Bol. Soc. Paran. Mat.
©SPM –ISSN-2175-1188 on line
SPM: www.spm.uem.br/bspm

(3s.) **v. 2022 (40)** : 1–6.
ISSN-0037-8712 in press
doi:10.5269/bspm.52539

The Binary Operations Calculus in $H^2_{a,d}$ *

Abdelâli Grini[1], Abdelhakim Chillali[2], Hakima Mouanis[3]

ABSTRACT: Let $\mathbb{F}_q$ be a finite field of q elements, where q is a power of a prime number p greater than or equal to 5, such that -3 is not a square in $\mathbb{F}_p$. In this paper, we will study the twisted Hessian curve over the ring $R_2 = \mathbb{F}_q[\epsilon]$, with the relation $\epsilon^2 = 0$. More precisely, we will give many various explicit formulas, which describe the binary operations calculus in $H^2_{a,d}$, where $H^2_{a,d}$ is the twisted Hessian curve over R_2, and we will reduce the cost of the complexity of the calculus in $H^2_{a,d}$.

Key Words: Finite field, Finite ring, Local ring, Twisted Hessian curve.

Contents

1. Introduction

In [1], the authors studied the twisted Hessian curves over a field. In this paper, we study the twisted Hessian curve defined over the ring $\mathbb{F}_q[X]/(X^2)$, [4,5]. More precisely, we will reduce the cost of the complexity of the calculus in $H^2_{a,d}$ by giving many various explicit formulas, which describe the binary operations calculus in $H^2_{a,d}$.
Let q be a power of a prime number p greater than or equal to 5. Consider the quotient ring $R_2 = \mathbb{F}_q[X]/(X^2)$, where $\mathbb{F}_q$ is the finite field of characteristic p and q elements. Then, the ring R_2 can be identified to the ring $\mathbb{F}_q[\epsilon]$, where $\epsilon^2 = 0$. In other words,

$$R_2 = \{a + b\epsilon / a, b \in \mathbb{F}_q\}.$$

We define a twisted Hessian curve over the ring R_2, as a curve in the projective space $P_2(R_2)$, which is given by the equation:

$$aX^3 + Y^3 + Z^3 = dXYZ,$$

where $a, d \in R_2$ and $a(27a - d^3)$ is invertible in R_2.
We denote the twisted Hessian curve over the ring R_2 by $H^2_{a,d}$. So we have:

$$H^2_{a,d} = \{[X : Y : Z] \in P_2(R_2) \backslash aX^3 + Y^3 + Z^3 = dXYZ\}.$$

We denote by π the canonical projection defined by

$$R_2 \mapsto \mathbb{F}_q$$

$$a + b\epsilon \mapsto a$$

Theorem 1.1. *Let $P = [X_1 : Y_1 : Z_1]$ and $Q = [X_2 : Y_2 : Z_2]$ two points in $H^2_{a,d}$.*

* Sidi Mohamed Ben Abdellah University, Morocco
2010 *Mathematics Subject Classification:* 11T71, 14G50, 94A60.
Submitted March 04, 2020. Published July 04, 2020

1. *Define:*

$$X_3 = X_1^2 Y_2 Z_2 - X_2^2 Y_1 Z_1,$$
$$Y_3 = Z_1^2 X_2 Y_2 - Z_2^2 X_1 Y_1,$$
$$Z_3 = Y_1^2 X_2 Z_2 - Y_2^2 X_1 Z_1.$$

If $(\pi(X_3), \pi(Y_3), \pi(Z_3)) \neq (0,0,0)$ *then* $P + Q = [X_3 : Y_3 : Z_3]$.

2. *Define:*

$$X_3' = Z_2^2 X_1 Z_1 - Y_1^2 X_2 Y_2,$$
$$Y_3' = Y_2^2 Y_1 Z_1 - a X_1^2 X_2 Z_2,$$
$$Z_3' = a X_2^2 X_1 Y_1 - Z_1^2 Y_2 Z_2.$$

If $(\pi(X_3'), \pi(Y_3'), \pi(Z_3')) \neq (0,0,0)$ *then* $P + Q = [X_3' : Y_3' : Z_3']$.

Proof. By using [1, Theorem 3.2 and Theorem 4.2], we prove the theorem.

Recall that R_2 is a local ring and its maximal ideal is $M = \epsilon\mathbb{F}_q$, see [6,7]. We have the following proposition.

Proposition 1.2. *Every element in* $H^2_{a,d}$ *is of the form* $[1 : Y : Z]$ *(where* Y *or* $Z \in R_2 \setminus M$*), or* $[X : Y : 1]$ *(where* $X \in M$*) and we write:*
$H^2_{a,d} = \{[1 : Y : Z] \in P_2(R_2) \backslash a + Y^3 + Z^3 = dYZ,$ *and* Y *or* $Z \in R_2 \setminus M\} \cup \{[x\epsilon : -1 - \frac{1}{3}d_0 x\epsilon : 1] \backslash x \in \mathbb{F}_q\}$.

Proof. Let $[X : Y : Z] \in H^2_{a,d}$, where X, Y and $Z \in R_2$.

- If X is invertible, then $[X : Y : Z] = [1 : X^{-1}Y : X^{-1}Z] \sim [1 : Y : Z]$. Suppose that Y and $Z \in M$; since $a + Y^3 + Z^3 = dYZ$ then $a \in M$, which is absurd.

- If X is non invertible, then $X \in M$, so $X = x\epsilon$, where $x \in \mathbb{F}_q$. Let $Y = y_0 + y_1\epsilon$, $Z = z_0 + z_1\epsilon$, $d = d_0 + d_1\epsilon$ and $a = a_0 + a_1\epsilon$.
  So, $[X : Y : Z] = [x\epsilon, y_0 + y_1\epsilon, z_0 + z_1\epsilon] \in H^2_{a,d}$. Then $y_0^3 + 3y_0^2 y_1\epsilon + z_0^3 + 3z_0^2 z_1\epsilon = d_0 y_0 z_0 x\epsilon$ implies that $y_0 = -1$ and $z_0 = 1$ (see 1, Theorem 2.2) and $y_1 + z_1 = \frac{-1}{3}d_0 x$, therefore

$$[X : Y : Z] = [x\epsilon, -1 + y_1\epsilon, 1 + z_1\epsilon]$$
$$= [x\epsilon, (-1 + y_1\epsilon)(1 - z_1\epsilon), 1]$$
$$= [x\epsilon, -1 + (y_1 + z_1)\epsilon, 1].$$
$$= [x\epsilon, -1 - \tfrac{1}{3}d_0 x\epsilon, 1].$$

2. Main results

2.1. Maple Procedures

The following Maple procedure will help us to calculate, expressively the sum of two points in the twisted Hessian curve over the ring R_2:

```
> sum1 := proc(P, Q)
localX, Y, Z;
X := expand(P[1]^2 * Q[2] * Q[3] - Q[1]^2 * P[2] * P[3]);
Y := expand(P[3]^2 * Q[1] * Q[2] - Q[3]^2 * P[1] * P[2]);
Z := expand(P[2]^2 * Q[1] * Q[3] - Q[2]^2 * P[1] * P[3]);
[X, Y, Z];
end :
> sum2 := proc(P, Q)
localX, Y, Z;
X := expand(Q[3]^2 * P[1] * P[3] - P[2]^2 * Q[1] * Q[2]);
Y := expand(Q[2]^2 * P[2] * P[3] - (a + b * ϵ) * P[1]^2 * Q[1] * Q[3]);
```

$Z := expand((a + b * \epsilon) * Q[1]^2 * P[1] * P[2] - P[3]^2 * Q[2] * Q[3]);$
$[X, Y, Z];$
$end :$

2.2. Binary operations

Lemma 2.1. *Let* $P = [x_1\epsilon : -1 - \frac{1}{3}d_0x_1\epsilon : 1]$ *and* $Q = [x_2\epsilon : -1 + \frac{1}{3}d_0x_2\epsilon : 1]$ *two points in* $H^2_{a,d}$*. Then:*

$$P + Q = [(x_1 + x_2)\epsilon : -1 - \frac{1}{3}(x_1 + x_2)d_0\epsilon : 1].$$

Proof. As $[\pi(x_1\epsilon) : \pi(-1 - \frac{1}{3}d_0x_1\epsilon) : \pi(1)] = [\pi(x_2\epsilon) : \pi(-1 - \frac{1}{3}d_0x_2\epsilon) : \pi(1)]$, then applying the second case of theorem 1.1; we find the result by using maple procedure "sum2".

Lemma 2.2. *Let* $P = [1 : y_0 + y_1\epsilon : z_0 + z_1\epsilon]$ *and* $Q = [x\epsilon : -1 - \frac{1}{3}d_0x\epsilon : 1]$ *two points in* $H^2_{a,d}$*. Then:*

$$P + Q = [1 : (-\frac{y_0d_0x}{3} + y_1 + xz_0^2)\epsilon + y_0 : (-xy_0^2 + z_1 + \frac{xd_0z_0}{3})\epsilon + z_0].$$

Proof. As $[\pi(1) : \pi(y_0 + y_1\epsilon) : \pi(z_0 + z_1\epsilon)] \neq [\pi(x\epsilon) : \pi(-1 - \frac{1}{3}d_0x\epsilon) : \pi(1)]$, then applying the first case of theorem 1.1; we find the result by using maple procedure sum1.

Lemma 2.3. *Let* $P = [1 : y_0 + y_1\epsilon : z_1\epsilon]$ *and* $Q = [1 : y_0 + t_1\epsilon : s_1\epsilon]$ *two points in* $H^2_{a,d}$*. Then:*

$$P + Q = [1 : (-z_1 + \frac{s_1a_0}{y_0^3})\epsilon : (\frac{a_0y_1 - a_1y_0 + a_0t_1}{y_0^3})\epsilon - \frac{a_0}{y_0^2}].$$

Proof. As $[\pi(1) : \pi(y_0 + y_1\epsilon) : \pi(z_1\epsilon)] = [\pi(1) : \pi(y_0 + t_1\epsilon) : \pi(s_1\epsilon)]$, then applying the second case of theorem 1.1; we find the result by using maple procedure "sum2".

Lemma 2.4. *Let* $P = [1 : y_0 + y_1\epsilon : z_0 + z_1\epsilon]$ *and* $Q = [1 : y_0 + t_1\epsilon : -z_0 + s_1\epsilon]$ *two points in* $H^2_{a,d}$ *where* $z_0 \neq 0$*. Then:*

$$P + Q = [1 : (\frac{z_0(y_1 - t_1)}{2y_0} - s_1 - z_1)\epsilon : \frac{y_1 + t_1}{2}\epsilon + y_0].$$

Proof. As $[\pi(1) : \pi(y_0 + y_1\epsilon) : \pi(z_0 + z_1\epsilon)] \neq [\pi(1) : \pi(y_0 + t_1\epsilon) : \pi(-z_0 + s_1\epsilon)]$, then applying the first case of theorem 1.1; we find the result by using maple procedure "sum1".

Lemma 2.5. *Let* $P = [1 : y_0 + y_1\epsilon : z_0 + z_1\epsilon]$ *and* $Q = [1 : y_0 + t_1\epsilon : z_0 + s_1\epsilon]$ *two points in* $H^2_{a,d}$ *where* $z_0 \neq 0$*. Then:*

$$P + Q = [X_0 + X_1\epsilon : Y_0 + Y_1\epsilon : Z_0 + Z_1\epsilon]$$

where

$$X_0 = z_0^3 - y_0^3$$

$$X_1 = z_0^2(z_1 + 2s_1) - y_0^2(t_1 + 2y_1)$$

$$Y_0 = z_0(y_0^3 - a_0)$$

$$Y_1 = y_0^2(y_0z_1 + z_0(y_1 + 2t_1)) - s_1a_0 - a_1z_0$$

$$Z_0 = y_0(a_0 - z_0^3)$$

$$Z_1 = a_0y_1 + a_1y_0 - z_0^2(y_0(s_1 + 2z_1) + z_0t_1).$$

Proof. As $[\pi(1) : \pi(y_0 + y_1\epsilon) : \pi(z_0 + z_1\epsilon)] = [\pi(1) : \pi(y_0 + t_1\epsilon) : \pi(z_0 + s_1\epsilon)]$, then applying the second case of theorem 1.1; we find the result by using maple procedure sum2.

Lemma 2.6. *Let $P = [1 : y_0 + y_1\epsilon : z_0 + z_1\epsilon]$ and $Q = [1 : t_0 + t_1\epsilon : s_0 + s_1\epsilon]$ two points in $H^2_{a,d}$ where $y_0 \neq t_0$. Then:*

$$P + Q = [X_0 + X_1\epsilon : Y_0 + Y_1\epsilon : Z_0 + Z_1\epsilon]$$

where

$$\begin{aligned} X_0 &= t_0 s_0 - y_0 z_0 \\ X_1 &= t_0 s_1 + t_1 s_0 - y_0 z_1 - z_0 y_1 \\ Y_0 &= z_0^2 t_0 - s_0^2 y_0 \\ Y_1 &= z_0(z_0 t_1 + 2 z_1 t_0) - s_0(s_0 y_1 + 2 s_1 y_0) \\ Z_0 &= y_0^2 s_0 - t_0^2 z_0 \\ Z_1 &= y_0(y_0 s_1 + 2 s_0 y_1) - t_0(t_0 z_1 + 2 t_1 z_0). \end{aligned}$$

Proof. As $[\pi(1) : \pi(y_0 + y_1\epsilon) : \pi(z_0 + z_1\epsilon)] \neq [\pi(1) : \pi(t_0 + t_1\epsilon) : \pi(s_0 + s_1\epsilon)]$, then applying the first case of theorem 1.1; we find the result by using maple procedure "sum1".
We summarize the results in the Table.1:

3. Reduction of complexity

Let s, m and i are respectively the costs of the sum, the multiplication and the inverse in the field $\mathbb{F}_q$. It is clear that : $s \leq m \leq i$. We neglect the cost of the inverse and his comparison. We have the following table:

Case	Sum cost	multiplication cost
Theorem- case1	$18 \times s$	$78 \times m$
Theorem- case2	$20 \times s$	$96 \times m$
Lemma 1	$2 \times s$	$2 \times m$
Lemma 2	$4 \times s$	$10 \times m$
Lemma 3	$3 \times s$	$7 \times m$
Lemma 4	$4 \times s$	$3 \times m$
Lemma 5	$14 \times s$	$30 \times m$
Lemma 6	$12 \times s$	$30 \times m$

Table 2: Complexity reduction of the sum law in the twisted Hessian curve $H^2_{a,d}$

The following graphics illustrate the results above:

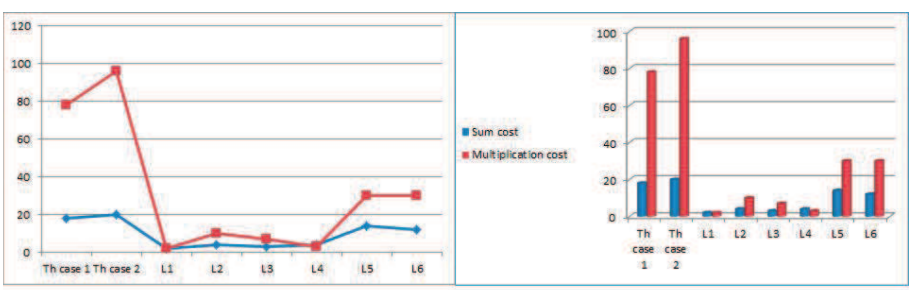

Figure 1: Complexity reduction of the sum law in the twisted Hessian curve $H^2_{a,d}$

4. Conclusion

The above results show that the cost of the sum and the multiplication in the lemmas 2.1, 2.2, 2.3, 2.4, 2.5, 2.6 are less than those in the theorem 1.1. Hence the complexity time in the lemmas is lower than the one in the theorem.
This shows the importance of these lemmas.

Acknowledgments

The author gratefully acknowledges that his research is supported by Sidi Mohamed Ben Abdellah University, Morocco. We thank the referee by your suggestions.

	P	Q	$P+Q$
1	$[x_1\epsilon : -1-\frac{1}{3}d_0x_1\epsilon : 1]$	$[x_2\epsilon : -1-\frac{1}{3}d_0x_2\epsilon : 1]$	$[(x_1+x_2)\epsilon : -1-\frac{1}{3}(x_1+x_2)d_0\epsilon : 1]$
2	$[1 : y_0+y_1\epsilon : z_0+z_1\epsilon]$	$[x\epsilon : -1-\frac{1}{3}d_0x\epsilon : 1]$	$[1 : (-\frac{y_0d_0x}{3}+y_1+xz_0^2)\epsilon+y_0 :$ $(-xy_0^2+z_1+\frac{xd_0z_0}{3})\epsilon+z_0]$
3	$[1 : y_0+y_1\epsilon : z_1\epsilon]$	$[1 : y_0+t_1\epsilon : s_1\epsilon]$	$[1 : (-z_1+\frac{s_1a_0}{y_0^3})\epsilon : (\frac{a_0y_1-a_1y_0+a_0t_1}{y_0^3})\epsilon-\frac{a_0}{y_0^2}]$
4	$[1 : y_0+y_1\epsilon : z_0+z_1\epsilon]$	$[1 : y_0+t_1\epsilon : -z_0+s_1\epsilon]$ and $z_0\neq 0$	$[1 : (\frac{z_0(y_1-t_1)}{2y_0}-s_1-z_1)\epsilon : \frac{y_1+t_1}{2}\epsilon+y_0]$
5	$[1 : y_0+y_1\epsilon : z_0+z_1\epsilon]$	$[1 : y_0+t_1\epsilon : z_0+s_1\epsilon]$ and $z_0\neq 0$	$[X_0+X_1\epsilon : Y_0+Y_1\epsilon : Z_0+Z_1\epsilon]$ where $X_0=z_0^3-y_0^3$, $Y_0=z_0(y_0^3-a_0)$, $X_1=z_0^2(z_1+2s_1)-y_0^2(t_1+2y_1)$, $Y_1=y_0^2(y_0z_1+z_0(y_1+2t_1))-s_1a_0-a_1z_0$, $Z_0=y_0(a_0-z_0^3)$, and $Z_1=a_0y_1+a_1y_0-z_0^2(y_0(s_1+2z_1)+z_0t_1)$
6	$[1 : y_0+y_1\epsilon : z_0+z_1\epsilon]$	$[1 : t_0+t_1\epsilon : s_0+s_1\epsilon]$ and $y_0\neq t_0$	$[X_0+X_1\epsilon : Y_0+Y_1\epsilon : Z_0+Z_1\epsilon]$ where $X_0=t_0s_0-y_0z_0$, $Y_0=z_0^2t_0-s_0^2y_0$, $X_1=t_0s_1+t_1s_0-y_0z_1-z_0y_1$, $Y_1=z_0(z_0t_1+2z_1t_0)-s_0(s_0y_1+2s_1y_0)$, $Z_0=y_0^2s_0-t_0^2z_0$, and $Z_1=y_0(y_0s_1+2s_0y_1)-t_0(t_0z_1+2t_1z_0)$

Table 1: The sum law in the twisted Hessian curve $H^2_{a,d}$

References

1. Daniel J. Bernstein, Chitchanok Chuengsatiansup, David Kohel, and Tanja Lange, *Twisted Hessian Curves*, In LATINCRYPT 2015, pp 269–294, (2015).http://cr.yp.to/papers.html#hessian
2. Lenstra, H.W, *Eliptic Curves and Number-Theoretic Algorithms*, Processing of the International Congress of Mathematicians, Berkely, California, USA, (1986).
3. N. Smart, *The Hessian form of an elliptic curve. Cryptographic hardware and embedded systems-CHES 2001 (Paris)*, 118-125, Lecture Notes in Computer Science, 2162, Springer, Berlin, (2001).
4. A. Boulbot, A. Chillali and A. Mouhib, *Elliptic Curves Over the Ring R*, Bol. Soc. Paran,v. 38 3, pp 193-201, (2020).
5. M. H. Hassib, A. Chillali, and M. A. Elomary,*The Binary Calculus in $E_{a,b}$*, Gulf Journal of Mathematics. Vol 8 p. 38-43, (2015).
6. M. H. Hassib, A. Chillali, M. A. Elomary, *Elliptic curves over a chain ring of characteristic 3*, Journal of Taibah University for Science, 40(9), pages 1687-1700, (2015).
7. A. Tadmori, A. Chillali, M. Ziane, *Elliptic Curve over Ring $A_4 = \mathbb{F}_2^d[\varepsilon]$, $\varepsilon^4 = 0$*, Applied Mathematical Sciences, Volume 9, Issue 33, Pages 1721-1733, (2015).

A. Grini and H. Mouanis,
Sidi Mohamed Ben Abdellah University, FSDM, Fez, Morocco
A. Chillali,
Sidi Mohamed Ben Abdellah University, FP, LSI, Taza, Morocco.
E-mail address: [1]abdelali.grini@usmba.ac.ma
E-mail address: [2]abdelhakim.chillali@usmba.ac.ma
E-mail address: [3]hmouanis@yahoo.fr