ACTA ARITHMETICA
XLIV (1984)

On a diophantine equation connected with the Fermat equation.

by

B. Brindza (Debrecen)

1. Introduction. Let $p > 2$ be a prime. In 1946 Inkeri [3] proved that there exists at most a finite number of positive integer triplets (x, y, z) which satisfy the conditions

$$x^p + y^p = z^p, \quad (x, y, z) = 1, \tag{1}$$

and for which at least one of the differences $|x-y|$, $z-x$, $z-y$ is less than a given positive number M. That (1) has only a finite number of solutions x, y and z with $y-x = v$ for v a fixed positive integer, was proved by Everett [2] by means of Roth's famous theorem [7] on approximation of algebraic numbers. Recently Stewart [8] and Inkeri and van der Poorten [5] (in the case where n is a prime) have shown that, for any positive number C_0, all positive integer solutions $x, y, z > 1$, $n > 2$, of the equation

$$x^n + y^n = z^n \quad \text{with} \quad |x-y| < C_0$$

satisfy $\max\{n, x, y, z\} < C$, where C is an effectively computable constant depending only on C_0. Their proofs involve the Gelfond–Baker method.

In [4] Inkeri studied the equation

$$h^p(x) + g^p(x) = z^p. \tag{2}$$

He proved that if h and g are distinct non-constant polynomials with integer coefficients which satisfy the conditions

$$D(g - \zeta^r h) \neq 0 \quad (r = 0, 1, \ldots, p-1); \qquad R(g, h) \neq 0,$$

where $D(\cdot)$ is the discriminant, $R(\cdot, \cdot)$ the resultant and ζ a primitive pth root of unity, then equation (2) has at most a finite number of solutions in rational integers x, z and all these solutions can effectively be determined. His proof depends also on the Gelfond–Baker method.

In [1] we have obtained an effective version of the well-known LeVeque's theorem [6] on the hyperelliptic equation. Our result enables us

to prove the following improvements of the later theorems of Inkeri and of Stewart.

THEOREM 1. *Let $n > 2$ be a rational integer, and let $G_0(X)$ and $H_0(X)$ be nonproportional,(1) non-zero polynomials with rational integer coefficients. Then all solutions $x, z \in \mathbf{Z}$ of the equation*

$$G_0^n(x) + H_0^n(x) = z^n \tag{3}$$

satisfy $\max\{|x|, |z|\} < C_1$ where C_1 is an effectively computable constant depending only on n, $G_0(X)$ and $H_0(X)$.

THEOREM 2. *Let $G(X)$ and $H(X)$ be nonproportional, non-zero polynomials with positive integer coefficients. Suppose that the leading coefficients of $G(X)$, $H(X)$ are equal. Then all positive integer solutions n, x, z with $n > 2$ of the equation*

$$G^n(x) + H^n(x) = z^n \tag{4}$$

satisfy $\max\{n, x, z\} < C_2$ where C_2 is an effectively computable constant depending only on $G(X)$ and $H(X)$.

In the proof of Theorem 1 we shall use the following effective version of a well-known theorem of LeVeque [6].

LEMMA 1. *Let $P(X) \in \mathbf{Z}[X]$,*

$$P(X) = a_0 X^N + \ldots + a_N = a_0 \prod_{i=1}^{k} (X - \alpha_i)^{r_i},$$

with $a_0 \neq 0$, $N > 0$ and $\alpha_i \neq \alpha_j$ for $i \neq j$. Let $0 \neq b \in \mathbf{Z}$, $2 \leqslant m \in \mathbf{Z}$ and define $t_i = m/(m, r_i)$. Suppose that $\{t_1, \ldots, t_k\}$ is not a permutation of the k-tuples

$$\text{(a) } \{t, \underbrace{1, \ldots, 1}\}, t \geqslant 1, \quad \text{and} \quad \text{(b) } \{2, 2, 1, \ldots, 1\}.$$

Then all solutions $x, y \in \mathbf{Z}$ of the equation

$$P(x) = by^m$$

satisfy $\max\{|x|, |y|\} < C_3$ where C_3 is an effectively computable constant depending only on $P(X)$, b and m.

Proof. See B. Brindza [1]. We note that the proof of this lemma is also based on the Gelfond–Baker method.

Proof of Theorem 1. It is well known that the equation

$$x^{2k} + y^{2k} = z^{2k}, \quad (x, y, z, k \in N)$$

has no solutions for $k > 1$. If $p \mid n$, where $p > 2$ is a prime, then we can write

$$[G_0^{n/p}(x)]^p + [H_0^{n/p}(x)] = [z^{n/p}]^p.$$

(1) i.e. $G_0(x)/H_0(x) \notin Q$.

Since (1) is not soluble if $p = 3$ or $p = 5$, we can assume that $p > 5$. Put $G(X) = G_0^{n/p}(X)$, $H(X) = H_0^{n/p}(X)$ and

$$L(X) = G^p(X) + H^p(X) = A \prod_{i=1}^{k} (X - X_i)^{r_i},$$

with $X_i \neq X_j$ for $i \neq j$. Further, put $t_i = p/(p, r_i)$ for $i = 1, \ldots, k$. In view of Lemma 1 it will be sufficient to show that $\{t_1, \ldots, t_k\}$ is not a permutation of any of the above k-tuples (a), (b). The case (b) is impossible, because $t_1, \ldots, t_k$ are odd. Suppose that the case (a) holds. Then we can write

$$L(X) = (X - \alpha)^q F_1^p(X),$$

where $q \geqslant 0$ and $F_1(X) \in \mathbf{C}[X]$. Let $q = ap + b$, where $b \in \{0, \ldots, p-1\}$ and a is a non-negative integer. We have now

$$L(X) = (X - \alpha)^b F_2^p(X), \quad \text{where} \quad F_2(X) = F_1(X)(X - \alpha)^a.$$

Let $K(X)$ be the greatest common divisor of $G(X)$ and $H(X)$ in $\mathbf{C}[X]$. We may suppose that $K(X)$ is a monic polynomial. Then $K(X) \in \mathbf{Q}[X]$ and

$$G(X) = K(X) G_1(X), \quad H(X) = K(X) H_1(X),$$

where $G_1(X)$, $H_1(X) \in \mathbf{Q}[X]$. Since

$$K^p(X) \mid (X - \alpha)^b F_2^p(X)$$

and $b < p$, we can write $F_2(X) = K(X) F(X)$, where $F(X) \in \mathbf{C}[X]$. Put

$$M(X) = G_1^p(X) + H_1^p(X) = (X - \alpha)^b F^p(X). \tag{5}$$

It is clear that $F^{p-1}(X) \mid M'(X)$ and

$$F^{p-1}(X) \mid M'(X) G_1(X) - pM(X) G_1'(X) = pH_1^{p-1}(X)[-H_1(X) G_1'(X) + H_1'(X) G_1(X)].$$

Since $G_1(X)$ and $H_1(X)$ are relatively prime, we find that $F(X)$ and $H_1(X)$ are also relatively prime. Then we get

$$F^{p-1}(X) \mid H_1'(X) G_1(X) - H_1(X) G_1'(X) = G_1^2(X)\big(H_1(X)/G_1(X)\big)' \not\equiv 0.$$

We may suppose without loss of generality that $\deg H_1 \leqslant \deg G_1 = n$. Then

$$(p-1) \deg F \leqslant \deg(H_1' G_1 - H_1 G_1') < 2n. \tag{6}$$

We are now going to prove that $\deg M \geqslant n(p-1)$. If

$$\deg H_1 < \deg G_1,$$

then this is trivial, because $\deg M = np$. We may assume that

$$\deg H_1 = \deg G_1 = n.$$

Then

$$H_1(X) = a_n X^n + \ldots + a_1 X + a_0$$

and

$$G_1(X) = b_n X^n + \ldots + b_1 X + b_0,$$

where $a_n \cdot b_n \neq 0$ and $a_i, b_i \in Q$ for $i = 0, 1, \ldots, n$. Let

$$i_0 \doteq \max_{a_i + b_i \neq 0} \{i\}.$$

If $i_0 = n$, then $\deg M = np > n(p-1)$. Let now $i_0 < n$ and

$$A(X) = a_n X^n + \ldots + a_{i_0+1} X^{i_0+1},$$

$$B(X) = a_{i_0} X^{i_0} + \ldots + a_0,$$

$$C(X) = b_{i_0} X^{i_0} + \ldots + b_0.$$

Then we have $H_1 = A + B$ and $G_1 = -A + C$. Further,

$$H_1^p + G_1^p = A^{p-1}(B+C)\binom{p}{1} + A^{p-2}(B^2 - C^2)\binom{p}{2} + \ldots$$

It is easy to see that

$$\deg\{A^{p-1}(B+C)\} = n(p-1) + i_0,$$

because $a_n^{p-1}(a_{i_0} + b_{i_0}) \neq 0$. If $j > 1$, then

$$\deg\{A^{p-j}(B^j \pm C^j)\} \leqslant n(p-j) + i_0 j < n(p-1) + i_0,$$

so we have

$$\deg M = n(p-1) + i_0 \geqslant n(p-1). \tag{7}$$

We shall now show that $\deg F > 0$. Supposing the contrary, we can write

$$p > b = \deg(X-\alpha)^b F^p(X) = \deg M \geqslant n(p-1).$$

From this it follows that $n = 1$, $b = p-1$ and $a_1 + b_1 = 0$. Then by (5) we have

$$(a_1 X + a_0)^p + (-a_1 X + b_0)^p = d(X-\alpha)^{p-1} \qquad (d \in C).$$

The derivatives take now the form

$$p a_1 [(a_1 X + a_0)^{p-1} - (-a_1 X + b_0)^{p-1}] = d(p-1)(X-\alpha)^{p-2}.$$

Then we get

$$(X-\alpha) | (a_1 X + a_0)^p - (a_1 X + a_0)(-a_1 X + b_0)^{p-1},$$

and so

$$(X-\alpha) | (a_1 X + a_0)^p + (-a_1 X + b_0)^p - \{(a_1 X + a_0)^p - (a_1 X + a_0)(-a_1 X + b_0)^{p-1}\} = (a_0 + b_0)(-a_1 X + b_0)^{p-1},$$

that is, $(X-\alpha) | -a_1 X + b_0$ and $(X-\alpha) | a_1 X + a_0$. But this is a contradiction which proves that

$$\deg F > 0. \tag{8}$$

Thus from (8), (7) and (6) we obtain

$$2p \deg F \geqslant p \deg F + p > \deg M \geqslant n(p-1) > \tfrac{1}{2}(p-1)^2 \deg F,$$

whence $2p > \frac{1}{2}(p-1)^2$ which is impossible if $p > 5$.

Consequently, we can apply Lemma 1 and we get $\max\{|x|, |y|\} < C$, where C is an effectively computable constant depending only on p, $G_0(X)$ and $H_0(X)$. This completes the proof of Theorem 1.

In the proof of Theorem 2 we shall use the following lemma.

LEMMA 2 (C. L. Stewart [8]). *If*

$$0 < y - x < C_0 z^{1 - 1/\sqrt{n}}$$

for some positive number C_0, and if

$$x^n + y^n = z^n \qquad (x, y, z, n \in N)$$

then n is less than C', a number which is effectively computable in terms of C_0.

Proof. See C. L. Stewart [8].

Proof of Theorem 2. Let

$$G(X) = a_g X^g + \ldots + a_1 X + a_0$$

and

$$H(X) = b_h X^h + \ldots + b_1 X + b_0$$

with non-negative integers $a_g, \ldots, a_0, b_h, \ldots, b_0$. Further, let

$$\mathcal{G} = \max_{0 \leqslant j \leqslant g} a_j.$$

We shall now distinguish the following cases:

(A) $\deg G \neq \deg H$;

(B) $g = \deg G = \deg H$.

Consider first the case (A). We may suppose without loss of generality that $\deg G < \deg H$. Then

$$G^n(x) < [(g+1)\mathcal{G}x^g]^n \leqslant [(g+1)\mathcal{G}x^{h-1}]^n$$

for any $x \in N$. Let now x, z, n be an arbitrary solution of (4) with $n > 2$

and write $G(x)=X$, $H(x)=Y$. Suppose that $x \leqslant [(g+1)\mathscr{G}]^{2h}$, and put $G([(g+1)\mathscr{G}]^{2h})=K$. Then $X \leqslant K$ and we have

$$Y < [(Y+1)^n - Y^n]^{1/(n-1)} \leqslant (z^n - Y^n)^{1/(n-1)} = X^{n/(n-1)} < K^2,$$

and $z < X+Y < K+K^2$. Moreover,

$$1 = \left(\frac{X}{z}\right)^n + \left(\frac{Y}{z}\right)^n \leqslant \left(\frac{X}{X+1}\right)^n + \left(\frac{Y}{Y+1}\right)^n$$
$$< \left(\frac{K}{K+1}\right)^n + \left(\frac{K^2}{K^2+1}\right)^n < 2\left(1-\frac{1}{K^2+1}\right)^n,$$

and so $n < K^2+1$. Therefore we can restrict ourselves to the case where

$$x > [(g+1)\mathscr{G}]^{2h}.$$

If $n < 2h$, then we have only to apply Theorem 1. We may assume that $n \geqslant 2h$. Then we can write

$$H^n(x) < H^n(x)+G^n(x) < H^n(x)+[(g+1)\mathscr{G}x^{h-1}]^n$$
$$< H^n(x)+x^{n(h-1)}[(g+1)\mathscr{G}]^{2h(n-h)} < H^n(x)+x^{(h-1)n}x^{n-h}$$
$$= H^n(x)+x^{h(n-1)} \leqslant H^n(x)+H^{n-1}(x) < (H(x)+1)^n,$$

whence $H(x) < z < H(x)+1$, which gives a contradiction.

Let us return to the case (B). Define the index i_0 by

$$i_0 = \max_{a_i \neq b_i} \{i\}.$$

We may suppose that $b_{i_0} > a_{i_0}$ and $x > \mathscr{G}+1$. Then

$$H(x)-G(x) = x^{i_0}\left(b_{i_0}-a_{i_0}+\frac{1}{x}(b_{i_0-1}-a_{i_0-1})+\ldots+\frac{1}{x^{i_0}}(b_0-a_0)\right)$$
$$\geqslant x^{i_0}[(b_{i_0}-a_{i_0})-a_{i_0-1}/x-\ldots-a_0/x^{i_0}]$$
$$> x^{i_0}(b_{i_0}-a_{i_0}-\mathscr{G}/x-\ldots-\mathscr{G}/x^g) > x^{i_0}(1-\mathscr{G}/(x-1)) > 0$$

and

$$H(x)-G(x) < b_{g-1}x^{g-1}+\ldots+b_0 \leqslant (b_{g-1}+\ldots+b_0)x^{g-1} = dx^{g-1},$$

where $d = b_{g-1}+\ldots+b_0$. If

(i) $$g^2 < n$$

and

(ii) $$H(x)-G(x) \geqslant dz^{1-1/\sqrt{n}},$$

then

$$x^g \leqslant a_g x^g \leqslant \tfrac{1}{2}(G(x)+H(x)) \leqslant \left[\tfrac{1}{2}(G^n(x)+H^n(x))\right]^{1/n}$$
$$= \sqrt[n]{\frac{z^n}{2}} < t \leqslant \left[\frac{1}{a}(H(x)-G(x))\right]^{1/(1-1/\sqrt{n})} < x^{(g-1)/(1-1/\sqrt{n})} < x^g.$$

This is impossible, so $g^2 \geqslant n$ or $H(x)-G(x) < dz^{1-1/\sqrt{n}}$. By Lemma 2 we have that

$$n < \max\{g^2, C'(d)\} = C(H, G)$$

and, by applying Theorem 1, that x, z are bounded. This proves Theorem 2.

I would like to thank K. Győry and the referee for their valuable remarks.

References

[1] B. Brindza, *On S-integral solutions of the equation $f(x)=y^m$*, Acta Math. Acad. Sci. Hungar., to appear.

[2] C. J. Everett, *Fermat's conjecture, Roth's theorem, Pythagorean triangles and Pell's equation*, Duke Math. J. 40 (1973), pp. 801–804.

[3] K. Inkeri, *Untersuchungen über die Fermatsche Vermutung*, Ann. Acad. Sci. Fenn. Ser. AI, 33 (1946), pp. 1–60.

[4] – *A note on Fermat's conjecture*, Acta Arith. 29 (1976), pp. 251–256.

[5] K. Inkeri, A. J. van der Poorten, *Some remarks on Fermat's conjecture*, ibid. 36 (1980), pp. 107–111.

[6] W. J. LeVeque, *On the equation $y^m = f(x)$*, ibid. 9 (1964), pp. 209–219.

[7] K. F. Roth, *Rational approximations to algebraic numbers*, Mathematika 2 (1955), pp. 1–20.

[8] C. L. Stewart, *A note on the Fermat equation*, ibid. 24 (1977), pp. 130–132.

MATHEMATICAL INSTITUTE
KOSSUTH LAJOS UNIVERSITY
4010 Debrecen 12,
Hungary

Received on 21.3.1983
and in revised form on 15.9.1983 (1347)