MATHEMATICS OF COMPUTATION
Volume 68, Number 226, April 1999, Pages 805–806
S 0025-5718(99)01043-1

ON THE DISCRETE LOGARITHM IN THE DIVISOR CLASS GROUP OF CURVES

HANS-GEORG RÜCK

ABSTRACT. Let X be a curve which is defined over a finite field k of characteristic p. We show that one can evaluate the discrete logarithm in $Pic_0(X)_{p^n}$ by $O(n^2 \log p)$ operations in k. This generalizes a result of Semaev for elliptic curves to curves of arbitrary genus.

Let k be a finite field of characteristic p. We consider a projective irreducible nonsingular curve X of genus $g \geq 1$ which is defined over k. We assume that the curve X has a k-rational point P_0. Let $Pic_0(X)_m$ be the subgroup of the m-torsion points in the group of divisor classes of degree 0 on X.

In [1] it is shown that one can reduce the evaluation of the discrete logarithm in $Pic_0(X)_m$ by $O(\log m)$ operations to the evaluation of the discrete logarithm in $k(\zeta_m)^*$, where ζ_m is a primitive m-th root of unity, if the integer m is prime to p. If $m = p$ and if the curve X is an elliptic curve (i.e., $g = 1$), then it is proved in [2] that the discrete logarithm in $Pic_0(X)_p$ can be evaluated by $O(\log p)$ operations in k. We want to extend this result to curves X of arbitrary genus g, and we will see that its proof is based on the connection between $Pic_0(X)_p$ and logarithmic holomorphic differentials on X.

Theorem. *The discrete logarithm in $Pic_0(X)_{p^n}$ can be evaluated by $O(n^2 \log p)$ operations in k.*

Proof. Let $x \in Pic_0(X)_{p^n}$ be an element of order p^n and let y be contained in the cyclic group generated by x. We have to show that $\lambda \in \mathbb{Z}/p^n\mathbb{Z}$ with $y = \lambda \cdot x$ can be evaluated by $O(n^2 \log p)$ operations. It is a standard argument to reduce the evaluation of $\lambda = \sum_{i=0}^{n-1} \lambda_i p^i$ with $0 \leq \lambda_i < p$ to the evaluation of λ_i (by multiplication with p^i, $0 \leq i \leq n-1$) as solutions of n discrete logarithms in $Pic_0(X)_p$. Hence we can assume that $n = 1$.

The key point of the proof is the following result of Serre ([3], Proposition 10). Let $\Omega^1(X)$ be the k-vector space of holomorphic differentials on X. Then there is an isomorphism from $Pic_0(X)_p$ into $\Omega^1(X)$ given by the following rule: Choose a divisor D of degree 0 with $p \cdot D = (f)$, where f is a function on X, then the divisor class $\overline{D} \in Pic_0(X)_p$ is mapped to the holomorphic differential df/f.

Received by the editor August 8, 1997.
1991 *Mathematics Subject Classification.* Primary 11T71; Secondary 94A60.

Now let t be a local parameter of P_0, then we get $df/f = \frac{\partial f/\partial t}{f}\,dt$. We evaluate the power series expansion

$$\frac{\partial f/\partial t}{f} = \sum_{i=0}^{\infty} a_i t^i \quad \text{with} \quad a_i \in k.$$

We denote by $(a_0, a_1, ..., a_{2g-2})(f)$ the vector of the coefficients at $1, t, ..., t^{2g-2}$ of $f^{-1}(\partial f/\partial t)$. The Riemann-Roch theorem says that these coefficients determine the holomorphic differential df/f uniquely. Hence we get an isomorphism ϕ from $Pic_0(X)_p$ into k^{2g-1} which is defined by $\phi(\overline{D}) = (a_0, a_1, ..., a_{2g-2})(f)$.

For elliptic curves this is the isomorphism in Lemma 2 of [2].

It remains to evaluate $\phi(\overline{D})$ by $O(\log p)$ operations, because the discrete logarithm in k^{2g-1} can be evaluated by this complexity. For this we modify the ideas of Chapter 3 in [1]. Since the addition in $Pic_0(X)$ should be given explicitly, it is possible to solve the following problem:

(*) 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 $A^{(1)} + A^{(2)} - A^{(3)} - gP_0$.

Let S be a finite subgroup of $Pic_0(X)_p$. We suppose that S has a set of representatives $\{A_s\}$ under c_g which are prime to P_0 (here c_g is given by $c_g(A_s) = \overline{A_s - gP_0}$).

We define the following group law on $S \times k^{2g-1}$:

$$(s_1, v_1) \odot (s_2, v_2) = (c_g(A_{s_3}), v_1 + v_2 + (a_0, ..., a_{2g-2})(h)),$$

where $A_{s_3} = A^{(3)}$ is the divisor and h is the function in (*) corresponding to $A^{(1)} = A_{s_1}$ and $A^{(2)} = A_{s_2}$; $(a_0, ..., a_{2g-2})(h)$ is defined as above, even if the differential $h^{-1}(\partial h/\partial t)\,dt$ has a pole at P_0. Furthermore s_3 is the sum of s_1 and s_2 in S.

In other words we use the 2-cocyle $S \times S \to k^{2g-1}$ with $(s_1, s_2) \mapsto (a_0, ..., a_{2g-2})(h)$ to define the group law. This is the additive version of the Tate pairing.

It can be shown easily by induction that $(\overline{D}, 0) \odot \cdots \odot (\overline{D}, 0)$ (p-times) is equal to $(0, \phi(\overline{D}))$.

Hence using repeated doubling in the group $(\langle \overline{D} \rangle \times k^{2g-1}, \odot)$ we can evaluate $\phi(\overline{D})$ by $O(\log p)$ operations in the field k.

References

[1] G. Frey and H.-G. Rück, *A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves*, Math. Comp. **62** (1994), 865-874. MR **94h**:11056

[2] I. A. Semaev, *Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p*, Math. Comp. **67** (1998), 353–356. MR **98c**:94017

[3] J. P. Serre, *Sur la topologie des variétés algébriques en caractéristique p*, Sympos. Internat. Topologia Algebraica, Mexico City 1956, 24-53. MR **20**:4559

Institut für Experimentelle Mathematik, Universität GH Essen, Ellernstr. 29, D-45326 Essen, Germany

E-mail address: rueck@exp-math.uni-essen.de