Second p-Descent on elliptic curves (or: Descent on genus one normal curves of prime degree)

Brendan Creutz

Rational Points 3, July 2010

Notation

- k is a number field.
- G_k is the absolute Galois group.
- p is a prime number.

Let C/k be an everywhere locally solvable genus one normal curve of degree p,

The model for C

- $p = 2$: a double cover of $\mathbb{P}^1$ ramified in 4 points
- $p = 3$: a cubic curve in $\mathbb{P}^2$
- $p \geq 5$: an intersection of $p(p-3)/2$ quadrics in $\mathbb{P}^{p-1}$

Remark

C represents an element of $\mathrm{Sel}^{(p)}(E/k)$ which sits in the exact sequence

$$0 \to E(k)/pE(k) \to \mathrm{Sel}^{(p)}(E/k) \to Ш(E/k)[p] \to 0\,.$$

An explicit p-descent on E computes $\mathrm{Sel}^{(p)}(E/k)$ and produces models for its elements as genus one normal curves of degree p as above.

p-coverings

Definition

A p-covering of C is an uramified Galois covering $D \xrightarrow{\pi} C$ with Galois group isomorphic (as a G_k-module) to $E[p]$. Define $\mathrm{Sel}^{(p)}(C/k)$ to be the set of isomorphism classes of p-coverings of C that are everywhere locally solvable.

Goal 2: Do a second p-descent.

Compute $\mathrm{Sel}^{(p)}(C/k)$.

Note: This might achieve Goal 1.

If $\mathrm{Sel}^{(p)}(C/k) = \emptyset$, then $C(k) = \emptyset$.

Flex Points

From now on p is an odd prime.

Definitions

- Let X denote the set of flex points of C.
- Let Y be the set of divisors on C of the form:

  $(p-2)[x] + [x+P] + [x-P]$, with $x \in X$ and $P \in E[p]$.

Remarks

- The action of E on C restricts to an action of $E[p]$ on X.
- X is a G_k-set and $\#X = p^2$.
- Y is a G_k-set of hyperplanes sections of C supported on X.

Etale algebras

Etale k-algebras

Corresponding to these finite G_k-sets we have étale k-algebras.

- $F := \mathrm{Map}_k(X, \bar{k})$, the 'flex algebra'
- $H := \mathrm{Map}_k(Y, \bar{k})$, the 'hyperplane algebra'

The induced norm map

The action of G_k on Y is derived from that of G_k on X. This gives rise to an induced norm map, $\partial : F \to H$.

$$\text{For } \varphi \in F \text{ and } y \in Y, \text{ we have } \partial\varphi(y) = \prod_{x \in y} \varphi(x).$$

Descent on $\mathrm{Pic}_k(C)$

A family of functions

Choose a G_k-equivariant family $f : Y \to \kappa(\bar{C})^\times$ of rational functions such that $\mathrm{div}(f_y) = y - \Delta$ where Δ is an effective divisor on C with support disjoint from X.

Proposition

The family f induces a unique homomorphism

$$\tilde{f} : \mathrm{Pic}_k(C) \to \frac{H^\times}{k^\times \partial F^\times}$$

with the property that, for any $Z \in \mathrm{Pic}_k(C)$, $\tilde{f}(Z) \equiv f(z)$ where z is any k-rational divisor representing Z with support disjoint from all poles and zeros of the f_y.

Descent on C

Remark

The proposition is functorial in k.

We have a commutative diagram:

$$\begin{tikzcd}
C(k) \arrow[r, equal] \arrow[d] & \mathrm{Pic}^1_k(C) \arrow[r, "\tilde{f}"] \arrow[d] & \frac{H^\times}{k^\times \partial F^\times} \arrow[d, "\prod \mathrm{res}_v"] \\
\prod_v C(k_v) \arrow[r, equal] & \prod_v \mathrm{Pic}^1_{k_v}(C) \arrow[r, "\prod \tilde{f}_v"] & \prod_v \frac{H_v^\times}{k_v^\times \partial F_v^\times}
\end{tikzcd}$$

One should consider $\bigcap_v \mathrm{res}_v^{-1}(\tilde{f}_v(\mathrm{Pic}^1_v(C))) \subset \frac{H^\times}{k^\times \partial F^\times}$.

Descent on C

Theorem 1

There is a bijective map
$\mathrm{Sel}^{(p)}(C/k) \xrightarrow{1:1} \left\{ \delta \in \frac{H^\times}{k^\times \partial F^\times} : \forall v,\ \mathrm{res}_v(\delta) \in \tilde{f}(\mathrm{Pic}^1_v(C)) \right\}$.

Theorem 1 (version 2)

There exists a finite set of primes S of k such that
$$\mathrm{Sel}^{(p)}(C/k) \xrightarrow{1:1} \left\{ \delta \in \frac{H^\times}{k^\times \partial F^\times} : \begin{array}{c} \delta \text{ is unramfied outside } S \text{ and} \\ \forall v \in S, \mathrm{res}_v(\delta) \in \tilde{f}_v(Pic^1_v(C)) \end{array} \right\}.$$

Computing $\mathrm{Sel}^{(p)}(C/k)$

H splits as $H \simeq F \times H_2$. Projection onto the first factor induces a surjective map $\frac{H^\times}{k^\times \partial F^\times} \to \frac{F^\times}{k^\times F^{\times p}}$ with finite kernel.

Corollary

There is an algorithm for computing (a set of representatives in $H^\times$ for) $Sel^{(p)}(C/k)$ that is efficient modulo

- computing S-class and -unit group information in F and
- extracting p-th roots of elements in $H_2^{\times p}$.

Remark

For $p = 3$ and $k = \mathbb{Q}$ this means computations are feasible in practice.

Models in projective space

Theorem 2

Given $\delta \in H^{\times}$ representing some p-covering (D, π) we can explicitly compute a set of $p^2(p^2 - 3)/2$ quadrics giving a model for D as a genus one normal curve of degree p^2 in $\mathbb{P}^{p^2-1}$.

Minimization and Reduction

Once we have produced a model, we would like to make a change of coordinates on $\mathbb{P}^{p^2-1}$ to get a nice model (i.e. with small coefficients and as few primes as possible dividing the invariants). I don't know how to do this...