ACTA ARITHMETICA
110.2 (2003)

On the Diophantine equation $F(x) = G(y)$

by

SZ. TENGELY (Leiden)

1. Introduction. Consider a polynomial

$$P(X,Y) = \sum_{i=0}^{m}\sum_{j=0}^{n} a_{i,j}X^iY^j,$$

where $a_{i,j} \in \mathbb{Z}$ and $m,n > 0$, which is irreducible in $\mathbb{Q}[X,Y]$. We recall Runge's result [14] on Diophantine equations: if there are infinitely many $(x,y) \in \mathbb{Z}^2$ such that $P(x,y) = 0$ then the following conditions hold:

- $a_{i,n} = a_{m,j} = 0$ for all non-zero i and j,
- for every term $a_{i,j}X^iY^j$ of P one has $ni + mj \le mn$,
- the sum of all monomials $a_{i,j}X^iY^j$ of P for which $ni + mj = mn$ is up to a constant factor a power of an irreducible polynomial in $\mathbb{Z}[X,Y]$,
- there is only one system of conjugate Puiseux expansions at $x = \infty$ for the algebraic function $y = y(x)$ defined by $P(x,y) = 0$.

If at least one of the above conditions does not hold, we say that P satisfies *Runge's condition.* The last two conditions have been sharpened by Schinzel [15] and by Ayad [1]. Runge's method of proof is effective, that is, it yields computable upper bounds for the sizes of the integer solutions to these equations. Using this method upper bounds were obtained by Hilliker and Straus [8] and by Walsh [20]. Grytczuk and Schinzel [6] applied a method of Skolem [17] based on elimination theory to obtain upper bounds for the solutions. Laurent and Poulakis [9] obtained an effective version of Runge's theorem over number fields by using interpolation determinants. Their result extends Walsh's result which holds for the field of rational numbers.

If $P(X,Y) = Y^n - R(X)$ is irreducible in $\mathbb{Q}[X,Y]$, R is monic and $\gcd(n, \deg R) > 1$, then P satisfies Runge's condition. Masser [11] considered the equation $y^n = P(x)$ in the special case $n = 2, \deg R = 4$, and Walsh [20] gave a bound for the general case.

2000 *Mathematics Subject Classification*: Primary 11D41; Secondary 11D25, 11Y50.
Key words and phrases: Diophantine equations, Runge's method.

In [13] Poulakis described an elementary method for computing the solutions of the equation $y^2 = R(x)$, where R is a monic quartic polynomial which is not a perfect square. Szalay [18] generalized the result of Poulakis by giving an algorithm for solving the equation $y^2 = R(x)$ where R is a monic polynomial of even degree. Recently, Szalay [19] established a generalization to equations $y^p = R(x)$, where R is a monic polynomial and $p \mid \deg R$.

Several authors (for references see e.g. [2], [3], [5]) have studied the question if the equation $F(x) = G(y)$ has finitely or infinitely many solutions in $x, y \in \mathbb{Z}$, where F, G are polynomials with rational coefficients. Bilu and Tichy [3] completely classified those polynomials $F, G \in \mathbb{Q}[X]$ for which the equation $F(x) = G(y)$ has infinitely many integer solutions. The method used in these papers is ineffective so they do not lead to algorithms to find all the solutions.

2. Result. We deal with the Diophantine equation

$$F(x) = G(y), \tag{1}$$

where $F, G \in \mathbb{Z}[X]$ are monic polynomials with $\deg F = n$, $\deg G = m$, such that $F(X) - G(Y)$ is irreducible in $\mathbb{Q}[X,Y]$ and $\gcd(n,m) > 1$. Then Runge's condition is satisfied. Let $d > 1$ be a divisor of $\gcd(n,m)$. Without loss of generality we can assume $m \geq n$. We denote by $H(\cdot)$ the classical height, that is, the maximal absolute value of the coefficients.

In the following theorem we extend a result of Walsh [20] concerning superelliptic equations for which Runge's condition is satisfied.

Theorem. *If $(x,y) \in \mathbb{Z}^2$ is a solution of (1) where F and G satisfy the above mentioned conditions then*

$$\max\{|x|,|y|\} \leq d^{2m^2/d-m}(m+1)^{3m/(2d)}\left(\frac{m}{d}+1\right)^{3m/2}(h+1)^{(m^2+mn+m)/d+2m},$$

where $h = \max\{H(F), H(G)\}$.

In the special case $G(Y) = Y^m$ Walsh [20, Theorem 3] obtained a far better result for the integer solutions of (1), viz.

$$|x| \leq d^{2n-d}\left(\frac{n}{d}+2\right)^d (h+1)^{n+d}.$$

In [20, Corollary of Theorem 1] Walsh has shown that if $P(X,Y)$ satisfies Runge's condition, then all integer solutions of the Diophantine equation $P(X,Y) = 0$ satisfy

$$\max\{|x|,|y|\} < (2m)^{18m^7} h^{12m^6},$$

where $m = \deg_Y P$ and $h = H(P)$. Grytczuk and Schinzel [6, Corollary] have stated that if $P(X,Y)$ satisfies Runge's condition, then

$$\max\{|x|,|y|\} < \begin{cases} (45H(P))^{250} & \text{if } m = 2, \\ ((4m^3)^{8m^2} H(P))^{96m^{11}} & \text{if } m > 2. \end{cases}$$

Here we cited corollaries from [6] and from [20] because it is easier to compare these results with the Theorem. We note that in the special case (1) our theorem gives a far better upper bound.

We will need the concept of resultant. The *resultant* of two polynomials $f, g \in \mathbb{C}[X,Y]$ of degrees r, t in Y, respectively, say $f(X,Y) = a_0(X)Y^r + a_1(X)Y^{r-1} + \ldots + a_r(X)$ with $a_0(X) \not\equiv 0$ and $g(X,Y) = b_0(X)Y^t + b_1(X)Y^{t-1} + \ldots + b_t(X)$ with $b_0(X) \not\equiv 0$, is defined to be the following determinant of order $r+t$:

$$\operatorname{Res}_Y(f(X,Y), g(X,Y)) = \begin{vmatrix} a_0(X) & \ldots & \ldots & a_r(X) & & \\ & \ddots & & & \ddots & \\ & & a_0(X) & \ldots & \ldots & a_r(X) \\ b_0(X) & \ldots & b_t(X) & & & \\ & \ddots & & \ddots & & \\ & & \ddots & & \ddots & \\ & & & b_0(X) & \ldots & b_t(X) \end{vmatrix}.$$

In the proof of the Theorem we use the following result.

LEMMA. *There exist Puiseux expansions*

$$u(X) = \sum_{i=-n/d}^{\infty} f_i X^{-i} \quad \textit{and} \quad v(X) = \sum_{i=-m/d}^{\infty} g_i X^{-i}$$

of the algebraic functions U, V defined by $U^d = F(X)$, $V^d = G(X)$, such that $d^{2(n/d+i)-1} f_i \in \mathbb{Z}$ for all $i > -n/d$, $d^{2(m/d+i)-1} g_i \in \mathbb{Z}$ for all $i > -m/d$, and $f_{-n/d} = g_{-m/d} = 1$. Furthermore $|f_i| \le (H(F)+1)^{n/d+i+1}$ for $i \ge -n/d$ and $|g_i| \le (H(G)+1)^{m/d+i+1}$ for $i \ge -m/d$.

Proof. See [20, pp. 169–170]. ∎

Proof of the Theorem. Let (1) admit a solution $(x,y) \in \mathbb{Z}^2$. Applying the lemma we write

$$F(X) = \Big(\sum_{i=-n/d}^{\infty} f_i X^{-i}\Big)^d, \tag{2}$$

$$G(Y) = \Big(\sum_{i=-m/d}^{\infty} g_i Y^{-i}\Big)^d, \tag{3}$$

where $|f_i|$ and $|g_i|$ are bounded as in the lemma. It follows from the lemma that

$$\left|\frac{d^{2m/d-1}f_k}{t^k}\right| < \frac{1}{2^{k+1}} \quad \text{for} \quad |t| > 4d^{2m/d-1}(H(F)+1)^{n/d+2} =: x_0.$$

Thus we have

$$\Big|\sum_{i=1}^{\infty} d^{2m/d-1} f_i t^{-i}\Big| < 1/2.$$

Similarly if $|t| > 4d^{2m/d-1}(H(G)+1)^{m/d+2} =: y_0$ then

$$\Big|\sum_{i=1}^{\infty} d^{2m/d-1} g_i t^{-i}\Big| < 1/2.$$

Since $F(x) = G(y)$, we have $u(x)^d - v(y)^d = 0$, that is,

$$(u(x)-v(y))(u(x)^{d-1} + u(x)^{d-2}v(y) + \ldots + v(y)^{d-1}) = 0 \quad \text{if } d \text{ is odd},$$
$$(u(x)^2-v(y)^2)(u(x)^{d-2} + u(x)^{d-4}v(y)^2 + \ldots + v(y)^{d-2}) = 0 \quad \text{if } d \text{ is even}.$$

First assume that d is odd and

$$u(x)^{d-1} + u(x)^{d-2}v(y) + \ldots + v(y)^{d-1} = 0. \tag{4}$$

Suppose $v(y) \neq 0$. In this case we can divide (4) by $v(y)^{d-1}$ to get

$$\left(\frac{u(x)}{v(y)}\right)^{d-1} + \left(\frac{u(x)}{v(y)}\right)^{d-2} + \ldots + \left(\frac{u(x)}{v(y)}\right) + 1 = 0.$$

It suffices to observe that $(t^k - 1)/(t-1)$ has no real root if k is odd. Thus $v(y) = 0$ and $u(x) = 0$.

Now assume that d is even. Note that

$$u(x)^{d-2} + u(x)^{d-4}v(y)^2 + \ldots + v(y)^{d-2} = 0$$

can only happen if $u(x) = v(y) = 0$. By the above considerations we have

$$u(x) = \begin{cases} v(y) & \text{if } d \text{ is odd}, \\ \pm v(y) & \text{if } d \text{ is even}. \end{cases}$$

Let $|x| > x_0$ and $|y| > y_0$. Then from

$$0 = |u(x) \pm v(y)| = \Big|\sum_{i=-n/d}^{\infty} f_i x^{-i} \pm \sum_{i=-m/d}^{\infty} g_i y^{-i}\Big|$$

we obtain

$$\Big|\sum_{i=-n/d}^{0} d^{2m/d-1} f_i x^{-i} \pm \sum_{i=-m/d}^{0} d^{2m/d-1} g_i y^{-i}\Big| < 1.$$

Since $d^{2m/d-1}f_i \in \mathbb{Z}$ for $i = -n/d, \ldots, 0$ and $d^{2m/d-1}g_i \in \mathbb{Z}$ for $i = -m/d, \ldots, 0$, we have

$$Q(x,y) := \sum_{i=0}^{n/d} d^{2m/d-1} f_{-i} x^i \pm \sum_{i=0}^{m/d} d^{2m/d-1} g_{-i} y^i = 0.$$

Hence x satisfies

$$\mathrm{Res}_Y(F(X) - G(Y), Q(X,Y)) = 0$$

and y satisfies

$$\mathrm{Res}_X(F(X) - G(Y), Q(X,Y)) = 0.$$

We note that these resultants are non-zero polynomials since $F(X) - G(Y)$ is irreducible over $\mathbb{Q}[X,Y]$ of degree n in X and of degree m in Y, whereas $\deg_X Q(X,Y) = n/d$ and $\deg_Y Q(X,Y) = m/d$. By applying Lemma 1 of Grytczuk and Schinzel [6] we obtain the following bounds for $|x|$ and $|y|$:

$$\begin{aligned} |x| &\le (h(n+1)\sqrt{m+1})^{m/d} \\ &\quad \times \left(d^{2m/d-1}(h+1)^{(n+m)/d+2}\left(\frac{n}{d}+1\right)\sqrt{\frac{m}{d}+1}\right)^m, \\ |y| &\le (h(m+1)\sqrt{n+1})^{n/d} \\ &\quad \times \left(d^{2m/d-1}(h+1)^{(n+m)/d+2}\left(\frac{m}{d}+1\right)\sqrt{\frac{n}{d}+1}\right)^n. \end{aligned} \tag{5}$$

By combining the bounds x_0, y_0 and (5) obtained for $|x|, |y|$ we get the bound given in the Theorem. ∎

3. Description of the algorithm. In this section we give an algorithm to find all integral solutions of concrete Diophantine equations of the form (1) by adapting the proof of the Theorem. Let p be the smallest prime divisor of $\gcd(m,n)$. Let $u(X) = \sum_{i=-n/p}^{\infty} f_i X^{-i}$ and $v(X) = \sum_{i=-m/p}^{\infty} g_i X^{-i}$ be the Puiseux expansions at ∞ of $u(X)^p = F(X), v(X)^p = G(X)$, respectively, with $f_{-n/p} = g_{-m/p} = 1$. We define $\widehat{f}$ and $\widehat{g}$ by

$$\begin{aligned} F(X) &= \Big(\sum_{i=-n/p}^{n-n/p} f_i X^{-i}\Big)^p + \sum_{i=1}^{np-n} \widehat{f}_i X^{-i}, \\ G(Y) &= \Big(\sum_{i=-m/p}^{m-m/p} g_i Y^{-i}\Big)^p + \sum_{i=1}^{mp-m} \widehat{g}_i Y^{-i}. \end{aligned} \tag{6}$$

We will use parameters $a_i, b_i \in \mathbb{R}_+$ for $i = 1, 2$, to be chosen later. Define

$$P_{a_1}(X) = a_1 X^{np-n} + \sum_{i=0}^{np-n-1} \widehat{f}_{np-n-i} X^i,$$

$$R_{a_1}(X) = a_1 X^{np-n} - \sum_{i=0}^{np-n-1} \widehat{f}_{np-n-i} X^i$$

and set $S(a_1) = \{r \in \mathbb{R} \mid P_{a_1}(r) = 0 \text{ or } R_{a_1}(r) = 0\}$. One can apply for example the method of Collins and Akritas [4], based on Descartes' rule of signs, or Schönhage's algorithm [16], which is implemented in Magma, to obtain the set $S(a_1)$. Denote by $I(a_1)$ the integers in the interval $[\min S(a_1), \max S(a_1)]$ if $S(a_1) \neq \emptyset$, otherwise $I(a_1) = \emptyset$. Since $np - n$ is even, we see that if $t \notin I(a_1)$ then $P_{a_1}(t) > 0$ and $R_{a_1}(t) > 0$, hence $|\sum_{i=1}^{np-n} \widehat{f}_i t^{-i}| < a_1$. For a_2 define

$$P_{a_2}(X) = a_2 X^{n-n/p} + \sum_{i=0}^{n-n/p-1} f_{n-n/p-i} X^i,$$

$$R_{a_2}(X) = a_2 X^{n-n/p} - \sum_{i=0}^{n-n/p-1} f_{n-n/p-i} X^i$$

and set $S(a_2) = \{r \in \mathbb{R} \mid P_{a_2}(r) = 0 \text{ or } R_{a_2}(r) = 0\}$. Denote by $I(a_2)$ the integers in $[\min S(a_2), \max S(a_2)]$ if $S(a_2) \neq \emptyset$, otherwise $I(a_2) = \emptyset$. It is easy to see that if $t \notin I(a_2)$ then $P_{a_2}(t) > 0$ and $R_{a_2}(t) > 0$, hence $|\sum_{i=1}^{n-n/p} \widehat{f}_i t^{-i}| < a_2$. In a similar way we define the sets $I(b_1)$ and $I(b_2)$. Suppose

$$\Big|\sum_{i=1}^{np-n} \widehat{f}_i x^{-i}\Big| < a_1, \qquad \Big|\sum_{i=1}^{n-n/p} f_i x^{-i}\Big| < a_2,$$

$$\Big|\sum_{i=1}^{mp-m} \widehat{g}_i y^{-i}\Big| < b_1, \qquad \Big|\sum_{i=1}^{m-m/p} g_i y^{-i}\Big| < b_2.$$

By (1),

$$\Big(\sum_{i=-n/p}^{n-n/p} f_i x^{-i} - \sum_{i=-m/p}^{m-m/p} g_i y^{-i}\Big)\Big(\sum_{k=0}^{p-1}\Big(\sum_{i=-n/p}^{n-n/p} f_i x^{-i}\Big)^{p-k-1}\Big(\sum_{i=-m/p}^{m-m/p} g_i y^{-i}\Big)^k\Big) = \sum_{i=1}^{mp-m} \widehat{g}_i y^{-i} - \sum_{i=1}^{np-n} \widehat{f}_i x^{-i}.$$

Hence at least one of the following inequalities holds:

$$\Big|\sum_{i=-n/p}^{n-n/p} f_i x^{-i} - \sum_{i=-m/p}^{m-m/p} g_i y^{-i}\Big| < \sqrt[p]{a_1 + b_1}, \tag{7}$$

$$(8) \qquad \Big|\sum_{k=0}^{p-1}\Big(\sum_{i=-n/p}^{n-n/p} f_i x^{-i}\Big)^{p-k-1}\Big(\sum_{i=-m/p}^{m-m/p} g_i y^{-i}\Big)^{k}\Big| < \sqrt[p]{(a_1+b_1)^{p-1}}.$$

Denote by D the least common multiple of the denominators of f_i for $i \in \{-n/p,\dots,-1\}$, of g_i for $i \in \{-m/p,\dots,-1\}$ and of $f_0 - g_0$. Similarly denote by $\widehat{D}$ the least common multiple of the denominators of f_i for $i \in \{-n/p,\dots,-1\}$, of g_i for $i \in \{-m/p,\dots,-1\}$ and of f_0+g_0. Then from (7) we get

$$(9) \qquad \Big|\sum_{i=-n/p}^{0} Df_i x^{-i} - \sum_{i=-m/p}^{0} Dg_i y^{-i}\Big| < D(\sqrt[p]{a_1+b_1} + a_2 + b_2) =: B_1,$$

and from (8) in the case $p = 2$ we obtain

$$(10) \qquad \Big|\sum_{i=-n/p}^{0} \widehat{D}f_i x^{-i} + \sum_{i=-m/p}^{0} \widehat{D}g_i y^{-i}\Big| < \widehat{D}(\sqrt[p]{a_1+b_1} + a_2 + b_2) =: \widehat{B}_1.$$

If $(x,y) \in \mathbb{Z}^2$ is a solution of (1) and (9) then there is an integer k with $|k| < B_1$ such that x satisfies

$$R_k(X) := \mathrm{Res}_Y\Big(F(X) - G(Y), \sum_{i=0}^{n/p} Df_{-i}X^i - \sum_{i=0}^{m/p} Dg_{-i}Y^i - k\Big) = 0.$$

If $p = 2$ and x is a solution of (1) and (10), then there is an integer $\widehat{k}$ with $|\widehat{k}| < \widehat{B}_1$ such that x satisfies

$$\widehat{R}_{\widehat{k}}(X) := \mathrm{Res}_Y\Big(F(X) - G(Y), \sum_{i=0}^{n/p} \widehat{D}f_{-i}X^i + \sum_{i=0}^{m/p} \widehat{D}g_{-i}Y^i - \widehat{k}\Big) = 0.$$

Choose integers FL, FU, GL, GU such that $I(a_1) \cup I(a_2) \subset [FL, FU]$ and $I(b_1) \cup I(b_2) \subset [GL, GU]$. If $p = 2$ then we can apply the above arguments to conclude that each solution $(x,y) \in \mathbb{Z}^2$ of (1) satisfies at least one of the following equations:

$$(11) \qquad R_k(X) = 0 \qquad \text{for some } k \text{ with } |k| < B_1,$$

$$(12) \qquad \widehat{R}_k(X) = 0 \qquad \text{for some } k \text{ with } |k| < \widehat{B}_1,$$

$$(13) \qquad G(Y) = F(k) \qquad \text{for some } k \in [FL, FU],$$

$$(14) \qquad F(X) = G(k) \qquad \text{for some } k \in [GL, GU].$$

Suppose that p is odd and $(x,y) \in \mathbb{Z}^2$ is a solution of (1) such that x and y satisfy (8). If $\sum_{i=-m/p}^{m-m/p} g_i y^{-i} = 0$ then y is a zero of the polynomial $\sum_{i=0}^{m} D_1 g_{-m+m/p-i} Y^i$, where D_1 is the least common multiple of the denominators of the coefficients g_i for $i = -m/p,\dots,m-m/p$. If

$\sum_{i=-m/p}^{m-m/p} g_i y^{-i} \neq 0$ and $\sqrt[p]{(a_1+b_1)^{p-1}}/(\sum_{i=-m/p}^{m-m/p} g_i y^{-i})^{p-1} < 1/2$ then from (8) we obtain

$$\frac{1}{2} \leq |t^{p-1} + t^{p-2} + \ldots + 1| < \frac{\sqrt[p]{(a_1+b_1)^{p-1}}}{(\sum_{i=-m/p}^{m-m/p} g_i y^{-i})^{p-1}} < \frac{1}{2},$$

where $t = \sum_{i=-n/p}^{n-n/p} f_i x^{-i} / \sum_{i=-m/p}^{m-m/p} g_i y^{-i}$, a contradiction. It remains to deal with the inequality

$$\frac{\sqrt[p]{(a_1+b_1)^{p-1}}}{(\sum_{i=-m/p}^{m-m/p} g_i y^{-i})^{p-1}} \geq \frac{1}{2}.$$

We have assumed that $|\sum_{i=1}^{m-m/p} g_i y^{-i}| < b_2$. Using this inequality we get

$$B_2 := D(\sqrt[p-1]{2}\sqrt[p]{a_1+b_1} + b_2) \geq \Big| \sum_{i=-m/p}^{0} D g_i y^{-i} \Big|.$$

It therefore suffices to find the integral roots of the polynomial equations $\sum_{i=0}^{m/p} D g_{-i} Y^i - k = 0$ for $|k| \leq B_2$, $k \in \mathbb{Z}$.

We conclude that every solution $(x, y) \in \mathbb{Z}^2$ of (1) satisfies at least one of the following equations if p is odd:

(11) $$R_k(X) = 0 \quad \text{for some } |k| < B_1,$$

(13) $$G(Y) = F(k) \quad \text{for some } k \in [FL, FU],$$

(14) $$F(X) = G(k) \quad \text{for some } k \in [GL, GU],$$

(15) $$\sum_{i=0}^{m/p} D g_{-i} Y^i - k = 0 \quad \text{for some } |k| < B_2,$$

(16) $$\sum_{i=0}^{m} D_1 g_{-m+m/p-i} Y^i = 0.$$

The remaining question is how we should fix the parameters a_1, a_2, b_1, b_2 such that the number of equations to be solved becomes as small as possible. If we increase a_1 then $|I(a_1)|$ will decrease and B_1, B_2 will become larger, but the number of equations may become smaller. We start the algorithm with the following initial values:

(17) $$\begin{aligned} a_1 &= \max_{i \in \{1,\ldots,np-n\}} |\widehat{f}_i|, & a_2 &= \max_{i \in \{1,\ldots,n-n/p\}} |f_i|, \\ b_1 &= \max_{i \in \{1,\ldots,mp-m\}} |\widehat{g}_i|, & b_2 &= \max_{i \in \{1,\ldots,m-m/p\}} |g_i|. \end{aligned}$$

In this situation, for $i = 1, 2$ all the zeros of P_{a_i}, P_{b_i} and R_{a_i}, R_{b_i} are in $[-2, 2]$ whence $|I(a_1) \cup I(a_2)| \leq 5$ and $|I(b_1) \cup I(b_2)| \leq 5$. However $B_1, \widehat{B}_1, B_2$ are large. Next we apply a kind of reduction to decrease the total number of equations if possible. In the algorithm we use the following lemma due to Cauchy (see [12, p. 201]):

LEMMA. *Let $P(X)$ be a univariate polynomial of degree n:*

$$P(X) = X^n + c_1 X^{n-1} + \ldots + c_n$$

with $c_n \neq 0$. Let $c_{m_1}, \ldots, c_{m_k}$ with $m_1 > \ldots > m_k$ be the strictly negative coefficients of P. Then all the positive real roots of P satisfy:

$$x \leq \max\{(k|c_{m_1}|)^{1/m_1}, \ldots, (k|c_{m_k}|)^{1/m_k}\}.$$

Let us introduce the following lists:

$$\begin{aligned} ff &:= [\widehat{f}_1, \ldots, \widehat{f}_{np-n}], \qquad & fb &:= [f_1, \ldots, f_{n-n/p}], \\ gf &:= [\widehat{g}_1, \ldots, \widehat{g}_{mp-m}], \qquad & gb &:= [g_1, \ldots, g_{m-m/p}]. \end{aligned} \tag{18}$$

The procedure Bound(w, s, k) starts from a list $w \in \{ff, fb, gf, gb\}$, a rational number $s \in \{a_1, a_2, b_1, b_2\}$ and a $k \in \{1, 2\}$. It returns the values $SR1, SR2$ which are a lower bound and upper bound, respectively, for the real zeros of the polynomials $\mathrm{pol1}(X) = P_s(X)$ and $\mathrm{pol2}(X) = R_s(X)$. If $k = 1$, then the lemma is applied to obtain bounds $\mathrm{Root}[1](\cdot)$. If $k = 2$, then a (much slower) root finding algorithm is used for that purpose, for example the previously mentioned algorithm of Schönhage. We denote these bounds by $\mathrm{Root}[2](\cdot)$ in the procedure. The value $k = 2$ is only chosen after finishing Reduction when it is relevant to have accurate values.

The procedure NumofEq$([a_1, a_2, b_1, b_2], k)$ with k as in Bound(w, s, k) serves to count the number of equations corresponding to a_1, a_2, b_1, b_2. If $p = 2$, then the total number of equations given by (11)–(14) is returned. If p is odd then the output is the total number of equations given by (11) and (13)–(16).

The procedure Reduction(a_1, a_2, b_1, b_2) is used to make the parameters a_1, a_2, b_1, b_2 smaller and thereby reduce the number of equations which have to be solved. At each step one of the parameters $s \in \{a_1, a_2, b_1, b_2\}$ is replaced with a smaller number and the corresponding number of equations is computed. If the maximal reduction exceeds the bound $10p$, then the corresponding value of s is replaced by the new one. In this procedure v is a vector which contains four numbers, the current values of the parameters. The vector $vecv$ consists of the next possible values of the parameters. The current number of equations which depends on v is $N0$. Now assume we are in the stage $v = [a_1, a_2, b_1, b_2]$; then we have the following four possible "directions": $vec_1 = [vecv[1], a_2, b_1, b_2], vec_2 = [a_1, vecv[2], b_1, b_2], vec_3 = [a_1, a_2, vecv[3], b_2], vec_4 = [a_1, a_2, b_1, vecv[4]]$, where $vecv[i]$ denotes the ith element of $vecv$. We compute the number of equations for these "directions", that is $N1, N2, N3, N4$. Let i be the smallest integer such that $Ni = \min\{N1, N2, N3, N4\}$. If $N0 - Ni > 10p$ then we set $v = vec_i$ and we decrease the ith element of $vecv$, otherwise Reduction stops. After reducing the parameters we decrease the number of equations further by means of a root finding algorithm.

4. The algorithm. Input: $n = \deg F, m = \deg G$ and the coefficients of the monic polynomials $F, G \in \mathbb{Z}[X]$. Output: all integer solutions of the Diophantine equation $F(X) = G(Y)$.

Procedure Bound(w, s, k)
let r be the length of w
set $\mathrm{pol1}(t) := st^r - w[1]t^{r-1} - \ldots - w[r]$ and
$\mathrm{pol2}(t) := st^r + w[1]t^{r-1} + \ldots + w[r]$,
if $\mathrm{Root}[k](\mathrm{pol1}(t)) \neq \emptyset$ or $\mathrm{Root}[k](\mathrm{pol2}(t)) \neq \emptyset$ **then**
let $SR1 := [\min \mathrm{Root}[k](\mathrm{pol1}(t)) \cup \mathrm{Root}[k](\mathrm{pol2}(t))]$ and
$SR2 := [\max \mathrm{Root}[k](\mathrm{pol1}(t)) \cup \mathrm{Root}[k](\mathrm{pol2}(t))]$,
else
set $SR1 := 0, SR2 := 0$
end if
return $[SR1, SR2]$

Procedure NumofEq$([a_1, a_2, b_1, b_2], k)$
set

$$\begin{aligned} fL &:= \min\{\mathrm{Bound}(ff, a_1, k), \mathrm{Bound}(fb, a_2, k)\}, \\ fU &:= \max\{\mathrm{Bound}(ff, a_1, k), \mathrm{Bound}(fb, a_2, k)\}, \\ gL &:= \min\{\mathrm{Bound}(gf, b_1, k), \mathrm{Bound}(gb, b_2, k)\}, \\ gU &:= \max\{\mathrm{Bound}(gf, b_1, k), \mathrm{Bound}(gb, b_2, k)\} \end{aligned}$$

if $p \bmod 2 = 1$ **then**
return

$$\begin{aligned} &fU - fL + gU - gL + 2\lfloor D(\sqrt[p]{a_1 + b_1} + a_2 + b_2)\rfloor \\ &+ 2\lfloor D(\sqrt[p-1]{2}\sqrt[p]{a_1 + b_1} + b_2)\rfloor + 4 \end{aligned}$$

else
return

$$\begin{aligned} &fU - fL + gU - gL + 2\lfloor D(\sqrt[p]{a_1 + b_1} + a_2 + b_2)\rfloor \\ &+ 2\lfloor \widehat{D}(\sqrt[p]{a_1 + b_1} + a_2 + b_2)\rfloor + 4 \end{aligned}$$

end if

Procedure Reduction(a_1, a_2, b_1, b_2)
set $v := [a_1, a_2, b_1, b_2]$ and $vecv := [\lfloor \sqrt[p]{a_1}\rfloor, \lfloor \sqrt[p]{a_2}\rfloor, \lfloor \sqrt[p]{b_1}\rfloor, \lfloor \sqrt[p]{b_2}\rfloor]$,
let $ja := true, N0 :=$ NumofEq$(v, 1)$,
while ja **do**
for $i = 1, 2, 3, 4$ **do**

let $vec_i := v, vec_i[i] := vecv[i]$
end for
for $i = 1, 2, 3, 4$ **do**
set $Ni :=$ NumofEq$(vec_i, 1)$
end for
put $N = \min\{N0, N1, N2, N3, N4\}$
if $N0 - N > 10p$ **then**
let i be the smallest integer such that $N = Ni$, let $N0 := N$,
set $v[i] := vecv[i], vecv[i] := vecv[i]/(16p)$
else
let $ja := false$
end if
end while
return v

Let p be the smallest prime divisor of $\gcd(m, n)$. Compute the coefficients $f_i, g_i, \widehat{f_i}, \widehat{g_i}$ from (6) and $D, \widehat{D}$ from the definitions after (8) and D_1 from the definition below (14). Define a_1, a_2, b_1, b_2 as in (17). Define ff, fb, gf, gb as in (18). Set $V :=$ Reduction(a_1, a_2, b_1, b_2). Let

$$\begin{aligned}
FL &:= \min\{\mathrm{Bound}(ff, V[1], 2), \mathrm{Bound}(fb, V[2], 2)\},\\
FU &:= \max\{\mathrm{Bound}(ff, V[1], 2), \mathrm{Bound}(fb, V[2], 2)\},\\
GL &:= \min\{\mathrm{Bound}(gf, V[3], 2), \mathrm{Bound}(gb, V[4], 2)\},\\
GU &:= \max\{\mathrm{Bound}(gf, V[3], 2), \mathrm{Bound}(gb, V[4], 2)\},\\
B_1 &:= 2\lfloor D(\sqrt[p]{V[1] + V[3]} + V[2] + V[4])\rfloor,\\
\widehat{B}_1 &:= 2\lfloor \widehat{D}(\sqrt[p]{V[1] + V[3]} + V[2] + V[4])\rfloor,\\
B_2 &:= 2\lfloor D(\sqrt[p-1]{2}\sqrt[p]{V[1] + V[3]} + V[4])\rfloor.
\end{aligned}$$

If $p = 2$ then solve (11)–(14) and list the resulting integer solutions. If p is odd then solve (11) and (13)–(16) and list the resulting integer solutions.

5. Examples. I implemented the algorithm in the computer algebra program package Magma. The program was run on an AMD-K7 550 MHz PC with 128 MB memory.

EXAMPLE 1. Consider the Diophantine equation

$$x^2 - 3x + 5 = y^8 - y^7 + 9y^6 - 7y^5 + 4y^4 - y^3.$$

We express F and G in the form (6):

$$F(X) = \left(X - \frac{3}{2} + \frac{11}{8X}\right)^2 + \frac{33}{8X} - \frac{121}{64X^2},$$

$$G(Y) = \left(Y^4 - \frac{1}{2}Y^3 + \frac{35}{8}Y^2 - \frac{21}{16}Y - \frac{1053}{128} + \frac{289}{256Y} + \frac{36551}{1024Y^2} + \frac{4323}{2048Y^3} - \frac{6142813}{32768Y^4}\right)^2 - \frac{3069115}{32768Y} + \frac{292534083}{131072Y^2} - \frac{141021313}{262144Y^3} - \frac{9150328067}{2097152Y^4} + \frac{1143233065}{4194304Y^5} + \frac{224451204647}{16777216Y^6} + \frac{26555380599}{33554432Y^7} - \frac{37734151552969}{1073741824Y^8}.$$

Here we have:

$$ff = \left[\frac{33}{8}, -\frac{121}{64}\right], \quad fb = \left[\frac{11}{8}\right],$$

$$gf = \left[-\frac{3069115}{32768}, \frac{292534083}{131072}, -\frac{141021313}{262144}, -\frac{9150328067}{2097152}, \frac{1143233065}{4194304}, \frac{224451204647}{16777216}, \frac{26555380599}{33554432}, -\frac{37734151552969}{1073741824}\right],$$

$$gb = \left[\frac{289}{256}, \frac{36551}{1024}, \frac{4323}{2048}, -\frac{6142813}{32768}\right],$$

$$D = \widehat{D} = 128.$$

In the table below we collect information on the reduction.

$[a_1, a_2, b_1, b_2]$	$[fL, fU]$	$[gL, gU]$	$B_1, \widehat{B}_1$
$\left[\frac{33}{8}, \frac{11}{8}, \frac{37734151552969}{1073741824}, \frac{6142813}{32768}\right]$	$[-2, 1]$	$[-1, 1]$	$48168, 48168$
$\left[\frac{33}{8}, \frac{11}{8}, 187, \frac{6142813}{32768}\right]$	$[-2, 1]$	$[-7, 7]$	$25941, 25941$
$\left[\frac{33}{8}, \frac{11}{8}, 187, 14\right]$	$[-2, 1]$	$[-7, 7]$	$3738, 3738$
$\left[\frac{33}{8}, \frac{11}{8}, 187, \frac{7}{16}\right]$	$[-2, 1]$	$[-9, 16]$	$2002, 2002$
$\left[\frac{33}{8}, \frac{11}{8}, \frac{187}{32}, \frac{7}{16}\right]$	$[-2, 1]$	$[-64, 64]$	$636, 636$
$\left[\frac{33}{8}, 1, \frac{187}{32}, \frac{7}{16}\right]$	$[-2, 1]$	$[-64, 64]$	$588, 588$
$\left[\frac{33}{8}, \frac{1}{32}, \frac{187}{32}, \frac{7}{16}\right]$	$[-44, 44]$	$[-64, 64]$	$464, 464$
$\left[2, \frac{1}{32}, \frac{187}{32}, \frac{7}{16}\right]$	$[-44, 44]$	$[-64, 64]$	$418, 418$
$\left[\frac{1}{16}, \frac{1}{32}, \frac{187}{32}, \frac{7}{16}\right]$	$[-132, 66]$	$[-64, 64]$	$371, 371$

Now we compute $FL = -66, FU = 66, GL = -29, GU = 13$. It remains to solve the following equations:

$$\mathrm{Res}_Y(F(X) - G(Y), 128X - P(Y) + 861 - k) = 0 \quad \text{for } k \in \{-371, \ldots, 371\},$$
$$\mathrm{Res}_Y(F(X) - G(Y), 128X + P(Y) - 1245 - k) = 0 \quad \text{for } k \in \{-371, \ldots, 371\},$$

where

$$P(Y) = 128Y^4 - 64Y^3 + 560Y^2 - 168Y,$$
$$G(y) = F(x) \quad \text{for } x \in \{-66, \dots, 66\},$$
$$F(x) = G(y) \quad \text{for } y \in \{-29, \dots, 13\}.$$

The complete list of integral solutions of these equations turns out to be

$$\{(-657, 5), (-3, -1), (0, 1), (3, 1), (6, -1), (660, 5)\}.$$

Computation time in seconds: 22.84.

EXAMPLE 2. We apply the method to the Diophantine equation

$$x^3 - 5x^2 + 45x - 713$$
$$= y^9 - 3y^8 + 9y^7 - 17y^6 + 38y^5 - 199y^4 - 261y^3 + 789y^2 + 234y.$$

As in Example 1 we express F and G by (6):

$$F(X) = \left(X - \frac{5}{3} + \frac{110}{9X} - \frac{15826}{81X^2}\right)^3 + \text{rest},$$
$$G(Y) = \left(Y^3 - Y^2 + 2Y - \frac{4}{3}\right.$$
$$\left. + \frac{4}{Y} - \frac{143}{3Y^2} - \frac{1909}{9Y^3} + \frac{998}{9Y^4} + \frac{2989}{3Y^5} + \frac{61672}{81Y^6}\right)^3 + \text{rest},$$
$$D = D_1 = 81.$$

In the table below we collect information on the reduction.

$[a_1, a_2, b_1, b_2]$	$[fL, fU]$	$[gL, gU]$	B_1, B_2
$\left[\frac{3963815979976}{531441}, \frac{15826}{81}, \frac{48425622648104}{19683}, \frac{2989}{3}\right]$	$[-1, 1]$	$[-1, 1]$	$7629, 8722$
$\left[\frac{3963815979976}{531441}, \frac{15826}{81}, 1350, \frac{2989}{3}\right]$	$[-1, 1]$	$[-62, 68]$	$4161, 3818$
$\left[\frac{3963815979976}{531441}, \frac{15826}{81}, 1350, 10\right]$	$[-1, 1]$	$[-62, 68]$	$1202, 859$
$\left[\frac{3963815979976}{531441}, 6, 1350, 10\right]$	$[-8, 6]$	$[-62, 68]$	$634, 859$
$[195, 6, 1350, 10]$	$[-77, 39]$	$[-62, 68]$	$83, 79$

Next we compute $FL = -19, FU = 10, GL = -2, GU = 10$. In this case we solve the following equations:

$$\text{Res}_Y(F(X) - G(Y), 3X - 3Y^3 + 3Y^2 - 6Y - 1 - k) = 0 \quad \text{for } k \in \{-83, \dots, 83\},$$
$$G(y) = F(x) \quad \text{for } x \in \{-19, \dots, 10\},$$
$$F(x) = G(y) \quad \text{for } y \in \{-2, \dots, 10\},$$
$$3y^3 - 3y^2 + 6y - 4 - k = 0 \quad \text{for } k \in \{-79, \dots, 79\},$$
$$81y^9 - 81y^8 + 162y^7 - 108y^6 + 324y^5 - 3861y^4$$
$$-17181y^3 + 8982y^2 + 80703y + 61672 = 0.$$

The only integral solution of these equations is $(x,y)=(-11,-2)$. Computation time in seconds: 12.66.

EXAMPLE 3 ([7, Theorem 1a]). Consider the Diophantine equation

$$x(x+1)(x+2)(x+3)=y(y+1)\dots(y+5).$$

There are many results in the literature concerning similar equations (cf. [2], [10]). We express F and G in the form (6):

$$F(X)=\left(X^2+3X+1-\frac{1}{2X^2}\right)^2+\text{rest},$$

$$G(Y)=\left(Y^3+\frac{15}{2}Y^2+\frac{115}{8}Y+\frac{75}{16}-\frac{189}{128Y}+\frac{945}{256Y^2}-\frac{17865}{1024Y^3}\right)^2+\text{rest},$$

$$D=\widehat{D}=16.$$

In the table below we collect information on the reduction.

$[a_1,a_2,b_1,b_2]$	$[fL,fU]$	$[gL,gU]$	$B_1,\widehat{B}_1$
$\left[3,1,\frac{7615179}{16384},\frac{17865}{1024}\right]$	$[-2,2]$	$[-2,2]$	$641,641$
$\left[3,1,22,\frac{17865}{1024}\right]$	$[-2,2]$	$[-39,31]$	$375,375$
$[3,1,22,4]$	$[-2,2]$	$[-39,31]$	$160,160$
$\left[3,1,22,\frac{1}{8}\right]$	$[-2,2]$	$[-39,31]$	$98,98$

Now we compute $FL=-1,FU=1,GL=-15,GU=10$. It remains to solve the following equations:

$$\text{Res}_Y(F(X)-G(Y),16X^2+48X-P(Y)-59-k)=0 \quad \text{for } k\in\{-98,\dots,98\},$$

$$\text{Res}_Y(F(X)-G(Y),16X^2+48X+P(Y)+91-k)=0 \quad \text{for } k\in\{-98,\dots,98\},$$

where

$$P(Y)=16Y^3+120Y^2+230Y,$$
$$G(y)=F(x) \quad \text{for } x\in\{-1,\dots,1\},$$
$$F(x)=G(y) \quad \text{for } y\in\{-15,\dots,10\}.$$

The complete list of non-trivial integral solutions of these equations is

$$\{(-10,-7),(-10,2),(7,-7),(7,2)\}.$$

Computation time in seconds: 8.35.

The following examples are from [19]. The method described in that paper is similar to ours in the sense that one has to find all the integral solutions of polynomial equations $P(x)=0$, where $P\in\mathbb{Z}[X]$. We compare both methods by comparing the number of equations which have to be solved. We remark that our algorithm works for equations $F(x) = G(y)$, where $F, G \in \mathbb{Z}[X]$ are monic polynomials with $\deg F = n$, $\deg G = m$, such that $F(X) - G(Y)$ is irreducible in $\mathbb{Q}[X, Y]$ and $\gcd(n, m) > 1$, while Szalay's algorithm can be applied only for the special case $G(y) = y^m$.

Equation 1: $x^2 = y^4 - 99y^3 - 37y^2 - 51y + 100$,

Equation 2: $x^2 = y^8 - 7y^7 - 2y^4 - y + 5$,

Equation 3: $x^2 = y^8 + y^7 + y^2 + 3y - 5$,

Equation 4: $x^3 = y^9 + 2y^8 - 5y^7 - 11y^6 - y^5 + 2y^4 + 7y^2 - 2y - 3$.

Equation 1	20761	985360
Equation 2	14866	118546
Equation 3	355	16
Equation 4	849	420

Here we did not use Cauchy's lemma in the procedures Bound, NumofEq and Reduction, but a root finding algorithm to get even fewer equations to solve. In the second column the numbers of equations to be solved by applying our method are stated, and in the third column the numbers of equations to be solved by applying the method described in [19]. In the first two cases one has to solve fewer equations by using our algorithm. The reason is that if the coefficient of the one but largest power of y (-99 and -7, respectively) is not "small" in absolute value, the reduction helps a lot.

Acknowledgements. I thank my supervisor Robert Tijdeman and Jan-Hendrik Evertse for their valuable remarks and suggestions.

References

[1] M. Ayad, *Sur le théorème de Runge*, Acta Arith. 58 (1991), 203–209.

[2] F. Beukers, T. N. Shorey and R. Tijdeman, *Irreducibility of polynomials and arithmetic progressions with equal products of terms*, in: Number Theory in Progress (Zakopane, 1997) Vol. 1, de Gruyter, Berlin, 1999, 11–26.

[3] Yu. F. Bilu and R. F. Tichy, *The Diophantine equation $f(x) = g(y)$*, Acta Arith. 95 (2000), 261–288.

[4] G. Collins and A. Akritas, *Polynomial real root isolation using Descartes' rule of signs*, in: Proc. 3rd ACM Symposium on Symbolic and Algebraic Computation, 1976, 272–275.

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

[6] A. Grytczuk and A. Schinzel, *On Runge's Theorem about Diophantine equations*, in: Colloq. Math. Soc. János Bolyai 60, North-Holland, 1991, 329–356.

[7] L. Hajdu and Á. Pintér, *Combinatorial Diophantine equations*, Publ. Math. Debrecen 56 (2000), 391–403.

[8] D. L. Hilliker and E. G. Straus, *Determination of bounds for the solutions to those binary diophantine equations that satisfy the hypotheses of Runge's theorem*, Trans. Amer. Math. Soc. 280 (1983), 637–657.

[9] M. Laurent and D. Poulakis, *On the global distance between two algebraic points on a curve*, J. Number Theory, to appear.

[10] R. A. MacLeod and I. Barrodale, *On equal products of consecutive integers*, Canad. Math. Bull. 13 (1970), 255–259.

[11] D. W. Masser, *Polynomial bounds for Diophantine equations*, Amer. Math. Monthly 93 (1980), 486–488.

[12] M. Mignotte, *Mathématiques pour le calcul formel*, Presses Univ. de France, Paris, 1989.

[13] D. Poulakis, *A simple method for solving the Diophantine equation* $Y^2 = X^4 + aX^3 + bX^2 + cX + d$, Elem. Math. 54 (1999), 32–36.

[14] C. Runge, *Über ganzzahlige Lösungen von Gleichungen zwischen zwei Veränderlichen*, J. Reine Angew. Math. 100 (1887), 425–435.

[15] A. Schinzel, *An improvement of Runge's theorem on diophantine equations*, Comment. Pontificia Acad. Sci. 2 (1969), 1–9.

[16] A. Schönhage, *The fundamental theorem of algebra in terms of computational complexity*, Technical report, Univ. Tübingen, 1982.

[17] T. Skolem, *Über ganzzahlige Lösungen einer Klasse unbestimmten Gleichungen*, Norsk. Mat. Forenings Skrifter, Ser. I, 1922, No. 10.

[18] L. Szalay, *Fast algorithm for solving superelliptic equations of certain types*, Acta Acad. Paedagog. Agriensis Sect. Mat. (N.S.) 27 (2000), 19–24.

[19] —, *Superelliptic equations of the form* $y^p = x^{kp} + a_{kp-1}x^{kp-1} + \ldots + a_0$, Bull. Greek Math. Soc. 46 (2002), 23–33.

[20] P. G. Walsh, *A quantitative version of Runge's theorem on diophantine equations*, Acta Arith. 62 (1992), 157–172; Corrections, ibid. 73 (1995), 397–398.

Mathematical Institute
Leiden University
P.O. Box 9512
2300 RA Leiden, The Netherlands
E-mail: tengely@math.leidenuniv.nl

Received on 11.9.2002 (4365)