ACTA ARITHMETICA
LXII.2 (1992)

A quantitative version of Runge's theorem on diophantine equations

by

P. G. Walsh (Waterloo, Ont.)

1. Introduction. Let

$$F(x,y)=\sum_{i=0}^{m}\sum_{j=0}^{n}a_{i,j}x^iy^j \tag{1.1}$$

be a polynomial with rational integer coefficients of degree $m>0$ in x and $n>0$ in y which is irreducible in $\mathbb{Q}[x,y]$. We say that F satisfies *Runge's Condition* unless the following conditions hold for F:

(C_1) $a_{i,n}=a_{m,j}=0$ for all non-zero i and j,

(C_2) $a_{i,j}=0$ for all pairs (i,j) satisfying $ni+mj>mn$,

(C_3) the sum of all monomials $a_{i,j}x^iy^j$ of F for which $ni+mj=nm$ is a constant multiple of a power of an irreducible polynomial in $\mathbb{Z}[x,y]$.

We note that (C_2) is a stronger condition than (C_1). The reason that (C_1) is included above will be made clear in the statement of Theorem 1. We will make reference to the following condition which, together with (C_1), is stronger than (C_2) and (C_3):

(C_4) the algebraic function $y=y(x)$ defined by $F(x,y)=0$ has only one class of conjugate Puiseux expansions.

In 1887 Runge [14] showed that if F is a polynomial for which at least one of (C_1), (C_2), (C_3) or (C_4) does not hold, then the diophantine equation $F(x,y)=0$ has only a finite number of solutions in rational integers x and y. Runge's method of proof is effective, and upper bounds for the size of integer solutions to these equations were obtained by Hilliker and Straus in [10]. They showed that any integer solution of $F(x,y)=0$ satisfies

$$\max\{|x|,|y|\}<\begin{cases}4(h+1)^2 & \text{if } d=1\,,\\ (8dh)^{d^{2d^3}} & \text{if } d>1\,,\end{cases}$$

where $d=\max\{m,n\}$ and $h=\max_{i,j}|a_{i,j}|$. In their work, Hilliker and Straus use a quantitative version of Eisenstein's theorem on power series

expansions of algebraic functions. Dwork and van der Poorten [4] have recently refined a quantitative result of Schmidt [16] on Eisenstein's theorem. In Theorem 1 we apply the result of Dwork and van der Poorten to Runge's method, and thereby improve on the result of Hilliker and Straus.

In what follows let $F(x,y)$ be the irreducible polynomial given in (1.1), $d = \max\{m,n\}$, $d_0 = \min\{m,n\}$, and $h = \text{height}\, F = \max_{i,j} |a_{i,j}|$. As well, define

$$B(h,n) = 4.8(8e^{-3}n^{4+2.74\log n}e^{1.22n}h^2)^n \quad \text{for } n \geq 1\,.$$

THEOREM 1. *Assume that $(x,y) \in \mathbb{Z}^2$ is a solution of the diophantine equation $F(x,y) = 0$.*

1. *If $a_{m,j} \neq 0$ for some non-zero j, or more generally, if* (C_4) *does not hold, then*

$$\begin{aligned} |x| &\leq B(h,n)^{2mn^3(n+1)}(2h(m+1)(n+1))^{12mn^4}\,, \\ |y| &\leq B(h,n)^{2m^2n^2(n+1)}(2h(m+1)(n+1))^{12m^2n^3}\,. \end{aligned} \tag{1.2}$$

2. *If* (C_1) *holds and either* (C_2) *or* (C_3) *does not, then*

$$\begin{aligned} |x| &\leq B(h,d_0)^{2mn^2d_0(d_0+1)}(2h(m+1)(n+1))^{12mn^2d_0^2}\,, \\ |y| &\leq B(h,d_0)^{2m^2nd_0(d_0+1)}(2h(m+1)(n+1))^{12m^2nd_0^2}\,. \end{aligned} \tag{1.3}$$

COROLLARY. *If $F(x,y)$ satisfies Runge's Condition, then all integer solutions of the diophantine equation $F(x,y) = 0$ satisfy*

$$\max\{|x|,|y|\} < (2d)^{18d^7}h^{12d^6}\,. \tag{1.4}$$

Thus, the main improvement on the result of Hilliker and Straus is the removal of the double exponential in d. This corresponds to the fact that the recent quantitative versions of Eisenstein's theorem in [4] and [16] improve on earlier versions by a similar margin. We note that Theorem 1 also improves on the special case of Runge's theorem proved in Theorem 3.31 of [10] except for finitely many equations of each degree d. The factor $B(h,n)$ in Theorem 1 is that which arises in the work of Dwork and van der Poorten. Any further quantitative improvements in this direction should reduce the bounds given in Theorem 1.

Grytczuk and Schinzel [8] have recently used a method of Skolem to obtain upper bounds for integer solutions to the same class of diophantine equations. In particular, if F is as in Theorem 1 and (m,n) denotes the greatest common divisor of m and n, then they have shown that:

1. *If $a_{m,j} \neq 0$ for some non-zero j, then*

$$\begin{aligned} |x| &\leq ((m+1)(n+1)(mn+1)^{2/n}h)^{2n(mn+1)^3}, \\ |y| &\leq ((m+1)(n+1)(mn+1)^{2/n}h)^{2(mn+1)^3}. \end{aligned}$$

2. *If* (C_1) *holds, but* (C_2) *does not, then*
$$|x| \le ((4mnd_0)^{8mn(m,n)^{-1}}h)^{96m^3n^4(m,n)^{-4}d_0^4+m^{-1}d_0},$$
$$|y| \le ((4mnd_0)^{8mn(m,n)^{-1}}h)^{96m^4n^3(m,n)^{-4}d_0^4+n^{-1}d_0}.$$
3. *If* (C_1) *and* (C_2) *hold, but* (C_3) *does not, then*
$$|x| \le ((mn)^{3mn(m,n)^{-1}}h)^{(5/128)m^3n^4(m,n)^4+m^{-1}(m,n)^2},$$
$$|y| \le ((mn)^{3mn(m,n)^{-1}}h)^{(5/128)m^4n^3(m,n)^4+n^{-1}(m,n)^2}.$$

Theorem 1 improves on this result in general, although there are many examples for which this result will provide smaller bounds, primarily in the case that (C_1) does not hold for F. We remark that Theorem 1 has been presented in such a manner as to facilitate a comparison between these two results.

Grytczuk and Schinzel also provide the example $F(x,y) = xy - ty - tx^d$, with solution $x = t^{d+1} + t$, $y = (t^d+1)^d$, which shows that the exponent $12d^6$ in (1.4) cannot be lowered below d^2. This example also shows that Theorem 3.3 of [10] is false for $d > 2$, wherein it is stated that if $d_0 = 1$ then $\max\{|x|,|y|\} < d(h+1)^{2d}$. It does follow from the proof of this theorem that $\min\{|x|,|y|\} < d(h+1)^{2d}$, from which one can deduce that $\max\{|x|,|y|\} < h(d+1)(d(h+1))^{2d^2}$. We will see in the proof of Theorem 1 that there is no need to distinguish this case separately, provided that the coefficient $a_{m,n} = 0$.

It was established by Runge that if $F \in \mathbb{Z}[x,y]$ is irreducible in $\mathbb{Q}[x,y]$, and if $F(x,y) = 0$ has infinitely many solutions in rational integers, then the algebraic function $y = y(x)$ satisfies (C_4). It is evident that the same holds for the algebraic function $x = x(y)$. It can be shown that this is equivalent to the condition that F is irreducible in $\mathbb{Q}((\frac{1}{x}))[y]$ and in $\mathbb{Q}((\frac{1}{y}))[x]$. M. Ayad [2] has recently improved on this by showing that such a polynomial F must either be irreducible or a product of two irreducibles of the same degree in $\overline{\mathbb{Q}}((\frac{1}{x}))[y]$ and in $\overline{\mathbb{Q}}((\frac{1}{y}))[x]$, where $\overline{\mathbb{Q}}$ denotes the algebraic closure of $\mathbb{Q}$. This generalizes a well known result of Schinzel [15]. The proofs of these results rely on an ineffective theorem of Siegel, hence they do not provide a method for obtaining upper bounds for the size of integer solutions.

As an application of the quantitative results of [8], we prove the following effective version of a theorem of Skolem [18, p. 90].

THEOREM 2. *Let F be a non-zero polynomial with rational integer coefficients, which is irreducible in $\mathbb{Q}[x,y]$ and satisfies $F(0,0) = 0$. If $m = \deg_x F$, $n = \deg_y F$, $h = \operatorname{height} F$, and g is a positive integer, then all*

integer solutions of $F(x,y)=0$ *with* $\gcd(x,y)=g$ *satisfy*

$$\begin{aligned} |x| &\le (m^6n^6(m+1)^{n-1}g^{mn}h^n)^{2m^6n^6}, \\ |y| &\le (m^6n^6(n+1)^{m-1}g^{mn}h^m)^{2m^6n^6}. \end{aligned} \tag{1.5}$$

There are certain subclasses of polynomials for which Runge's Condition is satisfied and for which the bound in (1.4) can be improved. One such class is the class of superelliptic equations $y^n = P(x)$ with $n \ge 2$ and $P(x) \in \mathbb{Z}[x]$ of degree $d \ge 2$.

Let us assume that $F(x,y) = y^n - P(x)$ is irreducible in $\mathbb{Q}[x,y]$, and for simplicity that $P(x)$ is monic. It follows that F satisfies Runge's Condition precisely if $y^n - x^d$ is reducible, and this is equivalent to the condition $\gcd(n,d) > 1$.

THEOREM 3. *Let* $n \ge 2$, $d \ge 2$ *be integers such that* $g = \gcd(n,d) > 1$. *Suppose further that* $P(x) = \sum_{i=0}^{d} a_i x^i \in \mathbb{Z}[x]$ *is a monic polynomial of degree* d *such that* $y^n - P(x)$ *is irreducible in* $\mathbb{Q}[x,y]$. *Put* $h = \max|a_i|$ *and let* l *denote a divisor of* g *with* $l > 1$. *All integer solutions of the superelliptic equation*

$$y^n = P(x) \tag{1.6}$$

satisfy

$$|x| \le l^{2d-l}((d/l)+2)^l(h+1)^{d+l}\,. \tag{1.7}$$

For the case $d = 2$, it is readily verified that the bound in (1.7) can be replaced by $(h^2+6h+1)/4$, which is best possible. For $d \ge 3$ it is not difficult to verify that the bound in (1.7) does not exceed $(2dh)^{2d}$.

Under the same hypotheses as Theorem 3, with the extra condition that $l > 2$, André [1] has shown that any rational solution $(x,y) = (a/b, c/d)$, $\gcd(a,b) = 1$, of (1.6), for which b is not divisible by any prime congruent to 1 modulo l, satisfies $\max\{|a|,|b|\} < (2^{8d}l^3h^2)^{3d+2}$.

Theorem 3 improves on André's result for the case of integer solutions. These results represent a substantial improvement on the best known result for integer solutions to the general hyperelliptic and superelliptic diophantine equations, due to Sprindžuk [19] and Turk [20], respectively. Masser [12] has proved a result which improves on Theorem 3 for the case $d = 4$ and $l = 2$. Note that our improvement on these more general results relies on the fact that we have restricted our attention to equations of the form (1.6) for which n and the degree of P have a non-trivial common divisor.

For more on Runge's method, we refer the reader to Ellison [7], Hilliker and Straus [11], Mordell [13], and Shorey and Tijdeman [17].

2. Eisenstein's theorem on algebraic functions. Eisenstein [6] proved that if a formal power series

$$y = \sum_{k=0}^{\infty} a_k x^k$$

satisfies a polynomial equation $F(x, y) = 0$, where F is a non-zero polynomial with algebraic coefficients, then there is an algebraic number field K such that $a_0, a_1, \ldots$ all lie in K, and there exist positive integers A_0, A such that $A_0 A^k a_k$ are algebraic integers for each integer k with $k \geq 0$.

Hermite [9], Coates [3], and Hilliker and Straus [10] have obtained quantitative versions of Eisenstein's theorem by computing upper bounds for the size of A_0 and A in terms of the degree and height of F. Schmidt [16] has recently improved on these results. More recently, Dwork and van der Poorten have refined Schmidt's result. The following result follows from the introduction and Section 4 of [4].

THEOREM A (Dwork and van der Poorten, 1991). *Let $H \in \mathbb{Z}[t, z]$ be a non-zero polynomial which has no multiple factors when regarded as a polynomial in z. Let $M = \deg_t H$, $N = \deg_z H$, and $h = \operatorname{height} H$. If the formal power series*

$$z(t) = \sum_{k=0}^{\infty} b_k t^k$$

satisfies $H(t, z(t)) = 0$, then there is a positive integer B with

$$B < 4.8(8e^{-3} N^{4+2.74 \log N} e^{1.22N} h^2)^N$$

for which $B^{M+k} b_k$ is an algebraic integer for all $k \geq 0$.

3. Puiseux expansions of algebraic functions. Let $F(x, y)$ be as in the statement of Theorem 1, and write $F(x, y)$ as

$$F(x, y) = A_n(x) y^n + A_{n-1}(x) y^{n-1} + \ldots + A_0(x)\,. \tag{3.1}$$

Puiseux's theorem (for example see Chapter 3 of [5]) asserts the existence of n distinct formal series

$$y_i(x) = \sum_{k=-f_i}^{\infty} c_{k,i} x^{-k/e_i}, \qquad i = 1, 2, \ldots, n\,, \tag{3.2}$$

such that

$$F(x, y) = A_n(x) \prod_{i=1}^{n} (y - y_i(x))\,, \tag{3.3}$$

where each e_i is a positive integer, each f_i is an integer chosen so that $c_{-f_i,i} \neq 0$, and the $c_{k,i} \in \mathbb{C}$. For each $i = 1, 2, \ldots, n$, the integer e_i is chosen to be minimal, meaning that for any divisor $e > 1$ of e_i, there is

some $c_{k,i} \neq 0$ for which e does not divide k. Moreover, by the version of Puiseux's theorem found on p. 98 of [21], any series $y(x)$ of the form (3.2) which satisfies $F(x, y(x)) = 0$ must be one of the n series in (3.2).

The series in (3.2) are referred to as the Puiseux expansions of the algebraic function y defined by $F(x, y) = 0$. It is known that they converge for all finite values x in the exterior of any circle about the origin which encloses all finite singularities of the algebraic function y. These finite singularities satisfy $\mathrm{res}_y(F, F_y) = 0$, where F_y denotes the partial derivative of F with respect to y and $\mathrm{res}_y(F, F_y)$ is the resultant (see p. 30 of [21]) of F and F_y with respect to y. By Lemma 1 of [8], it follows that each of the Puiseux series in (3.2) converges for $|x| \geq R_0$, where R_0 is given by

$$R_0 = (h(m+1)(n+1))^{2n-1}. \tag{3.4}$$

Thus, by (3.3), if $(x, y) \in \mathbb{C}^2$ satisfies $F(x, y) = 0$ with $|x| \geq R_0$, then (x, y) satisfies $y = y_i(x)$ for some i with $1 \leq i \leq n$.

Let

$$y(x) = \sum_{k=-f}^{\infty} c_k x^{-k/e} \tag{3.5}$$

represent one of the n Puiseux expansions in (3.2). It is well known that the coefficients $c_{-f}, c_{-f+1}, \ldots$ all lie in an algebraic number field. Let $K = \mathbb{Q}(c_{-f}, c_{-f+1}, \ldots)$, and put $s = [K : \mathbb{Q}]$. If $\sigma_1, \sigma_2, \ldots, \sigma_s$ denote the $\mathbb{Q}$-isomorphisms of K into $\mathbb{C}$, and ζ denotes a primitive eth root of unity, then each of the conjugate series

$$y(x, \sigma_i, j) = \sum_{k=-f}^{\infty} \sigma_i(c_k)(\zeta^j x^{-1/e})^k \quad (1 \leq i \leq s,\ 0 \leq j \leq e-1) \tag{3.6}$$

satisfies $F(x, y(x, \sigma_i, j)) = 0$, and hence is one of the n Puiseux expansions in (3.2). It can be shown that the n series in (3.2) can be partitioned into conjugacy classes, where the conjugacy class of the series in (3.5) is the set consisting of those series in (3.6). Let S denote this conjugacy class, and for each $i = 1, 2, \ldots, s$, define $S_i = \{y(x, \sigma_i, j) \in S\,;\ 0 \leq j \leq e-1\}$. It follows from the definition of e that each S_i has exactly e distinct elements. We will show that S is the disjoint union of $S_{i_1}, S_{i_2}, \ldots, S_{i_{s_0}}$ for some subset $\{i_1, i_2, \ldots, i_{s_0}\}$ of $\{1, 2, \ldots, s\}$, from which it follows that S contains precisely es_0 distinct elements. We need only show that each pair of sets S_{i_1} and S_{i_2} are either disjoint or equal. To see this, suppose that $y(x, \sigma_{i_1}, j_1) = y(x, \sigma_{i_2}, j_2) \in S_{i_1} \cap S_{i_2}$. Let $y(x, \sigma_{i_1}, a)$ be an arbitrary element of S_{i_1}, and put $b \equiv a + j_2 - j_1 \pmod{e}$. Then it follows that $y(x, \sigma_{i_1}, a) = y(x, \sigma_{i_2}, b)$, and so $y(x, \sigma_{i_1}, a) \in S_{i_2}$. This shows that $S_{i_1} \subseteq S_{i_2}$, and hence by the same argument for the reverse inclusion, we deduce that $S_{i_1} = S_{i_2}$.

LEMMA 1. *Let $F(x,y)$ be as in Theorem* 1, *and assume that $a_{m,n}=0$.*

1. *If $a_{m,j}\neq 0$ for some non-zero j, then the algebraic function y defined by $F(x,y)=0$ has more than one class of conjugate Puiseux expansions.*

2. *If* (C_1) *holds, but either* (C_2) *or* (C_3) *does not, then both of the algebraic functions x and y, defined by $F(x,y)=0$, have more than one class of conjugate Puiseux expansions.*

P r o o f. 1. Let (3.5) represent a Puiseux expansion of the algebraic function y and let S denote its conjugacy class. Assume that the elements of S are given by (3.6). If y has only one class of conjugate Puiseux expansions, then S has n distinct elements, and there is an integer s_0 such that $n=es_0$. Thus, the representation of $F(x,y)$ in (3.3) becomes

$$F(x,y)=A_n(x)\prod_{i=1}^{s_0}\prod_{j=0}^{e-1}\Big(y-\sum_{k=-f}^{\infty}\sigma_i(c_k)\zeta^{jk}x^{-k/e}\Big)\,. \tag{3.7}$$

Note that $f>0$ since $\deg_x F>0$ and $a_{m,n}=0$. From (3.7) it is clear that the monomial of highest degree in x of F is $x^{\deg A_n(x)+fs_0}$, and that it appears only with constant coefficient, contrary to our hypothesis.

2. The reader is referred to p. 433 of [14].

4. Proof of Theorem 1. 1. We shall follow closely the argument of Hilliker and Straus given in [10]. We may assume that $a_{m,n}=0$, for if $a_{m,n}\neq 0$, then by Theorem 3.2 of [10], $\max\{|x|,|y|\}<(2(h+1))^{d+1}$, and so (1.2) holds.

By part 1 of Lemma 1 the algebraic function y defined by $F(x,y)=0$ has more than one class of conjugate Puiseux expansions. Let (3.5) be a Puiseux expansion for y, S its conjugacy class, and s_0 an integer such that S has es_0 distinct elements. Then

$$1\leq es_0\leq n-1. \tag{4.1}$$

We now restrict our attention to the case $f>0$, as the other case is left for the end of the proof. We note that the integer f satisfies

$$fs_0\leq m\,. \tag{4.2}$$

To see this, apply (3.3) to write $F(x,y)$ as

$$F(x,y)=A_n(x)\prod_{T}(y-y_i(x))\prod_{T^c}(y-y_i(x))\,,$$

where T is the set of Puiseux expansions for y with $f_i>0$. If T has t elements and $\alpha=\sum_T f_i/e_i$, then $x^{\deg A_n(x)+\alpha}y^{n-t}$ appears as a monomial of F, and since $S\subseteq T$ we have $fs_0\leq \deg A_n(x)+\alpha\leq m$.

Let M denote the number of integer pairs (u,v) which satisfy

$$1\leq u\leq vf/e \quad\text{ and }\quad 1\leq v\leq es_0\,. \tag{4.3}$$

Then

$$M \le \tfrac{1}{2}(fs_0)(es_0+1) \le mn/2\,. \tag{4.4}$$

For $\varrho = 0, 1, \dots, 2M$ define

$$F(x,y,\varrho) = x^{\varrho}\prod_{S}(y - y(x,\sigma_i,j)) \tag{4.5}$$

where the product extends over the es_0 distinct elements of S. Then

$$F(x,y,\varrho) = P(x,y,\varrho) + \sum_u \sum_v b_{\varrho,u,v} y^v/x^u + E(x,y,\varrho)\,, \tag{4.6}$$

where $P(x,y,\varrho)$ is a polynomial with rational coefficients, the double sum is extended over all pairs (u,v) satisfying (4.3), and the terms collected in $E(x,y,\varrho)$ are those of the form y^v/x^u with $0 \le v \le es_0$ and $u > vf/e$. Note that for $\varrho = 0, 1, \dots, 2M$,

$$\deg_y P(x,y,\varrho) = es_0 \le n-1 \quad \text{and} \quad \deg_x P(x,y,\varrho) \le m(n+1)\,. \tag{4.7}$$

Our goal now is to estimate the denominators of the rational numbers $b_{\varrho,u,v}$ and the denominators of the coefficients of $P(x,y,\varrho)$. Put $x = t^{-e}$ and $y = zt^{-f}$. Then the series

$$z(t) = \sum_{k=0}^{\infty} b_k t^k\,, \tag{4.8}$$

with $b_k = c_{k-f}$, satisfies $F(t^{-e}, z(t)t^{-f}) = 0$. Put

$$r = \max_{a_{i,j}\neq 0}(ei+fj) \quad \text{and} \quad H(t,z) = t^r F(t^{-e}, zt^{-f})\,.$$

Then by our choice of r, $H \in \mathbb{Z}[t,z]$, $H(0,z) \not\equiv 0$, $r < 2mn$, and $z(t)$ satisfies $H(t,z(t)) = 0$.

The polynomial H also satisfies $\deg_z H \le n$, $\deg_t H < 2mn$, and height H = height F. Moreover, since F is irreducible in $\mathbb{Q}[x,y]$, H has no multiple factors when regarded as a polynomial in z. By Theorem A with $N = n$ and $M = 2mn$ there is a positive integer B with

$$B < 4.8(8e^{-3}n^{4+2.74\log n}e^{1.22n}h^2)^n \tag{4.9}$$

such that $B^{2mn+k}b_k$ is an algebraic integer for all $k \ge 0$.

By (4.5) and (4.6) it can be shown that the rational numbers $b_{\varrho,u,v}$ and the coefficients of $P(x,y,\varrho)$ can be written as symmetric polynomials, with integer coefficients, in the conjugates of b_k where $k \le fes_0 + 2Me$. The total degree of these symmetric polynomials in b_k and its conjugates is at most es_0. Therefore, $B^{(2mn+fes_0+2Me)es_0}b_{\varrho,u,v}$ is an integer for $\varrho = 0, 1, \dots, 2M$ and each pair (u,v) satisfying (4.3), and $B^{(2mn+fes_0+2Me)es_0}P(x,y,\varrho) \in \mathbb{Z}[x,y]$ for $\varrho = 0, 1, \dots, 2M$. By (4.1), (4.2) and (4.4), $(2mn + fes_0 + 2Me)es_0$ $\le (2mn + mn^2 - m)(n-1) < mn^2(n+1)$.

We now estimate the absolute values of the $b_{\varrho,u,v}$ and the coefficients of $P(x,y,\varrho)$. It follows from the argument given on p. 647 of [10] that the coefficients b_k of (4.8) satisfy

$$|\sigma_i(b_k)| \le \lambda_1 R_1^k \tag{4.10}$$

for $k \ge 0$ and $1 \le i \le s_0$, where $R_1 = R_0^{1/e}$, $\lambda_1 = 2(h+1)R_0^{2mn/e}$, and R_0 is given in (3.4).

Given formal expressions $\sum_{i\in I}\sum_{j\in J} a_{i,j}x^iy^j$ and $\sum_{i\in I}\sum_{j\in J} b_{i,j}x^iy^j$ with coefficients in $\mathbb{C}$, we write

$$\sum_{i\in I}\sum_{j\in J} a_{i,j}x^iy^j \ll \sum_{i\in I}\sum_{j\in J} b_{i,j}x^iy^j$$

if $|a_{i,j}| < b_{i,j}$ for all $i \in I$ and $j \in J$.

By (3.5) and (4.10), we deduce that for $1 \le i \le s_0$ and $0 \le j \le e-1$,

$$y(x,\sigma_i,j) \ll \lambda_1 R_1^f \sum_{k=-f}^{\infty} (R_1 x^{-1/e})^k = \lambda_1 x^{f/e}(1-(R_0/x)^{1/e})^{-1}\,. \tag{4.11}$$

In particular, if $(x,y) \in \mathbb{Z}^2$ satisfies (3.5) with $|x| > 2^e R_0$, then

$$|y| < 2\lambda_1 |x|^{f/e}\,. \tag{4.12}$$

We remark that (4.12) also holds in the case that $f \le 0$. Combining (4.5) and (4.11) we have for $\varrho = 0,1,\dots,2M$,

$$\begin{aligned} F(x,y,\varrho) &\ll x^{\varrho}(y + \lambda_1 x^{f/e}(1-(R_0/x)^{1/e})^{-1})^{n-1} \\ &\ll (4\lambda_1)^n x^{\varrho+nf/e}\Big(\sum_{\delta=0}^{n} y^{\delta}x^{-\delta f/e}\Big)(1-2(R_0/x)^{1/e})^{-1}\,. \end{aligned} \tag{4.13}$$

Also, with $E(x,y,\varrho)$ as in (4.6) we have for $\varrho = 0,1,\dots,2M$,

$$E(x,y,\varrho) \ll (4\lambda_1)^n x^{\varrho+nf/e}\Big(\sum_{\delta=0}^{n} y^{\delta}x^{-\delta f/e}\Big)\sum_{k=0}^{\infty}(2(R_0/x)^{1/e})^{k+\varrho e+nf}. \tag{4.14}$$

Let β represent the maximum of the numbers $|b_{\varrho,u,v}|$ and the absolute values of the coefficients of the polynomials $P(x,y,\varrho)$. Then by (4.13),

$$\beta \le (4\lambda_1)^n (2R_0^{1/e})^{mn^2}\,. \tag{4.15}$$

By (4.12) and (4.14), if $(x,y) \in \mathbb{Z}^2$ satisfies (3.5) with $|x| > 2^e R_0$, then

$$|E(x,y,\varrho)| < 2(n+1)(8\lambda_1^2)^n (2R_0^{1/e})^{mn^2}|x|^{-1/e}\,. \tag{4.16}$$

Define $B_{\varrho,u,v} = B^{mn^2(n+1)}b_{\varrho,u,v}$ so that each $B_{\varrho,u,v} \in \mathbb{Z}$. By Siegel's lemma (for example see Lemma 3.24 of [10]), there are integers T_ϱ for $\varrho = 0,1,\dots,2M$, not all zero, with $|T_\varrho| < (2M+1)\max|B_{\varrho,u,v}|$, such that $\sum_{\varrho=0}^{2M} T_\varrho B_{\varrho,u,v} = 0$ for all pairs (u,v) satisfying (4.3). By (4.4) and (4.15),

the integers T_ϱ satisfy

$$|T_\varrho| < (mn+1)B^{mn^2(n+1)}(4\lambda_1)^n(2R_0^{1/e})^{mn^2}\,. \tag{4.17}$$

Thus, from (4.6), we obtain

$$\begin{aligned} B^{mn^2(n+1)}&\sum_{\varrho=0}^{2M} T_\varrho F(x,y,\varrho) \\ &= B^{mn^2(n+1)}\sum_{\varrho=0}^{2M} T_\varrho P(x,y,\varrho) + B^{mn^2(n+1)}\sum_{\varrho=0}^{2M} T_\varrho E(x,y,\varrho). \end{aligned} \tag{4.18}$$

Put $Q(x,y) = B^{mn^2(n+1)}\sum_{\varrho=0}^{2M} T_\varrho P(x,y,\varrho)$; then $Q \in \mathbb{Z}[x,y]$, $\deg_y Q \le n-1$, $\deg_x Q \le m(n+1)$, and $Q(x,y) \not\equiv 0$ since $B^{mn^2(n+1)}T_\varrho$ is the coefficient of $x^\varrho y^{es_0}$ in $Q(x,y)$, and at least one of the integers T_ϱ is not zero. By combining (4.16) and (4.17),

$$\begin{aligned} \Big|B^{mn^2(n+1)}&\sum_{\varrho=0}^{2M} T_\varrho E(x,y,\varrho)\Big| \\ &< B^{mn^2(n+1)}(2M+1)(mn+1)B^{mn^2(n+1)} \\ &\quad\times (4\lambda_1)^n(2R_0^{1/e})^{mn^2}\max_{\varrho}|E(x,y,\varrho)| \\ &< B^{2mn^2(n+1)}(mn+1)^2(32\lambda_1^3)^n(2R_0^{1/e})^{2mn^2}(2(n+1))|x|^{-1/e}\,, \end{aligned} \tag{4.19}$$

provided that $|x| > 2^e R_0$. Put

$$\lambda_2 = B^{2mn^2(n+1)}(mn+1)^2(32\lambda_1^3)^n(2R_0^{1/e})^{2mn^2}(2(n+1))\,;$$

then for $|x| > \lambda_2^e$ we have $|B^{mn^2(n+1)}\sum_{\varrho=0}^{2M} T_\varrho E(x,y,\varrho)| < 1$.

If $(x,y) \in \mathbb{Z}^2$ satisfies (3.5) and $|x| \ge R_0$, then (x,y) satisfies $F(x,y,\varrho) = 0$ for $\varrho = 0,1,\dots,2M$. Thus, by (4.18) and (4.19), any such point (x,y) with $|x| > \lambda_2^e$ satisfies $Q(x,y) = 0$. Therefore the x-coordinate of such a point satisfies $\operatorname{res}_y(F(x,y),Q(x,y)) = 0$, and the y-coordinate satisfies $\operatorname{res}_x(F(x,y),Q(x,y)) = 0$. Since $\deg_y Q \le n-1 < \deg_y F$ and F is irreducible, $(F,Q) = 1$ and so both resultants are non-zero polynomials. By Lemma 1 of [8], it follows that

$$\begin{aligned} |x| &\le (h(m+1)\sqrt{n+1})^{n-1}((\text{height}\,Q)(mn+m+1)\sqrt{n})^n\,, \\ |y| &\le (h(n+1)\sqrt{m+1})^{m(n+1)}((\text{height}\,Q)n\sqrt{mn+m+1})^m. \end{aligned} \tag{4.20}$$

By (4.15) and (4.17),

$$\text{height}\,Q \le B^{2mn^2(n+1)}(mn+1)^2(4\lambda_1)^{2n}(2R_0^{1/e})^{2mn^2}\,, \tag{4.21}$$

hence the bounds in (1.2) now follow by combining (4.21) with (4.20). If $(x,y) \in \mathbb{Z}^2$ is an integer solution of $F(x,y) = 0$ satisfying (3.5) with $2^e R_0 <$

$|x| \le \lambda_2^e$, then by (4.12) we have $|y| < 2\lambda_1\lambda_2^f \le 2\lambda_1\lambda_2^m$, and again the bounds in (1.2) hold.

In the case that $(x, y) \in \mathbb{Z}^2$ is a solution of $F(x, y) = 0$ with $|x| \le 2^e R_0$, we see that y is then a root of a polynomial whose height does not exceed $(m + 1)(2^e R_0)^m h$, and so (1.2) holds in this case as well.

We complete the proof of Theorem 1 by considering the case that $f \le 0$. Let $(x, y) \in \mathbb{Z}^2$ be a solution of $F(x, y) = 0$ which satisfies (3.5). By the argument in the preceding paragraph, we may assume that $|x| > 2^e R_0$. It follows from (4.12) that $|y| < 2\lambda_1$, and so x is then a root of a polynomial whose height does not exceed $(n+1)(2\lambda_1)^n h$, and so (1.2) holds in this case.

2. By part 2 of Lemma 1 both of the algebraic functions x and y defined by $F(x, y) = 0$ have more than one class of conjugate Puiseux expansions. The bounds in (1.3) are obtained by taking the minimum of the bounds in (1.2) and those which are obtained from (1.2) with the roles of x and y interchanged.

5. Proof of Theorem 2. Assume without loss of generality that $\deg_x F > 0$. If $\deg_y F = 0$, then the irreducibility of F together with the assumption that $F(0, 0) = 0$ forces $F(x, y) = ax$ for some non-zero integer a. In this case, the only solutions of $F(x, y) = 0$ with $\gcd(x, y) = g$ are $(x, y) = (0, g)$ and $(x, y) = (0, -g)$. We therefore may assume that $\deg_y F > 0$.

Let $l \ge 1$ be the largest positive integer that divides all exponents of y in the non-zero monomials of F. Then $F(x, y)$ can be written as

$$F(x, y) = A_n(x)y^{nl} + A_{n-1}(x)y^{(n-1)l} + \ldots + A_0(x), \tag{5.1}$$

where $A_0(0) = 0$ and $A_0(x) \not\equiv 0$. Let k be the highest power of x dividing $A_0(x)$ and put $m = \max\{k, l\}$. If (x, y) is an integer solution of $F(x, y) = 0$ with $\gcd(x, y) = g$, then z defined by

$$z = \frac{A_0(x)g^m}{x^k y^l} \tag{5.2}$$

is an integer. Therefore, by putting $y^l = A_0(x)g^m/(x^k z)$ in (5.1) and factoring out the term $A_0(x)/(x^k z^n)$, it follows that the integers x and z satisfy $G(x, z) = 0$, where $G(x, z)$ is the polynomial defined by

$$G(x, z) = \sum_{i=0}^{n} A_i(x)(A_0(x)/x^k)^{i-1} g^{mi} z^{n-i}\,. \tag{5.3}$$

Our goal is to show that G satisfies the conditions of Theorem 1. It is clear that $G \in \mathbb{Z}[x, z]$, and is of positive degree in x and z. Moreover, since z^n has a non-constant coefficient, G does not satisfy (C_1) for the variable z. Thus it suffices to show that G is irreducible in $\mathbb{Q}[x, z]$.

Assume that $G = PQ$ for some $P, Q \in \mathbb{Z}[x,z]$. Let $P(x,z) = B_r(x)z^r + \ldots + B_0(x)$ and $Q(x,z) = C_s(x)z^s + \ldots + C_0(x)$, where $n = r+s$. Substituting $A_0(x)g^m/(x^k y^l)$ for z in the equation $G = PQ$ produces the polynomial equation

$$g^{nm}\left(\frac{A_0(x)}{x^k}\right)^{n-1} F(x,y) = \left[y^{lr}P\left(x, \frac{A_0(x)g^m}{x^k y^l}\right)\right]\left[y^{ls}Q\left(x, \frac{A_0(x)g^m}{x^k y^l}\right)\right]. \tag{5.4}$$

The two factors on the right hand side of (5.4) are polynomials in $\mathbb{Z}[x,y]$. The irreducibility of F in $\mathbb{Q}[x,y]$ forces one of the two factors, say $y^{lr}P(x, A_0(x)g^m/(x^k y^l))$, to be a polynomial in the variable x only. This implies that $P(x,z) = B_r(x)z^r$. By (5.3) and the fact that $A_n(x) \not\equiv 0$, it must be the case that $r = 0$, and so $P(x,z) = B_0(x)$. Again by (5.3), $B_0(x)$ must divide x^k, and so $P(x,z) = x^t$ for some t with $0 \le t \le k$. Thus, x^t divides the left hand side of (5.4). Since $A_0(x)/x^k$ has a non-zero constant term, it follows that x^t divides $F(x,y)$. Since F is irreducible and $\deg_y F > 0$, we must have $t = 0$. Therefore $P(x,z) = 1$, and so G is irreducible in $\mathbb{Q}[x,z]$.

By (5.3) we deduce that height $G \le g^{mn}(m+1)^{n-1}h^n$, $\deg_x G \le m(m-1)(n-1)$, and $\deg_z G \le n$. Since G does not satisfy condition (C_1) of the introduction, the result of Grytczuk and Schinzel provides a sharper estimate for $|x|$ than that in Theorem 1. Applying their result to G with z in the place of their x, and x as above in the place of their y, one obtains

$$|x| \le ((\deg_z G + 1)(\deg_x G + 1) \times (\deg_z G \deg_x G + 1)^{2/\deg_x G} \operatorname{height} G)^{2(\deg_z G \deg_x G + 1)^3}. \tag{5.5}$$

In the case that $m = n = 1$, it is easy to verify that $|x| \le gh$, so that the bound in (1.5) holds for $|x|$. If $mn > 1$ then $(\deg_x G+1)(\deg_z G+1) \le m^2n^2$, and so combining this estimate with that for $|x|$ in (5.5), the bound in (1.5) for $|x|$ follows. The same argument with the roles of x and y interchanged shows that the bound in (1.5) holds for $|y|$.

6. Proof of Theorem 3. Let $l > 1$ be a divisor of g, and put $n_0 = n/l$. If (x,y) is a solution of (1.6), then (x, y^{n_0}) is a solution of the superelliptic equation

$$y^l = P(x). \tag{6.1}$$

The bound in (1.7) will be obtained by applying Runge's method to equation (6.1).

The following result gives a precise description of the Puiseux expansions of the algebraic function y defined by (6.1).

LEMMA 2. *Let d, l, g, and $P(x)$ be as in the statement of Theorem* 3. *Let*

$$y = w(x) = \sum_{i=-s}^{\infty} c_i x^{-i/e} \tag{6.2}$$

be a Puiseux expansion of the algebraic function y defined by (6.1). *Then*

(i) *The l Puiseux expansions of y are given by $\zeta_l^j w(x)$, $j = 0, 1, \ldots, l-1$, where ζ_l denotes a primitive l-th root of unity.*

(ii) *The integers e and s satisfy $e = 1$ and $s = d/l$.*

(iii) *Exactly one of the l Puiseux expansions of y has leading coefficient equal to one and all of its coefficients rational. Moreover, if $w(x)$, given in* (6.2), *denotes this expansion, then $l^{2(d/l+i)-1} c_i \in \mathbb{Z}$ for all $i \geq -d/l + 1$.*

Proof. (i) follows from (6.1) and Puiseux's theorem. For (ii) and (iii), put $z = x^{-d} P(x)$ and apply Taylor's theorem to $z^{1/l}$, about $z_0 = 1$, to show that the l Puiseux expansions for y are given by

$$\zeta_l^t x^{d/l} \sum_{k=0}^{\infty} \binom{1/l}{k} \Big(\sum_{j=0}^{d-1} a_j x^{j-d} \Big)^k \qquad (0 \leq t \leq l-1)\,, \tag{6.3}$$

where the terms should be suitably arranged. It is now evident that $e = 1$ and $s = d/l$, which is (ii). The first statement in (iii) follows by putting $w(x)$ equal to that series in (6.3) with $t = 0$. The second statement in (iii) follows by observing that the coefficient c_i of x^{-i} in (6.2) is a linear combination, with integer coefficients, of the numbers $\binom{1/l}{k}$ with $0 \leq k \leq d/l + i$, and using the fact that $l^{2k-1}\binom{1/l}{k} \in \mathbb{Z}$ for each $k \geq 1$.

We now proceed with the proof of Theorem 3. Let $F(x, y) = y^l - P(x)$; then the resultant $\operatorname{res}_y(F, F_y) = (-P(x))^l l^l$, so that any finite singularity x of the algebraic function y defined by $F(x, y) = 0$ satisfies $P(x) = 0$, and hence satisfies $|x| < h + 1$. Thus, each of the Puiseux expansions of y is analytic for $|x| \geq h + 1$. Therefore any solution $(x, y) \in \mathbb{Z}^2$ of (6.1) with $|x| \geq h + 1$ satisfies $y = \zeta_l^j w(x)$ for some $0 \leq j \leq l - 1$, where $w(x)$ is chosen to be the unique Puiseux expansion of y with rational coefficients and leading coefficient equal to 1. With $w(x)$ chosen this way, it follows that only $\pm w(x)$ is real for integer values of x. Thus any solution $(x, y) \in \mathbb{Z}^2$ of (6.1) with $|x| \geq h + 1$ satisfies $y = \pm w(x)$. It is sufficient to consider those solutions which satisfy $y = w(x)$.

Let $m = d/l$, $t = x^{-1}$, $y = zt^{-m}$, and $b_j = c_{j-m}$ for $j \geq 0$. Then the series

$$z(t) = \sum_{j=0}^{\infty} b_j t^j \tag{6.4}$$

satisfies the polynomial equation

$$H(t,z) = t^{lm}F(t^{-1}, zt^{-m}) = z^l - 1 - a_{lm-1}t - \ldots - a_0 t^{lm} = 0\,.$$

Moreover, the series $z(t)$ in (6.4) is analytic for $|t| \le 1/(h+1)$. Fix $0 < r \le 1/(h+1)$; then for each $j \ge 0$,

$$|b_j| = \left| \frac{1}{2\pi i} \int\limits_{|t|=r} \frac{z(t)}{t^{j+1}}\, dt \right| \le \frac{1}{r^j} \max_{|t|=r} |z(t)|\,.$$

Either $|z(t)| \le 1$, or

$$\begin{aligned}\max_{|t|=r} |z(t)| &\le \max_{|t|=r} |z(t)|^l = \max_{|t|=r} |1 + a_{lm-1}t + \ldots + a_0 t^{lm}| \\ &\le h(1 + r + \ldots + r^{lm}) \le h(1 + 1/(h+1) + \ldots + (1/(h+1))^{lm}) \\ &= h + 1 - (1/(h+1))^{lm} < h + 1\,.\end{aligned}$$

In any case we have $\max_{|t|=r} |z(t)| < h+1$, and so by choosing $r = 1/(h+1)$ we see that

$$|b_j| \le (h+1)^{j+1}$$

for $j \ge 0$. Therefore,

$$|c_i| \le (h+1)^{i+m+1} \tag{6.5}$$

for $i \ge -m$.

By Lemma 2(iii), we have

$$l^{2(i+m)-1} c_i \in \mathbb{Z} \tag{6.6}$$

for $i \ge -m+1$. Put

$$Q(x) = l^{2m-1} \sum_{i=-m}^{0} c_i x^{-i} \quad \text{and} \quad E(x) = l^{2m-1} \sum_{i=1}^{\infty} c_i x^{-i}\,.$$

Then by (6.6), $Q \in \mathbb{Z}[x]$, $Q(x) \not\equiv 0$, and

$$l^{2m-1}(y - w(x)) = l^{2m-1}y - Q(x) - E(x)\,.$$

By (6.5),

$$\begin{aligned}|E(x)| &\le l^{2m-1} \sum_{j=1}^{\infty} |c_j|\, |x|^{-j} \le l^{2m-1}(h+1)^{m+2}|x|^{-1} \left(\sum_{j=0}^{\infty} \left(\frac{h+1}{|x|} \right)^j \right) \\ &< 2l^{2m-1}(h+1)^{m+2}|x|^{-1}\end{aligned}$$

provided that $|x| > 2(h+1)$. Thus

$$|E(x)| < 1$$

provided that $|x| > 2l^{2m-1}(h+1)^{m+2}$. Therefore, if $(x,y) \in \mathbb{Z}^2$ satisfies $y = w(x)$ with $|x| > 2l^{2m-1}(h+1)^{m+2}$, then $l^{2m-1}y = Q(x)$, and hence x

satisfies

$$l^{(2m-1)l}P(x) = Q(x)^l\,. \tag{6.7}$$

It is readily verified that equation (6.7) defines a polynomial whose height does not exceed $l^{(2m-1)l}(h+1)^{(m+1)l}(m+2)^l$, and the result follows.

Acknowledgements. I would like to thank my supervisor Cam Stewart for his many suggestions in the writing of this paper. I would also like to thank W. Schmidt, A. van der Poorten, B. Dwork, and A. Schinzel for providing preliminary versions of their papers, and showing interest in this work.

References

[1] Y. André, *G-functions and Geometry*, Vieweg, Braunschweig 1989.
[2] M. Ayad, *Sur le théorème de Runge*, Acta Arith. 58 (1991), 203–209.
[3] J. Coates, *Construction of rational functions on a curve*, Proc. Cambridge Philos. Soc. 68 (1970), 105–123.
[4] B. M. Dwork and A. J. van der Poorten, *The Eisenstein constant*, Macquarie Math. reports, report No.90-0062R (1991). (To appear in Duke Math. J.).
[5] M. Eichler, *Introduction to the Theory of Algebraic Numbers and Functions*, Academic Press, London 1966.
[6] G. Eisenstein, *Über eine allgemeine Eigenschaft der Reihen-Entwicklungen aller algebraischen Funktionen*, Bericht Königl. Preuss. Akad. d. Wiss. zu Berlin (1852), 441–443.
[7] W. J. Ellison, *Variations sur un thème de Carl Runge*, Séminaire Delange–Pisot–Poitou 13 (1970–71), 9.01–9.04.
[8] A. Grytczuk and A. Schinzel, *On Runge's theorem about diophantine equations*, to appear in Colloq. Math. Soc. J. Bolyai 60, 1992.
[9] C. Hermite, *Cours de M. Hermite rédigé en 1882*, 4th ed., Hermann, Paris 1891.
[10] 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.
[11] —, —, *On Puiseux series whose curves pass through an infinity of algebraic lattice points*, Bull. Amer. Math. Soc. (N.S.) 8 (1983), 59–62.
[12] D. W. Masser, *Polynomial bound for Diophantine equations*, Amer. Math. Monthly 93 (1980), 486–488.
[13] L. J. Mordell, *Diophantine Equations*, Academic Press, London 1969.
[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] W. M. Schmidt, *Eisenstein's theorem on power series expansions of algebraic functions*, Acta Arith. 56 (1990), 161–179.
[17] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge University Press, Cambridge 1986.

[18] T. Skolem, *Diophantische Gleichungen*, J. Springer, Berlin 1938; reprinted by Chelsea, New York 1950.
[19] V. G. Sprindžuk, *Classical Diophantine Equations in Two Unknowns*, Nauka, Moskva 1982 (in Russian).
[20] J. Turk, *On the difference between perfect powers*, Acta Arith. 45 (1986), 289–307.
[21] R. J. Walker, *Algebraic Curves*, Princeton University Press, Princeton, New Jersey, 1950.

DEPARTMENT OF PURE MATHEMATICS
THE UNIVERSITY OF WATERLOO
WATERLOO, ONTARIO, CANADA
N2L 3G1
E-mail: GWALSH@MANITOU.CSE.DND.CA

Received on 7.11.1991
and in revised form on 11.3.1992 (2189)