A Unified Approach to the Discrete Logarithm Problem for the Multiplicative Group and for Elliptic Curves over Finite Fields

Ming-Deh Huang and Wayne Raskind

September 20, 2004

Index calculus has had much success in treating the discrete logarithm problem for the multiplicative group of a finite field, but less so for elliptic curves over finite fields. In this lecture, we propose a unified method for treating both problems.

For the discrete logarithm problem over a finite field $\mathbb{F}_q$, one takes random liftings of elements of the muliplicative group to algebraic integers and derives relations between discrete logs using the primes dividing the lifts. This may be regarded as lifting the problem from $\mathbb{F}_q^*$ to $\mathcal{O}_S^*$, where $\mathcal{O}_S$ is the ring of S-integers of $\mathcal{O}$, for a suitable finite set S of places of the ring of integers $\mathcal{O}$ of an algebraic number field K. In the elliptic curve case, one lifts the curve $\tilde{E}$ over a finite field to a curve E over an algebraic number field K. But there is a big difference between these two cases: in the first case, the multiplicative group is an *affine* algebraic group, whereas in the second, the elliptic curve is *projective*. We propose to treat the discrete log problem for the multiplicative group as much as possible as a "projective" problem by lifting to the full ring of integers of a suitable algebraic number field and to pursue the analogies of our proposed solution with the elliptic curve case. As mentioned in Huang's talk, what is necessary in the elliptic curve case is to construct good lifted curves of *small* Mordell-Weil rank, rather than having to construct curves of large rank, as is required with index calculus.

Before describing our approach,

we need to recall the six functors of sheaf theory in algebraic geometry. Let $X = \mathrm{Spec}(\mathcal{O}_K)$, where K is an algebraic number field. Let U be a nonempty open subset of X and Z the complement. Thus U consists of all but finitely many places of K. We denote by j the inclusion of U in X and by i the inclusion of Z in X. Then we have the six functors: $j_*, j^*, i_*, i^*, j_!$ and $i^!$. The first four are familiar, given by direct and inverse image. The functor $j_!$ is extension by zero and $i^!$ is to form the subsheaf with support in Z. We have the sequences of adjoints:

$$j_! \dashv j^* \dashv j_*$$

$$i^* \dashv i_* \dashv i^!.$$

As it can be difficult to remember which functors are adjoint to which, here is a rule of thumb: A functor with an upper star (e.g.

i^*) is always left adjoint to a functor with a lower star (e.g. i_*). If you can't make a sequence of three functors, each left adjoint to the one to its right, then you have not recalled them correctly. We will consider exclusively sheaves and cohomology for the small étale site on X, which means that we consider the category of schemes that are étale over X with the étale topology. Let F be any sheaf on X and v a closed point.

Then we have the cohomology with support $H^i_v(X, F)$, which may also be described as $H^i(v, i^! F)$. Let A^h_v be the Henselization of X at v. This is a direct limit over étale neighborhoods of v in X; that is, the direct limit over rings A_i such that A_i is étale over the local ring of v in X and such that there is a closed point w of Spec(A_i) lying over v with the same residue field. In what follows, one may take completion instead of Henselization. By excision, we have

$$H^i_v(X, F) \cong H^i_v(A^h_v, F).$$

This provides a useful way of computing this cohomology. If K_v is the fraction field of A^h_v, then we have a long exact sequence of cohomology with support:

$$H^i_v(A^h_v, F) \to H^i(A^h_v, F)$$

$$\to H^i(K_v, F) \to H_v^{i+1}(A_v^h, F) \cdots .$$

If F is a sheaf of the form $j_!G$, for a sheaf G on U then we have for $v \in Z$

$$H^i(K_v, F) \cong H_v^{i+1}(A_v^h, F)$$

(see [MAD], Proposition 1.1, page 182). Thus for a sheaf of the form $j_!G$, we have a long exact sequence of cohomology with support:

$$\cdots \to H_Z^i(X, j_!G) \to H^i(X, j_!G)$$

$$\to H^i(U, j^*j_!G) \to H_Z^{i+1}(X, j_!G) \to \cdots$$

and using the result just mentioned and the definition (resp. identification)

$$H_c^i(U, G) = H^i(X, j_!G)$$

(the left side is usually called cohomology of U with compact support) and

$$H^i(U, G) = H^i(U, j^*j_!G),$$

we get the sequence:

$$\cdots \to H^i_c(U,G) \to H^i(U,G) \to$$

$$\bigoplus_{v \in Z} H^i(K_v,G) \to H^{i+1}(U,G) \cdots \to .$$

Our approach to the discrete log problem for the multiplicative group of a finite prime field $\mathbb{F}_p$ uses this sequence for $G = \mathbb{Z}/\ell\mathbb{Z}$, where U is an open subset of the ring of integers in a real quadratic field in which both p and ℓ split. For the discrete log problem for an elliptic curve $\tilde{E}$ over a finite field with a point of order ℓ and a 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, which is defined to be

$$\text{ker}[H^1(K,E) \to \bigoplus_v H^1(K_v,E)].$$

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 order ℓ in $H^1(U,G)$ against which to "test" liftings to K of elements of the multiplicative group (resp. rational points on the elliptic curve) over the finite field, 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 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 order ℓ starting from $H^1(U, G)^*$, the Pontryagin dual of $H^1(U,G)$, 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 and for an abelian group A, $A\{\ell\}$ denotes the ℓ-primary subgroup of A.

The sequence (*) always exists, and we have seen in Huang's talk that if ℓ does not divide the order of the class group of $\mathcal{O}_K$, then the last map is surjective. The sequence (**) 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 using all the places of K:

$$\widehat{E(K)} \to \prod_{v} E(K_v) \to$$

$$H^1(K, E)^* \to \mathcal{ST}(E) \to 0,$$

where $\hat{}$ denotes the completion of the group $E(K)$ with respect to the topology of subgroups of finite index and $\mathcal{ST}$ denotes the Shafarevich-Tate group of E.

We then use the following basic strategy. In the multiplicative groups case, compute the dimension as $\mathbb{F}_\ell$-vector space of the local groups $H^1(K_v, \mu_\ell)$. This is easy to do. Second, look for an algebraic number field K such that the $\mathbb{F}_\ell$-dimension of the image of the first term of the exact sequence (*) above in the second term is smaller than the $\mathbb{F}_\ell$-dimension of the second. If this is satisfied, then we are guaranteed the existence of a nontrivial element in $H^1(U, \mathbb{Z}/\ell\mathbb{Z})$ with the required ramification properties. One can take 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 hypothesis that ℓ does not divide the order of the class group of K and that the fundamental unit in K 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, we seek an algebraic number field K together with an elliptic curve E/K that lifts $\tilde{E}$, and whose group of points $E(K)$ is of small rank, e.g. 1. Then the exact sequence (**) above will guarantee us an element of order ℓ in $H^1(U, \mathcal{E})$ with the desired ramification properties. We believe that it is very reasonable, heuristically, that such curves should exist, although it is not known at present how to actually find them.

References

[MET] J.S. Milne, Etale Cohomology, Princeton Mathematical Series, Volume 33, Princeton University Press 1980

[MAD] J.S. Milne, Arithmetic Duality Theorems, Perspectives in Mathematics, Academic Press 1986