

On a set of diophantine equations

Citation for published version (APA):

van Lint, J. H. (1968). *On a set of diophantine equations*. (EUT report. WSK, Dept. of Mathematics and Computing Science; Vol. 68-WSK-03). Technische Hogeschool Eindhoven.

Document status and date:

Published: 01/01/1968

Document Version:

Publisher's PDF, also known as Version of Record (includes final page, issue and volume numbers)

Please check the document version of this publication:

- A submitted manuscript is the version of the article upon submission and before peer-review. There can be important differences between the submitted version and the official published version of record. People interested in the research are advised to contact the author for the final version of the publication, or visit the DOI to the publisher's website.
- The final author version and the galley proof are versions of the publication after peer review.
- The final published version features the final layout of the paper including the volume, issue and page numbers.

[Link to publication](#)

General rights

Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal.

If the publication is distributed under the terms of Article 25fa of the Dutch Copyright Act, indicated by the "Taverne" license above, please follow below link for the End User Agreement:

www.tue.nl/taverne

Take down policy

If you believe that this document breaches copyright please contact us at:

openaccess@tue.nl

providing details and we will investigate your claim.



September 1968

**Technological University Eindhoven
Netherlands**

Department of Mathematics

ON A SET OF DIOPHANTINE EQUATIONS

by

J.H. van Lint

1. Introduction

We are interested in the following set of equations to be solved in integers:

$$(1.1) \quad \begin{aligned} N + 1 &= x^2, \\ 3N + 1 &= y^2, \\ 8N + 1 &= z^2. \end{aligned}$$

The problem originates from the following one. The set $A: \{0, 1, 3, 8, 120\}$ has the property that if x and y ($x \neq y$) are taken from A then $xy + 1$ is a square. This implies that we know the solutions $N = 0$, $N = 120$ of (1.1). The question is whether more members can be added to A without losing the property mentioned above. Clearly any member that can be so added to A is a solution of (1.1).

This problem is mentioned in Dickson [1], vol 2, p 517. Apparently Diophantus first studied the problem of finding four numbers such that the product of any two increased by unity is a square. Fermat studied the equations (1.1) and found the solution $N = 120$. Euler was able to add a fifth positive number, which is not an integer, to the set A . In the past few years the problem has appeared in many places. After it was stated as a problem in [2] we proved that (1.1) has no solutions N with $120 < N < 10^{200}$ ([4]). This result and our method were reported at the 1968 Oberwolfach meeting on Number Theory. There are several ways of reducing (1.1) in such a way that Thue's theorem can be applied. Hence it was known that (1.1) had only a finite number of solutions. The problem of finding lower bounds for N became more interesting when at the same Oberwolfach meeting A. Baker reported on his results concerning effective bounds in Thue's theorem. Application of his theorem yields a very large number C such that (1.1) has no solutions N with $N > C$. It was remarked that such a number C can also be found by applying recent results of N.I. Fel'dman. Another approach is possible by using a method due to W. Ljunggren ([5]).

In a discussion with A. Baker we agreed that it might be possible to show that (1.1) has no other solutions than $N = 0$, $N = 120$ by increasing the lower bound 10^{200} and decreasing the constant C . In this note we show that (1.1) has no solutions in the interval $120 < N < 10^{1700000}$. The computation of this upper bound on a EL-X8 computer took only 7 minutes. It can very easily be increased using methods described below.

2. A computer-search

We replace the first two equations of (1.1) by

$$(2.1) \quad \begin{aligned} 3x - y &= 2A, \\ y - x &= 2B, \\ A^2 - 3B^2 &= 1. \end{aligned}$$

The solutions A_n, B_n of Pell's equation $A^2 - 3B^2 = 1$ are given by

$A_n + B_n\sqrt{3} = (2 + \sqrt{3})^n$. The quotients $\frac{A_n}{B_n}$ are convergents of the continued fraction for $\sqrt{3}$. We now find all solutions of the first two equations of (1.1) from (2.1) by taking $x_n = A_n + B_n$.

We find the sequence

$$(2.2) \quad x_0 = 1, x_1 = 3, x_2 = 11, \dots,$$

satisfying

$$(2.3) \quad x_{n+1} = 4x_n - x_{n-1}.$$

Explicitly we have

$$(2.4) \quad x_n = \left(\frac{3+\sqrt{3}}{6}\right) (2+\sqrt{3})^n + \left(\frac{3-\sqrt{3}}{6}\right) (2-\sqrt{3})^n.$$

In the same way we treat the equations $x^2 = N + 1$ and $z^2 = 8N + 1$. Here we have $z^2 - x^2 = 7N$, hence $z \equiv \pm x \pmod{7}$.

If $z \equiv -x \pmod{7}$ we write

$$\begin{aligned} 8x + z &= 7C, \\ x + z &= 7D, \\ C^2 - 8D^2 &= 1. \end{aligned}$$

We find $C_n + D_n\sqrt{8} = (3 + \sqrt{8})^n$ and in the same way as above the sequence of solutions \bar{x}_m :

$$(2.5) \quad \bar{x}_0 = 1, \bar{x}_1 = 2, \bar{x}_2 = 11, \dots$$

satisfying

$$(2.6) \quad \bar{x}_{m+1} = 6\bar{x}_m - \bar{x}_{m-1}.$$

Explicitly:

$$(2.7) \quad \bar{x}_m = \left(\frac{4-\sqrt{2}}{8}\right) (3+\sqrt{8})^m + \left(\frac{4+\sqrt{2}}{8}\right) (3-\sqrt{8})^m.$$

If $z \equiv +x \pmod{7}$ we transform to Pell's equation by

$$8x - z = 7C,$$

$$z - x = 7D,$$

$$C^2 - 8D^2 = 1.$$

This leads to the sequence x_k^* given by:

$$(2.8) \quad x_0^* = 1, x_1^* = 4, x_2^* = 23, \dots,$$

$$(2.9) \quad x_{k+1}^* = 6x_k^* - x_{k-1}^*,$$

$$(2.10) \quad x_k^* = \left(\frac{4+\sqrt{2}}{8}\right) (3+\sqrt{8})^k + \left(\frac{4-\sqrt{2}}{8}\right) (3-\sqrt{8})^k.$$

On a EL-X8 computer all terms of the sequences (2.2), (2.5) and (2.8) less than 10^{1200} were generated. The following pairs (n,m) for which $|\log x_n - \log \bar{x}_m| < 10^{-3}$ and the pairs (n,k) for which $|\log x_n - \log x_k^*| < 10^{-3}$ were found:

$$(2.11) \quad n = 2, \quad m = 2, \quad x_2 = \bar{x}_2 = 11,$$

$$(2.12) \quad n = 1125, m = 841, \log \bar{x}_m - \log x_n = 0,000725 \quad (\text{rounded upwards}),$$

$$(2.13) \quad n = 1643, m = 1228, \log x_n - \log \bar{x}_m = 0,000307 \quad (\quad " \quad " \quad),$$

$$(2.14) \quad n = 289, k = 216, \log x_n - \log x_k^* = 0,000456 \quad (\quad " \quad " \quad),$$

$$(2.15) \quad n = 1412, k = 1055, \log x_k^* - \log x_n = 0,000706 \quad (\quad " \quad " \quad),$$

$$(2.16) \quad n = 1930, k = 1442, \log x_n - \log x_k^* = 0,000330 \quad (\quad " \quad " \quad).$$

(This program took 27 minutes on the EL-X8).

3. A continued fraction method

Using continued fractions we shall extend the results of section 2. Let (ν, μ) be a pair of integers such that $x_\nu = (1 + \varepsilon)\bar{x}_\mu$ where $|\varepsilon|$ is small. Consider (2.4) and (2.7) for n, ν ($n > \nu$) and m, μ ($m > \mu$) respectively and take logarithms. If $x_n = \bar{x}_m$ then we have

$$\begin{aligned} & (n - \nu) \log(2 + \sqrt{3}) + \log\{1 + (2 - \sqrt{3})^{2n+1}\} - \log\{1 + (2 - \sqrt{3})^{2\nu+1}\} = \\ & = (m - \mu) \log(3 + \sqrt{8}) + \log\left\{1 + \frac{9 + 4\sqrt{2}}{7}(3 - \sqrt{8})^{2m}\right\} - \log\left\{1 + \frac{9 + 4\sqrt{2}}{7}(3 - \sqrt{8})^{2\nu}\right\} \\ & \qquad \qquad \qquad - \log(1 + \varepsilon) \end{aligned}$$

i.e.

$$(3.1) \quad \left| \frac{n - \nu}{m - \mu} - \frac{\log(3 + \sqrt{8})}{\log(2 + \sqrt{3})} \right| = \frac{c(\varepsilon, \nu, \mu)}{m - \mu}.$$

We shall use the following theorems (cf [3] chapter 10):

$$(3.2) \quad \text{If } \xi \text{ is irrational and } \left| \frac{p}{q} - \xi \right| < \frac{1}{2q^2} \text{ then}$$

$\frac{p}{q}$ is a convergent of the continued fraction for ξ .

$$(3.3) \quad \text{If } \frac{p_n}{q_n} ((p_n, q_n) = 1), n = 1, 2, \dots \text{ are the convergents of } \xi \text{ then}$$

$$\frac{1}{q_n q_{n+2}} < \left| \frac{p_n}{q_n} - \xi \right| < \frac{1}{q_n q_{n+1}}.$$

We apply these theorems to

$$\xi = \frac{\log(3 + \sqrt{8})}{\log(2 + \sqrt{3})} = [1, 2, 1, 20, 1, 5, 3, 8, 5, 1, 2, 1, 1, 1, 1, 4, 3, \dots].$$

The first 16 convergents of ξ are:

$$\frac{1}{1}, \frac{3}{2}, \frac{4}{3}, \frac{83}{62}, \frac{87}{65}, \frac{518}{387}, \frac{1641}{1226}, \frac{13646}{10195}, \frac{69871}{52201}, \frac{83517}{62396}, \frac{236905}{176993}, \frac{320422}{239389},$$

$$\frac{557327}{416382}, \frac{877749}{655771}, \frac{1435076}{1072153}, \frac{6618053}{4944383} \quad (27 \text{ seconds computation on EL-X8}).$$

We know from section 2 that $x_n = \bar{x}_m > 11$ implies $m > 1500$. Now assume $m < 3364$ and apply (3.1) with $v = 1643, \mu = 1228$. For $c(\varepsilon, v, \mu)$ we find 0,000234. Hence

$$\left| \frac{n-1643}{m-1228} - \xi \right| = \frac{0,000234}{m-1228} < \frac{1}{2(m-1228)^2}.$$

By (3.2) and (3.3) this is only possible if

$$m-1228 = 2*387 \quad \text{and} \quad n-1643 = 2*518,$$

$$\text{or} \quad \swarrow \quad m-1228 = 1226 \quad \text{and} \quad n-1643 = 1641.$$

Since $x_{1679} \equiv x_{3284} \equiv 1 \pmod{4}$ and $\bar{x}_{2002} \equiv \bar{x}_{2454} \equiv 3 \pmod{4}$ these two possible cases are excluded and hence we have

$$(3.4) \quad x_n \neq \bar{x}_m \quad \text{if} \quad 2 < m < 3364.$$

In the same way we treat $x_n = x_k^*$, starting from (2.16). The result then is

$$(3.5) \quad x_n \neq x_k^* \quad \text{if} \quad k < 3442.$$

From (3.4) and (3.5) we see that:

$$(3.6) \quad \text{The system (1.1) has no solutions } N \text{ with } 120 < N < 10^{5000}.$$

4. A sieve method

The best results we have found up to now were obtained by the following sieve method. Each of the sequences $\{x_n\}$, $\{\bar{x}_m\}$, $\{x_k^*\}$ is periodic mod p (for every integer p). The condition $x_n = \bar{x}_m$ implies, by considering $x_n \equiv \bar{x}_m \pmod{4}$:

$[n \equiv 0 \text{ or } 2 \pmod{4} \text{ and } m \equiv 0 \pmod{4}]$ or $[n \equiv 1 \text{ or } 2 \pmod{4} \text{ and } m \equiv 2 \pmod{4}]$

and also, by considering $x_n \equiv \bar{x}_m \pmod{3}$:

$[n \equiv 1 \text{ or } 5 \pmod{6} \text{ and } m \equiv 1 \text{ or } 3 \pmod{4}]$ or $[n \equiv 2 \text{ or } 3 \pmod{6} \text{ and } m \equiv 1 \text{ or } 2 \pmod{4}]$.

Combination of these yields

$[n \equiv 0 \text{ or } 11 \pmod{12} \text{ and } m \equiv 0 \pmod{4}]$ or $[n \equiv 2 \text{ or } 9 \pmod{12} \text{ and } m \equiv 2 \pmod{4}]$

By considering $x_n \pmod{p}$ for successive primes new conditions for n and m are found. This was executed on the EL-X8 for the primes ≤ 57 (5 minutes computing time). The same thing was done for x_n and x_k^* and the primes ≤ 53 (2 minutes computing time).

The results were:

(4.1) $x_n = \bar{x}_m$ implies:

n or $-n-1 \pmod{2550240}$ is one of the following numbers

- (a) 0, 191520, 695519, 887040;
- (b) 80640, 110880, 584639, 776160;
- (c) 2, 665277, 927357, 957602;
- (d) 110882, 776157, 816477, 846722;
- (e) 151197, 181442, 776162, 1108802;
- (f) 665279, 856800, 997919, 1189440;

and

$m \pmod{36340920}$ is one of the following numbers

- (a) 0, 5191560, 26860680, 32052240;
- (b) 6320160, 11511720, 20540520; 25732080;

- (c) 2, 10383122, 22120562, 32503682;
- (d) 6320162, 15800402, 16703282, 26183522;
- (e) 9480242, 12640322, 19863362, 23023442;
- (f) 2031480, 30020760, 33180840, 35212320.

If n is taken from the set (a) then m must be in (a) etc.

(4.2) $x_n = x_k^*$ implies for n what was stated above and $k \pmod{36340920}$ is one of the following numbers:

- (a) 0, 4288680, 9480240, 31149360;
- (b) 10608840, 15800400, 24829200, 30020760;
- (c) 3837238, 14220358, 25957798, 36340918;
- (d) 10157398, 19637638, 20540518, 30020758;
- (e) 13317478, 16477558, 23700598, 26860678;
- (f) 1128600, 3160080, 6320160, 34309440.

Again set (a) for n is combined with set (a) for k etc.

These conditions can be combined with the results of section 3 but even without doing that we immediately see that

(4.3) the system (1.1) has no solutions N with $120 < N < 10^{1700000}$.

With very little extra work this bound can be improved to 10^{10} .

References

- [1] L.E. Dickson, History of the theory of numbers (1920).
- [2] M. Gardner, Mathematical Diversions, Scientific American 216 (1967)³, p. 124.
- [3] G.H. Hardy and E.M. Wright, An introduction to the theory of numbers, Oxford 1954.
- [4] J.H. van Lint, notitie 20 (1967), Technische Hogeschool Eindhoven.
- [5] W. Ljunggren, On the integral solutions of the diophantine system
 $ax^2 - by^2 = c, a_1z^2 - b_1y^2 = c_1$, Proc. of the Int. Congress of Math. 1950,
p. 297.