ACTA ARITHMETICA
XII (1966)

The representation of primes by quadratic and cubic polynomials

by

P. A. B. Pleasants (Cambridge)

1. Introduction. Let

$$\phi(x_1, \ldots, x_n) = \phi(\boldsymbol{x}) = C(\boldsymbol{x})+Q(\boldsymbol{x})+L(\boldsymbol{x})+N \tag{1}$$

be a cubic polynomial with integer coefficients, where $C(\boldsymbol{x})$ denotes the cubic part of ϕ, $Q(\boldsymbol{x})$ the quadratic part, and so on. The invariant $h = h(C)$ is defined to be the least integer for which $C(\boldsymbol{x})$ is representable identically as

$$L_1Q_1+\ldots+L_hQ_h \tag{2}$$

where $L_1, \ldots, L_h$ and $Q_1, \ldots, Q_h$ are linear and quadratic forms respectively with integer coefficients.

The object of the present paper is to continue the investigation, started in [5], into the conditions under which $\phi(\boldsymbol{x})$ represents infinitely many primes. (Here and throughout this work we use the word "prime" to mean positive prime number.)

It was proved in [5] that if $h \geqslant 8$ ([1]) then $\phi(\boldsymbol{x})$ represents infinitely many primes for integer points $\boldsymbol{x}$ provided certain necessary congruence conditions are satisfied, and an asymptotic formula for the number of such representations was given. In the present paper we are interested in the case $h \leqslant 7$. We shall prove that under the same necessary conditions $\phi(\boldsymbol{x})$ represents infinitely many primes in this case also, provided that $\phi(\boldsymbol{x})$ is irreducible and n is large enough. It is assumed here that $\phi(\boldsymbol{x})$ is non-degenerate. It is in the nature of the method used that it does not give rise to an asymptotic formula. The proof depends on some results on the representation of primes by quadratic polynomials and the first part of the present paper (§§ 2-7) is taken up with proving the main result in this direction.

([1]) The main result of [5] was obtained under the hypothesis $h^* > 8$, the invariant h^* being defined somewhat differently from h, but $h > 8$ is a stronger hypothesis than this since, as was remarked in [5], we have $h^* > h$.

Let P be a large positive number and let

(3) $$\phi_P(x_1, \dots, x_n) = \phi_P(\boldsymbol{x}) = Q(\boldsymbol{x})+L_P(\boldsymbol{x})+N_P$$

be a quadratic polynomial with quadratic part $Q(\boldsymbol{x})$, linear part $L_P(\boldsymbol{x})$, and constant term N_P. Here the coefficients of $Q(\boldsymbol{x})$ are constant but the remaining coefficients of $\phi_P(\boldsymbol{x})$ may depend on P. Suppose that for all P the coefficients of ϕ_P are rational and the value of $\phi_P(\boldsymbol{x})$ is integral for every integer point $\boldsymbol{x}$. Denote by r the rank of $Q(\boldsymbol{x})$. Let f_1, f_2 be positive real numbers and let $\mathscr{B}$ be a box (i.e. a cartesian product of intervals) with volume V such that for every point ξ in the expanded box $P\mathscr{B}$

(4) $$f_1P^2 \leqslant \phi_P(\xi) \leqslant f_2P^2.$$

(It is necessary for the existence of such a box $\mathscr{B}$ that the coefficients of $L_p(\boldsymbol{x})$ are $O(P)$ and that N_P is $O(P^2)$.) Denote by $\mathscr{N}(P)$ the number of integer points $\boldsymbol{x}$ in $P\mathscr{B}$ for which the value of $\phi_P(\boldsymbol{x})$ is a prime. We shall prove the following result.

THEOREM 1. *If ϕ_P is as in* (3) *and $r \geqslant 3$, and if for all large P the numerators of the coefficients of ϕ_P in their lowest terms have no common factor and there is some integer point $\boldsymbol{x}$ such that $\phi_P(\boldsymbol{x}) \not\equiv 0 \pmod 2$, then*

$$\mathscr{N}(P) \sim \frac{VP^n}{\log P^2}\,\mathfrak{S}(P)$$

where $\mathfrak{S}(P)$ is a function of P lying between fixed positive bounds.

The proof of Theorem 1 uses the Hardy-Littlewood method and is on the same lines as the proof of the main theorem of [5] although the details are considerably less complicated. It is necessary for the applications, however, that Theorem 1 be stated in more general terms than the theorem of [5].

It can be easily verified that for any number c the number of solutions of the equation $\phi_P(\boldsymbol{x}) = c$ with $\boldsymbol{x} \in P\mathscr{B}$ is $\ll P^{n-1}$, where the implied constant depends only on n and $\mathscr{B}$. Thus it is a consequence of Theorem 1 that the number of distinct primes represented by $\phi_P(\boldsymbol{x})$ for $\boldsymbol{x} \in P\mathscr{B}$ is $\gg P/\log P$, and in particular that infinitely many distinct primes occur as values of the polynomials ϕ_P.

In the second part of this paper (§§ 8-11) we deal with the representation of primes by cubic polynomials ϕ having n substantially greater than h. The method is to fix some of the variables in such a way that ϕ reduces to a suitable quadratic or linear polynomial in the remaining variables and then apply to this resulting polynomial either Theorem 1 or else the well-known theorem on primes in an arithmetic progression. Both these theorems are also used in the initial reduction of ϕ to a polynomial of smaller degree.

Our main result is the following.

THEOREM 2. *If $\phi(\boldsymbol{x})$ is a non-degenerate, irreducible cubic polynomial of the form* (1) *such that for any integer $m > 1$ there is an integer point $\boldsymbol{x}$ with $\phi(\boldsymbol{x}) \not\equiv 0 \pmod m$, and if one of the following three conditions holds:*

(i) $h = 1$ *and* $n \geqslant 5$,

(ii) $h = 2$ *and* $n \geqslant 9$,

(iii) $h \geqslant 3$ *and* $n \geqslant h+3$;

then $\phi(\boldsymbol{x})$ represents infinitely many positive prime numbers for integer points $\boldsymbol{x}$.

Combining Theorem 2 with the main theorem of [5] we obtain the following general result.

THEOREM 3. *If $\phi(x_1, \dots, x_n)$ is a non-degenerate, irreducible cubic polynomial in n variables with $n \geqslant 10$, 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.*

For if $h \geqslant 8$ the theorem of [5] is applicable to ϕ, and if $h \leqslant 7$ Theorem 2 is applicable, so that in either case the result follows.

In the last two theorems and throughout this paper the word irreducible refers to irreducibility over the field of rational numbers.

We note that the hypothesis that the coefficients of ϕ have no common factor together with the cases $m = 2$ and $m = 3$ of the congruence condition would imply all the remaining cases of the congruence condition.

2. Elementary lemmas.

LEMMA 1. *If*

$$\phi(x_1, \dots, x_n) = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_ix_j + \sum_{i=1}^{n} l_ix_i + N$$

is a quadratic polynomial whose value is integral at every integer point $\boldsymbol{x}$, then N is an integer and the other coefficients of ϕ are rational numbers which, expressed in their lowest terms, have denominators at most 2.

Proof. Trivially $N = \phi(0, \dots, 0)$ is an integer. Next we have

$$\phi(1,1,0,\dots,0)-\phi(1,0,\dots,0)-\phi(0,1,0,\dots,0)+\phi(0,\dots,0) = 2a_{12}.$$

Since all the terms on the left-hand side of this equation are integers, so is $2a_{12}$, and similarly $2a_{ij}$ is an integer whenever $i \neq j$.

Finally

$$\phi(x+1,0,\dots,0)-\phi(x,0,\dots,0) = 2a_{11}x+a_{11}+l_1.$$

Since the left-hand side of this equation is an integer whenever x is, we deduce that $2a_{11}$ and $a_{11}+l_1$ are both integers and hence a_{11}

and l_1 are rational numbers with denominators at most 2. Similarly a_{ii} and l_i are rational numbers with denominators at most 2 for $i = 1, \ldots, n$.

LEMMA 2. *If $\phi(\boldsymbol{x})$ is a quadratic polynomial with rational coefficients whose value is integral at every integer point $\boldsymbol{x}$, and if ϕ is such that*

(i) *the numerators of the coefficients of ϕ in their lowest terms have no common factor,*

(ii) *there exists an integer point $\boldsymbol{x}$ for which*

$$\phi(\boldsymbol{x}) \not\equiv 0 \pmod 2,$$

then given any integer m there exists an integer point $\boldsymbol{y}$ such that

$$\big(\phi(\boldsymbol{y}), m\big) = 1.$$

Proof. First we prove the result of the lemma when $m = p$, a prime. If $p = 2$ the result is just condition (ii) of the statement of the lemma. Suppose $p > 2$. If the result were not true, we should have $\phi(\boldsymbol{x}) \equiv 0 \pmod p$ for all integer points $\boldsymbol{x}$, and so the polynomial $p^{-1}\phi(\boldsymbol{x})$ would be integer valued at all integer points. Hence, by Lemma 1, the coefficients of $p^{-1}\phi(\boldsymbol{x})$ have denominators at most 2 and so all the numerators of the coefficients of $\phi(\boldsymbol{x})$ are divisible by p, contradicting hypothesis (i) of the lemma.

Now let m be any integer. If $m = 1$ or -1 the conclusion of the lemma holds for all integer points $\boldsymbol{y}$. Otherwise denote by $p_1, \ldots, p_s$ the distinct prime factors of m. For each p_i there exists an integer point $\boldsymbol{y}_i$ such that $\phi(\boldsymbol{y}_i) \not\equiv 0 \pmod{p_i}$. Write

$$\boldsymbol{y} = \frac{m'}{p_1}\boldsymbol{y}_1 + \ldots + \frac{m'}{p_s}\boldsymbol{y}_s,$$

where

$$m' = \prod_{i=1}^{s} p_i.$$

Then $\boldsymbol{y}$ is an integer point, and $\phi(\boldsymbol{y}) \not\equiv 0 \pmod{p_i}$ for $i = 1, \ldots, s$, which is the conclusion of the lemma.

3 Exponential sums. Let g_1, g_2 be real numbers satisfying

(5) $$0 < g_1 < f_1 < f_2 < g_2,$$

where f_1, f_2 are the numbers occurring in (4).

We define the exponential sums $T(\alpha)$ and $S(\alpha)$ by

(6) $$T(\alpha) = \sum e(\alpha p),$$

where p runs through the primes in the range $g_1P^2 < p < g_2P^2$, and

(7) $$S(\alpha) = \sum_{\boldsymbol{x} \in P\mathscr{B}} e\big(\alpha\phi_P(\boldsymbol{x})\big),$$

where $\phi_P(\boldsymbol{x})$ is as in (3).

Then we have

(8) $$\mathscr{N}(P) = \int_0^1 S(\alpha) T(-\alpha)\, d\alpha.$$

Denote by $A = [a_{ij}]$ the symmetric matrix associated with the quadratic form $Q(\boldsymbol{x})$, so that

(9) $$Q(\boldsymbol{x}) = \boldsymbol{x}'A\boldsymbol{x} = \sum_{i=1}^{n}\sum_{j=1}^{n} a_{ij}x_ix_j.$$

It follows from Lemma 1 and the hypotheses of Theorem 1 that $2a_{ij}$ is an integer for all pairs of suffixes i, j.

Now define $A_i(\boldsymbol{x})$ by

(10) $$A_i(\boldsymbol{x}) = \sum_{j=1}^{n} a_{ij}x_j,$$

so that for all i the linear form $2A_i(\boldsymbol{x})$ has integer coefficients.

Denote by $\boldsymbol{A}(\boldsymbol{x})$ the vector $\big(A_1(\boldsymbol{x}), \ldots, A_n(\boldsymbol{x})\big)$.

LEMMA 3. *For a fixed box $\mathscr{B}$, we have*

(11) $$|S(\alpha)|^2 \ll \sum_{\boldsymbol{x}} \prod_{i=1}^{n} \min\big(P, \|2\alpha A_i(\boldsymbol{x})\|^{-1}\big),$$

where the sum is over integer points $\boldsymbol{x}$ satisfying $|\boldsymbol{x}| \ll P$.

Proof. We have

$$|S(\alpha)|^2 = \sum_{\boldsymbol{y} \in P\mathscr{B}} \sum_{\boldsymbol{z} \in P\mathscr{B}} e\big(\alpha\phi_P(\boldsymbol{y}) - \alpha\phi_P(\boldsymbol{z})\big) = \sum_{\boldsymbol{z} \in P\mathscr{B}} \sum_{\boldsymbol{x} \in P\mathscr{B} - \boldsymbol{z}} e\big(\alpha\phi_P(\boldsymbol{x}+\boldsymbol{z}) - \alpha\phi_P(\boldsymbol{z})\big),$$

and the box $P\mathscr{B} - \boldsymbol{z}$ is contained in the cube $|\boldsymbol{x}| \ll P$ for a suitable value of the implied constant depending on $\mathscr{B}$. Hence

(12) $$|S(\alpha)|^2 \leqslant \sum_{|\boldsymbol{x}| \ll P} \Big| \sum_{\boldsymbol{z} \in \mathscr{R}(\boldsymbol{x})} e\big(\alpha\phi_P(\boldsymbol{x}+\boldsymbol{z}) - \alpha\phi_P(\boldsymbol{z})\big) \Big|,$$

where $\mathscr{R}(\boldsymbol{x})$ denotes the common part of $P\mathscr{B}$ and $P\mathscr{B} - \boldsymbol{x}$.

Now

$$\phi_P(\boldsymbol{x}+\boldsymbol{z}) - \phi_P(\boldsymbol{z}) = 2\sum_{i=1}^{n} A_i(\boldsymbol{x})z_i + Q(\boldsymbol{x}) + L_P(\boldsymbol{x})$$

and the last two terms on the right-hand side are independent of z. Hence repeated application of the well-known inequality

$$\Big|\sum_{z} e(\lambda z)\Big| \leqslant \min(P, \|\lambda\|^{-1}),$$

where the summation is over any set of $\ll P$ consecutive integers, yields

$$\Big|\sum_{z\in\mathscr{R}(x)} e\big(\alpha\phi_P(x+z)-\alpha\phi_P(x)\big)\Big| = \Big|\sum_{z\in\mathscr{R}(x)} e\Big(2\alpha\sum_{i=1}^{n}A_i(x)z_i\Big)\Big|$$

$$\ll \prod_{i=1}^{n}\min\big(P, \|2\alpha A_i(x)\|^{-1}\big).$$

Now substitution in (12) gives (11).

Throughout the remainder of this paper we shall write $L = \log P$.

LEMMA 4. *Let U be a parameter satisfying*

(13) $$L \ll U \ll PL^{1/4}.$$

Then the hypothesis

(14) $$|S(\alpha)| > P^n L^n U^{-r/2}$$

implies that the number of integer points satisfying

$$|x| \ll P \quad \text{and} \quad \|2\alpha A(x)\| < P^{-1}$$

is

(15) $$\gg P^n L^n U^{-r}.$$

Proof. This follows from Lemma 3 in just the same way as Lemma 3.2 of [1] follows from Lemma 3.1 of that paper.

LEMMA 5. *Under the hypotheses* (13) *and* (14) *of Lemma* 4 *the number of integer points satisfying*

$$|x| \ll UL^{-1/2} \quad \text{and} \quad \|2\alpha A(x)\| \ll UP^{-2}L^{-1/2}$$

is

(16) $$\gg U^{n-r}L^{n/2}.$$

Proof. We apply Lemma 8 of [2] to the symmetric linear forms $2\alpha A(x)$, taking A (of [2]) $= P$, $Z = c_1$ (a suitable constant), and $Z_1 = UP^{-1}L^{-1/2}$. By (15) of Lemma 4

$$V(Z) \gg P^n L^n U^{-r}.$$

Condition (29) of [2] now takes the form

$$cU^{r/n}P^{-1}L^{-1} \leqslant Z_1 \leqslant c_1$$

which is satisfied by our choice of Z_1 if P is large enough. Now (30) of [2] gives

$$V(Z_1) \gg U^{n-r}L^{n/2}$$

which is equivalent to (16).

LEMMA 6. *Under the hypotheses* (13) *and* (14) *of Lemma* 4 *for all sufficiently large P α has a rational approximation a/q satisfying*

(17) $$(a, q) = 1, \quad |q| \leqslant U, \quad |\alpha q - a| < UP^{-2}.$$

Proof. The equation $A(x) = \mathbf{0}$ is identical to the matrix equation $Ax = \mathbf{0}$, and the integer points satisfying this equation form a lattice of dimension $n-r$. Hence the number of integer points in the range $|x| \ll UL^{-1/2}$ which satisfy $A(x) = \mathbf{0}$ is $\ll U^{n-r}L^{-(n-r)/2}$. But (16) of Lemma 5 states that the number of integer points in the range $|x| \ll UL^{-1/2}$ satisfying $\|2\alpha A(x)\| \ll UP^{-2}L^{-1/2}$ is $\gg U^{n-r}L^{n/2}$. Hence for large enough P there is some integer point satisfying $|x| \ll UL^{-1/2}$ and $\|2\alpha A(x)\| \ll UP^{-2}L^{-1/2}$ for which $A(x) \neq \mathbf{0}$. Suppose for instance that $A_i(x) \neq 0$. Then $2A_i(x)$ is a non-zero integer and there exists an integer b such that

$$|2\alpha A_i(x) - b| \ll UP^{-2}L^{-1/2}.$$

Take a/q to be the rational number $b/2A_i(x)$ in its lowest terms. Then

$$|q| \ll A_i(x) \ll |x| \ll UL^{-1/2},$$

and so $|q| \leqslant U$ if P is large enough. Also

$$|\alpha q - a| \leqslant |2\alpha A_i(x) - b| \ll UP^{-2}L^{-1/2},$$

so $|\alpha q - a| < UP^{-2}$ if P is large enough; and a/q satisfies the requirements of the lemma.

4. Minor arcs. Let $\mathscr{E}(U)$ denote the set of all real α in the interval $[0, 1]$ which have a rational approximation satisfying (17), and let $\mathscr{C}\mathscr{E}(U)$ denote the complement of this set relative to $[0, 1]$. We define the minor arcs, $\mathfrak{m}$, to be $\mathscr{C}\mathscr{E}(U_1)$ where

(18) $$U_1 = L^{4n}.$$

LEMMA 7. *If $r \geqslant 3$ we have*

(19) $$\int_{\mathfrak{m}} |S(\alpha)T(-\alpha)|\,d\alpha \ll P^n L^{-2}.$$

Proof. The proof follows the same lines as the proof of Lemma 14 of [5].

The set $\mathscr{E}(U)$ increases with U and, by Dirichlet's theorem on Diophantine approximation, if $U \geqslant P$ it consists of the whole interval $[0, 1]$. Denote by $\mathscr{F}(U)$ the complement of $\mathscr{E}(U)$ relative to $\mathscr{E}(2U)$. Then the interval $[0, 1]$ can be decomposed into

$$\mathscr{E}(U_1), \mathscr{F}(U_1), \mathscr{F}(2U_1), \ldots, \mathscr{F}(2^t U_1),$$

where t is the least integer such that $2^{t+1}U_1 \geqslant P$. Hence $\mathfrak{m}$ is the union of

$$\mathscr{F}(U_1), \mathscr{F}(2U_1), \ldots, \mathscr{F}(2^t U_1),$$

and clearly $t \ll L$.

Now take $U = 2^u U_1$, where $0 \leqslant u \leqslant t$. Then U satisfies (13). If $\alpha \in \mathscr{F}(U)$ then α does not have a rational approximation satisfying (17), and it follows from Lemma 6 that the hypothesis (14) fails to hold for such an α. Thus for all $\alpha \in \mathscr{F}(U)$ we have

$$|S(\alpha)| \leqslant P^n L^n U^{-r/2}.$$

Also

$$|\mathscr{F}(U)| \leqslant |\mathscr{E}(2U)| \leqslant \sum_{1\leqslant q\leqslant 2U} \sum_{a=1}^{q} 2q^{-1} 2UP^{-2} \leqslant 8U^2P^{-2}.$$

It follows that

$$\begin{aligned}\int_{\mathscr{F}(U)} |S(\alpha)T(-\alpha)|d\alpha &\leqslant P^n L^n U^{-r/2} \int_{\mathscr{F}(U)} |T(-\alpha)|\,d\alpha \\ &\leqslant P^n L^n U^{-r/2}\{|\mathscr{F}(U)|\}^{1/2}\Big\{\int_0^1 |T(-\alpha)|^2 d\alpha\Big\}^{1/2} \\ &\ll P^n L^n U^{-r/2}\{U^2P^{-2}\}^{1/2}\{P^2L^{-1}\}^{1/2} \\ &\ll P^n U^{1-r/2} L^{n-1/2} \ll P^n U^{-1/2} L^{n-1/2},\end{aligned}$$

since $r \geqslant 3$.

Since there are $\ll L$ sets $\mathscr{F}(U)$ and this estimate applies to each of them and the least value of U is $U_1 = L^{4n}$, we deduce that

$$\int_{\mathfrak{m}} |S(\alpha)T(-\alpha)|\,d\alpha \ll P^n L^{-n+1/2} \ll P^n L^{-2},$$

which is (19).

5. Major arcs. We denote by $\mathfrak{M}_{a,q}$ the interval (²) for α defined by

(20) $$\left\|\alpha - \frac{a}{q}\right\| < P^{-2}L^k, \quad 0 \leqslant \alpha \leqslant 1,$$

where k is a suitable constant, and we denote by $\mathfrak{M}$ the union of these intervals for

$$0 \leqslant a < q, \quad (a, q) = 1, \quad 1 \leqslant q \leqslant L^k.$$

The intervals (20) are disjoint for large enough P, and if we choose $k \geqslant 4n$ then $\mathfrak{M}$ contains $\mathscr{E}(U_1)$ where U_1 is given by (18).

LEMMA 8. *If α is in $\mathfrak{M}_{a,q}$ and $\beta = \alpha - a/q$, then we have*

(21) $$S(\alpha) = q^{-n} S_{a,q}(P) I(\beta) + O(P^{n-1}L^{2k}),$$

where

$$S_{a,q}(P) = \sum_{x(\mathrm{mod}\,q)} e\Big(\frac{a}{q}\phi_P(x)\Big),$$

and

$$I(\beta) = \int_{P\mathscr{B}} e\big(\beta\phi_P(\xi)\big)\,d\xi.$$

(²) In fact $\mathfrak{M}_{0,1}$ consists of two intervals, one at each end of the interval $[0, 1]$.

Proof. Except for some trivial differences this is the same as the proof of Lemma 15 of [5].

Writing $x = qy + z$ we have

(22) $$S(\alpha) = \sum_{z(\mathrm{mod}\,q)} e\Big(\frac{a}{q}\phi_P(z)\Big) \sum_y e\big(\beta\phi_P(qy+z)\big),$$

where the second summation is over the integer points in the box $(Pq^{-1})\mathscr{B} - q^{-1}z$. This box can be regarded as a union of $V(Pq^{-1})^n + O\big((Pq^{-1})^{n-1}\big)$ cubes of side 1, together with a boundary zone which has volume $O\big((Pq^{-1})^{n-1}\big)$ and contains $O\big((Pq^{-1})^{n-1}\big)$ integer points. Each cube corresponds to a single term of the sum, and we can replace this term by

$$\int e\big(\beta\phi_P(q\eta+z)\big)\,d\eta + O(|\beta|qP),$$

since, as was remarked in § 1, the coefficients of the linear part of ϕ_P are $O(P)$. The integral here is taken over the cube in question. Putting together these integrals and allowing for the boundary zone we obtain

$$S(\alpha) = q^{-n}S_{a,q}(P)I(\beta) + O\big(q^n|\beta|qP(Pq^{-1})^n\big) + O\big(q^n(Pq^{-1})^{n-1}\big).$$

Since $|\beta| < P^{-2}L^k$ and $q \leqslant L^k$, this gives (21).

LEMMA 9. *If α is in $\mathfrak{M}_{a,q}$ we have*

(23) $$T(\alpha) = \frac{\mu(q)}{\varphi(q)} I_1(\beta) + O\big(P^2\exp(-c_2L^{1/2})\big)$$

for some positive constant c_2, where

$$I_1(\beta) = \int_{g_1P^2}^{g_2P^2} \frac{e(\beta x)}{\log x}\,dx.$$

Proof. This is just Lemma 16 of [5], and a proof is given in [6], chapter VI, Satz 3.3.

LEMMA 10. *If $(a, q) = 1$ we have*

(24) $$|S_{a,q}(P)| \ll q^{n-r/2}(\log q)^n,$$

where the implied constant is independent of a, q, and P.

Proof. We note that the implied constants occurring in Lemmas 3, 4, 5, and 6 depend only on n, $\mathscr{B}$, and the coefficients, a_{ij}, of Q, and that they in no way depend on the other coefficients of ϕ_P. Hence we can apply Lemma 6 to the exponential sum $S_{a,q}(P)$ with P (of Lemma 6) $= q$, $U = q-1$, $\alpha = a/q$, and a unit cube in place of $\mathscr{B}$. The inequalities (13) are then satisfied, but a/q has no rational approximation satisfying (17), for if a'/q' is any rational number with $q' \leqslant q-1$ then $a'/q' \neq a/q$ (because $(a,q)=1$) and so

$$\left|q'\frac{a}{q}-a'\right| \geqslant \frac{1}{q} > \frac{q-1}{q^2}.$$

We deduce that inequality (14) does not hold with this choice of α, P, U, and $\mathscr{B}$ provided that $q > c_3$, where c_3 is a large constant. Thus for $q > c_3$ we have

$$|S_{a,q}(P)| \leqslant q^n(\log q)^n(q-1)^{-r/2} \ll q^{n-r/2}(\log q)^n.$$

For $q \leqslant c_3$ we have the trivial estimate

$$|S_{a,q}(P)| \leqslant q^n \leqslant c_3^n.$$

Hence in either case (24) holds.

LEMMA 11. *If $r \geqslant 3$ then for a suitable constant $c_4 > 0$ we have*

$$(25)\qquad \int_{\mathfrak{M}} S(\alpha)T(-\alpha)\,d\alpha = \{\mathfrak{S}(P)+O(L^{-c_4})\}\int_{|\beta|<P^{-2}L^k} I(\beta)I_1(-\beta)\,d\beta+O(P^nL^{-2}),$$

where

$$(26)\qquad \mathfrak{S}(P) = \sum_{q=1}^{\infty}\sum_{\substack{a=1\\(a,q)=1}}^{q}\frac{\mu(q)}{\varphi(q)}q^{-n}S_{a,q}(P).$$

Proof. The proof follows the same lines as the proof of Lemma 17 of [5] with only trivial differences, Lemmas 8, 9, and 10 being used in place of Lemmas 15, 16, and 13 respectively of [5].

6. The singular series.

LEMMA 12. *With the hypotheses of Theorem 1 we have*

$$1 \ll \mathfrak{S}(P) \ll 1.$$

Proof. It follows from (26) and (24) of Lemma 10 with $r \geqslant 3$ that the series $\mathfrak{S}(P)$ is uniformly absolutely convergent. Also, by well-known arguments,

$$\sum_{\substack{a=1\\(a,q)=1}}^{q} q^{-n}S_{a,q}(P)$$

is a multiplicative function of q. Hence, by (26),

$$(27)\qquad \mathfrak{S}(P) = \prod_{\tilde{\omega}}\chi(\tilde{\omega},P),$$

where $\tilde{\omega}$ runs through the primes and

$$(28)\qquad \chi(\tilde{\omega},P) = 1-\frac{1}{\tilde{\omega}-1}\tilde{\omega}^{-n}\sum_{a=1}^{\tilde{\omega}-1}S_{a,\tilde{\omega}}(P).$$

The infinite product (27) converges uniformly and so there exists a constant c_5 such that

$$(29)\qquad \tfrac{1}{2} < \prod_{\tilde{\omega}>c_5}\chi(\tilde{\omega},P) < 2.$$

Also for any integer point $\boldsymbol{x}$ and any prime $\tilde{\omega}$ we have

$$\sum_{a=1}^{\tilde{\omega}-1} e\left(\frac{a}{\tilde{\omega}}\phi_P(\boldsymbol{x})\right) = \begin{cases}\tilde{\omega}-1 & \text{if} \quad \phi_P(\boldsymbol{x}) \equiv 0 \pmod{\tilde{\omega}},\\ -1 & \text{if} \quad \phi_P(\boldsymbol{x}) \not\equiv 0 \pmod{\tilde{\omega}}.\end{cases}$$

Hence

$$(30)\qquad \sum_{a=1}^{\tilde{\omega}-1} S_{a,\tilde{\omega}}(P) = \sum_{a=1}^{\tilde{\omega}-1}\sum_{\boldsymbol{x}(\mathrm{mod}\,\tilde{\omega})} e\left(\frac{a}{\tilde{\omega}}\phi_P(\boldsymbol{x})\right) = (\tilde{\omega}^n-M)(\tilde{\omega}-1)-M,$$

where M is the number of integer points $\boldsymbol{x}$, distinct $(\mathrm{mod}\,\tilde{\omega})$, for which

$$\phi_P(\boldsymbol{x}) \not\equiv 0 \pmod{\tilde{\omega}}.$$

Substituting (30) in (28) we obtain

$$\chi(\tilde{\omega},P) = \frac{M}{\tilde{\omega}^{n-1}(\tilde{\omega}-1)}.$$

Now trivially $M \leqslant \tilde{\omega}^n$, and it follows from Lemma 2, with $\tilde{\omega}$ in place of m, that $M \geqslant 1$ for all sufficiently large P; and hence we obtain

$$\frac{1}{\tilde{\omega}^{n-1}(\tilde{\omega}-1)} \leqslant \chi(\tilde{\omega},P) \leqslant \frac{\tilde{\omega}}{\tilde{\omega}-1},$$

and so $\prod_{\tilde{\omega}\leqslant c_5}\chi(\tilde{\omega},P)$ lies between fixed positive bounds. On combining this last statement with (27) and (29) we obtain the result of the lemma.

7. Proof of Theorem 1 and a corollary.

We observed in § 5 that if k is chosen to be $\geqslant 4n$, then $\mathfrak{M}$ contains $\mathscr{E}(U_1)$, from which it follows that

$$\mathscr{C}\mathfrak{M} \subset \mathscr{C}\mathscr{E}(U_1) = \mathfrak{m}.$$

Hence, on dividing the range of integration in (8) into the two parts $\mathfrak{M}$ and $\mathscr{C}\mathfrak{M}$, we deduce from (8), (19), and (25), which are valid under the hypotheses of Theorem 1, that

$$(31)\qquad \mathscr{N}(P) = \{\mathfrak{S}(P)+O(L^{-c_4})\}J(P)+O(P^nL^{-2}),$$

where

$$J(P) = \int_{|\beta|<P^{-2}L^k} I(\beta) I_1(-\beta)\, d\beta. \tag{32}$$

As in § 10 of [5] we have

$$I_1(-\beta) = \frac{P^2}{2L} \int_{g_1}^{g_2} e(-\beta P^2 x)\, dx + O\big(P^2 L^{-2} \min(1, |\beta P^2|^{-1})\big),$$

and we multiply this approximation by $I(\beta)$, as defined in the statement of Lemma 8, and substitute the resulting product in (32). The main term is

$$\frac{P^2}{2L} \int_{|\beta|<P^{-2}L^k} \Big\{ \int_{P\mathscr{B}} e\big(\beta\phi_P(\boldsymbol{\xi})\big) d\boldsymbol{\xi} \Big\} \Big\{ \int_{g_1}^{g_2} e(-\beta P^2 x)\, dx \Big\}\, d\beta = \frac{P^n}{2L} J_1(P),$$

where

$$J_1(P) = \int_{-L^k}^{L^k} \Big\{ \int_{\mathscr{B}} e\big(\gamma P^{-2}\phi_P(P\boldsymbol{\xi})\big) d\boldsymbol{\xi} \Big\} \Big\{ \int_{g_1}^{g_2} e(-\gamma x)\, dx \Big\}\, d\gamma, \tag{33}$$

and the error term is majorised by

$$P^n P^2 L^{-2} \int_{|\beta|<P^{-2}L^k} \min(1, |\beta P^2|^{-1})\, d\beta \ll P^{n+2} L^{-2} P^{-2} \log L \ll P^n L^{-2} \log L.$$

Thus we have

$$J(P) = \frac{P^n}{2L} J_1(P) + O(P^n L^{-2} \log L). \tag{34}$$

Interchanging the order of integration in (33) and performing the integration with respect to γ we have

$$J_1(P) = \int_{\mathscr{B}} d\boldsymbol{\eta} \int_{g_1}^{g_2} dx \int_{-L^k}^{L^k} e\big(\gamma(P^{-2}\phi_P(P\boldsymbol{\eta}) - x)\big)\, d\gamma$$

$$= \int_{\mathscr{B}} d\boldsymbol{\eta} \int_{g_1}^{g_2} \frac{\sin 2\pi L^k \big(P^{-2}\phi_P(P\boldsymbol{\eta}) - x\big)}{\pi\big(P^{-2}\phi_P(P\boldsymbol{\eta}) - x\big)}\, dx$$

$$= \int_{\mathscr{B}} d\boldsymbol{\eta} \int_{a(\boldsymbol{\eta},P)}^{b(\boldsymbol{\eta},P)} \frac{\sin 2\pi L^k t}{\pi t}\, dt,$$

where

$$a(\boldsymbol{\eta}, P) = g_1 - P^{-2}\phi_P(P\boldsymbol{\eta}),$$

and

$$b(\boldsymbol{\eta}, P) = g_2 - P^{-2}\phi_P(P\boldsymbol{\eta}).$$

It follows from (4) and (5) that for all large P and all $\boldsymbol{\eta} \in \mathscr{B}$

$$a(\boldsymbol{\eta}, P) \leqslant g_1 - f_1 < 0$$

and

$$b(\boldsymbol{\eta}, P) \geqslant g_2 - f_2 > 0.$$

Hence the limit of the inner integral is 1 as $P \to \infty$, and this limit is uniform in $\boldsymbol{\eta}$. Thus

$$\lim_{P\to\infty} J_1(P) = \int_{\mathscr{B}} d\boldsymbol{\eta} = V. \tag{35}$$

It now follows from (31), (34), and (35) that

$$\mathscr{N}(P) = \frac{VP^n}{2L} \mathfrak{S}(P) + o(P^n L^{-1}) \quad \text{as} \quad P \to \infty$$

and, by Lemma 12, $\mathfrak{S}(P)$ lies between fixed positive bounds. This completes the proof of Theorem 1.

It will be convenient for later applications to have the following straightforward corollary to Theorem 1 stated explicitly.

COROLLARY. *Let*

$$\phi(\boldsymbol{x}) = Q(\boldsymbol{x}) + L(\boldsymbol{x}) + N$$

be a quadratic polynomial in n variables with constant rational coefficients whose numerators have no common factor. Suppose that the value of ϕ is integral at every integer point, and that there is some integer point at which the value of ϕ is odd. Suppose also that $Q(\boldsymbol{x})$, the quadratic part of $\phi(\boldsymbol{x})$, has rank $\geqslant 3$ and is neither negative definite nor negative semi-definite. Then for any box $\mathscr{B}$ with volume V in n dimensional space such that $Q(\boldsymbol{x})$ is positive in and on the boundary of $\mathscr{B}$ the number, $\mathscr{N}(P)$, of integer points $\boldsymbol{x}$ in the expanded box $P\mathscr{B}$ for which $\phi(\boldsymbol{x})$ is a prime satisfies

$$\mathscr{N}(P) \sim \frac{VP^n}{\log P^2} \mathfrak{S}$$

where $\mathfrak{S}$ is a positive constant.

Proof. Let e_1, e_2 be the lower and upper bounds of $Q(\boldsymbol{x})$ for $\boldsymbol{x}$ in $\mathscr{B}$, and let f_1, f_2 be real numbers satisfying

$$0 < f_1 < e_1 < e_2 < f_2.$$

For $\boldsymbol{x}$ in $\mathscr{B}$,

$$\phi(P\boldsymbol{x}) = P^2 Q(\boldsymbol{x}) + O(P)$$

and hence for $\boldsymbol{y}$ in $P\mathscr{B}$ and large enough P we have

$$f_1 P^2 < \phi(\boldsymbol{y}) < f_2 P^2.$$

Thus ϕ satisfies all the requirements of Theorem 1.

To obtain the result of the corollary it only remains to observe that since the coefficients of ϕ are constant, the exponential sums $S_{a,q}(P)$

defined in Lemma 8 are independent of P; hence, by (26), $\mathfrak{S} = \mathfrak{S}(P)$ is a constant, and it follows from Lemma 12 that this constant is positive.

8. Lemmas. In this section we derive a number of results about polynomials which are needed in the proof of Theorem 2.

LEMMA 13. *If $\phi(\boldsymbol{x}) = \phi(x_1, \ldots, x_n)$ is a quadratic polynomial in n variables with rational coefficients which satisfies the following four conditions:*

(i) *$\phi(\boldsymbol{x})$ is an integer at every integer point $\boldsymbol{x}$,*

(ii) *the numerators of the coefficients of ϕ in their lowest terms have no common factor,*

(iii) *there is an integer point $\boldsymbol{x}$ for which*

$$\phi(\boldsymbol{x}) \not\equiv 0 \pmod 2,$$

(iv) *the variable x_1 occurs in the linear part of ϕ but not in the quadratic part;*

then the value of $\phi(\boldsymbol{x})$ is prime for $\gg P^{n+1}/\log P$ of the integer points $\boldsymbol{x}$ satisfying

$$|x_1| < P^2,$$

$$|x_i| < P \quad (i = 2, \ldots, n),$$

where P is a large parameter.

Proof. By condition (iv), ϕ is of the form

$$\phi(x_1, \ldots, x_n) = \phi_1(x_2, \ldots, x_n) + ax_1, \tag{36}$$

where ϕ_1 is a quadratic polynomial in $x_2, \ldots, x_n$ and a is a constant, and it follows from condition (i) that a is an integer and $\phi_1(x_2, \ldots, x_n)$ is integral for integer values of the variables $x_2, \ldots, x_n$. By (i), (ii), and (iii), ϕ satisfies the conditions of Lemma 2, and so there exists an integer point $\boldsymbol{y} = (y_1, \ldots, y_n)$ such that $(\phi(\boldsymbol{y}), a) = 1$. If now $\boldsymbol{x} = (x_2, \ldots, x_n)$ is any integer point in $(n-1)$-dimensional space satisfying

$$(x_2, \ldots, x_n) \equiv (y_2, \ldots, y_n) \pmod a, \tag{37}$$

we have

$$(\phi_1(x_2, \ldots, x_n), a) = 1. \tag{38}$$

Denote by $Q_1(\boldsymbol{x}) = Q_1(x_2, \ldots, x_n)$ the quadratic part of ϕ_1 (which is also the quadratic part of ϕ), and choose a box in $(n-1)$-dimensional space such that for all points ξ in $\mathscr{B}$

$$|\xi| < 1 \tag{39}$$

and

$$|Q_1(\xi)| < \tfrac{1}{4}|a|. \tag{40}$$

This can be done, for example, by taking $\mathscr{B}$ to be a sufficiently small box containing the origin.

Take $\boldsymbol{x}$ to be any integer point in the expanded box $P\mathscr{B}$ satisfying (37). Then $\boldsymbol{x}$ satisfies (38) and also, by (40), we have

$$|\phi_1(\boldsymbol{x})| < P^2 \tfrac{1}{4}|a| + O(P) < P^2 \tfrac{1}{2}|a|$$

for large enough P, so that the range

$$[-P^2|a| + \phi_1(\boldsymbol{x}), P^2|a| + \phi_1(\boldsymbol{x})]$$

includes the range

$$[0, \tfrac{1}{2}P^2|a|].$$

We now apply the well-known theorem due to de la Vallee Poussin and Landau on the number of primes in an arithmetic progression (see, for example, [3], Satz 382) and deduce that the number of primes p satisfying

$$-P^2|a| + \phi_1(\boldsymbol{x}) < p < P^2|a| + \phi_1(\boldsymbol{x})$$

and

$$p \equiv \phi_1(\boldsymbol{x}) \pmod a$$

is

$$\gg \frac{P^2}{\log P}, \tag{41}$$

this estimate being uniform in $\boldsymbol{x}$.

Also the number of integer points $\boldsymbol{x}$ in $P\mathscr{B}$ satisfying (37) is

$$\gg P^{n-1} \tag{42}$$

and, by (39), all these points satisfy $|\boldsymbol{x}| < P$.

Now from (36), (41), and (42) we obtain the result that the number of integer points $\boldsymbol{x}$ with

$$|x_1| < P^2, \quad |x_i| < P \quad (i = 2, \ldots, n)$$

for which $\phi(\boldsymbol{x})$ is prime is $\gg P^{n+1}/\log P$.

LEMMA 14. *Let $L(\boldsymbol{x}) = l_0 + l_1x_1 + \ldots + l_nx_n$ be a non-constant linear polynomial in $x_1, \ldots, x_n$ such that $l_0, l_1, \ldots, l_n$ are integers having no common factor, and let $\mathscr{A}$ be a box in n dimensional space. If there is a point $\boldsymbol{a} = (a_1, \ldots, a_n)$ in the interior of $\mathscr{A}$ such that $l_1a_1 + \ldots + l_na_n \geqslant 0$, then the number of integer points $\boldsymbol{x}$ in $P\mathscr{A}$ for which $L(\boldsymbol{x})$ is prime is $\gg P^n/\log P$.*

Proof. Since $L(\boldsymbol{x})$ is not constant, we can find a point $\boldsymbol{b}$ in $\mathscr{A}$ such that $l_1b_1 + \ldots + l_nb_n > 0$, and then we can choose a small box $\mathscr{B}$ containing

b and contained in $\mathscr{A}$ such that $l_1\xi_1+\ldots+l_n\xi_n \geqslant 0$ for all points $\xi\in\mathscr{B}$. We shall in fact obtain the result of the lemma when x is restricted to lie in the box $P\mathscr{B}$.

We denote by $\mathscr{B}^1$ the projection of $\mathscr{B}$ on the x_1 axis, and by $\mathscr{B}^{n-1}$ the projection of $\mathscr{B}$ on the $(x_2, \ldots, x_n)$ hyperplane, and we write

$$L_1(x_2, \ldots, x_n) = l_0+l_2x_2+\ldots+l_nx_n$$

so that

$$L(x) = L_1(x_2, \ldots, x_n)+l_1x_1. \tag{43}$$

Since the coefficients of $L(x)$ have no common factor, we can find an integer point $(y_2, \ldots, y_n)$ in $(n-1)$-dimensional space such that

$$\big(L_1(y_2, \ldots, y_n), l_1\big) = 1,$$

and then for any integer point $(x_2, \ldots, x_n)$ satisfying

$$(x_2, \ldots, x_n) \equiv (y_2, \ldots, y_n) \pmod{l_1}$$

we have

$$\big(L_1(x_2, \ldots, x_n), l_1\big) = 1. \tag{44}$$

Hence the number of integer points $(x_2, \ldots, x_n)$ in $P\mathscr{B}^{n-1}$ satisfying (44) is

$$\gg P^{n-1}. \tag{45}$$

For each of these points the interval

$$l_1P\mathscr{B}^1+L_1(x_2, \ldots, x_n) \tag{46}$$

(i.e. the interval $l_1P\mathscr{B}^1$ translated by an amount $L_1(x_2, \ldots, x_n)$) has length a fixed multiple of P. Also for $(x_2, \ldots, x_n)$ in $P\mathscr{B}^{n-1}$ the interval (46) is bounded above by a constant multiple of P and is bounded below by the constant l_0.

It follows from the theorem cited in the previous lemma on the number of primes in an arithmetic progression that the number of primes p in the interval (46) satisfying

$$p \equiv L_1(x_2, \ldots, x_n) \pmod{l_1}$$

is

$$\gg \frac{P}{\log P}, \tag{47}$$

this estimate being uniform in $x_2, \ldots, x_n$.

The conclusion of the lemma now follows from (43), (45), and (47).

LEMMA 15. *Let $\phi_1(x_1, \ldots, x_n), \ldots, \phi_r(x_1, \ldots, x_n)$ be r polynomials with integer coefficients in the n variables $x_1, \ldots, x_n$ such that $\phi_1, \ldots, \phi_r$ have no common factor and ϕ_1 is not constant, and let $U_1, \ldots, U_n$ be n functions of P tending to infinity with P and each bounded above by a fixed power of P. Then for any $\varepsilon > 0$ the number of integer points x satisfying*

$$|x_i| < U_i \quad (i = 1, \ldots, n) \tag{48}$$

and

$$\phi_1(x)|\phi_j(x) \quad (j = 2, \ldots, r) \tag{49}$$

is

$$\ll \max_{1\leqslant i\leqslant n} U_i^{-1}UP^{\varepsilon}, \tag{50}$$

where

$$U = \prod_{i=1}^{n} U_i.$$

Proof. This is a generalization of Lemma 11 of [2] and method of proof is the same.

Since ϕ_1 is not constant, we can suppose, by permuting the variables if necessary, that ϕ_1 is not a polynomial in $x_2, \ldots, x_n$ only. Also, since $\phi_1, \ldots, \phi_r$ have no common factor, it follows from Satz 101 of [4] that there exist polynomials $\psi_1(x_1, \ldots, x_n), \ldots, \psi_r(x_1, \ldots, x_n), H(x_2, \ldots, x_n)$ with integer coefficients and with H not identically zero such that

$$\phi_1\psi_1+\ldots+\phi_r\psi_r = H$$

identically.

The number of integer points x satisfying (48) for which $H(x_2, \ldots, x_n) = 0$ is $\ll \max_{2\leqslant i\leqslant n} U_i^{-1}U$, and for x satisfying (48) $|H(x_2, \ldots, x_n)|$ is bounded by a fixed power of P and so if $H(x_2, \ldots, x_n) \neq 0$ it has $\ll P^{\varepsilon}$ divisors. If x also satisfies (49) we have

$$\phi_1(x)\,|\,H(x_2, \ldots, x_n),$$

and so for any particular set of values of $x_2, \ldots, x_n$ with $H(x_2, \ldots, x_n) \neq 0$ there are $\ll P^{\varepsilon}$ possible values for $\phi_1(x)$ with x satisfying (48) and (49). If c is any one of these values, the equation $\phi_1 = c$ can be written in the form

$$J_0(x_2, \ldots, x_n)x_1^k+J_1(x_2, \ldots, x_n)x_1^{k-1}+\ldots+J_k(x_2, \ldots, x_n) = 0,$$

where $k \geqslant 1$ and J_0 is not identically zero and is independent of c. The number of possibilities for $x_2, \ldots, x_n$ for which $J_0 = 0$ is $\ll \max_{2\leqslant i\leqslant n} U_i^{-1}U_1^{-1}U$ and for these there are $\ll U_1$ possibilities for x_1. Otherwise for any $x_2, \ldots, x_n$ there are $\ll P^{\varepsilon}$ possibilities for c and then at most k possibilities for x_1; and the total number of sets of integers $x_2, \ldots, x_n$ satisfying $|x_i| < U_i$ $(i = 2, \ldots, n)$ is $\ll U_1^{-1}U$.

Hence counting all the possibilities we obtain the result that the number of integer points $\boldsymbol{x}$ for which (48) and (49) hold satisfies (50).

LEMMA 16. *Let*

$$\phi(x_1, \ldots, x_n) = \phi(\boldsymbol{x}) = Q(\boldsymbol{x}) + L(\boldsymbol{x}) + N$$

be a quadratic polynomial with integer coefficients, irreducible over the rationals, whose coefficients have no common factor and for which there is some integer point $\boldsymbol{x}$ with $\phi(\boldsymbol{x}) \not\equiv 0 \pmod 2$. If Q, the quadratic part of ϕ, factorises over the rationals into distinct linear factors then $\phi(\boldsymbol{x})$ represents infinitely many primes for integer points $\boldsymbol{x}$.

Proof. Since $Q(\boldsymbol{x})$ factorises into distinct factors, there is an integral unimodular transformation taking $Q(\boldsymbol{x})$ into $x_1(ax_1+bx_2)$, where a and b are integers with $b \neq 0$. Such a transformation is permissible as it affects neither the hypotheses nor the conclusion of the lemma. If after this transformation ϕ contains a variable other than x_1, x_2, then it satisfies the conditions of Lemma 13 and our result follows. Hence we can suppose that ϕ is of the form

$$x_1(ax_1+bx_2)+cx_1+dx_2+e,$$

where all the coefficients are integers and $b \neq 0$.

Denote by m the product of the coefficients of this polynomial. The quadratic polynomial ϕ satisfies the conditions of Lemma 2 and so there exist integers X_1, X_2 such that

$$(51) \qquad \big(\phi(X_1, X_2), m\big) = 1.$$

We now make the substitution $x_1 = X_1+my$ and obtain

$$\begin{aligned}(52) \quad \phi(x_1, x_2) &= x_1(ax_1+bx_2)+cx_1+dx_2+e = x_2(bx_1+d)+ax_1^2+cx_1+e \\ &= x_2(bmy+bX_1+d)+am^2y^2+2amX_1y+cmy+cX_1+e+aX_1^2 \\ &= x_2L_1(y)+Q_1(y).\end{aligned}$$

Here $L_1(y)$ is a linear polynomial in y which is not constant, since $b \neq 0$, and $Q_1(y)$ is a quadratic polynomial in y.

The polynomials bx_1+d and $ax_1^2+cx_1+e$ have no common factor as, by (52), such a factor would divide $\phi(x_1, x_2)$, contradicting the irreducibility of ϕ. Hence there exist integers A, B, C, D with $D \neq 0$ such that

$$(53) \qquad (Ax_1+B)(bx_1+d)+C(ax_1^2+cx_1+e) = D,$$

and so for any integer x_1 the h.c.f. of bx_1+d and $ax_1^2+cx_1+e$ divides D. Thus for any integer y the h.c.f. of $L_1(y)$ and $Q_1(y)$ divides D.

Denote by λ_1 the h.c.f. of the coefficients of L_1; then $\lambda_1 | bm$ and so $\lambda_1 | m^2$. By Dirichlet's theorem on primes in arithmetic progression there are infinitely many integers y for which $L_1(y) = \lambda_1 p$, where p is prime, and so we can choose some integer, Y say, for which $L_1(Y) = \lambda_1 p$ and p is a prime not dividing D. For this Y the h.c.f. of $L_1(Y)$ and $Q_1(Y)$ is a factor of λ_1.

On the other hand it follows from (51) that $\phi(X_1+mY, X_2)$ is prime to m and hence, by (52), that the h.c.f. of $L_1(Y)$ and $Q_1(Y)$ is prime to m. Hence $\big(L_1(Y), Q_1(Y)\big) = 1$, and so, again by Dirichlet's theorem, $x_2L_1(Y)+Q_1(Y)$ is prime for infinitely many integers x_2, which, by (52), is the result of the lemma.

LEMMA 17. *If $Q_0(x_1, \ldots, x_n), Q_1(x_1, \ldots, x_n), \ldots, Q_r(x_1, \ldots, x_n)$ are quadratic forms, not all vanishing identically, with rational coefficients in the variables $x_1, \ldots, x_n$, then at least one of the following three propositions holds:*

(I) *there are $\ll P^{r-1}$ sets of integers $\lambda_1, \ldots, \lambda_r$ with $|\lambda_i| < P$ $(i = 1, \ldots, r)$ such that the rank of $Q_0+\lambda_1Q_1+\ldots+\lambda_rQ_r$ is $\leqslant 2$;*

(II) *there is an integral unimodular transformation of coordinates taking $Q_0, Q_1, \ldots, Q_r$ into $Q_0', Q_1', \ldots, Q_r'$, where the forms $Q_0', Q_1', \ldots, Q_r'$ do not involve the variables $x_3, \ldots, x_n$;*

(III) *$Q_0, Q_1, \ldots, Q_r$ have a common linear factor with rational coefficients.*

Proof. We express each of $Q_0, Q_1, \ldots, Q_r$ in diagonal form; that is we write each of these forms as a sum of rational multiples of squares of linear forms with rational coefficients. Denote by $L_1, \ldots, L_s$ the complete set of linear forms arising from $Q_0, \ldots, Q_r$ in this way.

First we show that if no three of the linear forms $L_1, \ldots, L_s$ are linearly independent over the rationals then (II) holds.

Write $L_1 = a_1x_1+\ldots+a_nx_n$. We can suppose, by taking a rational multiple of L_1 if necessary, that $a_1, a_2, \ldots, a_n$ are integers having no common factor, and then there exists an integral unimodular transformation taking L_1 into x_1. If on making this substitution $L_2, \ldots, L_s$ all become multiples of x_1 we have (II). Otherwise one of these linear forms, say L_2, is of the shape $L_2 = b_1x_1+b_2x_2+\ldots+b_nx_n$, where $b_2, \ldots, b_n$ are not all zero. Taking a rational multiple of L_2 if necessary, we can suppose that $b_2, \ldots, b_n$ are integers having no common factor, and then there is an integral unimodular transformation fo the variables $x_2, \ldots, x_n$ taking $b_2x_2+\ldots+b_nx_n$ into x_2. This transformation takes L_2 into $b_1x_1+x_2$ and, since we are supposing that no three of the linear forms $L_1, \ldots, L_s$ are linearly independent, it takes all the remaining linear forms into linear combinations of x_1 and x_2. Thus (II) holds.

To prove the lemma we can now assume that at least three of the linear forms $L_1, \ldots, L_s$ are linearly independent and that (I) does not hold and show that these assumptions imply that (III) holds.

If for any real numbers $\lambda_0, \lambda_1, \ldots, \lambda_r$ the quadratic form $\lambda_0 Q_0 + \lambda_1 Q_1 + \ldots + \lambda_r Q_r$ has rank $\geqslant 3$ then (I) holds, for in that case the 3×3 minors of the matrix of the quadratic form $Q_0 + \lambda_1 Q_1 + \ldots + \lambda_r Q_r$, considered as polynomials in $\lambda_1, \ldots, \lambda_r$, are not all identically zero, and hence at least one of these minors vanishes for $\ll P^{r-1}$ of the sets of integers $\lambda_1, \ldots, \lambda_r$ with $|\lambda_i| < P$ $(i = 1, \ldots, r)$.

Thus we can now suppose that each of the quadratic polynomials $Q_0, Q_1, \ldots, Q_r$ has rank $\leqslant 2$, and we consider separately the different cases that can arise. In each case we shall suppose that the linear forms $L_1, \ldots, L_s$ have been ordered in such a way that L_1, L_2, L_3 are linearly independent. For the remainder of this proof a, b, c, etc. will denote non-zero rational numbers.

Case 1. $Q_i = aL_1^2$, $Q_j = bL_2^2$, and $Q_k = cL_3^2$ each have rank 1 and L_1, L_2, L_3 are linearly independent.

In this case the quadratic form $Q_i + Q_j + Q_k$ has rank 3, and so, by our remark above, (I) holds.

Case 2. $Q_i = aL_1^2 + bL_2^2$ and $Q_j = cL_3^2$ have ranks 2 and 1 respectively and L_1, L_2, L_3 are linearly independent.

In this case $Q_i + Q_j$ has rank 3, and so again (I) holds.

Case 3. $Q_i = aL_1^2 + bL_2^2$ and $Q_j = cL_3^2 + dL_4^2$ both have rank 2 and L_1, L_2, L_3, L_4 are linearly independent.

Here $Q_i + Q_j$ has rank 4, again giving (I).

Case 4. $Q_i = aL_1^2 + bL_2^2$ and $Q_j = cL_3^2 + dL_4^2$ both have rank 2, L_1, L_2, L_3 are linearly independent, and L_4 is a linear combination of L_1, L_2, and L_3.

In this case there is a rational non-singular transformation taking Q_i and Q_j into $ay_1^2 + by_2^2$ and $cy_3^2 + d(l_1y_1 + l_2y_2 + l_3y_3)^2$ respectively, where l_1, l_2, l_3 are rationals with l_1 and l_2 not both zero. If (I) does not hold, then $\lambda Q_i + \mu Q_j$ has rank $\leqslant 2$ for all real λ, μ and so the determinant of $\lambda Q_i + \mu Q_j$ vanishes for all real λ, μ. This determinant is:

$$\begin{vmatrix} \lambda a + \mu d l_1^2 & \mu d l_1 l_2 & \mu d l_1 l_3 \\ \mu d l_1 l_2 & \lambda b + \mu d l_2^2 & \mu d l_2 l_3 \\ \mu d l_1 l_3 & \mu d l_2 l_3 & c + \mu d l_3^2 \end{vmatrix}.$$

This is a polynomial in λ and μ and since it is zero for all real λ, μ it is identically zero. The coefficient of $\lambda^2\mu$ in this polynomial is $ab(c + dl_3^2)$ and hence, since $ab \neq 0$, we must have

$$c = -dl_3^2. \tag{54}$$

Also the coefficient of $\lambda\mu^2$ is $cd(al_2^2 + bl_1^2)$, and so $al_2^2 + bl_1^2 = 0$, whence

$$\frac{l_1^2}{a} = -\frac{l_2^2}{b}.$$

Using (54) and (55) we can write Q_i and Q_j as

$$A(l_1^2 y_1^2 - l_2^2 y_2^2)$$

and

$$d(l_1y_1 + l_2y_2 + l_3y_3)^2 - dl_3^2 y_3^2$$

respectively, where A is a non-zero rational number, and these two polynomials have the common linear factor $l_1y_1 + l_2y_2$ with rational coefficients.

Hence another rational non-singular transformation takes Q_i and Q_j into z_1z_2 and z_1z_3 respectively.

Now if $Q_k = eL_5^2 + fL_6^2$ is another of the quadratic forms $Q_0, \ldots, Q_r$ with rank 2, we need to show that if (I) does not hold then z_1 is also a factor of Q_k. Neither L_1, L_2, L_5, L_6 nor L_3, L_4, L_5, L_6 can be a linearly independent set of linear forms, for if so we should have the situation of case 3 which leads to (I). On the other hand it is impossible for both L_5 and L_6, being linearly independent, to be linear combinations of L_1, L_2 and of L_3, L_4. Hence, on interchanging the roles of Q_i and Q_j if necessary, we can suppose that just three of the forms L_1, L_2, L_5, L_6 are linearly independent. But this is just the situation considered above, and we deduce, on the hypothesis that (I) does not hold, that Q_i and Q_k have a common linear factor. This linear factor is either z_1 or z_2, and in the latter case at least three of the linear forms L_3, L_4, L_5, L_6 are linearly independent. If all four of these linear forms were linearly independent we should again have the situation of case 3 and (I) would follow; hence just three of these linear forms are independent and, since we are assuming that (I) does not hold, we deduce as before that Q_j and Q_k have a common linear factor, and this factor can only be z_3. Thus Q_k is a multiple of z_2z_3, and so the quadratic form $Q_i + Q_j + Q_k$ has rank 3 which leads to (I). Hence, on the assumption that (I) is false, the only possibility is that z_1 is a factor of Q_k.

Finally, if $Q_l = gL_7^2$ is one of the forms $Q_0, \ldots, Q_r$ having rank 1 and (I) does not hold, then L_7 must be a linear combination of z_1 and z_2, since otherwise we should have the situation of case 2 which led to (I). Similarly L_7 is a linear combination of z_1 and z_3. Thus L_7 is a multiple of z_1 and so z_1 is a factor of Q_l.

Hence in case 4 either (I) holds or else all the quadratic forms $Q_0, \ldots, Q_r$ have a common rational linear factor, which is proposition (III) of the enunciation.

Cases 1-4 cover all the possible ways in which the linearly independent linear forms L_1, L_2, L_3 can occur in the quadratic forms $Q_0, \ldots, Q_r$ subject to the condition that none of these quadratic forms has rank greater than 2; and so this completes the proof of the lemma.

9. Cubic polynomials. In proving Theorem 2 we can always replace the cubic polynomial $\phi(\boldsymbol{x})$ by a polynomial obtained from ϕ by an integral unimodular transformation of coordinates, as such a transformation leaves unaltered the set of values taken by $\phi(\boldsymbol{x})$ at integer points $\boldsymbol{x}$ and preserves the property of having integer coefficients, so that both the hypotheses and the conclusion of the theorem are unaffected by the substitution.

If $\phi(\boldsymbol{x})$ is any cubic polynomial we can, by means of an integral unimodular transformation, arrange that the linear forms $L_1, \ldots, L_h$ occurring in the expression (2) involve only the variables $x_1, \ldots, x_h$. If at the same time we replace the variables $x_{h+1}, \ldots, x_n$ by $y_1, \ldots, y_s$, where $s = n-h$, ϕ takes the form

$$\phi = \phi(\boldsymbol{x}, \boldsymbol{y}) = C(x_1, \ldots, x_h) + \sum_{1\leqslant i\leqslant s} y_i Q_i(x_1, \ldots, x_h) + \sum_{1\leqslant j,k\leqslant s} y_j y_k L_{jk}(x_1, \ldots, x_h), \tag{56}$$

where C, Q_i, and L_{jk} are cubic, quadratic, and linear polynomials respectively in $x_1, \ldots, x_h$ with integer coefficients. Here some of the polynomials C, Q_i, L_{jk} may vanish identically or have degree less than their apparent degree, but, since we are interested in a non-degenerate cubic polynomial ϕ with $n > h$, not all the polynomials Q_i, L_{jk} $(1 \leqslant i, j, k \leqslant s)$ will vanish identically in our case.

Our object in the remaining sections of this paper will be to show that the variables $x_1, \ldots, x_h$ can be given integer values in such a way that the resulting quadratic or linear polynomial in the variables $y_1, \ldots, y_s$ represents infinitely many primes. For this purpose we shall be dealing with spaces of dimensions h and s $(= n-h)$. We use the symbols $\boldsymbol{x}, \boldsymbol{X}, \boldsymbol{\xi}, \boldsymbol{a}$, to denote points in h dimensional space, and $\mathscr{A}$ to denote a box in that space; and we use $\boldsymbol{y}, \boldsymbol{Y}, \boldsymbol{\eta}, \boldsymbol{b}$, to denote points and $\mathscr{B}$ to denote a box in s dimensional space.

Lemma 18. *If the cubic polynomial $\phi(\boldsymbol{x}, \boldsymbol{y})$ of* (56) *satisfies the conditions of Theorem 2 and μ denotes the product of the coefficients of ϕ, then there exist integer points $\boldsymbol{X} = (X_1, \ldots, X_h)$ and $\boldsymbol{Y} = (Y_1, \ldots, Y_s)$ such that for every point $\boldsymbol{x}$ satisfying*

$$\boldsymbol{x} \equiv \boldsymbol{X} \pmod{6\mu} \tag{57}$$

the h.c.f. of the integers $C(\boldsymbol{x}), Q_1(\boldsymbol{x}), \ldots, Q_s(\boldsymbol{x}), L_{11}(\boldsymbol{x}), L_{12}(\boldsymbol{x}), \ldots, L_{ss}(\boldsymbol{x})$ is prime to 6μ and $\phi(\boldsymbol{x}, \boldsymbol{Y}) \not\equiv 0 \pmod 2$.

Proof. One of the hypotheses of Theorem 2 is that for any integer $m > 1$ there exists an integer point at which the value of ϕ is not divisible by m. By choosing such points corresponding to each of the prime factors of 6μ and combining them in the same way as in the proof of Lemma 2 we obtain an integer point $(X_1, \ldots, X_h, Y_1, \ldots, Y_s) = (\boldsymbol{X}, \boldsymbol{Y})$ such that $\phi(\boldsymbol{X}, \boldsymbol{Y})$ is prime to 6μ. It is then clear that the integer points $\boldsymbol{X}$ and $\boldsymbol{Y}$ have the properties required by the lemma.

Lemma 19. *Let $\phi = \phi(\boldsymbol{x}, \boldsymbol{y})$ be a cubic polynomial of the form* (56) *satisfying the conditions of Theorem 2, and let $U_1, \ldots, U_h$ be functions of a large parameter P each bounded above and below by fixed positive powers of P. Denote by $R(\boldsymbol{x}) = R(x_1, \ldots, x_h)$ any particular one of the polynomials $Q_1(\boldsymbol{x}), \ldots, Q_s(\boldsymbol{x}), L_{11}(\boldsymbol{x}), L_{12}(\boldsymbol{x}), \ldots, L_{ss}(\boldsymbol{x})$ which is not constant, and write $U = \prod_{i=1}^{h} U_i$. Let μ be as in Lemma* 18, *and let $\boldsymbol{X}, \boldsymbol{Y}$ be the integer points whose existence is asserted by that lemma. If there are $\gg U/\log P$ integer points $\boldsymbol{x} = (x_1, \ldots, x_h)$ satisfying the following three conditions*

(i) $|x_i| < U_i$ $(i = 1, \ldots, h)$,

(ii) $\boldsymbol{x} \equiv \boldsymbol{X} \pmod{6\mu}$,

(iii) *$R(\boldsymbol{x})$ is of the form $R(\boldsymbol{x}) = mp$, where m is a factor of $(6\mu)^3$ and p is prime;*

then there are $\gg U/\log P$ of these points for which the integers $C(\boldsymbol{x}), Q_1(\boldsymbol{x}), \ldots, Q_s(\boldsymbol{x}), L_{11}(\boldsymbol{x}), \ldots, L_{ss}(\boldsymbol{x})$ have no common factor and $\phi(\boldsymbol{x}, \boldsymbol{Y}) \not\equiv 0 \pmod 2$.

Proof. If $\boldsymbol{x}$ is an integer point satisfying (ii) then, by Lemma 18, the h.c.f. of the integers $C(\boldsymbol{x}), \ldots, L_{ss}(\boldsymbol{x})$ is prime to 6μ. If in addition $\boldsymbol{x}$ satisfies (iii) and the h.c.f. of the integers $C(\boldsymbol{x}), \ldots, L_{ss}(\boldsymbol{x})$ is not 1, then this h.c.f., being a factor of mp and prime to 6μ, is equal to p. Hence p divides each of $C(\boldsymbol{x}), \ldots, L_{ss}(\boldsymbol{x})$ and so $R(\boldsymbol{x}) = mp$ divides each of $(6\mu)^3 C(\boldsymbol{x}), (6\mu)^3 Q_1(\boldsymbol{x}), \ldots, (6\mu)^3 L_{ss}(\boldsymbol{x})$. Since ϕ is irreducible, the polynomials $(6\mu)^3 C(\boldsymbol{x}), (6\mu)^3 Q_1(\boldsymbol{x}), \ldots, (6\mu)^3 L_{ss}(\boldsymbol{x})$ have no common factor and so Lemma 15 (with $\phi_1 = R$ and $n = h$) is applicable to this set of polynomials and we deduce that the number of integer points $\boldsymbol{x}$ satisfying (i) for which $R(\boldsymbol{x})$ divides each of $(6\mu)^3 C(\boldsymbol{x}), \ldots, (6\mu)^3 L_{ss}(\boldsymbol{x})$ is $\ll \max U_i^{-1} U P^{\varepsilon}$, for any $\varepsilon > 0$. Hence the number of integer points $\boldsymbol{x}$ satisfying (i), (ii), and (iii) for which the integers $C(\boldsymbol{x}), \ldots, L_{ss}(\boldsymbol{x})$ have a common factor is $\ll \max U_i^{-1} U P^{\varepsilon}$, and this number is of a smaller order of magnitude than $U/\log P$ if ε is small enough. Thus under the conditions of the lemma the number of integer points $\boldsymbol{x}$ satisfying (i), (ii), and (iii) for which $C(\boldsymbol{x}), \ldots, L_{ss}(\boldsymbol{x})$ have no common factor is $\gg U/\log P$. Finally we note that, by Lemma 18, $\phi(\boldsymbol{x}, \boldsymbol{Y})$

$\not\equiv 0 \pmod 2$ for any point $\boldsymbol{x}$ satisfying (ii). This completes the proof of the lemma.

In the proof of Theorem 2 we need only consider cubic polynomials ϕ which are expressible in the form (56), and we shall suppose from now on that ϕ is of this form. We shall deal separately with the two principal cases, namely:

Case A. Not all the linear polynomials $L_{jk}(x_1, \ldots, x_h)$ $(1 \leqslant j, k \leqslant s)$ are identically zero.

Case B. The linear polynomials $L_{jk}(x_1, \ldots, x_h)$ $(1 \leqslant j, k \leqslant s)$ are all identically zero.

10. Proof of Theorem 2 in case A. In this section we suppose that ϕ is expressible in the form (56), where not all the linear polynomials L_{jk} $(1 \leqslant j, k \leqslant s)$ are identically zero.

By rearranging the terms in the expression (56) we can write ϕ as

$$\phi = \phi(\boldsymbol{x}, \boldsymbol{y}) = C(x_1, \ldots, x_h) + \sum_{1 \leqslant i \leqslant s} y_i Q_i(x_1, \ldots, x_h) + Q_0^*(y_1, \ldots, y_s) + \sum_{1 \leqslant j \leqslant h} x_j Q_j^*(y_1, \ldots, y_s), \tag{58}$$

where $Q_0^*(y_1, \ldots, y_s), Q_1^*(y_1, \ldots, y_s), \ldots, Q_h^*(y_1, \ldots, y_s)$ are quadratic forms in $y_1, \ldots, y_s$, and, in case A, they are not all identically zero.

In proving Theorem 2 in case A we shall consider separately the three cases that arise according as the quadratic forms $Q_0^*, Q_1^*, \ldots, Q_h^*$ satisfy alternative (I), (II) or (III) of Lemma 17 (where r of Lemma 17 is now h and n is now s). In the first of these three cases, case I, the proof of Theorem 2 falls into three further cases depending on which of the following statements applies to ϕ.

(i) Not all the linear polynomials L_{jk} $(1 \leqslant j, k \leqslant s)$ occurring in (56) are constant.

(ii) The linear polynomials L_{jk} $(1 \leqslant j, k \leqslant s)$ are all constant but at least one of the quadratic polynomials Q_i $(1 \leqslant i \leqslant s)$ of (56) has non-vanishing quadratic part.

(iii) The linear parts of the polynomials L_{jk} $(1 \leqslant j, k \leqslant s)$ and the quadratic parts of the polynomials Q_i $(1 \leqslant i \leqslant s)$ are all identically zero but the cubic polynomial C of (56) has non-vanishing cubic part.

ϕ is certainly of one of these three forms since otherwise its cubic part would vanish identically.

Case I (i). *The quadratic forms $Q_0^*, \ldots, Q_h^*$ of* (58) *satisfy alternative* (I) *of Lemma* 17 *and condition* (i) *above holds.*

We suppose that the linear polynomial L_{JK} is not constant for some particular pair of suffixes J, K. It follows that not all of the quadratic forms $Q_1^*, \ldots, Q_h^*$ of (58) vanish identically, and so we can choose a poitn $\boldsymbol{\eta} = (\eta_1, \ldots, \eta_s)$ such that $Q_1^*(\boldsymbol{\eta}), \ldots, Q_h^*(\boldsymbol{\eta})$ are not all zero. Then we can find a point $\boldsymbol{a} = (a_1, \ldots, a_h)$ such that

$$a_1 Q_1^*(\boldsymbol{\eta}) + \ldots + a_h Q_h^*(\boldsymbol{\eta}) > 0$$

and a box $\mathscr{A}$ in h dimensional space containing $\boldsymbol{a}$ such that

$$\xi_1 Q_1^*(\boldsymbol{\eta}) + \ldots + \xi_h Q_h^*(\boldsymbol{\eta}) > \delta > 0 \tag{59}$$

whenever $\boldsymbol{\xi} \in \mathscr{A}$, where δ is a fixed positive number.

Let μ denote the product of the coefficients of ϕ and let $\boldsymbol{X} = (X_1, \ldots, X_h)$ be the integer point given by Lemma 18. We make the substitution

$$\boldsymbol{x} = \boldsymbol{X} + 6\mu \boldsymbol{z} \tag{60}$$

and let $\boldsymbol{z}$ range over the integer points in the expanded box $(6\mu)^{-1}P\mathscr{A}$, where P is a large parameter. Under this substitution $L_{JK}(\boldsymbol{x})$ becomes $L'_{JK}(\boldsymbol{z})$ where the coefficients of the linear part of L'_{JK} are just 6μ times the corresponding coefficients of L_{JK}, and so λ_{JK}, the h.c.f. of the coefficients of L'_{JK}, is a factor of $6\mu^2$.

Now at least one of the linear polynomials $\lambda_{JK}^{-1}L'_{JK}$, $-\lambda_{JK}^{-1}L'_{JK}$ satisfies the conditions of Lemma 14 with respect to the box $(6\mu)^{-1}\mathscr{A}$, and so it follows from that lemma that there are $\gg P^h/\log P$ integer points $\boldsymbol{z}$ with $\boldsymbol{z} \in (6\mu)^{-1}P\mathscr{A}$ and $L'_{JK}(\boldsymbol{z}) = mp$, where $m = \pm\lambda_{JK}$ and p is prime. For the corresponding points $\boldsymbol{x}$ we have $\boldsymbol{x} \in P\mathscr{A} - \boldsymbol{X}$ and $L_{JK}(\boldsymbol{x}) = mp$.

We now apply Lemma 19 to ϕ with $R(\boldsymbol{x}) = L_{JK}(\boldsymbol{x})$ and $U_i = cP$ $(i = 1, \ldots, h)$ for a suitable constant c, and deduce that there are $\gg P^h/\log P$ integer points $\boldsymbol{x}$ in the box $P\mathscr{A} - \boldsymbol{X}$ for which $\phi(\boldsymbol{x}, \boldsymbol{y})$, considered as a quadratic polynomial in $\boldsymbol{y}$, has integer coefficients with no common factor and is not even at all integer points $\boldsymbol{y}$. Furthermore the quadratic part of $\phi(\boldsymbol{x}, \boldsymbol{y})$, considered as a polynomial in $\boldsymbol{y}$, is

$$Q^*(\boldsymbol{x}, \boldsymbol{y}) = Q_0^*(\boldsymbol{y}) + x_1 Q_1^*(\boldsymbol{y}) + \ldots + x_h Q_h^*(\boldsymbol{y}).$$

For $\boldsymbol{x} \in P\mathscr{A} - \boldsymbol{X}$ we can write $\boldsymbol{x} = P\boldsymbol{\xi} - \boldsymbol{X}$, where $\boldsymbol{\xi} \in \mathscr{A}$, and then we have

$$Q^*(\boldsymbol{x}, \boldsymbol{\eta}) = Q_0^*(\boldsymbol{\eta}) + (P\xi_1 - X_1)Q_1^*(\boldsymbol{\eta}) + \ldots + (P\xi_h - X_h)Q_h^*(\boldsymbol{\eta})$$
$$> P\delta + O(1) \quad \text{(by (59))},$$

and so $Q^*(\boldsymbol{x}, \boldsymbol{y})$ is positive if P is large enough. Hence for $\boldsymbol{x} \in P\mathscr{A} - \boldsymbol{X}$ and P large enough $Q^*(\boldsymbol{x}, \boldsymbol{y})$, considered as a polynomial in $\boldsymbol{y}$, is neither negative definite nor negative semi-definite. Finally we are assuming that $Q_0^*, Q_1^*, \ldots, Q_h^*$ satisfy (I) of Lemma 17, and it follows from this that $Q^*(\boldsymbol{x}, \boldsymbol{y})$ has rank $\leqslant 2$ in $\boldsymbol{y}$ for $\ll P^{h-1}$ of the integer points $\boldsymbol{x}$ in the box $P\mathscr{A} - \boldsymbol{X}$.

Hence for large enough P there is some integer point $\boldsymbol{x}$ in the box $P\mathscr{A}-\boldsymbol{X}$ for which $\phi(\boldsymbol{x},\boldsymbol{y})$, as a quadratic polynomial in $\boldsymbol{y}$, satisfies all the conditions of the corollary to Theorem 1 (stated in § 7), and it follows that $\phi(\boldsymbol{x},\boldsymbol{y})$ represents infinitely many primes.

Case I (ii). *The quadratic forms $Q_0^*,\ldots,Q_h^*$ satisfy alternative* (I) *of Lemma* 17 *and condition* (ii) *holds.*

Since in this case the linear polynomials L_{jk} are all constant, we have $Q_i^*\equiv 0$ for $1\leqslant i\leqslant h$; and, since we are supposing in this section that the polynomials L_{jk} are not all identically zero, Q_0^* is not identically zero. Thus in this case the set of quadratic forms $Q_0^*, Q_1^*,\ldots,Q_h^*$ contains only one non-vanishing form, namely Q_0^*, and since we are supposing that this set of forms satisfies (I) of Lemma 17, the rank of Q_0^* is $\geqslant 3$.

Suppose that the particular linear polynomial L_{JK} does not vanish identically, so that $L_{JK}\equiv l_{JK}\neq 0$, where l_{JK} is a constant, and denote by $Q_1'(\boldsymbol{x}),\ldots,Q_s'(\boldsymbol{x})$ the quadratic parts of the polynomials $Q_1(\boldsymbol{x}),\ldots,Q_s(\boldsymbol{x})$ of (56), so that, by (ii), $Q_1',\ldots,Q_s'$ are not all identically zero. We fix a point $\boldsymbol{a}=(a_1,\ldots,a_h)$ such that $Q_1'(\boldsymbol{a}),\ldots,Q_s'(\boldsymbol{a})$ are not all zero, and then a point $\boldsymbol{b}=(b_1,\ldots,b_s)$ such that

$$Q_0^*(\boldsymbol{b})+b_1Q_1'(\boldsymbol{a})+\ldots+b_sQ_s'(\boldsymbol{a})>0.$$

Now we can choose a box $\mathscr{B}$ in s dimensional space containing $\boldsymbol{b}$ and so small that

(61) $$e_1<Q_0^*(\boldsymbol{\eta})+\eta_1Q_1'(\boldsymbol{a})+\ldots+\eta_sQ_s'(\boldsymbol{a})<e_2$$

for all points $\boldsymbol{\eta}\in\mathscr{B}$, where e_1 and e_2 are suitable positive numbers. We also choose numbers f_1 and f_2 such that

(62) $$0<f_1<e_1<e_2<f_2.$$

If $\boldsymbol{X}$ and $\boldsymbol{Y}$ are the integer points given by Lemma 18, then for any integer point $\boldsymbol{x}$ satisfying (57) the h.c.f. of the integers $C(\boldsymbol{x}),\ldots,L_{ss}(\boldsymbol{x})$ is prime to 6μ and $\phi(\boldsymbol{x},\boldsymbol{Y})$ is odd. (Here μ denotes, as before, the product of the coefficients of ϕ.) But the h.c.f. of $C(\boldsymbol{x}),\ldots,L_{ss}(\boldsymbol{x})$ is a factor of l_{JK}, which is itself a factor of μ, and so this h.c.f. is 1 for any integer point $\boldsymbol{x}$ satisfying (57).

Now for each large number P we choose an integer point $\boldsymbol{x}^{(P)}$ satisfying (57) as close as possible to the point $P^{1/2}\boldsymbol{a}$. If $\boldsymbol{y}$ is any point in $P\mathscr{B}$ we have $\boldsymbol{y}=P\boldsymbol{\eta}$, where $\boldsymbol{\eta}\in\mathscr{B}$, and substituting $\boldsymbol{x}^{(P)}$ and $\boldsymbol{y}$ in (58), remembering that $Q_i^*\equiv 0$ for $i=1,\ldots,h$, we obtain

$$\begin{aligned}\phi(\boldsymbol{x}^{(P)},\boldsymbol{y}) &= C(\boldsymbol{x}^{(P)})+\sum_{1\leqslant i\leqslant s} y_iQ_i(\boldsymbol{x}^{(P)})+Q_0^*(\boldsymbol{y})\\ &= P^2\big(Q_0^*(\boldsymbol{\eta})+\eta_1Q_1'(\boldsymbol{a})+\ldots+\eta_sQ_s'(\boldsymbol{a})\big)+O(P^{3/2}).\end{aligned}$$

It now follows from (61) and (62) that for P large enough and $\boldsymbol{y}\in P\mathscr{B}$ we have

$$f_1P^2<\phi(\boldsymbol{x}^{(P)},\boldsymbol{y})<f_2P^2.$$

Now $\phi(\boldsymbol{x}^{(P)},\boldsymbol{y})$, considered as a polynomial in $\boldsymbol{y}$, has quadratic part $Q_0^*(\boldsymbol{y})$ with constant coefficients and rank $\geqslant 3$. The coefficients of the other terms of $\phi(\boldsymbol{x}^{(P)},\boldsymbol{y})$ depend on P, but we have shown that, together with the box $\mathscr{B}$, $\phi(\boldsymbol{x}^{(P)},\boldsymbol{y})$ satisfies all the conditions on the quadratic polynomial of Theorem 1; and so we deduce that ϕ represents infinitely many primes.

Case I (iii). *The quadratic forms $Q_0^*,\ldots,Q_h^*$ satisfy alternative* (I) *of Lemma* 17 *and condition* (iii) *holds.*

In this case, as in case I(ii), $Q_i^*\equiv 0$ for $i=1,\ldots,h$, and the rank of Q_0^* is $\geqslant 3$. Also as in case I(ii), if $\boldsymbol{X}$ and $\boldsymbol{Y}$ are the integer points given by Lemma 18, then for any integer point $\boldsymbol{x}$ satisfying (57) the integers $C(\boldsymbol{x}),\ldots,L_{ss}(\boldsymbol{x})$ have no common factor and $\phi(\boldsymbol{x},\boldsymbol{Y})$ is odd.

Denote by $C'(\boldsymbol{x})$ the cubic part of $C(\boldsymbol{x})$. Then (iii) states that $C'(\boldsymbol{x})\not\equiv 0$ and so we can find a point $\boldsymbol{a}=(a_1,\ldots,a_h)$ such that $C'(\boldsymbol{a})>0$, and then we can choose a small box $\mathscr{B}$ in s dimensional space containing the origin such that

(63) $$e_1<C'(\boldsymbol{a})+Q_0^*(\boldsymbol{\eta})<e_2,$$

for all points $\boldsymbol{\eta}\in\mathscr{B}$, where e_1 and e_2 are suitable positive numbers. We also choose numbers f_1 and f_2 satisfying

(64) $$0<f_1<e_1<e_2<f_2.$$

For each large number P, we denote by $\boldsymbol{x}^{(P)}$ an integer point satisfying (57) which is as close as possible to $P^{2/3}\boldsymbol{a}$. Then if $\boldsymbol{y}$ is any point in $P\mathscr{B}$ we have $\boldsymbol{y}=P\boldsymbol{\eta}$, where $\boldsymbol{\eta}\in\mathscr{B}$, and substituting $\boldsymbol{x}^{(P)}$ and $\boldsymbol{y}$ in (58) (where in this case $Q_i^*\equiv 0$ for $i=1,\ldots,h$) we obtain

(65) $$\begin{aligned}\phi(\boldsymbol{x}^{(P)},\boldsymbol{y}) &= C(\boldsymbol{x}^{(P)})+\sum_{1\leqslant i\leqslant s} y_iQ_i(\boldsymbol{x}^{(P)})+Q_0^*(\boldsymbol{y})\\ &= P^2\big(C'(\boldsymbol{a})+Q_0^*(\boldsymbol{\eta})\big)+O(P^{5/3})+O(P^{4/3}),\end{aligned}$$

the order of magnitude of the first error term arising from the fact that, by (iii), the polynomials Q_i $(i=1,\ldots,s)$ have degree at most 1. It now follows from (63), (64), and (65) that for P large enough and $\boldsymbol{y}\in P\mathscr{B}$ we have

$$f_1P^2<\phi(\boldsymbol{x}^{(P)},\boldsymbol{y})<f_2P^2.$$

Now, as in case I (ii), $\phi(\boldsymbol{x}^{(P)},\boldsymbol{y})$, considered as a quadratic polynomial in $\boldsymbol{y}$ with coefficients depending on P, together with the box $\mathscr{B}$, satisfies the conditions of Theorem 1, and so represents infinitely many prime numbers.

Case II. *The quadratic forms* $Q_0^*, \ldots, Q_h^*$ *of* (58) *satisfy alternative* (II) *of Lemma* 17; *that is there exists an integral unimodular transformation of the variables* $y_1, \ldots, y_s$ *taking* $Q_0^*, Q_1^*, \ldots, Q_h^*$ *simultaneously into quadratic forms involving only the variables* y_1, y_2.

In this case the transformation in question reduces ϕ to the form

$$\phi(\boldsymbol{x}, \boldsymbol{y}) = C(x_1, \ldots, x_h) + \sum_{1 \leqslant i \leqslant s} y_i Q_i(x_1, \ldots, x_h) + y_1^2 L_{11}(x_1, \ldots, x_h) + y_1 y_2 L_{12}(x_1, \ldots, x_h) + y_2^2 L_{22}(x_1, \ldots, x_h),$$

where the polynomials C, Q_i, and L_{jk} are as in (56), and, since we are dealing with case A, at least one of the linear polynomials L_{11}, L_{12}, L_{22} is not identically zero, say $L_{JK} \not\equiv 0$. Also the quadratic polynomials $Q_3, \ldots, Q_s$ are not all identically zero as in that case ϕ would not involve the variables $y_3, \ldots, y_s$, whereas the hypotheses of Theorem 2 state that ϕ is non-degenerate and $n \geqslant h+3$. By permuting the variables $y_3, \ldots, y_s$ if necessary we can suppose that $Q_3 \not\equiv 0$.

Now let $\boldsymbol{X}, \boldsymbol{Y}$ be the integer points given by Lemma 18. If L_{JK} is constant it follows, as in case I (ii), that for every integer point $\boldsymbol{x}$ satisfying (57) the integers $C(\boldsymbol{x}), \ldots, L_{ss}(\boldsymbol{x})$ have no common factor and $\phi(\boldsymbol{x}, \boldsymbol{Y})$ is odd. If L_{JK} is not constant then, as in case I (i), there are $\gg P^h/\log P$ integer points $\boldsymbol{x}$ in the region $|\boldsymbol{x}| < P$ for which $C(\boldsymbol{x}), \ldots, L_{ss}(\boldsymbol{x})$ have no common factor and $\phi(\boldsymbol{x}, \boldsymbol{Y})$ is odd. In either case, since Q_3 is not identically zero, there are $\ll P^{h-1}$ integer points $\boldsymbol{x}$ in the region $|\boldsymbol{x}| < P$ for which $Q_3(\boldsymbol{x}) = 0$, and so there is some integer point $\boldsymbol{x}$ for which $C(\boldsymbol{x}), \ldots, L_{ss}(\boldsymbol{x})$ have no common factor, $\phi(\boldsymbol{x}, \boldsymbol{Y})$ is odd, and $Q_3(\boldsymbol{x}) \neq 0$. For this point $\boldsymbol{x}$, $\phi(\boldsymbol{x}, \boldsymbol{y})$, considered as a quadratic polynomial in $y_1, \ldots, y_s$, contains the variable y_3 in its linear part but not in its quadratic part and satisfies all the other conditions of Lemma 13. Hence ϕ represents infinitely many primes.

Case III. *The quadratic forms* $Q_0^*, \ldots, Q_h^*$ *of* (58) *satisfy alternative* (III) *of Lemma* 17; *that is* $Q_0^*, \ldots, Q_h^*$ *have a common linear factor with rational coefficients.*

In this case, after an integral unimodular transformation of the variables $y_1, \ldots, y_s$ if necessary, we can suppose that y_1 is a common factor of $Q_1^*, \ldots, Q_h^*$, and then ϕ has the shape

$$\phi(\boldsymbol{x}, \boldsymbol{y}) = C(x_1, \ldots, x_h) + \sum_{1 \leqslant i \leqslant s} y_i Q_i(x_1, \ldots, x_h) + \sum_{1 \leqslant j \leqslant s} y_1 y_j L_{1j}(x_1, \ldots, x_h), \tag{66}$$

where the polynomials C, Q_i, and L_{1j} are as in (56). Since we are dealing with case A, not all the linear polynomials $L_{11}, \ldots, L_{1s}$ are identically zero, and, in fact, we can suppose further that $L_{12}, \ldots, L_{1s}$ are not all identically zero since otherwise $\phi(\boldsymbol{x}, \boldsymbol{y})$ would be of the form considered in case II. Thus $L_{1J} \not\equiv 0$ for some J in the range $2 \leqslant J \leqslant s$.

Now, just as in the cases we have already dealt with, there are $\gg P^h/\log P$ integer points $\boldsymbol{x}$ in the region $|\boldsymbol{x}| < P$ such that $L_{1J}(\boldsymbol{x}) \neq 0$, the integers $C(\boldsymbol{x}), \ldots, L_{1s}(\boldsymbol{x})$ have no common factor, and such that there exists an integer point $\boldsymbol{Y}$ with $\phi(\boldsymbol{x}, \boldsymbol{Y}) \not\equiv 0 \pmod 2$. If, for any one of these points $\boldsymbol{x}$, $\phi(\boldsymbol{x}, \boldsymbol{y})$ were irreducible over the rational field as a polynomial in $y_1, \ldots, y_s$, then, for that $\boldsymbol{x}$, $\phi(\boldsymbol{x}, \boldsymbol{y})$, considered as a quadratic polynomial in $\boldsymbol{y}$, would satisfy all the conditions of Lemma 16, since the quadratic part of $\phi(\boldsymbol{x}, \boldsymbol{y})$ has y_1 as a factor but is not a multiple of y_1^2. Hence $\phi(\boldsymbol{x}, \boldsymbol{y})$ would represent infinitely many primes.

We now suppose that $\phi(\boldsymbol{x}, \boldsymbol{y})$ factorizes as a polynomial in $y_1, \ldots, y_s$ for $\gg P^h/\log P$ of the integer points $\boldsymbol{x}$ in the region $|\boldsymbol{x}| < P$, for some large P, and obtain a contradiction from this assumption.

We introduce a new variable, y_{s+1}, to make ϕ homogeneous in $y_1, \ldots, y_s, y_{s+1}$, and denote by $\phi_1(y_1, \ldots, y_{s+1})$ the quadratic form in $y_1, \ldots, y_{s+1}$, with coefficients in $\boldsymbol{Q}(x_1, \ldots, x_h)$, produced in this way. (Here $\boldsymbol{Q}(x_1, \ldots, x_h)$ denotes the field of rational functions of $x_1, \ldots, x_h$ over the rational field $\boldsymbol{Q}$.) Let A be the symmetric $(s+1)\times(s+1)$ matrix of ϕ_1 with elements in $\boldsymbol{Q}(x_1, \ldots, x_h)$.

Now ϕ_1 factorizes for $\gg P^h/\log P$ of the integer points $\boldsymbol{x}$ in the region $|\boldsymbol{x}| < P$, and for these points the rank of A is $\leqslant 2$. We deduce that the 3×3 minors of A all vanish identically, is these minors are polynomials in $x_1, \ldots, x_h$ and if any one of them did not vanish identically it would vanish for only $\ll P^{h-1}$ of the integer points $\boldsymbol{x}$ in $|\boldsymbol{x}| < P$. Hence A has identical rank $\leqslant 2$, and so ϕ_1 factorizes over $\mathscr{K}$, the algebraic closure of $\boldsymbol{Q}(x_1, \ldots, x_h)$. Thus

$$\phi_1(y_1, \ldots, y_{s+1}) \equiv (a_1 y_1 + \ldots + a_{s+1} y_{s+1})(b_1 y_1 + \ldots + b_{s+1} y_{s+1}), \tag{67}$$

where $a_l, b_l \in \mathscr{K}$ for $l = 1, \ldots, s+1$. But $\mathscr{K}[y_1, \ldots, y_s]$, the ring of polynomials in $y_1, \ldots, y_s$ over $\mathscr{K}$, is a unique factorization domain, and it follows from (66) that the part of ϕ_1 not involving y_{s+1} factorizes into

$$y_1(L_{11} y_1 + \ldots + L_{1s} y_s).$$

Hence, after exchanging an element of $\mathscr{K}$ between the factors of ϕ_1 in (67) if necessary, we have

$$a_1 = 1, \quad a_l = 0 \quad (2 \leqslant l \leqslant s), \quad b_l = L_{1l}(x_1, \ldots, x_h) \quad (1 \leqslant l \leqslant s).$$

We are supposing that L_{1J} is not identically zero for some integer J in the range $2 \leqslant J \leqslant s$, and for this J the coefficient of $y_J y_{s+1}$ in ϕ_1, which belongs to $\boldsymbol{Q}(x_1, \ldots, x_h)$, is $a_{s+1} b_J = a_{s+1} L_{1J}$. Hence, since $L_{1J} \not\equiv 0$, $a_{s+1} \in \boldsymbol{Q}(x_1, \ldots, x_h)$. Also the coefficient of $y_1 y_{s+1}$ in ϕ_1 belongs to $\boldsymbol{Q}(x_1, \ldots, x_h)$

and is equal to $b_{s+1}+a_{s+1}b_1$, and hence b_{s+1} belongs to $\boldsymbol{Q}(x_1, \ldots, x_h)$; since both a_{s+1} and $b_1 = L_{11}$ do. Thus ϕ_1 factorizes over $\boldsymbol{Q}(x_1, \ldots, x_h)$ and hence, since the coefficients of ϕ_1 are all polynomials in $x_1, \ldots, x_h$, ϕ_1 factorizes over $\boldsymbol{Q}[x_1, \ldots, x_h]$, the ring of polynomials in $x_1, \ldots, x_h$ over the rationals. On setting $y_{s+1} = 1$ this gives a polynomial factorization of $\phi(\boldsymbol{x}, \boldsymbol{y})$ in which both factors are linear in $y_1, \ldots, y_s$. Since we are dealing with case A in which ϕ has non-vanishing terms which are quadratic in $y_1, \ldots, y_s$, neither of these factors can be constant; and this contradicts the irreducibility of ϕ.

This completes the proof of Theorem 2 in case A.

11. Proof of Theorem 2 in case B. In case B all the linear polynomials L_{jk} $(1 \leqslant j, k \leqslant s)$ of (56) are identically zero, and so ϕ is of the form

$$\phi = \phi(\boldsymbol{x}, \boldsymbol{y}) = C(x_1, \ldots, x_h) + \sum_{1 \leqslant i \leqslant s} y_i Q_i(x_1, \ldots, x_h), \tag{68}$$

where $C, Q_1, \ldots, Q_s$ are the cubic and quadratic polynomials of (56). Thus the variables $y_1, \ldots, y_s$ occur only linearly in ϕ. Since ϕ is non-degenerate with $n > h$ not all the quadratic polynomials $Q_1, \ldots, Q_s$ vanish identically and so, by permuting the variables $y_1, \ldots, y_s$ if necessary, we can suppose that $Q_1(x_1, \ldots, x_h) \not\equiv 0$.

We deal first with the simple cases $h = 1$ and $h = 2$. In fact in case B both these values of h are incompatible with the hypotheses of Theorem 2.

If $h = 1$, by rearranging the terms of (68) we can express ϕ in the form

$$\phi(\boldsymbol{x}, \boldsymbol{y}) = x_1^2 L_1^*(x_1, y_1, \ldots, y_{n-1}) + x_1 L_2^*(x_1, y_1, \ldots, y_{n-1}) + \\ + L_3^*(x_1, y_1, \ldots, y_{n-1}),$$

where L_1^*, L_2^*, L_3^* are linear polynomials in $x_1, y_1, \ldots, y_{n-1}$. Hence $\phi(\boldsymbol{x}, \boldsymbol{y})$ is unimodularly equivalent to a polynomial in 4 variables, contradicting condition (i) of Theorem 2.

If $h = 2$, so that $s = n-2$, we can similarly rearrange (68) to express ϕ in the form

$$\phi(\boldsymbol{x}, \boldsymbol{y}) = x_1^2 L_1^*(x_1, x_2, y_1, \ldots, y_{n-2}) + x_1 x_2 L_2^*(x_1, x_2, y_1, \ldots, y_{n-2}) + \\ + x_2^2 L_3^*(x_1, x_2, y_1, \ldots, y_{n-2}) + x_1 L_4^*(x_1, x_2, y_1, \ldots, y_{n-2}) + \\ + x_2 L_5^*(x_1, x_2, y_1, \ldots, y_{n-2}) + L_6^*(x_1, x_2, y_1, \ldots, y_{n-2}),$$

where $L_1^*, \ldots, L_6^*$ are linear polynomials in $x_1, x_2, y_1, \ldots, y_{n-2}$, and hence $\phi(\boldsymbol{x}, \boldsymbol{y})$ is unimodularly equivalent to a polynomial in 8 variables, contradicting condition (ii) of Theorem 2.

Now we assume that $h \geqslant 3$. Here two cases arise according to whether or not the rank of the quadratic part of the polynomial Q_1 of (68) is $\geqslant 3$.

Case (i). *$h \geqslant 3$ and the rank of the quadratic part of $Q_1(\boldsymbol{x})$ is $\geqslant 3$.*

Let $\boldsymbol{X}$ be the integer point given by Lemma 18. We make the substitution (60) and let $\boldsymbol{z}$ range over the integer points satisfying

$$|\boldsymbol{z}| < cP, \tag{69}$$

where c is a constant satisfying $0 < c < |(6\mu)^{-1}|$. (Here μ again denotes the product of the coefficients of ϕ.) Then, provided that P is large enough, we have $|\boldsymbol{x}| < P$ for the corresponding points $\boldsymbol{x}$. With this substitution $Q_1(\boldsymbol{x})$ becomes $Q_1'(\boldsymbol{z})$, a quadratic polynomial in $\boldsymbol{z}$ whose quadratic part has coefficients which are just $(6\mu)^2$ times the corresponding coefficients of the quadratic part of $Q_1(\boldsymbol{x})$. Thus the quadratic part of $Q_1'(\boldsymbol{z})$ has rank $\geqslant 3$ and λ_1, the h.c.f. of the coefficients of $Q_1'(\boldsymbol{z})$, is a factor of $36\mu^3$.

The polynomial $\lambda_1^{-1}Q_1'(\boldsymbol{z})$ has coefficients having no common factor, and if $\lambda_1^{-1}Q_1'(\boldsymbol{z})$ is odd for any integer point $\boldsymbol{z}$ then at least one of the quadratic polynomials $\pm\lambda_1^{-1}Q_1'(\boldsymbol{z})$ satisfies the conditions of the corollary to Theorem 1 (§7), and we deduce that in this case $Q_1'(\boldsymbol{z}) = \pm\lambda_1 p$, where p is prime, for $\gg P^h/\log P$ of the integer points $\boldsymbol{z}$ satisfying (69). If, on the other hand, $\lambda_1^{-1}Q_1'(\boldsymbol{z})$ is even for all integer points $\boldsymbol{z}$ we consider the polynomial $(2\lambda_1)^{-1}Q_1'(\boldsymbol{z})$. This polynomial is integer valued at integer points $\boldsymbol{z}$ and cannot be even at all integer points $\boldsymbol{z}$, for if it were $(4\lambda_1)^{-1}Q_1'(\boldsymbol{z})$ would be an integer valued quadratic polynomial having some coefficient with denominator 4, which is contrary to the conclusion of Lemma 1. Hence at least one of the quadratic polynomials $\pm(2\lambda_1)^{-1}Q_1'(\boldsymbol{z})$ satisfies the conditions of the corollary to Theorem 1, and so we have $Q_1'(\boldsymbol{z}) = \pm 2\lambda_1 p$, where p is prime, for $\gg P^h/\log P$ of the integer points $\boldsymbol{z}$ satisfying (69).

Thus, in any case, for $\gg P^h/\log P$ of the integer points $\boldsymbol{z}$ satisfying (69) $Q_1'(\boldsymbol{z})$ is of the form $\lambda_1^* p$, where p is prime and λ_1^* is a factor of $(6\mu)^3$. The corresponding points $\boldsymbol{x}$ satisfy

$$|\boldsymbol{x}| < P, \quad \boldsymbol{x} \equiv \boldsymbol{X} \pmod{6\mu}, \quad Q_1(\boldsymbol{x}) = \lambda_1^* p,$$

and so the conditions of Lemma 19 are satisfied with $R(\boldsymbol{x}) = Q_1(\boldsymbol{x})$ and $U_i = P$ $(i = 1, \ldots, h)$. It follows that there is some integer point $\boldsymbol{x}$ such that the integers $C(\boldsymbol{x}), Q_1(\boldsymbol{x}), \ldots, Q_s(\boldsymbol{x})$ have no common factor and $Q_1(\boldsymbol{x}) \neq 0$, and for this point $\phi(\boldsymbol{x}, \boldsymbol{y})$ is a linear polynomial in $\boldsymbol{y}$ satisfying the conditions of Lemma 14 (with s in place of n). Hence $\phi(\boldsymbol{x}, \boldsymbol{y})$ represents infinitely many primes.

Case (ii). *ϕ is of the form (68), with $h \geqslant 3$, $Q_1 \not\equiv 0$, and the rank of the quadratic part of Q_1 $\leqslant 2$.*

In this case, after an integral unimodular transformation of the variables $x_1, \ldots, x_h$ if necessary, we can suppose that Q_1 is of the form

$$Q_1(\boldsymbol{x}) = a_1 x_1 + \ldots + a_{h-2}x_{h-2} + Q_1^*(x_{h-1}, x_h),$$

where Q_1^* is a quadratic polynomial in x_{h-1} and x_h with integer coefficients, and $a_1, \ldots, a_{h-2}$ are integers. We shall consider separately the cases $a_1 \neq 0$ and $a_1 = 0$.

If $a_1 \neq 0$ the variable x_1 occurs in the linear part of $Q_1(\boldsymbol{x})$ but not in the quadratic part. In this case we make the substitution (60), where $\boldsymbol{X}$ is the integer point given by Lemma 18 and μ is the product of the coefficients of ϕ, and restrict $\boldsymbol{z}$ to range over the integer points satisfying

$$|z_1| < cP^2, \quad |z_i| < cP \quad (2 \leqslant i \leqslant h),$$

where $0 < c < |(6\mu)^{-1}|$. The corresponding points $\boldsymbol{x}$ satisfy

$$|x_1| < P^2, \quad |x_i| < P \quad (2 \leqslant i \leqslant h),$$

for large P. With this substitution $Q_1(\boldsymbol{x})$ becomes $Q_1'(\boldsymbol{z})$, a quadratic polynomial in $\boldsymbol{z}$, where the variable z_1 occurs in the linear part of $Q_1'(\boldsymbol{z})$ but not in the quadratic part, and λ_1, the h.c.f. of the coefficients of $Q_1'(\boldsymbol{z})$, is a factor of $36\mu^3$. Just as in case (i) above either $\lambda_1^{-1}Q_1'(\boldsymbol{z})$ or $(2\lambda_1)^{-1}Q_1'(\boldsymbol{z})$ is an integer valued polynomial which is not always even, and then the appropriate one of these polynomials satisfies the conditions of Lemma 13. Hence we deduce that there are $\gg P^{h+1}/\log P$ integer points $\boldsymbol{x}$ satisfying

$$|x_1| < P^2, \quad |x_i| < P \quad (2 \leqslant i \leqslant h),$$

$$\boldsymbol{x} \equiv \boldsymbol{X} (\mathrm{mod}\, 6\mu), \quad Q_1(\boldsymbol{x}) = \lambda_1^* p,$$

where λ_1^* is a factor of $(6\mu)^3$ and p is prime. Lemma 19 now applies with $R(\boldsymbol{x}) = Q_1(\boldsymbol{x})$, $U_1 = P^2$, $U_i = P$ $(2 \leqslant i \leqslant h)$, and it follows that there is some integer point $\boldsymbol{x}$ for which the integers $C(\boldsymbol{x}), \ldots, Q_s(\boldsymbol{x})$ have no common factor and $Q_1(\boldsymbol{x}) \neq 0$. For this point $\phi(\boldsymbol{x}, \boldsymbol{y})$ is a linear polynomial in $\boldsymbol{y}$ satisfying the conditions of Lemma 14, and so $\phi(\boldsymbol{x}, \boldsymbol{y})$ represents infinitely many primes.

If on the other hand $a_1 = 0$, then Q_1 is a polynomial in $x_2, \ldots, x_h$ only which is not identically zero, and we can find a set of integers $x_2^*, \ldots, x_h^*$ satisfying

$$x_i^* \equiv X_i (\mathrm{mod}\, 6\mu) \quad (i = 2, \ldots, h), \quad Q_1(x_2^*, \ldots, x_h^*) \neq 0,$$

where $\boldsymbol{X}$ is the integer point given by Lemma 18 and μ is the product of the coefficients of ϕ. Now either the polynomial $C(x_1, \ldots, x_h)$ of (68) contains a term in x_1^3 or else one of the polynomials $Q_2(x_1, \ldots, x_h), \ldots, Q_s(x_1, \ldots, x_h)$ contains a term in x_1^2, for otherwise every term of the cubic part of ϕ would contain one of the variables $x_2, \ldots, x_h$, contrary to the minimality in the definition of h. We denote by $R(x_1, \ldots, x_h)$ an appropriate one of these polynomials, so that R has degree d, where $d = 2$ or 3, and the coefficient of x_1^d in R is not zero. We shall show that there exists an integer x_1^*, with $x_1^* \equiv X_1 (\mathrm{mod}\, 6\mu)$, such that any prime which divides both $R(x_1^*, \ldots, x_h^*)$ and $Q_1(x_1^*, \ldots, x_h^*)$ $(= Q_1(x_2^*, \ldots, x_h^*))$ also divides 6μ.

On making the substitution

$$x_1 = X_1 + 6\mu z_1, \quad x_i = x_i^* \quad (i = 2, \ldots, h),$$

$R(x_1, \ldots, x_h)$ becomes $R_1(z_1)$, a polynomial in z_1 of degree d whose leading coefficient is non-zero and divides $6^3\mu^4$. If p is a prime not dividing 6μ, then R_1 is not identically zero $(\mathrm{mod}\, p)$, and so, by a theorem of Lagrange, $R_1(z_1) \equiv 0 (\mathrm{mod}\, p)$ for at most d residue classes z_1 modulo p. Hence, since $p > 3 \geqslant d$, there is some integer z_1 with $R_1(z_1) \not\equiv 0 (\mathrm{mod}\, p)$. By finding such a z_1 for each prime p which divides $Q_1(x_2^*, \ldots, x_h^*)$ but not 6μ and combining these integers z_1 in the manner of the proof of Lemma 2 we obtain an integer z_1^* such that any prime which divides both $R_1(z_1^*)$ and $Q_1(x_2^*, \ldots, x_h^*)$ also divides 6μ. Then $x_1^* = X_1 + 6\mu z_1^*$ is an integer with the properties we require.

Now $\boldsymbol{x}^* \equiv \boldsymbol{X} (\mathrm{mod}\, 6\mu)$, and so it follows from Lemma 18 that the h.c.f. of $C(\boldsymbol{x}^*), Q_1(\boldsymbol{x}^*), \ldots, Q_s(\boldsymbol{x}^*)$ is prime to 6μ. Hence, since this h.c.f. divides both $R(\boldsymbol{x}^*)$ and $Q_1(\boldsymbol{x}^*)$, it must be 1. Thus $\phi(\boldsymbol{x}^*, \boldsymbol{y})$, considered as a linear polynomial in $\boldsymbol{y}$, satisfies the conditions of Lemma 14 and so represents infinitely many primes.

This completes the proof of Theorem 2 in case B.

The author is indebted to Professor H. Davenport for suggesting the problem which is the basis of this work.

References

[1] H. Davenport, *Cubic forms in thirty-two variables*, Philos. Trans. Roy. Soc. London, Ser. A, 251 (1959), pp. 193-232.

[2] — *Cubic forms in sixteen variables*, Proc. Roy. Soc. London, Ser. A, 272 (1963), pp. 285-303.

[3] E. Landau, *Vorlesungen über Zahlentheorie*, *II*, Leipzig 1927.

[4] O. Perron, *Algebra*, *I*, Berlin, Leipzig 1927.

[5] P. A. B. Pleasants, *The representation of primes by cubic polynomials*, Acta Arithm. 12 (1966), pp. 23-45.

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

Reçu par la Rédaction le 17. 2. 1966