ACTA ARITHMETICA
XXXVIII (1980)

On the relation between two conjectures on polynomials

by

A. SCHINZEL (Warszawa)

1. The aim of this paper is to establish a relation between the conjecture H on simultaneous representation of primes by several irreducible polynomials (see [12] and [5]) and a conjecture on Diophantine equations with parameters that we shall denote by C. Both conjectures involve the notion of the fixed divisor of a polynomial, i.e. the greatest common divisor of all values the polynomial takes for integral values of the arguments. The conjectures run as follows.

H. *Let $f_1(x), \ldots, f_k(x)$ be irreducible polynomials with integral coefficients and the leading coefficients positive such that $\prod_{j=1}^{k} f_j(x)$ has the fixed divisor 1. Then there exist infinitely many positive integers x such that all numbers $f_j(x)$ are primes.*

C. *Let $F(x, y) \in \mathbf{Z}[x, y]$ be a form such that*

$$(1)\qquad F(x, y) = F_1(ax+by, cx+dy) \quad \text{for any } F_1 \in \mathbf{Z}[x, y] \text{ and any } a, b, c, d \in \mathbf{Z} \text{ implies } \begin{vmatrix} a & b \\ c & d \end{vmatrix} = \pm 1.$$

If $f(t_1, \ldots, t_r) \in \mathbf{Z}[t_1, \ldots, t_r]$ has the fixed divisor equal to its content and the equation

$$(2)\qquad F(x, y) = f(t_1, \ldots, t_r)$$

is soluble in integers x, y for all integral vectors $[t_1, \ldots, t_r]$ then there exist polynomials $X, Y \in \mathbf{Z}[t_1, \ldots, t_r]$ such that identically

$$(3)\qquad F\big(X(t_1, \ldots, t_r), Y(t_1, \ldots, t_r)\big) = f(t_1, \ldots, t_r).$$

A conjecture similar to C has been proposed by Chowla [3]. He has made no assumption (1) but required F and f to be irreducible and have the fixed divisor 1. The following example shows that this is not enough:

$$F(x, y) = x^2+3y^2, \quad f(t_1, t_2) = t_1^2+t_1t_2+t_2^2.$$

In this example the set of values of $F(x, y)$ and of $f(t_1, t_2)$ is the same, but F and f are not equivalent by unimodular transformation, which answers in the negative a question of Chowla (ibid., p. 73) repeated in [9]. The condition imposed in C on the fixed divisor of f is essential, as the following example shows

$$F(x,y)=2x^2y^3,\qquad f(t)=t^3(t+1)^4.$$

Here the solutions of the equations (2) are given by

$$x=2(t+1)^2,\ y=\tfrac{1}{2}t\quad \text{if}\quad t\equiv 0 \bmod 2,$$

$$x=\tfrac{1}{4}(t+1)^2,\ y=2t\quad \text{if}\quad t\equiv 1 \bmod 2,$$

but there are no integer-valued polynomials $X(t)$, $Y(t)$ satisfying (3). Another example with F primitive is given at the end of Section 2.

One special case of C corresponding to $F=x^2+y^2$ has been proved in [3] and [4]. Chowla has also indicated how his conjecture for $F(x,y)$ quadratic should follow from the special case $k=1$ of H. We shall extend these results in the following two theorems.

THEOREM 1. *C holds if $F(x,y)=x^ky^l$ $(k\geq 1, l\geq 1)$ or if F is quadratic and equivalent (properly or improperly) to every form in its genus. For such and for no other quadratic F C extends to all polynomials $f\in \mathbf{Z}[t_1,\ldots,t_r]$.*

THEOREM 2. *H implies C if F is a quadratic form or a reducible cubic form.*

We shall see (Corollary to Lemma 3) that C implies the following, less precise but more general assertion.

D. *Let $F(x,y)\in\mathbf{Z}[x,y]$ be any form and $f\in\mathbf{Z}[t_1,\ldots,t_r]$ any polynomial. If the equation (2) is soluble in integers x,y for all integral vectors $[t_1,\ldots,t_r]$ then there exist polynomials $X, Y\in\mathbf{Q}[t_1,\ldots,t_r]$ satisfying (3).*

D has been proved for $F=x^n$ and any r in [7] and [11] also for any irreducible quadratic F and $r=1$ in [4], $r>1$ in [14]; for reducible quadratic F it follows easily. We shall show

THEOREM 3. *H implies D if F factorizes into two relatively prime factors in an imaginary quadratic field.*

In virtue of Theorem 3 H implies D for $F=x^n+y^n$. By a modification of the proof of that theorem in this special case we shall show yet

THEOREM 4. *H implies C if $F(x,y)=x^n+y^n$ $(n\geq 2)$. For $n=2$ and for no other n in question C extends to all polynomials $f\in\mathbf{Z}[t_1,\ldots,t_r]$.*

At the cost of considerable technical complications indicated briefly later one can extend Theorem 2 to all forms F splitting completely over a cyclic field except those with all zeros conjugate and real. The quantitative version of H formulated by Bateman and Horn [1] (see also [5]) implies C in the exceptional case at least for $r=1$. Similarly Theorem 3 can be extended to all forms F that factorize into two distinct complex conjugate factors over an imaginary cyclic field.

2. In the sequel we shall use the vector notation and write $\boldsymbol{t}$ instead of $[t_1,\ldots,t_r]$, $\boldsymbol{t}'$ instead of $[t_2,\ldots,t_r]$, $\|\boldsymbol{t}\|$ for $\max\limits_{1\leq i\leq r}|t_i|$. We shall denote the content of a polynomial f by $C(f)$, its total degree by $|f|$ and call a form F satisfying (1) primary. The letters $\mathbf{N},\mathbf{Z},\mathbf{Q}$ denote the set of positive integers, the ring of integers and the rational field, respectively. For a fixed field $\mathbf{K}$ N denotes the norm from $\mathbf{K}$ to $\mathbf{Q}$ or from $\mathbf{K}(\boldsymbol{t})$ to $\mathbf{Q}(\boldsymbol{t})$. The content of a polynomial over $\mathbf{K}$ is an ideal of $\mathbf{K}$ but if $\mathbf{K}=\mathbf{Q}$ it is often identified with the positive generator of this ideal.

LEMMA 1. *Let $P\in\mathbf{Z}[t]$, p be a prime dividing neither the leading coefficient nor the discriminant of P. If $t_0\in\mathbf{Z}$, $P(t_0)\equiv 0 \bmod p$ then either $P(t_0)\not\equiv 0\bmod p^2$ or $P(t_0+p)\not\equiv 0 \bmod p^2$.*

Proof. Denoting the leading coefficient of P by a, the discriminant of P by D and its derivative by P' we have

$$P(t)U(t)+P'(t)V(t)=aD,$$

where $U,V\in\mathbf{Z}[t]$. Setting $t=t_0$ we infer from $P(t_0)\equiv 0\bmod p$, $aD\not\equiv 0\bmod p$ that $P'(t_0)\not\equiv 0\bmod p$. Now from the expansion

$$P(t_0+p)=P(t_0)+P'(t_0)p+\frac{P''(t_0)}{2}p^2+\ldots$$

we get $P(t_0+p)-P(t_0)\not\equiv 0\bmod p^2$, whence the assertion.

LEMMA 2. *If a quadratic form F is primary then*

$$F=AG(x,y),\qquad \text{where}\quad A\in\mathbf{Z},\ G(x,y)\in\mathbf{Z}[x,y],$$

A is square-free, the discriminant Δ of G is either 1 or fundamental and $\left(\frac{\Delta}{p}\right)=-1$ for every prime factor p of A.

Proof. If G is reducible, $G=(ax+by)(a'x+b'y)$ we have

$$F(x,y)=(Aax+Aby)(a'x+b'y)$$

and by (1)

$$A\begin{vmatrix}a & b\\ a' & b'\end{vmatrix}=\pm 1,\qquad A=\pm 1\quad\text{and}\quad \Delta=\begin{vmatrix}a & b\\ a' & b'\end{vmatrix}^2=1.$$

If G is irreducible, let $G=ax^2+bxy+cy^2$, and let ω_1,ω_2 be a basis of the ideal $\mathfrak{a}=\left(a,\frac{b+\sqrt{\Delta}}{2}\right)$. Then we have for suitable integers a_1,a_2,b_1,b_2

$$a=a_1\omega_1+a_2\omega_2,$$

$$\frac{b+\sqrt{\Delta}}{2}=b_1\omega_1+b_2\omega_2.$$

Let $\mathbf{K}=\mathbf{Q}(\sqrt{\Delta})$ and let us set

$$F_1(x,y)=Aa^{-1}N(x\omega_1+y\omega_2).$$

Since $N\mathfrak{a} = |a|$ and $(\omega_1, \omega_2) \equiv 0 \bmod \mathfrak{a}$ we have

$$F_1(x, y) \in \mathbf{Z}[x, y].$$

On the other hand

$$ax + \frac{b+\sqrt{\Delta}}{2} y = (a_1 x + b_1 y)\omega_1 + (a_2 x + b_2 y)\omega_2,$$

hence

$$F(x, y) = F_1(a_1 x + b_1 y, a_2 x + b_2 y)$$

and by (1)

$$\begin{vmatrix} a_1 & b_1 \\ a_2 & b_2 \end{vmatrix} = \pm 1.$$

It follows that $\left[a, \frac{b+\sqrt{\Delta}}{2}\right]$ is itself a basis for $\mathfrak{a}$ and by a well known result

$$|a| = \frac{1}{\sqrt{|d|}} \operatorname{abs} \begin{vmatrix} a & \frac{b+\sqrt{\Delta}}{2} \\ a & \frac{b-\sqrt{\Delta}}{2} \end{vmatrix},$$

where d is the discriminant of K. It follows that $\Delta = d$ is a fundamental discriminant. If Δ is not square-free or for some $p|\Delta$ we have $\left(\frac{\Delta}{p}\right) = 0$ or 1 then for a suitable prime ideal $\mathfrak{p}$: $N\mathfrak{p}|\Delta$.

Let $\mathfrak{p}\mathfrak{a}$ have an integral basis $[\Omega_1, \Omega_2]$ and let us set

$$F_1(x, y) = Aa^{-1}N\mathfrak{p}^{-2}N(x\Omega_1 + y\Omega_2).$$

Since $N(\Omega_1, \Omega_2) = |a|N\mathfrak{p}$ we have

$$F_1(x, y) \in \mathbf{Z}[x, y].$$

On the other hand

$$\omega_i N\mathfrak{p} = c_i\Omega_1 + d_i\Omega_2 \quad (i = 1, 2)$$

for suitable $c_i, d_i \in \mathbf{Z}$, hence

$$(\omega_1 x + \omega_2 y)N\mathfrak{p} = (c_1 x + c_2 y)\Omega_1 + (d_1 x + d_2 y)\Omega_2$$

and we get

$$F(x, y) = F_1(c_1 x + c_2 y, d_1 x + d_2 y).$$

Now by (1)

$$\begin{vmatrix} c_1 & c_2 \\ d_1 & d_2 \end{vmatrix} = \pm 1,$$

hence $[\omega_1 N\mathfrak{p}, \omega_2 N\mathfrak{p}]$ is a basis for $\mathfrak{a}\mathfrak{p}$ and $\mathfrak{a}N\mathfrak{p} = \mathfrak{a}\mathfrak{p}$, a contradiction.

Remark. Similarly one can show that if a primary form $F(x, y)$ is irreducible and $F(\vartheta, 1) = 0$ then $[1, \vartheta]$ can be extended to a basis of the ideal $(1, \vartheta)$.

Proof of Theorem 1. Consider first $F(x, y) = x^k y^l$ and let

$$f(\mathbf{t}) = c\prod_{\nu=1}^{n} f_\nu(\mathbf{t})^{e_\nu} \tag{4}$$

be the canonical factorization of f into primitive irreducible polynomials with integral coefficients. In view of the condition on the fixed divisor of f for every prime factor p of c there exists a vector $\mathbf{t}_p \in \mathbf{Z}^r$ such that

$$\prod_{\nu=1}^{n} f_\nu(\mathbf{t}_p)^{e_\nu} \not\equiv 0 \bmod p.$$

It follows from (2) with $\mathbf{t} = \mathbf{t}_p$ that

$$\operatorname{ord}_p c = k\alpha + l\beta,$$

where $\alpha = \operatorname{ord}_p x$, $\beta = \operatorname{ord}_p y$ and we get

$$c = \pm \xi^k \eta^l, \quad \xi, \eta \in \mathbf{Z}. \tag{5}$$

On the other hand we can assume that $f(\mathbf{t})$ depends upon t_1. Let $a_0(\mathbf{t}')$, $D(\mathbf{t}')$ be the leading coefficient and the discriminant respectively of $\prod_{\nu=1}^{n} f_\nu(\mathbf{t})$ with respect to t_1. We have $a_0 D \neq 0$ and there exists a vector $\mathbf{t}'_0 \in \mathbf{Z}^{r-1}$ such that

$$a_0(\mathbf{t}'_0)D(\mathbf{t}'_0) \neq 0.$$

For every $\nu \leqslant n$ there exists a prime p and an integer t_0 such that

$$f_\nu(t_0, \mathbf{t}'_0) \equiv 0 \bmod p, \quad ca_0(\mathbf{t}'_0)D(\mathbf{t}'_0) \not\equiv 0 \bmod p. \tag{6}$$

Put

$$P(t) = \prod_{\nu=1}^{n} f_\nu(t, \mathbf{t}'_0). \tag{7}$$

Since $a_0(\mathbf{t}'_0) \neq 0$, the discriminant of $P(t)$ equals $D(\mathbf{t}'_0)$. Hence by (6) and Lemma 1 there exists a $t_1 \in \mathbf{Z}$ such that

$$P(t_1) \equiv 0 \bmod p, \quad P(t_1) \not\equiv 0 \bmod p^2.$$

We infer from (4), (5) and (6) that

$$f_\nu(t_1, \mathbf{t}'_0) \equiv 0 \bmod p, \quad f_\nu(t_1, \mathbf{t}'_0) \not\equiv 0 \bmod p^2, \quad f_\mu(t_1, \mathbf{t}'_0) \not\equiv 0 \bmod p \quad (\mu \neq \nu). \tag{8}$$

It follows from (2) with $\mathbf{t} = [t_1, \mathbf{t}'_0]$, (6) and (8) that

$$e_\nu = k\alpha_\nu + l\beta_\nu, \tag{9}$$

where $\alpha_\nu = \operatorname{ord}_{p_\nu} x$, $\beta_\nu = \operatorname{ord}_{p_\nu} y$. Take now

$$X_0(\boldsymbol{t}) = \xi \prod_{\nu=1}^{n} f_\nu(\boldsymbol{t})^{\alpha_\nu}, \qquad Y_0(\boldsymbol{t}) = \eta \prod_{\nu=1}^{n} f_\nu(\boldsymbol{t})^{\beta_\nu}.$$

It follows from (5) and (9) that

$$X_0(\boldsymbol{t})^k Y_0(\boldsymbol{t})^l = \pm f(\boldsymbol{t}).$$

If the sign on the right-hand side is positive we take $X = X_0$, $Y = Y_0$. If the sign is negative and either k or l is odd, we take $X = \pm X_0$, $Y = \pm Y_0$. If the sign is negative and k, l are both even we get a contradiction. Indeed by (5) $c < 0$, by (9) $e_\nu \equiv 0 \bmod 2$, hence by (4) $f(\boldsymbol{t}) \leqslant 0$. Taking $\boldsymbol{t} \in \boldsymbol{Z}^r$ such that $f(\boldsymbol{t}) \neq 0$ we get from (2) $x^k y^l < 0$, which is impossible.

Consider now the case of F quadratic. By Lemma 2 F is of the form $AG(x, y)$, where A is square-free, $G(x, y)$ is a primitive form with discriminant Δ, $\left(\frac{\Delta}{p}\right) = -1$ for every prime factor p of A and either $\Delta = 1$ or Δ is fundamental. In the first case $F(x, y)$ is equivalent to xy and for the latter form one can take $X(\boldsymbol{t}) = f(\boldsymbol{t})$, $Y(\boldsymbol{t}) = 1$. In the second case if $G(\vartheta, 1) = 0$, $\boldsymbol{K} = \boldsymbol{Q}(\vartheta)$ and $\mathfrak{a}$ is the ideal $(1, \vartheta)$ we have

$$G(x, y) = \frac{N(x - \vartheta y)}{N\mathfrak{a}}.$$

Changing if necessary the sign of A we can assume that

$$F(x, y) = \frac{A}{N\mathfrak{a}} N(x - \vartheta y). \tag{10}$$

The solubility of the equation $N(\omega) = \frac{N\mathfrak{a}}{A} f(\boldsymbol{t})$ for all $\boldsymbol{t} \in \boldsymbol{Z}^r$ implies by Theorem 1 of [14] the existence of a polynomial $\omega(\boldsymbol{t}) \in \boldsymbol{K}[\boldsymbol{t}]$ such that

$$N\big(\omega(\boldsymbol{t})\big) = \frac{N\mathfrak{a}}{A} f(\boldsymbol{t}). \tag{11}$$

Let $\mathfrak{b} = C(\omega)$ and let

$$\mathfrak{b}\mathfrak{a}^{-1} = \prod_{i=1}^{j} \mathfrak{p}_i^{a_i} \prod_{i=1}^{j} \mathfrak{p}_i'^{b_i} \prod_{i=1}^{k} \mathfrak{q}_i^{c_i}$$

be the factorization of $\mathfrak{b}\mathfrak{a}^{-1}$ in prime ideals of $\boldsymbol{K}$. Here $\mathfrak{p}_i$ are distinct pairwise non conjugate prime ideals of degree 1 in $\boldsymbol{K}$, $\mathfrak{p}_i'$ is conjugate to $\mathfrak{p}_i$ and $\mathfrak{q}_i$ are prime ideals of degree 2 in $\boldsymbol{K}$. Since $AN(\mathfrak{b}\mathfrak{a}^{-1}) \in \boldsymbol{Z}$ and A has

only prime ideal factors of degree 2 in $\boldsymbol{K}$ we get

$$a_i + b_i \geqslant 0 \quad (1 \leqslant i \leqslant j),$$
$$2c_i + 1 \geqslant 0 \quad (1 \leqslant i \leqslant k),$$

hence

$$\max\{0, a_i\} + \min\{0, b_i\} \geqslant 0, \quad \max\{0, b_i\} + \min\{0, a_i\} \geqslant 0 \quad (1 \leqslant i \leqslant j), \tag{12}$$
$$c_i \geqslant 0 \quad (1 \leqslant i \leqslant k).$$

Let us consider the ideal

$$\mathfrak{c} = \prod_{i=1}^{j} \mathfrak{p}_i^{\min(0, b_i) - \min(0, a_i)} \mathfrak{p}_i'^{\min(0, a_i) - \min(0, b_i)}.$$

Since F is equivalent to every form in its genus the same is true about G, thus there is only one narrow class in the genus of $\mathfrak{a}$ or there are two such classes represented by $\mathfrak{a}$ and $\mathfrak{a}'$. In any case the principal genus consists only of the principal class and the class of $\mathfrak{a}^2$. Since $\mathfrak{p}_i' \sim \mathfrak{p}_i^{-1}$, $\mathfrak{c}$ belongs to the principal genus and we get $\mathfrak{c} \sim 1$ or $\mathfrak{c} \sim \mathfrak{a}^2$. In the former case let $\mathfrak{c} = (\gamma_1)$ with γ_1 totally positive and consider the polynomial

$$\omega_1(\boldsymbol{t}) = \gamma_1 \omega(\boldsymbol{t}).$$

We have

$$C(\omega_1) = (\gamma_1) C(\omega) = \mathfrak{c}\mathfrak{b} = \mathfrak{a} \prod_{i=1}^{j} \mathfrak{p}_i^{\max\{0, a_i\} + \min\{0, b_i\}} \prod_{i=1}^{j} \mathfrak{p}_i'^{\max\{0, b_i\} + \min\{0, a_i\}} \prod_{i=1}^{k} \mathfrak{q}_i^{c_i}$$

and by (12) $C(\omega_1) \equiv 0 \bmod \mathfrak{a}$.

It follows that all the coefficients of ω_1 are in $\mathfrak{a}$ and since by Lemma 2 $[1, \vartheta]$ is a basis of $\mathfrak{a}$ we get

$$\omega_1(\boldsymbol{t}) = X_1(\boldsymbol{t}) - \vartheta Y_1(\boldsymbol{t}),$$

where $X_1, Y_1 \in \boldsymbol{Z}[\boldsymbol{t}]$. It follows now from (10) and (11) that

$$F\big(X_1(\boldsymbol{t}), Y_1(\boldsymbol{t})\big) = \frac{A}{N\mathfrak{a}} N\omega_1(\boldsymbol{t}) = \frac{A}{N\mathfrak{a}} N\gamma_1 N\omega(\boldsymbol{t}) = N\mathfrak{c} \cdot f(\boldsymbol{t}) = f(\boldsymbol{t}).$$

In the case $\mathfrak{c} \sim \mathfrak{a}^2$ let $\mathfrak{c}\mathfrak{a}^{-1}\mathfrak{a}' = (\gamma_2)$ with γ_2 totally positive and consider the polynomial

$$\omega_2(\boldsymbol{t}) = \gamma_2 \omega(\boldsymbol{t}).$$

We have

$$C(\omega_2) = (\gamma_2) C(\omega) = \mathfrak{c}\mathfrak{a}^{-1}\mathfrak{a}'\mathfrak{b}$$
$$= \mathfrak{a}' \prod_{i=1}^{j} \mathfrak{p}_i^{\max\{0, a_i\} + \min\{0, b_i\}} \prod_{i=1}^{j} \mathfrak{p}_i'^{\max\{0, b_i\} + \min\{0, a_i\}} \prod_{i=1}^{k} \mathfrak{q}_i^{c_i},$$

and by (12) $C(\omega_2) \equiv 0 \bmod \mathfrak{a}'$.

Since $[1, \vartheta']$ is a basis of $\mathfrak{a}'$ we infer that

$$\omega_2(\boldsymbol{t}) = X_2(\boldsymbol{t}) - \vartheta' Y_2(\boldsymbol{t}),$$

where $X_2, Y_2 \in \boldsymbol{Z}[\boldsymbol{t}]$. Since $N\gamma_2 = 1$ it follows as before that

$$F\big(X_2(\boldsymbol{t}), Y_2(\boldsymbol{t})\big) = f(\boldsymbol{t}).$$

It remains to prove that if there is a form inequivalent to F in the genus of F then C does not extend to all polynomials $f \in \boldsymbol{Z}[\boldsymbol{t}]$. For this purpose let us observe that there exists then in $\boldsymbol{K}$ a class C of ideals such that C^2 is neither the principal class nor the class of $\mathfrak{a}^2$. Choose in C^{-1} a prime ideal $\mathfrak{p}$ of degree 1 with $N\mathfrak{p} = p$. There exists a prime ideal $\mathfrak{q}$ such that $\mathfrak{p}^2\mathfrak{a}\mathfrak{q}$ is principal, equal, say (α). Consider the polynomials

$$\omega(t) = \alpha\frac{t^p - t}{p}, \qquad f(t) = \frac{A}{N\mathfrak{a}} N\omega(t). \tag{13}$$

We have

$$C(f) = \frac{|A|}{N\mathfrak{a}}\,\frac{|N\alpha|}{p^2} = |A|N\mathfrak{q} \in \boldsymbol{Z}$$

hence $f(t) \in \boldsymbol{Z}[t]$. Also, since $\frac{t^p - t}{p} \in \boldsymbol{Z}$ for all $t \in \boldsymbol{Z}$ we have for all $t \in \boldsymbol{Z}$: $\omega(t) \in \mathfrak{a}$; $\omega(t) = x - \vartheta y$ and

$$f(t) = F(x, y)$$

for suitable $x, y \in \boldsymbol{Z}$. On the other hand, suppose that

$$f(t) = F\big(X(t), Y(t)\big), \qquad X, Y \in \boldsymbol{Z}[t] \tag{14}$$

and let x, y be the leading coefficients of X, Y. Then comparing the leading coefficients on both sides of (14) we get by (13)

$$\frac{A}{N\mathfrak{a}}\,\frac{N\alpha}{p^2} = F(x, y) = \frac{A}{N\mathfrak{a}} N(x - \vartheta y), \qquad N\mathfrak{q} = N\frac{(x - \vartheta y)}{\mathfrak{a}}.$$

Since $\mathfrak{q}$ is a prime ideal, $x - \vartheta y \in \mathfrak{a}$ it follows that

$$\frac{(x - \vartheta y)}{\mathfrak{a}} = \mathfrak{q} \text{ or } \mathfrak{q}'.$$

Hence $\mathfrak{a}\mathfrak{q} \sim 1$ or $\mathfrak{a}\mathfrak{q}^{-1} \sim 1$. By the choice of $\mathfrak{q}$ this gives $\mathfrak{p}^2 \sim 1$ or $\mathfrak{p}^2\mathfrak{a}^2 \sim 1$ contrary to the choice of $\mathfrak{p}$.

Remark. The above proof seems to suggest that if F satisfies (1) and for all $\boldsymbol{t} \in \boldsymbol{Z}^r$ the equation (2) is soluble in integers x, y then there exist integer-valued polynomials $X(\boldsymbol{t}), Y(\boldsymbol{t})$ satisfying (3) identically. The following example shows that this is not the case.

Let $F(x, y) = x^2 + xy + 6y^2$, $\boldsymbol{K} = \boldsymbol{Q}(\sqrt{-23})$, $\omega = \frac{1 + \sqrt{-23}}{2}$,

$$f(t) = N\big(\tfrac{1}{2}(\omega^4 - \omega)t^2 + \omega - 8\big).$$

The discriminant of F is -23 hence F is primary. Further, $f(t) \in \boldsymbol{Z}[t]$ since $(\frac{1}{2}\omega^4 - \omega, \omega - 8) = \frac{(2, \omega)}{(2, \omega')}$ with ω' conjugate to ω.

Moreover the equation $F(x, y) = f(t)$ is soluble in integers x, y for all $t \in \boldsymbol{Z}$. Indeed if $t \equiv 0 \bmod 2$ we can take

$$x + y\omega = (\tfrac{1}{2}\omega^4 - \omega)t^2 + \omega - 8$$

and if $t \equiv 1 \bmod 2$ we can take

$$x + y\omega = \frac{-3 - \sqrt{-23}}{-3 + \sqrt{-23}}\,[(\tfrac{1}{2}\omega^4 - \omega)t^2 + \omega - 8].$$

The number on the right-hand side is an integer in $\boldsymbol{K}$ since for $t \equiv 1 \bmod 2$

$$(\tfrac{1}{2}\omega^4 - \omega)t^2 + \omega - 8 \equiv \tfrac{1}{2}\omega^4 - 8 \bmod 4(\omega^2 - 2\omega)$$

and we have in $\boldsymbol{K}$ the factorizations into prime ideals $(2) = \mathfrak{p}\mathfrak{p}'$, $(\omega) = \mathfrak{p}\mathfrak{q}$, $\big((-3 + \sqrt{-23})/2\big) = \mathfrak{p}^3$.

On the other hand, the polynomial $(\frac{1}{2}\omega^4 - \omega)t^2 + \omega - 8$ is irreducible over $\boldsymbol{K}$ since $N\frac{8 - \omega}{\frac{1}{2}\omega^4 - \omega} = \frac{62}{381}$ is not a square in $\boldsymbol{Q}$. Therefore, if integer-valued polynomials $X(t), Y(t)$ satisfied

$$F\big(X(t), Y(t)\big) = f(t)$$

identically, we would have either

$$X(t) + Y(t)\omega = \gamma(\tfrac{1}{2}\omega^4 - \omega)t^2 + \gamma(\omega - 8)$$

or

$$X(t) + Y(t)\omega' = \gamma(\tfrac{1}{2}\omega^4 - \omega)t^2 + \gamma(\omega - 8)$$

for some $\gamma \in \boldsymbol{K}$ with $N\gamma = 1$. Taking $t = 0$ and 1 we would get $\gamma(\frac{1}{2}\omega^4 - \omega, \omega - 8)$ integral, hence $(\gamma)\frac{\mathfrak{p}}{\mathfrak{p}'}$ integral and $(\gamma) = \frac{\mathfrak{p}'}{\mathfrak{p}}$. However the ideal on the right-hand side is not principal.

3. Lemma 3. *Every form $F(x, y)$ with at least two distinct zeros can be represented as $F_1(ax + by, cx + dy)$, where F_1 is primary, $a, b, c, d \in \boldsymbol{Z}$ and* $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0$.

Proof. Suppose that $F(x, y) = G(ax + by, cx + dy)$, $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0$. Let F^* be the product of all distinct primitive irreducible factors of F and similarly G^* for G. It follows that

$$F^* = C^{-1}G^*(ax + by, cx + dy),$$

where $C = C(G^*(ax+by, cx+dy))|C(F)$. Hence

$$\operatorname{disc} F^* = C^{2-2|F^*|} \operatorname{disc} G^* \cdot \begin{vmatrix} a & b \\ c & d \end{vmatrix}^{|F^*|(|F^*|-1)}$$

and since $\operatorname{disc} F^* \neq 0$, $|F^*| > 1$ the absolute value of $\begin{vmatrix} a & b \\ c & d \end{vmatrix}$ is bounded.

Take now a representation of $F(x, y)$ as $G(ax+by, cx+dy)$, where $\begin{vmatrix} a & b \\ c & d \end{vmatrix}$ is maximal. G must be primary, otherwise representing it as $G_1(a_1x+b_1y, c_1x+d_1y)$ we would obtain a representation of F as $G_1(\alpha x+\beta y, \gamma x+\delta y)$ with

$$\operatorname{abs}\begin{vmatrix} \alpha & \beta \\ \gamma & \delta \end{vmatrix} = \operatorname{abs}\begin{vmatrix} a & b \\ c & d \end{vmatrix}, \quad \operatorname{abs}\begin{vmatrix} a_1 & b_1 \\ c_1 & d_1 \end{vmatrix} > \operatorname{abs}\begin{vmatrix} a & b \\ c & d \end{vmatrix},$$

contrary to the choice of G, unless $\begin{vmatrix} a_1 & b_1 \\ c_1 & d_1 \end{vmatrix} = 0$. In the latter case however G and hence also F would have only one zero, contrary to the assumption.

COROLLARY. C *implies* D.

Proof. Let $F(x, y) \in \boldsymbol{Z}[x, y]$ be any form, $f(\boldsymbol{t}) \in \boldsymbol{Z}[\boldsymbol{t}]$ any polynomial and suppose that for all $\boldsymbol{t} \in \boldsymbol{Z}^r$ there exist $x, y \in \boldsymbol{Z}$ satisfying $F(x, y) = f(\boldsymbol{t})$. If $F(x, y) = \text{const}$ or $f(\boldsymbol{t}) = \text{const}$ D is trivial. If $F(x, y)$ has only one zero, we take without loss of generality $F(x, y) = a(bx+cy)^n$, where $b \neq 0$. Applying Theorem 3 of [13] to the equation $au^n = f(\boldsymbol{t})$ we infer the existence of a polynomial $U(\boldsymbol{t}) \in \boldsymbol{Q}[\boldsymbol{t}]$ such that $a\, U(\boldsymbol{t})^n = f(\boldsymbol{t})$. It suffices to take $X(\boldsymbol{t}) = b^{-1}U(\boldsymbol{t})$, $Y(\boldsymbol{t}) = 0$.

If $F(x, y)$ has at least two distinct zeros then by Lemma 3 $F(x, y) = F_1(ax+by, cx+dy)$, where F_1 is primary and $\begin{vmatrix} a & b \\ c & d \end{vmatrix} \neq 0$. On the other hand there exists a vector $\boldsymbol{t}_0 \in \boldsymbol{Z}^r$ such that $f(\boldsymbol{t}_0) = e \neq 0$. Consider now the equation

$$F_1(x, y) = f(e\boldsymbol{t}+\boldsymbol{t}_0).$$

The polynomial on the right-hand side has both the content and the fixed divisor equal to $|e|$, hence by C there exist polynomials $X_1, Y_1 \in \boldsymbol{Z}[\boldsymbol{t}]$ such that $F_1(X_1(\boldsymbol{t}), Y_1(\boldsymbol{t})) = f(e\boldsymbol{t}+\boldsymbol{t}_0)$. Determining $X(\boldsymbol{t}), Y(\boldsymbol{t})$ from the equations

$$aX(\boldsymbol{t})+bY(\boldsymbol{t}) = X_1\left(\frac{\boldsymbol{t}-\boldsymbol{t}_0}{e}\right),$$

$$cX(\boldsymbol{t})+dY(\boldsymbol{t}) = Y_1\left(\frac{\boldsymbol{t}-\boldsymbol{t}_0}{e}\right)$$

we get

$$X(\boldsymbol{t}), Y(\boldsymbol{t}) \in \boldsymbol{Q}[\boldsymbol{t}], \quad F(X(\boldsymbol{t}), Y(\boldsymbol{t})) = f(\boldsymbol{t}),$$

thus D holds.

LEMMA 4. H *implies the following.*

Let $f_\nu \in \boldsymbol{Z}[\boldsymbol{t}]$ $(1 \leqslant \nu \leqslant n)$ be distinct irreducible polynomials such that their leading forms $h_\nu(\boldsymbol{t})$ all assume a positive value for a $\boldsymbol{t} \in \boldsymbol{N}^r$ and that $\prod_{\nu=1}^{n} f_\nu(\boldsymbol{t})$ has the fixed divisor 1. Then for any B there exists a $\boldsymbol{t} \in \boldsymbol{N}^r$ such that $f_\nu(\boldsymbol{t})$ are distinct primes $> B$.

Proof. The condition that f_ν are irreducible and distinct implies that they are prime to each other. Indeed, otherwise two of them would differ by a constant factor $c \neq 1$. The numerator and the denominator of c would divide $\prod_{\nu=1}^{n} f_\nu(\boldsymbol{t})$ for all $\boldsymbol{t}$ hence $c = -1$. But this contradicts the condition on h_ν.

Let us choose an $\boldsymbol{a} \in \boldsymbol{N}^r$ such that

$$h_\nu(\boldsymbol{a}) > 0 \quad (1 \leqslant \nu \leqslant n) \tag{15}$$

and let

$$a = (|h_1|+|h_2|+\ldots+|h_r|)! \prod_{\nu=1}^{n} h_\nu(\boldsymbol{a}).$$

Since

$$f(\boldsymbol{t}) = \prod_{\nu=1}^{n} f_\nu(\boldsymbol{t})$$

has the fixed divisor 1 we infer from the Chinese Remainder Theorem the existence of a $\boldsymbol{\tau} \in \boldsymbol{Z}^r$ such that

$$(f(\boldsymbol{\tau}), a) = 1. \tag{16}$$

Consider the polynomials $f_\nu(\boldsymbol{a}x+a\boldsymbol{t}+\boldsymbol{\tau})$ $(1 \leqslant \nu \leqslant n)$.

They are irreducible as polynomials in $x, \boldsymbol{t}$ and prime to each other. Consequently the resultant $R_{\mu,\nu}(\boldsymbol{t})$ of $f_\mu(\boldsymbol{a}x+a\boldsymbol{t}+\boldsymbol{\tau})$ and $f_\nu(\boldsymbol{a}x+a\boldsymbol{t}+\boldsymbol{\tau})$ is non-zero for all $\mu < \nu \leqslant n$. By Hilbert's irreducibility theorem there exists a $\boldsymbol{t}_0 \in \boldsymbol{Z}^r$ such that $f_\nu(\boldsymbol{a}x+a\boldsymbol{t}_0+\boldsymbol{\tau})$ $(1 \leqslant \nu \leqslant n)$ are all irreducible as polynomials in x and

$$\prod_{\mu<\nu}^{n} R_{\mu,\nu}(\boldsymbol{t}_0) \neq 0. \tag{17}$$

The leading coefficients of $f_\nu(\boldsymbol{a}x+a\boldsymbol{t}_0+\boldsymbol{\tau})$ are positive by (15). Moreover

$$p(x) = \prod_{\nu=1}^{n} f_\nu(\boldsymbol{a}x+a\boldsymbol{t}_0+\boldsymbol{\tau})$$

has the fixed divisor 1. Indeed, the $|p|$th difference

$$\Delta^{|p|} p(0) = a,$$

on the other hand
$$p(0) = f(a\boldsymbol{t}_0+\boldsymbol{\tau}) \equiv f(\boldsymbol{\tau}) \bmod a$$
and we get $(p(0), \Delta^{|p|}(0)) = 1$ by (16).

By H there exist infinitely many $x \in \boldsymbol{N}$ such that $f_\nu(\boldsymbol{a}x+a\boldsymbol{t}_0+\boldsymbol{\tau})$ are primes. For sufficiently large x we have $\boldsymbol{a}x+a\boldsymbol{t}_0+\boldsymbol{\tau} \in \boldsymbol{N}^r$ and

$$f_\nu(\boldsymbol{a}x+a\boldsymbol{t}_0+\boldsymbol{\tau}) > |B| + \sum_{\mu<\nu}^{n} |R_{\mu,\nu}(\boldsymbol{t}_0)|. \tag{18}$$

Thus the primes in question are $> B$. They are distinct since the common value of $f_\mu(\boldsymbol{a}x+a\boldsymbol{t}_0+\boldsymbol{\tau})$ and $f_\nu(\boldsymbol{a}x+a\boldsymbol{t}_0+\boldsymbol{\tau})$ would have to divide $R_{\mu,\nu}(\boldsymbol{t}_0)$ which is impossible by (17) and (18).

LEMMA 5. *Let $\boldsymbol{K}$ be the rational field or a quadratic field, Δ be the discriminant of $\boldsymbol{K}$ and let $\varphi_\nu \in \boldsymbol{K}[\boldsymbol{t}]$ $(1 \leqslant \nu \leqslant n)$ be polynomials irreducible over $\boldsymbol{K}$ and prime to each other. If*

$$\text{the fixed divisor of } \prod_{\nu=1}^{n} N\varphi_\nu(\boldsymbol{t}) \text{ equals } \prod_{\nu=1}^{n} NC(\varphi_\nu) \tag{19}$$

then for every $M \in \boldsymbol{N}$, there exists a $\mu \in \boldsymbol{N}$ prime to M with no prime ideal factor of degree 1 in $\boldsymbol{K}$ and $\boldsymbol{\tau} \in \boldsymbol{Z}^r$ with the following property. Let
$$\psi_\nu(\boldsymbol{t}) = \varphi_\nu(\mu\boldsymbol{t}+\boldsymbol{\tau}) \qquad (1 \leqslant \nu \leqslant n).$$
For any $A \in \boldsymbol{N}$, $\boldsymbol{t}_1 \in \boldsymbol{Z}^r$ and $m \in \boldsymbol{N}$ prime to $A\prod_{\nu=1}^{n}\frac{N\psi_\nu(\boldsymbol{t}_1)}{NC(\psi_\nu)}$ H implies the existence of a $\boldsymbol{t}_2 \in \boldsymbol{N}^r$ such that $\boldsymbol{t}_2 \equiv \boldsymbol{t}_1 \bmod m$, all the ideals $\frac{(\psi_\nu(\boldsymbol{t}_2))}{C(\psi_\nu)}$ are prime in $\boldsymbol{K}$, distinct and do not divide A.

Moreover, either $\mu = 1$, $\boldsymbol{\tau} = \boldsymbol{0}$ have the above property (this happens for $\boldsymbol{K} = \boldsymbol{Q}$) or there is a sequence of pairs $\langle \mu_i, \boldsymbol{\tau}_i \rangle$ with the above property such that $(\mu_i, \mu_h) = 1$ for $i \neq h$, and the number of distinct $\mu_i \leqslant x$ is greater than $cx^{1/n}/\log x$ for a certain $c > 0$ and all $x > x_0$.

Proof. We begin with a remark concerning the fixed divisor that we shall use twice. If $P \in \boldsymbol{Z}[\boldsymbol{t}]$ has the fixed divisor d then any fixed prime divisor p of $P(m\boldsymbol{t}+\boldsymbol{a})$ divides dm. Indeed if $p \nmid d$ then there exists a $\boldsymbol{u} \in \boldsymbol{Z}^r$ such that $P(\boldsymbol{u}) \not\equiv 0 \bmod p$ and if $p \nmid m$ there exists a $\boldsymbol{v} \in \boldsymbol{Z}^r$ such that $m\boldsymbol{v}+\boldsymbol{a} \equiv \boldsymbol{u} \bmod p$, hence $P(m\boldsymbol{v}+\boldsymbol{a}) \not\equiv 0 \bmod p$.

Now we proceed to the proof of the lemma. Let
$$\varphi_\nu(\boldsymbol{t}) = a_\nu f_\nu(\boldsymbol{t}) \qquad (\nu \leqslant k),$$
$$N\varphi_\nu(\boldsymbol{t}) = a_\nu f_\nu(\boldsymbol{t}) \qquad (k < \nu \leqslant n),$$
where $f_\nu \in \boldsymbol{Z}[\boldsymbol{t}]$ are irreducible over $\boldsymbol{Q}$ and
$$(a_\nu) = C(\varphi_\nu) \qquad (\nu \leqslant k),$$
$$|a_\nu| = NC(\varphi_\nu) \qquad (k < \nu \leqslant n).$$

(If $\boldsymbol{K} = \boldsymbol{Q}$ we take $k = 0$.) Let h_ν be the leading form of f_ν. We can choose the signs of a_ν so that for a suitable $\boldsymbol{t} \in \boldsymbol{N}^r$: $h_\nu(\boldsymbol{t}) > 0$ for all $\nu \leqslant n$. We have

$$\prod_{\nu=1}^{n}\frac{N\varphi_\nu(\boldsymbol{t})}{NC(\varphi_\nu)} = \pm\prod_{\nu=1}^{k} f_\nu^2(\boldsymbol{t}) \prod_{\nu=k+1}^{n} f_\nu(\boldsymbol{t}) \tag{20}$$

and (19) implies on an application of the Chinese Remainder Theorem that for a suitable $\boldsymbol{\tau}_0 \in \boldsymbol{Z}^r$

$$\Big(\Delta, \prod_{\nu=1}^{n} f_\nu(\boldsymbol{\tau}_0)\Big) = 1. \tag{21}$$

Let $f_\nu(\boldsymbol{\tau}_0) \equiv \varrho_\nu \bmod \Delta$, $\varrho_\nu > 0$ $(\nu \leqslant k)$. Without loss of generality we may assume that

$$\left(\frac{\Delta}{\varrho_\nu}\right) = 1 \;\; (1 \leqslant \nu \leqslant j), \qquad \left(\frac{\Delta}{\varrho_\nu}\right) = -1 \;\; (j \leqslant \nu \leqslant k). \tag{22}$$

Since φ_ν are prime to each other

(23) $\quad (f_\lambda, f_\nu) = 1$ unless $\lambda = \nu$ or $\lambda > k$, $\nu > k$ and $\varphi_\lambda/\varphi'_\nu \in \boldsymbol{K}$,

where φ'_ν is conjugate to φ_ν over $\boldsymbol{Q}(\boldsymbol{t})$.

In particular, $f_1, \ldots, f_j$ and $\prod_{\nu=j+1}^{n} f_\nu$ are prime to each other.

Let $\boldsymbol{t} = [t, \boldsymbol{t}']$, $a_0(\boldsymbol{t}')$ be the leading coefficient of $\prod_{\nu=1}^{n} f_\nu(\boldsymbol{t})$, $D(\boldsymbol{t}')$ the discriminant of $\prod_{\nu=1}^{j} f_\nu(\boldsymbol{t})$ and $R(\boldsymbol{t}')$ the resultant of $\prod_{\nu=1}^{j} f_\nu(\boldsymbol{t})$, $\prod_{\nu=j+1}^{n} f_\nu(\boldsymbol{t})$ with respect to t. It follows that

$$a_0 DR \neq 0. \tag{24}$$

Since $f_\nu(\boldsymbol{t})$ are irreducible over $\boldsymbol{K}$ for $\nu \leqslant j$ we infer by Hilbert's irreducibility theorem that there exists a $\boldsymbol{\tau}' \in \boldsymbol{Z}^{r-1}$ such that $f_\nu(t, \boldsymbol{\tau}')$ are irreducible over $\boldsymbol{K}$ for $\nu \leqslant j$ and

$$a_0(\boldsymbol{\tau}')D(\boldsymbol{\tau}')R(\boldsymbol{\tau}') \neq 0. \tag{25}$$

Let $f_\nu(\vartheta_\nu, \boldsymbol{\tau}') = 0$ and $\boldsymbol{K}_\nu = \boldsymbol{Q}(\vartheta_\nu)$ $(\nu \leqslant j)$. We have $\boldsymbol{K} \not\subset \boldsymbol{K}_\nu$ and by Bauer's theorem there exist for each $\nu \leqslant j$ infinitely many primes with a prime ideal factor of degree 1 in $\boldsymbol{K}_\nu$, but not in $\boldsymbol{K}$. Choose for each $\nu \leqslant j$ a different prime p_ν with the above property and such that

$$p_\nu \nmid M a_0(\boldsymbol{\tau}')D(\boldsymbol{\tau}')R(\boldsymbol{\tau}'). \tag{26}$$

Since p_ν does not split in $\boldsymbol{K}$ we have

$$\left(\frac{\Delta}{p_\nu}\right) = -1 \qquad (\nu \leqslant j). \tag{27}$$

On the other hand, since p_ν has a prime ideal factor of degree 1 in $\boldsymbol{K}_\nu$ by Dedekind's theorem there exists an integer u such that
$$f_\nu(u, \boldsymbol{\tau}') \equiv 0 \bmod p_\nu.$$

By (25) and (26) the discriminant of $\prod_{i=1}^{j} f_i(t, \boldsymbol{\tau}')$ equals $D(\boldsymbol{\tau}') \not\equiv 0 \pmod{p_\nu}$. Since $a_0(\boldsymbol{\tau}') \not\equiv 0 \bmod p_\nu$ and $\prod_{i=1}^{j} f_i(u, \boldsymbol{\tau}') \equiv 0 \bmod p_\nu$ we infer from Lemma 1 that either

$$\prod_{i=1}^{j} f_i(u, \boldsymbol{\tau}') \not\equiv 0 \bmod p_\nu^2$$

or

$$\prod_{i=1}^{j} f_i(u+p_\nu, \boldsymbol{\tau}') \not\equiv 0 \bmod p_\nu^2.$$

Therefore, there exists an integer τ_ν such that

$$f_\nu(\tau_\nu, \boldsymbol{\tau}') \equiv 0 \bmod p_\nu, \tag{28}$$

$$\prod_{i=1}^{j} f_i(\tau_\nu, \boldsymbol{\tau}') \not\equiv 0 \bmod p_\nu^2. \tag{29}$$

Moreover, since by (25) and (26) the resultant of $\prod_{i=1}^{j} f_i(t, \boldsymbol{\tau}')$ and $\prod_{i=j+1}^{n} f_i(t, \boldsymbol{\tau}')$ equal to $R(\boldsymbol{\tau}') \not\equiv 0 \bmod p_\nu$ we have

$$\prod_{i=j+1}^{n} f_i(\tau_\nu, \boldsymbol{\tau}') \not\equiv 0 \bmod p_\nu. \tag{30}$$

Let us choose $\tau \equiv \tau_\nu \bmod p_\nu^2$ $(1 \leqslant \nu \leqslant j)$ and set

$$\mu = \prod_{\nu=1}^{j} p_\nu, \qquad \boldsymbol{\tau} = [\tau, \boldsymbol{\tau}']. \tag{31}$$

By (28)–(30) we have

$$f_\nu(\boldsymbol{\tau}) \equiv 0 \bmod p_\nu, \tag{32}$$

$$\prod_{i=1}^{n} f_i(\boldsymbol{\tau}) \not\equiv 0 \bmod p_\nu^2. \tag{33}$$

We shall show that

$$\prod_{i=1}^{n} f_i(\mu \boldsymbol{t}+\boldsymbol{\tau}) = P(\mu \boldsymbol{t}+\boldsymbol{\tau})$$

has the fixed divisor d equal to $p_1 p_2 \ldots p_j$. Indeed by (19) and (20) the fixed divisor of $P(\boldsymbol{t})$ equals 1, hence d consists of prime factors of μ. However by (33)

$$d \not\equiv 0 \bmod p_\nu^2 \qquad (\nu \leqslant j).$$

On the other hand by (31) and (32)

$$f_\nu(\mu \boldsymbol{t}+\boldsymbol{\tau}) \equiv f_\nu(\boldsymbol{\tau}) \equiv 0 \bmod p_\nu.$$

Thus $d = p_1 p_2 \ldots p_j$, the polynomials

$$\begin{aligned} g_\nu(\boldsymbol{t}) &= p_\nu^{-1} f_\nu(\mu \boldsymbol{t}+\boldsymbol{\tau}) \quad (\nu \leqslant j), \\ g_\nu(\boldsymbol{t}) &= f_\nu(\mu \boldsymbol{t}+\boldsymbol{\tau}) \quad (j < \nu \leqslant n) \end{aligned} \tag{34}$$

have integral coefficients, $\prod_{\nu=1}^{n} g_\nu(\boldsymbol{t})$ has the fixed divisor 1 and *a fortiori* the content 1. Moreover by (23)

$$g_\lambda \neq g_\nu \text{ unless } \lambda = \nu \text{ or } \lambda > k,\ \nu > k \text{ and } \varphi_\lambda/\varphi'_\nu \in \boldsymbol{K}. \tag{35}$$

It follows that

$$\begin{aligned} \psi_\nu(\boldsymbol{t}) &= a_\nu p_\nu g_\nu(\boldsymbol{t}) \quad (\nu \leqslant j), \\ \psi_\nu(\boldsymbol{t}) &= a_\nu g_\nu(\boldsymbol{t}) \quad (j < \nu \leqslant k), \end{aligned} \tag{36}$$

$$N\psi_\nu(\boldsymbol{t}) = a_\nu g_\nu(\boldsymbol{t}) \quad (k < \nu \leqslant n), \tag{37}$$

where besides

$$C(\psi_\nu) = (a_\nu p_\nu) \ (\nu \leqslant j), \qquad C(\psi_\nu) = (a_\nu) \ (j < \nu \leqslant k), \tag{38}$$

$$NC(\psi_\nu) = |a_\nu| \quad (k < \nu \leqslant n). \tag{39}$$

It follows that

$$\prod_{\nu=1}^{n} \frac{N\psi_\nu(\boldsymbol{t})}{NC(\psi_\nu)} = \pm \prod_{\nu=1}^{k} g_\nu^2(\boldsymbol{t}) \prod_{\nu=k+1}^{n} g_\nu(\boldsymbol{t}).$$

If now for a $\boldsymbol{t}_1 \in \boldsymbol{Z}^r$ we have

$$\left(m, \Delta \prod_{\nu=1}^{n} \frac{N\psi_\nu(\boldsymbol{t}_1)}{NC(\psi_\nu)}\right) = 1$$

there exists a $\boldsymbol{t}_0 \in \boldsymbol{Z}^r$ satisfying

$$\boldsymbol{t}_0 \equiv \boldsymbol{t}_1 \bmod m, \qquad \mu \boldsymbol{t}_0 + \boldsymbol{\tau} \equiv \boldsymbol{\tau}_0 \bmod \Delta. \tag{40}$$

Since

$$\left(m, \prod_{\nu=1}^{n} g_\nu(\boldsymbol{t}_0)\right) = \left(m, \prod_{\nu=1}^{n} g_\nu(\boldsymbol{t}_1)\right) = 1$$

and by (34) and (21)

$$\left(\Delta, \prod_{\nu=1}^{n} g_\nu(\boldsymbol{t}_0)\right) = \left(\Delta, \prod_{\nu=1}^{n} g_\nu(0)\right) = \left(\Delta, \prod_{\nu=1}^{n} f_\nu(\boldsymbol{\tau}_0)\right) = 1$$

it follows that

$$\prod_{\nu=1}^{n} g_\nu(\Delta m \boldsymbol{t} + \boldsymbol{t}_0)$$

has the fixed divisor 1. The polynomials $g_\nu(\Delta m\boldsymbol{t}+\boldsymbol{t}_0)$ are irreducible and their leading forms all take a positive value for a suitable $\boldsymbol{t}\in\boldsymbol{N}^r$ in virtue of the corresponding property of $f_\nu(\boldsymbol{t})$. By Lemma 4 H implies the existence of an $\boldsymbol{x}\in\boldsymbol{N}^r$ such that $g_\nu(\Delta m\boldsymbol{x}+\boldsymbol{t}_0)$ are primes greater than $|\Delta|$ and

$$(41)\qquad g_\lambda(\Delta m\boldsymbol{x}+\boldsymbol{t}_0)\neq g_\nu(\Delta m\boldsymbol{x}+\boldsymbol{t}_0)\quad\text{unless } g_\lambda=g_\nu .$$

Taking $\boldsymbol{t}_2=\Delta m\boldsymbol{x}+\boldsymbol{t}_0$ we get from (40)

$$(42)\qquad \boldsymbol{t}_2\equiv\boldsymbol{t}_1 \bmod m,\qquad \mu\boldsymbol{t}_2+\boldsymbol{\tau}\equiv\boldsymbol{\tau}_0 \bmod \Delta .$$

Thus by (34)

$$p_\nu g_\nu(\boldsymbol{t}_2)=f_\nu(\mu\boldsymbol{t}_2+\boldsymbol{\tau})\equiv f_\nu(\boldsymbol{\tau}_0)\equiv\varrho_\nu \bmod\Delta\qquad(\nu\leqslant j),$$
$$g_\nu(\boldsymbol{t}_2)=f_\nu(\mu\boldsymbol{t}_2+\boldsymbol{\tau})\equiv f_\nu(\boldsymbol{\tau}_0)\equiv\varrho_\nu \bmod\Delta\qquad(j<\nu\leqslant k)$$

and we infer from (22) and (27) that

$$\left(\frac{\Delta}{g_\nu(\boldsymbol{t}_2)}\right)=-1\qquad(\nu\leqslant k).$$

Hence for $\nu\leqslant k$ $g_\nu(\boldsymbol{t}_2)$ are prime in $\boldsymbol{K}$ not dividing Δ and in virtue of (36) and (38) the same applies to the ideals $\mathfrak{a}_\nu=\dfrac{(\psi_\nu(\boldsymbol{t}_2))}{C(\psi_\nu)}$. The remaining ideals $\mathfrak{a}_\nu$ $(\nu<k\leqslant n)$ are prime and do not divide Δ in virtue of (37) and (39).

Assuming

$$\lambda\neq\nu,\qquad\mathfrak{a}_\lambda=\mathfrak{a}_\nu$$

we get by (35) and (41) for a suitable $\gamma\in\boldsymbol{K}$

$$\lambda>k,\quad \nu>k,\quad \varphi_\lambda=\gamma\varphi'_\nu,\quad \psi_\lambda=\gamma\psi'_\nu,\quad C(\psi_\lambda)=(\gamma)C(\psi'_\nu),$$
$$\frac{(\psi_\nu(\boldsymbol{t}_2))}{C(\psi_\nu)}=\frac{(\psi'_\nu(\boldsymbol{t}_2))}{C(\psi'_\nu)},$$

thus the ideal $\mathfrak{a}_\nu$ is ambiguous.

By Dedekind's theorem $\mathfrak{a}_\nu|\Delta$, hence by (37) and (39)

$$g_\nu(\boldsymbol{t}_2)|\Delta .$$

However by (34) and (42)

$$g_\nu(\boldsymbol{t}_2)=f_\nu(\mu\boldsymbol{t}_2+\boldsymbol{\tau})\equiv f_\nu(\boldsymbol{\tau}_0)\bmod\Delta$$

and we get a contradiction with (21). The contradiction shows that the ideals $\mathfrak{a}_\nu$ are distinct and the proof of the first part of the lemma is complete.

To prove the second part we note that if $j=0$ (31) gives $\mu=1$. The value of $\boldsymbol{\tau}$ is then irrelevant and can be taken $\boldsymbol{0}$. Therefore assume that $j>0$ and that we have already defined $\langle\mu_1,\boldsymbol{\tau}_1\rangle,\ldots,\langle\mu_{i-1},\boldsymbol{\tau}_{i-1}\rangle$ $(i\geqslant1)$, each μ_i with j prime factors. Then we replace in the above proof M by $M\mu_1\ldots\mu_{i-1}$ and define $\mu_i,\boldsymbol{\tau}_i$ by (31). It is clear that the sequence

thus obtained satisfies $(\mu_i,\mu_h)=1$ for $i\neq h$. Denote by $P(\boldsymbol{K}_\nu)$ the set of primes with a prime ideal factor of degree 1 in $\boldsymbol{K}_\nu$. By Bauer's theorem $P(\boldsymbol{K}_\nu)\setminus P(\boldsymbol{K})$ has a positive density, say, δ_ν. Computing μ_i from (31) we take p_ν to be the least element of $P(\boldsymbol{K}_\nu)\setminus P(\boldsymbol{K})$ different from $\omega+j(i-1)+\nu-1$ given primes, where ω is the number of prime factors of $Ma_0(\boldsymbol{\tau}')D(\boldsymbol{\tau}')R(\boldsymbol{\tau}')$. Hence for $i>i_0$ we have $p_\nu\leqslant2\delta_\nu^{-1}ji\log ji$ and

$$\mu_i=\prod_{\nu=1}^{j}p_\nu\leqslant(c^{-1}ji\log ji)^j,\qquad c=\tfrac12\prod_{\nu=1}^{j}\delta_\nu^{1/j}.$$

Since the number of solutions of the inequality

$$(c^{-1}ji\log ji)^j\leqslant x$$

in positive integers i is for x large enough at least $\dfrac{cx^{1/j}}{\log x-1}$, the number of distinct $\mu_i\leqslant x$ is at least

$$\frac{cx^{1/j}}{\log x-1}-i_0>\frac{cx^{1/n}}{\log x}\qquad(x>x_0)$$

which completes the proof.

Remark. The lemma extends to all cyclic fields.

LEMMA 6. *Let $\boldsymbol{K}$ be any field, $f\in\boldsymbol{K}[\boldsymbol{t}]$ a non-zero polynomial. If a form $F\in\boldsymbol{K}[x,y]$ has at least three distinct zeros in the algebraic closure of $\boldsymbol{K}$ then there exist no more than $|F|^3 3^{|f|}$ pairs $\langle X(\boldsymbol{t}),Y(\boldsymbol{t})\rangle$ such that $X,Y\in\boldsymbol{K}(\boldsymbol{t})$, X,Y linearly independent over $\boldsymbol{K}$ and*

$$(43)\qquad F\big(X(\boldsymbol{t}),Y(\boldsymbol{t})\big)=f(\boldsymbol{t}).$$

Proof. Without loss of generality we may assume that $\boldsymbol{K}$ is algebraically closed. By a linear transformation we can transform F to the form

$$F(x,y)=x^ky^lG(x,y),\qquad k\geqslant1,\ l\geqslant1,\qquad\big(G(x,y),xy\big)=1.$$

Let us assign two solutions $\langle X_1,Y_1\rangle$ and $\langle X_2,Y_2\rangle$ of (43) to the same class if $X_2=\xi X_1$, $Y_2=\eta Y_1$ for some $\xi,\eta\in\boldsymbol{K}\setminus\{0\}$. The number of classes does not exceed the number of pairs of monic polynomials $x,y\in\boldsymbol{K}[\boldsymbol{t}]$ such that

$$xy|f(\boldsymbol{t}),$$

which is clearly bounded by $3^{|f|}$. The number of polynomials in one class can be estimated as follows.

If

$$F(\xi X_1,\eta Y_1)=F(X_1,Y_1)$$

then

$$F\left(\xi\frac{X_1}{Y_1},\eta\right)=F\left(\frac{X_1}{Y_1},1\right)$$

and since X_1/Y_1 takes in $\boldsymbol{K}$ infinitely many values we have identically

$$F(\xi u, \eta) = F(u, 1).$$

Hence

$$\xi^k \eta^l G(\xi u, \eta) = G(u, 1)$$

and the comparison of the leading coefficients and of the constant terms on both sides gives

$$\xi^k \eta^l \xi^{|G|} = 1, \quad \xi^k \eta^l \eta^{|G|} = 1.$$

It follows that

$$\xi^{|G|} = \eta^{|G|}, \quad \xi^{|G|(k+l+|G|)} = 1, \quad \xi^{|G||F|} = 1.$$

Thus there are $|G||F|$ possibilities for ξ and for each ξ at most $|G|$ possibilities for η, which gives at most $|F|\,|G|^2 \leqslant |F|^3$ possibilities for $\langle \xi, \eta \rangle$. The lemma follows.

LEMMA 7. *If $F(x, y) \in \boldsymbol{Z}[x, y]$ is a non-singular cubic form then for every integer $a \neq 0$ the number of solutions of the equation $F(x, y) = az^3$ in integers x, y, z such that $(x, y, z) = 1$ and $1 \leqslant z \leqslant Z$ is $O\left((\log Z)^b\right)$, where b is a constant depending on F and a.*

Proof. It is enough to estimate the number of solutions with $|x| \leqslant |y|$. Assume that

(44) $$F(x, y) = az^3, \quad 1 \leqslant z \leqslant Z \text{ and } |x| \leqslant |y|.$$

If $F(1, 0) = 0$ we have $|F(x, y)| \geqslant |y|$ hence $h = \max(|x|, |y|, |z|) \ll Z^3$, where the constant in the symbol $\ll$ depends on a, later also on F. If $F(1, 0) \neq 0$ let

(45) $$F(x, y) = a_0 \prod_{i=1}^{3} (x - \xi_i y),$$

where ξ_1 is the real zero of F nearest to x/y. Since $F(x, y) \neq 0$ we have by Thue's theorem

$$|x - \xi_1 y| \gg |y|^{-3/2}.$$

On the other hand $|x - \xi_2 y|\,|x - \xi_3 y| \gg y^2$. Hence by (44) and (45)

$$|a| z^3 = |F(x, y)| \gg y^{1/2} \quad \text{and} \quad h \ll Z^6.$$

Since $F(x, y) = az^3$ represents in projective coordinates a curve of genus 1, in virtue of a theorem of Néron (see [8], p. 82) the number of solutions of (44) is $O\left((\log Z^6)^{g/2+1}\right)$ where g is the rank of the curve.

Remark. The lemma extends to all forms F with at least three distinct zeros. If the genus of the curve $F(x, y) = az^{|F|}$ is greater than 1 one needs a theorem of Mumford [10].

LEMMA 8. *Let $\boldsymbol{K}$ be any field, U a finite subset of $\boldsymbol{K}$ and $P \in \boldsymbol{K}[\boldsymbol{t}]$, $P \neq 0$. The equation $P(\boldsymbol{t}) = 0$ has no more than $|P|\,|U|^{r-1}$ solutions $\boldsymbol{t} \in U^r$, where $|U|$ is the number of elements of U.*

Proof (by induction on r). For $r = 1$ the assertion is obvious. Assume that it holds for polynomials in $r-1$ variables and let

$$P(\boldsymbol{t}) = \sum_{i=0}^{p} P_i(\boldsymbol{t}') t_1^{p-i}.$$

The solutions of $P(\boldsymbol{t}) = 0$ are of two kinds: satisfying $P_0(\boldsymbol{t}') = 0$ and $P_0(\boldsymbol{t}') \neq 0$. Since t_1 can take at most $|U|$ values, by the inductive assumption the number of solutions of the first kind does not exceed $|P_0|\,|U|^{r-1}$. Similarly since $\boldsymbol{t}'$ can take at most $|U|^{r-1}$ values the number of solutions of the second kind does not exceed $p\,|U|^{r-1}$. However $|P_0| + p \leqslant |P|$ and the proof is complete.

Remark. A different proof can be obtained by an adaptation of the proof given by Schmidt for the special case $\boldsymbol{K} = U$ (see [17], p. 147, Lemma 3A).

LEMMA 9. *If $f(\boldsymbol{t}), g(\boldsymbol{t}) \in \boldsymbol{Q}[\boldsymbol{t}]$, $g(\boldsymbol{t}) \mid f(\boldsymbol{t})^n$ and the fixed divisor of $f(\boldsymbol{t})$ equals $C(f)$ then the fixed divisor of $g(\boldsymbol{t})$ equals $C(g)$.*

Proof. Let the fixed divisor of g be $C(g)d$, $d \in \boldsymbol{N}$ and let $f(\boldsymbol{t})^n = g(\boldsymbol{t})h(\boldsymbol{t})$. Clearly for all $\boldsymbol{t} \in \boldsymbol{Z}^r$ $f(\boldsymbol{t})^n$ is divisible by $C(g)\,d\,C(h) = d\,C(f^n) = d\,C(f)^n$. On the other hand the fixed divisor of $f(\boldsymbol{t})^n$ is $C(f)^n$. Hence $d = 1$.

Proof of Theorem 2. Consider first the case, where F is a quadratic form. Then by Lemma 2

$$F(x, y) = A(ax^2 + bxy + cy^2), \quad \text{where} \quad A, a, b, c \in \boldsymbol{Z}$$

and either $\Delta = b^2 - 4ac = 1$ or Δ is a fundamental discriminant. Since the fixed divisor of $f(\boldsymbol{t})$ equals $C(f)$ we have $A \mid C(f)$ and we can assume without loss of generality that $A = 1$. Let $\boldsymbol{K} = \boldsymbol{Q}(\sqrt{\Delta})$

(46) $$f(\boldsymbol{t}) = l \prod_{\nu=1}^{n} \varphi_\nu(\boldsymbol{t})^{e_\nu}$$

be a factorization of $f(\boldsymbol{t})$ over $\boldsymbol{K}$ into irreducible factors such that φ_ν are distinct and have the coefficient of the first term in the antilexicographic order equal to 1. Since the fixed divisor of f equals $C(f)$ the condition (19) is satisfied in virtue of Lemma 9. Let μ, τ be parameters whose existence for $\{\varphi_\nu\}$ and $M = a$ is asserted in Lemma 5 and let

$$\psi_\nu = \varphi_\nu(\mu\boldsymbol{t} + \tau) \quad (1 \leqslant \nu \leqslant n).$$

It follows that

(47) $$f(\mu\boldsymbol{t} + \tau) = l \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t})^{e_\nu}$$

and

(48) $$B = |l| \prod_{\nu=1}^{n} C(\psi_\nu)^{e_\nu} = C\left(f(\mu\boldsymbol{t} + \tau)\right) \in \boldsymbol{N},$$

where an ideal in $\boldsymbol{Q}$ is identified with its positive generator. If $\Delta = 1$ is equivalent to xy and Theorem 1 applies. Assume that $\Delta \neq 1$, thus is a quadratic field. Taking $m = 1$ in Lemma 5 we infer that H impli the existence of a $\boldsymbol{t}_2 \in \boldsymbol{Z}^r$ such that $\frac{(\psi_\nu(\boldsymbol{t}_2))}{C(\psi_\nu)}$ are distinct prime ide of $\boldsymbol{K}$ not dividing B. By the assumption there exist $x_0, y_0 \in \boldsymbol{Z}$ such th

$$ax_0^2 + bx_0y_0 + cy_0^2 = f(\mu\boldsymbol{t}_2 + \boldsymbol{\tau}). \tag{49}$$

Hence, after a transformation

$$N\frac{\left(ax_0 + \frac{b+\sqrt{\Delta}}{2}y_0\right)}{\mathfrak{a}} = |f(\mu\boldsymbol{t}_2+\boldsymbol{\tau})|, \quad \text{where} \quad \mathfrak{a} = \left(a, \frac{b+\sqrt{\Delta}}{2}\right).$$

It follows from (47) and (48) that for an integral ideal $\mathfrak{b}$ and some $a_\nu \geqslant$

$$\left(ax_0 + \frac{b+\sqrt{\Delta}}{2}y_0\right)\mathfrak{a}^{-1} = \mathfrak{b}\prod_{\nu=1}^{n}\frac{(\psi_\nu(\boldsymbol{t}_2))^{a_\nu}}{C(\psi_\nu)^{a_\nu}}, \qquad \left(\mathfrak{b}, \prod_{\nu=1}^{n}\frac{(\psi_\nu(\boldsymbol{t}_2))}{C(\psi_\nu)}\right) = 1. \tag{50}$$

On the other hand $\varphi_\nu^{e_\nu} \| f(\boldsymbol{t})$ implies $\varphi_\nu'^{e_\nu} \| f(\boldsymbol{t})$, where φ_ν' is conjugate to with respect to $\boldsymbol{Q}(\boldsymbol{t})$. If $\varphi_\nu \notin \boldsymbol{Q}[\boldsymbol{t}]$ we have $\varphi_\nu' \neq \varphi_\nu$ and since φ_ν' has tl coefficient of the leading term equal to 1, by (46)

$$\varphi_\nu' = \varphi_\lambda, \quad e_\nu = e_\lambda; \quad \psi_\nu' = \psi_\lambda \quad \text{for a } \lambda \neq \nu.$$

Thus without loss of generality we may assume that for a certai $k \equiv n \bmod 2$

$$\varphi_\nu' = \varphi_{\nu'}, \quad e_\nu = e_{\nu'}, \quad \psi_\nu' = \psi_{\nu'}, \quad \text{where} \quad \nu' = \nu \ (1 \leqslant \nu \leqslant k), \tag{51}$$
$$\nu' = \nu - (-1)^{n-\nu} \ (k < \nu \leqslant n).$$

Hence by (48)

$$|ax_0^2 + bx_0y_0 + cy_0^2| = N\mathfrak{b}\prod_{\nu=1}^{n}\left(\frac{\psi_\nu(\boldsymbol{t}_2)}{C(\psi_\nu)}\right)^{a_\nu + a_{\nu'}}, \qquad \left(N\mathfrak{b}, \prod_{\nu=1}^{n}\frac{(\psi_\nu(\boldsymbol{t}_2))}{C(\psi_\nu)}\right) = 1$$

and a comparison with (49) gives

$$a_\nu + a_{\nu'} = e_\nu \quad (1 \leqslant \nu \leqslant n). \tag{52}$$

Let us define now $X(\boldsymbol{t})$, $Y(\boldsymbol{t})$ by the equation

$$\vartheta(\boldsymbol{t}) = aX(\boldsymbol{t}) + \frac{b+\sqrt{\Delta}}{2}Y(\boldsymbol{t}) = \left(ax_0 + \frac{b+\sqrt{\Delta}}{2}y_0\right)\prod_{\nu=1}^{n}\left(\frac{\varphi_\nu(\boldsymbol{t})}{\psi_\nu(\boldsymbol{t}_2)}\right)^{a_\nu}. \tag{53}$$

The polynomials $X(\boldsymbol{t})$, $Y(\boldsymbol{t})$ have integral coefficients since by (50)

$$C(\vartheta(\mu\boldsymbol{t}+\boldsymbol{\tau})) = \left(ax_0 + \frac{b+\sqrt{\Delta}}{2}y_0\right)\prod_{\nu=1}^{n}\left(\frac{C(\varphi_\nu)}{(\psi_\nu(\boldsymbol{t}_2))}\right)^{a\nu} = \mathfrak{a}\mathfrak{b},$$

$$\mu^{|\vartheta|}C(\vartheta) \equiv 0 \bmod \mathfrak{a}$$

and $(\mu, a) = 1$ implies $C(\vartheta) \equiv 0 \bmod \mathfrak{a}$.

On the other hand, by (53), (49), (51), (52), (46) and (47)

$$\begin{aligned} F(X(\boldsymbol{t}), Y(\boldsymbol{t})) &= aX(\boldsymbol{t})^2 + bX(\boldsymbol{t})Y(\boldsymbol{t}) + cY(\boldsymbol{t})^2 \\ &= (ax_0^2 + bx_0y_0 + cy_0^2)\prod_{\nu=1}^{n}\left(\frac{\varphi_\nu(\boldsymbol{t})\varphi_\nu'(\boldsymbol{t})}{\psi_\nu(\boldsymbol{t}_2)\psi_\nu'(\boldsymbol{t}_2)}\right)^{a_\nu} \\ &= f(\mu\boldsymbol{t}_2 + \boldsymbol{\tau})\prod_{\nu=1}^{n}\left(\frac{\varphi_\nu(\boldsymbol{t})}{\psi_\nu(\boldsymbol{t}_2)}\right)^{a_\nu + a_{\nu'}} \\ &= f(\mu\boldsymbol{t}_2 + \boldsymbol{\tau})\prod_{\nu=1}^{n}\left(\frac{\varphi_\nu(\boldsymbol{t})}{\psi_\nu(\boldsymbol{t}_2)}\right)^{e_\nu} = f(\boldsymbol{t}). \end{aligned}$$

Assume now that F is a reducible cubic form. If F is singular we have $F = (ax+by)^2(cx+dy)$, hence by the condition (1)

$$\begin{vmatrix} a & b \\ c & d \end{vmatrix} = \pm 1,$$

F is equivalent to x^2y and Theorem 1 applies.

If F is non-singular we have

$$F(x, y) = (a_0x + b_0y)F_1(x, y), \tag{54}$$

where F_1 is a non-singular primitive quadratic form. By Lemma 3 we have

$$F_1(x, y) = G(a_1x + b_1y, a_2x + b_2y), \tag{55}$$

where G is primary and primitive. Let us put $G(x, y) = ex^2 + gxy + hy^2$. By Lemma 2, the discriminant $\Delta = g^2 - 4eh$ equals 1 or is fundamental. The condition that F is primary implies that

$$d = \left(\begin{vmatrix} a_0 & a_1 \\ b_0 & b_1 \end{vmatrix}, \begin{vmatrix} a_1 & a_2 \\ b_1 & b_2 \end{vmatrix}, \begin{vmatrix} a_2 & a_0 \\ b_2 & b_0 \end{vmatrix}\right) = 1. \tag{56}$$

Otherwise, by a classical result on integral matrices (see [2], p. 52) the linear forms $a_ix + b_iy$ $(0 \leqslant i \leqslant 2)$ would be expressible integrally in terms of two linear forms with determinant $d > 1$. Let $\boldsymbol{K} = \boldsymbol{Q}(\sqrt{\Delta})$ and let the factorization of $f(\boldsymbol{t})$ over $\boldsymbol{K}$ be given by (46). Since the fixed divisor of $f(\boldsymbol{t})$ equals $C(f)$ the condition (19) is satisfied in virtue of Lemma 9. By Lemma 6 the equation

$$F(X(\boldsymbol{t}), Y(\boldsymbol{t})) = f(\boldsymbol{t}) \tag{57}$$

has only finitely many solutions in polynomials $X(\mathbf{t}), Y(\mathbf{t}) \in \mathbf{Q}[\mathbf{t}]$ that are linearly independent. Let M be a positive integer such that MX, $MY \in \mathbf{Z}[\mathbf{t}]$ for all of them. We apply Lemma 5 to the sequence $\{\varphi_\nu\}$ with this M. Let μ, τ be any parameters with the property asserted in that lemma and let $\psi_\nu(\mathbf{t}) = \varphi_\nu(\mu\mathbf{t}+\tau)$. We have again the formulae (47) and (48).

We shall deduce from H the existence of polynomials $x(\mathbf{t}), y(\mathbf{t}) \in \mathbf{Z}[\mathbf{t}]$ such that $F(x(\mathbf{t}), y(\mathbf{t})) = f(\mu\mathbf{t}+\tau)$. This suffices to prove the theorem. Indeed the polynomials

$$X(\mathbf{t}) = x\left(\frac{\mathbf{t}-\tau}{\mu}\right), \quad Y(\mathbf{t}) = y\left(\frac{\mathbf{t}-\tau}{\mu}\right)$$

satisfy (57) and on one hand

$$\mu^{|x|}X,\ \mu^{|y|}Y \in \mathbf{Z}[\mathbf{t}],$$

on the other hand if X, Y are linearly independent we have by the choice of M

$$MX,\ MY \in \mathbf{Z}[\mathbf{t}].$$

Since $(\mu, M) = 1$ we get $X, Y \in \mathbf{Z}[\mathbf{t}]$.

If X, Y are linearly dependent, then $F(X(\mathbf{t}), Y(\mathbf{t})) = f(\mathbf{t}) = C_0(f)f_0(\mathbf{t})^3$, $C(f_0) = 1$ and

$$X(\mathbf{t}) = \xi\zeta^{-1}f_0(\mathbf{t}), \quad Y(\mathbf{t}) = \eta\zeta^{-1}f_0(\mathbf{t}), \quad \xi, \eta, \zeta \in \mathbf{Z},\ (\xi, \eta, \zeta) = 1;$$
$$F(\xi, \eta) = C(f)\zeta^3, \quad \zeta \mid \mu^{|f_0|}.$$

If the above holds for all pairs $\langle\mu_i, \tau_i\rangle$ of the sequence mentioned in the last assertion of Lemma 5 then using the obvious notation we infer from $(\mu_i, \mu_h) = 1$ that either $|\zeta_i| \neq |\zeta_h|$ for $i \neq h$ or there exists an i with $|\zeta_i| = 1$. In the former case since $|\zeta_i| \leqslant \mu_i^{|f_0|}$ the number of distinct $|\zeta_i| \leqslant Z$ is $\Omega\left(\frac{Z^{1/|f_0|n}}{\log Z}\right)$, which contradicts Lemma 7. Therefore, the latter case holds and $X_i, Y_i \in \mathbf{Z}[\mathbf{t}]$.

In order to deduce the existence of $x(\mathbf{t}), y(\mathbf{t})$ we shall consider successively the cases $\Delta = 1$, $\Delta < 0$, $\Delta > 1$.

If $\Delta = 1$ by (47), (48) and Lemma 5 H implies the existence for every $\mathbf{t}_1 \in \mathbf{Z}^r$ and every m prime to $f(\mu\mathbf{t}_1+\tau)$ of a $\mathbf{t}_2 \equiv \mathbf{t}_1 \bmod m$ such that $\frac{|\psi_\nu(\mathbf{t}_2)|}{C(\psi_\nu)}$ are distinct primes not dividing B $(1 \leqslant \nu \leqslant n)$.

On the other hand since a unimodular transformation of G does not affect the condition (56) we can assume $G(x, y) = xy$.

By the assumption of C there exist integers x, y such that

$$F(x, y) = f(\mu\mathbf{t}_2+\tau)$$

and it follows from (47), (48), (54) and (55) that for suitable integers c_i

and nonnegative integers $a_{i\nu}$ $(0 \leqslant i \leqslant 2,\ 1 \leqslant \nu \leqslant n)$

$$a_ix+b_iy = c_i\prod_{\nu=1}^{n}\left(\frac{\psi_\nu(\mathbf{t}_2)}{C(\psi_\nu)}\right)^{a_{i\nu}}, \tag{58}$$

$$c_0c_1c_2 = B\operatorname{sgn} l, \quad a_{0\nu}+a_{1\nu}+a_{2\nu} = e_\nu. \tag{59}$$

The set S of systems $[\{c_i\}, \{a_{i\nu}\}]$ satisfying (59) is finite. It follows from (58) that

$$\prod_{s\in S} D_s(\mathbf{t}_2) = 0, \tag{60}$$

where for $s = [\{c_i\}, \{a_{i\nu}\}]$:

$$D_s(\mathbf{t}) = \det[a_i, b_i, \Psi_{is}(\mathbf{t})]_{0\leqslant i\leqslant 2}, \quad \Psi_{is}(\mathbf{t}) = c_i\prod_{\nu=1}^{n}\left(\frac{\psi_\nu(\mathbf{t})}{C(\psi_\nu)}\right)^{a_{i\nu}}.$$

Since $\Psi_{is}(\mathbf{t}_2) \equiv \Psi_{is}(\mathbf{t}_1) \bmod m$, $D_s(\mathbf{t}_2) \equiv D_s(\mathbf{t}_1) \bmod m$ and (60) gives

$$\prod_{s\in S} D_s(\mathbf{t}_1) \equiv 0 \bmod m.$$

The latter congruence holds for all m prime to $f(\mu\mathbf{t}_1+\tau)$, hence

$$f(\mu\mathbf{t}_1+\tau)\prod_{s\in S} D_s(\mathbf{t}_1) = 0$$

and since $\mathbf{t}_1$ is an arbitrary integral vector

$$f(\mu\mathbf{t}+\tau)\prod_{s\in S} D_s(\mathbf{t}) = 0$$

identically. However $f(\mu\mathbf{t}+\tau) \neq 0$, thus there exists an $s \in S$ such that

$$D_s(\mathbf{t}) = 0.$$

By (56) the rank of the matrix $[a_i, b_i]_{0\leqslant i\leqslant 2}$ is two, thus the system of equations

$$a_ix+b_iy = \Psi_{is}(\mathbf{t}) \quad (0 \leqslant i \leqslant 2)$$

is soluble in polynomials $x, y \in \mathbf{Q}[\mathbf{t}]$.

Moreover, by Cramer's formulae

$$\begin{vmatrix} a_i & b_i \\ a_j & b_j \end{vmatrix} x,\ \begin{vmatrix} a_i & b_i \\ a_j & b_j \end{vmatrix} y \in \mathbf{Z}[\mathbf{t}] \quad (0 \leqslant i \leqslant j \leqslant 2)$$

and again by (56) $x, y \in \mathbf{Z}[\mathbf{t}]$. On the other hand by (59), (48) and (47)

$$F(x, y) = \prod_{i=0}^{2}(a_ix+b_iy) = \prod_{i=0}^{2} c_i\prod_{\nu=1}^{n}\left(\frac{\psi_\nu(\mathbf{t})}{C(\psi_\nu)}\right)^{a_{i\nu}} = B\operatorname{sgn} l\prod_{\nu=1}^{n}\left(\frac{\psi_\nu(\mathbf{t})}{C(\psi_\nu)}\right)^{e_\nu}$$
$$= l\prod_{\nu=1}^{n}\psi_\nu(\mathbf{t})^{e_\nu} = f(\mu\mathbf{t}+\tau).$$

Let us consider now the case $\Delta \neq 1$. Then by Lemma 5 and (47), (48) H implies the existence for every $\boldsymbol{t}_1 \in \boldsymbol{Z}^r$ and every m prime to $\Delta f(\mu \boldsymbol{t}_1 + \boldsymbol{\tau})$ of a $\boldsymbol{t}_2 \equiv \boldsymbol{t}_1 \bmod m$ such that the ideals $\frac{(\psi_\nu(\boldsymbol{t}_2))}{C(\psi_\nu)}$ $(\nu \leqslant n)$ are prime in $\boldsymbol{K}$, distinct and do not divide B. By the assumption of C there exist integers x, y such that

$$F(x, y) = f(\mu \boldsymbol{t}_2 + \boldsymbol{\tau})$$

and it follows from (47), (48), (51) and (55) that for suitable integral ideals $\mathfrak{a}, \mathfrak{b}$ and nonnegative integers α_ν, β_ν $(1 \leqslant \nu \leqslant n)$

$$(a_0 x + b_0 y) = \mathfrak{a} \prod_{\nu=1}^{n} \left(\frac{(\psi_\nu(\boldsymbol{t}_2))}{C(\psi_\nu)}\right)^{\alpha_\nu},$$

(61) $$\left(e(a_1 x + b_1 y) + \frac{g+\sqrt{\Delta}}{2}(a_2 x + b_2 y)\right)\mathfrak{g}^{-1} = \mathfrak{b} \prod_{\nu=1}^{n} \left(\frac{\psi_\nu(\boldsymbol{t}_2)}{C(\psi_\nu)}\right)^{\beta_\nu},$$

where $\mathfrak{g} = \left(e, \frac{g+\sqrt{\Delta}}{2}\right)$,

(62) $$\mathfrak{a} N \mathfrak{b} = (B), \quad \alpha_\nu + \beta_\nu + \beta_{\nu'} = c_\nu \quad (1 \leqslant \nu \leqslant n).$$

We get

$$a_0 x + b_0 y = \alpha \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t}_2)^{\alpha_\nu},$$

(63) $$e(a_1 x + b_1 y) + \frac{g+\sqrt{\Delta}}{2}(a_2 x + b_2 y) = \beta \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t}_2)^{\beta_\nu},$$

where

(64) $$(\alpha) = \mathfrak{a} \prod_{\nu=1}^{n} C(\psi_\nu)^{-\alpha_\nu}, \quad (\beta) = \mathfrak{g}\mathfrak{b} \prod_{\nu=1}^{n} C(\psi_\nu)^{-\beta_\nu}$$

and by (47) and (62)

(65) $$\alpha N \beta = le.$$

Since $\mathfrak{a}$ is integral $\Psi_0(\boldsymbol{t}; \alpha, \alpha_\nu) = \alpha \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t})^{\alpha_\nu}$ has integral coefficients. On the other hand, by (51) and (62) $\alpha_\nu = \alpha_{\nu'}$ $(k < \nu \leqslant n)$ and by (65) $\alpha \in \boldsymbol{Q}$, hence

$$\Psi_0(\boldsymbol{t}; \alpha, \alpha_\nu) \in \boldsymbol{Z}[\boldsymbol{t}].$$

Similarly, since $\mathfrak{b}$ is integral $\beta \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t})^{\beta_\nu} \in \mathfrak{g}[\boldsymbol{t}]$ and we get

(66) $$\beta \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t})^{\beta_\nu} = e\Psi_1(\boldsymbol{t}; \beta, \beta_\nu) + \frac{g+\sqrt{\Delta}}{2}\Psi_2(\boldsymbol{t}; \beta, \beta_\nu),$$

where

$$\Psi_i(\boldsymbol{t}; \beta, \beta_\nu) \in \boldsymbol{Z}[\boldsymbol{t}] \quad (i = 1, 2).$$

The equations (63) take the form

(67) $$a_0 x + b_0 y = \Psi_0(\boldsymbol{t}_2; \alpha, \alpha_\nu),$$
$$a_i x + b_i y = \Psi_i(\boldsymbol{t}_2; \beta, \beta_\nu) \quad (i = 1, 2).$$

For a system $s = [\alpha, \beta, \{\alpha_\nu\}, \{\beta_\nu\}]$ put

$$\Psi_{0s}(\boldsymbol{t}) = \Psi_0(\boldsymbol{t}; \alpha, \alpha_\nu), \quad \Psi_{is}(\boldsymbol{t}) = \Psi_i(\boldsymbol{t}; \beta, \beta_\nu) \quad (i = 1, 2)$$

and denote by S the set of all such systems satisfying (62) and (64). If $\Delta < 0$ the set S is finite. It follows from (67) that

(68) $$\prod_{s \in S} D_s(\boldsymbol{t}_2) = 0,$$

where

$$D_s(\boldsymbol{t}) = \det[a_i, b_i, \Psi_{is}(\boldsymbol{t})]_{0 \leqslant i \leqslant 2}.$$

Since $\Psi_{is}(\boldsymbol{t}_2) \equiv \Psi_{is}(\boldsymbol{t}_1) \bmod m$ we infer from (68) as in the case $\Delta = 1$ from (60) that for a suitable $s \in S$ the system of equations

$$a_i x + b_i y = \Psi_{is}(\boldsymbol{t}) \quad (0 \leqslant i \leqslant 2)$$

is soluble in polynomials $x, y \in \boldsymbol{Z}[\boldsymbol{t}]$. By (54), (55), (66), (47), (65) and (51) we get

$$F(x, y) = (a_0 x + b_0 y) N\left(e(a_1 x + b_1 y) + \frac{g+\sqrt{\Delta}}{2}(a_2 x + b_2 y)\right) e^{-1}$$
$$= \Psi_{0s}(\boldsymbol{t}) N\left(e\Psi_{1s}(\boldsymbol{t}) + \frac{g+\sqrt{\Delta}}{2}\Psi_{2s}(\boldsymbol{t})\right) e^{-1}$$
$$= \alpha \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t})^{\alpha_\nu} N\left(\beta \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t})^{\beta_\nu}\right) e^{-1}$$
$$= \alpha N \beta e^{-1} \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t})^{\alpha_\nu + \beta_\nu + \beta_{\nu'}} = l \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t})^{c_\nu} = f(\mu \boldsymbol{t} + \boldsymbol{\tau}).$$

If $\Delta > 0$ the set S is infinite. We can however divide it into finitely many classes assigning two systems $[\alpha, \beta, \{\alpha_\nu\}, \{\beta_\nu\}]$ and $[\alpha, \gamma, \{\alpha_\nu\}, \{\beta_\nu\}]$ to the same class if γ/β is a totally positive unit of $\boldsymbol{K}$. Then every class contains exactly one system satisfying

(69) $$1 \leqslant |\beta| < \varepsilon,$$

where $\varepsilon > 1$ is the fundamental totally positive unit. Denoting the set of all systems satisfying (62), (64) and (68) by S_0 we infer from (67) the existence of a $\sigma \in \boldsymbol{Z}$ such that

$$\prod_{s \in S_0} D_{\sigma s}(\boldsymbol{t}_2) = 0,$$

where for $s = [\alpha, \beta, \{\alpha_\nu\}, \{\beta_\nu\}]$

$$D_{\sigma s}(\boldsymbol{t}) = \begin{vmatrix} a_0 & b_0 & \Psi_0(\boldsymbol{t}; \alpha, \alpha_\nu) \\ a_1 & b_1 & \Psi_1(\boldsymbol{t}; \varepsilon^\sigma \beta, \beta_\nu) \\ a_2 & b_2 & \Psi_2(\boldsymbol{t}; \varepsilon^\sigma \beta, \beta_\nu) \end{vmatrix}.$$

Since $D_{\sigma s}(\boldsymbol{t}_2) \equiv D_{\sigma s}(\boldsymbol{t}_1) \bmod m$ for all s we conclude that

$$\prod_{s \in S_0} D_{\sigma s}(\boldsymbol{t}_1) \equiv 0 \bmod m \tag{70}$$

where σ depends on m.

We have an identity

$$u\left(e\Psi_{1s}(\boldsymbol{t}) + \frac{g+\sqrt{\Delta}}{2}\Psi_{2s}(\boldsymbol{t})\right) = e\Phi_{1s}(\boldsymbol{t}, u) + \frac{g+\sqrt{\Delta}}{2}\Phi_{2s}(\boldsymbol{t}, u), \tag{71}$$

where

$$\Phi_{1s}(\boldsymbol{t}, u) = \frac{1}{2}\left[u\left(1 - \frac{g}{\sqrt{\Delta}}\right) + u^{-1}\left(1 + \frac{g}{\sqrt{\Delta}}\right)\right]\Psi_{1s}(\boldsymbol{t}) - h\frac{u-u^{-1}}{\sqrt{\Delta}}\Psi_{2s}(\boldsymbol{t}),$$

$$\Phi_{2s}(\boldsymbol{t}, u) = e\frac{u-u^{-1}}{\sqrt{\Delta}}\Psi_{1s}(\boldsymbol{t}) + \frac{1}{2}\left[u\left(1 - \frac{g}{\sqrt{\Delta}}\right) + u^{-1}\left(1 + \frac{g}{\sqrt{\Delta}}\right)\right]\Psi_{2s}(\boldsymbol{t}) + g\frac{u-u^{-1}}{\sqrt{\Delta}}\Psi_{2s}(\boldsymbol{t}).$$

Since ε is conjugate to ε^{-1}

$$\Phi_{is}(\boldsymbol{t}, \varepsilon^\sigma) \in \boldsymbol{Q}[\boldsymbol{t}] \quad (i = 1, 2)$$

and by (71)

$$\Psi_i(\boldsymbol{t}; \varepsilon^\sigma \beta, \beta_\nu) = \Phi_{is}(\boldsymbol{t}, \varepsilon^\sigma) \quad (i = 1, 2).$$

The congruence (70) takes the form

$$\prod_{s \in S_0} E_s(\boldsymbol{t}_1, \varepsilon^\sigma) \equiv 0 \bmod m, \tag{72}$$

where

$$E_s(\boldsymbol{t}, u) = \begin{vmatrix} a_0 & b_0 & \Psi_{0s}(\boldsymbol{t}) \\ a_1 & b_1 & \Phi_{1s}(\boldsymbol{t}, u) \\ a_2 & b_2 & \Phi_{2s}(\boldsymbol{t}, u) \end{vmatrix}. \tag{73}$$

However $uE(\boldsymbol{t}, u) \in \boldsymbol{Q}[\boldsymbol{t}, u]$ and hence $u^{|S_0|}\prod_{s \in S_0} E(\boldsymbol{t}_1, u) \in \boldsymbol{Q}[u]$.

Since the congruence (72) is soluble for all m prime to $\Delta f(\mu \boldsymbol{t}_1 + \boldsymbol{\tau})$ it follows from Theorem 6 of [15] that the equation

$$f(\mu \boldsymbol{t}_1 + \boldsymbol{\tau}) \prod_{s \in S_0} E_s(\boldsymbol{t}_1, \varepsilon^\sigma) = 0$$

is soluble in integers σ. Thus for every $\boldsymbol{t}_1 \in \boldsymbol{Z}^r$ either $f(\mu \boldsymbol{t}_1 + \boldsymbol{\tau}) = 0$ or $f(\mu \boldsymbol{t}_1 + \boldsymbol{\tau}) \neq 0$ and there exist a $\sigma \in \boldsymbol{Z}$ and an $s = [\alpha, \beta, \{\alpha_\nu\}, \{\beta_\nu\}] \in S_0$ such that $E_s(\boldsymbol{t}_1, \varepsilon^\sigma) = 0$.

In the latter case it follows from (71) and (73) that

$$\begin{vmatrix} a_0 & b_0 & \Psi_{0s}(\boldsymbol{t}_1) \\ ea_1 + \frac{g+\sqrt{\Delta}}{2}a_2 & eb_1 + \frac{g+\sqrt{\Delta}}{2}b_2 & \varepsilon^\sigma \beta \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t}_1)^{\beta_\nu} \\ ea_1 + \frac{g-\sqrt{\Delta}}{2}a_2 & eb_1 + \frac{g-\sqrt{\Delta}}{2}b_2 & \varepsilon^{-\sigma}\beta' \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t}_1)^{\beta_{\nu'}} \end{vmatrix} = -e\sqrt{\Delta}E_s(\boldsymbol{t}_1, \varepsilon^\sigma) = 0$$

and $\varepsilon^\sigma \beta \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t}_1)^{\beta_\nu}$ satisfies the quadratic equation

$$Lz^2 - K\Psi_{0s}(\boldsymbol{t}_1)z - L'N\beta \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t}_1)^{\beta_\nu + \beta_{\nu'}} = 0,$$

where β', L' are conjugate to β, L respectively

$$L = \begin{vmatrix} a_0 & b_0 \\ ea_1 + \frac{g-\sqrt{\Delta}}{2}a_2 & eb_1 + \frac{g-\sqrt{\Delta}}{2}b_2 \end{vmatrix},$$

$$K = \begin{vmatrix} ea_1 + \frac{g+\sqrt{\Delta}}{2}a_2 & eb_1 + \frac{g+\sqrt{\Delta}}{2}b_2 \\ ea_1 + \frac{g-\sqrt{\Delta}}{2}a_2 & eb_1 + \frac{g-\sqrt{\Delta}}{2}b_2 \end{vmatrix}. \tag{74}$$

Since $e[a_0, b_0] \neq 0$ we have $L \neq 0$ by (56), and

$$\left\lceil \varepsilon^\sigma \beta \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t}_1)^{\beta_\nu} \right\rceil \ll \|\boldsymbol{t}_1\|^{|f|} \tag{75}$$

where $\lceil\;\rceil$ denotes the maximum modulus of the conjugates and the constant in the symbol $\ll$ depends on F, f, μ, τ, s.

On the other hand, by (47), (51), (62), (65) and (69)

$$\left\lceil \beta \prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t}_1)^{\beta_\nu} \right\rceil \ll \|\boldsymbol{t}_1\|^{|f|/2}.$$

Since $f(\mu t_1+\tau) \neq 0$ whence by (64)

$$\left|N\left(\beta\prod_{\nu=1}^{n}\varphi_\nu(t_1)^{\beta_\nu}\right)\right| \geqslant N\mathfrak{g}\mathfrak{b} \geqslant 1$$

we get

$$\left|\overline{\beta^{-1}\prod_{\nu=1}^{n}\varphi_\nu(t_1)^{-\beta_\nu}}\right| < \|t_1\|^{|f|/2}.$$

This together with (75) implies

$$\varepsilon^{|\sigma|} = \left|\overline{\varepsilon^{\sigma}}\right| \leqslant \|t_1\|^{\frac{3}{2}|f|}, \qquad |\sigma| \leqslant \frac{3}{2}|f|\frac{\log\|t_1\|}{\log\varepsilon}+\varrho,$$

where ϱ is a constant depending on F, f, μ, τ but independent of s (S_0 is finite).

Let us choose now a positive integer T so large that

$$2T+1 > |f|(|S_0|+1)\left(3|f|\frac{\log T}{\log\varepsilon}+2\varrho+1\right). \tag{76}$$

If t_1 runs through all integral vectors satisfying $\|t_1\| \leqslant T$ σ runs through integers satisfying

$$|\sigma| \leqslant \frac{3}{2}|f|\frac{\log T}{\log\varepsilon}+\varrho.$$

The number of vectors in question is $(2T+1)^r$, the number of integers does not exceed $3|f|\dfrac{\log T}{\log\varepsilon}+2\varrho+1$, hence there is an integer σ_0 that corresponds to at least

$$(2T+1)^r\left(3|f|\frac{\log T}{\log\varepsilon}+2\varrho+1\right)^{-1}$$

different vectors t_1 satisfying $\|t_1\| \leqslant T$. By (76) we get more than $|f|(|S_0|+1)\times\times(2T+1)^{r-1}$ such vectors satisfying the equation

$$f(\mu t_1+\tau)\prod_{s\in S_0}E_s(t_1, \varepsilon^{\sigma_0}) = 0.$$

Since by (62), (71) and (73) the degree of $E_s(t, \varepsilon^{\sigma_0})$ does not exceed $|f|$ the degree of the polynomial on the left-hand side does not exceed $|f|(|S_0|+1)$ and Lemma 8 shows that

$$f(\mu t+\tau)\prod_{s\in S_0}E_s(t, \varepsilon^{\sigma_0}) = 0$$

identically. Therefore, there exists an $s \in S_0$ such that $E_s(t, \varepsilon^{\sigma_0}) = 0$

and by (56) the system of equations

$$a_0x+b_0y = \Psi_{0s}(t),$$
$$a_ix+b_iy = \Phi_{is}(t) \qquad (i = 1, 2)$$

is soluble in polynomials $x, y \in \mathbf{Z}[t]$. By (54), (55), (71), (66), (47), (62), (65) and (51) we get for these polynomials

$$F(x, y) = (a_0x+b_0y)N\left(e(a_1x+b_1y)+\frac{g+\sqrt{\Delta}}{2}(a_2x+b_2y)\right)e^{-1}$$
$$= \Psi_{0s}(t)N\left(\varepsilon^{-\sigma_0}e(a_1x+b_1y)+\varepsilon^{-\sigma_0}\frac{g+\sqrt{\Delta}}{2}(a_2x+b_2y)\right)e^{-1}$$
$$= \Psi_{0s}(t)N\left(e\Psi_{1s}(t)+\frac{g+\sqrt{\Delta}}{2}\Psi_{2s}(t)\right)e^{-1} = f(\mu t+\tau)$$

and the proof is complete.

Remark. For the proof of a more general result mentioned in the introduction one needs more general versions of Lemmata 2, 5 and 7 and Theorem 7 of [16] instead of Theorem 6 of [15]. In the difficult case of an irreducible form F with all zeros real Theorem 7 of [16] does not suffice, but Skolem's conjecture on exponential congruences would do (see [18]). One could avoid this step in the proof provided it were known that the number of vectors t satisfying $\|t\| \leqslant T$ and the conditions of Lemma 4 grows faster than $T^{r-1}(\log T)^{|F|}$. For $r = 1$ much more has been conjectured by Bateman and Horn [1].

4. The next lemma is a refinement of Lemma 1 of [13].

LEMMA 10. *Let $P \in \mathbf{Q}[t, u]$ be a polynomial such that for no $\varphi \in \mathbf{Q}(t)$*

$$P(t, \varphi(t)) = 0$$

identically. Then there exists a $t_1 \in \mathbf{Z}^r$ such that for any $M \in \mathbf{N}$ there exists an $m \in \mathbf{N}$ prime to M such that for all $t \in \mathbf{Z}^r$, $t \equiv t_1 \bmod m$ and all $u \in \mathbf{Q}$

$$P(t, u) \neq 0.$$

Proof. Following the proof of Lemma 1 in [13] we take $m = q_1 \ldots q_k$, where in the notation of that paper the primes q_i are chosen not to divide M.

LEMMA 11. *Let $G, H \in \mathbf{Q}[x, y]$ be relatively prime forms, $p, g_i, h_i \in \mathbf{Q}[t]$ $(i \leqslant I)$ arbitrary polynomials, $p \neq 0$.*

If for every $t_1 \in \mathbf{Z}^r$ and for every integer m prime to $p(t)$ there are an $i \leqslant I$, a $t_2 \in \mathbf{Z}^r$, $t_2 \equiv t_1 \bmod m$ and $x, y \in \mathbf{Q}$ satisfying

$$G(x, y) = g_i(t_2), \qquad H(x, y) = h_i(t_2) \tag{77}$$

then there exist a $j \leqslant I$ and polynomials $X, Y \in \mathbf{Q}[t]$ such that

$$G(X, Y) = g_j, \qquad H(X, Y) = h_j.$$

Proof. If $G(x,y)-g_i(\boldsymbol{t})$, $H(x,y)-h_i(\boldsymbol{t})$ had a common factor $d(x,y,\boldsymbol{t})\neq$ const then the leading forms of d with respect to x, y would divide $G(x,y)$ and $H(x,y)$. Thus for each $i\leqslant I$

$$\big(G(x,y)-g_i(\boldsymbol{t}),\, H(x,y)-h_i(\boldsymbol{t})\big)=1.$$

Let $R_i(\boldsymbol{t},x)$, $S_i(\boldsymbol{t},y)$ be the resultants of $G(x,y)-g_i(\boldsymbol{t})$ and $H(x,y)-h_i(\boldsymbol{t})$ with respect to y and x respectively. It follows from the construction of resultants that the leading coefficients of R_i in x and of S_i in y are equal to the resultants of $G(1,z), H(1,z)$ and of $G(z,1), H(z,1)$ respectively. Hence these leading coefficients are independent of $\boldsymbol{t}$. Let

$$R_i(\boldsymbol{t},x)=R_{i0}(\boldsymbol{t},x)\prod_{\varrho=1}^{r_i}\big(x-R_{i\varrho}(\boldsymbol{t})\big), \tag{78}$$

$$S_i(\boldsymbol{t},y)=S_{i0}(\boldsymbol{t},y)\prod_{\sigma=1}^{s_i}\big(y-S_{i\sigma}(\boldsymbol{t})\big), \tag{79}$$

where R_{i0} and S_{i0} have no factor linear in x or y respectively. If for some triple (i,ϱ,σ) with $i\leqslant I$, $1\leqslant\varrho\leqslant r_i$, $1\leqslant\sigma\leqslant s_j$

$$G(R_{i\varrho},S_{i\sigma})=g_i\quad\text{and}\quad H(R_{i\varrho},S_{i\sigma})=h_i$$

the lemma follows.

Therefore, suppose that for each triple (i,ϱ,σ) in question

$$G(R_{i\varrho},S_{i\sigma})\neq g_i\quad\text{or}\quad H(R_{i\varrho},S_{i\sigma})\neq h_i.$$

Then

$$T_{i\varrho\sigma}=\big(G(R_{i\sigma},S_{i\sigma})-g_i\big)^2+\big(H(R_{i\varrho},S_{i\sigma})-h_i\big)^2\neq 0 \tag{80}$$

and we set in Lemma 10

$$P(\boldsymbol{t},u)=p(\boldsymbol{t})\prod_{i=1}^{I}R_{i0}(\boldsymbol{t},u)S_{i0}(\boldsymbol{t},u)\prod_{\varrho=1}^{r_i}\prod_{\sigma=1}^{s_i}T_{i\varrho\sigma}(\boldsymbol{t}). \tag{81}$$

By that lemma with $M=1$ there exist an $m\in\boldsymbol{N}$ and a $\boldsymbol{t}_1\in\boldsymbol{Z}^r$ such that if $\boldsymbol{t}\equiv\boldsymbol{t}_1\bmod m$ and $u\in\boldsymbol{Q}$ we have

$$P(\boldsymbol{t},u)\neq 0. \tag{82}$$

In particular, taking $\boldsymbol{t}=\boldsymbol{t}_1$ we get $p(\boldsymbol{t}_1)\neq 0$. Applying Lemma 10 again with $M=p(\boldsymbol{t}_1)$ we infer the existence of an integer m with the above property satisfying $\big(m,p(\boldsymbol{t}_1)\big)=1$. However now by the assumption there exists an $i\leqslant I$, a $\boldsymbol{t}_2\equiv\boldsymbol{t}_1\bmod m$ and $x,y\in\boldsymbol{Q}$ such that (77) holds. By the fundamental property of resultants we have

$$R_i(\boldsymbol{t},x)=0=S_i(\boldsymbol{t},y)$$

and in view of (78), (79), (81) and (82) there exist ϱ,σ such that $1\leqslant\varrho\leqslant r_i$, $1\leqslant\sigma\leqslant s_i$

$$x=R_{i\varrho}(\boldsymbol{t}_2),\qquad y=S_{i\sigma}(\boldsymbol{t}_2).$$

It follows from (77) and (80) that

$$T_{i\varrho\sigma}(\boldsymbol{t}_2)=0,$$

contrary to (81) and (82).

Remark. Lemma 11 extends to any system of forms $G_1, G_2, \ldots, G_k\in\boldsymbol{Q}[x_1,\ldots,x_k]$ without a common non-trivial zero.

Proof of Theorem 3. If $f=0$ the theorem is trivially true. If $f\neq 0$ let $f(\boldsymbol{t}_0)=e\neq 0$. We set $f_0(\boldsymbol{t})=f(e\boldsymbol{t}+\boldsymbol{t}_0)$ and find as in the proof of Corollary to Lemma 3 that the fixed divisor of $f_0(\boldsymbol{t})$ equals $C(f_0)$. (If the fixed divisor of f equals $C(f)$ we can take directly $e=1$, $\boldsymbol{t}_0=\boldsymbol{0}$.) Let $\boldsymbol{K}$ be the least field over which F factorizes into two coprime factors and let

$$f_0(\boldsymbol{t})=l\prod_{\nu=1}^{n}\varphi_\nu(\boldsymbol{t})^{e_\nu} \tag{83}$$

be a factorization of f over $\boldsymbol{K}$ into irreducible factors such that φ_ν are distinct and have the coefficient of the first term in the antilexicographic order equal to 1. Since the fixed divisor of $f_0(\boldsymbol{t})$ equals $C(f_0)$ the polynomials φ_ν satisfy (19) in virtue of Lemma 9. Let $\mu,\boldsymbol{\tau}$ be parameters whose existence for $\{\varphi_\nu\}$ and $\mu=1$ is asserted in Lemma 5 and let

$$\psi_\nu=\varphi_\nu(\mu\boldsymbol{t}+\boldsymbol{\tau})\qquad(1\leqslant\nu\leqslant n).$$

It follows that

$$f_0(\mu\boldsymbol{t}+\boldsymbol{\tau})=l\prod_{\nu=1}^{n}\psi_\nu(\boldsymbol{t})^{e_\nu} \tag{84}$$

and

$$B=|l|\prod_{\nu=1}^{n}C(\psi_\nu)^{e_\nu}=C\big(f_0(\mu\boldsymbol{t}+\boldsymbol{\tau})\big)\in\boldsymbol{N}, \tag{85}$$

where an ideal in $\boldsymbol{Q}$ is identified with its positive generator. Consider first the case where $\boldsymbol{K}=\boldsymbol{Q}$ and let

$$f_0(\mu\boldsymbol{t}+\boldsymbol{\tau})=g_i(\boldsymbol{t})h_i(\boldsymbol{t})\qquad(1\leqslant i\leqslant I) \tag{86}$$

be all possible factorizations of the left-hand side into two factors with integral coefficients. H implies that if $\big(m,f_0(\mu\boldsymbol{t}_1+\boldsymbol{\tau})\big)=1$ there exist an $i\leqslant I$, a $\boldsymbol{t}_2\equiv\boldsymbol{t}_1\bmod m$ and $x,y\in\boldsymbol{Z}$ such that

$$G(x,y)=g_i(\boldsymbol{t}_2),\qquad H(x,y)=h_i(\boldsymbol{t}_2). \tag{87}$$

Indeed, by (84) and (85) the condition $\big(m,f_0(\mu\boldsymbol{t}_1+\boldsymbol{\tau})\big)=1$ implies

$$\Big(m,\prod_{\nu=1}^{n}\frac{\psi_\nu(\boldsymbol{t}_1)}{C(\psi_\nu)}\Big)=1$$

and by Lemma 5 H implies the existence of a $\boldsymbol{t}_2 \in \boldsymbol{Z}^r$, $\boldsymbol{t}_2 \equiv \boldsymbol{t}_1 \bmod m$ such that $\frac{|\psi_\nu(\boldsymbol{t}_2)|}{C(\psi_\nu)}$ $(\nu \leqslant n)$ are distinct primes not dividing B. By the assumption of D there exist $x, y \in \boldsymbol{Z}$ such that

$$G(x, y)H(x, y) = F(x, y) = f_0(\mu \boldsymbol{t}_2 + \tau)$$

and it follows from (84) and (85) that for some $a, b, a_\nu, \beta_\nu \in \boldsymbol{Z}$, $a_\nu \geqslant 0$, $\beta_\nu \geqslant 0$ we have

$$G(x, y) = a \prod_{\nu=1}^{n} \left(\frac{\psi_\nu(\boldsymbol{t}_2)}{C(\psi_\nu)}\right)^{a_\nu}, \quad H(x, y) = b \prod_{\nu=1}^{n} \left(\frac{\psi_\nu(\boldsymbol{t}_2)}{C(\psi_\nu)}\right)^{\beta_\nu},$$

$$ab = B \operatorname{sgn} l, \quad a_\nu + \beta_\nu = e_\nu \quad (1 \leqslant \nu \leqslant n).$$

Taking

$$g_i(t) = a \prod_{\nu=1}^{n} \left(\frac{\psi_\nu(\boldsymbol{t})}{C(\psi_\nu)}\right)^{a_\nu}, \quad h_i(t) = b \prod_{\nu=1}^{n} \left(\frac{\psi_\nu(\boldsymbol{t})}{C(\psi_\nu)}\right)^{\beta_\nu}$$

we get (86) and (87). Now we apply Lemma 11 with $p(\boldsymbol{t}) = f_0(\mu \boldsymbol{t} + \tau)$ and we get the existence of $X_0, Y_0 \in \boldsymbol{Q}[\boldsymbol{t}]$ satisfying

$$G(X_0, Y_0) = g_j, \quad H(X_0, Y_0) = h_j$$

for some $j \leqslant I$. Setting

$$(88) \qquad X(\boldsymbol{t}) = X_0\left(\frac{\boldsymbol{t} - e\tau - \boldsymbol{t}_0}{e\mu}\right), \quad Y(\boldsymbol{t}) = Y_0\left(\frac{\boldsymbol{t} - e\tau - \boldsymbol{t}_0}{e\mu}\right)$$

we get by (86)

$$F(X(\boldsymbol{t}), Y(\boldsymbol{t})) = g_j\left(\frac{\boldsymbol{t} - e\tau - \boldsymbol{t}_0}{e\mu}\right) h_j\left(\frac{\boldsymbol{t} - e\tau - \boldsymbol{t}_0}{e\mu}\right) = f_0\left(\frac{\boldsymbol{t} - \boldsymbol{t}_0}{e}\right) = f(\boldsymbol{t}).$$

Consider now the case where $\boldsymbol{K}$ is an imaginary quadratic field with discriminant Δ. Then

$$(89) \qquad F(x, y) = \frac{v}{w} N\Phi(x, y),$$

where $v, w \in \boldsymbol{Z}$, $(v, w) = 1$, $\Phi \in \boldsymbol{K}[x, y]$ has integral coefficients and

$$(90) \qquad (\Phi(x, y), \Phi'(x, y)) = 1,$$

where Φ' is conjugate to Φ over $\boldsymbol{Q}(x, y)$. Let

$$(91) \qquad \frac{w}{v} f_0(\mu \boldsymbol{t} + \tau) = \eta_i(\boldsymbol{t})\eta_i'(\boldsymbol{t}) \quad (i \leqslant I)$$

be all the factorizations of the left-hand side into two conjugate polynomials with integral coefficients in $\boldsymbol{K}$. Since $\boldsymbol{K}$ has finitely many units the number of such factorizations is finite. H implies that if $(m, \Delta f_0(\mu \boldsymbol{t}_1 + \tau)) = 1$ there exist an $i \leqslant I$, a $\boldsymbol{t}_2 \equiv \boldsymbol{t}_1 \bmod m$ and $x, y \in \boldsymbol{Z}$ such that

$$(92) \qquad \Phi(x, y) = \eta_i(\boldsymbol{t}_2).$$

Indeed, by (84) and (85) we have

$$(93) \qquad \left(\frac{w}{v} f_0(\mu \boldsymbol{t} + \tau)\right) = \left(\frac{w}{v} B\right) \prod_{\nu=1}^{n} \frac{(\psi_\nu(\boldsymbol{t}))^{e_\nu}}{C(\psi_\nu)^{e_\nu}}.$$

Since by Lemma 5 $\prod_{\nu=1}^{n} \frac{N\psi_\nu(\boldsymbol{t})}{NC(\psi_\nu)}$ has the fixed divisor 1, $\prod_{\nu=1}^{n} \psi_\nu(\boldsymbol{t})^{e_\nu}$ has the fixed divisor $\prod_{\nu=1}^{n} C(\psi_\nu)^{e_\nu}$. On the other hand, for every $\boldsymbol{t} \in \boldsymbol{Z}^r$

$$\frac{w}{v} f_0(\mu \boldsymbol{t} + \tau) = N\Phi(x, y) \in \boldsymbol{Z}$$

hence

$$(94) \qquad \frac{w}{v} A \in \boldsymbol{Z}.$$

By (84) and (85) the condition $(m, \Delta f_0(\mu \boldsymbol{t}_1 + \tau)) = 1$ implies

$$\left(m, \Delta \prod_{\nu=1}^{n} \frac{N\psi_\nu(\boldsymbol{t}_1)}{NC(\psi_\nu)}\right) = 1$$

and by Lemma 5 H implies the existence of a $\boldsymbol{t}_2 \equiv \boldsymbol{t}_1 \bmod m$ such that $\frac{(\psi_\nu(\boldsymbol{t}_2))}{C(\psi_\nu)}$ $(\nu \leqslant n)$ are distinct prime ideals not dividing wB. By the assumption of D there exist $x_0, y_0 \in \boldsymbol{Z}$ such that

$$(95) \qquad N\Phi(x_0, y_0) = \frac{w}{v} F(x_0, y_0) = \frac{w}{v} f(\mu \boldsymbol{t}_2 + \tau)$$

and it follows from (93) and (94) that for an integral ideal $\mathfrak{b}$ and some integers $a_\nu \geqslant 0$

$$(\Phi(x_0, y_0)) = \mathfrak{b} \prod_{\nu=1}^{n} \frac{(\psi_\nu(\boldsymbol{t}_2))^{a_\nu}}{C(\psi_\nu)^{a_\nu}}, \quad \left(\mathfrak{b}, \prod_{\nu=1}^{n} \frac{(\psi_\nu(\boldsymbol{t}_2))}{C(\psi_\nu)}\right) = 1.$$

On the other hand in full analogy with (51) we can assume that for a certain $k \equiv n \bmod 2$

$$(96) \quad \psi_\nu' = \psi_{\nu'}, \quad e_\nu = e_{\nu'}, \quad \nu' = \nu \ (\nu \leqslant k), \quad \nu' = \nu - (-1)^{n-\nu} \ (\nu > k).$$

Hence

$$N\Phi(x_0, y_0) = N\mathfrak{b} \prod_{\nu=1}^{n} \left(\frac{(\psi_\nu(\boldsymbol{t}_2))}{C(\psi_\nu)}\right)^{a_\nu + a_{\nu'}}, \quad \left(N\mathfrak{b}, \prod_{\nu=1}^{n} \frac{(\psi_\nu(\boldsymbol{t}_2))}{C(\psi_\nu)}\right) = 1$$

and a comparison with (93) gives

$$(97)\qquad \alpha_\nu + \alpha_{\nu'} = e_\nu \quad (1 \leqslant \nu \leqslant n).$$

Now let us put

$$(98)\qquad \eta(\boldsymbol{t}) = \Phi(x_0, y_0) \prod_{\nu=1}^{n} \left(\frac{\psi_\nu(\boldsymbol{t})}{\psi_\nu(\boldsymbol{t}_2)}\right)^{\alpha_\nu}.$$

The polynomial $\eta(\boldsymbol{t})$ has integral coefficients in $\boldsymbol{K}$ since

$$C(\eta) = \big(\Phi(x_0, y_0)\big) \prod_{\nu=1}^{n} \frac{C(\psi_\nu)^{\alpha_\nu}}{\big(\psi_\nu(\boldsymbol{t}_2)\big)^{\alpha_\nu}} = \mathfrak{b}.$$

Moreover, by (95), (96), (97) and (84)

$$\eta(\boldsymbol{t})\eta'(\boldsymbol{t}) = N\Phi(x_0, y_0) \prod_{\nu=1}^{n} \left(\frac{\psi_\nu(\boldsymbol{t})\psi'_\nu(\boldsymbol{t})}{\psi_\nu(\boldsymbol{t}_2)\psi'_\nu(\boldsymbol{t}_2)}\right)^{\alpha_\nu} = \frac{w}{v} f_0(\mu\boldsymbol{t}_2+\tau) \prod_{\nu=1}^{n} \left(\frac{\psi_\nu(\boldsymbol{t})}{\psi_\nu(\boldsymbol{t}_2)}\right)^{\alpha+\alpha_{\nu'}}$$

$$= \frac{w}{v} f_0(\mu\boldsymbol{t}_2+\tau) \prod_{\nu=1}^{n} \left(\frac{\psi_\nu(\boldsymbol{t})}{\psi_\nu(\boldsymbol{t}_2)}\right)^{e_\nu} = \frac{w}{v} f_0(\mu\boldsymbol{t}+\tau).$$

Hence $\eta(\boldsymbol{t}) = \eta_i(\boldsymbol{t})$ for an $i \leqslant I$ and (92) follows immediately from (98). Now we apply Lemma 11 with $p(\boldsymbol{t}) = \Delta f_0(\mu\boldsymbol{t}+\tau)$,

$$G(x, y) = \Phi(x, y) + \Phi'(x, y), \qquad H(x, y) = \big(\Phi(x, y) - \Phi'(x, y)\big)/\sqrt{\Delta}$$

and we get the existence of $X_0, Y_0 \in \boldsymbol{Q}[\boldsymbol{t}]$ satisfying

$$(99)\qquad \Phi(X_0, Y_0) = \eta_j, \qquad \Phi'(X_0, Y_0) = \eta'_j$$

for a $j \leqslant I$. Using again the transformation (88) we get by (89) and (90)

$$F\big(X(\boldsymbol{t}), Y(\boldsymbol{t})\big) = \frac{v}{w}\eta_j\left(\frac{\boldsymbol{t}-e\tau-\boldsymbol{t}_0}{e\mu}\right)\eta'_j\left(\frac{\boldsymbol{t}-e\tau-\boldsymbol{t}_0}{e\mu}\right) = \frac{v}{w} f_0\left(\frac{\boldsymbol{t}-\boldsymbol{t}_0}{e}\right) = f(\boldsymbol{t}).$$

LEMMA 12. *Let $k \in \boldsymbol{N}$ be odd, $a_i(\boldsymbol{t}) \in \boldsymbol{Z}[\boldsymbol{t}]$ $(0 \leqslant i \leqslant k)$, $a_0(\boldsymbol{t}) = 1$, $x(\boldsymbol{t}) \in \boldsymbol{Q}[\boldsymbol{t}]$. If*

$$(100)\qquad \sum_{i=0}^{k-1} \binom{k}{i+1} a_i(\boldsymbol{t}) x(\boldsymbol{t})^{k-1-i} = 0$$

then $x(\boldsymbol{t}) \in \boldsymbol{Z}[\boldsymbol{t}]$.

Proof. Suppose that $C(x) \notin \boldsymbol{Z}$. Then for some prime p

$$\operatorname{ord}_p C(x) = -c \leqslant -1.$$

The function $\operatorname{ord}_p C(P)$ is a valuation of the ring $\boldsymbol{Q}[\boldsymbol{t}]$ (see [6], p. 171). In virtue of the properties of valuations (100) implies

$$\operatorname{ord}_p\big(kC(x)^{k-1}\big) \geqslant \min_{0<i<k} \operatorname{ord}_p\left(\binom{k}{i+1} C(a_i) C(x)^{k-1-i}\right),$$

hence for a positive $i < k$

$$\operatorname{ord}_p k - (k-1)c \geqslant \operatorname{ord}_p \binom{k}{i+1} - (k-1-i)c$$

and

$$(101)\qquad \operatorname{ord}_p k \geqslant \operatorname{ord}_p \binom{k}{i+1} + i.$$

However

$$\binom{k}{i+1} = \frac{k}{i+1}\binom{k-1}{i}$$

thus (101) implies

$$\operatorname{ord}_p(i+1) \geqslant i, \qquad i+1 \geqslant p^i; \qquad p = 2,$$

which is impossible since then the left-hand side of (101) is 0.

Proof of Theorem 4. Let $n = 2^\alpha k$, k odd. In order to prove the first part of the theorem let us assume that the fixed divisor of f equals $C(f)$ and take in the proof of Theorem 3 $f_0 = f$. If $k > 1$ we take further $\boldsymbol{K} = \boldsymbol{Q}$, $\mu = 1$, $\tau = \boldsymbol{0}$,

$$G(x, y) = x^{2^\alpha} + y^{2^\alpha}, \qquad H(x, y) = \sum_{i+j=k-1} x^{2^\alpha i}(-y^{2^\alpha})^j$$

and we get from (86) and (88) that for some polynomials $g, h \in \boldsymbol{Z}[\boldsymbol{t}]$ and $X, Y \in \boldsymbol{Q}[\boldsymbol{t}]$

$$g(\boldsymbol{t})h(\boldsymbol{t}) = f(\boldsymbol{t}),$$

$$(102)\qquad G(X, Y) = g, \qquad H(X, Y) = h.$$

However

$$H(X, Y) = \sum_{i=0}^{k-1} \binom{k}{i+1} G(X, Y)^i (-X^{2^\alpha})^{k-1-i}$$

hence taking in Lemma 12

$$a_i(\boldsymbol{t}) = g(\boldsymbol{t})^i \quad (0 \leqslant i < k-1), \qquad a_{k-1}(\boldsymbol{t}) = -h(\boldsymbol{t}), \qquad x(\boldsymbol{t}) = -X(\boldsymbol{t})^{2^\alpha}$$

we get from (102) that

$$-X(\boldsymbol{t})^{2^\alpha} \in \boldsymbol{Z}[\boldsymbol{t}].$$

Thus $X(\boldsymbol{t}) \in \boldsymbol{Z}[\boldsymbol{t}]$ and by symmetry $Y(\boldsymbol{t}) \in \boldsymbol{Z}[\boldsymbol{t}]$. Moreover

$$X(\boldsymbol{t})^n + Y(\boldsymbol{t})^n = G(X, Y)H(X, Y) = f(\boldsymbol{t}).$$

If $k = 1$ we take in the proof of Theorem 3 $\boldsymbol{K} = \boldsymbol{Q}(\zeta_4)$,

$$(103)\qquad \Phi(x, y) = x^{2^{\alpha-1}} + \zeta_4 y^{2^{\alpha-1}}, \qquad v/w = 1,$$

where ζ_q is a primitive qth root of unity.

By Lemma 5 μ factorizes in $\boldsymbol{K}$ into prime ideals of degree 2. By (92) and (99) for some polynomials $\eta \in \boldsymbol{Z}[\zeta_4, \boldsymbol{t}]$ and $X_0, Y_0 \in \boldsymbol{Q}[\boldsymbol{t}]$

(104) $$\eta(\boldsymbol{t})\eta'(\boldsymbol{t}) = f(\mu\boldsymbol{t}+\tau), \quad \eta' \text{ conjugate to } \eta \text{ over } \boldsymbol{Q}(\boldsymbol{t}),$$

(105) $$\Phi\big(X_0(\boldsymbol{t}), Y_0(\boldsymbol{t})\big) = \eta(\boldsymbol{t}).$$

Let us set

(106) $$\vartheta(\boldsymbol{t}) = \eta\left(\frac{\boldsymbol{t}-\tau}{\mu}\right), \quad X(\boldsymbol{t}) = X_0\left(\frac{\boldsymbol{t}-\tau}{\mu}\right), \quad Y(\boldsymbol{t}) = Y_0\left(\frac{\boldsymbol{t}-\tau}{\mu}\right).$$

We have

$$\mu^{|\eta|}\vartheta(\boldsymbol{t}) \in \boldsymbol{Z}[\zeta_4, \boldsymbol{t}]$$

hence if $\mathfrak{p}$ is a prime ideal of $\boldsymbol{K}$ in the denominator of $C(\vartheta)$ $\mathfrak{p}|\mu$ and $\mathfrak{p}=\mathfrak{p}'$. However by (104)

$$\vartheta(\boldsymbol{t})\vartheta'(\boldsymbol{t}) = f(\boldsymbol{t}), \quad NC(\vartheta) = C(f) \in \boldsymbol{Z}$$

hence $\operatorname{ord}_{\mathfrak{p}} C(\vartheta) = \frac{1}{2}\operatorname{ord}_{\mathfrak{p}} C(f) \geqslant 0$ and

$$\vartheta(\boldsymbol{t}) \in \boldsymbol{Z}[\zeta_4, \boldsymbol{t}].$$

Now (103), (105) and (106) imply

$$X(\boldsymbol{t})^{2^{\alpha-1}}, \ Y(\boldsymbol{t})^{2^{\alpha-1}} \in \boldsymbol{Z}[\boldsymbol{t}]; \quad X(\boldsymbol{t}), Y(\boldsymbol{t}) \in \boldsymbol{Z}[\boldsymbol{t}]$$

and we get by (104)

$$X(\boldsymbol{t})^{2^\alpha} + Y(\boldsymbol{t})^{2^\alpha} = f(\boldsymbol{t}).$$

The proof of the first part of the theorem is complete. In order to prove the second part it is enough to consider the case $n > 2$ (for $n = 2$ the assertion is contained in Theorem 1).

Let p be a prime satisfying

(107) $$p \equiv 1 \bmod 2^{\alpha+1}, \quad p \not\equiv 1 \bmod 2n \quad \text{if} \quad n \neq 2^\alpha$$

and let us choose an integer c such that

$$c^n + 1 \equiv 0 \bmod p^n, \quad c = -1 \quad \text{if} \quad \alpha = 0.$$

Consider now the polynomial

(108) $$f(t) = u(t)^n + v(t)^n,$$

where $u(t) = \dfrac{t(t-1)\dots(t-p+1)}{p}$, $v(t) = cu(t) + p^{n-1}$.

It is easily seen that $f(t) \in \boldsymbol{Z}[t]$ and

(109) $$|f| = \begin{cases} p^n & \text{if} \quad \alpha > 0, \\ p^{n-1} & \text{if} \quad \alpha = 0. \end{cases}$$

Moreover since polynomials $u(t)$, $v(t)$ are integer-valued the equation $x^n + y^n = f(t)$ is soluble in $x, y \in \boldsymbol{Z}$ for all $t \in \boldsymbol{Z}$. On the other hand suppose that

(110) $$X(t)^n + Y(t)^n = f(t), \quad X, Y \in \boldsymbol{Z}[t].$$

Since

$$X(t)^n + Y(t)^n = \prod_{i=0}^{n-1}\big(X(t) - \zeta_{2n}^{2i+1} Y(t)\big)$$

we have

$$|f| \geqslant \begin{cases} n\max\{|X|, |Y|\} & \text{if} \quad \alpha > 0, \\ (n-1)\max\{|X|, |Y|\} & \text{if} \quad \alpha = 0. \end{cases}$$

Hence by (109)

(111) $$\max\{|X|, |Y|\} \leqslant p.$$

Taking $i = 0, 1, \dots, p-1$ we get $u(i) = 0$ hence

(112) $$X(i)^n + Y(i)^n = p^{n(n-1)}.$$

If $n = 2^\alpha$, $\alpha > 1$ or $n = 3$ by special cases of Fermat's last theorem (111) implies

(113) $$X(i)Y(i) = 0 \quad (0 \leqslant i < p).$$

If $n > 3$, by Zsigmondy's theorem either $X(i)Y(i) = 0$ or $X(i) = \pm Y(i)$ or $X(i)^n + Y(i)^n$ has the so-called primitive prime factor $\equiv 1 \bmod 2n$. The last two possibilities are incompatible with (107) and (112) hence (113) holds for all $n > 2$. By (112) if $X(i) = 0$, $Y(i) = p^{n-1}$ for $\alpha = 0$, $Y(i) = \pm p^{n-1}$ for $\alpha > 0$. In view of symmetry between X and Y we may assume that there is a set $S \subset \{0, 1, \dots, p-1\}$ with the following properties

$$|S| \geqslant \frac{p+1}{2(n,2)}, \quad X(i) = 0, \quad Y(i) = p^{n-1} \quad \text{for } i \in S.$$

(If n is even we can replace Y by $-Y$.) Let

$$P(t) = \prod_{i \in S}(t-i).$$

It follows that

(114) $$|P| \geqslant \frac{p+1}{2(n,2)}, \quad X(t) \equiv 0 \bmod P(t), \quad Y(t) \equiv p^{n-1} \bmod P(t)$$

and we get from (108) and (110)

$$Y(t)^n \equiv v(t)^n \bmod P(t)^n.$$

Since $Y(t) \equiv v(t) \bmod P(t)$ and $(v, P) = 1$ we obtain

$$Y(t) \equiv v(t) \bmod P(t)^n.$$

However by (111)

$$\max\{|Y|, |v|\} \leqslant p < n|P|$$

hence

$$Y(t) = v(t) \notin \mathbf{Z}[t].$$

References

[1] P. T. Bateman and R. A. Horn, *A heuristic asymptotic formula concerning the distribution of prime numbers*, Math. Comp. 16 (1962), pp. 363–367.
[2] A. Châtelet, *Leçons sur la théorie des nombres*, Paris 1913.
[3] S. Chowla, *Some problems of elementary number theory*, J. Reine Angew. Math. 222 (1966), pp. 71–74.
[4] H. Davenport, D. J. Lewis and A. Schinzel, *Polynomials of certain special types*, Acta Arith. 9 (1964), pp. 107–116.
[5] H. Halberstam and H. E. Richert, *Sieve methods*, London–New York–San Francisco 1974.
[6] H. Hasse, *Zahlentheorie*, Berlin 1963.
[7] T. Kojima, *Note on number-theoretical properties of algebraic functions*, Tôhoku Math. J. 8 (1915), pp. 24–37.
[8] S. Lang, *Diophantine geometry*, New York–London 1962.
[9] W. J. LeVeque, *A brief survey of diophantine equations*, Studies in number theory, pp. 4–24, Englewood Cliffs N.J. 1969.
[10] D. Mumford, *A remark on Mordell's conjecture*, Amer. J. Math. 87 (1965), pp. 1007–1016.
[11] P. Ribenboim, *Polynomials whose values are powers*, J. Reine Angew. Math. 268/269 (1974), pp. 34–40.
[12] A. Schinzel et W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. 4 (1958), pp. 185–208, *Erratum* 5 (1959), p. 259.
[13] A. Schinzel, *On Hilbert's irreducibility theorem*, Ann. Polon. Math. 16 (1965), pp. 333–340.
[14] — *On a theorem of Bauer and some of its applications* II, Acta Arith. 22 (1972), pp. 221–231.
[15] — *Abelian binomials, power residues and exponential congruences*, ibid. 32 (1977), pp. 245–274.
[16] — *Addendum and corrigendum to* [15], ibid. 36 (1980), pp. 101–104.
[17] W. M. Schmidt, *Equations over finite fields. An elementary approach*, Lecture Notes in Mathematics No 536, Berlin–Heidelberg–New York 1976.
[18] T. Skolem, *Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen*, Vid. akad. Avh. Oslo I., 1937, nr 12.

Received on 7.4.1978 (1062)

ACTA ARITHMETICA
XXXVIII (1980)

Corrigendum to the paper "Periodic analogues of the Euler-Maclaurin and Poisson summation formulas with applications to number theory", Acta Arith. 28 (1975), pp. 23–68

by

BRUCE C. BERNDT (Urbana, Ill.) and
LOWELL SCHOENFELD (Buffalo, N.Y.)

There is a misprint in the formulation of Proposition 9.1 on p. 55 The correct formulation is as follows:

PROPOSITION 9.1. *For* $|y| < 2\pi/k$,

$$\frac{y\sum_{n=0}^{k-1} a_n e^{ny}}{e^{ky}-1} = \sum_{j=0}^{\infty} \frac{B_j(A)}{j!}\, y^j = e^{B(A)y}, \tag{9.2}$$

where the last expression uses the umbral convention according to which after the formal expansion into power series, the expression $\{B(A)\}^j$ *is to be replaced by* $B_j(A)$.

Moreover on p. 29, line 3 replace $1 \leqslant m \leqslant r$ by $2 \leqslant m \leqslant r$ and on p. 30, line 10 replace P by P_j.

Received on 14.7.1980