MATHEMATICS OF COMPUTATION
Volume 72, Number 244, Pages 2099–2110
S 0025-5718(03)01465-0
Article electronically published on May 1, 2003

A COMPUTATIONAL APPROACH FOR SOLVING $y^2 = 1^k + 2^k + \cdots + x^k$

M. J. JACOBSON, JR., Á. PINTÉR, AND P. G. WALSH

Abstract. We present a computational approach for finding all integral solutions of the equation $y^2 = 1^k + 2^k + \cdots + x^k$ for even values of k. By reducing this problem to that of finding integral solutions of a certain class of quartic equations closely related to the Pell equations, we are able to apply the powerful computational machinery related to quadratic number fields. Using our approach, we determine all integral solutions for $2 \leq k \leq 70$ assuming the Generalized Riemann Hypothesis, and for $2 \leq k \leq 58$ unconditionally.

1. Introduction

É. Lucas [18] proved that the diophantine equation

$$y^2 = 1^2 + 2^2 + \cdots + x^2 \tag{1}$$

has only the solutions $x = y = 1$ and $x = 24$, $y = 70$. Schäffer [20] furthered this work by studying the more general equation

$$y^q = 1^k + 2^k + \cdots + x^k. \tag{2}$$

The main result of this work was a proof that the only positive integers ($k \geq 1$, $q > 1$) for which this equation has infinitely many solutions are

$$(k, q) \in \{(1, 2), (3, 2), (3, 4), (5, 2)\}.$$

Schäffer also made the following

Conjecture 1.1 ([20])**.** Let k and $q > 1$ be positive integers, with (k, q) not in the above list. Then apart from the solution $(x, y) = (24, 70)$ when $k = q = 2$, the only solution to equation (2) is the trivial solution $x = y = 1$.

In recent years there have been numerous papers on this topic (see [2], [3], [7], [10], [22]). The interested reader may wish to refer to the notes at the end of chapter 10 in [21].

In a recent paper [4], the authors prove the following

Received by the editor June 5, 2001.

2000 *Mathematics Subject Classification.* Primary 11D25, 11J86.

Key words and phrases. Diophantine equations, elliptic curves, quadratic fields.

The first and third authors are supported by the Natural Sciences and Engineering Research Council of Canada.

The second author is supported by the Hungarian National Foundation for Scientific Research, grants T29330, F34891, and FKFP-066-2001.

Theorem 1.1 ([4])**.** *For $k \geq 2$ even, the equation*

$$y^2 = 1^k + 2^k + \cdots + (x-1)^k \tag{3}$$

has at most $\max\{c_1, 9^k\}$ *solutions in integers x and y, where c_1 is an effectively computable absolute constant.*

Although this theorem does not prove Conjecture 1.1, its proof provides a methodology for finding all integer solutions to equation (3). In particular, this was the goal in [19], wherein Pintér found all solutions to (3) for $k \in \{2, 4, 6, 8, 10, 14\}$.

The purpose of the present paper is to improve on the result in [19] by reducing the problem to finding all integer points on a certain class of quartic equations, and appealing to the ideas from [1] to improve the computation. As a result of this reduction, we can improve upon [19] as follows.

Theorem 1.2. *For $2 \leq k \leq 58$ and k even, the only positive integer solution (x, y) to equation* (3) *is the trivial solution $(x, y) = (2, 1)$, except in the case $k = 2$, for which there is the anomalous solution $(x, y) = (25, 70)$. Under the assumption of the Generalized Riemann Hypothesis* (*GRH*)*, the result also holds in the range $60 \leq k \leq 70$.*

The dependence of Theorem 1.2 on the GRH is due to our algorithm's use of a conditional subexponential algorithm for computing the regulator of a real quadratic field [11]. This is explained in more detail on Section 5

2. Reduction to a family of quartic diophantine equations

We begin by following the argument in [19]. For $k > 0$, we define $S_k(x)$ to be the polynomial

$$S_k(x) = 1^k + 2^k + \cdots + (x-1)^k.$$

It is well known that for k even, $(k+1)S_k(x) = B_{k+1}(x)$, where $B_{k+1}(x)$ represents the $k+1$-st Bernoulli polynomial (see [8] for details on Bernoulli numbers and polynomials). Suppose that $k \geq 2$ is even, and that (x, y) is a positive integer solution to $y^2 = S_k(x)$. From the above remark we have

$$\begin{aligned}(k+1)y^2 &= (k+1)S_k(x)\\ &= B_{k+1}(x) = \binom{k+1}{1} B_k x + \binom{k+1}{3} B_{k-2} x^3 + \cdots + x^{k+1},\end{aligned}$$

where $B_i (i \geq 0)$ is the ith Bernoulli number. Define d_k to be the minimal positive integer such that $d_k(k+1)S_k(x)$ has integer coefficients. It follows that

$$d_k(k+1)y^2 = x((k+1)d_k B_k + x^2 f(x)),$$

with $f(X)$ a polynomial with integer coefficients. Therefore, $x = au^2$ with $u \geq 1$, $a \geq 1$ square-free, and a divides $(k+1)d_k^2 B_k$.

From the relation

$$B_{k+1}(X) = (-1)^{k+1} B_{k+1}(1 - X),$$

we deduce that $x - 1 = cw^2$, where $w \geq 1$, $c \geq 1$ is square-free, and c also divides $(k+1)d_k^2 B_k$. For future reference, we will define A_k as

$$A_k = \{p \text{ prime} \mid p|(k+1)d_k^2 B_k\}.$$

We now wish to deduce a similar result for the integer $2x - 1$. We will use the following two properties of Bernoulli polynomials ($i \geq 1$):

1. $B'_{i+1}(X) = (i+1)B_i(X)$;
2. $B_i(1/2) = (2^{1-i} - 1)B_i$.

By Taylor's formula

$$B_{k+1}(X) = \sum_{i=0}^{k+1} \frac{B_{k+1}^{(i)}(1/2)}{i!}(X - 1/2)^i,$$

and so, by applying the above properties, we obtain

$$B_{k+1}(X) = \sum_{i=1}^{k+1} \binom{k+1}{i} (2^{i-k} - 1)B_{k+1-i} \cdot 2^{-i}(2X-1)^i.$$

Define e_k to be the smallest positive integer such that

$$e_i \sum_{i=1}^{k+1} \binom{k+1}{i} (2^{i-k} - 1)B_{k+1-i} \cdot 2^{-i}(2X-1)^i$$

is a polynomial with integer coefficients in the variable $(2X - 1)$. Therefore, as above, we obtain

$$e_k(k+1)y^2 = (2x-1)(e_k(k+1)(2^{1-k} - 1)B_k + (2x-1)g(x)),$$

where $g(X)$ is a polynomial with integer coefficients. Therefore, $2x - 1 = bv^2$, where $v \geq 1$, $b \geq 1$ is square-free, and b is a product of primes which are divisors of the integers

$$\{e_k, k+1, 2^{k-1} - 1, \text{ numerator}(B_k)\}. \tag{4}$$

For future reference, we will define the set of primes C_k to be those odd primes which divide any one of the integers in (4).

Let $Z = 2x - 1$, $\omega = abc$, and $W = 2uvw$, then (Z, W) is an integer point on the elliptic curve

$$Z^3 - Z = \omega W^2. \tag{5}$$

Thus, the problem now reduces to finding all integer points on all possible curves of the form (5), where ω ranges over the square-free integers composed of primes in $A_k \cup C_k$. It is well known that this can be accomplished in several ways, the most efficient likely being the implementation of Gebel, Pethö, and Zimmer [9]. The problem here is that the size of the sets A_k and C_k and the size of their elements grow very quickly with k, thereby requiring not only the diophantine resolution of many elliptic curves but, more importantly, curves whose defining parameters are indeed quite large.

The main point in the present paper is to provide an alternative approach. With a, b, c, u, v, w as defined above, let $d = ac$ and $z = 2uw$. Then $(X, Y) = (v, z)$ is a point on the quartic curve

$$b^2X^4 - dY^2 = 1. \tag{6}$$

3. The diophantine equation $b^2X^4 - dY^2 - 1$

Equation (6) has been studied in considerable detail. We state two theorems on its solubility which will provide the basis for our algorithm to solve equation (3). The first theorem can be found in [6], while the second can be found in [1].

Lemma 3.1 ([6])**.** *Let d denote a square-free positive integer, and let $T + U\sqrt{d}$ denote the minimal solution to the equation $X^2 - dY^2 = 1$. For $k \geq 1$, let $T_k + U_k\sqrt{d} = (T + U\sqrt{d})^k$. If $(X, Y) = (v, z)$ is a solution to $X^4 - dY^2 = 1$, then $v^2 = T_1$ or $v^2 = T_2$. T_1 and T_2 are both squares only for $d = 1785$.*

Lemma 3.2 ([1])**.** *Let $b > 1$ and $d > 1$ be square-free integers, then the equation $b^2X^4 - dY^2 = 1$ has at most one solution in positive integers (X, Y). If a solution exists, then $bX^2 = T_{\beta(b)}$, where $\beta(b)$ is defined to be the minimal index k for which b divides T_k (note that $\beta(b)$ may or may not exist).*

4. The algorithm

In this section we describe an algorithm based on the results of the previous section for finding all integer points (X, Y) on those curves $b^2X^4 - dY^2 = 1$, as b and d range over the set of square-free integers composed of primes in C_k and A_k, respectively. The bottleneck in the algorithm is easily seen to be the computation of the minimal solution to the Pell equation $X^2 - dY^2 = 1$. Once this has been computed for a given value d, the remaining computations are completed with relative ease. We remark that the steps involved in the algorithm are in some ways dictated by properties of solutions to Pell equations, and so the interested reader may wish to consult [15] or [23] for further details.

Algorithm 4.1. For each square-free integer $d > 1$ composed of primes in A_k, perform the following steps:

1. Compute $T + U\sqrt{d}$, the minimal solution to $X^2 - dY^2 = 1$.
2. For each $p \in C_k$ such that $p \not| d$, determine if ($\beta(p)$ exists, and if so, then compute $\beta(p)$.
3. Let $\{p_1, \ldots, p_t\}$ denote those primes p for which $\beta(p)$ exists. Partition the set $\{p_1, \ldots, p_t\}$ into equivalence classes, where p_i and p_j are in the same class if and only if $\beta(p_i)$ and $\beta(p_j)$ are exactly divisible by the same power of 2.
4. This step is repeated for each equivalence class determined in Step 3. Let C denote an equivalence class. For each square-free integer $m > 1$, divisible only by primes in C, define $\beta(m) = \mathrm{lcm}_{p|m}\{\beta(p)\}$. (Note that m divides some T_i if and only if the prime divisors of m are all in the same equivalence class).
5. Determine if T_1 or T_2 is a square. For each $m > 1$ divisible only by primes in C_k such that $\beta(m)$ exists, determine if $(T_{\beta(m)})/m$ is a square.

4.1. **Remarks concerning the implementation of Algorithm 4.1.** The main difficulty in implementing Algorithm 4.1 is computing and working with $\eta = T + U\sqrt{d}$, the minimal solution of $X^2 - dY^2 = 1$. In general, $\log \eta$ is $O(O\sqrt{d})$, so except for small values of d it is usually infeasible to compute T and U explicitly. However, given a sufficiently accurate approximation of $\log \eta$, and explicit representation of η called a *compact representation* can be computed in polynomial time [5]. This compact representation has the form

$$\eta = \gamma \prod_{j=1}^{k} (\alpha_j/d_j)^{2^{k-j}}$$

where $d_j \in \mathbb{Z}^+$, $\gamma \in \mathcal{O}_d$, $\alpha_j = (a_j + b_j\sqrt{\Delta})/2 \in \mathcal{O}_d$, a_j, $b_j \in \mathbb{Z}$ $(j = 1, 2, \ldots, k)$, Δ is the discriminant of the quadratic field $\mathbb{Q}(\sqrt{d})$, and $\mathcal{O}_d$ is the ring of integers of $\mathbb{Q}(\sqrt{d})$. For our purposes, having a compact representation of η is almost always sufficient. Indeed, unless a solution of $b^2X^4 - dY^2 = 1$ is actually found, we only need to know T and U modulo various primes, a computation which can be carried out very efficiently using the methods in [14] once a compact representation has been obtained.

To compute $\log \eta$, we first compute an approximation of $R = \log \varepsilon_d$, the regulator of $\mathbb{Q}(\sqrt{d})$. Since $\eta = \varepsilon_d^\nu$ with $\nu \in \{1, 2, 3, 6\}$ (see, for example, [13]) we can easily compute a compact representation of η from ν and R. Computing the regulator R is in fact the most time-consuming part of the algorithm. The best unconditional algorithm has complexity $O(d^{1/5+\varepsilon})$ [16], [12], but for values of $d > 10^{20}$, this is much too inefficient. For these values of d, we used the subexponential algorithm described in [11].

Once a compact representation of η has been computed, the next step is to compute $\beta(p)$ for each prime $p \in C_k$ not dividing d. If $\beta(p)$ exists, it must divide $(p-(d/p))/4$ (see [23]), so we only have to compute $T_l \bmod p$ for each $l|(p-(d/p))/4$ and take $\beta(p)$ to be the smallest such l for which $T_l \equiv 0 \pmod{p}$. Given the compact representation of η, we can use the methods of [14] to compute $T \mod p$. Using the identities $T_{2n} = T_n^2 + Y_n^2 d$ and $U_{2n} = 2T_nU_n$ (see, for example, [23]), T_l can be computed efficiently using an analogue of the well-known binary exponentiation method given the binary representation of l. Computing the set of admissible values of m and $\beta(m)$ (Step 3 and 4) is straightforward after the $\beta(p)$ have been computed.

The last step of the algorithm is to determine whether T_1, T_2, or $(T_{\beta(m)})/m$ is a square. Each square value yields an integral solution of the elliptic curve (5) where $\omega = md$, $Z = T_1$, T_2 or $T_{\beta(m)}$, and $W = \sqrt{(Z^3 - Z)/w}$, which can in turn be tested as to whether a solution of (3) has been found. In general, computing T_l explicitly is infeasible, but once again we use compact representations to solve this problem. In the vast majority of cases, especially for large values of d, we expect that T_l will not be a square. Thus, we expect that computing the Legendre symbol (T_l/p) for a number of small primes p will eventually yield a value of -1, demonstrating that T_l is not square. For this test, we only need $T_l \bmod p$ for each prime p; again, the methods described in [14] can be used for this purpose. If we have tried 30 primes p and we get $(T_l/p) = 1$ for each of them, then we assume that T_l is in fact square and are forced to compute it explicitly, which was in practice a rare occurrence (only occuring for small values of T_l).

5. Computational results

We have implemented Algorithm 4.1 from the previous section and used it to numerically verify Conjecture 1.1 for $2 \leq k \leq 70$. Our code is written with the C++ library LiDIA [17] and compiled with the GNU g++ complier version 2.91.66. The program was run on an 800 MHz Pentium processor running Linux. The entire computation took just over 11 days. Complete listings of the sets A_k and C_k, and all the integral points found on the curve (5) can be found in Table 2 and Table 3 in Appendix A. For each point in Table 3, we list the values of k for which that point was found. The only solutions of (3) we found were the trivial solution for each value of k, and for $k = 2$ the anomalous solution $x = 24$, $y = 70$.

Because the correctness of the subexponential algorithm described in [11] for computing R is conditional on the Generalized Riemann Hypothesis, the correctness of our results is also conditional for those values of k which made use of this algorithm. In practice, the subexponential algorithm does return a multiple of the regulator, but in order for the values of $\beta(p)$ to be correct, it is necessary that the value returned is the actual regulator so that η is the fundamental solution of Pell's equation.

In our implementation, we used the subexponential algorithm to compute R whenever $d > 10^{20}$ and the unconditional baby step–giant step variant of complexity $O(d^{1/5+\varepsilon})$ [16], [12] otherwise. For $k \leq 34$ there were no values of $d > 10^{20}$, so these results are unconditionally correct. For $36 \leq k \leq 58$, we were forced to use the subexponential algorithm to compute some of the regulators, but we were nevertheless able to verify unconditionally that these regulators were correct. Given a multiple S of the regulator produced by the subexponential algorithm, we first verify that $R > S^{2/3}$ using a baby step–giant step algorithm. Then, for each prime p such that $S/p > S^{2/3}$, we verify that S/p is not also a multiple of R by checking that the ideal closest to S/p from $\mathcal{O}_d$ is not $\mathcal{O}_d$. Both stages of the algorithm take time $O(S^{1/3})$ and, assuming that $S = R$, we get an overall run time of $O(d^{1/6+\varepsilon})$ for verifying that the value produced by the subexponential algorithm is indeed the regulator. This method for unconditionally computing r is the subject of ongoing research, and will be described in more detail in a forthcoming paper.

In Table 1 we present various run time statistics from the computation. For each even value of k between 2 and 70, we list the time to execute Algorithm 4.1 (Time), the maximum decimal length of d during the course of the algorithm ($\max d$), the number of values of d generated ($\# \ d = 2^{|A_k|} - 1$), the number of d values for which the assumption of the GRH is necessary (# GRH), and the time to verify that the value of R produced is unconditionally correct for all d (Verify Time). For the times, seconds, minutes, hours, and days are denoted by "s", "m", "h", and "d", respectively.

Clearly, two factors prevent us from extending this table much further. First of all, the number of d values which must be processed by Algorithm 4.1 is exponential in k. Even for $k \leq 70$ we have three cases where 2047 values of d were generated. The regulator has to be evaluated for each of them, and while a few examples of the required sizes can be computed efficiently, evaluating 1024 regulators for d having between 20 and 51 decimal digits, for example, is very time-consuming.

Secondly, the d values themselves get larger as k increases. Indeed, to do $k = 72$ would require processing 2047 values of d, the largest having 64 decimal digits. Computing the regulator for a *single* d value of this size takes over 2 hours, so the amount of computation required to process all 2047 values of d for $k = 72$ would be significantly greater than for the previous values of k.

As mentioned earlier, we were successful in removing the dependence on the GRH from our results for $k \leq 58$. Although we spent as much as 3.75 days verifying our results for a single k value, even this would not have been possible without the new $O(d^{1/6+\varepsilon})$ method mentioned above. Extending this part of the computation would also be difficult. For $k \leq 58$, we had to compute regulators unconditionally for d values with as many as 39 decimal digits. To do the same for $k = 60$ would require handling d values with up to 51 decimal digits, a computation which currently appears to be out of reach with the available methods.

Table 1. Run time statistics.

k	Time	max d	# d	# GRH	Verify Time
2	0.01s	1	3		
4	0.03s	2	7		
6	0.09s	2	7		
8	0.07s	2	7		
10	0.26s	3	15		
12	1.66s	7	63		
14	0.25s	3	15		
16	0.91s	7	31		
18	2.08s	9	63		
20	3.46s	9	127		
22	5.92s	9	127		
24	16.55s	12	127		
26	2.23s	9	31		
28	20.53s	14	127		
30	2m 38.32s	18	255		
32	4m 40.55s	18	511		
34	27.32s	15	63		
36	6m 41.59s	27	255	127	42m 42.43s
38	4m 58.13s	19	127		
40	5m 50.06s	26	255	64	23m 9.65s
42	3m 35.36s	27	127	64	37m 42.75s
44	39m 27.89s	27	1023	173	30m 37.89s
46	9m 38.90s	29	255	64	57m 27.35s
48	18m 46.91s	34	511	256	8h 49m 34.44s
50	14m 44.81s	31	255	86	2h 39m 44.29s
52	57m 56.25s	35	1023	391	12h 4m 5.38s
54	29m 12.05s	37	511	241	1d 6h 4m 25.78s
56	31m 49.05s	39	511	256	3d 17h 5m 14.47s
58	38m 49.77s	39	511	243	2d 18h 2m 6.00s
60	13h 13m 16.35s	51	2047	1024	?
62	2h 57m 20.11s	43	2047	1074	?
64	1h 9m 54.65s	47	255	125	?
66	19h 34m 6.74s	53	1023	512	?
68	7h 8m 6.09s	49	2047	1101	?
70	6h 42m 43.14s	53	511	383	?
total	2d 7h 15m 38.08s	53	14873	6187	81d 19h 56m 50.43s

A. Appendix

Table 2 contains the complete sets A_k and C_k described in Section 2. Table 3 contains all the integral points found on the elliptic curve (5) during the course of our computations. For each point in Table 3, we list the values of k for which that point was found.

Table 2. A_k and C_k values.

k	A_k and C_k
2	$A_k = \{2, 3\},\ C_k = \{3\}$
4	$A_k = \{2, 3, 5\},\ C_k = \{3, 5, 7\}$
6	$A_k = \{2, 3, 7\},\ C_k = \{3, 7, 31\}$
8	$A_k = \{2, 3, 5\},\ C_k = \{3, 5, 127\}$
10	$A_k = \{2, 3, 5, 11\},\ C_k = \{3, 5, 7, 11, 73\}$
12	$A_k = \{2, 3, 5, 7, 13, 691\},\ C_k = \{3, 5, 7, 13, 23, 89, 691\}$
14	$A_k = \{2, 3, 5, 7\},\ C_k = \{3, 5, 7, 8191\}$
16	$A_k = \{2, 3, 5, 17, 3617\},\ C_k = \{3, 5, 7, 17, 31, 151, 3617\}$
18	$A_k = \{2, 3, 5, 7, 19, 43867\},\ C_k = \{3, 5, 7, 19, 43867, 131071\}$
20	$A_k = \{2, 3, 5, 7, 11, 283, 617\},\ C_k = \{3, 5, 7, 11, 283, 617, 524287\}$
22	$A_k = \{2, 3, 5, 11, 23, 131, 593\},\ C_k = 3, 5, 7, 11, 23, 127, 131, 337, 593\}$
24	$A_k = \{2, 3, 5, 7, 13, 103, 2294797\},$ $C_k = \{3, 5, 7, 13, 47, 103, 178481, 2294797\}$
26	$A_k = 2, 3, 7, 13, 657931\},\ C_k = \{3, 7, 13, 31, 601, 1801, 657931\}$
28	$A_k = \{2, 3, 5, 7, 29, 9349, 362903\},$ $C_k = \{3, 5, 7, 29, 73, 9349, 262657, 362093\}$
30	$A_k = \{2, 3, 5, 7, 11, 31, 1721, 1001259881\},$ $C_k = \{3, 5, 7, 11, 31, 233, 1103, 1721, 2089, 1001259881\}$
32	$A_k = \{2, 3, 5, 7, 11, 17, 37, 683, 305065927\},$ $C_k = \{3, 5, 7, 11, 17, 37, 683, 305065927, 2147483647\}$
34	$A_k = \{2, 3, 5, 7, 17, 151628697551\},$ $C_k = \{3, 5, 7, 17, 23, 89, 599479, 151628697551\},$
36	$A_k = \{2, 3, 5, 7, 13, 19, 37, 26315271553053477373\},$ $C_k = \{3, 5, 7, 13, 19, 31, 37, 71, 127, 122921, 26315271553053477373\}$
38	$A_k = \{2, 3, 5, 7, 13, 19, 154210205991661\},$ $C_k = \{3, 5, 7, 13, 19, 223, 616318177, 154210205991661\}$
40	$A_k = \{2, 3, 5, 7, 11, 41, 137616929, 1897170067619\},$ $C_k = \{3, 5, 7, 11, 41, 79, 8191, 121369, 137616929, 1897170067619\}$
42	$A_k = \{2, 3, 5, 7, 11, 43, 1520097643918070802691\},$ $C_k = \{3, 5, 7, 11, 43, 13367, 164511353, 1520097643918070802691\}$
44	$A_k = \{2, 3, 5, 7, 11, 23, 59, 8089, 2947939, 1798482437\},$ $C_k = \{3, 5, 7, 11, 23, 59, 431, 8089, 9719, 2099863, 2947939, 1798482437\}$
46	$A_k = \{2, 3, 5, 7, 23, 47, 383799511, 67568238839737\},$ $C_k = \{3, 5, 7, 23, 31, 47, 73, 151, 631, 23311, 383799511, 67568238839737\}$
48	$A_k = \{2, 3, 5, 7, 13, 17, 653, 56039, 153289748932447906241\},$ $C_k = \{3, 5, 7, 13, 17, 653, 2351, 4513, 56039, 13264529,$ $153289748932447906241\}$
50	$A_k = \{2, 3, 5, 11, 13, 17, 417202699, 47464429777438199\},$ $C_k = \{3, 5, 11, 13, 17, 127, 417202699, 4432676798593, 47464429777438199\}$
52	$A_k = \{2, 3, 5, 11, 13, 53, 577, 58741, 401029177, 4534045619429\},$ $C_k = \{3, 5, 7, 11, 13, 53, 103, 577, 2143, 11119, 58741, 131071, 401029177,$ $4534045619429\}$
54	$A_k = \{2, 3, 5, 7, 11, 19, 39409, 660183281, 1120412849144121779\},$ $C_k = \{3, 5, 7, 11, 19, 6361, 39409, 69431, 20394401, 660183281,$ $1120412849144121779\}$

Table 2. (Continued)

k	A_k and C_k
56	$A_k = \{2, 3, 5, 7, 19, 29, 113161, 163979, 19088082706840550550313\}$, $C_k = \{3, 5, 7, 19, 23, 29, 31, 89, 881, 3191, 113161, 163979, 201961, 19088082706840550550313\}$
58	$A_k = \{2, 3, 5, 29, 59, 67, 186707, 6235242049, 37349583369104129\}$, $C_k = \{3, 5, 7, 29, 59, 67, 32377, 186707, 524287, 1212847, 6235242049, 37349583369104129\}$
60	$A_k = \{2, 3, 5, 7, 11, 13, 31, 61, 2003, 5549927, 109317926249509865753025015237911\}$, $C_k = \{3, 5, 7, 11, 13, 31, 61, 2003, 179951, 5549927, 3203431780337, 109317926249509865753025015237911\}$
62	$A_k = \{2, 3, 5, 7, 11, 13, 31, 157, 266689, 329447317, 28765594733083851481\}$, $C_k = \{3, 5, 7, 11, 13, 31, 157, 266689, 329447317, 28765594733083851481, 28765594733083851481\}$
64	$A_k = \{2, 3, 5, 11, 13, 17, 1226592271, 87057315354522179184989699791727\}$, $C_k = \{3, 5, 7, 11, 13, 17, 73, 127, 337, 92737, 649657, 1226592271, 87057315354522179184989699791727\}$
66	$A_k = \{2, 3, 5, 7, 11, 17, 23, 67, 839, 159562251828620181390358590156239282938769\}$, $C_k = \{3, 5, 7, 11, 17, 23, 31, 67, 839, 8191, 145295143558111, 159562251828620181390358590156239282938769\}$
68	$A_k = \{2, 3, 5, 7, 17, 23, 37, 101, 123143, 1822329343, 55254733665109300282227481\}$, $C_k = \{3, 5, 7, 17, 23, 37, 101, 123143, 193707721, 1822329343, 761838257287, 55254733665109300282227481\}$
70	$A_k = \{2, 3, 5, 7, 11, 71, 688531, 20210499584198062453, 3090850068576441179447\}$, $C_k = \{3, 5, 7, 11, 47, 71, 178481, 688531, 10052678938039, 20210499584198062453, 3090850068576441179447\}$

Table 3. Points on $Z^3 - Z = \omega W^2$.

k	ω	Z	W
$4, 8 - 24, 28 - 70$	5	9	12
$2 - 70$	6	3	2
$2 - 70$	6	49	140
$4, 8 - 24, 28 - 70$	15	4	2
4,6,10 − 48,52 − 70	21	7	4
10,20,22,30,32,40 − 44,50 − 54,60 − 66,70	22	99	210
28,56,58	29	9801	180180
4,8 − 24,28 − 70	30	5	2
16,32,34,48,50,64,66,68	34	17	12
12,24,26,36,38,48,50,52,60-64	39	25	20
46	141	48	28
28,56,58	145	289	408
18,36,38,54,56	190	19	6

Table 3. (Continued)

k	ω	Z	W
12,14,18,20,24,28 − 48,54,56,60,62,66 − 70	210	15	4
12,14,18,20,24,28 − 48,54,56,60 − 70	210	1681	4756
16,32,34,48,50,64 − 68	255	16	4
10,20,22,30,32,40 − 44,50 − 54,60 − 66,70	330	11	2
60	366	243	198
40	410	81	36
50,52,60 − 64	429	12	2
30,60,62	434	63	24
12,24,36,38,48,60,62	455	64	24
16,30,36,46,56,60,62,66	465	31	8
12,24,26,36,38,48,60,62	546	13	2
12,24,26,36,38,48,60,62	546	27	6
32,50,64,66	561	33	8
28,56,58	609	28	6
22,44,66	759	23	4
12,22,34,44,56,56,66,68	805	161	72
36	889	127	48
60	915	121	44
60	915	244	126
52	1154	577	408
20,30,32,40 − 44,54,60,62,66,70	1155	55	12
16,32,34,48,64 − 68	1190	35	6
32,36,68	1295	36	6
48,50,64	1326	51	10
36	1406	37	6
32,34,48,66,68	1785	169	52
32,34,48,66,68	1785	57121	323128
18,36,38,54,56	1995	20	2
30,60,62	2170	125	30
10,20,22,30,32,40 − 44,52,54,60 − 66,70	2310	21	2
42	2365	44	6
36,70	2485	71	12
22,44,66	2530	45	6
60,62	3003	351	120
24	3090	59535	261324
36,38	3705	39	4
52	4134	53	6
36	4218	75	10
50,52,60 − 64	4290	65	8
40	4305	41	4
54	4389	76	10
28,56	6090	29	2
46	6486	47	4
24,52	7210	721	228
36	7215	1444	646

Table 3. (Continued)

k	ω	Z	W
32	8547	1849	860
58	8555	13689	17316
56	11571	57	4
50	12155	441	84
44	13629	176	20
36	14430	961	248
66	17085	135	12
52	17490	529	92
42	19866	43	2
12	20930	13455	10788
58	51330	59	2
60	56730	61	2
66	62645	9841095	123345108
66	75174	67	2
66	78591	68	2
34,66,68	82110	69	2
32	85470	111	4
64	130305	511	32
46	201066	93	2
56	380190	115	2
46	473478	415151	388470
66	508530	18491	3526
68	607614	1701	90
46	609546	4417	376
70	700770	141	2
60,62	930930	155	2
62	949065	156	2
52	1332870	1155	34
52	6240255	2884	62
52	337567503	15001	100

References

1. M. A. Bennett and P. G. Walsh, *The Diophantine equation* $b^2X^4 - dY^2 = 1$, Proc. A.M.S., **127** (1999), 3481–3491. MR **2000b:**11025
2. B. Brindza, *On some generalizations of the diophantine equation* $1^k + 2^k + \cdots + x^k = y^z$, Acta Arith. **44** (1984), 99–107. MR **86j:**11029
3. B. Brindza, *Power values of the sum* $1^k + 2^k + \cdots + x^k$, in "Number Theory" (Budapest 1987), Colloq. Math. Soc. János Bolyai, vol. 51, North-Holland, Amsterdam, 1990, 595–603. MR **91g:**11027
4. B. Brindza and Á. Pintér, *On the number of solutions of the equation* $1^k + 2^k + \cdots + (x-1)^k = y^z$, Publ. Math. Debrecen **56/3-4** (2000), 271–277. MR **2001i:**11032
5. J. Buchmann, C. Thiel, and H. C. Williams, *Short representation of quadratic integers*, in "Computational Algebra and Number Theory, Mathematics and its Applications" **325**, Kluwer, Dordrecht, 1995, 159–185. MR **96c:**11144
6. J. H. E. Cohn, *The Diophantine equation* $x^4 - Dy^2 = 1$ *II.* Acta Arith. **78** (1997), 401–403. MR **98e:**11033
7. K. Dilcher, *On a Diophantine equation involving quadratic characters*, Compositio Math. **57** (1986), 383–403. MR **87e:**11046

8. K. Dilcher, *Zeros of Bernouli, generalized Bernouli, and Euler polynomials*, Mem. A.M.S., **73** no. 386 (1988) (94 pages). MR **89h:**30005
9. J. Gebel, A. Pethö, and H. Zimmer, *Computing integral points on elliptic curves*, Acta Arith. **68** (1994), 171–192. MR **95i:**11020
10. M. Voorhoeve, K. Györy and R. Tijdeman, *On the diophantine equation* $1^k+2^k+\cdots+x^k+R(x)=y^z$, Acta Math. **143** (1979), 1–8; Corr. **159** (1987), 151–152. MR **80e:**10020 & MR **88i:**11018
11. M. J. Jacobson, Jr., *Subexponential Class Group Computation in Quadratic Orders*, Ph.D. thesis, Technische Universität Darmstadt, Darmstadt, Germany, 1999.
12. M. J. Jacobson, Jr., R. F. Lukes, and H. C. Williams, *An investigation of bounds for the regulator of quadratic fields*, Experiment. Math. **4** (1995), no. 3, 211–225. MR **97d:**11173
13. M. J. Jacobson, Jr. and H. C. Williams, *The size of the fundamental solutions of consecutive Pell equations*, Experiment. Math. **9** (2000), no. 4, 631–640. MR **2002f:**11142
14. M. J. Jacobson, Jr. and H. C. Williams, *Modular arithmetic on elements of small norm in quadratic fields*, Submitted to Designs, Codes, and Cryptography.
15. D. H. Lehmer, *An extended theory of Lucas functions*, Ann. Math. **31** (1930), 419–448.
16. H. W. Lenstra, Jr., *On the calculation of regulators and class numbers of quadratic fields*, London Math. Soc. Lecture Note Series **56** (1982), 123–150. MR **86g:**11080
17. The LiDIA Group, *LiDia: a C++ library for computational number theory*, Software, Technische Univesität Darmstadt, Germany, 1997, see http://www.informatik.tu-darmstadt.de/TI/LiDIA.
18. É. Lucas, *Solution de la question 1180*, Nouv. Ann. Math. (2) **16** (1877), 429–432.
19. Á. Pintér, *On a conjecture of Schaffer concerning the power values of power sums*, preprint, (2000).
20. J. J. Schäffer, *The equation* $1^p+2^p+3^p+\cdots+n^p=m^q$, Acta Math. **95** (1956), 155–189. MR **17:**1187a
21. T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge University Press, **87**, New York, 1986. MR **88h:**11002
22. J. Urbanowicz, *On the equation* $f(1)1^k+f(2)2^k+\cdots+f(x)x^k+R(x)=by^z$, Acta Arith. **51** (1988), 349–368. MR **90b:**11025
23. H. C. Williams, *Édouard Lucas and Primality Testing*, Canadian Mathematical Society Series of Monographs and Advanced Texts, vol. 22, John Wiley & Sons, New York, 1998. MR **2000b:**11139

Department of Computer Science, University of Calgary, 2500 University Drive NW, Calgary, Alberta, T2N 1N4 Canada

E-mail address: jacobs@cpsc.ucalgary.ca

Institute for Mathematics, University of Debrecen, P.O. Box 12, H-4010 Debrecen, Hungary

E-mail address: pinterak@freemail.hu

Department of Mathematics, University of Ottawa, 585 King Edward St., Ottawa, Ontario, K1N 6N5 Canada

E-mail address: gwalsh@mathstat.uottawa.ca