

CONSTRUCTING ELLIPTIC CURVES
WITH GIVEN WEIL PAIRING

Hugues Verdure

Department of Mathematics

Faculty of Education

Bergen University College

P.O. Box 7030, Bergen, 5020, NORWAY

e-mail: Hugues.Verdure@hib.no

Abstract: We give a parametrization of the set of isomorphism classes of triples (E, P, Q) , where E is an elliptic curve and P, Q are rational l -torsion points with given Weil pairing, when $l = 5, 7$. When the base field is finite, we also investigate the cardinality of this set.

AMS Subject Classification: 14H52, 12E05

Key Words: elliptic curve, Weil pairing

1. Introduction and Notation

Let E be an elliptic curve defined over a field \mathbb{K} . Let $l \geq 3$ be a prime number which is relatively prime to the characteristic of the field \mathbb{K} . We assume that \mathbb{K} has a primitive l -th root of unity ζ_l . We also assume that E has a rational l -torsion point. In [3], we give a method for finding a criterium that distinguishes whether or not all the l -torsion points are rational. We also make this criterium explicit in the cases $l = 3, 5$ and 7 .

In the present paper, we shall give an explicit parametrization of the set $\mathcal{W}_l(\mathbb{K})$ of isomorphism classes of triples (E, P, Q) , where E is an elliptic curve defined over \mathbb{K} , P and Q are rational l -torsion points on E such that the Weil pairing $e_l(P, Q) = \zeta_l$, in the cases $l = 5$ and $l = 7$. When \mathbb{K} is a finite field, we shall be able to give the cardinality of this set.

The paper is organized in the following way: in the next section, we shall give the general method for finding the parametrization, while we shall make everything explicit in the two next sections, which will deal with $l = 5$ and $l = 7$ respectively. The interested reader may find two *MAGMA* files (see [5, 6]) that have the parametrization.

We will freely use the results from [3]. The notation will be the one from [2].

2. The Method

We assume that $l \geq 5$. Using the Tate normal form, we can parametrize the set $Y_1(l)(\mathbb{K})$ of isomorphism classes of pairs (E, P) , where E is an elliptic curve defined over \mathbb{K} and $P \in E[l]$. The set $Y_1(l)(\mathbb{K})$ can be given as a (singular) curve

$$C_l : f(b, c) = 0,$$

where we remove a finite number of points that would correspond to curves with discriminant 0. We denote by $C_l^*(\mathbb{K})$ the curve without these points. The parametrization is then given by

$$\begin{aligned} \pi : C_l^*(\mathbb{K}) &\longrightarrow Y_1(l)(\mathbb{K}), \\ (b, c) &\longmapsto [E_{b,c}, P], \end{aligned}$$

where

$$E_{b,c} : y^2 + (1 - c)xy - by = x^3 - bx^2$$

and

$$P = (0, 0).$$

Remark 1. The equation of C_l is in fact $\psi_l(0) = 0$, where $\psi_l(x)$ is the l -th division polynomial of the curve $y^2 + (1 - c)xy - by = x^3 - bx^2$ defined over $\mathbb{K}(b, c)$. The bad points that have to be removed are those which satisfy

$$\Delta = 16b^5 - 8b^4c^2 - 20b^4c + b^4 + b^3c^4 - 3b^3c^3 + 3b^3c^2 - b^3c = 0.$$

Our criterium was a function $R_1 \in \mathbb{K}(C_l)$ never vanishing on $Y_1(l)(\mathbb{K})$ such that

$$E_{b,c}[l] \subset E_{b,c}(\mathbb{K}) \Leftrightarrow R_1(b, c) \in \mathbb{K}^{(l)}.$$

The function R_1 was found by considering the points Q such that $e_l(P, Q) = \zeta_l$. This function R_1 can be expressed as $R_1 = \frac{g}{h}$, where g, h are polynomials in two variables B, C and coefficients in \mathbb{K} .

We can define the curve

$$X_l : \begin{cases} g(B, C) - U^l h(B, C) = 0, \\ f(B, C) = 0. \end{cases}$$

It is obvious to see that we have a point on this curve if and only if the corresponding curve has full rational l -torsion. When we work on the function field $\mathbb{K}(X_l)$, the polynomial $\varphi_{l,1}$ necessarily splits. Let x_Q be one of the roots (x_Q can be expressed as a function of b, c, u), and y_Q the corresponding y -coordinate (y_Q can be expressed as a function of x_Q , and thus of b, c, u) of the point $Q = (x_Q, y_Q)$ such that $e_l(P, Q) = \zeta_l$. This gives our parametrization:

$$\phi : \begin{array}{ccc} X_l^*(\mathbb{K}) & \longrightarrow & \mathcal{W}_l(\mathbb{K}), \\ (b, c, u) & \longmapsto & [(E_{b,c}, P, Q)], \end{array}$$

where X_l^* is the curve X_l without the bad points.

Remark 2. For any point $(b, c, u) \in X_l^*(\mathbb{K})$, there are $l - 1$ other points, namely $(b, c, \zeta_l^i u)$, $1 \leq i \leq l - 1$, which correspond to the $l - 1$ other points R such that $e_l(P, R) = \zeta_l$.

3. The Case $l = 5$

3.1. Parametrization

In this case, we can replace $C_5(\mathbb{K})$ by \mathbb{K} using the bijection

$$\begin{array}{ccc} \mathbb{K} & \longrightarrow & C_5(\mathbb{K}), \\ t & \longmapsto & (t, t). \end{array}$$

The function R_1 is $R_1 = \frac{t - \alpha_5}{t - \beta_5}$ with $\alpha_5 = 8 + 5\zeta_5 + 5\zeta_5^4$ and $\beta_5 = 3 - 5\zeta_5 - 5\zeta_5^4$. This gives the curve

$$X_5 : (T - \alpha_5) - U^5(T - \beta_5) = 0.$$

Here, the bad points correspond to $t = \alpha_5$, $t = \beta_5$ and $t = 0$. Working with *MAGMA*, we find that

$$x_Q = \frac{n_x}{d_x} \quad \text{and} \quad y_Q = \frac{n_y}{d_y}$$

with

$$\begin{aligned} n_x &= (-3\zeta_5^3 - 3\zeta_5^2 - 5)u^4 - (2\zeta_5^3 + \zeta_5^2 + \zeta_5 + 2)u^3 - \zeta_5^3 u^2 \\ &\quad + (\zeta_5^3 + 2\zeta_5^2 + \zeta_5)u - 3\zeta_5^2 - 5\zeta_5 - 3 \\ d_x &= u^4 + (2\zeta_5^3 + \zeta_5^2 + \zeta_5 + 2)u^3 + (2\zeta_5^3 + 2\zeta_5 + 2)u^2 + (\zeta_5^3 - \zeta_5^2 + \zeta_5)u + \zeta_5 \\ n_y &= -(13\zeta_5^3 + 13\zeta_5^2 + 21)u^7 - (11\zeta_5^3 + \zeta_5^2 + 6\zeta_5 + 8)u^6 - (5\zeta_5^3 + 4\zeta_5 + 3)u^5 \end{aligned}$$

$$\begin{aligned}
 & -(2\zeta_5^3 - \zeta_5^2 + \zeta_5 - 2)u^4 + (3\zeta_5^3 + 6\zeta_5^2 + 4\zeta_5 + 2)u^3 \\
 & + (\zeta_5^3 - 6\zeta_5^2 - 11\zeta_5 - 7)u^2 - (11\zeta_5^3 + 8\zeta_5^2 - 5\zeta_5 - 10)u \\
 & + (13\zeta_5^3 + 21\zeta_5^2 + 13\zeta_5), \\
 d_y = & u^7 + (3\zeta_5^3 + \zeta_5^2 + 2\zeta_5 + 2)u^6 + (\zeta_5^3 - 2\zeta_5^2 + 3\zeta_5 - 1)u^5 \\
 & - (4\zeta_5^3 + 3\zeta_5^2 + 2\zeta_5 + 6)u^4 - (4\zeta_5^3 - 2\zeta_5^2 + 2\zeta_5 + 1)u^3 \\
 & + (\zeta_5^3 + 2\zeta_5^2 - 2\zeta_5 + 3)u^2 + (3\zeta_5^3 + \zeta_5^2 + \zeta_5 + 2)u - \zeta_5^2.
 \end{aligned}$$

The interested reader may find these quantities in the *MAGMA* file [5].

3.2. A Brief Study of the Curve X_5

The projective closure $\overline{X_5}$ of X_5 is given by the equation

$$\overline{X_5} : (T - \alpha_5 V)V^5 - U^5(T - \beta_5 V)$$

in $\mathbb{P}^2(\mathbb{K})$. This is a curve of degree 6 with a unique ordinary singularity of order $m_\infty = 5$ at the point $S_\infty = [1 : 0 : 0]$. The genus of $\overline{X_5}$ is thus

$$g = \binom{d-1}{2} - \binom{m_\infty}{2} = 0.$$

Since it has a rational point, it is birationally equivalent to $\mathbb{P}^1(\mathbb{K})$.

Remark 3. It is possible to define a nonsingular model $\widetilde{X_5}$ in $\mathbb{P}^4(\mathbb{K})$ for $\overline{X_5}$. It is given by

$$\widetilde{X_5} : \begin{cases} \alpha_5 Z_2 Z_4^4 - \beta_5 Z_3 Z_5^4 - Z_4^5 - Z_5^5 = 0 \\ \beta_5 Z_1^3 Z_3 - Z_1^3 Z_5 - \alpha_5 Z_2^2 Z_3^2 + Z_2^2 Z_3 Z_5 = 0 \\ -\beta_5 Z_1 Z_3 Z_5^2 + Z_1 Z_5^3 + \alpha_5 Z_2^2 Z_4^2 - Z_2 Z_4^3 = 0 \\ -\beta_5 Z_1^2 Z_3 + Z_1^2 Z_5 + \alpha_5 Z_2^3 - Z_2^2 Z_4 = 0 \\ Z_1 Z_2 - Z_3^2 = 0 \\ Z_1 Z_4 - Z_3 Z_5 = 0 \\ Z_2 Z_5 - Z_3 Z_4 = 0 \end{cases}$$

The bijection between the regular points of $\overline{X_5}$ and the points of $\widetilde{X_5}$ with Z_1, Z_2, Z_3 not all equal to 0 is given by

$$[T : U : V] \longmapsto [U^2 : V^2 : UV : TV : TU].$$

3.3. Cardinality of $\mathcal{W}_5(\mathbb{F}_q)$

From the equation of X_5 , we see that the curve can be parametrized by the variable U , and this gives us the cardinality of $\mathcal{W}_5(\mathbb{F}_q)$ in a straightforward way. We just have to remove from \mathbb{F}_q the values of u that lead to bad points. Those

are:

- $u = 0$ (leads to $t = \alpha_5$),
- $u = \zeta_5^i, 1 \leq i \leq 5$,
- $u = \zeta_5^i(1 + \zeta_5 - \zeta_5^3), 1 \leq i \leq 5$ (leads to $t = 0$),

that is 11 points. We get then the following proposition:

Proposition 1. *Let \mathbb{F}_q be a finite field with q elements, with $q \equiv 1 \pmod{5}$. Then*

$$\#\mathcal{W}_5(\mathbb{F}_q) = q - 11.$$

4. The Case $l = 7$

4.1. Parametrization

In this case, we can replace $C_7(\mathbb{K})$ by \mathbb{K} using the bijection

$$\begin{aligned} \mathbb{K} &\longrightarrow C_7(\mathbb{K}), \\ t &\longmapsto (t^3 - t^2, t^2 - t). \end{aligned}$$

The function R_1 is $R_1 = \frac{(t-\alpha_7)(t-\beta_7)^2}{(t-\gamma_7)^3}$ with $\alpha_7 = 1 - 2\zeta_7 - 3\zeta_7^2 - 3\zeta_7^5 - 2\zeta_7^6$, $\beta_7 = 1 - 2\zeta_7^2 - 3\zeta_7^3 - 3\zeta_7^4 - 2\zeta_7^5$ and $\gamma_7 = 1 - 3\zeta_7 - 2\zeta_7^3 - 2\zeta_7^4 - 3\zeta_7^6$. This gives the curve

$$X_7 : (T - \alpha_7)(T - \beta_7)^2 - U^7(T - \gamma_7)^3 = 0.$$

Here, the bad points correspond to $t = \alpha_7, t = \beta_7, t = \gamma_7, t = 0$ and $t = 1$. Working with MAGMA, we find that

$$x_Q = \frac{n_x}{d_x} \quad \text{and} \quad y_Q = \frac{n_y}{7d_y}.$$

The interested reader may find the quantities n_x, d_x, n_y and n_y in [4], as well as in the MAGMA file [6].

4.2. A Brief Study of the Curve X_7

The projective closure $\overline{X_7}$ of X_7 is given by

$$\overline{X_7} : (T - \alpha_7V)(T - \beta_7V)^2V^7 - U^7(T - \gamma_7V)^3.$$

This is a curve of degree 10 with 3 singular points which are all rational:

- the point $S_{\infty_1} = [1 : 0 : 0]$, is ordinary, of multiplicity $m_{\infty_1} = 7$. When we blow it up, we get 7 rational points lying above it,

— the point $S_{\infty_2} = [0 : 1 : 0]$ is not ordinary, of multiplicity $m_{\infty_2,0} = 3$. We need to blow it up 3 times in order to resolve the singularity. In doing so, we get 1 point over it on every blowing-up, which are respectively of multiplicity $m_{\infty_2,1} = m_{\infty_2,2} = 3$ and $m_{\infty_2,3} = 1$. Note that all the blown-up points are rational,

— the point $S_1 = [\beta_7 : 0 : 1]$ is not ordinary, of multiplicity $m_{1,0} = 2$. We need to blow it up 3 times in order to resolve the singularity. In doing so, we get 1 point over it on every blowing-up, which are respectively of multiplicity $m_{1,1} = m_{1,2} = 2$ and $m_{1,3} = 1$. Note that all the blown-up points are rational.

The genus of $\overline{X_7}$ is thus

$$g = \binom{10-1}{2} - \binom{m_{\infty_1}}{2} - \sum_{i=0}^3 \binom{m_{1,i}}{2} - \sum_{i=0}^3 \binom{m_{\infty_2,i}}{2} = 3.$$

4.3. Cardinality of $\mathcal{F}_7(\mathbb{F}_q)$

If $\widetilde{X_7}$ is a nonsingular model of $\overline{X_7}$, then we know that $\widetilde{X_7}$ is also of genus 3. If $\mathbb{K} = \mathbb{F}_q$ is a finite field with q elements, then Weil’s theorem implies that

$$\left| \#\widetilde{X_7}(\mathbb{F}_q) - (q + 1) \right| \leq 2g\sqrt{q} = 6\sqrt{q}.$$

Now, we know that

$$\#\widetilde{X_7} - \#\overline{X_7}(\mathbb{F}_q)$$

is given by the number of \mathbb{F}_q -rational of $\widetilde{X_7}$ points lying over the singular points of $\overline{X_7}$ minus the number of rational singularities of $\overline{X_7}(\mathbb{F}_q)$. In our case, we have 7 rational points lying above S_{∞_1} , 1 over S_{∞_2} and 1 over S_1 . Thus,

$$\#\widetilde{X_7} - \#\overline{X_7}(\mathbb{F}_q) = 9 - 3 = 6.$$

We also know that

$$\#\overline{X_7}(\mathbb{F}_q) - \#X_7(\mathbb{F}_q) = 2$$

which is the number of added rational points added in the projective closure.

Finally,

$$\#X_7(\mathbb{F}_q) - \#\mathcal{W}_7(\mathbb{F}_q)$$

is given by the number of rational bad points on $X_7(\mathbb{F}_q)$. Those are:

- the point $(\alpha_7, 0)$,
- the point $(\beta_7, 0)$,
- the points $(0, (1 - \zeta_7^2 + \zeta_7)\zeta_7^i)$, $0 \leq i \leq 6$,

— and the points $(1, (1 + \zeta_7 + \zeta_7^2 - \zeta_7^4 - \zeta_7^5)\zeta_7^i)$, $0 \leq i \leq 6$,
and thus

$$\#X_7(\mathbb{F}_q) - \#\mathcal{W}_7(\mathbb{F}_q) = 16.$$

We get therefore the following proposition.

Proposition 2. *Let \mathbb{F}_q be a finite field with q elements, with $q \equiv 1 \pmod{7}$. Then*

$$|\#\mathcal{W}_7(\mathbb{F}_q) - (q - 23)| \leq 6\sqrt{q}.$$

Remark 4. This is the best possible bound, since there is equality up and down for $\mathbb{F}_q = \mathbb{F}_{13^2}$ and $\mathbb{F}_q = \mathbb{F}_{13^4}$.

Remark 5. Using the zeta function of the curve X_7 , we can even find the following result for finite fields of characteristic 2 and 3:

$$\#\mathcal{W}_7(\mathbb{F}_{729^n}) = 729^n - 23 - 6(-27)^n$$

and

$$\#\mathcal{W}_7(\mathbb{F}_{8^n}) = 8^n - 23 - 3(\alpha_1^{-n} + \alpha_2^{-n})$$

where $\alpha_1, \alpha_2 \in \mathbb{C}$ are the roots of the polynomial $8T^2 + 5T + 1$.

Acknowledgments

This work was partially supported by Grant-in-Aid for Scientific Research (B)18 340005, Japan Society for the Promotion of Science.

This work was done while visiting Institute of Mathematics and Statistics, University of Tromsø, Norway.

References

- [1] R. Hartshorne, *Algebraic Geometry*, Graduate Texts in Mathematics, **52**, Springer-Verlag (1977).
- [2] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Graduate Texts in Mathematics, **106**, Springer-Verlag (1986).
- [3] H. Verdure, Lagrange resolvents and torsion of elliptic curves, *Int. J. Pure Appl. Math.*, **33**, No. 1 (2006), 75-92.
- [4] H. Verdure, Constructing elliptic curves with given Weil pairing, <http://hdl.handle.net/10049/153>
- [5] File `verif5.magma`, Available at <http://hdl.handle.net/10049/153>
- [6] File `verif7.magma`, Available at <http://hdl.handle.net/10049/153>