P. Spelier

A geometric approach to linear and quadratic Chabauty

Master thesis

February 11, 2020

Thesis supervisor: prof. dr. S.J. Edixhoven

Leiden University
Mathematical Institute

Contents

1 Introduction

Say something about the problem, Faltings, et cetera

Say something about Chabauty's general idea

Mention Flynn, Coleman, Kim, Balakrishnan, Dogra, and other mentionable people. and their way of doing (quadratic) Chabauty

Say something about linear Chabauty geometric style.

Say something about quadratic Chabauty geometric style.

Say how much is borrowed from the article by Bas and Guido, but with a focus on the linear part, and more explanations.

2 Linear Chabauty

Let $p > 2$ be a prime, and C be a scheme over $\mathbb{Z}$, proper, flat, regular with C smooth over $\mathbb{Z}_{(p)}$ and $C_{\mathbb{Q}}$ of dimension 1 and geometrically connected, of genus $g \geq 1$ and with the Jacobian J of $C_{\mathbb{Q}}$ having Mordell-Weil rank $r < g$. Assume we have a $\mathbb{Q}$-point b in C, or equivalently a $\mathbb{Z}$-point. We view $C_{\mathbb{Q}}$ as a subscheme of J, using the map $Q \mapsto Q - b$ on points. Let $P \in C(\mathbb{F}_p)$ be a point such that $t := P - b \in J(\mathbb{F}_p)$ lies in the image of $J(\mathbb{Z})$.

Definition 2.1. Let S be a scheme, $T \to U$ a morphism of schemes and $x : T \to S$ a T-point. We define $S(U)_x$ as the morphisms from U to S that, after precomposing with $T \to U$, give x.

We want to find an upper bound for the cardinality of $C(\mathbb{Z})_P$

2.1 Points on a smooth scheme over $\mathbb{Z}_p$

Let $X/\mathbb{Z}_p$ be a smooth scheme of relative dimension d, and let $x \in X(\mathbb{F}_p)$ be a point. Then $X(\mathbb{Z}_p)_x$ is in bijection with $\mathbb{Z}_p^d$. This bijection is given by choosing parameters at x; evaluating at $X(\mathbb{Z}_p)_x$ gives a bijection with $(p\mathbb{Z}_p)^d$, and then we divide by p. For putting up a nice framework to work in, we start with blowing up X at x.

Assume, by looking at a neighborhood of x, that $X = \operatorname{Spec} A$ is affine and that $p, t_1, \ldots, t_d$ generate the maximal ideal of $O_{X,x}$ with $t_1, \ldots, t_d$ elements of $O_X(X) = A$, also called *parameters* at x. By shrinking X even more, we may assume as X is smooth that $t = (t_1, \ldots, t_d) : X \to \mathrm{A}^d_{\mathbb{Z}_p}$ is étale. Now consider the blowup $\tilde{X}_x \to X$ of X at x, and let $\tilde{X}_x^p$ be the part where p generates the inverse image of the maximal ideal of $O_{X,x}$. Equivalently, that is the part where $t_1, \ldots, t_d$ are multiples of p, so informally it consists of the points that reduce to x modulo p.

There is an explicit description of the map $\tilde{X}_x^p \to X$; as t is étale, the ideal of X defining x is the pullback along t of the ideal of $\mathrm{A}^d_{\mathbb{Z}_p}$ defining the origin a over $\mathbb{F}_p$. That means that the blowup $\tilde{X}_x \to X$ is the pullback of the blowup $\tilde{\mathrm{A}}^d_{\mathbb{Z}_p,a} \to \mathrm{A}^d_{\mathbb{Z}_p}$. Then the part $\tilde{X}_x^p$ is the pullback of the corresponding part of $\tilde{\mathrm{A}}^d_{\mathbb{Z}_p,a}$, i.e. $\operatorname{Spec} \mathbb{Z}_p[\tilde{x_1}, \ldots, \tilde{x_d}] = \operatorname{Spec} \mathbb{Z}_p[x_1/p, \ldots, x_d/p]$ with the morphism $\mathbb{Z}_p[x_1, \ldots, x_d] \to \mathbb{Z}_p[\tilde{x_1}, \ldots, \tilde{x_d}]$ given by $x_i \mapsto p\tilde{x_i}$. That implies that $\tilde{X}_x^p$ is $\operatorname{Spec} A[t_1/p, \ldots, t_d/p]$, with the map $\tilde{X}_x^p \to X$ given by the inclusion $A \to \operatorname{Spec} A[t_1/p, \ldots, t_d/p]$ (remember that the t_i are elements of $O_X(X) = A$).

This now enables us to characterise explicitly the $\mathbb{Z}_p$-points above x, as in the following two lemmas.

Lemma 2.2. *With X as above, there is a natural bijection $X(\mathbb{Z}_p)_x \to \tilde{X}_x^p(\mathbb{Z}_p)$,*

Proof. Note that by (I,2.4.4) of [GD71], a $\mathbb{Z}_p$ point of a scheme S is just an $\mathbb{F}_p$-point s together with a local morphism $\mathcal{O}_{S,s} \to \mathbb{Z}_p$. In our case, we find that

$X(\mathbb{Z}_p)_x$ is naturally in bijection with $\mathrm{Hom}_{\mathrm{local}}(A_x, \mathbb{Z}_p)$. As the maximal ideal of A_x is generated by $p, t_1, \ldots, t_d$, the locality property just means that the images of $t_1, \ldots, t_d$ are divisible by p, i.e. exactly those morphisms that extend to a morphism $A[t_1/p, \ldots, t_d/p] \to \mathbb{Z}_p$, i.e. a $\mathbb{Z}_p$-point of $\tilde{X}^p_x$. Hence we find the natural bijection. □

Lemma 2.3. *With X as above, evaluating t at $X(\mathbb{Z}_p)_x$ gives a bijection to $(p\mathbb{Z}_p)^d$.*

Proof. As t is locally of finite type, by (IV,17.6.3) of [GD71] we have an isomorphism between the p-adic completion $O(\tilde{X}^p_x)^{\wedge p}$ and the completion $\mathbb{Z}_p\langle \tilde{x_1}, \ldots, \tilde{x_d}\rangle$ of $\mathbb{Z}_p[\tilde{x_1}, ..., \tilde{x_d}]$, with the latter completion being the ring of convergent power series, i.e.

$$\mathbb{Z}_p\langle \tilde{x_1}, \ldots, \tilde{x_d}\rangle = \{f \in \mathbb{Z}_p[[\tilde{x_1}, \ldots, \tilde{x_d}]] \mid \forall n \geq 0, f + (p^n) \in \mathbb{Z}/p^n\mathbb{Z}[\tilde{x_1}, \ldots, \tilde{x_d}] + (p^n)\}.$$

By the universal property of completions, as t induces the isomorphism between completion, t also induces a bijection

$$\mathrm{Hom}(O(X(\mathbb{Z}_p)_x), \mathbb{Z}_p) \to \mathrm{Hom}(O(X(\mathbb{Z}_p)_x)^{\wedge p}, \mathbb{Z}_p) = \mathrm{Hom}(\mathbb{Z}_p\langle \tilde{x_1}, \ldots, \tilde{x_d}\rangle, \mathbb{Z}_p) = \mathbb{Z}_p^d.$$

Following all the bijections, we indeed get the bijection we wanted. □

Note that this construction is functorial, as in the following lemma:

Lemma 2.4. ?? *Given two smooth schemes X, Y over $\mathbb{Z}_p$ and two $\mathbb{F}_p$-points $x \in X(\mathbb{F}_p), y \in Y(\mathbb{F}_p)$, a map $f : Y \to X$ satisfying $f(y) = x$ gives rise to a morphism $\tilde{Y}^p_y \to \tilde{X}^p_x$.*

Proof. TODO: give proof. □

[TODO: add that the map $\tilde{Y}^p_y(\mathbb{Z}_p) \to \tilde{X}^p_x(\mathbb{Z}_p)$ is, after choosing parameters, given by convergent power series; are these in general linear modulo p? And what happens modulo higher powers?]

Finally, we look at the specific case of X being of relative dimension 1 over $\mathbb{Z}_p$. It then turns out that there is additionally a free transitive $\mathbb{F}_p$-action on $X(\mathbb{Z}/p^2\mathbb{Z})_0$. [TODO: maybe replace this by an action of the tangent space of $X_{\mathbb{F}_p}$ at x]. We can parametrise $X(\mathbb{Z}/p^2\mathbb{Z})_0$ by $t = t_1 : X(\mathbb{Z}/p^2\mathbb{Z})_0 \to p\mathbb{Z}/p^2\mathbb{Z}$; write P_λ for the point with t-value λp. Then as Cartier divisor, the point P_λ is defined by $t - \lambda p \in O(X_{\mathbb{Z}/p^2\mathbb{Z}})_x$, so $P_\lambda + P_\mu$ is defined by $(t-\lambda p)(t-\mu p) = t^2 - (\lambda+\mu)tp$, which defines the same Cartier divisor as $P_{\lambda'} + P_{\mu'}$ if and only if $\lambda + \mu = \lambda' + \mu'$. So as a Cartier divisor, $P_\lambda + P_\mu$ is in fact equal to $P_{\lambda'} + P_{\mu'}$.

2.2 From $J(\mathbb{Z})$ to $J(\mathbb{Z}_p)$

For $p > 2$, we know that the torsion of $J(\mathbb{Z})$ injects into $J(\mathbb{F}_p)$, by Proposition 2.3 of [Par00]. Hence for $0 \in J(\mathbb{F}_p)$, we know $J(\mathbb{Z})_0$ is as a group isomorphic

to $\mathbb{Z}^r$ with r the Mordell-Weil rank. By assumption, we also know $J(\mathbb{Z})_t$ is in bijection with $J(\mathbb{Z})_0$, with the bijection giving by translating with a lift of t. By Subsection 2.1 we know $J(\mathbb{Z}_p)_t$ is in bijection with $\mathbb{Z}_p^g$, with the bijection given by evaluating parameters and dividing by p. Let $\kappa : \mathbb{Z}^r \to \mathbb{Z}_p^g$ be the map resulting from the inclusion $J(\mathbb{Z})_t \to J(\mathbb{Z}_p)_t$. Then κ turns out to have a special property.

Theorem 2.5. *There are uniquely determined $\kappa_1, \ldots, \kappa_g \in \mathbb{Z}_p\langle z_1, ..., z_r\rangle$ such that for all $x \in \mathbb{Z}^r$ we have $\kappa(x) = (\kappa_1(x), \ldots, \kappa_g(x))$ and the image $\overline{\kappa_i}$ of κ_i in $\mathbb{F}_p[z_1, ..., z_r]$ has degree at most 1.*

We will prove this using results about formal group as defined in [HON70]. To be able to use this theory, we first give some results about going from a group scheme over $\mathbb{Z}_p$ to a formal group. First we introduce some notation that will be used in this section. Let R be a commutative ring, and $x = (x_1, \ldots, x_n)$ and sometimes y, z are vectors of variables. Then $R[[x]]$ denotes as usual the powerseries in the x_i, and $R[[x]]_0$ denotes those power series with constant term 0. With $x = (x_1, \ldots, x_n)$ and $y = (y_{,1}, \ldots, y_m)$, let $f \in R[[x]]^m$ and assume $f(0) = 0$. Then for $g \in R[[y]]^k$ for some $k \in \mathbb{Z}_{\geq 0}$, we can compose g and f to get $g \circ f := (g_1(f(x)), \ldots, g_k(f(x))) \in R[[x]]]^k$. This definition makes sense because f^i converges to 0, so for any $a \in R^{\mathbb{Z}_{\geq 0}}$ the sum $\sum_i a_i f^i$ always converges.

2.2.1 From group schemes to formal groups

We first recall the definition of a formal group. For this entire section, R is a ring, and x, y, z are vectors of variables.

Definition 2.6. Let n be a non-negative integer. Let x, y, z be vectors of n variables. An n-dimensional formal group is an element $F = (F_1, \ldots, F_n) \in R[[x, y]]_0^n$ satisfying $F \equiv x + y \mod (x, y)^2$ and $F(F(x, y), z) = F(x, F(y, z))$. If furthermore $F(x, y) = F(y, x)$, this formal group is said to be commutative.

Example 2.7. Take $n = 1$ and $F(x, y) = x + y + xy = (1 + x)(1 + y) - 1$, also known as the multiplicative formal group. This satisfies associativity as $F(F(x, y), z) = (1 + x)(1 + y)(1 + z) - 1 = F(x, F(y, z))$.

Example 2.8. For any n, we can take $F(x, y) = x + y$, also known as the n-dimensional additive formal group.

[TODO: add text explaining the following lemma] Note there is no mention of an inverse, but the following lemma, a formal version of the implicit function theorem, tells us that the inverse follows automatically from the definitions.

Lemma 2.9. *Let x, y have length n. Let $F \in R[[x, y]]_0^n$ such that $F \equiv Ax+By \mod (x, y)^2$ with $B \in \mathrm{GL}_n(R)$. Then there's a unique $\iota \in R[[x]]_0^n$ such that $F(x, \iota(x)) = 0$.*

Proof. If F is a polynomial, this is a special case of a multivariate version of Hensel's lemma, as in Corrolaire 2 of [Bou98, III,4.5], over $R[[x]]$ with maximal ideal $\mathfrak{m} = (x)$, as the derivative matrix of $F(x, \iota)$ with respect to ι is B, which is invertible, and $\iota = 0$ gives a solution modulo $\mathfrak{m}$. Now for F any power series, let F_j be the polynomial consisting of all terms in F of degree at most j, and let ι_j be the unique power series in $R[[x]]_0^n$such that $F_j(x, \iota_j) = 0$. Note that both ι_j and ι_{j+1} are solutions to $F_j(x, \iota) \equiv 0 \mod \mathfrak{m}^j$, so by the uniquess guaranteed by Hensel's lemma used over $R[[x]]/\mathfrak{m}^j$, these must be equal. Hence they converge to $\iota \in R[[x]]_0^n$, which is the unique solution of $F(x, \iota(x)) = 0$. □

This has the following corollary about the inverse of a power series.

Corollary 2.10. *Let x have length n. Let $a \in R[[x]]_0^n$ with $a \equiv Px \mod x$ for some matrix $A \in \mathrm{GL}_n(R)$. Then there is a unique $b \in R[[x]]_0^n$ such that $a \circ b = b \circ a = x$.*

Proof. Let $F(x, y) = x - a(x)$. This satisfies the constraints of Lemma 2.9, so we find a unique b such that $a \circ b = x$. Applying Lemma 2.9 again gives a unique c such that $b \circ c = x$. But then $a = a \circ (b \circ c) = (a \circ b) \circ c = c$ shows $a = c$ and hence we are done. □

So a formal group F does by Lemma 2.9 indeed have a right inverse ι_F. Also, by $F(0, 0) = 0$ we have that $F(x, F(\iota_f, 0)) = 0$ so $F(\iota_f, 0)$ is in fact equal to ι_F; as $\iota_F \equiv -x \mod (x)^2$, it has a formal inverse and hence $F(x, 0) = x$, so 0 is indeed a right unit. A standard argument now shows that ι_F is also a left inverse and 0 is also a right unit, so F gives $R[[x]]$ the structure of a group object in the category of topological rings; for two continuous morphisms f_1, f_2 from $R[[x]]$ to some ring A, given by sending x to a_1, a_2 respectively, we define $(f_1 \oplus f_2)(x) = F(a_1, a_2)$, and by our considerations this makes $\mathrm{Hom}_{\mathrm{cont}} R, A$ into a group, functorially in A.

Given a smooth scheme G over $\mathbb{Z}_p$ of relative dimension d, together with a $\mathbb{Z}_p$-point e, we can look at the completion $\hat{O}_{G,e}$ along the section e. By smoothness, after picking parameters, this is isomorphic as topological $\mathbb{Z}_p$-algebras to the ring of power series $\mathbb{Z}_p[[x_1, \ldots, x_d]]$. This completion naturally gives rise to a formal scheme denoted $\mathrm{Spf}\, \hat{O}_{G,e}$; in a categorical notion, this is a functor on finite length $\mathbb{Z}_p$-algebras sending A to $\mathrm{Hom}_{\mathrm{cont}}(\hat{O}_{G,e}, A)$, but we can also think of it as a locally ringed space with $\mathrm{Spec}\, \mathbb{Z}_p$ as topological space, and sheaf of rings $\hat{O}_{G,e}$.

If furthermore G is a group scheme over $\mathbb{Z}_p$, then this formal scheme promotes to a formal group scheme, i.e. for every finite $\mathbb{Z}_p$-algebra A the set $\mathrm{Hom}_{\mathrm{cont}}(\hat{O}_{G,e}, A)$ gets a group structure, functorially in A. By functoriality, this is the same [TODO: why exactly?] as an continuous coproduct $\mu : \hat{O}_{G,e} \to \left(\hat{O}_{G,e}\right)^{\hat{\otimes} 2}$. After choosing an isomorphism between $\hat{O}_{G,e}$ and $\mathbb{Z}_p[[x_1, \ldots, x_d]]$, let $F_j \in \mathbb{Z}_p[[x, y]]$ denote $\mu(x_i)$. Then it is clear that $F_G = (F_1, \ldots, F_d)$ is a d-dimensional formal group scheme, and commutative if G was commutative.

Example 2.11. Take $G = \mathbb{G}_m$ over $\mathbb{Z}_p$, i.e. $\mathbb{Z}_p[u, u^{-1}]$. Then the zero section e is the map sending u to 1, and we can identify the completion $\hat{O}_{G,e}$ with the power series ring $\mathbb{Z}_p[[u-1]] \cong \mathbb{Z}_p[[x]]$, sending $u-1$ to x. The group structure on G then gives rise to the coproduct $\mathbb{Z}_p[[u-1]] \to \mathbb{Z}_p[[u-1, v-1]], u \mapsto uv$ so the coproduct on $\mathbb{Z}_p[[x]]$ sends x to $uv - 1 = (x+1)(y+1) - 1 = x + y + xy$. Hence the formal group $F_{\mathbb{G}_m}$ corresponding to this group scheme is exactly the multiplicative formal group from Example 2.7.

This formal group tells us exactly how multiplication works on $G(\mathbb{Z}/p^e\mathbb{Z})_0$; if we let $t = (t_1, \ldots, t_d)$ denote the formal parameters giving the isomorphism $\hat{O}_{G,e} \to \mathbb{Z}_p[[x_1, \ldots, x_d]]$, and we represent a point P in $G(\mathbb{Z}/p^e\mathbb{Z})_0$ by their parameter values $t(P) \in p\mathbb{Z}/p^e\mathbb{Z}$, then the multiplication $p\mathbb{Z}/p^e\mathbb{Z} \times p\mathbb{Z}/p^e\mathbb{Z} \to p\mathbb{Z}/p^e\mathbb{Z}$ is exactly F. By taking limits, F also gives the multiplication on $G(\mathbb{Z}_p)_0$.

Now we will look at the theory of formal groups, and how that will help us. For a n-dimensional formal group F over a ring R, Proposition 1.1 of [HON70] gives us a canonical R-basis $\omega_1, \ldots, \omega_n$ of the right invariant differentials; these are elements of $\bigoplus_{j=1}^n R[[x]]\,\mathrm{d}x_j$. If the formal group is furthermore commutative, then by Proposition 1.3 of [HON70] these are closed, i.e. $d\omega_j = 0$. A 1-form $d\omega = \sum_{i=1}^n f_i\,\mathrm{d}x_i$ being closed means exactly that $\frac{\partial f_i}{\partial x_j} = \frac{\partial f_j}{\partial x_i}$ for all i, j, and then, if R has no torsion, we can formally integrate ω, i.e. write it as df where $f \in (\mathbb{Q} \otimes R)[[x]]$. We make this unique by demanding that $f(0) = 0$. Writing this f as $\sum_{I \in \mathbb{N}^n} a_I x^I$ with I denoting a multi index and $a_I \in \mathbb{Q} \otimes R$, we see that a_I, although itself not necessarily lying in R, is close: writing $I = (I_1, \ldots, I_n)$ we see that for all j we must have $I_j a_I \in R$ as $f_j = \frac{\partial f}{\partial x_j} \in R[[x]]$.

In particular, we write $\log_i$ for the unique element of $(\mathbb{Q} \otimes R)[[x]]$ such that $d\log_i = \omega_i$. Together, these $\log_i$ give an element $\log \in R[[x]]^n$, and by Theorem 1 of [HON70], this logarithm satisfies $\log(x) = x \mod (x)^2$, and $\log(F(x,y)) = \log(x) + \log(y)$. By the first result, log has an inverse which we will call exp, also given by powerseries in $(\mathbb{Q} \otimes R)[[x]])$, and also satisfying $\exp(x) = x \mod (x)^2$.

Example 2.12. Taking F the multiplicative group as in Example 2.7, Proposition 1.1 of [HON70] gives us $\omega = \frac{1}{x+1}dx$; as a power series this is $\sum_{j \geq 0}(-x)^j$. The formal anti-derivative of this is $\log = \sum_{j \geq 1} \frac{-(-x)^j}{j}$, and Theorem 1 will tell us what we already know in the context of analysis $\log(x+y+xy) = \log(x) + \log(y)$. Then analysis will also explicitly tell us what exp looks like: namely, $\exp(x) = \sum_{j \geq 1} \frac{x^j}{j!}$.

Now we will see how we can use this formal logarithm in our case of the formal group F_G stemming from a d-dimensional smooth group scheme $G/\mathbb{Z}_p$. Recall that we have a bijection $G(\mathbb{Z}_p)_0 \to p\mathbb{Z}_p^d \to \mathbb{Z}_p^d$ given by evaluating at parameters $t = (t_1, \ldots, t_d)$ and then dividing by p; furthermore, recall that the group structure on $G(\mathbb{Z}_p)_0$ is the same as the group structure defined by F_G on $p\mathbb{Z}_p^d$. Let $\log \in \mathbb{Z}_p[[x]]^d$ denote the logarithm corresponding to F_G, and let $\log_p$ denote the power series $\log(px)/p = (\log_1(px)/p, \ldots, \log_d(px)/p)$. We then have the following little lemma to bridge the gap between power series and maps.

Lemma 2.13. *With notation as above, we have the following statements about* $\log_p$*:*

1. $\log_p$ *lies in* $\mathbb{Z}_p\langle x_1, \ldots, x_d\rangle^d$*, the ring of convergent power series, and hence defines a map* $\log_p : \mathbb{Z}_p^d \to \mathbb{Z}_p^d$*.*
2. *Letting* $\oplus$ *denote the group structure on* $\mathbb{Z}_p^d$ *coming from the bijection* $G(\mathbb{Z}_p)_0 \to p\mathbb{Z}_p^d \to \mathbb{Z}_p^d$*, the map* $\log_p$ *is a group morphism from* $(\mathbb{Z}_p^d, \oplus)$ *to* $(\mathbb{Z}_p^d, +)$*.*
3. *If* $p > 2$*, the map* $\log_{p,i}$ *reduces to* x_i *modulo* p *and hence* $\log_p$ *has an inverse* $\exp_p$*, which is also an element of* $\mathbb{Z}_p\langle x_1, \ldots, x_d\rangle$*. Then this* $\exp_p$ *is a two-sided inverse of* $\log_p$*, and hence* $\log_p : \mathbb{Z}_p^d \to \mathbb{Z}_p^d$ *is a bijection.*
4. *Let* $m \in \mathbb{Z}_{>0}$*. For* $p > m+1$*, the map* $\log_p$ *and* $\exp_p$ *are of degree at most* m *modulo* p^m*.*

Proof. Write $\log_i = \sum_I a_{i,I} x^I$ and $log_{p,i} = \sum_I a_{i,I} p^{|I|-1} x^I$ where I ranges over the multi indices. Recall that $a_{i,0} = 0$. Also, recall that although a priori the coefficients a_I lie in $\mathbb{Q}_p$, we have $I_j a_{i,I} \in \mathbb{Z}_p$ for all I and i, j. For purposes of easy estimation, this also means $|I| a_{i,I} \in \mathbb{Z}_p$. As we have, with no constraint on p, for all $n \geq$ that $c_n \coloneqq p^{n-1}/n$ lies in $\mathbb{Z}_p$ and converges to 0, this means that

$$\log_{p,i} = \sum_I a_{i,I} p^{|I|-1} x^I = \sum_I |I| a_{i,I} c_{|I|} x^I$$

is indeed an element of $\mathbb{Z}_p\langle x_1, \ldots, x_d\rangle^n$, and hence defines a map $\mathbb{Z}_p^d \to \mathbb{Z}_p$. Hence all the $\log_{p,i}$ together give a map $\mathbb{Z}_p^d \to \mathbb{Z}_p^d$. By the equality of power series $\log(F(x,y)) = \log(x) + \log(y)$ from the definition of the logarithm, and the fact that all these powerseries converge on $p\mathbb{Z}_p^d$, this $\log_{p,i}$ is indeed a group morphism from $(\mathbb{Z}_p^d, \oplus)$ to $(\mathbb{Z}_p^d, +)$

To study $\log_p$ modulo p, we note that if $n \geq 3$, then p actually divides c_n, and for $p > 2$ we even have $p | c_2$. As $\log_{p,i} = x_i \mod (x)^2$, this means that for $p > 2$ we have

$$\log_{p,i} \equiv \sum_{|I|=1} |I| a_{i,I} c_{|} I | x^I \equiv x_i \bmod p.$$

Note that as $\log_p \equiv x \mod (x)^2$, by Lemma 2.10 it has an inverse $\exp_p \in \mathbb{Z}_p[[x]]_0^n$. Modulo p, this $\exp_p$ must be x, which lies in $\mathbb{Z}_p\langle x\rangle_0^n$; as $\mathbb{Z}_p\langle x\rangle$ is p-adically complete, using Hensel this shows $\exp_p$ is indeed in $\mathbb{Z}_p\langle x\rangle_0^n$.

As c_n has p-adic valuation $n-1$ for ... □

[TODO: I'd like to study what happens modulo higher powers of p; for example, if $\log_p$ is at most quadratic mod p^2, then so is $\exp_p$; and similar for $\log_p$ at most cubic mod p^3. Even in general, if $\log_p$ has degree at most d modulo p^k, then $\exp_p$ has degree at most $f = f(d,k)$ (seen most easily by working in a "universal" ring $\mathbb{Z}[p]/(p^k)$).

This lemma makes the proof of Theorem 2.5 relatively easy.

Proof of Theorem 2.5. Write $\log_p$ for the logarithm corresponding to the formal group corresponding to the The map $\kappa : \mathbb{Z}^d \to \mathbb{Z}_p^g$ given by the inclusion $J(\mathbb{Z})_0$ to $J(\mathbb{Z}_p)_0$ is a group morphism with the group structure on $\mathbb{Z}^d$ being addition and the group structure on $\mathbb{Z}_p^g$, denoted by $\oplus$, given by the bijection with $J(\mathbb{Z}_p)_0$ induced by choosing parameters at 0. Then by Lemma 2.13 the map factors as in the diagram of groups

$$\begin{array}{ccc} (\mathbb{Z}^d, +) & \xrightarrow{\quad\kappa\quad} & (\mathbb{Z}_p^g, \oplus) \\ & {\scriptstyle \log_p \circ \kappa} \searrow \quad \nearrow {\scriptstyle \exp_p} & \\ & (\mathbb{Z}_p^g, +) & \end{array}$$

Then the arrow $\log_p \circ \kappa$ is just a linear map, and $\exp_p$ is a convergent power series that is linear modulo p, so their composite κ is also a convergent power series linear modulo p. □

This immediately gives rise to the following corollary.

Corollary 2.14. *The map κ extends uniquely to a continuous map $\kappa : \mathbb{Z}_p^r \to \mathbb{Z}_p^g$, given by the same power series, and the closure $\overline{J(\mathbb{Z})_t} \subset J(\mathbb{Z}_p)_t$ is given by the image of $\mathbb{Z}_p^r$ under κ.*

[TODO: in general, generators of the Mordell-Weil group are computationally out of reach. But, if we only generate a subgroup of $J(\mathbb{Z})_0$ of index finite and coprime to p, then the closure of this in $J(\mathbb{Z}_p)_0$ will be the same. This happens in particular if we generate a subgroup of $J(\mathbb{Z})$ of index finite and coprime to $p|J(\mathbb{F}_p)|$. Preferably, find a source for this?]

2.3 From $C(\mathbb{Z}_p)$ to $J(\mathbb{Z}_p)$

By Subsection 2.1, we also know that $C(\mathbb{Z}_p)_P$ is in bijection with $\mathbb{Z}_p$, again with the bijection given by evaluating a parameter and dividing by p. The resulting function $\mathbb{Z}_p \to \mathbb{Z}_p^g$ is linear and non-constant modulo p, i.e. there are power series $f_1, ..., f_{g-1} \in \mathbb{Z}_p\langle z_1, ..., z_g\rangle$ such that the image of $C(\mathbb{Z}_p)_P$ is exactly given by $V(f_1, ..., f_{g-1})$, and all f_i are linear modulo p. Another way to think of this, is as $C(\mathbb{Z}/p^2\mathbb{Z})_P$ being an affine line inside $J(\mathbb{Z}/p^2\mathbb{Z})_t$. TODO: give proof. This uses the functoriality of smooth $\mathbb{Z}_p$-points reducing to a point. That $C(\mathbb{Z}/p^2\mathbb{Z})_P$ is an affine line inside $J(\mathbb{Z}/p^2\mathbb{Z})_t$ can also be seen more easily, using Lemma **??**.

2.4 Finding $C(\mathbb{Z})$

Clearly, as subsets of $J(\mathbb{Z}_p)_t$, we have the inclusion $C(\mathbb{Z})_P \subset C(\mathbb{Z}_p)_P \cap \overline{J(\mathbb{Z})_t}$. Let $\kappa^* f_1, ..., \kappa^* f_{g-1}$ be the pullbacks along κ of the f_i, and let I be the ideal they generate inside $A := \mathbb{Z}_p\langle z_1, ..., z_r\rangle$. Then $C(\mathbb{Z}_p)_P \cap \overline{J(\mathbb{Z})_t}$ is in bijection with $\mathrm{Hom}(A/I, \mathbb{Z}_p)$. By Theorem 4.2 of Edixhoven-Lido, we just need to check whether $\overline{A}/\overline{I}$ is finite. As all $\overline{\kappa^* f_i}$ are linear, in fact, $\overline{A}/\overline{I}$ is always of the form 0

(meaning no solutions) or $\mathbb{F}_p[w_1, ..., w_s]$ for some $s \leq r$, and $s = 0$ iff the system of linear equations $\overline{\kappa^* f_i} = 0, i \in \{1, ..., g-1\}$ has a unique solution. In general, we may hope an upper bound for $|C(\mathbb{Z})_P|$ of 1 if $r \leq g - 1$.

2.5 Calculations modulo p^2

Say something about how, for the right set of points $\{p_1, ..., p_g\}$, the map $C^g \to J$ is etale at that set of points. Then say something about what that implies about $J(\mathbb{Z}_p)_0$ (equal to $\sum q_i - p_i$ where $q_i \in C(\mathbb{Z}_p)_{p_i}$), and $J(\mathbb{Z}/p^2\mathbb{Z})_0$, which becomes isomorphic as vector spaces to $\mathbb{F}_p^g$, and how we can find κ by expressing elements of $J(\mathbb{Z})_0$ in that basis, and similarly $f_1, ..., f_{g-1}$ by finding $P_1 - P_2$ in that basis for some $Q_1, Q_2 \in C(\mathbb{Z}/p^2\mathbb{Z})_P$ not equal.

An important part of this, is that there is a parametrisation $P_\mu, \mu \in \mathbb{F}_p$ of the points in $C(\mathbb{Z}/p^2\mathbb{Z})_P$ such that $P_\mu + P_\nu = P_{\mu+\nu} + P_0$ as Cartier divisors.

3 Implementations of linear Chabauty and an explicit example

[TODO: make sure I clearly differentiate divisors and divisor classes] We now assume that C is hyperelliptic, i.e. given by the degree $2g + 2$ homogenisation of an equation of the form

$$y^2 = f(x)$$

inside $\mathbb{P}(1, g+1, 1)$ where f is a monic polynomial of degree $2g+1$ or $2g+2$. An alternative way of defining such a curve, and the one we will be using mainly, is as a glueing of two affine charts: $y^2 = f(x)$, and $w^2 = f^r(v)$, where $f^r(v)$ is the polynomial $v^{2g+2} f(1/v)$, and a birational map between them is given by $(x, y) \mapsto (\frac{1}{x}, \frac{y}{x^{-g-1}})$. We also have the coordinates X, Y, Z of $\mathbb{P}(1, g+1, 1)$, with $x = X/Z, y = Y/Z^{g+1}, v = Z/X, w = Y/X^{g+1}$, but beware; these coordinates do not behave nicely on the origin of the patch $D(Y)$. We mainly use the first chart; we call any point that lies on it an affine point of C. We will treat the case that f has degree $2g + 2$ (this can be done by translating f until the constant coefficient is non-zero, and then looking at f^r). In that case, near the line at infinity C looks like $Y^2 = X^{2g+2}$, i.e. $(Y - X^{g+1})(Y + X^{g+1}) = 0$, and we see there are two points $\infty_+ = (1 : 1 : 0)$ and $\infty_- = (1 : -1 : 0)$. Finally, we note that there is an involution on C given by $\sigma(x, y) = (x, -y)$ and $\sigma(v, w) = (v, -w)$.

3.1 Makdisis algorithms

Say something about how Makdisis algorithms work (i.e., give an introduction to the terminology) [KM04].

As we are using and adding on an implementation by Mascot [Mas18], we briefly introduce his notation. This is a summary of section 2.1 in [Mas18].

We first look at representing $J(k)$ where k is a field. Given a divisor D on C, denote

$$\mathcal{L}(D) = \{f \in k(C)^\times : \mathrm{div}(f) + D \geq 0\} \sqcup \{0\}.$$

We pick D_0 an effective divisor of degree $d_0 \geq 2g+1$; in the case of hyperelliptic curves, this will be $(g+1)(\infty_+ + \infty_-)$. We set $V_n = \mathcal{L}(nD_0)$. We let n_Z be an integer $\geq 5d_0 + 1$, and assume, if necessary passing to an extension of k, that we have a set Z of size n_Z of distinct points in $C(k)$ outside the support of D_0; in fact, this will consist of affine points in our case. We have an evaluation map $V_5 \to k^Z$, evaluating a rational function at Z. By our choice of n_Z, this is an injective map, i.e. we can represent rational functions in V_5 by their values in k^Z. In this representation, we can add, subtract, or, if the degree at infinity is not too large, even multiply rational functions, by respectively adding, subtracting or multiplying the correspondig vectors in k^Z. It is now also possible to represent subspaces of V_5 by giving a basis in k^Z. (Instead of passing to an extension of k, one could also evaluate functions on infinitesemal neighborhoods of k-points, i.e. compute Taylor expansions near those points.)

We now explain the representation of $J(k)$. Note that for any $x \in J(k)$, we have that $x + [D_0]$ is a divisor class of degree at least $2g + 1$ and hence is equivalent to an effective divisor $E \geq 0$ of degree d_0. Then we represent x by $\mathcal{L}(2D_0 - E)$ inside V_2; by Riemann-Roch this is a d_W-dimensional subspace of V_2 where $d_W = d_0 + 1 - g$, and in particular we can represent it as a $n_z \times d_W$ matrix, itself representing a subspace of k^Z. This representation is nowhere near unique; there are many different effective divisors E equivalent to $x + D_0$, and many bases for a subspace of k^Z.

As explained in Mascot's article, using this representation one can do all relevant computations in $J(k)$; adding, subtracting, finding the zero element, and most importantly: checking equality.

3.1.1 Going from $\mathbb{F}_p$ to $\mathbb{Z}/p^e\mathbb{Z}$

We now know how to compute in $J(k)$ for k a field such that $C(k)$ is big enough. In practice, if we want to calculate in $J(\mathbb{F}_p)$, this means passing to $J(\mathbb{F}_q)$ for some $q = p^a$ with a large enough; by the Hasse-Weil bound this will work. However, for Chabauty we want to compute inside $J(\mathbb{Z}/p^e\mathbb{Z})$. Luckily, Mascots code takes care of this too, by passing from vector spaces over $\mathbb{F}_p$ to free R-submodules of R^n with $R = \mathbb{Z}/p^e\mathbb{Z}$; in fact, all submodules of R^n we will be seeing are free. That means all these submodules will have good reduction, i.e. they will remain free and of the same rank after tensoring with $\mathbb{F}_p$. If the maps between such modules also have good reduction, then all kernels, images, et cetera will also have these properties, and can first be calculated modulo p using linear algebra and then by Hensel lifting modulo higher powers of p.

The final trick we need is extensions of $\mathbb{Z}/p^e\mathbb{Z}$. As said before, we need n_Z affine points that are distinct modulo p, so we passed from $\mathbb{F}_p$ to an extension of $\mathbb{F}_q$. The corresponding notion of an extension of $\mathbb{Z}/p^e\mathbb{Z}$ is given by taking an irreducible polynomial $\overline{T} \in \mathbb{F}_p[t]$ with $\mathbb{F}_q \cong \mathbb{F}_p[t]/\overline{T}$, arbitrarily lifting $\overline{T}$ to a

polynomial $T \in \mathbb{Z}/p^e\mathbb{Z}$, and looking at $R = \mathbb{Z}/p^e\mathbb{Z}[t]/T$. Again, we will only be looking at free submodules of R^n, so we can again do normal linear algebra over $R \otimes \mathbb{F}_p = \mathbb{F}_q$, and using Hensel to lift.

3.2 Implementing the Abel-Jacobi map

Say something about implementing the Abel-Jacobi map $C \to J, Q \mapsto Q - \infty_+$. Right now, information about this (the implementation and why it works) can be found in Hyper2RR.gp.

Now that we can do computations with elements in the Jacobian over $\mathbb{Z}/p^2\mathbb{Z}$, it only remains to construct elements in the Jacobian. Explicitly, we want to go from a degree zero divisor to an element in Mascots representation. Generally these divisors are not always sums of points over the ring we are working with, but if $J(\mathbb{Z})$ is generated by $C(\mathbb{Z})$, then we only need this in cases where divisors are sums of points. Since we can add elements in the Jacobian, for this it is enough to compute the Abel-Jacobi embedding

$$\begin{aligned} j_{\infty_+} : C &\to J \\ P &\mapsto P - \infty_+. \end{aligned}$$

If the degree zero divisor is not a sum of points, one can temporarily pass to an extension, knowing that the result at the end will be defined over the ring we started with. We will only need $j_{\infty_+}(P)$ and $j_{\infty_-}(P)$ for affine points P; as the calculation of $j_{\infty_-}(P)$ is entirely similar to $j_{\infty_+}(P)$, we only focus on $j_{\infty_+}(P)$. For this, we present the following algorithm:

Algorithm 1: The Abel-Jacobi embedding

Data: C, J, an affine point $P \in C(R)$ where $R = \mathbb{Z}/p^e\mathbb{Z})$
Result: A space of the form $\mathcal{L}(2D_0 - E)$ where $E - D_0 = P - \infty_+$ as divisors and $E \geq 0$

$Z' \leftarrow Z \sqcup \{P\}$;
$B = (b_1, \ldots, b_{g+3}) \leftarrow$ a basis of $\mathcal{L}(D_0)$;
if $(f^r)'(0) \neq 0$ **then**
  $F \leftarrow x^{g+1} + y$;
else
  $F \leftarrow x^{g+1} + x^g + y$;
end
$b_{g+4} \leftarrow xF$;
$W \leftarrow$ a $(n_Z + 1) \times (g + 4)$ matrix with rows being the evaluations of $B \sqcup b_{g+4}$ on a point in Z'.;
$V \leftarrow \ker(\operatorname{im} W \subset R^{n_Z+1} \to R)$, the projection on the last coordinate.;
$U \leftarrow \operatorname{im}(V \to R^{n_Z})$, where the last map is the projection on the first coordinates.;
Return U;

Proposition 3.1. *Algorithm 1 gives correct output.*

Before this proof, we start with a quick lemma.

Lemma 3.2. *The poles of F, as defined in line 4 or 6, are exactly $g(\infty_+ + \infty_-) + \infty_+$.*

Proof. We start by recalling that at the other affine patch, the curve C is given by $w^2 = f^r(v)$ and by the assumption that f is monic of degree $2g+2$ we have $f^r(0) = 1$. The points $\infty_\pm$ correspond to $(v, w) = (0, \pm 1)$ in this patch. Letting $g^r(v)$ be the polynomial $(f^r(v) - 1)/v$, we can rewrite the equation for C to $(w-1)(w+1) = vg^r(v)$. As the derivative of $(w-1)(w+1)$ to w doesn't vanish at both of $\infty_\pm$, we see that v is a uniformiser at both these points. That means that $v_{\infty_\pm}(x)$, the order of x at $\infty_\pm$, is equal to -1.

Now, if $g^r(0)$ is non-zero, then $w - \pm 1$ is also a uniformiser at $\infty_\pm$ and non-zero at $\infty_\mp$, so

$$(w+1)/v^{g+1} = y + x^{g+1}$$

has poles exactly $(g+1)(\infty_+ + \infty_-) - \infty_-$ as we wanted to show. And if $g^r(0)$ is zero, then $v_{\infty_\pm}(w - \pm 1)$ is at least 2 so $w - \pm 1 + v$ is a uniformiser at $\infty_\pm$ and non-zero at $\infty_\mp$, so

$$(w + 1 + v)/v^{g+1} = y + x^{g+1} + x^g$$

again has the right poles. □

Proof of Proposition **??**. First note that by Riemann-Roch, the dimension of $\mathcal{L}(D_0)$ is $g+3$, and we also have by the proof of the previous lemma that $1, x, \ldots, x^{g+1}, y$ all lie in $\mathcal{L}(D_0)$ and hence form a basis, so we can indeed find B as in line 2. Note that by Lemma 3.2 the element b_{g+4} lies in $\mathcal{L}(D_0 + \infty_+)$ but not in $\mathcal{L}(D_0)$, so as adding a point to a divisor causes the the dimension to increase by at most 1, we have by that $b_1, \ldots, b_{g+4}$ is a basis for $\mathcal{L}(D_0 + \infty_+)$; that it is in fact a basis is evident as this argument tells us it is a basis when tensored with $\mathbb{F}_p$.

Evaluating $\mathcal{L}(D_0 + \infty_+)$ on P gives a linear map $\mathcal{L}(D_0 + \infty_+) \to R$, and the kernel is exactly $\mathcal{L}(D_0 + \infty_+ - P)$; this is the resulting U in line 10. Furthermore we have the equality of divisors $P - \infty_+ = E - D_0$ where $E = P + D_0 - \infty_+ \geq 0$, so $\mathcal{L}(D_0 + \infty_+ - P)$ is as a subspace of V_2 equal to $\mathcal{L}(2D_0 - E)$. This last term is in fact in Mascots representation, so this represents $P - \infty_+$ in the Jacobian. □

Say something about how with just this map and Mascots code, one can already find the $\overline{\kappa^* f_i}$ and compute an upper bound for $C(\mathbb{Z})_P$ using brute force.

3.3 Speeding up the calculations

Say something about how one express an element in $J(\mathbb{Z}/p^2\mathbb{Z})_0$ on the basis in something like $O(g)$ hopefully (ignoring the time for adding,multiplying, et cetera in the Jacobian), identify $J(Z/p^2)_0$ with F_p^g using g generators of the ideal of the zero section of J_{Z/p^2}, then the group structure that J induces on F_p^g is the usual addition. This is currently done using code from Mascot. Say what the final complexity is.

3.4 An explicit example

Treat the example in ExChabauty.gp.

4 The Poincare torsor

Define and cite theorems about the Poincare Torsor

5 Quadratic Chabauty using the Poincare torsor

Explain how to do Chabauty in the case $r < g + \rho - 1$, where ρ is the Néron-Severirank.

6 Implementations of quadratic Chabauty and an explicit example

Explain something about implementing quadratic Chabauty.

References

[Bou98] Nicolas Bourbaki. *Commutative algebra. Chapters 1–7*. Elements of Mathematics (Berlin). Springer-Verlag, Berlin, 1998. Translated from the French, Reprint of the 1989 English translation.

[GD71] A. Grothendieck and J. A. Dieudonné. *Eléments de géométrie algébrique. I*, volume 166 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Sciences]*. Springer-Verlag, Berlin, 1971.

[HON70] Taira HONDA. On the theory of commutative formal groups. *J. Math. Soc. Japan*, 22(2):213–246, 04 1970.

[KM04] Kamal Khuri-Makdisi. Linear algebra algorithms for divisors on an algebraic curve. *Math. Comp.*, 73(245):333–357, 2004.

[Mas18] Nicolas Mascot. Hensel-lifting torsion points on jacobians and galois representations, 2018.

[Par00] Pierre Parent. Torsion des courbes elliptiques sur les corps cubiques. *Ann. Inst. Fourier (Grenoble)*, 50(3):723–749, 2000.