Pell Numbers of the form px^2

K.A. Draziotis

19 May, 2009
3rd International Conference on Algebraic Informatics
Thessaloniki

Binary Reccurence Sequences

- We call binary recurrence sequence, a sequence of integers satisfying the reccurent relation

$$u_{n+2} = Pu_{n+1} - Qu_n,$$

where P and Q are integers such that $P^2 - 4Q \neq 0$.

Binary Reccurence Sequences

- We call binary recurrence sequence, a sequence of integers satisfying the reccurent relation

$$u_{n+2} = Pu_{n+1} - Qu_n,$$

where P and Q are integers such that $P^2 - 4Q \neq 0$.

- The characteristic polynomial of the the previous binary recurrence sequence is $x^2 - Px + Q$. If α and β are its roots, then the general term of the sequence is given by the relation :

$$u_n = c\alpha^n + d\beta^n$$

where

$$c = \frac{-\beta u_0 + u_1}{\alpha - \beta}, \quad d = \frac{\alpha u_0 - u_1}{\alpha - \beta}$$

Binary Reccurence Sequences of Special Type

- If the initial terms are $u_0 = 0,\ u_1 = 1$ is called Lucas Sequence and if $u_0 = 2,\ u_1 = P$ is called companion Lucas sequence.

Binary Reccurence Sequences of Special Type

- If the initial terms are $u_0 = 0,\ u_1 = 1$ is called Lucas Sequence and if $u_0 = 2,\ u_1 = P$ is called companion Lucas sequence.
- Let $P(x)$ be a polynomial and u_n a reccurence sequence. We wonder, if there are integers n and x, such that $u_n = P(x)$.

Binary Reccurence Sequences of Special Type

- If the initial terms are $u_0 = 0,\ u_1 = 1$ is called Lucas Sequence and if $u_0 = 2,\ u_1 = P$ is called companion Lucas sequence.
- Let $P(x)$ be a polynomial and u_n a reccurence sequence. We wonder, if there are integers n and x, such that $u_n = P(x)$.
- Nemes and Pethö, described neccesary conditions for these type of equations to have infinitely many solutions.

Binary Reccurence Sequences of Special Type

- If the initial terms are $u_0 = 0,\ u_1 = 1$ is called Lucas Sequence and if $u_0 = 2,\ u_1 = P$ is called companion Lucas sequence.
- Let $P(x)$ be a polynomial and u_n a reccurence sequence. We wonder, if there are integers n and x, such that $u_n = P(x)$.
- Nemes and Pethö, described neccesary conditions for these type of equations to have infinitely many solutions.
- For the case $P(x) = bx^2,\ (b \in \mathbb{Z})$, precise results on the solutions of the equation $u_n = bx^2$ have been obtained by Ljunggren, Cohn, Walsh, Stewart, Bennett, Shorey, Ribenboim and a host of others.

Applications

- In Public Key Cryptography, we have the Lucas-Based cryptosystems (Müller, 1985).

Applications

- In Public Key Cryptography, we have the Lucas-Based cryptosystems (Müller, 1985).
- Digital Signatures (Yen; Laith, 1995)

Applications

- In Public Key Cryptography, we have the Lucas-Based cryptosystems (Müller, 1985).
- Digital Signatures (Yen; Laith, 1995)
- The divisibility properties of Lucas Sequences allow us to test the primality of an integer N, knowing the prime factorisation of $N + 1$. (Pomerance; Selfridge; Wagstaff; 1980)

Applications

- In Public Key Cryptography, we have the Lucas-Based cryptosystems (Müller, 1985).
- Digital Signatures (Yen; Laith, 1995)
- The divisibility properties of Lucas Sequences allow us to test the primality of an integer N, knowing the prime factorisation of $N+1$. (Pomerance; Selfridge; Wagstaff; 1980)
- In number theory, properties of specific binary recurrence sequences allow us to solve diophantine equations

Examples

- An investigation, of the Italian mathematician Leonardo Fibonacci in 1202, how fast rabbits could breed under ideal circumstances, led him to the study of the binarry recurrence sequence :

$$F_0 = 0, \; F_1 = 1, \; F_{n+2} = F_{n+1} + F_n.$$

which is called Fibonacci Sequence. Some terms are :

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233...$$

Examples

- A natural question is to ask how many numbers of the form $P(x)$, where P is a polynomial, there are among the Fibonacci numbers.

Examples

- A natural question is to ask how many numbers of the form $P(x)$, where P is a polynomial, there are among the Fibonacci numbers.
- For instance if $P(x) = x^2$ we note that $1 = 1^2$ and $144 = 12^2$ are some Fibonnaci numbers which are perfect squares.

Examples

- A natural question is to ask how many numbers of the form $P(x)$, where P is a polynomial, there are among the Fibonacci numbers.
- For instance if $P(x) = x^2$ we note that $1 = 1^2$ and $144 = 12^2$ are some Fibonnaci numbers which are perfect squares.
- If $P(x) = x^3$ then we note that $1 = 1^3$ and $8 = 2^3$ are some perfect cubes.

Examples

- A natural question is to ask how many numbers of the form $P(x)$, where P is a polynomial, there are among the Fibonacci numbers.
- For instance if $P(x) = x^2$ we note that $1 = 1^2$ and $144 = 12^2$ are some Fibonnaci numbers which are perfect squares.
- If $P(x) = x^3$ then we note that $1 = 1^3$ and $8 = 2^3$ are some perfect cubes.
- A deep result of Bugeud-Mignote-Siksek showed that these are the only perfect powers.

Examples

- A natural question is to ask how many numbers of the form $P(x)$, where P is a polynomial, there are among the Fibonacci numbers.
- For instance if $P(x) = x^2$ we note that $1 = 1^2$ and $144 = 12^2$ are some Fibonnaci numbers which are perfect squares.
- If $P(x) = x^3$ then we note that $1 = 1^3$ and $8 = 2^3$ are some perfect cubes.
- A deep result of Bugeud-Mignote-Siksek showed that these are the only perfect powers.
- We shall study such type of problems for the case of Pell numbers.

Definition

- Pell sequence is a Lucas sequence defined by the relation

$$P_n = 2P_{n-1} + P_{n-2}, \quad n \geq 2$$

and $P_0 = 0, \; P_1 = 1$. Some terms are :

$$2, 5, 12, 29, 70, 169, 408, 985, 2378, 5741, 13860, \ldots$$

Definition

- Pell sequence is a Lucas sequence defined by the relation

$$P_n = 2P_{n-1} + P_{n-2}, \quad n \geq 2$$

and $P_0 = 0, \; P_1 = 1$. Some terms are :

$$2, 5, 12, 29, 70, 169, 408, 985, 2378, 5741, 13860, \ldots$$

- The general term is $P_n = \frac{\epsilon^n - \bar{\epsilon}^n}{2\sqrt{2}}$, where $\epsilon = 1 + \sqrt{2}$.

- Some properties of Pell sequence are the following.

  i. The denominators of continued fraction convergents to

$$\sqrt{2} : 1,\ 3/2,\ 7/5,\ 17/12,\ 41/29,\ 99/70,$$

$$239/169,\ 577/408,\ 1393/985, \ldots$$

- Some properties of Pell sequence are the following.
  i. The denominators of continued fraction convergents to

$$\sqrt{2} : 1,\ 3/2,\ 7/5,\ 17/12,\ 41/29,\ 99/70,$$

$$239/169,\ 577/408,\ 1393/985, \ldots$$

- Also, they have the following combinatorial meaning :
  ii. Number of lattice paths from $(0,0)$ to the line $x = n - 1$ consisting of $U = (1,1),\ D = (1,-1)$ and $H = (2,0)$ steps.
  iii. Number of $132-$ avoiding two-stack sortable permutations (E.Egg, T.Mansour).

- Some properties of Pell sequence are the following.
  i. The denominators of continued fraction convergents to

$$\sqrt{2} : 1,\ 3/2,\ 7/5,\ 17/12,\ 41/29,\ 99/70,$$

$$239/169,\ 577/408,\ 1393/985, \ldots$$

- Also, they have the following combinatorial meaning :
  ii. Number of lattice paths from $(0,0)$ to the line $x = n - 1$ consisting of $U = (1,1),\ D = (1,-1)$ and $H = (2,0)$ steps.
  iii. Number of $132-$ avoiding two-stack sortable permutations (E.Egg, T.Mansour).
- An application : The Pell primality test is "If N is an odd prime, then $P_n - \left(\frac{2}{n}\right)$ is divisible by N". "Most" composite numbers fail this test, so it makes a useful pseudoprimality test.

The connection with the Elliptic curves

- We are interested in finding the Pell numbers of the form px^2. That is to find positive integers n and x such that $P_n = px^2$ for some fixed, but arbitrary, prime number p.

The connection with the Elliptic curves

- We are interested in finding the Pell numbers of the form px^2. That is to find positive integers n and x such that $P_n = px^2$ for some fixed, but arbitrary, prime number p.
- If n is even or $p \equiv 3 \mod 4$ then using elementary number theory we can prove that $p = 3,\ n = 4$ $(P_4 = 12 = 3 \cdot 2^2.)$

The connection with the Elliptic curves

- We are interested in finding the Pell numbers of the form px^2. That is to find positive integers n and x such that $P_n = px^2$ for some fixed, but arbitrary, prime number p.
- If n is even or $p \equiv 3 \mod 4$ then using elementary number theory we can prove that $p = 3,\ n = 4$ $(P_4 = 12 = 3 \cdot 2^2.)$
- We suppose that n is odd. We set $P_{2n-1} = pr^2,\ P_{2n+1} = t$. A straightforward calculation with the general term of Pell sequence,

$$P_n = \frac{\epsilon^n - \bar{\epsilon}^n}{2\sqrt{2}}, \text{ where } \epsilon = 1 + \sqrt{2},$$

gives

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

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

- So, $p^2r^4 + t^2 + 4 = 6pr^2t$.
- This equation defines an elliptic curve over $\mathbb{Q}$. Using the map

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

we get the curve

$$Y^2 = 8p^2X^4 - 4. \tag{2}$$

(Note that if (r, t) is an integer point, then also (X, Y) is integer point. That is the map preseves the integer points.)

- So, $p^2 r^4 + t^2 + 4 = 6pr^2 t$.
- This equation defines an elliptic curve over $\mathbb{Q}$. Using the map
$$(r, t) \to (X, 3pX^2 + Y),$$
we get the curve
$$Y^2 = 8p^2 X^4 - 4. \tag{2}$$
(Note that if (r, t) is an integer point, then also (X, Y) is integer point. That is the map preseves the integer points.)
- Finally, setting $x = 2(2pX)^2$ and $y = 2(2pX)(pY)$ we get the elliptic curve
$$y^2 = x^3 - 32p^2 x. \tag{3}$$
So we have to determine its integer points under the condition x to be of the form $2X'^2$.

- So, $p^2r^4 + t^2 + 4 = 6pr^2t$.
- This equation defines an elliptic curve over $\mathbb{Q}$. Using the map

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

we get the curve

$$Y^2 = 8p^2X^4 - 4. \tag{2}$$

(Note that if (r, t) is an integer point, then also (X, Y) is integer point. That is the map preseves the integer points.)
- Finally, setting $x = 2(2pX)^2$ and $y = 2(2pX)(pY)$ we get the elliptic curve

$$y^2 = x^3 - 32p^2x. \tag{3}$$

So we have to determine its integer points under the condition x to be of the form $2X'^2$.
- We have to say some basic things about the Ellipitic Curves and how we can find its integer points.

Elliptic Curves

Let K be a number field and $\overline{K}$ its algebraic closure. Let E be an algebraic curve defined by the equation

$$E : y^2 = x^3 + Ax + B, \quad A, B \in K, \quad 4A^3 + 27B^2 \neq 0.$$

Elliptic curve over K is the set of points of E with coordinates from K and one more point, the point of infinity. That is the point $[0 : 1 : 0]$ in projective coordinates.

Elliptic Curves

Over the $K-$points of E we define an addition :

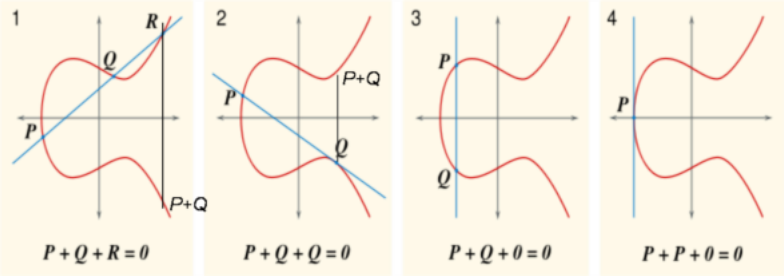

Figure: The neurtal element is the point at infinity of E, that is $\mathbf{0} = [0 : 1 : 0]$.

- We can easily check that the set of points $E(K)$ with this addition form an Abelian group. Mordell proved that, if $K = \mathbb{Q}$ then is finitely generated and A.Neron generalize to the case where $K \neq \mathbb{Q}$. So

$$E(K) \simeq E_{torsion}(K) \oplus \mathbb{Z}^r.$$

The non-negative integer r is called *rank* of the Elliptic E over K.

- If the Elliptic curve has rank zero, then the determination of its integer (and also rational) points is very simple in practice (application of Lutz-Nagel Theorem). The number of integer points of an elliptic curve (over a number field) is always finite (Theorem of Siegel). The number of rational points are infinitely many, if the rank is larger than zero.

- There are many methods to study the integer points on Elliptic curves. The most general is that of Tzanakis-Stroeker which is called *Elliptic Logarithm Method*. The disadnantage of this method is that we need a basis of independent points, which is sometimes a difficult and expensive task. Also the so called Thue method, is used for the resolution of integer points. This method is not always applicable. Also there are ad hoc methods from elementary number theory such as reduction $\mod p$, manipulations with Legendre symbol, factorisation over a number field and others.

- We shall apply a relatively "new" method which we call "multuplication by 2 Chabauty method". Historically first Chabauty presented the idea of the reduction of the study of the integer points on an Elliptic curve to the study of some unit equations over some number fields. This method is applied for the practical solution of diophantine equations $y^2 = x^3 - n^2x$, first time by Poulakis and Draziotis.

- In our problem, in order to find the Pell terms of the form px^2, we have to find the integer points of the elliptic curve $C : y^2 = x^3 - 32p^2x$.

- In our problem, in order to find the Pell terms of the form px^2, we have to find the integer points of the elliptic curve $C : y^2 = x^3 - 32p^2x$.
- The method of Chabauty consists from (say) four steps.

- Let P be a point with integer coordinates on C and $R = (s, t)$ a point such that $2R = P$. In the first step we shall compute all the possible number fields $\mathbb{Q}(R) = \mathbb{Q}(s, t)$, as P runs in all integer points of C.

- Let P be a point with integer coordinates on C and $R=(s,t)$ a point such that $2R=P$. In the first step we shall compute all the possible number fields $\mathbb{Q}(R)=\mathbb{Q}(s,t)$, as P runs in all integer points of C.
- Then we shall prove that the elements $u_{1,2}=\frac{s\pm\sqrt{2}}{2}$ are units in $\mathbb{Q}(R)$. Units means that their norms are equal to ± 1. Also note that they satisfy the relation $u_1-u_2=\sqrt{2}$. From a basic theorem of Siegel the "unit equation" $X-Y=\sqrt{2}$ has finitely many solutions in a number field.

- Let P be a point with integer coordinates on C and $R=(s,t)$ a point such that $2R=P$. In the first step we shall compute all the possible number fields $\mathbb{Q}(R)=\mathbb{Q}(s,t)$, as P runs in all integer points of C.
- Then we shall prove that the elements $u_{1,2}=\frac{s\pm\sqrt{2}}{2}$ are units in $\mathbb{Q}(R)$. Units means that their norms are equal to ± 1. Also note that they satisfy the relation $u_1-u_2=\sqrt{2}$. From a basic theorem of Siegel the "unit equation" $X-Y=\sqrt{2}$ has finitely many solutions in a number field.
- In order to solve this we use the algorithm of Wildanger which is implemented in the computer algebra system Kash/Kant and Magma.

- Let P be a point with integer coordinates on C and $R=(s,t)$ a point such that $2R=P$. In the first step we shall compute all the possible number fields $\mathbb{Q}(R)=\mathbb{Q}(s,t)$, as P runs in all integer points of C.
- Then we shall prove that the elements $u_{1,2}=\frac{s\pm\sqrt{2}}{2}$ are units in $\mathbb{Q}(R)$. Units means that their norms are equal to ± 1. Also note that they satisfy the relation $u_1-u_2=\sqrt{2}$. From a basic theorem of Siegel the "unit equation" $X-Y=\sqrt{2}$ has finitely many solutions in a number field.
- In order to solve this we use the algorithm of Wildanger which is implemented in the computer algebra system Kash/Kant and Magma.
- Once we find the possible units $u_{1,2}$ then we find R and so we shall find all the possible integer points P. We are done.

- Let $P = (a, b)$ be an integer point of C. Let also $R = (s, t)$, be a point of C such that $2R = P$. Then

$$a = \frac{s^4 + 64p^2s^2 + 1024p^4}{4(s^3 - 32p^2s)} \text{ (duplication formula)}$$

and so s is a root of the polynomial

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

- The roots of $\Theta_a(T)$ are given by,

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

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

- The roots of $\Theta_a(T)$ are given by,

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

  where the first $\pm$ coincide with the third.
- Our goal is to express more explicit the number field $\mathbb{Q}(R)$ which is proved that, is equal with $\mathbb{Q}(s)$.

- The roots of $\Theta_a(T)$ are given by,

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

  where the first $\pm$ coincide with the third.
- Our goal is to express more explicit the number field $\mathbb{Q}(R)$ which is proved that, is equal with $\mathbb{Q}(s)$.
- If we set L be the number field with defining polynomial $\Theta_a(T)$, that is $L = \mathbb{Q}(s)$ we get

$$L = \mathbb{Q}\left(\sqrt{2a^2 \pm 2a\sqrt{a^2 - 32p^2}}\right).$$

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

- *Lemma.* The extension $L/\mathbb{Q}$ is a cyclic extension of $\mathbb{Q}$.
- From Kenneth we get

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

with $B \geq 1$, A squarefree and odd, $D \geq 2$ squarefree, $D - B^2$ is square and $\gcd(A, D) = 1$.

- *Lemma.* The extension $L/\mathbb{Q}$ is a cyclic extension of $\mathbb{Q}$.
- From Kenneth we get

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

with $B \geq 1$, A squarefree and odd, $D \geq 2$ squarefree, $D - B^2$ is square and $\gcd(A, D) = 1$.
- The Neron-Ogg-Shafarevich Criterion gives $A \in \{\pm 1, \pm p\}$.

- *Lemma.* The extension $L/\mathbb{Q}$ is a cyclic extension of $\mathbb{Q}$.
- From Kenneth we get

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

with $B \geq 1$, A squarefree and odd, $D \geq 2$ squarefree, $D - B^2$ is square and $\gcd(A, D) = 1$.

- The Neron-Ogg-Shafarevich Criterion gives $A \in \{\pm 1, \pm p\}$.
- Finally, from a Theorem of Henri Cohen we get that the extension $\mathbb{Q}(s)$, is totally real.

- *Lemma.* The extension $L/\mathbb{Q}$ is a cyclic extension of $\mathbb{Q}$.
- From Kenneth we get

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

with $B \geq 1$, A squarefree and odd, $D \geq 2$ squarefree, $D - B^2$ is square and $\gcd(A, D) = 1$.
- The Neron-Ogg-Shafarevich Criterion gives $A \in \{\pm 1, \pm p\}$.
- Finally, from a Theorem of Henri Cohen we get that the extension $\mathbb{Q}(s)$, is totally real.
- We finally get two possible number fields : $L_1 = \mathbb{Q}(\sqrt{2 + \sqrt{2}})$ or $L_2 = \mathbb{Q}\left(\sqrt{p(2 + \sqrt{2})}\right)$.

- We shall find a new defining polynomial for our extension $L/\mathbb{Q}$ in order to have simpler unit equations.

- We shall find a new defining polynomial for our extension $L/\mathbb{Q}$ in order to have simpler unit equations.
- It easy to check that $r = s/4pr$, is another generator of L and that the elements $u = \frac{r+\sqrt{2}}{2}$ and $v = \frac{\sqrt{2}-r}{2}$ are units of L. Also they satisfy the unit equation $u + v = \sqrt{2}$ in L.

Elliptic Curves

- In case we work in L_1, we did not found any integer solution.

Elliptic Curves

- In case we work in L_1, we did not found any integer solution.
- So we have only to work over the number field L_2.

1. $P_n = 5r^2$. We solve the unit equation $u + v = \sqrt{2}$ in the field $L = \mathbb{Q}\left(\sqrt{5(2+\sqrt{2})}\right)$. From Kant/Kash we get the following solutions to the unit equation :
$[[11, 7, -3, -2], [-13, -7, 4, 2]], [[-13, 7, 4, -2], [11, -7, -3, 2]],$

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

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

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

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

From these solutions we get the integer solution $(200, \pm 2800)$ on the elliptic curve $C : y^2 = x^3 - 800x$, (here $32p^2 = 800$). We finally get $n = 3$ and so the only term of the form $5r^2$ is $P_3 = 5$.

2. We are interested in the equation $P_n = 29r^2$. We have to solve the unit equation $u + v = \sqrt{2}$ in the field $L = \mathbb{Q}\left(\sqrt{29(2+\sqrt{2})}\right)$.
From Kant/Kash 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 only one integer point $(6728, \pm 551696)$, on the curve $C : y^2 = x^3 - 26912x$, which give us $P_5 = 29$.

- 3. For all primes $p \equiv 1 \mod 4$, $1000 < p < 2000$ we did not get any solution for $P_n = px^2$.

- 3. For all primes $p \equiv 1 \mod 4$, $1000 < p < 2000$ we did not get any solution for $P_n = px^2$.
- Thank you.