

# A new implementation of Miura-Arita algorithm for Miura curves

A. Basiri, S. Rahmany, D. Khatibi

**Abstract**—The aim of this paper is to review some of standard fact on Miura curves. We give some easy theorem in number theory to define Miura curves, then we present a new implementation of Arita algorithm for Miura curves.

**Keywords**—Miura curve, discrete logarithm problem, algebraic curve cryptography, Jacobian group.

## I. INTRODUCTION

**T**HE The goal of this paper is to describe a practical and efficient algorithm for computing in the Jacobian of a  $C_A$  curves over a finite field. Authors in [6] proposed an algorithm to complete the arithmetic in the base field for superelliptic curves, and the authors in [2], [7], generalise the algorithm to the class of  $C_{ab}$  curves and in [3] generalise the algorithm to the class of  $C_A$  curves, which includes superelliptic and  $C_{ab}$  curves as a special case. Furthermore, in [4], [5], [1], for the case of  $C_{34}$  curves, has presented some faster method to compute the addition of two point on the curve.

## II. NUMERICAL SEMIGROUP

In this paper we denote by  $\mathbb{N}_0$ , the set of all non negative integers numbers, so  $\mathbb{N}_0$  is an additive semigroup. In addition we suppose that  $M$  be a proper sub semigroup of  $\mathbb{N}_0$  such that  $0 \in M \neq 0$ .

**Theorem 1:** There is an integer number  $t$  and there exist some members  $a_1, a_2, \dots, a_t$  in  $M$  such that

$$M = \langle a_1, a_2, \dots, a_t \rangle, \quad a_1 < a_2 < \dots < a_t, \quad t \leq a_1.$$

In other words,  $M$  is a finitely generated semigroup in  $\mathbb{N}_0$ .

**Proof:** Since  $<$  is a well-ordering order in  $\mathbb{N}_0$ , then there exists a minimal member, say  $a_1$ , in  $M - \{0\}$ . On the other hand since  $M$  is a proper semigroup, then  $1 \neq a_1$ , so  $1 < a_1$ . Now let  $T_2$  be the set of all members  $a \in M$  such that  $a \equiv 1 \pmod{a_1}$ , so there are two cases: if  $T_2$  is the empty set then  $M = \langle a_1 \rangle$  and the proof is completed, else if  $T_2 \neq \emptyset$  then the minimum of  $T_2$ , denoted  $a_2$ , exists. we then suppose  $T_3$  be the set of all members  $a \in M$  such that  $a \equiv 2 \pmod{a_1}$ , so if  $T_3 \neq \emptyset$  then the minimum of  $T_3$ , denoted  $a_3$ , exists. Here suppose that the  $T_2, T_3, \dots, T_l$  and the  $a_2, a_3, \dots, a_l$  are chosen, we claim that  $M = \langle a_1, a_2, \dots, a_t \rangle$ . The inclusion  $M \supseteq \langle a_1, a_2, \dots, a_t \rangle$  follow directly from the definition. Going the other way, note that,  $w \in M$ , by division algorithm, there exist  $q \in \mathbb{N}_0$  and  $0 \leq r \leq a_1 - 1$  such that  $w = a_1q + r$ .

Hence  $T_{r+1}$  is a non empty set and has a minimum denoted by  $a_{r+1}$  and so  $a_{r+1} = a_1q' + r$  with  $q' \leq q$  and so

$$w = a_1(q - q') + a_1q' + r = a_1(q - q') + a_{r+1} \in \langle a_1, a_2, \dots, a_t \rangle$$

■

**Example 2:** If  $M = \{0, 7, 8, 14, 15, 16, 19, 21, 22, 23, \dots\}$  then  $a_1 = 7, a_2 = 8, a_3 = 16, a_4 = 24, a_5 = 25, a_6 = 19$  and  $a_7 = 27$ .

The following theorem express whenever the complement of any semigroup with identity of  $\mathbb{N}_0$  is finite?

**Theorem 3:** The set  $\bar{M} = \mathbb{N}_0 - M$  is finite if and only if  $\gcd(a_1, a_2, \dots, a_t) = 1$ , and in this case,  $|\bar{M}| = \sum_{i=1}^{a_1-1} \lfloor \frac{b_i}{a_1} \rfloor$ , where  $b_i$  is the minimum amount of members  $a$  in  $M$  with  $a \equiv i \pmod{a_1}$ .

**Proof:** Firstly, suppose that  $\bar{M}$  is a finite set, to have a contrast let there exists a prime number  $p$  such that  $p|a_i$  for all  $1 \leq i \leq t$ . We claim that for all non negative integer  $q$ ,  $a_1q + 1 \notin M$ , if it is not the case then there exists  $q \in \mathbb{N}_0$  such that  $a_1q + 1 \in M$  and so the  $T = \{a_1u + 1 : u \in \mathbb{N}_0, a_1u + 1 \in M\}$  is a non empty set and so has a minimum, denoted by  $a_2$ . Hence there exists  $r \in \mathbb{N}_0$  such that  $a_2 = a_1r + 1$ , but  $p|a_1$  and  $p|a_2$ , and this implies that  $p$  divides 1 and this contradicts the fact that  $p$  is a prime number. A consequence of all this is that the set  $\{a_1q + 1 : q \in \mathbb{N}_0\}$  is a subset of  $\bar{M}$  and so  $\bar{M}$  is infinite which contradicts the hypothesis. To get the opposite direction, let  $\gcd(a_1, a_2, \dots, a_t) = 1$ . Note that for  $0 \leq i \leq a_1 - 1$ ,

$$b_i = \min\{\lambda a_1 + i : \lambda \in \mathbb{N}_0, \lambda a_1 + i \in M\}$$

, let  $s = a_1 - 1$ ,  $b_i = w_i a_1 + i$  and for  $1 \leq i \leq s$  put

$$A_i = \{i, a_1 + i, 2a_1 + i, \dots, (w_i - 1)a_1 + i\},$$

we claim that  $A_1, A_2, \dots, A_s$  are a partition of  $\bar{M}$ . We show first that for  $i \neq j$ ,  $A_i \cap A_j = \emptyset$ , if this is not the case then there are  $r, r'$  such that

$$ra_1 + i = r'a_1 + j \Leftrightarrow (r - r')a_1 = j - i \Leftrightarrow a_1|j - i,$$

but  $1 \leq i, j \leq s = a_1 - 1 < a_1$ , hence  $j - i = 0$  which is a contradiction and so  $A_i \cap A_j = \emptyset$ . we now show that  $\bigcup_{i=1}^s A_i = \bar{M}$ . To establish the desired equality, we use the usual strategy of proving containment in both directions. The inclusion  $\bigcup_{i=1}^s A_i \subseteq \bar{M}$  follow directly from the fact that  $A_i \subseteq \bar{M}$  for all  $1 \leq i \leq s$ . To get the opposite inclusion, suppose  $x \in \bar{M}$  so there are  $\lambda \in \mathbb{N}_0$  and  $1 \leq j \leq s$  such that  $x = \lambda a_1 + j$ . We claim that  $\lambda \leq w_j - 1$  and this implies that  $x \in A_j \subseteq \bigcup_{i=1}^s A_i \subseteq \bar{M}$ . If it is not the case, then  $w_j \leq \lambda$ , hence

$$x = (w_j + (\lambda - w_j))a_1 + j = b_j + (\lambda - w_j)a_1 \in M$$

A. Basiri, S. Rahmany, D. khatibi : School of Mathematics and Computer Sciences, Damghan University of Basic Science , Damghan, Iran, e-mail: basiri,rahmany@dubs.ac.ir.

Manuscript received October 31, 2009.

which is a contradiction. Hence  $A_1, A_2, \dots, A_s$  are a partition of  $\bar{M}$ , and so

$$|\bar{M}| = \left| \bigcup_{i=1}^s A_i \right| = \sum_{i=1}^s |A_i| = \sum_{i=1}^s w_i$$

but since  $a_1 > 1$  we have

$$w_i = \left\lfloor w_i + \frac{1}{a_1} \right\rfloor = \left\lfloor \frac{w_i a_1 + 1}{a_1} \right\rfloor = \left\lfloor \frac{b_i}{a_1} \right\rfloor.$$

A semigroup  $M$  of  $\mathbb{N}_0$  with  $0 \in M \neq 0$  is called a numerical semigroup if its complement in  $\mathbb{N}_0$  be a finite set.

*Example 4:* The semigroup introduced in example 2 is a numerical semigroup because

$$\gcd(7, 8, 16, 24, 25, 19, 27) = 1$$

and

$$|\bar{M}| = \left\lfloor \frac{8}{7} \right\rfloor + \left\lfloor \frac{16}{7} \right\rfloor + \left\lfloor \frac{24}{7} \right\rfloor + \left\lfloor \frac{25}{7} \right\rfloor + \left\lfloor \frac{19}{7} \right\rfloor + \left\lfloor \frac{27}{7} \right\rfloor = 14,$$

in this case we have

$$M = \{1, 2, 3, 4, 5, 6, 9, 10, 11, 12, 13, 17, 18, 20\}.$$

In the rest of this article we suppose that  $M$  is a numerical semigroup which is generated by the set  $\{a_1, a_2, \dots, a_t\}$  and  $t \leq a_1$ . For a numerical semigroup  $M$  there is a unique surjective map

$$\psi : \mathbb{N}_0^t \rightarrow M$$

where

$$\psi(n_1, n_2, \dots, n_t) = \sum_{i=1}^t n_i a_i$$

*Definition 5:* Every numerical semigroup  $M$  with the above notations introduced a  $C_A$  order as follow:

For  $\alpha, \beta \in \mathbb{N}_0^t$  we say that  $\alpha < \beta$  if  $\psi(\alpha) < \psi(\beta)$  or  $\psi(\alpha) = \psi(\beta)$  and there exists  $1 \leq i \leq t-1$  such that  $\alpha_1 = \beta_1, \alpha_2 = \beta_2, \dots, \alpha_i = \beta_i$  and  $\alpha_{i+1} > \beta_{i+1}$ .

Note that if  $K$  is a field then the  $C_A$  order defined a monomial order in the polynomial ring  $K[x_1, x_2, \dots, x_t]$ .

*Definition 6:* For  $a \in M$  we define

$$\mu(a) = \min\{\alpha \in \mathbb{N}_0^t : \alpha \in \psi^{-1}(a)\}$$

and

$$B(A) = \{\mu(a) : a \in M\},$$

$$T(A) = \{\mu(b_i) \in B(A) : 0 \leq i \leq a_1 - 1\},$$

at last we denote by  $V(A)$ , the set of all  $\gamma \in \mathbb{N}_0^t - B(A)$  such that for all  $\alpha \in \mathbb{N}_0^t - B(A)$  and  $\beta \in \mathbb{N}_0^t$ , the equality  $\gamma = \alpha + \beta$  implies that  $\beta = 0$ .

### III. MIURA $C_A$ CURVES

In this section we denote by  $K$ , a finite field with  $q$  elements. For  $m \in V(A)$ , suppose that the polynomial  $F_m \in K[x_1, x_2, \dots, x_t]$  has two following conditions:

i) for all  $m \in V(A)$ ,

$$F_m = X^m + a_l X^l + \sum_{l \neq n < m} a_n X^n$$

where  $l = \mu(\psi(m))$ ,  $a_l \neq 0$ .

ii)  $\text{Span}\{X^n : n \in B(A)\} \cap \langle F_m : m \in V(A) \rangle = \langle 0 \rangle$ .

In the above conditions  $\text{Span}\{X^n : n \in B(A)\}$  means the set of all polynomials generated by  $X^n$ 's with coefficients in  $K$  and  $\langle F_m : m \in V(A) \rangle$  is the ideal generated by  $F_m$ 's in  $K[x_1, x_2, \dots, x_t]$ .

*Definition 7:* Let  $M$  be a numerical semigroup of  $\mathbb{N}_0$  which is generated by  $A = \{a_1, a_2, \dots, a_t\}$  and let  $I$  be an ideal in  $K[x] := K[x_1, x_2, \dots, x_t]$  which is generated by some polynomials which satisfy in the above two conditions. In this case  $\text{spec}(\frac{K[x]}{I})$  is called a Miura curve or a  $C_A$  curve over the field of fractions  $R = \frac{K[x]}{I}$ .

Using Arita algorithm we can compute the addition of two points on a  $C_A$  curve, in Appendix A we give an another implementation of this algorithm on Maple 11.

### IV. CONCLUSION

By the implementation presented in Appendix A we can compute the addition of two distinct point on a  $C_A$  curve or compute the  $n^{it}$  power of a point on the curve.

### ACKNOWLEDGMENT

The authors would like to thank Damghan university of Basic Science for support this research.

### REFERENCES

- [1] F. K. Abu Salem, K. Khuri Makdasi, Fast Jacobian group operations for  $C_{3,4}$  curves over a large finite field, LMS Journal of Computation and Mathematics 10 (2007), 307-328.
- [2] S. Arita. Algorithms for computations in Jacobian group of  $C_{ab}$  curve and their application to discrete-log based public key cryptosystems. *IEICE Transactions*, J82-A(8):1291–1299, 1999. In Japanese. English translation in the proceedings of the Conference on The Mathematics of Public Key Cryptography, Toronto 1999.
- [3] S. Arita, S. Miura, and T. Sekiguchi. An addition algorithm on the jacobian varieties of curves. *Journal of the Ramanujan Mathematical Society*, 19(4):235–251, December 2004.
- [4] A. Basiri, A. Enge, J.-C. Faugère, and N. Gürel. Implementing the arithmetic of  $c_{3,4}$  curves. In *Lecture Notes in Computer Science, Proceedings of ANTS*, pages 87–101. Springer-Verlag, June 2004.
- [5] A. Basiri, A. Enge, J.-C. Faugère, and N. Gürel. The arithmetic of jacobian groups of superelliptic cubics. *Math. Comp.*, 74:389–410, 2005.
- [6] S.-D. Galbraith, S. Paulus, and N.-P. Smart. Arithmetic on superelliptic curves. *Mathematics of Computation*, 71(237):393–405, 2002.
- [7] R. Harasawa and J. Suzuki. Fast Jacobian group arithmetic on  $C_{ab}$  curves. In W. Bosma, editor, *Algorithmic Number Theory — ANTS-IV*, volume 1838 of *Lecture Notes in Computer Science*, pages 359–376, Berlin, 2000. Springer-Verlag.

## APPENDIX A

## IMPLEMENTATION OF THE ALGORITHM IN MAPLE 11

```

> with(Ore_algebra):
> with(PolynomialIdeals):
> with(Groebner):
> Initial:=proc(n1,p1)
> global p,nn,Tlex,C_A,A:
> local Jabr,i,xInput;
> nn:=n1;p:=p1;
> Jabr:=poly_algebra(t,seq(x[i],i=1..nn),characteristic=p):
> for i from 1 to nn do
> xInput:=scanf("%d",a);
> A[i]:=xInput[1];
> end do;
> Tlex:=MonomialOrder(Jabr,'matrix'([[1,seq(0,i=1..nn)],
seq([seq(0,j=1..nn-i),1,seq(0,j=0..i-1)],i=0..
nn-1)], [t,seq(x[i],i=1..nn)])):
> C_A:=MonomialOrder(Jabr,'matrix'([[1,seq(0,i=1..nn)],
seq([0,seq(0,j=1..i),seq(A[j],j=i+1..nn)],i=0..
nn-1)], [t,seq(x[i],i=1..nn)])):
> end:
> #[J:g]
> xQuotient:=proc(J,g,TT)
> local h,G,res,i:
> G:=Basis(expand([seq(t*h,h=J),(1-t)*g]),TT):
> res:=[]:
> for i from 1 to nops(G) do
> if (not member(t,indets(LeadingMonomial(G[i],TT))))
then
> res:=[op(res),Normal(G[i]/g) mod p]:
> fi:
> end do:
> return res:
> end:
> #I1 Intersect I2
> IntersectId:=proc(I1,I2,TT)
> local i,G,res:
> G:=Basis(expand([seq(t*i,i=I1),seq((1-t)*i,i=I2)]),TT):
> res:=[]:
> for i from 1 to nops(G) do
> if (not member(t,indets(LeadingMonomial(G[i],TT))))
then
> res:=[op(res),G[i]]:
> fi:
> end do:
> return res:
> end:
> #[J:K]
> QuotientId:=proc(J,K,TT)
> local i,G:
> G:=xQuotient(J,K[1],TT):
> for i from 2 to nops(K) do
> G:=IntersectId(G,xQuotient(J,K[i],TT),TT):
> end do:
> return G:
> end:
> #J1*J2
> ProductId:=proc(J1,J2,TT)
> local i,j:
> Basis([op(F),seq(seq(modp(expand(J1[i]*J2[j]),p),j=1..nops(J2)),i=1..nops(J1))],TT):
> end:

```

```

> #Arita's Algorithm
> AritaAlg:=proc(J12,Tlex,C_A)
> local J,fff,J3,J4,J5,h,i3:
> fff:=J12[1]:# step 2 of algorithm
> J3:=QuotientId([fff,op(F)],J12,C_A):#step
3
> J3:=Basis(J3,C_A):#step 3
> h:=modp(expand(op(1,J3)/lcoeff(op(1,J3))),p):#step
3
> # if modp(h-(coeff(h,y,3)*F),p)=0
then h:=J3[2] fi:
> i3:=1:
> while NormalForm(h,[op(F)],C_A)=0
and i3 < nops(J3) do
> i3:=i3+1:
> h:=J3[i3]:
> end do:
> if nops(J3)<i3 then print("Error"):
fi:
> J4:=Basis([op(F),seq(h*J12[i],i=1..nops(J12))],C_A):
> J5:=xQuotient(J4,fff,C_A):
> end:
> SumId:=proc(I1,I2)
> local Multi,Ans;
> Multi:=ProductId(I1,I2,C_A);
> Ans:=AritaAlg(Multi,Tlex,C_A);
> return Ans:
> end:
> Powern:=proc(n,II)
> local r,e,i,J12;
> r:=[1];
> e:=II;
> i:=n;
> while(i>0) do
> if(i mod 2)=1 then
> J12:=ProductId(r,e,C_A);r:=AritaAlg(J12,Tlex,C_A):
> print(r);
> i:=((i-1)/2);
> else
> i:=(i/2);
> fi;
> if(i>0) then
> J12:=ProductId(e,e,C_A);
e:=AritaAlg(J12,Tlex,C_A);
> print(e);
> fi;
> end do;
> return r;
> end:

```