EXERCISES IN DIOPHANTINE GEOMETRY

SPARSITY OF ALGEBRAIC POINTS, MSRI JUNE 2021

This is a selection of exercises in Diophantine geometry prepared for the MSRI Summer school on Sparsity of algebraic points jointly with Yunqing Tang. These have been edited to be independent of the lectures.

Manin–Mumford conjecture for curves

This series of exercises deduces the Manin-Mumford conjecture from a deep theorem of Serre concerning Galois action on the Tate module of an abelian variety, following Baker-Ribet. Throughout X will denote a curve of genus $g \geqslant 2$ defined over a field K of characteristic zero, and $i : X \to \operatorname{Jac} X$ will denote the Abel–Jacobi embedding of X relative to a rational degree 0 divisor D. (For our purpose, it is OK to consider an Abel–Jacobi map over $\overline{K}$ and pick D to be the divisor given by a $\overline{K}$-point on X.)

The Manin–Mumford conjecture asserts that $i(X)(\overline{K}) \cap \operatorname{Jac} X(\overline{K})_{\mathrm{tors}}$ is finite.

(1) Suppose $K = \mathbb{C}$ and $P, Q, R \in X(\mathbb{C})$ are distinct points on X. Suppose that $2i(P) = i(Q) + i(R)$. Show that X is hyperelliptic and P is fixed by the hyperelliptic involution.

(2) Suppose $e \geqslant 1$ is an integer. Show that there exists a constant $C(e)$ such that for every $m > C(e)$ the equation $x^e + y^e = 2z^e$ has solutions in $\mathbb{Z}/m\mathbb{Z}$ such that x^e, y^e, z^e are pairwise distinct and x, y, z are invertible to $\mathbb{Z}/m\mathbb{Z}$.

Note. Consider the cases when m is a prime, and m is a power of a fixed small prime (e.g. 2) first.

(3) We use the following theorem.

Theorem 1 (Serre)**.** *Suppose K is a number field and A/K is an abelian variety. Then there exists a constant e such that for all $n \in \mathbb{Z} \setminus \{0\}$, there exists an element $g \in \operatorname{Gal}(\overline{K}/K)$ that acts on any torsion point P of A of order prime to n via multiplication by n^e.*

Suppose K is a number field and let e denote the constant from Theorem 1 applied to $\operatorname{Jac} X$. Suppose $P \in X(\overline{K})$ is a torsion point of order $m > C(e)$. Use part (1) to conclude that there exists $z \in \mathbb{Z}$ prime to m such that $z^e P$ is a hyperelliptic branch point. Conclude that $X(\overline{K})$ has only finitely many torsion points.

(4) Use spreading out to prove the Manin–Mumford conjecture for any curve $X/\mathbb{C}$.

Remark 2. Recent (2021) work of Dimitrov–Gao–Habegger and Kühne implies that there is a uniform upper bound for the number of torsion points on a curve of genus g. At the same time the order of a torsion point on a genus g curve is known to be unbounded!

Tarski's theorem

This series of exercises presents a proof Tarski's theorem. This proof uses the notion of the topological degree of a map from $\mathbb{RP}^1 = S^1$ to itself.

A basic semialgebraic set in $\mathbb{R}^n$ is a set of the form $\{x \in \mathbb{R}^n | f_1(x) = f_2(x) = ... = f_m(x) = 0, g_1(x) > 0, g_2(x) > 0, ..., g_k(x) > 0\}$ for polynomials f_i, g_j. A semialgebraic set is a finite union of basic semialgebraic sets.

Theorem 3 (Tarski)**.** *The image of a semialgebraic set under a linear projection $\pi : \mathbb{R}^n \to \mathbb{R}^k$ is semialgebraic.*

(1) Check that the collection of semialgebraic sets is closed under unions, complements and intersections.

(2) Show that Tarski's theorem is equivalent to showing that the image $\pi(S)$ of a basic semialgebraic set $S \subset \mathbb{R}^n$ under the coordinate projection $\pi : \mathbb{R}^n \to \mathbb{R}^{n-1}$ is semialgebraic.

(3) Show that it suffices to show the following:

For given integers (d, m, k) let $\mathbb{R}^N = \mathbb{R}^{(m+k)(d+1)}$ be the linear space parameterizing all tuples of one-variable polynomials $f_1, ..., f_m, g_1, ..., g_k \in \mathbb{R}[x]$ of degree at most d. Then the subset of $\mathbb{R}^N$ corresponding to tuples $f_1, ..., f_m, g_1, ..., g_k$ for which the system $f_i = 0, g_j > 0$ has a solution $x \in \mathbb{R}$ is semialgebraic.

(4) Calculate the topological degree of the map $f : \mathbb{RP}^1 \to \mathbb{RP}^1$ given by a polynomial $f = x^d + O(x^{d-1})$.

(5) Suppose $f, g \in \mathbb{R}(x)$ are rational functions without common poles. Show that the topological degree $[\cdot]$ satisfies $[f+g] = [f] + [g]$ and $[1/f] = -[f]$.

(6) Suppose a rational function $f/g,\ f, g \in \mathbb{R}[x]$ has a continued fraction expansion

$$\frac{f}{g} = f_0 + \cfrac{1}{f_1 + \cfrac{1}{\ddots + \cfrac{1}{f_k}}}.$$

Show that $[f/g] = [f_0] - [f_1] + ... + (-1)^k [f_k]$.

(7) A real-valued function on a semialgebraic set S is called *constructive* if it takes only finitely many values and the level sets of the function are semialgebraic. Show that the function $[f/g]$ defined on the space $\mathbb{R}^{d+1} \times \{\mathbb{R}^{d+1} \setminus \{0\}\}$ of pairs of degree at most d polynomials f, g, $g \neq 0$ is constructive.

(8) In the notation of problem (6), show that

$$[gf'/f] = [f_0] + \sum_{\alpha \text{ root of } f} \text{sign } g(\alpha).$$

Therefore $(f, g) \mapsto \sum_{f(x)=0} \text{sign } g(x)$ is a constructive function on the set of pairs of polynomials f, g with $f \neq 0$.

(9) Use the constructivity of functions $\sum_{f(x)=0} \text{sign } g(x)$ and $\sum_{f(x)=0} \text{sign } g^2(x)$ to show that the number of zeroes of f on the set $g(x) > 0$ is a constructive function (as P, Q vary over all nonzero polynomials of degree at most d and $P \neq 0$).

(10) Show that the number of real roots of a polynomial P that satisfy the constraints $f_1 = ... = f_m = 0, g_1, ..., g_k > 0$ for some polynomials f_i, g_j is a constructive function on the set of all polynomial tuples (f_i, g_j, P) of degree at most d for which $P \neq 0$.

(11) Given $g_1, ..., g_m \in \mathbb{R}[x]$, consider the rational function $R = g_1 ... g_m/(1+x^N)$. Let $G := g_1 ... g_m$ and let $P = G'(1 + x^N) - NGx^{N-1}$ be the numerator of the derivative of R. Show that for large enough N the system $P = 0, g_1 > 0, ..., g_m > 0$ has a solution if and only if the sustem $g_1 > 0, ..., g_m > 0$ has a solution.

(12) Show that the subset of the set of all tuples of polynomials $g_1, ..., g_m$ of degree at most d consisting of tuples for which the system $g_1 > 0, ..., g_m > 0$ is solvable is semialgebraic.

(13) Prove Tarski's theorem.

The topological approach to Sturm-like theorems is taken from Khovanskii-Burda "Degree of rational mappings, and the theorems of Sturm and Tarski".

Ax's theorem using o-minimality

The goal of this problem is to give a proof of the following theorem of Ax, following Tsimerman.

Theorem 4. *Let $\Delta \subset \mathbb{C}$ be a domain and suppose $f_1, ..., f_m : \Delta \to \mathbb{C}$ are holomorphic functions that are $\mathbb{Q}$-linearly independent* modulo constants. *Then*

$$\text{tr.deg}(\mathbb{C}(f_1, ..., f_m, \exp(f_1), ..., \exp(f_m))/\mathbb{C}) \geqslant m + 1$$

(1) Prove that Ax's theorem is equivalent to the following statement.
Let $\Gamma \subset \mathbb{C}^m \times (\mathbb{C}^\times)^m$ denote the graph of exp. Let $V \subset \mathbb{C}^m \times (\mathbb{C}^\times)^m$ be an irreducible algebraic subvariety. Let U denote an irreducible component of $V \cap \Gamma$. Suppose the projection of U to $(\mathbb{C}^\times)^m$ does not lie in a coset of a proper subtorus of $(\mathbb{C}^\times)^m$. Then

$$\dim_{\mathbb{C}} V \geqslant \dim_{\mathbb{C}} U + m.$$

In the remaining exercises we will prove this statement by induction on $(m, \dim V - \dim U, m - \dim U)$. We may assume that $\dim U > 0$ as $\dim U = 0$ case is trivial.

(2) Let W denote the smallest affine linear subvariety in $\mathbb{C}^m$ containing the projection of U to $\mathbb{C}^m$ and let $\mathcal{F}$ denote the fundamental domain

$$\{(z_1, \ldots, z_m, w_1, \ldots, w_m) \in \mathbb{C}^m \times (\mathbb{C}^\times)^m \mid 0 \leqslant \Re(z_i) < 1, 1 \leqslant i \leqslant m\}.$$

Prove that the following subset $I \subset \mathbb{R}^m$ is definable in $\mathbb{R}_{\text{an,exp}}$

$$I = \{x \in \mathbb{R}^m \mid G_{\dim U}((x + V) \cap (\Gamma \cap \mathcal{F}), W) \neq \emptyset\},$$

where $G_{\dim U}(Y, W)$ is the set of all $y \in Y$ such that Y is regular of dimension $\dim U$ around y and the smallest affine linear subvariety in $\mathbb{C}^m$ containing the irreducible component of Y containing y is a translation of W.

(3) Prove that if $I \cap \mathbb{Z}^m$ is finite, then U is definable.
From here we prove by contradiction that $I \cap \mathbb{Z}^m$ is infinite because U, a definable closed analytic subvariety in $\mathbb{C}^m \times (\mathbb{C}^\times)^m$, must be algebraic by a theorem of Peterzil and Starchenko ("Tame complex analysis and o-minimality" Theorem 4.5); on the other hand U being algebraic contradicts with U is contained in the graph of exp.

(4) Use $I \cap \mathbb{Z}^m$ is infinite to prove that I contains a semi-algebraic curve $C_{\mathbb{R}}$.

(5) By the definition of I, for each $c \in C_{\mathbb{R}}$, we consider an irreducible component X_c of $(C+V) \cap (\Gamma \cap \mathcal{F})$ of dimension $\dim U$ such that the smallest affine linear subvariety containing X_c is a translation of W. Prove that if there are infinitely many distinct W_c, then there is an irreducible component X of $(C + V) \cap \Gamma$ of dimension $\dim U + 1$ and show that we can apply induction hypothesis to $(C + V)$ to conclude.

(6) Prove that if there is only finitely many distinct X_c, then there exists X_{c_0} which is contained in $c+V$ for all $c \in C$. Show that we may apply inductive hypothesis to conclude if $C+V \neq V$.

(7) The remaining case is when $C + V = V$. Prove that there exists V^0 such that $V = \mathbb{C} \times V^0$ with $V^0 \subset \mathbb{C}^{m-1} \times (\mathbb{C}^\times)^{m-1} \times \mathbb{C}^\times$ after a suitable linear change of coordinates. Conclude by applying induction hypothesis on m.

Reference: Tsimerman "Ax–Schanuel and o-minimality"

The class number one problem

This problem shows that the class number one problem for imaginary quadratic fields can be reduced to finding integral points on certain modular curves. Let K denote an imaginary quadratic field of discriminant D and class number 1, and let $\mathcal{O}_K$ denote its ring of integers.

(1) Suppose K is a quadratic imaginary field of class number 1, and $E = \mathbb{C}/\Lambda$ is an elliptic curve with CM by $\mathcal{O}_K$. Show that E is isomorphic to $\mathbb{C}/\mathcal{O}_K$.
(2) Suppose that E is an elliptic with CM by $\mathcal{O}_K$. Show that $j(E) \in Y(1)$ is a rational number.
(3) Suppose p is a fixed prime. Show that for $D \gg 0$ and K as above the prime p has to either be inert or ramify in $\mathcal{O}_K$.
From now on we fix a small prime p and assume it to be inert; the ramified case is similar.
(4) Show that the action of $\mathcal{O}_K/p$ on $E[p]$ defines a point on the nonsplit Cartan modular curve $X_{ns}(p)$. This modular curve is a quotient of the modular curve $X(p)$, parameterizing elliptic curves with a basis of $E[p]$, by the action of the normalizer of nonsplit Cartan subgroup $H \subset \mathrm{GL}_2(\mathbb{F}_p)$.
(5) Show that the j-invariant of a CM elliptic curve is an integer.

Thus it suffices to find integral points on $X_{ns}(p)$ for some small p. For example one finds that the curve $X_{ns}(7)$ has geometric genus 0 and three "cusps"; one can find integral points on such curves effectively.
(6) The case of a ramified prime can be handled similarly using modular curves. There is also a more straighforward approach: show that if the discriminant D is divisble by 2 distinct primes then the class group of K has nontrivial 2-torsion.

Runge's method

Suppose that the equation $f(x, y) = 0,\ f \in \mathbb{Q}[x, y]$ defines a smooth affine curve X, and that the intersection of X with the line at infinity contains two nonintersecting Galois orbits D_1, D_2.

(1) Show that there exists a pair of polynomials $P_1, P_2 \in \mathbb{Z}[x, y]$ such that P_i restricted to X has no poles outside D_i.
(2) Show that the equation $f(x, y) = 0$ has only finitely many integral solutions.
(3) Suppose $F, G \in \mathbb{Z}[x]$ are irreducible relatively prime monic polynomials of the same degree $d \geqslant 2$. Use Runge's method to show that the equation $F(X) = G(Y)$ has only finitely many integer solutions.

Max Noether's theorem

The gonality of a curve X is the minimal degree of a nonconstant morphism $f : X \to \mathbb{P}^1$.

(1) Show that the gonality of a smooth plane curve of degree d is at most $d - 1$.
(2) Suppose X is a smooth plane curve of degree $d \geqslant 3$ and $f : X \to \mathbb{P}^1$ is a map of degree less than $d - 1$. Let $\mathcal{L} := f^*\mathcal{O}(1)$, and let $\mathcal{O}_X(n)$ denote the pullback of $\mathcal{O}(n)$ on $\mathbb{P}^2$ to X. Show that there exists an embedding $\mathcal{L} \hookrightarrow \mathcal{O}_X(d - 2)$.
(3) Show that there exists a pencil of plane curves of degree $k < (d - 1)$ that cuts out the linear series given by f on X. Conclude that the degree of f is at least $k(d - k)$, and thus the gonality of a smooth plane curve is equal to $d - 1$.
(4) Show that the gonality of an irreducible singular plane curve is less than $d - 1$.

Miscellaneous exercises

(1) Show that there does *not* exists an elliptic curve $E/\mathbb{Q}$ with surjective adelic Galois action $\rho_E : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \prod_p \mathrm{GL}_2(\mathbb{Z}_p)$.

(2) (**Schanuel's theorem**) Show that as X goes to infinity the following formula hods:

$$\#\{P \in \mathbb{P}^n(\mathbb{Q}) : H(P) < X\} \sim \frac{2^n}{\zeta(n+1)} X^{n+1},$$

where $\zeta(s) = \prod_p (1 - p^{-s})^{-1}$ is the Riemann zeta function.
Note. The case $n = 1$ is already interesting.

(3) Suppose $\mathscr{X} / \operatorname{Spec} \mathbb{Z}$ is a regular curve and $P \in \mathscr{X}(\mathbb{Z})$ is an integral point. Show that for every prime p the reduction of P in $\mathscr{X}_{\mathbb{F}_p}$ is a smooth point of $\mathscr{X}_{\mathbb{F}_p}$.

(4) (**Hall's conjecture for polynomials**) Suppose $A, B \in \mathbb{C}[z]$ are relatively prime, $\deg A = 2d$, $\deg B = 3d$. Show that $\deg(A^3 - B^2) \geqslant d + 1$

(5) Prove the following result of Siegel.

Theorem 5. *Let $f \in \mathbb{Z}[x]$ be a polynomial of degree $d \geqslant 2$ without repeated factors. For a nonzero integer N let $\mathscr{P}(N)$ denote the largest prime factor of N. Then the sequence $\mathscr{P}(f(n))$, $n = 1, 2...$ grows to infinity.*

(6) This exercise shows that the "normal crossing divisor" assumption in Vojta's conjecture is necessary.

Let K be a number field and consider $X = \mathbb{P}^2_K$ with homogenenous coordinates $[x_0 : x_1 : x_2]$ and a divisor $D = (x_1 = 0) + (x_2 = 0) + ((x_1 - x_2)x_0 = (x_1 + x_2)^2)$.
(a) Prove that D is *not* a normal crossing divisor.
(b) Prove that $\kappa(\mathcal{K}_X \otimes \mathcal{O}_X(D)) = \dim(X)$.
(c) Prove that for large enough S, the set of S-integral points in $X \setminus D$ is Zariski dense.