THE RAMANUJAN JOURNAL, 6, 209–270, 2002

Applications of the Hypergeometric Method to the Generalized Ramanujan-Nagell Equation

MARK BAUER m-bauer@math.uiuc.edu
MICHAEL A. BENNETT* mabennet@math.uiuc.edu
Department of Mathematics, University of Illinois, Urbana, Illinois 61801

Received March 15, 2001; Accepted November 13, 2001

Abstract. In this paper, we refine work of Beukers, applying results from the theory of Padé approximation to $(1-z)^{1/2}$ to the problem of restricted rational approximation to quadratic irrationals. As a result, we derive effective lower bounds for rational approximation to $\sqrt{m}$ (where m is a positive nonsquare integer) by rationals of certain types. For example, we have

$$\left|\sqrt{2}-\frac{p}{q}\right| \gg q^{-1.47} \quad \text{and} \quad \left|\sqrt{3}-\frac{p}{q}\right| \gg q^{-1.62},$$

provided q is a power of 2 or 3, respectively. We then use this approach to obtain sharp bounds for the number of solutions to certain families of polynomial-exponential Diophantine equations. In particular, we answer a question of Beukers on the maximal number of solutions of the equation $x^2 + D = p^n$ where D is a nonzero integer and p is an odd rational prime, coprime to D.

Key words: Ramanujan-Nagell equation, hypergeometric method, Padé approximation

2000 Mathematics Subject Classification: Primary—11D45, 11D61; Secondary—11J82, 11J86.

1. Introduction

A seemingly innocent question of Ramanujan [38] as to the squares in the sequence $2^n - 7$ (i.e. are there any other than those corresponding to $n = 3, 4, 5, 7$ and 15?) has led over subsequent years to an extensive body of work on what are now known as "Ramanujan-Nagell" equations (in reference to the first person to answer Ramanujan's question; see [37]). Though definitions vary, these are usually taken to mean equations of the form

$$f(x) = p_1^{n_1} \ldots p_r^{n_r}, \tag{1.1}$$

where $f(x)$ is a polynomial with integral coefficients and at least two simple zeros, $p_1, \ldots, p_r$ are distinct rational primes and $n_1, \ldots, n_r \geq 2$ are integers. These questions have attracted attention in such diverse fields as coding theory and group theory, and it would not be overstating the case to describe the literature on them as vast. In our bibliography, we

*The second author was supported in part by NSF Grant DMS-0088913.

have attempted to include references to such equations, dating from 1987 or so. We direct the reader to the survey article of Cohen [17] for details of earlier work.

The original techniques used to attack equations like (1.1) were elementary, based upon properties of the number fields generated by the roots of $f(x)$ (again, see [17]). A second approach, relying on Baker's lower bounds for linear forms in logarithms of algebraic numbers, provides an effective algorithm for solving any such equation which, in many instances, can be made practical. To derive sharp bounds upon the number of such solutions in positive integers to families of these equations, via these techniques, appears to be rather difficult, though, as we shall see in Section 11, they do have a role to play.

A third method for solving equations like (1.1) is what we will address in this paper. Though the techniques, based upon explicit rational function approximation to binomial functions, date back, in a number theoretic context, at least to work of Thue [43] and Siegel [42], they were first applied to polynomial-exponential equations by Beukers in [9–11] (see also [44] and [45]). Much of our paper is devoted to assessing both the strengths and the limitations of this approach.

1.1. Diophantine approximation results

The traditional use of the so-called hypergeometric method in Diophantine approximation, as first espoused by Thue [43] and subsequently refined by many others (see e.g. [2, 3, 6–8, 16, 34, 42]), is to generate a dense set of good rational approximations to a fixed algebraic number (usually of the shape $\theta = \sqrt[n]{a/b}$) in order to explicitly improve Liouville's theorem on rational approximation. In our context, we require something rather different as we are concerned with quadratic irrational values of θ, where Liouville's theorem is essentially best possible. For our purposes, we will instead deduce lower bounds for rational approximation to a given θ by rationals with restricted denominators. The model for the type of result we wish to obtain is the following theorem of Beukers [10]:

Theorem 1.1 (Beukers). *If p and q are integers with $q = 2^k$, where k is a non-negative integer, then*

$$\left| \sqrt{2} - \frac{p}{q} \right| > 2^{-43.9} q^{-1.8}.$$

Such a bound leads (almost immediately) to

Corollary 1.2 (Beukers). *If x, D and n are integers for which $x^2 + D = 2^n$, then*

$$n < \frac{10 \log |D|}{\log 2} + 435.$$

This enables one to quickly answer Ramanujan's question with which we opened this section (in the negative). Indeed, we are left only to check the values $n \leq 485$.

We aim, in this paper, to significantly sharpen and generalize these bounds, with the goal of making them more flexible for applications. Before stating our results, we require some notation. Given real numbers x and α, with $|x| < 1$ and $\alpha \geq 1$, let us define $F(z, \alpha, x)$ by

$$F(z, \alpha, x) = \frac{(1 - zx)^{\alpha}}{z(1 - z)^{\alpha}}. \tag{1.2}$$

By calculus, we find that $F(z, \alpha, x)$ attains its minimum on $z \in (0, 1)$ at

$$r(\alpha, x) = \frac{1}{2x}((\alpha + 1) - (\alpha - 1)x - \sqrt{((\alpha + 1) - (\alpha - 1)x)^2 - 4x}). \tag{1.3}$$

We will use these quantities to measure the Archimedean contribution of our approximating forms. To deal with non-Archimedean contributions, we define

$$S_1(\alpha) = \sum_{i=1}^{\infty} \sum_{i\alpha - \frac{\alpha-1}{2} \leq j \leq i\alpha} \left(\frac{2\alpha}{2j - 1} - \frac{\alpha}{j} \right), \tag{1.4}$$

$$S_2(\alpha) = \sum_{i=1}^{\infty} \sum_{i\alpha < j < i\alpha + 1/2} \left(\frac{2\alpha}{2j - 1} - \frac{1}{i} \right), \tag{1.5}$$

$$S_3(\alpha) = \sum_{i=1}^{\infty} \sum_{i\alpha - \frac{\alpha}{2} < j < i\alpha - \frac{\alpha-1}{2}} \left(\frac{2}{2i - 1} - \frac{\alpha}{j} \right) \tag{1.6}$$

and set

$$c(\alpha) = e^{S_1(\alpha) + S_2(\alpha) + S_3(\alpha)}. \tag{1.7}$$

Though it is by no means clear from this definition, we may show (though, for brevity's sake, we will not do so here) that $c(\alpha)$ is a continuous function of α for $\alpha \geq 1$, with $\lim_{\alpha \to \infty} c(\alpha) = 2$. Define, for an integer t,

$$\kappa(t) = \begin{cases} 1 & \text{if } t \equiv 0 \pmod 4 \\ 2 & \text{if } t \equiv 2 \pmod 4 \\ 4 & \text{if } t \equiv \pm 1 \pmod 4). \end{cases}$$

Let us suppose that we are given a, y and m_0 positive integers with $y \geq 2$, and Δ a nonzero integer. For our purposes, these quantities will satisfy

$$x_0^2 + \Delta = a^2 y^{m_0}$$

for some integer x_0. If m_0 is odd and Δ is suitably small, we thus have $\sqrt{y}$ well approximated by

$$\frac{x_0}{a y^{(m_0 - 1)/2}}.$$

To measure the quality of this approximation, we set

$$\Delta_0 = \gcd(\Delta, a^2 y^{m_0}), \quad \xi = \frac{\Delta}{a^2 y^{m_0}}, \quad \Omega = \kappa(\Delta/\Delta_0)\, a^2 y^{m_0}$$

and define

$$m_1 = \min_{p|y} \frac{\mathrm{ord}_p \Omega}{\mathrm{ord}_p y}.$$

Here, if p is a rational prime and k a nonzero integer, we denote by $\mathrm{ord}_p k$ the largest power of p dividing k. It follows that $m_1 \geq m_0$. Further, let us take Ω_1 to be the least positive integer multiple of Ω/Δ_0 satisfying

$$\min_{p|y} \frac{\mathrm{ord}_p \Omega_1}{\mathrm{ord}_p y} = m_1$$

(whereby $\Omega_1 \leq \Omega$) and set $\Delta_1 = \Delta_0 \Omega_1 / \Omega$. These quantities appear to be rather mysterious. We choose them in such a fashion to ensure that Ω/Δ_0 is the denominator of $\xi/4$ (which we will take later as the argument of a particular hypergeometric function). The integers Ω_1 and Δ_1 satisfy

$$\Omega_1/\Delta_1 = \Omega/\Delta_0$$

but are modified in a certain manner to reflect the relative weights of the prime factors of y in, respectively, y and a.

Our first result is

Theorem 1.3. *Suppose that a, y, x_0, m_0 and Δ are integers with m_0 odd and positive and a, y and x_0 positive, y not a square, satisfying*

$$x_0^2 + \Delta = a^2 y^{m_0} \geq 2|\Delta|. \tag{1.8}$$

Further, suppose that there exists a real number $\alpha \geq 3/2$ satisfying

$$c(\alpha)(a^2 y^{m_0})^{\alpha+1} \; \Delta_1 \; F(r(\alpha, \xi), \alpha, \xi) > \Omega_1^{\alpha} \; |\Delta|^{\alpha+1} \tag{1.9}$$

where the various quantities are as defined previously. If s is a given positive integer and $\epsilon > 0$ is real, then there exists an effectively computable constant $q_0 = q_0(a, y, m_0, \Delta, \alpha, s, \epsilon)$ such that, if $p \in \mathbb{Z}$, $q = y^k$ for k a nonnegative integer and $q \geq q_0$, we have

$$\left| \sqrt{y} - \frac{p}{sq} \right| > q^{-\lambda-\epsilon},$$

where

$$\lambda = \frac{\log\left(\frac{\Omega_1^{\alpha} F(r(\alpha,\xi),\alpha,\xi)}{c(\alpha)\;\Delta_1}\right)}{(\alpha-1)\, m_1 \log y}.$$

Let us note that this lower bound is nontrivial (in the sense that $\lambda < 2$) precisely when

$$\Omega_1^{\alpha} \; F(r(\alpha, \xi), \alpha, \xi) < c(\alpha) \; \Delta_1 \; y^{2(\alpha-1)m_1}. \tag{1.10}$$

It may not be immediately apparent that the above theorem can ever be applied to give a nontrivial approximation measure. To demonstrate its utility, we provide the following corollary, where we specialize Theorem 1.3 to values of y with $2 \leq y < 100$:

Corollary 1.4. *Suppose that y is a positive integer in the table below and s is a given positive integer. Then there exists an effectively computable constant $q_0 = q_0(y, s)$ such that, if $p \in \mathbb{Z}$, $q = y^k$ for some nonzero integer k and $q \geq q_0$, we have*

$$\left| \sqrt{y} - \frac{p}{sq} \right| > q^{-\lambda(y)}, \tag{1.11}$$

where $\lambda(y)$ is as follows:

y	$\lambda(y)$	y	$\lambda(y)$	y	$\lambda(y)$	y	$\lambda(y)$	y	$\lambda(y)$
2	1.465	26	1.952	46	1.203	65	1.740	83	1.539
3	1.620	28	1.602	47	1.634	66	1.564	84	1.448
5	1.344	29	1.577	48	1.618	68	1.434	85	1.403
6	1.444	30	1.873	50	1.788	69	1.682	87	1.845
10	1.917	31	1.691	51	1.619	70	1.740	89	1.930
12	1.625	33	1.725	52	1.786	72	1.558	90	1.968
13	1.518	34	1.712	53	1.478	73	1.496	91	1.778
14	1.770	35	1.829	54	1.281	74	1.679	92	1.567
17	1.929	37	1.522	55	1.383	75	1.850	93	1.694
18	1.849	38	1.689	56	1.700	76	1.264	95	1.920
19	1.858	40	1.522	57	1.747	77	1.414	96	1.381
20	1.647	42	1.575	58	1.648	78	1.690	98	1.522
21	1.641	43	1.871	60	1.449	79	1.545	99	1.671
23	1.443	44	1.658	62	1.572	80	1.703		
24	1.624	45	1.501	63	1.745	82	1.699		

(1.12)

Note that, for obvious reasons, we have omitted values of y which are perfect powers. To compare the above result to its analogue in [10], we observe that, apparently, Theorem 5 of [10] implies a nontrivial bound of the shape (1.11), for $2 \leq y \leq 99$ and y not a perfect power, only when $y \in \{2, 3, 23, 46, 55, 76\}$.

For applications to Diophantine problems, we desire more explicit versions of Theorem 1.3 and Corollary 1.4. To state these, we beg the reader's indulgence as we introduce yet more notation. Let

$$\chi_1 = \frac{c_1(\alpha)(a^2 y^{m_0})^{\alpha+1} \, \Delta_1 F(r(\alpha, \xi), \alpha, \xi)}{\Omega_1^{\alpha} |\Delta|^{\alpha+1}} \tag{1.13}$$

and

$$\chi_2 = 2sa^{4\alpha-5} y^{(2\alpha-5/2)m_0} \, (\alpha+1)^2 \, |\Delta|^{3-2\alpha} \, d_1(\alpha)^{-1}. \tag{1.14}$$

Further, let us define

$$m_2 = \min_{p|y}\left\{2(\alpha-1)\frac{\log\chi_2}{\log\chi_1}\left(\frac{\mathrm{ord}_p\Omega_1}{\mathrm{ord}_p y}\right) + \frac{2\mathrm{ord}_p a}{\mathrm{ord}_p y} + m_0\right\}. \tag{1.15}$$

Write

$$\chi_3 = \frac{\Omega_1^\alpha\, F(r(\alpha,\xi),\alpha,\xi)}{c_1(\alpha)\;\Delta_1}, \tag{1.16}$$

and, for the following values of α, define $c_1(\alpha)$ and $d_1(\alpha)$ by

α	$c_1(\alpha)$	$\log d_1(\alpha)$	α	$c_1(\alpha)$	$\log d_1(\alpha)$	α	$c_1(\alpha)$	$\log d_1(\alpha)$
1.5	1.952	−20.184	3.5	1.828	−16.814	5.5	1.828	−16.951
1.6	1.892	−11.057	3.6	1.801	−14.245	5.6	1.811	−15.303
1.7	1.860	−19.422	3.7	1.774	−13.362	5.7	1.793	−14.892
1.8	1.751	−17.520	3.8	1.736	−18.144	5.8	1.769	−15.852
1.9	1.667	−13.031	3.9	1.696	−26.810	5.9	1.743	−16.914
2.0	1.613	−18.495	4.0	1.660	−16.384	6.0	1.719	−12.599
2.1	1.660	−24.199	4.1	1.687	−14.913	6.1	1.738	−11.905
2.2	1.704	−25.928	4.2	1.717	−13.293	6.2	1.760	−15.935
2.3	1.748	−29.238	4.3	1.745	−13.822	6.3	1.780	−14.180
2.4	1.779	−30.478	4.4	1.764	−13.811	6.4	1.794	−17.332
2.5	1.808	−29.261	4.5	1.783	−15.083	6.5	1.807	−19.408
2.6	1.868	−22.140	4.6	1.833	−17.414	6.6	1.843	−18.265
2.7	1.947	−24.505	4.7	1.879	−13.963	6.7	1.875	−17.606
2.8	2.064	−27.823	4.8	1.946	−21.254	6.8	1.922	−20.170
2.9	2.207	−16.762	4.9	2.040	−25.964	6.9	1.986	−23.824
3.0	2.458	−17.335	5.0	2.202	−33.331	7.0	2.097	−35.679
3.1	2.246	−16.558	5.1	2.053	−16.208	7.1	1.993	−16.101
3.2	2.107	−19.243	5.2	1.970	−23.161	7.2	1.934	−22.281
3.3	2.011	−29.883	5.3	1.912	−16.238	7.3	1.892	−15.840
3.4	1.947	−21.044	5.4	1.872	−20.496	7.4	1.863	−16.416

(1.17)

With the notation we have now established, we may state

Theorem 1.5. *Suppose that a, y, x_0, m_0 and Δ are integers with m_0 odd and positive and a, y and x_0 positive, y not a square, satisfying*

$$x_0^2 + \Delta = a^2 y^{m_0} \geq 2|\Delta|.$$

Further, suppose that there exists a real number $\alpha \geq 3/2$ such that $\chi_1 > 1$. If s is a given positive integer, then, if $p \in \mathbb{Z}$ and $q = y^k$, for k a nonnegative integer with $k \geq \frac{m_2-1}{2}$, *we have*

$$\left|\sqrt{y} - \frac{p}{sq}\right| > c_2 q^{-\lambda_1},$$

where

$$c_2 = \frac{d_1(\alpha)}{4s(\alpha+1)\,ay^{m_0/2}}\;\chi_3^{-\frac{(4\alpha-2)m_1+1}{(2\alpha-2)m_1}}$$

and

$$\lambda_1 = \frac{\log \chi_3}{(\alpha-1)m_1\ \log y}.$$

Here, we may either take $c_1(\alpha) = d_1(\alpha) = 1$, *or, for* α *in Table* (1.17), *the values stated.*

In both Theorems 1.3 and 1.5, the restriction to $\alpha \geq 3/2$ is unimportant. With suitable changes to c_2, we may in fact suppose that $\alpha \geq \alpha_0$, for any fixed $\alpha_0 > 1$. Again, we can apply this result to obtain explicit bounds for numerous small values of y. With sufficient computation, we can derive nontrivial bounds for any y with $\lambda(y) < 2$ in Theorem 1.3. For technical reasons, however, we omit the case $y = 89$, treated in Corollary 1.4.

Corollary 1.6. *If y is a positive integer in the table below, then, if $p \in \mathbb{Z}$ and $q = y^k$, for some integer $k > 2$, with*

$$(y,k) \notin \{(2,3),(2,7),(2,8),(3,7)\},$$

we have

$$\left|\sqrt{y} - \frac{p}{q}\right| > q^{-\lambda_2(y)},$$

where $\lambda_2(y)$ *is as follows*:

y	$\lambda_2(y)$	y	$\lambda_2(y)$	y	$\lambda_2(y)$	y	$\lambda_2(y)$	y	$\lambda_2(y)$	y	$\lambda_2(y)$
2	1.48	21	1.67	38	1.72	53	1.51	69	1.73	83	1.55
3	1.65	23	1.45	40	1.55	54	1.29	70	1.75	84	1.46
5	1.36	24	1.64	42	1.61	55	1.39	72	1.58	85	1.43
6	1.46	26	1.97	43	1.91	56	1.76	73	1.51	87	1.89
10	1.99	28	1.64	44	1.68	57	1.76	74	1.69	90	1.98
12	1.65	29	1.60	45	1.53	58	1.66	75	1.91	91	1.82
13	1.53	30	1.91	46	1.21	60	1.47	76	1.27	92	1.58
14	1.84	31	1.70	47	1.66	62	1.58	77	1.44	93	1.73
17	1.94	33	1.73	48	1.63	63	1.76	78	1.70	95	1.95
18	1.87	34	1.74	50	1.81	65	1.76	79	1.56	96	1.41
19	1.87	35	1.87	51	1.65	66	1.57	80	1.72	98	1.54
20	1.67	37	1.55	52	1.81	68	1.46	82	1.71	99	1.69

(1.18)

1.2. Diophantine equations

An almost immediate consequence of the preceding result is the following generalization and sharpening of Corollary 1.2.

Corollary 1.7. *Suppose that y and $\lambda_2(y)$ are as in* (1.18) *and that D is a nonzero integer. If x and $n > 1$ are positive integers for which*

$$x^2 + D = y^n,$$

then we may conclude that

$$n < \frac{2}{2 - \lambda_2(y)} \frac{\log |D|}{\log y},$$

unless

$$(y, n, D) \in \{(2, 3, -1), (2, 15, 7), (5, 3, 4), (5, 5, -11), (23, 5, -26)$$
$$(40, 3, -9), (46, 3, -8), (55, 5, 19), (76, 5, 60)\}.$$

For arbitrary values of y, we may not be able to immediately apply Theorem 1.3 to obtain nontrivial bounds (this is apparently the case, for instance, when $y = 7$). On the other hand, in conjunction with certain "gap principles", we can still use such techniques to derive sharp bounds on the *number* of solutions to generalized Ramanujan-Nagell equations, rather than upon their *size*. In what follows, we restrict our attention to equations of the shape

$$x^2 - D = y^n \tag{1.19}$$

where we will take y to be an odd rational prime and D a nonzero integer. The case $y = 2$ has been admirably treated by Beukers [10] and Le [21, 23], culminating in the following

Theorem 1.8 (Beukers, Le). *Let D be an odd, positive integer. Then the equation*

$$x^2 + D = 2^n$$

has at most one solution in positive integer x and n, unless $D = 7, 23$ or $2^k - 1$ for some $k \geq 4$. The solutions in these exceptional cases are given by
(1) $D = 7, (x, n) = (1, 3), (3, 4), (5, 5), (11, 7), (181, 15)$
(2) $D = 23, (x, n) = (3, 5), (45, 11)$
(3) $D = 2^k - 1 (k \geq 4), (x, n) = (1, k), (2^{k-1} - 1, 2k - 2)$.
Further, the equation

$$x^2 - D = 2^n$$

has at most three solutions in positive integers x and n, unless $D = 2^{2m} - 3 \cdot 2^{m+1} + 1$ for $m \geq 3$ an integer. In these cases, this equation has four positive solutions, given by

$$(x, n) = (2^m - 3, 3), (2^m - 1, m + 2), (2^m + 1, m + 3) \quad \textit{and} \quad (3 \cdot 2^m - 1, 2m + 3).$$

If we take D in (1.19) to be a negative integer and y a rational prime, then, as noted by Beukers [9], distinct solutions in positive integer x and n to (1.19) correspond to integers $m > 1$ for which

$$\frac{\lambda^m - \bar{\lambda}^m}{\lambda - \bar{\lambda}} = \pm 1,$$

where λ is an integer in $\mathbb{Q}(\sqrt{D})$. Recent work on primitive divisors of Lucas-Lehmer numbers by Bilu et al. [12] almost immediately implies the following

Theorem 1.9 (Apéry [1], Bugeaud and Shorey [13]). *Let D be a positive integer and p be an odd prime, not dividing D. Then the Diophantine equation*

$$x^2 + D = p^n$$

has at most one solution in positive integers x and n, unless $(p, D) = (3, 2)$ or $(p, D) = (4a^2 + 1, 3a^2 + 1)$ for some $a \in \mathbb{N}$. In these cases, there are precisely two such solutions.

If, however, $D > 0$, it appears to be somewhat more difficult to derive a sharp bound for the number of solutions to Eq. (1.19). In 1981, Beukers [11] proved

Theorem 1.10. *Let D be a positive integer and p be an odd prime, not dividing D. Then the Diophantine equation*

$$x^2 - D = p^n$$

has at most four solutions in positive integers x and n.

Subsequently, Le [19, 29] (see Yuan [47] for a correction and improvement) showed that the number of such solutions is, in fact, at most three, provided $\max\{p, D\}$ exceeds some effectively computable constant. By combining Theorem 1.5 with lower bounds for linear forms in logarithms of algebraic numbers, we may prove

Theorem 1.11. *Let D be a positive integer and p be an odd prime, not dividing D. Then the Diophantine equation*

$$x^2 - D = p^n$$

has at most three solutions in positive integers x and n.

We note that this last result is sharp. Indeed, take either

$$(p, D) = \left(3, \left(\frac{3^m + 1}{4}\right)^2 - 3^m\right)$$

or

$$(p, D) = \left(4a^2 + 1, \left(\frac{p^m - 1}{4a}\right)^2 - p^m\right),$$

where a and m are positive integers with $m > 1$ (and, if $p = 3$, m odd). It is then easy to check that we have three solutions in positive integers x and n to the equation $x^2 - D = p^n$, given by

$$(x_1, n_1) = \left(\frac{3^m - 7}{4}, 1\right), \quad (x_2, n_2) = \left(\frac{3^m + 1}{4}, m\right)$$

and

$$(x_3, n_3) = \left(2 \cdot 3^m - \frac{3^m + 1}{4}, 2m + 1\right),$$

if $p = 3$, or

$$(x_1, n_1) = \left(\frac{p^m - 1}{4a} - 2a, 1\right), \quad (x_2, n_2) = \left(\frac{p^m - 1}{4a}, m\right)$$

and

$$(x_3, n_3) = \left(2ap^m + \frac{p^m - 1}{4a}, 2m + 1\right),$$

if $p = 4a^2 + 1$. For future reference, we will refer to these (p, D) as *exceptional pairs*. It would be of some interest to know if there are coprime pairs (p, D) which are nonexceptional, for which the equation $x^2 - D = p^n$ has three positive solutions.

Before we proceed further, let us note that the p-adic version of Roth's theorem (see e.g. Ridout [39]) immediately implies, for y a nonsquare positive integer and $\epsilon > 0$, that

$$\left|\sqrt{y} - \frac{p}{q}\right| > q^{-1-\epsilon},$$

provided $q = y^k$ for k sufficiently large. This result is, however, ineffective, in that it is not possible to quantify the term "sufficiently large". Our bounds are, while weaker and less general, completely explicit. Additionally, we would like to comment that the techniques developed in this paper are applicable to Diophantine equations of the shape (1.19) with composite values of y. We omit such results, however, as consideration of y composite introduces some additional complications (but see [15, 31] and [46]).

The layout of this paper is as follows. In Section 2, we introduce the rational function approximations which lie at the heart of our method. In Sections 3 and 4, we derive upper bounds upon the Archimedean valuations of our approximations. Sections 5–7 are all devoted to studying the analogous non-Archimedean valuations. In the first two of these sections, we show that these evaluations are closely related to the function $c(\alpha)$ defined in (1.7). In Section 7, we find explicit lower bounds for a certain approximation to $c(\alpha)$, while, in Section 8, we collect the ingredients from the previous sections and use them to prove Theorems 1.3 and 1.5. Corollaries 1.4 and 1.6 are proven in Section 9.

Those readers primarily interested in applications to Diophantine problems may wish to skip to Sections 10 and 11, within which we present the proofs of Corollary 1.7 and Theorem 1.11, respectively.

2. Padé approximants to $(1-z)^{1/2}$

To prove the results stated in the previous section, we will begin by constructing what is essentially the Padé table for $(1-z)^{1/2}$. Our argument will closely follow that of Beukers [10], though we will derive our Padé approximants via consideration of contour integrals, rather than as special cases of the hypergeometric function. These representations have the advantage of being especially easy to estimate by, say, the saddle-point method. Let us define

$$I_{n_1,n_2}(x) = \frac{1}{2\pi i} \int_\gamma \frac{(1-zx)^{n_2}(1-zx)^{1/2}}{z^{n_1+1}(1-z)^{n_2+1}}\, dz$$

where n_1 and n_2 are positive integers, γ is a closed, counter-clockwise contour enclosing $z=0$ and $z=1$, and $|x|<1$. Cauchy's theorem implies that

$$I_{n_1,n_2}(x) = P_{n_1,n_2}(x) - (1-x)^{1/2} Q_{n_1,n_2}(x) \tag{2.1}$$

where $P_{n_1,n_2}(x)$ and $Q_{n_1,n_2}(x)$ are polynomials with rational coefficients and degrees n_1 and n_2, respectively. In fact, calculating the relevant residues, we find that

$$P_{n_1,n_2}(x) = \sum_{k=0}^{n_1} \binom{n_2+1/2}{k}\binom{n_1+n_2-k}{n_2}(-x)^k \tag{2.2}$$

and

$$Q_{n_1,n_2}(x) = \sum_{k=0}^{n_2} \binom{n_2-1/2}{k}\binom{n_1+n_2-k}{n_2}(-x)^k. \tag{2.3}$$

While it is not difficult to show that $I_{n_1,n_2}(x)$ has a zero of multiplicity n_1+n_2+1 at $x=0$, we will not explictly use this fact. In the next three sections, we will derive archimedean estimates for $|I_{n_1,n_2}(x)|$ and $|P_{n_1,n_2}(x)|$, and discuss the p-adic valuations of the coefficients of the polynomials $P_{n_1,n_2}(x)$ and $Q_{n_1,n_2}(x)$. As is typical of this approach, this last problem is by far the most difficult. For analogous work on analytic and arithmetic properties of Padé approximants to $(1-z)^\nu$ where ν is rational, the reader is directed to the papers of Chudnovsky [16] and the second author [6–8]. In the situation where the approximants are far from diagonal (i.e. n_2/n_1 is large), it does not appear that full arithmetic information is available in the literature.

3. Bounding $|P_{n_1,n_2}(x)|$

In this section, we will obtain an upper bound for $|P_{n_1,n_2}(x)|$, under some minor restrictions. We use a straightforward application of the saddle-point method to prove

Lemma 3.1. *Suppose that x is a real number with $|x| \leq 1/2$ and n_1 and n_2 are positive integers such that there exists a real number $\alpha \geq 3/2$ with*

$$0 \leq \alpha n_1 - n_2 < 2(\alpha - 1). \tag{3.1}$$

It follows that

$$\left|P_{n_1,n_2}(x)\right| < 2(\alpha+1)\ F(r(\alpha,x),\alpha,x)^{n_1},$$

where $F(z,\alpha,x)$ *and* $r(\alpha,x)$ *are as defined in* (1.2) *and* (1.3).

Proof: First, note that if $0 < r < 1$, we may write

$$P_{n_1,n_2}(x) = \frac{1}{2\pi i}\int_\Gamma \frac{(1-zx)^{n_2}(1-zx)^{1/2}}{z^{n_1+1}(1-z)^{n_2+1}}\,dz$$

where Γ is defined by $|z| = r$, oriented positively. Writing $z = re^{i\theta}$, we have that

$$\left|P_{n_1,n_2}(x)\right| \le \frac{1}{2\pi}\int_0^{2\pi}\left|\frac{(1-zx)^{n_2}(1-zx)^{1/2}}{z^{n_1+1}(1-z)^{n_2+1}}\right| d\theta$$

and so

$$\left|P_{n_1,n_2}(x)\right| \le \frac{1}{r^{n_1+1}}\max_{0\le\theta\le 2\pi}\left|\frac{(1-re^{i\theta}x)^{n_2+1/2}}{(1-re^{i\theta})^{n_2+1}}\right|.$$

Since $|x| < 1$ and $0 < r < 1$, both $|1-re^{i\theta}|$ and $|\frac{1-re^{i\theta}}{1-re^{i\theta}x}|$ are increasing functions of θ on the interval $[0,\pi]$ (and hence minimal at $\theta = 0$), whereby

$$\left|P_{n_1,n_2}(x)\right| \le \frac{\sqrt{1-rx}}{r^{n_1+1}(1-r)}\left(\frac{1-rx}{1-r}\right)^{n_2}.$$

Let us now choose $r = r(\alpha,x)$, as defined in Section 1. We claim that $0 < r(\alpha,x) < 1$. In fact, by a routine application of the mean value theorem, we have

$$\frac{1}{1+\alpha} < r(\alpha,x) < \frac{1}{(1-x)(1+\alpha)}, \quad \text{if } 0 < x < 1,$$

and

$$\frac{1}{(1-x)(1+\alpha)} < r(\alpha,x) < \frac{1}{\alpha+1}, \quad \text{if } -1 < x < 0.$$

We may also show that

$$0.6\frac{\alpha+1}{e^{x-1}} < F(r(\alpha,x),\alpha,x) < \frac{\alpha+1}{e^{x-1}}, \tag{3.2}$$

where the minimal value for $\frac{e^{x-1}F(r(\alpha,x),\alpha,x)}{\alpha+1}$, with $|x| \le 1/2$ and $\alpha \ge 3/2$, is obtained for $x = -1/2$ and $\alpha = 3/2$. Further, it is an easy exercise in calculus to deduce the inequality

$$\frac{\sqrt{1-r(\alpha,x)x}}{r(\alpha,x)(1-r(\alpha,x))} < 2(\alpha+1)$$

for all x and α with $|x| \leq 1/2$ and $\alpha \geq 3/2$. Since $n_2 \leq \alpha n_1$, we reach the desired conclusion. □

4. Bounding $|I_{n_1,n_2}(x)|$

To bound $|I_{n_1,n_2}(x)|$, as in the analogous situation in [6], we cannot directly apply the saddle-point method, since the second root of $F(z, \alpha, x)$ corresponds to a point on a branch cut of $(1 - zx)^{1/2}$. We may nonetheless prove the following

Lemma 4.1. *Suppose that x is a real number with $|x| \leq 1/2$ and n_1 and n_2 are positive integers. If there exists a real number α satisfying $\alpha \geq 3/2$ and Eq.* (3.1), *it follows that*

$$\left|I_{n_1,n_2}(x)\right| < (\alpha+1)^2|x|^{3-2\alpha}\left(|x|^{-(\alpha+1)}\, F(r(\alpha, x), \alpha, x)\right)^{-n_1},$$

where $F(z, \alpha, x)$ and $r(\alpha, x)$ are as defined in (1.2) *and* (1.3).

Proof: Let us assume that $x \in \mathbb{R}$ with $|x| \leq 1/2$. Following the arguments of [6], we make the change of variables $1 - zx \to -w$ in the contour integral representation for $I_{n_1,n_2}(x)$ to find that

$$I_{n_1,n_2}(x) = \frac{-x^{n_1+n_2+1}}{2\pi} \int_{\gamma'} \frac{w^{n_2} w^{1/2}}{(1+w)^{n_1+1}(1+w-x)^{n_2+1}}\, dw \tag{4.1}$$

where $\gamma' = \gamma_1 + \gamma_2 + \gamma_3 + \gamma_4$ is a contour containing the poles of the integrand of (4.1) while avoiding a branch cut along the nonnegative real axis (see Fig. 1).

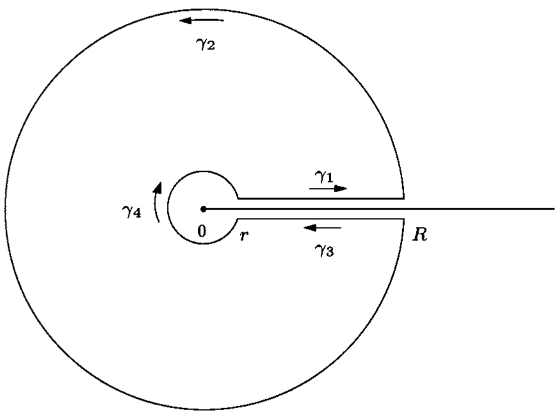


Figure 1. The contour γ'.

Since

$$\left|\int_{\gamma_l} \frac{w^{n_2} w^{1/2} dw}{(1+w)^{n_1+1}(1+w-x)^{n_2+1}}\right| \le \int_0^{2\pi} \left|\frac{w^{n_2} w^{1/2}}{(1+w)^{n_1+1}(1+w-x)^{n_2+1}}\right| d\theta,$$

for $l = 2$ or 4, (where $w = Re^{i\theta}$ or $re^{i\theta}$ respectively) we have that the contribution to (4.1) associated with the arcs γ_2 and γ_4 becomes negligible as $r \to 0$ and $R \to \infty$. Therefore, from

$$\frac{w^{n_2} w^{1/2}}{(1+w)^{n_1+1}(1+w-x)^{n_2+1}} = \begin{cases} \dfrac{u^{n_2+1/2}}{(1+u)^{n_1+1}(1+u-x)^{n_2+1}} & \text{on } \gamma_1 \\ \dfrac{-u^{n_2+1/2}}{(1+u)^{n_1+1}(1+u-x)^{n_2+1}} & \text{on } \gamma_3, \end{cases}$$

we may conclude, letting $r \to 0$ and $R \to \infty$, that

$$\left|I_{n_1,n_2}(x)\right| = \frac{|x|^{n_1+n_2+1}}{\pi} \int_0^\infty \frac{u^{n_2+1/2}\, du}{(1+u)^{n_1+1}(1+u-x)^{n_2+1}}.$$

To estimate this, we make the change of variables $u \to \frac{v}{1-v}$, so that

$$\left|I_{n_1,n_2}(x)\right| = \frac{|x|^{n_1+n_2+1}}{\pi} \int_0^1 \frac{v^{n_2+1/2}(1-v)^{n_1-1/2}\, dv}{(1-(1-v)x)^{n_2+1}}. \tag{4.2}$$

Suppose first that $n_1 = 1$. Then, from (4.2), we have

$$\left|I_{1,n_2}(x)\right| < \frac{|x|^{n_2+2}}{\pi} \max_{v\in(0,1)}\left(\frac{v^{1/2}(1-v)^{1/2}}{1-(1-v)x}\right)\left(\max_{v\in(0,1)}\left(\frac{v}{1-(1-v)x}\right)\right)^{n_2}.$$

The function

$$\frac{v^{1/2}(1-v)^{1/2}}{1-(1-v)x}$$

is maximal on (0, 1) for $v = \frac{1-x}{2-x}$ and substituting this value for v yields a function of x, increasing on $[-1/2, 1/2]$, whereby

$$\max_{v\in(0,1)}\left(\frac{v^{1/2}(1-v)^{1/2}}{1-(1-v)x}\right) \le \frac{1}{\sqrt{2}}.$$

Since $\frac{v}{1-(1-v)x}$ is monotone increasing in v, on the interval (0, 1), we thus have that

$$\left|I_{1,n_2}(x)\right| < \frac{1}{\sqrt{2}\pi}|x|^{n_2+2}. \tag{4.3}$$

Next suppose that $n_1 \geq 2$. If we write

$$\tau = \frac{\alpha n_1 - n_2}{2(\alpha - 1)},$$

so that, from (3.1), $0 \leq \tau < 1$, and set

$$\beta = (2 - 2\tau)\,\alpha + 2\tau + 1/2,$$

then the integrand in (4.2) becomes

$$\frac{v^{\beta}(1-v)^{3/2}}{(1-(1-v)x)^{\beta+1/2}} \left(\frac{v^{\alpha}(1-v)}{(1-(1-v)x)^{\alpha}} \right)^{n_1-2}.$$

Since $x \leq 1/2$, we have that

$$\frac{v^{\beta}(1-v)^{3/2}}{(1-(1-v)x)^{\beta+1/2}} \leq \frac{v^{\beta}(1-v)^{3/2}}{\left(\frac{1}{2}(1+v)\right)^{\beta+1/2}}.$$

By calculus, the latter quantity is maximal on (0, 1) for

$$v = \frac{1}{2}(\sqrt{\beta^2 + 8\beta + 4} - (\beta + 2)).$$

Substituting this value for v in

$$\frac{v^{\beta}(1-v)^{3/2}}{\left(\frac{1}{2}(1+v)\right)^{\beta+1/2}},$$

and noting that the resulting expression is a decreasing function of β for

$$5/2 \leq \beta \leq 2\alpha + 1/2,$$

it follows that

$$\frac{v^{\beta}(1-v)^{3/2}}{(1-(1-v)x)^{\beta+1/2}} \leq \frac{4}{27}.$$

We conclude, then, if $n_1 \geq 2$, that

$$\left|I_{n_1,n_2}(x)\right| < \frac{4}{27\pi}|x|^{n_1+n_2+1} \int_0^1 F(z,\alpha,x)^{2-n_1}\,dz,$$

where $F(z, \alpha, x)$ is as in (1.2). We therefore have

$$\left|I_{n_1,n_2}(x)\right| < \frac{4}{27\pi}|x|^{n_1+n_2+1} F(r(\alpha,x),\alpha,x)^{2-n_1},$$

whereby, by (3.1) and (3.2),

$$\left|I_{n_1,n_2}(x)\right| < \frac{4}{27\pi}|x|^{3-2\alpha}(\alpha+1)^2 e^{2(1-x)} \left(|x|^{-(1+\alpha)} F(r(\alpha,x),\alpha,x)\right)^{-n_1}.$$

From $|x| \leq 1/2$, it follows that

$$\left|I_{n_1,n_2}(x)\right| < (\alpha+1)^2 |x|^{3-2\alpha} \left(|x|^{-(1+\alpha)} F(r(\alpha,x),\alpha,x)\right)^{-n_1},$$

provided $n_1 \geq 2$. From (3.2), (4.3) and $\alpha \geq 3/2$, the above inequality also holds if $n_1 = 1$, completing the proof of our lemma. □

5. Arithmetic properties of our coefficients

In this section, we will study common factors of the numerators of the (rational) coefficients of $P_{n_1,n_2}(x)$ and $Q_{n_1,n_2}(x)$. With this in mind, let us define

$$\Pi(n_1, n_2) = \gcd\{\Pi_1(n_1, n_2), \Pi_2(n_1, n_2)\},$$

where $\Pi_1(n_1, n_2)$ denotes the greatest common divisor of the numerators of the coefficients of $P_{n_1,n_2}(x)$ and $\Pi_2(n_1, n_2)$ is the greatest common divisor of the numerators of the coefficients of $Q_{n_1,n_2}(x)$. Our aim will be to show that $\log \Pi(n_1, n_2)$ grows exponentially in n_1, where the exact order of growth depends on the ratio n_2/n_1. We will derive both asymptotic results and also explicit lower bounds for $\Pi(n_1, n_2)$. The latter will find greater application to specific Diophantine problems. We have

Proposition 5.1. *Suppose that $\alpha > 1$ is a given real number and that n_1 and n_2 are positive integers such that*

$$0 \leq \alpha n_1 - n_2 < 2(\alpha - 1).$$

Then

$$\lim_{n_1 \to \infty} \frac{1}{n_1} \log \Pi(n_1, n_2) = \log c(\alpha),$$

where $c(\alpha)$ is as defined in (1.7).

Also

Proposition 5.2. *If $\alpha > 1$ is real and n_1 and n_2 are positive integers such that*

$$0 \leq \alpha n_1 - n_2 < 2(\alpha - 1),$$

then

$$\Pi(n_1, n_2) \geq d_1(\alpha) c_1(\alpha)^{n_1},$$

where we may take either $c_1(\alpha) = d_1(\alpha) = 1$, or, for the values of α represented in Table (1.17), *$c_1(\alpha)$ and $d_1(\alpha)$ as given in that table.*

Throughout, we will denote by $[x]$ the greatest integer not exceeding a real number x and set $\{x\} = x - [x]$ (so that $0 \leq \{x\} < 1$). Here as before, if a is an integer, we define $\mathrm{ord}_p(a)$ to be the highest power of a prime p which divides a and, if $r = a/b$ is rational, we take $\mathrm{ord}_p(a/b) = \mathrm{ord}_p(a) - \mathrm{ord}_p(b)$. The following lemma provides a useful description of the "large" primes that divide $\Pi(n_1, n_2)$:

Lemma 5.3. *Suppose that p is an odd prime, not dividing n_1n_2, with $p^2 > 2n_2 + 2$ and*

$$\left\{\frac{n_i - 1}{p}\right\} > \frac{1}{2} \quad \textit{for } i = 1 \textit{ and } 2.$$

Then

$$ord_p \binom{n_2 + 1/2}{k}\binom{n_1 + n_2 - k}{n_2} \geq 1 \quad \textit{for } 0 \leq k \leq n_1$$

and

$$ord_p \binom{n_1 - 1/2}{k}\binom{n_1 + n_2 - k}{n_1} \geq 1 \quad \textit{for } 0 \leq k \leq n_2.$$

Proof: We begin by noting that

$$\left\{\frac{n_i - 1}{p}\right\} > \frac{1}{2}$$

p odd, and p relatively prime to n_1n_2 implies that

$$\left\{\frac{n_i}{p}\right\} \geq \frac{p+3}{2p}. \tag{5.1}$$

If $k = 0$, then

$$\binom{n_2 + 1/2}{k}\binom{n_1 + n_2 - k}{n_2} = \binom{n_1 - 1/2}{k}\binom{n_1 + n_2 - k}{n_1} = \binom{n_1 + n_2}{n_1}$$

and, since $n_1 < n_2$, if $p^2 > 2n_2$, we have

$$\text{ord}_p \binom{n_1 + n_2}{n_1} = \left\{\frac{n_1}{p}\right\} + \left\{\frac{n_2}{p}\right\} - \left\{\frac{n_1 + n_2}{p}\right\}.$$

It follows that $\text{ord}_p\binom{n_1+n_2}{n_1} \geq 1$ if and only if $\{\frac{n_1}{p}\} + \{\frac{n_2}{p}\} \geq 1$. The result therefore follows from (5.1). Similarly, if $k = 1$, then

$$\text{ord}_p \binom{n_2 + 1/2}{k}\binom{n_1 + n_2 - k}{n_2} \geq 1$$

follows from

$$\left\{\frac{n_1 - 1}{p}\right\} + \left\{\frac{n_2}{p}\right\} \geq 1$$

while

$$\operatorname{ord}_p \binom{n_1 - 1/2}{k} \binom{n_1 + n_2 - k}{n_1} \geq 1$$

is a consequence of

$$\left\{ \frac{n_1}{p} \right\} + \left\{ \frac{n_2 - 1}{p} \right\} \geq 1.$$

Let us next suppose that $k \geq 2$. From Lemma 4.5 of Chudnovsky [16], if $n \in \mathbb{N}$ and $p^2 > 2n + 2$, we have

$$\operatorname{ord}_p \binom{n + 1/2}{k} = \left[\frac{n + 1 - q}{p} \right] - \left[\frac{n + 1 - q - k}{p} \right] - \left[\frac{k}{p} \right]$$

where $q = (p - 1)/2$. It follows that

$$\operatorname{ord}_p \binom{n_2 + 1/2}{k} = \left\{ \frac{n_2 + 1 - q - k}{p} \right\} + \left\{ \frac{k}{p} \right\} - \left\{ \frac{n_2 + 1 - q}{p} \right\} \tag{5.2}$$

and

$$\operatorname{ord}_p \binom{n_1 + n_2 - k}{n_2} = \left\{ \frac{n_2}{p} \right\} + \left\{ \frac{n_1 - k}{p} \right\} - \left\{ \frac{n_1 + n_2 - k}{p} \right\}. \tag{5.3}$$

Suppose now that $\operatorname{ord}_p \binom{n_2 + 1/2}{k} \binom{n_1 + n_2 - k}{n_2} = 0$. From (5.2), we have

$$\left\{ \frac{n_2 + 1 - q}{p} \right\} \geq \left\{ \frac{k}{p} \right\}.$$

This, with (5.1), implies that

$$\left\{ \frac{n_2 + 1 - q}{p} \right\} = \left\{ \frac{n_2}{p} \right\} - \frac{p - 3}{2p} \geq \left\{ \frac{k}{p} \right\}. \tag{5.4}$$

On the other hand, $\operatorname{ord}_p \binom{n_1 + n_2 - k}{n_2} = 0$ together with (5.3) yields

$$\left\{ \frac{n_2}{p} \right\} + \left\{ \frac{n_1 - k}{p} \right\} < 1. \tag{5.5}$$

If

$$\left\{ \frac{n_1 - k}{p} \right\} = \left\{ \frac{n_1}{p} \right\} - \left\{ \frac{k}{p} \right\} + 1,$$

then

$$\left\{ \frac{n_1}{p} \right\} + \left\{ \frac{n_2}{p} \right\} < \left\{ \frac{k}{p} \right\},$$

contradicting (5.1). It therefore follows from (5.4) and (5.5) that

$$\left\{\frac{n_1}{p}\right\} + \left\{\frac{n_2}{p}\right\} < 1 + \left\{\frac{k}{p}\right\} \leq 1 + \left\{\frac{n_2}{p}\right\} - \frac{p-3}{2p},$$

whence

$$\left\{\frac{n_1}{p}\right\} < \frac{p+3}{2p},$$

contradicting (5.1). Similarly,

$$\operatorname{ord}_p\binom{n_1-1/2}{k} = \left\{\frac{n_1-q-k}{p}\right\} + \left\{\frac{k}{p}\right\} - \left\{\frac{n_1-q}{p}\right\} \tag{5.6}$$

and

$$\operatorname{ord}_p\binom{n_1+n_2-k}{n_1} = \left\{\frac{n_1}{p}\right\} + \left\{\frac{n_2-k}{p}\right\} - \left\{\frac{n_1+n_2-k}{p}\right\} \tag{5.7}$$

and so $\operatorname{ord}_p\binom{n_1-1/2}{k}\binom{n_1+n_2-k}{n_1} = 0$, (5.6) and (5.7) imply that

$$\left\{\frac{n_1-q}{p}\right\} = \left\{\frac{n_1}{p}\right\} - \frac{p-1}{2p} \geq \left\{\frac{k}{p}\right\}$$

and

$$\left\{\frac{n_1}{p}\right\} + \left\{\frac{n_2-k}{p}\right\} = \left\{\frac{n_1}{p}\right\} + \left\{\frac{n_2}{p}\right\} - \left\{\frac{k}{p}\right\} < 1.$$

Combining these, we find that

$$\left\{\frac{n_2}{p}\right\} < \frac{p+1}{2p},$$

again contradicting (5.1). This completes the proof of Lemma 5.3. □

We will apply this lemma to approximate $\Pi(n_1, n_2)$; indeed, as the contribution of "small" primes to $\Pi(n_1, n_2)$ is, in some sense, negligible, it is the key result in the proofs of Propositions 5.1 and 5.2. Note that if we define $S(n_1, n_2)$ to be the set of rational primes p satisfying $p^2 > 2n_2 + 2$, $\gcd(p, n_1 n_2) = 1$,

$$\left\{\frac{n_1-1}{p}\right\} > \frac{1}{2} \quad \text{and} \quad \left\{\frac{n_2-1}{p}\right\} > \frac{1}{2},$$

then Lemma 5.3 immediately yields the inequality

$$\Pi(n_1, n_2) \geq \prod_{p \in S(n_1, n_2)} p. \tag{5.8}$$

6. Asymptotics for $\Pi(n_1, n_2)$

In this section, we will prove Proposition 5.1. Let α be a positive real number and define

$$\Upsilon_\alpha(n) = \frac{1}{n}\sum_p \log p,$$

where the sum is over primes p satisfying

$$\left\{\frac{n}{p}\right\} > \frac{1}{2}, \quad \left\{\frac{\alpha n}{p}\right\} > \frac{1}{2} \quad \text{and} \quad p^2 > 2\alpha n + 2.$$

We note that $\exp(\Upsilon_\alpha(n))$ is approximately equal to $\Pi(n, [\alpha n])$, an observation which we will make more precise later. It is relatively easy to describe the asymptotic behavior of $\Upsilon_\alpha(n)$. We have

Lemma 6.1. *Let $\alpha > 1$ be a real number. If $c(\alpha)$ is as defined in* (1.7), *then*

$$\lim_{n\to\infty} \Upsilon_\alpha(n) = \log c(\alpha).$$

Proof: Let $\alpha > 1$ be a real number, n a positive integer and p a rational prime such that

$$\left\{\frac{n}{p}\right\} > \frac{1}{2} \quad \text{and} \quad \left\{\frac{\alpha n}{p}\right\} > \frac{1}{2}.$$

It is readily seen that these two conditions hold simultaneously, precisely when

$$p \in \left(\frac{n}{i}, \frac{2n}{2i-1}\right) \cap \left(\frac{\alpha n}{j}, \frac{2\alpha n}{2j-1}\right), \tag{6.1}$$

for some positive integers i and j. To determine how these intervals intersect, we consider three cases, depending on whether

$$\left(\frac{n}{i}, \frac{2n}{2i-1}\right) \cap \left(\frac{\alpha n}{j}, \frac{2\alpha n}{2j-1}\right) = \left(\frac{\alpha n}{j}, \frac{2\alpha n}{2j-1}\right), \tag{6.2}$$

$$\left(\frac{n}{i}, \frac{2n}{2i-1}\right) \cap \left(\frac{\alpha n}{j}, \frac{2\alpha n}{2j-1}\right) = \left(\frac{n}{i}, \frac{2\alpha n}{2j-1}\right) \tag{6.3}$$

or

$$\left(\frac{n}{i}, \frac{2n}{2i-1}\right) \cap \left(\frac{\alpha n}{j}, \frac{2\alpha n}{2j-1}\right) = \left(\frac{\alpha n}{j}, \frac{2n}{2i-1}\right). \tag{6.4}$$

We note, since $\alpha > 1$, that we can never have an interval of the form $(\frac{n}{i}, \frac{2n}{2i-1})$ contained within $(\frac{\alpha n}{j}, \frac{2\alpha n}{2j-1})$. In case (6.2), we find that

$$\frac{n}{i} \le \frac{\alpha n}{j} \quad \text{and} \quad \frac{2n}{2i-1} \ge \frac{2\alpha n}{2j-1},$$

whereby, fixing i, it follows that

$$j \in \left[i\alpha - \frac{\alpha - 1}{2}, i\alpha \right]. \tag{6.5}$$

Similarly, if we have (6.3), but not (6.2), then

$$j \in \left(i\alpha, i\alpha + \frac{1}{2} \right), \tag{6.6}$$

while (6.4) without (6.2) implies

$$j \in \left(i\alpha - \frac{\alpha}{2}, i\alpha - \frac{\alpha - 1}{2} \right). \tag{6.7}$$

Let $S_1 = \sum_p \log p$, where the summation is over primes p satisfying (6.1) and $p^2 > 2\alpha n + 2$, with i and j ranging over positive integers constrained by (6.5). In order to obtain a lower bound for S_1, we note, from (6.1), that

$$i < \frac{n}{\sqrt{2\alpha n + 2}} \Rightarrow j < \frac{\alpha n}{\sqrt{2\alpha n + 2}} \Rightarrow p^2 > 2\alpha n + 2,$$

and hence

$$S_1 \geq \sum_{i < \frac{n}{\sqrt{2\alpha n + 2}}} \sum_{i\alpha - \frac{\alpha - 1}{2} \leq j \leq i\alpha} \left(\theta\left(\frac{2\alpha n}{2j - 1} \right) - \theta\left(\frac{\alpha n}{j} \right) - \log\left(\frac{2\alpha n}{2j - 1} \right) \right),$$

where

$$\theta(x) = \sum_{p \leq x} \log p,$$

with the summation taken over primes. Here, the term $\log(\frac{2\alpha n}{2j-1})$ is included to account for the possibility that $\frac{2\alpha n}{2j-1}$ is prime. Using the asymptotic formula

$$\theta(x) = x + O\left(x e^{-c(\log x)^{1/2}}\right),$$

for some positive constant c, as $x \to \infty$ (see e.g. [40]), it is straightforward to show that

$$S_1 \geq n \sum_{i < \frac{n}{\sqrt{2\alpha n + 2}}} \sum_{\substack{j \in \\ [i\alpha - \frac{\alpha - 1}{2}, i\alpha]}} \left(\frac{2\alpha}{2j - 1} - \frac{\alpha}{j} \right) + R_1(n),$$

for $c' > 0$ and

$$R_1(n) = O\left(\frac{n(\log n)^{1/2}}{\exp(c'(\log n)^{1/2})} \right),$$

where the implicit constant depends only on α. Note that the terms of the form $\log(\frac{2\alpha n}{2j-1})$ contribute, in total, at most $O(\sqrt{n} \log n)$. To derive an upper bound for S_1, we note that

$$p^2 > 2\alpha n + 2 \Rightarrow j < \frac{\alpha n}{\sqrt{2\alpha n+2}} + \frac{1}{2} \Rightarrow i < \frac{n}{\sqrt{2\alpha n+2}} + \frac{1}{2},$$

which implies the inequality

$$S_1 \leq \sum_{i<\frac{n}{\sqrt{2\alpha n+2}}+\frac{1}{2}} \sum_{i\alpha-\frac{\alpha-1}{2}\leq j\leq i\alpha} \left(\theta\left(\frac{2\alpha n}{2j-1}\right) - \theta\left(\frac{\alpha n}{j}\right)\right).$$

Arguing as before, we obtain an upper bound of the form

$$S_1 \leq n \sum_{i<\frac{n}{\sqrt{2\alpha n+2}}+\frac{1}{2}} \sum_{i\alpha-\frac{\alpha-1}{2}\leq j\leq i\alpha} \left(\frac{2\alpha}{2j-1} - \frac{\alpha}{j}\right) + R_2(n),$$

where

$$R_2(n) = O\left(\frac{n(\log n)^{1/2}}{\exp(c'(\log n)^{1/2})}\right).$$

Letting n tend to infinity, we see that

$$\lim_{n\to\infty} \frac{1}{n} S_1 = S_1(\alpha),$$

for $S_1(\alpha)$ as in (1.4). Now, defining in an analogous fashion $S_2 = \sum_p \log p$ and $S_3 = \sum_p \log p$, where the primes in question satisfy (6.1) and $p^2 > 2\alpha n + 2$, with i and j as in (6.6) or (6.7), respectively, we find that

$$\lim_{n\to\infty} \frac{1}{n} S_2 = S_2(\alpha)$$

and

$$\lim_{n\to\infty} \frac{1}{n} S_3 = S_3(\alpha).$$

Here, $S_2(\alpha)$ and $S_3(\alpha)$ are as in (1.5) and (1.6). Since

$$\Upsilon_\alpha(n) = \frac{S_1 + S_2 + S_3}{n},$$

this completes the proof of the lemma. □

While definition (1.7) makes it possible to obtain numerical approximations to $c(\alpha)$ of arbitrary precision, in case α is rational, however, we may derive a different formula which is more suitable for computations. This takes the form of a summation over terms involving $\psi(x)$, the derivative of the logarithm of the gamma function $\Gamma(x)$. In the following, we let $\lfloor x \rfloor$ denote the greatest integer $\leq x$ and $\lceil x \rceil$ the least integer $\geq x$.

Lemma 6.2. *Let $\alpha = b/a$ where a and b are positive, coprime integers, with $b > a$ (so that $\alpha > 1$). If we define*

$$R_{1,i}(\alpha) = \sum_{j=\lfloor(2i-1)b/a\rfloor+1}^{\lceil 2ib/a\rceil-1} (-1)^j \psi\left(\frac{j}{2b}\right),$$

$$R_{2,i}(\alpha) = \begin{cases} -\psi\left(\dfrac{2i-1}{2a}\right) & \text{if } \lfloor(2i-1)b/a\rfloor \text{ is odd} \\ 0 & \text{otherwise} \end{cases}$$

and

$$R_{3,i}(\alpha) = \begin{cases} \psi\left(\dfrac{i}{a}\right) & \text{if } \lfloor 2ib/a\rfloor \text{ is even} \\ 0 & \text{otherwise,} \end{cases}$$

then

$$\log c(\alpha) = \frac{1}{a}\sum_{i=1}^{a}(R_{1,i}(\alpha) + R_{2,i}(\alpha) + R_{3,i}(\alpha)).$$

Proof: As mentioned in the previous proof, it is possible to express $\log c(\alpha)$ as the measure of the set

$$\left(\bigcup_{i=1}^{\infty}\left(\frac{1}{i}, \frac{2}{2i-1}\right)\right) \bigcap \left(\bigcup_{j=1}^{\infty}\left(\frac{\alpha}{j}, \frac{2\alpha}{2j-1}\right)\right).$$

Consequently, $a\log c(\alpha)$ is equal to the sum of the lengths of the intervals in

$$I = \left(\bigcup_{i=1}^{\infty}\left(\frac{a}{i}, \frac{2a}{2i-1}\right)\right) \bigcap \left(\bigcup_{j=1}^{\infty}\left(\frac{b}{j}, \frac{2b}{2j-1}\right)\right).$$

As in the proof of Lemma 6.1, there are three distinct possibilities for the intervals that are contained in this set, corresponding to the existence of positive integers i and j with

$$j \in \left(\frac{b}{a}(i-1/2) + 1/2, \frac{bi}{a}\right),$$

$$j \in \left(\frac{b}{a}(i-1/2), \frac{b}{a}(i-1/2) + 1/2\right)$$

or

$$j \in \left[\frac{b}{a}i, \frac{b}{a}i + 1/2\right),$$

respectively. Here, for convenience, we have partitioned the values of j slightly differently than in (6.5), (6.6) and (6.7). We thus have

$$I = \bigcup_{i=1}^{\infty}(I_{1,i} \cup I_{2,i} \cup I_{3,i}),$$

where we define

$$I_{1,i} = \bigcup_{j\in(\frac{b}{a}(i-1/2)+1/2,\frac{bi}{a})} \left(\frac{b}{j}, \frac{2b}{2j-1}\right),$$
$$I_{2,i} = \bigcup_{j\in(\frac{b}{a}(i-1/2),\frac{b}{a}(i-1/2)+1/2]} \left(\frac{b}{j}, \frac{2a}{2i-1}\right)$$

and

$$I_{3,i} = \bigcup_{j\in[\frac{b}{a}i,\frac{b}{a}i+1/2)} \left(\frac{a}{i}, \frac{2b}{2j-1}\right).$$

Note that $I_{2,i}$ and $I_{3,i}$ each contain at most a single interval. Fixing $i \in [1, a]$, if

$$j \in \left(\frac{b}{a}(i-1/2)+1/2, \frac{bi}{a}\right),$$

then, similarly,

$$j + bk \in \left(\frac{b}{a}(i+ak-1/2)+1/2, \frac{b(i+ak)}{a}\right)$$

for every integer k. This reduces the problem of characterizing the sets $I_{1,i}$ to a matter of determining them for each residue class modulo a. We may therefore write

$$I = \bigcup_{i=1}^{a} (J_{1,i} \cup J_{2,i} \cup J_{3,i}),$$

where

$$J_{1,i} = \bigcup_{j\in(\frac{b}{a}(i-1/2)+1/2,\frac{bi}{a})} \bigcup_{k=0}^{\infty} \left(\frac{b}{j+bk}, \frac{2b}{2j+2bk-1}\right),$$
$$J_{2,i} = \bigcup_{j\in(\frac{b}{a}(i-1/2),\frac{b}{a}(i-1/2)+1/2]} \bigcup_{k=0}^{\infty} \left(\frac{b}{j}, \frac{2a}{2i-1}\right)$$

and

$$J_{3,i} = \bigcup_{j\in[\frac{b}{a}i,\frac{b}{a}i+1/2)} \bigcup_{k=0}^{\infty} \left(\frac{a}{i}, \frac{2b}{2j-1}\right),$$

in all cases for $1 \le i \le a$. Since these are disjoint sets, we may compute their measures independently:

$$|J_{1,i}| = \sum_{j\in(\frac{b}{a}(i-1/2)+1/2,\frac{bi}{a})} \sum_{k=0}^{\infty} \left(\frac{2b}{2j+2bk-1} - \frac{b}{j+bk}\right),$$
$$|J_{2,i}| = \sum_{j\in(\frac{b}{a}(i-1/2),\frac{b}{a}(i-1/2)+1/2]} \sum_{k=0}^{\infty} \left(\frac{2a}{2i+2ak-1} - \frac{b}{j+bk}\right)$$

and

$$|J_{3,i}| = \sum_{j \in [\frac{b}{a}i, \frac{b}{a}i+1/2)} \sum_{k=0}^{\infty} \left(\frac{2b}{2j+2bk-1} - \frac{a}{i+ak} \right).$$

From the following well known formula for $\psi(x)$, valid for $x > 0$,

$$\psi(x) = -\gamma - \frac{1}{x} + \sum_{i=1}^{\infty} \left(\frac{1}{i} - \frac{1}{i+x} \right),$$

we have

$$\psi\left(\frac{j}{b}\right) - \psi\left(\frac{2j-1}{2b}\right) = \sum_{k=0}^{\infty} \left(\frac{2b}{2j+2bk-1} - \frac{b}{j+bk} \right),$$

which is precisely the inner sum appearing in $|J_{1,i}|$. Applying the same argument to the summations in $|J_{2,i}|$ and $|J_{3,i}|$, we find that

$$|J_{1,i}| = \sum_{j \in (\frac{b}{a}(i-1/2)+1/2, \frac{bi}{a})} \left(\psi\left(\frac{j}{b}\right) - \psi\left(\frac{2j-1}{2b}\right) \right),$$

$$|J_{2,i}| = \sum_{j \in (\frac{b}{a}(i-1/2), \frac{b}{a}(i-1/2)+1/2]} \left(\psi\left(\frac{j}{b}\right) - \psi\left(\frac{2i-1}{2a}\right) \right)$$

and

$$|J_{3,i}| = \sum_{j \in [\frac{b}{a}i, \frac{b}{a}i+1/2)} \left(\psi\left(\frac{i}{a}\right) - \psi\left(\frac{2j-1}{2b}\right) \right).$$

We next note that $|J_{2,i}|$ is not the empty sum exactly when there exists an integer in the interval $(\frac{b}{a}(i-1/2), \frac{b}{a}(i-1/2)+1/2]$, or, equivalently, if there is an even integer in the interval $(\frac{b}{a}(2i-1), \frac{b}{a}(2i-1)+1]$. This is possible if and only if $\lfloor \frac{b}{a}(2i-1) \rfloor$ is odd. A similar argument shows that $|J_{3,i}|$ is not the empty sum if and only if $\lfloor 2i\frac{b}{a} \rfloor$ is even. The term $\psi(\frac{j}{b})$ occurs in one of the three sums precisely when $j \in (\frac{b}{a}(i-1/2), \frac{b}{a}i)$ which implies $2j \in (\frac{b}{a}(2i-1), \frac{b}{a}2i)$. Finally, the term $\psi(\frac{2j-1}{2b})$ occurs in one of the three sums just when $j \in (\frac{b}{a}(i-1/2)+1/2, \frac{b}{a}i+1/2)$, i.e. when $2j-1 \in (\frac{b}{a}(2i-1), \frac{b}{a}2i)$. Using these facts, we may manipulate the above summations to find that

$$|J_{1,i}| + |J_{2,i}| + |J_{3,i}| = R_{1,i}(\alpha) + R_{2,i}(\alpha) + R_{3,i}(\alpha),$$

which completes the proof. □

In the event α is a rational with small denominator, the preceding lemma takes a particularly simple form. By way of example, if α is an integer, say $\alpha = n \geq 2$, we have

$$R_{1,1}(n) = \sum_{j=n+1}^{2n-1} (-1)^j \psi\left(\frac{j}{2n}\right), \quad R_{2,1}(n) = \begin{cases} -\psi\left(\frac{1}{2}\right) & \text{if } n \text{ is odd} \\ 0 & \text{otherwise} \end{cases}$$

and $R_{3,1}(n) = \psi(1)$, whence a simple manipulation yields

$$\log c(n) = \sum_{j=\lceil\frac{n+1}{2}\rceil}^{n} \left(\psi\left(\frac{j}{n}\right) - \psi\left(\frac{2j-1}{2n}\right)\right). \tag{6.8}$$

Similarly, if $a = 2$ (and, say, $b = 2n + 1$), we may derive

$$2\,\log c\left(\frac{2n+1}{2}\right) = \sum_{j=n+1}^{2n} (-1)^j \psi\left(\frac{j}{4n+2}\right) + \sum_{j=3n+2}^{4n+2} (-1)^j \psi\left(\frac{j}{4n+2}\right) - \delta(n),$$

where

$$\delta(n) = \begin{cases} \psi\left(\frac{3}{4}\right) & \text{if } n \text{ is even} \\ \psi\left(\frac{1}{4}\right) & \text{if } n \text{ is odd.} \end{cases}$$

We are now in a position to complete the proof of Proposition 5.1. Let $\alpha > 1$ be real and define $\Gamma(\alpha)$ to be the set of all $(n_1, n_2) \in \mathbb{N}^2$, such that

$$0 \le \alpha n_1 - n_2 < 2(\alpha - 1). \tag{6.9}$$

Lemma 6.3. *Let $\alpha \in \mathbb{Q}$ with $\alpha > 1$. Define*

$$\Pi(\alpha) = \lim_{\substack{n_1\to\infty \\ (n_1,n_2)\in\Gamma(\alpha)}} \frac{1}{n_1} \sum_{p\in S(n_1,n_2)} \log p,$$

where $S(n_1, n_2)$ is as defined previously. Then

$$\Pi(\alpha) = \log c(\alpha).$$

Proof: We begin by fixing $\alpha > 1$ real, choosing $(n_1, n_2) \in \Gamma(\alpha)$ and setting $\alpha' = \frac{n_2-1}{n_1-1}$ (so that, from (6.9), we have $|\alpha - \alpha'| \le \frac{\alpha-1}{n_1-1}$). For a given $p \in S(n_1, n_2)$, we know that p lies in the intersection of intervals of the form

$$\left(\frac{n_1-1}{i}, \frac{2(n_1-1)}{2i-1}\right) \quad \text{and} \quad \left(\frac{n_2-1}{j}, \frac{2(n_2-1)}{2j-1}\right),$$

for an appropriate choice of i and j. Similarly, the primes involved in the sum related to $\Upsilon_\alpha(n_1-1)$ lie in the intersection of intervals of the shape

$$\left(\frac{n_1-1}{i}, \frac{2(n_1-1)}{2i-1}\right) \quad \text{and} \quad \left(\frac{\alpha(n_1-1)}{j}, \frac{2\alpha(n_1-1)}{2j-1}\right),$$

again, with appropriate choices for i and j. We observe that any difference between the primes involved in the two sums must correspond to the difference in the right hand intervals, in addition to those primes which divide n_1 and n_2. It follows that we have

$$\left|(n_1-1)\Upsilon_{\alpha'}(n_1-1) - \sum_{p\in S(n_1,n_2)} \log p\right| \leq \Sigma_1 + \Sigma_2 + \log(n_1 n_2),$$

where

$$\Sigma_1 = \sum_{j<\sqrt{2\alpha n_1+2}} \left|\theta\left(\frac{\alpha(n_1-1)}{j}\right) - \theta\left(\frac{n_2-1}{j}\right)\right|$$

and

$$\Sigma_2 = \sum_{j<\sqrt{2\alpha n_1+2}} \left|\theta\left(\frac{2\alpha(n_1-1)}{2j-1}\right) - \theta\left(\frac{2(n_2-1)}{2j-1}\right)\right|.$$

From the Prime Number Theorem, there exists a positive constant c for which

$$\Sigma_1 \leq \sum_{j<\sqrt{2\alpha+2}} |\alpha-\alpha'|\frac{n_1-1}{j} + O\left(\frac{n_1-1}{j}\exp\left(-c\left(\log\frac{\alpha(n_1-1)}{j}\right)^{1/2}\right)\right).$$

Since we have $|\alpha-\alpha'| \leq \frac{\alpha-1}{n_1-1}$, this is majorized by

$$\left(\sum_{j<\sqrt{2\alpha n_1+2}} \frac{\alpha}{j}\right) + o(n_1)$$

and hence is itself $o(n_1)$. Arguing similarly for Σ_2, we conclude that

$$\left|(n_1-1)\Upsilon_{\alpha'}(n_1-1) - \sum_{p\in S} \log p\right| = o(n_1),$$

whereby

$$\left|\Upsilon_{\alpha'}(n_1-1) - \frac{\sum_{p\in S}\log p}{n_1}\right| = o(1).$$

Letting n tend to infinity and applying Lemma 6.1 yields the desired result. □

Combining Lemmata 5.3 and 6.3 leads, immediately, to Proposition 5.1.

Before we conclude this section, we would like to take the opportunity to mention a few properties of the function $c(\alpha)$ defined in (1.7). Most of these are not strictly necessary for the proofs of our main results, but may be of independent interest and suggest the limitations of our method. We summarize them in the following proposition.

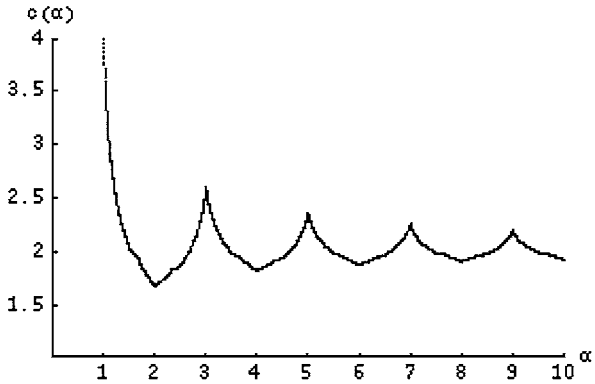
Proposition 6.4.
(1) *$c(\alpha)$ is a continuous function in α, for $\alpha > 0$.*
(2) *If $\alpha \geq 1$, then*

$$\frac{8}{e^{\pi/2}} = c(2) \leq c(\alpha) \leq c(1) = 4.$$

(3)

$$\lim_{\alpha \to \infty} c(\alpha) = 2.$$

The proof of the above proposition depends primarily upon Euler-McLaurin summation. We note that one may, in fact, show that $c(\alpha)$ is uniformly continuous on the interval $[r, \infty)$, where r is any fixed positive real number. For our purposes, however, this is not of great importance. If we plot the graph of $c(\alpha)$, there are a number of features which suggest themselves:



It is tempting to hypothesize, for instance, that $c(\alpha)$ is monotone on the intervals between integers. This is not the case, however, as is demonstrated by the fact that $c(2.35) = 1.8257\ldots$, $c(2.36) = 1.8251\ldots$ and $c(2.37) = 1.8255\ldots$.

7. Lower bounds for $\Pi(n_1, n_2)$

In this section, we address the problem of constructing explicit lower bounds for $\Pi(n_1, n_2)$, as per Proposition 5.2. We combine inequalities for primes in intervals due to Schoenfeld [41] (sharpening Rosser and Schoenfeld [40]) with rather lengthy computations. We will describe the latter in some detail.

Let $\alpha > 1$ be a fixed rational number. If $c_1(\alpha) > c(\alpha)$, then Proposition 5.1 implies the existence of a positive constant $d_1(\alpha)$ such that for all $(n_1, n_2) \in \Gamma(\alpha)$, $\Pi(n_1, n_2) \geq$

$d_1(\alpha)c_1(\alpha)^{n_1}$. The level of difficulty involved in computing $d_1(\alpha)$ depends heavily upon both the size of $c(\alpha) - c_1(\alpha)$ and upon α itself. For the values of α in (1.17), we will always choose $c(\alpha) - c_1(\alpha)$ to be between 0.05 and 0.15. For certain α, we take $c(\alpha) - c_1(\alpha)$ particularly small, with applications to Corollary 1.6 in mind.

Once α and $c_1(\alpha)$ are chosen, we find the value of $d_1(\alpha)$ in (1.17) in four basic stages. Specifically, we define, for each α under consideration, positive integers $N_i(\alpha)$ for $1 \leq i \leq 3$, with

$$1 \leq N_1(\alpha) < N_2(\alpha) < N_3(\alpha),$$

and separately treat the cases with n_1 "small" ($1 \leq n_1 < N_1(\alpha)$), n_1 "middling" ($N_1(\alpha) \leq n_1 < N_2(\alpha)$), n_1 "large" ($N_2(\alpha) \leq n_1 < N_3(\alpha)$) and n_1 "very large" ($n_1 \geq N_3(\alpha)$). In the first of these situations, we will compute $\Pi(n_1, n_2)$ for all relevant pairs $(n_1, n_2) \in \Gamma(\alpha)$, directly from the definition. If $N_1(\alpha) \leq n_1 < N_2(\alpha)$ or $N_2(\alpha) \leq n_1 < N_3(\alpha)$, we will instead estimate $\Pi(n_1, n_2)$, using inequality (5.8). In the latter range, we will apply a "bootstrapping" argument to enable us to calculate the set $S(n_1, n_2)$ for only certain pairs (n_1, n_2) in $\Gamma(\alpha)$. Finally, if $n_1 \geq N_3(\alpha)$, we will utilize the aforementioned bounds for primes in intervals.

We begin by considering this last case; this will reduce the problem to a finite computation. If n_1 is sufficiently large, say $n_1 \geq N_3(\alpha)$, suitable upper and lower bounds for $\theta(x)$, due to Schoenfeld [41] (extending those of Rosser and Schoenfeld [40]), enable us to derive a good lower bound for $\Pi(n_1, n_2)$. Specifically, we apply lower bounds of the shape

$$\theta(x) > x\left(1 - \frac{1}{c \log x}\right),$$

valid for $x \geq d$, where the values of c and d are given in Corollary 2^* of [41], together with the inequality

$$\theta(x) < 1.000081x,$$

valid for all $x > 0$ (see the closing remarks of [41]). If we set $\alpha' = \frac{n_2-1}{n_1-1}$, we can then obtain a lower bound for $\Upsilon_{\alpha'}(n_1 - 1)$ of the form $c'n_1$ for some positive constant c' by approximating the sums S_1, S_2, and S_3 defined in the proof of Lemma 6.1. Combining this with the fact that

$$\log \Pi(n_1, n_2) \geq \Upsilon_{\alpha'}(n_1 - 1) - \ln(n_1 n_2),$$

we arrive at a bound $N_3(\alpha)$ such that for all $n_1 \geq N_3(\alpha)$, $\Pi(n_1, n_2) \geq c_1(\alpha)^{n_1}$. While this reduces verifying Proposition 5.2, for a given value of α, to a finite computation, the remaining problem is still non-trivial since the values of $N_3(\alpha)$ that arise exceed 3×10^5.

For n_1 small, say with $1 \leq n_1 < N_1(\alpha)$, where $N_1(\alpha)$ is 1000 or less, we compute the values of $\Pi(n_1, n_2)$ explicitly. In many cases, the pair (n_1, n_2) corresponding to $d_1(\alpha)$ (i.e. minimizing $\Pi(n_1, n_2)c_1(\alpha)^{-n_1}$) has n_1 in this range. Since $\Pi(n_1, n_2)$ is defined to be the greatest common divisor of $\Pi_1(n_1, n_2)$ and $\Pi_2(n_1, n_2)$, we first compute these two values. Each of these terms is itself a greatest common divisor, of the coefficients of $P_{n_1,n_2}(x)$ and $Q_{n_1,n_2}(x)$ respectively. Naively computing each of the binomial coefficients involved here would be taxing, even for values of n_1 this small. However, we circumvent this by exploiting the following identities.

$$\binom{n_2+1/2}{k} = \binom{n_2+1/2}{k-1}\left(\frac{n_2+3/2-k}{k}\right) \tag{$*$}$$

$$\binom{n_1+n_2-k}{n_2} = \binom{n_1+n_2-k+1}{n_2}\left(\frac{n_1-k+1}{n_1+n_2-k+1}\right) \tag{$*$}$$

$$\binom{n_1-1/2}{k} = \binom{n_1-1/2}{k-1}\left(\frac{n_1+1/2-k}{k}\right) \tag{$\dagger$}$$

$$\binom{n_1+n_2-k}{n_1} = \binom{n_1+n_2-k+1}{n_1}\left(\frac{n_2-k+1}{n_1+n_2-k+1}\right) \tag{$\dagger$}$$

To compute $\Pi_1(n_1, n_2)$, we begin by setting

$$G_1 = \binom{n_1+n_2}{n_1} \quad \text{and} \quad n = 1.$$

Using the two formulae labeled $(*)$, we can see that in general the next coefficient of $P_{n_1,n_2}(x)$ may be obtained by multiplying the previous one by

$$f_k = \frac{(n_1-k+1)(n_2+3/2-k)}{(n_1+n_2-k+1)k}.$$

If we write $nf_k = \frac{a_k}{b_k}$ in reduced form, then we note that a_k does not contribute to $\Pi_1(n_1, n_2)$ and b_k diminishes it. Therefore, we set G_1 equal to the numerator of G_1/b_k. Now, a_k may serve to reduce b_{k+1}, so we set $n := na_k$. Iterating this process until k equals n_1, we obtain the value for $\Pi_1(n_1, n_2)$. We compute $\Pi_2(n_1, n_2)$ using the same idea, except with an analogous definition for f_k, derived from equations $(\dagger)$. Explicitly evaluating

$$\Pi(n_1, n_2) = \gcd\{\Pi_1(n_1, n_2), \Pi_2(n_1, n_2)\}$$

for all $n_1 < N_1(\alpha)$, we set

$$d_2(\alpha) = \min_{\substack{(n_1,n_2)\in\Gamma(\alpha)\\ n_1<N_1(\alpha)}} \frac{\Pi(n_1, n_2)}{c_1(\alpha)^{n_1}}.$$

As mentioned previously, in most cases under consideration, we have $d_1(\alpha) = d_2(\alpha)$. If, however, $c_1(\alpha)$ is chosen particularly close to $c(\alpha)$, the value for $d_1(\alpha)$ may come from a pair (n_1, n_2) that is larger.

Once n_1 exceeds $N_1(\alpha)$, the above exhaustive computation becomes too burdensome. Luckily, the asymptotic behavior of $\Pi(n_1, n_2)$ is starting to play a role, a fact we can exploit. Given $t \in \mathbb{N}$ minimal such that $t \geq N_1(\alpha)(\alpha - 1)$, if n_1 is the smallest positive integer such that $n_1 \geq \frac{t}{\alpha-1}$, setting $n_2 = n_1 + t$, we find that both (n_1, n_2) and (n_1+1, n_2+1) are in the set $\Gamma(\alpha)$ (and, indeed, $n_1 \geq N_1(\alpha)$ is minimal with this property in $\Gamma(\alpha)$). Let

$r = \frac{n_2-1}{n_1-1}$ and define

$$S'(n_1, n_2) = \bigcup_{i=1}^{\lfloor (n_1-1)/\sqrt{2n_2+2} \rfloor} (I_{1,i} \cup I_{2,i} \cup I_{3,i}),$$

where

$$\begin{aligned} I_{1,i} &= \bigcup_{j=\lceil r(i-1/2)+1/2 \rceil}^{\lfloor ri \rfloor} \left(\frac{n_2-1}{j}, \frac{2(n_2-1)}{2j-1} \right), \\ I_{2,i} &= \left(\frac{n_2-1}{\lceil r(i-1/2)+1/2 \rceil - 1}, \frac{2(n_1-1)}{2i-1} \right) \end{aligned}$$

if

$$\lfloor r(i-1/2)+1 \rfloor < \lceil r(i-1/2)+1/2 \rceil$$

and the empty set otherwise, and

$$I_{3,i} = \left(\frac{n_1-1}{i}, \frac{2(n_2-1)}{2\lfloor ri \rfloor + 1} \right),$$

provided $\lfloor ri \rfloor < \lceil ri - 1/2 \rceil$, and the empty set, if this inequality fails to be satisfied. Comparing definitions, it is easy to see that

$$S'(n_1, n_2) \subseteq S(n_1, n_2) \cup \{p \text{ prime} : n_1 n_2 \equiv 0 \pmod{p}\},$$

where $S(n_1, n_2)$ is as defined before inequality (5.8). If we let $P = \prod_{p \in S'(n_1,n_2)} p$, then (5.8) implies that

$$\Pi(n_1, n_2) \geq P/\gcd(P, n_1 n_2).$$

Furthermore, closer examination of the above definitions reveals that if

$$p \in S'(n_1, n_2), \quad \text{but } p \notin S'(n_1+1, n_2+1),$$

then, necessarily, p divides $n_1 n_2$. It follows, additionally, that

$$\Pi(n_1+1, n_2+1) \geq P/\gcd(P, n_1 n_2 (n_1+1)(n_2+2)).$$

We may therefore conclude, if

$$\frac{P}{\gcd(P, n_1 n_2 (n_1+1)(n_2+2))} \geq d_1(\alpha) c_1(\alpha)^{n_1+1}, \tag{7.1}$$

that a like lower bound holds for $\Pi(n_1, n_2)$ and $\Pi(n_1+1, n_2+1)$. If (7.1) fails for (n_1, n_2), we term (n_1, n_2) a *potentially minimal pair*. We repeat this computation for all $n_1 < N_2(\alpha)$, which we usually take to be between 5000 and 10000. We then explicitly compute $\Pi(n_1, n_2)$

and $\Pi(n_1+1, n_2+1)$ using the previous techniques, for all of the potentially minimal pairs, and set

$$d_3(\alpha) = \min_{\substack{(n_1,n_2)\in\Gamma(\alpha)\\ n_1<N_2(\alpha)}} \frac{\Pi(n_1, n_2)}{c_1(\alpha)^{n_1}}.$$

In all our cases, it turns out that $d_1(\alpha) = d_3(\alpha)$; indeed our choices of $N_2(\alpha)$ are made so that this occurs. The following table lists the pairs (n_1, n_2) for each α that give us our lower bound for $d_1(\alpha)$, i.e. $\Pi(n_1, n_2) = d_1(\alpha)c_1(\alpha)^{n_1}$ (the values for $\log d_1(\alpha)$ given in Table (1.17) are rounded down to 3 decimal places).

α	n_1	n_2	α	n_1	n_2	α	n_1	n_2
1.5	296	444	3.5	404	1411	5.5	362	1985
1.6	277	443	3.6	395	1421	5.6	353	1972
1.7	723	1229	3.7	379	1402	5.7	98	550
1.8	284	511	3.8	523	1983	5.8	95	550
1.9	398	756	3.9	509	1983	5.9	94	551
2.0	448	895	4.0	496	1983	6.0	201	1205
2.1	2360	4954	4.1	344	1405	6.1	92	552
2.2	372	818	4.2	473	1983	6.2	303	1870
2.3	3503	8055	4.3	331	1421	6.3	107	672
2.4	336	806	4.4	460	2024	6.4	190	1207
2.5	1912	4778	4.5	181	814	6.5	286	1855
2.6	535	1390	4.6	433	1985	6.6	283	1859
2.7	212	570	4.7	121	564	6.7	181	1209
2.8	507	1419	4.8	410	1965	6.8	252	1703
2.9	484	1403	4.9	401	1964	6.9	287	1972
3.0	456	1365	5.0	394	1965	7.0	2102	14706
3.1	190	586	5.1	386	1965	7.1	204	1445
3.2	174	554	5.2	378	1965	7.2	2045	14722
3.3	426	1405	5.3	105	552	7.3	608	4438
3.4	163	551	5.4	365	1965	7.4	600	4438

(7.2)

To complete our computation, we need to handle the "large" values of n_1, between $N_2(\alpha)$ and $N_3(\alpha)$. Here, we expect the asymptotics of $\Pi(n_1, n_2)$ to assert themselves. We employ a technique used in Bennett [7] to reduce the remaining calculations. As in the previous step, we begin by computing $S'(n_1, n_2)$ with n_1 and n_2 minimal in $\Gamma(\alpha)$ with $n_1 \geq N_2(\alpha)$. For positive integers r_1 and r_2, we define an auxilliary set $S''(r_1, r_2)$ (where we suppress dependence on n_1 and n_2) via

$$S''(r_1, r_2) = \bigcup_{i=1}^{\lfloor (n_1-1)/\sqrt{2n_2+2}\rfloor} (I'_{1,i} \cup I'_{2,i} \cup I'_{3,i}).$$

Here, we set

$$I'_{1,i} = \bigcup_{j=\lfloor r(i-1/2)+1/2\rfloor}^{\lfloor ri\rfloor} \left(\frac{n_2-1}{j}, \frac{n_2-1+r_2}{j}\right]$$

and define

$$I'_{2,i} = \left(\frac{n_2-1}{\lfloor r(i-1/2)+1\rfloor}, \frac{2(n_2-1+r_2)}{2(\lfloor r(i-1/2)+1\rfloor)-1}\right],$$

provided

$$\lfloor r(i-1/2)+1\rfloor < \lceil r(i-1/2)+1/2\rceil$$

and

$$I'_{3,i} = \left(\frac{n_1-1}{i}, \frac{n_1-1+r_1}{i}\right],$$

provided

$$\lfloor ri\rfloor < \lceil ri-1/2\rceil.$$

In the latter two cases, we take $I'_{2,i}$ and $I'_{3,i}$ to be empty if the given inequalities are not satisfied. From the definition of S', we have that

$$S'(n_1,n_2)\backslash S''(r_1,r_2) \subseteq S'(n_1+r'_1, n_2+r'_2)$$

for any $r'_1 < r_1$ and $r'_2 < r_2$. This enables us to approximate the set

$$S'(n_1+r'_1, n_2+r'_2)$$

in terms of $S'(n_1,n_2)$ and $S''(r_1,r_2)$. If we define P as before and set

$$Q = \prod_{p\in S''(r_1,r_2)} p,$$

then for any $(n'_1,n'_2) \in \Gamma(\alpha)$ such that $0 \le n'_1 - n_1 < r_1$ and $0 \le n'_2 - n_2 < r_2$, we have

$$\Pi(n'_1,n'_2) \ge \frac{P}{Q(n_1+r_1)(n_2+r_2)}.$$

If the value on the right hand side is greater than $d_1(\alpha)c_1(\alpha)^{n_1+r_1}$, it follows that

$$\Pi(n'_1,n'_2) \ge d_1(\alpha)c_1(\alpha)^{n'_1}$$

for all (n'_1,n'_2) in the given range. If we choose r_1 and r_2 to be as large as possible while still making the above inequalities hold, this enables us to automatically verify the bound on $\Pi(n_1,n_2)$ stated in Proposition 5.2 for each of the values (n'_1,n'_2) with $0 \le n'_1 - n_1 < r_1$ and $0 \le n'_2 - n_2 < r_2$. Since computing the set S'' is much easier than computing S', this "bootstrapping technique" is computationally efficient. For our purposes, determining values of r_1 and r_2 that satisfy the above requirements is more or less a matter of trial and error. Applying this approach for all $n_1 < N_3(\alpha)$ completes the proof of Proposition 5.2, for the α under consideration. We note that we choose

$$N_1(\alpha) = \begin{cases} 1000 & \text{if } \alpha \in \{2.4, 2.5\} \\ 900 & \text{if } \alpha = 2.0 \\ 800 & \text{if } \alpha \in \{1.7, 2.1, 2.2, 2.3, 3.1, 3.2, 3.3, 3.4\} \\ 500 & \text{otherwise,} \end{cases}$$

$$N_2(\alpha) = \begin{cases} 18000 & \text{if } \alpha = 2.1 \\ 12000 & \text{if } \alpha = 1.7 \\ 10000 & \text{if } \alpha \in \{1.5, 1.6, 1.8, 1.9, 2.0, 2.3, 2.4, 2.5\} \\ 8000 & \text{if } \alpha \in \{2.2, 3.1, 3.2, 3.3, 3.4\} \\ 5000 & \text{otherwise} \end{cases}$$

and $N_3(\alpha)$ as in the following table (where we also list the number of potentially minimal pairs corresponding to our choices of $N_1(\alpha)$ and $N_2(\alpha)$).

α	pairs	$N_3(\alpha)$	α	pairs	$N_3(\alpha)$	α	pairs	$N_3(\alpha)$
1.5	0	3.5×10^5	3.5	22	3×10^5	5.5	294	3×10^5
1.6	36	5.5×10^5	3.6	106	3×10^5	5.6	354	3×10^5
1.7	38	1.5×10^6	3.7	190	3×10^5	5.7	386	3×10^5
1.8	10	5×10^5	3.8	184	3×10^5	5.8	650	3×10^5
1.9	72	4.5×10^5	3.9	174	3×10^5	5.9	394	3×10^5
2.0	318	6×10^5	4.0	40	3×10^5	6.0	392	3×10^5
2.1	1192	1.3×10^6	4.1	32	3×10^5	6.1	408	3×10^5
2.2	948	1.35×10^6	4.2	116	3×10^5	6.2	368	3×10^5
2.3	1296	1.45×10^6	4.3	126	3×10^5	6.3	396	3×10^5
2.4	1198	1.7×10^6	4.4	146	3×10^5	6.4	366	3×10^5
2.5	1864	1.8×10^6	4.5	134	2.25×10^5	6.5	362	3×10^5
2.6	1002	7.5×10^5	4.6	278	3×10^5	6.6	734	4×10^5
2.7	684	7.5×10^5	4.7	350	3×10^5	6.7	1138	4×10^5
2.8	1454	1.05×10^6	4.8	284	3×10^5	6.8	1238	5×10^5
2.9	1092	5.5×10^5	4.9	286	3×10^5	6.9	1134	5.5×10^5
3.0	770	4.5×10^5	5.0	588	6×10^5	7.0	2324	9×10^5
3.1	1150	6×10^5	5.1	696	3×10^5	7.1	1822	5×10^5
3.2	532	5.1×10^5	5.2	128	3×10^5	7.2	1998	5×10^5
3.3	256	5×10^5	5.3	310	3×10^5	7.3	1806	5×10^5
3.4	448	5×10^5	5.4	276	3×10^5	7.4	1676	5×10^5

(7.3)

Now that we have the framework for the computations in place, we will indicate how they play out in a particular example, where we choose $c(\alpha) - c_1(\alpha)$ rather small, in order to illustrate various complexities that may arise. We take $\alpha = 2.1$, calculate $c(2.1) = 1.705$ to three decimal places and let $c_1(2.1) = 1.66$. There is no particular significance to this value, other than that it makes the resulting computations somewhat more challenging. We note, for each value of $n_1 \in \mathbb{N}$, that there are either two or three choices for $n_2 \in \mathbb{N}$ with $(n_1, n_2) \in \Gamma(2.1)$.

To begin, we need to determine a suitable value for $N_3(2.1)$. We wish to take it as small as possible in order to minimize subsequent calculations. We claim that $N_3(2.1) = 1.3 \times 10^6$ is a valid choice. Let $(n_1, n_2) \in \Gamma(2.1)$, set $r = \frac{n_2-1}{n_1-1}$ and define $S'(n_1, n_2)$ as previously. We therefore have

$$\log \Pi(n_1, n_2) \geq -\log(n_1 n_2) + \sum_{p \in S'(n_1,n_2)} \log p.$$

One may readily show that

$$I_{1,1} = \left(\frac{n_2 - 1}{2}, \frac{2(n_2 - 1)}{3}\right)$$

and so

$$\sum_{p \in I_{1,1}} \log p = \theta\left(\frac{2(n_2 - 2)}{3}\right) - \theta\left(\frac{n_2 - 1}{2}\right).$$

Applying the bounds of Schoenfeld [41],

$$\sum_{p \in I_{1,1}} \log p \geq \frac{2(n_2 - 2)}{3}\left(1 - \frac{1}{41 \log(2(n_2 - 2)/3)}\right) - 1.000081\frac{(n_2 - 1)}{2}.$$

Now $n_1 \geq 1.3 \times 10^6$ and so $n_2 \geq 2.73 \times 10^6$, whereby

$$\sum_{p \in I_{1,1}} \log p \geq 0.16549\,(n_2 - 1).$$

Since $0 \leq 2.1n_1 - n_2 < 2.2$ implies that

$$|r - 2.1| \leq \frac{1.1}{n_1 - 1} < 8.47 \times 10^{-7},$$

we have

$$0.16549(n_2 - 1) \geq 0.34752(n_1 - 1) \geq 0.3475n_1,$$

whence

$$\sum_{p \in I_{1,1}} \log p > 0.3475n_1.$$

Since $I_{2,1}$ and $I_{3,1}$ are empty, we next consider

$$I_{1,2} = \left(\frac{n_2 - 1}{4}, \frac{2(n_2 - 1)}{7}\right),$$

whereby

$$\sum_{p\in I_{1,2}} \log p = \theta\left(\frac{2(n_2-2)}{7}\right) - \theta\left(\frac{n_2-1}{4}\right).$$

It follows that

$$\sum_{p\in I_{1,2}} \log p \geq \frac{2(n_2-2)}{7}\left(1 - \frac{1}{41\log(2(n_2-2)/7)}\right) - 1.000081\frac{(n_2-1)}{4}$$

and, arguing as before, this exceeds $0.073869n_1$. Again, $I_{2,2}$ and $I_{3,2}$ are empty. Repeating this process for $i \leq 23$, we find that

$$\sum_{p\in s'(n_1,n_2)} \log p \geq 0.50694n_1$$

and hence we conclude that

$$\log \Pi(n_1, n_2) \geq 0.50694n_1 - \log(n_1n_2) \geq 0.50691n_1 > \log(1.66)n_1.$$

It follows that $\Pi(n_1, n_2) > 1.66^{n_1}$, provided $n_1 \geq N_3(2.1) = 1.3 \times 10^6$.

It remains to check the desired inequality for all $(n_1, n_2) \in \Gamma(2.1)$ such that $n_1 < 1.3 \times 10^6$. We choose $N_1(2.1) = 800$ and find that

$$d_2(2.1) = \min_{\substack{(n_1,n_2)\in\Gamma(2.1)\\ n_1<800}} \frac{\Pi(n_1, n_2)}{1.66^{n_1}} = \frac{\Pi(573, 1202)}{1.66^{573}} \sim 2.625 \times 10^{-7}.$$

We note that, in this case, $d_2(2.1) \neq d_1(2.1)$. The computation of $d_2(2.1)$ took approximately 41 minutes 29 seconds of CPU time on a Sun Ultrasparc 10.

If $N_1(2.1) \leq n_1 < N_2(2.1) = 18000$, we use the second technique described for approximating $\Pi(n_1, n_2)$. We begin by choosing $(n_1, n_2) = (800, 1680) \in \Gamma(2.1)$ and proceed by computing, for all pairs (n_1, n_2) in the chosen ranges, both $S'(n_1, n_2)$ and the associated values

$$P = \prod_{p\in S'(n_1,n_2)} p, \quad d = \left(\frac{P}{\gcd(P, n_1n_2)}\right)1.66^{-n_1}$$

and

$$d' = \left(\frac{P}{\gcd(P, n_1n_2(n_1+1)(n_2+1))}\right)1.66^{-n_1-1}.$$

We find precisely 1192 pairs (n_1, n_2) with $800 \leq n_1 < 18000$ for which either d or d' is less than $d_2(2.1)$. These correspond to (n_1, n_2) (respectively, $(n_1 + 1, n_2 + 1)$) being a potentially minimal pair. For each of these pairs, we explicitly compute

$$\Pi(n_1, n_2)1.66^{-n_1} \tag{7.4}$$

and check to see if any of the resulting values is less than $d_2(2.1)$. We find four such pairs, corresponding to

$$(n_1, n_2) \in \{(1017, 2135), (1016, 2133), (1413, 2967), (2360, 4954)\}.$$

The minimum value of (7.4) for these pairs is that with $n_1 = 2360$ and $n_2 = 4954$, whence we set

$$d_3(2.1) = \min_{\substack{(n_1,n_2)\in\Gamma(2.1)\\ n_1<18000}} \frac{\Pi(n_1, n_2)}{1.66^{n_1}} = \frac{\Pi(2360, 4954)}{1.66^{2360}} \sim 3.094 \times 10^{-11}.$$

On an Ultrasparc 10, these computations took 8 hours 35 minutes 36 seconds of CPU time.

We now proceed to the "bootstrapping" which we will use to deal with the remaining values between $n_1 = 18000$ and $n_1 = 1.3 \times 10^6$. This represents the majority of the overall computation. We remind the reader that computing $S'(n_1, n_2)$, is significantly more difficult than computing $S''(r_1, r_2)$, since n_1 and n_2 will generally be much larger than r_1 and r_2. This motivates our desire to choose the pair (r_1, r_2) to be as large as possible. For our example, we begin with $(n_1, n_2) = (18000, 37800)$. When we choose r_1 and r_2, we do so in such a fashion that $(n_1 + r_1, n_2 + r_2) \in \Gamma(2.1)$. In this case, we start with $r_1 = 41$ and $r_2 = 86$ (although these values look peculiar, they arise from a third parameter which we are suppressing). Computing $S'(18000, 37800)$ we find that $\log P > 9528.4$, and the value of $\log Q$ associated to S'' (41, 86) is less than 343.6. It follows that

$$\log P - \log Q - \log(n_1 + r_1) - \log(n_2 + r_2) > 9164.4$$

while

$$(n_1 + r_1) \log c_1(2.1) - \log d_1(2.1) = 18041 \log 1.66 - 24.199 < 9119.3.$$

Since the first of these values is larger, we conclude that, for any pair $(n_1, n_2) \in \Gamma(2.1)$ such that $0 \le n_1 - 18000 < r_1$ and $0 \le n_2 - 37800 < r_2$, our desired lower bound for $\Pi(n_1, n_2)$ holds. We observe that this has reduced our problem to checking pairs $(n_1, n_2) \in \Gamma(2.1)$ such that $n_1 \ge 18041$. As n_1 gets larger, we can increase the values of r_1 and r_2 for which the above procedure works. To move from $n_1 \ge 18000$ to $n_1 \ge 25000$, we apply this bootstrapping technique 206 times. For larger n_1, however, this approach becomes increasingly efficient. The following table summarizes this information.

n_1	Number of bootstraps
18000 to 25000	206
25000 to 50000	351
50000 to 100000	332
100000 to 200000	322
200000 to 400000	326
400000 to 1.3×10^6	566

(7.5)

This final stage of the computation took 27 hours and 29 minutes of CPU time, completing the proof of Proposition 5.2 in case $\alpha = 2.1$. Run times for the other values of α were similar. We should emphasize that we have not made especially great efforts to optimize the aforementioned algorithms.

8. Proofs of Theorems 1.3 and 1.5

We will actually begin by proving Theorem 1.5; the proof of Theorem 1.3 will follow along similar lines, essentially just replacing $c_1(\alpha)$ with $c(\alpha)$.

Let us suppose that a, y, x_0, m_0 and Δ are integers with m_0 odd and positive, a, y and x_0 positive, y not a square, and $x_0^2 + \Delta = a^2 y^{m_0}$. Since

$$\binom{n+1/2}{k} 4^k \in \mathbb{Z}$$

for all positive integer n and k, it follows from (2.2) and (2.3) that

$$\frac{\Delta_0^{-n_1}\Omega^{n_1}}{\Pi(n_1, n_2)} P_{n_1,n_2}(\xi) = A \in \mathbb{Z}$$

and

$$\frac{\Delta_0^{-n_2}\Omega^{n_2}}{\Pi(n_1, n_2)} Q_{n_1,n_2}(\xi) = B \in \mathbb{Z}.$$

Equation (2.1) therefore implies that

$$\Delta_0^{-n_1}\Pi(n_1, n_2)^{-1}\left|I_{n_1,n_2}(\xi)\right| = \left|\frac{A}{\Omega^{n_1}} - \frac{x_0}{ay^{m_0/2}}\frac{B\Delta_0^{n_2-n_1}}{\Omega^{n_2}}\right|.$$

Let us next suppose that p, s and m are positive integers with $m > m_2$ odd (where m_2 is as in (1.15)) and set

$$\Xi = \left|\frac{p}{sy^{m/2}} - 1\right|.$$

Since each prime dividing y also divides Ω_1, we can choose $t \in \mathbb{N}$ minimal such that

$$\Omega_1^t a y^{\frac{1}{2}(m_0 - m)} \in \mathbb{Z}. \tag{8.1}$$

Given a real number $\alpha \geq 3/2$, we then may take n_1 integral, satisfying

$$\frac{t}{\alpha - 1} \leq n_1 < \frac{t}{\alpha - 1} + 2 \tag{8.2}$$

and set $n_2 = n_1 + t$. We note that this provides precisely two choices for n_1.

Defining

$$\Lambda = \left|\frac{p}{sy^{m/2}} - \frac{x_0 B\Delta_0^{n_2-n_1}}{aAy^{m_0/2}\Omega^{n_2-n_1}}\right|,$$

we therefore have

$$\Lambda < \Xi + \Pi(n_1, n_2)^{-1} A^{-1} \left(\frac{\Omega}{\Delta_0} \right)^{n_1} \left| I_{n_1,n_2}(\xi) \right|$$

(note that the nonvanishing of A is a consequence of the contour integral representation for $P_{n_1,n_2}(x)$ given in Section 3). From Lemma 4 of Beukers [10], for one of our two choices for n_1, we have $\Lambda \neq 0$ and so, from (8.1),

$$\Lambda \geq \left(saAy^{m_0/2} \Omega_1^{n_2-n_1} \right)^{-1}.$$

Combining our upper and lower bounds for Λ, we find that

$$1 < \Xi \Lambda_1 + \Lambda_2, \tag{8.3}$$

where, upon substituting for A,

$$\Lambda_1 = s\Pi(n_1, n_2)^{-1} a y^{m_0/2} \left(\frac{\Omega}{\Delta_0} \right)^{n_1} \Omega_1^{n_2-n_1} \left| P_{n_1,n_2}(\xi) \right|.$$

and

$$\Lambda_2 = s\Pi(n_1, n_2)^{-1} a y^{m_0/2} \left(\frac{\Omega}{\Delta_0} \right)^{n_1} \Omega_1^{n_2-n_1} \left| I_{n_1,n_2}(\xi) \right|.$$

Now, applying Lemma 4.1, Proposition 5.2 and the fact that $n_2 \leq \alpha n_1$ leads to the inequality

$$\Lambda_2 < \frac{s(\alpha+1)^2 \Omega_1^{\alpha n_1} |\Delta|^{(\alpha+1)n_1+3-2\alpha}}{d_1(\alpha) a^{2(\alpha+1)n_1+5-4\alpha} y^{((\alpha+1)n_1+5/2-2\alpha)m_0} (c_1(\alpha)\Delta_1 F(r(\alpha,\xi),\alpha,\xi))^{n_1}},$$

whereby

$$\Lambda_2 < \frac{1}{2} \chi_2 \, \chi_1^{-n_1}. \tag{8.4}$$

Suppose that p is a prime dividing y. It follows, since $\Omega_1^t a y^{\frac{1}{2}(m_0-m)}$ is an integer, that necessarily

$$\mathrm{ord}_p\left(\Omega_1^t a y^{\frac{1}{2}(m_0-m)} \right) = t \, \mathrm{ord}_p \Omega_1 + \mathrm{ord}_p a + \frac{1}{2}(m_0 - m) \, \mathrm{ord}_p y \geq 0,$$

and so

$$t \left(\frac{2\mathrm{ord}_p \Omega_1}{\mathrm{ord}_p y} \right) + \frac{2\mathrm{ord}_p a}{\mathrm{ord}_p y} + m_0 \geq m.$$

Since the choice of p dividing y was arbitrary, from $m \geq m_2$, we conclude that

$$t \geq (\alpha - 1) \frac{\log \chi_2}{\log \chi_1}$$

and hence, via (8.2),

$$n_1 \geq \frac{\log \chi_2}{\log \chi_1}.$$

We conclude, from (8.4), that $\Lambda_2 < 1/2$ and so (8.3) implies the inequality

$$\Xi > \frac{1}{2\Lambda_1} = \frac{\Pi(n_1, n_2)\Delta_1^{n_1}}{2say^{m_0/2}\Omega_1^{n_2}\left|P_{n_1,n_2}(\xi)\right|}.$$

Again using that $n_2 \leq \alpha n_1$ and applying Lemma 3.1 and Proposition 5.2, we have

$$\Xi > \frac{d_1(\alpha)}{4s(\alpha+1)\,ay^{m_0/2}}\left(\frac{c_1(\alpha)\Delta_1}{\Omega_1^{\alpha}F(r(\alpha,\xi),\alpha,\xi)}\right)^{n_1}. \tag{8.5}$$

Now if

$$t_0 = \left[\frac{m}{2m_1}\right] + 1$$

and p is a prime dividing y, we have

$$\mathrm{ord}_p\left(\Omega_1^{t_0}\right) \geq t_0\, m_1\, \mathrm{ord}_p y > \frac{m}{2}\mathrm{ord}_p y = \mathrm{ord}_p(y^{m/2}).$$

and so (8.1) implies that

$$t \leq t_0 < \frac{m}{2m_1} + 1.$$

From (8.2), we thus have

$$n_1 < \frac{t}{\alpha-1} + 2 < \frac{m}{2(\alpha-1)m_1} + \frac{2\alpha-1}{\alpha-1} = \frac{m-1}{2(\alpha-1)m_1} + \frac{(4\alpha-2)m_1+1}{2(\alpha-1)m_1}. \tag{8.6}$$

Substituting the values for χ_3 and λ_1 completes the proof of Theorem 1.5.

The proof of Theorem 1.3 proceeds similarly. If $\epsilon_1 > 0$, from Proposition 5.1 we have, for n_1 exceeding some effectively computable bound (depending on ϵ_1 and α), that

$$\Pi(n_1, n_2) \geq c(\alpha)^{(1-\epsilon_1)n_1}.$$

Arguing as before, we obtain, in analogue to (8.5),

$$\Xi > C\left(\frac{c(\alpha)^{1-\epsilon_1}\Delta_1}{\Omega_1^{\alpha}F(r(\alpha,\xi),\alpha,\xi)}\right)^{n_1},$$

where the constant C is effective and depends upon α, s, a, y and m_0 (and, again, n_1 is suitably large). Applying (8.6) and choosing ϵ_1 suitably small relative to a given $\epsilon > 0$ completes the proof.

9. Proof of Corollaries 1.4 and 1.6

Corollary 1.4 follows immediately from Theorem 1.3 upon choosing parameters y, m_0, Δ, a and α as follows; we leave verification to the reader:

y	m_0	Δ	a	α	y	m_0	Δ	a	α
2	15	7	1	3.457	54	1	2	3	6.589
3	15	−37	1	3.195	55	5	19	1	4.724
5	3	4	1	5.019	56	3	−784	1	1.967
6	5	32	1	3.088	57	3	56	3	3.323
10	5	144	1	2.094	58	3	24	7	5.369
12	3	−36	1	2.447	60	1	−4	1	4.306
13	3	−12	1	3.335	62	1	−2	1	5.046
14	13	−372992	1	2.196	63	1	−1	1	5.503
17	7	−1192	11	2.910	65	1	1	1	5.507
18	5	92	13	4.016	66	1	2	1	5.049
19	5	15	16	5.143	68	1	4	1	4.333
20	1	4	1	3.265	69	3	180	1	2.380
21	1	−4	1	3.507	70	3	−49	3	3.413
23	5	−26	1	3.926	72	1	−9	6	3.071
24	1	−9	3	3.015	73	5	−368	1	3.157
26	3	40	7	3.729	74	5	−145	3	3.427
28	3	48	1	2.674	75	3	−625	1	1.964
29	1	4	1	3.563	76	5	60	1	5.143
30	7	−13696	11	2.664	77	1	−4	1	4.529
31	3	6	5	6.141	78	3	−169	1	2.415
33	3	−16	7	5.440	79	1	−2	1	5.186
34	1	−2	1	4.416	80	1	−1	1	5.685
35	3	26	1	2.576	82	1	1	1	5.687
37	3	28	1	3.181	83	1	2	1	5.191
38	1	2	1	4.435	84	3	−196	1	2.818
40	1	4	1	3.830	85	1	4	1	4.548
42	5	608	1	2.684	87	3	−841	1	1.947
43	3	−17	1	2.676	89	1	8	1	2.410
44	3	−80	1	2.532	90	1	−1	2	7.003
45	1	−4	1	4.038	91	3	147	1	2.365
46	3	−8	1	6.613	92	1	−8	1	3.055
47	1	−2	1	4.734	93	7	−75087	1	2.357
48	1	−9	3	3.248	95	5	16606	11	2.543
50	1	1	1	5.319	96	1	−4	1	4.757
51	1	2	1	4.750	98	1	−2	1	5.328
52	3	−17	1	2.848	99	1	−1	1	5.839
53	1	4	1	4.070					

(9.1)

It appears that these choices are optimal or close to being so, though we will provide no proof of this here. For many values of y, other parameter sets also lead to nontrivial measures (i.e. those with $\lambda(y) < 2$). By way of example, while the best measure we have been able to find for $\sqrt{12}$ corresponds to the choices $(m_0, \Delta, a, \alpha) = (3, -36, 1, 2.447)$ (where the identical measure is also obtained by taking $(m_0, \Delta, a, \alpha) = (1, -9, 6, 2.447)$), we may also choose the quadruple (m_0, Δ, a, α) as follows:

m_0	Δ	a	α	$\lambda(12)$
1	−4	1	3.190	1.775
5	−97	6	2.362	1.796
5	−1296	7	2.459	1.976
7	−388	1	2.362	1.796
7	−6208	4	2.362	1.796
11	−3652	3	2.664	1.662
13	−58432	1	2.440	1.667
13	−525888	3	2.162	1.766
13	−2103552	6	1.974	1.852
15	−8414208	1	1.974	1.852
15	−75727872	3	1.843	1.919
15	−302911488	6	1.743	1.979
17	−1211645952	1	1.743	1.979

(9.2)

Note that a number of these sets of parameters actually correspond to the same "examples" and yield identical approximation measures. If we define $N(X)$ to be the set of $y \leq X$ for which we may apply Theorem 1.3 to deduce a value of $\lambda(y) < 2$, it appears to be rather difficult to obtain sharp lower bounds for $N(X)$ as $x \to \infty$. While, in all likelihood, $N(X) = o(X)$, its exact order of growth is complicated to determine.

To prove Corollary 1.6, if $y \neq 10, 89$, we make the same choices for m_0, Δ and a as in Table (9.1), which generate the (presumably) optimal measures $\lambda(y)$. If $y = 10$, however, we take $m_0 = 1, a = 5$ and $\Delta = 25$ which, due to the vagaries of our computations of $c_1(\alpha)$ and $d_1(\alpha)$, yields a (barely) nontrivial $\lambda_2(10)$ (which $m_0 = 5, a = 1, \Delta = 144$ and, say, $\alpha = 2.0$ fails to do).

We choose α as follows:

y	α	y	α	y	α	y	α	y	α	y	α
2	3.4	21	3.4	38	4.3	53	3.9	69	2.3	83	5.1
3	3.1	23	3.9	40	3.7	54	6.5	70	3.4	84	2.8
5	4.9	24	3.0	42	2.6	55	4.7	72	3.0	85	4.4
6	3.0	26	3.7	43	2.6	56	1.9	73	3.1	87	1.9
10	1.7	28	2.6	44	2.5	57	3.3	74	3.4	90	6.9
12	2.4	29	3.5	45	3.9	58	5.3	75	1.9	91	2.3

(*Continued on next page.*)

(*Continued*).

y	α	y	α	y	α	y	α	y	α	y	α
13	3.3	30	2.6	46	6.5	60	4.2	76	5.1	92	3.0
14	2.1	31	6.1	47	4.6	62	5.0	77	4.4	93	2.3
17	2.9	33	5.4	48	3.2	63	5.4	78	2.4	95	2.5
18	3.9	34	4.3	50	5.2	65	5.4	79	5.1	96	4.6
19	5.1	35	2.5	51	4.6	66	5.0	80	5.6	98	5.2
20	3.2	37	3.1	52	2.8	68	4.2	82	5.6	99	5.7

(9.3)

In each case, we may readily check that Theorem 1.5 yields a value for $\lambda_1(y)$ which is less than the $\lambda_2(y)$ given in (1.18). Moreover, Theorem 1.5 implies, for each such y, an inequality of the shape

$$\left|\sqrt{y} - \frac{p}{q}\right| > c_2(y) q^{-\lambda_1(y)},$$

for $q = y^k$ and $k \geq \frac{m_2(y)-1}{2}$. It follows that if we set

$$k_0(y) = \max\left\{\frac{m_2(y)-1}{2}, \frac{\log c_2(y)}{(\lambda_1(y) - \lambda_2(y)) \log y}\right\},$$

then

$$\left|\sqrt{y} - \frac{p}{q}\right| > q^{-\lambda_2(y)}, \tag{9.4}$$

for all $q = y^k$ with $k \geq k_0(y)$. For the integers y under consideration, we find the following values of $k_0(y)$:

y	$k_0(y)$	y	$k_0(y)$	y	$k_0(y)$	y	$k_0(y)$
2	53620	30	7414	53	17304	76	27204
3	21428	31	200978	54	49217	77	2581
5	189873	33	69443	55	162770	78	9324
6	57622	34	4705	56	2229	79	3426
10	27426	35	28510	57	11160	80	8769
12	12805	37	3415	58	10943	82	23921
13	15152	38	3911	60	34735	83	12517
14	32595	40	13134	62	11710	84	7475
17	73087	42	10139	63	6772	85	3397
18	62512	43	15461	65	3444	87	3424
19	27085	44	4735	66	46962	90	56505
20	4405	45	8683	68	6084	91	3904

(*Continued on next page.*)

(*Continued*).

y	$k_0(y)$	y	$k_0(y)$	y	$k_0(y)$	y	$k_0(y)$
21	6156	46	27139	69	5604	92	34071
23	82521	47	5263	70	24671	93	7078
24	80463	48	40214	72	2831	95	4977
26	20043	50	2867	73	38801	96	2410
28	3861	51	3106	74	12414	98	3145
29	38888	52	9137	75	2533	99	3140

(9.5)

As a final step in proving Corollary 1.6, we must show, for all values of $k < k_0(y)$ given in Table (9.5), that the corresponding inequality (9.4) still holds. Many of the values of $k_0(y)$ given in this table are too large to easily perform an exhaustive search, so we take a different approach. We begin by computing the y-ary expansion of $\sqrt{y}$, that is

$$\sqrt{y} = \sum_{n=0}^{\infty} \frac{a_n}{y^n} \quad \text{where } a_n \in \{0, \ldots, y-1\}.$$

Straightforward consideration of the terms in this expansion provides us with a simple way of searching for good rational approximations to $\sqrt{y}$ with denominators a power of y:

Lemma 9.1. *Let y be a non-square positive integer and $\lambda > 1$ be real If $q = y^k$ and there exists an integer p such that*

$$\left| \sqrt{y} - \frac{p}{q} \right| \le q^{-\lambda} \tag{9.6}$$

then, in the y-ary expansion of $\sqrt{y}$, either $a_j = 0$ for all values of j between $k+1$ and $\lfloor \lambda k \rfloor$ or $a_j = y-1$ for all j in this range.

Proof: Write

$$\sqrt{y} = \sum_{n=0}^{\infty} \frac{a_n}{y^n} \quad \text{where } a_n \in \{0, \ldots, y-1\}$$

and assume that p/q is a rational number with denominator $q = y^k$, satisfying (9.6). From the y-ary expansion for p/q,

$$\frac{p}{q} = \sum_{n=0}^{k} \frac{b_n}{y^n} \quad \text{where } b_n \in \{0, \ldots, y-1\},$$

inequality (9.6) implies that

$$-y^{-k\lambda} \le \sum_{n=0}^{k} \frac{a_n - b_n}{y^n} - \sum_{n=k+1}^{\infty} \frac{a_n}{y^n} \le y^{-k\lambda}. \tag{9.7}$$

Let us note first that

$$\sum_{n=k+1}^{\infty} \frac{a_n}{y^n} < \frac{1}{y^k},$$

where the strict inequality follows from the fact that $\sqrt{y}$ is irrational. Secondly, if we write

$$\left| \sum_{n=0}^{k} \frac{a_n - b_n}{y^n} \right| = \frac{c}{y^k},$$

where c is a nonnegative integer, then, if $c \geq 2$,

$$\left| \sum_{n=0}^{k} \frac{a_n - b_n}{y^n} \right| - \sum_{n=k+1}^{\infty} \frac{a_n}{y^k} > \frac{1}{y^k},$$

contradicting (9.7). It follows that $c = 0$ or $c = 1$. In the first case,

$$\sum_{n=k+1}^{\infty} \frac{a_n}{y^k} < \frac{1}{y^{k\lambda}}.$$

Choosing $a_j \neq 0$ to be the first non-zero coefficient with index at least $k + 1$, we thus have

$$\sum_{n=k+1}^{\infty} \frac{a_n}{y^k} > \frac{1}{y^j}$$

Combining these two inequalities, we find that

$$\frac{1}{y^j} < \frac{1}{y^{k\lambda}}$$

and so $j > \lambda k$; i.e. the y-ary expansion of $\sqrt{y}$ has a string of zeros from index $n = k + 1$ to $n = \lfloor \lambda k \rfloor$. On the other hand, if $c = 1$, then we have

$$\frac{1}{y^k} - \sum_{n=k+1}^{\infty} \frac{a_n}{y^k} < \frac{1}{y^{k\lambda}}.$$

In this case, choose a_j to be the first coefficient not equal to $y - 1$, with index at least $k + 1$. Then

$$\sum_{n=k+1}^{\infty} \frac{a_n}{y^k} < \frac{1}{y^k} - \frac{1}{y^j}.$$

Combining the last two inequalities, we once again find that

$$\frac{1}{y^j} < \frac{1}{y^{k\lambda}} \Rightarrow j > \lambda k,$$

whereby $a_j = y - 1$ for all values of j between $k + 1$ and $\lfloor \lambda k \rfloor$. □

Applying this lemma, in order to verify inequality (9.4) for $q = y^k$ with $k < k_0(y)$, it suffices to check for suitably long strings of zeros or $y-1$'s in the y-ary expansion of $\sqrt{y}$. With this in mind, we turn our attention to computing the coefficients a_n. Suppose that we have a suitably good decimal approximation to $\sqrt{y}$, say x with

$$|\sqrt{y} - x| \leq y^{-(\lambda+1)k_0/2}$$

(this is easily achieved via Newton's method). If $\sqrt{y}$ has a string of zeros in its expansion of the certain length, then it is easy to see that x either has a string of zeros, or a string of $y-1$'s in its expansion, of the same length. A similar argument holds for strings of $y-1$'s. We may thus use x to search for strings of zeros and $y-1$'s in the expansion for $\sqrt{y}$. Computing the first thousand coefficients in the expansion of x, we check for any such strings of length ≥ 3. If we find none, we may deduce that any integer k which fails to satisfy (9.4) must have either $k \leq 10$ or $k \geq 1000$. If such a string does exist, we check and see whether it satisfies the requirements of Lemma 9.1. Once this is completed, we note that we are looking for strings whose length roughly exceeds $(\lambda-1)k$, beginning with the kth coefficient (where we can suppose that $k \geq 1000$). It follows, if we compute two consecutive coefficients which are not equal, say a_k and a_{k+1}, that in order to satisfy the conditions of Lemma 9.1, the $\lfloor(\lambda-1)k/2\rfloor$th coefficient must be 0 or $y-1$. In fact, at least the next $\lfloor(\lambda-1)k/2\rfloor$ coefficients must all be 0's or all $y-1$'s. Hence we can skip forward and compute the coefficients starting with $a_{k+\lfloor(\lambda-1)k/2\rfloor}$. If two consecutive coefficients differ or are not equal to 0 or $y-1$, we may perform another such jump. As long as we do not find $\lfloor(\lambda-1)k/3\rfloor$ identical, consecutive coefficients, we are in no danger of violating (9.4). Carrying out this procedure, we verify the desired inequalities for all values of y and k up to $k_0(y)$, with the noted exceptions, in under two hours of CPU time (on an Ultrasparc 10).

Let us work out the details in case $y = 2$. Applying Theorem 1.5 with $a = 1$, $\Delta = 7$, $m_0 = 15$, (noting that $181^2 + 7 = 2^{15}$) and $\alpha = 3.4$, we find that

$$\chi_1 > 1.157, \quad \chi_2 < 8.557 \times 10^{26}, \quad \chi_3 < 1.363 \times 10^{18}, \quad c_2 > 2.045 \times 10^{-57},$$

$m_2 < 34640$ and $\lambda_1 = 1.476487\ldots$. It follows, if p is an integer and $q = 2^k$ for k a non-negative integer, that

$$\left|\sqrt{2} - \frac{p}{q}\right| > q^{-1.48},$$

provided $k \geq k_0(2) = 53620$.

To check the values of k below this bound, we compute the binary expansion of $\sqrt{2}$ to, say, 55000 binary digits. To do this, we use Newton's method to derive a rational x such that

$$|\sqrt{2} - x| \leq 10^{-20480} < 2^{-1.24\times 55000}.$$

Computing the digits a_n in the binary expansion to x for $0 \leq n \leq 1000$, we find 65 strings of consecutive zeros or ones, of length at least 3. Since the longest of these has length 8, we conclude that if $k < 1000$ is such that

$$\left|\sqrt{2} - \frac{p}{2^k}\right| \leq 2^{-1.48k},$$

then

$$\lfloor 1.48k \rfloor - (k+1) + 1 \leq 8 \Rightarrow k \leq 18.$$

Using brute force, we check the remaining $p/2^k$ with $k \leq 18$ and find that $3/2$ and $181/2^7$ are the only exceptions to inequality (9.4) for $k < 1000$. Examining the binary expansion of x, we find that $a_{1000} = 0$ and $a_{1001} = 1$. Since these are distinct, Lemma 9.1 enables us to look ahead in the expansion to $a_{1240} = 0$. Since $a_{1241} = a_{1242} = 0$, but $a_{1243} = 1$, we may jump again to consideration of $a_{1537} = 1$. The fact that $a_{1538} = 0$ allows us to skip still further ahead in the binary expansion. We iterate this process, performing a total of 19 jumps, thus verifying inequality (9.4) for all $k < k_0(2)$, except for $k \in \{1, 7\}$. This completes the proof of Corollary 1.6 in case $y = 2$. The other values of y follow in a similar fashion.

The computations corresponding to $y = 2$ are, in a certain sense, a worst case scenario as they always require calculating at least two consecutive coefficients in the binary expansion of $\sqrt{2}$. As y gets larger, this technique becomes rather more efficient, since there are more residue classes in which a_n can lie, and hence it is less likely that a given coefficient is 0 or $y - 1$.

10. Proof of Corollary 1.7

Suppose that D is a nonzero integer and that $x^2 + D = y^n$ for some positive integers x and n where y is an integer in Table (1.18). If n is even, say $n = 2k$, then

$$|D| = |x^2 - y^n| \geq y^{2k} - (y^k - 1)^2 = 2y^k - 1 > y^k$$

and so

$$n = 2k < 2\frac{\log |D|}{\log y}.$$

If, however, $n = 2k + 1$ for $k > 2$ and

$$(y, k) \notin \{(2, 3), (2, 7), (2, 8), (3, 7)\},$$

$$|D| = |x^2 - y^{2k+1}| = y^{2k}\left(\sqrt{y} + \frac{x}{y^k}\right)\left|\sqrt{y} - \frac{x}{y^k}\right|$$

and so

$$\left|\sqrt{y} - \frac{x}{y^k}\right| = \frac{|D|}{y^{2k}\left(\sqrt{y} + \frac{x}{y^k}\right)}.$$

Applying Corollary 1.6, we find that

$$|D| > y^{(2-\lambda_2(y))k}\left(\sqrt{y} + \frac{x}{y^x}\right),$$

i.e.

$$y^{2k}\left(\sqrt{y}+\frac{x}{y^k}\right)^{\frac{2}{2-\lambda_2(y)}} < |D|^{\frac{2}{2-\lambda_2(y)}}.$$

Since $1 < \lambda_2(y) < 2$, we have $(\sqrt{y}+\frac{x}{y^k})^{\frac{2}{2-\lambda_2(y)}} > y$ and so $y^n < |D|^{\frac{2}{2-\lambda_2(y)}}$, which yields the desired result. On the other hand, if $n = 3$ or 5, or if (y, n) is one of (2, 7), (2, 15), (2, 17) or (3, 15), it is easy to check that, for the values of y under consideration, the only triples (y, n, D) contradicting the inequality

$$n < \frac{2}{2-\lambda_2(y)}\frac{\log|D|}{\log y}$$

are given by

$$(y, n, D) \in \{(2, 3, -1), (2, 15, 7), (5, 3, 4), (5, 5, -11), (23, 5, -26)\\ (40, 3, -9), (46, 3, -8), (55, 5, 19), (76, 5, 60)\}.$$

This completes the proof of Corollary 1.7.

11. The equation $x^2 - D = p^n$ with D positive

In this section, we will deal with the Diophantine equation

$$x^2 - D = p^n, \tag{11.1}$$

where p is an odd rational prime and D is a positive integer. Specifically, we will prove Theorem 1.11. If D is square, then, as noted by Beukers [11], factorization of the right hand side of (11.1) leads, almost immediately, to the conclusion that the equation possesses at most two solutions in positive integers x and n. We will therefore assume, here and henceforth, that D is a positive, nonsquare integer, coprime to p (this last is a technical condition, imposed for simplicity). Treatment of Eq. (11.1), in contrast to the analogous equation with $D < 0$, is complicated by the presence of infinite units in $\mathbb{Q}(\sqrt{D})$. We will have use of the following lemma of Le [19].

Lemma 11.1. *Let D be a positive nonsquare integer and p be a positive prime, coprime to D. Suppose that $u_1 + v_1\sqrt{D}$ is the fundamental solution to the equation*

$$u^2 - Dv^2 = 1. \tag{11.2}$$

If the equation

$$X^2 - DY^2 = p^Z, \quad \gcd(X, Y) = 1, \quad Z > 0 \tag{11.3}$$

has a solution in positive integers (X, Y, Z), then it has a unique positive solution (X_1, Y_1, Z_1) satisfying

$$Z_1 \le Z, \quad 1 < \frac{X_1 + Y_1\sqrt{D}}{X_1 - Y_1\sqrt{D}} < (u_1 + v_1\sqrt{D})^2,$$

where Z runs over all solutions in positive integers (X, Y, Z) of (11.3). *Further, every positive solution (X, Y, Z) of* (11.3) *may be written as*

$$Z = Z_1 t,\ X + Y\sqrt{D} = (X_1 \pm Y_1\sqrt{D})^t(u + v\sqrt{D})$$

where $t \in \mathbb{N}$ and (u, v) is an integral solution of (11.2).

Let us write $\theta = u_1 + v_1\sqrt{D}$ and $\sigma = X_1 + Y_1\sqrt{D}$, for u_1, v_1, X_1 and Y_1 the positive integers whose existence is guaranteed by the previous lemma. Suppose that (A, m) is a solution in positive integers to Eq. (11.1). Arguing as in the proofs of Lemma 4 of Beukers [11] and Lemma 4 of Le [19], we have

$$A \pm \sqrt{D} = \bar{\theta}^s \sigma^t, \tag{11.4}$$

where $m = tZ_1$ for Z_1 as defined in Lemma 11.1, s and t integers with $0 \leq s \leq t$, and $\gcd(s, t) = 1$. Conjugating (11.4) in $\mathbb{Q}(\sqrt{D})$, we find that

$$|\bar{\theta}^s\sigma^t - \theta^s\bar{\sigma}^t| = 2\sqrt{D}$$

and so

$$|(\bar{\sigma}/\sigma)^t(\theta/\bar{\theta})^s - 1| = \frac{2\sqrt{D}}{|A \pm \sqrt{D}|}. \tag{11.5}$$

This last equation will prove crucial in the proof of Theorem 1.11. It leads to a linear form in logarithms of algebraic numbers, to which we can apply lower bounds from transcendental number theory. Initially, we will use (11.5) to prove a gap principle for solutions to (11.1); i.e. a result that ensures that two suitably large solutions cannot lie too close together.

Lemma 11.2. *Suppose that D is a nonsquare, positive integer and p is a rational prime, coprime to D. If (A_1, m_1) and (A_2, m_2) are solutions to Eq.* (11.1) *in positive integers with $m_2 > 2m_1$ and $p^{m_1} > (k^2 - 1)D$, where $k \geq 5$, then it follows that*

$$m_2 > Z_1 \log\theta \left(\frac{2p}{2p+1}\right)\left(\frac{k-1}{k+1}\right)^{3/2}\left(\frac{p^{m_1}}{D}\right)^{1/2}.$$

Proof: We will closely follow the proof of Lemma 4 of Beukers [11]. Writing

$$A_i \pm \sqrt{D} = \bar{\theta}^{s_i}\sigma^{t_i},$$

we have, under our hypotheses, that

$$|A_i \pm \sqrt{D}| \geq |A_i| - \sqrt{D} \geq \sqrt{p^{m_i} + D} - \sqrt{D} > \sqrt{\frac{k-1}{k+1}}\, p^{m_i/2},$$

and thus, from (11.5),

$$|(\bar{\sigma}/\sigma)^{t_i}(\theta/\bar{\theta})^{s_i} - 1| < 2\sqrt{\frac{k+1}{k-1}}\left(\frac{D}{p^{m_i}}\right)^{1/2}.$$

Now, it is well known, if $|\delta| < 1/2$, that

$$|\log(1-\delta)| < |\delta|(1+|\delta|)$$

and so, since $k \geq 5$ and $\theta/\bar{\theta} = \theta^2$, we conclude that

$$|t_i \log(\sigma/\bar{\sigma}) - 2s_i \log\theta| < 2\left(\frac{k+1}{k-1}\right)^{3/2}\left(\frac{D}{p^{m_i}}\right)^{1/2}. \tag{11.6}$$

Arguing as in the proof of Lemma 4 of Beukers [11], $s_1/t_1 \neq s_2/t_2$ and hence, eliminating $\log(\sigma/\bar{\sigma})$ from the inequalities in (11.6), we find that

$$\frac{1}{t_1 t_2} \leq \left|\frac{s_2}{t_2} - \frac{s_1}{t_1}\right| < \frac{1}{t_1 \log\theta}\left(\frac{k+1}{k-1}\right)^{3/2}\left(\frac{D}{p^{m_1}}\right)^{1/2}\left(1 + \frac{t_1}{t_2} p^{(\frac{t_1-t_2}{2})}\right).$$

Since $m_2 > 2m_1$, it follows that $t_2 > 2t_1$ and $t_2 \geq t_1 + 2$, whereby

$$1 + \frac{t_1}{t_2} p^{(\frac{t_1-t_2}{2})} < 1 + \frac{1}{2p}.$$

This yields the desired result. □

A second gap principle is the following:

Lemma 11.3. *Suppose that D is a nonsquare, positive integer and p is a rational prime, coprime to D. If (x_1, n_1), (x_2, n_2) and (x_3, n_3) are three solutions in positive integers to Eq.* (11.1), *with $n_1 < n_2 < n_3$, then $n_3 = 2n_2 + r$ where r is an odd positive integer. Further, if $r = 1$, then (p, D) is an exceptional pair, as defined in Section* 1. *If $r > 1$, then*

$$r \geq \begin{cases} \max\left\{n_1, \dfrac{2n_2-1}{3}\right\} & \text{if } p = 3 \\ \max\left\{n_1, \dfrac{2n_2+1}{3}\right\} & \text{if } p > 3. \end{cases} \tag{11.7}$$

Proof: This is a minor sharpening (in case $r > 1$ and $p > 3$) of Lemma 5 of Beukers [11]. In the penultimate displayed equation in the proof of that lemma, we find, for $n_3 = 2n_2 + r$, where r is an odd positive integer with $r > 1$, that

$$p^{2n_2} < p^{3r} \cdot 4(1 + p^{-r/2})^6$$

and that there exists a positive integer d such that both

$$|2d - p^{r/2}| < 0.29 \quad \text{and} \quad p^{n_2+r} \equiv 1 \pmod{4d}. \tag{11.8}$$

Now $4(1+p^{-r/2})^6 < p$ provided $p \geq 7$ (if $r = 3$) or $p \geq 5$ (if $r > 3$). It follows that either $p = 3$, both $p = 5$ and $r = 3$, or $p^{2n_2} < p^{3r+1}$, whence $2n_2 \leq 3r$. In the last case, since r is odd, necessarily $2n_2 \leq 3r - 1$, which leads to the stated conclusion. If $p = 5$ and $r = 3$, the first inequality in (11.8) is not satisfied for integral d and so the lower bound for r holds, as advertised. □

Let us suppose, here and henceforth, that we have four distinct solutions in positive integers x and n to Eq. (11.1), say (x_i, n_i) for $1 \leq i \leq 4$, where $n_1 < n_2 < n_3 < n_4$.

11.1. Exceptional pairs (p, D)

We begin by proving Theorem 1.11 in the case of exceptional pairs (p, D). In this situation, we will not require any lower bounds for linear forms in logarithms, but will instead rely upon Theorem 1.5 and various gap principles. To start, assume that $p = 4a^2 + 1$ for some integer $a \geq 5$; we will treat $p = 3, 5, 17$ and 37 later. We apply Theorem 1.5 with

$$y = p, \Delta = \Delta_0 = \Delta_1 = a = m_0 = 1, \quad \Omega = \Omega_1 = 4p$$

and $\alpha = 5$. It follows that

$$\chi_1 > \frac{1}{466} pF_p,$$

where $F_p = F(r(5, 1/p), 5, 1/p)$. Since we may readily show, by calculus, that F_p is increasing in p,

$$14.806\ldots = F_{101} \leq F_p < 6\,e = 16.309\ldots,$$

and so $\chi_1 > 0.031p$. Similarly,

$$\chi_2 < 2.152 \times 10^{16} p^{7.5},$$

whence

$$m_2 < 8\frac{\log(2.152 \times 10^{16} p^{7.5})}{\log(0.031p)} + 1.$$

The right hand side of this last expression is monotone decreasing in p for $p \geq 101$ and hence we may conclude that $m_2 < 508$, if $p \geq 101$. Next, note that

$$\chi_3 < \frac{(4p)^5 6\,e}{2.202} < 7585p^5$$

and so

$$\lambda_1 < \frac{\log(7585p^5)}{4\log p} < 1.734,$$

where the last inequality is a consequence of $p \geq 101$. Since

$$c_2^{-1} < 7.173 \times 10^{15} p^{1/2} \chi_3^{19/8} < 1.177 \times 10^{25} p^{99/8},$$

choosing $\lambda_2 = 1.8$, we have

$$\frac{\log c_2}{(\lambda_1 - \lambda_2)\log y} < \frac{\log(1.177 \times 10^{25} p^{99/8})}{0.066 \log p} < 378,$$

where, again, the last bound follows from $p \geq 101$. Defining

$$k_0 = \max\left\{\frac{m_2 - 1}{2}, \frac{\log c_2}{(\lambda_1 - \lambda_2)\log y}\right\},$$

we thus have $k_0 < 378$, if $p \geq 101$. If $k \geq k_0$, arguing as in the proof of Corollary 1.6,

$$\left|\sqrt{p} - \frac{x}{p^k}\right| > p^{-1.8k},$$

for any integer x and so, as in the proof of Corollary 1.7, we may conclude that any solution (x, n) in positive integers to the equation $x^2 + D = p^n$ (where $D \neq 0$) satisfies

$$n < 10\frac{\log|D|}{\log p}, \tag{11.9}$$

provided $p = 4a^2 + 1 \geq 101$ and $n > 757$.

Since we suppose that (p, D) is exceptional, we have

$$D = \left(\frac{p^m - 1}{4a}\right)^2 - p^m < \frac{p^{2m}}{4(p-1)}$$

and so, from $n_3 = 2m + 1$,

$$\frac{p^{n_3}}{D} > 4p(p-1) = (2p-1)^2 - 1.$$

Applying Lemma 11.2 with $k = 2p - 1$, we thus have

$$n_4 > \frac{4(p-1)^2}{2p+1}\log\theta. \tag{11.10}$$

Now D is minimal for $m = 2$ and $p = 101$ and so $D \geq 249899$, whence $\log\theta > \log(2\sqrt{D}) > 6.9$. Inequality (11.10) thus implies that $n_4 > 1359$. Also, $\log\theta > \log(2\sqrt{D}) > \frac{1}{2}\log D$ and so

$$n_4 > \frac{2(p-1)^2}{2p+1}\log D. \tag{11.11}$$

In combination with (11.9) (taking $n = n_4$), this contradicts $p \geq 101$.

Let us next suppose that $p = 5$, 17 or 37. In these cases, we apply Corollary 1.7. Since $n_4 > n_3 \geq 2m + 1 \geq 5$, in each instance, we have $n_4 < c\log D$, where we may take

$c = 1.95$, 11.77 or 1.24, if $p = 5$, 17 or 37, respectively. Arguing as previously, we once again obtain inequality (11.11) and hence another contradiction.

Finally, if $p=3$, we require a slightly stronger gap principle than that provided by Lemmata 11.2 and 11.3. The following is a combination of Assertions 2 and 3 (restricted to the case $p=3$) of Le [29]:

Lemma 11.4. *Suppose that $m > 1$ is an odd positive integer and $D = (\frac{3^m+1}{4})^2 - 3^m$. If the Diophantine equation $x^2 - D = 3^n$ has a solution in positive integers (x_4, n_4) with $n_4 > 2m+1$, then there exist positive integers k_1 and k_2 such that*

$$n_4 = mk_1 + (2m+1)k_2 \quad \textit{and} \quad k_1 + k_2 \geq 2 \cdot 3^{m-1} + 1.$$

Applying this lemma, we find that

$$n_4 \geq 2 \cdot 3^{m-1}m + 2m + 1,$$

while, from Corollary 1.7,

$$n_4 < 5.21 \log D = 5.21 \log\left(\left(\frac{3^m+1}{4}\right)^2 - 3^m\right).$$

Taken together, these two inequalities contradict $m \geq 3$, completing the proof of Theorem 1.11, in case (p, D) is an exceptional pair.

11.2. Nonexceptional pairs (p, D)

Let us now suppose that (p, D) is not an exceptional pair. In this situation, we will use Eq. (11.5), with s and t corresponding to a putative fourth solution (x_4, n_4) to (11.1). In this manner, we will deduce the existence of a small linear form in logarithms of algebraic numbers. Before we carry this out, however, we state a trio of technical lemmata which, in the first two instances, will simplify our computations. The third will provide, via the p-adic hypergeometric method, an "anti-gap" principle to use in conjunction with Lemma 11.2. We have

Lemma 11.5. *Suppose that D is a nonsquare, positive integer and p is a rational prime, coprime to D. If (x_1, n_1), (x_2, n_2) and (x_3, n_3) are three solutions in positive integers to Eq. (11.1), with $n_1 < n_2 < n_3$. If $r = n_3 - 2n_2 > 1$, then $p^r > 10^{27}$. Further, if $3 \leq p < 10^6$, we have $p^r > 10^{54}$.*

Proof: This is a routine if not especially short computation, following Lemma 6 of Beukers [11]. For each prime p with $3 \leq p < 10^9$ and each odd integer $r \geq 3$, with

$$p < \begin{cases} 10^{54/r} & \text{if } 3 \leq p < 10^6 \\ 10^{27/r} & \text{if } 10^6 < p < 10^9, \end{cases}$$

we check to see if (11.8) is satisfied, noting that, by Lemma 11.3, $2 \leq n_2 \leq \frac{3r\pm1}{2}$. Here, the sign depends on whether $p = 3$ or otherwise. If we denote by $\pi(x)$ the number of primes

$p \leq x$, there are precisely

$$\pi(10^9) + 3\pi(10^6) - 4 + \sum_{k=5}^{56} \left(\pi\left(10^{54/(2k+1)}\right) - 1\right) = 51093638$$

such pairs (r, p) to be considered. We perform this calculation using Maple V (being careful to remind Maple that neither 1093^2 nor 3511^2 is prime!) and verify our results with Pari GP. The only quadruples (p, r, n_2, d) we find, satisfying (11.7) and (11.8), are in the set

$$\{(29, 3, 3, 78), (47, 3, 3, 161), (439, 3, 3, 4599), (443, 3, 3, 4662), (5, 5, 7, 28)\}.$$

Arguing as in Lemma 5 of Beukers [11], we have

$$x_2 = \left| \frac{p^{n_2+r} - 1}{4d} - dp^{n_2} \right|,$$

i.e. for the five cases in question,

$$x_2 = 4143, 22409, 6047779, 6205217 \text{ and } 7673,$$

respectively. In each instance, we may check that the equation

$$x_2^2 - x_1^2 = p^{n_2} - p^{n_1}$$

has no solution in positive integers $x_1 < x_2$ and $n_1 < n_2$. This completes the proof of Lemma 11.5. $\square$

We will later have use of an upper bound for the quantity θ defined after Lemma 11.1.

Lemma 11.6. *Suppose that D is a nonsquare, positive integer and p is a rational prime, coprime to D. Suppose that Eq.* (11.1) *has two solutions in positive integers* (A_1, m_1) *and* (A_2, m_2), *with*

$$p^{m_1} < p^{m_2} \leq D^{4/5},$$

where $D \geq 3^8$. Then, we may conclude that

$$\log\theta < \frac{(\log D)^2}{Z_1 \log p}.$$

Proof: Writing $m_i = t_i Z_1$, we have $A_i \pm \sqrt{D} = \sigma^{t_i}\bar{\theta}^{s_i}$, where $0 \leq s_i \leq t_i$ are integers. It follows that

$$|t_2 \log(A_1 \pm \sqrt{D}) - t_1 \log(A_2 \pm \sqrt{D})| = |s_2 t_1 - s_1 t_2| \log\theta \geq \log\theta, \tag{11.12}$$

since $s_1/t_1 \neq s_2/t_2$ (again, from the proof of Lemma 4 of [11]). On the other hand,

$$|t_2 \log(A_1 \pm \sqrt{D}) - t_1 \log(A_2 \pm \sqrt{D})| \leq t_2 \log(A_1 + \sqrt{D}) + t_1 \log(A_2 + \sqrt{D}). \tag{11.13}$$

Since $p^{m_i} \leq D^{4/5}$, we have $t_i \leq \frac{4}{5} \frac{\log D}{Z_1 \log p}$, while

$$A_i + \sqrt{D} = \frac{p^{m_i}}{A_i - \sqrt{D}} \leq \frac{D^{4/5}}{A_i - \sqrt{D}}$$

implies (crudely!) that $A_i + \sqrt{D} < 3\sqrt{D}$. It follows, from (11.12) and (11.13), that

$$\log \theta < \frac{8 \log(D) \log(3\sqrt{D})}{5 Z_1 \log p}.$$

Since $D \geq 3^8$, $\log(3\sqrt{D}) \leq \frac{5}{8} \log D$ and we conclude as stated. □

The next lemma is a (very) slight modification of Theorem 1 of Beukers [11].

Lemma 11.7. *Let $D > 220$ be a nonsquare integer and p be an odd rational prime, coprime to D. If Eq.* (11.1) *has two solutions in positive integers* (A_1, m_1) *and* (A_2, m_2), *with $m_2 > 2m_1$, then*

$$p^{m_1} < 160 D^2.$$

Proof: We note that the proof of Theorem 1 of Beukers [11] depends upon upper bounds for $|P_{n_1,n_2}(x)|$, $|Q_{n_1,n_2}(x)|$ and $|I_{n_1,n_2}(x)|$, in case x is large in modulus. It follows that we cannot apply Lemmata 3.1 and 4.1 directly. While it is still possible to sharpen the upper bounds in [11], through consideration of nonarchimedean contributions, we have no need to do so. Following Beukers, we write

$$\xi = A_1 (4D)^{n_2} Q_{n_1,n_2}(-p^{m_1}/D) \quad \text{and} \quad \eta = (4D)^{n_2} P_{n_1,n_2}(-p^{m_1}/D),$$

and notice that ξ and η are integers, satisfying

$$\|\xi - \eta\sqrt{D}\|_p \leq p^{-m_1(n_1+n_2+1)},$$
$$|\xi| < 4^{n_2+1} p^{n_2 m_1} (D + p^{m_1})^{1/2} \tag{11.14}$$

and

$$|\eta| < 2^{2n_1+n_2} p^{n_1 m_1} \left(\frac{2D}{p^{m_1}} + 1 \right)^{n_1} (4D)^{n_2 - n_1}. \tag{11.15}$$

Here, $\|\cdot\|_p$ denotes the usual p-adic norm. The last two inequalities are valid provided $n_2 > 2n_1$. If, further, $p^{m_1} \geq 160 D^2$, we may apply Lemma 11.2 with $k = 4\sqrt{10D}$ to conclude, since $\theta > 2\sqrt{D}$, that

$$m_2 > 0.4 \log(\theta^2) \left(\frac{p^{m_1}}{D} \right)^{1/2} \geq \frac{0.8 \log(3) m_1 \log(4D)}{\log(p^{m_1})} \left(\frac{p^{m_1}}{4D} \right)^{1/2}.$$

From $p^{m_1} \geq 160 D^2$ and $D > 220$, we thus have

$$\frac{\log(4D)}{\log(p^{m_1})} \left(\frac{p^{m_1}}{4D} \right)^{1/2} > 40$$

and so $m_2 > 35m_1$. We now choose positive integers n_1 and n_2 such that

$$m_1(n_1 + n_2) \leq m_2 < m_1(n_1 + n_2 + 1),$$
$$n_2 - 9 \leq 7n_1 \leq n_2 + 6$$

and $\xi - \eta A_2 \neq 0$. The first of these guarantees (together with $m_2 > 35m_1$) that $n_1 + n_2 \geq 35$; the last is possible by Lemma 2 of [11], since, for a fixed value of $n_1 + n_2$, the inequality $n_2 - 9 \leq 7n_1 \leq n_2 + 6$ affords precisely two choices for n_1. From the argument preceding displayed Eq. (10) of [11], we have

$$|\xi| + |\eta A_2| \geq p^{m_2}.$$

On the other hand, since $p^{m_1} \geq 160D^2$ and $D > 220$, (11.14) and (11.15) imply that

$$|\xi| + |\eta A_2| < 4.1 \cdot 4^{n_2} p^{(n_2+1/2)m_1} + 4.1^{n_1} 2^{n_2} p^{n_1 m_1} (4D)^{n_2 - n_1} \sqrt{D + p^{m_2}}.$$

Combining these inequalities, either

$$4.1 \cdot 4^{n_2} p^{(n_2+1/2)m_1} > \frac{1}{2} p^{m_2} \geq p^{m_1(n_1+n_2)},$$

or

$$1.05 \cdot 4.1^{n_1} 2^{n_2} p^{n_1 m_1 + m_2/2} (4D)^{n_2 - n_1} > \frac{1}{2} p^{m_2} \geq p^{m_1(n_1+n_2)}.$$

In the first case, we have

$$p^{(n_1-1/2)m_1} < 8.2 \cdot 4^{n_2},$$

while the second yields

$$p^{\frac{1}{2} m_1 (n_2 - n_1)} < 2.1 \cdot 4.1^{n_1} 2^{n_2} (4D)^{n_2 - n_1}.$$

We thus have

$$p^{m_1} < \max\left\{ 8.2^{\frac{1}{n_1 - 1/2}} 2^{\frac{2n_2}{n_1 - 1/2}}, 2.1^{\frac{2}{n_2 - n_1}} 4.1^{\frac{2n_1}{n_2 - n_1}} 2^{\frac{2n_2}{n_2 - n_1}} (4D)^2 \right\}. \tag{11.16}$$

Since $n_1 + n_2 \geq 35$ and $n_2 - 9 \leq 7n_1 \leq n_2 + 6$, it is readily checked that $n_1 \geq 4$, $n_2 - n_1 \geq 25$, $n_1/(n_2 - n_1) \leq 1/5$ and $n_2/(n_2 - n_1) \leq 6/5$ (all corresponding to $n_1 = 5$ and $n_2 = 30$). We thus have

$$8.2^{\frac{1}{n_1 - 1/2}} 2^{\frac{2n_2}{n_1 - 1/2}} \leq 8.2^{\frac{1}{3.5}} 2^{\frac{2.31}{3.5}} < 4 \times 10^5$$

and

$$2.1^{\frac{2}{n_2 - n_1}} 4.1^{\frac{2n_1}{n_2 - n_1}} 2^{\frac{2n_2}{n_2 - n_1}} \leq 2.1^{\frac{2}{25}} 4.1^{\frac{2}{5}} 2^{\frac{12}{5}} < 9.85.$$

Since $D > 220$, we thus have $p^{m_1} < 160D^2$, as claimed. $\square$

From (11.4) and (11.5), we can find integers s_4 and t_4 with $0 \leq s_4 \leq t_4$ and $n_4 = t_4 Z_1$, so that

$$|(\bar{\sigma}/\sigma)^{t_4}(\theta/\bar{\theta})^{s_4} - 1| = \frac{2\sqrt{D}}{|x_4 \pm \sqrt{D}|}. \tag{11.17}$$

Defining

$$\Lambda = |t_4 \log(\sigma/\bar{\sigma}) - 2s_4 \log \theta|,$$

we will use inequality (11.6) to show that Λ is "small". On the other hand, we may apply the following corollary to Theorem 2 of Mignotte [36], here, $h(\alpha)$ denotes the absolute logarithmic Weil height of α, defined, for algebraic α, by

$$h(\alpha) = \frac{1}{[\mathbb{Q}(\alpha) : \mathbb{Q}]}\left(\log a_0 + \log \prod_{\sigma} \max\{1, |\sigma(\alpha)|\}\right),$$

where σ runs over the embeddings of $\mathbb{Q}(\alpha)$ into $\mathbb{C}$ and $a_0 > 0$ is the leading term in the minimal polynomial for α over $\mathbb{Z}$.

Lemma 11.8. *Consider the linear form*

$$\Lambda = b_2 \log \alpha_2 - b_1 \log \alpha_1$$

where b_1 and b_2 are positive integers and α_1, α_2 are nonzero, multiplicatively independent algebraic numbers. Set

$$D = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}]/[\mathbb{R}(\alpha_1, \alpha_2) : \mathbb{R}]$$

and let ρ, λ, a_1 and a_2 be positive real numbers with $\rho \geq 4$, $\lambda = \log \rho$,

$$a_i \geq \max\{1, \rho|\log\alpha_i| - \log|\alpha_i| + 2Dh(\alpha_i)\} \quad (1 \leq i \leq 2)$$

and

$$a_1 a_2 \geq \max\{20, 4\lambda^2\}.$$

Further suppose h is a real number with

$$h \geq \max\left\{3.5, 1.5\lambda, D\left(\log\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right) + \log \lambda + 1.377\right) + 0.023\right\},$$

$\chi = h/\lambda$ and $\upsilon = 4\chi + 4 + 1/\chi$. We may conclude, then, that

$$\log|\Lambda| \geq -(C_0 + 0.06)(\lambda + h)^2 a_1 a_2,$$

where

$$C_0 = \frac{1}{\lambda^3}\left\{\left(2 + \frac{1}{2\chi(\chi+1)}\right)\left(\frac{1}{3} + \sqrt{\frac{1}{9} + \frac{4\lambda}{3\upsilon}\left(\frac{1}{a_1} + \frac{1}{a_2}\right) + \frac{32\sqrt{2}(1+\chi)^{3/2}}{3\upsilon^2\sqrt{a_1 a_2}}}\right)\right\}^2.$$

Since

$$p^{n_2} > x_2^2 - x_1^2 \geq 4x_1 > 4\sqrt{D} \tag{11.18}$$

and, via Lemma 11.5, $p^r > 10^{27}$, we have

$$p^{n_3} = p^{2n_2+r} > 1.6 \times 10^{28} D > 160 D^2,$$

provided $D < 10^{26}$. It follows, from Lemma 11.7, that we may assume, henceforth, that $D \geq 10^{26}$. As noted in Le [29], $\sigma/\bar{\sigma}$ is a root of the polynomial

$$p^{Z_1} x^2 - 2\left(X_1^2 + DY_1^2\right) x + p^{Z_1},$$

while θ satisfies $\theta^2 - 2u_1\theta + 1 = 0$. We thus have $h(\sigma/\bar{\sigma}) = \log \sigma$ and $h(\theta) = \frac{1}{2}\log\theta$. Further, $\sigma/\bar{\sigma} < \theta^2$, by Lemma 11.1, and so

$$\sigma^2 < \sigma\bar{\sigma}\theta^2 = p^{Z_1}\theta^2,$$

whereby $\sigma < p^{Z_1/2}\theta$. We will apply Lemma 11.8, taking

$$\alpha_1 = \theta, \quad \alpha_2 = \sigma/\bar{\sigma}, \quad b_1 = 2s_4, b_2 = t_4, \quad \rho = 5, \quad a_1 = 6\log\theta,$$

and

$$a_2 = 12\log\theta + 2Z_1 \log p,$$

a valid choice by the above upper bounds for σ and $\sigma/\bar{\sigma}$. Since $s_4 \leq t_4$, we have

$$\log\left(\frac{b_1}{a_2} + \frac{b_2}{a_1}\right) < \log\left(\frac{t_4}{3\log\theta}\right).$$

From Lemma 11.3 and (11.18),

$$p^{n_3} = p^{2n_2+r} \geq 3^{-\frac{1}{3}} p^{\frac{8}{3}n_2} > 3^{-1/3}(4\sqrt{D})^{8/3},$$

and so, from $D > 10^{26}$ and $p \geq 3$, we may take $k = 10^5$ in Lemma 11.2 to conclude that

$$t_4 > 4.53 D^{1/6} \log\theta. \tag{11.19}$$

It follows that $t_4 > 9.75 \times 10^4 \log\theta$ and hence we may take

$$h = 2\left(\log\left(\frac{t_4}{\log\theta}\right) + 1.58\right) - \log 5$$

in Lemma 11.8, whereby $h > 24$. Since

$$a_1 > 6\log(2\sqrt{D}) > 6\log(2 \times 10^{13}) = 183.76\ldots$$

and $a_2 > 2a_1$, we may readily compute that $C_0 < 0.43$. Applying Lemma 11.8, it follows that

$$\log \Lambda > -141.12\left(\log\left(\frac{t_4}{\log\theta}\right) + 1.58\right)^2 \log\theta\left(\log\theta + \frac{1}{6}Z_1 \log p\right).$$

From (11.6), since we may take $k = 10^5$,

$$\log \Lambda < \log(2.1\sqrt{D}) - \frac{t_4 Z_1}{2}\log p.$$

Combining these two inequalities and dividing by $\frac{1}{2}Z_1 \log p \log\theta$, we find that

$$\frac{t_4}{\log\theta} < \frac{2\log(2.1\sqrt{D})}{Z_1 \log p \log\theta} + 282.24\left(\log\left(\frac{t_4}{\log\theta}\right) + 1.58\right)^2\left(\frac{\log\theta}{Z_1 \log p} + \frac{1}{6}\right).$$

Since $\theta > 2\sqrt{D}$, $D > 10^{26}$ and $p \geq 3$, we have

$$\frac{2\log(2.1\sqrt{D})}{Z_1 \log p \log\theta} < 1.83,$$

which, together with $t_4 > 9.75 \times 10^4 \log\theta$, implies that

$$\frac{t_4/\log\theta}{\left(\log\left(\frac{t_4}{\log\theta}\right) + 1.58\right)^2} < \frac{282.24\log\theta}{Z_1 \log p} = 47.06. \tag{11.20}$$

We will finish the proof of Theorem 1.11 by considering two cases. First; let us suppose that $p > 10^6$. From $p > 3$, Lemma 11.3 and (11.18),

$$p^{n_3} = p^{2n_2+r} \geq p^{\frac{8}{3}n_2+\frac{1}{3}} > (4\sqrt{D})^{8/3}p^{1/3}$$

and so, with $D > 10^{26}$ and $p > 10^6$, we may choose $k = 10^6$ in Lemma 11.2 to conclude that

$$t_4 > 0.992^{8/3}p^{1/6}D^{1/6}\log\theta > 62.86D^{1/6}\log\theta. \tag{11.21}$$

Applying inequality (11.21) and Lemma 11.6 to (11.20), it follows that

$$\frac{D^{1/6}}{(\log(62.86D^{1/6}) + 1.58)^2} < \frac{4.49\log^2 D}{\log^2(10^6)} + 0.75,$$

contradicting $D > 10^{26}$.

If, on the other hand, $3 \leq p < 10^6$, we may suppose from Lemmata 11.5 and 11.7, in conjuction with (11.18), that $D > 10^{53}$. From (11.19) and (11.20), we conclude that

$$\frac{D^{1/6}}{(\log(4.53D^{1/6}) + 1.58)^2} < \frac{62.31\log^2 D}{\log^2 3} + 10.39,$$

again contradicting our lower bound upon D.

12. Concluding remarks

The techniques of this paper may be generalized to handle a wide variety of Diophantine equations of the shape

$$f(x) = y^n, \tag{12.1}$$

where $f(x)$ is a fixed polynomial with integer coefficients and at least two distinct roots (over $\mathbb{C}$) and $y > 1$ is a fixed integer. In the simplest case generalizing (1.19), where $f(x)$ is a monic quadratic with distinct roots, we may apply either Theorem 1.3 or Theorem 1.5 with $s = 1$ or 4. For more general polynomials, we require more than a single "good" approximation to obtain analogous results; indeed, for a fixed y, it may be necessary to have as many as $\deg f(x)$ triples (x_0, a, m_0) with

$$\left| f(x_0) - a^{\deg f(x)} y^{m_0} \right|$$

suitably small, in order to completely solve Eq. (12.1).

As mentioned at the end of our Introduction, one would like to extend Theorem 1.11 to characterize those pairs (p, D) for which Eq. (11.1) has exactly three positive solutions (to parallel Theorem 1.9). Besides its intrinsic interest, such a result would enable us to remove the technical condition in Theorem 1.11 that p and D are coprime. Along these lines, the following is an easy consequence of Theorem 1.9:

Theorem 12.1. *Let D be a positive integer and p be an odd prime. Then the Diophantine equation*

$$x^2 + D = p^n$$

has at most one solution in positive integers x and n, unless $(p, D) = (3, 2 \times 3^{2j})$ or $(p, D) = (4a^2 + 1, (3a^2 + 1)(4a^2 + 1)^{2j})$ for some positive integer a and nonnegative integer j. In these cases, there are precisely two such solutions.

To see this, note that if p is a rational prime and D is a positive integer multiple of p for which the equation $x^2 + D = p^n$ has two solutions in positive integers (x_1, n_1) and (x_2, n_2), with $n_2 > n_1$, then, if $\mathrm{ord}_p D = l$, we have, from $p^{n_1} > D \geq p^l$, that $n_1 \geq l + 1$. It follows from $x_1^2 + D = p^{n_1}$ that l is necessarily even, say $l = 2l_1$, whence

$$(x_i/p^{l_1})^2 + (D/p^{2l_1}) = p^{n_i - 2l_1} \quad \text{for } i = 1, 2.$$

Since $n_2 > n_1 > 2l_1$ and p is coprime to D/p^{2l_1}, it follows from Theorem 1.9 that $(p, D/p^{2l_1}) = (3, 2)$ or $(4a^2 + 1, 3a^2 + 1)$ for $a \in \mathbb{N}$.

References

1. R. Apéry, "Sur une équation diophantienne," *C. R. Acad. Sci. Paris Sér.* A **251** (1960), 1451–1452.
2. A. Baker, "Rational approximations to certain algebraic numbers," *Proc. London Math. Soc.* **14**(3) (1964), 385–398.

3. A. Baker, "Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers," *Quart. J. Math. Oxford Ser*. **15**(2) (1964), 375–383.
4. E. Bender and N. Herzberg, "Some Diophantine equations related to the quadratic form $ax^2 + by^2$," *Bull. Amer. Math. Soc*. **81** (1975), 161–162.
5. E. Bender and N. Herzberg, "Some Diophantine equations related to the quadratic form $ax^2 + by^2$," Studies in algebra and number theory, *Adv. in Math. Suppl. Stud*., Vol. 6, Academic Press, New York-London, 1979, pp. 219–272.
6. M. Bennett, "Simultaneous rational approximation to binomial functions," *Trans. Amer. Math. Soc*. **348** (1996), 1717–1738.
7. M. Bennett, "Effective measures of irrationality for certain algebraic numbers," *J. Austral. Math. Soc*. **62** (1997), 329–344.
8. M. Bennett, "Explicit lower bounds for rational approximation to algebraic numbers," *Proc. London Math. Soc*. **75** (1997), 63–78.
9. F. Beukers, The generalised Ramanujan-Nagell equation. Dissertation, Rijksuniversiteit, Leiden, 1979. With a Dutch summary. Rijksuniversiteit te Leiden, Leiden, 1979, 57 pp.
10. F. Beukers, "On the generalized Ramanujan-Nagell equation I," *Acta Arith*. **38** (1980/1981), 389–410.
11. F. Beukers, "On the generalized Ramanujan-Nagell equation II," *Acta Arith*. **39** (1981), 113–123.
12. Y. Bilu, G. Hanrot, and P. Voutier, "Existence of primitive divisors of Lucas and Lehmer numbers," *J. Reine Angew. Math*. **539** (2001), 75–122.
13. Y. Bugeaud and T. Shorey, "On the number of solutions of the generalized Ramanujan-Nagell equation," *J. Reine Angew. Math*. **539** (2001), 55–74.
14. X. Chen, Y. Guo, and M. Le, "On the number of solutions of the generalized Ramanujan-Nagell equation $x^2 + D = k^n$," *Acta Math. Sinica* **41** (1998), 1249–1254.
15. X. Chen and M. Le, "On the number of solutions of the generalized Ramanujan-Nagell equation $x^2 - D = k^n$," *Publ. Math. Debrecen* **49** (1996), 85–92.
16. G.V. Chudnovsky, "On the method of Thue-Siegel," *Ann. Math. II Ser*. **117** (1983), 325–382.
17. E.L. Cohen, "On the Ramanujan-Nagell equation and its generalizations," Number theory (Banff, AB, 1988), de Gruyter, Berlin, 1990, pp. 81–92.
18. C. Heuberger and M. Le, "On the generalized Ramanujan-Nagell equation $x^2 + D = p^z$," *J. Number Theory* **78** (1999), 312–331.
19. M. Le, "On the generalized Ramanujan-Nagell equation $x^2 - D = p^n$," *Acta Arith*. **58** (1991), 289–298.
20. M. Le, "On the number of solutions to the Diophantine equation $x^2 - D = p^n$" *Acta Math. Sinica* **34** (1991), 378–387 (Chinese).
21. M. Le, "On the number of solutions of the generalized Ramanujan-Nagell equation $x^2 - D = 2^{n+2}$," *Acta Arith*. **60** (1991), 149–167.
22. M. Le, "On the Diophantine equation $x^2 + D = 4p^n$," *J. Number Theory* **41** (1992), 87–97.
23. M. Le, "On the generalized Ramanujan-Nagell equation $x^2 - D = 2^{n+2}$," *Trans. Amer. Math. Soc*. **334** (1992), 809–825.
24. M. Le, "On the Diophantine equation $x^2 - D = 4p^n$," *J. Number Theory* **41** (1992), 257–271.
25. M. Le, "On the Diophantine equations $d_1x^2 + 2^{2m}d_2 = y^n$ and $d_1x^2 + d_2 = 4y^n$," *Proc. Amer. Math. Soc*. **118** (1993), 67–70.
26. M. Le, "On the Diophantine equation $D_1x^2 + D_2 = 2^{n+2}$," *Acta Arith*. **64** (1993), 29–41.
27. M. Le, "A note on the Diophantine equation $x^2 + 4D = y^p$," *Monatsh. Math*. **116** (1993), 283–285.
28. M. Le, "On the number of solutions of the Diophantine equation $x^2 + D = p^n$," *C. R. Acad. Sci. Paris Sér. I Math*. **317** (1993), 135–138.
29. M. Le, "On the number of solutions of the generalized Ramanujan-Nagell equation $x^2 - D = p^n$," *Publ. Math. Debrecen* **45** (1994), 239–254.
30. M. Le, "A note on the generalized Ramanujan-Nagell equation," *J. Number Theory* **50** (1995), 193–201.
31. M. Le, "A note on the number of solutions of the generalized Ramanujan-Nagell equation $x^2 - D = k^n$," *Acta Arith*. **78** (1996), 11–18.
32. M. Le, "A note on the Diophantine equation $D_1x^2 + D_2 = 2y^n$," *Publ. Math. Debrecen* **51** (1997), 191–198.
33. M. Le, "On the Diophantine equation $(x^3 - 1)/(x - 1) = (y^n - 1)/(y - 1)$," *Trans. Amer. Math. Soc*. **351** (1999), 1063–1074.

34. K. Mahler, "Ein Beweis des Thue-Siegelschen Satzes über die Approximation algebraischer Zahlen für binomische Gleichungen," *Math. Ann*. **105** (1931), 267–276.
35. K. Mahler, "Zur Approximation algebraischer Zahlen, I: Ueber den grössten Primteiler binärer Formen," *Math. Ann*. **107** (1933), 691–730.
36. M. Mignotte, "A corollary to a theorem of Laurent-Mignotte-Nesterenko," *Acta Arith*. **86** (1998), 101–111.
37. T. Nagell, "The diophantine equation $x^2 + 7 = 2^n$," *Ark. Math*. **4** (1960), 185–187.
38. S. Ramanujan, "Question 464," *J. Indian Math. Soc*. **5** (1913), 120.
39. D. Ridout, "The p-adic generalization of the Thue-Siegel-Roth theorem," *Mathematika* **5** (1958), 40–48.
40. J.B. Rosser and L. Schoenfeld, "Approximate formulas for some functions of prime numbers," *Ill, J. Math*. **6** (1962), 64–94.
41. L. Schoenfeld, "Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$ II," *Math. Comp*. **30** (1976), 337–360.
42. C.L. Siegel, "Die Gleichung $ax^n - by^n = c$," *Math. Ann*. **114** (1937), 57–68.
43. A. Thue, "Berechnung aller Lösungen gewisser Gleichungen von der form," *Vid. Skrifter I Mat.-Naturv. Klasse* (1918), 1–9.
44. N. Tzanakis and J. Wolfskill, "On the Diophantine equation $y^2 = 4q^n + 4q + 1$," *J. Number Theory* **23** (1986), 219–237.
45. N. Tzanakis and J. Wolfskill, "The Diophantine equation $x^2 = 4q^{a/2} + 4q + 1$, with an application to coding theory," *J. Number Theory* **26** (1987), 96–116.
46. T. Xu and M. Le, "On the Diophantine equation $D_1x^2 + D_2 = k^n$," *Publ. Math. Debrecen* **47** (1995), 293–297.
47. P. Yuan, "On the number of the solutions of $x^2 - D = p^n$," *Sichuan Daxue Xuebao* **35** (1998), 311–316.