On the Pell equation in polynomials

Laura Capuano

Politecnico di Torino

25/10/2019

Pell equation in polynomials

The classical Pell equation

$$A^2 - DB^2 = 1,$$

to be solved in integers $A, B \in \mathbb{Z}$ with $B \neq 0$ has a natural analogue in the polynomial ring $K[X]$.

The classical Pell equation

$$A^2 - DB^2 = 1,$$

to be solved in integers $A, B \in \mathbb{Z}$ with $B \neq 0$ has a natural analogue in the polynomial ring $K[X]$.

Let $D \in K[X]$; we ask if there exist $A, B \in K[X]$ with $B \neq 0$ such that

$$A^2 - DB^2 = 1.$$

If such a solution exists, we call the polynomial D **"Pellian"**.

Pell equation in polynomials

The classical Pell equation

$$A^2 - DB^2 = 1,$$

to be solved in integers $A, B \in \mathbb{Z}$ with $B \neq 0$ has a natural analogue in the polynomial ring $K[X]$.

Let $D \in K[X]$; we ask if there exist $A, B \in K[X]$ with $B \neq 0$ such that

$$A^2 - DB^2 = 1.$$

If such a solution exists, we call the polynomial D **"Pellian"**.

- This equation is less famous than the classical one, but it goes back to Abel in 1826 who studied it in the context of integration of algebraic differentials.

Necessary conditions for solvability

- $\deg(D) = 2d$;
- D is not a square in $K[X]$;
- l.c. of D is a square in K.

Pell equation in polynomials

Necessary conditions for solvability

- $\deg(D) = 2d$;
- D is not a square in $K[X]$;
- l.c. of D is a square in K.

These conditions however are not sufficient in general to guarantee the existence of a non-trivial solution.

- If K is a finite field of char $\neq 2$, these conditions are also sufficient and the theory is completely analogous to the classical case;
- In general the problem is much more complicated and these conditions are not enough.

Necessary conditions for solvability

- $\deg(D) = 2d$;
- D is not a square in $K[X]$;
- l.c. of D is a square in K.

These conditions however are not sufficient in general to guarantee the existence of a non-trivial solution.

- If K is a finite field of char $\neq 2$, these conditions are also sufficient and the theory is completely analogous to the classical case;
- In general the problem is much more complicated and these conditions are not enough.

Questions:

- Given $D \in K[X]$, how is it possible to decide if D is Pellian?

Pell equation in polynomials

Necessary conditions for solvability

- $\deg(D) = 2d$;
- D is not a square in $K[X]$;
- l.c. of D is a square in K.

These conditions however are not sufficient in general to guarantee the existence of a non-trivial solution.

- If K is a finite field of char $\neq 2$, these conditions are also sufficient and the theory is completely analogous to the classical case;
- In general the problem is much more complicated and these conditions are not enough.

Questions:

- Given $D \in K[X]$, how is it possible to decide if D is Pellian?
- "How many" Pellian polynomials do we have?

Pell equation in polynomials

Necessary conditions for solvability

- $\deg(D) = 2d$;
- D is not a square in $K[X]$;
- l.c. of D is a square in K.

These conditions however are not sufficient in general to guarantee the existence of a non-trivial solution.

- If K is a finite field of char $\neq 2$, these conditions are also sufficient and the theory is completely analogous to the classical case;
- In general the problem is much more complicated and these conditions are not enough.

Questions:

- Given $D \in K[X]$, how is it possible to decide if D is Pellian?
- "How many" Pellian polynomials do we have?

Example

In this talk K will be an algebraically closed field of char 0 (usually $\overline{\mathbb{Q}}$ or $\mathbb{C}$).

Example

In this talk K will be an algebraically closed field of char 0 (usually $\overline{\mathbb{Q}}$ or $\mathbb{C}$).

- $\mathbf{deg(D) = 2}$: every polynomial which is not a square in $K[X]$ is Pellian;

Example

In this talk K will be an algebraically closed field of char 0 (usually $\overline{\mathbb{Q}}$ or $\mathbb{C}$).

- $\mathbf{deg(D) = 2}$: every polynomial which is not a square in $K[X]$ is Pellian;
- $\mathbf{deg(D) = 4}$: there are examples of polynomials which are not Pellian and are not squares in $K[X]$.

Example

In this talk K will be an algebraically closed field of char 0 (usually $\overline{\mathbb{Q}}$ or $\mathbb{C}$).

- $\mathbf{deg(D) = 2}$: every polynomial which is not a square in $K[X]$ is Pellian;
- $\mathbf{deg(D) = 4}$: there are examples of polynomials which are not Pellian and are not squares in $K[X]$.

Examples

- $D(X) = X^4 + X + 1$ *is not Pellian;*

Example

In this talk K will be an algebraically closed field of char 0 (usually $\overline{\mathbb{Q}}$ or $\mathbb{C}$).

- **$\deg(D) = 2$**: every polynomial which is not a square in $K[X]$ is Pellian;
- **$\deg(D) = 4$**: there are examples of polynomials which are not Pellian and are not squares in $K[X]$.

Examples

- $D(X) = X^4 + X + 1$ *is not Pellian;*
- $D(X) = X^4 + X$ *is Pellian as*

$$(2X^3 + 1)^2 - (X^4 + X)(2X)^2 = 1.$$

Pell equation in families of polynomials

What does it happen if we let the polynomial vary in a family?

Pell equation in families of polynomials

What does it happen if we let the polynomial vary in a family?

Example

Let us take $D_t(X) = X^4 + X + t \in \overline{\mathbb{Q}}(t)[X]$;

- $A^2 - D_t B^2 = 1$ *is not identically solvable;*
- *For how many specializations of the parameter* $t \in \mathbb{C}$ *the specialized polynomial is Pellian?*

Pell equation in families of polynomials

What does it happen if we let the polynomial vary in a family?

Example

Let us take $D_t(X) = X^4 + X + t \in \overline{\mathbb{Q}}(t)[X]$;

- $A^2 - D_t B^2 = 1$ *is not identically solvable;*
- *For how many specializations of the parameter* $t \in \mathbb{C}$ *the specialized polynomial is Pellian?*

Proposition

$D_{t_0}(X) = X^4 + X + t_0$ *is Pellian* $\iff$ $(0, 1)$ *is a torsion point of the elliptic curve* $y^2 = x^3 - 4t_0 x + 1$ *(with* $256t_0^3 \neq 27$*).*

Pell equation in families of polynomials

What does it happen if we let the polynomial vary in a family?

Example

Let us take $D_t(X) = X^4 + X + t \in \overline{\mathbb{Q}}(t)[X]$;

- $A^2 - D_t B^2 = 1$ *is not identically solvable;*
- *For how many specializations of the parameter* $t \in \mathbb{C}$ *the specialized polynomial is Pellian?*

Proposition

$D_{t_0}(X) = X^4 + X + t_0$ *is Pellian* $\iff$ $(0, 1)$ *is a torsion point of the elliptic curve* $y^2 = x^3 - 4t_0 x + 1$ *(with* $256 t_0^3 \neq 27$*).*

Silverman specialization theorem → bounded height.

$\mathbf{deg(D) = 6}$: Let us take

$$D_t(X) = X^6 + X + t \in \overline{\mathbb{Q}}(t)[X];$$

$\mathbf{deg(D) = 6}$: Let us take

$$D_t(X) = X^6 + X + t \in \overline{\mathbb{Q}}(t)[X];$$

- D_t is not identically Pellian
  (for example $D_1(X)$ is not Pellian);

$\mathbf{deg(D) = 6}$: Let us take

$$D_t(X) = X^6 + X + t \in \overline{\mathbb{Q}}(t)[X];$$

- D_t is not identically Pellian (for example $D_1(X)$ is not Pellian);
- $D_0(X) = X^6 + X$ is Pellian (because $(2X^5+1)^2 - (X^6+X)(2X^2)^2 = 1$);

deg(D) = 6: Let us take

$$D_t(X) = X^6 + X + t \in \overline{\mathbb{Q}}(t)[X];$$

- D_t is not identically Pellian
  (for example $D_1(X)$ is not Pellian);
- $D_0(X) = X^6 + X$ is Pellian
  (because $(2X^5 + 1)^2 - (X^6 + X)(2X^2)^2 = 1$);

Theorem (Masser-Zannier 2015)

There exist only finitely many $t_0 \in \mathbb{C}$ such that D_{t_0} is Pellian.

Geometric criteria for solvability

Let D be a *squarefree* polynomial of even degree. Consider the hyperelliptic curve defined by

$$Y^2 = D(X).$$

Let D be a *squarefree* polynomial of even degree. Consider the hyperelliptic curve defined by

$$Y^2 = D(X).$$

If we take a non-singular model H_D of the curve, it will have two points at infinity, which we call ∞^+ and ∞^-.

Geometric criteria for solvability

Let D be a *squarefree* polynomial of even degree. Consider the hyperelliptic curve defined by

$$Y^2 = D(X).$$

If we take a non-singular model H_D of the curve, it will have two points at infinity, which we call ∞^+ and ∞^-.

Let us take the Jacobian variety associated to the curve H_D, i.e. the abelian group:

$$\mathcal{J}_D = Div^0(H_D)/PDiv(H_D).$$

Geometric criteria for solvability

Let D be a *squarefree* polynomial of even degree. Consider the hyperelliptic curve defined by

$$Y^2 = D(X).$$

If we take a non-singural model H_D of the curve, it will have two points at infinity, which we call ∞^+ and ∞^-.

Let us take the Jacobian variety associated to the curve H_D, i.e. the abelian group:

$$\mathcal{J}_D = Div^0(H_D)/PDiv(H_D).$$

Theorem (Abel)

The Pell equation $A^2 - DB^2 = 1$ is non-trivially solvable if and only if $[\infty^+ - \infty^-]$ is a torsion point in $\mathcal{J}_D$. Moreover, the order of the torsion point is equal to the minimal degree of the polynomial A.

- $D_t(X) \in \overline{\mathbb{Q}}(t)[X]$ a squarefree polynomial of degree ≥ 6;

- $D_t(X) \in \overline{\mathbb{Q}}(t)[X]$ a squarefree polynomial of degree ≥ 6;
- $\mathcal{J}_{D_t}$ the Jacobian variety of $Y^2 = D_t(X)$; assume $\mathcal{J}_{D_t}$ is simple;

Linear relations in families of abelian varieties

- $D_t(X) \in \overline{\mathbb{Q}}(t)[X]$ a squarefree polynomial of degree ≥ 6;
- $\mathcal{J}_{D_t}$ the Jacobian variety of $Y^2 = D_t(X)$; assume $\mathcal{J}_{D_t}$ is simple;
- $P_t : \mathbb{P}^1 \setminus \{0, 1, \infty\} \to \mathcal{J}_{D_t}$ a section defined over $\overline{\mathbb{Q}(t)}$;

Linear relations in families of abelian varieties

- $D_t(X) \in \overline{\mathbb{Q}}(t)[X]$ a squarefree polynomial of degree ≥ 6;
- $\mathcal{J}_{D_t}$ the Jacobian variety of $Y^2 = D_t(X)$; assume $\mathcal{J}_{D_t}$ is simple;
- $P_t : \mathbb{P}^1 \setminus \{0, 1, \infty\} \to \mathcal{J}_{D_t}$ a section defined over $\overline{\mathbb{Q}(t)}$;

Theorem (Masser-Zannier 2018)

If P_t is not identically torsion, then there exist at most finitely many $t_0 \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$ such that P_{t_0} is torsion on $\mathcal{J}_{D_{t_0}}$.

More in general, let $P_1, \ldots, P_n : \mathbb{P}^1 \setminus \{0, 1, \infty\} \to \mathcal{J}_{D_t}$ be n sections defined over $\overline{\mathbb{Q}(t)}$; call $R = \mathrm{End}(\mathcal{J}_{D_t})$.

More in general, let $P_1, \dots, P_n : \mathbb{P}^1 \setminus \{0, 1, \infty\} \to \mathcal{J}_{D_t}$ be n sections defined over $\overline{\mathbb{Q}(t)}$; call $R = \mathrm{End}(\mathcal{J}_{D_t})$.

Theorem (Barroero-C. 2018)

Assume that $P_1, \dots, P_n$ does not identically satisfy any linear relation of the form $a_1 P_1 + \cdots + a_n P_n = 0$ with $a_i \in R$ not all zero;

Linear relations in families of abelian varieties

More in general, let $P_1, \dots, P_n : \mathbb{P}^1 \setminus \{0, 1, \infty\} \to \mathcal{J}_{D_t}$ be n sections defined over $\overline{\mathbb{Q}(t)}$; call $R = \mathrm{End}(\mathcal{J}_{D_t})$.

Theorem (Barroero-C. 2018)

Assume that $P_1, \dots, P_n$ does not identically satisfy any linear relation of the form $a_1 P_1 + \dots + a_n P_n = 0$ with $a_i \in R$ not all zero; then, there exist at most finitely many values $t_0 \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$ such that $P_1(t_0), \dots, P_n(t_0)$ satisfy a linear relation with coefficients in R on $\mathcal{J}_{D_{t_0}}$.

Linear relations in families of abelian varieties

More in general, let $P_1, \ldots, P_n : \mathbb{P}^1 \setminus \{0, 1, \infty\} \to \mathcal{J}_{D_t}$ be n sections defined over $\overline{\mathbb{Q}(t)}$; call $R = \mathrm{End}(\mathcal{J}_{D_t})$.

Theorem (Barroero-C. 2018)

Assume that $P_1, \ldots, P_n$ does not identically satisfy any linear relation of the form $a_1 P_1 + \cdots + a_n P_n = 0$ with $a_i \in R$ not all zero; then, there exist at most finitely many values $t_0 \in \mathbb{P}^1 \setminus \{0, 1, \infty\}$ such that $P_1(t_0), \ldots, P_n(t_0)$ satisfy a linear relation with coefficients in R on $\mathcal{J}_{D_{t_0}}$.

- These questions are related to problems of "unlikely intersections" in families of abelian varieties.

We can use these results about "linear independence" of sections for families of Jacobians to recover results about the solvability of the polynomial Pell equation; more generally, we can study the generalized Pell equation

$$A^2 - DB^2 = F,$$

with $F \in \overline{\mathbb{Q}}[X]$.

We can use these results about "linear independence" of sections for families of Jacobians to recover results about the solvability of the polynomial Pell equation; more generally, we can study the generalized Pell equation

$$A^2 - DB^2 = F,$$

with $F \in \overline{\mathbb{Q}}[X]$. In this case,

solvability of the generalized Pell equation

$\Updownarrow$

relations of linear dependence for certain points on $\mathcal{J}_D$.

Theorem (Barroero-C. 2018)

Let $D_t(X) \in \overline{\mathbb{Q}}(t)[X]$ such that the Jacobian variety $\mathcal{J}_{D_t}$ of the curve of equation $Y^2 = D_t(X)$ does not contain any proper abelian subvariety of dimension 1. Let $F_t(X) \in \overline{\mathbb{Q}}(t)[X] \setminus \{0\}$. Then, either the generalized Pell equation is identically solvable, or there exist at most finitely many $t_0 \in \mathbb{C}$ such that the specialized equation

$$A^2 - D_{t_0} B^2 = F_{t_0}$$

has a non-trivial solution $A, B \in \mathbb{C}[X]$.

Example

Let $K = \overline{\mathbb{Q}}(t)$ and let us consider the generalized Pell equation

$$A^2 - D_t B^2 = F,$$

where $D_t \in K[X]$ is the family of polynomials defined by

$$D_t(X) = (X - t)(X^7 - X^3 - 1) \quad \text{and} \quad F(X) = 4X + 1 \in \overline{\mathbb{Q}}[X].$$

Example

Let $K = \overline{\mathbb{Q}}(t)$ and let us consider the generalized Pell equation

$$A^2 - D_t B^2 = F,$$

where $D_t \in K[X]$ is the family of polynomials defined by

$$D_t(X) = (X - t)(X^7 - X^3 - 1) \quad \text{and} \quad F(X) = 4X + 1 \in \overline{\mathbb{Q}}[X].$$

- the polynomial $X^7 - X^3 - 1$ has no multiple roots and the Galois group of its splitting field over $\mathbb{Q}$ is S_7;
- Zarhin $\rightarrow \mathcal{J}_{D_t}$ is simple;
- the equation is not identically solvable.

Example

Let $K = \overline{\mathbb{Q}}(t)$ and let us consider the generalized Pell equation

$$A^2 - D_t B^2 = F,$$

where $D_t \in K[X]$ is the family of polynomials defined by

$$D_t(X) = (X - t)(X^7 - X^3 - 1) \quad \text{and} \quad F(X) = 4X + 1 \in \overline{\mathbb{Q}}[X].$$

- the polynomial $X^7 - X^3 - 1$ has no multiple roots and the Galois group of its splitting field over $\mathbb{Q}$ is S_7;
- Zarhin $\rightarrow$ $\mathcal{J}_{D_t}$ is simple;
- the equation is not identically solvable.

Then, there exist at most finitely many $t_0 \in \mathbb{C}$ such that the specialized Pell equation has a non-trivial solution.

Example 2

Let $D_t(X) = X^{12} + X^4 + t \in \mathbb{Q}(t)[X]$ and $F(X) = X^4 - 1$. We can define the map

$$\beta : H_{D_t} \to H_{\widetilde{D}_t} \quad \beta(X, Y) = (X_1, Y_1) = (X^4, X^2 Y),$$

where $H_{\widetilde{D}_t}$ is the genus 1 curve defined by the equation

$$Y_1^2 = \widetilde{D}_t(X_1) = X_1^4 + X_1^2 + tX_1.$$

Example 2

Let $D_t(X) = X^{12} + X^4 + t \in \mathbb{Q}(t)[X]$ and $F(X) = X^4 - 1$. We can define the map

$$\beta : H_{D_t} \to H_{\widetilde{D}_t} \quad \beta(X, Y) = (X_1, Y_1) = (X^4, X^2 Y),$$

where $H_{\widetilde{D}_t}$ is the genus 1 curve defined by the equation

$$Y_1^2 = \widetilde{D}_t(X_1) = X_1^4 + X_1^2 + tX_1.$$

Let $\widetilde{F}(X_1) = X_1 - 1$ and let us consider the generalized Pell equation

$$A^2 - \widetilde{D}_t B^2 = \widetilde{F}. \tag{1}$$

Example 2

Let $D_t(X) = X^{12} + X^4 + t \in \mathbb{Q}(t)[X]$ and $F(X) = X^4 - 1$. We can define the map

$$\beta : H_{D_t} \to H_{\widetilde{D}_t} \quad \beta(X,Y) = (X_1, Y_1) = (X^4, X^2Y),$$

where $H_{\widetilde{D}_t}$ is the genus 1 curve defined by the equation

$$Y_1^2 = \widetilde{D}_t(X_1) = X_1^4 + X_1^2 + tX_1.$$

Let $\widetilde{F}(X_1) = X_1 - 1$ and let us consider the generalized Pell equation

$$A^2 - \widetilde{D}_t B^2 = \widetilde{F}. \tag{1}$$

- (1) is not identically solvable but there exist infinitely many $t_0 \in \mathbb{C}$ such that the specialized equation is solvable;

Example 2

Let $D_t(X) = X^{12} + X^4 + t \in \mathbb{Q}(t)[X]$ and $F(X) = X^4 - 1$. We can define the map

$$\beta : H_{D_t} \to H_{\widetilde{D}_t} \quad \beta(X,Y) = (X_1, Y_1) = (X^4, X^2 Y),$$

where $H_{\widetilde{D}_t}$ is the genus 1 curve defined by the equation

$$Y_1^2 = \widetilde{D}_t(X_1) = X_1^4 + X_1^2 + tX_1.$$

Let $\widetilde{F}(X_1) = X_1 - 1$ and let us consider the generalized Pell equation

$$A^2 - \widetilde{D}_t B^2 = \widetilde{F}. \tag{1}$$

- (1) is not identically solvable but there exist infinitely many $t_0 \in \mathbb{C}$ such that the specialized equation is solvable;
- $(\tilde{A}(X_1), \tilde{B}(X_1))$ is a solution of (1) $\iff$ $(\tilde{A}(X^4), X^2\tilde{B}(X^4))$ is a solution of $A^2 - D_t B^2 = F$.