Abh. Math. Sem. Univ. Hamburg **73** (2003), 253–270

On the Greatest Common Divisor of Two Cullen Numbers

By F. LUCA

Introduction

Recently, BUGEAUD, CORVAJA, and ZANNIER (see [2]) showed that if a and b are two multiplicatively independent positive integers, then for every $\varepsilon > 0$ there exists a positive integer n_ε so that $\gcd(a^n - 1, b^n - 1) \ll \exp(\varepsilon n)$ holds for all $n > n_\varepsilon$. The restriction that a and b be multiplicatively independent integers is, of course, needed for such a result to hold, for if otherwise, then it is easy to see that there exists a computable constant c_1 depending only on a and b such that $\gcd(a^n - 1, b^n - 1) \gg \exp(c_1 n)$ holds for infinitely many positive integers n. The result from [2] was recently generalized in [5], and such a generalization was efficiently used to give an affirmative answer to a question concerning the largest prime divisor of an expression of the form $(ab + 1)(ac + 1)(bc + 1)$ with positive integers a, b, and c due to GYŐRY, SÁRKÖZY and STEWART which was stated in [4]. This question was also settled independently by P. CORVAJA and U. ZANNIER (see [3]).

Also recently, a different kind of problem which in a sense is related to the above result from [2] was investigated by us in [7], and slightly extended to more general situations in [6]. Namely, in [7], we investigated the following problem:

Let r and s be non-zero integers with $r^2 + 4s \neq 0$ and let $(u_n)_{n \geq 0}$ be a *non-degenerate binary recurrent sequence of integers of characteristic equation*

$$x^2 - rx - s = 0. \tag{1}$$

That is, $u_0, u_1 \in \mathbb{Z}$ and the recurrence

$$u_{n+2} = ru_{n+1} + su_n$$

holds for all non-negative integers n. It is then well-known that there exist two constants c, d which can be immediately computed in terms of u_0, u_1, r and s, so that with α and β the two roots of the equation shown at (1), the formula

$$u_n = c\alpha^n + d\beta^n \tag{2}$$

holds for all $n \geq 0$. By non-degenerate above we mean that α/β is not a root of 1 and that $cd \neq 0$. Then, in [7], it is shown that if r and s are coprime and c/d and α/β are multiplicatively independent, then there exists an effectively computable

2000 *Mathematics Subject Classification.* 11B39.

constant c_2 so that $\gcd(u_n, u_m) \ll \exp(c_2\sqrt{m})$ holds for all $m > n$. Both conditions, namely the fact that r and s are coprime and the fact that c/d and α/β are multiplicatively independent are necessary for such a result to hold, for if not then there exists an effectively computable constant c_3 depending on u_0, u_1, r and s so that the inequality $\gcd(u_n, u_m) \gg \exp(c_3 m)$ holds for infinitely many pairs of positive integers $m > n$.

An interesting application of the main argument in [7] to the characterization of pairs of integers (a, b) in terms of the occasional "largeness" of $\gcd(F_m + a, F_n + b)$ as a function of $\max(m, n)$, where F_n is the nth Fibonacci number, is given in [6].

In this paper, we extend the main result from [7] in the following sense.

Let a and b be two non-zero coprime integers with $a/b \neq \pm 1$ and let f and g be non-zero polynomials with integer coefficients such that the rational function $h := f/g$ is non-constant. For any positive integer n set

$$u_n := f(n)a^n + g(n)b^n. \tag{3}$$

Our main result is the following:

Theorem. *Suppose that $(u_n)_{n\geq 0}$ is a sequence of integers whose general term is given by formula (3), where $a \neq \pm b$ are coprime non-zero integers and f and g are non-zero polynomials with integer coefficients such that the rational function $h := f/g$ is non-constant. Then there exist two computable constants c_1 and c_2 such that the inequality*

$$\gcd(u_n, u_m) < \exp(c_2(m \log m)^{\frac{1}{2}}) \tag{4}$$

holds for all but finitely many pairs of positive integers $m > n > c_1$.

The constant c_1 above can be chosen to be any constant larger than both the maximum absolute value of the roots z of the polynomial equation $f(z) \cdot g(z) = 0$, and the largest n for which $u_n = 0$, while the constant c_2 above can be chosen to be any constant larger than $2 \cdot \max(r_0 \deg(fg), \log|a|, \log|b|)$, where r_0 is the leading coefficient of the non-constant polynomial $f \cdot g$ and $\deg(fg)$ is its degree. While the above Theorem provides a very specific (and rather "small") upper bound for $\gcd(u_n, u_m)$, we do not have a way of computing all the (finitely many) pairs of positive integers $m > n > c_1$ for which inequality (4) might fail. The reason is due to the nature of the auxiliary results from Diophantine Equations which we will use during the proof of the above Theorem. That is, we show that unless the pair of integers $m > n > c_1$ satisfies a certain exponential-polynomial type of diophantine equation, then inequality (4) must hold. Thus, the problem reduces to deciding whether or not the exponential-polynomial diophantine equation that we encounter does indeed have only finitely many solutions. In some cases (for example, when the polynomial $f \cdot g$ is a power of a linear polynomial), we can employ effective methods to conclude that inequality (4) holds for all pairs of integers $m > n > c_1$, except for, eventually, finitely many effectively computable such pairs, but for the general case we employ a result of W. SCHMIDT concerning the finitenes of the number of integer solutions (x, y) of a diophantine equation of the type $\alpha^x = R(x, y)$, where α is a non-zero complex number which is not a root of unity and $R \in \mathbb{C}(X, Y)$ is a

rational function which is not of a certain form, but this result is ineffective in the sense that its method of proof does not allow one to compute an upper bound for the largest possible integer solution (x, y) of the above diophantine equation.

Recall that for a fixed non-negative integer $n \geq 0$ the *nth Cullen number* is given by the formula $C_n := n2^n + 1$. Notice that the general formula of the nth Cullen number is precisely formula (3) with $a = 2, b = 1, f(X) = X$ and $g(X) = 1$, and from what we have said before, $\gcd(C_n, C_m)$ can be bounded from above as shown in formula (4) for all pairs of positive integers $m > n$, except for finitely many effectively computable such pairs.

The method of proof of the above Theorem can be used to derive even more general results. For example, it follows from our method of proof, that if

$$u_n = f(n)a^n + g(n)b^n \tag{5}$$

and

$$v_n = f_1(n)a^n + g_1(n)b^n \tag{6}$$

hold for all non-negative integers n with f, f_1, g and g_1 non-zero polynomials with integer coefficients such that at least one of the two rational functions $h := f/g$ and $h_1 := f_1/g_1$ is non-constant, then there exist two computable constants c_3 and c_4 depending only on a, b, f, g, f_1 and g_1 so that the inequality

$$\gcd(u_n, v_m) < \exp(c_3(m \log m)^{\frac{1}{2}}) \tag{7}$$

holds for all but finitely many pairs of positive integers $m > n > c_1$ provided that both rational functions h and h_1 satisfy some mild technical assumptions (for example, when all four polynomials f, g, f_1 and g_1 are monic and both rational functions h and h_1 have at least three simple singular points (i.e., zeros and poles)). Of course, "bad examples" of pairs of numbers (u_n, v_m) of the form shown at (5) and (6) and for which $\gcd(u_n, v_m)$ is large infinitely often do exist, such as

$$u_n = 2^n - 9n^2$$

and

$$v_n = 2^n + 8n^3$$

for which $2^n + 6n$ divides $\gcd(u_{2n}, v_{3n})$ for all $n \geq 0$.

The Proof of the Theorem

Throughout this proof, we use $c_1, c_2, \ldots$ to denote constants (which are computable or not) depending on our initial data a, b, f and g, and we use the Landau symbols O, o and the Vinogradov symbols $\ll$ and $\gg$, with the meaning that they too depend on our initial data.

We also assume that $|a| > |b|$. It is clear that a constant c_1 exists so that $u_n \neq 0$ when $n > c_1$. We shall also assume that c_1 is larger than anyone of the roots of the polynomial equation $f(z) \cdot g(z) = 0$ and from now on we shall work under the assumption that $m > n > c_1$.

We also notice that we may assume that f and g are coprime in $\mathbb{Q}[X]$. Indeed, for if not, then with $d := \gcd(f, g)$, $f = df_1$, and $g = dg_1$, we have that all three polynomials f_1, g_1, d are with integer coefficients and so setting

$$u'_n = f_1(n)a^n + g_1(n)b^n$$

for all $n \geq 0$, we obviously get that

$$\gcd(u_n, u_m) \leq \gcd(u'_n, u'_m) \cdot d(n)d(m) \leq \gcd(u'_n, u'_m) \cdot \exp(c_2 \log m), \tag{8}$$

holds with any constant c_2 strictly larger than $2\deg(d)$ and for large enough values of m. By comparing (8) with (4) and using the fact that $\log m = o((m \log m)^{\frac{1}{2}})$, it follows that it suffices to prove that (4) holds for the sequence $(u_n)_{n\geq 0}$ replaced by $(u'_n)_{n\geq 0}$; i.e., we may assume that f and g are coprime.

For two positive integers $m > n > c_1$ set $D(m, n)$ to be the largest common divisor of u_m and u_n which is free of prime factors dividing $f(m)g(m)f(n)g(n)ab$. And we claim that it suffices to show that

$$D(m, n) < \exp(c_3(m \log m)^{\frac{1}{2}}) \tag{9}$$

holds for $m > n > c_1$. Indeed, write $\gcd(u_m, u_n) = D(m, n)D'$, where D' is the largest divisor of $\gcd(u_m, u_n)$ composed of primes dividing $f(m)g(m)f(n)g(n)ab$ and let p be a prime divisor of D'. Assume, for example, that $p \mid f(m)$. Since $p \mid u_m$, we get that $p \mid bg(m)$. Then either $p \mid b$ or $p \mid g(m)$. Assume that $p \mid g(m)$. Since f and g are coprime in $\mathbb{Q}[X]$, a positive integer E exists so that $\gcd(f(m), g(m)) \mid E$ holds for all integers m (here, one may take $E := \mathrm{Res}(f, g)$ to be the resultant of the two polynomials f and g). The above argument shows that all prime divisors of D' are also prime divisors of abE. Let p be any fixed prime divisor of D'. Clearly, $p \mid u_m$ and p cannot divide both a and b because a and b are coprime. Assume again that $p \mid f(m)$. Then either $p \mid b$ or $p \mid g(m)$. Assume, for example, that p does not divide $g(m)$. Then $p \mid b$ and obviously

$$\mathrm{ord}_p(f(m)) \ll \log m$$

because $f(m) \neq 0$, and since $\mathrm{ord}_p(b^m) \geq m$, we get that

$$\mathrm{ord}_p(u_m) \ll \log m. \tag{10}$$

Here, and throughout the paper, for a non-zero rational number r and a fixed prime number p we use $\mathrm{ord}_p(r)$ for the exact order at which p appears in the prime factor factorization of r.

Assume now that $p \mid g(m)$. If $p \mid b$, we get again inequality (10). If p does not divide b, set $\mu_m = \min(\mathrm{ord}_p(f(m)), \mathrm{ord}_p(g(m)))$ and notice that

$$u_m = p^{\mu_m}(f_1(m)a^m + g_1(m)b^m), \tag{11}$$

where $f_1(m) := \dfrac{f(m)}{p^{\mu_m}}$ and $g_1(m) := \dfrac{g(m)}{p^{\mu_m}}$ are integers. Clearly, $\mu_m \leq c_4$, where one can take c_4 to be the maximal exponent at which some prime number appears in the prime factor factorization of E, and it remains to bound the order at which

p can divide $f_1(m)a^m + g_1(m)b^m$. Since this last expression is not zero (because $u_m \neq 0$), one may use a p-adic linear form in logarithms (see [10]), to infer that

$$\mathrm{ord}_p(f_1(m)a^m + g_1(m)b^m) \ll \log^2 m \tag{12}$$

holds, where the implied constant in $\ll$ above depends on p, but p is a prime divisor of the fixed number E. From (10) and (12) above, we get that

$$\mathrm{ord}_p(u_m) \ll \log^2 m$$

holds for all $m > c_1$, so that

$$D' \leq \exp(c_5 \log^2 m). \tag{13}$$

By comparing (13) with (4), and using the fact that $\log^2 m = o((m \log m)^{\frac{1}{2}})$, we get that in order to prove the Theorem it suffices to show that inequality (9) holds.

Let us now notice that

$$\exp(c_6 n) \leq |u_n| \leq \exp(c_7 n), \tag{14}$$

holds for all sufficiently large positive integers n, where one can take c_6 and c_7 to be two positive constants with c_6 slightly smaller than $\log|a|$ and c_7 slightly larger than $\log|a|$ (this is because $|a| > |b| \geq 1$). In particular, if $n \leq (m \log m)^{\frac{1}{2}}$, then

$$\gcd(u_n, u_m) \leq |u_n| \leq \exp(c_7 n) \leq \exp(c_7 (m \log m)^{\frac{1}{2}}) \tag{15}$$

and therefore inequality (4) is satisfied in this case. From now on, we shall assume that $n > (m \log m)^{\frac{1}{2}}$.

We now use the method explained in [7]. We write $m_0 := m$, $m_1 := n$, and the Euclidian algorithm

$$\begin{aligned} m_0 &:= q_0 m_1 + m_2, \\ m_1 &:= q_1 m_2 + m_3, \\ &\cdots\cdots\cdots\cdots\cdots, \\ m_j &:= q_j m_{j+1} + m_{j+2}, \end{aligned}$$

where we assume that $j \geq 0$ is the smallest index for which $m_{j+2} \leq (m \log m)^{\frac{1}{2}}$. Here, $m_i > m_{i+1}$ holds for all $i = 0, 1, \ldots, j+1$, and $q_i := \left\lfloor \dfrac{m_i}{m_{i+1}} \right\rfloor$ is always a positive integer. The existence of the index j follows from the fact that we are assuming that $m_1 = n > (m \log m)^{\frac{1}{2}}$. Notice that m_{j+2} might be equal to zero, but this happens precisely when $m_{j+1} > (m \log m)^{\frac{1}{2}}$ is the greatest common divisor of m_0 and m_1.

We now fix $i \in \{0, 1, \ldots, j+2\}$. From the Euclidian algorithm above, we deduce the existence of two integers A_i and B_i so that

$$m_i = A_i m_0 - B_i m_1. \tag{16}$$

It is easy to see that $A_0 = 1$, $B_0 = 0$, $A_1 = 0$, $B_1 = -1$ and that if $i \geq 2$ but $i \leq j+2$, then

$$A_i := A_{i-2} - q_{i-1} A_{i-1} \tag{17}$$

and

$$B_i := B_{i-2} - q_{i-1}B_{i-1} \tag{18}$$

hold. Indeed, (17) and (18) follow immediately from the relation

$$\begin{aligned} A_i m_0 - B_i m_1 &= m_i = m_{i-2} - q_{i-1}m_{i-1} \\ &= (A_{i-2}m_0 - B_{i-2}m_1) - q_{i-1}(A_{i-1}m_0 - B_{i-1}m_1) \\ &= (A_{i-2} - q_{i-1}A_{i-1})m_0 - (B_{i-2} - q_{i-1}B_{i-1})m_1 \end{aligned}$$

by identifying the coefficients of m_0 and m_1. It is clear that A_i and B_i are coprime for all $i \in \{0, 1, \ldots, j+2\}$. Indeed, this is clear for $i = 0$ and $i = 1$, and for $i \geq 2$, by multiplying, say (17) by B_{i-1} and (18) by A_{i-1}, respectively, and subtracting the two resulting equations we get

$$A_i B_{i-1} - A_{i-1}B_i = -(A_{i-1}B_{i-2} - A_{i-2}B_{i-1}). \tag{19}$$

But repeated applications of (19) show that

$$A_i B_{i-1} - A_{i-1}B_i = (-1)^{i-1}(A_1 B_0 - A_0 B_1) = (-1)^{i-1}, \tag{20}$$

which, in particular, implies that A_i and B_i are coprime.

We shall make use of the properties of the numbers A_i and B_i as follows. Write $D := D(m, n)$ and rewrite the relations $D \mid u_m$ and $D \mid u_n$ as

$$f(m_0)a^{m_0} + g(m_0)b^{m_0} \equiv 0 \pmod{D} \tag{21}$$

and

$$f(m_1)a^{m_1} + g(m_1)b^{m_1} \equiv 0 \pmod{D}. \tag{22}$$

Since D is free of primes dividing $f(m)g(m)f(n)g(n)ab$, it follows that we may invert some elements modulo D in the relations (21) and (22), and rewrite them as

$$\alpha^{m_0} + h(m_0) \equiv 0 \pmod{D}, \tag{23}$$

and

$$\alpha^{m_1} + h(m_1) \equiv 0 \pmod{D}, \tag{24}$$

with $\alpha := b/a$ and $h := f/g$. We claim that (23) and (24) are particular instances of a more general congruence, namely that for all $i \in \{0, 1, \ldots, j+2\}$ the congruence

$$\alpha^{m_i} \pm h(m_0)^{A_i} \cdot h(m_1)^{-B_i} \equiv 0 \pmod{D} \tag{25}$$

holds, where A_i and B_i are the numbers defined previously. In (25) above, we mean that there exists a choice of the sign $\pm$ so that (25) holds with this choice of sign. Notice that (23) and (24) prove (25) at $i = 0$ and $i = 1$. Assume, by induction, that $i \geq 2$ and that (25) holds at $i - 1$ and $i - 2$. Hence, both

$$\alpha^{m_{i-2}} \equiv \mp h(m_0)^{A_{i-2}} h(m_1)^{-B_{i-2}} \pmod{D} \tag{26}$$

and

$$\alpha^{m_{i-1}} \equiv \mp h(m_0)^{A_{i-1}} h(m_1)^{-B_{i-1}} \pmod{D} \tag{27}$$

hold. We raise congruence (27) to the power q_{i-1} and use the fact that $m_{i-2} = q_{i-1}m_{i-1} + m_i$ to rewrite the system of congruences (26) and (27) as

$$(\alpha^{m_{i-1}q_{i-1}}) \cdot \alpha^{m_i} \pm h(m_0)^{A_{i-2}} h(m_1)^{-B_{i-2}} \equiv 0 \pmod{D} \tag{28}$$

and

$$(\alpha^{m_{i-1}q_{i-1}}) \pm h(m_0)^{A_{i-1}q_{i-1}} h(m_1)^{-B_{i-1}q_{i-1}} \equiv 0 \pmod{D}. \tag{29}$$

Equations (28) and (29) tell us that the pair $(X, Y) := (\alpha^{m_{i-1}q_{i-1}}, 1)$ is a non-zero solution (modulo D) of the modular homogeneous linear system

$$\begin{cases} \alpha^{m_i} X \pm h(m_0)^{A_{i-2}} h(m_1)^{-B_{i-2}} Y & \equiv 0 \pmod{D}, \\ X \pm h(m_0)^{A_{i-1}q_{i-1}} h(m_1)^{-B_{i-1}q_{i-1}} Y & \equiv 0 \pmod{D}. \end{cases} \tag{30}$$

In particular, the modular homogeneous system shown at (30) is degenerate, and therefore its determinant which is

$$\begin{vmatrix} \alpha^{m_i} & \pm h(m_0)^{A_{i-2}} h(m_1)^{-B_{i-2}} \\ 1 & \pm h(m_0)^{A_{i-1}q_{i-1}} h(m_1)^{-B_{i-1}q_{i-1}} \end{vmatrix}, \tag{31}$$

is zero modulo D. Imposing the condition that the determinant shown at (31) is zero modulo D and inverting some elements, we get

$$\alpha^{m_i} \pm h(m_0)^{A_{i-2}-q_{i-1}A_{i-1}} h(m_1)^{-B_{i-2}+q_{i-1}B_{i-1}} \equiv 0 \pmod{D}, \tag{32}$$

and, in light of the recurrence formulae (17) and (18), we recognize that congruence (32) is precisely congruence (25) at i.

We now evaluate (25) at $i := j + 2$ and read that

$$\alpha^{m_{j+2}} \pm h(m_0)^{A_{j+2}} h(m_1)^{-B_{j+2}} \equiv 0 \pmod{D}.$$

Set

$$\lambda_{j+2} := \alpha^{m_{j+2}} \pm h(m_0)^{A_{j+2}} \cdot h(m_1)^{-B_{j+2}}. \tag{33}$$

In what follows, we will make the following Hypothesis

$$\lambda_{j+2} \neq 0. \tag{H}$$

Assuming that (H) holds, it then follows that D must divide the numerator of the non-zero rational number λ_{j+2}, and an immediate calculation then shows that this numerator is not larger than

$$\exp(c_8 \max(m_{j+2}, |A_{j+2}| \log m, |B_{j+2}| \log m)), \tag{34}$$

where the constant c_8 can be chosen to be any constant larger than $\max(\log|a|, 2\deg(fg))$. Clearly, $m_{j+2} \leq (m \log m)^{1/2}$, and so the inequality (9) will follow from (34) (under hypothesis (H)), where the constant c_3 shown at (9) can be taken to be equal to our present c_8, provided that we can show that

$$\max(|A_{j+2}|, |B_{j+2}|) \leq \left(\frac{m}{\log m}\right)^{\frac{1}{2}}. \tag{35}$$

Let us make the following observations:

1. $(-1)^i A_i \geq 0$ for all $i \geq 0$ and $A_i \neq 0$ for $i \geq 2$.
2. $(-1)^i B_i \geq 0$ for all $i \geq 0$ and $B_i \neq 0$ for $i \geq 1$.

3. $|B_i| \geq |A_i|$ for all $i \geq 1$.
4. The formula

$$m_0 = |B_{i+1}|m_i + |B_i|m_{i+1} \tag{36}$$

holds for all $i \in \{0, 1, \ldots, j+1\}$.

To justify 1, notice that it is true at $i = 0$ and at $i = 1$, and now the recurrence formula (17) tells us that

$$(-1)^i A_i = q_{i-1} \cdot (-1)^{i-1} A_{i-1} + (-1)^{i-2} A_{i-2} \tag{37}$$

holds for $i \in \{2, \ldots, j+2\}$, therefore, by induction, $(-1)^i A_i > 0$. In particular, $(-1)^i A_i = |A_i|$ holds for all $i \in \{0, 1, \ldots, j+2\}$ and the above recurrence (37) also implies that $A_i \neq 0$ for $i \geq 2$. The same argument proves 2 above and the fact that

$$(-1)^i B_i = (-1)^{i-1} q_{i-1} B_{i-1} + (-1)^{i-2} B_{i-2} \qquad \text{holds for } i \in \{2, \ldots, j+2\}. \tag{38}$$

The facts 1 and 2 above together with formulae (37) and (38) show that both relations

$$|A_i| = q_{i-1}|A_{i-1}| + |A_{i-2}| \tag{39}$$

and

$$|B_i| = q_{i-1}|B_{i-1}| + |B_{i-2}| \tag{40}$$

hold for all $i \in \{2, \ldots, j+2\}$. Since $|B_1| = 1 > 0 = |A_1|$ and $|B_2| = q_1 \geq 1 = |A_2|$, it follows, by induction on i using recurrences (39) and (40), that 3 holds as well. Finally, to see 4, let $i \in \{0, 1, \ldots, j+1\}$, write

$$\begin{cases} A_i m_0 - B_i m_1 & = m_i, \\ A_{i+1} m_0 - B_{i+1} m_1 & = m_{i+1}, \end{cases} \tag{41}$$

and treat the system (41) as a system of two linear equations in the unknowns m_0 and m_1. Solving the above system with Kramer's rule and using (20), we get precisely formula (36).

It is now easy to see that the combination of 1-4 above prove (35). Indeed, since $m_{j+1} > (m \log m)^{1/2}$, we get, by (36), that

$$m = m_0 = |B_{j+2}|m_{j+1} + |B_{j+1}|m_{j+2} \geq |B_{j+2}|m_{j+1} > |B_{j+2}| \cdot (m \log m)^{\frac{1}{2}},$$

therefore

$$|B_{j+2}| < \left(\frac{m}{\log m}\right)^{\frac{1}{2}}. \tag{42}$$

Inequality (42) together with the fact that $|B_{j+2}| \geq |A_{j+2}|$ proves (35).

In order to complete the proof of the Theorem, it suffices to show that hypothesis (H) holds for all but finitely many pairs of positive integers $m > n > c_1$.

So, we shall suppose that $\lambda_{j+2} = 0$ and write $A := |A_{j+2}|$ and $B := |B_{j+2}|$. Since at any rate A_{j+2} and B_{j+2} have the same signs and are coprime, we get, from (33), that

$$h(m_0)^A = \pm \gamma^{m_{j+2}} h(m_1)^B, \tag{43}$$

where $\gamma = \alpha$ or α^{-1}, according to whether $A_{j+2} \geq 0$ or $A_{j+2} < 0$.

Let $S(h)$ be the set of all singular points of h (i.e., zeros and poles), counted without multiplicities; that is, $S(h)$ is the set of complex roots z of the polynomial equation $f(z) \cdot g(z) = 0$. We distinguish the following two cases:

Case 1. $|S(h)| \geq 2$.

In this case, we first show that both A and B are bounded. Indeed, relation (43) together with the fact that A and B are coprime implies, in particular, that there exist two rational numbers r and s such that both their numerators and denominators are divisible only with primes p dividing ab, and some other rational number ρ, so that

$$h(m_0) = r\rho^B \qquad \text{and} \qquad h(m_1) = s\rho^A. \tag{44}$$

Writing $h(m_0) = f(m_0)/g(m_0)$ and using the fact that $\gcd(f(m_0), g(m_0)) \mid E$, we get that there exist two integers r_1 and r_2 composed only of primes dividing abE, and two other integers v_1 and v_2 so that both relations

$$f(m_0) = r_1 v_1^B \qquad \text{and} \qquad g(m_0) = r_2 v_2^B \tag{45}$$

hold, and multiplying now relations (45) we get that relation

$$f(m_0) \cdot g(m_0) = r_3 v_3^B \tag{46}$$

holds with $r_3 = r_1 r_2$ and $v_3 = v_1 v_2$. Set u to be the radical of $f \cdot g$ (i.e., the product of all the irreducible factors of $f \cdot g$) and set $\Delta := \operatorname{disc}(u)$ to be the discriminant of u. Notice that $\deg(u) \geq 2$. Pick k_1 to be any irreducible factor of $f \cdot g$ and assume that $k_1^{\mu_1} \parallel f \cdot g$; that is, that the power at which k_1 appears in the factorization of $f \cdot g$ in $\mathbb{Q}[X]$ is precisely μ_1. Equation (46) implies that

$$k_1^{\mu_1}(m_0) = r_4 v_4^B, \tag{47}$$

where r_4 is an integer composed only of primes dividing $abE\Delta$, and therefore that

$$k_1(m_0) = r_5 v_5^{B'} \tag{48}$$

holds with some r_5 composed only of primes dividing $abE\Delta$ and some integer v_5, where $B' = B/\gcd(B, \mu_1)$. If $\deg(k_1) \geq 2$, then it is known (see [9]) that an equation like (48) has a totality of finitely many effectively computable solutions (m_0, r_5, v_5, B') for which $B' \geq 3$. So, except for these finitely many effectively computable values of m_0, we should have $B' \leq 2$, which shows that B is bounded. If we now assume that $\deg(k_1) = 1$, then from the fact that $\deg(u) \geq 2$, it follows that there exists another irreducible factor k_2 (which is also linear) of u, so that with μ_2 being the order at which k_2 appears in the factorization of $f \cdot g$ in $\mathbb{Q}[X]$, we have that

$$k_2(m_0) = r_6 v_6^{B''} \tag{49}$$

holds with some integer r_6 which is divisible only by primes dividing $abE\Delta$, and with $B'' = B/\gcd(B, \mu_2)$. Let

$$l := \frac{B}{\operatorname{lcm}(\gcd(B, \mu_1), \gcd(B, \mu_2))}. \tag{50}$$

If $l \geq 3$, then equations (48) and (49) show that

$$k_1(m_0)k_2(m_0) = r_7 v_7^l \tag{51}$$

holds with $r_7 = r_5 \cdot r_6$ and some integer v_7, and since the polynomial $k_1 \cdot k_2$ has only two simple roots, it follows by the same argument as above that an equation like (51) can have only finitely many effectively computable solutions (m_0, r_7, v_7, l) with $l \geq 3$. In particular, except for these finitely many effectively computable solutions m_0, we should have $l \leq 3$, which puts again a bound on B. Since $B \geq A$, we get that both A and B are bounded.

The above argument shows that we may assume that $A := A_{j+2}$ and $B := B_{j+2}$ are fixed, and now since $\pm m_{j+2} = Am_0 - Bm_1$, it follows that we may write $m_0 = c_{10}m_1 + c_{11}m_{j+2}$, where $c_{10} := B/A \geq 1$ and $c_{11} := \pm 1/A \neq 0$ are fixed rational numbers. Set $x := m_{j+2}$ and $y := m_1$, therefore $m_0 = c_{10}y + c_{11}x$. We return to equation (43) and write it as

$$\frac{h(c_{10}y + c_{11}x)^A}{h(y)^B} = \pm\gamma^x. \tag{52}$$

And we want to show that equation (52) has only finitely many integer solutions (x, y). Assuming that this were not so, we would distinguish two instances:

Subcase 1. *There exists a constant K such that all integer solutions (x, y) of equation* (52) *have $|x| < K$.*

In this case, there exists an integer value x_0, such that equation (52) has infinitely many integer solutions (x, y) with $x := x_0$. And so, with fixed γ (equal to either α or α^{-1}), $c_{12} := c_{11}x_0$ and $c_{13} := \gamma^{x_0}$ or $-\gamma^{x_0}$, the equation

$$\frac{h(c_{10}y + c_{12})^A}{h(y)^B} = c_{13} \tag{53}$$

has infinitely many solutions y. In particular, the rational function

$$h_1(X) := \frac{h(c_{10}X + c_{12})^A}{h(X)^B} \tag{54}$$

is constant, therefore $S(h_1) = \emptyset$. This tells us that every singularity of $h(X)$ is also a singularity of $h(c_{10}X + c_{12})$ and viceversa, and therefore with the linear function $L(X) := c_{10}X + c_{12}$ we get that $S(h)$ is invariant under L. But $S(h)$ is finite, and the only instance in which the linear function L with c_{10} and c_{11} rational numbers and $c_{10} \geq 1$ can have *finite orbits*; i.e., finite subsets of the form $\{L^n(X_0) \mid n \geq 0\}$, where we use L^n for the nth fold composition of L with itself, is when $c_{12} = 0$ and $c_{10} = 1$. But in this case we have $m_0 = m_1$, or $m = n$, which is not acceptable.

Subcase 2. *Equation* (52) *has solutions with arbitrarily large values of x.*

In this case, there exists a choice of sign $\varepsilon = \pm 1$ and a choice of γ (equal to either α or α^{-1}) such that equation (52) has solutions with arbitrarily large positive

values of x with this particular choice of signs ε and this fixed γ appearing in the right hand side of (52). In particular, with

$$h_1(X, Y) := \varepsilon \frac{h(c_{10}Y + c_{11}X)^A}{h(Y)^B} \tag{55}$$

the diophantine equation

$$h_1(x, y) = \gamma^x \tag{56}$$

has solutions with arbitrarily large positive values of x. Let us now make a few remarks about this subcase:

1. $\deg(f) \neq \deg(g)$.
2. $A \neq B$.

Indeed, assume, for example, that $\deg(f) = \deg(g)$. In this case, for large values of z, $h(z)$ tends to a fixed limit c_{14}, where c_{14} is the ratio of the leading coefficient of f to the leading coefficient of g, and rewriting now equation (43) as

$$\frac{h(m_0)^A}{h(m_1)^B} = \pm\gamma^{m_{j+2}}$$

we get that for large m_0 and $m_1 \geq (m_0 \log m_0)^{\frac{1}{2}}$, the number $|\gamma^{m_{j+2}}|$ is close to c_{14}^{A-B}. This shows that m_{j+2} is bounded, which is not the case we are discussing. If $A = B$, then since A and B are coprime, it follows that $A = B = 1$. By interchanging f with g, and a with b (hence, h with h^{-1}, and γ with γ^{-1}) if needed, we may assume that $\deg(f) > \deg(g)$. In particular, h has an expansion at infinity of the type

$$h(X) = c_{14}X^l + c_{15}X^{l-1} + \ldots, \tag{57}$$

where c_{14} is again the ratio of the leading coefficient of f to the leading coefficient of g and $l = \deg(f) - \deg(g) > 0$. But in this case, with $A = B = 1$, we get $m_0 = m_1 + m_{j+2}$, where $m_{j+2} < \left(\frac{m_0}{\log m_0}\right)^{\frac{1}{2}}$, and so

$$\pm\gamma^{m_{j+2}} = \frac{h(m_0)^A}{h(m_1)^B} = \frac{h(m_0)}{h(m_0 + m_{j+2})}$$

is close to 1 for large values of m_0, which shows again that m_{j+2} is bounded, which is not the case we are discussing.

And so, we may assume that $\deg(f) \neq \deg(g)$ and that $A < B$. By interchanging again f with g and a with b (hence, h with h^{-1}, and γ with γ^{-1}) if needed, we may assume that $\deg(f) > \deg(g)$. Set

$$h_2(X, Y) = h_1(X, Y)^{-1} = \varepsilon \frac{h(Y)^B}{h(c_{10}Y + c_{11}X)^A} \in \mathbb{Q}[X, Y], \tag{58}$$

and notice that we are assuming that the equation

$$h_2(x, y) = \gamma_1^x \tag{59}$$

has integer solutions (x, y) with arbitrarily large values of x, where $\gamma_1 = \gamma^{-1}$. Notice also that the function $h_2(X, Y)$ has (as a rational function of Y) an expansion at infinity of the form

$$h_2(X, Y) = c_{15}Y^t + R_1(X)Y^{t-1} + \ldots, \tag{60}$$

where $t = (B - A)l = (B - A)(\deg(f) - \deg(g)) > 0$, $c_{15} = \varepsilon c_{14}^{B-A} c_{10}^{-Al}$, and $R_1, \ldots$ are rational functions in X. We now recall the following Theorem due to W. SCHMIDT (see [8]):

Theorem S. *Suppose that $R(X, Y) \in \mathbb{C}(X, Y)$ is a rational function which, as a function of Y, has an expansion at infinity of the type*

$$R(X, Y) = r_0 Y^t + r_1(X)Y^{t-1} + \ldots, \tag{61}$$

where $r_0 \neq 0$ is a constant and $r_1, \ldots$ are rational functions in X, and assume that γ is a non-zero complex number which is not a root of unity. If the equation

$$\gamma^x = R(x, y) \tag{62}$$

has integer solutions (x, y) with arbitrarily large values of $|x|$, then R is of the type

$$R(X, Y) = r_0(Y - u(X))^t, \tag{63}$$

where $t \neq 0$, $u(X) \in \mathbb{Q}(X)$, and $\gamma^v \in \mathbb{Z}$ for some $v \in \mathbb{Z}\backslash\{0\}$.

And so, if equation (59) has integer solutions (x, y) with arbitrarily large positive values of x we conclude, by Theorem S above, that h_2 must be of the form $\dfrac{v(X, Y)}{w(X)^t}$ for some polynomials $v \in \mathbb{Q}[X, Y]$ and $w \in Q[X]$. But we obviously have

$$h_2(X, Y) = \varepsilon \frac{f(Y)^B g(c_{10}Y + c_{11}X)^A}{g(Y)^B f(c_{10}Y + c_{11}X)^A} \tag{64}$$

and the expression (64) is already in reduced form because f and g are coprime as polynomials. In particular, g must be constant and $f(c_{10}Y + c_{11}X)$ must not depend on Y, therefore f must be constant as well, which is impossible.

The above arguments take care of Case 1, but are ineffective.

Case 2. $|S(h)| = 1$.

Our proof for this case is *effective*, in the sense that here we can show that an equation like the counterpart of (H) has only finitely many effectively computable positive integer solutions $m > n > c_1$.

Let us notice first that since f and g are coprime, it follows that up to interchanging f with g, and a with b if needed, we may assume that $f(X) = cl(X)^\mu$ and $g(X) = d$, where c, d are nonzero integers and $l(X) := rX + s$ is a linear polynomial with integer coefficients. Up to simultaneously changing the signs of both f and g, we may assume that $r > 0$. The trick that we employ here is to notice that we may assume that $l(X) := X$. Indeed to see why this is so, notice that for every positive integer n, we have

$$u_n \mid u'_n, \tag{65}$$

holds for all positive integers $n > -s/r$, with

$$u'(n) = f_1(n)a^{rn+s} + g_1(n)b^{rn+s}, \tag{66}$$

where $f_1(X) := b^s f(X)^r = c^r b^s (rX + s)^{\mu r}$, and $g_1(X) := -a^s g(X)^r = -a^s d^r$, and in particular,

$$\gcd(u_m, u_n) \mid \gcd(u'_m, u'_n) \tag{67}$$

holds for all pairs of positive integers $m > n > c_1$. So that, provided that $m > n > c_1$ (notice that c_1 is larger than the absolute value $|s|/r$ of the unique root of f), we may replace the pair of positive integers $m > n$ by the pair of positive integers $m' > n'$, where $m' := rm + s$ and $n' := rn + s$, and therefore we may assume that $l(X) = X$ (notice that this transformation will affect only the degree of $f \cdot g$; i.e., will affect only the constant c_2 shown in formula (4)).

And so, from now on we shall assume that $f(X) = cX^\mu$ and $g(X) = d$, where μ and c are positive integers and d is a non-zero integer. In particular, $h(X) = \frac{f(X)}{g(X)} = \frac{c}{d} \cdot X^\mu$.

We first treat the case $m_{j+2} = 0$. In this case $Am_0 = Bm_1$, and since A and B are coprime we read $A = n/d$ and $B = m/d$, where $d := \gcd(m, n)$. Taking absolute values in equation (43) and raising the resulting equation to the power d, we read

$$|h(m)|^n = |h(n)|^m \tag{68}$$

therefore

$$\frac{\log|h(m)|}{m} = \frac{\log|h(n)|}{n}. \tag{69}$$

But certainly the function $x \mapsto \dfrac{\log|h(x)|}{x}$ is decreasing for large x (and tends to zero when x tends to infinity), and since for us $(m \log m)^{\frac{1}{2}} \leq n < m$, we get that equation (69) has only finitely many (obviously effectively computable) positive integer solutions m, n satisfying the above inequality. From now on, we shall assume that $m_{j+2} \neq 0$. We first notice that

$$m_{j+2} \ll B \log m. \tag{70}$$

Indeed, this follows immediately by taking first absolute values and then logarithms in formula (43) and using the facts that $m > n$ and $B \geq A$.

Since $m_{j+2} = A_{j+2}m_0 - B_{j+2}m_1$, we may rewrite the equation $\lambda_{j+2} = 0$, with λ_{j+2} being given by (33), as

$$\left(\frac{c}{d} \cdot \left(\frac{a}{b}\right)^{m_0} \cdot m_0^\mu\right)^{A_{j+2}} = \pm\left(\frac{c}{d} \cdot \left(\frac{a}{b}\right)^{m_1} \cdot m_1^\mu\right)^{B_{j+2}}, \tag{71}$$

which implies

$$\left(\left|\frac{c}{d}\right| \cdot \left|\frac{a}{b}\right| \cdot m_0^\mu\right)^A = \left(\left|\frac{c}{d}\right| \cdot \left|\frac{a}{b}\right|^{m_1} \cdot m_1^\mu\right)^B. \tag{72}$$

And so, since A and B are coprime, we conclude that a positive rational number ρ exists such that both relations

$$\left|\frac{c}{d}\right| \cdot \left|\frac{a}{b}\right|^{m_0} \cdot m_0^\mu = \rho^B \qquad \text{and} \qquad \left|\frac{c}{d}\right| \cdot \left|\frac{a}{b}\right|^{m_1} \cdot m_1^\mu = \rho^A \tag{73}$$

hold. We shall now use equations (73) to infer that the inequality

$$B \ll \log m \tag{74}$$

holds.

Let $p_1 < p_2 < \cdots < p_t$ be all the prime numbers dividing $cdab$ (notice that $t \geq 1$ because a and b are coprime and $a \neq \pm b$), and write

$$\left|\frac{a}{b}\right| := p_1^{\alpha_1} \cdot \cdots \cdot p_t^{\alpha_t} \qquad \text{and} \qquad \left|\frac{c}{d}\right| := p_1^{\beta_1} \cdot \cdots \cdot p_t^{\beta_t}$$

for some integers $\alpha_i, \beta_i, i = 1, \ldots, t$. We also write

$$\rho = p_1^{\gamma_1} \cdot \cdots \cdot p_t^{\gamma_t} \cdot \lambda \tag{75}$$

for some (unknown) integers γ_i and some (unknown) positive rational number λ having the property that when written in reduced form both its numerator and denominator are coprime to $p_1 \cdot \cdots \cdot p_t$. And so, we may rewrite the system of two equations (73) as

$$m_0^{\mu} = \lambda^B \cdot \prod_{i=1}^{t} p_i^{\mu_{0i}} \qquad \text{and} \qquad m_1^{\mu} = \lambda^A \cdot \prod_{i=1}^{t} p_i^{\mu_{1i}}, \tag{76}$$

where

$$\mu_{0i} := B\gamma_i - \alpha_i m_0 - \beta_i \qquad \text{and} \qquad \mu_{1i} := A\gamma_i - \alpha_i m_1 - \beta_i \qquad \text{for } i = 1, \ldots, t. \tag{77}$$

Since m_0 is an integer and λ is a rational number which when written in reduced form has the property that both its numerator and denominator are coprime to $p_1 \cdot \cdots \cdot p_t$, we read, from equations (76), that $\lambda \geq 1$ is a positive integer. In particular, if $\lambda \neq 1$, then equation (76) implies that inequality (74) holds. Moreover, in this case, it follows that λ^A divides both m_0^{μ} and m_1^{μ}, and therefore it will divide $\gcd(m_0^{\mu}, m_1^{\mu}) = \gcd(m_0, m_1)^{\mu} \leq m_{j+2}^{\mu}$ (it is clear that $\gcd(m_0, m_1)$ divides m_{j+2}). In particular, we also get that

$$\log \lambda \ll \log m_{j+2}. \tag{78}$$

When $\lambda = 1$, we simply discard the factors λ^B and λ^A appearing in the equations (76).

From the above remarks, it follows that in order to show that inequality (74) holds, it suffices to show that it holds when $\lambda = 1$. To prove this, let us go back to formula (76) and using the fact that m_0 is an integer, we get that

$$0 \leq \mu_{0i} = O(\log m) \qquad \text{holds for all } i = 1, \ldots, t. \tag{79}$$

Using (77), we read that

$$|B\gamma_i - \alpha_i m_0| = O(\log m) \qquad \text{holds for all } i = 1, \ldots, t. \tag{80}$$

And so, applying (80) for two different indices i and j (assuming that we have two different indices i and j), we get

$$\begin{aligned} |(\gamma_i\alpha_j - \gamma_j\alpha_i)B| &= |\alpha_j(\gamma_i B - \alpha_i m_0) - \alpha_i(\gamma_j B - \alpha_j m_0)| \\ &\leq |\alpha_j||\gamma_i B - \alpha_i m_0| + |\alpha_i||\gamma_j B - \alpha_j m_0| = O(\log m). \end{aligned} \tag{81}$$

So, if two indices $i \neq j$ exist such that $\alpha_i\gamma_j - \alpha_j\gamma_i \neq 0$ then, from (81), we read that

$$B = O(\log m)$$

must hold, which is precisely inequality (74). So, we shall assume now that $\alpha_i\beta_j = \alpha_j\beta_i$ holds for all indices $i, j \in \{1, \ldots, t\}$ (this is, for example, the case in which $t = 1$). It then follows that the number

$$\frac{\gamma_i B - \alpha_i m_0}{\alpha_i} = \delta \tag{82}$$

is independent of i, and further that

$$\frac{\gamma_i A - \alpha_i m_1}{\alpha_i} = \zeta = \frac{A}{B}\delta + \frac{Am_0 - Bm_1}{B}$$

is independent of i as well. In particular, we get that both relations

$$\left|\frac{c}{d}\right| \cdot m_0^{\mu} = \left|\frac{a}{b}\right|^{\delta} \qquad \text{and} \qquad \left|\frac{c}{d}\right| \cdot m_1^{\mu} = \left|\frac{a}{b}\right|^{\zeta} \tag{83}$$

hold, where δ and ζ are some rational numbers. Assuming that $|a| > |b|$, we get that both δ and ζ are positive. Moreover, if we set $w \geq 1$ to be the largest possible integer exponent for which $|a/b| = r_1^w$ has a rational solution r_1, we get that $|a| = a_1^w$ and $|b| = b_1^w$ hold with some positive integers a_1 and b_1, and now relations (83) show that

$$\left|\frac{c}{d}\right| m_0^{\mu} = \left(\frac{a_1}{b_1}\right)^{w\delta} \qquad \text{and} \qquad \left|\frac{c}{d}\right| m_1^{\mu} = \left(\frac{a_1}{b_1}\right)^{w\zeta}. \tag{84}$$

It now follows that both $w\delta$ and $w\zeta$ are integers. If $b_1 > 1$, we get, from the fact that m_0 is an integer, that $w\delta$ is bounded from above, and therefore m_0 is bounded from above as well (obviously in a computable way). Thus, we may assume that $b_1 = 1$, and now relations (84) together with the fact that $m_1 < m_0$ imply that $w\zeta < w\delta$. In particular, $a_1^{w\zeta}$ divides $a_1^{w\delta}$, which shows that $m_1^{\mu} \mid m_0^{\mu}$. Hence, $m_1 \mid m_0$, but this shows that the Euclidian algorithm finishes at the first step; i.e., $j = 0$ and $m_{j+2} = 0$, which is a case already treated. So, this instance cannot occur and inequality (74) holds.

The combination of (70) and (74) shows that

$$m_{j+1} \ll \log^2 m \tag{85}$$

holds, and now inequality (78) shows that

$$\log\lambda \ll \log_2 m, \tag{86}$$

where we use $\log_2$ to denote the composition of the natural logarithm function with itself.

We now return to equations (76) and write these equations as

$$m_0 = \lambda^{B/\mu} \prod_{i=1}^{t} p_i^{\mu'_{0i}} \qquad \text{and} \qquad m_1 = \lambda^{B/\mu} \prod_{i=1}^{t} p_i^{\mu'_{1i}}, \tag{87}$$

where

$$\mu'_{0i} = \frac{\mu_{0i}}{\mu} \quad \text{and} \quad \mu'_{1i} = \frac{\mu_{1i}}{\mu} \quad \text{are all non-negative integers for } i = 1, \ldots, t. \tag{88}$$

Let us notice that since A and B are coprime, it follows, from (87), that $\lambda = \lambda_1^{\mu}$ for some positive integer λ_1.

We now multiply the first relation (87) with A and the second relation with B, substract them and use the fact that $\pm m_{j+2} = Am_0 - Bm_1 \neq 0$, to get

$$m_{j+2} = \left| A\lambda_1^B \prod_{i=1}^{t} p_i^{\mu'_{0i}} - B\lambda_1^A \prod_{i=1}^{t} p_i^{\mu'_{i1}} \right| \neq 0. \tag{89}$$

We are now all set to apply lower bounds for linear forms in logarithms á la BAKER (see [1]) to equation (89). That is, for every index $i \in \{1, \ldots, t\}$ we set

$$X_i := \max(\mu'_{0i}, \mu'_{1i}), \qquad Y_i := \min(\mu'_{0i}, \mu'_{1i}), \qquad Z_i := X_i - Y_i, \tag{90}$$

and if $\lambda \geq 2$ we also set

$$X_0 := B, \qquad Y_0 := A, \qquad Z_0 := B - A.$$

If $\lambda = \lambda_1 = 1$, we simply set $X_0 = Y_0 = 1$ and $Z_0 = 0$.

We notice that equation (89) can be written as

$$m_{j+2} = \lambda_1^{Y_0} \prod_{i=1}^{t} p_i^{Y_i} \left(A\lambda_1^{Z'_0} \prod_{i=1}^{t} p_i^{Z'_{0i}} - B\lambda_1^{Z'_1} \prod_{i=1}^{t} p_i^{Z'_{1i}} \right), \tag{91}$$

where

$$Z'_0 = B - A, \qquad Z'_1 = A - A = 0,$$

when $\lambda \geq 2$, and for $i \geq 1$

$$Z'_{0i} = \mu'_{0i} - Y_i, \qquad Z'_{1i} = \mu'_{1i} - Y_i.$$

It is clear that both numbers Z'_{0i} and Z'_{1i} are non-negative, and one of them is always zero. Since $m_{j+2} \neq 0$, it follows that

$$Y_i \ll \log m_{j+2} \ll \log_2 m \tag{92}$$

holds for all $i = 0, 1, \ldots, t$. To get a lower bound on the expression apearing in parenthesis on the right hand side, we write equation (91) both as

$$m_{j+2} = A\lambda_1^{X_0} \prod_{i=1}^{t} p_i^{\mu'_{0i}} \left| 1 - BA^{-1}\lambda_1^{-Z_0} \prod_{i=1}^{t} p_i^{\mu'_{1i} - \mu'_{0i}} \right| \tag{93}$$

as well as

$$m_{j+2} = B\lambda_1^{Y_0} \prod_{i=1}^{t} p_i^{\mu'_{1i}} \left| 1 - AB^{-1}\lambda_1^{Z_0} \prod_{i=1}^{t} p_i^{\mu'_{0i} - \mu'_{1i}} \right|. \tag{94}$$

Notice that $\mu'_{0i} - \mu'_{1i} = \pm Z_i$ for all $i \in \{1, \ldots, t\}$ and $X_0 - Y_0 = Z_0$. We now multiply the two relations (93) and (94) above and use the obvious fact that

$\mu'_{0i} + \mu'_{1i} \geq Z_i$ for all $i = 1, \ldots, t$ and $B + A = X_0 + Y_0 > Z_0$ holds when $\lambda \geq 2$, to get that there exist choices of signs $\varepsilon_{-1}, \varepsilon_0, \ldots, \varepsilon_t \in \{\pm 1\}$, so that

$$m_{j+2}^2 \geq \lambda_1^{Z_1} \prod_{i=1}^{t} p_i^{Z_i} \left| 1 - (B/A)^{\varepsilon_{-1}} \lambda_1^{\varepsilon_0} \prod_{i=1}^{t} p_i^{\varepsilon_i Z_i} \right| \cdot \left| 1 - (B/A)^{-\varepsilon_{-1}} \lambda_1^{-\varepsilon_0} \prod_{i=1}^{t} p_i^{-\varepsilon_i Z_i} \right|. \tag{95}$$

We now set

$$Z := \max(e, Z_i \mid i = 0, \ldots, t), \tag{96}$$

and use a lower bound for a linear form in logarithms (see [1]) to conclude that an effectively computable constant c_{16} exists such that

$$\begin{aligned} \min(|1 - (B/A)^{\varepsilon_{-1}} \lambda_1^{\varepsilon_0} \prod_{i=1}^{t} p_i^{\varepsilon_i Z_i}|, |1 - (B/A)^{-\varepsilon_{-1}} \lambda_1^{-\varepsilon_0} \prod_{i=1}^{t} p_i^{-\varepsilon_i Z_i}|) \\ > \exp(-c_{16} \log B \log Z \log \lambda'_1), \end{aligned} \tag{97}$$

where $\lambda'_1 = \max(\lambda_1, e)$. The effectively computable constant c_{16} appearing above depends on t and on the prime numbers $p_1, \ldots, p_t$. Thus, by taking logarithms in (95) and using (97), we get that

$$Z_0 \log \lambda_1 + \sum_{i=1}^{t} Z_i \log p_i \leq c_{16} \log B \log Z \log \lambda'_1 + 2 \log m_{j+2}. \tag{98}$$

So, either $Z_i \leq e$ holds for all $i = 0, \ldots, t$, or $Z_i = Z$ for some $i = 0, \ldots, t$ and if this is so, then

$$Z \leq c_{17} \log Z \log B \log \lambda'_1 + c_{18} \log m_{j+2} \tag{99}$$

holds, where $c_{17} := c_{16}/\log 2$ and $c_{18} := 2/\log 2$. We now use inequalities (74), (85) and (86) to conclude that inequality (99) implies that

$$Z \leq c_{19} \log Z \log_2^2 m. \tag{100}$$

But inequality (100) implies that

$$Z \leq c_{20} \log_2^2 m \log_3 m$$

holds for large enough values of m, where we use $\log_3 m$ for the composition of the natural logarithm with itself three times evaluated in m provided that m is large. So, at any rate, we get that

$$Z_i \leq c_{20} \log_2^2 m \log_3 m \tag{101}$$

holds for all $i = 0, 1, \ldots, t$ provided that m is large. With inequality (92), we get that

$$X_i \leq c_{21} \log_2^2 m \log_3 m \tag{102}$$

holds for all $i = 0, 1, \ldots, t$. We now return to (87) and take logarithms and notice that we get

$$\log m \leq X_0 \log \lambda_1 + \sum_{i=1}^{t} X_i \log p_i, \tag{103}$$

and now inequalitites (86), (102) and (103) lead to the inequality

$$\log m < c_{22} \log_2^3 m \log_3 m \tag{104}$$

for sufficiently large m. But (104) clearly implies that $m < c_{23}$.

This disposes of Case 2 and ends the proof of our Theorem. □

Acknowledgements. Work for this paper was supported in part by Grant SEP-CONACYT 37259-E.

References

[1] A. BAKER and G. WÜSTHOLZ, Logarithmic forms and group varieties. *J. reine angew. Math* **442** (1993), 19–62.

[2] Y. BUGEAUD, P. CORVAJA, and U. ZANNIER, An upper bound for the G.C.D. of $a^n - 1$ and $b^n - 1$. *Math. Z.* **243** no. 1 (2003), 79–84.

[3] P. CORVAJA and U. ZANNIER, On the greatest prime factor of $(ab + 1)(ac + 1)$. *Proc. Amer. Math. Soc.* **131** no. 6 (2003), 1705–1709.

[4] K. GYŐRY, A. SÁRKÖZY, and C. L. STEWART, On the number of prime factors of integers of the form $ab + 1$. *Acta Arith.* **74** no. 4 (1996), 365–385.

[5] S. H. HERNÁNDEZ and F. LUCA, On the greatest prime factor of $(ab+1)(bc+1)(ca+1)$. *Bol. Soc. Math. Mexicana*, to appear.

[6] ———, S. H. HERNÁNDEZ and F. LUCA, Common factors of shifted Fibonacci numbers. *Per. Math. Hungarica*, to appear.

[7] F. LUCA, Arithmetic properties of members of a binary recurrent sequence. *Acta Arith.* **109** no. 1 (2003), 81–107.

[8] W. SCHMIDT, Equations $\alpha^x = R(x, y)$. *J. Number Theory* **47** (1994), 348–358.

[9] T. N. SHOREY and R. TIJDEMAN, *Exponential Diophantine Equations*. Cambridge University Press, Cambridge, 1986.

[10] K. R. YU, p-adic logarithmic forms and group varieties. II. *Acta Arith.* **89** no. 4 (1999), 337–378.

Received: 31 January 2003

Communicated by: R. Berndt

Author's address: Florian Luca, Mathematical Institute, UNAM, Campus Morelia, Ap. Postal 61-3 (Xangari), CP 58 089, Morelia, Michoacán, Mexico

E-mail: `fluca@matmor.unam.mx`.