Pell equations for polynomials. Solutions and hints

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

A. Introductory cycle. The classical Pell equation

Problem A.1. The first assertion is verified by a direct calculation. In the following problems, observe that a power of a solution always can be presented in this form.

Similarly to the first assertion, observe that a pair of solutions of the required form can form a new solution due to the fact that $(x + y\sqrt{D})(x' + y'\sqrt{D})$ is again of the form $X + Y\sqrt{D}$.

Problem A.2. Consider the set of nonnegative solutions and arrange them by increasing x. It is easily verified that all solutions are comparable. Moreover if $x < x'$ then $y < y'$ in the respective solution (a direct calculation). The product operation introduced above is monotonous on this set in each variable (in the sense of the ordering just introduced), this is verified by a direct calculation as well. Each nontrivial solution is strictly greater than each trivial one. Hence the powers of a nontrivial solution form an infinite increasing sequence. Now it remains to introduce an analogue of division with remainder and to show the existence, for any two solutions, of a «common remainder» such that both are its powers. Now consider the minimal nontrivial nonnegative solution and show that it is a «common divisor» for all nontrivial nonnegative solutions. It remains to clear up the sign, which is not difficult.

Problem A.3. For $D = m^2$ we have $1 = x^2 - m^2y^2 = (x - my)(x + my)$. Thus clearly $\pm 1 = x + my = x - my$, and hence $y = 0$, $x = \pm 1$ for $m \neq 0$. The case $m = 0 = D$ is to be considered separately, with no difficulty.

Problem A.4. Due to a disappointing formulation, the problem occurred to be trivial.

Problem A.5. Suppose the contrary. Let t_k be the hyperbole with the equation $x^2 - Dy^2 = k$. Then each t_k contains only a finite number of integer points. Hence for each M the domain between t_M and t_{-M} also contains only a finite number of integer points. Denote this domain by T_M.

The asymptotes of the hyperboles divide the plane into 4 domains. Each of the domains contains a half-hyperbole. Every integer point (a, b) lies in one of the domains. From this point, draw two rays parallel to the borderlines of the domain (to the asymptotes of hyperboles). Denote by $L_{a,b}$ the domain bounded by the rays.

The rays meet the corresponding half-hyperbole at two points. The part of the half-hyperbole between these points (that is, inside $L_{a,b}$) will be called «forbidden».

Now take an arbitrary point $(\hat{x}, \hat{y})$ of the hyperbole $x^2 - Dy^2 = k$. Draw two lines through this point, parallel to the asymptotes of the hyperboles, and two lines symmetrric to these about the origin. These two pairs of parallel lines bound a parallelogram $P_{\hat{x},\hat{y}}$ with vertices on the hyperboles. Hence its interior lies inside T_M. A direct calculation shows that the area of $P_{\hat{x},\hat{y}}$ is independent of the choice of $(\hat{x}, \hat{y})$ at the hyperbole, and equals $2M/\sqrt{D}$.

It is easily seen that a point (a, b) lies inside $P_{\hat{x},\hat{y}}$ iff $(\hat{x}, \hat{y})$ lies inside $L_{a,b}$ (that is, in the forbidden domain).

Since the number of integer points inside T_M is finite, the union of the corresponding forbidden domains is a restricted domain. Hence there exists a point $(\hat{x}, \hat{y})$ of t_M, which does not belong to any forbidden domain. Thus the parallelogram $P_{\hat{x},\hat{y}}$ contains no integer points. But this contradicts Minkowski lemma because for arbitrarily large M the area of the parallelogram increases without bound.

The above argument enables us to obtain a specific estimate for M. It suffices to require $2M/\sqrt{D} > 4$, that is, $M > 2\sqrt{D}$.

Problem A.6. The preceding problem implies existence of M such that there exist infinitely many solutions for $m \leq M$. Now it suffices to take the minimum of such M for k.

Problem A.7. Let us return to the «generalized» Pell equation $x^2 - Dy^2 = k$ where k is the parameter to be chosen. Solutions of such equations for different k and l can be «multiplied» according to the same formulas as for usual equations, and this results in a new solution for kl. This enables us to define the notion of «division» of solutions (observe that its result is not always an integer point but always a rational point).

Multiplying a solution for 1 by a solution for k, we obtain a new solution for k. Thus we may try to construct a nontrivial solution for 1 from two different solutions for an arbitrary k. We already have proved the existence of k for which the number of different solutions is infinite. It remains to determine when the result of division is a pair of integers. This is performed by a straightforward calculation.

Problem A.8. Let (x, y) be a nontrivial rational solution. Draw a line through (x, y) and $(1, 0)$. Its slope $\lambda = (x-1)/y$ is rational. Conversely, suppose a line through $(1, 0)$ has a rational slope. Then it meets the hyperbole $x^2 - Dy^2 = 1$ at two points, one of which is $(1, 0)$. Hence the second point also has rational coordinates (uniquely determined).

Thus there is a bijection between the lines of the above form and the nontrivial rational solutions of the Pell equation. It remains to write down this bijection explicitly.

B. Pell equations for polynomials

Problem B.1. Clearly for any nontrivial solution (P, Q) we have $\deg P = \deg Q + 1$. The pair $(x, 1)$ is a solution. Thus each solution (P, Q) produces new solutions $(Px + Q(x^2-1), P + Qx)$ and $(Px - Q(x^2-1), P - Qx)$ (by multiplication of (P, Q) by $(x, 1)$ and $(x, -1)$). Observe that these new solutions are powers of $(x, 1)$ iff (P, Q) is its power.

Let us arrange the solutions according to $\deg Q$ and show that for any (P, Q) some solution of the form $(Px + Q(x^2-1), P + Qx)$, $(Px - Q(x^2-1), P - Qx)$ is smaller than the original one.

Write down the original equation in the form

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

The degree of the right part is just $2\deg Q$. Decompose the left part into factors:

$$(P - xQ)(P + xQ) = 1 - Q^2.$$

Thus $\deg(P - xQ) + \deg(P + xQ) = 2\deg Q$. Hence at least in one of the factors, the leading monomials of the summands cancel. But $\deg P = \deg((P - xQ) + (P + xQ)) \leq \max(\deg(P - xQ), \deg(P + xQ))$, so this cancellation cannot occur in both factors. Thus one of the degrees is just $\deg P$, and the second degree equals $2\deg Q - \deg P = \deg Q - 1 < \deg Q$. This pair is just the required solution which is smaller than the original one.

Now let (P, Q) be the smallest of the solutions that are not powers of $(x, 1)$. If $\deg Q > 0$ then the above procedure results in a smaller solution which also is not a power of $(x, 1)$. This contradicts the minimality of (P, Q). For $\deg Q = 0$ a direct calculation gives the only possible cases $P = \pm x, Q = \pm 1$.

Problem B.2. Similarly to A.8.

Problem B.3. In part b, consider the equation $(P - iQ)(P + iQ) = 1$. Both factors are polynomials but this equation has only constant solutions of the form $(\lambda, 1/\lambda)$. Furthermore a direct calculation gives $P = \frac{\lambda^2+1}{2\lambda}$, $Q = \frac{\lambda^2-1}{2i\lambda}$, thus all solutions are trivial. Part a is equivalent to part b for rational functions. In this case λ is not necessarily a constant but an arbitrary rational function. The form of the solutions remains the same.

Problem B.4. Use the «school» formula

$$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + \ldots + xy^{n-2} + y^{n-1})$$

for $x = P$, $y = \psi Q$ where $\psi^n = -1$. Now observe that the number of such ψ's is n, so we can choose 3 different ones.

Problem B.5. The preceding problem implies that $P - \psi_i Q$ are divisors of $P^n + Q^n$, and hence of R^n. Since all $P - \psi_i Q$ are coprime, any linear factor can be present in one of them at most. However its degree in R^n is a multiple of n. Hence each of $P - \psi_i Q$ is the product of nth degrees of its linear factors, and so has the form R_i^n for some R_i.

In the condition of problem, it is worth while to exclude the trivial solutions (those for which P and Q differ by a constant complex factor).

Problem B.6. Let P, Q, R be a nontrivial solution of minimal degree. Then the preceding problem implies $R_i^n = P - \psi_i Q$. Choose $\lambda_i \neq 0$ such that $\lambda_1 R_1^n + \lambda_2 R_2^n = \lambda_3 R_3^n$. For this, it suffices to solve the system

$$\begin{cases} \lambda_1 & + & \lambda_2 & = & \lambda_3 \\ \lambda_1\psi_1 & + & \lambda_2\psi_2 & = & \lambda_3\psi_3, \end{cases}$$

obviously consistent. It remains to observe that the triple

$$(\lambda_1^{1/n} R_1, \lambda_2^{1/n} R_2, \lambda_3^{1/n} R_3)$$

produces a new solution of lesser degree than that of (P, Q, R).

The case of rational functions reduces to that of polynomials.

C. Applications of Kollar theorem

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

Problem C.1. Similarly to A.3.

Problem C.2. The solution is close to that of B.1. The pair $(R, 1)$ is a solution, and for every nontrivial solution (P, Q) we have $\deg P = \deg Q + \deg P$.

Multiplying by $(R, \pm 1)$, we obtain solutions $(PR + Q(R^2 - 1), P + QR)$ and $(PR - Q(R^2 - 1), P - QR)$, and they are powers of $(R, 1)$ iff (P, Q) is.

Arrange the solutions according to $\deg Q$. We will show that for every solution (P, Q) one of the solutions $(PR + Q(R^2 - 1), P + QR)$, $(PR - Q(R^2 - 1), P - QR)$ is smaller than the original one.

Rewrite the original equation as

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

The degree of the right part is just $2 \deg Q$. Decompose the left part:

$$(P - RQ)(P + RQ) = 1 - Q^2.$$

Hence $\deg(P - RQ) + \deg(P + RQ) = 2 \deg Q$. Thus the leading monomials of the summands cancel in some factor. But $\deg P = \deg((P - RQ) + (P + RQ)) \leq \max(\deg(P - RQ), \deg(P + RQ))$, so the cancellation cannot occur in both parts simultaneously. Hence one of the degrees is just $\deg P$, and the second one equals $2 \deg Q - \deg P = \deg Q - \deg R < \deg Q$. This pair is a solution smaller than the original one.

Now let (P, Q) be the smallest of the solutions that are not powers of $(R, 1)$. If $\deg Q > 0$ then the above procedure gives a smaller solution which also is not a power of $(R, 1)$. This contradicts minimality of (P, Q). For $\deg Q = 0$ a direct calculation shows that the only possible cases are $P = \pm R, Q = \pm 1$.

Problem C.3. Similarly to C.2. Indeed, solving C.2 we haven't used the structure of the basic ring.

Problem C.4. Similarly to A.3.

Up to the end of cycle C, we suppose $R \neq \text{const}$. Furthermore Kollar theorem may be used.

Problem C.5. Straightforward.

Problem C.6. Straightforward.

Problem C.7. The problem requires «comprehension». The last equation guarantees that U and V are constants (polynomials of degree 0). The possible solutions of the first equation are described in the above problems as series of the form (P_n, Q_n). Furthermore

$$Q_n = n \bmod (R-1).$$

The second equation implies $V = n$. The remaining variables are calculated directly.

Problem C.8. The main problem. The idea is to copy the system from the preceding problem n times, and use the fact that nontrivial series arise only for integer constant V_i. Add the equation $W(V_1, \ldots, V_n) = 0$, and the required equivalence is almost proved.

It remains to exclude the case of constant R. For $R \neq 1$ all solutions of the system are trivial (constant). The special case $R = 1$ can be excluded for reals, for instance by adding the equation $R = S^2 + 2$.

D. Affine varieties.

Problem D.1. All parts of the problem are solved by a straightforward calculation. Hint: first of all find out how systems of equations for sets produce equations for their intersections and unions.

Problem D.2. Let f and g are two distinct functions from the same equivalence class. Then $f-g = R_1P_1+\ldots+R_kP_k$. In particular, $f(x)-g(x) = R_1(x)P_1(x)+\ldots+R_k(x)P_k(x)$. Since all $P_i(x) = 0$for $x \in X$, we have $f(x) - g(x) = 0$.

Problem D.3. Set $t = \frac{y}{x}$. The rest is provided by a straightforwrd calculation.

Problem D.4. The formulas for inclusion of the 2-dimensional torus have been obtained in part 6 of Problem D.1. It remains to adjust the parametric representations of 1-fold and 2-fold cables so that the second one would be traced with double speed. For instance, it is possible to use the trigonometric parametrization of the circle and the formulas for the double angle (which are polynomial).

Problem D.5.
(1) Suppose Pete can proceed infinitely. Then there exists an infinite set of projectors such that they don't light up each other. Surely this is impossible for $n = 1$. Let us proceed by induction in n. Consider an arbitrary projector $(\hat{x}_1, \ldots, \hat{x}_n)$. Each other projector has at least one coordinate such that $x_m < \hat{x}_m$. Hence for at least one m there exists an infinite number of projectors such that $x_m < \hat{x}_m$. Among them, choose an infinite subset of projectors with the same value of x_m. Excluding this coordinate we reduce the problem to the dimension $n-1$.

(2) The vectors of powers of the leading summands may be considered as coordinates of projectors from the preceding part of the problem.

(3) Hint: divide one polynomial by another one with remainder. The remainder will decrease if at each step the leading summand of the dividend is greater or equal to the leading summand of the divisor.

E. Maps of affine varieties

Problem E.1. All parts are verified by a straightforward calculation.

Problem E.2. 1) In an ideal, choose a polynomial of the minimal degree. Using Euclid's algorithm show that all the other elements of the ideal are its multiples.

2) For instance, $\mathbb{C}[x, y]$.

Problem E.3. Verified by a straightforward calculation.

Problem E.4. The natural way to induce φ by a given $f : X \to Y$ is as follows. Put $\varphi(g) = h$, where $h(x) = g(f(x))$ for each $x \in X$. It is easy to verify that $\varphi : R[Y] \to R[X]$ is a homomorphism of rings. Now let us construct f starting from a given φ. We must obtain $g \circ f = \varphi(g)$ for any g. Let $\pi_i \in R[Y]$ be a function which attaches the ith coordinate to a point y. Then $h_i = \pi \circ f = \varphi(\pi)$, and the map $h : x \to (h_1(x), \ldots, h_n(x))$ satisfies the necessary conditions. It remains to check that h maps the points of X to points of Y. This is done by a straightforward calculation (taking in account that φ is a homomorphism).

Problem E.5. We have $\varphi^*(g) = g \circ \varphi$, hence $\varphi^*(g) = g$ iff $g(x, y) = g(-x, -y)$ for any $(x, y) \in \mathbb{C}^2$. A straightforward calculation shows that this is true just for the polynomials that are sums of monomials with even degrees in total. Such monomials of minimal degree are x^2, xy and y^2. The others are polynomials in these. In other words, the invariant ring in question is generated (as a ring) by these monomials and 1. It remains to construct the required isomorphism explicitly. Put $u \to x^2$, $v \to y^2$, $w \to xy$ and extend this map to a ring homomorphism. A straightforward calculation shows that it is an isomorphism. Having an explicit isomorphism we reduce the second part of the problem to E.4.

Problem E.6. For solution we construct the corresponding function rings and embeddings explicitly. Then we have to show that the embedding of the ring of functions over $\mathbb{C}^n$ into the ring of functions over $(\mathbb{C} \setminus 0)^n$ is not a factorization. For this we can use the fact that only constants are invertible over $\mathbb{C}^n$ but the invertible functions over $(\mathbb{C} \setminus 0)^n$ are much more numerous (for instance they include all polynomials $f(x) = x^n$ $\mathbb{C} \setminus 0$).

Problem E.7. The idea of solution is similar to that in the preceding problem. We have to show that $\mathbb{C}[t^2, t^3]$ is not isomorphic to any quotient ring of $\mathbb{C}[t]$. Clearly $\mathbb{C}[t^2, t^3]$ is not isomorphic to $\mathbb{C}[t]$. So we have to consider factorization by a proper ideal. Since all ideals are here pricipal, we consider factorization by some ideal $\langle f \rangle$, where $f \in \mathbb{C}[t]$ is a nonconstant polynomial. Further we have to describe such quotient rings and to show that no of these are isomorphic to $\mathbb{C}[t^2, t^3]$. The idea is to consider the roots of f.

Problem E.8. The first assertion of the problem becomes evident after construction of the graph. For the second assertion we have to explicitly compute the self-intersection points of the plane graph, and to choose a polynomial h so that these points form the due configuration in the space (that is, the values of $h(t)$ for corresponding t appear in the due order). This is provided by a straightforward calculation.

Problem E.9 (Weak Hilbert's Nullstellensatz)**.** (1) For a, take a root of p. Since $p(a) = 0$, we have $p(x_1) = (x_1 - a)q(x_1)$ for some $q \in \mathbb{C}[x_1]$, $\deg q = \deg p - 1$.

Suppose the assertion (1) fails. Then $ev_a(I) = \mathbb{C}[x_2, \ldots, x_n]$, hence $1 \in ev_a(I)$. For any $f \in \mathbb{C}[x_1, \ldots, x_n]$ we have $f = (x_1 - a)g + ev_a(f)$, where $g \in \mathbb{C}[x_1, \ldots, x_n]$ (we divide by $x_1 - a$ with remainder). Hence there exists $\hat{f} \in I$ such that $\hat{f} = (x_1 - a)\hat{g} + 1$. Multiplying the equation by $q(x_1)$, we have $q\hat{f} = (x_1 - a)q\hat{g} + q$, or $q = q\hat{f} - p\hat{g}$. In the right-hand side, both summands lie in I because $\hat{f} \in I$ and $p \in I$. Thus $q \in I \cap \mathbb{C}[x_1] = \langle p(x_1) \rangle$. But this is impossible since $q = p/(x_1 - a)$. This contradiction proves assertion (1).

(2) Clearly the map ev_a is a ring homomorphism. It produces analogues over vectors and matrices with polynomial coefficients. These maps also are homomorphisms. Also the following fact is easy proved: for any tuple of pairwise distinct numbers $a_0, \ldots, a_d$ and any integer i, $0 \le i \le d$, there exists a unique polynomial $\chi_i(t)$ of degree d, such that $\chi_i(a_i) = 1$ and $\chi_i(a_j) = 0$ for any $j \ne i$.

This fact implies that for any commutative ring R including $\mathbb{C}$ as a subring, any tuple of pairwise distinct numbers $a_0, \ldots, a_d$, and any tuple of elements $r_0, \ldots, r_d$ there exists a unique polynomial $r \in R[t]$ of degree d at most, such that $r(a_i) = r_i$ for all i. In fact it suffices to take $r(t) = \sum_{i=0}^{d} r_i \chi_i(t)$.

In the last part of Problem D.5 we see that any ideal has a finite basis. Denote the elements of such finite basis for I by $g_1, \ldots, g_m$. Clearly $ev_a(g_1), \ldots, ev_a(g_m)$ form a basis in $ev_a(I)$. Denote by d the maximum for degrees of g_i in the variable x_1.

Each of g_i can be represented in the form $g_i = \sum_{i=0}^{d} x_1^j g_{ij}$, where $g_{ij} \in \mathbb{C}[x_2]$. Denote by G the matrix $m \times (d+1)$ that consists of elements of the form $g_{ij} \in \mathbb{C}[x_2]$, where $1 \le i \le m$, $0 \le j \le d$. Since all elements of G are polynomials from $\mathbb{C}[x_2]$, we have $ev_a(G) = G$.

If v is row vector then denote by v^T the corresponding column vector.

Denote by $V(z)$ the row vector $(1, z, \ldots, z^d)$ of length $d+1$. Here z may be any polynomial but we will use it only for $z = x_1$ or $z \in \mathbb{C}$. It is easy to prove that $ev_a(V(x_1)) = V(a)$, $ev_a(V^T(x_1)) = V^T(a)$.

A straightforward calculation shows that $GV^T(x_1) = (g_1, \ldots, g_m)^T$ is a column vector consisting of basis polynomials for I. Using the ev_a operation, we can explicitly represent the bases for $ev_a(I)$ in the matrix-vector form. Namely,

$$ev_a(GV^T(x_1)) = G \cdot ev_a(V^T(x_1)) = GV(a)$$

is a matrix such that its rows form a basis in $ev_a(I)$.

Now suppose that the assertion (2) fails. Then consider an arbitrary tuple of pairwise distinct numbers $a_0, \ldots, a_d$. For each of them we have $ev_{a_i}(I) = \mathbb{C}[x_2]$. This means that $1 \in ev_{a_i}(I)$, so there exist $h_{ij} \in \mathbb{C}[x_2]$ such that $1 = \sum_{j=1}^{m} h_{ij} \cdot ev_{a_i}(g_j)$. For each j, $1 \le j \le m$ denote by H_j the polynomial from $\mathbb{C}[x_1, x_2]$ of degree d at most (in x_1), such that $ev_{a_i}(H_j) = h_{ij}$. As mentioned above, it does exist and is unique.

Now consider the row vector $H = (H_1, \ldots, H_m)$ and the matrix product $HGV^T(x_1)$. On one hand, it is a polynomial from $\mathbb{C}[x_1, x_2]$. It is easy to check that it is a linear combination of rows from $GV^T(x_1)$ with polynomial coefficients (H_j). Since the rows of $GV^T(x_1)$ are elements of a basis in I, we have $HGV^T(x_1) \in I$. On the other hand, if we fix i and consider $ev_{a_i}(HGV^T(x_1))$ then we get

$$ev_{a_i}(HGV^T(x_1)) = \sum_{j=1}^{m} h_{ij} \cdot ev_{a_i}(g_j) = 1.$$

Thus $HGV^T(x_1)$ equals 1 in $d+1$ distinct points (as a polynomial in x_1). But its degree in x_1 is $\le d$. This implies $HGV^T(x_1) = 1$. Thus $1 \in I$. This contradicts the initial requirement $I \subsetneq \mathbb{C}[x_1, \ldots, x_n]$. The contradiction proves assertion (2).

(3) Similarly to part (2). Observe that we never used that the number of variables is just 2. So it suffices to replace $\mathbb{C}[x_2]$ by $\mathbb{C}[x_2, \ldots, x_n]$ (and respectively $\mathbb{C}[x_1, x_2]$ by $\mathbb{C}[x_1, x_2, \ldots, x_n]$).

(4) Part (4) is proved on the base of the preceding parts by induction in n. For $n = 1$ the assertion is equivalent to part (1). For $n > 1$ we have two options: either $I \cap \mathbb{C}[x_1] = \emptyset$ and the problem reduces to part (3) and to the similar assertion for $n-1$ variables (that is, the induction hypothesis), or $I \cap \mathbb{C}[x_1] = \emptyset$ and the problem reduces to part (1) and again the induction hypothesis.

Observe that in fact we have proved an assertion stronger than the original one, namely: if I contains equation in a single variable x_i then some equation $P_i(x_i) = 0$ has minimal degree; furthermore in all equations of the system the coordinate x_i must be equal to a root of P_i but on the other hand, any root of P_i is contained in a solution of the original system; otherwise all values of x_i are contained in these solutions except a finite number of values, not exceeding the maximal degree of equations in x_i.

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's theorem. *There is no algorithm to determine whether an integer solution exists for a polynomial equation $H(x_1, \ldots, x_m) = 0$.* [1]

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

Cycle F1. Permutations and decomposition of polynomials.

Problem F.1. A straightforward calculation.

Problem F.2. To be published later.

Remark. The jury has no proof for the similar fact even for a cubic polynomial. A proof is known for the binomials $ax^n + b$.

Problem F.3. A straightforward calculation.

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

Let us construct families of polynomials $H_m(x_1, \ldots, x_m)$, $P_m(x_1, \ldots, x_m)$ such that we have $H_k(x_1, \ldots, x_k) \mid (P_m(x_1, \ldots, x_m) - k)$ for all $k \in \{1, \ldots, m\}$.

For $m = 1$ take $H_1(x_1) = x_1$, $P_1(x_1) = x_1 + 1$.

Suppose the required families have been constructed for some m. Put $P'_{mk} = P_m - k$ and

$$Q_m(x_1, \ldots, x_m) = \prod_{k=1}^{m} P'_{mk}(x_1, \ldots, x_m) = \prod_{k=1}^{m} (P_m(x_1, \ldots, x_m) - k)$$

Consider the polynomial

$$P''_m(x_1, \ldots, x_m, u) = P(x_1 + uQ_m(x_1, \ldots, x_m), \ldots, x_m + uQ_m(x_1, \ldots, x_m)).$$

The solution of Problem F.1 implies that $P''_m(x_1, \ldots, x_m, u)$ has a representation of the form

$$P_m(x_1, \ldots, x_m) + Q_m(x_1, \ldots, x_m)R_m(x_1, \ldots, x_m, u)$$

Denote $P'''_{mk} := P''_m - k$ to obtain a similar representation

$$P'''_{mk}(x_1, \ldots, x_m, u) = P'_{mk}(x_1, \ldots, x_m) + Q_m(x_1, \ldots, x_m)R_m(x_1, \ldots, x_m, u)$$

By induction we have the following divisibility conditions for P_m: $H_k \mid P'_{mk}$. Since Q_m also is a multiple of P'_{mk}, we have

$$P'''_{mk}(x_1, \ldots, x_m, u) = P'_{mk}(x_1, \ldots, x_m)R'_{mk}(x_1, \ldots, x_m, u) \tag{1}$$

where

$$R'_{mk}(x_1, \ldots, x_m, u) = 1 + R_m(x_1, \ldots, x_m, u) \cdot \frac{Q_m(x_1, \ldots, x_m)}{P'_{mk}(x_1, \ldots, x_m)} \tag{2}$$

This means that the polynomial $P''_m(x_1, \ldots, x_m, u)$ is a multiple of P'_{mk} and hence of H_k (for all $k \in \{1, \ldots, m\}$).

Thus the constructed polynomial P''_m (in $m + 1$ variables) looks suitable for the role of the new P_{m+1}. It remains to choose an appropriate H_{m+1} and provide the divisibility condition for $k = m + 1$.

The condition in question is $H_{m+1} \mid P'''_{m,m+1}$. By (1) and (2) we obtain

$$P'''_{m,m+1}(x_1, \ldots, x_m, u) = P'_{m,m+1}(x_1, \ldots, x_m)R'_{m,m+1}(x_1, \ldots, x_m, u)$$

where

$$R'_{m,m+1}(x_1, \ldots, x_m, u) = 1 + R_m(x_1, \ldots, x_m, u) \cdot \frac{Q_m(x_1, \ldots, x_m)}{P'_{m,m+1}(x_1, \ldots, x_m)}$$

To provide the divisibility conditions it suffices to assume

$$H_{m+1}(x_1, \ldots, x_m, x_{m+1}) = R'_{m,m+1}(x_1, \ldots, x_m, x_{m+1})$$

and

$$P_{m+1}(x_1, \ldots, x_m, x_{m+1}) = P''_m(x_1, \ldots, x_m, x_{m+1})$$

The extended families of polynomials satisfy the divisibility conditions for all $k \in \{1, \ldots, m+1\}$, which implies the solution of the problem.

Problem F.5. Construction of polynomials in the preceding problem implies that H_{m+1} and P_{m+1} significantly depend on x_{m+1}.

Problem F.6. An example is given by the construction from the preceding problems.

Cycle F2. Construction of systems.

Problem F.7. The possibility for construction of the required polynomial $\hat{P}$ follows from the solutions of the preceding cycle of problems. Clearly the system of equations in question determines a variety.

Problem F.8. A straightforward calculation.

Problem F.9. Construct a variety using the pattern from Problem F.7. Its nontrivial solutions are coded by integer-valued parameters (one parameter for each subsystem). The ideas similar to those from the solution of Problem C.8 lead to the possibility for construction of a variety which is nontrivial only if some polynomial eqaution in several variables has an integer solution. The solution of Problem F.8 enables us to control the case of «surplus» components generated by «partially constant» solutions (when constants are present only in certain subsystems). This is done by control of dimension. Thus the problem on existing of an inclusion reduces to the question of solvability of Diophantine equations. The latter is undecidable by Matiyasevich's theorem.