International Journal of Pure and Applied Mathematics
Volume 33 No. 1 2006, 75-92

LAGRANGE RESOLVENTS AND TORSION OF ELLIPTIC CURVES

Hugues Verdure §
Department of Mathematics
Faculty of Education
Bergen University College
P.O. Box 7030, Bergen, 5020, NORWAY
e-mail: Hugues.Verdure@hib.no
and
Department of Mathematics and Statistics
University of Tromsø
Tromsø, 9037, NORWAY
e-mail: Hugues.Verdure@matnat.uit.no

Abstract: By studying the Lagrange resolvents of factors of the l-th division polynomials of an elliptic curve defined over a field with l-th roots of unity and having a rational l-torsion point, we find a criterion for deciding whether all the l-torsion points are rational or not. We then compute it explicitly in the case $l = 3$, 5 and 7.

AMS Subject Classification: 14H52, 12E05
Key Words: elliptic curve, rational torsion points, Lagrange resolvent

1. Introduction and Notation

The cyclicity of the group of rational points of an elliptic curve defined over a finite field plays an important role in modern cryptography [4], and for instance, Kaliski requires it in designing a one-way permutation [3]. Actually, the order of the largest cyclic subgoup is far more important than the order of the group itself. Recently, it has been shown that these two are

Received: November 9, 2006

§Correspondence address: Department of Mathematics, Faculty of Education, Bergen University College, P.O. Box 7030, Bergen, 5020, NORWAY

of approximately the same size for almost all elliptic curves [2]. It is thus natural to try to find criteria for deciding this cyclicity.

How should such criteria look like? Let l be an odd prime number and $\mathbb{K}$ any field of characteristic different from l. The Weil pairing shows that a necessary condition for an elliptic curve defined over $\mathbb{K}$ to have all its l-torsion points rational is that $\mathbb{K}$ has a primitive l-th root of unity. Thus, without loss of generality, we can assume that this is the case. In the language of modular curves, an elliptic curve over $\mathbb{K}$ together with a rational point of l-torsion gives rise to a rational point P on $X_1(l)$. We can therefore reformulate our problem in the following way: given a rational point on the curve $X_1(l)$, when does this point lift to a rational point on the modular curve $X(l)$? It is known that the extension $\mathbb{K}(X(l))$ is Galois of degree l over $\mathbb{K}(X_1(l))$ and is therefore a Kummer extension [1]. Thus there exists a function $f \in K(X_1(l))$ such that

$$K(X(l)) = K(X_1(l))(f^{1/l}).$$

If we specialize to P, we see that it admits a rational lift on $X(l)$ if and only if $f(P)$ is a l-th power in $\mathbb{K}$. We will make this function f explicit in this article.

We begin this paper by giving a brief presentation of the notation and concepts used in the sequel. In Section 2, we study Lagrange resolvents for polynomials of prime degree l over a field $\mathbb{K}$ containing a primitive l-th root of unity such that its Galois group is of order dividing l. We show that in this case, there exists a criterion for deciding whether the polynomial splits or is irreducible. In Section 3, we show that if an elliptic curve E has a rational l-torsion point over $\mathbb{K}$, then its l-th division polynomial is the product of $\frac{l-1}{2}$ linear factors and $\frac{l-1}{2}$ factors of degree l, whose Galois group is of order dividing l. Using the results from the previous part, we can determine whether all the torsion points are rational or not. Finally, in Section 4, we compute an easy criterion when $l = 3$, 5 or 7.

In this paper, $\mathbb{K}$ is a field, and $\overline{\mathbb{K}}$ a fixed algebraic closure. If n is a positive integer, $\mathbb{K}^n$ denotes the cartesian product of n copies of $\mathbb{K}$, while $\mathbb{K}^{(n)}$ is the subset of $\mathbb{K}$ which consists of n-powers of elements of $\mathbb{K}$. We refer to [5] for the theory of elliptic curves, and we will use the notation found there. In particular, if E is an elliptic curve defined by a Weierstrass equation

$$E : y^2 = a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

and if $\mathbb{L}/\mathbb{K}$ is any field extension and n is an integer, then $E(\mathbb{L})$ denotes the group of $\mathbb{L}$-rational points on the curve, $E[n]$ denotes the subgroup of

n-torsion of $E(\overline{K})$, while $E(\mathbb{L})[n] = E(\mathbb{L}) \cap E[n]$. It is known that if n is prime to the characteristic of K, then $E[n] \approx (\mathbb{Z}/n\mathbb{Z})^2$, and in the case where n is odd, the x-coordinates of the points of $E[n]$ are exactly the roots of the n-th division polynomial ψ_n, which is a separable polynomial in one variable of degree $\frac{n^2-1}{2}$. Further, we denote by $\mathbb{K}_x(E[n])$ (resp. $\mathbb{K}(E[n])$) the field extension obtained from $\mathbb{K}$ by adjoining the x-coordinates (resp. x- and y-coordinates) of the points of n-torsion.

2. Lagrange Resolvents

Let l be an odd prime number, and $\mathbb{K}$ a field of characteristic different from l. We assume that $\mathbb{K}$ contains a primitive l-th root of unity ζ_l. Let $P(X)$ be a separable polynomial of degree l over $\mathbb{K}$ with the property that its Galois group G is of order dividing l. Then G is cyclic, generated by an element σ, and P is either irreducible or splits. We would like to have an easy criterion for distinguishing these two possibilities. Let $(x_0, x_1, \cdots, x_{l-1}) \in \overline{\mathbb{K}}^l$ be the l distinct roots of P, indexed in such a way that when $\#G = l$, then $\sigma x_i = x_{i+1}$ for $i \in \{0, \cdots, l-2\}$ (for convenience, we shall write $x_{n+kl} = x_n$ for $k \in \mathbb{Z}$). Then, for $i \in \{0, \cdots, l-1\}$, we define the quantities

$$r_i = \sum_{j=0}^{l-1} \zeta_l^{ij} x_j$$

and

$$R_i = r_i^l.$$

Proposition 1. *All the R_i's are in $\mathbb{K}$.*

Proof. This is obvious when P splits. When P is irreducible, we have

$$\sigma r_i = \sum_{j=0}^{l-1} \zeta_l^{ij} \sigma x_j = \sum_{j=0}^{l-1} \zeta_l^{ij} x_{j+1} = \zeta_l^{-i} r_i$$

and therefore

$$\sigma R_i = (\sigma r_i)^l = \left(\zeta_l^{-i} r_i\right)^l = R_i. \qquad \square$$

Remark 1. Note that if P is irreducible, $i \neq 0$ and $r_i \neq 0$, then $r_i \notin \mathbb{K}$.

Choosing another primitive l-th root will just induce a permutation of the r_i's and R_i's. Namely, if ξ_l is another primitive l-th root of unity, we can write $\xi_l = \zeta_l^a$. Then we have

$$\sum_{j=0}^{l-1} \xi_l^{ij} x_j = \sum_{j=0}^{l-1} \zeta_l^{iaj} x_j = r_{ia},$$

and since a and l are relatively prime, $i \mapsto ia$ is a permutation of the set of integers modulo l.

Changing the order of the roots is more problematic. Actually, one can get something completely different in the case when P splits. But we have an extra condition on the order of the roots when P is irreducible. In this case, permuting the roots is equivalent to choosing one root, the others being given by the action of σ. Assume that the permutation is given by the root x_k. Then we have

$$\sum_{j=0}^{l-1} \zeta_l^{ij} x_{k+j} = \sigma^k r_i$$

and therefore the R_i's defined either way would be the same. In the following sections however, the roots of our polynomials will be ordered in such a way that even in the case when P splits, changing the order of the roots will not change the R_i's.

Finally, taking another generator τ of G obviously does not change anything when G is trivial. In the other case, the roots have to be reordered to satisfy the extra condition, and as we have just noticed, we can assume that the first root still is x_0. As τ is a generator of G, we have $\sigma = \tau^t$ for some integer t relatively prime to l. Then we have

$$\sum_{j=0}^{l-1} \zeta_l^{ij} \tau^j x_0 = \sum_{j'=0}^{l-1} \zeta_l^{itj'} \tau^{tj'} x_0 = \sum_{j'=0}^{l-1} \zeta_l^{itj'} \sigma^{j'} x_0 = r_{it}$$

and once again, we obtain a permutation of the r_i's.

Proposition 2. *The following assertions are equivalent:*

1. *P splits.*
2. *$\forall i \in \{0, \cdots, l-1\}$, $R_i \in \mathbb{K}^{(l)}$.*
3. *$\exists i \in \{1, \cdots, l-1\}$, $R_i \in \mathbb{K}^{(l)} \setminus \{0\}$.*

Proof. Since $\mathbb{K}$ contains all the l-th roots of unity, we have

$$R_i \in \mathbb{K}^{(l)} \Leftrightarrow r_i \in \mathbb{K}.$$

Now,

$$\begin{bmatrix} r_0 \\ r_1 \\ \vdots \\ r_{l-1} \end{bmatrix} = M \cdot \begin{bmatrix} x_0 \\ x_1 \\ \vdots \\ x_{l-1} \end{bmatrix},$$

where

$$M = \left[\zeta_l^{(i-1)(j-1)}\right]_{1\leq i,j\leq l}$$

is an invertible Vandermonde matrix defined over $\mathbb{K}$. We have therefore proved that (1) and (2) are equivalent. Moreover, since the inverse of M is

$$M^{-1} = \frac{1}{l}\left[\zeta_l^{(1-i)(j-1)}\right]_{1\leq i,j\leq l},$$

if $r_1 = \cdots = r_{l-1} = 0$, then $x_0 = \cdots = x_{l-1} = \frac{r_0}{l}$ which contradicts the separability of P. Whence (2) implies (3). Finally, Remark 1 shows the converse. □

3. Effective Factorisation of the l-th Division Polynomial

Specialization usually does not respect the Galois structure of field extensions. So even though we know that the covering map $X(l) \longrightarrow X_1(l)$ is Galois of degree l, we cannot assert that the field extension $K(E[l])/\mathbb{K}$ is Galois of degree dividing l. We begin then by showing that this is in fact the case.

Lemma 1. *Let l be an odd prime, and $\mathbb{K}$ a field of characteristic different from l. Let E be an elliptic curve defined over $\mathbb{K}$ by a Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Then $\mathbb{K}(E[l])/\mathbb{K}$ is Galois.

Proof. Let $Q = (x_Q, y_Q)$ and $R = (x_R, y_R)$ form a basis of $E[l]$. We obviously have $\mathbb{K}(E[l]) = \mathbb{K}_x(E[l])(y_Q, y_R)$. In the tower

$$\begin{array}{c} \mathbb{K}(E[l]) \\ | \\ \mathbb{K}_x(E[l])(y_Q) \\ | \\ \mathbb{K}_x(E[l]) \\ | \\ \mathbb{K} \end{array}$$

the stages $\mathbb{K}(E[l])/\mathbb{K}_x(E[l])(y_Q)$ and $\mathbb{K}_x(E[l])(y_Q)/\mathbb{K}_x(E[l])$ are of degree at most 2, and separable since y_Q and y_R are roots of separable polynomials. Indeed, for any $x \in \overline{\mathbb{K}}$, the polynomial

$$Y^2 + (a_1 x + a_3)Y - (x^3 + a_2 x^2 + a_4 x + a_6)$$

is separable if and only if x is not the $x-$coordinate of a $2-$torsion point.

The extension $\mathbb{K}_x(E[l])/\mathbb{K}$ is Galois since $\mathbb{K}_x(E[l])$ is the splitting field of the separable polynomial ψ_l. Finally, the extension $\mathbb{K}(E[l])/\mathbb{K}$ is normal. Indeed, if σ is an embedding of $\mathbb{K}(E[l])$ in $\overline{\mathbb{K}}$ over $\mathbb{K}$, and $P = (x_P, y_P) \in E[l]$, then $\sigma P = (\sigma x_P, \sigma y_P) \in E[l]$ because the elliptic curve and the polynomial ψ_l are defined over $\mathbb{K}$. This shows that σ induces an automorphism of $\mathbb{K}(E[l])$, that is, the extension is normal. Putting all the pieces together proves the lemma. □

Proposition 3. *Let ζ_l be a primitive l-th root of unity in $\overline{\mathbb{K}}$. Assume that there exists a non-trivial point $P \in E(\mathbb{K}(\zeta_l))[l]$. Let $\mathbb{L}$ be either $\mathbb{K}(E[l])(\zeta_l)$ or $\mathbb{K}_x(E[l])(\zeta_l)$. Then* Gal $(\mathbb{L} : \mathbb{K}(\zeta_l))$ *is cyclic of order either* 1 *or* l.

Proof. Since Gal $(\mathbb{K}_x(E[l])(\zeta_l) : \mathbb{K})$ is a quotient of $G =$ Gal $(\mathbb{K}(E[l])(\zeta_l) : \mathbb{K})$, it is sufficient to prove the assertion for G. We may also assume that $\zeta_l \in \mathbb{K}$. Let $Q = (x_Q, y_Q) \in E[l]$ be a point such that (P, Q) forms a basis of $E[l]$. Let e_l be the Weil pairing. Then $e_l(P, Q)$ is a primitive l-th root of unity, and taking a multiplum of Q, we may assume that this root is ζ_l. Let $\sigma \in G$. Since σQ still is a l-torsion point, it can be expressed uniquely as

$$\sigma Q = \lambda_\sigma P + \mu_\sigma Q\,,$$

where $0 \leq \lambda_\sigma, \mu_\sigma \leq l - 1$. Moreover, the correspondance $\sigma \mapsto (\lambda_\sigma, \mu_\sigma)$ is one-to-one since the coordinates of P and Q generate $\mathbb{K}(E[l])$ over $\mathbb{K}$. Since

e_l is Galois invariant,

$$\zeta_l = \sigma\zeta_l = \sigma e_l(P,Q) = e_l(\sigma P, \sigma Q) = e_l(P, \lambda_\sigma P + \mu_\sigma Q) = e_l(P,Q)^{\mu_\sigma} = \zeta_l^{\mu_\sigma}$$

and the primitivity of ζ_l shows that $\mu_\sigma = 1$. We therefore have an injective group homomorphism

$$\begin{array}{rccc} \Lambda: & G & \longrightarrow & \mathbb{Z}/l\mathbb{Z}, \\ & \sigma & \longmapsto & \lambda_\sigma, \end{array} \tag{1}$$

which proves the proposition. □

Corollary 1. *Let $Q = (x_Q, y_Q) \in E[l]$ be such that (P,Q) forms a basis of $E[l]$. Then*

$$\mathbb{K}(E[l])(\zeta_l) = \mathbb{K}_x(E[l])(\zeta_l) = \mathbb{K}(\zeta_l, x_Q).$$

Proof. Since P is defined over $\mathbb{K}(\zeta_l)$, we have $\mathbb{K}(E[l])(\zeta_l) = \mathbb{K}(\zeta_l, x_Q, y_Q)$. Moreover, $[\mathbb{K}(E[l])(\zeta_l) : \mathbb{K}_x(E[l])(\zeta_l)]$ and $[\mathbb{K}(E[l])(\zeta_l) : \mathbb{K}(\zeta_l, x_Q)]$ are powers of 2. But we know that $[\mathbb{K}(E[l])(\zeta_l) : \mathbb{K}(\zeta_l)]$ is odd, so the two first extensions have to be trivial. □

Let E be an elliptic curve defined over a field $\mathbb{K}$ by a Weierstrass equation

$$E: y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

We assume that there exists a non-trivial point $P \in E(\mathbb{K}(\zeta_l))[l]$. Then we know that $\psi_l(X)$ has at least $\frac{l-1}{2}$ linear factors, corresponding to the x-coordinates of the points kP, for $k \in \{1, \cdots, \frac{l-1}{2}\}$, and we can therefore write

$$\psi_l(X) = l \cdot \phi_l(X) \prod_{k=1}^{\frac{l-1}{2}} (X - x(kP)),$$

where $\phi_l(X)$ is a monic polynomial of degree $l\frac{l-1}{2}$ over $\mathbb{K}$.

Corollary 2. *Over $\mathbb{K}(\zeta_l)$, the polynomial $\phi_l(X)$ is either split or is the product of $\frac{l-1}{2}$ distinct monic irreducible factors $\varphi_{l,i}(X)$ of degree l, and whose Galois group has order l.*

Proof. Let $x_Q \in \overline{\mathbb{K}}$ be any root of the polynomial ϕ_l. Let $y_Q \in \overline{\mathbb{K}}$ be such that $Q = (x_Q, y_Q) \in E[l]$. Since (P,Q) forms a basis of $E[l]$, we have

$$[\mathbb{K}(\zeta_l, x_Q) : \mathbb{K}(\zeta_l)] = [\mathbb{K}_x(E[l])(\zeta_l) : \mathbb{K}(\zeta_l)] = \#\mathrm{Gal}\,(\mathbb{K}_x(E[l])(\zeta_l) : \mathbb{K}(\zeta_l)).$$

This also shows that the Galois group of the splitting field of the irreducible factors of ϕ_l is $\mathrm{Gal}\,(\mathbb{K}_x(E[l])(\zeta_l) : \mathbb{K}(\zeta_l))$. Finally, the irreducible factors are distinct since ψ_l is separable. □

Corollary 3. *Let $Q \in E[l]$ be such that (P, Q) forms a basis of $E[l]$. The polynomials*

$$\rho_{l,i}(X) = \prod_{j=1}^{l} (X - x(iQ + jP))$$

for $i \in \{1, \cdots, \frac{l-1}{2}\}$ are in $\mathbb{K}(\zeta_l)[X]$. In particular, they are either split or irreducible over $\mathbb{K}(\zeta_l)$. In the latter case, we have $\rho_{l,i} = \varphi_{l,k_i}$ for a unique k_i and there exists a generator $\sigma_i \in G = \mathrm{Gal}\,(\mathbb{K}_x(E[l])(\zeta_l) : \mathbb{K}(\zeta_l))$ such that

$$\sigma_i(x(iQ + jP)) = x(iQ + (j+1)P).$$

Proof. If $\#G = 1$, there is nothing to prove. If $\#G = l$, then the morphism (1) is an isomorphism. Let us fix an $i \in \{1, \cdots, \frac{l-1}{2}\}$, and let $k \in \mathbb{Z}$ be such that $ki \equiv 1\ [l]$. Let $\sigma_i = \Lambda^{-1}(i)$. By definition of Λ, σ_i is a generator of G and $\sigma_i(Q) = P + kQ$. We have therefore, for all j,

$$\sigma_i(iQ + jP) = iQ + (j + ki)P = iQ + (j+1)P.$$

Thus $\rho_{l,i} \in \mathbb{K}(\zeta_l)[X]$. The existence and uniqueness of k_i results from the degrees of the $\rho_{l,i}$ and the fact that their product is ϕ_l. □

Proposition 4. *We have*

$$\begin{aligned} E(\mathbb{K}(\zeta_l))[l] \approx (\mathbb{Z}/l\mathbb{Z})^2 &\Leftrightarrow \forall i,\ \rho_{l,i} \text{ splits}, \\ &\Leftrightarrow \exists i,\ \rho_{l,i} \text{ splits}. \end{aligned}$$

Proof. This follows directly from Corollaries 1 to 3. □

4. Application to 3−, 5− and 7−Torsion

Using the results of the two previous parts, we can easily find a generalization of a theorem on 3-torsion proved in [6].

Theorem 4. *Let $\mathbb{K}$ be a field of characteristic different from 3. Let E be an elliptic curve defined over $\mathbb{K}$ by a Weierstrass equation*

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$

Assume that E has a $\mathbb{K}$-rational point of 3-torsion. Then we have

$$E(\mathbb{K}(\zeta_3))[3] \approx (\mathbb{Z}/3\mathbb{Z})^2 \Leftrightarrow \Delta \in \mathbb{K}(\zeta_3)^{(3)}.$$

We will not present the proof here, since it is very similar to the proofs of the two other theorems of this section.

We are interested in finding a similar statement for $5-$ and $7-$torsion. Obviously, the previous theorem cannot be generalized to these cases since the discriminant Δ of the elliptic curve E is defined up to a 12-th power of a non-zero element.

From now on, $l = 5$ or $l = 7$. Elliptic curves having a rational $l-$torsion point can be parametrized by the affine part of a curve of genus 0 (cf. [1]). Namely, there is a one-to-one correspondence between $Y_1(l)(\mathbb{K})$ and the set $\mathcal{ELL}_l$ of couples (E, P), where E is an elliptic curve defined over $\mathbb{K}$ and P is a non-zero point in $E(\mathbb{K})[l]$, up to $\mathbb{K}$-isomorphism (that is an isomorphism $E \longrightarrow E'$ over $\mathbb{K}$ that sends P to P'). In our case, the smooth projective model $X_1(l)(\mathbb{K})$ of $Y_1(l)(\mathbb{K})$ is a curve of genus 0. Moreover, one can explicitly write down a bijection between a Zariski open of the affine line and $\mathcal{ELL}_l$. These bijections are the following:

$$\begin{array}{ccc} & Y_1(l)(\mathbb{K}) & \\ \swarrow^{\approx} & & \searrow^{\approx} \\ V(P_l) & \xrightarrow[\theta]{\approx} & \mathcal{ELL}_l \end{array}$$

where

$$\begin{cases} P_5(T) = T^5(T^2 - 11T - 1) = T^5Q_5(T)\,, \\ P_7(T) = T^7(T-1)^7(T^3 - 8T^2 + 5T + 1) = T^7(T-1)^7Q_7(T)\,, \\ V(P_l) = \mathbb{K}\backslash\{\text{roots of } P_l\}\,, \end{cases}$$

$$\begin{cases} E_{5,t} : y^2 + (1-t)xy - ty = x^3 - tx^2\,, \\ E_{7,t} : y^2 + (1 + t - t^2)xy + (t^2 - t^3)y = x^3 + (t^2 - t^3)x^2\,, \end{cases}$$

and $\theta(T) = E_{l,T}$. Note that the value of the polynomial $P_l(T)$ at t is equal to the discriminant of the curve $E_{l,t}$ in both cases. The polynomials $P_l(T)$

split over $\mathbb{K}(\zeta_l)$, and their roots are $\alpha_5 = 8+5\zeta_5+5\zeta_5^4$ and $\beta_5 = 3-5\zeta_5-5\zeta_5^4$ when $l=5$, and when $l=7$, $\alpha_7 = 1-2\zeta_7-3\zeta_7^2-3\zeta_7^5-2\zeta_7^6$, $\beta_7 = 1-2\zeta_7^2-3\zeta_7^3-3\zeta_7^4-2\zeta_7^5$ and finally $\gamma_7 = 1-3\zeta_7-2\zeta_7^3-2\zeta_7^4-3\zeta_7^6$.

Theorem 5. *Let $\mathbb{K}$ be a field of characteristic different from 5. Let $\zeta_5 \in \overline{\mathbb{K}}$ be a primitive 5-th root of unity. Define $\alpha_5 = 8+5\zeta_5+5\zeta_5^4$ and $\beta_5 = 3-5\zeta_5-5\zeta_5^4$. Let $t \in \mathbb{K}$ be such that $P_5(t) \neq 0$, and consider the elliptic curve $E_{5,t}$. Then*

$$E_{5,t}(\mathbb{K}(\zeta_5))[5] \approx (\mathbb{Z}/5\mathbb{Z})^2 \Leftrightarrow \frac{t-\alpha_5}{t-\beta_5} \in \mathbb{K}(\zeta_5)^{(5)}.$$

We state the analogous theorem for $l=7$.

Theorem 6. *Let $\mathbb{K}$ be a field of characteristic different from 7. Let $\zeta_7 \in \overline{\mathbb{K}}$ be a primitive 7-th root of unity. Define $\alpha_7 = 1-2\zeta_7-3\zeta_7^2-3\zeta_7^5-2\zeta_7^6$, $\beta_7 = 1-2\zeta_7^2-3\zeta_7^3-3\zeta_7^4-2\zeta_7^5$ and $\gamma_7 = 1-3\zeta_7-2\zeta_7^3-2\zeta_7^4-3\zeta_7^6$. Let $t \in \mathbb{K}$ be such that $P_7(t) \neq 0$, and consider the elliptic curve $E_{7,t}$. Then*

$$E_{7,t}(\mathbb{K}(\zeta_7))[7] \approx (\mathbb{Z}/7\mathbb{Z})^2 \Leftrightarrow \frac{(t-\alpha_7)(t-\beta_7)^2}{(t-\gamma_7)^3} \in \mathbb{K}(\zeta_7)^{(7)}.$$

Proof of Theorem 5. Consider the elliptic curve

$$E_T : x^2 + (1-T)xy - Ty = x^3 - Tx^2$$

defined over the ring $\mathbb{Z}\left[\frac{1}{5}\right][T]$. Its discriminant is $\Delta_T = T^5(T^2-11T-1)$. We will work in projective coordinates so that no division will be needed to add points on this curve. All the computations are done with *MAGMA*. We know that the points $P=[0,0,1]$, $2P=[T,T^2,1]$, $3P=[T,0,1]$ and $4P=[0,T,1]$ are points of 5-torsion on that curve. Let z_5 be the image of U under the canonical projection in the ring $S = R[U]/<U^4+U^3+U^2+U+1>$. The fifth division polynomial $\psi_5(X)$ factorizes over S in the following way:

$$\psi_5(X) = 5X(X-T)\varphi_{5,1}(X)\varphi_{5,2}(X)$$

with

$$\begin{aligned} 5\varphi_{5,1}(X) = {} & 5X^5 + \left(2T^2 - 7T + 3 - Q_5(T)(z_5+z_5^4)\right)X^4 \\ & + T\left(T^2 + 9T - 11 + 2Q5(T)(z_5+z_5^4)\right)X^3 + 5T^3(T-3)X \\ & + T^2\left(2T^2 - 12T + 18 - Q_5(T)(z_5+z_5^4)\right)X^2 + 5T^4 \end{aligned}$$

and

$$\begin{aligned}5\varphi_{5,2}(X) = 5X^5 &+ \left(3T^2 - 18T + 2 + Q_5(T)(z_5 + z_5^4)\right) X^4 \\ &+ T\left(-T^2 + 31T - 9 - 2Q_5(T)(z_5 + z_5^4)\right) X^3 + 5T^3(T-3)X \\ &+ T^2\left(3T^2 - 23T + 17 + Q_5(T)(z_5 + z_5^4)\right) X^2 + 5T^4.\end{aligned}$$

These last two polynomials are irreducible over S since they are irreducible over the fraction field of S. Denote by x_0 the canonical image of X in the quotient ring $V = S[X]/ < \varphi_{5,1}(X) >$. Let

$$X_0 = 5x_0\Delta_T,$$

$$\begin{aligned}Y_0 = &-5\left(z_5^3 + 3z_5^2 + 4z_5 + 2\right) T^4x_0^4 + 5\left(3z_5^3 - z_5^2 + 2z_5 + 1\right) T^3x_0^4 \\ &- \left(2z_5^3 + 4z_5^2 + 6z_5 + 3\right) T^6x_0^3 + 6\left(3z_5^3 + z_5^2 + 4z_5 + 2\right) T^5x_0^3 \\ &- 2\left(27z_5^3 - z_5^2 + 26z_5 + 13\right) T^4x_0^3 + \left(4z_5^3 - 2z_5^2 + 2z_5 + 1\right) T^3x_0^3 \\ &- \left(2z_5^3 + 4z_5^2 + 6z_5 + 3\right) T^7x_0^2 + \left(8z_5^3 + 6z_5^2 + 14z_5 + 7\right) T^6x_0^2 \\ &+ \left(66z_5^3 + 32z_5^2 + 98z_5 + 49\right) T^5x_0^2 - 4\left(4z_5^3 - 2z_5^2 + 2z_5 + 1\right) T^4x_0^2 \\ &- \left(z_5^3 + 2z_5^2 + 3z_5 - 1\right) T^8x_0 + \left(9z_5^3 + 13z_5^2 + 22z_5 - 19\right) T^7x_0 \\ &- \left(17z_5^3 + 59z_5^2 + 76z_5 + 13\right) T^6x_0 + \left(22z_5^3 - 11z_5^2 + 11z_5 + 8\right) T^5x_0 \\ &- 5\left(z_5^2 + z_5\right) T^8 - 5\left(z_5^3 - 6z_5^2 - 5z_5 + 3\right) T^7 - 5\left(2z_5^3 - z_5^2 + z_5 + 1\right) T^6,\end{aligned}$$

and

$$Z_0 = 5\Delta_T.$$

We easily check that $P_0 = [X_0, Y_0, Z_0]$ is a point in $E(V)[5]$. We compute the points $P_i = [X_i, Y_i, Z_i] = P_0 + iP$ for $i \in \{1, \cdots, 4\}$. Since we will not need the Y_i's afterwards, we will not write them down – the interested reader can find their expression on my web page, see [7]. The only thing we need to know is that they can be expressed as polynomials in $\mathbb{Z}\left[\frac{1}{5}, z_5, T, x_0\right]$, and we even can choose the Z_i's such that

$$Z_1 = Z_2 = Z_3 = Z_4 = Z_0.$$

Then

$$\begin{aligned}X_1 = &\left(z_5^3 - 3z_5^2 - 2z_5 - 1\right) T^5x_0^4 - 2\left(7z_5^3 - 16z_5^2 - 9z_5 - 2\right) T^4x_0^4 \\ &+ \left(22z_5^3 - 26z_5^2 - 4z_5 + 53\right) T^3x_0^4 + \left(8z_5^3 - 4z_5^2 + 4z_5 + 7\right) T^2x_0^4\end{aligned}$$

$$
\begin{aligned}
&+ \left(z_5^3 - z_5^2\right) T^7 x_0^3 - \left(241 z_5^3 + 98 z_5^2 + 101 z_5 + 220\right) T^4 x_0^3 \\
&+ \left(141 z_5^3 - 10 z_5^2 + 87 z_5 + 92\right) T^5 x_0^3 - \left(22 z_5^3 - 12 z_5^2 + 8 z_5 + 7\right) T^6 x_0^3 \\
&- \left(50 z_5^3 + 33 z_5^2 + 39 z_5 + 13\right) T^3 x_0^3 + \left(z_5^3 - 3 z_5^2 + 2\right) T^2 x_0^3 \\
&+ \left(379 z_5^3 + 67 z_5^2 + 89 z_5 + 295\right) T^5 x_0^2 - \left(8 z_5^3 - 7 z_5^2 + 4 z_5 + 10\right) T^3 x_0^2 \\
&- \left(224 z_5^3 + 25 z_5^2 + 183 z_5 + 108\right) T^6 x_0^2 - \left(z_5^3 + z_5^2 + 2 z_5 + 1\right) T^8 x_0^2 \\
&+ 2 \left(20 z_5^3 + 31 z_5^2 + 18 z_5 - 24\right) T^4 x_0^2 + \left(28 z_5^3 + 12 z_5^2 + 37 z_5 + 18\right) T^7 x_0^2 \\
&+ \left(z_5^3 - z_5^2\right) T^9 x_0 - \left(2 z_5^2 + z_5 + 2\right) T^9 - \left(8 z_5^3 - 2 z_5^2 + 5 z_5 + 9\right) T^5 \\
&+ 5 \left(23 z_5^3 - 19 z_5^2 + 4 z_5 + 9\right) T^7 x_0 - \left(71 z_5^3 - 168 z_5^2 - 97 z_5 + 44\right) T^6 x_0 \\
&+ \left(59 z_5^3 - 27 z_5^2 + 32 z_5 + 146\right) T^5 x_0 + \left(15 z_5^3 - 6 z_5^2 + 9 z_5 + 17\right) T^4 x_0 \\
&+ 2 \left(2 z_5^3 + 16 z_5^2 + 7 z_5 + 15\right) T^8 - \left(21 z_5^3 - 18 z_5^2 + 3 z_5 + 4\right) T^8 x_0 \\
&- \left(41 z_5^3 + 115 z_5^2 + 37 z_5 + 82\right) T^7 - 2 \left(26 z_5^3 - z_5^2 + 14 z_5 + 46\right) T^6 ,
\end{aligned}
$$

$$
\begin{aligned}
X_2 = &\left(4 z_5^3 + 8 z_5^2 + 12 z_5 + 11\right) T^4 x_0^4 - \left(26 z_5^3 + 22 z_5^2 + 48 z_5 + 79\right) T^3 x_0^4 \\
&- 2 \left(16 z_5^3 + 7 z_5^2 + 23 z_5 + 14\right) T^2 x_0^4 - \left(3 z_5^3 + z_5^2 + 4 z_5 + 2\right) T x_0^4 \\
&+ \left(3 z_5^3 + 3 z_5^2 + 4 z_5 + 5\right) T^6 x_0^3 - \left(49 z_5^3 + 26 z_5^2 + 31 z_5 + 64\right) T^5 x_0^3 \\
&+ \left(202 z_5^3 + 85 z_5^2 + 49 z_5 + 194\right) T^4 x_0^3 - \left(z_5^3 + z_5^2 + 2 z_5 + 1\right) T x_0^3 \\
&- \left(16 z_5^2 + 18 z_5 + 11\right) T^2 x_0^3 + \left(118 z_5^3 - 41 z_5^2 + 33 z_5 + 10\right) T^3 x_0^3 \\
&- \left(2 z_5^3 - 2 z_5^2 - 3 z_5 - 2\right) T^7 x_0^2 + \left(61 z_5^3 + 4 z_5^2 - z_5 + 16\right) T^6 x_0^2 \\
&- \left(383 z_5^3 + 145 z_5^2 + 171 z_5 + 336\right) T^5 x_0^2 + 5 \left(z_5^2 + z_5 + 1\right) T^8 \\
&+ \left(30 z_5^3 + 29 z_5^2 + 62 z_5 + 39\right) T^3 x_0^2 + \left(4 z_5^3 + 2 z_5^2 + 6 z_5 + 3\right) T^2 x_0^2 \\
&+ \left(z_5^3 + 2 z_5^2 + 3 z_5 + 4\right) T^8 x_0 - \left(18 z_5^3 + 21 z_5^2 + 39 z_5 + 57\right) T^7 x_0 \\
&+ 2 \left(48 z_5^3 + 26 z_5^2 + 74 z_5 + 97\right) T^6 x_0 - \left(47 z_5^3 + 34 z_5^2 + 81 z_5 + 168\right) T^5 x_0 \\
&- \left(66 z_5^3 + 27 z_5^2 + 93 z_5 + 59\right) T^4 x_0 - 2 \left(3 z_5^3 + z_5^2 + 4 z_5 + 2\right) T^3 x_0 \\
&- \left(137 z_5^3 - 49 z_5^2 + 22 z_5 - 55\right) T^4 x_0^2 - \left(4 z_5^3 + 48 z_5^2 + 52 z_5 + 61\right) T^7 \\
&+ 2 \left(33 z_5^3 + 11 z_5^2 + 44 z_5 + 62\right) T^6 + \left(37 z_5^3 + 14 z_5^2 + 51 z_5 + 33\right) T^5 \\
&+ \left(3 z_5^3 + z_5^2 + 4 z_5 + 2\right) T^4 ,
\end{aligned}
$$

$$
\begin{aligned}
X_3 = &- \left(4 z_5^3 + 8 z_5^2 + 12 z_5 + 1\right) T^4 x_0^4 + \left(26 z_5^3 + 22 z_5^2 + 48 z_5 - 31\right) T^3 x_0^4 \\
&+ 2 \left(16 z_5^3 + 7 z_5^2 + 23 z_5 + 9\right) T^2 x_0^4 - \left(74 z_5^3 - 85 z_5^2 + 33 z_5 + 23\right) T^3 x_0^3 \\
&- \left(z_5^3 + z_5^2 + 4 z_5 - 1\right) T^6 x_0^3 + \left(5 z_5^3 - 18 z_5^2 + 31 z_5 - 33\right) T^5 x_0^3
\end{aligned}
$$

$$
\begin{aligned}
&+\left(36z_5^3+153z_5^2-49z_5+145\right)T^4x_0^3+\left(3z_5^3+z_5^2+4z_5+2\right)Tx_0^4\\
&+\left(2z_5^3+18z_5^2+18z_5+7\right)T^2x_0^3+\left(5z_5^3+62z_5^2+z_5+17\right)T^6x_0^2\\
&+\left(71z_5^3-115z_5^2+22z_5+77\right)T^4x_0^2-\left(z_5^3+2z_5^2+3z_5-1\right)T^8x_0\\
&-\left(z_5^3+5z_5^2+3z_5+1\right)T^7x_0^2-\left(33z_5^3+32z_5^2+62z_5+23\right)T^3x_0^2\\
&-\left(4z_5^3+2z_5^2+6z_5+3\right)T^2x_0^2+\left(26z_5^3-212z_5^2+171z_5-165\right)T^5x_0^2\\
&+\left(18z_5^3+21z_5^2+39z_5-18\right)T^7x_0+\left(4z_5^3+48z_5^2+52z_5-9\right)T^7\\
&+\left(47z_5^3+34z_5^2+81z_5-87\right)T^5x_0+\left(66z_5^3+27z_5^2+93z_5+34\right)T^4x_0\\
&+2\left(3z_5^3+z_5^2+4z_5+2\right)T^3x_0-2\left(48z_5^3+26z_5^2+74z_5-23\right)T^6x_0\\
&-5\left(z_5^2+z_5\right)T^8-\left(3z_5^3+z_5^2+4z_5+2\right)T^4+\left(z_5^3+z_5^2+2z_5+1\right)Tx_0^3\\
&-2\left(33z_5^3+11z_5^2+44z_5-18\right)T^6-\left(37z_5^3+14z_5^2+51z_5+18\right)T^5,
\end{aligned}
$$

and

$$
\begin{aligned}
X_4=&-\left(z_5^3-3z_5^2-2z_5-1\right)T^5x_0^4+2\left(7z_5^3-16z_5^2-9z_5-7\right)T^4x_0^4\\
&-\left(22z_5^3-26z_5^2-4z_5-57\right)T^3x_0^4-\left(8z_5^3-4z_5^2+4z_5-3\right)T^2x_0^4\\
&+\left(20z_5^3-14z_5^2+8z_5+1\right)T^6x_0^3+\left(3z_5^3-140z_5^2+101z_5-119\right)T^4x_0^3\\
&-\left(97z_5^3-54z_5^2+87z_5-5\right)T^5x_0^3-\left(3z_5^3-z_5^2-2\right)T^2x_0^3\\
&+\left(6z_5^3-11z_5^2+39z_5+26\right)T^3x_0^3+\left(z_5^3+z_5^2+2z_5+1\right)T^8x_0^2\\
&+\left(158z_5^3-41z_5^2+183z_5+75\right)T^6x_0^2-\left(25z_5^3+9z_5^2+37z_5+19\right)T^7x_0^2\\
&-\left(22z_5^3-290z_5^2+89z_5-206\right)T^5x_0^2+2\left(13z_5^3+2z_5^2-18z_5-42\right)T^4x_0^2\\
&+\left(11z_5^3-4z_5^2+4z_5-6\right)T^3x_0^2-\left(59z_5^3-27z_5^2+32z_5-114\right)T^5x_0\\
&-5\left(23z_5^3-19z_5^2+4z_5-5\right)T^7x_0+\left(21z_5^3-18z_5^2+3z_5-1\right)T^8x_0\\
&+\left(71z_5^3-168z_5^2-97z_5-141\right)T^6x_0+\left(7z_5^3-3z_5^2+5z_5-4\right)T^5\\
&-\left(15z_5^3-6z_5^2+9z_5-8\right)T^4x_0+2\left(9z_5^3-5z_5^2-7z_5+8\right)T^8\\
&-\left(z_5^3-z_5^2-z_5+1\right)T^9-\left(z_5^3-z_5^2\right)T^9x_0-\left(z_5^3-z_5^2\right)T^7x_0^3\\
&-\left(78z_5^3+4z_5^2-37z_5+45\right)T^7+2\left(15z_5^3-12z_5^2+14z_5-32\right)T^6.
\end{aligned}
$$

We now compute

$$
\begin{aligned}
&\left(X_0+z_5X_1+z_5^2X_2+z_5^3X_3+z_5^4X_4\right)^5\\
&\qquad=\left(z_5+z_5^4-2\right)^5T^{25}\left(T-A_5\right)^{11}\left(T-B_5\right)^9,
\end{aligned}
$$

where $A_5=8+5z_5+5z_5^4$ and $B_5=3-5z_5-3z_5^4$. Consider any field $\mathbb{K}$ of characteristic different from 5. We have a canonical mapping from $\mathbb{Z}\left[\frac{1}{5}\right]$

into this field which canonically extends to mappings from R to $\mathbb{K}[T]$ and from S to $\mathbb{K}(\zeta_5)[T]$. Since no inversion was required in all the computations done previously, the formulas hold if we replace the ring R by the ring $\mathbb{K}[T]$. Thus, keeping the notation from Section 3, we get that

$$\Delta_T^5 R_1 = \left(\zeta_5 + \zeta_5^4 - 2\right)^5 T^{25} \left(T - \alpha_5\right)^{11} \left(T - \beta_5\right)^9 .$$

Now, by specializing to $t \in \mathbb{K}$ such that $P_5(t) \neq 0$ and remarking that Δ_T, T, $T - \alpha_5$ and $T - \beta_5$ remain non-zero under specialization, we get that R_1 is non-zero, and that it is a fifth power in $\mathbb{K}(\zeta_5)$ if and only if $\frac{t-\alpha_5}{t-\beta_5}$ is. □

Proof of Theorem 6. The idea of the proof is exactly the same as in the previous proof, and we refer to it for the notation. The computational difficulty here is to find a y_0 such that $[x_0, y_0, 1]$ is a point on the curve. The method that we used was the following: *MAGMA* found easily such a y_0 for the elliptic curve

$$E_T : y^2 + (1 + T - T^2)xy + (T^2 - T^3)y = x^3 + (T^2 - T^3)x^2$$

over $\mathbb{F}_p(T)$, where $\mathbb{F}_p$ was a prime finite field with p elements, and such that $p \equiv 1$ [7], so that the field had primitive 7-th roots of unity. The result was of the form $\frac{Y(T)T(T-1)(T-\beta_7)}{7\Delta_T(T-\gamma_7)}$, where $Y(T)$ was a polynomial in T with coefficients in $\mathbb{F}_p(x_0)$ of degree 18. We then decomposed the polynomial $Y(T)$ into 7 unique polynomials $Y_i(T)$ over $\mathbb{F}_p$ such that

$$Y(T) = \sum_{i=0}^{6} Y_i(T) x_0^i .$$

We looked afterwards at the same curve E_T, defined this time over $\mathbb{Q}(z_7)[T]$, and specialized it at 19 different places by taking $T = T_j \in \mathbb{Z}$. *MAGMA* found easily the two different $y_{0,T_j,k}$ corresponding to our given x_{0,T_j}. We reduced these $y_{0,T_j,k}$ modulo our previous prime p, and kept the one corresponding to the y_0 we had previously found. We denote it by y_{T_j}. This being done, for $i \in \{0, \cdots, 18\}$, we decomposed

$$\frac{7\Delta_{T_j} y_{T_j}}{T_j(T_j - 1)(T_j - \beta_7)} = \sum_{i=0}^{6} \eta_{j,i} x_{0,T_j}^i ,$$

where $\eta_{j,i} \in \mathbb{Q}(z_7)$. For $i \in \{0 \cdots, 6\}$, we then solved the matrix equations

$$\begin{bmatrix} \eta_{0,i} \\ \vdots \\ \eta_{18,i} \end{bmatrix} = M \cdot \begin{bmatrix} e_{0,i} \\ \vdots \\ e_{18,i} \end{bmatrix} ,$$

where M is the Vandermonde matrix

$$M = \left[T_j^i\right]_{0\le i,j\le 18}.$$

Finally we defined for $i \in \{0, \cdots, 6\}$, the polynomials

$$Y_i^\dagger(T) = \sum_{j=0}^{18} e_{j,i} T^j \in \mathbb{Q}(z_7)[T]$$

and

$$Y^\dagger(T) = \sum_{i=0}^{6} Y_i^\dagger(T) x_0^i \in Q(z_7)(x_0)[T].$$

The latter polynomial was in $\mathbb{Z}[z_7, x_0, T]$. We then checked that the point

$$P_0 = \left[7x_0\Delta_T^2, Y^\dagger(T)T^8(T-1)^8(T-A_7)(T-B_7)^2, 7\Delta_T^2\right]$$

was in fact a point on the elliptic curve E_T, necessarily of 7-torsion. We give here the polynomial $Y^\dagger(T)$:

$$\begin{aligned} Y^\dagger(T) = {} & 7d_6x_0^6 + d_5x_0^5 + d_4T(T-1)x_0^4 + d_3T^2(T-1)^2x_0^3 \\ & + d_2T^4(T-1)^3x_0^2 + d_1T^6(T-1)^4x_0 + 7d_0T^8(T-1)^5, \end{aligned}$$

where

$$\begin{aligned} d_6 = {} & \left(3z_7^5 - z_7^4 + 3z_7^3 - z_7^2 + 2z_7 + 1\right)T^3 - 9z_7^5 + 5z_7^4 - 11z_7^3 + 3z_7^2 - 6z_7 - 3 \\ & - \left(19z_7^5 - 7z_7^4 + 21z_7^3 - 5z_7^2 + 14z_7 + 7\right)T^2 \\ & + 2\left(13z_7^5 - 4z_7^4 + 14z_7^3 - 3z_7^2 + 10z_7 + 5\right)T, \end{aligned}$$

$$\begin{aligned} d_5 = {} & \left(6z_7^5 - 2z_7^4 + 4z_7^3 - 4z_7^2 + 2z_7 + 1\right)T^7 \\ & - \left(37z_7^5 - 10z_7^4 + 20z_7^3 - 27z_7^2 + 10z_7 + 5\right)T^6 \\ & - \left(73z_7^5 - 64z_7^4 + 128z_7^3 - 9z_7^2 + 64z_7 + 32\right)T^5 \\ & + \left(755z_7^5 - 401z_7^4 + 921z_7^3 - 235z_7^2 + 520z_7 + 260\right)T^4 \\ & - \left(1349z_7^5 - 690z_7^4 + 1618z_7^3 - 421z_7^2 + 928z_7 + 464\right)T^3 \\ & + \left(843z_7^5 - 393z_7^4 + 989z_7^3 - 247z_7^2 + 596z_7 + 298\right)T^2 \\ & - \left(41z_7^5 - 16z_7^4 + 46z_7^3 - 11z_7^2 + 30z_7 + 15\right)T \end{aligned}$$

$$- 88z_7^5 + 41z_7^4 - 103z_7^3 + 26z_7^2 - 62z_7 - 31\,,$$

$$\begin{aligned}
d_4 = {} & \left(9z_7^5 - 3z_7^4 + 13z_7^3 + z_7^2 + 10z_7 + 5\right) T^8 \\
& - \left(117z_7^5 - 46z_7^4 + 162z_7^3 - z_7^2 + 116z_7 + 58\right) T^7 \\
& + \left(505z_7^5 - 236z_7^4 + 626z_7^3 - 115z_7^2 + 390z_7 + 195\right) T^6 \\
& - 3\left(190z_7^5 - 117z_7^4 + 241z_7^3 - 66z_7^2 + 124z_7 + 62\right) T^5 \\
& - \left(1336z_7^5 - 373z_7^4 + 1411z_7^3 - 298z_7^2 + 1038z_7 + 519\right) T^4 \\
& + \left(3599z_7^5 - 1580z_7^4 + 4154z_7^3 - 1025z_7^2 + 2574z_7 + 1287\right) T^3 \\
& - \left(2871z_7^5 - 1265z_7^4 + 3321z_7^3 - 815z_7^2 + 2056z_7 + 1028\right) T^2 \\
& + \left(613z_7^5 - 265z_7^4 + 705z_7^3 - 173z_7^2 + 440z_7 + 220\right) T \\
& + 113z_7^5 - 47z_7^4 + 129z_7^3 - 31z_7^2 + 82z_7 + 41\,,
\end{aligned}$$

$$\begin{aligned}
d_3 = {} & \left(6z_7^5 - 2z_7^4 + 4z_7^3 - 4z_7^2 + 2z_7 + 1\right) T^9 \\
& - \left(103z_7^5 - 32z_7^4 + 92z_7^3 - 43z_7^2 + 60z_7 + 30\right) T^8 \\
& + 2\left(367z_7^5 - 120z_7^4 + 394z_7^3 - 93z_7^2 + 274z_7 + 137\right) T^7 \\
& - \left(2855z_7^5 - 1115z_7^4 + 3217z_7^3 - 753z_7^2 + 2102z_7 + 1051\right) T^6 \\
& + \left(6327z_7^5 - 2725z_7^4 + 7249z_7^3 - 1803z_7^2 + 4524z_7 + 2262\right) T^5 \\
& - 7\left(1035z_7^5 - 470z_7^4 + 1202z_7^3 - 303z_7^2 + 732z_7 + 366\right) T^4 \\
& + \left(3399z_7^5 - 1399z_7^4 + 3869z_7^3 - 929z_7^2 + 2470z_7 + 1235\right) T^3 \\
& + 2\left(103z_7^5 - 46z_7^4 + 120z_7^3 - 29z_7^2 + 74z_7 + 37\right) T^2 \\
& - \left(305z_7^5 - 139z_7^4 + 355z_7^3 - 89z_7^2 + 216z_7 + 108\right) T \\
& - 88z_7^5 + 41z_7^4 - 103z_7^3 + 26z_7^2 - 62z_7 - 31\,,
\end{aligned}$$

$$\begin{aligned}
d_2 = {} & \left(5z_7^5 - 4z_7^4 + 8z_7^3 - z_7^2 + 4z_7 + 2\right) T^8 \\
& - 7\left(11z_7^5 - 9z_7^4 + 17z_7^3 - 3z_7^2 + 8z_7 + 4\right) T^7 \\
& + 7\left(66z_7^5 - 49z_7^4 + 89z_7^3 - 26z_7^2 + 40z_7 + 20\right) T^6 \\
& - \left(1248z_7^5 - 724z_7^4 + 1518z_7^3 - 454z_7^2 + 794z_7 + 397\right) T^5 \\
& + \left(1093z_7^5 - 467z_7^4 + 1235z_7^3 - 325z_7^2 + 768z_7 + 384\right) T^4 \\
& + \left(865z_7^5 - 524z_7^4 + 1090z_7^3 - 299z_7^2 + 566z_7 + 283\right) T^3 \\
& - \left(1532z_7^5 - 618z_7^4 + 1740z_7^3 - 410z_7^2 + 1122z_7 + 561\right) T^2
\end{aligned}$$

$$+\left(151z_7^5-111z_7^4+201z_7^3-61z_7^2+90z_7+45\right)T$$
$$+223z_7^5-107z_7^4+263z_7^3-67z_7^2+156z_7+78\,,$$

$$\begin{aligned}d_1=&\left(3z_7^5-z_7^4+2z_7^3-2z_7^2+z_7+4\right)T^7\\&-\left(53z_7^5+8z_7^4+40z_7^3+2z_7^2+20z_7+59\right)T^6\\&+7\left(38z_7^5+14z_7^4+22z_7^3+18z_7^2+12z_7+41\right)T^5\\&-\left(306z_7^5+304z_7^4+8z_7^3+454z_7^2-59z_7+499\right)T^4\\&-\left(428z_7^5-502z_7^4+780z_7^3-612z_7^2+607z_7-162\right)T^3\\&+\left(633z_7^5-232z_7^4+716z_7^3-177z_7^2+498z_7+235\right)T^2\\&+\left(69z_7^5-114z_7^4+165z_7^3-214z_7^2+198z_7-111\right)T\\&-156z_7^5+143z_7^4-237z_7^3+139z_7^2-157z_7+9\,,\end{aligned}$$

$$\begin{aligned}d_0=&\left(z_7^5+z_7^3+z_7+1\right)T^5-\left(13z_7^5+z_7^4+12z_7^3+z_7^2+9z_7+11\right)T^4\\&+\left(47z_7^5+3z_7^4+39z_7^3+14z_7^2+22z_7+40\right)T^3\\&-\left(49z_7^5+16z_7^4+27z_7^3+40z_7^2+6z_7+56\right)T^2\\&+\left(10z_7^5+22z_7^4-11z_7^3+40z_7^2-19z_7+33\right)T\\&+3z_7^5-11z_7^4+11z_7^3-14z_7^2+9z_7-8\,.\end{aligned}$$

Now, in the same way as we did in the previous proof, we are able to compute the points $P_i=[X_i,Y_i,Z_i]$ for $i\in\{0,\cdots,6\}$. If we take

$$Z_i=7\Delta_T^2\,,$$

then

$$X_i,Y_i\in\mathbb{Z}[z_7,T].$$

We do not write here the expressions for the X_i's and Y_i's, but the interested reader can find them on my homepage [7]. We can now compute the quantity $\left(X_0+z_7^iX_1+\cdots z_7^{6i}X_6\right)^7$ for $i\in\{0,\cdots,6\}$. For $i=3$, we find that

$$\begin{aligned}&\left(X_0+z_7^3X_1+\cdots z_7^{18}X_6\right)\\&\qquad=D_7^7T^{98}(T-1)^{98}\,(T-A_7)^{24}\,(T-B_7)^{20}\,(T-C_7)^{26}\,,\end{aligned}$$

with $D_{/} = z_7^5 + z_7^4 - 2z_7^2 - 5z_7 - 2$. As we saw in the case $l = 5$, this equality is valid also in the ring $\mathbb{K}[T]$, which leads to

$$7^7 \Delta_T^{14} R_3 = \delta_7^7 T^{98} (T-1)^{98} (T-\alpha_7)^{24} (T-\beta_7)^{20} (T-\gamma_7)^{26},$$

with $\delta_7 = \zeta_7^5 + \zeta_7^4 - 2\zeta_7^2 - 5\zeta_7 - 2$. If we specialize to $t \in \mathbb{K}$, we remark that none of the factors can be 0, since $\Delta_t = t^7(t-1)^7(t-\alpha_7)(t-\beta_7)(t-\gamma_7) \neq 0$. This means that $R_3 \neq 0$, and therefore, it is a 7-th power in $\mathbb{K}(\zeta_7)$ if and only if the group $E(\mathbb{K}(\zeta_7))[7]$ is isomorphic to $(\mathbb{Z}/7\mathbb{Z})^2$. The result follows immediately.

References

[1] F. Diamond, J. Shurman, *A First Course in Modular Forms*, Graduate Texts in Mathematics, **228**, Springer-Verlag (2005).

[2] W. Duke, Almost all reductions modulo p of an elliptic curve have a large exponent, *C.R. Math. Acad. Sci. Paris*, **337** (2003), 689-692.

[3] B.S. Kaliski, One-way permutation on elliptic curves, *J. Cryptology*, **3**, No. 3 (1991), 187-199.

[4] A.J. Menezes, P.C. van Oorschot, S.A. Vanstone, *Handbook of Applied Cryptography*, CRC Press (1997).

[5] J.H. Silverman, *The Arithmetic of Elliptic Curves*, Number 106 in Graduate Texts in Mathematics, Springer-Verlag (1986).

[6] H. Verdure, A simple criterion for the m-cyclicity of the group of rational points on an elliptic curve defined over a finite field, *Arch. Math.*, Basel, **86** (2006), 121-128.

[7] http://www.math.uit.no/users/verdure/Lagrange.html