• ARTICLES •

SCIENCE CHINA
Mathematics

COMBINATORICS
CODING THEORY
CRYPTOGRAPHY

July 2013 Vol. 56 No. 7: 1421–1427
doi: 10.1007/s11425-013-4674-1

The discrete logarithm problem from a local duality perspective

HUANG MingDeh

Department of Computer Science, University of Southern California, Los Angeles, CA 90089-0781*, USA*
Email: mdhuang@usc.edu

Received January 1, 2013; accepted June 3, 2013

Abstract The discrete logarithm problem is analyzed from the perspective of Tate local duality. Local duality in the multiplicative case and the case of Jacobians of curves over p-adic local fields are considered. When the local field contains the necessary roots of unity, the case of curves over local fields is polynomial time reducible to the multiplicative case, and the multiplicative case is polynomial time equivalent to computing discrete logarithm in finite fields. When the local field does not contains the necessary roots of unity, similar results can be obtained at the cost of going to an extension that contains these roots of unity. There was evidence in the analysis that suggests that the minimal extension where the local duality can be rationally and algorithmically defined must contain the roots of unity. Therefore, the discrete logarithm problem appears to be well protected against an attack using local duality. These results are also of independent interest for algorithmic study of arithmetic duality as they explicitly relate local duality in the case of curves over local fields to the multiplicative case and Tate-Lichtenbaum pairing (over finite fields).

Keywords discrete logarithm, local duality

MSC(2010) 11T71, 11Y16

Citation: Huang M D. The discrete logarithm problem from a local duality perspective. Sci China Math, 2013, 56: 1421–1427, doi: 10.1007/s11425-013-4674-1

1 Introduction

Suppose $\bar{E}$ is an elliptic curve over a finite field $\mathbb{F}_p$, where the group of rational points $\bar{E}(\mathbb{F}_p)$ has prime order ℓ different from p. Let E be an elliptic curve over $\mathbb{Q}_p$ that reduces to $\bar{E}$ modulo p. Then $E(\mathbb{Q}_p)/\ell E(\mathbb{Q}_p)$ is isomorphic to $\bar{E}(\mathbb{F}_p)$ via the reduction map. Now consider the Tate local duality

$$H^1(\mathbb{Q}_p, E)[\ell] \times E(\mathbb{Q}_p)/\ell E(\mathbb{Q}_p) \to \mathrm{Br}(Q_p)[\ell] \overset{\mathrm{inv}}{\to} \frac{1}{\ell}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/\ell\mathbb{Z}.$$

For $a, b \in \bar{E}(\mathbb{F}_p)$, let $\alpha, \beta \in E(\mathbb{Q}_p)$ such that $a = \alpha \bmod p$ and $b = \beta \bmod p$. If $b = ma$ in $\bar{E}(\mathbb{F}_p)$, then $\langle \chi, \beta \rangle = m\langle \chi, \alpha \rangle$ for any nontrivial $\chi \in H^1(\mathbb{Q}_p, E)[\ell]$, hence solving the discrete-log problem on $\bar{E}(\mathbb{F}_p)$ is reduced to local duality computation. It is therefore interesting to ask how efficiently can the local duality be computed (see [5]). A related question is what is the minimal extension of $\mathbb{Q}_p$ over which the local duality can be rationally and algorithmically defined.

Similar consideration can be made when $\bar{E}$ is replaced by the Jacobian of a curve over a finite field. For discrete logarithm in the multiplicative group $\mathbb{F}_p^*/\mathbb{F}_p^{*\ell}$, one can similarly lift to $\mathbb{Q}_p^*/\mathbb{Q}_p^\ell$ and consider using the local duality

$$H^1(\mathbb{Q}_p, \mathbb{Z}/\ell\mathbb{Z}) \times \mathbb{Q}_p^*/\mathbb{Q}_p^\ell \to \mathrm{Br}(Q_p)[\ell] \to \mathbb{Z}/\ell\mathbb{Z}$$

to reduce the discrete logarithm problem.

We will show that local duality for a curve over $\mathbb{Q}_p$ is polynomial time reducible to local duality in the multiplicative case when $\mathbb{Q}_p$ contains the group μ_ℓ of the ℓ-th roots of unity, and the multiplicative case is polynomial time equivalent to computing discrete logarithm in finite fields.

When the local field does not contain the necessary roots of unity, the local duality for curves can be carried out at the cost of going to the extension field $\mathbb{Q}_p(\mu_\ell)$. In fact, our analysis suggests that the minimal extension of $\mathbb{Q}_p$ over which the local duality can be rationally and algorithmically defined is $\mathbb{Q}_p(\mu_\ell)$. One evidence is that the 1-cocycles representing nontrivial elements in $H^1(\mathbb{Q}_p, E)[\ell]$ must involve points that are defined in $\mathbb{Q}_p(\mu_\ell)$ and not anywhere lower. Therefore, the discrete logarithm problem appears to be well protected against an attack using local duality.

These results are also of independent interest for algorithmic study of arithmetic duality as they explicitly relate local duality in the case of curves (over local fields) to the multiplicative case, and the Tate-Lichtenbaum pairing (over finite fields).

The results that are actually proven are for more general finite fields and local fields. For this purpose the following notation will be fixed throughout the paper. Let k be a p-adic local field with a residue field $\mathbb{F}$, k^s a fixed separable closure of k, and k^{ur} the maximal unramified subfield of k^s. Let $G_k = \mathrm{Gal}(k^s/k)$ be the absolute Galois group over k, $\mathcal{I}$ the inertia group $\mathrm{Gal}(k^s/k^{ur})$, G_{ab} denote the Galois group of the maximal abelian extension of k, and $G_{\mathbb{F}} = \mathrm{Gal}(k^{ur}/k) \cong \mathrm{Gal}(\bar{\mathbb{F}}/\mathbb{F})$ where $\bar{\mathbb{F}}$ denotes an algebraic closure of $\mathbb{F}$. Let v denote the unique discrete valuation of k and π be a uniformizing element. Let m be a natural number not divisible by p, the characteristic of $\mathbb{F}$. Let $\mu_m(\bar{\mathbb{F}})$ and $\mu_m(k^s)$ denote the group of m-th roots of unity in $\bar{F}$ and k^s, respectively. Fix a primitive m-th root of unity ζ. We write μ_m instead of $\mu_m(\bar{\mathbb{F}})$ or $\mu_m(k^s)$ when the context is clear.

2 Local duality in the multiplicative case

Local duality in the multiplicative case (see [9, I, §2]) is a perfect pairing

$$\langle\cdot\rangle : H^1(k, \mathbb{Z}/m\mathbb{Z}) \times k^*/k^{*m} \to Br(k)[m] \overset{\mathrm{inv}}{\to} \frac{1}{m}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z}$$

that can be defined as follows.

For $\chi \in H^1(k, \mathbb{Z}/m\mathbb{Z}) \cong \mathrm{Hom}(G_{ab}, \mathbb{Z}/m\mathbb{Z})$ and $\alpha \in k^*$,

$$\langle \chi, \alpha\rangle = \chi(\theta(\alpha)),$$

where $\theta : k^* \to G_{ab}$ is the local Artin map.

From local class field theory we also have that

$$\chi(\theta(\alpha)) = \mathrm{inv}(\alpha \cup \delta\chi),$$

where $\alpha \in k^* = H^0(k, k^{s*})$, $\delta\chi$ is the image of $\chi \in H^1(k, \mathbb{Z}/m\mathbb{Z}) \cong H^1(k, \frac{1}{m}\mathbb{Z}/\mathbb{Z}) \subset H^1(k, \mathbb{Q}/\mathbb{Z})$ in the connecting map $H^1(k, \mathbb{Q}/\mathbb{Z}) \overset{\delta}{\to} H^2(k, \mathbb{Z})$ with respect to

$$0 \to \mathbb{Z} \to \mathbb{Q} \to \mathbb{Q}/\mathbb{Z} \to 0$$

and $\mathrm{inv} : \mathrm{Br}(k) \to \mathbb{Q}/\mathbb{Z}$ is the invariant map (see [1, VI], [11, XI, §3] and [9, I, §1]).

We discuss how elements in the pairing groups can be represented for purpose of computation.

Since

$$k^*/k^{*m} \cong \mathbb{F}^*/\mathbb{F}^{*m} \times \{\pi^i \mid i = 0, \ldots, m-1\},$$

each element of k^*/k^{*m} can be specified in the form $a\pi^i$ with $a \in \mathbb{F}^*/\mathbb{F}^{*m}$ and $0 \leqslant i \leqslant m-1$.

Since $H^1(k, \mathbb{Z}/m\mathbb{Z}) \cong \mathrm{Hom}(G_{ab}, \mathbb{Z}/m\mathbb{Z})$, each $\chi \in H^1(k, \mathbb{Z}/m\mathbb{Z})$ is determined by the cyclic extension of degree dividing m fixed by $\ker\chi$, and $\chi(\sigma)$ where σ is a generator of $G_{ab}/\ker\chi$. Suppose $\zeta \in k$. Then the field fixed by $\ker\chi$ is generated by an m-th root of some $a \in k^*$, so $\chi \in H^1(k, \mathbb{Z}/m\mathbb{Z}) \cong \mathrm{Hom}(G_{ab}, \mathbb{Z}/m\mathbb{Z})$ can be specified by $a \in k^*/k^{*m}$ where $k(\alpha)$ is the field fixed by $\ker\chi$ with $\alpha^m = a$, and for $\sigma \in G_{ab}$, $\chi(\sigma) = i$ if $\sigma(\alpha) = \zeta^i\alpha$.

Theorem 2.1. *Suppose $\mu_m \subset k$ and under the representation of elements in k^*/k^{*m} and $H^1(k, \mathbb{Z}/m\mathbb{Z})$ as described above, the discrete-log problem on the subgroup of order m of $\mathbb{F}$ is polynomial time equivalent to computing the local duality*

$$H^1(k, \mathbb{Z}/m\mathbb{Z}) \times k^*/k^{*m} \to \mathbb{Z}/m\mathbb{Z}.$$

For $a, b \in k^*$, the (local) *norm residue symbol* [1] is defined by

$$(a, b)_v = \frac{\theta(b)\alpha}{\alpha},$$

where $\alpha^m = a$.

Let b be an element of k^*/k^{*m} represented by $(\tilde{b}, \pi^i)$ in $\mathbb{F}^*/\mathbb{F}^{*m} \times \{\pi^i \mid i = 0, \ldots, m-1\}$. Let χ be an element of $H^1(k, \mathbb{Z}/m\mathbb{Z})$ represented by some $a \in k^*/k^{*m}$.

From the definition of χ and the fact that $\langle \chi, b\rangle = \chi(\theta(b))$ we have

$$\langle \chi, b\rangle = i \Leftrightarrow \theta(b)\alpha = \zeta^i\alpha \Leftrightarrow (a, b)_v = \zeta^i.$$

So $\langle \chi, b\rangle$ can be obtained from $(a, b)_v$ by taking the discrete logarithm based ζ. Therefore, the theorem follows if the norm residue symbol $(a, b)_v$ is computable in polynomial time. This follows from [11, XIV, §3, Proposition 8], or a simple derivation which we provide below.

Suppose a is a unit. Then $k(\alpha)$ is an unramified abelian extension over k and $\theta(b)$ when restricted to $k(\alpha)$ is $\tau^{v(b)}$, where $\tau \in \mathrm{Gal}(k(\alpha)/k)$ is the Frobenius automorphism. Let u be the extension of v to $k(\alpha)$. Then

$$\tau\alpha \equiv \alpha^q \mod u,$$

where $q = \#\mathbb{F}$ and since α is a unit

$$\tau\alpha/\alpha \equiv \alpha^{q-1} \equiv a^{\frac{q-1}{m}} \mod u.$$

Hence,

$$(a, b)_v = (\tau\alpha/\alpha)^{v(b)}$$

and can be represented by $\tilde{a}^{\frac{q-1}{m}v(b)} \in \mu_m(\mathbb{F})$. So in this case $(a, b)_v$ is computable in polynomial time.

Since for $a, b \in k^*$, $(a, b)_v(b, a)_v = 1$ (see [1, p. 351]), it follows that $(a, b)_v$ is computable in polynomial time if either a or b is a unit.

Since $(a, -a)_v = 1$ for all $a \in k^*$ (see [1, p. 350]), we have $(\pi, -\pi) = 1$. Since

$$(-1, \pi)_v = (-1)^{\frac{q-1}{m}v(\pi)} = (-1)^{\frac{q-1}{m}},$$

it follows that $(\pi, -1)_v = (-1)^{\frac{q-1}{m}}$, so

$$(\pi, \pi)_v = (\pi, -\pi)_v(\pi, -1)_v = (-1)^{\frac{q-1}{m}}.$$

Therefore, in all cases $(a, b)_v$ can be computed in polynomial time, and Theorem 2.1 follows.

3 Local duality computation for Jacobians of curves

Let A be a principally polarized abelian variety over k. For any field K containing k, let $A(K)$ denote the group of K-rational points on A. Let $A[m] = A(k^s)[m]$. The Tate local duality for abelian varieties over the local field k (see [9, I, §3] and [12]) is a perfect pairing

$$H^1(k, A)[m] \times A(k)/mA(k) \to \mathrm{Br}(k)[m] \overset{\mathrm{inv}}{\to} \frac{1}{m}\mathbb{Z}/\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z}.$$

This pairing can be described as follows. By taking Galois cohomology from the exact Kummer sequence of G_k-modules:

$$0 \to A[m] \to A(k^s) \overset{m}{\to} A(k^s) \to 0,$$

we get the exact sequence

$$0 \to A(k)/mA(k) \xrightarrow{\delta} H^1(k, A[m]) \to H^1(k, A)[m] \to 0.$$

For $\alpha \in H^1(K, A)[m]$ and $R \in A(k)$, the pairing between α and R is defined to be $\mathrm{inv}(\delta R \cup \beta)$, where $\beta \in H^1(k, A[m])$ is such that its image is α in $H^1(k, A[m]) \to H^1(k, A)[m]$, and the cup product is

$$H^1(k, A[m]) \times H^1(k, A[m]) \to H^2(k, \mu_m) = \mathrm{Br}(k)[m]$$

relative to the Weil pairing

$$A[m] \times A[m] \to \mu_m,$$

where $A[m]$ is identified with the m-torsion group of the dual abelian variety of A through a canonical principal polarization.

Next, we discuss how elements in $H^1(k, A)[m]$ and $A(k)/mA(k)$ can be efficiently represented.

Since p does not divide m, and suppose A has good reduction at v, $A(k)/mA(k)$ is isomorphic to $\tilde{A}(\mathbb{F})/m\tilde{A}(\mathbb{F})$ through the reduction map, where $\tilde{A}$ denote the reduction of A at v. Hence an element of $A(k)/mA(k)$ can be represented by its reduction in $\tilde{A}(\mathbb{F})/m\tilde{A}(\mathbb{F})$.

Let $k_{\pi,m} = k(\mu_m)(\pi^{\frac{1}{m}})$. Let τ be a generator of $\mathrm{Gal}(k_{\pi,m}/k(\mu_m))$. Let χ be the cyclotomic character so that $\sigma(\zeta) = \zeta^{\chi(\sigma)}$ for $\sigma \in G_k$. For any G_k-module B let B^χ consists of all $b \in B$ such that $\sigma b = \chi(\sigma)b$. Suppose $b \in B^\chi$. For $\sigma \in G_k$, $\sigma(b) = b$ if and only if $\sigma(\zeta) = \zeta$. Thus, $(A[m])^\chi$ contains all elements of $A[m]$ that are defined in $k(\zeta)$ over k but not any proper subextension of $k(\zeta)$. If $\mu_m \subset k$, then $\sigma(\zeta) = \zeta$ for $\sigma \in G_k$, so $\chi(\sigma) = 1$ for $\sigma \in G_k$. In this case $(A[m])^\chi = A(k)[m]$.

Lemma 3.1. *Let A be an abelian variety over k with good reduction at v. Then*

$$H^1(k, A)[m] \cong \mathrm{Hom}(\mathrm{Gal}(k_{\pi,m}/k(\mu_m)), (A[m])^\chi).$$

To prove the lemma we observe that

$$H^1(G_k, A)[m] \cong \mathrm{Hom}(\mathrm{Gal}(k^{ur}(\pi^{\frac{1}{m}})/k^{ur}), A[m])^{G_k/\mathcal{I}}.$$

(see for example the proof of [4, Lemma 2.2].)

Let $\varphi \in \mathrm{Hom}(\mathrm{Gal}(k^{ur}(\pi^{\frac{1}{m}})/k^{ur}), A[m])$. Let $R_\tau = \varphi(\tau)$. Then for $t \in G_k$, we have

$$\begin{aligned} &\varphi^t(\tau) = t^{-1}R_{\tau^t}, \\ &R_{\tau^t} = \varphi(\tau^t) = \varphi(\tau^{\chi(t)}) = \chi(t)R_\tau. \end{aligned}$$

So

$$t^{-1}R_{\tau^t} = R_\tau \Leftrightarrow tR_\tau = \chi(t)R_\tau.$$

Therefore,

$$\mathrm{Hom}(\mathrm{Gal}(k^{ur}(\pi^{\frac{1}{m}})/k^{ur}), A[m])^{G_k/\mathcal{I}} = \mathrm{Hom}(\mathrm{Gal}(k^{ur}(\pi^{\frac{1}{m}})/k^{ur}), (A[m])^\chi).$$

Finally,

$$\mathrm{Hom}(\mathrm{Gal}(k^{ur}(\pi^{\frac{1}{m}})/k^{ur}), (A[m])^\chi) \cong \mathrm{Hom}(\mathrm{Gal}(k_{\pi,m}/k(\mu_m)), (A[m])^\chi)$$

and the lemma follows.

Let τ be a generator of $\mathrm{Gal}(k_{\pi,m}/k)$ such that $\tau(\pi^{1/m})/\pi^{1/m} = \zeta$. From the lemma it follows that an element $f \in H^1(k, A)[m]$ can be represented by $f(\tau) \in (A[m])^\chi$. An important computational implication of Lemma 3.1 is also that modulo 1-coboundaries in $H^1(k, A)$, 1-cocycle representation of elements of $H^1(k, A)[m]$ must involve points in $(A[m])^\chi$. As observed before these are points exactly defined in $k(\mu_m)$ over k. Hence in such representation the minimal extension of k over which the local duality can be algorithmically defined must contain $k(\mu_m)$. We argue below that the local duality can indeed be carried out computationally in $k(\mu_m)$.

Let $L = k(\mu_m)$. For $\alpha \in H^1(k, A)[m]$ and $R \in A(k)$, the pairing between α and R is defined to be $\mathrm{inv}(\delta R \cup \beta)$ where $\beta \in H^1(k, A[m])$ is such that its image is α in $H^1(k, A[m]) \to H^1(k, A)[m]$. We have

$$(\alpha, R)_k = \mathrm{inv}_k(\delta R \cup \beta).$$

Since cup product commutes with restriction and $\mathrm{inv}_L \circ \mathrm{Res}_{k/L} = [L : k]\,\mathrm{inv}_k$ (see [1, p. 131]), it follows that

$$\mathrm{inv}_k(\delta R \cup \beta) = \phi(m)^{-1}(\alpha, R)_L.$$

With this reduction it is enough to show that the local duality can be algorithmically defined over k in the case where $\mu_m \subset k$.

We now focus on the case where A is the Jacobian of a curve. In this case, a variant of the Tate pairing defined by Lichtenbaum [4, 7] renders the local duality more accessible algorithmically. Though defined differently, it is identical to the Tate pairing up to a sign [7].

Let C be a smooth projective irreducible curve over k of genus greater than 0, with a k-rational point. We assume that C has good reduction at v, denoted by $\tilde{C}$. Let $\mathrm{Div}^0(C)$ denote the group of divisors of C of degree 0 over k^s, $\mathcal{P}(C)$ the group of principal divisors of C over k^s, and $\mathrm{Pic}^0(C)$ the factor group $\mathrm{Div}^0(C)/\mathcal{P}(C)$, which is isomorphic to $J(k^s)$ where J is the Jacobian variety of C over k. More generally for a field k' with $k \subset k' \subset k^s$, let $\mathrm{Div}^0_{k'}(C)$ denote the group of divisors of C of degree 0 over k', $\mathcal{P}_{k'}(C)$ the group of principal divisors of C over k', and $\mathrm{Pic}^0_{k'}(C)$ the factor group $\mathrm{Div}^0_{k'}(C)/\mathcal{P}_{k'}(C)$, which is isomorphic to $J(k')$ where J is the Jacobian variety of C over k. These groups are naturally G_k-modules. Lichtenbaum's pairing can be described as follows. By taking Galois cohomology from the exact sequence

$$0 \to \mathcal{P}(C) \to \mathrm{Div}^0(C) \to \mathrm{Pic}^0(C) \to 0,$$

we get

$$0 = H^1(k, \mathrm{Div}^0(C)) \to H^1(k, \mathrm{Pic}^0(C)) \xrightarrow{\delta} H^2(k, \mathcal{P}(C)).$$

For $\alpha \in H^1(k, \mathrm{Pic}^0(C))$ and $\bar{D} \in \mathrm{Pic}^0_k(C)$, the pairing of α and $\bar{D}$ is

$$(\alpha, \bar{D}) = \mathrm{inv}[(f_{\sigma,\tau}(D))_{\sigma,\tau \in G_k}],$$

where $\delta\alpha = [(f_{\sigma,\tau})_{\sigma,\tau \in G_k}]$ with $f_{\sigma,\tau} \in k^s(C)$ and $D \in \bar{D}$ such that D is prime to the principal divisors $(f_{\sigma,\tau})$ for all $\sigma, \tau \in G_k$.

From now on, suppose $\mu_m \subset k$. As before let $k_{\pi,m} = k(\mu_m)(\pi^{\frac{1}{m}}) = k(\pi^{\frac{1}{m}})$, and let τ be a generator of $\mathrm{Gal}(k_{\pi,m}/k)$ such that $\tau(\pi^{1/m})/\pi^{1/m} = \zeta$. Let $\chi \in H^1(G_k, \mathbb{Q}/\mathbb{Z})$ be the composition of the natural homomorphism from G_k to $\mathrm{Gal}(k_{\pi,m}/k)$ and the homomorphism from $\mathrm{Gal}(k_{\pi,m}/k)$ to $\mathbb{Q}/\mathbb{Z}$ that sends τ to $\frac{1}{m}$. By Lemma 3.1, $H^1(k, \mathrm{Pic}^0(C))[m]$ can be identified with $\mathrm{Hom}(\langle\tau\rangle, \mathrm{Pic}^0_k(C)[m])$, thus an element $\alpha \in H^1(k, \mathrm{Pic}^0(C))[m]$ can be represented by $\alpha(\tau) \in \mathrm{Pic}^0_k(C)[m]$.

Theorem 3.2. *Let $\alpha \in H^1(k, \mathrm{Pic}^0(C))[m]$ be represented by $\bar{S} = \alpha(\tau)$. Let $\bar{D} \in \mathrm{Pic}^0_k(C)$. Then*

$$(\alpha, \bar{D}) = \langle \chi, F_S(D) \rangle,$$

where F_S is a function in $k(C)$ such that $(F_S) = mS$ with $S \in \bar{S}$, and $D \in \bar{D}$ is such that D is prime to S.

For computation $F_S(D)$ is represented by $\tilde{F}_{\tilde{S}}(\tilde{D})$, where $\tilde{S}$, $\tilde{D}$ and $\tilde{F}_{\tilde{S}}$ are the reductions at v of S, D and F_S. In fact, $\tilde{F}_{\tilde{S}}(\tilde{D})$ is the value of the *Tate-Lichtenbaum pairing*

$$\mathrm{Pic}^0_{\mathbb{F}}(\tilde{C})[m] \times \mathrm{Pic}^0_{\mathbb{F}}(\tilde{C})/m\mathrm{Pic}^0_{\mathbb{F}}(\tilde{C}) \to \mathbb{F}^*/\mathbb{F}^{*m}$$

defined in [4]. This pairing is well known in cryptography [2,3,6,8], and it can be computed in polynomially many group operations in $\mathrm{Pic}^0_{\mathbb{F}}(\tilde{C})$. From this and the proof of Theorem 2.1, we have the following theorem.

Theorem 3.3. *Suppose $\mu_m \subset k$. Then the local duality*

$$H^1(k, \mathrm{Pic}^0(C)) \times \mathrm{Pic}_k^O(C)/m\mathrm{Pic}_k^0(C) \to \mathbb{Z}/m\mathbb{Z}$$

is computable with polynomially many group operations in $\mathrm{Pic}_{\mathbb{F}}^0(\tilde{C})$ and solving one discrete logarithm problem in the subgroup of order m of $\mathbb{F}$.

The above theorems show that when $\mu_m \subset k$, local duality in the multiplicative case and the case of Jacobians of curves over local fields can both be computed in polynomially many group operations over $\mathbb{F}$, together with solving a discrete logarithm problem in $\mathbb{F}$.

The proof of the theorem involves cohomological computations. Recall that in defining Galois cohomology over G-modules we can take the resolution P of $\mathbb{Z}$:

$$\cdots \to P_1 \to P_0 \to \mathbb{Z} \to 0,$$

where $P_i = \mathbb{Z}[G^{i+1}]$, and form the complex $K(A) = \mathrm{Hom}_G(P, A)$ for a G-module A. Then $H^i(G, A)$ is the i-th cohomology group of this complex. An element of $K^i(A) = \mathrm{Hom}_G(P_i, A)$ is determined by a function from G^i to A. Let d denote the boundary maps

$$\cdots K^i(A) \xrightarrow{d} K^{i+1}(A) \cdots$$

For an exact sequence of G-modules

$$0 \to A \to B \to C \to 0,$$

the induced

$$0 \to K^i(A) \to K^i(B) \to K^i(C) \to 0$$

is also exact, and we let δ denote the connecting homomorphisms

$$\delta : H^i(G, C) \to H^{i+1}(G, A).$$

Let $\tau \in \mathrm{Gal}(k(\pi^{\frac{1}{m}})/k)$ be such that $\tau\pi^{\frac{1}{m}} = \pi^{\frac{1}{m}}\zeta$. Let $\chi \in H^1(G_k, \mathbb{Q}/\mathbb{Z})$ be the composition of the natural homomorphism from G_k to $\mathrm{Gal}(k_{\pi,m}/k)$ and $\bar{\chi} \in \mathrm{Hom}(\mathrm{Gal}(k_{\pi,m}/k), \frac{1}{m}\mathbb{Z}/\mathbb{Z})$ with $\bar{\chi}(\tau) = 1/m$. Let $\alpha \in H^1(k, \mathrm{Pic}^0(C))[m]$ and suppose when identifying $H^1(k, \mathrm{Pic}^0(C))[m]$ with $\mathrm{Hom}(\langle\tau\rangle, \mathrm{Pic}_k^0(C)[m])$, we have $\bar{S} = \alpha(\tau)$. Let $\bar{D} \in \mathrm{Pic}_k^0(C)$. We would like to show that

$$(\alpha, \bar{D}) = \langle \chi, F_S(D) \rangle,$$

where F_S is a function in $k(C)$ such that $(F_S) = mS$ with $S \in \bar{S}$ and $D \in \bar{D}$ such that D is prime to S.

Let $\bar{\lambda} : \frac{1}{m}\mathbb{Z}/\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ $\bar{S}$ be the homomorphism sending $1/m$ to $\bar{S}$. Then $\varphi_\alpha = \bar{\lambda} \circ \chi$ is a function from G_k to $\mathrm{Pic}^0(C)$ that represents α.

We will relate $\delta\alpha$ in

$$H^1(G_k, \mathrm{Pic}^0(C)) \xrightarrow{\delta} H^2(G_k, \mathcal{P}(C))$$

with respect to the exact sequence

$$0 \to \mathcal{P}(C) \to \mathrm{Div}^0(C) \to \mathrm{Pic}^0(C) \to 0$$

to $\delta\chi$ in

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

with respect to the exact sequence

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

In fact, a 2-cocycle that represents $\delta\alpha$ can be directly derived and expressed in terms of F_S (see [10, (10.18)]). However, comparing $\delta\alpha$ to $\delta\chi$ will allow us to explicitly relate the pairing of $(\alpha, \bar{D})$ to the pairing $\langle \chi, F_S(D) \rangle$.

Let $\hat{\chi} \in \mathrm{Hom}(G_k, \mathbb{Q})$ be a natural lift of χ so that $\hat{\chi}$ composed with the map $\mathbb{Q} \to \mathbb{Q}/\mathbb{Z}$ is χ. Thus, $\hat{\chi}$ maps to χ in $K^1(\mathbb{Q}) \to K^1(\mathbb{Q}/\mathbb{Z})$.

Let $S \in \bar{S}$ and $\lambda : \frac{1}{m}\mathbb{Z} \to \mathbb{Z}S \subset \mathrm{Div}_k^0(C) \subset \mathrm{Div}^0(C)$ be the isomorphism sending $1/m$ to S. Then $\hat{\varphi}_\alpha = \lambda \circ \hat{\chi}$ maps to φ_α in $K^1(\mathrm{Div}^0(C)) \to K^1(\mathrm{Pic}^0(C))$ (See diagram below):

$$\begin{array}{ccc} G_k & \to & \frac{1}{m}\mathbb{Z} \to \frac{1}{m}\mathbb{Z}/\mathbb{Z} \\ & & \downarrow \qquad \downarrow \\ & & \mathbb{Z}S \ \to \ \frac{\mathbb{Z}}{m\mathbb{Z}}\bar{S}. \end{array}$$

By construction we have for all $\sigma, \sigma' \in G_k$,

$$d\hat{\varphi}_\alpha(\sigma, \sigma') = iS \Leftrightarrow (d\hat{\chi})(\sigma, \sigma') = \frac{i}{m},$$

hence

$$d\hat{\varphi}_\alpha(\sigma, \sigma') = m(d\hat{\chi})(\sigma, \sigma')S.$$

From the general property of connecting homomorphism, we know that there is a 2-cocycle $G_k \times G_k \to \mathbb{Z}$ that when composed with the inclusion map $\mathbb{Z} \to \mathbb{Q}$ is identical to $d\hat{\chi}$. Therefore, it is the case that $(d\hat{\chi})(\sigma, \sigma') \in \mathbb{Z}$ for all $\sigma, \sigma' \in G_k$. Let $a_{\sigma,\sigma'} = (d\hat{\chi})(\sigma, \sigma') \in \mathbb{Z}$ for all $\sigma, \sigma' \in G_k$. Then $(a_{\sigma,\sigma'})_{\sigma,\sigma' \in G_k}$ is a 2-cocycle that represents $\delta\chi$. And we have

$$d\hat{\varphi}_\alpha(\sigma, \sigma') = m(d\hat{\chi})(\sigma, \sigma')S = ma_{\sigma,\sigma'}S = (F_S^{a_{\sigma,\sigma'}}).$$

This shows that $\delta\alpha$ can be represented by the 2-cocycle $((F_S^{a_{\sigma,\sigma'}}))_{\sigma,\sigma' \in G_k}$.

So,

$$(\alpha, D) = \mathrm{inv}[(F_S(D)^{a_{\sigma,\sigma'}})_{\sigma,\sigma' \in G_k}] = \mathrm{inv}[\delta\chi \cup F_S(D)] = \langle \chi, F_S(D) \rangle.$$

Theorem 3.2 follows.

References

1 Cassels J W S, Fröhlich A. Algebraic Number Theory. New York: Academic Press, 1967
2 Frey G. On Bilinear Structures on Divisor Class Groups. Ann Math Blaise Pascal, 2009, 16: 1–26
3 Frey G, Müller M, Rück H G. The Tate pairing and the discrete logarithm applied to elliptic curve cryptosystems. IEEE Trans Inform Theory, 1999, 45: 1717–1719
4 Frey G, Rück H G. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Math Comput, 1994, 62: 865–874
5 Huang M D. Local duality and the discrete logarithm problem. In: Lecture Notes in Computer Science, vol. 6639. Berlin: Springer, 2011, 213–222
6 Joux A. The Weil and Tate Pairings as Building Blocks for Public Key Cryptosystems. In: Lecture Notes in Computer Science, vol. 2369. Berlin: Springer, 2002, 20–32
7 Lichtenbaum S. Duality theorems for curves over p-adic fields. Invent Math, 1969, 7: 120–136
8 Menezes A, Okamoto S, Vanstone T. Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Trans Infor Theory, 1993, 39: 1639–1646
9 Milne J S. Arithmetic Duality Theorems. New York: Academic Press, 1986
10 Nguyen K. Explicit Arithmetic of Brauer Groups–Ray Class Fields and Index Calculus. PhD Thesis. Essen: University of Essen, 2001
11 Serre J P. Local Fields. New York: Springer-Verlag, 1979
12 Tate J. WC-groups over p-adic fields. Sem Bourbaki, 1957, 4: 265–277