DIOPHANTINE GEOMETRY

ELISA LORENZO GARCÍA

Contents

We are mainly following [2] and [1].

1. Absolute values on number fields and the product formula

This is extracted from [2, Section B1] and [1, Sections 1.2-1.4].

The traditional way to describe the size of an algebraic number is through the use of absolute values.

Recall: algebraic number, number field, Galois closure, Galois group. Examples: $\mathbb{Q}(i, \sqrt{3})$, $\mathbb{Q}(\alpha)$ with $\alpha^3 + \alpha^2 - 1 = 0$ that it is not Galois, you need to add $\sqrt{-23}$ to get the Galois closure.

Definition 1.1. An absolute value on a field K is a function $\mid \cdot \mid : K \to [0, \infty)$ such that

i) $\mid x \mid = 0$ if and only if $x = 0$ (non degenerate)
ii) $\mid xy \mid = \mid x \mid\mid y \mid$ (multiplicative)
iii) $\mid x + y \mid \leq \mid x \mid + \mid y \mid$ (triangle inequality)

It is said to be nonarchimedean if it satisfies:

iv) $\mid x + y \mid \leq \max\{\mid x \mid, \mid y \mid\}$ (ultrametric inequality)

Example 1.2. Let us consider $K = \mathbb{Q}$:

- Archimedean absolute value on $\mathbb{Q}$: $\mid x \mid_\infty = \max\{x, -x\}$.
- Nonarchimedean p-adic absolute value on $\mathbb{Q}$: $x = p^{\mathrm{ord}_p(x)} \frac{a}{b}$ with $a, b \in \mathbb{Z}$ and $p \nmid ab$. If $x = 0$ we set $\mathrm{ord}_p(x) = \infty$. $\mid x \mid_p = p^{-\mathrm{ord}_p(x)}$.

The number x is p-adically small if it is divisible by a large power of p. ord_p is the p-adic valuation on $\mathbb{Q}$.

Definition 1.3. Two absolute values are equivalent if they define the same topology, i.e., if there exists $s \in \mathbb{R}_{>0}$ such that $\mid x \mid_2 = \mid x \mid_1^s$.

Definition 1.4. M_K is the set of absolute values up to equivalence, M_K^∞ the archimedean ones, and M_K^0 the nonarchimedean ones.

Given an absolute value $|\cdot|\in M_K$ we can define a valuation (or place) $v(x) = -\log |x|$ and we write $|\cdot|$ as $|\cdot|_v$ and even $v \in M_K$.

Definition 1.5. Let K'/K be a field extension. Let $v \in M_K$ and $w \in M_{K'}$. We say that $w \mid v$ if $w|_K = v$. If K is a number field we say that v is a p-adic valuation if $v|_{\mathbb{Q}} = p$.

Definition 1.6. A completion of K with respect to the place v is an extension field K_v with a place w such that:

i) $w \mid v$.
ii) the topology of K_v induced by w is complete (all Cauchy sequences converge).
iii) $K \subseteq K_v$ is dense.

By abuse of notation we denote w by v.

Theorem 1.7. *The completion exists and it is unique up to isometric isomorphism.*

Proof. (ideas) As in the construction of $\mathbb{R}$ from $\mathbb{Q}$. Take all the Cauchy series and consider then equivalent if their difference converges. □

Theorem 1.8. *(Ostrowski, several references in* [1]*) The only complete archimedean fields are $\mathbb{R}$ and $\mathbb{C}$.*

Corollary 1.9. *$\mathbb{Q}$ has a unique archimedean absolute value.*

Example 1.10. $\mathbb{Q}_3$ is the completion of $\mathbb{Q}$ with respect to the 3-adic valuation. $x = \sum_{n\geq n_0}^{\infty} x_n 3^n \in \mathbb{Q}_3$ with $x_n \in \{0,1,2\}$ can be seen as the Cauchy sequence $\{X_N\}$ with $X_N = \sum_{n\geq n_0}^{N} x_n 3^n \in \mathbb{Q}$. For instance: $\frac{1}{5} = ...121012102_3$

Proposition 1.11. *Let $K/\mathbb{Q}$ be a number field of degree $n = r_1 + 2r_2$ with $\{\rho_1, ..., \rho_{r_1}\}$ real embeddings and $\{\tau_1, \bar{\tau}_1, ..., \tau_{r_2}, \bar{\tau}_{r_2}\}$ complex embeddings. Then there is a bijection:*

$$\{\rho_1, ..., \rho_{r_1}, \tau_1, \tau_2, ..., \tau_{r_2}\} \leftrightarrow M_K^{\infty},$$

where $|x|_\sigma = |\sigma(x)|_\infty$. Let $(p) = \mathfrak{p}_1^{e_1} ... \mathfrak{p}_r^{e_r}$ be the factorization of the prime ideal (p) in the maximal order of K. Then there is a bijection

$$\{\mathfrak{p}_1, ..., \mathfrak{p}_r\} \leftrightarrow \{p - adic\ absolute\ values\ on\ K\},$$

where $|x|_{\mathfrak{p}} = p^{-\operatorname{ord}_{\mathfrak{p}}(x)/e_{\mathfrak{p}}}$.

The ring of integers of a number field may be characterized using absolute values:

$$\mathcal{O}_K = \{x \in K : |x|_v \leq 1 \text{ for all } v \in M_K^0\}. \tag{1.1}$$

Proposition 1.12. *Let $L = K(\alpha)$ be a finite extension. Let $f(t)$ the minimal polynomial of α and*

$$f(t) = f_1^{k_1}(t) ... f_r^{k_r}(t)$$

its factorization in $K_v[t]$. Then the homomorphisms

$$L \to K_j := K_v[t]/(f_j(t))$$

are injective. Moreover, K_j is the completion of L with respect to the only absolute value of K_j extending this of K_v. The absolute values corresponding to different j's are different and all appear in this way.

Proof. (ideas) verify the statements, see Proposition 1.3.1 in [1]. □

Corollary 1.13. *(Degree formula) Let L/K be a finite separable extension, then*

$$\sum_{w|v} [L_w : K_v] = [L : K].$$

Proof. By the primitive element theorem $L = K(\alpha)$ and we apply Proposition1.12. $\square$

Let K be a number field and $v \in M_K$, the local degree of v is $n_v = [K_v : \mathbb{Q}_v]$. The normalized absolute value is $|| \ x \ ||_v = | \ x \ |_v^{n_v}$.

Example 1.14. Take $K = \mathbb{Q}$, then $\prod_{v \in M_{\mathbb{Q}}} | \ x \ |_v = 1$.

Proposition 1.15. *(Product formula) Let K be a number field (in a slightly more general framework also works) and be $x \in K^*$. Then $\prod_{v \in M_K} || \ x \ ||_v = 1$.*

Proof. Assume the result over $\mathbb{Q}$. Then

$$\prod_{v \in M_K} || \ x \ ||_v = \prod_{v_0 \in M_{\mathbb{Q}}} \prod_{v | v_0} || \ x \ ||_v = \prod_{v_0 \in M_{\mathbb{Q}}} || \ \mathrm{N}_{K/\mathbb{Q}}(x) \ ||_{v_0} = 1.$$

$\square$

Example 1.16. Let $K = \mathbb{Q}(i)$, then $M_K^\infty = \{\tau\}$ with $| \ x \ |_\tau = (x\bar{x})^{1/2}$ and $||x||_\tau = |x|_\tau^2 = N_{\mathbb{Q}(i)/\mathbb{Q}}(x) = x\bar{x}$. Let $p \equiv 3 \bmod 4$, then p is still prime in K and $| \ x \ |_p = | \ \mathrm{N}(x) \ |_p^{1/2}$, where the first absolute value is in K and the second in $\mathbb{Q}$. We have $||x||_p = |x|_p^2$. If $p \equiv 1 \bmod 4$, then $p = \mathfrak{p}\bar{\mathfrak{p}}$ and $| \ x \ |_{\mathfrak{p}} = p^{-\operatorname{ord}_{\mathfrak{p}}(x)}$ and $||x||_p = |x|_p$. Finally, $(2) = (1+i)^2$ and $| \ x \ |_{1+i} = 2^{-\operatorname{ord}_{(1+i)}(x)/2}$ and $||x||_{1+i} = |x|_{1+i}^2 = ||N(x)||_2$. For $x = 2 + i$ all normalized absolute values are 1 except $||x||_{2+i} = 5^{-1}$ and $||x||_\tau = x\bar{x} = 5$ and the product formula holds.

2. Heights in projective spaces

This is extracted from [2, Section B2] and [1, Section 1.5].

Let $P \in \mathbb{P}^n(\mathbb{Q}) = \{(x_0, x_1, ..., x_n) \in \mathbb{Q}^{n+1}\}/\sim$[1], it can be written in the form $P = (x_0, x_1, ..., x_n)$ with $x_i \in \mathbb{Z}$ and $\gcd((x_0, x_1, ..., x_n) = 1$. We define the height of P as

$$H(P) = \max\{|x_0|, ..., |x_n|\}.$$

Definition 2.1. Let K be a number field and $P = (x_0, x_1, ..., x_n) \in \mathbb{P}^n(K)$. The (multiplicative) height and the logarithmic height are defined as:

$$H_K(P) = \prod_{v \in M_K} \max\{||x_0||_v, ..., ||x_n||_v\}, \text{ and}$$

$$h_K(P) = \log H_K(P) = \sum_{v \in M_K} -n_v \min\{v(x_0), ..., v(x_n)\}.$$

Lemma 2.2. *Let K be a number field and $P \in \mathbb{P}^n(K)$. Then*

- *$H_K(P)$ is independent of the choice of homogeneous coordinates.*
- *$H_K(P) \geq 1$ for all $P \in \mathbb{P}^n(K)$.*
- *Let K' be a finite extension of K, then $H_{K'}(P) = H_K(P)^{[K':K]}$.*

Proof. Write $P = (cx_0, ..., cx_n)$. Then

$$\prod_{v \in M_K} \max\{||cx_0||_v, ..., ||cx_n||_v\} = \prod_{v \in M_K} ||c||_v \prod_{v \in M_K} \max\{||x_0||_v, ..., ||x_n||_v\} =$$

$$= \prod_{v \in M_K} \max\{||x_0||_v, ..., ||x_n||_v\}.$$

We can make one coordinate equal to 1, this implies the second item. The third one is a consequence of the degree formula. $\square$

[1]Two such points are equivalent if the coordinates of one are a multiple of the coordinates of the other.

Definition 2.3. The absolute heights in $\mathbb{P}^n$ are defined as:

$$H(P) = H_K(P)^{1/[K:\mathbb{Q}]} \text{ and } h(P) = \log H(P) = \frac{1}{[K:\mathbb{Q}]} h_K(P).$$

We can see elements $\alpha \in K$ as elements of $\mathbb{P}^1$ as $(\alpha, 1)$ and compute the corresponding heights.

Example 2.4. Let $P = (1, 3+\sqrt{3}, 4, 1+i)$, then $\prod_{v|\infty} \max\{||x_i||_v\} = 4^2(3+\sqrt{3})^2$, and $\prod_{v|p} \max\{||x_i||_v\} = 1$. Hence, $H_K(P) = 4^2(3+\sqrt{3})^2$, and $H(P) = 2\sqrt{3+\sqrt{3}}$. Check it with Magma!! Use `HeightOnAmbient(P);`. Go to `http://magma.maths.usyd.edu.au/calc/`.

Proposition 2.5. *$H(\sigma(P)) = H(P)$.*

Proof. We have isomorphisms $\sigma : K \to \sigma(K)$ and $\sigma : M_K \to M_{\sigma(K)}$. Then

$$H_{\sigma(K)}(\sigma(P)) = \prod_{w \in M_{\sigma(K)}} \max\{|\sigma(x_i)|_w\}^{n_w} = \prod_{v \in M_K} \max\{|\sigma(x_i)|_{\sigma(v)}\}^{n_{\sigma(v)}} =$$

$$\prod_{v \in M_K} \max\{|x_i|_v\}^{n_v} = H_K(P).$$

□

Theorem 2.6. *For any $B, D \geq 0$, the set*

$$\{P \in \mathbb{P}^n(\bar{\mathbb{Q}}) : H(P) \leq B \text{ and } [\mathbb{Q}(P) : \mathbb{Q}] \leq D\}$$

is finite.

Proof. Take $P = (x_0 : x_1 : ... : x_n)$ with some coordinate equal to 1. Then $\max\{||x_0||_v, ..., ||x_n||_v\} \geq \max\{||x_i||_v, 1\}$. Then $H(P) \geq H(x_i)$. We need to prove that for each $1 \leq d \leq D$, the set $\{x \in \bar{\mathbb{Q}} : H(x) \leq B \text{ and } [\mathbb{Q}(x) : \mathbb{Q}] = d\}$ is finite.

Let $x \in \bar{\mathbb{Q}}$ of degree d and $x_1, .., x_d$ its conjugates. Let its minimal polynomial bee $F_x(T) = \prod(T - x_i) = \sum(-1)^r s_r(x) T^{d-r}$.

$$|s_r(x)|_v = |\sum_{1 \leq i_1 \leq ... \leq i_r \leq d} x_{i_1} ... x_{i_r}|_v \leq c(v, r, d) \max_{1 \leq i_1 \leq ... \leq i_r \leq d} |x_{i_1} ... x_{i_r}|_v \leq c(v, r, d) \max_{1 \leq i \leq d} |x_i|_v^r.$$

Here $c(v, r, d) = \binom{d}{r} \leq 2^d$ if v is archimedean and $= 1$ if it is not. Then

$$\max\{|s_0|_v, ..., |s_d(x)|_v\} \leq c(v, d) \prod_{i=1}^{d} \max\{|x_i|_v, 1\}^d$$

where $c(v, d) = 2^d$ if v is archimedean and 1 otehrwise. Hence,

$$H(s_0(x), ..., s_d(x)) \leq 2^d \prod_{i=1}^{d} H(x_i)^d = 2^d H(x)^{d^2}.$$

Then for all $x \in \bar{\mathbb{Q}}$ with $H(x) \leq B$ and $[\mathbb{Q}(x) : \mathbb{Q}] = d$, it is a root of a polynomial with coefficients $H(s_0, ..., s_d) \leq 2^d B^{d^2}$. But there are only finitely many possibilities for those coefficients. □

Corollary 2.7. *(Kronecker's theorem) Let K be a number field, and let $P = (x_0, ..., x_n) \in \mathbb{P}^n(K)$. Fix i with $x_i \neq 0$. Then $H(P) = 1$ if and only if the x_j/x_i is a root of unity or 0 for all j.*

Proof. Given $P = (x_0, ..., x_n)$ we define $P^r = (x_0^r, ..., x_n^r)$. If $H(P) = 1$ then $H(P^r) = 1$, but there is only a finite number of points with height equal to 1, so the result follows. □

Corollary 2.8. *(Northcott's theorem) There are only finitely many algebraic integers of bounded degree and bounded height.*

Theorem 2.9. *Let $\phi = (f_0, ..., f_m) : \mathbb{P}^n \to \mathbb{P}^m$ be a rational map of degree d defined over $\bar{\mathbb{Q}}$. Let $Z \subset \mathbb{P}^n$ be the subset of common zeros of the f_i's. Notice that ϕ is defined on $\mathbb{P}^n/Z$.*

- *$h(\phi(P)) \leq dh(P) + O(1)$ for all $P \in \mathbb{P}^n(\bar{\mathbb{Q}})/Z$.*
- *Let X be a closed subvariety of $\mathbb{P}^n$ with $X \cap Z = \emptyset$. Then $h(\phi(P)) = dh(P) + O(1)$ for all $P \in X(\bar{\mathbb{Q}})$.*

Proof. We will prove only the first item, for the second we refer to Theorem B.2.5 in [2]. Notice that $f_i = \sum_{|e|=d} a_{i,e} x^e$ has $\binom{n+d}{n}$ terms. Write $|P|_v = \max\{|x_j|_v\}$, $|f|_v = \max\{|a_e|_v\}$ and $\epsilon_v(r) = r$ if v is archimedean and 1 if it is not. Then $|a_1 + ... + a_r|_v \leq \epsilon_v(r) \max\{|a_i|_v\}$.

$$|f_i(P)|_v = |\sum_{|e|=d} a_{i,e} x^e|_v \leq \epsilon_v \binom{n+d}{n} \max |a_{i,e}|_v \max |x^e|_v \leq$$

$$\leq \epsilon_v \binom{n+d}{n} |f_i|_v \max |x_j|_v^d = \epsilon_v \binom{n+d}{n} |f_i|_v |P|_v^d.$$

We take the maximum over i, raise to the $n_v/[K : \mathbb{Q}]$ and multiply for all $v \in M_K$.

$$H_K(\phi(P)) \leq \binom{n+d}{n} H(\phi) H(P)^d,$$

where $H(\phi) = \prod_{v \in M_K} \max\{|f_0|_v, ..., |f_m|_v\}^{n_v/[K:\mathbb{Q}]}$. Taking logarithms

$$h(\phi(P)) \leq dh(P) + h(\phi) + \log \binom{n+d}{n}.$$

□

3. Some results on the geometry of curves and abelian varieties

For this section and really depending on your background I have different suggestions:

- You already know about curves, varieties and abelian varieties: feel free to skip this lecture.
- You a bit, but not that much: watch the video, it will be perfect to recall the concepts we need in the follow.
- You do not know that much: then maybe the video is not enough and you need to read more detailed material. Some suggestions: section A in [2], or if you only want to focus only on dimension one varieties (curves), see [3, Chapters 1, 2].

4. The Néron-Tate height on abelian varieties

This is extracted from [2, Section B3, B4, B5] and [1, Section 9].

Definition 4.1. Let $\phi : V \to \mathbb{P}^n$ be a morphism. The height on V relative to ϕ is $h_\phi(P) = h(\phi(P))$.

Theorem 4.2. *(Weil's Height Machine) Let K be a number field. For every smooth projective variety V/K there exists a map:*

$$h_V : \operatorname{Div}(V) \to \{functions\ V(\bar{K}) \to \mathbb{R}\}$$

with the following properties:

(1) *(Normalization) For all hyperplane H, $h_{\mathbb{P}^n,H}(P) = h(P) + O(1)$.*
(2) *(Functoriality) Let $\phi : V \to W$ be a morphism and $D \in \operatorname{Div}(W)$, then*

$$h_{V,\phi^* D}(P) = h_{W,D}(\phi(P)) + O(1).$$

(3) *(Additivity) $h_{V,D+E}(P) = h_{V,D}(P) + h_{V,E}(P) + O(1)$.*
(4) *(Linear equivalence) If $D \sim E$, then $h_{V,D}(P) = h_{V,E}(P) + O(1)$.*
(5) *(Positivity) If $D > 0$ and B is the base locus of the linear system $|D|$, then $h_{V,D}(P) \geq O(1)$ for all $P \in V \setminus B$.*
(6) *(Algebraic equivalence) D ample and E alg. eq. to 0, then*

$$\lim_{h_{V,D}(P)\to\infty} \frac{h_{V,E}(P)}{h_{V,D}(P)} = 0.$$

(7) *(Finiteness) D ample, K'/K finite, B fixed, then $\{P \in V(K') : h_{V,D}(P) \leq B\}$ is finite.*
(8) *(Uniqueness) The height functions $h_{V,D}$ are determined up to $O(1)$.*

Proof. The construction: if $\mathcal{L}(D)$ has no base point, we chose $\phi_D : V \to \mathbb{P}^n$ associated to D and define $h_{V,D}(P) = h(\phi_D(P))$ for all $P \in V(\bar{K})$. For very other divisor D we write it as $D = D_1 - D_2$ with D_i with linear systems not having base points, we can even ask for them to be ample. Then $h_{V,D}(P) := h_{V,D_1}(P) - h_{V,D_2}(P)$.

One needs to check that up to $O(1)$, the height function $h_{V,D}$ is independent of the morphism ϕ_D. See Theorem B.3.1 in [2].

The properties are left as an exercise. □

Remark 4.3. The constants are effective.

Corollary 4.4. *Let A/K be an abelian variety over a number field. Let D be a divisor and m an integer.*

(1) *$h_{A,D}([m]P) = \frac{m^2+m}{2} h_{A,D}(P) + \frac{m^2-m}{2} h_{A,D}(-P) + O(1)$.*
(2) *If D is symmetric ($[-1]^* D \sim D$), then $h_{A,D}(P+Q) + h_{A,D}(P-Q) = 2h_{A,D}(P) + 2h_{A,D}(Q) + O(1)$.*
(3) *If D is antisymmetric ($[-1]^* D \sim -D$), then $h_{A,D}(P+Q) = h_{A,D}(P) + h_{A,D}(Q) + O(1)$.*

Proof. Just notice that $[m]^* D \sim \frac{m^2+m}{2} D + \frac{m^2-m}{2}[-1]^* D$, and that $h_{A,D} \circ [-1] = \pm h_{A,D} + O(1)$ accordingly to D be symmetric or antisymmetric. □

Proposition 4.5. *Let C/K be a smooth projective curve.*

- *Let D, E be divisors with $\deg(D) \geq 1$. Then*

$$\lim_{h_D(P)\to\infty} \frac{h_D(P)}{h_E(P)} = \frac{\deg(E)}{\deg(D)}.$$

- *Let $f, g \in K(C)$ with f non-constant, then*

$$\lim_{h(f(P))\to\infty} \frac{h(g(P))}{h(f(P))} = \frac{\deg(g)}{\deg(f)}.$$

Proof. Let $d = \deg(D)$ and $e = \deg(E)$, Make $A_n = n(eD - dE) + D$ who is ample for having degree greater or equal than 1. The positivity property of the Weil machine gives a constant:

$$-\kappa(D,E,n) \leq h_{A_n}(P) = n(eh_D(P) - dh_E(P)) + h_D(P),$$

that can be rewritten as

$$-\frac{\kappa(D,E,n)}{ndh_D(P)} - \frac{1}{nd} \leq \frac{e}{d} - \frac{h_E(P)}{h_D(P)} \leq \frac{\kappa(D,E,n)}{ndh_D(P)} + \frac{1}{nd},$$

and by taking limits the first point holds.

For the second one, take $\mathrm{div}(f) = D - D'$ and $\mathrm{div}(g) = E - E'$. On the other hand $h_D = h \circ f + O(1)$. Then,

$$\lim_{h(f(P))\to\infty} \frac{h(g(P))}{h(f(P))} = \lim_{h_D(P)\to\infty} \frac{h_D(P) + O(1)}{h_E(P) + O(1)} = \frac{\deg(E)}{\deg(D)} = \frac{\deg(g)}{\deg(f)}.$$

□

Theorem 4.6. *(Néron-Tate) Let V/K be a smooth variety defined over a number field, let $D \in \mathrm{Div}(V)$ and $\phi : V \to V$ be a morphism such that $\phi^* D \sim \alpha D$ for some $\alpha > 1$. Then there is a unique function (the canonical height on V relative to ϕ and D), $\hat{h}_{V,\phi,D} : V(\bar{K}) \to \mathbb{R}$ such that:*

- $\hat{h}_{V,\phi,D}(P) = h_{V,D}(P) + O(1)$.
- $\hat{h}_{V,\phi,D}(\phi(P)) = \alpha \hat{h}_{V,\phi,D}(P)$.

It only depends on the linear equivalence of D and it can be computed as:

$$\hat{h}_{V,\phi,D}(P) = \lim_{n\to\infty} \frac{1}{\alpha^n} h_{V,D}(\phi^n(P)).$$

Proof. Applying the height machinery to $\phi^* D \sim \alpha D$ we get that there is a constant C such that $|h_{V,D}(\phi(Q)) - \alpha h_{V,D}(Q)| \leq C$. The sequency $\alpha^{-n} h_{V,D}(\phi^n(P))$ converges because it is Cauchy:

$$|\alpha^{-n} h_{V,D}(\phi^n(P)) - \alpha^{-m} h_{V,D}(\phi^m(P))| = |\sum_{i=m+1}^{n} \alpha^{-i}(h_{V,D}(\phi^i(P)) - \alpha h_{V,D}(\phi^{i-1}(P)))| \leq$$

$$\sum_{i=m+1}^{n} \alpha^{-i} |h_{V,D}(\phi^i(P)) - \alpha h_{V,D}(\phi^{i-1}(P))| \leq \sum_{i=m+1}^{n} \alpha^{-i} C = \frac{\alpha^{-m} - \alpha^{-n}}{\alpha - 1} C.$$

If $m = 0$ and $n \to \infty$ we get the first property. The second comes from the definition. □

Let us take in Theorem 4.6 $V = A$ an abelian variety, $\phi = [2]$, D a symmetric divisor and $\alpha = 4$, then: the canonical height on A relative to D is such that:

1. $\hat{h}_{A,D}(P) = h_{A,D}(P) + O(1)$.
2. $\hat{h}_{A,D}([m]P) = m^2 \hat{h}_{A,D}(P)$
3. $\hat{h}_{A,D}(P+Q) + \hat{h}_{A,D}(P-Q) = 2\hat{h}_{A,D}(P) + 2\hat{h}_{A,D}(Q)$
4. $< P, Q >_D = \frac{\hat{h}_{A,D}(P+Q) - \hat{h}_{A,D}(P) - \hat{h}_{A,D}(Q)}{2}$ is bilinear.
5. It only depends on the linear equivalence of D.
6. $\hat{h}_{A,D}(P) \geq 0$ with equality if and only if P is of finite order.

Example 4.7. Let $E : y^2 = x^3 - x$ and $D = 3\infty$. $\mathcal{L}(D) = < 1, x, y >$. Then $h_{E,D}$ is the height on $\mathbb{P}^2$. $\phi = [2]$ and $\alpha = 4$.

$$\hat{h}_E(P) = \lim_{n\to\infty} \frac{1}{2^{2n}} h_E(2^n P).$$

Notice that $\hat{h}_E(2P) = 4\hat{h}_E(P)$. Let us take $P = (2, \sqrt{6}, 1)$, then $h_E(P) = \log\sqrt{6} = 0.8958...$. $2P = (300 : -35\sqrt{6} : 288)$ and $h_E(2P)/4 = \frac{1}{8}\log\frac{300^2}{6} = 1.20197$. Check it with Magma!! `NaiveHeight(P); Log(HeightOnAmbient(P)); Height(Q);`

5. The (Weak) Mordell-Weil theorem

We follow here Section $C.0$ in [2] and Section 8 in [4].

Theorem 5.1. *(Mordell-Weil) Let A be an abelian variety defined over a number field K. Then the group $A(K)$ of K-rational points of A is finitely generated.*

Using elementary group theory we can rephrase previous theorem by saying that there exist $P_1, ..., P_r \in A(K)$ such that:

$$A(K) = A(K)_{tors} \oplus \mathbb{Z}P_1 \oplus ... \oplus \mathbb{Z}P_r,$$

with $A(K)_{tors} \simeq (\mathbb{Z}/m_1\mathbb{Z}) \oplus ... \oplus (\mathbb{Z}/m_s\mathbb{Z})$ and $m_i \mid m_{i+1}$ and $s \leq 2\dim A$. The integer r is called the rank and $A(K)$ the Mordell-Weil group of A/K.

Theorem 5.2. *(Weak Mordell-Weil) Let A be an abelian variety defined over a number field K. Let $A(K)$ be the group of K-rational points of A, and let $m \geq 2$ be an integer. Then the group $A(K)/mA(K)$ is finite.*

Lemma 5.3. *(Descent lemma) Let G be an abelian group equipped with a quadratic form $q : G \to \mathbb{R}$[2] such that for all C the set $\{x \in G \mid q(x) \leq C\}$ is finite. Assume further that for some integer $m \geq 2$, the group G/mG is finite. Then G is finitely generated. More precisely, let $g_1, ..., g_s$ be a set of representatives for G/mG, and let $C_0 := \max_i q(g_i)$. Then G is generated by the finite set $\{x \in G \mid q(x) \leq C_0\}$.*

Proof. We can assume $q(x) \geq 0$. We set $|x| := \sqrt{q(x)}$, $c_0 := \max |g_i|$ and $S = \{x \in G : |x| \leq c_0\}$. Let $x_0 \in G$, si $x_0 \in S$ we are done, otherwise $|x_0| > c_0$ and $x_0 = g_i + mx_1$ for some $x_1 \in G$. The triangle inequality $m|x_1| = |x_0 - g_i| \leq |x_0| + |g_i| < 2|x_0|$. Since $m \geq 2$, we find that $|x_1| < |x_0|$. If $x_1 \in S$, then $x_0 \in \langle S \rangle$. Otherwise, $x_1 = g_j + mx_2$ and $|x_2| < |x_1|$. Continuing in this fashion $|x_0| > |x_1| > |x_2| > ...$ but G has only a finite number of elements of bounded size. □

Proof. (Theorem 5.2 implies Theorem 5.1) We take q as the the Néron-Tate height on $A(K)$ associated to an ample divisor on A. □

Remark 5.4.
(1) "descent"
(2) All the points of bounded height can be computed.
(3) The order of $A(K)/mA(K)$ can be effectively bounded, and hence the rank.

Theorem 5.5. *Let A be an abelian variety defined over a number field K, let v be a finite place of K at which A has good reduction. Let k be the residue field and let p be the characteristic. Then for any m with $p \nmid m$, the reduction map*

$$A[m](K) \to \bar{A}(k)$$

is injective.

I'm not following the proof in [2, Thm. C.1.4.] but the one suggested in the exercise C.9 from the same reference.

[2] i.e., satisfying $q(P+Q+R) - q(P+Q) - q(P+R) - q(Q+R) + q(P) + q(Q) + q(R) - q(0) = 0$, so the pairing $(q(P+Q) - q(P) - q(Q) + q(0))/2$ is bilinear.

Lemma 5.6. *(Hensel's) Let K be a p-adic field, i.e., the completion of a number field with respect to a nonarchimedean place, let R be the ring of integers of K, and let π be a uniformizer (a generator of the maximal ideal). Let $P \in R[x]$ and $x_0 \in R$ be an element satisfying $P(x_0) \equiv 0$ mod π and $P'(x_0) \neq 0$ mod π, then there exists a unique $x \in R$ such that $P(x) = 0$ and $x \equiv x_0$ mod π.*

Proof. We construct x as the limit of a sequence $x_0, x_1, x_2, ...$ such that $P(x_i) \equiv 0 \bmod \pi^{m+1}$ and $x_m \equiv x_{m-1} \bmod \pi^m$. Write $x_m = x_{m-1} + \pi^m y_m$ and $P(x_m) = \sum a_i(x_{m-1} + \pi^m y_m)^i \equiv \sum a_i(x_{m-1}^i + i\pi^m x_{m-1}^{i-1} y_m) \bmod \pi^m = P(x_m) + y_m P'(x_m)$. Moreover, $P'(x_{m-1}) \equiv P'(x_0) \neq 0 \bmod \pi$. □

Lemma 5.7. *(Hensel's lemma generalization) Let $P_1, ..., P_r \in R[x_1, ..., x_s]$ and $X_0 \in R^s$ be an element satisfying $P_i(X_0) \equiv 0$ mod π and such that the matrix $(\partial P_i/\partial x_j(X_0)$ mod $\pi)$ has rank r. Then there exists a $X \in R^s$ such that $P_i(X) = 0$ and $X \equiv X_0$ mod π.*

Proof. We construct X as the limit of a sequence $X_0, X_1, X_2, ...$ such that $P(X_i) \equiv 0 \bmod \pi^{m+1}$ and $x_m \equiv X_{m-1} \bmod \pi^m$. □

Proof. (of theorem 5.5) From the generalization of Hensel's Lemma we have that if A is a variety over K and $\bar{A}$ its reduction, given $\bar{P} \in \bar{A}(R/\pi)$ a non-singular point, there exists a point $P \in A(K)$ whose reduction is $\bar{P}$. Then $A[m] \to \bar{A}[m]$ is onto and hence an isomorphism. In particular, it is injective and the result in the theorem holds.

□

Theorem 5.8. *Let A be an abelian variety of dimension g defined over a number field K, and fix an integer $m \geq 2$. Suppose that the m-torsion of A is K-rational. Let S be a finite set of places of K that contains all places dividing m and all places of bad reduction of A. Assume further that the ring of S-integers $\mathcal{O}_{K,S}$ is principal. Then*

$$\operatorname{rank} A(K) \leq 2g \operatorname{rank} \mathcal{O}_{K,S}^* = 2g(r_1 + r_2 + |S| - 1).$$

Elliptic curve rank's records

Theorem 5.9. *(Mazur's Theorem) Let E be an elliptic curve, suppose that $E(\mathbb{Q})$ contains a point of finite order m. Then either $1 \leq m \leq 10$ or $m = 12$. More precisely, the set of points of finite order in $E(\mathbb{Q})$ forms a subgroup that has one of the following forms:*

(i) *A cyclic group of order N with $1 \leq N \leq 10$ or $N = 12$.*
(ii) *The product of a cyclic group of order two and a cyclic group of order $2N$ with $1 \leq N \leq 4$.*

Theorem 5.10. *(Lutz-Nagell) Let E be given by $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$. Let $P = (x, y) \in E(\mathbb{Q})$. Suppose P has finite order. Then $x, y \in \mathbb{Z}$. If $y \neq 0$ then $y^2 | 4A^3 + 27B^2$.*

Proof. (idea) If denominators the multiples do not have bounded height. □

Theorem 5.11. *Let E be given by $y^2 = (x-e_1)(x-e_2)(x-e_3)$ with $e_1, e_2, e_3 \in \mathbb{Z}$. The map $\phi : E(\mathbb{Q}) \to (\mathbb{Q}^\times/\mathbb{Q}^{\times 2}) \oplus (\mathbb{Q}^\times/\mathbb{Q}^{\times 2}) \oplus (\mathbb{Q}^\times/\mathbb{Q}^{\times 2})$ defined by $(x, y) \mapsto (x - e_1, x - e_2, x - e_3)$ when $y \neq 0$, $\infty \mapsto (1, 1, 1)$, $(e_1, 0) \mapsto ((e_1 - e_2)(e_1 - e_3), e_1 - e_2, e_1 - e_3)$, $(e_2, 0) \mapsto (e_2 - e_1, (e_2 - e_1)(e_2 - e_3), e_2 - e_3)$ and $(e_3, 0) \mapsto (e_3 - e_1, e_3 - e_2, (e_3 - e_1)(e_3 - e_2))$ is a homomorphism. The kernel of ϕ is $2E(\mathbb{Q})$.*

Example 5.12. Let us consider the elliptic curve $E : y^2 = x^3 - 25x$. We easily find the following rational points $\{\infty, (0, 0), (5, 0), (-5, 0), (-4, 6)\}$. We have that $2(-4, 6) = (\frac{41^2}{25^2}, -\frac{62279}{1728})$, so it is non-torsion. Lutz-Nagell theorem actually implies that $E(\mathbb{Q})_{tors} =$

$\{\infty, (0,0), (5,0), (-5,0)\} \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$. We will try to prove now that the rank is actually 1 and the nontorsion points are generated by $(-4,6)$. We have that $\phi(-4,6) = (-1,-1,1)$, $\phi(0,0) = (-1,-5,5)$, $\phi(5,0) = (5,2,10)$ and $\phi(-5,0) = (-5,-10,2)$. Hence, $\phi(-4,6)$ times the previous values correspond to some points: $(1,5,5), (-5,-2,10), (5,10,2)$. If we write $x = au^2$, $x - 5 = bv^2$ and $x + 5 = cw^2$ we have $\phi(x,y) = (a,b,c)$. Where $a,b,c \in \{\pm1, \pm2, \pm5, \pm10\}$. Since abc is a square we can forget about c. There are 64 possibilities for (a,b). We already got 8 of them. We will eliminate the other 56. If $a < 0$ it is also b, and if $a > 0$, also c and hence b. This eliminates 32 possibilities. One by one inspection of the remaining cases removes the other possibilities. Hence, $E(\mathbb{Q})/2E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus (\mathbb{Z}/2\mathbb{Z})^r$ with $r = 1$ since the image of ϕ has order 8. So, finally, $E(\mathbb{Q}) \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}$.

6. Falting's theorem and proof strategy

Theorem 6.1. *(Faltings) Let K be a number field, and let C/K be a curve of genus $g \geq 2$. Then $C(K)$ is finite.*

Conjectured by Mordell in 1922 and proved by Faltings in 1983: quite complicated techniques. Vojta came up with a proof based on Diophantine Geometry. Faltings simplified it and then Bombieri even more.

Theorem 6.2. *(Vojta's inequality) Let C/K be a smooth projective curve of genus $g \geq 2$ with $C(K) \neq \emptyset$. There are constants $\kappa_1 = \kappa_1(C)$ and $\kappa_2 = \kappa_2(g)$ such that if $z, w \in C(\bar{K})$ are two points satisfying $|z| \geq \kappa_1$ and $|w| \geq \kappa_2|z|$, then $\langle z, w\rangle \leq \frac{3}{4}|z||w|^3$.*

Proof. (Vojta's inequality implies Falting's Theorem) The kernel of $J(K) \to J(K) \otimes \mathbb{R}$ is the torsion group $J(K)_{tors}$ which is finite. In order to prove that $C(K)$ is finite we will prove that its image in $J(K) \to J(K) \otimes \mathbb{R}$ is finite. The bilinear form $\langle \cdot, \cdot \rangle$ makes $J(K) \to J(K) \otimes \mathbb{R}$ into a finite-dimensional Euclidean space. We define the angle: $\theta(x,y)$ as

$$cos\theta(x,y) = \frac{\langle x, y\rangle}{|x||y|},\ 0 \leq \theta(x,y) \leq \pi.$$

We define the cone $\Gamma_{x_0,\theta_0} = \{x \in J(K) \otimes \mathbb{R} \mid \theta(x, x_0) < \theta_0\}$. Assume $\#(\Gamma_{x_0,\theta_0} \cap C(K)) = \infty$, then there exists $z \in \Gamma_{x_0,\theta_0} \cap C(K)$ with $|z| \geq \kappa_1$ and then $w \in \Gamma_{x_0,\theta_0} \cap C(K)$ with $|w| \geq \kappa_2|z|$. Then $\langle z, w\rangle \leq \frac{3}{4}|z||w|$, or equivalently $\theta(z,w) \geq \pi/6$. But the angle between them is lees or equal than $2\theta_0$. Then $\Gamma_{x_0,\pi/12} \cap C(K)$ is finite for all $x_0 \in J(K) \to J(K) \otimes \mathbb{R}$. We can cover $J(K) \to J(K) \otimes \mathbb{R}$ with a finite number of this cones. So there is only a finite number of rational points. □

How to prove Vojta's inequality?

Some non-trivial lower and upper bounds for h_Ω are obtained as well as "small" enough equations for a positive divisor in the class of Ω. Roth's Lemma is also used.

Nice survey on computing rational points ... and another one!

7. Height Bounds and Height Conjectures

Most important unsolved problem in Diophantine Geometry.

Conjecture 7.1. (abc, Masser-Oesterlé) For all $\epsilon > 0$ there exists a constant $C_\epsilon > 0$ such that if $a, b, c \in \mathbb{Z}$ are coprime integers satisfying $a + b + c = 0$, then

$$\max\{|a|, |b|, |c|\} \leq C_\epsilon(\mathrm{rad}(abc))^{1+\epsilon}.$$

[3]Let Θ be the theta divisor in $J(C)$ who is ample and $|\cdot|$ the norm induce by $|x|^2 = \hat{h}_{J,\Theta}(x)$. Then we have the pairing $\langle x, y\rangle = \frac{1}{2}(|x+y|^2 - |x|^2 - |y|^2)$

Mochizumi 2012, Scholze and Stix 2018.

The abc-conjecture implies Falting's Theorem, asymptotic Fermat's Last Theorem, Szpiro conjecture, Lang conjecture, and many others.

Proof. (abc implies asymptotic Fermat's Last Theorem) Suppose $x^p + y^p + z^p = 0$ for nonzero coprime integers x, y, z. We may assume $|x| \le |y| \le |z|$. Then the abc conjecture implies that $|z|^p = \max\{|x|^p, |y|^p, |z|^p\} \le C_\epsilon(\mathrm{rad}(x^p y^p z^p))^{1+\epsilon} \le C_\epsilon |xyz|^{1+\epsilon} \le C_\epsilon |z|^{3+\epsilon}$. Hence, $p - 3(1+\epsilon) \le \log_2 C_\epsilon$. So there is not nontrivial solution for p big enough. □

Proof. (abc implies Falting's Theorem, Elkies) For any rational number $x \neq 0, 1$, let $N_0(x) = \prod_{\mathrm{ord}_p(x)>0} p$, $N_1(x) = \prod_{\mathrm{ord}_p(x-1)>0} p$, $N_\infty(x) = \prod_{\mathrm{ord}_p(x)<0} p$ and set $N(x) = N_0(x)N_1(x)N_\infty(x)$. We re-state the abc conjecture as $N(x) \ge C_\epsilon H(x)^{1-\epsilon}$.

Let $C/\mathbb{Q}$ be a curve of genus $g \ge 2$. Belyi's theorem says that there is a finite map $f : C \to \mathbb{P}^1$, say of degree d, that is ramified only above the three points $\{0, 1, \infty\}$. Letting $m := \#(f^{-1}(0, 1, \infty))$ and using Riemann-Hurwitz theorem we get

$$2g - 2 = -2d + (3d - m) = d - m.$$

We will take $\epsilon < (2g-2)/d$ in order to get $m/d < 1 - \epsilon$.

Let $D_0 = \sum_{\mathrm{ord}_Q(f)>0} \mathrm{ord}_Q(f)(Q)$ and $D_0' = \sum_{\mathrm{ord}_Q(f)>0}(Q)$. Let $d_0' = \deg(D_0')$. The divisor $d_0' D_0 - dD_0'$ has degree 0 so it is algebraically equivalent to 0 in C, and D_0 is ample, so $h_{D_0'} = \frac{d_0'}{d} h_{D_0} + O(\sqrt{h_{D_0}})$.

Let $P \in C(\mathbb{Q})$ with $f(P) \neq 0, \infty$, a prime occurs in the numerator of $f(P)$ if and only if it contributes to the height $H_{D_0'}(P)$, so $N_0(f(P)) \ll H_{D_0'}(P)$. Then $\log N_0(f(P)) \le \frac{d_0'}{d} h_{D_0}(P) + O(\sqrt{h_{D_0}(P)}) = \frac{d_0'}{d} h(f(P)) + O(\sqrt{h(f(P))})$. We repeat the argument with 1 and ∞. Noting that $d_0' + d_1' + d_\infty' = m$ yields:

$$\log N(f(P)) \le \frac{m}{d} h(f(P)) + O(\sqrt{h(f(P))}).$$

The abc conjecture tells us that for any $\epsilon > 0$ there is a constant c_ϵ such that $\log N(f(P)) \ge (1-\epsilon)h(f(P)) - c_\epsilon$. Then $(1 - \epsilon - \frac{m}{d})h(f(P)) \le c_\epsilon'$ and we get an upper bound for $h(P)$. So, there is a finite number of rational points and the bound is effective. □

The abc conjecture implies among others, the following conjectures and Roth's theorem:

Conjecture 7.2.

- (Szpiro) $\log |\Delta_{E/K}| \le (6+\epsilon)\log \mathcal{F}_{E,K} + C(K, \epsilon)$. [4]
- (Frey) $h_K(j_E) \le (6+\epsilon)\log \mathcal{F}_{E,K} + C(K, \epsilon)$
- (Lang) $\hat{h}(P) \ge c(K) \log \mathrm{N}_{K/\mathbb{Q}} \Delta_{E,K}$ for all non-torsion point $P \in E(K)$.

Theorem 7.3. *(Roth's theorem) For every algebraic number α and every $\epsilon > 0$, the inequality $\mid \frac{p}{q} - \alpha \mid \le \frac{1}{q^{2+\epsilon}}$ has only finitely many rational solutions $p/q \in \mathbb{Q}$.*

8. Exercises

Exercise 8.1. Prove the equivalence in Definition 1.3.

Exercise 8.2. Prove equation 1.1.

Exercise 8.3. Take $K = \mathbb{Q}$ and $S = \{2, 3, 5\}$ in **??**. Take $x_2 = x_3 = x_5 = 2$ and $\epsilon = 1/30$. Find an x as in the theorem.

Exercise 8.4. Prove that $\prod_{v|v_0} \| x \|_v = \| \mathrm{N}_{K/\mathbb{Q}}(x) \|_{v_0}$.

[4] The conductor is $\mathcal{F}_{E,K} = \prod_{p|\Delta_E} p^{\delta_p}$.

Exercise 8.5. Example with cubic field and Proposition 1.12.

Exercise 8.6. Add the details of the third point in Lemma 2.2.

Exercise 8.7. Let $a_1, ..., a_r$ algebraic numbers, then

$$h(a_1 + ... + a_r) \leq h(a_1) + ... + h(a_r) + \log r.$$

Exercise 8.8. Let $\phi : \mathbb{P}^2 \to \mathbb{P}^2$ be the rational map $\phi(x, y, z) = (x^2, y^2, xz)$. It is defined except at $(0, 0, 1)$.

- Take $P = (x, y, z)$ with $x, y, z \in \mathbb{Z}$ and $\gcd(x, y, z) = 1$. Prove that $h(\phi(P)) = \log \max\{|x^2|, |y^2|, |xz|\} - \log(\gcd(x, y^2))$.
- Show that there is no value c such that $h(\phi(P)) \geq 2h(P) - c$ holds for all P.
- More generally, prove that

$$\left\{ \frac{h(\phi(P))}{h(P)} : P \in \mathbb{P}^2(\mathbb{Q}) \, and \, h(P) \neq 0 \right\}$$

  is dense in $[1, 2]$.

Exercise 8.9. Let $a \in \mathbb{Z}$ be a nonzero square-free integer, and let $\phi : \mathbb{P}^1 \to \mathbb{P}^1$ be the map $\phi(x, y) = (2xy : x^2 + ay^2)$. Then $phi^*(0, 1) = (0, 1) + (1, 0) \sim 2(0, 1)$, so there is a canonical height associated to ϕ and the divisor $D = (0, 1)$. Find an explicit formula for this caninical height on $\mathbb{P}^1(\mathbb{Q})$. (Hint. This one of the few rational maps on $\mathbb{P}^1$ for which it is possible to find a simple closed formula for the iterates ϕ^n).

Exercise 8.10. Let G be an abelian group, let $m > 2$ an integer such that the quotient G/mG is finite, and let $x_1, ..., x_s \in G$ be a complete set of coset representatives for G/mG. Suppose that there are constants $A, B, C, D \geq 0$ with $A > B$ (depending on G, m, and $x_1, ..., x_s$) and a function $h : G \to \mathbb{R}$ with the property that $h(mx) \geq A(h(x) - C)$ and $h(x+x_i) \leq Bh(x)+D$ for all $x \in G$ and $1 \leq i \leq s$. Prove that the set $\{x \in G | h(x) \leq \frac{C+D}{A-B}\}$ generates the group G.

Exercise 8.11. Give a bound, or even better compute exactly, the quantity $\#A_{tors}(\mathbb{Q})$ for the following elliptic curves $A/\mathbb{Q}$:

1. $y^2 = x^3 - 1$.
2. $y^2 = x^3 - 4x$.
3. $y^2 = x^3 + 4x$.
4. $y^2 + 17xy - 1208 = x^3 - 60x^2$.

Exercise 8.12. Let C be a curve of genus g defined over $\mathbb{F}_p$, and let $J = \mathrm{Jac}(C)$ be its Jacobian variety. For each integer $m \geq 1$, let $N_m(C) = \#C(F_{p^m})$ and $N_m(J) = \#J(\mathbb{F}_{p^m})$. There exist algebraic integers a_i such that $N_m(C) = p^m + 1 - (a_1^m + ... + a_{2g}^m)$ for all $m \geq 1$. Furthermore, the polynomial $P(T) := \prod_{i=1}^{2g}(1 - a_i T)$ has integer coefficients and leading coefficient p^g, and it satisfies $P(T) = p^g T^{2g} P(1/pT)$. Then $N_1(J) = \#J(\mathbb{F}_p) = P(1) = \prod_{i=1}^{2g}(1 - a_i)$. Prove that the first g cardinalities $N_1(C), N_2(C), ..., N_g(C)$ for C determine the cardinality $N_1(J)$. In particular, prove that when $g = 2$, $N_1(J) = \frac{1}{2}(N_1(C)^2 + N_2(C)) - p$. Find a similar formula for $g = 3$. (Hint. Use Newton's formulas relating elementary symmetric polynomials to sums of powers.)
Let A be the Jacobian of the curve $y^2 = x^5 - x$. Compute the torsion subgroup $A_{tors}(\mathbb{Q})$. (Hint. Determine the rational 2- torsion points in $A(\mathbb{Q})$. Then use the first part and reduce modulo 3 and modulo 5 to prove that $A_{tors}(\mathbb{Q})$ is generated by its 2-torsion and possibly a single rational 3-torsion point. Finally, determine whether or not there is such a 3-torsion point.)

Exercise 8.13. For each of the following curves $C/\mathbb{Q}$, let $J = Jac(C)$ and find as accurate a bound as you can for the Mordell-Weil rank of J.

(1) Let $C : y^2 = x^5 - x$. Find bounds for $rank\, J(\mathbb{Q})$ and $rank\, J(\mathbb{Q}(i))$. (Hint. Use Theorem 5.8 and show that $rank\, J(\mathbb{Q}(i)) = 2rank\, J(\mathbb{Q})$.)
(2) Let $C : y^2 = x^6 - 1$, and let $\eta = e^{2\pi i/3}$ be a primitive cube root of unity. Find bounds for $rank J(\mathbb{Q})$ and $rank\, J(\mathbb{Q}(\eta))$. (Hint. Use Theorem 5.8 and show that $rank\, J(\mathbb{Q}(n)) = 2rank\, J(\mathbb{Q})$.)
(3) Let $C : y^2 = x(x^2 - 1)(x^2 - 4)$. Find a bound for rank $J(\mathbb{Q})$.

Exercise 8.14. Let $C/\mathbb{Q}$ be the smooth projective curve birational to the affine curve $2y^2 = x^4 - 17$. This exercise sketches a proof that $C(\mathbb{Q}_v) \neq \emptyset$ for all places v of $\mathbb{Q}$, yet $C(\mathbb{Q}) = \emptyset$.

(1) Show that C has good reduction at all primes except 2 and 17, and that $\bar{C}(\mathbb{F}_p)$ contains a nonsingular point for every prime p. Conclude that $C(\mathbb{Q}_p) \neq \emptyset$ for all primes p. (Hint. Use Weil's estimate (Exercise 8.12) to get points modulo p, and then Hensel's lemma to lift them to p-adic points.)
(2) Check that $C(\mathbb{R}) \neq 0$.
(3) Show that the two points at infinity on C are not rational over $\mathbb{Q}$.
(4) Suppose that $C(\mathbb{Q})$ contained a point. Prove that there would then exist coprime integers a, b, c satisfying $a^4 - 17b^4 = 2c^2$.
(5) Let a, b, c be as before. Prove that c is a square modulo 17. (Hint. For odd p dividing c, use the fact that p is a square modulo 17 if and only if 17 is a square modulo p.) Conclude that 2 is a 4th power modulo 17. This contradiction implies that $C(\mathbb{Q}) = \emptyset$.

Exercise 8.15. Let C be the smooth projective curve with affine open subset U defined by $y^2 + y = x^5$, let $P_0 = (0, 0)$, let $P_1 = (0, -1)$, and let P_∞ denote the point at infinity. Consider the Jacobian variety J of C and the natural embedding $j : C \to J$ defined by mapping P to the divisor class of $(P) - (P_\infty)$.

(1) It turns out that $rank\, J(\mathbb{Q}) = 0$. Assuming this, prove that $J(\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z}$.
(2) Prove that $j(P_1) = 4j(P_0)$.
(3) Prove that $2j(P_0), 3j(P_0) \notin j(C)$.
(4) Conclude that $C(\mathbb{Q}) = \{P_0, P_1, P_\infty\}$.
(5) Use this exercise to prove Fermat's Last Theorem for exponent p = 5. (Hint. Use the fact that if $A^5+D^5 = B^5$ with $D \neq 0$, then $(x, y) = (AB/D^2, A^5/D^5) \in C(\mathbb{Q})$.)

Exercise 8.16. (1) Let $E/\mathbb{Q}$ be an elliptic curve, let Δ_E and N_E be respectively the minimal discriminant and conductor of $E/\mathbb{Q}$, and write $1728\Delta_E = c_4^3 - c_6^2$ as usual. (See, e.g., [3, Section III.1]). Apply the abc conjecture to this equality (suitably divided by a gcd) to prove that $\max\{|Delta_E|, |c_4^3|, |c_6^2|\} \leq C_\epsilon N_E^{6+\epsilon}$. Deduce that the abc conjecture implies Szpiro's conjecture and Frey's conjecture.
(2) Let a, b, and c be coprime integers satisfying $a + b + c = 0$ and 24 divides abc. Consider the elliptic curve $E_{a,b,c} : y^2 = x(x - a)(x + b)$. Prove that $\Delta_{E_{a,b,c}} = (2^{-4}abc)^2$ and $j(E_{a,b,c}) = 2^8(a^2 + ab + b^2)/(abc)^2$.
(3) Prove that Frey's conjecture implies that the abc conjecture is true. (Hint. Apply Frey's conjecture to the curve $E_{a,b,c}$)
(4) Consider the elliptic the curve $E'_{a,b,c} : y^2 = x^3 - 2(a - b)x^2 + (a + b)^2x$. Prove that $E'_{a,b,c}$, has discriminant 2^8abc^4. Verify that the map $E_{a,b,c} \to E'_{a,b,c} : (x, y) \mapsto (y^2/x^2, -y(ab + x^2)/x^2)$, is an isogeny of degree 2. Use these facts to show that Szpiro's conjecture implies the abc conjecture with the weaker exponents $6/5 + \epsilon$.

References

[1] Bombieri, E., Gubler W. (2006). Heights in diophantine geometry, new Mathematical Monographs 4. Cambridge University Press.

[2] Hindry, M., Silverman, J. H. (2000). Diophantine geometry, Graduate Texts in Mathematics 201, Springer-Verlag, New York.

[3] Silverman, J. H. (1986). The Arithmetic of Elliptic curves, Graduate Texts in Mathematics, Springer-Verlag, New York.

[4] Washington, L.C. (2008). Elliptic curves, Number Theroy and Cryptography, Second Edition, Chapman and Hall/CRC.

Elisa Lorenzo García, Institut de Mathématiques, Université de Neuchâtel, rue Emile-Argand 11, 2000 Neuchâtel Switzerland.

Email address: elisa.lorenzo@unine.ch