Computation of Pell Numbers of the Form pX^2

Konstantinos A. Draziotis

Technological and Educational Institute of Kavala
Department of Exact Sciences
65 404 Kavala, Greece
drazioti@gmail.com

Abstract. We give an algorithm for the computation of Pell numbers of the form $P_n = px^2$, where p is prime and $x \in \mathbb{Z}$.

1 Introduction

The Pell sequence is defined by the linear recurrence relation :

$$P_0 = 0,\ P_1 = 1,\ P_n = 2P_{n-1} + P_{n-2},\quad n \geq 2.$$

This sequence has many combinatorial meaning. For instance, the number of 132−avoiding two-stack sortable permutations involves Pell and Fibonacci numbers, [3]. Also we have the Pell primality test : "If N is odd prime, then $P_n - \left(\frac{2}{n}\right)$ is divisible by N," where $\left(\frac{2}{n}\right)$ is the Kronecker symbol. For other information and applications of Pell numbers see [14].

The arithmetic properties of Pell numbers of special form have held the interest of many mathematicians. In [7], Ljunggren showed that a Pell number is a positive square only if $n = 1$ or 7. Pethö in [9], proved that these are the only perfect powers of the Pell sequence. For the numbers of the form $P_n = a^m \pm t$, where $m = 2, 3$ and $t \in \{1, 2, 5, 6, 14\}$, some results are obtained in [11]. In [8], it was shown that if k is an integer all of whose prime factors are congruent to 3 modulo 4, then neither term of sequence P_n is of the form kx^2.

Furthermore, Robbins [12], in order to compute Pell numbers of the form $P_n = px^2$, computed the number $z^*(p) = \min\{k :\ p|P_k\}$ and checked if $P_{z^*(p)}$ is equal to px_1^2. Note that, there is not known upper bound for the size of $z^*(p)$, as p is increasing and so is not clear if p is a factor of P_k for some k. So this may cause an endless searching in order to compute $z^*(p)$. For a comparison see example 4 in section 4. This method is very fast in practice, for small primes. Our purpose is to give an algorithm for the computation of Pell numbers of the form $P_n = px^2$, for p fixed prime number. The main idea is a reduction of the problem to the study of the integer points (x, y) to the elliptic curve $Y^2 = X^3 - 32p^2X$, with x even. The determination of these integral points is achieved using the *multiplication by 2 Chabauty method*, [10], [1]. The simplicity and the usefulness of the method is illustrated by examples.

S. Bozapalidis and G. Rahonis (Eds.): CAI 2009, LNCS 5725, pp. 220–226, 2009.

2 The Reduction

Suppose that n is odd and $P_{2n-1} = pr^2$. Since P_n is odd, then necessarily p is an odd prime. A straightforward calculation with the general term of Pell sequence,

$$P_n = \frac{\sqrt{2}}{4}(\lambda_+^n - \lambda_-^n),\ \lambda_\pm = 1 \pm \sqrt{2},$$

gives

$$P_{2n-1}^2 + P_{2n+1}^2 + 4 = 6P_{2n-1}P_{2n+1}. \tag{1}$$

Since $P_{2n-1} = pr^2$ and setting $P_{2n+1} = t$, we get

$$p^2r^4 + t^2 + 4 = 6pr^2t.$$

This equation defines an elliptic curve over $\mathbb{Q}$. Using the map

$$(r, t) \to (X, 3pX^2 + Y),$$

we get the curve $Y^2 = 8p^2X^4 - 4$. Note that if (r, t) is an integer point, then also (X, Y) is integer point. Setting $Y = 2Y''$ we get $Y''^2 = 2p^2X^4 - 1$, thus $Y''^2 \equiv -1/p$. So $(-1/p) = 1$, when $p \equiv 1/4$. Multiplying both parts with $16p^2$, we get $(2pY'')^2 = 2(2pX)^4 - 16p^2$, and this implies $Y'^2 = 2X'^4 - 16p^2$. Finally, setting $x = 2X'^2$ and $y = 2X'Y'$ we get the elliptic curve $y^2 = x^3 - 32p^2x$. So we have to determine its integer points under the condition x to be of the form $2X'^2$. The relation between x, r is $x = 8p^2r^2$ and also $P_{2n-1} = x/8p$. We note that x cannot be a square.

Now if n is even, Theorem 2 of [12] give us the following.

Lemma 1. *If p is an odd and $P_{2m} = px^2$, then $p = 3$ and $m = 2$.*

So the problem of computation of Pell numbers of the form $P_n = pr^2$ splits to two cases. Firstly, if n is odd, then $p \equiv 1/4$ and using the equation (1), we reduce the problem to the study of the elliptic curve $y^2 = x^3 - 32p^2x$. Secondly, if n is even then $n = 4,\ p = 3$. If $p = 2$, then from [12, Theorem 1] we get $n = 2$. Thus in the next section we shall determine the integer points of the elliptic curve $Y^2 = X^3 - 32p^2X$, with X even.

3 Integer Points to $Y^2 = X^3 - 32p^2X$

Let $E : Y^2 = X^3 + AX$. We set $P = (a, b) \in E(\mathbb{Z})$ and let $R = (s, t)$ be a point of E over the algebraic closure $\overline{\mathbb{Q}} \subset \mathbb{C}$ of $\mathbb{Q}$, such that $2R = P$. By [13, chapter 3, p.59], we get

$$a = \frac{s^4 - 2As^2 + A^2}{4(s^3 + As)} \tag{2}$$

and so s is a root of the polynomial

$$\Theta_a(T) = T^4 - 4aT^3 - 2AT^2 - 4AaT + A^2. \tag{3}$$

If $A=-32p^2$, then we get

$$\Theta_a(T)=T^4-4aT^3+64p^2T^2+128p^2aT+1024p^4.$$

We have

$$0=\frac{\Theta_a(s)}{s^2}=\Big(s-\frac{32p^2}{s}\Big)^2-4a\Big(s-\frac{32p^2}{s}\Big)+128p^2,$$

whence

$$s=a\pm\sqrt{a^2-32p^2}\pm\sqrt{2a^2\pm 2a\sqrt{a^2-32p^2}},$$

where the first $\pm$ coincide with the third. Thus,

$$L=\mathbb{Q}(s)=\mathbb{Q}\big(\sqrt{2a^2\pm 2a\sqrt{a^2-32p^2}}\big). \tag{4}$$

Since a is not a square, then also a^2-32p^2 is not a square and so L can not be neither a quadratic extension of $\mathbb{Q}$ nor equal to $\mathbb{Q}$. Necessarily L is a quartic extension of $\mathbb{Q}$. Since a is of the form $2r_1^2$, we get that $a^2-32p^2=2r_2^2$, for some $r_2\in\mathbb{Z}$. Thus from (4) we get $L=\mathbb{Q}\big(\sqrt{2a^2\pm 2ar_2\sqrt{2}}\big)$. Note also that $K=\mathbb{Q}(\sqrt{2})\subset L$. From the form of the number field L we conclude that its Galois group is either the Dihedral group or the Cyclic group of 4 elements or the Klein group. The relation between a,r_1,r_2 allow us to prove the following.

Lemma 2. *The extension $L/\mathbb{Q}$ is a cyclic extension of $\mathbb{Q}$.*

Proof. Since $L/\mathbb{Q}$ is quartic, $\Theta_a(T)$ is an irreducible polynomial. We shall use the result of [6]. The cubic resolvent of $\Theta_a(T)$ is

$$r(T)=(T+64p^2)(T^2-128Tp^2-512a^2p^2+4096p^4)$$

and the auxiliary polynomial is

$$g(x)=(x^2+64p^2x+1024p^4)(x^2-4ax+128p^2)=(x+32p^2)^2(x^2-4ax+128p^2).$$

The second factor of $g(x)$ has discriminant $2a\pm 2\sqrt{a^2-32p^2}=2a\pm 2r_2\sqrt{2}$. Remarking that the splitting field of $r(x)$ is $K=\mathbb{Q}(\sqrt{2})$, we conclude that $g(x)$ splits in K, so the Galois group is $\mathbb{Z}_4$.

From [4] or [5] we get that L can be written in a unique way as

$$L=\mathbb{Q}\Big(\sqrt{A(D+B\sqrt{D})}\Big),$$

with $B\geq 1$, A square free and odd, $D\geq 2$ square free, $D-B^2$ is square and $\gcd(A,D)=1$. Further, using again [4] or [5], the discriminant Δ_L is equal to $2^cA^2D^3$, where $c\in\{0,4,6,8\}$. Since $D=2$ we get $B=1$ and $\Delta_L=2^{c+3}A^2$. From [13, Proposition 1.5, p.193], we get that the number field $K(s)$ is unramified outside the primes dividing the discriminant of E, so L is unramified outside

$\{2, p\}$. Using that $\Delta_L = 2^{c+3}A^2$ and since A is odd, we get $A \in \{\pm 1, \pm p\}$. So the possible number fields are

$$L_{p,+} = \mathbb{Q}\big(\sqrt{2p \pm p\sqrt{2}}\big),\ L_{p,-} = \mathbb{Q}\big(\sqrt{-2p \pm p\sqrt{2}}\big),$$

$$L_{2,+} = \mathbb{Q}\big(\sqrt{2 \pm \sqrt{2}}\big),\ L_{2,-} = \mathbb{Q}\big(\sqrt{-2 \pm \sqrt{2}}\big).$$

The minimal polynomials are

$$f_{\pm}(T) = T^4 \mp 4pT^2 + 2p^2$$

for $L_{p,\pm}$ and

$$g_{\pm}(T) = T^4 \mp 4T^2 + 2$$

for $L_{2,\pm}$. The first two are ramified at $\{2, p\}$ and the other two only at $\{2\}$.

From the set up of our problem we have $a = 4pz$. So $s = 4pr$. Then r is a root of the polynomial

$$\theta_z(T) = T^4 - 4zT^3 + 4T^2 + 8zT + 4.$$

The element

$$r_{\pm} = \frac{r \pm \sqrt{2}}{2}$$

is a root of the polynomial with integer coefficients:

$$\begin{aligned} \lambda(S) &= (1/256) res_W(\theta_z(2T \mp W), W^2 - 2) \\ &= T^8 - 4aT^7 + \cdots + 1, \end{aligned}$$

where $res_W(\cdot, \cdot)$ denotes the resultant of two polynomials with respect to W. Since the constant term is 1, the norm of $r_{\pm}$ shall divide 1. Thus $r_{\pm}$ is a unit in L. So

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

satisfy the unit equation $u + v = \sqrt{2}$ in L. Also from [2, Chapter 9, Proposition 9.4.1, p.461] we get that the polynomial $\theta_z(T)$ defines a totally real quartic extension, thus $\mathbb{Q}(s) = \mathbb{Q}(r)$, is totally real. We conclude therefore that the possible number fields are either

$$L_1 = \mathbb{Q}\big(\sqrt{2 + \sqrt{2}}\big) \ \text{ or } L_2 = \mathbb{Q}\Big(\sqrt{p(2 + \sqrt{2})}\Big).$$

The algorithm of Wildanger [15] which is implemented in the computer algebra system Kant 2.5[1] provide us with the solutions of this unit equation in L. Since $s = 4pr$, then the relation

$$a = \frac{(s^2 + 32p^2)^2}{4s(s^2 - 32p^2)},$$

[1] http://www.math.tu-berlin.de/˜kant

transforms to

$$a = p\frac{(r^2+2)^2}{r(r^2-2)},$$

and from $r = 2u - \sqrt{2}$ we get

$$a = \frac{p((2u-\sqrt{2})^2+2)^2}{(2u-\sqrt{2})((2u-\sqrt{2})^2-2)}.$$

In the case we work in L_1, the solutions of the unit equation are listed in table 1, where we have put $[a_1\ a_2\ a_3\ a_4] = a_0 + a_1\omega_1 + a_2\omega_2 + a_3\omega_3$, and $\{\omega_0 = 1, \omega_1, \omega_2, \omega_3\}$ is an integral basis of the number field L_1. We found that $a = \pm 1352p$ or $\pm 8p$. If we substitute these values to equation $y^2 = x^3 - 32p^2x$, and since p is odd, does not provide us with an integer value for y,

Table 1. The solutions (u, v) of the unit equation $u + v = \sqrt{2}$ in $\mathbb{Q}\big(\sqrt{2+\sqrt{2}}\big)$

[-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]	

If we work with the number field L_2, we have the dependence from p and so the set of solutions of the unit equation varies. So we have the following algorithm.

Input. p odd prime.

Output. The integer solutions of the equation

$$P_n = px^2. \tag{5}$$

1. If $p \equiv 3/4$, then the only solutions of (5) are given by the triple $(p, n, P_n) = (3, 4, 12)$.
2. if $p \equiv 1/4$, then solve the unit equation $u + v = \sqrt{2}$ in $\mathbb{Q}\Big(\sqrt{p(2+\sqrt{2})}\Big)$.
3. Check if $r = 2u - \sqrt{2}$ gives integer value to the expression $c = (r^2+1)^2/(r(r^2-2))$.

4. If $c \notin \mathbb{Z}$, then the equation (5) does not have any solution.
5. If $c \in \mathbb{Z}$, then find the integer n such that $P_n = c/(8p)$. (The values of n from that step, give all the solutions of (5)).

Remark

(**i**) If the rank of the elliptic curve $y^2 = x^3 - 32p^2x$ is 0, then does not have any integer non trivial solution and so the same holds for equation (5).

(**ii**) As we saw in section 2 the solutions to the equation $P_n = px^2$, with p odd prime, is reduced to the study of integral points to the elliptic curve $Y^2 = X^3 - 32p^2X$. If instead of the prime p we consider a square free integer k, then again considering n odd, we get the elliptic curve $Y^2 = X^3 - 32k^2X$. If the rank of this curve is zero then necessarily the equation $P_n = kx^2$ does not have any solution for n odd.

4 Examples

All the computations are implemented with Kash 2.5. We assume that our hardware and mainly the software was working properly.

1. $p = 5$. We are interested in the equation $P_n = 5r^2$. Since $p \equiv 1/4$, we have to solve the unit equation $u + v = \sqrt{2}$ in the field $\mathbb{Q}\left(\sqrt{5(2+\sqrt{2})}\right)$. From Kash 2.5 we get the following solutions :

$$[[11, 7, -3, -2], [-13, -7, 4, 2]], [[-13, 7, 4, -2], [11, -7, -3, 2]],$$

$$[[1, 1, -3, -1], [-3, -1, 4, 1]],$$

$$[[-3, 1, 4, -1], [1, -1, -3, 1]], [-1, [-1, 0, 1, 0]], [1, [-3, 0, 1, 0]],$$

$$[[-3, 0, 1, 0], 1], [[-1, 0, 1, 0], -1],$$

$$[[1, -1, -3, 1], [-3, 1, 4, -1]], [[-3, -1, 4, 1], [1, 1, -3, -1]],$$

$$[[11, -7, -3, 2], [-13, 7, 4, -2]], [[-13, -7, 4, 2], [11, 7, -3, -2]]$$

From these solutions we get the integer solution $(200, \pm 2800)$ on the elliptic curve

$$y^2 = x^2 - 800x.$$

So $P_n = x/8 = 200/40 = 5$. This gives $n = 3$. Thus, $(n, r) = (3, 1)$.

2. $p = 29$. We are interested in the equation $P_n = 29r^2$. Since $p \equiv 1/4$, we have to solve the unit equation $u + v = \sqrt{2}$ in the field $\mathbb{Q}\left(\sqrt{29(2+\sqrt{2})}\right)$. From Kash 2.5 we get the following solutions:

$$[[71, 99, -21, -29], [-69, -99, 20, 29]], [[-69, 99, 20, -29], [71, -99, -21, 29]],$$

$$[[13, -1, -21, 0], [-11, 1, 20, 0]], [[13, 1, -21, 0], [-11, -1, 20, 0]], [[1, 0, -1, 0], 1],$$

$$[[3,0,-1,0],-1],[-1,[3,0,-1,0]],[1,[1,0,-1,0]],$$
$$[[-11,-1,20,0],[13,1,-21,0]],[[-11,1,20,0],[13,-1,-21,0]],$$
$$[[71,-99,-21,29],[-69,99,20,-29]],[[-69,-99,20,29],[71,99,-21,-29]].$$

These, provide us with the integer point $(6728, \pm 551696)$, on the curve $y^2 = x^3 - 26912x$, which give us $P_n = 29$, so $(n,r) = (5,1)$.

3. For all primes $p \equiv 1/4$, $1000 < p < 2000$ we did not get any solution for $P_n = px^2$.
4. For $p = 95317$ it took less than 10 minutes in Kant, in order to compute the solution of the unit equation, and we found that there is not any solution to $P_n = px^2$. Further in Maple, we computed that $z^*(p) > 21000$, and we did not continue the computations further, since only for the lower bound took many hours.

References

1. Bugeaud, Y.: On the size of integer solutions of elliptic equations. Bull. Austral. Math. Soc. 57(2), 199–206 (1998)
2. Cohen, H.: Advanced topics in computational number theory. Graduate Texts in Mathematics, vol. 193., pp. xvi+578. Springer, New York (2000)
3. Egge, E.S., Mansour, T.: 132-avoiding two-stack sortable permutations, Fibonacci numbers, and Pell numbers. Discrete Appl. Math. 143(1-3), 72–83 (2004)
4. Hardy, K., Hudson, R.H., Richman, D., Williams, K.S.: Determination of all imaginary cyclic quartic fields with class number 2. Trans. Am. Math. Soc. 311(1), 1–55 (1989)
5. Huard, J.G., Spearman, B.K., Williams, K.S.: Integral bases for quartic fields with quadratic subfields. J. Number Theory 51(1), 87–102 (1995)
6. Kappe, L.-C., Warren, B.: An elementary test for the Galois group of a quartic polynomial. Amer. Math. Monthly 96(2), 133–137 (1989)
7. Ljunggren, W.: Zur Theorie der Gleichung $\mathrm{x}^2 + 1 = \mathrm{Dy}^4$. Avh. Norsk. Vid. Akad. Oslo, 1–27 (1942)
8. McDaniel, W.L.: On Fibonacci and Pell numbers of the form kx^2 (Almost every term has a 4r + 1 prime factor). Fibonacci Q. 40(1), 41–42 (2002)
9. Pethö, A.: Full cubes in the Fibonacci sequence. Publ. Math. Debrecen 30, 117–127 (1983)
10. Poulakis, D.: Integer points on algebraic curves with exceptional units. J. Austral. Math. Soc. Ser. A 63(2), 145–164 (1997)
11. Ribenboim, P.: Pell numbers, squares and cubes. Publ. Math. Debrecen 54(1-2), 131–152 (1999)
12. Robbins, N.: On Pell numbers of the form px^2, where p is prime. Fibonacci Quart 22(4), 340–348 (1984)
13. Silverman, J.H.: The Aritmetic of Elliptic Curves. Springer, Heidelberg (1986)
14. Sloane, N.J.A.: An On-Line Version of the Encyclopedia of Integer Sequences, `http://www.research.att.com/~njas/sequences/A000129`
15. 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(2), 188–224 (2000)