Università degli Studi Roma Tre
Facoltà di Scienze Matematiche, Fisiche e Naturali
Corso di Laurea in Matematica

Tesi di Laurea Magistrale in Matematica

Distribution of rational points on algebraic curves

Synthesis

Candidato
Luca Schaffler

Relatore
Prof.ssa Lucia Caporaso

Anno Accademico 2011-2012
Luglio 2012

AMS classification: 14G05, 14H99, 11G05, 11G30, 11D45
Key words: schemes, rational points, varieties of general type, elliptic and hyperelliptic curves, Diophantine problems, Faltings' Theorem, Lang's Conjectures, Bound Conjectures

Synthesis

This is a thesis in Algebraic Geometry and its interactions with another field of mathematics: Number Theory. More precisely, we will study rational points on schemes with emphasis on the case of algebraic curves. Let's cite a famous open problem concerning rational points in which we can see how the two fields of mathematics may interact.

Open problem (the perfect cuboid). *It's not known if there exists a cuboid having rational sides, rational face diagonals and rational space diagonals. Equivalently, it's not known if there exists a solution over $\mathbb{Q}$ to the following Diophantine problem:*

$$\begin{cases} x^2 + y^2 = a^2 \\ x^2 + z^2 = b^2 \\ y^2 + z^2 = c^2 \\ x^2 + y^2 + z^2 = d^2, \end{cases}$$

where x, y, z, a, b, c, d are indeterminate.

This kind of problem can be studied with an arithmetic approach, that uses tools from the world of Number Theory (for example, one can start asking if there exists a solution over $\mathbb{Z}$), and with a geometric approach. The geometric approach consists in the interpretation of the system above as a closed subscheme X in $\mathbf{P}^6_{\mathbb{Q}}$ (it was proven by van Luijk that X is a surface of general type) and the rational solutions of the system (if any) will correspond to $\mathbb{Q}$-rational points of the scheme X. Now that we have an idea of our subject, let's go through this work.

Let X be a k-scheme with structural morphism $f\colon X \to \mathrm{Spec}(k)$ and let $X(k)$ be the set of sections of the k-scheme X, i.e. the morphisms $s\colon \mathrm{Spec}(k) \to X$ such that $f \circ s = \mathrm{id}_{\mathrm{Spec}(k)}$. The first concept we introduce is the definition of k-rational point on X.

Definition of k-rational point. Let X be a scheme over k. A point $x \in X$ is called *k-rational* if there exists $s \in X(k)$ such that $s((0)) = x$. If $s \in X(k)$, the map $s \mapsto s((0))$ is a bijection between $X(k)$ and the set of k-rational points, which we will identify.

The structural morphism f induces an injection $k \hookrightarrow k(x)$, which allows to give the following characterization of k-rational points:

Proposition 1. *Let X be a scheme over k. A point $x \in X$ is k-rational $\Leftrightarrow$ the injection $k \hookrightarrow k(x)$ associated to the structural morphism is surjective.*

Therefore, for a k-rational point $x \in X$ we have $k \cong k(x)$, but the converse is not true: just take $k := \mathbb{Q}(x_1, x_2, \ldots)$ where $x_1, x_2, \ldots$ are indeterminate over $\mathbb{Q}$, $X := \mathrm{Spec}(k)$ and define as structural morphism the morphism f induced by the ring homomorphism $\varphi\colon k \to k$ obtained by extending $x_i \mapsto x_{i+1}$, $i \geq 1$. It's easy to see that $k((0)) \cong k$ while the inclusion $k \hookrightarrow k(x)$ induced by f is not surjective. However, $k(x) \cong k$ implies $x \in X(k)$ with some more hypotheses, for instance assuming that k is a finite extension of its base field or $k = \overline{k}$ and $k \hookrightarrow k(x)$ algebraic.
k-rational points on a k-scheme X behaves well with subschemes.

Proposition 2. *Let X be a k-scheme and let $Y \subseteq X$ be an open or closed subscheme. If $i\colon Y \to X$ is the inclusion morphism, Y can be viewed as a k-scheme through the structural morphism $f \circ i$, where f is the structural morphism of the k-scheme X. Then $Y(k) = X(k) \cap Y$.*

Now we focus our attention on k-schemes locally of finite type. In this case k-rational points are closed points.

Theorem 1. *Let X be a scheme locally of finite type over k with structural morphism f and let $x \in X$. If $k \hookrightarrow k(x)$ is induced by f, the following are equivalent:*

(i) *x is closed;*

(ii) *$k \hookrightarrow k(x)$ is finite;*

(iii) *$k \hookrightarrow k(x)$ is algebraic.*

Since it is a topological fact that a nonempty, quasi-compact and T_0 topological space has a closed point (this is a consequence of Zorn's Lemma), we get at once the following result:

Proposition 3. *If X is a nonempty scheme of finite type over $k = \overline{k}$, then $X(k) \neq \emptyset$.*

Now we come to the previously announced link between k-rational points of a scheme locally of finite type over k and polynomial systems over k.

Proposition 4. *Let $x_1, \ldots, x_n$ be indeterminate over k and let $f_1, \ldots, f_c \in k[x_1, \ldots, x_n]$. If we consider the scheme:*

$$X := \operatorname{Spec}\left(\frac{k[x_1, \ldots, x_n]}{(f_1, \ldots, f_c)}\right),$$

there is a one-to-one correspondence between k-rational points of X (which is a scheme over k with the structural morphism f induced by the natural injection $i\colon k \hookrightarrow \frac{k[x_1,\ldots,x_n]}{(f_1,\ldots,f_c)}$) and solutions in $\mathbb{A}_k^n$ of the polynomial system:

$$\begin{cases} f_1(x_1, \ldots, x_n) = 0 \\ \vdots \\ f_c(x_1, \ldots, x_n) = 0. \end{cases}$$

In other words, we have that:

$$X(k) \leftrightarrow Z(f_1, \ldots, f_c) := \{p \in \mathbb{A}_k^n | f_i(p) = 0,\ \forall\ i = 1, \ldots, c\}.$$

In particular:

$$X(k) = \left\{ \frac{(x_1 - p_1, \ldots, x_n - p_n)}{(f_1, \ldots, f_c)} \middle| (p_1, \ldots, p_n) \in Z(f_1, \ldots, f_c) \right\}.$$

Corollary 1. *Let X be a scheme of finite type over a finite field k. Then $|X(k)| < \infty$.*

Proposition 4 has a projective analogous:

Proposition 5. *Let $X_0, \ldots, X_n$ be indeterminate over k and let $F_1, \ldots, F_c \in k[X_0, \ldots, X_n]$ be homogeneous polynomials. Consider the scheme:*

$$X := \operatorname{Proj}\left(\frac{k[X_0, \ldots, X_n]}{(F_1, \ldots, F_c)}\right).$$

Then there is a one-to-one correspondence between k-rational points of X and solutions in $\mathbb{P}_k^n$ of the polynomial system:

$$\begin{cases} F_1(X_0, \ldots, X_n) = 0 \\ \vdots \\ F_c(X_0, \ldots, X_n) = 0. \end{cases}$$

In other words, we have that:

$$X(k) \leftrightarrow V(F_1, \ldots, F_c) := \{p \in \mathbb{P}_k^n | F_i(p) = 0,\ \forall\ i = 1, \ldots, c\}.$$

The property we mention here is that k-rational points are compatible with field extensions. Roughly speaking, we mean that if X is a k-scheme and $k \subseteq K$ is a field extension, k-rational points on X are a subset of K-rational points of $X_K := X \times_k \mathrm{Spec}(K)$. Formally:

Proposition 6. *Let X be a k-scheme and let $k \subseteq K$ be a field extension. Then there is a natural injection $X(k) \hookrightarrow X_K(K)$.*

Now we study how some properties of a k-scheme X of finite type, such as dimension, connectedness, irreducibility, reducedness and regularity, behave under an algebraic extension of the base field. This discussion makes sense because we want to introduce the concept of variety over a field which is not algebraically closed, and this is worth to be clarified since a first approach to Algebraic Geometry deals with the algebraically closed case. In our definition, we want that if a projective k-scheme X is a variety, then $X_{\overline{k}}$ is regular, projective and irreducible. Of course we need to understand what happens with this base extension in order to have $X_{\overline{k}}$ with the right hypotheses (and X with the minimal ones). Let's give some more details.

Proposition 7. *Let X be a scheme of finite type over k and let $k \subseteq K$ be an algebraic field extension. Then* $\dim(X) = \dim(X_K)$.

The key of the proof of previous proposition is Noether Normalization Lemma. Now let P be a property between connected, irreducible, reduced and integral. It's possible to exhibit schemes X of finite type over a field k with property P such that $X_{\overline{k}}$ is not P. This motivates the definition of *geometrically P* scheme.

Definition 1. A scheme X of finite type over k is said to be *geometrically connected* (resp. *irreducible*, *reduced*, *integral*) if $X_{\overline{k}}$ is connected (resp. irreducible, reduced, integral).

Geometrically P is stronger than P.

Proposition 8. *Let X be a k-scheme of finite type. X is geometrically $P \Leftrightarrow$ for each algebraic field extension $k \subseteq K$, X_K is P.*

However, if $P =$ reduced and the base field is perfect, reduced and geometrically reduced are equivalent. This is a consequence of next proposition.

Proposition 9. *Let X be a reduced scheme over k of finite type and let $k \subseteq K$ be a separable field extension. Then X_K is reduced.*

We treat now regularity and projectivity. Regularity is not preserved under an algebraic extension of the base field, therefore we introduce the concept of *smooth* scheme.

Definition 2. Let X be a scheme of finite type over k, $x \in X$ and let $p\colon X_{\overline{k}} \to X$ be the projection. X is *smooth at* x if $X_{\overline{k}}$ is regular at x' for each $x' \in p^{-1}(x)$. X is *smooth* if it is smooth at every point $x \in X$. Equivalently, X is smooth if $X_{\overline{k}}$ is regular.

It's natural to ask how smoothness relates with regularity.

Theorem 2. *Let X be a scheme of finite type over k. If X is smooth, then X is regular.*

The proof of this theorem is delicate and involves k-rational points and the Jacobian criterion of regularity, which we don't state here since requires the introduction of several notations. The converse of Theorem 2 holds if the base field k is perfect. About projectivity and base field extension, we prove the following more general result:

Proposition 10. *Let A, B and C be rings with B graded A-algebra and C A-algebra. Then we have a canonical isomorphism of schemes:* $\operatorname{Proj}(B \otimes_A C) \cong \operatorname{Proj}(B) \times_A \operatorname{Spec}(C)$.

From this proposition we can understand how a base field extension operates on a projective scheme over k, whose structure is here described:

Proposition 11. *Let X be a projective scheme over a field k. Then there exist $n \geq 0$ and a homogeneous ideal $I \subseteq k[X_0, \ldots, X_n]$ such that:*

$$X \cong \operatorname{Proj}\left(\frac{k[X_0, \ldots, X_n]}{I}\right).$$

Moreover, X is a noetherian scheme, of finite type over k and proper over k.

After this discussion, we are ready to define varieties over any field k, in case $k \subsetneq \overline{k}$.

Definition 3. Let k be a field. A *variety* over k is a scheme X which is projective over k, geometrically irreducible and smooth. A *curve* is a variety of dimension one and a *surface* is a variety of dimension two.

For the theory of varieties over non algebraically closed fields, see for example the exposition of [Liu02]. *Varieties of general type* will be important to us.

Definition 4. Let X be a scheme of finite dimension n and let $\mathscr{L} \in \mathrm{Pic}(X)$. We will say that $\mathscr{L}$ is *big* if there exist a real number $c > 0$ and $N_0 \in \mathbb{N}$ such that for each $N > N_0$:

$$h^0(X, \mathscr{L}^{\otimes N}) > cN^n.$$

Definition 5. Let X be a variety. X is said to be of *general type* if the canonical sheaf is big.

A curve of genus $g \geq 2$ is a first example of variety of general type. More precisely, using Riemann-Roch Theorem we can show that a curve X is of general type $\Leftrightarrow g(X) \geq 2$. There is another equivalent definition of variety of general type which uses the notion of *Kodaira dimension*, which we want to introduce. First we fix some notation. If X is a variety over a field k and $\mathscr{L}$ is an invertible sheaf on X, define:

$$N(X, \mathscr{L}) := \{m \geq 0 | h^0(X, \mathscr{L}^{\otimes m}) > 0\},$$

which is a commutative monoid under addition (it's always true that $0 \in N(X, \mathscr{L})$). Therefore, if $m \in N(X, \mathscr{L})$, we can define a rational map:

$$\phi_{\mathscr{L}^{\otimes m}} \colon X \dashrightarrow \mathbf{P}(H^0(X, \mathscr{L}^{\otimes m})).$$

Definition 6. Let X be a variety and let $\mathscr{L} \in \mathrm{Pic}(X)$. We define the *Iitaka dimension of X relative to $\mathscr{L}$*, in symbols $\kappa(X, \mathscr{L})$, to be $-\infty$ if $N(X, \mathscr{L}) = \{0\}$ and:

$$\max_{m \in N(X, \mathscr{L})} \{\dim \phi_{\mathscr{L}^{\otimes m}}(X)\}$$

otherwise. The Iitaka dimension of X relative to ω_X is called the *Kodaira dimension of X*, which is denoted by $\kappa(X)$.

The Kodaira dimension is an important birational invariant. The equivalent definition of variety of general type is a consequence of next theorem:

Theorem 3. *Let X be a variety and let $\mathscr{L}$ be an invertible sheaf on X. $\mathscr{L}$ is big $\Leftrightarrow \dim(X) = \kappa(X, \mathscr{L})$.*

Corollary 2. *A variety X is of general type $\Leftrightarrow \dim(X) = \kappa(X)$.*

An example of variety which is not of general type is for instance $\mathbf{P}^2_k$.

As mentioned earlier, we want to focus on the study of k-rational points on curves and *hyperelliptic curves* will play a central role. Therefore we develop in details the theory of hyperelliptic curves, with particular emphasis on the study of their isomorphism classes. Here we put ourself in the case of classical Algebraic Geometry over an algebraically closed field $\overline{k}$ of characteristic different from 2. In $\mathbb{P}^1_{\overline{k}}$ we make the identification $\infty := (1:0)$ and $a := (a:1)$.

Definition 7. Let $\mathscr{C}$ be a curve over $\overline{k}$ of genus $g \geq 2$. Then $\mathscr{C}$ is said to be *hyperelliptic* if there exists a degree 2 regular map $f\colon \mathscr{C} \to \mathbb{P}^1_{\overline{k}}$. Using Hurwitz formula we get immediately that f has $2g+2$ ramification points, and hence $2g+2$ branch points. The map $\iota\colon \mathscr{C} \to \mathscr{C}$ such that $\iota(p) := q$ where $f(p) = f(q)$ is called the *hyperelliptic involution*. Obviously, ι is the identity on the ramification points and $\iota \circ \iota = \mathrm{id}_{\mathscr{C}}$.

Theorem 4. *Let $\mathscr{C}$ be a hyperelliptic curve over $\overline{k}$ of genus g with $f\colon \mathscr{C} \to \mathbb{P}^1_{\overline{k}}$ as degree 2 regular map. Then $\mathscr{C}$ is isomorphic to the desingularization of the projective closure of the affine plane closed subset of equation:*

$$y^2 = \prod_{j=1}^{2g+2} (x - a_j),$$

where the $a_j \in \overline{k}$ are the distinct branch points of f (here we assume, up to compose f with a projective transformation of $\mathbb{P}^1_{\overline{k}}$, that f hasn't a branch point at ∞). In addition, the morphism f is uniquely determined up to an automorphism of $\mathbb{P}^1_{\overline{k}}$.

Corollary 3. *Let $\mathscr{C}_1$, $\mathscr{C}_2$ be two hyperelliptic curve over $\overline{k}$ with degree 2 morphism f_1 and f_2 respectively. If the branch points of f_1 differ from those of f_2 by a projective transformation of $\mathbb{P}^1_{\overline{k}}$, then $\mathscr{C}_1$ and $\mathscr{C}_2$ are isomorphic.*

The following is a sort of converse of Theorem 4

Theorem 5. *Let $\widetilde{\mathscr{C}}$ be the desingularization of $\mathscr{C}$, which is the projective closure of the affine plane closed subset of equation:*

$$y^2 = P(x),$$

where $P \in \overline{k}[x]$ with distinct roots and degree $n \geq 5$. Then $\widetilde{\mathscr{C}}$ is a hyperelliptic curve with genus g given by:

$$g = \begin{cases} \frac{n-1}{2} & \textit{if } n \textit{ is odd,} \\ \frac{n-2}{2} & \textit{otherwise.} \end{cases}$$

Now we start studying the isomorphism classes of hyperelliptic curves.

Definition 8. Let $g \geq 2$ be an integer, S_{2g+2} the group of permutations of $2g+2$ objects and let E be any set. If $(e_1, \ldots, e_{2g+2}) \in E^{2g+2}$, define:

$$\pi(e_1, \ldots, e_{2g+2}) := (e_1, \ldots, e_{2g-1}).$$

If $\sigma \in S_{2g+2}$, define also:

$$\sigma(e_1, \ldots, e_{2g+2}) := (e_{\sigma(1)}, \ldots, e_{\sigma(2g+2)}).$$

If F is a second set and $\varphi \colon E \to F$ is a function, define:

$$\varphi(e_1, \ldots, e_{2g+2}) := (\varphi(e_1), \ldots, \varphi(e_{2g+2})).$$

Now consider the following open subset of $\mathbb{A}_{\overline{k}}^{2g-1}$ with respect to Zariski topology:

$$\mathcal{X}_{\overline{k}}^{g} := \{(\beta_1, \ldots, \beta_{2g-1}) \in \mathbb{A}_{\overline{k}}^{2g-1} | \forall\ i, j \text{ with } i \neq j, \beta_i \neq 0, 1 \text{ and } \beta_i \neq \beta_j\}.$$

Define an action of S_{2g+2} over $\mathcal{X}_{\overline{k}}^{g}$ as follows. Take $\sigma \in S_{2g+2}$, $(\beta_1, \ldots, \beta_{2g-1}) \in \mathcal{X}_{\overline{k}}^{g}$ and let be $\beta_{2g} := 0$, $\beta_{2g+1} := 1$, $\beta_{2g+2} := \infty$. Let φ_σ be the projective transformation of $\mathbb{P}_{\overline{k}}^{1}$ such that:

$$\varphi_\sigma(\beta_{\sigma(2g)}, \beta_{\sigma(2g+1)}, \beta_{\sigma(2g+2)}) = (0, 1, \infty).$$

Then define:

$$\sigma * (\beta_1, \ldots, \beta_{2g-1}) := \pi\varphi_\sigma\sigma(\beta_1, \ldots, \beta_{2g+2}).$$

Lastly, let $\mathcal{Y}_{\overline{k}}^{g}$ be the set $\mathcal{X}_{\overline{k}}^{g}$ modulo the action of " $*$ ".

Proposition 12. *There is a bijection between $\mathcal{Y}_{\overline{k}}^{g}$ and the isomorphism classes of hyperelliptic curves over $\overline{k}$ of genus g.*

Observe in particular that $\mathcal{Y}^2_{\overline{k}}$ parametrizes all genus 2 curves. Over a field k which is not algebraically closed, we will say that a curve $\mathscr{C}$ over k is hyperelliptic if $\mathscr{C}_{\overline{k}}$ is hyperelliptic.

Let's start with the study of k-rational points on curves considering the case $g = 0$. First we observe that:

Proposition 13. *Let $\mathscr{C}$ be a curve over k of genus 0. Then $\mathscr{C}$ is isomorphic to a smooth conic over k and conversely.*

Then, if we know that at least one k-rational point exists, we can give explicitly all the others (here we put ourselves in zero characteristic).

Theorem 6. *Let $\mathscr{C}$ be a smooth conic in $\mathbb{P}^2_k$. Then $\mathscr{C} \cong \mathbb{P}^1_k \Leftrightarrow \mathscr{C}(k) \neq \emptyset$. Under these hypotheses, $|\mathscr{C}(k)| = \infty$ and if our conic is in the form:*

$$XY + \varepsilon XZ - (1+\varepsilon)YZ = 0$$

with $\varepsilon \in k\backslash\{0, -1\}$ (this can be assumed up to a projective transformation of $\mathbb{P}^2_k$), then k-rational points can be parametrized in the following way:

$$\mathscr{C}(k) = \{((1+\varepsilon)uv : -v(v-u\varepsilon) : u(v-u\varepsilon)) | (u:v) \in \mathbb{P}^1_k\}.$$

Hence, the only problem now concerns the existence of a k-rational point on a genus 0 curve (of course, the answer is trivial if $k = \overline{k}$). We will give a criterion to establish the existence of k-rational points in the case $k = \mathbb{Q}$. After some elementary considerations, the study of the existence of a $\mathbb{Q}$-rational point on a smooth conic over $\mathbb{Q}$ is equivalent to establish the existence of a solution to one of the following Diophantine equations:

$$aX^2 + bY^2 = \pm Z^2,$$

where $a, b \in \mathbb{N}^*$ are square free[†] (a, b are nonzero because the conic is smooth). Obviously, equation $aX^2+bY^2 = -Z^2$ has no solutions. Hence the interesting case is:

$$aX^2 + bY^2 = Z^2, \tag{1}$$

which is known as Legendre's equation.

Theorem 7. *In equation (1), let $h := \mathrm{GCD}(a, b)$ and set $a = ha_1, b = hb_1$. Equation (1) has a solution $\Leftrightarrow$ the following congruences are solvable: $\alpha^2 \equiv a (\mathrm{mod}\ b)$, $\beta^2 \equiv b (\mathrm{mod}\ a)$, $\gamma^2 \equiv -a_1b_1 (\mathrm{mod}\ h)$.*

[†] $a \in \mathbb{Z}^*$ is square free if $a = \pm p_1 \dots p_n$ where $p_1, \dots, p_n$ are distinct prime numbers.

The hard part in Theorem 7 is that the solubility of the three congruences implies the existence of a solution. The idea is the following: if $a > b$ (and similarly if $a < b$), we build a second equation $AX^2 + bY^2 = Z^2$ whose coefficients verify hypotheses similar to the ones verified by a and b. More formally, $A > 0$, $\alpha^2 \equiv A(\text{mod } b)$, $\beta^2 \equiv b(\text{mod } A)$ are solvable and, if $H := \text{GCD}(A, b)$, $A = A_2H$, $b = b_2H$, $\gamma^2 \equiv -A_2b_2(\text{mod } H)$ is solvable. The interesting fact is that the equation $AX^2 + bY^2 = Z^2$ can be build in such a way that $A < a$ and its solubility implies the solubility of $aX^2+bX^2 = Z^2$. By iteration, we can reduce ourselves to the cases $cX^2+Y^2 = Z^2$, $X^2+dY^2 = Z^2$ or $eX^2 + eY^2 = Z^2$, whose solubility can be easily established.

The case $g = 1$ is more complicated. Firstly, a genus 1 curve over k with at least one k-rational point is isomorphic to a smooth plane cubic.

Theorem 8. *Let $\mathscr{C}$ be a genus 1 curve with $x \in \mathscr{C}(k)$. Then $\mathscr{L}(3x)$ is very ample and induces a closed immersion into $\mathbb{P}^2_k$ whose image is a smooth cubic.*

An example of genus 1 curve over $\mathbb{Q}$ with no $\mathbb{Q}$-rational points is Selmer's equation:

$$3X^3 + 4Y^3 + 5Z^3 = 0.$$

We show that this equation has no $\mathbb{Q}$-rational points using standard techniques in Algebraic Number Theory. Firstly, $3X^3 + 4Y^3 + 5Z^3 = 0$ has a solution $\Leftrightarrow$ $X^3 + 6Y^3 = 10Z^3$ has a solution. If $\alpha := \sqrt[3]{6}$, $K := \mathbb{Q}(\alpha)$ and (x, y, z) is a (nontrivial) solution of $X^3 + 6Y^3 = 10Z^3$, we consider the following ideals equality in $\mathcal{O}_K$:

$$(x + \alpha y)(x^2 - \alpha xy + \alpha^2 y^2) = (10)(z)^3. \tag{2}$$

By studying the factorization of the ideals involved in equality (2), we will find a contradiction.
We focus now on *elliptic curves*:

Definition 9. An *elliptic curve* over k is a smooth cubic in $\mathbb{P}^2_k$ with at least one k-rational point, which will be denoted by O. If O is a flex and $\text{Char}(k) \neq 2$, then our curve will be isomorphic to the projective closure of the affine plane closed subset of equation:

$$y^2 = Ax^3 + Bx^2 + Cx + D,$$

where the right hand polynomial is of degree three with distinct roots in $\overline{k}$.

Observe that an elliptic curve can be embedded in $\mathbb{P}^3_k$ as the intersection of two irreducible quadrics and, conversely:

Proposition 14. *If Q_1, Q_2 are two irreducible quadrics in $\mathbb{P}^3_k$ with transverse intersection over $\overline{k}$ such that $Q_1 \cap Q_2$ is smooth and $k(Q_1 \cap Q_2) \neq \emptyset$, then $Q_1 \cap Q_2$ is an elliptic curve over k.*

The remarkable property of k-rational points on an elliptic curve $\mathscr{C}$ is that they form a group together with an adequate operation "+". If we put ourselves over $\mathbb{Q}$, a lot (but not everything) is known about $(\mathscr{C}(\mathbb{Q}), +)$.

Mordell-Weil Theorem. *Given an elliptic curve $\mathscr{C}$ over $\mathbb{Q}$, the group $(\mathscr{C}(\mathbb{Q}), +)$ is finitely generated.*

We can give thus the following definition.

Definition 10. Given an elliptic curve $\mathscr{C}$ over $\mathbb{Q}$, we have from Mordell-Weil Theorem that $\mathscr{C}(\mathbb{Q}) \cong \mathscr{C}(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r$ for some $r \in \mathbb{N}$, where $\mathscr{C}(\mathbb{Q})_{\text{tors}}$ is the torsion subgroup of $\mathscr{C}(\mathbb{Q})$. r is called the *rank* of $\mathscr{C}$.

About this torsion subgroup, we have two important theorems:

Mazur's Theorem. *Given an elliptic curve $\mathscr{C}$ over $\mathbb{Q}$, the torsion subgroup of $(\mathscr{C}(\mathbb{Q}), +)$ is isomorphic to one of the following abelian groups:*

- $\mathbb{Z}/n\mathbb{Z}$ *with* $1 \leq n \leq 10$ *or* $n = 12$*;*
- $(\mathbb{Z}/2\mathbb{Z}) \oplus (\mathbb{Z}/2m\mathbb{Z})$ *with* $1 \leq m \leq 4$*.*

Moreover, each of these groups occurs as the torsion subgroup of $(\mathscr{C}(\mathbb{Q}), +)$ for some elliptic curve $\mathscr{C}$ over $\mathbb{Q}$.

Nagell, Lutz Theorem. *Let $\mathscr{C}$ be the elliptic curve over $\mathbb{Q}$ defined by $y^2 = x^3 + ax + b$ with $a, b \in \mathbb{Z}$. If $(x, y) \in \mathscr{C}(\mathbb{Q})_{\text{tors}}$, then:*

1. *$x, y \in \mathbb{Z}$;*
2. *either $y = 0$ or $y^2 | 4a^3 + 27b^2$.*

The rank of an elliptic curve is hard to determine. For instance we have the following conjecture:

Rank Conjecture. *For each $n \in \mathbb{N}$, there exists an elliptic curve $\mathscr{C}$ over $\mathbb{Q}$ whose rank is greater than n.*

More information about the rank can be found in [RS02].

Our starting point for the case $g \geq 2$ is Faltings' Theorem:

Faltings' Theorem. *Any curve of genus $g \geq 2$ defined over a number field K has finitely many K-rational points.*

This theorem implies finiteness for the number of solutions of a Diophantine equation which represents a curve of general type over a number field. We won't prove Faltings' result, which involves important instruments of Diophantine Geometry such as Weil Height Function and Vojta's Inequality. A reference for these arguments is [HiSi00]. Indeed, our interest is devoted to the consequences of this theorem. As far as a curve over K of genus $g \geq 2$ has finitely many K-rational points, it makes sense to ask if, fixed K and $g \geq 2$, there exists a constant in $\mathbb{N}$, named $B(K, g)$, such that any curve over K of genus g has at most $B(K, g)$ K-rational points. The existence of such a constant is an important conjecture in Arithmetic Geometry:

Uniform Bound Conjecture. *For every number field K and for every integer $g \geq 2$, there exists a natural number $B(K, g)$ such that no curve of genus g defined over K has strictly more than $B(K, g)$ K-rational points. We take $B(K, g)$ minimal with this property.*

In the same fashion, there is a second conjecture which rises:

Universal Generic Bound Conjecture. *For every integer $g \geq 2$, there exists a natural number $N(g)$ such that for any number field K there are only finitely many K-isomorphism classes of curves of genus g defined over K having strictly more than $N(g)$ K-rational points. We take $N(g)$ minimal with this property.*

It was shown by Caporaso, Harris and Mazur that this two conjectures are indeed consequences of the Lang Conjectures, that we are going to state.

Weak Lang's Conjecture. *Let X be a variety of general type defined over a number field K. Then the set of K-rational points of X is not dense in X with respect to the Zariski topology.*

Weak Lang's Conjecture in dimension one is equivalent to Faltings' Theorem. This is because dimension one varieties of general type are exactly curves of genus $g \geq 2$ and a subset S of a curve which is not dense with respect to the Zariski topology is a finite set. Hence Lang's Conjectures try to generalize Faltings' Theorem to varieties of general type of higher dimension.

Strong Lang's Conjecture. *Let X be a variety of general type defined over a number field K. Then there exists a proper Zariski closed subvariety Ξ in X such that for any number field L containing K, all of the L-rational points of X are contained in Ξ, with the exception of finitely many of them.*

The key theorem which, together with the Lang's Conjectures, implies the Bound Conjectures is known as the Correlation Theorem.

Correlation Theorem. *Let $X \to B$ be a proper morphism of varieties over a number field K whose general fiber is a curve of genus at least 2. Then for n big enough, the n-th fiber product of X over B admits a dominant rational map h to a positive dimensional variety of general type W, and both W and h are defined over K.*

Proof. See [CHM97]. □

Assuming the Weak Lang's Conjecture, Pacelli proved the following result concerning $B(K, g)$.

Theorem 9. *Assume that the Weak Lang's Conjecture is true. Let $g \geq 2$ and $d \geq 1$ be integers, and let K be a number field. Then there exists an integer $B_K(d, g)$ such that for any field extension $K \subseteq L$ of degree d and for any genus g curve $\mathscr{C}$ over L:*

$$|\mathscr{C}(L)| \leq B_K(d, g).$$

Proof. See [Pac96]. □

This theorem generalizes Abramovich's one with $d = 2$ (see [Abr95]).

What should we do with these two numbers $B(K, g)$ and $N(g)$? A good idea is to find lower bounds for $B(K, g)$ and $N(g)$. This is mostly for two reasons: first of all, if we are able to increase indefinitely the lower bounds in some particular case, the conjecture will be proven to be false. Secondly, if the conjectures are true, it's interesting to know the exact value of $B(K, g)$ and $N(g)$. Therefore we explain Mestre's idea which allows to establish:

$$B(K, g) \geq 8g + 12, \ B(\mathbb{Q}(\xi), g) \geq 16(g + 1), \ N(g) \geq 16(g + 1),$$

where K is a number field, $g \geq 2$ and ξ is a primitive $(2g + 2)$-th root of 1.

Proposition 15. *Given $n \in \mathbb{N}^*$, there exist distinct $a_1, \ldots, a_{2n} \in K$ such that $P(x) := \prod_{i=1}^{2n}(x - a_i)$ can be written as $P = Q^2 - R$ where $Q, R \in K[x]$, Q is monic, $\deg(Q) = n$, $\deg(R) = n - 1$ and, if $n > 1$, R has distinct roots in $\overline{K}$. In addition, $(a_1, \ldots, a_{2n})$ can be chosen in a Zariski dense open subset of $\mathbb{A}_K^{2n}$, that we call $\mathbb{U}_K^{2n}$.*

That said, with the same notations, if K is a number field, $g \geq 2$ and $n := 2g + 3$, the hyperelliptic curve:

$$y^2 = R(x),$$

has at least $(a_j, \pm Q(a_j))$, $j = 1, \ldots, 4g + 6$, as K-rational points, hence $B(K, g) \geq 8g + 12$. Moreover, since $(a_1, \ldots, a_{2n})$ can be chosen in a Zariski dense open subset, we can exhibit infinitely many isomorphism classes of hyperelliptic curves with at least $8g + 12$ K-rational points, and this means that $N(g) \geq 8g + 12$. With analogous ideas, one can prove the remaining inequalities.
A different method due to Brumer will lead to (a similar result):

$$B(\mathbb{Q}(\zeta), g) \geq 16(g + 1), \ N(g) \geq 16(g + 1),$$

where $g \geq 2$ and ζ is a primitive $(g + 1)$-th root of 1. Brumer's idea is to consider the family $\{\mathscr{C}_{a,b}\}$ of hyperelliptic curves associated to the equations:

$$y^2 = a(x^n + 1)^2 + bx^n,$$

with $a, b \in \mathbb{Q}$ and $ab \neq 0$. The automorphisms:

$$\iota \colon (x, y) \mapsto (x, -y),$$

$$\varphi \colon (x, y) \mapsto \left(\frac{1}{x}, \frac{y}{x^n}\right),$$

$$\psi_i \colon (x, y) \mapsto (\zeta^i x, y).$$

generates a subgroup G of $\mathrm{Aut}(\mathscr{C}_{a,b})$ of order $4(g + 1)$. It's possible then to find four points $(x_1, y_1), \ldots, (x_4, y_4) \in \mathbb{Q}^2$ and two rational numbers a, b with $ab \neq 0$ such that the curve $\mathscr{C}_{a,b}$ passes through $(x_1, y_1), \ldots, (x_4, y_4)$ and their orbits under the action of G are disjoint, hence $B(\mathbb{Q}(\zeta), g) \geq 16(g+1)$. Moreover, $N(g) \geq 16(g+1)$, since in this way we can obtain infinitely many isomorphism classes of curves.
The last method we study allows to find a (hyperelliptic) curve $\mathscr{C}$ defined over $\mathbb{Q}$ over the rational surface $\mathbb{P}^1 \times \mathbb{P}^1$ such that:

$$|\mathscr{C}(\mathbb{Q})| \geq 2|G|(3\rho_G(g) - 1),$$

where $g \geq 2$, G is a finite subgroup of $\mathrm{PGL}(2, \mathbb{Q})$ and $\rho_G(g)$ is the dimension of the vector subspace of homogeneous polynomial of degree $g+1$ in two variables which are invariant under the action of G. So, the matter now is to understand who are the possible finite subgroups G and then which group makes the quantity $2|G|(3\rho_G(g)-1)$ bigger for a fixed g.

Theorem 10. *In* $\mathrm{PGL}(2, \mathbb{Q})$ *every finite subgroup is isomorphic to one of the following groups:*

$$\{0\}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, \mathbb{Z}/4\mathbb{Z}, (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}), \mathbb{Z}/6\mathbb{Z}, S_3, D_4, D_6.$$

Moreover, for each group G in the list there exists a subgroup of $\mathrm{PGL}(2, \mathbb{Q})$ *which is isomorphic to G.*

We prove this theorem starting from Klein's classification of finite subgroups of $\mathrm{PGL}(2, \mathbb{C})$ (see [Kle13]) and taking some results from [Dre04].
In conclusion, the best we can obtain with this method is:

$$B(\mathbb{Q}, g) \geq \begin{cases} 6g+12 & \text{if } g \equiv 2 (\mathrm{mod}\ 6), \\ 6g+10 & \text{if } g \text{ is even and } g \not\equiv 2 (\mathrm{mod}\ 6), \text{ or } g \equiv 3 (\mathrm{mod}\ 6), \\ 6g+18 & \text{if } g \equiv 1 (\mathrm{mod}\ 6), \\ 6g+30 & \text{if } g \equiv 5 (\mathrm{mod}\ 6), \\ 6g+26 & \text{if } g \equiv 1 (\mathrm{mod}\ 8), \\ 6g+14 & \text{if } g \equiv 3 (\mathrm{mod}\ 8), \\ 6g+38 & \text{if } g \equiv 7 (\mathrm{mod}\ 8). \end{cases}$$

which improves previous methods for $g = 5, 7$.
The bounds we found for $B(K, g)$ and $N(g)$ are not the best for some values of g. The strength of our argument is that we were able to provide examples of curves with many rational points for every $g \geq 2$. However, one can concentrate on a particular g. For example, in the case $g = 2$ the best lower bound for $B(\mathbb{Q}, 2)$ is 588 and it was established by L. Kulesz with the hyperelliptic curve:

$$y^2 = 278271081x^2(x^2-9)^2 - 229833600(x^2-1)^2.$$

As far as $N(2)$ is concerned, the record is $N(2) \geq 128$ (see [CHM95, Proposition 4.1]).

As conclusion, assuming Lang's Conjecture and therefore the existence of $B(K, g)$ and $N(g)$, we make some considerations. It's clear that for fixed

$N \in \mathbb{N}$, we can find a number field K and a curve $\mathscr{C}$ over K such that $|\mathscr{C}(K)| > N$. However, it can be interesting to find a way to exhibit a number field K and a curve $\mathscr{C}$ over K with arbitrarily many K-rational points in such a way that K is as "small" as possible. Roughly speaking, we would like to economize on the base field K. The idea that we use is that we can find an arbitrary long (but finite) succession of consecutive natural numbers such that no one of these is a prime number.

Proposition 16. *For any genus $g \geq 2$ and $N \in \mathbb{N}$, there exists a number field $\widetilde{K}$ and a curve $\mathscr{C}$ over $\widetilde{K}$ such that:*

$$|\mathscr{C}(\widetilde{K})| > N.$$

In particular, if $N := N(g)$, $N(g) < B(\widetilde{K}, g)$.

In the proof, $\widetilde{K}$ will be $\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n})$, where $p_1, \ldots, p_n$ are the prime numbers smaller than $M! + 2$ and $M \in \mathbb{N}$ is such that $\prod_{i=N}^{2g+1+N} i \leq M! + M$. The curve with at least N $\widetilde{K}$-rational points is $y^2 = (x-1)\ldots(x-2g-2)$. Last proposition regards the number of isomorphism classes of genus g curves over a number field K with more than $N(g)$ K-rational points.

Definition 11. Let K be a number field and let $g \geq 2$. Define $e(K, g)$ to be the number of K-isomorphism classes of curves over K with at least $N(g) + 1$ K-rational points. This number exists if the Universal Generic Bound Conjecture is true.

We prove the following result:

Proposition 17. *Fixed $g \geq 2$, there exists a succession $K_0 \subseteq K_1 \subseteq K_2 \subseteq ...$ of number fields such that:*

$$\lim_{m \to \infty} e(K_m, g) = \infty.$$

Bibliography

[Abr95] D. Abramovich. *Uniformité des points rationnels des courbes algébriques sur les extensions quadratiques et cubiques*, C.R. Acad. Sci. Paris, t. 321, Série I, p. 755-758, 1995.

[AM69] M. F. Atiyah, I. G. MacDonald. *Introduction to Commutative Algebra*, Addison-Wesley Series in Mathematics, 1969.

[Cap95] L. Caporaso. *Counting rational points on algebraic curves*, Rend. Sem. Mat. Politecnico dell'Un. di Torino, Vol. 53,3 (1995) Number theory.

[CHM95] L. Caporaso, J. Harris, B. Mazur. *How many rational points can a curve have?*, The Moduli space of curves, Progress in mathematics n. 129, Birkhäuser (1995) 13-32.

[CHM97] L. Caporaso, J. Harris, B. Mazur. *Uniformity of rational points*, Journal of American Mathematics Society, Vol.10, N.1, Jan.97, 1-35.

[Dav83] H. Davenport. *The Higher Arithmetic: an Introduction to the Theory of Numbers*, Dover, 1983.

[Dre04] G. P. Dresden. *There Are Only Nine Finite Groups of Fractional Linear Transformations with Integer Coefficients*, Mathematics Magazine, Vol. 77, No. 3 (Jun., 2004), pp. 211-218, published by: Mathematical Association of America.

[Har77] R. Hartshorne. *Algebraic Geometry*, Springer-Verlag, New York, 1977, Graduate Texts in Mathematics, 52.

[HiSi00] M. Hindry, J. H. Silverman. *Diophantine Geometry: An Introduction*, Springer, 2000, Graduate Text in Mathematics, 201.

[Kle13] F. Klein. *Lectures on the icosahedron and the solution of equations of the fifth degree*. Kegan Paul, Trench, Trubner and Co., London (1913). Reprinted by Dover Publications Inc., New York, N.Y., 1956.

[Laz04] R. Lazarsfeld. *Positivity in Algebraic Geometry, Volume 1.* Springer, A Series of Modern Surveys in Mathematics, Vol. 48.

[Liu02] Quing Liu. *Algebraic Geometry and Arithmetic Curves*, Oxford mathematics, 2002, Oxford Graduate Texts in Mathematics, 6.

[Mil11] J. S. Milne. *Algebraic Number Theory*, Course notes, v3.03, May 29, 2011. http://www.jmilne.org/math/CourseNotes/ANT.pdf

[Pac96] P. Pacelli. *Uniform boundedness for rational points*, Ph.D. Thesis, Boston University, 1996.

[RS02] K. Rubin, A. Silverberg. *Ranks of Elliptic Curves*, Bulletin of the American Mathematical Society, Volume 39, Number 4, Pages 455-474, July8, 2002.

[Sil09] J. H. Silverman. *The Arithmetic of Elliptic Curves*, second edition, Springer, 2009, Graduate Texts in Mathematics, 106.