QUADRATIC POLYNOMIALS AND QUADRATIC FORMS

BY

JOHN FRIEDLANDER and HENRYK IWANIEC

Scuola Normale Superiore, Pisa

1. Introduction

Let $g(n)=an^2+bn+c$ be a polynomial with integral coefficients ($a>0$) and discriminant $D=b^2-4ac<-4$. We shall be concerned with the problem of showing that, for φ a binary quadratic form satisfying certain natural conditions, the number of $n\leqslant X$ for which $g(n)$ is represented by φ has the expected order of magnitude. The method involves an injection into the half dimensional sieve of a combination of ideas due largely to Chen [1] and Hooley [3]. A sketch of the proof is given in section 2.

For m an integer let $\varrho(m)$ denote the number of solutions of the congruence

$$g(n)\equiv 0 \pmod m.$$

Let P denote a set of primes satisfying:

$$0\leqslant \varrho(p)<p, \tag{1.1}$$

For some fixed K, and all $z\geqslant 2$,

$$\left|\sum_{\substack{p\leqslant z\\ p\in P}} \frac{\varrho(p)}{p-\varrho(p)}\log p-\tfrac{1}{2}\log z\right|\leqslant K. \tag{1.2}$$

For $z\geqslant 2$, we let $P(z)=\prod_{\substack{p<z\\ p\in P}} p$, $\mathcal{A}=\{g(n)\,|\,n\leqslant X\}$ and

$$S(\mathcal{A},P,z)=\sum_{\substack{m\in\mathcal{A}\\ (m,P(z))=1}} 1.$$

THEOREM 1. *There exists a positive δ, depending on a, b, c and K such that*

$$S(\mathcal{A},P,z)>\delta X\prod_{\substack{p<z\\ p\in P}}\left(1-\frac{\varrho(p)}{p}\right)-6\pi(z). \tag{1.3}$$

1 – 782901 *Acta mathematica* 141. Imprimé le 1 Septembre 1978

Remark. The restriction $D<-4$ is not essential but is included to simplify the proof. Since we do not assume D is a fundamental discriminant we may, for example, immediately get the result for $g(n)=n^2+1$ by applying the theorem to the polynomial $4n^2+1$. In the case $D>0$ the method of proof may again be applied but is somewhat complicated by the existence of non-trivial units in $Q(\sqrt{D})$.

Definition. We write $m \mid n^\infty$ if m divides some power of n.

THEOREM 2. *Let ∂ be a fundamental discriminant (such that $Q(\sqrt{D}) \neq Q(\sqrt{\partial})$) and $\varphi = Au^2+Buv+Cv^2$ a binary quadratic form, indefinite or positive definite, of discriminant $\partial = B^2-4AC$. Suppose there exist integers n_0, x_0, y_0 and m with $m \mid \partial^\infty$, such that*

$$g(n_0) \equiv \varphi(x_0, y_0) \pmod{\partial m}$$

and

$$(\varphi(x_0, y_0), \partial m) = m.$$

The number of $n \leqslant X$ such that $g(n)$ is represented by φ is then $\gg X (\log X)^{-1/2}$, the implied constant depending on the coefficients of g and φ.

Remarks. 1. The stated congruence condition is clearly necessary. It obviously may be replaced by the simpler condition that, for some n_0, $g(n_0)$ is represented by φ, but this latter condition may, in practice, be more difficult to verify.

2. For all sufficiently large p, we have

$$\varrho(p) = \begin{cases} 2 & \text{if } \left(\frac{D}{p}\right) = 1 \\ 0 & \text{if } \left(\frac{D}{p}\right) = -1 \end{cases}$$

Letting $P = \left\{p \mid \left(\frac{\partial}{P}\right) = -1\right\}$, we have

$$\sum_{\substack{p<z \\ p \in P}} \frac{\varrho(p)}{p-\varrho(p)} \log p = \tfrac{1}{2} \log z + O(1).$$

Using the upper bound sieve (Lemma 1) one gets an upper bound $\ll X (\log X)^{-1/2}$. In the case $Q(\sqrt{D}) = Q(\sqrt{\partial})$ the product $\prod_{p \in P} (1-\varrho(p)/p)$ has only finitely many factors and the sieve is of dimension zero, so we immediately get the lower bound $\gg X$. Thus, in either case one gets upper and lower bounds of the same order of magnitude.

3. Hooley's method (as pointed out in [3]) may be used to give asymptotic results if the representations of φ are counted with multiplicity.

4. We have not required the middle coefficient of φ to be even. In the course of the proof of Theorem 1, we shall have need of some facts about quadratic forms, and there, in

order to take advantage of some references, we have used the Gaussian theory. Hopefully, this will not cause confusion.

5. In a letter Professor Hooley has suggested that an alternative approach to the above results may be obtained by combining the method of [3] with that of another of his papers [5].

2. Sketch of the proof

The proof referred to is that of Theorem 1, the latter result being in the nature of a corollary. We begin by collecting together some facts about the half dimensional sieve. See [6] for details.

LEMMA 1. *Let $X \geqslant 2$ be fixed. Let $\mathcal{A}$ be a finite sequence of integers and P a set of primes. Suppose that ϱ is a multiplicative function such that (1.2) is satisfied. For $d \mid P(z)$ define*

$$\mathcal{A}_d = \{m \in \mathcal{A} \mid m \equiv 0 \pmod{d}\},$$

$$R(\mathcal{A}, d) = \sum_{m \in \mathcal{A}_d} 1 - \frac{\varrho(d)}{d} X = |\mathcal{A}_d| - \frac{\varrho(d)}{d} X,$$

and

$$V(z) = \prod_{p \mid P(z)} \left(1 - \frac{\varrho(p)}{p}\right).$$

For all $z \geqslant 2$, $y \geqslant 2$ we have

$$S(\mathcal{A}, P, z) \leqslant X V(z)\{F(s) + O((\log y)^{-1/5})\} + \sum_{\substack{d < y \\ d \mid P(z)}} |R(\mathcal{A}, d)| \tag{2.1}$$

$$S(\mathcal{A}, P, z) \geqslant X V(z)\{f(s) + O((\log y)^{-1/5})\} - \sum_{\substack{d < y \\ d \mid P(z)}} |R(\mathcal{A}, d)| \tag{2.2}$$

where $s = \log y / \log z$ and the functions $f(s)$, $F(s)$ are the continuous solutions of the system of differential-difference equations

$$f(s) = 0,\ F(s) = 2(e^{\gamma}/\pi s)^{\frac{1}{2}} \quad \text{for } 0 < s \leqslant 1, \tag{2.3}$$

$$2s^{\frac{1}{2}}(s^{\frac{1}{2}} f(s))' = F(s-1),\ 2s^{\frac{1}{2}}(s^{\frac{1}{2}} F(s))' = f(s-1) \quad \text{for } s > 1. \tag{2.4}$$

For $s > 1$ we have

$$0 < f(s) < 1 < F(s)$$

$$F'(s) < 0 < f'(s).$$

Applying (2.2) to the sequence $\mathcal{A} = \{g(n) \mid n \leqslant X\}$ with $y = X (\log X)^{-2}$, Theorem 1 follows immediately for $z \leqslant X^{\frac{1}{2}}$, which case we henceforth exclude.

Let $\alpha>0$ be fixed, and $X^{\alpha}<z_2<z_1<X^{\frac{1}{2}}<z$ and $z_0=\frac{1}{3}X$. We have

$$\sum_{\substack{z\leqslant p<z_0\\ p\in P}}\frac{\varrho(p)}{p}V(p)F\left(\frac{\log X/p}{\log p}\right)=V(z)f\left(\frac{\log X}{\log z}\right)+O(V(z)(\log z)^{-1/2}). \tag{2.5}$$

This result follows by partial summation from (1.2), (2.3) and (2.4).

Applying (2.1) to the sequence $\mathcal{A}_p$ with $z_2\leqslant p<z_0$ and $y=(X/p)(\log(X/p))^{-2}$ we obtain

$$S(\mathcal{A}_p,P,p)<X\frac{\varrho(p)}{p}V(p)F\left(\frac{\log X/p}{\log p}\right)+O\left(\frac{X}{p}\left(\log\frac{X}{p}\right)^{-7/10}\right)=S^+(\mathcal{A}_p,P,p),\quad\text{say,} \tag{2.6}$$

and applying (2.2) to the sequence $\mathcal{A}$ with $y=X(\log X)^{-2}$ we obtain

$$S(\mathcal{A},P,z_2)>XV(z_2)\left\{f\left(\frac{\log X}{\log z_2}\right)+O((\log X)^{-1/5})\right\}.$$

In the (possibly void) interval $z_0\leqslant p<z$ we have the trivial estimation

$$\sum_{\substack{z_0\leqslant p<z\\ p\in P}}S(\mathcal{A}_p,P,p)\leqslant\sum_{z_0\leqslant p<z}|\mathcal{A}_p|\leqslant 6\pi(z)$$

and in the interval $z_2\leqslant p<z_0$, by (2.5) and (2.6) we have

$$\sum_{\substack{z_2\leqslant p<z_0\\ p\in P}}S^+(\mathcal{A}_p,P,p)<XV(z_2)\left\{f\left(\frac{\log X}{\log z_2}\right)+O((\log z_2)^{-1/5})\right\}.$$

Substituting these in the Buchstab identity,

$$S(\mathcal{A},P,z)=S(\mathcal{A},P,z_2)-\sum_{z_2\leqslant p<z}S(\mathcal{A}_p,P,p),$$

we get

$$S(\mathcal{A},P,z)>\sum_{\substack{z_2\leqslant p<z_1\\ p\in P}}\{S^+(\mathcal{A}_p,P,p)-S(\mathcal{A}_p,P,p)\}-6\pi(z)+O(XV(z_1)(\log z_2)^{-1/5}). \tag{2.7}$$

Remarks. 1. It is now possible to see where the method is headed. The "classical" estimate gives $S\leqslant S^+$ and we wish to save on this, at least on average. Moreover, an arbitrarily small but fixed saving will be sufficient and this is rather crucial, since our improvements are not large.

A similar situation exists in the case of other dimensions. The constant 1/2 in (1.2) is by no means essential and results analogous to Theorem 1 can be proved. These are, for the most part, of limited interest due to the special nature of the set $\mathcal{A}$. In the case, however, of the linear sieve, since the sieving limit is 1/2, one gets immediately the result

$n^2+1=P_4$ and "just misses" improving this. The method of this paper, thus, gives a new proof of the result that there are infinitely many n such that $n^2+1=P_3$, without using a weighted sieve (at least in the usual sense). In fact it was the suggestion of Professor Halberstam that a combination of the ideas of Chen and Hooley might be used to attack $n^2+1=P_2$, which led to this work. (The method also can be used to prove Hoheisel type theorems for these problems.)

2. Following Chen's idea we "keep" the error term, reducing the problem to the estimation of exponential sums. In our case, van der Corput estimates do not apply and we use Hooley's idea to transfer the problem to Kloosterman sums. In contrast with [3], we shall be averaging over primes rather than over all integers. This necessitates the use of the Cauchy–Schwarz inequality which leads to some complication of detail concerning the composition of quadratic forms. Let

$$P^* = \{p \in P \mid \varrho(p) > 0,\ z_2 \leqslant p < z_1\}$$

$$P' = P^* \cap [Q, Q') \quad \text{where } z_2 \leqslant Q \leqslant Q' < 2Q.$$

Let $\mathcal{B}$ denote the sequence of elements m of $\mathcal{A}$, m repeated once for each prime divisor of m in P'. For $d \mid P(Q)$, define $R(\mathcal{B}, d)$ by

$$|\mathcal{B}_d| = \frac{\varrho(d)}{d} X \sum_{p \in P'} \frac{\varrho(p)}{p} + R(\mathcal{B}, d).$$

The bulk of the work will be devoted to the proof of the following result.

PROPOSITION. *If* $NQ^{1/2} < X$ *and* $Q < X^{1/500}$, *then*

$$\sum_{\substack{d \leqslant N \\ d \mid P(Q)}} |R(\mathcal{B}, d)| \ll (NQ^{1/2} + X^{0.99})(\log X)^2. \tag{2.8}$$

Note that the trivial estimation is NQ. We conclude this section by showing how (2.8) leads to the proof of Theorem 1.

Applying (2.1) to the sequence $\mathcal{B}$ with $z = Q$ and $y = N = XQ^{-\frac{1}{2}} (\log X)^{-4}$ we get

$$\sum_{p \in P'} S(\mathcal{A}_p, P, p) \leqslant S(\mathcal{B}, P, Q) \leqslant XV(Q) \sum_{p \in P'} \frac{\varrho(p)}{p} \left\{ F\left(\frac{\log X/\sqrt{Q}}{\log Q} \right) + O((\log Q)^{-1/5}) \right\}.$$

Choosing $z_1 = z_2^2 = X^{1/500}$, and summing over intervals of the type $[Q, Q')$, gives

$$\sum_{p \in P^*} S(\mathcal{A}_p, P, p) \leqslant \sum_{p \in P^*} X \frac{\varrho(p)}{p} V(p) \left\{ F\left(\frac{\log X/\sqrt{p}}{\log p} \right) + O((\log X)^{-1/5}) \right\}.$$

From (2.7) we get

$$S(\mathcal{A},P,z)\geqslant \sum_{p\in P^*} X\frac{\varrho(p)}{p}V(p)\left\{F\left(\frac{\log X/p}{\log p}\right)-F\left(\frac{\log X/\sqrt{p}}{\log p}\right)+O((\log X)^{-1/5})\right\}$$
$$-6\pi(z)+O(XV(z_2)(\log X)^{-1/5}).$$

By the mean value theorem

$$F\left(\frac{\log X/p}{\log p}\right)-F\left(\frac{\log X/\sqrt{p}}{\log p}\right)\geqslant 1,$$

and Theorem 1 follows since

$$\sum_{p\in P^*}\frac{\varrho(p)}{p}\geqslant 1.$$

3. Lemmata

This section contains lemmata to be used in the proof of the proposition. The first one embodies an idea of Vinogradov, although we know of no reference to it in this form.

LEMMA 2. *Let* $0<\Delta<1$, $e(\alpha)=e^{2\pi i\alpha}$, *and* $\psi(x)=x-[x]-\frac{1}{2}$. *Let*

$$a(x)=\begin{cases}(1-\Delta^{-1})x & \text{for } 0\leqslant x<\frac{1}{2}\Delta\\ x-\frac{1}{2} & \text{for } \frac{1}{2}\Delta\leqslant x<1-\frac{1}{2}\Delta\\ (1-\Delta^{-1})(x-1) & \text{for } 1-\frac{1}{2}\Delta\leqslant x<1\end{cases}$$

and

$$b(x)=\begin{cases}1-\Delta^{-1}x & \text{for } 0\leqslant x<\Delta\\ 0 & \text{for } \Delta\leqslant x<1-\Delta\\ 1+\Delta^{-1}(x-1) & \text{for } 1-\Delta\leqslant x<1.\end{cases}$$

We have

(i)
$$a(x)=\sum_{m\neq 0}\frac{i}{2\pi m}\frac{\sin\pi m\Delta}{\pi m\Delta}e(mx)$$

$$b(x)=\Delta+\Delta\sum_{m\neq 0}\left(\frac{\sin\pi m\Delta}{\pi m\Delta}\right)^2 e(mx)$$

(ii) *The* m*'th Fourier coefficients* $(m\neq 0)$ *of* $a(x)$ *and* $b(x)$ *are, in absolute value* $\leqslant Z_m$ *where*

$$Z_m=\begin{cases}\dfrac{1}{|m|} & \text{if } |m|\leqslant\Delta^{-1}\\ \dfrac{1}{\Delta m^2} & \text{if } |m|>\Delta^{-1}\end{cases}$$

(iii) $|\psi(x)-a(x)|\leqslant b(x)$.

The notation $\bar{r}$, used either as $\bar{r}/s$ or in a congruence (mod s) means that $\bar{r}r\equiv 1 \pmod{s}$.

LEMMA 3. *Let x, y and π be pairwise coprime integers. We have*

$$\frac{\bar{x}}{\pi y}+\frac{\bar{y}}{\pi x}\equiv\frac{\overline{xy}}{\pi}+\frac{1}{\pi xy} \pmod 1.$$

Proof. Multiply through by πxy and check modulo each factor.

The following result, due to Hooley, (Lemma 3 of [4]) is a consequence of Weil's estimate for Kloosterman sums. Using Hooley's method and the earlier estimate of Kloosterman, a weaker result could be derived which would still be sufficient for our purpose.

LEMMA 4. *If h and r are integers with $r\neq 0$ and if $0<\xi_2-\xi_1\leqslant 2|r|$, then*

$$\sum_{\substack{\xi_1\leqslant s\leqslant\xi_2\\ s\equiv\nu \pmod\lambda\\ (s,r)=1}} e\left(-h\frac{\bar{s}}{r}\right)\ll|r|^{(1/2)+\varepsilon}(h,r)^{1/2},$$

the implied constant depending on ε.

LEMMA 5. *Select one form (A, B, C) from each class of primitive positive definite forms of determinant $D=B^2-AC<-4$. Let m be a positive integer. There is a one to one correspondence between the solutions $\omega \pmod m$ of*

$$\omega^2\equiv D \pmod m$$

and pairs $\pm(r, s)$ of proper representations by the given forms. If $m=Ar^2+2Brs+Cs^2$, $(r, s)=1$, $s\neq 0$, then

$$\omega=-\frac{Ar+Bs}{s}+\frac{\bar{r}}{s}(Ar^2+2Brs+Cs^2).$$

Proof. This result, due of course to Gauss, is to be found in Article 86 of [7]).

By completing the square, we get

COROLLARY. *There exists a one to one correspondence between the roots of*

$$g(\nu)\equiv 0 \pmod m$$

and pairs $\pm(R, S)$ of proper representations of $4am$ (by the given forms), such that

$$AR+(B+b)S\equiv 0 \pmod{2a}. \tag{3.1}$$

This correspondence is given by

$$\nu=-\frac{AR+(B+b)S}{2aS}+\frac{\bar{R}}{S}\frac{AR^2+2BRS+CS^2}{2a}. \tag{3.2}$$

We now choose a system of representatives (A_i, B_i, C_i), $1 \leqslant i \leqslant h$, of the classes of primitive forms of determinant D in a way convenient for composition. Note first that the A_i may be chosen to be pairwise coprime and coprime with $2D$. Having done this, since changing B_i by a multiple of A_i does not change the class, the Chinese Remainder Theorem allows us to choose all the B_i equal ($=B$ say). We are still free to change B by multiples of $A_1A_2\cdots A_h$ and, since $B^2 \equiv D \pmod{A_1A_2\cdots A_h}$ we can demand $B^2 \equiv D \pmod{(A_1A_2\cdots A_h)^2}$. Let $\mathcal{D}$ denote a fixed set of representatives so chosen:

$$D = \{\phi_i = (A_i, B, C_i), \quad i = 1, \ldots, h\}.$$

From Gaussian composition (see Article 111 of [7]) we immediately get:

LEMMA 6. *Let $A_j\alpha^2 + 2B\alpha\beta + C_j\beta^2$ be a fixed proper representation of $p \in P'$ by (A_j, B, C_j) in $\mathcal{D}$. Let $d \mid P(Q)$. As (r, s) runs once through the proper representations $A_ir^2 + 2Brs + C_is^2$ of $4ad$ by forms of $\mathcal{D}$, $AR^2 + 2BRS + CS^2$ runs once through the proper representations of $4adp$, where*

$$A = A_iA_j; \quad C = \frac{B^2 - D}{A_iA_j}, \tag{3.3}$$

$$R = \alpha r - C\beta s, \quad \text{and } S = A_i\beta r + 2B\beta s + A_j\alpha s. \tag{3.4}$$

Notation. Let P_l ($l = 1, 2$) be distinct primes in P' (represented by the same class) and $A_j\alpha_l^2 + 2B\alpha_l\beta_l + C_j\beta_l^2$ fixed representations of them by (A_j, B, C_j). Let $d \mid P(Q)$ and let $A_ir^2 + 2Brs + C_is^2$ be a proper representation of $4ad$. For $l = 1, 2$ let $AR_l^2 + 2BR_lS_l + CS_l^2$ be the corresponding representations of $4adp_l$ from Lemma 6. Let

$$\delta = A_j\alpha_1\alpha_2 + B(\alpha_1\beta_2 + \alpha_2\beta_1) + C_j\beta_1\beta_2 \quad \text{and} \quad \nabla = \beta_1\alpha_2 - \beta_2\alpha_1.$$

Since $(A_j, B, C_j)\begin{pmatrix}\alpha_1 & \alpha_2 \\ \beta_1 & \beta_2\end{pmatrix} = (p_1, \delta, p_2)$, comparing determinants, we get

$$p_1p_2 = \delta^2 - D\nabla^2$$

and hence $\nabla \neq 0$, $(\delta, \nabla) = 1$, $(p_1p_2, \nabla) = 1$.

LEMMA 7. *We have*

$$A\nabla r = (2B\beta_2 + A_j\alpha_2)S_1 - (2B\beta_1 + A_j\alpha_1)S_2 \tag{3.5}$$

$$A\nabla s = -A_i\beta_2S_1 + A_i\beta_1S_2 \tag{3.6}$$

$$A\nabla R_1 = (\delta - B\nabla)S_1 - p_1S_2 \tag{3.7}$$

$$A\nabla R_2 = p_2S_1 - (\delta + B\nabla)S_2 \tag{3.8}$$

Proof. These are straight-forward consequences of Lemma 6.

Definition. Let $(S_1, S_2)=\eta$. We say the residue classes of S_1, $S_2 \pmod{2aA\nabla\eta}$ form an admissible pair if the following three conditions hold:

$$r \text{ and } s \text{ are integers} \tag{3.9}$$

$$AR_l+(B+b)S_l \equiv 0 \pmod{2a} \quad \text{for } l=1, 2, \tag{3.10}$$

$$(R_l, \eta)=1 \quad \text{for } l=1, 2. \tag{3.11}$$

Remark. Using Lemma 7 it is easily checked that the above notion is well-defined.

LEMMA 8. *Assume* $z_2>\max_i A_i^2$. *The conditions*

$$AR_l+(B+b)S_l \equiv 0 \pmod{2a}, \quad l=1, 2, \tag{3.12}$$

$$r \text{ and } s \text{ are integers such that } (R_l, S_l)=1, \quad l=1, 2, \tag{3.13}$$

are equivalent to the conditions

$$p_l \nmid S_l \quad l=1, 2 \tag{3.14}$$

there exists $\eta \mid A\nabla$ *such that* $(S_1, S_2)=\eta$ *and* S_1, S_2 *are an admissible pair* $\pmod{2aA\nabla\eta}$. (3.15)

Proof. Assume first that we have (3.12) and (3.13). Let $\eta=(S_1, S_2)$. Since $(R_1, S_1)=1$, if $p_1 \mid S_1$ we would have, from (3.7), $p_1 \mid A\nabla$. But $p_1>A$ and we cannot have $p_1 \mid \nabla$ for $p_1 \neq p_2$. Thus $p_1 \nmid S_1$. Similarly $p_2 \nmid S_2$. (3.9) and (3.10) are immediate and (3.11) follows from (3.13).

Conversely suppose (3.14) and (3.15) hold. We must show $(R_l, S_l)=1$. Clearly $\eta \mid (A\nabla, S_1)$ and, since $p_1 \nmid S_1$, (3.7) implies that $(A\nabla, S_1)$ divides S_2 and hence η. Thus, we have

$$(A\nabla, S_1)=\eta=(A\nabla, S_2). \tag{3.16}$$

From (3.7), $(R_1, S_1) \mid \eta$ and dividing (3.7) through by η the result follows.

Notation. Let $(S_1, S_2)=\eta$. We write $S_l=\eta\eta_l T_l$ $(l=1, 2)$, where $\eta_l \mid \eta^\infty$, $\eta_l>0$ and

$$(A\nabla, T_l)=(T_1, T_2)=(\eta_1, \eta_2)=1.$$

LEMMA 9. *Let* $\pi=\eta\eta_1\eta_2$. *We have*

$$\frac{\overline{R_1}}{S_1} \equiv -\frac{A\nabla}{\eta}\frac{\overline{p_1T_2}}{\pi T_1}+\frac{E_1}{\pi} \pmod 1 \tag{3.17}$$

$$\frac{\overline{R_2}}{S_2} \equiv \frac{A\nabla}{\eta}\frac{\overline{p_2T_1}}{\pi T_2}+\frac{E_2}{\pi} \pmod 1 \tag{3.18}$$

where E_1, E_2 *depend only on the residue classes of* T_1, $T_2 \pmod{A\nabla\eta_1\eta_2}$.

Proof. We prove only (3.17), the other being similar. (3.17) is equivalent to

$$\eta_2 \tilde{R}_1 \equiv -\frac{A \nabla}{\eta} (\overline{p_1 T_2}) + E_1 T_1 \pmod{\pi T_1}, \tag{3.19}$$

where $\tilde{}$ means inverse (mod S_1). Since $(\pi, T_1)=1$ it is sufficient to check (mod T_1) and (mod π). Modulo T_1, $^-$ and $\tilde{}$ coincide and from (3.7) it follows that the congruence holds for any E_1. Since $(\pi, T_1)=1$, we can choose E_1 so that the congruence holds (mod π). If T_1, T_2 are changed by multiples of $A \nabla \eta_1 \eta_2$, (3.7) implies that R_1 is changed by a multiple of π and so (3.19) implies that E_1 is changed by a multiple of π.

4. Proof of proposition

For $d \mid P(Q)$ we have

$$|\mathcal{A}_d| = \sum_{\substack{\nu \\ g(\nu) \equiv 0 \bmod d)}} \sum_{\substack{0<n\leqslant X \\ n \equiv \nu \,(\mathrm{mod}\ d)}} 1 = \sum_{\nu} \left(\left[\frac{X-\nu}{d} \right] - \left[\frac{-\nu}{d} \right] \right) = X \frac{\varrho(d)}{d} - \sum_{\nu} \left\{ \psi\left(\frac{X-\nu}{d} \right) - \psi\left(\frac{-\nu}{d} \right) \right\}.$$

Hence, $R(\mathcal{B}, d) = -R(X, \mathcal{B}, d) + R(O, \mathcal{B}, d)$, where

$$R(x, \mathcal{B}, d) = \sum_{p \in P'} \sum_{\substack{\nu \\ g(\nu) \equiv 0 \,(\mathrm{mod}\ pd)}} \psi\left(\frac{x-\nu}{pd} \right), \quad (x = 0 \text{ or } X).$$

By Lemma 2

$$\sum_{\substack{d<N \\ d \mid P(Q)}} |R(x, \mathcal{B}, d)| \ll NQ\Delta \log X + \sum_{m \neq 0} Z_m \sum_{\substack{d<N \\ d \mid P(Q)}} \left| \sum_{p \in P'} \sum_{\nu (pd)} e\left(m \frac{x-\nu}{pd} \right) \right|. \tag{4.1}$$

We consider

$$T_m = \sum_{\substack{N_2 \leqslant d < N_1 \\ d \mid P(Q)}} \left| \sum_{p \in P'} \sum_{\nu (pd)} e\left(m \frac{x-\nu}{pd} \right) \right|, \tag{4.2}$$

where $N_1 \leqslant \min\{N, 2N_2\}$. By Lemma 5, Corollary and Lemma 6

$$T_m = \tfrac{1}{4} \sum_{d} \left| \sum_{\phi_i \in \mathcal{D}} \sum_{\phi_j \in \mathcal{D}} \sum_{\phi_i(r,s) = d} \sum_{\phi_j(\alpha, \beta) = p \in P'} e\left(m \frac{x-\nu}{pd} \right) \right|$$

where ν is given by (3.2), and where the sum over α, β is restricted to those pairs for which R, S given by (3.4) satisfy (3.1) and $(R, S)=1$.

By the Cauchy Schwarz inequality

$$T_m \leqslant \tfrac{1}{4} \sum_{\phi_i \in \mathfrak{D}} \sum_{\phi_j \in \mathfrak{D}} \sum_{\substack{r,\,s \\ 4aN_2 \leqslant \phi_i(r,s) < 4aN_1}} \left| \sum_{\substack{\alpha,\,\beta \\ \phi_j(\alpha,\beta) = p \in P'}} e\left(m\frac{x-v}{pd}\right)\right|$$

$$\leqslant \sum_{1 \leqslant i,\, j \leqslant h} N_1^{1/2} \left\{ \sum_{r,\,s} \sum_{\substack{\alpha_1,\,\beta_1 \\ \alpha_2,\,\beta_2}} e\left(m\frac{x-v_1}{p_1 d} - m\frac{x-v_2}{p_2 d}\right)\right\}^{1/2}.$$

$$T_m \ll \sum_{1 \leqslant i,\, j \leqslant h} N_1^{1/2} \left\{ N_1 Q + \sum_{\substack{\alpha_1,\,\beta_1 \\ \alpha_2,\,\beta_2 \\ p_1 \neq p_2}} \left| \sum_{r,\,s} e\left(m\frac{x-v_1}{p_1 d} - m\frac{x-v_2}{p_2 d}\right)\right|\right\}^{1/2}.$$

Ne now fix $\alpha_1, \beta_1, \alpha_2, \beta_2, i, j$ such that $\phi_j(\alpha_l, \beta_l) = p_l \in P'$ with $p_1 \neq p_2$, and consider

$$U = \sum_{\substack{r,\,s \\ 4aN_2 \leqslant \phi_i(r,\,s) < 4aN_1}} e\left(m\frac{x-v_1}{p_1 d} - m\frac{x-v_2}{p_2 d}\right), \tag{4.4}$$

where (r, s) are restricted to those pairs for which (in view of Lemma 5, Corollary) we have (3.12) and (3.13). Here we have, in the notation of (3.3),

$$\frac{x-v_1}{p_1 d} - \frac{x-v_2}{p_2 d} = \frac{x}{d}\left(\frac{1}{p_1} - \frac{1}{p_2}\right) + \frac{AR_1 + (B+b)S_1}{2aS_1 p_1 d} - \frac{AR_2 + (B+b)S_2}{2aS_2 p_2 d} - 2\frac{\overline{R_1}}{S_1} + 2\frac{\overline{R_2}}{S_2}. \tag{4.5}$$

We now transform the variables of U from r, s to S_1, S_2. Since $p_1 \neq p_2$, $\nabla \neq 0$ and we can do this. We have $AR_1^2 + 2BR_1S_1 + CS_1^2 = 4ap_1 d$. Multiplying through by $A\nabla^2$, using (3.7) and $\delta^2 - D\nabla^2 = p_1 p_2$, we see that the condition $N_2 \leqslant d < N_1$ is equivalent to

$$4aA\nabla^2 N_2 \leqslant F(S_1, S_2) < 4aA\nabla^2 N_1, \tag{4.6}$$

where

$$F(S_1, S_2) = p_2 S_1^2 - 2\delta S_1 S_2 + p_1 S_2^2 \tag{4.7}$$

which is definite of determinant $D\nabla^2$. From Lemma 8, we have

$$U = \sum_{\eta \mid A\nabla} \sum_{(k_1, k_2)} \sum_{\substack{(S_1, S_2) = \eta \\ S_l \equiv k_l \,(\mathrm{mod}\, 2aA\nabla\eta)}} e\left(m\frac{x-v_1}{p_1 d} - m\frac{x-v_2}{p_2 d}\right)$$

where (k_1, k_2) runs through admissible pairs (mod $2aA\nabla\eta$), and S_1, S_2 satisfy (3.14) and (4.6). Defining η_1, η_2, T_1, T_2 as in section 3,

$$U = \sum_{\eta} \sum_{(k_1, k_2)} \sum_{\substack{(\eta_1, \eta_2) = 1 \\ \eta_1 \eta_2 \mid \eta^\infty}} {\sum_{}}' \sum_{\substack{(p_2 T_1,\, p_1 T_2) = 1 \\ \eta\eta_l T_l \equiv k_l \,(\mathrm{mod}\, 2aA\nabla\eta)}} e\left(m\frac{x-v_1}{p_1 d} - m\frac{x-v_2}{p_2 d}\right) = U'_M + U''_M, \tag{4.8}$$

say, where $\sum'$ stands for summation over those T_1 and T_2 satisfying (4.6) and all other conditions written under the symbol $\sum'$; the sum U'_M is restricted to those pairs (η_1, η_2) such that $\eta_1\eta_2 \leqslant M$, and U''_M is the sum over the remaining pairs. For U''_M we trivially estimate the exponential sum. We have

$$S_l^2 \leqslant -DS_l^2 \leqslant (AR_l + BS_l)^2 - DS_l^2 = 4aAp_l d,$$

so $|S_l| \ll (QN_1)^{\frac{1}{2}}$ and $|T_l| \ll (QN_1)^{1/2}(\eta\eta_l)^{-1}$. Thus the sum over T_1, T_2 is trivially $\ll QN_1/\eta^2\eta_1\eta_2$, so

$$U''_M \ll \sum_{\eta} \sum_{(k_1, k_2)} \sum_{\substack{\eta_1\eta_2 > M \\ \eta_1\eta_2 | \eta^\infty}} QN_1(\eta^2\eta_1\eta_2)^{-1} \ll \frac{QN_1}{M^{1/2}} \sum_{\eta} \sum_{(k_1, k_2)} \sum_{\eta_1\eta_2 | \eta^\infty} \eta^{-2}(\eta_1\eta_2)^{-1/2}$$

$$\ll \frac{QN_1}{M^{1/2}} \nabla^2 \sum_{\eta | A\nabla} \sum_{\eta_1\eta_2 | \eta^\infty} (\eta_1\eta_2)^{-1/2} \ll QN_1 \nabla^4 M^{-1/2} \ll Q^5 N_1 M^{-1/2}, \tag{4.9}$$

since $\nabla^2 < \delta^2 - D\nabla^2 = p_1p_2 \ll Q^2$.

Next U'_M is estimated more carefully using Hooley's lemma. We have

$$U'_M = \sum_{\eta | A\nabla} \sum_{(k_1, k_2)} \sum_{\substack{(\eta_1, \eta_2)=1 \\ \eta_1\eta_2 | \eta^\infty \\ \eta_1\eta_2 \leqslant M}} \sum_{(t_1, t_2)} \sum'_{\substack{(p_2T_1, p_1T_2)=1 \\ T_l \equiv t_l \pmod{A\nabla\eta_1\eta_2}}} e(m\theta(T_1, T_2)) \tag{4.10}$$

where (t_1, t_2) run through the pairs of classes (mod $A\nabla\eta_1\eta_2$), $\sum'$ has the same meaning as in (4.8) and $\theta(T_1, T_2) = \theta_1(T_1, T_2) + 2\theta_2(T_1, T_2)$, where, by (3.7), (3.8), and (4.5)

$$\theta_1(T_1, T_2) = \frac{x}{d}\left(\frac{1}{p_1} - \frac{1}{p_2}\right) + \frac{1}{2ad\nabla}\left(\frac{\delta + b\nabla}{p_1} + \frac{\delta - b\nabla}{p_2}\right) - \frac{1}{2ad\nabla}\left(\frac{\eta_2T_2}{\eta_1T_1} + \frac{\eta_1T_1}{\eta_2T_2}\right),$$

where, by (4.5) and Lemma 9

$$\theta_2(T_1, T_2) = \frac{A\nabla}{\eta}\left(\frac{\overline{p_1T_2}}{\pi T_1} + \frac{\overline{p_2T_1}}{\pi T_2}\right) + \frac{E_2 - E_1}{\pi},$$

and

$$d = \frac{F(\eta\eta_1T_1, \eta\eta_2T_2)}{4aA\nabla^2}.$$

We shall, in estimating U'_M, assume $|S_2| \leqslant |S_1|$. The other part of the sum, where $|S_1| < |S_2|$, is done in similar fashion. We have, by Lemma 3,

$$\frac{\overline{p_1T_2}}{\pi T_1} + \frac{\overline{p_2T_1}}{\pi T_2} \equiv p_2\frac{\overline{p_1T_2}}{\pi p_2T_1} + p_1\frac{\overline{p_2T_1}}{\pi p_1T_2} \equiv (p_2 - p_1)\frac{\overline{p_1T_2}}{\pi p_2T_1} + \frac{\overline{p_2T_1T_2}}{\pi} + \frac{1}{p_2T_1T_2\pi} \pmod 1.$$

Thus,

$$\theta(T_1, T_2) \equiv \psi(T_1, T_2) + 2\frac{A\nabla}{\eta}(p_2 - p_1)\frac{\overline{p_1T_2}}{\pi p_2T_1} \pmod 1,$$

where

$$\psi(T_1, T_2)=\theta_1(T_1, T_2)+\frac{2A\nabla}{p_2\pi\eta T_1T_2}+\frac{2A\nabla}{\eta}\frac{\overline{p_2t_1t_2}}{\pi}+2\frac{E_2-E_1}{\pi}.$$

A computation shows that for T_1, T_2 in the range of summation (since $|S_1|\geqslant|S_2|$),

$$\frac{\partial\psi}{\partial T_2}(T_1, T_2)\ll xMQ^{1/2}N_1^{-3/2}+MQ^{3/2}N_1^{-3/2}+Q^{1/2}N_1^{-1/2}+MQ^2N_1^{-1}.$$

Since we have either $x=0$ or $x=X$, choosing $M=Q^{20}$, $N<X$, we have

$$\frac{\partial\psi}{\partial T_2}(T_1, T_2)\ll XQ^{22}N_1^{-3/2}.$$

We have

$$\sum_{T_1, T_2}\ll\sum_{T_1}\left|\sum_{\substack{\xi_1\leqslant T_2\leqslant\xi_2\\ T_2\equiv t_2\,(\mathrm{mod}\,A\nabla\eta_1\eta_2)\\ (T_2,\,\pi p_2T_1)=1}} e\left\{m\psi(T_1, T_2)+m\frac{2A\nabla}{\eta}(p_2-p_1)\frac{\overline{p_1T_2}}{\pi p_2T_1}\right\}\right| \tag{4.11}$$

where for each T_1, in view of (4.6), the sum for T_2 is actually in two intervals of the above type and, for each of these,

$$\xi_2-\xi_1\ll 2\frac{\eta_1}{\eta_2}|T_1|<2\pi p_2|T_1|.$$

Letting

$$S(\xi)=\sum_{\substack{\xi_1\leqslant T_2\leqslant\xi\\ T_2\equiv t_2\,(\mathrm{mod}\,A\nabla\eta_1\eta_2)\\ (T_2,\,\pi p_2T_1)=1}} e\left(m\frac{A\nabla}{\eta}(p_2-p_1)\frac{\overline{p_1T_2}}{\pi p_2T_1}\right),$$

Lemma 4 gives, for $\xi_1\leqslant\xi\leqslant\xi_2$, after a little computation,

$$S(\xi)\ll m^{1/2}Q^{12}T_1^{(1/2)+\varepsilon}.$$

Letting $\phi(T_1, \xi)=e(m\psi(T_1, \xi))$,

$$\frac{\partial\phi}{\partial\xi}(T_1, \xi)\ll mXQ^{22}N_1^{-3/2}.$$

By partial summation, the sum over T_2 in (4.11) satisfies

$$\sum_{T_2}\ll m^{1/2}Q^{12}T_1^{(1/2)+\varepsilon}\{1+(\xi_2-\xi_1)mXQ^{22}N_1^{-3/2}\}\ll m^{3/2}XQ^{35}N_1^{-3/4}.$$

Since $|T_1|\ll(QN_1)^{1/2}$,

$$\sum_{T_1, T_2}\ll Xm^{3/2}Q^{36}N_1^{-1/4}.$$

Returning to (4.10),

$$U'_M \ll Q^{2+\varepsilon} M^{1+\varepsilon}(QM)^2 (Xm^{3/2}Q^{36}N_1^{-1/4}) \ll m^{3/2}XQ^{101}N_1^{-1/4}.$$

Combining this with (4.9),

$$U \ll m^{3/2}XQ^{101}N_1^{-1/4} + N_1Q^{-5}.$$

From (4.3),

$$T_m \ll N_1^{1/2}\{N_1Q + m^{3/2}XQ^{103}N_1^{-1/4}\}^{1/2} \ll N_1Q^{1/2} + m^{3/4}X^{1/2}Q^{52}N_1^{3/8}.$$

Summing up over $\ll \log X$ intervals of the type $[N_2, N_1)$, returning to (4.1) and choosing $\Delta = Q^{-1/2}$, we have

$$\sum_{\substack{d<N \\ d|P(Q)}} |R(\mathcal{B}, d)| \ll (\log X)^2 (NQ^{1/2} + Q^{52}X^{1/2}N^{3/8}(\sum_{m\leqslant Q^{1/2}} m^{-1/4} + \sum_{m>Q^{1/2}} Q^{1/2}m^{-5/4}))$$

$$\ll (NQ^{1/2} + N^{3/8}X^{1/2}Q^{53})(\log X)^2. \tag{4.12}$$

Since $NQ^{1/2} < X$ and $Q < X^{1/500}$, $N^{3/8}X^{1/2}Q^{53} < Q^{53}X^{7/8} < X^{0.99}$, which completes the proof of the proposition and, in view of the arguments of section 2, completes the proof of Theorem 1.

Remark. Aside from improvements of the exponent 53, (4.12) seems to be essentially the best estimate that can be derived by this method.

5. Proof of Theorem 2

From genus theory it follows that for $q|\partial$, $(\varphi(x, y), \partial) = 1$, $\left(\frac{q}{\varphi(x,y)}\right)$ depends only on the genus of φ. Let $D = D_1D_2$ where $(D_1, \partial) = 1$, $D_1 > 0$, and $D_2|\partial^\infty$. By a corollary of Fogels [2] there exist infinitely many primes p for which $\left(\frac{D_1}{p}\right) = \left(\frac{D_2}{\varphi(x,y)}\right)$, so that $\left(\frac{D}{p}\right) = 1$ and such that p is represented by φ. Thus we can choose an integer Q which is:

(i) prime to $2aD\partial$,

(ii) divisible only by primes p satisfying $\left(\frac{D}{p}\right) = 1$,

(iii) divisible by integers represented by forms of each class of discriminant ∂.

Moreover, by properties (i) and (ii), we may take $g(n_0) \equiv 0 \pmod{Q^2}$. Letting

$$P = \left\{p \,\middle|\, \left(\frac{\partial}{p}\right) = -1\right\},\ G(n) \equiv g(\partial mnQ^2 + n_0),\ \mathcal{A} = \{G(n) \,|\, n \leqslant X\},$$

Theorem 1 gives, for large X,

$$S(\mathcal{A}, P, X(\log X)^{1/3}) \gg X(\log X)^{-1/2}$$

and it suffices to prove that S counts only n for which $G(n)$ is represented by φ.

Let a^* be an integer so counted and so $a^* = ma'$ where $(a', \partial) = 1$. For $\varphi(x_0, y_0) = b^*m$, we have $\left(\frac{\partial}{b^*}\right) = 1$, so $\left(\frac{\partial}{a'}\right) = 1$. Thus, a^* is divisible by an even number of primes in P and each is $\geqslant X\,(\log X)^{1/3}$. Thus, if X is large, there are no such prime factors and so a^* is represented by some form of discriminant ∂ (as are a', a'/Q^2, and b^*). Since $(a', \partial) = 1$ and $a' \equiv b^* \pmod{\partial}$, forms representing a', a'/Q^2, and b^* are in the same genus. Letting ψ represent a'/Q^2, A the class of ψ, $B = AC^2$ another class of the same genus, and q a divisor of Q represented by forms of C, we have $a'q^2/Q^2 = \varphi^*(x^*, y^*)$ for some ψ^* in B and some integers x^*, y^*. Thus $a' = \varphi^*((Q/q)\,x^*,\ (Q/q)\,y^*)$. Hence every form representing b^*, represents a' and so every form representing b^*m (φ in particular) represents a^*. This completes the proof.

References

[1]. Chen, J. R., On the distribution of almost primes in an interval. *Scientia Sinica*, XVIII 5 (1975), 611–627.

[2]. Fogels, E., On the abstract theory of primes III. *Acta Arith.*, XI (1966), 293–331.

[3]. Hooley, C., On the number of divisors of quadratic polynomials. *Acta Math.*, 110 (1963), 97–114.

[4]. —— On the greatest prime factor of a quadratic polynomial. *Acta Math.*, 117 (1967), 281–299.

[5]. —— On the intervals between numbers that are the sums of two squares III. *J. Reine Angew.*, 267 (1974), 207–218.

[6]. Iwaniec, H., The half dimensional sieve. *Acta Arith.*, XXIX (1976), 69–95.

[7]. Smith, H. J. S., Report on the theory of numbers. *Collected mathematical papers*, vol. I, reprinted, Chelsea 1965.

Received July 4, 1977