Bull. Aust. Math. Soc. **100** (2019), 206–215
doi:10.1017/S0004972719000625

ON THE FACTORISATION OF $x^2 + D$

AMIR GHADERMARZI

(Received 24 November 2018; accepted 28 March 2019; first published online 27 May 2019)

Abstract

Let D be a positive nonsquare integer, p a prime number with $p \nmid D$ and $0 < \sigma < 0.847$. We show that there exist effectively computable constants C_1 and C_2 such that if there is a solution to $x^2 + D = p^n$ with $p^n > C_1$, then for every $x > C_2$ with $x^2 + D = p^n m$ we have $m > x^\sigma$. As an application, we show that for $x \neq \{5, 1015\}$, if the equation $x^2 + 76 = 101^n m$ holds, then $m > x^{0.14}$.

2010 *Mathematics subject classification*: primary 11D61; secondary 11D75.

Keywords and phrases: hypergeometric method, Padé approximant, Ramanujan–Nagell equation.

1. Introduction

Let $f(x)$ be a polynomial with integer coefficients and at least two distinct complex roots. We wish to bound the p-adic norm of $f(n)$ at least for large integer values of n. To be more precise, let $[f(n)]_p = |f(n)|_p^{-1}$, where $|a|_p$ denotes the usual p-adic norm of a. Is it possible to find a good upper bound for $[f(n)]_p$ in terms of n and $f(n)$? Mahler [9] answered this question affirmatively by finding sharp bounds. He proved that for the equation $f(n) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} m$, where $(m, \prod p_i) = 1$ and for any $\epsilon > 0$, there exists a constant C such that for any $n > C$, we have $m > n^{1-\epsilon}$. This gives a bound of the shape $[f(n)]_p \ll f(n)/n^{1-\epsilon}$. Mahler's proof depends on the p-adic version of Roth's theorem, so one cannot effectively compute the value C using Mahler's argument. While quantifying this result in general is a difficult task, there are some effective results with much weaker bounds. Stewart [10], by means of Baker's theory of linear forms in logarithms, proved effective results for products of consecutive integers. He showed that if $n(n+1)\cdots(n+k) = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s} m$, where $(m, \prod p_i) = 1$, then $m \gg n^{\sigma(p_1, p_2, \ldots, p_s)}$ for some small number $\sigma(p_1, p_2, \ldots, p_s) > 0$. Gross and Vincent [8] extended Stewart's approach to polynomials with at least two distinct roots.

The effective result in this note is not as general as those of Stewart, Vincent and Gross, but it gives much better bounds for $[f(n)]_p$ for polynomials of the form $x^2 + D$ under some restrictions. These restrictions enable us to use a method based upon Padé

This research was in part supported by a grant from IPM (No. 95110044).

approximation. Such an approach has been used before to prove effective versions of Mahler's result. Bennett *et al.* [4] proved that if $n^2 + n = 2^\alpha 3^\beta m$ and $n > 8$, then $m > n^{0.285}$. They also showed that if $n^2 + 7 = 2^\alpha m$, then either $n \in \{1, 3, 5, 11, 181\}$ or $m > n^{1/2}$ [3]. This hypergeometric method has also been used to find upper bounds on the number of solutions to equations of the form $x^2 + D = p^n$ (see [1, 5, 6]). We use this approach to find an effective upper bound for $[f(n)]_p$ when $f(x) = x^2 + D$ and p is a prime number with $p \nmid D$. Our result relies on the existence of a relatively large solution to the equation $x^2 + D = p^n$, which we will term 'huge'. In order to obtain explicit results, we need to define what we mean by a huge solution. Obviously, the bigger this solution is, the easier it is to obtain an explicit result.

Let $0 < \sigma < 0.847$ be a real number. We set a condition for a huge solution that depends on σ. Assume that (x_0, n_0) is a positive solution to the equation $X^2 + D = p^N$ with $p \nmid D$. If p is an odd prime, the condition for (x_0, n_0) to be a σ-huge solution is

$$\left|x_0 + \sqrt{-D}\right| = p^{n_0/2} > C_{\sigma,p} D^\eta, \tag{1.1}$$

where

$$\eta = \frac{7.84 - 4\sigma}{7.64 - 9\sigma} \quad \text{and} \quad C_{\sigma,p} = (2008.832)^{(1.96-\sigma)/(7.64-9\sigma)}.$$

If $p = 2$, the condition for (x_0, n_0) to be a σ-huge solution is

$$\tfrac{1}{2}\left|x_0 + \sqrt{-D}\right| = 2^{n_0/2-1} > C_{\sigma,2} D^\eta, \tag{1.2}$$

where

$$C_{\sigma,2} = (7.847)^{(1.96-\sigma)/(7.64-9\sigma)}.$$

For such solutions, we define $\beta = x_0 + \sqrt{-D}$ when p is an odd prime and we define $\beta = \frac{1}{2}(x_0 + \sqrt{-D})$ when $p = 2$.

THEOREM 1.1. *Let $0 < \sigma < 0.847$. Assume that D is a positive integer, p is a prime with $p \nmid D$ and the equation $X^2 + D = p^N$ has a σ-huge solution (x_0, n_0) with $|\beta| \geq 90.93$. Let $M = 250 n_0$. If $x^2 + D = p^n m$ with $n > M$, then $m > x^\sigma$.*

Since $\sigma < 1$, as an immediate corollary we have the following result.

COROLLARY 1.2. *Assume that the equation $X^2 + D = p^N$ has a σ-huge solution which satisfies the conditions of Theorem 1.1. If $x > p^{250 n_0}$ and $x^2 + D = p^n m$, then $m > x^\sigma$.*

Note that for $D \leq 12$ based on the table at the end of the paper [7], the only equation with a huge solution corresponds to $D = 7$, where $181^2 + 7 = 2^{15}$ is a huge solution for any σ with $\sigma < 0.49268$. But, as mentioned before, Bennett *et al.* [3] proved that if $n^2 + 7 = 2^\alpha m$, then either $n \in \{1, 3, 5, 11, 181\}$ or $m > n^{0.5}$. Therefore, the theorem holds for $D \leq 12$. From now on, let D be a nonsquare positive integer bigger than 12. The idea of the proof is to approximate $(\bar{\beta}/\beta)^k$ with rational and algebraic numbers. From the equation $x^2 + D = p^n m$, whenever m is small compared to $|\beta|$, we obtain a good approximation for $(\bar{\beta}/\beta)^k$. If the equation $X^2 + D = p^N$ has a huge solution, then there exists a good approximation for $k = 1$. We use a method based on Padé approximation

https://doi.org/10.1017/S0004972719000625 Published online by Cambridge University Press

to show that if there exists a huge solution, we have a good approximation for $k = 1$. However, it is not possible to get such a good approximation (with m small) for larger values of k.

We proceed as follows. In Section 2, we use Padé approximations to the function $(1 - x)^k$ to generate approximations for $(\bar{\beta}/\beta)^k$. In Section 3, using a huge solution of $X^2 + D = p^N$, we get an approximation for $(\bar{\beta}/\beta)^k$. In Section 4, by combining the approximations of Sections 2 and 3, we prove Theorem 1.1. In Section 5, we consider the equation $x^2 + 78 = 101^n m$ to show that the value M in Theorem 1.1 is not unattainably large and that the equation $x^2 + D = p^n m$ can be solved relatively quickly for any x less than p^M.

2. Padé approximation

In this section, we use Padé approximations to the function $(1 - x)^k$ to get approximations of $(\bar{\beta}/\beta)^k$. We follow Bennett [2] to produce these approximations. Let A, B and C be positive integers. Define

$$\begin{aligned} P_A(z) &= \frac{(A+B+C+1)!}{A!B!C!} \int_0^1 t^A (1-t)^B (z-t)^C \, dt, \\ Q_A(z) &= \frac{(-1)^C (A+B+C+1)!}{A!B!C!} \int_0^1 t^B (1-t)^C (1-t+zt)^A \, dt, \\ E_A(z) &= \frac{(A+B+C+1)!}{A!B!C!} \int_0^1 t^A (1-t)^C (1-zt)^B \, dt. \end{aligned} \tag{2.1}$$

From these definitions,

$$P_A(z) - (1-z)^{B+C+1} Q_A(z) = z^{A+C+1} E_A(z). \tag{2.2}$$

So, these equations provide a set of approximations to $(1 - z)^{B+C+1}$, valid close to $z = 0$. Expanding the formulas above leads to the following lemma.

Lemma 2.1 [2, Lemma 1]. *With the notation as above, the functions P_A, Q_A and E_A satisfy*

$$\begin{aligned} P_A(z) &= \sum_{i=0}^{C} \binom{A+B+C+1}{i} \binom{A+C-i}{A} (-z)^i, \\ Q_A(z) &= (-1)^C \sum_{i=0}^{A} \binom{A+C-i}{C} \binom{B+i}{i} (z)^i, \\ E_A(z) &= \sum_{i=0}^{B} \binom{A+i}{i} \binom{A+B+C+1}{A+C+i+1} (-z)^i. \end{aligned} \tag{2.3}$$

Moreover, $P_A(z)Q_{A+1}(z) - Q_A(z)P_{A+1}(z) = cz^{A+C+1}$ [2], which means that we have distinct approximations for $(1 - z)^{B+C+1}$. For our purpose, namely for finding

https://doi.org/10.1017/S0004972719000625 Published online by Cambridge University Press

approximations to $(\bar{\beta}/\beta)^k$, we take $A = C = r$ and $B = k - r - 1$. Taking $A = C$ gives a diagonal approximation and, from our choice of B, we get the desired approximation of $(1 - z)^k$. With this choice of parameters, the Equations (2.1) can be rewritten as the following lemma.

LEMMA 2.2 [3]. *For positive integers k and r with $k > r$, there exist polynomials $P_r(z)$, $Q_r(z)$ and $E_r(z)$ with integer coefficients such that:*

(1) $Q_r(z) = ((k+r)!/(k-r-1)!r!r!) \int_0^1 t^{k-r-1}(1-t)^r(1-t+zt)^r dt$;

(2) $E_r(z) = ((k+r)!/(k-r-1)!r!r!) \int_0^1 t^r(1-t)^r(1-tz)^{k-r-1} dt$;

(3) $\deg P_r = \deg Q_r = r$ *and* $\deg E_r = k - r - 1$;

(4) $P_r(z) - (1-z)^k Q_r(z) = (-1)^r z^{2r+1} E_A(z)$;

(5) $P_r(z)Q_{r+1}(z) - Q_r(z)P_{r+1}(z) = cz^{2r+1}$ *for some nonzero constant c.*

An important parameter in these approximations is the ratio r/k. Smaller ratios give better results, but only for larger values of $|\beta|$. To get more general results, we take

$$k = 5j, \quad r = 4j - g, \tag{2.4}$$

where $g \in \{0, 1\}$. With our choices of k and r, we can rewrite the functions $Q_r(z)$, $P_r(z)$ and $E_r(z)$ of Lemma 2.1 as

$$P_r(z) = (-1)^g \sum_{i=0}^{4j-g} \binom{9j-g}{i}\binom{8j-2g-i}{4j-g}(-z)^i,$$

$$Q_r(z) = \sum_{i=0}^{4j-g} \binom{8j-2g-i}{4j-g}\binom{j+g-1+i}{i}(z)^i,$$

$$E_r(z) = \sum_{i=0}^{j+g} \binom{4j-g+i}{i}\binom{9j-g}{8j-2g+i+1}(-z)^i.$$

To use Padé approximations, we need explicit bounds for $Q_r(z_0)$ and $E_r(z_0)$. The polynomials P_r, Q_r and E_r have integer coefficients and, by dividing by the greatest common divisor of their coefficients, we get polynomials with integer coefficients and smaller heights and, consequently, a better approximation. Set

$$c_g(j) = \gcd_{i\in\{0,1,\ldots,4j-g\}} \binom{8j-2g-i}{4j-g}\binom{j+g-1+i}{i}.$$

Then $p_r^*(z) = c_g(j)^{-1}P_r(z)$, $Q_r^*(z) = c(j)^{-1}Q_r(z)$ and $E_r^*(z) = c_g(j)^{-1}E_r(z)$ have integer coefficients and, by Lemma 2.2(4) and (5),

$$P_r^*(z) - (1-z)^k Q_r^*(z) = (-1)^r z^{2r+1} E_A^*(z)$$

and

$$P_r(z)g^* Q_{r+1}^*(z) - Q_r^*(z)P_{r+1}^*(z)g = cz^{2r+1}$$

for some nonzero constant c. We have the following result to bound $c_g(j)$.

https://doi.org/10.1017/S0004972719000625 Published online by Cambridge University Press

LEMMA 2.3 [4]. *For $j > 50$ and $g \in \{0, 1\}$,*

$$c_g(j) > 2.943^j.$$

PROOF. This is the special case of [4, Proposition 5.1] with $d = 4, c = 5$ and $m = j$. □

2.1. Explicit bounds for approximations. From now on, we take

$$z_0 = 1 - \frac{\bar{\beta}}{\beta} = \frac{\lambda}{\beta},$$

where $\lambda = 2\sqrt{-D}$ if p is an odd prime and $\lambda = \sqrt{-D}$ if $p = 2$.

2.1.1. Upper bound for $|Q_r^*(z_0)|$. For $g = 1$, there is a much stronger upper bound for $Q_r^*(z_0)$. Therefore, to determine an upper bound for $|Q_r^*(z_0)|$, we assume that $g = 0$. First we recall a useful lemma.

LEMMA 2.4 [2]. *For positive integers A, B and C,*

$$\frac{(A+B+C)!}{A!B!C!} < \frac{1}{2\pi}\sqrt{\frac{A+B+C}{ABC}}\,\frac{(A+B+C)^{A+B+C}}{A^A B^B C^C}.$$

From this lemma, by making suitable choices of A, B and C,

$$\frac{(k+r)!}{(k-r-1)!r!r!} = \frac{(9j)!}{(j-1)!((4j)!)^2} < \frac{3}{8\pi}(3^{18}2^{-16})^j.$$

For $0 < t < 1$, since $1 - z_0 = \bar{\beta}/\beta$,

$$|1 - (1 - z_0)t|^2 = 1 - 2bt + t^2 \quad \text{where } b = 1 - \frac{2D}{|\beta|^2}.$$

Since $D > 12$, from (1.1) or (1.2), b is a positive number between 0.953 and 1. With a smaller value of b, we get a larger value of $\{(1-z)^4 z(1-2bz+z^2)^2\}$. It follows that

$$\max_{t\in[0,1]} \{(1-t)^4 t(1-2bt+t^2)^2\} \le 0.044479.$$

Also, under the same conditions,

$$\int_0^1 (1-t)^4(1-2bt+t^2)^2 dt < 0.114552.$$

Therefore,

$$\begin{aligned}
&\left|\frac{(k+r)!}{(k-r-1)!r!r!}\int_0^1 t^{k-r-1}(1-t)^r(1-t+z_0t)^r\,dt\right| \\
&\quad\le \frac{3}{8\pi}(3^{18}2^{-16})^j \int_0^1 ((1-t)^4 t(1-2bt+t^2)^2)^{j-1}(1-t)^4(1-2bt+t^2)^2\,dt \\
&\quad\le \frac{3}{8\pi}(3^{18}2^{-16})^j 0.044479^{j-1}\int_0^1 (1-t)^4(1-2bt+t^2)^2\,dt \\
&\quad\le 0.308 \times (262.9407)^j.
\end{aligned}$$

It follows that

$$\left|Q_r^*(z_0)\right| < 0.308 \times (89.3445)^j. \tag{2.5}$$

https://doi.org/10.1017/S0004972719000625 Published online by Cambridge University Press

2.1.2. An upper bound for $|E_r^*(z_0)|$. For any $t \in [0, 1]$,

$$|1 - tz_0|^2 = 1 - \frac{|\lambda|}{|\beta|}t(1-t) \le 1.$$

Therefore,

$$\begin{aligned}|E_r(z_0)| &= \left|\frac{(k+r)!}{(k-r-1)!r!r!}\int_0^1 t^r(1-t)^r(1-tz_0)^{k-r-1}\,dt\right| \\ &\le \frac{(k+r)!}{(k-r-1)!r!r!}\int_0^1 (1-t)^r t^r\,dt \\ &= \frac{(k+r)!}{(k-r-1)!(2r+1)!}.\end{aligned}$$

LEMMA 2.5. *Let A and B be positive integers. Then*

$$\frac{(A+B)!}{A!B!} < \frac{1}{\sqrt{2\pi}}\sqrt{\frac{A+B}{AB}}\,\frac{(A+B)^{A+B}}{A^A B^B}.$$

PROOF. The result follows from the explicit version of Stirling's formula by considering the following inequality for positive integers A and B:

$$\frac{1}{12(A+B)} - \frac{1}{12A+1/4} - \frac{1}{12B+1/4} < 0. \qquad \square$$

This lemma gives a weaker bound for $|E_r(z_0)|$ when $g = 1$ and so

$$|E_r(z_0)| \le \frac{(9j-1)!}{(j)!(8j-1)!} < \frac{0.377}{\sqrt{j}}\left(\frac{9^9}{8^8}\right)^j.$$

Consequently,

$$|E_r^*(z_0)| < \frac{0.377}{j} \times (7.847)^j. \tag{2.6}$$

To summarise, we have the approximation

$$\beta^k P_r^*(z_0) - \bar{\beta}^k Q_r^*(z_0) = \beta^{k-2r+1}\lambda^{2r+1}E_r^*(z_0) \tag{2.7}$$

with explicit exponential bounds on $P_r^*(z_0)$ and $E_r^*(z_0)$ in terms of r, as desired.

3. Second approximation: algebraic setup

We assume that the equation $X^2 + D = P^N$ has a σ-huge solution (x_0, n_0) and $x^2 + D = p^n M$ with $n \gg n_0$. Then, working in the ring of algebraic integers of the number field $\mathbb{Q}(\sqrt{-D})$, we will relate this solution (x, n) to the given solution (x_0, n_0). This enables us to find an approximation for $(\bar{\beta}/\beta)^k$.

THEOREM 3.1. *Let x_0, D and β be as in Theorem 1.1 and $x^2 + D = p^n m$ with $n > 5n_0$. Then there exist a rational integer j and an algebraic integer μ in the number field $\mathbb{Q}(\sqrt{-D})$ such that $\beta^k\mu - \bar{\beta}^k\bar{\mu} = \pm\lambda$, where $k = 5j$, $\lambda = 2\sqrt{-D}$ if p is an odd prime and $\lambda = \sqrt{-D}$ if $p = 2$.*

https://doi.org/10.1017/S0004972719000625 Published online by Cambridge University Press

PROOF. As outlined above, consider the two solutions

$$x_0^2 + D = p^{n_0} \tag{3.1}$$

and

$$x^2 + D = p^n m. \tag{3.2}$$

First assume that p is an odd prime number. Since $(-D/p) = 1$, the ideal (p) of $\mathbb{Q}(\sqrt{-D})$ splits into two prime ideals (α) and (α') with $(p) = (\alpha)(\alpha')$. Factoring Equation (3.1) in the ring of integers of the number field $\mathbb{Q}(\sqrt{-D})$ gives

$$(x_0 + \sqrt{-D})(x_0 - \sqrt{-D}) = (\alpha)^{n_0}(\alpha')^{n_0}, \tag{3.3}$$

where α and α' are prime ideals. Each of α and α' divides at least one of the two factors on the left-hand side of (3.3). Moreover, since none of the factors on the left-hand side of (3.3) belongs to the ideal (p), the ideals (α) and (α') cannot both divide the same factor. Therefore, we can assume that

$$(x_0 + \sqrt{-D}) = (\alpha)^{n_0}, \quad (x_0 - \sqrt{-D}) = (\alpha')^{n_0}.$$

Both ideals $(\alpha)^{n_0}$ and $(\alpha')^{n_0}$ are principal ideals. Define $\beta = x_0 + \sqrt{-D}$ as a generator of the ideal $(\alpha)^{n_0}$ and $\beta' = x_0 - \sqrt{-D}$ as a generator of the ideal $(\alpha')^{n_0}$. Factoring the Equation (3.2) in the ring of integers of number field $\mathbb{Q}(\sqrt{-D})$ gives

$$(x + \sqrt{-D})(x - \sqrt{-D}) = (\alpha)^n(\alpha')^n(m).$$

By a similar argument, each of the factors $(x \pm \sqrt{-D})$ belongs to exactly one of the ideals $(\alpha)^n$ and $(\alpha')^n$. Let us assume that $(x + \sqrt{-D})$ belongs to the ideal $(\alpha)^n$. Then it belongs to any ideal $(\alpha)^i$ with $i < n$. Since $n > 5n_0$, there exists an integer j with $k = 5j$ such that $n = 5n_0 j + l = n_0 k + l$, where $l < 5n_0$. Therefore, $(x + \sqrt{-D})$ belongs to the ideal $(\alpha^{n_0})^k = (\beta)^k$. On the other hand, $(\beta)^k$ is a principal ideal with β^k as a generator. Hence, there is an algebraic integer μ in the number field $\mathbb{Q}(\sqrt{-D})$ such that $x + \sqrt{-D} = \beta^k\mu$. Taking conjugates, $x - \sqrt{-D} = \bar{\beta}^k\bar{\mu}$. If $(x + \sqrt{-D})$ belongs to the ideal $(\alpha')^n$, the same steps show that there is an algebraic integer μ in the number field $\mathbb{Q}(\sqrt{-D})$ such that $x + \sqrt{-D} = \bar{\beta}^k\mu$. Thus, in any case, $\beta^k\mu - \bar{\beta}^k\bar{\mu} = \pm 2\sqrt{D}$.

For $p = 2$, the argument is similar with minor modifications. Let $x_0^2 + D = 2^{n_0}$. Since $-D \equiv 1 \pmod 4$, we can factorise the equation as

$$\tfrac{1}{2}(x_0 + \sqrt{-D}) \cdot \tfrac{1}{2}(x_0 - \sqrt{-D}) = 2^{n-2}.$$

There is an algebraic integer μ in the number field $\mathbb{Q}(\sqrt{-D})$ such that either

$$\tfrac{1}{2}(x + \sqrt{-D}) = \beta^k\mu \quad \text{and} \quad \tfrac{1}{2}(x - \sqrt{-D}) = \bar{\beta}^k\bar{\mu}$$

or

$$\tfrac{1}{2}(x + \sqrt{-D}) = \bar{\beta}^k\mu \quad \text{and} \quad \tfrac{1}{2}(x - \sqrt{-D}) = \beta^k\bar{\mu}.$$

In any case $\beta^k\mu - \bar{\beta}^k\bar{\mu} = \pm\sqrt{D} = \pm\lambda$. □

https://doi.org/10.1017/S0004972719000625 Published online by Cambridge University Press

Theorem 3.1 states that, whenever $|\mu|$ is small compared to β^k, there exists a good approximation for $(\bar{\beta}/\beta)^k$. In fact, $\mu\bar{\mu} = 2^l m$, where $l < 5n_0$ for an odd prime p and $l < 5(n_0 - 2)$ for the case $p = 2$. Thus, whenever m is small compared to β^k, there exists a good approximation for $(\bar{\beta}/\beta)^k$.

The following inequalities will also be helpful in the proof of Theorem 1.1. If $p = 2$, then $|\beta^k\mu| = \frac{1}{2}\sqrt{x^2 + D} > 0.7x$ and, if p is an odd prime, then $|\beta^k\mu| = \sqrt{x^2 + D} > x$.

4. Proof of Theorem 1.1

In this section, we prove Theorem 1.1 using approximations of $(\bar{\beta}/\beta)^k$ in (2.7) and Theorem 3.1. Throughout the proof, we assume that

$$k = 5j, \quad j \geq 50 \quad \text{and} \quad n > M \geq 250n_0.$$

Let $x^2 + D = p^n m$ with $n > M$, it follows that $x^2 + D \geq p^{M+1}$. Since $x_0^2 + D = p^{n_0}$, we can conclude that $x > p^{125n_0}$. Multiplying both sides of the Equation (2.7) by β^r,

$$\beta^k P - \bar{\beta}^k Q = E, \tag{4.1}$$

where

$$P = \beta^r P_r^*(z_0), \quad Q = \beta^r Q_r^*(z_0) \quad \text{and} \quad E = \beta^{k-r-1}\lambda^{2r+1}E_r^*(z_0).$$

Note that by considering the degrees of P_r, Q_r and E_r, we can see that P, Q and E are algebraic integers in the quadratic number field $\mathbb{Q}(\sqrt{-D})$.

From Equations (4.1) and (3.1),

$$\beta^k(Q\mu - P\bar{\mu}) = \pm Q\lambda - E\bar{\mu}.$$

From Lemma 2.2(5), for at least one of the values of g in $r = 4j - g$, the left-hand side of the equation above is nonzero. Thus, $Q\mu - P\bar{\mu}$ is an algebraic integer in the number field $\mathbb{Q}(\sqrt{-D})$, so its norm is at least 1. Therefore,

$$|\beta^k| \leq |Q|\,|\lambda| + |E|\,|\bar{\mu}|.$$

From (2.5) and (1.1),

$$|Q|\,|\lambda| < 0.238074 \times (89.3445)^j \beta^r \beta^{0.4873}.$$

Thus, whenever $\beta > 90.93$,

$$|Q|\,|\lambda| < \tfrac{9}{10}|\beta^k|$$

and so

$$\tfrac{1}{10}|\beta|^k \leq |\beta|^{k-r-1}|\lambda|^{2r+1}|E_r^*(z_0)|\,|\mu|.$$

It follows that

$$|\mu| \geq \left(\frac{\beta^{r+1}}{\lambda^{2r+1}}\right)\frac{1}{10E_r^*(Z_0)} > \left(\frac{\beta^4}{7.847(\lambda)^8}\right)^j \frac{\lambda\sqrt{j}}{3.7}.$$

https://doi.org/10.1017/S0004972719000625 Published online by Cambridge University Press

Using the conditions in (1.1),

$$(|\beta|^k)^{(\sigma+0.04)/(1.96-\sigma)} = (|\beta|^{(5\sigma+0.2)/(1.96-\sigma)})^j < \left(\frac{\beta^4}{\lambda^8 7.847}\right)^j \le \frac{|\mu|}{6.89}.$$

It is easy to check that $\beta^k\mu > 0.7x$, so $(0.7x)^{(\sigma+0.04)/(1.96-\sigma)} < (\beta^k\mu)^{(\sigma+0.04)/(1.96-\sigma)}$. But, from the above, $(|\beta|^k)^{(\sigma+0.04)/(1.96-\sigma)} < |\mu|/6.89$ and so

$$\mu^{2/(1.96-\sigma)} > 5.24x^{(\sigma+0.04)/(1.96-\sigma)} \Longrightarrow \mu^2 > 6.32x^{\sigma+0.04}.$$

Finally, since $x > p^{125n_0}$,

$$m \ge \frac{|\mu|^2}{p^{5n_0-1}} > \frac{6.32x^{\sigma+0.04}}{p^{5n_0-1}} > x^{\sigma}.$$

This completes proof of Theorem 1.1.

As mentioned before, smaller values of r/k give stronger results for larger values of $|\beta|$. As an example, we take the case in which $k = 7j$ and $r = 6j - \sigma$ without a detailed proof. For $|\beta| > 1300$, it is enough to take $\eta_\epsilon = (11.76 - 6\sigma)/(11.48 - 13\sigma)$, $C_{\sigma,p} = (42106)^{(1.96-\sigma)/(11.48-13\sigma)}$ and $C_{\sigma,2} = (10.28)^{(1.96-\sigma)/(11.48-13\sigma)}$ to obtain a similar result to Theorem 1.1.

5. The equation $x^2 + 76 = 101^n m$

As an application of Theorem 1.1, we consider the equation $x^2 + 76 = 101^n m$. The value of M in Corollary 1.2 might appear extraordinary large. In practice it is easy to check the values less than P^M. To see this, we present the following result.

THEOREM 5.1. *Let $x^2 + 76 = 101^n m$. Then either $x \in \{5, 1015\}$ or $m > x^{0.14}$.*

PROOF. Note that $(1015, 3)$ is a solution to the equation $X^2 + 76 = 101^N$. This can be considered as a large solution. To be more precise, $(1015, 3)$ is a σ-huge solution for any σ with $\sigma \le 0.14$ and it satisfies the conditions of Theorem 1.1. Therefore, from Corollary 1.2, the result holds for $x > 101^{750}$.

Assume that $x < 101^{750}$ and $m < x^{0.14}$. We have to check for solutions of the equation $x^2 + 76 = 101^n m$ for $n \le 750$ and $x < 101^n$. For any $n < 750$, we solve the equation $x^2 + 76 \equiv 0 \pmod{101^n}$ and find $m = (x^2 + 76)/101^n$. From Hensel's lemma, for each n there are two values that need to be checked and this can be easily done using a recursion relation. In this way it is easy to confirm the theorem for all the values $n < 750$. In fact, for $x < 101^{3000}$, we have the stronger result that $m > x^{0.9}$ or $x \in \{5, 1015\}$. □

Acknowledgements

The author would like to thank Professor Rahim Zare Nahandi for his careful reading of the earlier version and Professor Michael Bennett for helpful comments and suggestions that improved the presentation of the manuscript. The author is also grateful to the referee for the careful reading and many comments and corrections.

References

[1] M. Bauer and M. Bennett, 'Applications of the hypergeometric method to the generalized Ramanujan–Nagell equation', *Ramanujan J.* **6**(2) (2002), 209–270.
[2] M. Bennett, 'Fractional parts of powers of rational numbers', *Math. Proc. Cambridge Philos. Soc.* **114**(2) (1993), 191–201.
[3] M. A. Bennett, M. Filaseta and O. Trifonov, 'Yet another generalization of the Ramanujan–Nagell equation', *Acta Arith.* **134**(3) (2008), 211–217.
[4] M. A. Bennett, M. Filaseta and O. Trifonov, 'On the factorization of consecutive integers', *J. reine angew. Math.* **629** (2009), 171–200.
[5] F. Beukers, 'On the generalized Ramanujan–Nagell equation. I', *Acta Arith.* **38**(4) (1980–1981), 389–410.
[6] F. Beukers, 'On the generalized Ramanujan–Nagell equation. II', *Acta Arith.* **39**(2) (1981), 113–123.
[7] Y. Bugeaud, M. Mignotte and S. Siksek, 'Classical and modular approaches to exponential Diophantine equations. II. The Lebesgue–Nagell equation', *Compos. Math.* **142**(1) (2006), 31–62.
[8] S. S. Gross and A. F. Vincent, 'On the factorization of $f(n)$ for $f(x)$ in $\mathbb{Z}[x]$', *Int. J. Number Theory* **9**(5) (2013), 1225–1236.
[9] K. Mahler, *Lectures on Diophantine Approximations. Part I: G-adic Numbers and Roth's Theorem* (University of Notre Dame Press, Notre Dame, IN, 1961), prepared from the notes by R. P. Bambah of lectures given at the University of Notre Dame in the fall of 1957.
[10] C. L. Stewart, 'A note on the product of consecutive integers', in: *Topics in Classical Number Theory, Vols. I, II (Budapest, 1981)*, Colloquium Mathematicum Societatis János Bolyai, 34 (North-Holland, Amsterdam, 1984), 1523–1537.

AMIR GHADERMARZI, School of Mathematics,
Statistics and Computer Science, College of Science,
University of Tehran, Tehran, Iran
and
School of Mathematics,
Institute for Research in Fundamental Science (IPM),
P.O. Box 19395-5746, Tehran, Iran
e-mail: a.ghadermarzi@ut.ac.ir

https://doi.org/10.1017/S0004972719000625 Published online by Cambridge University Press