delta}{q}\right) = 1}} \sum_{\substack{p \leqslant N \\ \frac{A}{(A,B)}p + \frac{B}{(A,B)} = \frac{Cr^2d}{(A,B,Cr^2d)} p' m_2}} 1 = \Sigma\Sigma\Sigma\Sigma_5$$

where $M = |AN + B|(A, B, Cr^2d)/(A, B)Cr^2d$. Let l be a solution of the congruence

$$\frac{A}{(A,B)} l + \frac{B}{(A,B)} \equiv 0 \left(\bmod \frac{Cr^2dm_2}{(A,B,Cr^2d)}\right)$$

and set in Lemma 9

$$a_1 = \frac{Cr^2dm_2}{(A,B,Cr^2d)},\quad b_1 = l,\quad a_2 = \frac{A}{(A,B)},\quad b_2 = \frac{(Al+B)(A,B,Cr^2d)}{(A,B)Cr^2dm_2}.$$

Hence

$$E = a_1 a_2 (a_1 b_2 - a_2 b_1) = \frac{ABCr^2dm_2}{(A,B)^2(A,B,Cr^2d)^2}$$

and we get from the said Lemma

$$\Sigma_5 = \sum_{\substack{0 < x \leqslant N(A,B,Cr^2d)/Cr^2dm_2 \\ |a_i x + b_i| \text{ primes for } i=1,2}} 1 \ll \frac{N}{dr^2m_2} \log^{-2}\left(\frac{N}{dr^2m_2} + 3\right) \prod_{p \mid rm_2} \left(1 - \frac{1}{p}\right)^{-2}.$$

Hence by Lemma 10

$$\sum_{\substack{p \leqslant N \\ Ap+B = C\varphi(x,y)}} 1 \ll \sum_d \sum_r \frac{N}{r^2 d} \log^{-3/2}\left(\frac{N}{r^2d} + 3\right) \ll N \log^{-3/2} N$$

and the proof is complete.

References

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

[2] E. Hecke, *Eine neue Art von Zetafunktionen und ihre Beziehungen zur Verteilung der Primzahlen, Zweite Mitteilung*, Mathematische Zeitschrift, Bd. 6, (1920), pp. 11–51.

[3] H. Iwaniec, *Primes represented by quadratic polynomials in two variables*, Bull. Acad. Polon. Sci., Sér. Sci. Math. Astronom. Phys. 20 (3) (1972), pp. 195–202.

[4] — *Primes of the type $\varphi(x, y) + A$, where φ is a quadratic form*, Acta Arith. 21 (1972), pp. 203–234.

[5] H. L. Montgomery, *Topics in Multiplicative Number Theory*, Berlin 1971.

[6] P. A. B. Pleasants, *The representation of primes by quadratic and cubic polynomials*, Acta Arith. 12 (1966), pp. 131–163.

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

Received on 22. 12. 1972 (363)