MATHEMATICS OF COMPUTATION
Volume 75, Number 254, Pages 935–940
S 0025-5718(05)01805-3

THE DIOPHANTINE EQUATION $x^4 + 2y^4 = z^4 + 4w^4$

ANDREAS-STEPHAN ELSENHANS AND JÖRG JAHNEL

ABSTRACT. We show that, within the hypercube $|x|, |y|, |z|, |w| \leq 2.5 \cdot 10^6$, the Diophantine equation $x^4 + 2y^4 = z^4 + 4w^4$ admits essentially one and only one nontrivial solution, namely $(\pm 1\,484\,801, \pm 1\,203\,120, \pm 1\,169\,407, \pm 1\,157\,520)$. The investigation is based on a systematic search by computer.

1. INTRODUCTION

1.1. An algebraic curve C of genus $g > 1$ admits at most a finite number of $\mathbb{Q}$-rational points. On the other hand, for genus one curves, $\#C(\mathbb{Q})$ may be zero, finite nonzero, or infinite. For genus zero curves, one automatically has $\#C(\mathbb{Q}) = \infty$ as soon as $C(\mathbb{Q}) \neq \emptyset$.

1.2. In higher dimensions, there is a conjecture, due to S. Lang, stating that if X is a variety of general type over a number field, then all but finitely many of its rational points are contained in the union of closed subvarieties which are not of general type. On the other hand, abelian varieties (as well as, e.g., elliptic and bielliptic surfaces) behave like genus one curves, i.e., $\#X(\mathbb{Q})$ may be zero, finite nonzero, or infinite. Finally, rational and ruled varieties comport in the same way as curves of genus zero in this respect.

This list does not yet exhaust the classification of algebraic surfaces, to say nothing of dimension three or higher. In particular, the following problem is still open.

Problem 1.3. Does there exist a $K3$ surface S over $\mathbb{Q}$ which has a finite nonzero number of $\mathbb{Q}$-rational points, i.e., such that $0 < \#S(\mathbb{Q}) < \infty$?

Remark 1.4. This question was posed by Sir P. Swinnerton-Dyer as Problem/Question 6.a) in the problem session to the workshop [PT]. We are not able to give an answer to it.

Received by the editor January 25, 2005.

2000 *Mathematics Subject Classification.* Primary 11Y50; Secondary 14G05, 14J28.

Key words and phrases. $K3$ surface, diagonal quartic surface, rational point, Diophantine equation, computer solution, hashing.

The first author was partially supported by a Doctoral Fellowship of the Deutsche Forschungsgemeinschaft (DFG).

The computer part of this work was executed on the Linux PCs of the Gauß Laboratory for Scientific Computing at the Göttingen Mathematisches Institut. Both authors are grateful to Professor Y. Tschinkel for the permission to use these machines as well as to the system administrators for their support.

1.5. One possible candidate for a $K3$ surface with the property $0 < \#S(\mathbb{Q}) < \infty$ is given by the following

Problem. Find a third point on the projective surface $S \subset \mathbf{P}^3$ defined by

$$x^4 + 2y^4 = z^4 + 4w^4.$$

Remarks 1.6. i) Problem 1.5 is also due to Sir P. Swinnerton-Dyer [PT, Problem/Question 6.c)]. It was raised, in particular, during his talk [S-D, at the very end of the article] at the Göttingen Mathematisches Institut on June 2, 2004.

ii) $x^4 + 2y^4 = z^4 + 4w^4$ is a homogeneous quartic equation. It, therefore, defines a $K3$ surface S in $\mathbf{P}^3$. As trivial solutions of the equation, we consider those corresponding to the $\mathbb{Q}$-rational points $(1\!:\!0\!:\!1\!:\!0)$ and $(1\!:\!0\!:\!-1\!:\!0)$.

iii) Our main result is the following theorem which contains an answer to Problem 1.5.

Theorem 1.7. *The diagonal quartic surface S in $\mathbf{P}^3$ defined by*

$$x^4 + 2y^4 = z^4 + 4w^4 \tag{$*$}$$

admits precisely ten $\mathbb{Q}$-rational points which allow integral coordinates within the hypercube $|x|, |y|, |z|, |w| < 2.5 \cdot 10^6$. These are $(\pm 1 : 0 : \pm 1 : 0)$ *and* $(\pm 1\,484\,801 : \pm 1\,203\,120 : \pm 1\,169\,407 : \pm 1\,157\,520)$.

Remark 1.8. This result clearly does not exclude the possibility that $\#S(\mathbb{Q})$ is actually finite. It might indicate, however, that a proof for that property is deeper than one originally hoped for.

2. Congruences

2.1. It seems natural to first try to understand the congruences

$$x^4 + 2y^4 \equiv z^4 + 4w^4 \pmod{p} \tag{$+$}$$

modulo a prime number p. For $p = 2$ and 5, one finds that all primitive solutions in $\mathbb{Z}$ satisfy

a) x and z are odd,
b) y and w are even,
c) y is divisible by 5.

For other primes, it follows from the Weil conjectures, proven by P. Deligne [De], that the number of solutions to the congruence (+) is

$$\#\mathrm{C}_S(\mathbb{F}_p) = 1 + (p-1)(p^2 + p + 1 + E) = p^3 + E(p-1),$$

where E is an error-term which may be estimated by $|E| \leq 21p$.

Indeed, consider the projective variety S over $\mathbb{Q}$ defined by ($*$). It has good reduction at every prime $p \neq 2$. Therefore, [De, Théorème (8.1)] may be applied to the reduction S_p. This yields $\#S_p(\mathbb{F}_p) = p^2 + p + 1 + E$ and $|E| \leq 21p$. We note that $\dim H^2(\mathscr{S}, \mathbb{R}) = 22$ for every complex surface $\mathscr{S}$ of type $K3$ [Bv, p. 98].

2.2. Another question of interest is to count the numbers of solutions to the congruences $x^4 + 2y^4 \equiv c \pmod{p}$ and $z^4 + 4w^4 \equiv c \pmod{p}$ for a certain $c \in \mathbb{Z}$.

This means to count the $\mathbb{F}_p$-rational points on the affine plane curves C^l_c and C^r_c defined over $\mathbb{F}_p$ by $x^4 + 2y^4 = \overline{c}$ and $z^4 + 4w^4 = \overline{c}$, respectively. If $p \nmid c$ and $p \neq 2$, then these are smooth curves of genus three.

By the work of André Weil [We, Corollaire 3 du Théorème 13], the numbers of $\mathbb{F}_p$-rational points on their projectivizations are given by

$$\#\overline{C}^l_c(\mathbb{F}_p) = p + 1 + E_l \qquad \text{and} \qquad \#\overline{C}^r_c(\mathbb{F}_p) = p + 1 + E_r,$$

where the error-terms can be bounded by $|E_l|, |E_r| \leq 6\sqrt{p}$. There may be up to four $\mathbb{F}_p$-rational points on the infinite line. For our purposes, it suffices to note that both congruences admit a number of solutions which is close to p.

The case $p|c$, $p \neq 2$, is slightly different, since it corresponds to the case of a reducible curve. The congruence $x^4 + ky^4 \equiv 0 \pmod{p}$ admits only the trivial solution if $(-k)$ is not a biquadratic residue modulo p. Otherwise, it has exactly $1 + (p-1)\gcd(p-1, 4)$ solutions.

Finally, if $p = 2$, then $\#C^l_0(\mathbb{F}_2) = \#C^l_1(\mathbb{F}_2) = \#C^r_0(\mathbb{F}_2) = \#C^r_1(\mathbb{F}_2) = 2$.

Remark 2.3. The number of solutions to the congruence (+) is

$$\#\mathrm{C}_S(\mathbb{F}_p) = \sum_{c \in \mathbb{F}_p} \#C^l_c(\mathbb{F}_p) \cdot \#C^r_c(\mathbb{F}_p).$$

Hence, the formulas just mentioned yield an elementary estimate for that count. They show once more that the dominating term is p^3. The estimate for the error is, however, less sharp than the one obtained via the more sophisticated methods in 2.1.

3. NAIVE METHODS

3.1. The most naive method to search for solutions of $(*)$ is probably the following: Start with the set

$$\{(x, y, z, w) \in \mathbb{Z} \mid 0 \leq x, y, z, w \leq N\},$$

and test the equation for every quadruple.

Obviously this method requires about N^4 steps. It can be accelerated using the congruence conditions for primitive solutions noted above.

3.2. A somewhat better method is to start with the set

$$\{x^4 + 2y^4 - 4w^4 \mid x, y, w \in \mathbb{Z}, 0 \leq x, y, w \leq N\}$$

and to search for fourth powers. This set has about N^3 elements, and the algorithm takes about N^3 steps. Again, it can be sped up by the above congruence conditions for primitive solutions. We used this approach for a trial run with $N = 10^4$.

An interesting aspect of this algorithm is the optimization by further congruences. Suppose x and y are fixed. Then about one-half or three-quarter of the values for w are not solutions to the congruence modulo a new prime. Following in this way, one can find more congruences for w and the size of the set may be reduced by a constant factor.

4. OUR FINAL ALGORITHM

4.1. **The basic idea.**

4.1.1. We need to compute the intersection of two sets

$$\{x^4 + 2y^4 \mid x, y \in \mathbb{Z}, 0 \leq x, y \leq N\} \cap \{z^4 + 4w^4 \mid z, w \in \mathbb{Z}, 0 \leq z, w \leq N\}.$$

Both have about N^2 elements.

It is a standard problem in Computer Science to find the intersection of two sets which both fit into memory. Using the congruence conditions modulo 2 and 5, one can reduce the size of the first set by a factor of 20 and the size of the second set by a factor of 4.

4.2. **Some details.**

4.2.1. The two sets described above are too big, at least for our computers and for interesting values of N. Therefore, we introduce a prime number p_p which we call the *page prime.*

We define the sets

$$L_c := \{x^4 + 2y^4 \mid x, y \in \mathbb{Z}, 0 \leq x, y \leq N, x^4 + 2y^4 \equiv c \pmod{p_p}\}$$

and

$$R_c := \{z^4 + 4w^4 \mid z, w \in \mathbb{Z}, 0 \leq z, w \leq N, z^4 + 4w^4 \equiv c \pmod{p_p}\}.$$

This means that the intersection problem is divided into p_p pieces and that the sets L_c and R_c fit into the computer's memory if p_p is big enough. We worked with $N = 2.5 \cdot 10^6$ and chose $p_p = 30\,011$.

For every value of c, our program computes L_c and stores this set in a hash table. Then, it determines the elements of R_c and looks them up in the table. Assuming uniform hashing, the expected running-time of this algorithm is $O(N^2)$.

Remark 4.2.2. An important further aspect of this approach is that the problem may be attacked in parallel on several machines. The calculations for one particular value of c are independent of the analogous calculations for another one. Thus, it is possible, say, to let c run from 0 to $(p_p - 1)/2$ on one machine and, at the same time, from $(p_p + 1)/2$ to $(p_p - 1)$ on another.

4.3. **Some more details.**

4.3.1. *The page prime.* For each value of c, it is necessary to find the solutions of the congruences $x^4 + 2y^4 \equiv c \pmod{p_p}$ and $z^4 + 4w^4 \equiv c \pmod{p_p}$ in an efficient manner. We do this in a rather naive way by letting y (w) run from 0 to $p_p - 1$. For each value of y (w), we compute x^4 (z^4). Then, we extract the fourth root modulo p_p.

Note that the page prime fulfills $p_p \equiv 3 \pmod 4$. Hence, the fourth roots of unity modulo p are just ± 1 and, therefore, a fourth root modulo p_p, if it exists, is unique up to sign. This makes the algorithm easier to implement.

Actually, we do not execute any modular powering operation or even computation of fourth roots in the lion's share of the running time. For more efficiency, all fourth powers and all fourth roots modulo p_p are computed and stored in an array during an initialization step. Thus, the main speed limitation to find all solutions to a congruence modulo p_p is, in fact, the time it takes to look up values stored in the machine's main memory.

4.3.2. *Hashing.* We do not compute L_c and R_c directly, because this would require the use of multiprecision integers within the inner loop. Instead, we choose two other primes, the *hash prime* p_h and the *control prime* p_c, which fit into the 32-bit registers of our computers. All computations are done modulo p_h and p_c.

More precisely, for each pair (x, y) considered, the expression $\big((x^4+2y^4) \bmod p_h\big)$ defines its position in the hash table. In other words, we hash pairs (x, y), whereas $(x, y) \mapsto \big((x^4+2y^4) \bmod p_h\big)$ plays the role of the hash function. For each pair (x, y), we write two entries into the hash table, namely the value of $\big((x^4+2y^4) \bmod p_c\big)$ and the value of y.

In the main computation, we worked with the numbers $p_h = 25\,000\,009$ for the hash prime and $p_c = 400\,000\,009$ for the control prime.

Note that, when working with a particular value of c, there are around p_p pairs $((x \bmod p_p), (y \bmod p_p))$ which fulfill the required congruence

$$x^4 + 2y^4 \equiv c \pmod{p_p}.$$

Therefore, approximately

$$p_p \cdot \left(\frac{N/2}{p_p} \cdot \frac{N/10}{p_p}\right) = \frac{N^2}{20p_p}$$

values will be written into the table. For our choices,

$$\frac{N^2}{20p_p} \approx 10\,412\,849,$$

which means that the hash table will become approximately 41.7% filled.

As for many other rules, there is an exception to this one. If $c = 0$, then approximately $1 + (p_p - 1)\gcd(p_p - 1, 4)$ pairs $((x \bmod p_p), (y \bmod p_p))$ may satisfy the congruence

$$x^4 + 2y^4 \equiv 0 \pmod{p_p}.$$

As $p_p \equiv 3 \pmod 4$, this is not more than $2p_p - 1$, and the hash table will be filled by not more than about 83.3%.

In order to resolve collisions within the hash table, we use an open addressing method. We are not particularly afraid of clustering and choose linear probing. We feel free to use open addressing as, thanks to the Weil conjectures, we have a priori estimates available for the load factor.

4.3.3. *Miscellanea.* The program makes frequent use of fourth powers modulo p_h and p_c. Again, we compute these data in the initialization part of our program and store them in arrays, once and for all.

Test versions of the program were written in Delphi. The final version was written in C. It took about 130 hours of CPU time on a 3.00 GHz Pentium 4 processor with 512 kByte cache memory. The main computation was executed in parallel on two machines during the very first days of December 2004.

4.4. **Post-processing.** Instead of looking for solutions of $x^4 + 2y^4 = z^4 + 4w^4$, our algorithm searches, in fact, for solutions to the corresponding simultaneous congruences modulo p_p and p_c which, in addition, fulfill that $\big((x^4 + 2y^4) \bmod p_h\big)$ and $\big((z^4 + 4w^4) \bmod p_h\big)$ are "almost equal".

To this modified problem, we found approximately 3800 solutions such that $(y, w) \neq (0, 0)$. These congruence solutions were checked by an exact computation using O. Forster's [Fo] Pascal-style multi-precision interpreter language ARIBAS.

Among the congruence solutions, exact equality occurs only once. This solution is as follows.

```
==> 1484801**4 + 2 * 1203120**4.
-: 90509_10498_47564_80468_99201

==> 1169407**4 + 4 * 1157520**4.
-: 90509_10498_47564_80468_99201
```

References

[Bv] Beauville, A.: Complex algebraic surfaces, London Mathematical Society Lecture Note Series 68, *Cambridge University Press,* Cambridge 1983. MR0732439 (85a:14024)

[Be] Bernstein, D. J.: Enumerating solutions to $p(a) + q(b) = r(c) + s(d)$, *Math. Comp.* 70 (2001) 389–394. MR1709145 (2001f:11203)

[CLR] Cormen, T., Leiserson, C., and Rivest, R.: Introduction to algorithms, *MIT Press* and *McGraw-Hill*, Cambridge and New York 1990. MR1066870 (91i:68001)

[De] Deligne, P.: La conjecture de Weil I, *Publ. Math. IHES* 43 (1974) 273–307. MR0340258 (49:5013)

[Fo] Forster, O.: Algorithmische Zahlentheorie, *Vieweg*, Braunschweig 1996.

[PT] Poonen, B. and Tschinkel, Y. (eds.): Arithmetic of higher-dimensional algebraic varieties, Proceedings of the Workshop on Rational and Integral Points of Higher-Dimensional Varieties held in Palo Alto, CA, December 11–20, 2002, *Birkhäuser,* Progress in Mathematics 226, Boston 2004. MR2028897 (2004h:11001)

[Se] Sedgewick, R.: Algorithms, *Addison-Wesley,* Reading 1983. MR0784432 (86k:68037)

[Sm] Smart, N. P.: The algorithmic resolution of Diophantine equations, London Mathematical Society Student Texts 41, *Cambridge University Press,* Cambridge 1998. MR1689189 (2000c:11208)

[S-D] Swinnerton-Dyer, Sir P.: Rational points on fibered surfaces, in: Tschinkel, Y. (ed.): Mathematisches Institut, Seminars 2004, *Universitätsverlag*, Göttingen 2004, 103–109.

[We] Weil, A.: Sur les courbes algébriques et les variétés qui s'en déduisent, Actualités Sci. Ind. 1041, *Hermann et Cie.,* Paris 1948. MR0027151 (10:262c)

Mathematisches Institut der Universität Göttingen, Bunsenstrasse 3–5, D-37073 Göttingen, Germany
E-mail address: `elsenhan@uni-math.gwdg.de`

Mathematisches Institut der Universität Göttingen, Bunsenstrasse 3–5, D-37073 Göttingen, Germany
E-mail address: