How to compute regulators using Arakelov intersection theory

Raymond van Bommel

25 October 2018

These are notes for a talk given in the SFB/TRR45 Kolloquium held in Mainz, Germany, in the autumn of 2018. All readers are encouraged to e-mail to bommel@uni-mainz.de in case of errors, unclarities and other imperfections.

Abstract. In this talk, I will explain how one can efficiently compute regulators for Jacobians of plane curves, using Arakelov intersection theory. This talk is based on joint work with David Holmes and Steffen Müller, see [vBHM18], and is a continuation of [Hol12] and [Mül14].

Acknowledgements. Most of this work is done at the workshop *Arithmetic of curves*, held in Baskerville Hall in August 2018. We would like to thank the organisers and the staff for their support. We also thank Christian Neurohr for sharing his code to compute Abel-Jacobi maps and answering several questions, and Martin Bright for his help in one of the technical parts.

1 Regulator of a Jacobian

Let C be a smooth projective geometrically irreducible curve of genus g over $\mathbb{Q}$, let $J = \mathrm{Pic}^0(C)$ be its Jacobian, and let K be the Kummer variety associated to J, i.e. the variety obtained by identifying every point in J with its inverse.

Let $D \in \mathrm{Pic}^{g-1}(C)$ be a divisor class on C such that $2 \cdot D = K_C$, where K_C is the canonical divisor class. Then the image of the map

$$C^{g-1} \longrightarrow J : \quad (P_1, \ldots, P_g) \longmapsto [P_1 + \ldots + P_{g-1}] - D$$

is called a Theta divisor Θ of J. Its class depends on the choice of D, but the divisor class of 2Θ does not.

The divisor 2Θ is not very ample, but it descends to K, where it gives rise to a very ample divisor. This very ample divisor on its turn, gives rise to an embedding of K inside $\mathbb{P}^{2^g-1}$.

In this way, we can associate to each point $P \in J(\mathbb{Q})$ a point $(x_1 : \ldots : x_{2^g})$ inside $\mathbb{P}^{2^g-1}(\mathbb{Q})$. We will assume that $x_1, \ldots, x_{2^g} \in \mathbb{Z}$ are primitive (i.e. not sharing a non-trivial factor).

Definition 1. The *naive height of* P is

$$h^{\text{naive}}(P) = \log(\max(|x_1|, \ldots, |x_{2^g}|)).$$

The *Kummer height of* P is

$$h^{\text{Kum}}(P) = \lim_{n\to\infty} \frac{h^{\text{naive}}(nP)}{n^2}.$$

The *canonical (Kummer) height pairing on* J is defined by

$$\begin{array}{rccc} \langle -,- \rangle_{\text{Kum}} : & J(\mathbb{Q}) \times J(\mathbb{Q}) & \longrightarrow & \mathbb{R}_{\geq 0} \\ & (P, Q) & \longmapsto & \frac{1}{2}\left(h^{\text{Kum}}(P+Q) - h^{\text{Kum}}(P) - h^{\text{Kum}}(Q)\right) \end{array}$$

Remark 2. The height pairing can be extended to $\overline{\mathbb{Q}}$-points of J easily, but one has to take care of taking the right normalisation at the different places. This is beyond the scope of this talk. △

Remark 3. The height pairing on $J \times J$ is related to the Néron-Tate height pairing $\langle -,- \rangle_{\text{NT}}$ on $J \times J^\vee$ in the following way:

$$\langle -,- \rangle_{\text{Kum}} = \langle -,- \rangle_{\text{NT}} \circ (\text{id}_J, \theta),$$

where θ is the canonical principal polarisation $\theta \colon J \xrightarrow{\sim} J^\vee$, which naturally arises from J being a Jacobian. △

By the Mordell-Weil theorem the group $J(\mathbb{Q})$ is finitely generated, and hence of the shape $T \times \mathbb{Z}^r$, where T is a finite group and r is a non-negative integer, called the *algebraic rank* of J.

Definition 4. Let $x_1, \ldots, x_r$ be generators of $J(\mathbb{Q})/J(\mathbb{Q})_{\text{tors}}$. The *regulator* of J is defined as

$$\left|\det\left(\langle x_i, x_j \rangle_{\text{Kum}}\right)_{i,j=1}^{r}\right|.$$

Example 5. Let E be the elliptic curve given by

$$y^2 = x^3 + 3x.$$

Then the Jacobian J is canonically isomorphic to E, and the Kummer embedding is just the projection on the x-coordinate. Moreover, E has rank 1 and $E(\mathbb{Q})/E(\mathbb{Q})_{\text{tors}}$ is generated by the point $P = (3, 6)$. We can then compute

$$2 \cdot P = (\tfrac{1}{4}, \tfrac{7}{8}), \quad 3 \cdot P = (\tfrac{27}{121}, -\tfrac{1098}{1331}), \quad 4 \cdot P = (\tfrac{2209}{784}, -\tfrac{121871}{21952}), \quad \ldots$$

For example, we can compute $2000 \cdot P$, and then compute the logarithm of both the numerator and the denominator of the x-coordinate, and divide the largest of these by 2000^2. In this way, we obtain 0.5011822707 as candidate value for the regulator of E. This computation takes more than 8 seconds on a dedicated computation server and is only accurate for up to 6 digits; the actual regulator is 0.5011823920. △

Our goal is to explicitly compute these regulators, i.e. to produce an algorithm that given an equation for a curve computes the regulator. The method illustrated in Example 5 is not efficient at all. In practice, one decomposes the regulator in local contributions for each place (both finite and infinite) of $\mathbb{Q}$. For the finite places, it suffices to look at the discriminant and some other easily computable arithmetic invariants of the elliptic curves. For the infinite place, one needs to compute an elliptic integral, which can be done reasonably fast using AGM (arithmetic-geometric mean) methods.

Another problem with the Kummer embedding $K \hookrightarrow \mathbb{P}^{2^g-1}$, however, is that the ambient space and the number of equations to represent the image of K therein, grows exponentially with g. For genus 1, 2 and maybe 3, this is not a big issue, but for higher genus this will become a problem.

In this talk, I will present an alternative way to compute the regulator, using Arakelov intersection theory. This method was already used for hyperelliptic curves by Holmes [Hol12] and Müller [Mül14], and now has been extended by the three of us to the case of plane non-hyperelliptic curves [vBHM18].

2 Introduction to arithmetic surfaces

From now on, we let S be a Dedekind scheme of dimension 1. For this talk, we will take $S = \mathrm{Spec}(\mathbb{Z}_{(p)})$, the spectrum of the ring of rationals with no factor p in the denominator, where p is a prime. Let η be the generic point of S, with residue field $\mathbb{Q}$, and let s be the closed point of S, with residue field $\mathbb{F}_p$.

Definition 6. An *arithmetic surface* $A \,/\, S$ is an integral, normal, projective, flat S-scheme of relative dimension 1.

Example 7. For the prime $p = 2$, we could for example take the arithmetic surface A, defined by the equation $Y^2Z = X^3 + 3XZ^2$ inside $\mathbb{P}^2$ over $\mathbb{Z}_{(2)}$. Then the generic fibre A_η is just the curve E from Example 5 over $\mathbb{Q}$.

On the affine chart $Z \neq 0$, with coordinates x and y, we consider the point $(x, y) = (1, 0)$ inside the special fibre $A_s \,/\, \mathbb{F}_2$. It corresponds to the maximal ideal $(x - 1, y, 2)$ in the ring $\mathbb{Z}_{(2)}[x, y]$. The original equation, which can be rewritten as $y^2 - x(x - 1)^2 - 2x(x - 1) - 4x = 0$, is in the square of this

maximal ideal. That means that the point is not regular. We can blow this non-regular point up to get another arithmetic surface, which does turn out to be regular. △

Definition 8. Let $C \,/\, \mathbb{Q}$ be a curve, then a *(regular) model* of C is the data of a (regular) arithmetic surface $A \,/\, S$ together with an isomorphism $A_\eta \cong C$.

Remark 9. The fact that one can always get a regular model by starting with any model and repeatedly blowing up non-regular points, is non-trivial. For reduced varieties over a field of characteristic 0, this problem of resolution of singularities has been solved by Hironaka. However, for varieties of dimension greater than 4 over a field of characeristic $p > 0$, this problem is still open.

In the case of arithmetic surfaces, it is proven and also feasible (though cumbersome) in practice using `Magma`. △

3 Intersection theory on arithmetic surfaces / The local contribution at the finite places

Let $A \,/\, S$ be a regular model of $C \,/\, \mathbb{Q}$. We will consider *divisors* on A, i.e. formal sums of integral closed subschemes of codimension 1 (also called *prime divisors*). We distinguish two types of prime divisors. The so-called *horizontal prime divisors* are those obtained by taking the closure of a point in the generic fibre C. The *vertical prime divisors* are irreducible components of the special fibre A_s.

If $\mathcal{P}$ and $\mathcal{Q}$ are two distinct prime divisors, then we can define their intersection

$$\iota(\mathcal{P}, \mathcal{Q}) := \sum_{P \in A \text{ closed}} \operatorname{length}_{\mathcal{O}_{A,P}} \left(\frac{\mathcal{O}_{A,P}}{\mathcal{O}_{A,P}(-\mathcal{P}) + \mathcal{O}_{A,P}(-\mathcal{Q})} \right) \log |k(P)|,$$

where $k(P)$ is the residue field of P.

Example 10. Let A be the regular arithmetic surface over $\mathbb{Z}_{(2)}$ defined by the equation $Y^2Z = X^3 - 7XZ^2$ inside $\mathbb{P}^2_{\mathbb{Z}_{(2)}}$. Let $\mathcal{P}$ be the closure of $(4 : 6 : 1) \in C$, and let $\mathcal{Q}$ be the closure of $(4 : -6 : 1) \in C$. Then $\mathcal{P}$ and $\mathcal{Q}$ only intersect in the point $P = (0 : 0 : 1) \in A_s$ and

$$\iota(\mathcal{P}, \mathcal{Q}) = \operatorname{length}_R \left(\frac{R}{(x-4, y-6) + (x-4, y+6)} \right) \cdot \log(2) = 2 \log(2),$$

where $R = \mathcal{O}_{A,P} = \big(\mathbb{Z}_{(2)}[x, y]/(y^2 - x^3 - x)\big)_{(2,x,y)}$. Moreover, one can verify easily that $\iota(\mathcal{P}, \mathcal{R}) = \iota(\mathcal{Q}, \mathcal{R}) = \log(2)$, where $\mathcal{R}$ is the special fibre of A. △

In the example above, one sees that this intersection does not respect linear equivalence. However, if $\mathcal{D}$ is a horizontal divisor on A whose restriction to C has degree 0 and Y is the zero locus of p inside A (i.e. the special fibre), then $\mathcal{D} \cdot Y = 0$. This allows us to extend the intersection pairing to any two divisors $\mathcal{D}$ and $\mathcal{E}$ whose restrictions to C have degree 0 and disjoint support (but not necessarily disjount support on the special fibre).

For a divisor D on the generic fibre C, we let $\Gamma(D)$ be the divisor on A, whose horizontal part is D and for which $\iota(\Gamma(D), \mathcal{Y}) = 0$ for all vertical divisors $\mathcal{Y}$. The divisor $\Gamma(D)$ can be obtained by computing $\iota(\overline{D}, \mathcal{Y})$ for all vertical divisors $\mathcal{Y}$ and subtracting the appropriate vertical divisor. It is unique up to addition of multiples of the whole special fibre.

Definition 11. For two divisors D and E on C, of degree 0, and with disjoint support, we define the *local Néron pairing between D and E at p* by

$$\langle D, E \rangle_p := \iota(\Gamma(D), \Gamma(E)).$$

The way to compute these local Néron pairings, is by computing the aforementioned intersections. `Magma` can compute a regular model A of C by repeatedly blowing up non-regular points. It also keeps track of a disjoint cover of A consisting of constructible subsets. After several reduction steps, making use of the inclusion-exclusion principle, we can reduce the computation to finitely many computations of lengths of modules inside rings of finite type over $\mathbb{Z}_p$.

4 Green's functions and theta functions / The local contribution at the infinite place

For the contribution at the infinite place, we consider C as curve over $\mathbb{C}$. For each divisor E on C and each volume form φ on C, there is the so-called *Green's function*

$$g_{E,\varphi} \colon C(\mathbb{C}) \setminus \operatorname{supp}(E) \longrightarrow \mathbb{R}.$$

It is determined by the following properties (see also [Lang88, II, §1]):

- $g_{E,\varphi}$ has a logarithmic singularity at $\operatorname{supp}(E)$;
- $dd^c\, g_{E,\varphi} = (\deg(E)) \cdot \varphi$, where $d = \partial + \overline{\partial}$ and $d^c = \frac{1}{4\pi i}(\partial - \overline{\partial})$;
- $\int_C g_{E,\varphi} \varphi = 0$.

This Green's function is used to define a metric on $\mathcal{O}(E)$ and it is also used to define the local Néron pairing.

Definition 12. Let $D = \sum_P n_P P$ and E be divisors on C of degree 0 with disjoint support. The *local Néron pairing at the infinite place* is defined by

$$\langle D, E \rangle_\infty := \sum_P n_P g_{E,\varphi}(P).$$

Remark 13. This pairing is bilinear, symmetric, independent of φ, but not invariant under linear equivalence. △

In order to compute the contribution at the infinite place, one needs to explicitly compute a period matrix for the Jacobian of C and an Abel-Jacobi map from C to the analytic Jacobian, which is done using code of Neurohr [Neu18]. The calculation can then be reduced to several evaluations of the classical Jacobi theta function. More details can be found in our paper [vBHM18].

5 Back to the regulator

The following result is due to Faltings and Hriljac.

Theorem 14 ([Fal84, Hril85, Gro86])**.** *Let D and E be divisors on C, of degree 0, with disjoint support. Then*

$$h^{\mathrm{Kum}}([D], [E]) = -\sum_v \langle D, E \rangle_v,$$

where we sum over all places, finite and infinite, of $\mathbb{Q}$.

Remark 15. In particular, the sum on the right hand side does respect linear equivalence, while the summands do not. △

In order for our algorithm to function in general, we need to:

- move divisors to get divisors with disjoint support (and for practical reasons with no support at infinity for a certain affine model);
- identify the primes for which there is a local contribution to the height pairing; these are the primes of bad reduction and the primes for which we can verify in a quick way that there is intersection.

In the end, our algorithm has two bottlenecks:

- to identify the relevant primes, one sometimes needs to factor a very large integer; this can probably be avoided by using the idea used in [MüSt16] to factor into coprimes;
- the Gröbner basis computations are very expensive; a lot of time could potentially be saved by doing fewer of them; especially when computing a regulator a lot of work is done multiple times.

Example 16. We managed to compute the height pairing on the split Cartan modular curve of level 13, and thereby verified the Birch and Swinnerton-Dyer conjecture in the following sense. We computed everything, except for the Tate-Shafarevich group, and the regulator only provably up to squares, and we numerically checked that the conjecture holds up to squares. This took about 10 seconds. △

Example 17. We were also able to compute the height pairing on a curve with very bad reduction: the curve

$$3x^3y + 5x^2 + 5y^4 - 1953125 = 0,$$

for which the special fibre of our regular model at the bad prime 5 has 9 irreducible components. This took several minutes. △

References

[vBHM18] Raymond van Bommel, David Holmes, J. Steffen Müller, *Explicit arithmetic intersection theory and computation of Néron-Tate heights.* Preprint (2018), ArXiv:1809.06791.

[Fal84] Gerd Faltings, Calculus on arithmetic surfaces, *Ann. of Math. (2)* **119** (1984), no. 2, 387–424.

[Gro86] Benedict H. Gross, Local heighs on curves. *Arithmetic geometry (Storrs, Conn., 1984)*, 327–339, *Springer, New York,* 1986.

[Hol12] David Holmes, Computing Néron-Tate heights of points on hyperelliptic Jacobians. *J. Number Theory* **132** (2012), no. 6, 1295–1305.

[Hril85] Paul Hriljac, Heights and Arakelov's intersection theory. *Amer. J. Math.* **107** (1985), no. 1, 23–38.

[Lang88] Serge Lang, *Introduction to Arakelov theory.* Springer-Verlag, New York, 1988.

[Mül14] Jan Steffen Müller, Computing canonical heights using arithmetic intersection theory. *Math. Comp.* **83** (2014), no. 285, 311–336.

[MüSt16] Jan Steffen Müller, Michael Stoll, Canonical heights on genus-2 Jacobians. *Algebra Number Theory* **10** (2016), no. 10, 2153–2234.

[Neu18] Christian Neurohr, *Efficient integration on Riemann surfaces & applications*, PhD thesis, Carl von Ossietzky Universität Oldenburg, 2018. `http://oops.uni-oldenburg.de/3607/1/neueff18.pdf`.