MATHEMATICS OF COMPUTATION
Volume 87, Number 314, November 2018, Pages 2903–2914
http://dx.doi.org/10.1090/mcom/3298
Article electronically published on January 18, 2018

SEARCH FOR GOOD EXAMPLES OF HALL'S CONJECTURE

STÅL AANDERAA, LARS KRISTIANSEN, AND HANS KRISTIAN RUUD

Abstract. A good example of Hall's conjecture is a pair of natural numbers x, y such that $0 < |x^3 - y^2| < x^{1/2}$. We have implemented a new algorithm and found nine not previously known good examples. Moreover, we have verified that all good examples with $x < 10^{29}$ are now found.

1. Introduction

Consider the equation

$$x^3 - y^2 = k, \tag{1}$$

where $x, y \in \mathbb{N}$ and $k \in \mathbb{Z}$. It is easy to see that the equation has infinitely many solutions when $k = 0$ (let $x = t^2$ and $y = t^3$ where t is a natural number). By Siegel's theorem, there will be only finitely many solutions of the equation when $k \neq 0$. Moreover, it is hard to find solutions where k is small compared to x and y. Hall [4] conjectured that there is a constant C such that $|k| > Cx^{1/2}$ for any solution of (1) where $k \neq 0$. This conjecture is discussed in, e.g., Danilov [2] and Elkies [3]. The general opinion is that Hall's original conjecture is too strong, and his conjecture has been reformulated to a weaker modern variant: *For any exponent $e < \frac{1}{2}$, there exists a constant $C_e > 0$ such that $|k| > C_e x^e$.* For more on Hall's conjecture and further references, see Calvo et al. [1].

Hall's Conjecture is neither proved nor disproved. To shed some light on the conjecture, researchers have searched for solutions of (1) where $0 < |k| < x^{1/2}$. We follow the terminology of Calvo et al. [1] and refer to such solutions as *good examples of Hall's conjecture*. We will say that a pair of natural numbers (x, y) is a *good example* when $0 < |x^3 - y^2| < x^{1/2}$.

We have implemented a new algorithm for finding good examples. We have found 9 not previously known good examples, and we have checked that all good examples (x, y) where x is less than 10^{29} are now found. Other algorithms for finding good examples can be found in Elkies [3] and Calvo et al. [1]. The algorithm of Elkies has an asymptotic running time similar to ours. The algorithm of Calvo et al. seems to have slightly better asymptotic running time, but the authors offer no proof that their algorithm will detect all good examples within its search space. However, it is easily verified that the algorithm will find all the new good examples presented in this paper if it is given enough running time.

Received by the editor November 15, 2015, and, in revised form, November 16, 2016, and May 17, 2017.

2010 *Mathematics Subject Classification.* Primary 11Y50, 65A05; Secondary 11D25.

2. The algorithm

Definition 2.1. We define the polynomials B, C, F and H by

$$\begin{aligned} B(q,p,x) &= p^2 - q^2x, \\ C(q,p,x,y) &= p^3 - 3pq^2x + 2q^3y, \\ F(q,p,x,y) &= 4pC - 3B^2, \\ H(q,p,x,y) &= 9FB - 8C^2, \end{aligned}$$

where x, y, p, q are positive integers.

Our algorithm is based on the four polynomials given by the definition above. The values of these polynomials will be small when (x, y) is a good example and $\frac{p}{q}$ is the approximation to $x^{1/2}$ given by the next theorem.

Theorem 2.2. *Let (x, y) be a good example. Then, there exist $p, q, Q \in \mathbb{N}$, and $\delta \in \mathbb{R}$ such that*
(i) $p = qx^{1/2}(1 + \delta)$,
(ii) $0 < q < x^{1/6} < Q$, *and*
(iii) $\frac{1}{qx^{1/2}(Q+q)} < |\delta| < \frac{1}{qx^{1/2}Q}$.
Moreover, p and q are co-prime.

Proof. In this proof we use continued fractions. For more on continued fractions, see, e.g., Niven et al. [7] or Khintchine [6].

First we note that $x^{1/2}$ is an irrational number when (x, y) is a good example. (If $x^{1/2}$ is a natural number, then (x, y) will not be a good example as $x^3 - y^2 = 0$. But $x^{1/2}$ is either a natural number or an irrational number. Thus, $x^{1/2}$ is irrational.)

Let $a_0, a_1, a_2, \ldots$ be the coefficients for the continued fraction for $x^{1/2}$, that is,

$$x^{1/2} = \lim_{n\to\infty} [a_0; a_1, \ldots, a_n] .$$

The list of coefficients will be infinite as $x^{1/2}$ is irrational. Let h_i and k_i be, respectively, the nominator and the denominator of the convergent $[a_0; a_1, \ldots, a_i]$, that is, $\frac{h_i}{k_i} = [a_0; a_1, \ldots, a_i]$. Then, for any $i \in \mathbb{N}$, we have

$$\frac{1}{k_i(k_i + k_{i+1})} \;<\; \left|\frac{h_i}{k_i} - x^{1/2}\right| \;<\; \frac{1}{k_i k_{i+1}}$$

and $k_i < k_{i+1}$. Now, pick the least j such that $k_{j+1} > x^{1/6}$. Let $q = k_j$, let $p = h_j$ and let $Q = k_{j+1}$. Then, we have

$$\frac{1}{q(q + Q)} \;<\; \left|\frac{p}{q} - x^{1/2}\right| \;<\; \frac{1}{qQ},$$

where $q < x^{1/6} < Q$ (we cannot have $q = x^{1/6}$ as $x^{1/6} \notin \mathbb{N}$). Next, let δ be the real number such that $p = qx^{1/2}(1 + \delta)$. Then, we have

$$\frac{1}{q(q + Q)} \;<\; \left|\frac{qx^{1/2}(1 + \delta)}{q} - x^{1/2}\right| \;<\; \frac{1}{qQ} .$$

Thus

$$\frac{1}{qx^{1/2}(q + Q)} \;<\; |\delta| \;<\; \frac{1}{qx^{1/2}Q} .$$

Note that p and q are co-prime since h_j and k_j are co-prime for any convergent $\frac{h_j}{k_j}$. □

The proof of the next theorem will be given in Section 5.

Theorem 2.3. *Let (x, y) be a good example, where $x \neq 2$. Then, there exist co-prime natural numbers p and q such that $q < x^{1/6}$ and*

$$0 < C < 3qx^{1/6} + 1\,, \quad |F| < 8q + 1 \quad \text{and} \quad |H| < 72q^4 + 1\,.$$

In order to explain our algorithm, we introduce the notion of a good septuple.

Definition 2.4. Let $x, y, p, q, c \in \mathbb{N}$ and $f, h \in \mathbb{Z}$. The sequence (x, y, p, q, f, c, h) is a *good septuple* if p and q are co-prime and

$$q < x^{1/6}, \quad f = F(q, p, x, y), \quad c = C(q, p, x, y), \quad h = H(q, p, x, y),$$

and $|x^3 - y^2| < x^{1/2}$. We define the function $\mathbf{E}$ by

$$\mathbf{E}(q, f, c, h) = \begin{cases} (x, y) & \text{if there exists } p \text{ such that} \\ & (x, y, p, q, f, c, h) \text{ is a good septuple,} \\ (0, 0) & \text{otherwise.} \end{cases}$$

An algorithm for computing $\mathbf{E}(q, f, c, h)$. It follows from Definition 2.1 that

$$B = \frac{H + 8C^2}{9F}, \tag{2}$$

$$p = \frac{F + 3B^2}{4C}, \tag{3}$$

$$x = \frac{p^2 - B}{q^2}, \tag{4}$$

$$y = \frac{3pq^2x - p^3 + C}{2q^3}\,. \tag{5}$$

If (x, y, p, q, f, c, h) is a good septuple, we have $f = F(q, p, x, y)$ and $c = C(q, p, x, y)$ and $h = H(q, p, x, y)$. Thus, we can compute $\mathbf{E}(q, f, c, h)$ by the following procedure:

- Compute b such that $b = B$ and equality (2) holds. Use f, c, h for, respectively, F, C, H.
- Compute p such that equality (3) holds. Use f, c, b for, respectively, F, C, B.
- Compute x such that equality (4) holds. Use p, q, and use b for B.
- Compute y such that equality (5) holds. Use p, q, and use c for C.
- Check if (x, y, p, q, f, c, h) is a good septuple, that is, check if p, x, y are natural numbers and check if $|x^3 - y^2| < x^{1/2}$. If it is a good septuple, the output is (x, y); otherwise, the output is $(0, 0)$.

Overview of the algorithm. We are now ready to give an overview of our algorithm for finding good examples (where $x \neq 2$). A pair (x, y) is a good example if and only if there exist p, q, f, c, h such that (x, y, p, q, f, c, h) is good septuple (this follows straightforwardly from Theorem 2.3). Since $q < x^{1/6}$ when (x, y, p, q, f, c, h) is a good septuple, we can decide if (x, y) is a good example checking all good septuples where $q < x^{1/6}$. Our algorithm works by generating good septuples by a sieve method. The input to the algorithm is a natural number $x_{\max}$. The algorithm outputs all good examples (x, y), where $x < x_{\max}$. Figure 1 gives a high-level description of the algorithm.

```
q_max := ⌊x_max^{1/6}⌋.
for q := 1, 2, ..., q_max do
    begin
    Generate a set F_q of possible values for f.
    for each f ∈ F_q do
        begin
        Generate a set C_qf of possible values of c.
        for each c ∈ C_qf do
            begin
            Generate a set H_qfc of possible values for h.
            for each h ∈ H_qfc do
                begin
                (x, y) := E(q, f, c, h) (see Definition 2.4).
                Output (x, y) if (x, y) ≠ (0, 0).
                end
            end
        end
    end
```

FIGURE 1. The high-level description of our algorithm.

Our algorithm might also output good examples (x, y), where $x \geq x_{\max}$. If $x \geq x_{\max}$, there might exist a good septuple (x, y, p, q, f, c, h), where $q < x_{\max}^{1/6}$ and $c < 3qx_{\max}^{1/6}$. This is why our algorithm has found good examples with $x > 10^{29}$.

3. More on the algorithm

In this section we explain how the algorithm in Figure 1 computes the sets $\mathcal{F}_q$, $\mathcal{C}_{qf}$ and $\mathcal{H}_{qfc}$. We will also discuss the running time. The correctness of our algorithm is based on the next couple of lemmas.

Lemma 3.1. *We have:*

(i) $C \equiv p^3$, $F \equiv p^4$ *and* $H \equiv p^6 \pmod{q^2}$,
(ii) $H \equiv -8C^2 \pmod{9|F|}$,
(iii) $p^4 - 2pC + F \equiv 0$ *and* $H \equiv 5p^3C - 4p^6 \pmod{q^3}$,
(iv) *either* $F \equiv 0$ *or* $F \equiv 1 \pmod 4$,
(v) $|F|$ *and* q *are co-prime if* p *and* q *are co-prime.*

Proof. Clauses (i), (ii), and (iii) follow straightforwardly from Definition 2.1.

In the case when B is even there exists $i \in \mathbb{Z}$ such that

$$F = -3B^2 = -3(2i)^2 = -12i^2 .$$

Hence, we have $F \equiv 0 \pmod 4$ when B is even. A similar argument shows that $F \equiv 1 \pmod 4$ when B is odd. This proves (iv).

In order to see that (v) holds, assume that $|F|$ and q are not co-prime. Then there is a prime m that divides both $|F|$ and q. By (i), m will also divide p. Hence, p and q are not co-prime. □

The proof of the next lemma is straightforward.

Lemma 3.2. *Let m and n be natural numbers such that $m \le n$, and let $P(x)$ be a polynomial. Furthermore, let $x_0 \equiv x \pmod{q^m}$, and let $y \equiv P(x) \pmod{q^n}$. Then we have $y \equiv P(x_0) \pmod{q^m}$.*

3.1. **The construction of the set $\mathcal{F}_q$.** Assume that (x, y, p, q, f, c, h) is a good septuple. By Lemma 3.1 (i), we have $f \equiv p^4 \pmod{q^2}$. Now, let p_0 be any natural number such that $p_0 \equiv p \pmod{q}$. By Lemma 3.2, we have $f \equiv p_0^4 \pmod{q}$. Thus, f can be written in the form

$$f \;=\; (p_0^4 \mod q) \;+\; iq \tag{6}$$

for some $i \in \mathbb{Z}$ and some p_0, where $p_0 < q$. By Theorem 2.3 we have

$$-(8q+1) \;<\; f \;<\; 8q+1 \tag{7}$$

and by Lemma 3.1 (iv), we have

$$f \equiv 0 \text{ or } f \equiv 1 \pmod 4. \tag{8}$$

If $q > 1$, our algorithm computes the set $\mathcal{F}_q$ such that $f \in \mathcal{F}_q$ iff (6), (7), and (8) hold. In the case when $q = 1$, for the algorithm let

$$\mathcal{F}_q \;=\; \{\,-8\,,\,-7\,,\,-4\,,\,-3\,,\,0\,,\,1\,,\,4\,,\,5\,,\,8\,\}\,.$$

Note that we only need q to determine the set $\mathcal{F}_q$ (in particular we do not need the value of p).

3.2. **The construction of the set $\mathcal{C}_{qf}$.** Assume that (x, y, p, q, f, c, h) is a good septuple where $x < x_{\max}$. By Lemma 3.1 (i), we have $f \equiv p^4 \pmod{q^2}$. Let p_1 be any natural number such that $p_1 \equiv p \pmod{q^2}$. By Lemma 3.2, we have $f \equiv p_1^4 \pmod{q^2}$. Hence,

$$p_1^4 \;=\; f \;+\; iq^2 \tag{9}$$

for some $i \in \mathbb{Z}$. Let $p_1 \in \mathcal{P}_1$ iff $0 < p_1 < q^2$ and (9) holds. Our algorithm computes the set $\mathcal{P}_1$ from q and f (the set will contain at most four elements).

By Lemma 3.1 (i), we have $c \equiv p^3 \pmod{q^2}$. By Lemma 3.2, we have $c \equiv p_1^3 \pmod{q^2}$. Hence, c can be written in the form

$$c \;=\; (p_1^3 \mod q^2) \;+\; iq^2 \tag{10}$$

for some $p_1 \in \mathcal{P}_1$ and some $i \in \mathbb{Z}$. By Theorem 2.3, we have $0 < c < 3qx^{1/6} + 1$. Recall that $q_{\max} = \lfloor x_{\max}^{1/6} \rfloor$. Hence

$$0 \;<\; c \;\le\; 3qq_{\max} + 1\,. \tag{11}$$

If $q > 1$, our algorithm computes the set $\mathcal{C}_{qf}$ such that $c \in \mathcal{C}_{qf}$ iff (10) and (11) holds. If $q = 1$, the algorithm computes the set $\mathcal{C}_{qf}$ such that $c \in \mathcal{C}_{qf}$ iff (11) holds. We need q, $q_{\max}$ and the set $\mathcal{P}_1$ to determine the set $\mathcal{C}_{qf}$ (and we need q and $f \in \mathcal{F}_q$ to determine $\mathcal{P}_1$).

3.3. **The construction of the set $\mathcal{H}_{qcf}$.** Assume that (x, y, p, q, f, c, h) is a good septuple. Let p_2 be such that $p_2 \equiv p \pmod{q^3}$. By Lemma 3.1 (iii), we have $p^4 - 2pc + f \equiv 0 \pmod{q^3}$. By Lemma 3.2, we have

$$p_2^4 - 2p_2c + f \equiv 0 \pmod{q^3}\,. \tag{12}$$

Our algorithm computes the set $\mathcal{P}_2$ such that $p_2 \in \mathcal{P}_2$ iff $0 \leq p_2 < q^3$ and (12) holds. We need q, $c \in \mathcal{C}_{qf}$ and $f \in \mathcal{F}_q$ to determine the set $\mathcal{P}_2$.

By clause (ii) and (iii) of Lemma 3.1 and Lemma 3.2, there is $p_2 \in \mathcal{P}_2$ such that

$$h \equiv -8c^2 \pmod{9|f|} \quad \text{and} \quad h \equiv 5p_2^3c - 4p_2^6 \pmod{q^3}\,. \tag{13}$$

By Theorem 2.3, we have

$$-(72q^4 + 1) < h < 72q^4 + 1\,. \tag{14}$$

The case when 3 *does not divide* q. We will now explain how our algorithm computes the set $\mathcal{H}_{qfc}$ when 3 does not divide q. We know that p and q are co-prime (since (x, y, p, q, f, c, h) is a good septuple). By Lemma 3.1 (v), $|f|$ and q are co-prime. Thus, $9|f|$ and q^3 will also be co-prime since 3 does not divide q. The Chinese Remainder Theorem and (13) yield h_1 such that

$$0 \leq h_1 < 9|f|q^3 \quad \text{and} \quad h = h_1 + i9|f|q^3 \tag{15}$$

for some $i \in \mathbb{Z}$. Let $\mathbf{S}(q, p_2, f, c)$ denote the unique h_1 such that (15) holds. The number $\mathbf{S}(q, p_2, f, c)$ can be computed from q, p_2, f, c by the Euclidean method. If $q > 1$, our algorithm computes the set $\mathcal{H}_{qfc}$ such that $h \in \mathcal{H}_{qfc}$ iff (14) holds and $h = \mathbf{S}(q, p_2, f, c) + i9|f|q^3$ for some $p_2 \in \mathcal{P}_2$ and some $i \in \mathbb{Z}$. The set $\mathcal{H}_{qfc}$ will be computed by a tailored algorithm when $q = 1$.

The case when 3 *divides* q. By Lemma 3.1 (v), $|f|$ and q are co-prime. Thus, if 3 divides q, the greatest common divisor of $9|f|$ and q^3 will be 9. The equations in (13) have a solution iff $h \equiv -8c^2 \pmod 9$. If there is a solution, the Chinese Remainder Theorem yields h_1 such that

$$0 \leq h_1 < |f|q^3 \quad \text{and} \quad h = h_1 + i|f|q^3 \tag{16}$$

for some $i \in \mathbb{Z}$, and our algorithm can proceed as described in the case when 3 does not divide q.

We need q, $f \in \mathcal{F}_q$, $c \in \mathcal{C}_{qf}$, and the set $\mathcal{P}_2$ to determine $\mathcal{H}_{qfc}$ (and we need q, $f \in \mathcal{F}_q$, $c \in \mathcal{C}_{qf}$ to determine $\mathcal{P}_2$).

3.4. **The running time.** Let $|\mathcal{S}|$ denote the number of elements in the set $\mathcal{S}$. It is easy to see that $|\mathcal{F}_q| \leq 17q$. It follows from (10) and (11) that

$$|\mathcal{C}_{qf}| \leq \frac{|\mathcal{P}_1|(3qq_{\max} + 1)}{q^2}\,.$$

We have computed the set $\mathcal{P}_1$ from q and f, but the number of elements in the set will not depend on q or f (tedious considerations will show that $|\mathcal{P}_1| \leq 4$). Hence there is a constant k such that $|\mathcal{C}_{qf}| \leq (kq_{\max})/q$. We can now determine an upper

TABLE 1. Good examples of Hall's conjecture.

#	x	r	$\frac{p}{q}$	Comments
⋮				1)
41	1074783508347108126882585 6	1.35	$\frac{42884607802081920}{13081}$	2)
42	37223900078734215181946587	1.87	$\frac{467774345862973 19}{7667}$	3)
43	69586951610485633367491417	1.22	$\frac{72198966044283893}{8655}$	4)
44	36904453831732273063766347 20	1.51	$\frac{121619570207840431}{2002}$	3)
45	13354576357426205461714764 1349	1.69	$\frac{17888245804569497941}{48950}$	4)
46	16292129774381720734239614 0787	10.65	$\frac{20237053244197156774}{50137}$	4)
47	37419269089621921087812164 5171	2.97	$\frac{335053515165048478 93}{54773}$	4)
48	40184477450081878116462382 1177	1.29	$\frac{30878500908406560580}{48711}$	4)
49	50085922458864610640366900 9291	1.06	$\frac{442880396580683213 15}{62579}$	4)
50	11145923086309958051235711 51844	1.04	$\frac{955246406702660924 18}{90481}$	5)
51	39739590925054773507790363 346813	3.75	$\frac{211515916260522809737}{33553}$	4)
52	86261114381072476361336611 6643858	1.10	$\frac{930889835660831460142}{31695}$	4)
53	10625217510247713765900622 79975859	1.01	$\frac{109526981085078598 4986}{33601}$	4)
54	60786730431260840650079021 75846955	1.03	$\frac{20224028423712303104623}{259396}$	3)

1) The first 40 entries of the table can be found in [1]. These entries are found by Hall [4], Gebel et al. [5], Elkies [3], Calvo et al. [1], and Johan Bosman using the software of Calvo et al. [1]
2) Found by Jiménez Calvo [8].
3) Found by Calvo et al. [1].
4) Found by the authors of this paper.
5) From the Danilov-Elkies infinite Fermat-Pell family, see [3] or [1].

bound for how many times the third loop in Figure 1 will be executed. We have

$$\begin{aligned}\sum_{q=1}^{q_{\max}} \sum_{f\in\mathcal{F}_q} |\mathcal{C}_{qf}| \;&\le\; \sum_{q=1}^{q_{\max}} \sum_{f\in\mathcal{F}_q} \frac{kq_{\max}}{q} \;\le\; 17q_{\max} \sum_{q=1}^{q_{\max}} \frac{kq_{\max}}{q} \\ &= kq_{\max}17q_{\max} \sum_{q=1}^{q_{\max}} \frac{1}{q} \;=\; O(q_{\max}^2 \log q_{\max})\,.\end{aligned}$$

This shows that the number of times the loop **for each** $c \in \mathcal{C}_{qf} \ldots$ will be executed is of order $O(q_{\max}^2 \log q_{\max})$.

It follows from (14), (15), and (16) that there exists a constant k such that the number of elements in $\mathcal{H}_{qfc}$ is bounded by kq. Thus the number of elements in $\mathcal{H}_{qfc}$ is of order $O(q_{\max})$. This entails that the innermost loop of the algorithm in Figure 1 will be executed $O(q_{\max}^2 \log q_{\max}) \times O(q_{\max})$ times. In the innermost loop numbers will be added, multiplied and divided. The running time of these arithmetical computations will be of order $O(\log^2 x)$. Thus, as $q_{\max} = \lfloor x_{\max}^{1/6} \rfloor$ and $x < x_{\max}$, our algorithm runs in time

$$\begin{aligned}&O(q_{\max}^2 \log q_{\max}) \times O(q_{\max}) \times O(\log^2 x_{\max}) \\ &\quad = O(q_{\max}^3 \log q_{\max}) \times O(\log^2 x_{\max}) \;=\; O((x_{\max}^{1/6})^3 \log x_{\max}^{1/6}) \times O(\log^2 x_{\max}) \\ &\quad = O(x_{\max}^{1/2} \log^{O(1)} x_{\max})\,.\end{aligned}$$

The algorithm of Elkies [3] has a similar running time.

4. Computations and results

A first implementation of the algorithm was written in Python. The results of test runs looked promising, and we reimplemented the algorithm in C using the Gnu Multi-Precision library to carry out operations with arbitrary-length integers. The C implementation was run with $q_{\max} = 10000$ (corresponding to a $x_{\max}$ of 10^{24}). The run lasted for 1368 processor-hours, and after 840 processor-hours the algorithm found example #43 in Table 1. A subsequent run, with $q_{\max} = 20000$ (corresponding to a $x_{\max}$ of 64×10^{24}), lasted for 10580 processor-hours and found an example that was earlier found by Calvo et al. [1].

After these experiences we modified our C code to be run on the Norwegian national computing facilities (Notur). The computations at national facilities took about 1.3 million processor-hours. Our computations have detected 9 previously unknown good examples and verified that all good examples where x is less than 10^{29} are included in Table 1.

The second column of Table 1 shows the x of a good example (x, y). The r appearing in the third column of the table, is given by $r = x^{1/2}/(x^3 - y^2)$. High values of r indicate that (the original) Hall's conjecture is false. The fourth column shows the rational approximation $\frac{p}{q}$ to $x^{1/2}$.

5. The proof of Theorem 2.3

Throughout this section we will use w to denote $x^{1/2}$ and k to denote $x^3 - y^2$.

Lemma 5.1. *Let (x, y) be a good example. Then there exists $\gamma \in \mathbb{R}$ such that*

$$y = x^{3/2}(1+\gamma) \quad \textit{and} \quad \frac{|k|-1}{2x^3} \;<\; |\gamma| \;<\; \frac{|k|+1}{2x^3}\,.$$

Proof. Let $\gamma \in \mathbb{R}$ be such that $y = x^{3/2}(1+\gamma)$. Then we have

$$y \;=\; x^{3/2}(1+\gamma) \;=\; w^3(1+\gamma)\,. \tag{17}$$

Furthermore, we have

$$\begin{aligned}
\gamma w^3 &= w^3(1+\gamma) - w^3 \\
&= y - w^3 && (17),\\
&= (y^2 - w^6)/(y + w^3) \\
&= (y^2 - x^3)/(y + w^3) && \text{since } w = x^{1/2},\\
&= -k/(y + w^3) && \text{since } x^3 - y^2 = k.
\end{aligned}$$

This establishes that $\gamma w^3 = -k/(y + w^3)$, and thus $\gamma = -k/w^3(y + w^3)$. Furthermore, since $|k| < w = x^{1/2}$ and $x \geq 2$, we have

$$|\gamma| \;=\; \frac{|k|}{w^3(y+w^3)} \;<\; \frac{|k|}{w^6} \;<\; \frac{1}{w^5} \;<\; 1\,. \tag{18}$$

We also have

$$|\gamma| \;=\; \frac{|k|}{2w^6}\frac{1}{(1+\frac{1}{2}\gamma)} \tag{19}$$

since

$$|\gamma| \overset{(18)}{=} \frac{|k|}{w^3(y+w^3)} \overset{(17)}{=} \frac{|k|}{w^3(w^3(1+\gamma)+w^3)} = \frac{|k|}{w^6(2+\gamma)} = \frac{|k|}{2w^6}\frac{1}{(1+\frac{1}{2}\gamma)}.$$

Next we prove that

$$1-|\gamma| < \frac{1}{(1+\frac{\gamma}{2})} < 1+|\gamma|. \tag{20}$$

Let r be a real number such that $0<r<1$. Then we have

$$1 < 1+\frac{r}{2}-\frac{r^2}{2} = (1+r)(1-\frac{r}{2})$$

and thus $1/(1-\frac{r}{2}) < 1+r$. By (18), we have $|\gamma|<1$. Hence, if $\gamma>0$, we have

$$\frac{1}{1+\frac{\gamma}{2}} < \frac{1}{1-\frac{\gamma}{2}} < 1+\gamma = 1+|\gamma|$$

and if $\gamma<0$, we have

$$\frac{1}{1+\frac{\gamma}{2}} = \frac{1}{1-\frac{|\gamma|}{2}} < 1+|\gamma|.$$

This shows that $1/(1+\frac{\gamma}{2}) < 1+|\gamma|$. A symmetric argument shows that $1-|\gamma| < 1/(1+\frac{\gamma}{2})$. Use that

$$1 > 1-\frac{r}{2}-\frac{r^2}{2} = (1-r)(1+\frac{r}{2})$$

when $0<r<1$. This concludes the proof of (20).

By (19) and (20), we have

$$\frac{|k|-|k||\gamma|}{2w^6} = \frac{|k|(1-|\gamma|)}{2w^6} < |\gamma| < \frac{|k|(1+|\gamma|)}{2w^6} = \frac{|k|+|k||\gamma|}{2w^6}.$$

Finally, as $|k||\gamma| < \frac{1}{w^4} < 1$, we have

$$\frac{|k|-1}{2w^6} < |\gamma| < \frac{|k|+1}{2w^6}.$$

This proves the lemma as $w = x^{1/2}$. □

We are now ready to prove Theorem 2.3. Let (x,y) be a good example where $x \neq 2$. We need to prove that there exist co-prime natural numbers p and q such that $q \leq x^{1/6}$ and:

(Claim 1) $$0 < C(q,p,x,y) < 3qx^{1/6}+1.$$

(Claim 2) $$|F(q,p,x,y)| < 8q+1.$$

(Claim 3) $$|H(q,p,x,y)| < 72q^4+1.$$

By Theorem 2.2 and Lemma 5.1, we have $\delta,\gamma \in \mathbb{R}$ and $p,q,Q \in \mathbb{N}$ such that p and q are co-prime and

$$p = qw(1+\delta) \quad \text{and} \quad y = w^3(1+\gamma). \tag{21}$$

Moreover, we have the following bounds:

$$0 \;<\; q \;<\; w^{1/3} \;<\; Q, \tag{22}$$

$$|\delta| \;<\; \frac{1}{qwQ}, \tag{23}$$

$$|\gamma| \;<\; \frac{|k|}{2w^6}\,. \tag{24}$$

Note that we also have $|k| < w$ as (x, y) is a good example. Furthermore, note that (x, y) is a good example where $x \neq 2$. There are no other good examples where x is less than 5234 except the one where $x = 2$. It follows that $w > 72$ and $Q > 4$.

The Proof of (Claim 1). The definition of C says that

$$C \;=\; p^3 - 3pq^2x + 2q^3y. \tag{25}$$

By (21) and (25), we have $C = q^3w^3(\delta^3 + 3\delta^2 + 2\gamma)$ (substitute $qw(1 + \delta)$ and $w^3(1 + \gamma)$ for, respectively, p and y and simplify the expression).

First we prove $0 < C$. It follows from (23) that $|\delta| < \frac{1}{2}$, and thus we have

$$\delta^3 + 3\delta^2 \;=\; 2\delta^2 + \delta^2(1 + \delta) \;>\; 0. \tag{26}$$

If $\gamma \geq 0$, it follows trivially from (26) that $0 < C$. If $\gamma < 0$, then $y < w^3$, i.e., $x^3 - y^2 = k > 0$. Then we have

$$C \;=\; q^3w^3(\delta^3 + 3\delta^2 + 2\gamma) \overset{(26)}{>} q^3w^3 2\gamma \overset{(24)}{>} q^3w^3 2\frac{-|k|}{2w^6} \;=\; \frac{-q^3|k|}{w^3}$$

$$\overset{(22)}{>} \frac{-|k|}{w^2} \;>\; -1\,.$$

This proves that $C > -1$. We will now prove that $C \neq 0$ (and thus we have $C > 0$).

Assume that $C = 0$ (we prove that (x, y) is not a good example). By (25), we have $p^3 = q(2q^2y - 3pqx)$. This shows that any prime divisor of q divides p, but p and q are co-prime, and thus $q = 1$. Equation (25) with $C = 0$ and $q = 1$ gives

$$0 \;=\; p^3 - 3px + 2y. \tag{27}$$

We will prove that a solution of (27) cannot yield a good example. The proof splits into the three cases: the case when $x = p^2$, the case when $x > p^2$, and the case when $x < p^2$.

Assume $x = p^2$. Then $y = p^3$ gives a solution of (27), but $x^3 - y^2 = 0$. Thus, (x, y) is not a good example.

Assume $x > p^2$. Then we have $x = p^2 + m$ for some positive natural number m. Thus

$$x^3 \;=\; (p^2 + m)^3 \;=\; p^6 + 3p^4m + 3p^2m^2 + m^3.$$

By (27) we have

$$y \;=\; \frac{3px - p^3}{2} \;=\; \frac{3p(p^2 + m) - p^3}{2} \;=\; p^3 + \frac{3pm}{2}$$

and

$$y^2 \;=\; p^6 + 3p^4m + \frac{9p^2m^2}{4}\,.$$

Hence

$$x^3 - y^2 \;=\; \frac{3p^2m^2}{4} + m^3 \;>\; p$$

and we conclude that (x, y) is not a good example as $p \approx x^{1/2}$. A similar argument shows that (x, y) is not a good example if $x < p^2$. This proves that $C > 0$.

Next we prove that $C < 3qw^{1/3} + 1$. This will complete the proof of (Claim 1) since $w^{1/3} = x^{1/6}$. We have

$$C \;=\; q^3w^3(\delta^3 + 3\delta^2 + 2\gamma) \;\le\; q^3w^3(|\delta|^3 + 3|\delta|^2 + 2|\gamma|)$$

$$\overset{(23,24)}{<} q^3w^3\left(\left[\frac{1}{qwQ}\right]^3 + 3\left[\frac{1}{qwQ}\right]^2 + 2\left[\frac{|k|}{2w^6}\right]\right) \;=\; \frac{1}{Q^3} + \frac{3qw}{Q^2} + \frac{q^3|k|}{w^3}$$

$$\overset{(22)}{<} \frac{1}{w} + 3qw^{1/3} + \frac{|k|}{w^2} \;<\; \frac{1}{w} + 3qw^{1/3} + \frac{1}{w}\,.$$

Thus, we have $C < 3qw^{1/3} + 1$ as $w = x^{1/2} > 72$ in any good example where $x \neq 2$.

The Proof of (Claim 2). It follows straightforwardly from Definition 2.1 that $F = p^4 - 6p^2q^2w^2 + 8pq^3y - 3q^4w^4$. By (21), we have $F = q^4w^4(\delta^4 + 4\delta^3 + 8\gamma + 8\gamma\delta)$. We have

$$|F| \;\le\; q^4w^4(|\delta|^4 \,+\, 4|\delta|^3 \,+\, 8|\gamma| \,+\, 8|\gamma||\delta|)$$

$$\overset{(23,24)}{<} q^4w^4\left(\left[\frac{1}{qwQ}\right]^4 \,+\, 4\left[\frac{1}{qwQ}\right]^3 \,+\, 8\left[\frac{|k|}{2w^6}\right] \,+\, 8\left[\frac{|k|}{2w^6}\right]\left[\frac{1}{qwQ}\right]\right)$$

$$= \;\frac{1}{Q^4} \,+\, \frac{4qw}{Q^3} \,+\, \frac{4q^4|k|}{w^2} \,+\, \frac{4q^3|k|}{w^3Q} \;<\; \frac{1}{Q^4} \,+\, \frac{4qw}{Q^3} \,+\, \frac{4q^4}{w} \,+\, \frac{4q^3}{w^2Q}$$

$$\overset{(22)}{<} \;\frac{1}{Q^4} \,+\, 4q \,+\, 4q \,+\, \frac{4}{wQ}\,.$$

Thus, $|F| < 8q + 1$ as $w > 72$ and $Q > 4$.

The Proof of (Claim 3). It follows straightforwardly from Definition 2.1 that

$$H \;=\; p^6 - 15p^4q^2w^2 + 40p^3q^3y - 45p^2q^4w^4 + 24q^5pw^2y + 27q^6w^6 - 32q^6y^2\,.$$

By (21), we have

$$H \;=\; q^6w^6(144\delta\gamma - 32\gamma^2 + 40\delta^3\gamma + 120\delta^2\gamma + 6|\delta|^5 + |\delta|^6)\,.$$

In order to prove that that $|H| < 72q^4 + 1$, we need

$$q^6w^6(32|\gamma|^2 + 40|\delta|^3|\gamma| + 120|\delta|^2|\gamma| + 6|\delta|^5 + |\delta|^6) \;<\; 1 \tag{28}$$

and

$$144q^6w^6|\delta||\gamma| \;\overset{(23,24)}{<}\; 144q^6w^6\left[\frac{1}{qwQ}\right]\left[\frac{|k|}{2w^6}\right] \;=\; \frac{72q^5|k|}{wQ} \;\overset{(22)}{<}\; 72q^4\,. \tag{29}$$

The proof of (28) is tedious, but straightforward. Use that $|k| < w$, that $q < w^{1/3} < Q$, that $w > 72$, and that $Q > 4$.

Now we have

$$\begin{aligned} |H| &\leq q^6w^6(144|\delta||\gamma| + 32|\gamma|^2 + 40|\delta|^3|\gamma| + 120|\delta|^2|\gamma| + 6|\delta|^5 + |\delta|^6) \\ &= 144q^6w^6|\delta||\gamma| \quad + \quad q^6w^6(32|\gamma|^2 + 40|\delta|^3|\gamma| + 120|\delta|^2|\gamma| + 6|\delta|^5 + |\delta|^6)\ . \end{aligned}$$

Thus, we have $|H| < 72q^4 + 1$ by (28) and (29).

Acknowledgments

The authors want to thank the referees and the editor for valuable advice regarding the presentation. Furthermore, the authors want to thank N. D. Elkies for comments on an earlier version of this paper and R. H. Johansen for helpful advice on parallel programming. The authors gratefully acknowledge the support from the Norwegian meta-center for computational science (Notur).

References

[1] I. Jiménez Calvo, J. Herranz, and G. Sáez, *A new algorithm to search for small nonzero $|x^3 - y^2|$ values*, Math. Comp. **78** (2009), no. 268, 2435–2444, DOI 10.1090/S0025-5718-09-02240-6. MR2521296

[2] L. V. Danilov, *The Diophantine equation $x^3 - y^2 = k$ and a conjecture of M. Hall* (Russian), Mat. Zametki **32** (1982), no. 3, 273–275, 425. MR677595

[3] N. D. Elkies, *Rational points near curves and small nonzero $|x^3 - y^2|$ via lattice reduction*, Algorithmic number theory (Leiden, 2000), Lecture Notes in Comput. Sci., vol. 1838, Springer, Berlin, 2000, pp. 33–63, DOI 10.1007/10722028_2. MR1850598

[4] M. Hall Jr., *The Diophantine equation $x^3 - y^2 = k$*, Computers in number theory (Proc. Sci. Res. Council Atlas Sympos. No. 2, Oxford, 1969), Academic Press, London, 1971, pp. 173–198. MR0323705

[5] J. Gebel, A. Pethö, and H. G. Zimmer, *On Mordell's equation*, Compositio Math. **110** (1998), no. 3, 335–367, DOI 10.1023/A:1000281602647. MR1602064

[6] A. Ya. Khintchine, *Continued Fractions*, Translated by Peter Wynn, P. Noordhoff, Ltd., Groningen, 1963. MR0161834

[7] I. Niven, H. S. Zuckerman, and H. L. Montgomery, *An Introduction to the Theory of Numbers*, 5th ed., John Wiley & Sons, Inc., New York, 1991. MR1083765

[8] `http://ijcalvo.galeon.com/hall.htm`

Department of Mathematics, University of Oslo, P.O. Box 1053 Blindern, NO-0316 Oslo, Norway

Email address: `staal@math.uio.no`

Department of Mathematics, University of Oslo, P.O. Box 1053 Blindern, NO-0316 Oslo, Norway

Email address: `larsk@math.uio.no`

Department of Mathematics, University of Oslo, P.O. Box 1053 Blindern, NO-0316 Oslo, Norway