MATHEMATICS OF COMPUTATION
VOLUME 62, NUMBER 206
APRIL 1994, PAGES 865–874

A REMARK CONCERNING m-DIVISIBILITY AND THE DISCRETE LOGARITHM IN THE DIVISOR CLASS GROUP OF CURVES

GERHARD FREY AND HANS-GEORG RÜCK

ABSTRACT. The aim of this paper is to show that the computation of the discrete logarithm in the m-torsion part of the divisor class group of a curve X over a finite field k_0 (with $\mathrm{char}(k_0)$ prime to m), or over a local field k with residue field k_0, can be reduced to the computation of the discrete logarithm in $k_0(\zeta_m)^*$. For this purpose we use a variant of the (tame) Tate pairing for Abelian varieties over local fields. In the same way the problem to determine all linear combinations of a finite set of elements in the divisor class group of a curve over k or k_0 which are divisible by m is reduced to the computation of the discrete logarithm in $k_0(\zeta_m)^*$.

1. RESULTS

Let k_0 be a finite field with q elements and X_0 a projective irreducible nonsingular curve of genus g over k_0. For simplicity we assume that the curve X_0 has a point P_0 which is rational over k_0. Let $\mathrm{Div}_0(X_0)$ be the group of divisors of degree 0 on X_0. In particular, the set of divisors of functions on X_0 is a subgroup of this group. The quotient group, i.e., the group of divisor classes of degree 0, is denoted by $\mathrm{Pic}_0(X_0)$. We consider a positive integer m which divides $q-1$. Then m is prime to the characteristic of k_0 and the mth roots of unity are contained in k_0. We denote by $\mathrm{Pic}_0(X_0)_m$ the group of divisor classes whose m-fold is zero. We want to treat the problem of the discrete logarithm in the group $\mathrm{Pic}_0(X_0)_m$: Let $\overline{D_1}$ and $\overline{D_2}$ be given elements in $\mathrm{Pic}_0(X_0)_m$ with $\overline{D_2} = \mu\overline{D_1}$ and $\mu \in \mathbf{N}$; then evaluate the integer μ (notice that the group law in $\mathrm{Pic}_0(X_0)$ is written additively, contrary to the notation "discrete logarithm"). In particular, we want to reduce this problem to the corresponding one in the multiplicative group k_0^*: Given elements η and ζ of k_0^* with an integer μ such that $\zeta = \eta^\mu$; determine this element μ.

It is not our aim to give explicit formulas for the addition law in $\mathrm{Pic}_0(X_0)$. We want to assume that the elements in $\mathrm{Pic}_0(X_0)$ are represented in the following way: The theorem of Riemann-Roch asserts that each class of $\mathrm{Pic}_0(X_0)$ contains a divisor of the form $A - gP_0$, where A is a positive divisor on X_0 of degree g (without mentioning it explicitly, we mean that the divisor A is rational over k_0). If A is given as $A = \sum_{i=1}^g P_i$, then the points P_i on X_0 are rational over a finite extension of k_0 of degree $g!$. Notice that this degree is

Received by the editor July 5, 1991 and, in revised form, December 30, 1992.
1991 *Mathematics Subject Classification*. Primary 11G20, 11Y99.

independent of the field k_0. Now we assume that we know the surjective map c_g which assigns to each positive divisor A of degree g the class $c_g(A) = \overline{A - gP_0}$ in $\mathrm{Pic}_0(X_0)$; furthermore, the addition in $\mathrm{Pic}_0(X_0)$ should be given explicitly, in other words, we assume that it is possible to solve the following problem in a fixed number of elementary operations in k_0:

(*) Let A_1 and A_2 be positive divisors of degree g on X_0; find a positive divisor A_3 of degree g and a function h on X_0 such that the divisor of h is equal to $A_1 + A_2 - A_3 - gP_0$.

In the following the evaluation of (*) will be called a step.

In general it will be hard to satisfy these assumptions. We will give two examples where the solution of the computational problems in $\mathrm{Pic}_0(X_0)$ is well known:

Examples. (a) If X_0 is an elliptic curve given by an affine equation $y^2 = x^3 + ax + b$, let P_0 be the point at infinity. Then three points P_i $(i = 1, 2, 3)$ with coordinates (x_i, y_i) satisfy $\overline{P_1 - P_0} + \overline{P_2 - P_0} + \overline{P_3 - P_0} = 0$ in $\mathrm{Pic}_0(X_0)$ if and only if the points (x_i, y_i) $(i = 1, 2, 3)$ lie on a straight line $l(x, y)$. Furthermore, $\overline{P_1 - P_0}$ is the inverse of $\overline{P_2 - P_0}$ if and only if $x_1 = x_2$ and $y_1 = -y_2$. Hence, the function h in (*) is given by the equation $l(x, y)/(x - x_3)$.

(b) If X_0 is a hyperelliptic curve, then the addition law (*) can be given by a reduction algorithm (see, e.g., [2]).

The key point in the following is the construction of a nondegenerate pairing and the estimation of its computing time.

Notation. Let D be a divisor with $\overline{D} \in \mathrm{Pic}_0(X_0)_m$, and let $E = \sum_{i=1}^r a_i P_i$ $(a_i \in \mathbf{Z}, P_i$ on $X_0)$ be an element in $\mathrm{Div}_0(X_0)$ such that D and E have no points in common; furthermore, let f be a function whose divisor is equal to mD. Then define $f(E) := \prod_{i=1}^r f(P_i)^{a_i}$.

Theorem. *If m divides $q - 1$, then the assignment $\{\overline{D}, \overline{E}\}_{0,m} := f(E)$ defines a nondegenerate bilinear pairing*

$$\{\ ,\ \}_{0,m}\colon \mathrm{Pic}_0(X_0)_m \times \mathrm{Pic}_0(X_0)/m\,\mathrm{Pic}_0(X_0) \to k_0^*/k_0^{*m}.$$

For given $\overline{D}$ and $\overline{E}$ the value $f(E)$ can be evaluated in $\log m$ *steps, i.e., one has to perform* $\log m$ *times a fixed number of elementary operations in an extension field of k_0 of bounded degree.*

In §2 we show that $\{\ ,\ \}_{0,m}$ is indeed a nondegenerate pairing; this is the crucial part of the theorem. Finally, in the third section the complexity of the evaluation of $f(E)$ is studied.

From this thecrem we get as a corollary the reduction of the discrete logarithm.

Corollary 1. *Under the condition of the theorem (especially when m divides $q - 1$) the evaluation of the discrete logarithm in the group* $\mathrm{Pic}_0(X_0)_m$ *can be reduced to the corresponding evaluation in k_0^* in a probabilistic polynomial time in* $\log q$.

Proof. Using the zeta function of the curve X_0 over k_0, one gets $\#\mathrm{Pic}_0(X_0) = \prod_{i=1}^{2g}(1 - \omega_i)$, where ω_i are complex numbers with $|\omega_i| = q^{1/2}$. Therefore, $\log m = O(\log q)$.

The first step is to evaluate bases of $\mathrm{Pic}_0(X_0)_m$ and of $\mathrm{Pic}_0(X_0)/m\,\mathrm{Pic}_0(X_0)$ in a probabilistic polynomial time in $\log q$. As was pointed out before, each element in $\mathrm{Pic}_0(X_0)$ has a representative of the form $\sum_{i=1}^{g} P_i - gP_0$, where P_i are points on X_0 which are rational over an extension l_0 of k_0 of the fixed degree $g!$. Hence the task is to find enough points of X_0 which are rational over l_0. We use the following facts:

1. There is an irreducible polynomial $F(X, Y) \in l_0[X, Y]$ whose degree in Y is bounded by g such that (up to a finite set whose cardinality is bounded by g) the zeros of $F(X, Y)$ in l_0 are the l_0-rational points on X_0.
2. By the theorem of Riemann-Roch we have $|\#X_0(l_0) - \#l_0 - 1| \le 2g(\#l_0)^{1/2}$.

Hence there is a positive probability, depending only on the genus g, that to a value $x \in l_0$ there is a $y \in l_0$ such that $F(x, y) = 0$. Note that the existence of y can be tested in a probabilistic polynomial time in $\log q$ by Berlekamp's algorithm.

From this, one sees that it is possible to find an element in $\mathrm{Pic}_0(X_0)$ in a probabilistic polynomial time in $\log q$; and since multiplication by m needs only $O(\log q)$ steps, the same is true for an element in $\mathrm{Pic}_0(X_0)_m$ in all interesting cases where m is of the same size as q, i.e., $\frac{q-1}{m}$ is bounded by a small integer.

The next task is to determine generators of $\mathrm{Pic}_0(X_0)_m$ in a probabilistic polynomial time in $\log q$. For the sake of simplicity we explain this in the special case that m is prime. Then $\mathrm{Pic}_0(X_0)_m$ is isomorphic to $(\mathbf{Z}/m\mathbf{Z})^r$, where r is bounded by $2g$. The probability that r elements form a basis of $\mathrm{Pic}_0(X_0)_m$ is positive and independent of q. The same is true for $\mathrm{Pic}_0(X_0)/m\,\mathrm{Pic}_0(X_0)$. If one wants to verify that one actually has bases of $\mathrm{Pic}_0(X_0)_m$ and $\mathrm{Pic}_0(X_0)/m\,\mathrm{Pic}_0(X_0)$, one uses the nondegenerate pairing $\{\ ,\ \}_{0m}$ of the theorem. Since the evaluation of $\{\ ,\ \}_{0,m}$ can be done in $\log m$ steps, it is possible to find bases in a probabilistic polynomial time in $\log q$.

Now let $\{\overline{E_1}, \dots, \overline{E_r}\}$ be a basis of $\mathrm{Pic}_0(X_0)/m\,\mathrm{Pic}_0(X_0)$. Let $\overline{D_1}$ and $\overline{D_2}$ be elements in $\mathrm{Pic}_0(X_0)_m$ with $\overline{D_2} = \mu\overline{D_1}$ and μ an integer. For each $i = 1, \dots, r$ we compute $\eta_i = \{\overline{D_1}, \overline{E_i}\}_{0,m}$ and $\zeta_i = \{\overline{D_2}, \overline{E_i}\}_{0,m}$. This can be done in a polynomial time in $\log q$. We get $\zeta_i \equiv \eta_i^{\mu}$ modulo k_0^{*m} for each i. Since the pairing $\{\ ,\ \}_{0,m}$ is nondegenerate, there is a unique solution μ (modulo m), which can be evaluated by an algorithm for the discrete logarithm in k_0^*. □

Remarks. (1) The discrete logarithm for some finite fields k_0^* is known to be subexponential (cf. [7]).

(2) We want to discuss the assumptions of the theorem in the case of an elliptic curve. Let X_0 be an elliptic curve over a finite field k_0 with q $(q = p^f)$ elements. The theory of the zeta functions yields (cf. [9])

$$\#\,\mathrm{Pic}_0(X_0) = (1 - \omega)(1 - \bar{\omega}),$$

where ω, $\bar{\omega}$ are complex numbers with $\omega\bar{\omega} = q$ and $|\omega| = |\bar{\omega}| = q^{1/2}$. If $\tilde{k}_0$ is an extension of k_0 of degree n, then

$$\#\,\mathrm{Pic}_0(X_0 \times \tilde{k}_0) = (1 - \omega^n)(1 - \bar{\omega}^n).$$

If the elliptic curve is supersingular, i.e., p divides $\omega + \bar{\omega}$, then $\omega^n = \bar{\omega}^n$ for $n = 1, 2, 3, 4$, or 6 (cf. [9], see also the discussion in [5]). Hence, if m divides $\#\operatorname{Pic}_0(X_0)$, then the mth roots of unity are contained in $\tilde{k}_0$, where $\tilde{k}_0/k_0$ is an extension of degree at most 6.

Now let the elliptic curve be ordinary; i.e., p does not divide $\omega+\bar{\omega}$. Suppose m is a prime number which is inert in the imaginary quadratic field $\mathbf{Q}(\omega)$. If m divides $\#\operatorname{Pic}_0(X_0)$, then the mth roots of unity are contained in k_0. Hence, the only possible pairs (X_0, m) where the assumptions of the theorem are not satisfied are ordinary elliptic curves X_0 and integers m which are decomposed in the field $\mathbf{Q}(\omega)$.

(3) The authors of [5] use the Weil pairing to reduce the discrete logarithm of elliptic curves to the discrete logarithm of the multiplicative group. If one uses the Weil pairing, one must assume that all the m-torsion points of the elliptic curve are defined over k_0. This implies that k_0 contains the mth roots of unity. But the converse is not true in general. However, the main advantage of our pairing is the following. If the genus of X_0 is greater than 1, it is much weaker to assume that the mth roots of unity are in k_0 than forcing all m-torsion points to be defined over k_0. Also, a generalization of the Weil pairing algorithm, which is indeed possible, requires calculations of functions on the Jacobian variety of the curve X_0, whereas our algorithm only deals with functions on the curve X_0 itself.

Examples of hyperelliptic curves. Koblitz [2] considers hyperelliptic curves for use as cryptosystems based on the discrete logarithm. As examples he gives curves X_0 of genus 2 over a finite field k_0 of characteristic 2 with the equations (a) $v^2 + v = u^5 + u^3$, (b) $v^2 + v = u^5 + u^3 + u$, or (c) $v^2 + v = u^5$. An easy computation shows that if m divides $\#\operatorname{Pic}_0(X_0)$, then the mth roots of unity are contained in $\tilde{k}_0$, where $\tilde{k}_0/k_0$ is an extension of degree n with $n = 12$, 6, or 4 in case (a), (b), or (c), respectively. Hence, the discrete logarithm of $(\tilde{k}_0)^*$ is not too "complicated" compared with the logarithm in k_0^*.

Changing the role of $\operatorname{Pic}_0(X_0)_m$ and $\operatorname{Pic}_0(X_0)/m\operatorname{Pic}_0(X_0)$, one gets

Corollary 2. *Let $\overline{E}_1, \dots, \overline{E}_s$ be elements in $\operatorname{Pic}_0(X_0)$. The evaluation of the set*

$$\left\{ (\lambda_1, \dots, \lambda_s) \in (\mathbf{Z}/m\mathbf{Z})^s \,\middle|\, \sum_{i=1}^{s} \lambda_i \overline{E}_i \in m\operatorname{Pic}_0(X_0) \right\}$$

can be reduced to the evaluation of at most $(2g)^2$ discrete logarithms in k_0^* in probabilistic polynomial time in $\log q$.

Proof. Let $\{\overline{D}_1, \dots, \overline{D}_r\}$ be a basis of $\operatorname{Pic}_0(X_0)_m$, which will be constructed as in Corollary 1. Let ω be a primitive root in k_0^*. If one has $a_{ji} \in \mathbf{Z}/m\mathbf{Z}$ $(j = 1, \dots, r;\ i = 1, \dots, s)$ with $\{\overline{D}_j, \overline{E}_i\}_{0,m} = \omega^{a_{ji}}$, then $\sum_{i=1}^{s} \lambda_i \overline{E}_i \in m\operatorname{Pic}_0(X_0)$ if and only if $(\lambda_1, \dots, \lambda_s)$ is a solution of the linear system

$$\sum_{i=1}^{s} a_{ji}\lambda_i \equiv 0 \mod m \qquad (j = 1, \dots, r). \quad \square$$

Remark. If k is a local field and X is a curve with good reduction at the valuation of k, then results similar to the theorem and the corollaries can be proved. Indeed, in the next section we first study a pairing $\{\ ,\ \}_m$ for the curve X over k and then reduce it to our pairing $\{\ ,\ \}_{0,m}$ of the theorem.

2. The pairing

Let k be a local field, i.e., k is either a finite extension of a p-adic field $\mathbf{Q}_p$ or a power series field over a finite field $\mathbf{F}_q$ with $q = p^f$. The field k is complete with respect to a discrete valuation v with residue field k_0. By $\bar{k}$ we denote the separable closure of k, and G_k is the Galois group of $\bar{k}/k$.

Let X be a projective irreducible nonsingular curve of genus g over k. For simplicity we assume that X has a k-rational point. Let $\overline{X}$ be equal to $X \times \bar{k}$ and X_0 be the special fibre of the minimal model of X with respect to v. We will assume that X has good reduction modulo v, and so X_0 is a nonsingular irreducible projective curve over k_0 of genus g.

Some more notation: Let $\bar{k}(X)$ be the field of functions on $\overline{X}$; by $\mathrm{Div}_{(0)}(\overline{X})$ we denote the G_k-module of divisors (of degree 0) of $\overline{X}$, $H(\overline{X})$ are the principal divisors, and $\mathrm{Pic}_{(0)}(\overline{X})$ is the factor G_k-module $\mathrm{Div}_{(0)}(\overline{X})/H(\overline{X})$.

We have the following exact sequences of the G_k-modules:

$$1 \to \bar{k}^* \to \bar{k}(X)^* \to H(\overline{X}) \to 0,$$
$$0 \to H(\overline{X}) \to \mathrm{Div}_0(\overline{X}) \to \mathrm{Pic}_0(\overline{X}) \to 0,$$

and hence sequences of cohomology groups

$$H^2(G_k, \bar{k}(X)^*) \xrightarrow{\varphi} H^2(G_k, H(\overline{X})) \to H^3(G_k, \bar{k}^*) = 0,$$
$$0 = H^1(G_k, \mathrm{Div}_0(\overline{X})) \to H^1(G_k, \mathrm{Pic}_0(\overline{X})) \xrightarrow{\delta} H^2(G_k, H(\overline{X})).$$

Remark. We have $H^1(G_k, \mathrm{Div}_0(\overline{X})) = 0$, because there is a divisor of degree 1 in $\mathrm{Div}(\overline{X})^{G_k}$ by assumption.

For the following construction, cf. [3].

Take a cohomology class $\alpha \in H^1(G_k, \mathrm{Pic}_0(\overline{X}))$, and let β be an element in $H^2(G_k, \bar{k}(\overline{X})^*)$ with $\delta(\alpha) = \varphi(\beta)$. Let $\overline{D}$ be a class in $\mathrm{Pic}_0(\overline{X})^{G_k} = \mathrm{Pic}_0(X)$. It is easily proved (cf. [3]) that there is a 2-cocycle $(f_{\sigma,\tau})_{\sigma,\tau \in G_k} \in \beta$ and a divisor $D \in \overline{D}$ such that for all $\sigma, \tau \in G_k$ the principal divisor of $f_{\sigma,\tau}$ is prime to D. This allows us to define

$$c_{\sigma,\tau} := f_{\sigma,\tau}(D) := \prod_{P \in \overline{X}(\bar{k})} f_{\sigma,\tau}(P)^{n_P}, \qquad \text{where } D = \sum n_P P.$$

Again, it is not difficult to see (cf. [3] again) that $(c_{\sigma,\tau})$ is a 2-cocycle from G_k to $\bar{k}^*$ and that its class $[c_{\sigma,\tau}] \in H^2(G_k, \bar{k}^*)$ depends only on α and $\overline{D}$.

Define $\langle \alpha, \overline{D} \rangle := [c_{\sigma,\tau}]$. An important result of Lichtenbaum [3] is

Proposition 2.1. *The map*

$$\langle\ ,\ \rangle : H^1(G_k, \mathrm{Pic}_0(\overline{X})) \times \mathrm{Pic}_0(X) \to H^2(G_k, \bar{k}^*) \cong \mathbf{Q}/\mathbf{Z}$$

is a nondegenerate pairing.

Since $H^1(G_k, \mathrm{Pic}_0(\overline{X}))$ is a torsion group, we can restate this proposition:

Proposition 2.1′. *For all* $m \in \mathbf{N}$ *we have a nondegenerate pairing*

$$\langle\ ,\ \rangle_m\colon H^1(G_k, \mathrm{Pic}_0(\overline{X}))_m \times \mathrm{Pic}_0(X)/m\,\mathrm{Pic}_0(X) \to H^2(G_k, \bar{k}^*)_m \cong \mathbf{Z}/m\mathbf{Z}.$$

Remark. A crucial step in the paper of Lichtenbaum is to show that $\langle\ ,\ \rangle$ is (up to a sign) equal to the Tate pairing (cf. [8]).

From now on we assume that m is prime to the characteristic of k_0. Our aim is to transform the pairing $\langle\ ,\ \rangle_m$ into an easily computable form. At first we assume, in addition, that the mth roots of unity are contained in k.

Lemma 2.2. *Assume that the* m*th roots of unity are contained in* k. *Let* π *be a uniformizing element of* k, *i.e.,* π *generates the maximal ideal of* v, *and let* $\langle\tau\rangle$ *be the Galois group of* $k(\sqrt[m]{\pi})/k$. *Then*

$$\begin{aligned} H^1(G_k, \mathrm{Pic}_0(\overline{X}))_m &= \inf_{\overline{k}} H^1(\langle\tau\rangle, \mathrm{Pic}_0(X \times k(\sqrt[m]{\pi})))_m \\ &= \mathrm{Hom}(\langle\tau\rangle, \mathrm{Pic}_0(X)_m). \end{aligned}$$

Proof. The claim of the lemma is well known; for the convenience of the reader we repeat the arguments. Let k_u be the maximal unramified extension of k. Since m is prime to the characteristic of k_0, and since X, and so its Jacobian, have good reduction modulo v, it follows that $H^1(G(k_u/k), \mathrm{Pic}_0(X \times k_u))_m = H^2(G(k_u/k), \mathrm{Pic}_0(X \times k_u))_m = 0$. Therefore, the inflation-restriction sequence implies that

$$H^1(G_k, \mathrm{Pic}_0(\overline{X}))_m = H^1(G_{k_u}, \mathrm{Pic}_0(\overline{X}))_m^{G(k_u/k)}.$$

The exact sequence of G_{k_u}-modules

$$0 \to \mathrm{Pic}_0(\overline{X})_m \to \mathrm{Pic}_0(\overline{X}) \xrightarrow{m} \mathrm{Pic}_0(\overline{X}) \to 0$$

yields

$$0 \to H^1(G_{k_u}, \mathrm{Pic}_0(\overline{X})_m) \to H^1(G_{k_u}, \mathrm{Pic}_0(\overline{X}))_m \to 0,$$

because $\mathrm{Pic}_0(X \times k_u)$ is divisible by m (again we use that X has good reduction modulo v and that m is prime to the characteristic of the residue field). But G_{k_u} acts trivially on $\mathrm{Pic}_0(\overline{X})_m$; therefore, we get

$$H^1(G_{k_u}, \mathrm{Pic}_0(\overline{X}))_m = \mathrm{Hom}(G_{k_u}, \mathrm{Pic}_0(\overline{X})_m).$$

The maximal m-quotient of G_{k_u} is cyclic and equal to $G(k_u(\sqrt[m]{\pi})/k_u)$; hence

$$H^1(G_k, \mathrm{Pic}_0(\overline{X}))_m = \mathrm{Hom}(G(k_u(\sqrt[m]{\pi})/k_u), \mathrm{Pic}_0(\overline{X})_m)^{G(k_u/k)}.$$

Since τ commutes with each element of $G(k_u/k)$, the latter is equal to $\mathrm{Hom}(\langle\tau\rangle, \mathrm{Pic}_0(X)_m)$. □

Lemma 2.2 shows that the restriction of the pairing in Proposition 2.1′,

$$\begin{aligned} \langle\ ,\ \rangle_m\colon H^1(\langle\tau\rangle, \mathrm{Pic}_0(X \times k(\sqrt[m]{\pi})))_m &\times \mathrm{Pic}_0(X)/m \cdot \mathrm{Pic}_0(X) \\ &\to H^2(\langle\tau\rangle, k(\sqrt[m]{\pi})^*), \end{aligned}$$

is nondegenerate. Let φ be the map which assigns to $\overline{D} \in \mathrm{Pic}_0(X)_m$ the class of the 1-cocycle $(f_\rho)_{\rho\in\langle\tau\rangle}$ with $f_\tau = \overline{D}$. It is another consequence of the lemma that φ is an isomorphism from $\mathrm{Pic}_0(X)_m$ onto $H^1(\langle\tau\rangle, \mathrm{Pic}_0(X \times k(\sqrt[m]{\pi})))_m$.

The group $H^2(\langle\tau\rangle, k(\sqrt[m]{\pi})^*)$ is canonically isomorphic to

$$k^*/N_{k(\sqrt[m]{\pi})/k}(k(\sqrt[m]{\pi})^*),$$

where $N_{k(\sqrt[m]{\pi})/k}$ denotes the norm map. Since m is prime to the characteristic of the residue field k_0, and since $k(\sqrt[m]{\pi})/k$ is fully ramified, the latter is isomorphic to k_0^*/k_0^{*m}. We denote by ψ the isomorphism from $H^2(\langle\tau\rangle, k(\sqrt[m]{\pi})^*)$ onto k_0^*/k_0^{*m}.

If we apply the isomorphisms φ and ψ, we get a nondegenerate pairing between $\mathrm{Pic}_0(X)_m$ and $\mathrm{Pic}_0(X)/m\,\mathrm{Pic}_0(X)$.

We describe this pairing in a different manner. Take $\overline{D} \in \mathrm{Pic}_0(X)_m$ and a divisor $D \in \overline{D}$; then mD is the divisor of a function f. Let $\overline{E} \in \mathrm{Pic}_0(X)$ be a representative of a class modulo $m\,\mathrm{Pic}_0(X)$, and let E be a divisor in $\overline{E}$. We can choose E such that E and D are prime modulo v. Then $f(E)$, which is by definition $\prod f(P)^{n_P}$, where $E = \sum n_P P$, depends only on the divisor of f. Now Weil reciprocity allows us to define $\{\overline{D}, \overline{E}\}_m := \overline{f(E)}$ in k_0^*/k_0^{*m}. An explicit calculation shows that $\{\ ,\ \}_m$ is a new definition of the original pairing $\langle\ ,\ \rangle_m$; i.e., we get

Proposition 2.3. *Let $m \in \mathbf{N}$ be prime to the characteristic of k_0, and assume that the mth roots of unity are contained in k; then*

$$\{\ ,\ \}_m \colon \mathrm{Pic}_0(X)_m \times \mathrm{Pic}_0(X)/m\,\mathrm{Pic}_0(X) \to k_0^*/k_0^{*m}$$

satisfies $\{\overline{D}, \overline{E}\}_m = \psi\langle\varphi(\overline{D}), \overline{E}\rangle_m$ for each $\overline{D} \in \mathrm{Pic}_0(X)_m$, $\overline{E}$ in $\mathrm{Pic}_0(X)$. In particular, $\{\ ,\ \}_m$ is nondegenerate.

What can be done when the mth roots of unity are not contained in k?

Let ζ_m be a primitive mth root of unity, and let $\langle\sigma\rangle$ be the Galois group of $k(\zeta_m)/k$. We denote by χ_m the cyclotomic character of $\langle\sigma\rangle$ defined by $\sigma(\zeta_m) = \zeta_m^{\chi_m(\sigma)}$.

Now we consider the nondegenerate pairing of Proposition 2.3 for the field $k(\zeta_m)$,

$$\{\ ,\ \}_m \colon \mathrm{Pic}_0(X \times k(\zeta_m))_m \times \mathrm{Pic}_0(X \times k(\zeta_m))/m\,\mathrm{Pic}_0(X \times k(\zeta_m)) \to k_0(\zeta_m)^*/k_0(\zeta_m)^{*m}.$$

The group $\langle\sigma\rangle$ acts on divisors, and the operation on $k_0(\zeta_m)^*/k_0(\zeta_m)^{*m}$ is induced by χ_m; hence we get

$$\{\sigma(\overline{D}), \sigma(\overline{E})\}_m = \{\overline{D}, \overline{E}\}_m^{\chi_m(\sigma)}.$$

If $[k(\zeta_m) : k]$ is prime to m, then the action of $\langle\sigma\rangle$ is semisimple, and the decomposition in eigenspaces for characters yields a nondegenerate pairing

$$\{\ ,\ \}_m \colon \mathrm{Pic}_0(X \times k(\zeta_m))_m[\chi_m] \times (\mathrm{Pic}_0(X \times k(\zeta_m))/m\,\mathrm{Pic}_0(X \times k(\zeta_m)))^{\langle\sigma\rangle} \to k_0(\zeta_m)^*/k_0(\zeta_m)^{*m},$$

where $\mathrm{Pic}_0(X \times k(\zeta_m))_m[\chi_m]$ is the subgroup of elements $\overline{D} \in \mathrm{Pic}_0(X \times k(\zeta_m))_m$ which satisfy $\sigma(\overline{D}) = \chi_m(\sigma)\overline{D}$.

Again using the fact that $[k(\zeta_m) : k]$ is prime to m, one sees that

$$(\mathrm{Pic}_0(X \times k(\zeta_m))/m\,\mathrm{Pic}_0(X \times k(\zeta_m)))^{\langle\sigma\rangle}$$

is canonically isomorphic to $\mathrm{Pic}_0(X)/m\,\mathrm{Pic}_0(X)$. This yields

Proposition 2.4. *Let $m \in \mathbf{N}$ be prime to the characteristic of k_0. Let ζ_m be a primitive mth root of unity, and assume that the degree of $k(\zeta_m)/k$ is prime to m. Then $\{\ ,\ \}_m$ is a nondegenerate pairing*

$$\{\ ,\ \}_m \colon \mathrm{Pic}_0(X \times k(\zeta_m))_m[\chi_m] \times \mathrm{Pic}_0(X)/m\,\mathrm{Pic}_0(X) \to k_0(\zeta_m)^*/k_0(\zeta_m)^{*m}.$$

Remark. Proposition 2.3 is a special case of the last statement. The assumptions of Proposition 2.4 are satisfied if m is a prime number different from the characteristic of k_0.

The definition of $\{\ ,\ \}_m$ can be reduced modulo v to get a pairing corresponding to a curve over a finite field.

Let X_0 be a projective irreducible nonsingular curve of genus g over a finite field k_0. Take $\overline{D}_0 \in \mathrm{Pic}_0(X_0)_m$ and $\overline{E}_0 \in \mathrm{Pic}_0(X_0)$, and choose divisors $D_0 \in \overline{D}_0$ and $E_0 \in \overline{E}_0$ which are relatively coprime. Then mD_0 is the divisor of a function f_0, and we can define $\{\overline{D}_0, \overline{E}_0\}_{0,m} := \overline{f_0(E_0)}$ in k_0^*/k_0^{*m}. This definition only deals with curves over finite fields. In order to prove that $\{\ ,\ \}_{0,m}$ is nondegenerate, we take a local field k with residue field k_0 and a curve X of genus g whose special fibre is X_0. It is not difficult to see that $\{\overline{D}_0, \overline{E}_0\}_{0,m} = \{\overline{D}, \overline{E}\}_m$, where D, E are divisors whose reduction is D_0, E_0, respectively. With this remark we get from Propositions 2.3 and 2.4

Proposition 2.5. *Let $m \in \mathbf{N}$ be prime to the characteristic of k_0. Let ζ_m be a primitive mth root of unity, and assume that the degree of $k_0(\zeta_m)/k_0$ is prime to m. Then the pairing*

$$\{\ ,\ \}_{0,m} \colon \mathrm{Pic}_0(X_0 \times k_0(\zeta_m))_m[\chi_m] \times \mathrm{Pic}_0(X_0)/m\,\mathrm{Pic}_0(X_0) \to k_0(\zeta_m)^*/k_0(\zeta_m)^{*m}$$

is nondegenerate.

If m divides $q-1$, then Proposition 2.5 shows the first part of the theorem in §1.

3. Evaluation of the pairing

In the previous section it was shown that the evaluation of the Tate pairing can be reduced to the following problem: Let k be a field whose characteristic does not divide m, and let X be a projective irreducible nonsingular curve over k of genus g. For elements $\overline{D} \in \mathrm{Pic}_0(X)_m$ and $\overline{E} \in \mathrm{Pic}_0(X)$, take any divisor $D \in \overline{D}$ and find a function f on X whose divisor is equal to mD; take a divisor $E \in \overline{E}$ which is prime to D and then evaluate $f(E)$.

In the following we present an algorithm for an evaluation of $f(E)$ which takes $O(\log m)$ elementary operations. In order to achieve this, it is of course necessary to do explicit calculations in the group $\mathrm{Pic}_0(X)$. As it was pointed out in §1, we assume that we can do the following step:

(*) Let A_1 and A_2 be positive divisors of degree g; find a positive divisor A_3 of degree g and a function h such that the divisor of h is equal to $A_1 + A_2 - A_3 - gP_0$.

We denote by c_g the surjective map which assigns to a positive divisor A of degree g the element $c_g(A) = \overline{A - gP_0}$ in $\mathrm{Pic}_0(X)$ (cf. §1). Let E be a divisor in $\mathrm{Div}_0(X)$ whose support does not contain P_0. Let S be a finite subgroup of $\mathrm{Pic}_0(X)$. We suppose that S has a set of representatives $\{A_s\}$ under c_g which are prime to E. We fix such a set of representatives and define the following group law on $S \times k^*$:

$$(s_1, a_1) \odot (s_2, a_2) = (c_g(A_{s_3}), a_1 a_2 h(E)),$$

where A_{s_3} is the divisor and h is the function in step $(*)$ corresponding to A_{s_1} and A_{s_2}; furthermore, s_3 is the sum of s_1 and s_2 in S. The assumptions guarantee that $h(E)$ is a nonzero element in k.

Remark. For the theoretical background of this group law we refer to the theory of theta groups (cf. [6]).

Lemma 3.1. *Let E be a divisor in $\mathrm{Div}_0(X)$ which is prime to P_0, and let $\overline{D} \in \mathrm{Pic}_0(X)_m$; we suppose that the subgroup of $\mathrm{Pic}_0(X)$ which is generated by $\overline{D}$ has a set of representatives which are prime to E; the representative of 0 should be gP_0. Then*

$$(\overline{D}, 1) \underbrace{\odot \cdots \odot}_{m \text{ times}} (\overline{D}, 1) = (0, f(E)),$$

where f is the function on X whose divisor is equal to mD.

Proof. Let A_i be the representative of $i\overline{D}$. One sees immediately that

$$(\overline{D}, 1) \underbrace{\odot \cdots \odot}_{m \text{ times}} (\overline{D}, 1) = (i\overline{D}, h_i(E)),$$

where h_i has the divisor $iA_1 - A_i - (i-1)gP_0$. Since $m\overline{D} = 0$ and $A_m = gP_0$, we get $h_m(E) = f(E)$. □

With this lemma one can evaluate $f(E)$ with $O(\log m)$ elementary operations by using repeated doubling in the group $(\langle\overline{D}\rangle \times k^*, \odot)$.

Remark. If $g = 1$, one can use Lemma 3.1 to evaluate the Weil pairing of the elliptic curve X. These ideas are used in [1, 4].

Let $\overline{D} \in \mathrm{Pic}_0(X)_m$ and $\overline{E} \in \mathrm{Pic}_0(X)$. In order to evaluate $f(E)$ with Lemma 3.1, it is not necessary to assume that the divisor $E \in \overline{E}$ is prime to the representative of each $i\overline{D}$. Only those representatives are important which are used to perform the m-fold addition by the repeated doubling method. Hence E can be chosen in $O(\log m)$ steps.

From this, we get

Proposition 3.2. *Let $\overline{D} \in \mathrm{Pic}_0(X)_m$ and $\overline{E} \in \mathrm{Pic}_0(X)$, take divisors $D \in \overline{D}$ and $E \in \overline{E}$ which are relatively prime, and let f be a function whose divisor is mD. Then $f(E)$ (modulo k^{*m}) can be evaluated in $O(\log m)$ elementary operations.*

Bibliography

1. B. Kaliski, *Elliptic curves and cryptology: A pseudorandom bit generator and other tools*, Ph.D. thesis, M.I.T., 1988.
2. N. Koblitz, *Hyperelliptic cryptosystems*, J. Cryptology **1** (1989), 139–150.
3. S. Lichtenbaum, *Duality theorems for curves over p-adic fields*, Invent. Math. **7** (1969), 120–136.
4. V. Miller, *Short programs for functions on curves*, unpublished manuscript, 1986.
5. A. Menezes, S. Vanstone, and T. Okamato, *Reducing elliptic curve logarithms to logarithms in a finite field*, preprint.

6. D. Mumford, *Abelian varieties*, Oxford Univ. Press, New York, 1970.

7. A. Odlyzko, *Discrete logarithms and their cryptographic significance*, Advances in Cryptology: Proceedings of Eurocrypt '84, Lecture Notes in Comput. Sci., vol. 209, Springer-Verlag, Berlin and New York, 1985, 224–314.

8. J. Tate, *WC-groups over p-adic fields*, Sem. Bourbaki, no. 156, December 1957, 13p.

9. W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École. Norm. Sup. **2** (1969), 521–560.

Institute for Experimental Mathematics, University of Essen, Ellernstrasse, W-45326 Essen, Germany

E-mail address: mem030@vm.hrz.uni-essen.de