International Journal of Pure and Applied Mathematics
Volume 19 No. 2 2005, 249-254

PROJECTIVE CURVES AND CRYPTOGRAPHY

E. Ballico[1 §], Claudio Fontanari[2]
[1,2]Department of Mathematics
University of Trento
380 50 Povo (Trento) - Via Sommarive, 14, ITALY
[1]e-mail: ballico@science.unitn.it
[2]e-mail: fontanar@science.unitn.it

Abstract: We describe an explicit algorithm for addition in the Jacobian of projective curves satisfying very mild assumptions (in particular, arbitrary singularities are allowed).

AMS Subject Classification: 1T71, 14Q05, 14H99, 14N05
Key Words: algebraic curves cryptography, Cartier divisors on singular curves, arithmetically Cohen-Macaulay curve

1. Introduction

The beginning of a fruitful interaction between public key cryptography and algebraic geometry over finite fields goes back at least to 1985, when elliptic curve cryptosystems were proposed independently by Koblitz and Miller in order to increase the flexibility in the choice of the group (see [6], Chapter 6, § 2.1). In the past twenty years, this branch of research has obtained significant results, attracting a great deal of interest; as a natural consequence, the first steps have been done towards the application to cryptography of a broader class of algebraic curves. In particular, the theory of hyperelliptic cryptosystems has already reached the stage of a systematical development (see for instance Appendix in [6]). As pointed out in [6], Chapter 6, § 5.2, the advantage of working with the Jacobian of a hyperelliptic curve is essentially twofold: first

Received: January 7, 2005

[§] Correspondence author

of all, in this case every element of the Jacobian admits a sort of canonical representation; moreover, it is relatively straightforward to add two elements in the Jacobian. However, in the last few years it has been realized that the above two properties are not strictly peculiar to hyperelliptic curves: for instance, the case of Picard curves, i.e. smooth genus 3 cyclic trigonal curves, has been investigated by several authors (see in particular [2]). The paper [5] contains an updated and comprehensive survey of the available solutions for smooth algebraic curves.

In the present note we develop the approach of [2], obtaining much more general results. First of all, in Theorem 1 we settle once and for all the problem of expressing any Cartier divisor of degree zero on a projective curve in a unique simple way (we stress that we allow arbitrary singularities). Next, we present an explicit algorithm for addition in the Jacobian, which is inspired by a geometrical construction proposed in [2] for smooth plane curves of genus 3 with a hyperflex. Our algorithm works for arbitrarily singular curves of arbitrary arithmetic genus embedded in a projective space of arbitrary dimension; we only assume that the embedded curve has a smooth hyperflex and is arithmetically Cohen-Macaulay (see Definition 1 and Definition 2). After proving in Theorem 2 that our recipe produces the correct result, we show in Proposition 1 that every projective curve with a smooth rational point admits infinitely many natural embeddings satisfying all assumptions of Algorithm 1. Finally, in Proposition 2 we determine the explicit equation of every plane curve to which Algorithm 1 can be applied.

This research is part of the T.A.S.C.A. project of I.N.d.A.M., supported by P.A.T. (Trento) and M.I.U.R. (Italy).

2. The Results

We work over an arbitrary (perfect) field. We are going to use freely notation and terminology from the standard reference book [4]. Once and for all, we point out that we can apply every cohomological statement proved on an algebraically closed field thanks to the basic fact that cohomology commutes with flat base extension (see [4], III, Proposition 9.3).

Theorem 1. *Let C be an integral projective curve of arithmetic genus g with a smooth rational point P_0. Let D be a Cartier divisor on C with $\deg(D) = 0$. Then there is an effective divisor E with $e := \deg(E) \leq g$ such that $D \sim E - eP_0$. Moreover, if e is minimal, then E is uniquely determined.*

Proof. We are going to apply the Riemann-Roch Theorem

$$h^0(C,F) - h^1(C,F) = \deg(F) - g + 1,$$

which holds for every Cartier divisor F on any integral projective curve C of aritmetic genus g (see for instance [7], Theorem 1 on p. 79). It follows that

$$h^0(C, D + eP_0) = h^1(C, D + eP_0) + e - g + 1 \geq 1$$

for every $e \geq g$, hence there is at least one effective Cartier divisor $E \sim D + gP_0$. If $h^0(C, D + gP_0) > 1$, since the passage through any point imposes at most one linear condition, there is an integer $e < g$ such that $h^0(C, D + eP_0) = 1$, and in this case the effective divisor E is uniquely determined. □

Definition 1. Let $C \subset \mathbb{P}^n$ be an integral curve of degree d with a rational point P_0. We say that P_0 is a *hyperflex* if there exists a hyperplane $H \subset \mathbb{P}^n$ such that (scheme-theoretically) $H \cap C = dP_0$. If moreover P_0 is a nonsingular point of C, we say that P_0 is a *smooth hyperflex*.

Definition 2. Let $C \subset \mathbb{P}^n$ be an integral curve. We say that C is *arithmetically Cohen-Macaulay* if $H^1(\mathbb{P}^n, \mathcal{I}_C(i)) = 0$ for every $i \geq 1$.

Algorithm 1. Let $C \subset \mathbb{P}^n$ be an integral curve of degree d and arithmetic genus g with a smooth hyperflex P_0 and assume that C is arithmetically Cohen-Macaulay.

Input. two Cartier divisors of degree zero $D_1 := E_1 - e_1 P_0, e_1 \leq g$, and $D_2 := E_2 - e_2 P_0, e_2 \leq g$.

Output. the unique Cartier divisor $S - sP_0, s \leq g$, such that $D_1 + D_2 \sim S - sP_0$.

- define integers h, u, as follows:

$$g + e_1 + e_2 = hd - u, \qquad 0 \leq u \leq d - 1;$$

- take a homogeneous polynomial f of degree h in $n+1$ indeterminates such that the divisor $A := C \cap \{f = 0\}$ contains E_1, E_2 and passes through P_0 with maximal possible multiplicity $m \geq u$;
- let $R := A - E_1 - E_2 - mP_0$ and $r := \deg(R) \leq g$;
- define integers k, v, as follows:

$$g + r = kd - v, \qquad 0 \leq v \leq d - 1;$$

- take a homogeneous polynomial φ of degree k in $n+1$ indeterminates such that the divisor $B := C \cap \{\varphi = 0\}$ contains R and passes through P_0 with maximal possible multiplicity $\mu \geq v$;
- let $S := B - R - \mu P_0$ and $s := \deg(S) \leq g$.

Theorem 2. *We have $D_1 + D_2 \sim S - sP_0$.*

Proof. By the Riemann-Roch Theorem, we have

$$h^0(C, hdP_0 - E_1 - E_2 - uP_0) \geq 1;$$

moreover, since C is arithmetically Cohen-Macaulay, the natural map

$$H^0(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(h)) \to H^0(C, \mathcal{O}_C(h)) = H^0(C, hdP_0)$$

is surjective. Hence we get the polynomial f and we obtain

$$E_1 - e_1P_0 + E_2 - e_2P_0 = -(R - rP_0) + (f).$$

Similarly, we have

$$h^0(C, kdP_0 - R - vP_0) \geq 1$$

and

$$H^0(\mathbb{P}^n, \mathcal{O}_{\mathbb{P}^n}(k)) \to H^0(C, kdP_0) \to 0.$$

It follows that

$$S - sP_0 = -(R - rP_0) + (\varphi)$$

for some polynomial φ. Summing up, we see that

$$E_1 - e_1P_0 + E_2 - e_2P_0 \sim S - sP_0,$$

as claimed. □

Proposition 1. *Let C be an integral projective curve of arithmetic genus g with a smooth rational point P_0. If $d \geq 2g+1$ then the complete linear series $|dP_0|$ embeds C in $\mathbb{P}^{d-g}$ as an arithmetically Cohen-Macaulay curve having P_0 as a smooth hyperflex.*

Proof. By Serre duality (see [4], III, Corollary 7.7), we have $H^1(C, F) = 0$ for every Cartier divisor F such that $\deg(F) \geq 2g-1$, so we may deduce from the Riemann-Roch Theorem that the divisor dP_0 is very ample for every $d \geq 2g+1$ (see [1], Remark 2.1) and the corresponding morphism is an embedding. Since the linear series $|dP_0|$ is complete, we have $H^1(C, \mathcal{I}_C(1)) = 0$; hence by using the natural exact sequence

$$0 \to \mathcal{I}_C(i-1) \to \mathcal{I}_C(i) \to \mathcal{I}_{C\cap H}(i) \to 0,$$

where H is a general hyperplane, we may deduce that C is arithmetically Cohen-Macaulay inductively from $H^1(\mathbb{P}^n, \mathcal{I}_{C\cap H}(i)) = 0$ for every $i \geq 2$. Indeed, by [8], Theorem 2.5, if H is general then $C \cap H$ is formed by d points in linearly general position; on the other hand, by [3], Theorem 2.1, if S is a set of $d \leq 2r+1$ points in linearly general position we have $H^1(\mathbb{P}^r, \mathcal{I}_S(i)) = 0$ for every $i \geq 2$, so the claim follows. □

Proposition 2. *Let C be a projective plane curve of degree d with a rational point P_0. Then C is integral and arithmetically Cohen Maculay with P_0 as a smooth hyperflex if and only if there are coordinates X, Y, Z on $\mathbb{P}^2$ in which $P_0 = (0,0,1)$ and the equation of C is given by*

$$cY^d + Xp(X,Y,Z) = 0,$$

where p is a homogeneous polynomial of degree $d-1$ such that $p(0,0,1) \neq 0$.

Proof. We recall that any plane curve embedded by a complete linear series is arithmetically Cohen-Macaulay by [4], III, Theorem 5.1 (b). The check of the stated equivalence is completely elementary and left to the interested reader. □

References

[1] F. Catanese, M. Franciosi, K. Hulek, M. Reid, Embeddings of curves and surfaces, *Nagoya Math. J.*, **154** (1999), 185-220.

[2] S. Flon, R. Oyono, Fast arithmetic on Jacobians of Picard curves, *Cryptology ePrint Archive*, Report 2003/079.

[3] M. Green, R. Lazarsfeld, Some results on the syzygies of finite sets and algebraic curves, *Compositio Math.*, **67** (1988), 301-314.

[4] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, **52**, Springer-Verlag, New York-Heidelberg (1977).

[5] K. Khuri-Makdisi, Linear algebra algorithms for divisors on an algebraic curve, *Math. Comp.*, **73** (2004), 333-357.

[6] N. Koblitz, *Algebraic Aspects of Cryptography*, with an Appendix by Alfred J. Menezes, Yi-Hong Wu, Robert J. Zuccherato, *Algorithms and Computation in Mathematics*, **3**, Springer-Verlag, Berlin (1998).

[7] D. Mumford, Lectures on curves on an algebraic surface, with a section by G. M. Bergman, *Annals of Mathematics Studies*, **59**. Princeton University Press, Princeton, N.J. (1966).

[8] J. Rathmann: The uniform position principle for curves in characteristic *p*, *Math. Ann.*, **276** (1987), 565-579.