For full screen in pdf pres ctrl+L and then ctrl+

On the Ljunggren Equation $y^2 = 2x^4 - 1$

Konstantinos A. Draziotis

Patra, 7-11 July, Greece
13th International Conference on
Fibonacci Numbers and their Applications

In this talk we are concerned for the integer solutions of the diophantine equation

$$y^2 = 2x^4 - 1. \tag{1.1}$$

There have been a number of contributions dealing with this diophantine equation. First Ljunggren in 1942, proved that the positive integer solutions are $(|x|, |y|) = (1, 1), (13, 239)$.

Note that if $y^2 - 2x^2 = 1$, then $s_n + p_n\sqrt{2} = \varepsilon^n$, where $\varepsilon = 1 + \sqrt{2}$, and p_n the sequence of Pell numbers $0, 1, 2, 5, 12, 29, ...$

So the solution of Ljunggren equation gives the squares of Pell numbers.

Also Tzanakis and Steiner gave a proof using the theory of Baker

Simplifying the solution of Ljunggren's equation $X^2 + 1 = 2Y^4$. *J. Number Theory 37 (1991), no. 2, 123–132.*

Another proof was given by Chen using the Thue-Siegel method combined with Pade approximation on algebraic functions.

A new solution of the Diophantine equation $X^2 + 1 = 2Y^4$. *J. Number Theory 48 (1994), 62-74.*

In this talk we shall give another method, which relies on the construction of a unit equation on a quartic number field. We can trace the roots of this method to the Chabauty paper in 1943.
Démonstration de quelques lemmes de rehaussement. (French) C. R. Acad. Sci. Paris 217, (1943). 413–415.

The method is used by Poulakis and later by Bugeaud to obtain an upper bound for the height of the integer points on an Elliptic curve defined over a number field. Also this method, eventually uses Baker's theory since we need to solve a unit equation.

The proof consists of two parts. The first uses the group structure of the elliptic curve and the second is a reduction to a unit equation in a certain quartic number field.
We recall that the set of rational points of an elliptic curve form an abelian group. The group law is showed in the figure.

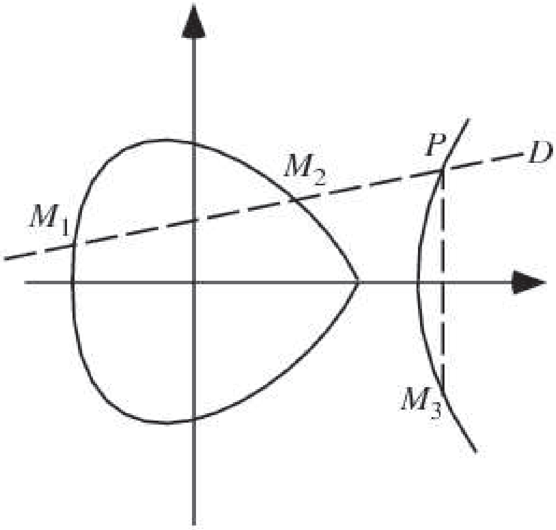

FIGURE 1. $M_1 + M_2 = M_3$

To solve the equation of Ljunggren $L : y^2 = 2x^4 - 1$ it is enough to solve the elliptic diophantine equation $C : y^2 = x^3 - 2x$. Indeed, if (x, y) is an integer solution of the equation L, then the point

$$P = (a, b) = (2x^2, 2xy)$$

belongs to C. Assume that $|a| \geq 2$. Let $R = (s, t)$ be a point of C such that $2R = P$. Then, from duplication formula we get

$$a = \frac{(s^2 + 2)^2}{4s(s^2 - 2)}$$

and so s is a root of the polynomial

$$\Theta_a(S) = S^4 - 4aS^3 + 4S^2 + 8aS + 4.$$

The roots of $\Theta_a(S)$ are:

$$a \pm \sqrt{a^2 - 2} \pm \sqrt{2a^2 \pm 2a\sqrt{a^2 - 2}},$$

where the first $\pm$ coincides with the third.

Our first goal now is to compute the number field $L = \mathbb{Q}(s)$. Then we shall prove that the following elements of L

$$u = \frac{s+\sqrt{2}}{2} \text{ and } v = \frac{\sqrt{2}-s}{2},$$

are units of L and satisfy the unit equation

$$X + Y = \sqrt{2}.$$

Then using the algorithm of Wildanger Wildanger, K., Über das Lösen von Einheiten- und Indexformgleichungen in algebraischen Zahlkörpern. (German) [Solving unit and index form equations in algebraic number fields] J. Number Theory 82 (2000), no. 2, 188–224. we can expilicitly calculate the solutions of this unit equation and so we can find s. These values of s we substitue to the expression

$$\frac{(s^2+2)^2}{4s(s^2-2)}$$

which gives the integer solutions of C.

First Step. The computation of the field L

Put $L = \mathbb{Q}(s)$. Since $a = 2x^2$, we have $a^2 - 2 = 4x^4 - 2 = 2y^2$ and so $L = \mathbb{Q}(\sqrt{2x^2 \pm y\sqrt{2}})$. Also, $K = \mathbb{Q}(\sqrt{2}) \subset L$ and $N_K(2x^2 \pm y\sqrt{2}) = 2$. It follows that the only prime dividing the discriminant of L is 2. So the only prime ramified in L is 2. Furthermore, from

Cohen, Henri; Advanced topics in computational number theory. Graduate Texts in Mathematics, 193. Springer-Verlag, New York, 2000. [Chapter 9, Proposition 9.4.1, p.461]

L is a totally real quartic extension of $\mathbb{Q}$. So from Jones list

Jones, W.J., http://math.la.asu.edu/~jj/numberfields/. Tables of number fields with prescribed ramification.

or the database of Jürgen Klüners and Gunter Malle,

http://www.mathematik.uni-kassel.de/~klueners/minimum/minimum.html

we conclude that $L = \mathbb{Q}(\sqrt{2 + \sqrt{2}})$.

Second Step. $u = \frac{s+\sqrt{2}}{2},\ v = \frac{\sqrt{2}-s}{2}$ *are units of* L

The elements $u = \frac{s+\sqrt{2}}{2},\ v = \frac{\sqrt{2}-s}{2}$ are roots of the polynomial with integer coefficients:

$$\begin{aligned} \lambda(S) &= \frac{1}{256}\mathrm{res}_W\big(\Theta_a(2S \mp W), W^2 - 2\big) \\ &= S^8 - 4aS^7 + \cdots + 1, \end{aligned}$$

where $\mathrm{res}_W(\cdot,\cdot)$ denotes the resultant of two polynomials with respect to W. Thus u, v are units in the number field L. Since $u + v = \sqrt{2}$ we conclude that u and v satisfy the unit equation $X + Y = \sqrt{2}$ in L.

Third Step. The solution of Unit equation

The algorithm of Wildanger which is implemented in the computer algebra system Magma, gives the solutions of this unit equation in L, which are listed in table 1 where we have put
$[a_0\ a_1\ a_1\ a_3] = a_0 + a_1\theta + a_2\theta^2 + a_3\theta^3$,
with $\theta = \sqrt{2+\sqrt{2}}$. We substitute to the realtion

$$a = \frac{(s^2+2)^2}{4s(s^2-2)}$$

each solution of the unit equation and we check if it gives an integer. Thus, it follows that $a = 2, 338$. So, for $|a| \geq 2$, we get $|a| = 2$ or 338. Since $a = 2x^2$ we get $|x| = 1$ or 13. We conclude that $L(\mathbb{Z}) = \{(\pm 1, \pm 1), (\pm 13, \pm 239)\}$.

Thank you

Table 1-The 44 solutions of the unit equation $X + Y = \sqrt{2}$ in the number field $L = \mathbb{Q}(\sqrt{2+\sqrt{2}})$.

[-1,0,0,0] [-1,0,1,0]	[1,0,0,0] [-3 0,1,0]	[-1,-1,0,0] [-1,-1,1,0]
[-1,1,0,0] [-1,-1,1,0]	[-1,-1,1,0] [-1,1,0,0]	[-3,0,1,0] [1,0,0,0]
[407,533,-119,-156] [-409,-533,120,156]	[-1,1,1,0] [-1,-1,0,0]	[-1,0,1,0] [-1,0,0,0]
[-409,533,120,-156] [407,-533,-119,156]	[5,7,-1,-2] [-7,-7,2,2]	[1,4,0,-1] [-3,-4,1,1]
[-71,39,120,-65] [69,-39,-119,65]	[-1,-1,-1,1] [-1,1,2,-1]	[1,2,-3,-2] [-3,-2,4,2]
[69,39,-119,-65] [-71,-39,120,65]	[-7,7,2,-2] [5,-7,-1,2]	[-3,2,4,-2] [1,-2,-3,2]
[-71,-39,120,65] [69,39,-119,-65]	[-1,2,0,-1] [-1,-2,1,1]	[1,3,0,-1] [-3,-3,1,1]
[11,14,-3,-4] [-13,-14,4,4]	[-1,2,1,-1] [-1,-2,0,1]	[-3,3,1,-1] [1,-3,0,1]
[-1,1,-1,-1] [-1,-1,2,1]	[-1,1,2,-1] [-1,-1,-1,1]	[-3,-4,1,1] [1,4,0,-1]
[11,-14,-3,4] [-13,14,4,-4]	[1,-3,0,1] [-3,3,1,-1]	[-1,-2,0,1] [-1,2,1,-1]
[-13,14,4,-4] [11,-14,-3,4]	[-3,-3,1,1] [1,3,0,-1]	[-1,-2,1,1] [-1,2,0,-1]
[-409,-533,120,156] [407,533,-119,-156]	[1,-2,-3,2] [-3,2,4,-2]	[5,-7,-1,2] [-7,7,2,-2]
[69,-39,-119,65] [-71,39,120,-65]	[-1,-1,2,1] [-1,1,-1,-1]	[1,-4,0,1] [-3,4,1,-1]
[-13,-14,4,4] [11,14,-3,-4]	[-3,-2,4,2] [1,2,-3,-2]	[-3,4,1,-1] [1,-4,0,1]
[407,-533,-119,156] [-409,533,120,-156]	[-7,-7,2,2] [5,7,-1,-2]	