Pell equations over polynomial rings.

D. Bertrand (IMJ-PRG)

IHP, March 20, 2018

Paulo Ribenboim 90

Pell → Abel

Teorema (Fermat) : *seja D um número inteiro positivo, que* não é um quadrado perfeito. *Então a equação de Pell-Fermat*

$$x^2 - Dy^2 = 1$$

possui uma solução em números inteiros (x, y)*, com* $y \neq 0$*, e portanto uma infinidade de tais soluções.*

NB : (i) so, for $O = \mathbb{Z}[\sqrt{D}]$, O^* has rank 1.

(ii) The classical proof uses the box principle 3 times, and studies the "generalized" Pell equation $x^2 - Dy^2 = k$. (See also [R].)

(iii) non squarefree is allowed. If $\Delta = f^2 D$, $[O : O_\Delta] = f$, then O_Δ^* contains $Ker\{O^* \to (O/fO)^*\}$, so same rank.

Abel : replace $\mathbb{Z}$ by $\mathbb{C}[X]$ to study why $\int \frac{f(x)}{\sqrt{D(x)}} dx$ can sometimes be computed without abelian integrals.

Let $k = \overline{\mathbb{Q}}$. A non constant polynomial $D \in k[X]$ is *pellian* if there exists $A, B \in k[X]$, with $B \neq 0$, such that

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

Then, $deg(D) = d$ is even, and D is not a square. Any such D with $d = 2$ is Pellian, so from now on, $d \geq 4$, and we also assume that *D is square-free*. Consider the (hyper)elliptic curve $y^2 = D(x)$. The ring $k[x, y]$ is a Dedekind domain, the smooth complete model C of the curve has two additional places ∞^+, ∞^-, and $g(C) = (d/2) - 1$.

Theorem (Abel) : • *D is pellian if and only if the class p of $(\infty^+) - (\infty^-)$ in $Jac(C)$ is a torsion point.*

Let now $\Delta = (X - \rho)^2 D$, where $D(\rho) \neq 0$, and let $Jac_{\mathfrak{q}}(C)$ be the generalized jacobian for the modulus $\mathfrak{q} = \mathfrak{q}^+ + \mathfrak{q}^-$ (above ρ). Then,

• *Δ is pellian if and only if the class $\tilde{p}$ of $(\infty^+) - (\infty^-)$ in $Jac_{\mathfrak{q}}(C)$ is a torsion point.*

And if $\overline{\Delta} = (X - \rho)^2 D$, where $D(\rho) = 0$, so one point $\overline{\mathfrak{q}}$ above ρ:

• *$\overline{\Delta}$ is pellian if and only if the class $\overline{p}$ of $(\infty^+) - (\infty^-)$ in $Jac_{2\overline{\mathfrak{q}}}(C)$ is torsion.*

Unlikely intersections

How often can this happen ?

This is the theme of *Unlikely intersections*, a topic initiated by Bombieri-Masser-Zannier for tori, then Zilber, then merging with conjectures of Pink which generalize Manin-Mumford, Mordell-Lang, André-Oort, ...

General principle : *it is unlikely that a subvariety W of a special variety G meets the union of the special subvarieties of G of codimension $>$ dim(W) Zariski-densely, unless W lies in a proper special subvariety. Same principle for a family $\{G_\lambda, \lambda \in S\}$ of special varieties.*

Following Masser-Zannier, let D_λ depend on a parameter λ varying on a *curve* $S/\overline{\mathbb{Q}}$ (but allow finite base change S'/S in next statements). Let

$$S_D = \{\lambda \in S(\overline{\mathbb{Q}}), D_\lambda \text{ is Pellian}\}.$$

S_D can be empty, finite, full... Say it is *sparse* if it has finitely many elements of given degree over $\mathbb{Q}$; e.g. any subset of $S(\overline{\mathbb{Q}})$ of bounded height. Same notation for Δ_λ, $\overline{\Delta}_\lambda$.

Some examples

$(d = 4.i)$: $D_\lambda(x) = x^4 + x + \lambda \Rightarrow S_D$ is infinite, but sparse;
$(d = 4.ii)$: $D'_\lambda(x) = x^4 + (2\lambda + 1)x^3 + 3\lambda x^2 + \lambda \Rightarrow S_{D'}$ idem.
$(d = 4.iii)$: $D''_\lambda(x) = x(x^3 + x + \lambda) \Rightarrow S_{D''}$ idem.

[Masser-Zannier (2013), and (2015) for $d \geq 6$]
$(d = 6.i)$: $\mathcal{D}_\lambda(x) = x^6 + x + \lambda \Rightarrow S_{\mathcal{D}}$ is finite;
$(d = 6.ii)$: $\mathcal{D}''_\lambda(x) = x^6 + x^2 + \lambda \Rightarrow S_{\mathcal{D}''}$ infinite but sparse !

[B.-Masser-Pillay-Zannier & Edixhoven (2016)]
$(d = 4 + 2.i)$: $\Delta_\lambda = (x + \frac{1}{2})^2 D_\lambda(x) \Rightarrow S_\Delta$ is finite
$(d = 4 + 2.ii)$: $\Delta'_\lambda(x) = (x + \frac{1}{2})^2 D'_\lambda(x) \Rightarrow S_{\Delta'} = S_{D'}$!!

[H. Schmidt (2017)]
$(d = 3 + 3)$: $\overline{\Delta}''_\lambda = x^3(x^3 + x + \lambda) = x^2 D''_\lambda(x) \Rightarrow S_{\overline{\Delta}''}$ is finite

(Un-)likely intersections I : relative Manin-Mumford

Theorem

[Masser-Zannier] *Let A/S be an abelian scheme of relative dimension $g \geq 2$, over the curve $S/\overline{\mathbb{Q}}$, and let $p \in A(S)$ be a section. Then the set*

$$S_p := \{\lambda \in S(\overline{\mathbb{Q}}), p(\lambda) \in A_\lambda^{tor}\}$$

is infinite if and only if one of the following conditions holds :
a) *p is a torsion section;*
b) *there exists an elliptic subscheme E/S of A/S such that a multiple of p factors through E, and is not a constant section if E/S is isoconstant.*

In (**b**), we are in " **relative dimension 1**" : if p is a section of E/S which is not constant (and not torsion), it meets E^{tor} densely (but *with bounded height* (Silverman)). Hence the ($d = 4$) and ($d = 6.ii$) cases.

Similarly, for a 2-rel.-dim'l $G \in Ext_S(E, \mathbb{G}_m) \simeq \hat{E}(S) \simeq E(S)$,

Theorem

[B-M-P-Z, B-E] *Let* $S/\overline{\mathbb{Q}}$, G/S, *parametrized by* $q \in E(S)$, *and let* $\tilde{p} \in G(S)$ *be a section, with projection* $p \in E(S)$. *Then, the set*

$$S_{\tilde{p}} := \{\lambda \in S(\overline{\mathbb{Q}}), \tilde{p}(\lambda) \in G_\lambda^{tor}\}$$

is infinite if and only if one of the following conditions is satisfied :

a) $\tilde{p}$ *is a torsion section;*

b) *there exists an elliptic subscheme* E'/S *of* G/S *(equivalently,* q *is a torsion section) and a multiple of* $\tilde{p}$ *which factors through* E', *and is not constant if* E'/S *(equivalently* E/S*) is isoconstant.*

b') *a multiple of* $\tilde{p}$ *factors though* $\mathbb{G}_{m/S}$ *(equivalently,* p *is torsion), and is not constant;*

c) $\tilde{p}$ *is a Ribet section (in particular,* $p(\lambda) \in E_\lambda^{tor} \Rightarrow \tilde{p}(\lambda) \in G_\lambda^{tor}$*).*

Back to the examples

$(d = 4.i)$: $D_\lambda(x) = x^4 + x + \lambda \Rightarrow S_D$ is infinite, but sparse;
$(d = 4.ii)$: $D'_\lambda(x) = x^4 + (2\lambda + 1)x^3 + 3\lambda x^2 + \lambda \Rightarrow S_{D'}$ idem.
$(d = 4.iii)$: $D''_\lambda(x) = x(x^3 + x + \lambda) \Rightarrow S_{D''}$ idem.

[Masser-Zannier (2013), and (2015) for $d \geq 6$] $G = A$
$(d = 6.i)$: $\mathcal{D}_\lambda(x) = x^6 + x + \lambda \Rightarrow S_{\mathcal{D}}$ is finite;
$(d = 6.ii)$: $\mathcal{D}''_\lambda(x) = x^6 + x^2 + \lambda \Rightarrow S_{\mathcal{D}''}$ infinite but sparse !

[B.-Masser-Pillay-Zannier & Edixhoven (2016)], $G \in Ext(E, \mathbb{G}_m)$
$(d = 4 + 2.i)$: $\Delta_\lambda = (x - \rho(\lambda))^2 D_\lambda(x) \Rightarrow S_\Delta$ is finite (for a.a. ρ)
$(d = 4 + 2.ii)$: $\Delta'_\lambda(x) = (x + \frac{1}{2})^2 D'_\lambda(x) \Rightarrow S_{\Delta'} = S_{D'}$!!

[H. Schmidt (2017)] $G \in Ext(E, \mathbb{G}_a)$
$(d = 3 + 3)$: $\overline{\Delta}''_\lambda = x^3(x^3 + x + \lambda) = x^2 D''_\lambda(x) \Rightarrow S_{\overline{\Delta}''}$ is finite

Indeed, for $G = Jac_{\mathfrak{q}}(C) \in Ext(E, \mathbb{G}_m)$:

$$\mathfrak{q}^{\pm} = (\rho(\lambda), \pm\sqrt{D_\lambda(\rho(\lambda))}) \rightsquigarrow q = ((\mathfrak{q}^+) - (\mathfrak{q}^-)) \in \hat{E}(S) \rightsquigarrow G = G_q$$

$$G(S) \ni \tilde{p} = [(\infty_+) - (\infty_-)] \to p = ((\infty_+) - (\infty_-)) \in E(S).$$

• in (4+2.i), E is not isoconstant, p is not torsion, most ρ's give a non-torsion $q \rightsquigarrow$ usual case of [BMPZ]. While if q is torsion, G is (iso)split, but $\tilde{p}$ projects to a non constant point of $\mathbb{G}_m$, barring its Case (**b**).

• in (4+2.ii), $E \simeq E' : y^2 = x^3 + \lambda(1-\lambda)x$, which has CM by $\mathbb{Z}[i]$, and the points $\infty^{\pm}, \mathfrak{q}^{\pm}$ are given on this model by $\mathfrak{p}'^{\pm}(\lambda) = (\lambda, \pm\lambda)$, $\mathfrak{q}'^{\pm}(\lambda) = (-\lambda, \pm i\lambda)$. So, $\mathfrak{q}'^{+} = [i]\mathfrak{p}'^{+}$, $\mathfrak{q}'^{-} = [i]\mathfrak{p}'^{-}$, and $q = [i]p$. Then, $\tilde{p}' = [(\mathfrak{p}'^{+}) - (\mathfrak{p}'^{-})] \in G'(S) \simeq G(S) \ni \tilde{p} := s_R$ is a Ribet section, and by Weil's law of reciprocity :

$$[n]p(\lambda) = 0 \Rightarrow [2n^2]\tilde{p}(\lambda) = 0.$$

• As for (d = 3 + 3) : $Jac_{2\overline{\mathfrak{q}}}(C) \in Ext(E, \mathbb{G}_a)$ is never split.

Generalized Pell equations

These have recently been studied by Barroero-Capuano, after previous work of Masser-Zannier. Here is a (slightly different) presentation of a special case.

Let D be separable as before, with $d \geq 4$, *fix* $\alpha \in k$ with $D(\alpha) \neq 0$, and consider the equation in unknowns $A, B \in k[X]$, $B \neq 0$ and $e \in \mathbb{Z}_{\geq 0}$:

$$A^2 - DB^2 = (X - \alpha)^e.$$

Let $\mathfrak{a}^{\pm} \in C(k)$ above α, and $s = ((\mathfrak{a}^+) - (\infty^-)) \in Jac(C)$. Recall that $p = ((\infty^+) - (\infty^-))$.

Proposition : *the equation has a solution if and only if the points s and p of $Jac(C)$ are linearly dependent over $\mathbb{Z}$.*

NB : p is torsion iff there is a solution with $e = 0$. Whereas $e > 0$ forces s to lie in the *divisible hull of* $\mathbb{Z}.p$ (including torsion): a Mordell-Lang pb.

Now, how often (still over a parameter curve $S/\overline{\mathbb{Q}}$) ?

Unlikely intersections II : relative Mordell-Lang

Theorem

[Ba-Ca](2018) *Let A/S be an abelian scheme of relative dimension $g \geq 2$, et let $P \in A(S)$ be a section. Let $A^{[2]}$ be the union of all the flat subgroup schemes of A/S of codimension ≥ 2. Then, the set*

$$S_P^{[2]} := \{\lambda \in S(\overline{\mathbb{Q}}), P(\lambda) \in (A^{[2]})_\lambda\}$$

is finite, unless P factors through a strict subgroup scheme of A/S.

In particular, let B/S be an abelian scheme, *whose generic fiber contains no elliptic curve*, and let $s, p \in B(S)$ be two sections. Assume that the set

$$S_{s,p}^{\ell d} = \{\lambda \in S(\overline{\mathbb{Q}}), s(\lambda) \text{ and } p(\lambda) \text{ are lin. dep. over } \mathbb{Z}\}$$

is infinite. Then, *s and p are linearly dependent over $\mathbb{Z}$.*

Example with $d = 8$: take $D_\lambda(X) = (X - \lambda)(X^7 - X^3 - 1)$, for which $End(Jac(C)) = \mathbb{Z}$, and $\alpha = -1/4$: no generic solution with $e = 1$.

Similarly, replace B by $G \in Ext_S(E_0, \mathbb{G}_m)$, where E_0 has CM, and $G = G_q$ for a non constant $q \in E_0(S)$. In particular, $q \notin E_0^{tor}$, so G contains no elliptic curve. The Ribet sections form a group of rank 1 of $G(S)$, and we fix a non-torsion one, say $s_R = \tilde{p}_R$.

Fix another section $s \in G(S)$. Since $S_{s_R} = \{\lambda \in S(\overline{\mathbb{Q}}), s_R(\lambda) \in G_\lambda^{tor}\}$ is infinite (cf. Example 4+2.ii), we should focus on its complement in $S_{s,s_R}^{\ell d}$:

Theorem

[B-Sch](2018) *Let $s \in G(S)$, and assume that the set*

$$S_{R,s} = \{\lambda \in S(\overline{\mathbb{Q}}), s(\lambda) \text{ lies in the divisible hull of } \mathbb{Z}.s_R(\lambda) \text{ in } G_\lambda.\}$$

is infinite. Then, $s = s' + s"$, where s' lies in the divisible hull of $\mathbb{Z}.s_R$ in G (i.e. is a Ribet section), and $s"$ factors through $\mathbb{G}_m$.

"Proofs" : - bounded height ;
- height of relations controled by degrees ;
- *o*-minimal count on an incidence variety (Habegger-Pila) ;
- functional algebraic (in-)dependence $\rightsquigarrow$ possible obstructions.

References

[Ba-Ca] F. Barroero, L. Capuano : *Unlikely intersections in families of abelian varieties ...* ; ArXv:1801.02885v1, 27 p.

[B-M-P-Z] D. B., D. Masser, A. Pillay, U. Zannier : *Relative Manin-Mumford for semi-abelian surfaces*; J. Edin. MS 59, 2016, 837-875.

[B-E] D. B., B. Edixhoven : *Pink's conjecture, Poincaré bi-extensions and generalized jacobians*; in preparation (and ArXiv 1104.5178v1).

[B-Sch] D. B., H. Schmidt : *Unlikely intersections in semi-abelian surfaces*; ArXiv 1803.04835v1, 17 p.

[M-Z] D. Masser, U. Zannier : *Torsion points ... and Pell's equation over polynomial rings ...*, J. Eur. MS, 17, 2015, 2375-2416.

[R] P. Ribenboim : *Solving parametrized systems of Pell equations*, Acta Arithm. 118, 2005, 1-9.

[Z] U. Zannier : *Unlikely intersections and Pell's equations in polynomials*; Springer Indam 8, 151, DOI 10.1007/978-3-319-05254-0_12 (Jan. 2014)

Et pour finir :

Joyeux anniversaire,

Paulo !