ANNALES
POLONICI MATHEMATICI
XX (1968)

Diophantine equations involving primes, II

by J. Wójcik (Warszawa)

I have proved in [3] the following theorem: Let f and g be irreducible polynomials of degree r with integer coefficients and the same leading coefficient; m and n be non-zero integers. If arbitrarily chosen roots of f and g generate the same normal field and $\sqrt[r]{m/n}$ is irrational, then there exists only finitely many primes $p = \frac{f(x)}{m} = \frac{g(y)}{n}$, where x, y are integers. For the special case $f(x) = ax^2+b\xi x+c\xi^2$, $g(y) = ay^2+b\eta y+c\eta^2$ I have obtained in [2] the same assertion under a less stringent condition, namely $amn(n\xi^2-m\eta^2) \neq 0$. The aim of this paper is to generalize the above results. The examples given at the end of the paper show that these results can be applicable is some cases, where the equation $\frac{f(x)}{m} = \frac{g(y)}{n}$ has infinitely many solutions in integers.

In the sequel Q denotes the rational field, and N_F is the norm from F to Q for any number field F.

THEOREM 1. *Let $f, f_1, \ldots, f_k$ be polynomials defined and irreducible over Q; $\eta, \xi_1, \ldots, \xi_k$ any of their roots. Suppose that for each $j \leqslant k$, the field $Q(\xi_j)$ is normal and contains η. If there exists infinitely many integers x, y such that*

(1) $\quad f_1(x)f_2(x)\ldots f_k(x) = f(y)$ *and* $f_j(x)$ *are primes* $(1 \leqslant j \leqslant k)$,

then there exists a polynomial $h(x)$ with integer coefficients and two integers a, b such that

$$f_1(ax+b)\ldots f_k(ax+b) = f\big(h(x)\big), \tag{2}$$

the polynomials $f_j(ax+b)$ $(1 \leqslant j \leqslant k)$ have integer coefficients and $f\big(h(x)\big)$ has no constant factor > 1.

We set $K = Q(\eta)$, $K_j = Q(\xi_j)$, $r = |K|$, $t_j = |K_j|$, $r_j = t_j/r$ $(1 \leqslant j \leqslant k)$ ($|\ |$ denotes the degree of a field, later also the order of a group) and prove first:

LEMMA. *Let a be an integer of K, β_j an integer of K_j, m, n_j rational integers $\neq 0$ $(1 \leqslant j \leqslant k)$. If primes $p_1, p_2, \ldots, p_k$ satisfy the conditions*

$$(p_1p_2\ldots p_k, mn_1\ldots n_k) = 1\,, \quad p = \frac{N_{k_j}(\beta_j)}{n_j} \quad (1 \leqslant j \leqslant k)\,,$$

$$p_1p_2\ldots p_k = \frac{N_k(a)}{m}\,,$$

then there exists a system of integers conjugate to β_j's, say $\beta_1^{(s_{11})}, \ldots, \beta_1^{(s_{r_1 1})}, \ldots$ $\ldots, \beta_k^{(s_{1k})}, \ldots, \beta_k^{(s_{r_k k})}$ such that

$$a\prod_{j=1}^{k} n_j^{r_j}\Big/\prod_{j=1}^{k}\prod_{i=1}^{r_j}\beta_j^{(s_{ij})}$$

is an algebraic integer.

Proof. Let j be any index $\leqslant k$, $n = p_1p_2\ldots p_k$, $\mathfrak{q}_{ji} = (p_j, \beta_j^{(i)})$ $(1 \leqslant i \leqslant t_j)$, $\mathfrak{a} = (n, a)$. We have

$$p_j = \big(p_j, N_{k_j}(\beta_j)\big)|N_{K_j}\mathfrak{q}_{ji}$$

and

$$N_{K_j}\mathfrak{q}_{ji}|\big(p_j^{t_j}, N_{K_j}(\beta_j)\big) = (p_j^{t_j}, n_jp_j) = p_j$$

thus

(3) $$p_j = \mathfrak{q}_{j1}\mathfrak{q}_{j2}\ldots\mathfrak{q}_{jt_j}$$

is a factorization of p into prime ideals of K_j. Further $n = (n, N_K a)|N_K\mathfrak{a}$ and $N_K\mathfrak{a}|(n^r, N_K a) = (n^r, nm) = n$, i.e., $n = N_K\mathfrak{a}$. Since $K \subset K_j$ and $\mathfrak{q}_{js}$ are prime ideals of the first degree in K_j we get

$$(n, a) = \mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_k\,,$$

where $N_K\mathfrak{p}_j = p_j$, $\mathfrak{p}_j$ is a prime ideal in K.

From (3) and the divisibility $\mathfrak{p}_j|p_j$ we infer the existence of a system $s_{1j}, s_{2j}, \ldots, s_{r_jj}$ such that

$$\mathfrak{p}_j = \mathfrak{q}_{js_{1j}}\mathfrak{q}_{js_{2j}}\ldots\mathfrak{q}_{js_{r_jj}}\,.$$

Since $\mathfrak{q}_{j,s_{ij}}|(\beta_j^{s_{ij}})$ we get

$$\mathfrak{p}_j|\gamma_j\,,$$

where

$$\gamma_j = \prod_{i=1}^{r_j}\beta_j^{(s_{ij})}\,, \quad \gamma_j = \mathfrak{p}_j\mathfrak{c}_j\,,$$

$$N_{K_j}(\gamma_j) = N_{K_j}^{r_j}(\beta_j) = p_j^{r_j}n_j^{r_j} = N_{K_j}(\mathfrak{p}_j)N_{K_j}(\mathfrak{c}_j) = p_j^{r_j}N_{K_j}(\mathfrak{c}_j)\,,$$

$$n_j^{r_j} = N_{K_j}(\mathfrak{c}_j)\,, \quad \text{i.e.,} \quad \mathfrak{c}_j|n_j^{r_j}\,.$$

Hence and from the divisibility

$$\mathfrak{p}_1\mathfrak{p}_2\ldots\mathfrak{p}_k|a$$

we infer

$$\beta = \prod_{j=1}^{k} \gamma_j = \prod_{j=1}^{k} \mathfrak{p}_j \prod_{j=1}^{k} \mathfrak{c}_j | \alpha \prod_{j=1}^{k} n_j^{r_j}$$

which shows that $a \prod_{j=1}^{k} n_j^{r_j}/\beta$ is an algebraic integer.

Proof of the theorem. Assume that there exists infinitely many integers x, y satisfying (1). Let for each $j \leqslant k$

$$f_j(x) = \frac{\bar{f}_j(x)}{n_j}, \quad f(x) = \frac{\bar{f}(x)}{m}, \tag{4}$$

where $\bar{f}_j, \bar{f}$ are polynomials with integer coefficients and n_j, m are integers. Let $\bar{a}_j, \bar{a}_0$ be the leading coefficients of $\bar{f}_j$ and $\bar{f}$, respectively. It follows from the assumption that

$$p_{jl} = f_j(x_l) = \frac{N_{K_j}(\bar{a}_j x_l - a_j \xi_j)}{a_j^{t_j-1} n_j}, \tag{5}$$

$$p_{1l} \dots p_{kl} = f(y_l) = \frac{N_K(\bar{a}_0 y_l - \bar{a}_0 \eta)}{a_0^{r-1} m},$$

where $\lim_{l\to\infty} |x_l| = \infty$, $\lim_{l\to\infty} |y_l| = \infty$, p_{jl} are primes.

Let

$$F(x) = \prod_{j=1}^{k} f_j(x) = \sum_{i=0}^{R} A_i x^{R-i}, \quad f(x) = \sum_{i=0}^{r} a_i x^{r-i}.$$

We have

$$R = \deg F = r \sum_{j=1}^{k} r_j. \tag{6}$$

By lemma there exist an infinite subsequence of l's (which without loss of generality can be taken as $1, 2, 3, \dots$) such that for a fixed system of conjugates (s_{ij}) of the numbers ξ_j, $c\gamma_l$ is an algebraic integer, where

$$c = a_0 \prod_{j=1}^{k} (a_j^{t_j-2} n_j)^{r_j}, \quad \gamma_l = \frac{y_l - \eta}{\prod_{j=1}^{k} \prod_{i=1}^{r_j} (x_l - \xi_j^{(s_{ij})})}. \tag{7}$$

We have

$$\frac{y_l^r}{x_l^R} = \frac{A_0 + \sum_{i=1}^{R} A_i / x_l^i}{a_0 + \sum_{i=1}^{r} a_i / y_l^i}, \quad \text{whence} \quad \lim_{l\to\infty} \frac{y_l^r}{x_l^R} = \frac{A_0}{a_0}.$$

Without loss of generality we can write

$$(8)\qquad \lim_{l\to\infty}\frac{y_l}{x_l^{R/r}} = B, \quad \text{where} \quad B = \varepsilon\sqrt[r]{\frac{A_0}{a_0}}, \quad \varepsilon = \pm 1, \quad \varepsilon^r = 1.$$

Let $L = K_1K_2\ldots K_k$. $\lambda = |L|$. Clearly $\gamma_l \in L$. Denote by $\gamma_l^{(s)}$ $(s = 1, 2, \ldots, \lambda)$ the conjugates of γ_l in L in such a way that $\gamma_l^{(1)} = \gamma_l$. We get from (6), (7) and (8)

$$(9)\qquad \lim_{l\to\infty}\gamma_l^{(s)} = \lim_{l\to\infty}\frac{\dfrac{y_l}{x_l^{R/r}} - \dfrac{\eta(s)}{x_l^{R/r}}}{\prod_{j=1}^{k}\prod_{i=1}^{r_j}\left(1-\dfrac{\xi_j^{(\sigma_{ijs})}}{x_l}\right)} = B,$$

where $(\xi_j^{(s_{ij})})^{(s)} = \xi_j^{\sigma_{ijs}}$.

Let ϑ be an algebraic integer generating L. We have

$$(10)\qquad \gamma_l^{(s)} = \sum_{j=0}^{\lambda-1} u_{jl}\vartheta^{(s)j} \quad (s = 1, 2, \ldots, \lambda), \quad u_{jl} \text{ rational}.$$

Solving the above system by Cramer's formulae and passing to a limit we get from (9):

$$(11)\qquad \lim_{l\to\infty} u_{0l} = \lim_{l\to\infty}\frac{1}{\det(\vartheta^{(s)j})}\begin{vmatrix} \gamma_l & \vartheta & \ldots & \vartheta^{\lambda-1} \\ \gamma_l^{(2)} & \vartheta^{(2)} & \ldots & \vartheta^{(2)\lambda-1} \\ \cdots & \cdots & \cdots & \cdots \\ \gamma_l^{(\lambda)} & \vartheta^{(\lambda)} & \ldots & \vartheta^{(\lambda)\lambda-1} \end{vmatrix} = B;$$

$$(12)\qquad \lim_{l\to\infty} u_{jl} = \lim_{l\to\infty}\frac{1}{\det(\vartheta^{(s)j})}\begin{vmatrix} 1 & \vartheta & \ldots & \vartheta^{j-1} & \gamma_l & \vartheta^{j+1} & \ldots & \vartheta^{\lambda-1} \\ 1 & \vartheta^{(2)} & \ldots & \vartheta^{(2)j-1} & \gamma_l^{(2)} & \vartheta^{(2)j+1} & \ldots & \vartheta^{(2)\lambda-1} \\ \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & \vartheta^{(\lambda)} & \ldots & \vartheta^{(\lambda)j-1} & \gamma_l^{(\lambda)} & \vartheta^{(\lambda)j+1} & \ldots & \vartheta^{(\lambda)\lambda-1} \end{vmatrix} = 0.$$

Since $c\gamma_l^{(s)}$ are algebraic integers, the numbers $cu_{jl}(\mathrm{disc}\,\vartheta)^2$ are rational integers. It follows hence by (11) and (12) that for sufficiently large l the numbers u_{jl} are constant and

$$(13)\qquad u_{0l} = B, \quad u_{jl} = 0 \quad (j = 1, 2, \ldots, \lambda-1).$$

Hence by (13)

$$(14)\qquad \gamma_l = B.$$

Let

$$(15)\qquad g(x) = \eta + B\prod_{j=1}^{k}\prod_{i=1}^{r_j}(x-\xi_j^{(s_{ij})}) = \sum_{j=0}^{R/r} b_j x^j.$$

We shall show that the coefficients b_j of the polynomial g are rational. Since by (14) $B \in L$ we have $b_j \in L$ $(j = 0, 1, \ldots, R/r-1)$. Therefore

$$b_j = \sum_{i=0}^{\lambda-1} v_{ji}\vartheta^i ,$$

where v_{ji} are rationals. Hence and from the formulae (7), (14) and (15) we get

$$(16) \qquad y_l = g(x_l) = \sum_{i=0}^{\lambda-1} \Big(\sum_{j=0}^{R/r} v_{ji} x_l^j\Big)\vartheta^i .$$

Comparing the coefficients of ϑ^i we obtain

$$\sum_{j=0}^{R/r} v_{ji} x_l^j = 0 \qquad (i > 0) .$$

Since this equality holds for infinitely many values x_l we have $v_{ji} = 0$ $(i > 0,\ j = 0, 1, \ldots, R/r)$. Therefore $b_j = v_{j0}$ $(j = 0, 1, \ldots, R/r)$, and b_j are rationals.

For each $j \leqslant k$ let G_j denote the Galois group of K_j, H_j the subgroup of G_j leaving invariant K. Clearly

$$(17) \qquad |H_j| = r_j .$$

Let $\xi_j^{T_1}, \xi_j^{T_2}, \ldots, \xi_j^{T_{u_j}}$ $(T_i \in G_j)$ be all the distinct conjugates of ξ_j occurring in the product $\prod_{j=1}^{k}\prod_{i=1}^{r_j}(x-\xi_j^{(s_{ij})})$ and let $\xi_j^{T_i}$ occurs there with the multiplicity k_{ij}. Clearly

$$(18) \qquad \sum_{i=1}^{u_j} k_{ij} = r_j e_j ,$$

where e_j is the number of polynomials $f_\nu(x)$ $(1 \leqslant \nu \leqslant k)$ divisible by $f_j(x)$.

By (15) we have

$$(19) \qquad \eta = g(\xi_j^{T_1}) , \qquad \eta^{T_1^{-1}T_i} = g(\xi_j^{T_i}) = \eta .$$

Since η generates K it follows that $T_1^{-1}T_i \in H_j$. Hence by (17)

$$(20) \qquad u_j \leqslant r_j .$$

It follows from (18) and (20) that at least one of the numbers k_{ij} must be greater than or equal to e_j and we may assume without loss of generality that

$$k_{1j} \geqslant e_j .$$

By (15)

$$(x-\xi_j^{T_1})^{e_j} | g(x)-\eta , \qquad \text{thus} \qquad (x-\xi_j^{T_1})^{e_j-1} | g'(x) .$$

By (19)

$$f\big(g(\xi_j^{T_1})\big) = f(\eta) = 0 .$$

Since $f\big(g(x)\big)' = f'\big(g(x)\big)\cdot g'(x)$ we get

$$(x-\xi_j^{T_1})^{e_j} | f\big(g(x)\big) .$$

Since $f_j(x)$ is an irreducible polynomial it follows

$$f_j^{e_j}(x) | f\big(g(x)\big) \qquad (1 \leqslant j \leqslant k) ,$$

whence

$$F(x) | f\big(g(x)\big) .$$

By (6) and (15) the polynomials F and $f(g)$ are of degree R. Therefore, there exists a rational number C such that

$$f\big(g(x)\big) = CF(x) .$$

Comparing the leading coefficients on both sides we get $C = 1$, i.e.

(21) $$f\big(g(x)\big) = F(x) .$$

Let

(22) $$g(x) = \frac{H(x)}{N} ,$$

where $H(x)$ is a polynomial with integer coefficiets, N is an integer $\neq 0$, $a = Nn_1, \ldots, n_k$. We choose from the sequence $\{x_l\}$ $a+1$ terms, say $x_1, \ldots, x_{a+1}$ such that

(23) $$\big(F(x_i), F(x_j)\big) = 1 \quad \text{for} \quad i \neq j .$$

The choice is possible since the least prime factor of $F(x_l)$ tends to infinity, as is clear from the formula

$$F(x_l) = f_1(x_l)f_2(x_l)\ldots f_k(x_l) = p_{1l}p_{2l}\ldots p_{kl} .$$

Now, by the box principle there exist integers μ, ν, b, z_μ and z_ν such that

(24) $$x_\mu = az_\mu + b , \quad x_\nu = az_\nu + b , \quad 1 \leqslant \mu \leqslant a+1 , \quad 1 \leqslant \nu \leqslant a+1 , \ \mu \neq \nu .$$

We take $h(x) = g(ax+b)$. By (21) we have

$$f\big(h(x)\big) = F(ax+b)$$

what was to be proved as (2).

By (5) and (16) the numbers $g(x_\mu)$, $f_j(x_\mu)$ $(j = 1, 2, \ldots, k)$ are integers. Hence and from (4), (22) and (24) we get

$$H(ax+b) \equiv H(b) \equiv H(x_\mu) \equiv 0 \bmod N ,$$
$$\bar{f}_j(ax+b) = \bar{f}_j(b) \equiv \bar{f}_j(x_\mu) \equiv 0 \bmod n_j \qquad (j = 1, 2, \ldots, k) .$$

This means, that the polynomials $h(x)$, $f_j(ax+b)$ have integer coefficients $(j = 1, 2, \dots, k)$. It follows from (23) and (24) that

$$\big(F(az_\mu+b), F(az_\nu+b)\big) = \big(F(x_\mu), F(x_\nu)\big) = 1 .$$

Therefore $F(ax+b)$ has no constant factor >1, which completes the proof.

Remark 1. It follows from the conjecture H of A. Schinzel [1] that the condition given in Theorem 1 as necessary for the existence of infinitely many integers x, y satisfying (1) is also sufficient.

Remark 2. The method of proof of Theorem 1 works also for polynomials defined over imaginary quadratic fields. More precisely, holds the following

THEOREM 2. *Let $f(x), f_1(x), \dots, f_k(x)$ be polynomials defined and irreducible over an imaginary quadratic number field R, η, $\xi_1, \dots, \xi_k$ any of their roots. Suppose that for each $j \leqslant k$, $R(\xi_j)$ is a normal extension of R containing η. If there exists infinitely many integers x, y of R such that $\big(f_j(x)\big)$ are prime ideals of R $(1 \leqslant j \leqslant k)$ and*

$$f_1(x)f_2(x)\dots f_k(x) = f(y) ,$$

then there exists a polynomial $h(x)$ with coefficients integral in R and a, b integers of R such that

$$f\big(h(x)\big) = f_1(ax+b)\dots f_k(ax+b) .$$

The coefficients of all the polynomials $f_j(ax+b)$ $(1 \leqslant j \leqslant k)$ are integers of R, $N_R\, f\big(h(x)\big)$ has no constant factor >1.

A similar but easier and purely algebraic proof can be given for

THEOREM 3. *Let K be an arbitrary field, $X = (x_1, \dots, x_n)$, $f(x)$, $f_1(x), \dots, f_k(x)$ be polynomials defined, irreducible and separable over K, η, $\xi_1, \dots, \xi_k$ any of their roots. Suppose that $K(\xi_j)$ is for each $j \leqslant k$ a normal extension of K containing η. The equation*

$$f_1\big(\varphi(X)\big)\dots f_k\big(\varphi(X)\big) = f\big(\psi(X)\big)$$

with the side condition that all $f_j\big(\varphi(X)\big)$ are irreducible over K is solvable in polynomials $\varphi(X)$, $\psi(X)$ if and only if there exists a polynomial $h(x)$ defined over K such that

$$f_1(x)\dots f_k(x) = f\big(h(x)\big) .$$

EXAMPLE 1. There exist only finitely many primes p of the form

$$p = \frac{x^4+15x^2+9}{25} = 225y^4+51y^2+1 .$$

Indeed, any roots of the above polynomials generate the same normal field $Q(\sqrt{-1}, \sqrt{21})$ and (2) does not hold since $\sqrt[4]{25\cdot 225}$ is irrational. On the other hand, the equation

$$\frac{x^4+15x^2+9}{25} = 225y^4+51y^2+1$$

has infinitely many integer solutions, e.g. $x = \alpha, y = \beta$, where $\alpha^2-75\beta^2 = 1$.

EXAMPLE 2. There exist only finitely many primes p of the form

$$p = \frac{4x^4-2x^2+1}{3} = \frac{2y^2+1}{3}.$$

Indeed, any root of $4x^4-2x^2+1$ generates the normal field $Q(\sqrt{-2}, \sqrt{-3})$ and (2) does not hold since $\sqrt{2}$ is irrational. On the other hand, the equation

$$\frac{4x^4-2x^2+1}{3} = \frac{2y^2+1}{3}$$

has infinitely many integer solutions, e.g. $x = \beta$, $y = \alpha\beta$, where $\alpha^2-2\beta^2 = -1$.

Added in proof. 1. The result of [3] has been misquoted in Math. Rev. 34, 2526; the condition on f and g assumed in [3] is more stringent than the coincidence of their minimal splitting fields.

2. If we assume in (1) that $f_j(x)$ are powers of primes, the assertion of Theorem 1 holds except for the statement concerning the constant factor of $f(h(x))$.

References

[1] A. Schinzel et W. Sierpiński, *Sur certaines hypothèses concernant les nombres premiers*, Acta Arith. 4 (1958), pp. 185-208.

[2] J. Wójcik, *O przedstawieniach liczb pierwszych przez formy kwadratowe*, Prace Mat. 9 (1965), pp. 19-21.

[3] — *Diophantine equations involving primes*, Ann. Polon. Math. 18 (1966), pp. 315-321.

Reçu par la Rédaction le 29. 4. 1967