ANNALES
POLONICI MATHEMATICI
XVIII (1966)

Diophantine equations involving primes

by J. Wójcik (Warszawa)

I have proved ([3]) the following theorem: for all integers a, b, c, ξ, η, m, n satisfying the condition $amn(n\xi^2-m\eta^2)\neq 0$ the number of primes p representable in the form

$$p=\frac{ax^2+b\xi x+c\xi^2}{m}=\frac{ay^2+b\eta y+c\eta^2}{n},$$

where x, y are integers, is finite.

The aim of this paper is to generalize that theorem to the representations of primes in the form

$$p=\frac{f(x)}{m}=\frac{g(y)}{n}, \tag{1}$$

where f and g are polynomials of an arbitrary degree r satisfying certain restrictions. If $r>2$ it happens often (cf. [2]) that the equation

$$\frac{f(x)}{m}=\frac{g(y)}{n} \tag{2}$$

has only a finite number of integral solutions and then the finite number of solutions of (1) does not seem of interest. However, the theorem given below permits to find effectively all the solutions of (1), which at the present cannot in general be done for (2) even if the number of its solution is finite.

In the sequel $\|z\|$ denotes the distance between z and the nearest integer.

THEOREM. *Let f and g be irreducible polynomials of degree r with integral coefficients and the same highest coefficient a, m and n be non-zero integers.*

If f and g determine the same normal field and $\sqrt[r]{m/n}$ is irrational, then there exist only finitely many primes p representable in the form

$$p=\frac{f(x)}{m}=\frac{g(y)}{n},$$

where x, y are integers. Such primes p either divide mn or can be obtained for

$$(3)\qquad |x| \leqslant c_r H(f)\frac{|na^{r-1}\sqrt[r]{m/n}|}{\|na^{r-1}\sqrt[r]{m/n}\|} \quad \text{or} \quad |y| \leqslant c_r H(g)\frac{|na^{r-1}\sqrt[r]{m/n}|}{\|na^{r-1}\sqrt[r]{m/n}\|},$$

where $H(f)$, $H(g)$ are the heights of f and g respectively, and

$$c_r = 24\Gamma(r)\Gamma(2+\tfrac{1}{2}r)\pi^{-r/2}.$$

Remark 1. In virtue of symmetry $|na^{r-1}\sqrt[r]{m/n}|/\|na^{r-1}\sqrt[r]{m/n}\|$ can be replaced in the inequalites (3) by

$$\min\left\{\frac{|na^{r-1}\sqrt[r]{m/n}|}{\|na^{r-1}\sqrt[r]{m/n}\|},\ \frac{|ma^{r-1}\sqrt[r]{n/m}|}{\|ma^{r-1}\sqrt[r]{n/m}\|}\right\}.$$

If $\sqrt[r]{m/n}$ is rational and $\frac{f(x)}{m}-\frac{g(y)}{n}$ is irreducible, then all the solutions of (2) can be found effectively by the method of Runge.

LEMMA 1. *In every algebraic number field of degree r there exists an integral basis $\omega_1 = 1, \omega_2, \ldots, \omega_r$ such that*

$$(4)\qquad \sqrt{\prod_{i=1}^{r}\Big(\sum_{s=1}^{r}|\omega_i^{(s)}|^2\Big)} \leqslant 2r!\,\Gamma(1+\tfrac{1}{2}r)\pi^{-r/2}\sqrt{|D|}.$$

The superscripts denote conjugates and D is the discriminant of the field.

Proof (due to A. Schinzel). Let $\Omega_1, \Omega_2, \ldots, \Omega_r$ be any integral basis of the field K in question. Clearly

$$1 = \sum_{j=1}^{r} a_j\Omega_j,$$

where a_j are rational integers and $(a_1, \ldots, a_r) = 1$. By Hermite's theorem there exists an integral unimodular matrix a_{ij} such that $a_{1j} = a_j$. Putting

$$\Omega_i' = \sum_{j=1}^{r} a_{ij}\Omega_j \qquad (1 \leqslant i \leqslant r)$$

we find a new basis $\Omega_1', \ldots, \Omega_r'$ such that $\Omega_1' = 1$.

Let the field K have r_1 real and $2r_2$ complex conjugates so that

$$\Omega_j'^{(s)} \text{ is real for } s = 1, 2, \ldots, r_1$$

and

$$\bar{\Omega}_j'^{(s)} = \Omega_j'^{(s+r_2)} \quad \text{for} \quad s = r_1+1, \ldots, r_1+r_2 \quad (1 \leqslant j \leqslant r)$$

(the bar denotes complex conjugate).

Consider in the r-dimensional Euclidean space, the ellipsoide E

$$\sum_{s=1}^{r_1}\Big(\sum_{j=1}^{r}\Omega_j'^{(s)}x_j\Big)^2+\sum_{s=r_1+1}^{r_1+r_2}2\Big(\sum_{j=1}^{r}R\Omega_j'^{(s)}x_j\Big)^2+\sum_{s=r_1+1}^{r_1+r_2}2\Big(\sum_{j=1}^{r}J\Omega_j'^{(s)}x_j\Big)^2\leqslant 1\,.$$

E is obtained from the r-dimensional sphere $y_1^2+y_2^2+\ldots+y_r^2\leqslant 1$ by the linear transformation

$$y_s=\begin{cases}\displaystyle\sum_{j=1}^{r}\Omega_j'^{(s)}x_j & \text{for}\quad 1\leqslant s\leqslant r_1\,,\\ \displaystyle\sqrt{2}\sum_{j=1}^{r}R\Omega_j'^{(s)}x_j & \text{for}\quad r_1<s\leqslant r_1+r_2\,,\\ \displaystyle\sqrt{2}\sum_{j=1}^{r}J\Omega_j'^{(s)}x_j & \text{for}\quad r_1+r_2<s\leqslant r\end{cases}$$

with the determinant equal in the absolute value to

$$|\det\Omega_j^{(s)}|=\sqrt{|D|}\,.$$

Therefore the volume V of E equals $\pi^{r/2}\Gamma^{-1}(1+\frac{1}{2}r)/\sqrt{|D|}$.

On the other hand, the ellipsoide E induces the distance function

$$F(x_1,\ldots,x_n)=\sqrt{\sum_{s=1}^{r}\Big|\sum_{j=1}^{r}\Omega_j'^{(s)}x_j\Big|^2}\,.$$

In virtue of the theorem of Mahler (cf. [1], appendix II, Theorem VI) there exists an integral unimodular matrix y_{ij} such that

$$V\prod_{i=1}^{r}F(y_{i1},\ldots,y_{ir})\leqslant 2r!\,. \tag{5}$$

Moreover, it follows from the proof of that theorem (l.c., p. 157) that $y_{ij}=0$ for $j>i$, $y_{ii}=1$ $(1\leqslant i\leqslant r)$.

We put $\omega_i=\sum_{j=1}^{r}y_{ij}\Omega_j'$ $(1\leqslant i\leqslant r)$. Clearly $\omega_1,\ldots,\omega_r$ is an integral basis for K and $\omega_1=1$.

Further,

$$F(y_{i1},\ldots,y_{ir})=\sqrt{\sum_{s=1}^{r}|\omega_i^{(s)}|^2}$$

and by (5)

$$\sqrt{\prod_{i=1}^{r}\sum_{s=1}^{r}|\omega_i^{(s)}|^2}\leqslant 2r!\,\Gamma(1+\tfrac{1}{2}r)\,\pi^{-r/2}\sqrt{|D|}\,,$$

q.e.d.

Remark 2. The constant $2r!\Gamma(1+\frac{1}{2}r)\pi^{-r/2}$ could be improved by using more refined arguments from the geometry of numbers.

LEMMA 2. *Let K be a normal field; a, β integers in K, $Na, N\beta$ their norms, m, n rational integers $\neq 0$. If p is a rational prime,*

$$p \nmid mn \quad \text{and} \quad p = \frac{N(a)}{m} = \frac{N(\beta)}{n}$$

then there exists a conjugates of β, say $\beta^{(s)}$ such that $na/\beta^{(s)}$ is an integer.

Proof. Let $\mathfrak{p}_i = (p, a^{(i)})$, $\mathfrak{q}_i = (p, \beta^{(i)})$ $(1 \leqslant i \leqslant r)$. We have $p = (p, Na) | N\mathfrak{p}_i$ and $N\mathfrak{p}_i | (p^r, Na) = (p^r, pm) = p$ thus $(p) = \mathfrak{p}_1\mathfrak{p}_2 \dots \mathfrak{p}_r$ is the factorization of (p) into prime ideals. Similarly $(p) = \mathfrak{q}_1\mathfrak{q}_2 \dots \mathfrak{q}_r$ and it follows from the uniqueness of factorization that for some s

$$\mathfrak{p}_1 = \mathfrak{q}_s, \qquad \mathfrak{p}_1 | \beta^{(s)}.$$

We have

$$(\beta^{(s)}) = \mathfrak{p}_1\mathfrak{b},$$

$$|N(\beta^{(s)})| = |N(\beta)| = p|n| = N(\mathfrak{p}_1)N(\mathfrak{b}) = pN(\mathfrak{b}), \qquad |n| = N(\mathfrak{b}).$$

Hence $\mathfrak{b} | n$ and since $\mathfrak{p}_1 | a$

$$(\beta^{(s)}) = \mathfrak{p}_1\mathfrak{b} | na$$

and the number $na/\beta^{(s)}$ is integral, q.e.d.

Remark 3. The assumption that K is normal is necessary, as shows the example

$$K = Q(\sqrt[3]{2}), \quad a = -1+2\sqrt[3]{4}, \quad \beta = 3+\sqrt[3]{4}, \quad m = n = 1, \quad p = 31.$$

LEMMA 3. *If f, g, m, n satisfy the assumptions of the theorem, x, y are rational integers, (2) holds and*

$$A > 6, \qquad |x| > AH(f), \qquad |y| > AH(g), \tag{6}$$

then for a suitable $\varepsilon = \pm 1$

$$\left|\frac{x}{y} - \varepsilon\sqrt[r]{\frac{m}{n}}\right| < \frac{6}{Ar}\sqrt[r]{\left|\frac{m}{n}\right|}.$$

Proof. Let

$$f(x) = \sum_{i=0}^{r} a_i x^{r-i}, \quad g(y) = \sum_{i=0}^{r} b_i y^{r-i}, \quad a_0 = b_0 = a,$$

$$H(f) = \max_{0 \leqslant i \leqslant r} |a_i|, \quad H(g) = \max_{0 \leqslant i \leqslant r} |b_i|.$$

We have

$$\left|\left(\frac{x}{y}\right)^r - \frac{m}{n}\right| = \left|\frac{m}{n}\right| \frac{\left|\sum_{i=1}^{r} b_i y^{-i} - \sum_{i=1}^{r} a_i x^{-i}\right|}{\left|a_0 + \sum_{i=1}^{r} a_i x^{-i}\right|}..$$

Now, by (6)

$$|x| \geqslant 6H(f), \qquad |y| \geqslant 6H(g) \geqslant 6\,,$$

thus

$$\left|a+\sum_{i=1}^{r} a_i x^{-i}\right| \geqslant 1-H(f)\sum_{i=1}^{r}\big(6H(f)\big)^{-i} > 1-\frac{H(f)}{6H(f)-1} = \frac{5H(f)-1}{6H(f)-1},$$

$$\left|\sum_{i=1}^{r} b_i y^{-i}-\sum_{i=1}^{r} a_i x^{-i}\right| \leqslant H(g)|y|^{-1}\sum_{i=0}^{r-1}6^{-i}+H(f)|x|^{-1}\sum_{i=0}^{r-1}\big(6H(f)\big)^{-i}$$

$$\leqslant \frac{1}{A}\left(\frac{6}{5}+\frac{6H(f)}{6H(f)-1}\right) \leqslant \frac{3}{A}\cdot\frac{5H(f)-1}{6H(f)-1},$$

hence

$$\left|\left(\frac{x}{y}\right)^r-\frac{m}{n}\right| < \frac{3}{A}\left|\frac{m}{n}\right|.$$

Since $A > 6$, $\operatorname{sgn}\dfrac{m}{n} = \operatorname{sgn}\left(\dfrac{x}{y}\right)^r$ and in particular $\dfrac{m}{n} > 0$ if r is even. Put

$$\varepsilon = \begin{cases} 1 & \text{if } r \text{ is odd,} \\ \operatorname{sgn}\dfrac{x}{y} & \text{if } r \text{ is even.} \end{cases}$$

Clearly x/y and $\varepsilon\sqrt[r]{m/n}$ are of the same sign. Applying the mean value theorem we get

$$\left|\frac{x}{y}-\varepsilon\sqrt[r]{\frac{m}{n}}\right| = \frac{1}{r}\left|\left(\frac{x}{y}\right)^r-\frac{m}{n}\right||\theta|^{1/r-1} < \frac{6}{Ar}\sqrt[r]{\left|\frac{m}{n}\right|}$$

(θ is here a mean value between $\left(\dfrac{x}{y}\right)^r$ and $\dfrac{m}{n}$, whence $|\theta| > \dfrac{1}{2}\left|\dfrac{m}{n}\right|$).

Proof of the theorem. Suppose that equation (1) holds but $p\nmid mn$ and none of the inequalities (3) is satisfied. Since $c_r > 6$ the assumptions of Lemma 3 are satisfied with

$$A = c_r\frac{|na^{r-1}\sqrt[r]{m/n}|}{\|na^{r-1}\sqrt[r]{m/n}\|}. \tag{7}$$

Thus for a suitable $\varepsilon = \pm 1$

$$\left|\frac{x}{y}-\varepsilon\sqrt[r]{\frac{m}{n}}\right| < \frac{6}{Ar}\sqrt[r]{\left|\frac{m}{n}\right|}. \tag{8}$$

Let ξ and η be any roots of f and g, respectively. By the assumption ξ and η generate the same normal field K. The numbers $ax-a\xi$ and $ay-a\eta$ are integers in K and by (1)

$$p = \frac{N(ax-a\xi)}{a^{r-1}m} = \frac{N(ay-a\eta)}{a^{r-1}n},$$

where N denotes the norm with respect to K. By Lemma 2 for some $s \leqslant r$

$$\gamma = a^{r-1}n\frac{x-\xi}{y-\eta^{(s)}}$$

is an integer (superscripts denote conjugates). We have

$$\gamma^{(i)} = a^{r-1}n\frac{x-\xi^{(i)}}{y-\eta^{(j)}}, \quad \text{where} \quad \eta^{(j)} = (\eta^{(s)})^{(i)} \quad (1 \leqslant i \leqslant r).$$

Now

$$|\xi^{(i)}| < H(f)+1.$$

Indeed, either

$$|\xi^{(i)}| < 1$$

or

$$0 = |f(\xi^{(i)})| \geqslant |a|\,|\xi^{(i)}|^r - \sum_{j=1}^{r} |a_j|\,|\xi^{(i)}|^{r-j} > |\xi^{(i)}|^r - H(f)|\xi^{(i)r}|\frac{1}{|\xi^{(i)}|-1},$$

whence $|\xi^{(i)}| < H(f)+1$.

Similarly $|\eta^{(j)}| < H(g)+1$.

It follows that

$$\frac{|\xi^{(i)}|}{|x|} < \frac{2}{A} < \frac{1}{3}, \quad \frac{|\eta^{(i)}|}{|y|} < \frac{2}{A} < \frac{1}{3},$$

hence putting

$$\delta_i = \frac{1}{na^{r-1}}\left(\gamma^{(i)} - na^{r-1}\varepsilon\sqrt[r]{\frac{m}{n}}\right)$$

and using (8), we have

$$|\delta_i| = \left|\frac{x-\xi^{(i)}}{y-\eta^{(j)}} - \varepsilon\sqrt[r]{\frac{m}{n}}\right| \tag{9}$$

$$= \left|\varepsilon\sqrt[r]{\frac{m}{n}}\,\frac{(\eta^{(i)}/y)-(\xi^{(i)}/x)}{1-\eta^{(j)}/y} + \frac{1-\xi^{(i)}/x}{1-\eta^{(j)}/y}\left(\frac{x}{y}-\varepsilon\sqrt[r]{\frac{m}{n}}\right)\right|$$

$$< \sqrt[r]{\left|\frac{m}{n}\right|}\left(\frac{6}{A}+2\frac{6}{Ar}\right) = \frac{12}{Ar}\sqrt[r]{\left|\frac{m}{n}\right|}\left(1+\frac{r}{2}\right).$$

On the other hand by Lemma 1 there is in the field K and integral basis $\omega_1 = 1, \omega_2, \ldots, \omega_r$ satisfying (4). We have

$$\gamma^{(i)} = u_1 + \sum_{j=2}^{r} u_j\omega_j^{(i)},$$

where $u_1, \ldots, u_r$ are rational integers.

It follows that

$$(10)\qquad \frac{1}{na^{r-1}}\left(u_1-na^{r-1}\varepsilon\sqrt[r]{\frac{m}{n}}\right)=\frac{1}{\det(\omega_j^{(i)})}\begin{vmatrix}\delta_1 & \omega_2 & \dots & \omega_r\\ \delta_2 & \omega_2^{(2)} & \dots & \omega_r^{(2)}\\ \cdot & \cdot & \cdot & \cdot\\ \delta_r & \omega_2^{(r)} & \dots & \omega_r^{(r)}\end{vmatrix}.$$

Let D be the discriminant of K. By the Hadamard's inequality, by (9), (4) and (7)

$$\left|\frac{1}{\det(\omega_j^{(i)})}\begin{vmatrix}\delta_1 & \omega_2 & \dots & \omega_r\\ \delta_2 & \omega_2^{(2)} & \dots & \omega_r^{(2)}\\ \cdot & \cdot & \cdot & \cdot\\ \delta_r & \omega_2^{(r)} & \dots & \omega_r^{(r)}\end{vmatrix}\right|\leqslant\frac{1}{\sqrt{|D|}}\sqrt{\sum_{j=1}^{r}|\delta_j|^2\prod_{j=2}^{r}\sum_{i=1}^{r}|\omega_j^{(i)}|^2}$$

$$<\frac{1}{\sqrt{|D|}}\cdot\frac{12}{Ar}\sqrt[r]{\left|\frac{m}{n}\right|}\left(1+\frac{r}{2}\right)\sqrt{\prod_{j=1}^{r}\sum_{i=1}^{r}|\omega_j^{(i)}|^2}$$

$$\leqslant\frac{12}{Ar}\sqrt[r]{\left|\frac{m}{n}\right|}\left(1+\frac{r}{2}\right)2r!\,\Gamma\left(1+\frac{r}{2}\right)\pi^{-r/2}$$

$$=\frac{1}{|n|\,|a|^{r-1}}\left\|na^{r-1}\sqrt[r]{\frac{m}{n}}\right\|.$$

Since u_1 is a rational integer this contradicts (10) and the proof is complete.

References

[1] J. W. S. Cassels, *An Introduction to Diophantine Approximation*, Cambridge 1957.

[2] H. Davenport, D. J. Lewis and A. Schinzel, *Equations of the form* $f(x)=g(y)$, Quart. J. Math. (2) 12 (1961), pp. 304-312.

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

Reçu par la Rédaction le 30. 6. 1965