

# Global Methods for Discrete Logarithm Problems I: A Unified Approach for the Multiplicative Group and for Elliptic Curves over a Finite Field

Ming-Deh Huang and Wayne Raskind

Let  $A$  be a finite abelian group and  $x$  an element of  $A$ . Let  $y$  be in the subgroup generated by  $x$ , so that  $y = nx$  for some positive integer  $n$ . Recall that the *discrete logarithm problem* is to determine  $n$  in a computationally efficient way. The computational complexity of solving this problem when the bit size of the inputs is large is the basis of many public-key encryption schemes used today. Two of the most important examples of finite abelian groups that are used in public-key cryptography are the multiplicative group of a finite field and the group of points on an elliptic curve over a finite field (see [K] and [Mill] for the original papers and [KMV] for a survey of work as of 2000).

In what follows below, we will assume that  $\ell$  is a large prime number dividing the order of  $A$  and that  $x$  is an element of order  $\ell$ . For  $p$  a prime number and  $q$  a power of  $p$ , we denote by  $\mathbb{F}_q$  the finite field with  $q$  elements and by  $\mathbb{F}_q^*$  its multiplicative group of nonzero elements.

Index calculus has been successful in many cases for treating the discrete logarithm problem for the multiplicative group of a finite field (see e.g. [Mc], §5 or [SWD]), but less so for elliptic curves over a finite field (see e.g. [HKT] or [JKSST]). This is the first in a series of at least three papers in which we seek to “explain” why this might be the case from the perspective of arithmetic duality and propose a unified method for treating both problems. We will treat the multiplicative group case in more detail in the second paper [HR1] and the elliptic curve case in more

detail in the third [HR2]. In [HR1] we approach the discrete logarithm problem for the multiplicative group of a finite prime field  $\mathbb{F}_p$  by lifting points to a real quadratic field  $K$  and deriving relations by using the reciprocity law of global class field theory. We then prove the random polynomial time equivalence of the discrete logarithm problem with the problem of computing the ratios of “signatures”, which are values (in  $\mathbb{Z}/\ell\mathbb{Z}$ ) at places of  $K$  above  $p$  and  $\ell$  of local pairings of a certain Dirichlet character of  $K$  with liftings of units of  $\mathbb{F}_p$  to units of the ring of integers of  $K$ . In [HR2], we pursue an analogous strategy for an elliptic curve over  $\mathbb{F}_p$ , using liftings of the curve and some of its points to an algebraic number field and computing the ratios of the pairings at places above  $p$  and  $\ell$  of the lifted points with certain principal homogeneous spaces of order  $\ell$  under the lifted curve. In this case, we must make the assumption that we can find a lifted curve whose Mordell-Weil group of rational points is of *small* rank and whose Shafarevich-Tate group of everywhere locally trivial principal homogeneous spaces is finite. While this is unproven, in general, the first condition is considered to be very reasonable and the second is known in some cases and expected to always be true. This strategy is in contrast to previous attempts to use index calculus in the elliptic curve case, which required lifted curves of *large* Mordell-Weil rank. To distinguish our methods from those of index calculus, we refer to them as *signature calculus*. The main purpose of this paper is to introduce this method and hopefully convince the reader that it is more robust than index calculus.

The idea of using global methods in this way was originally proposed by Frey [F], whom we thank for inspiration, helpful discussions and for inviting us to present our work at the Elliptic Curve Cryptography (ECC) conference in Bochum in September 2004. Methods of this type have also been used by Frey and Rück [FR], Nguyen [N] and by Huang, Kueh and Tan [HKT].

## 1. Global Framework

### 1.1. Notation and Review of Algebraic Number Theory.

This subsection is meant primarily to fix notation and to recall some basic concepts from algebraic number theory. Let  $K$  be a field that is a finite extension of the field of rational numbers  $\mathbb{Q}$ . We call such a field an *algebraic number field*. We fix an algebraic closure  $\overline{K}$  of  $K$  and let  $G = \text{Gal}(\overline{K}/K)$ . We consider equivalence classes of absolute values on

$K$ , which are in one-to-one correspondence with the prime ideals of the ring of integers of  $K$  together with the absolute values obtained by the various embeddings of  $K$  in the real or complex numbers. An equivalence class of absolute value will be denoted by  $v$  and called a *place*. For each  $v$ , we denote by  $K_v$  the completion of  $K$  with respect to the corresponding absolute value. This field will be either a finite extension of the field of  $p$ -adic numbers  $\mathbb{Q}_p$  for some prime  $p$  (nonarchimedean), the real numbers or the complex numbers (archimedean). As most of our discussion will pertain to abelian groups that are  $\ell$ -torsion, where  $\ell$  is an odd prime number, we shall ignore for the most part the real places.

Recall that the Brauer group  $Br(K)$  is an abelian group that classifies the equivalence classes of central simple algebras over  $K$ , where two such algebras  $A$  and  $B$  are equivalent if there are matrix algebras  $M_n(K), M_m(K)$  such that

$$A \otimes_K M_n(K) \cong B \otimes_K M_m(K).$$

We have that  $Br(K_v) \cong \mathbb{Q}/\mathbb{Z}$  if  $v$  is nonarchimedean,  $Br(\mathbb{R}) \cong \mathbb{Z}/2\mathbb{Z}$  and  $Br(\mathbb{C}) = 0$ . We can describe  $Br(K)$  in terms of Galois cohomology by

$$Br(K) \cong H^2(G, \overline{K}^*).$$

One of the most important results in algebraic number theory is the exact sequence:

$$(*) \quad 0 \rightarrow Br(K) \rightarrow \sum_v Br(K_v) \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0.$$

This is the beginning of the theory of *global duality*, which shows how to relate the arithmetic of  $K$  with that of all of the  $K_v$ . The following subsections review this theory briefly in the context in which we shall use it.

### 1.2. Reciprocity Law for the Case of Multiplicative Group.

We review the reciprocity law in this context, mostly following the exposition of ([Se], Chapter XIV). Let  $K^*$  denote the set of nonzero elements of  $K$ , which is an abelian group under multiplication. A Dirichlet character  $\chi$  of  $K$  is a homomorphism of  $G = Gal(\overline{K}/K)$  into  $\mathbb{Q}/\mathbb{Z}$ , which we view as an element of the Galois cohomology group  $H^1(G, \mathbb{Q}/\mathbb{Z})$ . Let  $\partial(\chi)$  denote the image of  $\chi$  under the boundary map

$$H^1(G, \mathbb{Q}/\mathbb{Z}) \xrightarrow{\partial} H^2(G, \mathbb{Z})$$

in the long exact cohomology exact sequence associated to the short exact sequence of  $G$ -modules with trivial action:

$$0 \rightarrow \mathbb{Z} \rightarrow \mathbb{Q} \rightarrow \mathbb{Q}/\mathbb{Z} \rightarrow 0.$$

Then for  $a \in K^*$  we consider

$$\langle \chi, a \rangle = \partial(\chi) \cup a \in H^2(G, \overline{K}^*)$$

under the pairing:

$$K^* = H^0(G, \overline{K}^*) \times H^2(G, \mathbb{Z}) \rightarrow H^2(G, \overline{K}^*) \cong Br(K).$$

If  $K$  is nonarchimedean, then  $Br(K) \cong \mathbb{Q}/\mathbb{Z}$ , so that we can view  $\langle \chi, a \rangle$  as an element of  $\mathbb{Q}/\mathbb{Z}$ . If  $K$  is an algebraic number field,  $\chi \in H^1(G, \mathbb{Q}/\mathbb{Z})$ ,  $a \in K^*$  and  $v$  is a place of  $K$ , then we can restrict  $\chi$  to each  $K_v$  and regard  $a$  as an element of  $K_v^*$ . We then denote the local pairing by  $\langle \chi_v, a_v \rangle_v$ . Note that if  $v$  is a place where  $\chi$  is unramified and  $a$  is a unit at  $v$ , then  $\langle \chi_v, a_v \rangle_v = 0$ . Thus  $\langle \chi_v, a_v \rangle_v = 0$  for all but finitely many  $v$ . Since the local pairings are compatible with the global pairings, the exact sequence (\*) above for the Brauer group of an algebraic number field shows that we have the *reciprocity law*

$$\sum_v \langle \chi_v, a_v \rangle_v = 0 \in \mathbb{Q}/\mathbb{Z}.$$

**1.3. Reciprocity Law for the Case of Elliptic Curves.** Let  $E$  be an elliptic curve over  $K$ . Thus  $E$  is a smooth, projective algebraic curve of genus 1 together with a distinguished rational point  $O$ , which serves as the identity element in an abelian group structure on  $E$  that can be defined geometrically by a chord and tangent method. We can write an affine equation for  $E$  in Weierstrass form

$$y^2 = x^3 + ax + b,$$

where  $a$  and  $b$  are in the ring of integers  $K$  with  $4a^3 + 27b^2 \neq 0$ . This last condition ensures that the polynomial  $x^3 + ax + b$  has no double roots. If  $\mathfrak{p}$  is a prime ideal of the ring of integers of  $K$  with residue field  $\mathbb{F}$  of characteristic at least 5 and  $\mathfrak{p}$  does not divide  $4a^3 + 27b^2$ , then we get an elliptic curve  $\tilde{E}$  over  $\mathbb{F}$ . We call  $E$  a *lifting* of  $\tilde{E}$  to  $K$ . We denote by  $\tilde{E}(\mathbb{F})$  the set of solutions of this equation with  $x$  and  $y$  in  $\mathbb{F}$ , together with a

point “at infinity” and by  $E(K)$  the set of rational points of  $E$  over  $K$ . Recall that a *principal homogeneous space* of  $E$  over  $K$  is a curve  $F$  of genus 1 over  $K$  together with a group action of  $E$  on  $F$ . The isomorphism classes of such principal homogeneous spaces are classified by the group  $H^1(G, E(\overline{K}))$ , where  $G = \text{Gal}(\overline{K}/K)$ . A principal homogeneous space is trivial if and only if it has a rational point over  $K$ , in which case it is isomorphic to  $E$  over  $K$ . Thus any principal homogeneous space becomes isomorphic to  $E$  over a finite extension of  $K$ . Let  $Q$  be a point of  $E$ . Then we consider the pairings

$$\langle \alpha, Q \rangle \in \text{Br}(K)$$

$$\langle \alpha_v, Q_v \rangle_v \in \text{Br}(K_v) \cong \mathbb{Q}/\mathbb{Z}$$

These are not as easy to describe explicitly as in the case of the multiplicative group, but we give here a quick if somewhat terse definition. Given an abelian variety  $A$  over  $K$ , let  $\hat{A}$  denote its dual, which is  $\text{Ext}_K^1(A, \mathbb{G}_m)$ , where  $\mathbb{G}_m$  is the multiplicative group scheme and the  $\text{Ext}$  is taken in the category of algebraic groups over  $K$ . An elliptic curve is self-dual, so that we can identify  $E(K)$  with  $\text{Ext}_K^1(E, \mathbb{G}_m)$ . Given  $Q \in E(K)$ , represent it as a 1-extension of algebraic groups using this identification

$$0 \rightarrow \mathbb{G}_m \rightarrow X \rightarrow E \rightarrow 0,$$

and let

$$(**) 0 \rightarrow \overline{K}^* \rightarrow X(\overline{K}) \rightarrow E(\overline{K}) \rightarrow 0$$

be the short exact sequence of  $\overline{K}$ -points of these groups. Then given an element  $\alpha \in H^1(G, E(\overline{K}))$ , let  $\partial_Q(\alpha)$  be the image of  $\alpha$  under the boundary map:

$$H^1(G, E(\overline{K})) \xrightarrow{\partial_Q} H^2(G, \overline{K}^*)$$

in the long exact cohomology sequence obtained from the short exact sequence (\*\*). We can make a similar definition over the nonarchimedean fields  $K_v$  for  $\alpha \in H^1(G_v, E(\overline{K}_v))$  and  $Q \in E(K_v)$  to get  $\langle \alpha, Q \rangle_v \in \text{Br}(K_v) \cong \mathbb{Q}/\mathbb{Z}$ . For  $\alpha \in H^1(G, E(\overline{K}))$  and  $Q \in E(K)$  we denote by  $\alpha_v$  the image of  $\alpha$  in  $H^1(G_v, E(\overline{K}_v))$  (which may be zero) and by  $Q_v$  the image of  $Q$  in  $E(K_v)$ . We then have that  $\langle \alpha_v, Q_v \rangle_v = 0$  for almost all  $v$  and the *reciprocity law*:

$$\sum_v \langle \alpha_v, Q_v \rangle_v = 0 \in \mathbb{Q}/\mathbb{Z}.$$

## 2. The Index Calculus Method

The basic idea in our unified approach for discrete-log problems is as follows. Suppose we lift the problems from a finite field  $\mathbb{F}_p$  to a global field  $K$  where discrete logarithms are preserved at a place over  $p$ . The reciprocity laws then allow us to distribute information of the discrete logarithms among a set of places. This set of places depend on the choice of a Dirichlet character (resp. homogeneous space) and the manner of lifting. In this section we demonstrate how the classical index calculus method emerges in this context as the result of one particular choice of Dirichlet character and method of lifting.

Let  $p$  and  $\ell$  be odd primes such that  $p \equiv 1 \pmod{\ell}$  but  $p \not\equiv 1 \pmod{\ell^2}$ . Suppose  $t = s^n$  in  $\mathbb{F}_p^*[\ell]$  and  $n$  is to be computed, given  $s$  and  $t$ . Let  $K$  be a number field with a place  $v$  over  $p$  such that the residue field  $\mathbb{F}_v$  is isomorphic to  $\mathbb{F}_p$ . Let  $\alpha, \beta \in O_K$  be lifting of  $s$  and  $r = s^a t$  (with  $a$  random) so that  $\alpha \equiv s \pmod{v}$  and  $\beta \equiv r \pmod{v}$ . Then the relation  $r = s^{n+a}$  is preserved at  $v$  in the sense that  $\beta = \alpha^{n+a} \gamma^\ell$  for some  $\gamma \in O_v$ . Therefore for all  $\chi \in H^1(K, \mathbb{Z}/\ell\mathbb{Z})$ ,  $\langle \chi, \beta \rangle_v = (a+n) \langle \chi, \alpha \rangle_v$ . It follows that

$$(a+n) \langle \chi, \alpha \rangle_v = \langle \chi, \beta \rangle_v = - \sum_{u \neq v} \langle \chi, \beta \rangle_u.$$

Note that if  $\chi$  is ramified at  $v$ , then  $\langle \chi, \alpha \rangle_v \neq 0$  since the class of  $\alpha$  generates  $O_v^*/\ell \cong \mathbb{F}_p^*/\ell \cong \mathbb{F}_p^*[\ell]$ .

In particular by choosing  $K = \mathbb{Q}$ , lifting  $s$  to  $s$  (considered as an integer), targeting the lifting  $r$  to some  $\beta$  which is smooth over a factor base, and choosing  $\chi$  to be ramified only at  $p$ ,

$$(a+n) \langle \chi, s \rangle_p = \langle \chi, \beta \rangle_p = - \sum_q e_q \langle \chi, q \rangle_q$$

where  $\beta = \prod_q q^{e_q}$ . If  $\beta$  is  $B$ -smooth then we get a linear relation modulo  $\ell$  of  $n$  and  $\langle \chi, q \rangle_q (\langle \chi, s \rangle_p)^{-1}$ ,  $q < B$ , and  $O(B)$  relations will allow us to solve for the unknown quantities, including  $n$ . What we have derived is in essence the classical index calculus method.

The reason why index calculus is viable in the multiplicative case is due to the fact that locally unramified Dirichlet characters are nontrivially paired with primes. In particular,  $\langle \chi, q \rangle_q \neq 0$  if  $\chi$  is unramified and nontrivial at  $q$ . Similar observation holds for  $K$  being a number field as well.

In contrast, for an elliptic curve  $E$  defined over a number field  $K$ , though we similarly have from reciprocity law

$$0 = \sum_v \langle \chi_v, \alpha_v \rangle_v$$

for  $\chi \in H^1(G, E(\overline{K}))[\ell]$  and  $\alpha \in E(K)$ , the local duality dictates that  $\langle \chi_v, \alpha_v \rangle_v$  is trivial where  $E$  has good reduction at  $v$  and  $E(K_v)/\ell$  is trivial, which is most likely the case where the norm of  $v$  is smaller than  $\ell$ . This makes the smaller places irrelevant and seems to have inherently inhibited index calculus from working for elliptic curves.

### 3. Review of cohomology

The idea of the index calculus method is to reduce the discrete-log computation from one prime to a set of smaller primes. A different strategy is to shift the problem from one prime to another where the problem may become easier. To this end we would like to be able to construct Dirichlet characters and homogeneous spaces with prescribed ramification. The remainder of this paper is devoted to a uniform theoretical treatment of this issue, followed by a brief discussion of the resulting strategy for solving the discrete logarithm problem in the multiplicative case and the elliptic curve case. The actual algorithms will be presented in [HR2] and [HR3].

Before describing our approach, we need to recall the six functors of sheaf theory in algebraic geometry and a bit about the cohomology of number fields. Everything described here is well-known, but we try to put it in one place for the convenience of the reader. The basic references are [MET], [MAD] and [Ma].

Let  $X = \text{Spec}(\mathcal{O}_K)$ , 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. Recall that the cohomology with compact support of  $U$  with values in a sheaf  $F$  is the group  $H^i(X, j_!F)$ . It is denoted by  $H_c^i(U, F)$ .

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 (see e.g. [MET], Chapter II, §1 and Chapter III for more details). Let  $F$  be any sheaf on  $X$  and  $v$  a closed point. Then we have the cohomology with support  $H_v^i(X, F)$ , which may also be described as  $H^i(v, i^!F)$ . Let  $A_v^h$  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  $\text{Spec}(A_i)$  lying over  $v$  with the same residue field. By excision, we have:

$$H_v^i(X, F) = H_v^i(A_v^h, F).$$

This provides a useful way of computing this cohomology. If  $K_v$  is the fraction field of  $A_v^h$ , then we have a long exact sequence:

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

If  $F$  is a sheaf of the form  $j_!G$ , for a sheaf  $G$  on  $U$ , then we have that:

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

for  $v \in S$  (see [MAD], Proposition 1.1, page 182). Thus for a sheaf of the form  $j_!G$ , we have a long exact sequence

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

and using the result just mentioned and the identifications

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

we get the exact sequence:

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

#### 4. Duality

**4.1. Number Fields.** Recall that an étale sheaf  $F$  of  $\mathbb{Z}/\ell\mathbb{Z}$ -modules on  $U$  is called *locally constant* if there is a finite étale morphism  $V \rightarrow U$  such that the pullback of  $F$  to  $V$  is a constant sheaf.  $F$  is *constructible* if there is a nonempty open subset  $V$  of  $U$  such that the restriction of  $F$  to  $V$  and to  $U - V$  are locally constant with finite stalks. Examples of such sheaves that will be important for us include  $\mathbb{Z}/\ell\mathbb{Z}$  and  $\mu_\ell$ , the sheaf of  $\ell$ -th roots of unity. Note that  $\mu_\ell$  is not locally constant if  $\ell$  is not invertible on  $U$ . We then have the following theorem

**THEOREM 1.** (*Artin-Verdier duality; see e.g. [MAD], Chapter II, §3, Corollary 3.2*) *Let  $G$  be a constructible sheaf of  $\mathbb{Z}/\ell\mathbb{Z}$ -modules on  $U$ . Then there is a nondegenerate pairing of finite groups:*

$$H_c^i(U, G) \times \text{Ext}_U^{3-i}(G, \mathbb{G}_m) \rightarrow \mathbb{Q}/\mathbb{Z}.$$

**LEMMA 1.** (*see e.g. [MAD], Chapter II, §1, Proof of Corollary 1.10a*) *If  $G = \mu_\ell$  with  $\ell$  invertible on  $U$ , then we have*

$$\text{Ext}_U^{3-i}(\mu_\ell, \mathbb{G}_m) \cong H^{3-i}(U, \mathbb{Z}/\ell\mathbb{Z}).$$

Then the exact sequence (\*) gives after applying Artin-Verdier duality the *Poitou-Tate exact sequence*:

$$\begin{aligned} 0 \rightarrow H^0(U, \mu_\ell) \rightarrow \bigoplus_{v \in Z} H^0(K_v, \mu_\ell) \rightarrow H^2(U, \mathbb{Z}/\ell\mathbb{Z})^* \rightarrow \\ H^1(U, \mu_\ell) \rightarrow \bigoplus_{v \in Z} H^1(K_v, \mu_\ell) \rightarrow H^1(U, \mathbb{Z}/\ell\mathbb{Z})^* \rightarrow \\ H^2(U, \mu_\ell) \rightarrow \bigoplus_{v \in Z} H^2(K_v, \mu_\ell) \rightarrow H^0(U, \mathbb{Z}/\ell\mathbb{Z})^* \rightarrow 0. \end{aligned}$$

Here, for an abelian group  $A$ ,  $A^*$  denotes  $\text{Hom}(A, \mathbb{Q}/\mathbb{Z})$ . We are mainly interested in the part

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

If the order of the class group of  $K$  is not divisible by  $\ell$ , then the last map in this sequence is surjective (see [HR2]).

**4.2. Elliptic curves.** Let  $\tilde{E}$  be an elliptic curve over a finite prime field  $\mathbb{F}_p$  that has a rational point of prime order  $\ell$ . Suppose that  $E$  is a lifting of  $\tilde{E}$  to an algebraic number field  $K$  in which  $p$  and  $\ell$  split completely. Let  $\mathcal{E}$  be a smooth proper model of  $E$  over an open subset  $U$  of the ring of integers of  $K$  on which  $\ell$  is invertible and put  $S = X - U$ . Recall the Shafarevich-Tate group

$$\text{III}(E) = \ker[H^1(K, E) \rightarrow \bigoplus_{\text{all } v} H^1(K_v, E)],$$

where the sum runs over all places of  $K$ . It is conjectured that  $\text{III}(E)$  is finite for any elliptic curve over a number field, but this is not known, in general. It has been proved in many cases for  $E$  of small rank. In what follows we will need to assume this. Then we take  $G = \mathcal{E}$  in the exact sequence (\*) above and use the duality theorem for abelian varieties (see [MAD], Chapter 3, §5, Theorem 5.2) together with the identification

$$\text{Ext}_U^1(\mathcal{E}, \mathbb{G}_m) \cong \mathcal{E}(U) = E(K),$$

to get the exact sequence:

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

Here  $(\ell)$  denotes completion with respect to subgroups of  $\ell$ -power index and  $\{\ell\}$  denotes the  $\ell$ -primary part. This sequence is usually called the *Cassels-Tate exact sequence*.

## 5. Applications to the discrete log problem

Our approach to the discrete log problem for the multiplicative group of a finite field uses the Poitou-Tate exact sequence (\*) in §4.1 above. For the discrete log problem for an elliptic curve  $\tilde{E}$  over a finite field with a point of order  $\ell$  and a suitable lifting  $E$  of  $\tilde{E}$  to an algebraic number field  $K$ , we will use the Cassels-Tate sequence (\*\*) in §4.2, where  $U$  is an open subset of  $\text{Spec}(\mathcal{O}_K)$  on which  $E$  has good reduction and  $\ell$  is invertible, and  $\mathcal{E}$  is a smooth proper model of  $E$  over  $U$ . In each

case, the method will be to find a suitable element of  $H^1(U, G)$  of order  $\ell$  against which to “test” a lifting to  $K$  of an element over the finite field whose discrete log we seek to compute and then use the reciprocity laws that are encoded in the exact sequences to compute the discrete logs. To find such an element, we use the following basic strategy. In the multiplicative group case, look for an algebraic number field  $K$  such that the  $\mathbb{F}_\ell$ -dimension of the first term of (\*) is smaller than that of the second. This will then guarantee the existence of an element of order  $\ell$  in  $H^1(U, G)$ . This can be accomplished by taking for  $K$  a real quadratic field in which  $\ell$  and  $p$  split, taking for  $U$  the complement of the set consisting of both primes above  $\ell$  and one  $w$  above  $p$ , and making the mild hypothesis that the fundamental unit is not an  $\ell$ -th power in at least one of  $\mathcal{O}_v^* = \mathbb{Z}_\ell^*$  or  $\mathcal{O}_w^* = \mathbb{Z}_p^*$  (this last hypothesis will guarantee that we have the desired ramification at the primes above  $\ell$  and  $p$ ; see [HR2]). In the elliptic curve case, we look for an algebraic number field  $K$  together with an elliptic curve  $E/K$  that lifts  $\tilde{E}$ , such that  $E(K)$  is of small rank, e.g.  $\leq 2$ . This is much trickier, but we believe that it is very reasonable, heuristically. We also assume that at least one of the generators of the torsion-free quotient of  $E(K)$  is not divisible by  $\ell$  in  $E(K_u)$  for all  $u \in T$ , where  $T$  consists of one place above  $p$  and both above  $\ell$  in a quadratic extension  $K/\mathbb{Q}$  in which both  $p$  and  $\ell$  split. For more details, see [HR3].

## References

- [F] G. Frey, *Applications of arithmetical geometry to cryptographic constructions*, In Proceedings of the Fifth International Conference on Finite Fields and Applications. Springer Verlag, page 128-161, 1999; Preprint also available at <http://www.exp-math.uni-essen.de/zahlentheorie/preprints/Index.html>.
- [FR] G. Frey and H.-G. Rück, A remark concerning  $m$ -divisibility and the discrete logarithm in the divisor class group of curves, *Mathematics of Computation*, 62(206):865–874, 1994.
- [HKT] M.-D. Huang, K. L. Kueh, and K.-S. Tan *Lifting elliptic curves and solving the elliptic curve discrete logarithm problem* In ANTS, Lecture Notes in Computer Science, Volume 1838 Springer-Verlag, 2000.
- [HR2] M.-D. Huang and W. Raskind, *Global methods for the discrete logarithm problem II: the multiplicative group case*, preprint 2004
- [HR3] M.-D. Huang and W. Raskind, *Global methods for the discrete logarithm problem III: the elliptic curve case*, in preparation
- [JKSST] M.J. Jacobson, N. Koblitz, J.H. Silverman, A. Stein, and E. Teske. Analysis of the Xedni calculus attack. Design, Codes and Cryptography, 20 41-64, 2000
- [K] N. Koblitz *Elliptic curve cryptosystems* Mathematics of Computation, 48 203-209, 1987.
- [KMV] N. Koblitz, A. Menezes and S. Vanstone *The state of elliptic curve cryptography*, Design, Codes and Cryptography, 19, 173-193 (2000)
- [Ma] B. Mazur, *Notes on the étale cohomology of number fields*, Ann. Sci. École Normale Supérieure 6 (1973) 521-556
- [Mc] K. McCurley, *The discrete logarithm problem*, in Cryptology and Computational Number Theory, C. Pomerance, editor, Proceedings of Symposia in Applied Mathematics, Volume 42, 49-74, 1990
- [Mill] V. Miller *Uses of elliptic curves in cryptography*, In Advances in Cryptology: Proceedings of Crypto 85, Lecture Notes in Computer Science, volume 218, 417-426. Springer-Verlag, 1985.
- [MET] J.S. Milne, *Étale Cohomology*, Princeton Mathematical Series, Volume 33, Princeton University Press 1980

- [MAD] J.S. Milne, *Arithmetic Duality Theorems*, Perspectives in Mathematics, Volume 1., Academic Press 1986
- [N] K. Nguyen, Thesis, Univesität Essen, 2001
- [SWD] O. Schirokauer, D.Weber, and T. Denny *Discrete logarithms: The effectiveness of the index calculus method* In ANTS II, volume 1122 of Lecture Notes in Computer Science. Springer-Verlag, 1996.
- [Se] J.-P. Serre, *Corps Locaux*, Paris Hermann 1962; English translation: *Local Fields*, Graduate Texts in Mathematics, Volume 67, Springer Verlag, Heidelberg-New York, 1979

DEPARTMENT OF COMPUTER SCIENCE, UNIVERSITY OF SOUTHERN CALIFORNIA,  
LOS ANGELES, CA 90089-0781, DEPARTMENT OF MATHEMATICS, UNIVERSITY OF  
SOUTHERN CALIFORNIA, LOS ANGELES, CA 90089-2532, USA  
*E-mail address:* `huang@pollux.usc.edu`, `raskind@math.usc.edu`