Estimates for the solutions of certain Diophantine equations by Runge's method

A. Sankaranarayanan and N. Saradha

Abstract :
We consider the two Diophantine equations $y^m = F(x)$ and $G(y) = F(x)$ under the assumption that $\gcd(m, \deg F) > 1$ and $\gcd(\deg G, \deg F) > 1$, respectively. We prove that the bounds for the denominator of the coefficients of the power series arising from the above two situations can be improved considerably and thus we establish improved upper bounds for the size of the solutions (namely for $|x|$ and $|y|$). [1] [2]

1 Introduction

In 1887, Runge showed that certain binary Diophantine equations have only finitely many solutions. An important feature of his result is that his method of proof is *effective*. We describe below the class of equations for which Runge proved his result. Let $f \in \mathbb{Z}[X, Y]$ be an irreducible polynomial with $\deg_X f = m$ and $\deg_Y f = n$. Suppose *at least one* of the following conditions *does not* hold :

(i) the highest power of X and Y in f occur as isolated terms aX^m and bY^n.

(ii) for every term $a_{ij}X^iY^j$ of f, we have $ni + mj \leq mn$.

(iii) the sum of all terms of f for which $ni + mj = mn$ is up to a constant factor a power of an irreducible polynomial.

[1]**AMS subject classification :** Primary 11D61, Secondary 11D41
[2]**Keywords :** Binary Diophantine equations, Runge's method, power series, denominator, prime number theorem.

Then f has only *finitely* many solutions. Explicit bounds for the solutions were given by Hilliker and Straus (see [4]). One of the ingredients in their proof is the quantitative version of Eisenstein's theorem on power series expansions of algebraic functions. The classical theorem of Eisenstein states that if a power series with rational coefficients represents an algebraic function and regular at the origin, then there exists an integer q such that $q^n a_n$ is an integer for each $n > 0$ where a_n denotes the coefficient of x^n in the power series. When the algebraic function satisfied by the power series is of some special type, then the value of q can be explicitly given, see for instance, Baker [1]. Dwork and van der Poorten (see [2]) have refined a result of Schmidt [9] to give a better bound for q in terms of quantities associated with the algebraic function. Using the result of [2], Walsh (see [12]) had provided better upper bounds for the solutions (x, y) of $f(x, y) = 0$ whenever f does not satisfy at least one of the conditions (i) to (iii). In some special cases of f, bounds for the denominators can be calculated by other means and this leads to improvement in the upper bounds for $\mid x \mid$ and $\mid y \mid$. For instance, suppose F and G are polynomials with integral coefficients, then

$$y^m = F(x) \text{ with } \gcd(m, \deg F) > 1; F(x) = G(y) \text{ with } \gcd(\deg F, \deg G) > 1$$

can be treated without appealing to quantitative version of Eisenstein's theorem. We refer to Walsh (see Theorem 3 of [12]) and Tengely ([10] or Chapter 2 of [11]) for details. In this paper our main purpose is to show that the bounds for the denominator of the coefficients of the power series arising in the above two situations can be improved considerably and this leads to improvement in the bounds for the solutions (see Theorems 4.1 and 5.1). We also present some generalisations to the above situation in section 6. We also extend and improve a result of Le (see [5]) on hyperelliptic equations.

We refer to Grytczuk and Schinzel ([3]) for a detailed study of Runge's method using Skolem's approach. We also refer to the papers [7] and [8] and several other papers mentioned there, in connection with equal products in arithmetic progression where the method used is reminiscent of Runge's method.

2 Denominator for the binomial coefficient $\binom{1/d}{k}$

Let $d > 1$ and $k \geq 1$ be integers. Let d be fixed. The binomial coefficient $\binom{1/d}{k}$ occurs in the power series expansion of the d-th root of a polynomial. The denominator of this coefficient determines the denominator of the coefficients of the power series. Hence it is desirable to get a good bound for the denominator of $\binom{1/d}{k}$. Let E_k denote the denominator of $\binom{1/d}{k}$. Since

$$\binom{1/d}{k} = \frac{1(1-d)(1-2d)\dots(1-(k-1)d)}{d^k\ k!}, \tag{2.1}$$

it is clear that

$$E_1 = d, \quad E_2 = \begin{cases} d^2 \text{ if } d \text{ is odd} \\ 2d^2 \text{ if } d \text{ is even} \end{cases} \tag{2.2}$$

and

$$E_k \leq d^k k! \tag{2.3}$$

The bound in (2.3) is rather large when k is large. We improve this in the following two lemmas. We denote by $Q^*(d), \omega(d)$ and $p(d)$, the square free part of d, the number of distinct prime divisors of d and the *least odd prime divisor* of d, respectively.

Lemma 2.1 *Let $k \geq 3$.*
(i) Let $d = p^\beta$ with p prime. Then

$$E_k \leq d^{k(1+\frac{1}{\beta(p-1)})}.$$

(ii) Let $\omega(d) \geq 2$. Then

$$E_k \leq \left(d\ Q^*(d)^{\frac{1}{p(d)+1}} p(d)^{\frac{2}{p^2(d)-1}}\right)^k \text{ if } d \text{ is odd}$$

and

$$E_k \leq \left(d\ Q^*(d)^{\frac{1}{p(d)+1}} p(d)^{\frac{2}{p^2(d)-1}} 2^{\frac{p(d)}{p(d)+1}}\right)^k \text{ if } d \text{ is even.}$$

Proof In (2.1), the numerator on the right hand side is a product of k terms in an arithmetic progression with common difference d. Hence it is divisible by all prime powers in $k!$ except by those prime powers dividing d. Thus, (for all $k \geq 1$) we have

$$E_k \leq d^k \prod_{p|d} p^{\mathrm{ord}_p(k!)} \leq d^k \prod_{p|d} p^{k(\frac{1}{p}+\frac{1}{p^2}+\cdots)} \leq d^k \prod_{p|d} p^{k/(p-1)}. \tag{2.4}$$

Let $d = p^\beta$. Then

$$E_k \leq d^k p^{k/(p-1)} = d^k \cdot d^{k/\beta(p-1)}$$

which gives *(i)*. Let $\omega(d) \geq 2$ and d odd. Then

$$1/(p-1) \leq 1/(p(d)+1) \text{ for } p \neq p(d)$$

and

$$\frac{1}{p(d)-1} = \frac{1}{p(d)+1} + \frac{2}{p^2(d)-1},$$

which proves the first assertion in *(ii)*.

Let $d = 2^\beta d_1$, with $d_1 > 1$, odd and $\beta > 0$. Then by (2.4),

$$E_k \leq (2d)^k \ \left(Q^*(d_1)\right)^{\frac{k}{p(d)+1}} \left(p(d)\right)^{\frac{2k}{p^2(d)-1}}.$$

Now the result follows on observing that $2Q^*(d_1) = Q^*(d)$.

□

As a consequence of Lemma 2.1 and (2.2), we get the following improvement of (2.3).

Corollary 2.2 *For all $k \geq 1$, we have*

$$E_k \leq \left(1.32\ d^{5/4}\right)^k \ \textit{if } d \textit{ is odd or if } d = 2^\beta,\ \beta \geq 4$$

and

$$E_k \leq \left(2.64\ d^{5/4}\right)^k \ \textit{otherwise.}$$

Remark 1. Let $p_1(d)$ denote the least prime divisor of d. For $d \geq 2$ and $k \geq 1$, we get from (2.4) the estimate

$$
\begin{aligned}
E_k &\leq d^k \ \exp\left(k \sum_{p|d} \frac{\log p}{p-1}\right) \leq d^k \ \exp\left(k \ \frac{\log p_1(d)}{p_1(d)-1} \sum_{p|d} 1\right) \\
&\leq \begin{cases} d^k \ \exp\left(k \ \omega(d) \ \log 2\right) & \text{if } d \text{ is even} \\ d^k \ \exp\left(k \ \omega(d) \ \frac{\log 3}{2}\right) & \text{if } d \text{ is odd.} \end{cases}
\end{aligned}
$$

It is well known that $\omega(d)$ has normal order as $\log\log d$, i.e, for almost all d, we have

$$
|\omega(d) - \log\log d| < (\log\log d)^{\frac{1}{2}+\delta}
$$

for any $\delta > 0$. Thus, it is reasonable to expect an upper bound for E_k as $d^k \ (\log d)^k$ for almost all d. Towards this, we prove the following lemma which is of independent interest.

Lemma 2.3 *Let $d \geq 2$ be an integer. Then, for $k \geq 1$, we have the estimate*

$$
E_k \leq d^k \ (\log d)^k \ e^{2k}.
$$

Proof First of all we prove the desired estimate assuming $d > e^e$. As seen in the Remark 1,

$$
E_k \leq d^k \ \exp\left(k \sum_{p|d} \frac{\log p}{p-1}\right). \tag{2.5}
$$

Let $y = \log d$. Since $\log d$ is an increasing function of d for $d > e^e$, we have $y > e$. We write

$$
\begin{aligned}
\sum_{p|d} \frac{\log p}{p-1} &= \sum_{p|d} \frac{\log p}{p} + \sum_{p|d} \frac{\log p}{p(p-1)} \\
&\leq \sum_{\substack{p|d \\ p \leq y}} \frac{\log p}{p} + \sum_{\substack{p|d \\ p > y}} \frac{\log p}{p} + \sum_{p \geq 2} \frac{\log p}{p(p-1)} \qquad (2.6) \\
&:= S_1 + S_2 + S_3 \ \text{ say.}
\end{aligned}
$$

Using the estimate

$$\sum_{p\le y}\frac{\log p}{p}\le \log y$$

for which we refer to the inequality (3.24) on page 70 of [6], we obtain

$$S_1\le \log y\le \log\log d \tag{2.7}$$

and

$$S_2\le \frac{\log d}{y}=1 \tag{2.8}$$

by the choice of y. We note that

$$\sum_{p\le 13}\frac{\log p}{p(p-1)}<0.7$$

by direct computation. Using integration by parts, we observe that

$$\begin{aligned}\frac{17}{16}\left(\frac{\log 17}{(17)^2}+\int_{\log 17}^{\infty} t\ e^{-t}dt\right) &= \frac{17}{16}\left(\frac{\log 17}{(17)^2}+\frac{\log 17}{17}+\frac{1}{17}\right)\\ &= \frac{17+18\log 17}{272}\\ &< \frac{1}{4}.\end{aligned}$$

Hence, we have

$$\begin{aligned}S_3 &= \sum_{p\ge 2}\frac{\log p}{p(p-1)}\\ &\le \sum_{2\le p\le 13}\frac{\log p}{p(p-1)}+\frac{17}{16}\left(\sum_{n\ge 17}\frac{\log n}{n^2}\right)\\ &\le \sum_{p\le 13}\frac{\log p}{p(p-1)}+\frac{17}{16}\left(\frac{\log 17}{(17)^2}+\int_{\log 17}^{\infty} t\ e^{-t}dt\right)\\ &\le 0.7+0.25\\ &< 1.\end{aligned} \tag{2.9}$$

From (2.6), (2.7), (2.8) and (2.9), we get

$$\sum_{p|d} \frac{\log p}{p-1} \leq \log\log d + 2. \tag{2.10}$$

The lemma follows from (2.5) and (2.10) whenever $d > e^e$.

If $d \in \{2, 3, 4, 5, \cdots, 23\}$, we compute E_k explicitly from (2.2) and (2.4) and verify that the bound in Lemma 2.3 still holds for these values of d too. Thus we obtain the desired estimate for all $d \geq 2$.

□

Remark 2. Let $d > e^{32}$. Then from inequality (3.23) of [6], we have

$$S_1 \leq \log y - 1.0439.$$

Thus we get

$$E_k \leq d^k \ (e \ \log d)^k.$$

This upper bound is better than the bounds given in Corollary 2.2.

Now, we define

$$\rho = \begin{cases} d^2 & \text{if } \ d = 2, \\ \min\left(1.32 \ d^{\frac{5}{4}}, \ d \ (\log d) \ e^2\right) & \text{if } d \geq 3 \text{ with } d \text{ odd} \ \text{ or } d = 2^\beta \text{ with } \beta \geq 4, \\ \min\left(2.64 \ d^{\frac{5}{4}}, \ d \ (\log d) \ e^2\right) & \text{otherwise.} \end{cases} \tag{2.11}$$

Hence we have for $d \geq 2$,

$$E_k \leq \rho^k \ \text{ for } \ \text{all } k \geq 1. \tag{2.12}$$

3 The d-th root of a polynomial

We are interested in a particular case of the theory of Puiseux expansions of algebraic functions. To motivate our situation we consider a monic polynomial

$$A(X) = X^r + a_1 X^{r-1} + \cdots + a_r \in \mathbb{Z}[X].$$

Suppose $d > 1$ is a divisor of r. Let

$$B(X) = A(X)^{1/d}.$$

Then

$$B(X) = X^{r/d}\left(1 + \frac{a_1}{X} + \cdots + \frac{a_r}{X^r}\right)^{1/d} = X^{r/d}\sum_{j\geq 0} c_j X^{-j}$$

with

$$c_j = \sum_{t=1}^{j} \binom{1/d}{t} \sum{}' \frac{t!}{i_1! \cdots i_r!} a_1^{i_1} \cdots a_r^{i_r} \tag{3.1}$$

where the inner sum $\sum'$ is taken over all tuples $(i_1, \cdots, i_r)$ such that $i_1 + \cdots + i_r = t$ and $i_1 + 2i_2 + \cdots + ri_r = j$. Hence c_j are rational numbers with denominator bounded by E_j where E_j is the denominator of $\binom{1/d}{j}$. The fact that $B(X)$ is the unique Puiseux (in fact Laurent) series with rational coefficients follows from the theory of Puiseux expansions. The series converges for $\mid X \mid \geq h+1$ where $h = h(A) =$ height of $A(X)$. We refer to [12] for details. Now we give an estimate for $\mid c_j \mid$. Consider

$$B_1(X) = X^{r/d}\left(1 - \left(\frac{\mid a_1 \mid}{X} + \cdots + \frac{\mid a_r \mid}{X^r}\right)\right)^{-1/d} = X^{r/d}\sum_{j\geq 0} d_j X^{-j}.$$

Then we observe that all $d_j > 0$ and

$$\mid c_j \mid \leq d_j.$$

Let $X = X_0$ be fixed. Then

$$d_j \leq X_0^j \left(d_0 + \frac{d_1}{X_0} + \cdots + \frac{d_j}{X_0^j} + \cdots\right) \leq X_0^j \left(1 - \frac{h}{X_0 - 1}\right)^{-1/d}.$$

Take $X_0 = h + 2$. Then

$$d_j \leq (h+2)^j \left(\frac{1}{h+1}\right)^{-1/d} \leq (h+2)^{j+\frac{1}{d}}.$$

Summarizing, we get the following lemma.

Lemma 3.1 *Let $d > 1$. Suppose $A(X)$ is a monic polynomial with integral coefficients and of degree $r = dr_0$. Then there exists a Laurent expansion*

$$B(X) = \sum_{i \geq 0} c_i X^{r_0 - i}$$

satisfying

$$B^d(X) = A(X) \tag{3.2}$$

such that $c_0 = 1$ and if D_i denotes the denominator of c_i, then

$$D_i \leq E_i \leq (\rho)^i \quad \textit{for } i > 0,$$

where

$$\rho \ \textit{is as in } (2.11). \tag{3.3}$$

Thus for any nonzero c_i, we have

$$|c_i| \geq \frac{1}{\rho^i}. \tag{3.4}$$

Further

$$| \ c_i \ | \leq (h(A) + 2)^{i+1/d} \ \textit{for } i > 0.$$

The next lemma is an extension of a result of Le (see [5]). This again deals with the fractional powers of polynomials.

Lemma 3.2 *Let $d > 1$ with $d|r$. Suppose*

$$A(X) = X^r + a_s X^s + \cdots + a_r \in \mathbb{Z}[X], \ a_s \neq 0.$$

Assume that for any prime $p|d$,

$$\text{ord}_p\,(a_s) < \frac{ds}{r + ds}\ \text{ord}_p(d). \tag{3.5}$$

Then there exists a Laurent expansion as in Lemma 3.1 satisfying (3.2) such that

$$c_{qs} \neq 0 \quad \textit{for any positive integer } q \leq \frac{r}{ds} + 1.$$

Note that (3.5) is satisfied whenever $\gcd(a_s, r) = 1$. As the proof is simple, we present it here.

Proof Let $q \le \frac{r}{ds} + 1$. In the present situation the formula (3.1) becomes

$$c_{qs} = \sum_{t=1}^{qs} \sum{}' \frac{\frac{1}{d}\left(\frac{1}{d}-1\right)\cdots\left(\frac{1}{d}-(t-1)\right)}{i_s! \ \cdots i_r!} a_s^{i_s} \cdots a_r^{i_r}, \tag{3.6}$$

where $\sum'$ denotes the summation taken over all tuples $(i_s, \cdots, i_r)$ such that $i_s + \cdots + i_r = t$ and $si_s + \cdots + ri_r = qs$. Corresponding to the tuple $(i_s, \cdots, i_r) = (q, 0, \cdots, 0)$, we get a term

$$c' = \frac{(1-d)\cdots(1-(q-1)d)}{q! \ d^q} \ a_s^q.$$

Thus, for any prime $p|d$,

$$\begin{aligned} \mathrm{ord}_p(\text{denominator of } c') &= q \ \mathrm{ord}_p(d) + \mathrm{ord}_p(q!) - q \ \mathrm{ord}_p(a_s) \\ &> (q-1) \ \mathrm{ord}_p(d) + \mathrm{ord}_p(q!) \end{aligned}$$

by (3.5) and $q \le \frac{r}{ds} + 1$. For any other tuple $(i_s, \cdots, i_r) \ne (q, 0, \cdots, 0)$, we find that $0 < i_s + \cdots + i_r = t < q$. Hence from (3.6), it is clear that for any other term c'', corresponding to $(i_s, \cdots, i_r) \ne (q, 0, \cdots, 0)$, we have

$$\begin{aligned} \mathrm{ord}_p(\text{denominator of } c'') &\le t \ \mathrm{ord}_p(d) + \mathrm{ord}_p(i_s! \cdots i_r!) \\ &\le (q-1) \ \mathrm{ord}_p(d) + \mathrm{ord}_p((q-1)!). \end{aligned}$$

Hence $c_{qs} \ne 0$.

□

Let us denote by $B_0(X)$, the polynomial part of $B(X)$ i.e.,

$$B_0(X) = X^{r_0} + c_1 X^{r_0 - 1} + \cdots + c_{r_0}.$$

Then by Lemma 3.1, we find

$$h(B_0) \le (h(A) + 2)^{r_0 + \frac{1}{d}}. \tag{3.7}$$

4 The equation $y^m = F(x)$

In this section we consider the equation

$$y^m = F(x) \tag{4.1}$$

where $F(x)$ is a monic polynomial with integer coefficients of degree n and $\gcd(m, n)$ is divisible by an integer $d > 1$. In this case, Walsh has given upper bounds for the solution (x, y) (see Theorem 3 of [12]). Under the assumption that

$$Y^m - F(X) \text{ is irreducible} \tag{4.2}$$

he has shown that

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

We shall improve this in the following theorem.

Theorem 4.1 *(i). Suppose* (4.1) *holds with* (4.2) *and* $d|\gcd(m, n)$*. Then*

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

where ρ *is as given in* (2.11)*.*
(ii). Suppose (4.1) *holds with* (4.2) *and* $m|n$*. Let*

$$F(X) = X^n + a_s X^s + \cdots + a_n \quad \textit{with} \quad a_s \neq 0$$

and for any prime $p|m$*,*

$$\mathrm{ord}_p\,(a_s) < \frac{ms}{n + ms}\,\mathrm{ord}_p(m).$$

Then

$$|x| \leq 2\rho^{\frac{2n}{m}} (h(F) + 2)^{\frac{n+1}{m}+1}$$

where ρ *is as given in* (2.11)*.*

Remark 3. Part (ii) of Theorem 4.1 gives a better bound for $|x|$ compared to the bound obtained by Le (see [5]). Further the condition on a_s here is more relaxed than Le's condition of $\gcd(a_s, m) = 1$.

The next lemma is a result on the height of products of polynomials. As the proof is simple, we record it here.

Lemma 4.2 *Let* $P(X) = a_0 + a_1X + \cdots + a_rX^r \in \mathbb{Z}[X]$. *Then for any integer* $t > 0$,

$$h\left(P^t(X)\right) \leq \{(r+1)h(P)\}^t.$$

Further if $Q(X) = b_0 + b_1X + \cdots + b_sX^s \in \mathbb{Z}[X]$, *then*

$$h(PQ) \leq (r+s+1)\ h(P)\ h(Q).$$

Proof Let

$$P^t(X) = \sum_{j=0}^{rt} b_j X^j.$$

Then

$$b_j = \sum{}' \frac{t!}{i_0! \cdots i_r!} a_0^{i_0}\ a_1^{i_1} \cdots a_r^{i_r}$$

where the sum is taken over all tuples $(i_0, \cdots, i_r)$ with $i_0 + \cdots + i_r = t$ and $i_1 + 2i_2 + \cdots + ri_r = j$. Thus

$$\mid b_j \mid \leq h^t(P) \sum{}'' \frac{t!}{i_0! \cdots i_r!}$$

where $\sum''$ denotes the sum over all $(i_0, \cdots, i_r)$ with $i_0 + \cdots + i_r = t$. Hence

$$\mid b_j \mid \leq h^t(P)(r+1)^t.$$

Let

$$P(X)\ Q(X) = \sum_{j=0}^{r+s} c_j X^j.$$

Then

$$c_j = \sum_{i_1+i_2=j} a_{i_1}\ b_{i_2}.$$

Hence

$$|c_j| \le h(P)h(Q) \sum_{i_1+i_2=j} 1 = h(P)h(Q)(j+1).$$

Thus

$$h(PQ) \le (r+s+1)h(P)h(Q).$$

□

Proof of Theorem 4.1 (i) : Suppose (x, y) is a solution of (4.1). Since d divides $\gcd(m, n)$, we find that $(x, y^{m/d})$ is a solution of the equation

$$y^d = F(x). \tag{4.3}$$

We consider the polynomial

$$Y^d = F(X).$$

We take the d-th root on either side and use Lemma 3.1 to find

$$Y = \sum_{i\ge 0} f_i X^{\frac{n}{d}-i}$$

satisfying $f_0 = 1$ and if D_i denotes the denominator of f_i, then

$$D_i \le (\rho)^i \text{ for } i > 0$$

and

$$| f_i | \le (h(F)+2)^{i+1/d} \text{ for } i > 0.$$

Now we write

$$Y = U_0(X) + V_0(X)$$

where

$$U_0(X) = X^{n/d} + f_1 X^{n/d-1} + \cdots + f_{n/d-1}X + f_{n/d} \ ; \ V_0(X) = \sum_{i>0} f_{\frac{n}{d}+i} X^{-i}.$$

By (3.7) with $A = F,\ B_0 = U_0$ and $r_0 = n/d$, we get

$$h(U_0) \leq (h(F)+2)^{(n+1)/d}. \tag{4.4}$$

Let D be the denominator of $f_1, \cdots, f_{n/d}$. Then

$$D \leq (\rho)^{n/d}. \tag{4.5}$$

We estimate

$$| DV_0(X) | \leq \frac{D(h(F)+2)^{\frac{n+1}{d}+1}}{X}\left(1+\frac{h(F)+2}{X}+\frac{(h(F)+2)^2}{X^2}+\cdots\right).$$

Suppose $|X| > 2D\,(h(F)+2)^{\frac{n+1}{d}+1}$. Then we get

$$| DV_0(X) | < 1.$$

Thus

$$| DY - DU_0(X) | < 1.$$

Taking $X = x,\ Y = y$, we conclude that for $|x| > 2D\,(h(F)+2)^{\frac{n+1}{d}+1}$, we have

$$y = U_0(x), \tag{4.6}$$

which gives

$$F(x) = (U_0(x))^d.$$

Hence

$$G(X) = D^d F(X) - (DU_0(X))^d$$

defines a polynomial with integral coefficients of degree $\leq n$ such that $G(x) = 0$. Further by (4.4) and Lemma (4.2), $G(X)$ is of height

$$h(G) \leq D^d\,(h(F)+2)^{n+1}\left(\frac{n}{d}+1\right)^d.$$

The result follows from (4.5).

Proof of Theorem 4.1 (ii) : We follow the proof of Le ([5]). We may also apply part (i) above with $d = m$, since $m|n$. Assume that $|x| > 2D\,(h(F)+2)^{\frac{n+1}{m}+1}$. From (4.6), we get

$$V_0(x) = 0. \tag{4.7}$$

Also from (4.1), we have

$$y^m = x^n + a_s x^{n-s} + \cdots + a_n.$$

Hence

$$0 < |y^m - x^n| \le 2\ h(F)\ |x|^{n-s}.$$

As $y \neq x^{\frac{n}{m}}$, we get for $|x| > m$,

$$|y^m - x^n| \ge m\ |x|^{n-\frac{n}{m}} - \frac{2}{3}\ m\ |x|^{n-\frac{n}{m}} = \frac{1}{3}\ m\ |x|^{n-\frac{n}{m}}.$$

Thus,

$$s < \frac{n}{m}. \tag{4.8}$$

We observe that there exists t with $\frac{n}{m} < t \le \frac{n}{m} + s$ such that $f_t \neq 0$, by Lemma 3.2 since there is a multiple of s in this interval. Let t_0 be the least such t. Thus, from (4.8), we have

$$f_{t_0} \neq 0 \ \text{ with } t_0 \le \frac{2n}{m}, \quad f_t = 0 \ \text{ for } \frac{n}{m} < t < t_0.$$

Hence

$$V_0(x) = f_{t_0} x^{-\left(t_0 - \frac{n}{m}\right)} + \cdots \tag{4.9}$$

From (3.4), we have

$$\frac{|f_{t_0}|}{|x|^{t_0-\frac{n}{m}}} \ge \frac{1}{\rho^{t_0}|x|^{t_0-\frac{n}{m}}}.$$

Now,

$$\left|f_{t_0+1}x^{-\left(t_0+1-\frac{n}{m}\right)}+\cdots\right| \le \frac{(h(F)+2)^{t_0+1+\frac{1}{m}}}{|x|^{t_0+1-\frac{n}{m}}}\times$$
$$\times\left(1+\frac{h(F)+2}{|x|}+\frac{(h(F)+2)^2}{|x|^2}+\cdots\right)$$
$$\le \frac{2\left(h(F)+2\right)^{t_0+1+\frac{1}{m}}}{|x|^{t_0+1-\frac{n}{m}}}.$$

Thus

$$\begin{aligned}|V_0(x)| &\ge \left|f_{t_0}x^{-(t_0-\frac{n}{m})}\right| - \left|f_{t_0+1}x^{-(t_0+1-\frac{n}{m})}+\cdots\right| \\ &\ge \frac{1}{\rho^{\frac{2n}{m}}|x|^{t_0-\frac{n}{m}}} - \frac{2(h(F)+2)^{t_0+1+\frac{1}{m}}}{|x|^{t_0+1-\frac{n}{m}}} \\ &\ge \frac{|x|^{t_0+1-\frac{n}{m}} - 2\rho^{\frac{2n}{m}}(h(F)+2)^{t_0+1+\frac{1}{m}}|x|^{t_0-\frac{n}{m}}}{\rho^{\frac{2n}{m}}|x|^{t_0+1-\frac{2n}{m}}}.\end{aligned}$$

Thus if $|x| > 2\rho^{\frac{2n}{m}}(h(F)+2)^{\frac{n}{m}+1+\frac{1}{m}}$, then

$$V_0(x) \ne 0.$$

This is a contradiction to (4.7).

□

5 The equation $F(x) = G(y)$

In this section we consider the equation

$$F(x) = G(y) \tag{5.1}$$

where $F(x)$ and $G(y)$ are monic polynomials of degree n and m with $\gcd(n, m)$ divisible by $d > 1$. Without loss of generality, we assume that $m > n$. Further let $G(Y) \ne Y^m$ as this case has already been dealt with in Section 4. Tengley has given upper bounds for the solution (x, y), (see [10] and his Thesis [11]). Thus under the assumption

$$F(X) - G(Y) \text{ is irreducible} \tag{5.2}$$

he has shown that

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

where $H = \max(h(F), h(G))$. In the following theorem, we improve the exponents of d and $H+1$ in the above result.

Theorem 5.1 *Suppose* (5.1) *holds with* (5.2). *Then*

$$| x | \leq (H+2)^{\frac{m(m+2)}{d}}(\rho)^{m^2/d}\left((n+1)^{1/d}(m+1)^{1/2d}\left(\frac{n}{d}+1\right)\left(\frac{m}{d}+1\right)^{1/2}\right)^m$$

and

$$| y | \leq (H+2)^{\frac{n(n+2)}{d}}(\rho)^{n^2/d}\left((m+1)^{1/d}(n+1)^{1/2d}\left(\frac{m}{d}+1\right)\left(\frac{n}{d}+1\right)^{1/2}\right)^n.$$

We need the following lemma of Grytchuk and Schinzel [GS].

Lemma 5.2 *Let* $P, Q \in \mathbb{Z}[X, Y]$ *with* $\gcd(P, Q) = 1, \ \deg_X P = p_1, \deg_Y P = p_2 \ ; \ \deg_X Q = q_1, \ \deg_Y Q = q_2$. *If*

$$P(x, y) = Q(x, y) = 0,$$

then

$$| x | \leq (h(P)(p_1+1)\sqrt{p_2+1})^{q_2}(h(Q)(q_1+1)\sqrt{q_2+1})^{p_2}$$

and

$$| y | \leq (h(P)(p_2+1)\sqrt{p_1+1})^{q_1}(h(Q)(q_2+1)\sqrt{q_1+1})^{p_1}.$$

Proof of Theorem 5.1. We write the d-th root of $F(X)$ and $G(Y)$ as

$$(F(X))^{1/d} = F_0(X) + F_1(X) \text{ and } (G(Y))^{1/d} = G_0(Y) + G_1(Y)$$

with $F_0(X)$ and $G_0(Y)$ denoting the polynomial parts. Taking $X = x, \ Y = y$, we get

$$(F_0(x) + F_1(x))^d = F(x) = G(y) = (G_0(y) + G_1(y))^d \,.$$

Thus

$$F_0(x) + F_1(x) = \pm \left(G_0(y) + G_1(y)\right)$$

as we are interested only in real roots.

Let

$$H_0 := \max\left(h(F_0),\ h(G_0)\right).$$

Then by Lemma 3.1,

$$H_0 \le (H+2)^{\frac{m+1}{d}}.$$

We consider the case

$$F_0(x) + F_1(x) = G_0(y) + G_1(y). \tag{5.3}$$

The other case is similar. Let D denote the maximum of the denominators for the polynomials $F_0(X)$ and $G_0(Y)$. Then it is clear that as $m > n$,

$$D \le (\rho)^{m/d}.$$

We have

$$\mid D\left(F_0(x) - G_0(y)\right) \mid = \mid D\left(G_1(y) - F_1(x)\right) \mid \le \mid DG_1(y) \mid + \mid DF_1(x) \mid . \tag{5.4}$$

Arguing as in Section 3, we see that for

$$x > 4D\left(h(F_0) + 2\right)^{\frac{n+1}{d}+1} \text{ and } y > 4D\left(h(G_0) + 2\right)^{\frac{m+1}{d}+1} \tag{5.5}$$

the right hand side of (5.4) can be made < 1. Since the left hand side is an integer, for $x, y > 4D(H+2)^{\frac{m+1}{d}+1}$, we get

$$F_0(x) = G_0(y). \tag{5.6}$$

Now consider the two polynomials

$$R(X, Y) = F(X) - G(Y)$$

and

$$R_0(X,Y) = D\left(F_0(X) - G_0(Y)\right).$$

By assumption and (5.6), we find that (x, y) is a solution of both R and R_0. Since $F(X) - G(Y)$ is irreducible and $R_0(X,Y)$ is of degree n/d and m/d with respect to X and Y, respectively, we see that $\gcd(R, R_0) = 1$. Now we apply Lemma 5.2, to get

$$\begin{aligned} \mid x \mid &\leq \left(H(n+1)\sqrt{m+1}\right)^{\frac{m}{d}} \left(DH_0\left(\frac{n}{d}+1\right)\sqrt{m/d+1}\right)^{m} \\ &\leq H^{m/d} H_0^m \left(\rho\right)^{m^2/d} (n+1)^{m/d} \left(\frac{n}{d}+1\right)^{m} (m+1)^{m/2d} \left(\frac{m}{d}+1\right)^{m/2}. \end{aligned}$$

This gives the required bound. The upper bound for $\mid y \mid$ is obtained similarly.

□

Remark 3. In [7], [8] and the papers mentioned in them, the special equation

$$(x+1)\cdots(x+k) = (y+1)\cdots(y+mk)$$

has been studied extensively. According to our notation, here $F(X) = (X+1)\cdots(X+k)$ and $G(Y) = (Y+1)\cdots(Y+mk)$. Using the properties of consecutive integers, it has been shown in [7] that this equation implies that

$$\max(x, y, k) \leq C(m)$$

where $C(m)$ is an effectively computable number depending only on m. Further it has been shown that the above equation with $2 \leq m \leq 6$ has the only solution $8.9.10 = 6!$.

Remark 4. Tengely (see [11]) has given an algorithm to solve completely an equation of the type considered in this section. Using this algorithm, he solves equations

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

$$x(x+1)(x+2)(x+3) = y(y+1)\cdots(y+5),$$

and several other equations of similar type.

6 Some generalizations

The equations considered in sections 4 and 5 can be generalized as follows. we consider $P(X),\ Q(X)\ (\neq 1) \in \mathbb{Z}[X]$ where

$$P(X) = X^{r_1} + a_1 X^{r_1-1} + \cdots + a_{r_1} \text{ and } Q(X) = X^{r_2} + b_1 X^{r_2-1} + \cdots + b_{r_2}$$

with $r_1 > r_2$. Let

$$Q(x)\ y^m = P(x) \tag{6.1}$$

with gcd $(m, r_1 - r_2)$ divisible by an integer $d > 1$. Let

$$r_0 d = r_1 - r_2 \text{ and } h = \max\left(h(P), h(Q)\right).$$

Also assume that

$$Q(X)\ Y^m - P(X) \text{ is irreducible over } \mathbb{Q}.$$

Then (6.1) implies that

$$|x| \leq \rho^{r_1-r_2}\,(r_1+1)\,h(Q)\left(\frac{r_1-r_2}{d}+1\right)^d (h+2)^{r_1-r_2+2}. \tag{6.2}$$

To achieve this, we need to compute the d-th root of the rational function $P(X)/Q(X)$ as in section 3. Let $|X| > h+1$ and

$$R(X) = \left(\frac{P(X)}{Q(X)}\right)^{1/d}.$$

Then

$$\begin{aligned} R(X) &= X^{r_0}\left(1+\frac{a_1}{X}+\cdots+\frac{a_{r_1}}{X^{r_1}}\right)^{1/d}\left(1+\frac{b_1}{X}+\cdots+\frac{b_{r_2}}{X^{r_2}}\right)^{-1/d} \\ &= X^{r_0}\sum_{j\geq 0} C_j X^{-j}. \end{aligned}$$

It is easy to see if E_j is the denominator of C_j, then

$$E_j \leq \rho^j$$

where ρ is as in (2.11). Further $R(X)$ is dominated by the product

$$X^{r_0}\left(1-\left(\frac{|a_1|}{X}+\cdots+\frac{|a_{r_1}|}{X^{r_1}}\right)\right)^{-1/d}\left(1-\left(\frac{|b_1|}{X}+\cdots+\frac{|b_{r_2}|}{X^{r_2}}\right)\right)^{-1/d}.$$

Hence as in section 3, we find that

$$|C_j| \le (h+2)^j \left(\frac{1}{h+1}\right)^{-2/d} \le (h+2)^{j+2/d}.$$

Now we proceed as in section 4. Writing

$$R(X) = R_0(X) + R_1(X)$$

where $R_0(X)$ is the polynomial part of $R(X)$, we find that for
$x > 2\ \rho^{r_0}\ (h+2)^{r_0+\frac{2}{d}}$, we get

$$y = R_0(x)$$

giving

$$\frac{P(x)}{Q(x)} = \left(R_0(x)\right)^d.$$

Thus x satisfies the equation

$$D^d\ P(x) - Q(x)\ \left(D\ R_0(x)\right)^d = 0.$$

Now we use Lemma 4.2 to compute the height of the polynomial on the left hand side which leads to the estimate in (6.2).

Our next equation generalizes the one in section 5. We consider the equation

$$R_1(x) = R_2(y) \tag{6.3}$$

where $R_1(X)$ and $R_2(Y)$ are rational functions of the form

$$R_1(X) = \frac{P_1(X)}{Q_1(X)}\ ,\ R_2(Y) = \frac{P_2(Y)}{Q_2(Y)}$$

where P_1, Q_1, P_2, Q_2 are monic polynomials with integral coefficients. We assume that

$$P_1(X)\ Q_2(Y) - P_2(Y)\ Q_1(X) \text{ is irreducible.} \tag{6.4}$$

Further, let deg $P_i = p_i$, deg $Q_i = q_i$ and $p_i > q_i$ for $i = 1, 2$. we assume that there exists an integer $d > 1$ such that

$$d |\gcd(p_1 - q_1,\ p_2 - q_2).$$

Let $h = \max(h(P_1), h(Q_1), h(P_2), h(Q_2))$ and $r = \max(p_1 - q_1,\ p_2 - q_2)$. We argue as in section 5. We write

$$R_1(X) = R_1^{(0)}(X) + R_1^{(1)}(X), \quad R_2(Y) = R_2^{(0)}(Y) + R_2^{(1)}(Y)$$

where $R_1^{(0)}(X)$, $R_2^{(0)}(Y)$ are the polynomial parts of $R_1(X)$ and $R_2(Y)$, respectively. We find that for $x > 4\ \rho^{\frac{r}{d}}\ (h+2)^{\frac{r}{d}+2}$ and $y > 4\ \rho^{\frac{r}{d}}\ (h+2)^{\frac{r}{d}+2}$,

$$R_1^{(0)}(x) = R_2^{(0)}(y).$$

Thus (x, y) is a solution of

$$R(X, Y) = P_1(X)\ Q_2(Y) - Q_1(X)\ P_2(Y)$$

and

$$R_0(X, Y) = D\left(R_1^{(0)}(X) - R_2^{(0)}(Y)\right).$$

Further $\gcd(R, R_0) = 1$ by the assumption (6.4). Now we apply Lemma 5.2 to get

$$|x| \le \rho^{\frac{rp_2}{d}} (h+2)^{\frac{r(p_2+2)+p_2}{d}}\ (p_1+1)^{\frac{2r}{d}}\ (p_2+1)^{\frac{3r}{2d}} \left(\frac{r}{d}+1\right)^{\frac{3p_2}{2}}$$

and

$$|y| \le \rho^{\frac{rp_1}{d}} (h+2)^{\frac{r(p_1+2)+p_1}{d}}\ (p_2+1)^{\frac{2r}{d}}\ (p_1+1)^{\frac{3r}{2d}} \left(\frac{r}{d}+1\right)^{\frac{3p_1}{2}}.$$

References

[1] A. Baker, *Power series representing algebraic functions*, J. London Math Soc., **40** (1965), 108-110.

[2] B.M. Dwork and A.J. van der Poorten, *The Eisenstein constant*, Duke Math. J., **65** (1992), no 1, 23-43, *Corrections to : The Eisenstein constant*, Duke Math.J., **76** (1994), no.2, 669-672.

[3] A. Grytczuk and A. Schinzel, *On Runge's theorem about Diophantine equations*, In Sets, graphs and numbers (Budapest, 1991), **60** of Colloq. Math. Soc., J'anos Bolyai, pages 329-356. North-Holland, Amsterdam, 1992.

[4] 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.

[5] Maohua Le, *A note on the integer solutions of hyperelliptic equations*, Colloqu.Math., **68** (1995), 171-177.

[6] B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math., **6** (1962), 64-94.

[7] N. Saradha and T.N. Shorey, *On the equation* $(x+1)\cdots(x+k) = (y+1)\cdots(y+mk)$, Indag. Mathem., N.S. **3** (1), (1992), 79-90.

[8] N. Saradha, T.N. Shorey and R. Tijdeman, *On arithmetic progressions with equal products*, Acta Arith., **68** (1994), 89-100.

[9] W.M. Schmidt, *Eisenstein's theorem on power series expansions of algebraic functions*, Acta. Arith., **56** (1990), 161-179.

[10] Sz. Tengely, *On the Diophantine equation* $F(x) = G(y)$, Acta Arith., **110** (2), (2003), 185-200.

[11] Sz. Tengely, *Effective methods for Diophantine Equations, Thesis,* Leiden University, 2005.

[12] P.G. Walsh, *A quantitative version of Runge's theorem on Diophantine equations*, Acta Arith., **62** (1992), 157-172, *Correction to : A*

quantitative version of Runge's theorem on Diophantine equations, Acta Arith., **73** (1995), 397-398.

Address of the authors :
School of Mathematics,
Tata Institute of Fundamental Research,
Homi Bhabha Road,
Mumbai-400 005, INDIA.

emails:

sank@math.tifr.res.in
saradha@math.tifr.res.in