Pell equations for polynomials

Alexey Chilikov, Boris Frenkin, Ilya Ivanov-Pogodayev, Alexey Kanel-Belov,
Roman Krutovsky, Igor Melnikov

A. Introductory cycle. The classical Pell equation.

The introductory cycle A deals with some classical facts regarding the *Pell equation* $x^2-Dy^2=1$ for integers. The solution $(\pm1,0)$ is called *trivial*, and all the others *nontrivial*.

Problem A.1. *Let (x_1,y_1) be a solution of a Pell equation: $x_1^2-Dy_1^2=1$. Let $(x_1+\sqrt{D}y_1)^n=x_n+\sqrt{D}y_n$. Prove that (x_n,y_n) also is a solution of the Pell equation (observe that $x_{-n}=x_n, y_{-n}=-y_n$). The solution (x_n,y_n) is called a power of the solution (x_1,y_1). Define the notion of the product of solutions.*

Problem A.2. *Prove that all nontrivial solutions (if any) are powers of a single solution (x_1,y_1) (up to the sign of x).*

Problem A.3. *Prove that if D is a square of an integer then the Pell equation has no nontrivial solutions.*

Up to the end of the cycle we suppose $D\neq m^2\ \forall m\in\mathbb{Z}, D\in\mathbb{Z}$.

Problem A.4. *Prove that there exist $M>0$ and a point with integer nonzero coordinates (x,y) such that $|x^2-Dy^2|\leq M$.*

Problem A.5. *Using Minkowski lemma, prove that there exists $M>0$ such that there is an infinite number of such points.*

Problem A.6. *Prove that there exists a positive integer $k<M$ such that the equation $|x^2-Dy^2|=k$ has infinitely many solutions.*

Problem A.7. *Using the above items, prove that there exists a nontrivial solution of the Pell equation.*

Problem A.8. *Describe all rational solutions of a Pell equation in a general way.*

B. Pell equations for polynomials.

Problem B.1. *Describe all pairs of polynomials $(P(x),Q(x))$ over $\mathbb{R}$, such that*

$$P^2(x)-(x^2-1)Q^2(x)=1.$$

Problem B.2. *Solve the Pell equation for rational functions.*

Problem B.3. *Solve the equations a) $P^2+Q^2=R^2$, b) $P^2+Q^2=1$ for polynomials with complex coefficients.*

Problem B.4. *Prove that for $n>2$ and for polynomials P, Q there exist complex numbers ψ_1,ψ_2,ψ_3 such that $\psi_i^n=-1$ and P^n+Q^n is a multiple of $(P-\psi_1Q)(P-\psi_2Q)(P-\psi_3Q)$.*

Problem B.5. *Suppose $P^n+Q^n=R^n$. In the conditions of item B4, prove that there exist polynomials R_1, R_2, R_3 such that $P-\psi_iQ=R_i^n$.*

Problem B.6. *Prove that for $n>2$ the Fermat equation for polynomials and for rational functions $x^n+y^n=z^n$ has no nontrivial solutions.*

C. Applications of Kollar theorem

Here *a nontrivial solution* means a non-constant solution.

Problem C.1. *Solve the Pell equation if D is the square of a polynomial.*

Problem C.2. *Consider the following equation over polynomials from $\mathbb{Z}[x]$:*

$$P^2(x)-(R^2-1)Q^2(x)=1. \tag{1}$$

Here R is an arbitrary non-constant polynomial, not necessarily a variable.

Prove that the set of the solutions consists of the powers of a single nontrivial solution $(R,1)$.

Problem C.3. The theorem of J.Kollar*.** *The similar statement is valid for polynomials from* $\mathbb{C}[x]$.

Problem C.4. *Solve the equation (1) for a constant* R. *Consider cases* $R^2 = 1$ *and* $R^2 \neq 1$ *separately.*

Up to the end of cycle C we assume $R \neq$ const. Furthermore Kollar theorem may be used.

Problem C.5. *Prove that* Q *is of the form* $Q_n = \sum_{k=0}^{[n/2]} \binom{n}{2k+1} (T^2-1)^k T^{n-1-2k}$ *for some integer* n. *Find the similar formula for* P.

Problem C.6. *Prove that* $Q_n \equiv n$ *modulo* $R^2 - 1$, *that is,* $Q_n - n = (R^2-1)S$ *for some polynomial* S.

Problem C.7. *Solve the following system of equations for polynomials from* $\mathbb{C}[x]$*:*

$$\begin{cases} X^2 - (R^2-1)Y^2 = 1 \\ Y - (R^2-1)Z = V \\ V \cdot U = 1. \end{cases} \tag{2}$$

Problem C.8. Main problem. *Prove that for an arbitrary equation* W *for integers there exists a system of equations for polynomials from* $\mathbb{C}[x]$, *which has a solution iff* W *has a solution.*

D. Affine varieties

Problem D.1. *Define the following sets by equations or systems of equations:*

(1) an ellips;

(2) a pair of lines in the plane;

(3) a circle and an ellips;

(4) a circle and a parabola both containing the origin and touching in this point, Y-axis being the axis of the parabola;

(5) the equatorial circle on the unit sphere in the space;

(6) the n*-dimensional torus (the Cartesian product of* n *circles).*

Definition 1. Let S be a ring. An *affine variety* over R is a set X of the solutions of a finite system of algebraic equations in several variables, that is, the equations of the form $P(x_1, \ldots, x_n) = 0$ for some polynomial P.

Definition 2. *Let* X *be determined by some equations over* $R[x_1, \ldots, x_n]$. *The left parts of these equations generate an ideal in* $R[x_1, \ldots, x_n]$, *in the sequel denoted by* $I(X)$. The ring of functions $R[X]$ *on* X *will mean the ring* $R[x_1, \ldots, x_n]/I(X)$.

Problem D.2. *Ensure that in every point of* X *the value of every element from* $R[X]$ *can be uniquely determined.*

Problem D.3. *Show that the ring of functions on the* semicubic parabola *determined by the equation* $y^2 = x^3$ *over* $\mathbb{C}$ *is isomorphic to* $\mathbb{C}[t^2, t^3] \subset \mathbb{C}[t]$.

Problem D.4. *Let* X *and* Y *be affine varieties, and let* $\varphi\colon R[Y] \to R[X]$ *be an arbitrary map. Construct the corresponding map* $f\colon X \to Y$ *that induces* φ.

Remark 1. *We are interested only in those maps between varieties that stem from maps of the corresponding rings. Such maps will be called* algebraic. *Investigation of these maps enables us to get information about varieties from the algebraic structure of rings of functions.*

Problem D.5. *Consider the action of* $\mathbb{Z}/2\mathbb{Z}$ *on* $\mathbb{C}^2$ *such that the nontrivial element of the group takes* (x, y) *to* $(-x, -y)$. *This action induces an automorphism of the ring* $\mathbb{C}[x, y]$. *Show that the subring invariant under this action is isomorphic to* $\mathbb{C}[u, v, w]/(uv - w^2)$.

Construct an isomorphism (of topological spaces) between the affine variety determined by this ring, and the quotient space of $\mathbb{C}^2$ *modulo* $\mathbb{Z}/2$.

Let I be an ideal in $R[x_1, \dots, x_n]$. The variety corresponding to $R[x_1, ..., x_n]/I$ will be denoted by $V(I)$. The radical of I is the set $rad(I)$ consisting of all elements from $R[x_1, ..., x_n]$ such that some their power belongs to I.

Theorem 2 (Hilbert Nullstellensatz)**.** *Let k be an algebraically closed field. Then for every ideal $I \subset k[x_1, ..., x_n]$ we have*

$$I(V(I)) = rad(I).$$

Problem D.6. *Using the above theorem, show that there is a bijection between the points of an affine variety X over $\mathbb{C}$ and the maximal ideals of the ring $\mathbb{C}[X]$.*

Problem D.7. *Let X and Y be two affine varieties over $\mathbb{C}$. Given a map $\varphi\colon \mathbb{C}[Y] \to \mathbb{C}[X]$, construct a map from the set of maximal ideals of $\mathbb{C}[X]$ to the set of maximal ideals of $\mathbb{C}[Y]$ not using Nullstellensatz. Ensure that this map is identical to the map constructed in Problem 4.*

Definition 3. *A map $\iota\colon X \to Y$ between affine varieties will be called a* closed embedding *if $R[X] = R[Y]/I$ and the map of the rings of functions, corresponding to ι is the factorization map $R[Y] \to R[Y]/I$.*

Remark 4. *Clearly every affine variety over $\mathbb{C}$ is canonically embedded into some $\mathbb{C}^n$.*

Problem D.8. *Define a twofold cable as a closed embedding of a circle into a torus.*

Problem D.9. *Consider the natural embedding $(\mathbb{C} \setminus 0)^n \hookrightarrow \mathbb{C}^n$. Show that this is an algebraic map. Prove that it is not a closed embedding.*

Problem D.10. *Show that the standard embedding $\varphi\colon \mathbb{C}[t^2, t^3] \hookrightarrow \mathbb{C}[t]$ does not determine a closed embedding of a line into a semicubic parabola.*

E. Maps of affine varieties

Don't forget to apply with questions and for hints!

Definition 5. *A set R with two associative commutative binary operations $\cdot$ and $+$ (multiplication and addition) is called a (commutative associative) ring if the following conditions are fulfilled:*

(1) $\exists 0 \in R\colon 0 + a = a + 0 = a \ \ \forall a \in R$;
(2) $\forall a \in R \, \exists \, b \in R\colon a + b = b + a = 0$;
(3) $\exists 1 \in R\colon 1 \cdot a = a \cdot 1 = a \ \ \forall a \in R$;
(4) $a \cdot (b + c) = a \cdot b + a \cdot c$;
(5) $(a + b) \cdot c = a \cdot c + b \cdot c$.

Remark 6. *We will be interested mainly (except the rings of integers, rational, real and complex numbers)in rings of polynomials as well as* rings of functions on affine varieties.

Remark 7. *Polynomials $P_1(x_1, ..., x_n), \dots P_k(x_1, \dots, x_n)$ that determine an affine variety X, also generate the set of functions $I = P_1 \cdot R[x_1, \dots, x_n] + \dots + P_k \cdot R[x_1, \dots, x_n] \subset R[x_1, \dots, x_n]$. All these functions vanish at the points of the variety.*

Such a subset is an ideal in the ring of functions on X.

Definition 8. An ideal *of a ring R is a set I such that*

(1) $I \cdot R \subset I$;
(2) $I + I \subset I$.

An ideal is called principal *if it is generated by a single element.*

Problem E.1. *Let I be an ideal of the polynomial ring $\mathbb{C}[x_1, \dots, x_n]$. Let X_I be the variety corresponding to this ideal. Prove the following properties:*

(1) $I \subseteq J \Rightarrow X_J \subseteq X_I$;
(2) $X_I \cup X_J = X_{I \cdot J} = X_{I \cap J}$;
(3) if $I + J = R$ *then* $I \cdot J = I \cap J$;
(4) the ideals $I_1 = \langle x \rangle$ *and* $I_2 = \langle x^2 \rangle$ *of the ring* $\mathcal{R}[x]$ *determine the same set of zeroes.*

Problem E.2. *(1) Prove that in the ring $\mathcal{R}[x]$ of polynomials in a single variable, all ideals are principal. Such rings are called* rings of principal ideals *(RPI).*

(2) Give an example of a ring which is not a RPI.

Definition 9. *Given an ideal $I \subseteq R$. The* quotient ring *R/I is the set of equivalence classes of elements from R modulo I: $a \sim b \Leftrightarrow a - b \in I$. Multiplication and addition in the quotient ring are defined by the following formulas:*

(1) $(a + I) + (b + I) = (a + b) + I$;

(2) $(a + I) \cdot (b + I) = (a \cdot b + I)$.

Problem E.3. *Check correctness of the above definition. Prove that the quotient ring is a ring.*

Remark 10. *In Problem 2 from the cycle "Varieties and equations" we already did implicitly use a quotient ring. Namely we have shown that for a variety X_I over $\mathbb{C}$ determined by the ideal I (X_I is the set of common zeroes for all elements from I) the values of the polynomial functions over X_I are determined by the quotient ring $\mathbb{C}[x_1, \dots, x_n]/I$.*

Definition 11. *Let a variety X over R be determined by an ideal $I(X)$ (here we assume that a set of equations determines an ideal). Then the* ring of (polynomial) functions *$R[X]$ over X is the quotient ring $R[x_1, \dots, x_n]/I(X)$.*

Remark 12. *In Problem 5 of the preceding cycle it was shown that any ideal $I \subset \mathbb{C}[x_1, \dots, x_n]$ is generated by some finite set of elements $\Gamma = \{g_1, \dots, g_k\}$.*

Consider the ideal G generated by the leading monomials of all elements from I. In Problem 5 we have proved that the leading monomials of the elements from Γ also generate G. Such a set of generators for I is called a Groebner basis.

Definition 13. *A map $\iota\colon X \to Y$ between affine varieties is called a* closed embedding *if $R[X] = R[Y]/I$ and the map corresponding to ι is the map of factorization $R[Y] \to R[Y]/I$.*

Remark 14. *Clearly any affine variety over $\mathbb{C}$ has a canonical closed embedding to some $\mathbb{C}^n$.*

Problem E.4. *Here we construct a nontrivial algebraic embedding of a line $\mathcal{R}$ into $\mathcal{R}^3$. To begin with, consider the map*

$$\varphi\colon \mathcal{R} \to \mathcal{R}^2\colon t \mapsto (t^3 - 3t, t^4 - 4t^2).$$

Ensure that its image in $\mathcal{R}^2$ is the projection to the plane from a trefoil with a single point removed (to infinity).

Find a polynomial $h(t)$ such that the map

$$t \mapsto (\varphi(t), h(t))$$

transforms a line to a trefoil in $\mathcal{R}^3$ with a single point removed (also to infinity).

Remark 15. *Obviously not every system of polynomial equations has a solution. For instance, the system $\{x - y = 0, x - y + 1 = 0\}$ has no solution. Observe that the ideal generated by these two polynomials coincides with the whole ring $R[x, y]$ because $1 \in I$.*

So if an ideal I is generated by elements $g_1, \dots, g_k$ and for some $h_1, \dots, h_k \in R[x_1, \dots, x_n]$ we have

$$g_1 h_1 + \dots g_k h_k = 1$$

then I coincides with $R[x_1 \dots, x_n]$. In the next problem we prove that if $1 \notin I$ then there exists a solution common for all elements of I.

Problem E.5 (Weak Hilbert Nullstellensatz)**.** *Every proper ideal $I \subsetneq \mathbb{C}[x_1, \dots, x_n]$ determines a nonempty set of solutions.*

The proof consists of several steps. Consider the map which replaces the first coordinate by some number $a \in \mathbb{C}$:

$$ev_a\colon \mathbb{C}[x_1, \dots, x_n] \to \mathbb{C}[x_2, \dots, x_n]\colon f(x_1, \dots, x_n) \mapsto f(a, x_2, \dots, x_n).$$

(1) Suppose $I \cap \mathbb{C}[x_1] = \langle p(x_1) \rangle$, $\deg p > 0$. Then there exists $a \in \mathbb{C}$ such that $ev_a(I) \subsetneq \mathbb{C}[x_2, \dots, x_n]$.
(2) Suppose $I \cap \mathbb{C}[x_1] = \emptyset$. Prove that for some $a \in \mathbb{C}$ we have $ev_a(I) \subsetneq \mathbb{C}[x_2]$.
(3) Suppose $I \cap \mathbb{C}[x_1] = \emptyset$. Prove that for some $a \in \mathbb{C}$ we have $ev_a(I) \subsetneq \mathbb{C}[x_2, \dots, x_n]$
(4) Prove the theorem.

F. The complex case.

We require the following theorem that was the subject of the project https://www.turgor.ru/lktg/2007/2/index.php .

Matiyasevich theorem. *There is no algorithm to check existence of an integer root for a polynomial $H(x_1, \dots, x_m)$ in several variables, using the set of its coefficients.* [1]

We will consider the complex case which implies the case of an arbitrary field.

Cycle F1. Decomposition of polynomials, and substitutions.

Problem F.1. *Prove that $P(x + P(x))$ is a multiple of $P(x)$.*

Problem F.2. *Given a square trinomial $P(x) \neq const$ with integer coefficients. Prove that there exists an integer n such that all prime divisors of $P(n)$ are less than $n/2019$.*

Remark. *The similar fact is unknown even for cubic polynomials. We can prove it for binomials $ax^n + b$.*

Problem F.3.
Let $P(x_1, \dots, x_n)$, $Q(x_1, \dots, x_n)$ be arbitrary polynomials in n variables. Suppose

$$\widehat{P}(x_1, \dots, x_n, u) = P(x_1 + uQ(x_1, \dots, x_n), \dots, x_n + uQ(x_1, \dots, x_n))$$

Then there exists $R(x_1, \dots, x_n, u)$ such that

$$\widehat{P}(x_1, \dots, x_n, u) = P(x_1, \dots, x_n) + Q(x_1, \dots, x_n)R(x_1, \dots, x_n, u).$$

Problem F.4. *There exists a polynomial $H(x_1, \dots, x_n)$ such that for all integer k with $1 \leq k \leq 2019$ all polynomials $H(x_1, \dots, x_n) - k$ have a nontrivial factor decomposition.*

Problem F.5. *In the above problem we can choose $H(x_1, \dots, x_n)$ in the form $P_k Q_k + k$ where Q_i are algebraically independent (there is no nonzero polynomial R such that $R(Q_1, \dots, Q_{2019}) \equiv 0$).*

Problem F.6.
There exist families of polynomials $H_m(x_1, \dots, x_m)$, $P_m(x_1, \dots, x_m)$ which both fulfil the conditions of divisibility

$$H_k(x_1, \dots, x_k) \mid (P_m(x_1, \dots, x_m) - k)$$

for all $k \in \{1, \dots, m\}$, and furthermore H_m and P_m essentially depend on x_m but H_s for $s < m$ don't depend on x_m.

Cycle F2. Construction of systems.

Problem F.7. *Let us determine the variety $\mathcal{B}_{(d,e)}$ by the system of generators and relations:*

$$\left\{ \begin{array}{c} X_{ij}^2 - (T_j^2 - 1)Y_{ij}^2 = 1 \\ Y_{ij} - (T_j - 1)Z_{ij} = V_{ij} \\ V_{ij}U_{ij} = 1 \\ T_{j+1} = \prod\limits_{k=1}^{j} \left((T_k^2 - 1)W_k\right) W_{j+1}^{m_{j+1}} \\ T_1 = \hat{P}(W_1, \dots, W_n) \end{array} \right. \tag{3}$$

where $1 \leq i \leq d$, $1 \leq j \leq e$, $\{m_j\}_{j=1}^e$ is a sequence of integers with rather fast growth. The polynomial $\hat{P}$ is to be chosen so that W_i is a divisor of $\hat{P}(W_1, \dots, W_n) - 3i$. (This polynomial can be constructed explicitly, see item 6 of the preceding cycle.)

[1] In fact it suffices to take $m = 11$.

The sequence $\{m_j\}_{j=1}^{e}$ is to be chosen so that if all variables in T_1 are different then the polynomials T_j are algebraically independent.

Problem F.8. *Suppose we have $T_N = C_N \neq 0$ for some N (so T_N is a nonzero constant). Then all W_k for $k \leq N$ and all T_k for $k \leq N-1$ are constant.*

Problem F.9. *The problem of embeddability of an arbitrary algebraic variety $\mathcal{A}$ over $\mathbb{C}$ into an arbitrary algebraic variety $\mathcal{B}$ is algorithmically unsolvable.*