CONSTRUCTING ELLIPTIC CURVES WITH GIVEN WEIL PAIRING

HUGUES VERDURE

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.

1. Introduction and notation

Let E be an elliptic curve defined over a field $\mathbb{K}$. Let $l \geqslant 3$ 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 ([5, 6]) that have the parametrization.

We will freely use the results from [3]. The notation will be the one from [2]. This is the detailed version of the article [4].

2. The method

We assume that $l \geqslant 5$. 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

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

2000 *Mathematics Subject Classification.* Primary 14H52, Secondary 12E05.

Key words and phrases. Elliptic Curve, Weil pairing.

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

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

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

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

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 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:

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

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 $(b,c,\zeta_l^i u)$, $1 \leqslant i \leqslant l-1$, 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

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

with

$$\begin{array}{rcl} n_x & = & (-3\zeta_5^3 - 3\zeta_5^2 - 5)u^4 - (2\zeta_5^3 + \zeta_5^2 + \zeta_5 + 2)u^3 - \zeta_5^3 u^2 \\ & & +(\zeta_5^3 + 2\zeta_5^2 + \zeta_5)u - 3\zeta_5^2 - 5\zeta_5 - 3 \\ d_x & = & u^4 + (2\zeta_5^3 + \zeta_5^2 + \zeta_5 + 2)u^3 + (2\zeta_5^3 + 2\zeta_5 + 2)u^2 + (\zeta_5^3 - \zeta_5^2 + \zeta_5)u + \zeta_5 \\ n_y & = & -(13\zeta_5^3 + 13\zeta_5^2 + 21)u^7 - (11\zeta_5^3 + \zeta_5^2 + 6\zeta_5 + 8)u^6 - (5\zeta_5^3 + 4\zeta_5 + 3)u^5 \\ & & -(2\zeta_5^3 - \zeta_5^2 + \zeta_5 - 2)u^4 + (3\zeta_5^3 + 6\zeta_5^2 + 4\zeta_5 + 2)u^3 \\ & & +(\zeta_5^3 - 6\zeta_5^2 - 11\zeta_5 - 7)u^2 - (11\zeta_5^3 + 8\zeta_5^2 - 5\zeta_5 - 10)u \\ & & +(13\zeta_5^3 + 21\zeta_5^2 + 13\zeta_5) \\ d_y & = & u^7 + (3\zeta_5^3 + \zeta_5^2 + 2\zeta_5 + 2)u^6 + (\zeta_5^3 - 2\zeta_5^2 + 3\zeta_5 - 1)u^5 \\ & & -(4\zeta_5^3 + 3\zeta_5^2 + 2\zeta_5 + 6)u^4 - (4\zeta_5^3 - 2\zeta_5^2 + 2\zeta_5 + 1)u^3 \\ & & +(\zeta_5^3 + 2\zeta_5^2 - 2\zeta_5 + 3)u^2 + (3\zeta_5^3 + \zeta_5^2 + \zeta_5 + 2)u - \zeta_5^2 \end{array}$$

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 birationnaly 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*

$$\widetilde{X_5} : \begin{cases} \alpha_5 Z_2 Z_4^4 - \beta_5 Z_3 Z_5^4 - Z4^5 - Z_5^5 = 0 \\ \beta_5 Z_1^3 Z_3 - Z_1^3 Z_5 - \alpha_5 Z_2^2 Z_3^2 + Z_2^2 Z_3 Z_5 = 0 \\ -\beta_5 Z_1 Z_3 Z_5^2 + Z_1 Z_5^3 + \alpha_5 Z_2^2 Z_4^2 - Z_2 Z_4^3 = 0 \\ -\beta_5 Z_1^2 Z_3 + Z_1^2 Z_5 + \alpha_5 Z_2^3 - Z_2^2 Z_4 = 0 \\ Z_1 Z_2 - Z3^2 = 0 \\ Z_1 Z_4 - Z_3 Z_5 = 0 \\ Z_2 Z_5 - Z_3 Z_4 = 0 \end{cases}$$

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

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

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 straithforward 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 $t = \alpha_5$),
- $u = \zeta_5^i$, $1 \leqslant i \leqslant 5$,
- $u = \zeta_5^i(1 + \zeta_5 - \zeta_5^3)$, $1 \leqslant i \leqslant 5$ (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 $q \equiv 1 \ (mod\, 5)$. 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

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

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

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

with

$$
\begin{aligned}
n_x &= (28\zeta_7^5+6\zeta_7^4+18\zeta_7^3+18\zeta_7^2+6\zeta_7+28)t^2u^9\\
&+(13\zeta_7^5+13\zeta_7^4+21\zeta_7^2-3\zeta_7+21)t^2u^8\\
&-(6\zeta_7^5-9\zeta_7^4+14\zeta_7^3-9\zeta_7^2+6\zeta_7)t^2u^7\\
&-(31\zeta_7^5+26\zeta_7^3+11\zeta_7^2+11\zeta_7+26)t^2u^6\\
&-(12\zeta_7^5+4\zeta_7^4+4\zeta_7^3+12\zeta_7^2+10)t^2u^5\\
&-(15\zeta_7^4-11\zeta_7^3+27\zeta_7^2-11\zeta_7+15)t^2u^4\\
&+(12\zeta_7^5-12\zeta_7^4+12\zeta_7^3+\zeta_7+1)t^2u^3\\
&-(4\zeta_7^5+15\zeta_7^4+5\zeta_7^3+5\zeta_7^2+15\zeta_7+4)t^2u^2\\
&-(5\zeta_7^5+5\zeta_7^4+2\zeta_7^2+9\zeta_7+2)t^2u\\
&-(2\zeta_7^5+5\zeta_7^4+6\zeta_7^3+5\zeta_7^2+2\zeta_7)t^2\\
&-(404\zeta_7^5+80\zeta_7^4+260\zeta_7^3+260\zeta_7^2+80\zeta_7+404)tu^9\\
&-(164\zeta_7^5+164\zeta_7^4+296\zeta_7^2-74\zeta_7+296)tu^8\\
&+(77\zeta_7^5-60\zeta_7^4+109\zeta_7^3-60\zeta_7^2+77\zeta_7)tu^7\\
&+(262\zeta_7^5+208\zeta_7^3+95\zeta_7^2+95\zeta_7+208)tu^6\\
&+(47\zeta_7^5+18\zeta_7^4+18\zeta_7^3+47\zeta_7^2+52)tu^5\\
&+(22\zeta_7^4-18\zeta_7^3+34\zeta_7^2-18\zeta_7+22)tu^4\\
&-(12\zeta_7^5-19\zeta_7^4+12\zeta_7^3-6\zeta_7-6)tu^3\\
&+(9\zeta_7^5+19\zeta_7^4-5\zeta_7^3-5\zeta_7^2+19\zeta_7+9)tu^2\\
&+(23\zeta_7^5+23\zeta_7^4-10\zeta_7^2-6\zeta_7-10)tu\\
&+(15\zeta_7^5+35\zeta_7^4+44\zeta_7^3+35\zeta_7^2+15\zeta_7)t\\
&+(1474\zeta_7^5+292\zeta_7^4+948\zeta_7^3+948\zeta_7^2+292\zeta_7+1474)u^9\\
&+(600\zeta_7^5+600\zeta_7^4+1081\zeta_7^2-267\zeta_7+1081)u^8\\
&-(67\zeta_7^5-54\zeta_7^4+97\zeta_7^3-54\zeta_7^2+67\zeta_7)u^7\\
&-(206\zeta_7^5+166\zeta_7^3+74\zeta_7^2+74\zeta_7+166)u^6\\
&-(40\zeta_7^5+18\zeta_7^4+18\zeta_7^3+40\zeta_7^2+52)u^5\\
&-(8\zeta_7^4-4\zeta_7^3+6\zeta_7^2-4\zeta_7+8)u^4\\
&-(2\zeta_7^5+12\zeta_7^4+2\zeta_7^3+6\zeta_7+6)u^3\\
&-(8\zeta_7^5+14\zeta_7^4+4\zeta_7^3+4\zeta_7^2+14\zeta_7+8)u^2\\
&-(4\zeta_7^5+4\zeta_7^4+5\zeta_7^2+11\zeta_7+5)u\\
&+3\zeta_7^5+6\zeta_7^4+7\zeta_7^3+6\zeta_7^2+3\zeta_7\\
d_x &= 7u(u-\zeta_7)(u-\zeta_7^2)^2(u-\zeta_7^3)
\end{aligned}
$$

$$
\begin{aligned}
n_y \quad = \quad & (734\zeta_7^5 - 79\zeta_7^4 + 652\zeta_7^3 + 148\zeta_7^2 + 325\zeta_7 + 510)t^2u^{18} \\
& +(511\zeta_7^5 + 87\zeta_7^4 + 342\zeta_7^3 + 307\zeta_7^2 + 113\zeta_7 + 498)t^2u^{17} \\
& +(156\zeta_7^5 + 153\zeta_7^4 + 9\zeta_7^3 + 269\zeta_7^2 - 61\zeta_7 + 278)t^2u^{16} \\
& +(47\zeta_7^5 + 1022\zeta_7^4 - 777\zeta_7^3 + 1488\zeta_7^2 - 798\zeta_7 + 1058)t^2u^{15} \\
& -(735\zeta_7^5 + 38\zeta_7^4 + 561\zeta_7^3 + 290\zeta_7^2 + 252\zeta_7 + 608)t^2u^{14} \\
& -(2309\zeta_7^5 + 782\zeta_7^4 + 1243\zeta_7^3 + 1914\zeta_7^2 + 240\zeta_7 + 2584)t^2u^{13} \\
& -(1049\zeta_7^5 + 761\zeta_7^4 + 284\zeta_7^3 + 1480\zeta_7^2 - 187\zeta_7 + 1611)t^2u^{12} \\
& +(535\zeta_7^5 - 295\zeta_7^4 + 624\zeta_7^3 - 243\zeta_7^2 + 405\zeta_7 + 36)t^2u^{11} \\
& +(2108\zeta_7^5 - 403\zeta_7^4 + 1979\zeta_7^3 + 174\zeta_7^2 + 1067\zeta_7 + 1271)t^2u^{10} \\
& +(599\zeta_7^5 + 389\zeta_7^4 + 153\zeta_7^3 + 495\zeta_7^2 - 76\zeta_7 + 773)t^2u^{9} \\
& +(355\zeta_7^5 + 828\zeta_7^4 - 144\zeta_7^3 + 766\zeta_7^2 - 408\zeta_7 + 627)t^2u^{8} \\
& +(\zeta_7^5 + 645\zeta_7^4 + 124\zeta_7^3 + 661\zeta_7^2 - 226\zeta_7 + 74)t^2u^{7} \\
& -(190\zeta_7^5 - 292\zeta_7^4 - 508\zeta_7^3 - 591\zeta_7^2 - 338\zeta_7 + 13)t^2u^{6} \\
& -(421\zeta_7^5 + 219\zeta_7^4 - 186\zeta_7^3 - 500\zeta_7^2 - 646\zeta_7 - 190)t^2u^{5} \\
& -(485\zeta_7^5 + 900\zeta_7^4 + 737\zeta_7^3 + 248\zeta_7^2 - 201\zeta_7 - 189)t^2u^{4} \\
& -(218\zeta_7^5 + 664\zeta_7^4 + 900\zeta_7^3 + 824\zeta_7^2 + 494\zeta_7 + 152)t^2u^{3} \\
& +(78\zeta_7^5 + 95\zeta_7^4 - 113\zeta_7^3 - 274\zeta_7^2 - 157\zeta_7 - 22)t^2u^{2} \\
& -(10\zeta_7^5 - 61\zeta_7^4 + 10\zeta_7^3 - 177\zeta_7 - 177)t^2u \\
& -(50\zeta_7^5 + 117\zeta_7^4 + 151\zeta_7^3 + 126\zeta_7^2 + 61\zeta_7 + 5)t^2 \\
& -(10714\zeta_7^5 - 1150\zeta_7^4 + 9514\zeta_7^3 + 2162\zeta_7^2 + 4746\zeta_7 + 7442)tu^{18} \\
& -(7470\zeta_7^5 + 1262\zeta_7^4 + 4978\zeta_7^3 + 4490\zeta_7^2 + 1654\zeta_7 + 7252)tu^{17} \\
& -(2510\zeta_7^5 + 807\zeta_7^4 + 1364\zeta_7^3 + 2064\zeta_7^2 + 247\zeta_7 + 2819)tu^{16} \\
& -(2090\zeta_7^5 + 12569\zeta_7^4 - 8404\zeta_7^3 + 18912\zeta_7^2 - 9336\zeta_7 + 14243)tu^{15} \\
& +(9131\zeta_7^5 + 360\zeta_7^4 + 7032\zeta_7^3 + 3764\zeta_7^2 + 2968\zeta_7 + 7675)tu^{14} \\
& +(14417\zeta_7^5 + 4460\zeta_7^4 + 8020\zeta_7^3 + 11566\zeta_7^2 + 1588\zeta_7 + 15984)tu^{13} \\
& +(13395\zeta_7^5 + 6455\zeta_7^4 + 5633\zeta_7^3 + 14149\zeta_7^2 - 351\zeta_7 + 17223)tu^{12} \\
& -(2480\zeta_7^5 - 2223\zeta_7^4 + 3759\zeta_7^3 - 2394\zeta_7^2 + 2661\zeta_7 - 369)tu^{11} \\
& -(9262\zeta_7^5 - 2399\zeta_7^4 + 9359\zeta_7^3 - 225\zeta_7^2 + 5240\zeta_7 + 4946)tu^{10} \\
& -(3985\zeta_7^5 + 968\zeta_7^4 + 2566\zeta_7^3 + 2499\zeta_7^2 + 795\zeta_7 + 3970)tu^{9} \\
& -(478\zeta_7^5 + 1181\zeta_7^4 - 298\zeta_7^3 + 1619\zeta_7^2 - 479\zeta_7 + 1373)tu^{8} \\
& +(264\zeta_7^5 - 313\zeta_7^4 + 564\zeta_7^3 - 449\zeta_7^2 + 566\zeta_7 - 213)tu^{7} \\
& +(136\zeta_7^5 - 295\zeta_7^4 - 229\zeta_7^3 - 198\zeta_7^2 + 225\zeta_7 + 235)tu^{6} \\
& +(325\zeta_7^5 - 85\zeta_7^4 - 684\zeta_7^3 - 1017\zeta_7^2 - 923\zeta_7 - 269)tu^{5} \\
& +(797\zeta_7^5 + 1380\zeta_7^4 + 1023\zeta_7^3 + 111\zeta_7^2 - 531\zeta_7 - 424)tu^{4} \\
& +(317\zeta_7^5 + 872\zeta_7^4 + 1107\zeta_7^3 + 933\zeta_7^2 + 524\zeta_7 + 144)tu^{3}
\end{aligned}
$$

$$
\begin{aligned}
& +(125\zeta_7^5 - 185\zeta_7^4 - 431\zeta_7^3 - 631\zeta_7^2 - 820\zeta_7 - 561)tu^2 \\
& +(755\zeta_7^5 + 961\zeta_7^4 + 755\zeta_7^3 - 897\zeta_7 - 897)tu \\
& +(356\zeta_7^5 + 835\zeta_7^4 + 1077\zeta_7^3 + 899\zeta_7^2 + 435\zeta_7 + 35)t \\
& +(39084\zeta_7^5 - 4195\zeta_7^4 + 34707\zeta_7^3 + 7887\zeta_7^2 + 17313\zeta_7 + 27148)u^{18} \\
& +(27249\zeta_7^5 + 4604\zeta_7^4 + 18160\zeta_7^3 + 16378\zeta_7^2 + 6033\zeta_7 + 26456)u^{17} \\
& +(10001\zeta_7^5 - 2002\zeta_7^4 + 9626\zeta_7^3 + 676\zeta_7^2 + 5175\zeta_7 + 6018)u^{16} \\
& +(12782\zeta_7^5 + 37512\zeta_7^4 - 19830\zeta_7^3 + 58767\zeta_7^2 - 25519\zeta_7 + 47761)u^{15} \\
& -(33314\zeta_7^5 + 3699\zeta_7^4 + 23746\zeta_7^3 + 17233\zeta_7^2 + 8918\zeta_7 + 30413)u^{14} \\
& -(23117\zeta_7^5 + 9120\zeta_7^4 + 11237\zeta_7^3 + 21425\zeta_7^2 + 939\zeta_7 + 27647)u^{13} \\
& -(44383\zeta_7^5 + 14923\zeta_7^4 + 23648\zeta_7^3 + 37427\zeta_7^2 + 3886\zeta_7 + 50530)u^{12} \\
& +(1132\zeta_7^5 - 7240\zeta_7^4 + 6723\zeta_7^3 - 10095\zeta_7^2 + 6218\zeta_7 - 6392)u^{11} \\
& +(9738\zeta_7^5 - 2662\zeta_7^4 + 9983\zeta_7^3 - 386\zeta_7^2 + 5650\zeta_7 + 5114)u^{10} \\
& +(3669\zeta_7^5 + 435\zeta_7^4 + 2635\zeta_7^3 + 1877\zeta_7^2 + 1031\zeta_7 + 3367)u^9 \\
& +(270\zeta_7^5 + 493\zeta_7^4 - 144\zeta_7^3 + 719\zeta_7^2 - 238\zeta_7 + 668)u^8 \\
& -(64\zeta_7^5 - 133\zeta_7^4 + 145\zeta_7^3 - 231\zeta_7^2 + 169\zeta_7 - 125)u^7 \\
& -(109\zeta_7^5 + 92\zeta_7^4 + 131\zeta_7^3 + 37\zeta_7^2 + 139\zeta_7 - 11)u^6 \\
& -(11\zeta_7^5 + 71\zeta_7^4 + 166\zeta_7^3 + 205\zeta_7^2 + 230\zeta_7 + 136)u^5 \\
& +(160\zeta_7^5 + 165\zeta_7^4 + 122\zeta_7^3 + 52\zeta_7^2 - 109\zeta_7 - 176)u^4 \\
& +(57\zeta_7^5 + 116\zeta_7^4 + 179\zeta_7^3 + 178\zeta_7^2 + 77\zeta_7 - 14)u^3 \\
& +(50\zeta_7^5 + 97\zeta_7^4 - 11\zeta_7^3 - 103\zeta_7^2 - 32\zeta_7 + 23)u^2 \\
& +(178\zeta_7^5 + 313\zeta_7^4 + 178\zeta_7^3 - 17\zeta_7 - 17)u \\
& +(58\zeta_7^5 + 136\zeta_7^4 + 175\zeta_7^3 + 146\zeta_7^2 + 71\zeta_7 + 6) \\
d_y \quad = \quad & u^{14} - (\zeta_7^5 + 2\zeta_7^4 + 3\zeta_7^3 + 4\zeta_7^2 + 2\zeta_7 + 1)u^{13} \\
& +(4\zeta_7^5 + \zeta_7^4 - 2\zeta_7^3 - 6\zeta_7^2 - 7\zeta_7 - 3)u^{12} \\
& +(7\zeta_7^5 + 14\zeta_7^4 + 10\zeta_7^3 + 2\zeta_7^2 - 4\zeta_7 - 7)u^{11} \\
& +(10\zeta_7^5 + 21\zeta_7^4 + 31\zeta_7^3 + 25\zeta_7^2 + 15\zeta_7 + 4)u^{10} \\
& -(6\zeta_7^5 - 7\zeta_7^4 - 20\zeta_7^3 - 32\zeta_7^2 - 26\zeta_7 - 13)u^9 \\
& -(14\zeta_7^5 + 20\zeta_7^4 + 7\zeta_7^3 - 7\zeta_7^2 - 21\zeta_7 - 14)u^8 \\
& -(14\zeta_7^5 + 28\zeta_7^4 + 35\zeta_7^3 + 21\zeta_7^2 + 7\zeta_7 - 6)u^7 \\
& -(6\zeta_7^5 + 19\zeta_7^4 + 32\zeta_7^3 + 38\zeta_7^2 + 26\zeta_7 + 13)u^6 \\
& +(10\zeta_7^5 + 6\zeta_7^4 - 5\zeta_7^3 - 15\zeta_7^2 - 21\zeta_7 - 11)u^5 \\
& +(7\zeta_7^5 + 14\zeta_7^4 + 11\zeta_7^3 + 5\zeta_7^2 - 3\zeta_7 - 7)u^4 \\
& +(4\zeta_7^5 + 7\zeta_7^4 + 11\zeta_7^3 + 10\zeta_7^2 + 6\zeta_7 + 3)u^3 \\
& -(\zeta_7^5 - \zeta_7^3 - 3\zeta_7^2 - 2\zeta_7 - 1)u^2 - \zeta_7^4 u.
\end{aligned}
$$

4.2. **A brief study of the curve X_7.** The projective closure $\overline{X_7}$ of X_7 is given by

$$\overline{X_7} : (T-\alpha_7 V)(T-\beta_7 V)^2 V^7 - U^7 (T-\gamma_7 V)^3.$$

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

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

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

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

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 $(0, (1-\zeta_7^2+\zeta_7)\zeta_7^i)$, $0 \leqslant i \leqslant 6$,

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

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 $q \equiv 1$ $(mod\, 7)$. Then*

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

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 $8T^2 + 5T + 1$.

5. Acknowledgments

This work was partially supported by Grant-in-Aid for Scientific Research (B)18340005, 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*, Number 52 in Graduate texts in mathematics, Springer-Verlag, 1977.

[2] J.H. Silverman, *The arithmetic of elliptic curves.* Number 106 in Graduate texts in mathematics, Springer-Verlag, 1986.

[3] H. Verdure, *Lagrange resolvents and torsion of elliptic curves.* Int. J. Pure Appl. Math., **33** (2006), No 1, 75–92.

[4] H. Verdure, *Constructing elliptic curves with given Weil pairing.* Int. J. Pure Appl. Math., to appear.

[5] File verif5.magma.

[6] File verif7.magma.

Department of Mathematics, Faculty of Education, Bergen University College, PB 7030, 5020 Bergen, Norway
E-mail address: Hugues.Verdure@hib.no