Global Duality and the Discrete Logarithm Problem for Abelian Algebraic Groups Finite Fields

Ming-Deh Huang and Wayne Raskind

October 12, 2006

Let $\mathbb{F}$ be a perfect field and $\overline{\mathbb{F}}$ an algebraic closure of $\mathbb{F}$. Let $\tilde{G}$ be a connected algebraic group over $\mathbb{F}$. Thus $\tilde{G}$ is a group that has the structure of an algebraic variety such that the group operations are morphisms of algebraic varieties. It is known (Chevalley, Rosenlicht) that an abelian algebraic group sits in an exact sequence:

$$0 \to L \to \tilde{G} \to B \to 0,$$

where L is an abelian linear algebraic group (a closed algebraic subgroup of some general linear group GL_n) and B is an abelian variety. Then it is known that $L = S \times U$, where S is a torus and U is unipotent. That is, $S \cong \mathbb{G}_m^d$ over $\overline{\mathbb{F}}$, where $\mathbb{G}_m$ is the multiplicative group. We will say that $\tilde{G}$ has no unipotent part if $U = 0$. We will assume this from now on, although we do not think it is necessary. Suppose now that

$\mathbb{F}$ is a finite field and that $\tilde{G}$ may be lifted to an algebraic group G over an algebraic number field. That is, suppose there exists a discrete valuation ring A whose fraction field is an algebraic number field K and whose residue field is our finite field $\mathbb{F}$, and an algebraic group $\mathcal{G}$ over A whose fibre over $\mathbb{F}$ is our $\tilde{G}$. The functor $\mathrm{Hom}(-, \mathbb{G}_m)$ need not be exact and we consider its "total derived functor" $\mathrm{RHom}(-, \mathbb{G}_m)$.

Then there should be a derived cup-product pairing:

$$< , >: \ H^i(K, G) \times H^{2-i}(K, \mathsf{RHom}(G, \mathbb{G}_m)) \to H^2(K, \mathbb{G}_m).$$

If this seems too abstract, here are some examples:

The Multiplicative Group: Suppose G is the multiplicative group $\mathbb{G}_m$ over $\mathbb{F}$. We can lift this to the

multiplicative group over any algebraic number field K having a place v with residue field $\mathbb{F}$. We have:

$$\mathsf{RHom}(\mathbb{G}_m, \mathbb{G}_m) \cong \mathbb{Z}.$$

Now $H^2(K, \mathbb{Z}) \cong H^1(K, \mathbb{Q}/\mathbb{Z})$ and the pairing becomes:

$$K^* \times H^1(K, \mathbb{Q}/\mathbb{Z}) \to Br(K).$$

This is the norm residue symbol that is familiar from class field theory. If v is a nonarchimedean place we have $Br(K_v) \cong \mathbb{Q}/\mathbb{Z}$ and the reciprocity law: for $\alpha \in H^i(K, G)$ and $\beta \in H^{2-i}(K, \mathsf{RHom}(\tilde{G}, \mathbb{G}_m))$,

$$\sum_v < \alpha_v, \beta_v >= 0.$$

Elliptic Curves Let $\tilde{E}$ be an elliptic curve over $\mathbb{F}$. Then $\tilde{E}$ may

be lifted to an elliptic curve over an algebraic number field K. In this case, we have that

$$H^2(K, \mathsf{RHom}(E, \mathbb{G}_m)) \cong H^1(K, E).$$

Then our pairing becomes one that is familiar from the theory of elliptic curves:

$$E(K) \times H^1(K, E) \to Br(K).$$

Basic Method: Lift the discrete log problem over $\mathbb{F}$ to a suitable K and a place v of K with residue field $\mathbb{F}$ such that the discrete log may be computed in K_v via the homomorphism $G(A_v) \to \tilde{G}(\mathbb{F})$, where A_v is the valuation ring of K_v. That is, given $\tilde{\alpha} \in \tilde{G}(\mathbb{F})$ in the subgroup generated by b, lift

$\tilde{\alpha}$ to some α in $G(A_v)$. Then find a good "test element" $\beta \in H^2(K, \mathsf{RHom}(G, \mathbb{G}_m))$ and use the reciprocity law to shift the computation of $< \alpha_v, \beta_v >$ to other places where we might hope it will be easier. If β is very well chosen, there will be few other terms in this sum. This method seems very robust. The technique of index calculus for the multiplicative group may be viewed

as a particular choice of Dirichlet character β.

To produce such a β, we use exact sequences from global duality, which sometimes guarantee the existence of an appropriate β. The extent to which β must be known explicitly is not clear, and it seems that much information can be learned from the interaction of β with α.

This method is not new and has been discussed by several authors including Frey, Frey-Rück and Nguyen

Our approach to the discrete log problem for the multiplicative group of a finite prime field $\mathbb{F}_p$ uses the Poitou-Tate duality sequence for $G = \mathbb{Z}/\ell\mathbb{Z}$, where U is an open subset of the ring of integers in a real quadratic field. For the discrete log problem for an elliptic curve $\tilde{E}$ over a finite field with

a point of order ℓ and an suitable lifting E of $\tilde{E}$ to an algebraic number field K, we take $G = \mathcal{E}$, where U is an open subset of Spec($\mathcal{O}_K$) on which E has good reduction and ℓ is invertible, and $\mathcal{E}$ is a smooth proper model of E over U. We will need to assume the finiteness of the Shafarevich-Tate group of such an E. This is not known, in general, but it has been proved in many cases for E of small rank. In each

case, the method will be to find a suitable element of $H^1(U, G)[\ell]$ against which to "test" a lifting to K of an element over the finite field whose discrete log we seek to compute, using the reciprocity law that is encoded in the duality of class field theory (resp. duality for elliptic curves over number fields). Let U be a suitable open subset of $\mathrm{Spec}(\mathcal{O}_K)$ and let $G = \mathbb{Z}/\ell\mathbb{Z}$ or $\mathcal{E}$ according

to whether we are in the multiplicative group or elliptic curve case. Actually, it will be somewhat easier to construct the required element of $H^1(U,G)[\ell]^*$, the Pontryagin dual of $H^1(U,G)[\ell]$, using the exact sequences:

$$\cdots H^1(U,\mu_\ell) \to \bigoplus_{v\in S} H^1(K_v,\mu_\ell) \to H^1(U,\mathbb{Z}/\ell\mathbb{Z})^*$$

for the multiplicative case and

$$E(K)^{(\ell)} \to \bigoplus_{v\in S} E(K_v)^{(\ell)} \to H^1(U,\mathcal{E})\{\ell\}^* \cdots$$

for the elliptic curve case. Here the superscript (ℓ) denotes completion with respect to subgroups of ℓ-power index.

The first sequence always exists, and if ℓ does not divide the order of the class group of $\mathcal{O}_K$, then the last map is surjective. The second exists if one assumes finiteness of the ℓ-primary component of the Shafarevich-Tate group of E (see [MAD], II, §5, Theorem

5.6); this is an expression of *global duality for elliptic curves*. It is usually called the *Cassels-Tate* sequence and written in the form:

$$E(K) \to \prod_v E(K_v) \to$$

$$H^1(K, E)^* \to Ш(E)$$

where $Ш(E)$ denotes the Shafarevich-Tate group of E.

We then use the following simple strategy. First, compute the dimension as $\mathbb{F}_\ell$-vector space of the local groups $H^1(K_v, G)^*$. This is not that hard to do in either case. Second, look for an algebraic number field K (resp. an algebraic number field K together with an elliptic curve E/K that lifts $\tilde{E}$) such that the $\mathbb{F}_\ell$-dimension of the first term is smaller than that of the second. This will then guarantee the existence of

a nontrivial element in $H^1(U, G)[\ell]^*$. In the multiplicative group case, this can be easily accomplished by taking for K a real quadratic field in which ℓ and p split, taking for S the set consisting of one prime v above ℓ and one w above p, and making the mild hypothesis that the fundamental unit is not an ℓ-th power in at least one of $\mathcal{O}_v^* = \mathbb{Z}_\ell^*$ or $\mathcal{O}_w^* = \mathbb{Z}_p^*$. In the elliptic curve case, it is much trickier, as one must find

a curve of small rank, e.g. 2. We believe that this is very reasonable, heuristically.

One case that is promising is when $\ell - 1$ is sufficiently smooth.