PERFECT POWERS WITH FEW BINARY DIGITS AND RELATED DIOPHANTINE PROBLEMS, II

MICHAEL A. BENNETT, YANN BUGEAUD AND MAURICE MIGNOTTE

Abstract. We prove that if $q \geq 5$ is an integer, then every q-th power of an integer contains at least 5 nonzero digits in its binary expansion. This is a particular instance of one of a collection of rather more general results, whose proofs follow from a combination of refined lower bounds for linear forms in Archimedean and non-Archimedean logarithms with various local arguments.

1. Introduction

The present paper may be viewed as a computational companion to [3], where we established effective (but inexplicit) upper bounds for solutions to certain classes of Diophantine equations. The goal of the paper at hand is to demonstrate the degree to which our approach leads to sharp, explicit upper bounds, which can be combined with sieve methods to completely solve exponential and polynomial-exponential equations.

Let $x \geq 2$ be an integer. The starting point for this paper is the problem of finding all perfect powers whose base-x representation contains relatively few non-zero digits. It is notable that if we permit as many as four such digits, it is apparently beyond current technology to even determine whether the corresponding set of powers is finite (or finite outside of certain parametrized families). As an example of the latter situation, from the identity $(1 + x^\ell)^2 = 1 + 2x^\ell + x^{2\ell}$, we observe that there are infinitely many squares with three non-zero digits in base x; a theorem of Corvaja and Zannier [6] implies that, for x fixed, all such squares may be classified via like identities, with at most finitely many exceptions. For bases $x > 2$, an analogous result for squares with four non-zero digits is unknown.

Date: 07 Dec. 2011.

2000 *Mathematics Subject Classification.* Primary: 11A63, Secondary: 11D61, 11J86.

Key words and phrases. Polynomial-exponential equations, digital problems.

Research supported by NSERC.

Generalizing this problem, the main results of [3] are effective upper bounds upon integer q for which equations of the shape

$$x_1^a + x_2^b + 1 = y^q \quad \text{or} \quad x_1^a + x_2^b + x_3^c + 1 = y^q$$

have solutions. Here, x_1 and x_2 (or, in the second case, x_1, x_2 and x_3) are positive integers which, importantly for our techniques, fail to be coprime. In the special case of the first equation with $x_1 = x_2 = q = 2$, odd squares with three binary digits have been completely classified by Szalay [13].

Theorem S. All solutions of the equation

$$(1) \qquad 2^a + 2^b + 1 = y^2, \quad \text{with } a > b > 0$$

are given by $(a, b, y) = (5, 4, 7), (9, 4, 23)$ or $(2t, t + 1, 2^t + 1)$, for some $t \geq 2$.

This result was subsequently extended by Scott [12] and Luca [11] to show that there are no squares of the form $p^a + p^b + 1$, where p is an odd prime and $a > b > 0$.

In the present paper, we will provide completely explicit versions of special cases of Theorems 1, 2 and 3 of [3]. We begin by completely solving the Diophantine equation $x^a + x^b + 1 = y^q$ for $x \in \{2, 3\}$ and $q \geq 2$.

Theorem 1. *If there exist integers $a > b > 0$ and $q \geq 2$ for which*

$$x^a + x^b + 1 = y^q, \quad \textit{with} \quad x \in \{2, 3\},$$

then

$$(x, a, b, y, q) = (2, 5, 4, 7, 2),\ (2, 9, 4, 23, 2),\ (3, 7, 2, 13, 3),\ (2, 6, 4, 3, 4),\ (4, 3, 2, 9, 2),\ (4, 3, 2, 3, 4)$$

or $(x, a, b, y, q) = (2, 2t, t + 1, 2^t + 1, 2)$, for some integer $t = 2$ or $t \geq 4$.

Similarly, in the case of perfect powers with four binary digits, we have

Theorem 2. *If there exist positive integers a, b, c, y and q such that*

$$(2) \qquad 2^a + 2^b + 2^c + 1 = y^q,$$

then $q \leq 4$.

A computer search shows that equation (2) has at least five solutions not corresponding to equation (1) (i.e. with a, b and c distinct), namely those given by

$$(3) \quad (a, b, c, q, y) = (4, 3, 1, 3, 3),\ (7, 5, 3, 2, 13),\ (7, 6, 5, 2, 15),\ (11, 7, 5, 2, 47),\ (13, 12, 5, 2, 111),$$

where we assume that $a > b > c$. We conjecture that there are no other solutions; by recent work of Corvaja and Zannier [7], there exist at most finitely many with $q \in \{2, 3, 4\}$. In [7], the authors independently establish that (2) has no solution when q exceeds some effectively computable q_0.

Finally, in the case of an equation considered by Corvaja and Zannier [6], we prove

Theorem 3. *If there exist positive integers a, b, y and $q \geq 2$ for which*

$$6^a + 2^b + 1 = y^q, \tag{4}$$

then $q \in \{2, 3, 6\}$.

For the remaining untreated cases $q = 2, 3$ and 6, it should be noted that the aforementioned result of Corvaja and Zannier [6], based upon Schmidt's Subspace Theorem, implies that equation (4) has, in each case, at most finitely many solutions. The only ones known correspond to

$$(a, b, y^q) = (1, 0, 2^3), (0, 1, 2^2), (1, 1, 3^2), (3, 3, 15^2) \text{ and } (3, 9, 3^6). \tag{5}$$

Their argument depends crucially upon the fact that 6 and 2 have a common prime divisor and, in particular, fails to yield a like result for the similar equation

$$3^a + 2^b + 1 = y^q.$$

This last equation, in case $q = 2$, has been completely solved by Leitner [10], essentially by observing that integers of the shape $3^a + 2^b + 1$ are quadratic nonresidues modulo $N = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \cdot 13$, provided $a \geq 4$ and $b \geq 2$ (note that $\gcd(2^{12} - 1, 3^{12} - 1) = 5 \cdot 7 \cdot 13$).

The key tool in all our proofs is lower bounds for linear forms in two logarithms, both Archimedean and non-Archimedean, specifically the refinements given in [5]. The relative sharpness of these bounds is absolutely crucial in obtaining results of the flavour of those given here.

The outline of the remainder of the paper is as follows. In Section 2, we record a number of lower bounds available on the literature for linear forms in two logarithms. Sections 3 and 4 are devoted to the proof of Theorem 1, in case $x = 2$ or $x = 3$, respectively. Section 5 contains the proof of Theorem 3. Finally, in Section 6, we prove Theorem 2 (which represents the main achievement of this paper, from a computational and technical viewpoint).

2. Linear forms in two logarithms

In this section, we will collect various estimates for linear forms in two logarithms, both Archimedean and non-Archimedean. Let us first state a special version of a corollary obtained in [8]. In the sequel, if

$r = m/n$ is a nonzero rational (with m and n relatively prime integers), we will define the logarithmic height of r to be $h(r) = \max\{\log|m|, \log|n|, 1\}$.

Theorem 4. *Let α_1 and α_2 be multiplicatively independent positive rational numbers, and b_1 and b_2 be positive integers. Define*

$$\Lambda = |b_2 \log \alpha_2 - b_1 \log \alpha_1|\,.$$

Then

$$\log \Lambda \geq -25.2\ \left(\max\left\{\log b' + 0.38, 10\right\}\right)^2\ h(\alpha_1)\, h(\alpha_2),$$

where

$$b' = \frac{b_1}{h(\alpha_2)} + \frac{b_2}{h(\alpha_1)}.$$

We will also appeal to the most general version of the main result of [8] :

Theorem 5. *Let α_1 and α_2 be nonzero algebraic numbers, with, say, $|\alpha_1|, |\alpha_2| > 1$ and*

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

Let b_1 and b_2 be positive integers. Define

$$\Lambda = |b_2 \log \alpha_2 - b_1 \log \alpha_1|\,.$$

Further, let $K \geq 2$ be an integer, L, R_1, R_2, S_1 and S_2 be positive integers, and choose ρ and μ to be real numbers with $\rho > 1$ and $1/3 \leq \mu \leq 1$. Put

$$R = R_1 + R_2 - 1, \quad S = S_1 + S_2 - 1, \quad N = KL, \quad g = \frac{1}{4} - \frac{N}{12RS}, \quad \sigma = \frac{1 + 2\mu - \mu^2}{2},$$

and set

$$\beta = \frac{(R-1)b_2 + (S-1)b_1}{2} \left(\prod_{k=1}^{K-1} k!\right)^{-2/(K^2-K)}.$$

Let a_1 and a_2 be positive real numbers such that

$$a_i \geq \rho\, |\log \alpha_i| - \log|\alpha_i| + 2\, D\, h(\alpha_i),$$

for $i \in \{1, 2\}$, and suppose that

$$\text{(6)} \qquad \begin{aligned} &Card\{\alpha_1^r \alpha_2^s \;:\; 0 \leq r < R_1,\ 0 \leq s < S_1\} \geq L, \\ &Card\{r b_2 + s b_1 \;:\; 0 \leq r < R_2,\ 0 \leq s < S_2\} > (K-1)L, \end{aligned}$$

and

$$K(\sigma L - 1)\log \rho - (D+1)\log N - D(K-1)\log \beta - gL(Ra_1 + Sa_2) > \epsilon(N),$$

where

$$\epsilon(N) = \frac{2}{N} \log\left(N!\, N^{-N+1}\, \left(e^N + (e-1)^N\right)\right).$$

Then

$$\Lambda \max\left\{\frac{LSe^{LS|\Lambda|/(2b_2)}}{2b_2}, \frac{LRe^{LR|\Lambda|/(2b_1)}}{2b_1}\right\} > \rho^{-\mu KL}.$$

We now state the non-Archimedean results we require. Let α_1 and α_2 be multiplicatively independent positive rational numbers. Define g as the smallest positive integer for which both $\nu_p(\alpha_1^g - 1)$ and $\nu_p(\alpha_2^g - 1)$ are positive. Finally, choose E for which

$$\nu_p(\alpha_i - 1) \geq E > \frac{1}{p-1}, \quad \text{for } i = 1, 2.$$

A special case of Theorem 2 of [5] is the following.

Theorem 6. *Let α_1 and α_2 be multiplicatively independent positive rational numbers, and b_1 and b_2 be positive integers. Consider the "linear form"*

$$\Lambda = \alpha_2^{b_2} - \alpha_1^{b_1}.$$

Then, for any fixed prime number p,

$$\nu_p(\Lambda) \leq \frac{36.1\, g}{E^3 (\log p)^4} \left(\max\{\log b' + \log(E \log p) + 0.4, 6\, E\, \log p, 5\}\right)^2 (\log A_1)\, (\log A_2)\,, \tag{7}$$

if p is odd or if $p = 2$ and $\nu_2(\alpha_2 - 1) \geq 2$, where

$$b' = \frac{b_1}{\log A_2} + \frac{b_2}{\log A_1} \quad \textit{and} \quad \log A_i \geq \max\{h(\alpha_i), E \log p\}.$$

If $p = 2$ and $\nu_2(\alpha_2 - 1) \leq 1$, then

$$\nu_p(\Lambda) \leq 208 \left(\max\{\log b' + 0.04, 10\}\right)^2 (\log A_1)\, (\log A_2)\,,$$

Finally, we state a strong, general version of a lower bound for linear forms in two p-adic logarithms, from [5].

Theorem 7. *Let α_1 and α_2 be two rational numbers which are multiplicatively independent, of respective logarithmic height h_1 and h_2. Consider the "linear form"*

$$\Lambda = \alpha_1^{b_1} - \alpha_2^{b_2},$$

where b_1 and b_2 are non-zero integers. Let p be a prime number which does not divide $b_1 b_2$. Assume that

$$\nu_p(\alpha_i - 1) \geq E > \frac{1}{p-1}, \quad i = 1, 2,$$

and also that $\nu_p(\alpha_2 - 1) \geq 2$ *if* $p = 2$*. Let* $K \geq 3$*,* $L \geq 2$ *and* R_1*,* R_2*,* S_1 *and* S_2 *be positive integers. Put* $R = R_1 + R_2 - 1$*,* $S = S_1 + S_2 - 1$ *and* $N = KL$*. Assume that*

$$R_1 S_1 \geq L \quad \text{and} \quad \mathrm{Card}\{rb_2 + sb_1,\ 0 \leq r < R_2,\ 0 \leq s < S_2\} > (K-1)L.$$

Put also

$$\gamma = \frac{1}{2} - \frac{N}{6RS}, \quad \beta = \frac{(R-1)b_2 + (S-1)b_1}{2} \left(\prod_{k=1}^{K-1} k\,! \right)^{-2/(K^2-K)}.$$

Then, under the condition

$$K(L-1)E\log p - 3\log N - (K-1)\log\beta - \gamma L(Rh_1 + Sh_2) > 0, \tag{8}$$

we have

$$\nu_p(\Lambda) \leq E(KL - 1/2).$$

3. The equation $2^a + 2^b + 1 = y^q$

In light of Theorem S, to complete the proof of Theorem 1 in case $x = 2$, it remains to show that the Diophantine equation

$$2^a + 2^b + 1 = y^q \tag{9}$$

has no solutions with $a > b \geq 1$ and $q \geq 3$ odd. In this section, we will refine the arguments that lead to Theorem 1 of [3] (which provide an effectively computable upper bound for q in (9)), to show that, in fact, $q \leq 7$. Before we proceed, it is worth noting that the proof of Theorem S appeals to a result of Beukers [4] on restricted approximation to $\sqrt{2}$, obtained via the hypergeometric method, while the resolution of (9) will, as with all the theorems of the paper at hand, depend primarily upon the theory of linear forms in logarithms.

3.1. **Preliminaries.** Our goal in this subsection is to deduce a strong lower bound upon y in equation (9), which will lead to good upper bounds for q via lower bounds for linear forms in logarithms. From (9), it is immediate that $y^q \equiv 1 \pmod{2^b}$ and, since q is odd, that $y \equiv 1 \pmod{2^b}$. Write $y = 1 + h2^b$. Since (9) implies that $\gcd(2^b + 1, y) = 1$, necessarily $h > 1$ is odd, whereby $y > 3 \cdot 2^b$, and hence, modulo 8, we may suppose that $y \geq 11$.

Substituting the relation $y = 1 + 2^b h$ in (9), we have that

$$2^a + 2^b + 1 = (2^b h)^q + \binom{q}{1}(2^b h)^{q-1} + \binom{q}{2}(2^b h)^{q-2} + \cdots + \binom{q}{q-1}(2^b h) + 1,$$

and hence the inequality

$$bq < a. \tag{10}$$

Simplifying the previous equality gives

$$2^{b(q-1)}h^q + \binom{q}{1} 2^{b(q-2)} h^{q-1} + \cdots + qh = 2^{a-b} + 1,$$

which shows that $2^b \mid (qh - 1)$ and hence

$$h \geq (2^b + 1)/q.$$

It follows that

$$2^{b(q-1)} \left(\frac{2^b + 1}{q} \right)^q < 2^{a-b},$$

which implies the inequality $2^{2bq} < q^q 2^a$, and so

$$b < \frac{\log q}{2 \log 2} + \frac{a}{2q}. \tag{11}$$

Appealing to the Taylor expansion

$$(1+x)^{1/q} = 1 + \frac{x}{q} - \frac{q-1}{2q^2} x^2 + \frac{(q-1)(2q-1)}{6q^3} x^3 + \cdots$$

with $x = 2^b + 2^a$ considered as a 2–adic integer, we have that

$$\nu_2(q^2 y - q^2 - 2^b q + (q-1)\, 2^{2b-1}) \geq 3b,$$

for $b \geq 2$. More precisely, if we suppose that $b \geq \nu_2(q-1)$, we have that

$$\nu_2(q^2 y - q^2 - 2^b q + (q-1)\, 2^{2b-1}) = 3b,$$

which implies

$$q^2 y \geq 2^{3b} - (q-1)\, 2^{2b-1} + 2^b + q^2,$$

and so

$$y > \frac{2^{3b}}{q^2} - \frac{q-1}{2q^2} 2^{2b}. \tag{12}$$

3.2. **Bounds on q.** We first consider the Archimedean linear form

$$\Lambda = a \log 2 - q \log y.$$

From (9), we obtain the inequality

$$|\Lambda| < \frac{2^b+1}{2^a}.$$

If we had $2^b + 1 \geq y$, then, since 2^b+1 and y are coprime, necessarily $2^b + 1 \geq y+1$ whereby, via inequality (10),

$$y^q \leq 2^{bq} \leq 2^{a-1},$$

a contradiction. It follows that $2^b + 1 \leq y - 1$ and so

$$\log |\Lambda| < -(q-1) \log y. \tag{13}$$

A direct application of Theorem 4 yields

$$\log |\Lambda| \geq -25.2 \left(\max\left\{ \log \left(q + \frac{a}{\log y} \right) + 0.38, 10 \right\} \right)^2 \log y,$$

whence

$$q < 25.2 \left(\max\left\{ \log \left(q + \frac{a}{\log y} \right) + 0.38, 10 \right\} \right)^2 + 1.$$

If we suppose that $y \geq 11$ and $q > 200$, say, then

$$\frac{a}{\log y} < 1.45\, q$$

and so either

$$\max\left\{ \log \left(q + \frac{a}{\log y} \right) + 0.38, 10 \right\} = 10,$$

whence $q \leq 2520$, or

$$q < 25.2 \, (1.28 + \log q)^2 + 1,$$

whereby $q \leq 1985$. In either case, we necessarily have that $q \leq 2520$.

To find a (much) better upper bound for q, we combine Theorem 5 with the inequality $y \geq 11$. We further write $a = qs + r$, with $|r| \leq \frac{q-1}{2}$, so that

$$\Lambda = r \log 2 - q \log(y/2^s).$$

The advantage of doing this is that the height of $y/2^s$ is still, essentially, $\log y$, while the logarithm of this number is absolutely bounded (i.e. we may choose a rather smaller value for a_1 in Theorem 5). In particular, we may take $\alpha_1 = y/2^s, \alpha_2 = 2, b_1 = q, b_2 = r$ (considering $-\Lambda$ in the case $r < 0$),

$$a_2 = 2 + (\rho - 1) \log 2 \quad \text{and} \quad a_1 = 2 \log y + \frac{\rho+3}{2} \log 2.$$

We specify values for L, ρ, μ and k and, in each case, choose

$$K = \lceil kLa_1a_2 \rceil,\ R_1 = \left\lceil \sqrt{\tfrac{La_2}{a_1}} \right\rceil,\ R_2 = \left\lceil \sqrt{\tfrac{(K-1)La_2}{a_1}} \right\rceil,$$
$$S_1 = \left\lceil \sqrt{\tfrac{La_1}{a_2}} \right\rceil,\ S_2 = \left\lceil \sqrt{\tfrac{(K-1)La_1}{a_2}} \right\rceil. \tag{14}$$

Note that, since y is odd, the first inequality in (6) is immediately satisfied. To ensure the second inequality, we will, in all cases assume that q is prime and that $q > R_2$. To see that this is sufficient, note that

$$r_1r + s_1q = r_2r + s_2q \implies q \mid r\,(r_2 - r_1) \implies q < R_2,$$

unless $(r_1, s_1) = (r_2, s_2)$, provided $0 \le r_1, r_2 < R_2$.

For reasonably small values of q, we can calculate the quantity β in Theorem 5 explicitly; in many cases it simplifies matters to use an upper bound derived from the inequality

$$\left(\prod_{k=1}^{K-1} k!\right)^{-2/(K^2-K)} \le \exp\left\{-\log(K-1) + \frac{3}{2} - \frac{\log(2\pi(K-1)/\sqrt{e})}{K-1} + \frac{\log K}{6K(K-1)}\right\}$$

(see line 11, page 307 of [9]). Choosing our parameters $L = 10$, $\rho = 6.6$, $\mu = 1/3$ and $k = 0.31$ (for $397 \le q < 450$), $k = 0.36$ (for $450 \le q < 650$), or $k = 0.51$ (for $650 \le q \le 2520$), Theorem 5, inequality (13) and some routine calculus imply that necessarily $q \le 389$. A brute force computation (of around 40 seconds on a home computer), using this upper bound and calculating binary expansions of y^q, shows that $y > 10^4$. Appealing a second time to Theorem 5, this time with $L = 8$, $\rho = 6.6$, $\mu = 1/3$ and values of k with $0.375 \le k \le 0.46$, we find that $q \le 199$. A second computation (of less than 25 minutes) using this new upper bound leads to the conclusion that $y > 10^6$. A third application of Theorem 5, now with $L = 8$, $\rho = 7$, $\mu = 1/3$ and $k = 0.316$, then implies that $q \le 181$.

We are now in a good position to apply Theorem 7 with $p = 2$. Here we consider the "linear form"

$$\Lambda = y^q - B, \quad \text{where } B = 1 + 2^b,$$

which satisfies $\nu_2(\Lambda) = a$, and for which both B and y are 2-adically close to 1 (a situation which is essentially optimal for application of Theorem 7). Since B and y are coprime and > 1, they are multiplicatively independent. We choose $\alpha_1 = y$, $\alpha_2 = B$ (or $\alpha_1 = -y$ and $\alpha_2 = -B$, if $b = 1$), so that $E = \max\{b, 2\}$, $b_1 = q$, $b_2 = 1$, $h_1 = \log y$, $h_2 = \log B$, and may take

$$a_1 = \frac{\log y}{\log 2} \text{ and } a_2 = \frac{\log B}{\log 2}.$$

Appealing to Theorem 7, with suitably chosen parameters, we obtain upper bounds of the shape $q \leq q_0$, where

b	q_0	b	q_0	b	q_0
1	173	4	61	7	29
2	181	5	43	8	29
3	101	6	37	≥ 9	23

We provide full details for the case $b = 1$; for larger values of b, data is available at the website http://math.ubc.ca/∼bennett/BeBuMi-data. For $10^6 \leq y \leq 1680342$, we readily check that the choices

$$K = 198, L = 9, R_1 = 1, R_2 = 12, S_1 = 9, S_2 = 148, b = 1, q = 179$$

lead to the desired contradiction (and hence to the conclusion that $q \leq 173$). For values of y with $1680343 \leq y < 10^{11}$, we, in each case, take $L = 10, R_1 = 1, R_2 = 12, S_1 = 10$, and choose our pair (K, S_2) satisfying

$$\begin{aligned}(K, S_2) \in \; & \{(185, 154), (191, 159), (198, 165), (205, 171), (213, 177), (224, 186), (236, 196), \\ & (244, 203), (252, 210), (260, 216), (272, 226), (293, 244), (316, 263)\}.\end{aligned}$$

For example, the choice $(K, S_2) = (185, 154)$ does the trick for $1680343 \leq y \leq 2672042$. Finally, for $y \geq 10^{11}$, we may choose K, R_1, R_2, S_1 and S_2 as in (14) with $L = 10$ and $k = 0.56$. Verifying inequality (8), while admittedly painful, is a reasonably routine exercise.

Armed with the preceding upper bounds upon q, there are two different approaches we can employ to finish the proof of Theorem 1, in case $x = 2$. Both rely upon elementary arguments working modulo suitably chosen primes congruent to 1 modulo q. In the first case, we can use such techniques to eliminate many cases for b fixed, with, say, $1 \leq b \leq 1000$. By way of example, if, say, $q = 13$, we can eliminate all such small values of b from consideration by showing that the congruence $2^a + 2^b + 1 \equiv y^q \pmod{N}$ has no solutions for N some product of the primes

$$p \in \{53, 79, 131, 157, 313, 521, 937\}.$$

Continuing in this fashion enables us to suppose that $b > 1000$, whereby a final application of Theorem 7 with parameters chosen as in (14) (with k proportional to $1/b^2$ and taking full advantage of the very large lower bound upon y implicit in (12)) enables us to conclude that $q \leq 7$. Again, the details are available at http://math.ubc.ca/∼bennett/BeBuMi-data.

3.3. **The 'coup de grâce'.** Alternatively (or in any case to handle the remaining values $q \in \{3,5,7\}$), we can treat equation (9) for fixed $q \leq 181$ by local means. Specifically, we consider primes $p_i \equiv 1 \pmod{q}$ for which $\mathrm{ord}_2(p_i) = mq$ with m a "suitably small" integer. Here, by $\mathrm{ord}_l(p_i)$, we mean the smallest positive integer k for which $l^k \equiv 1 \pmod{p_i}$. Fixing some integer M, for each such p_i with $m \mid M$, we let a and b loop over integers from 1 to Mq and store the resulting pairs (a,b) with the property that either $2^a + 2^b + 1 \equiv 0 \pmod{p_i}$ or

$$\left(2^a + 2^b + 1\right)^{(p_i-1)/q} \equiv 1 \pmod{p_i}.$$

For a given prime p_i, if we denote by S_i the set of corresponding pairs (a,b), then our hope is to find primes $p_1, p_2, \ldots, p_k$ corresponding to M with

$$\bigcap_{i=1}^{k} S_i = \emptyset. \tag{15}$$

Checking that we have such sets of primes (with M reasonably small) for each prime $3 \leq q \leq 181$ is a short calculation of a few minutes on a laptop (particularly if one uses the fact that $b \in \{1,2\}$ provided $q > 101$). By way of example, for $q = 3$ and $M = 60$, we obtain (15) for

$$p_i \in \{7, 19, 37, 61, 73, 109, 151, 181, 331, 1321\}.$$

For $q = 5$ or 7, we may take $M = 20$ and

$$p_i \in \{11, 31, 41, 101, 251, 601\}$$

and

$$p_i \in \{29, 43, 71, 113, 127\},$$

respectively. Once more, full details (including our code) are available at
http://math.ubc.ca/∼bennett/BeBuMi-data.

4. The equation $3^a + 3^b + 1 = y^q$

We will argue in a similar fashion to the preceding section; the complication that arises here is that local arguments prove insufficient to tackle the case $q = 3$ (where we find a solution with $a = 7$ and $b = 2$). Appealing, as in the preceding section, to Theorems 5 and 7, we find that if there exist solutions to the equation

$$3^a + 3^b + 1 = y^q, \tag{16}$$

then necessarily $q < 1160$ (using only that $y \geq 2$). A short calculation allows us to assume therefore that $y \geq 50$, whereby our lower bounds for linear forms in logarithms now imply that $q < 100$. We will thus assume that we have a solution to equation (16), where $a \geq b$, and $q < 100$ is prime. From the aforementioned work of Scott [12] (cf Luca [11]), we may suppose further that q is odd.

We first treat the case $q = 3$. As previously remarked, here the behaviour is different than for larger values of q, since we have a solution to (16), namely $3^7 + 3^2 + 1 = 2197 = 13^3$. Our treatment of this equation relies upon a result from an old paper of the first author [2], which itself depends upon Padé approximation to the binomial function (and hence has more in common with the techniques used to prove Theorem S than to those of the rest of this paper).

Let us begin by noting that if $b = 0$ or $b = 1$, then we have $3^a + k = y^3$ for $k \in \{2, 4\}$, in each case an immediate contradiction modulo 9. We may thus suppose that $b \geq 2$. Also, since the congruence $2 \cdot 3^b + 1 \equiv y^3 \pmod{13}$ has no solutions, we may further assume that $a > b$. From the fact that

$$\gcd\left(y - 1, \frac{y^3 - 1}{y - 1}\right) \in \{1, 3\},$$

it follows that $y \equiv 1 \pmod{3^{b-1}}$, and so $y \geq 3^{b-1} + 1$, whereby

$$3^a = y^3 - 3^b - 1 > 3^{3b-3}.$$

We thus have $a \geq 3b - 2$.

If $3 \mid a$, say $a = 3a_0$ for a positive integer a_0, then $y \geq 3^{a_0} + 1$ and so

$$3^a + 3^b + 1 \geq 3^a + 3^{2a/3} + 1$$

which implies that $b > 2a/3$, contradicting $a \geq 3b - 2$ and $b \geq 2$. We thus have $a \equiv \pm 1 \pmod 3$. Writing $a = 3a_0 + \delta$, for $\delta = \pm 1$, it follows that

$$\left| y^3 - 3 \cdot (3^{a_0})^3 \right| = 3^b + 1$$

or

$$\left| 3y^3 - 3\,(3^{a_0})^3 \right| = 3^{b+1} + 3,$$

for $\delta = 1$ or -1, respectively. Applying the inequality

$$\left| A^3 - 3B^3 \right| \geq \max\{|A|, |B|\}^{0.24}, \tag{17}$$

valid for all integers A and B (see Theorem 6.1 of Bennett [2]), it follows, in either case, that

$$3^b + 1 \geq 3^{0.08a - 0.92}, \tag{18}$$

which implies the following upper bounds upon a :

b	a
2	≤ 37
3	≤ 49
4	≤ 61
≥ 5	$\leq 25(b+1)/2$

It is convenient at this time to dispose of a few more small values of b; a short check, using the bounds in the table above shows that the only solution to (16) with $q = 3$ and $b \leq 4$ corresponds to $3^7 + 3^2 + 1 = 13^3$. We will assume henceforth that

$$b \geq \max\{5, -1 + 2a/25\}. \tag{19}$$

Considering the Taylor series

$$(1+x)^{1/3} = 1 + \frac{x}{3} - \frac{x^2}{9} + \frac{5x^3}{81} - \frac{10x^4}{243} + \frac{22x^5}{729} - \frac{154x^6}{6561} + \cdots ,$$

and viewing $3^a + 3^b$ as a 3-adic integer, we have, from (19) and $a \geq 3b - 2$, that

$$\nu_3(y - 1 - 3^{b-1}) = 2b - 2.$$

We thus have

$$y \geq 3^{2b-2} + 3^{b-1} + 1$$

and so, after a little work, $a \geq 6b - 5$. Returning to our Taylor expansion,

$$\nu_3(y - 1 - 3^{b-1} + 3^{2b-2}) = 3b - 4$$

and so

$$y \geq 3^{3b-4} - 3^{2b-2} + 3^{b-1} + 1$$

which implies, from (19), that $a \geq 9b - 13$. We thus have

$$\nu_3(y - 1 - 3^{b-1} + 3^{2b-2} - 5 \cdot 3^{3b-4}) = 4b - 5,$$

and so

$$y \geq 3^{4b-5} + 5 \cdot 3^{3b-4} - 3^{2b-2} + 3^{b-1} + 1$$

and $a \geq 12b - 14$. Finally, we have

$$\nu_3(y - 1 - 3^{b-1} + 3^{2b-2} - 5 \cdot 3^{3b-4} + 10 \cdot 3^{4b-5}) = 5b - 6,$$

whence

$$y \geq 3^{5b-6} - 10 \cdot 3^{4b-5} + 5 \cdot 3^{3b-4} - 3^{2b-2} + 3^{b-1} + 1.$$

It follows that $a \geq 15b - 19$, contradicting (19), for $b \geq 15$. Computing $3^a + 3^b + 1$ for each pair (a, b) with $5 \leq b \leq 14$ and $15b - 19 \leq a \leq 25(b+1)/2$, we find no further solutions to the equation $3^a + 3^b + 1 = y^3$.

For the remaining primes values of q, with $5 \leq q < 100$, local methods suffice, in each case, to show that equation (16) has no solutions in integers. As in the case of equation (9), we simply search over primes $p_i \equiv 1 \pmod{q}$ with the property that $\mathrm{ord}_3(p_i) = mq$ for m a "suitably small" integer. With the notation of the preceding section, by way of example, if $q = 5$, then, taking $M = 20$, we find

$$p_i \in \{11, 61, 101, 151, 1181, 8951\},$$

with corresponding $S_1, \ldots, S_6$ having between 1608 and 2580 elements (note that $(j,k) \in S_i$ implies the same for (k, j)), and $\bigcap_{i=1}^{6} S_i = \emptyset$. This completes the proof of Theorem 1.

5. The equation $6^a + 2^b + 1 = y^q$

Presumably, the only solutions to the equation

$$6^a + 2^b + 1 = y^q \tag{20}$$

are as given in (5). In this section, we will prove Theorem 3, whereby all solutions to (20) necessarily have $q \in \{2, 3, 6\}$.

To begin, note that the case of equation (20) with $ab = 0$ is all but immediate; the only solutions are with $y^q \in \{4, 8\}$. We will therefore suppose that $q \geq 5$ is prime (returning to the cases $q \in \{4, 9\}$ later), and that a and b are positive integers. If $y = 3$ then necessarily $\min\{a, b\} = 1$. If $b = 1$, there are no solutions modulo 9, while $a = 1$ implies, modulo 7, that q is even. We may thus suppose that $y \geq 5$.

As in the preceding section, we will split our argument, depending on the relative sizes of the exponents a and b. Specifically, we will consider two cases : (i) $a \geq b/1.3$, and (ii) $b > 1.3\,a$. In the first of these, we have

$$|6^a y^{-q} - 1| \leq 2^b y^{-q} \leq 2^{1.3a} y^{-q} \leq y^{-0.497\,q},$$

and work with

$$\Lambda = r \log 6 - q \log(y/6^s), \quad \text{where } a = qs + r,\ |r| \leq \frac{q-1}{2}.$$

An immediate application of Theorem 4 yields the upper bond $q \leq 17331$. Turning to Theorem 5, with the choices $\rho = 3.1$, $L = 4$ and $\mu = 1/3$, (whereby, after a short computation, we may assume that $y > 100$), we obtain the (much sharper) bound $q < 130$.

In case (ii), we distinguish between two subcases: $6^a > 2^b$ or $6^a < 2^b$, and apply Theorem 7 with $4 \leq L \leq 9$. After a little work, we obtain bounds of the shape

$$q < 620 \text{ when } a = 1$$
$$q < 450 \text{ when } a = 2$$
$$q < 120 \text{ when } a = 3$$
$$q < 60 \text{ when } a \geq 4.$$

As previously, we appeal to local arguments to handle the remaining (prime) values of q (and for $q \in \{4, 9\}$), considering equation (20) modulo various $p \equiv 1 \pmod{q}$. For example, we treat $q = 4$ with

$$p \in \{13, 17, 37, 41, 61, 97, 181, 193, 241, 401, 577, 1153, 1601, 4801, 9601, 14401, 55201, 57601\}$$

and $q = 5$ using

$$p \in \{11, 41, 61, 101, 151, 181, 251, 401, 601, 751, 1201, 1801, 2251, 3001, 4801, 9001\}.$$

No effort has been made here to find what is in any sense a "minimal" set of such primes p. Our code and output are, as previously, available at http://math.ubc.ca/∼bennett/BeBuMi-data.

6. The equation $2^a + 2^b + 2^c + 1 = y^q$

In this section, we will prove Theorem 2. Here, the interplay between theory and computation is at its most intriguing; even with the full strength of Theorems 5 and 7, the remaining calculations are highly nontrivial.

Without loss of generality, via Theorem 1, we may suppose that $a > b > c \geq 1$. We begin by noting that a short computer verification shows that the only solutions to equation (2) with $a \leq 100$ are those given in (3). We may thus suppose $a > 100$; we will also assume, for the time being, that $q > 420$ is an odd prime. Our goal is to deduce an absolute upper bound of the shape $q \leq q_0$ where q_0 is small enough that the remaining cases of equation (2) can be treated by local arguments.

We begin by eliminating some "easy cases". The following very elementary remark will prove useful.

Remark. If $y \equiv 7 \pmod 8$ then $b = 2$ and $c = 1$. Moreover, if $y \equiv 15 \pmod{16}$ then there is no solution to equation (2) with $q > 2$ prime.

To see this, note that if $y \equiv -1 \pmod{2^k}$ and q is odd then $y^q \equiv -1 \pmod{2^k}$, and apply this observation with $k=3$ and $k=4$.

With this in mind, we will begin by showing that equation (2) has no solutions with $a > 100$, $q > 420$ and $y \equiv 7 \pmod 8$. In case $y = 7$, by the preceding remark, we necessarily have

$$7^q = 7 + 2^a.$$

Here $a > 2q$. It follows that 2^a divides $7^{q-1} - 1$, whereby $2^{a-3} \mid q - 1$ for $a \geq 3$ (a contradiction for $a > 100$).

The case $y \equiv 7 \pmod{16}$ with $y > 7$ is more difficult, but still requires only appeal to bounds for Archimedean logarithms. We have

$$y^q = 2^a + 2^b + 2^c + 1 = 2^a + 7$$

whereby

$$|2^a y^{-q} - 1| \leq 7 \cdot y^{-q}$$

and hence

$$|a \log 2 - q \log y| < 8\, y^{-q}. \tag{21}$$

In fact, as previously, we do better to write Λ as

$$\Lambda = r \log 2 - q \log(y/2^s), \quad \text{where } a = qs + r,\ |r| \leq \frac{q-1}{2}. \tag{22}$$

Then we apply Theorem 5 with the lower bound $y \geq 15$, $L = 9$ and $\rho = 10$ to deduce an upper bound of the shape $q < 430$ for $y \equiv 7 \pmod{16}$ A very quick computer verification shows that there is no solution for our problem for $y = 23$ and a second application of Theorem 5, using now $y \geq 39$ improves our upper bound, as desired, to $q < 420$. Here, we choose the other parameters in Theorem 5 by "optimizing" over the possibilities corresponding to (14) (in practice, we try about 10^4 different pairs (k, μ) and select the one that leads to the best bound).

The second straightforward case to treat is when y and 2^c+1 are multiplicatively dependent. Under this assumption, after a little work, we find that either

$$2^a + 2^b + 9 = 3^q \tag{i}$$

or

$$2^a + 2^b + C = C^q, \tag{ii}$$

where $C = 2^c + 1$ and $c \neq 3$. In the first case, it follows that $3^{q-2} \equiv 1 \pmod{2^b}$, which, with $b \geq 2$, contradicts the fact that q is odd. In case (ii), we write $q - 1 = 2^k Q$ where Q is odd, so that

$$\nu_2 \left(C^{2^k} - 1 \right) = b.$$

On the other hand, expanding via the binomial theorem, it is easy to see that

$$\nu_2 \left(C^{2^k} - 1 \right) \leq c + k + 2,$$

whereby $b \leq c + k + 2$. Since (ii) implies that $a \geq cq$, we thus have

$$b \leq c + k + 2 \leq \frac{a}{q} + \frac{\log q}{\log 2} + 2 \leq \frac{a}{q} + \frac{\log a}{\log 2} + 2.$$

Since we assume that $a > 100$ and $q > 420$, it follows that $a > 11b$, whereby, arguing as previously with Theorem 5 applied to (22) leads to a contradiction.

We may therefore suppose that $y \not\equiv 7 \pmod 8$ and that y and $2^c + 1$ are multiplicatively independent. For these remaining values, we must also appeal to estimates for linear forms in non-Archimedean logarithms. Let θ be a fixed real number, $0.2 \leq \theta < 1$, to be chosen later. We distinguish two cases, depending on whether $\theta a > b$ or $\theta a \leq b$. In the first case, we have

$$|2^a y^{-q} - 1| \leq \left(3 \cdot 2^{b-1} + 1 \right) y^{-q},$$

and thus

$$|a \log 2 - q \log y| < 2 \cdot 2^{a\theta} y^{-q} \leq 2\, y^{-q(1-\theta)}, \tag{23}$$

whereby we may apply Theorem 4 to the linear form $\Lambda = a \log 2 - q \log y$, to obtain an upper bound on q. As usual, we rewrite Λ as

$$\Lambda = r \log 2 - q \log(y/2^s), \quad \text{where } a = qs + r,\ |r| \leq \frac{q-1}{2}.$$

From Theorem 4, noticing that

$$h(y/2^s) = \log \max\{y, 2^s\} < \log \left(\sqrt{2}\, y \right),$$

we obtain

$$\log |\Lambda| \geq -25.2 \left(\max\left\{ \log b' + 0.38, 10 \right\} \right)^2 \log \left(\sqrt{2}\, y \right),$$

where

$$b' = q + \frac{|r|}{\log \left(\sqrt{2}\, y \right)}.$$

We thus have

$$\log|\Lambda| \geq -25.2 \left(\max\left\{ \log\left(q + \frac{q-1}{2\log\left(\sqrt{2}\,y\right)} \right) + 0.38, 10 \right\} \right)^2 \log\left(\sqrt{2}y\right),$$

and hence, for each fixed θ, an bound of the shape $q \leq q_0(\theta) \leq q_0(0.2)$.

In the second case, we have $\theta a \leq b$, and so

$$\nu_2\left(2^a + 2^b\right) = \nu_2\left(y^q - (2^c+1)\right) = b \geq \theta a \geq \theta\left(\frac{q\log y}{2\log 2} - 1\right).$$

On the other hand, one can deduce an upper bound for $\nu_2\left(y^q - (2^c+1)\right)$ using Theorem 7.

From our initial bounds, we now apply Theorems 5 and 7 to obtain a sharpened upper bound of the shape $q < 1230$, using only the inequality $y \geq 11$. After a routine verification that there are no further solutions with $y < 3000$, we apply again the same strategy and we obtain now the inequality $q < 730$. After a rather more painful calculation, we find that there are no (new) solutions for $y \leq 10^5$.

Now, as we may, we suppose $y > 10^5$ and use that $y \neq 2^c + 1$ (so that $y > 3 \cdot 2^c$). To obtain good results, we choose a suitable value for θ, say θ_c, for each value of c. And we find that $q \leq q_0$, where

(24)

c	θ_c	q_0	c	θ_c	q_0	c	θ_c	q_0
1	0.47	499	2	0.54	597	3	0.39	413
4	0.34	381	5	0.32	367	≥ 6	0.35	363

Here we have chosen one of the two pairs $(L, \rho) = (9, 10)$ or $(8, 11)$ in the Archimedean case and $L = 10$ for the 2–adic lower bound. The (extensive) details of our parameter choices are available, as before at the website http://math.ubc.ca/∼bennett/BeBuMi-data. Note that, for $c \geq 3$, these upper bounds contradict our assumption that $q > 420$.

We finish the proof of Theorem 2 by finding suitable local obstructions to solvability of equation (2) for the remaining quadruples (a, b, c, q) under consideration, namely

(25) $$a > b > c \geq 1, \text{ with } q \in \{5, 6, 7, 8, 9\} \text{ or } 11 \leq q \leq 419 \text{ prime},$$

(26) $$a > b > c = 1, \text{ with } 421 \leq q \leq 499 \text{ prime}$$

and

(27) $$a > b > c = 2, \text{ with } 421 \leq q \leq 593 \text{ prime}.$$

Our local arguments in this situation are necessarily more involved than for those with only 3 "digits". As previously, for fixed q, with either $q \in \{6, 8, 9\}$ or $q \geq 5$ prime, we choose a prime $p_1 \equiv 1 \pmod{q}$

dividing $2^{Mq}-1$ for relatively small M, and then produce a set of triples (a,b,c) such that (2) is solvable modulo p_1. Constructing such a set requires us to test $\gg q^3$ such triples which can prove computationally taxing. Subsequently, we determine for which of these triples equation (2) passes a local solubility test modulo a number of further p_i dividing, in each case, $2^{M_i q}-1$ for suitably small M_i. By way of example, if $q=167$, we start with $p_1 = 2349023$ for which $\text{ord}_2(p_1)=167$; our set of (a,b,c) modulo 167 contains 4705 triples (where we assume $a \geq b \geq c$). Taking

$$(p_2,p_3,p_4) = (514361, 6020351, 7322617),$$

where, in each case, we have $M_i = 7$, we find that the only triples for which (2) is solvable modulo $p_1 \cdot p_2 \cdot p_3 \cdot p_4$ are

$$(a,b,c) \equiv (1113, 809, 373) \;\text{ or }\; (1015, 527, 201) \pmod{7 \cdot 167}.$$

Choosing $p_5 = 304609$ and $p_6 = 223318747$ (with $M_5 = M_6 = 6$) then leads to the desired contradiction. We argue similarly to handle tuples (a,b,c,q) with $q < 421$, finishing case (25). The computation required to extend this approach to treat the particular case $q = 421$ for arbitrary (a,b,c) appears to be disproportionally large. For the tuples in (26) and (27), we apply the same arguments; the larger values of q here are feasible due to the fact that c is no longer variable.

Full details of our computations are again available at http://math.ubc.ca/∼bennett/BeBuMi-data. These calculations are quite time-consuming and are only really within range due to the strength of the bounds inherent in Theorems 5 and 7.

Acknowledgements: The authors would like to thank Umberto Zannier for providing us with his preprint [7].

References

[1] M. Bauer and M. Bennett, *Application of the hypergeometric method to the generalized Ramanujan-Nagell equation*, Ramanujan J. 6 (2002), 209–270.

[2] M. Bennett, *Effective measures of irrationality for certain algebraic numbers.* J. Austral. Math. Soc. Ser. A 62 (1997), no. 3, 329–344.

[3] M. A. Bennett, Y. Bugeaud, and M. Mignotte, *Perfect powers with few binary digits and related Diophantine problems.* Submitted for publication.

[4] F. Beukers, *On the generalized Ramanujan–Nagell equation. I.*, Acta Arith. 38 (1980/81), 389–410.

[5] Y. Bugeaud, *Linear forms in p-adic logarithms and the Diophantine equation* $(x^n-1)/(x-1)=y^q$, Math. Proc. Cambridge Philos. Soc. 127 (1999), 373–381.

[6] P. Corvaja and U. Zannier, *On the Diophantine equation* $f(a^m,y)=b^n$, Acta Arith. 94 (2000), 25–40.

[7] P. Corvaja and U. Zannier, *Finiteness of odd perfect powers with four nonzero binary digits*. Preprint.

[8] M. Laurent, *Linear forms in two logarithms and interpolation determinants. II.*, Acta Arith. 133 (2008), 325–348.

[9] M. Laurent, M. Mignotte and Y. Nesterenko, *Formes linéaires en deux logarithmes et déterminants d'interpolation*, J. Number Theory 55 (1995), 285–321.

[10] D. J. Leitner, *Two exponential Diophantine equations*, J. Théor. Nombres Bordeaux 23 (2011), 479–487.

[11] F. Luca, *The Diophantine equation* $x^2 = p^a \pm p^b + 1$, Acta Arith. 112 (2004), 87–101.

[12] R. Scott, *Elementary treatment of* $p^a \pm p^b + 1 = x^2$. Available online at the homepage of Robert Styer : http://www41.homepage.villanova.edu/robert.styer/ReeseScott/index.htm

[13] L. Szalay, *The equations* $2^n \pm 2^m \pm 2^l = z^2$, Indag. Math. (N.S.) 13 (2002), 131–142.

Michael A. Bennett, Department of Mathematics, University of British Columbia, Vancouver, British Columbia, V6T 1Z2, CANADA

E-mail address: bennett@math.ubc.ca

Yann Bugeaud, Mathématiques, Université de Strasbourg, 7, rue René Descartes, 67084 Strasbourg, FRANCE

E-mail address: bugeaud@math.unistra.fr

Maurice Mignotte, Mathématiques, Université de Strasbourg, 7, rue René Descartes, 67084 Strasbourg, FRANCE

E-mail address: mignotte@math.unistra.fr