

FIELDS GENERATED BY TORSION POINTS OF ELLIPTIC CURVES

ANDREA BANDINI AND LAURA PALADINO

ABSTRACT. We look for small (sometimes “minimal”) set of generators for the fields $K(\mathcal{E}[m])$ generated by the m -torsion points of an elliptic curve $\mathcal{E}$ (where K is any number field). For $m = 3$ we use this to provide informations on the extension $K(\mathcal{E}[m])/K$ such as its degree and its Galois group.

1. INTRODUCTION

Let $\mathcal{E}$ be an elliptic curve with Weierstrass form $y^2 = x^3 + Ax + B$ defined over a number field K and let m be a positive integer. We denote by $\mathcal{E}[m]$ the m -torsion subgroup of $\mathcal{E}$ and by $K_m := K(\mathcal{E}[m])$ the number field generated by the coordinates of the m -torsion points of $\mathcal{E}$. As usual for any point $P \in \mathcal{E}$, we let $x(P)$, $y(P)$ be its coordinates and indicate its m -th multiple simply by mP . We shall investigate the set of generators for the extension K_m/K . In [2] we studied the case $K = \mathbb{Q}$ (in particular for the case $m = 3$) and noted that many of the techniques could be extended to a general number field K . In Section 2 we generalize [2, Theorem 2.2] and easily prove

Theorem 1.1. *Let $m > 2$ and let $\{P_1, P_2\}$ be a $\mathbb{Z}$ -basis for $\mathcal{E}[m]$, then*

$$K_m = K(x(P_1), x(P_2), \zeta_m, y(P_1))$$

(where ζ_m is a primitive m -th root of unity).

We expected a close similarity between the roles of the x -coordinates and y -coordinates and this turned out to be true in relevant cases. Indeed in Section 3 (mainly by analysing the possible elements of the Galois group $\text{Gal}(K_m/K)$) we prove that $K_m = K(x(P_1), \zeta_m, y(P_1), y(P_2))$ at least for odd $m \geq 5$ and we have (for more precise and general statements see Theorems 3.1 and 3.6)

Theorem 1.2. *If $m \geq 4$, then*

$$K_m = K(x(P_1), \zeta_m, y(P_1), y(P_2)) \implies K_m = K(x(P_1), \zeta_m, y(P_2)) .$$

The set $\{x(P_1), \zeta_m, y(P_2)\}$ seems a good candidate (in general) for a “minimal” set of generators for K_m/K for $m = p$ prime. Indeed Serre’s open image theorem (see, e.g., [6, Appendix C, Theorem 19.1]) tells us to expect $\text{Gal}(K_p/K) \simeq \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ for almost all primes p (for a curve $\mathcal{E}$ without complex multiplication) and there are mild hypothesis (see Theorem 3.14) which lead to

$$[K(x(P_1), \zeta_m, y(P_2)) : K] = (p^2 - 1)(p^2 - p) = |\text{GL}_2(\mathbb{Z}/p\mathbb{Z})| .$$

2010 *Mathematics Subject Classification.* 11G05.

Key words and phrases. Elliptic curves; torsion points.

L. Paladino is supported by the European Commission through the European Social Fund and by Calabria Region.

The final sections are dedicated to the cases $m = 3$ and 4 for which we use the explicit formulas for the torsion points to give more informations on K_m/K , such as its degree and its Galois group.

Acknowledgement. The authors would like to express their gratitude to Antonella Perucca for suggesting the topic of a generalization of the results of [2] and for providing several suggestions, comments and improvements on earlier drafts of this paper.

2. THE IDENTITY $K_m = K(x_1 + x_2, x_1x_2, \zeta_m, y_1)$

As mentioned above we consider an elliptic curve $\mathcal{E}$ defined over a number field K with Weierstrass equation $y^2 = x^3 + Ax + B$ and consider its group of m -torsion points $\mathcal{E}[m]$ ($m > 2$). We fix two points P_1 and P_2 which form a $\mathbb{Z}$ -basis of $\mathcal{E}[m]$ and, to ease notations, from now on we put $x_i := x(P_i)$ and $y_i := y(P_i)$ ($i = 1, 2$). These points are fixed, but it is important to notice that they can be arbitrarily chosen. We define $K_m := K(\mathcal{E}[m])$ and we write $K_{m,x}$ for the extension of K generated by the x -coordinates of the points in $\mathcal{E}[m]$. So we have

$$K(x_1, x_2) \subseteq K_{x,m} \subseteq K_m = K(x_1, x_2, y_1, y_2) .$$

Let $e_m : \mathcal{E}[m] \times \mathcal{E}[m] \rightarrow \mu_m$ be the Weil Pairing, where μ_m is the group of m -th roots of unity. By the properties of e_m , we know that $\mu_m \subseteq K_m$ and our choice of P_1 and P_2 yields $e_m(P_1, P_2) = \zeta_m$ for some primitive m -root of unity ζ_m .

Let (x_3, y_3) be the coordinates of the point $P_3 := P_1 + P_2$ and let (x_4, y_4) be the coordinates of the point $P_4 := P_1 - P_2$. By the group law of $\mathcal{E}$, we may express x_3 and x_4 in terms of x_1, x_2, y_1 and y_2 : indeed

$$(1) \quad x_3 = \frac{(y_1 - y_2)^2}{(x_1 - x_2)^2} - x_1 - x_2 \quad \text{and} \quad x_4 = \frac{(y_1 + y_2)^2}{(x_1 - x_2)^2} - x_1 - x_2 .$$

(note that $x_1 \neq x_2$ because P_1 and P_2 are independent so $P_1 \neq \pm P_2$). By taking the difference of these two equations we get

$$(2) \quad y_1 y_2 = (x_4 - x_3)(x_1 - x_2)^2 / 4 .$$

Lemma 2.1. *We have $K(x_1, x_2, y_1 y_2) = K(x_1, x_2, x_3, x_4)$ and $K_m = K_{m,x}(y_1)$*

Proof. The first field is included in the second by equation (2). Recall that, by the Weierstrass equation, $y_i^2 \in K(x_i)$ for $i = 1, 2$. Then considering equations (1) one proves the other inclusion. For the final statement just note that $K_m = K_{m,x}(y_1, y_2) = K_{m,x}(y_1)$. $\square$

More precisely, we have

Lemma 2.2. *Let $L = K(x_1, x_2)$. Exactly one of the following cases holds:*

- (a) $[K_m : L] = 1$;
- (b) $[K_m : L] = 2$ and $L(y_1 y_2) = K_m$;
- (c) $[K_m : L] = 2$, $L = L(y_1 y_2)$ and $L(y_1) = L(y_2) = K_m$;
- (d) $[K_m : L] = 4$ and $[L(y_1 y_2) : L] = 2$.

Proof. Obviously the degree of K_m over L divides 4. If $[K_m : L] = 1$, then we are in case (a). If $[K_m : L] = 4$, then y_1 and y_2 must generate different quadratic extensions of L and so $[L(y_1 y_2) : L] = 2$ and we are in case (d). If $[K_m : L] = 2$ and $y_1 y_2 \notin L$, then we are in case (b). Now suppose that $[K_m : L] = 2$ and $y_1 y_2 \in L$. Then y_1 and y_2 generate the same extension of L and this extension should be nontrivial, so we are in case (c). $\square$

Proposition 2.3. *We have $K(\zeta_m) \subseteq K(x_1, x_2, y_1 y_2) \subseteq K_{m,x}$.*

Proof. We consider the four cases of Lemma 2.2. Recall that $K(\zeta_m) \subseteq K_m$ and that, by Lemma 2.1, we have $K(x_1, x_2, y_1 y_2) \subseteq K_{m,x}$.

Case (a) or (b): we have $K(x_1, x_2, y_1 y_2) = K_m$ so the statement clearly holds.

Case (c): we have $K_m = L(y_1)$ and $y_1 y_2 \in L$ so the nontrivial element $\tau \in \text{Gal}(K_m/L)$ maps y_i to $-y_i$ for $i = 1, 2$. In particular, $P_i^\tau = -P_i$ for $i = 1, 2$ and so

$$\zeta_m^\tau = e_m(P_1, P_2)^\tau = e_m(P_1^\tau, P_2^\tau) = e_m(-P_1, -P_2) = e_m(P_1, P_2) = \zeta_m$$

hence $\zeta_m \in L = K(x_1, x_2)$.

Case (d): since $K_m = L(y_1, y_2)$ and $\text{Gal}(K_m/L) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, there exists $\tau \in \text{Gal}(K_m/L)$ such that $\tau(y_i) = -y_i$ for $i = 1, 2$. The field fixed by τ is $L(y_1 y_2)$ and, as in the previous case, we get $\zeta_m^\tau = \zeta_m$: so $\zeta_m \in L(y_1 y_2) = K(x_1, x_2, y_1 y_2)$. $\square$

Lemma 2.4. *If $y_1 y_2 \notin K(x_1, x_2)$, then $\zeta_m \notin K(x_1, x_2)$.*

Proof. We are in case (b) or case (d) of Lemma 2.2. We have $[L(y_1 y_2) : L] = 2$ and there exists $\tau \in \text{Gal}(K_m/L)$ such that $(y_1 y_2)^\tau = -y_1 y_2$. Without loss of generality, we may suppose $y_1^\tau = -y_1$ and $y_2^\tau = y_2$ so that $P_1^\tau = -P_1$ and $P_2^\tau = P_2$. Then we have

$$\zeta_m^\tau = e_m(P_1, P_2)^\tau = e_m(P_1^\tau, P_2^\tau) = e_m(-P_1, P_2) = e_m(P_1, P_2)^{-1} = \zeta_m^{-1}.$$

Since $m \neq 2$, we have $\zeta_m^{-1} \neq \zeta_m$ and we get $\zeta_m \notin L$. $\square$

The following theorem generalizes [2, Theorem 2.2].

Theorem 2.5. *We have $K(x_1, x_2, \zeta_m) = K(x_1, x_2, y_1 y_2)$ and $K_m = K(x_1, x_2, \zeta_m, y_1)$.*

Proof. Let $L = K(x_1, x_2)$: by Proposition 2.3, we have $L(\zeta_m) \subseteq L(y_1 y_2)$. So the first assertion is clear if we are in case (a) or in case (c) of Lemma 2.2. In cases (b) and (d) of Lemma 2.2 we have $[L(y_1 y_2) : L] = 2$, $\zeta_m \notin L$ (by Lemma 2.4) and $L(\zeta_m) \subseteq L(y_1 y_2)$. These three properties yield $L(\zeta_m) = L(y_1 y_2)$. The second statement is straightforward. $\square$

We conclude this section with the identity appearing in the title, which still focuses more on the x -coordinates. For that we shall need the following

Lemma 2.6. *The extension $K(x_1, x_2)/K(x_1 + x_2, x_1 x_2)$ has degree ≤ 2 . Its Galois group consists at most of the identity and of an automorphism that swaps x_1 and x_2 .*

Proof. Obviously $K(x_1, x_2) = K(x_1 + x_2, x_1 x_2, x_1 - x_2)$. The equation $(x_1 + x_2)^2 - 4x_1 x_2 = (x_1 - x_2)^2$ shows that the extension has degree at most 2. Moreover, if $\sigma \in \text{Gal}(K_m/K)$ fixes $x_1 + x_2$ and $x_1 x_2$, then it can map $(x_1 - x_2)$ only to $\pm(x_1 - x_2)$, thus σ either fixes or swaps x_1 and x_2 . $\square$

Theorem 2.7. *For $m \geq 3$ we have $K_m = K(x_1 + x_2, x_1 x_2, \zeta_m, y_1)$.*

Proof. We consider the tower of fields (coming from Theorem 2.5)

$$K(x_1 + x_2, x_1 x_2) \subseteq K(x_1, x_2) \subseteq K(x_1, x_2, \zeta_m, y_1) = K_m$$

and adopt the following notations:

$$G := \text{Gal}(K_m/K(x_1 + x_2, x_1 x_2)),$$

$$H := \text{Gal}(K_m/K(x_1, x_2)) \triangleleft G,$$

$$G/H = \text{Gal}(K(x_1, x_2)/K(x_1 + x_2, x_1 x_2)).$$

If we have $K(x_1 + x_2, x_1 x_2) = K(x_1, x_2)$, then the statement clearly holds.

By Lemma 2.6, we may now assume that G/H has order 2 and its nontrivial automorphism swaps

x_1 and x_2 . Then there is at least one element $\tau \in G$ such that $\tau(x_i) = x_j$ and, consequently, $\tau(y_i) = \pm y_j$. The possibilities are:

$$\tau_1 : \begin{cases} P_1 \mapsto P_2 \\ P_2 \mapsto P_1 \end{cases} \quad [-1]\tau_1 : \begin{cases} P_1 \mapsto -P_2 \\ P_2 \mapsto -P_1 \end{cases}$$

both of order 2 and

$$\tau_2 : \begin{cases} P_1 \mapsto P_2 \\ P_2 \mapsto -P_1 \end{cases} \quad [-1]\tau_2 : \begin{cases} P_1 \mapsto -P_2 \\ P_2 \mapsto P_1 \end{cases}$$

of order 4. Note, $\tau_2^2 = [-1]$ fixes both x_1 and x_2 . The automorphisms τ_1 and τ_2 generate a non abelian group of order 8 with two elements of order 4, i.e., the dihedral group

$$D_4 = \langle \tau_1, \tau_2 : \tau_1^2 = \tau_2^4 = \text{Id and } \tau_1\tau_2\tau_1 = \tau_2^3 \rangle.$$

So G is a subgroup of D_4 . Since G/H has order 2, H is isomorphic to either 1, $\mathbb{Z}/2$ or $(\mathbb{Z}/2)^2$ (note that $\tau_2 \notin H$) and its nontrivial elements can at most be the following

$$\tau_1\tau_2 = \tau_2^3\tau_1 : \begin{cases} P_1 \mapsto -P_1 \\ P_2 \mapsto P_2 \end{cases} \quad \tau_2\tau_1 = \tau_1\tau_2^3 : \begin{cases} P_1 \mapsto P_1 \\ P_2 \mapsto -P_2 \end{cases} \quad [-1] : \begin{cases} P_1 \mapsto -P_1 \\ P_2 \mapsto -P_2 \end{cases}.$$

The case $K_m = K(x_1, x_2)$. Since $|H| = 1$ and $|G/H| = 2$, we have $|G| = 2$. The nontrivial automorphism of G has to be τ_1 or $[-1]\tau_1$. In both cases G does not fix ζ_m : so $\zeta_m \in K(x_1, x_2) - K(x_1 + x_2, x_1x_2)$ and we deduce $K(x_1 + x_2, x_1x_2, \zeta_m) = K(x_1, x_2) = K_m$.

The case $[K_m : K(x_1, x_2)] = 4$. Since $|H| = 4$ and $|G/H| = 2$, we have $G \simeq D_4$. The subgroup $\langle \tau_2 \rangle$ of D_4 is normal of index 2 and it does not contain τ_1 . Moreover, τ_2 fixes ζ_m and τ_1 does not. Then we have

$$\text{Gal}(K_m/K(x_1 + x_2, x_1x_2, \zeta_m)) = \langle \tau_2 \rangle \text{ and } [K(x_1 + x_2, x_1x_2, \zeta_m) : K(x_1 + x_2, x_1x_2)] = 2.$$

If $y_1^2 \in K(x_1 + x_2, x_1x_2, \zeta_m)$, then $y_1^2 = \tau_2(y_1)^2 = y_2^2$, giving $y_1 = \pm y_2$. This would imply that $K_m = K(x_1, x_2, y_1)$ has degree 2 over $K(x_1, x_2)$, contradicting the assumptions of this case. Then the degree of the extensions

$$K(x_1 + x_2, x_1x_2) \subset K(x_1 + x_2, x_1x_2, \zeta_m) \subset K(x_1 + x_2, x_1x_2, \zeta_m, y_1)$$

are respectively 2 and at least 4. Since the extension $K_m/K(x_1 + x_2, x_1x_2)$ has degree 8 the statement follows.

The case $[K_m : K(x_1, x_2)] = 2$. Since $|H| = 2$ and $|G/H| = 2$, we have $|G| = 4$. We have to exclude $G = \langle \tau_2\tau_1, [-1] \rangle$, because these automorphisms fix both x_1 and x_2 so we would have $G = H$. We are left with $H = \langle [-1] \rangle$ and one the following two possibilities:

$$G = \langle \tau_2 \rangle \quad \text{or} \quad G = \langle \tau_1, [-1] \rangle.$$

We now consider each of the two subcases separately. Assume $G = \langle \tau_2 \rangle$ and note that $y_1 \neq \pm y_2$: indeed, if $y_1 = \pm y_2$, then τ_2 fixes y_1 or y_2 and so y_1, y_2 are both contained in $K(x_1 + x_2, x_1x_2)$. This yields $K_m = K(x_1, x_2)$, a contradiction. So we know $y_1 \neq \pm y_2$. Then y_1 and y_1^2 are not fixed by any element in G , i.e.,

$$[K(x_1 + x_2, x_1x_2, y_1) : K(x_1 + x_2, x_1x_2)] = 4 \text{ and } K(x_1 + x_2, x_1x_2, y_1) = K_m.$$

Now assume $G = \langle \tau_1, [-1] \rangle$: since τ_1 does not fix ζ_m while $[-1]$ does, we have

$$K(x_1, x_2) = K(x_1 + x_2, x_1x_2, \zeta_m).$$

By Theorem 2.5 we conclude that $K_m = K(x_1 + x_2, x_1x_2, \zeta_m, y_1)$. $\square$

Remark 2.8. The identity $K_2 = K(x_1 + x_2, x_1x_2, \zeta_2, y_1)$ does not hold in general. Indeed it is equivalent to $K_2 = K(x_1 + x_2, x_1x_2)$ and one can take $\mathcal{E} : y^2 = x^3 - 1$ (defined over $\mathbb{Q}$) and the points $\{P_1 = (\zeta_3, 0), P_2 = (\zeta_3^2, 0)\}$ (which form a $\mathbb{Z}$ -basis for $\mathcal{E}[2]$) to get $K_2 = \mathbb{Q}(\mu_3)$ and $\mathbb{Q}(x_1 + x_2, x_1x_2) = \mathbb{Q}$. The equality would hold for any other basis but the previous theorems allow total freedom in the choice of P_1 and P_2 .

3. THE IDENTITY $K_m = K(x_1, \zeta_m, y_2)$

We start by proving that for every odd $m \geq 4$ we have the identity $K_m = K(x_1, \zeta_m, y_1, y_2)$. The cases $m = 2$ and $m = 3$ are treated in Remark 3.3 and Section 4 respectively.

Theorem 3.1. *Let $m \geq 4$, then either $K_m = K(x_1, \zeta_m, y_1, y_2)$ or the following holds: m is even, $K_m/K(x_1, \zeta_m, y_1, y_2)$ is an extension of degree 2 and its Galois group is generated by the element sending P_2 to $\frac{m}{2}P_1 + P_2$. In particular, if $m \geq 4$ is odd, we have $K_m = K(x_1, \zeta_m, y_1, y_2)$ and, if m is even, we get $K_{\frac{m}{2}} \subseteq K(x_1, \zeta_m, y_1, y_2)$.*

Proof. Let $\sigma \in \text{Gal}(K_m/K(x_1, \zeta_m, y_1, y_2))$ and write $\sigma(P_2) = \alpha P_1 + \beta P_2$ for some integers $0 \leq \alpha, \beta \leq m - 1$. Since P_1 and ζ_m are σ -invariant we get

$$\zeta_m = \zeta_m^\sigma = e_m(P_1, P_2)^\sigma = e_m(P_1, P_2^\sigma) = \zeta_m^\beta$$

yielding $\beta = 1$ and so $\sigma(P_2) = \alpha P_1 + P_2$. Since $K_m = K(x_1, \zeta_m, y_1, y_2, x_2)$ and x_2 is a root of $X^3 + AX + B - y_2^2$, the order of σ is at most 3. Assume now that $\sigma \neq \text{Id}$.

If the order of σ is 3: we have

$$P_2 = \sigma^3(P_2) = \sigma^2(\alpha P_1 + P_2) = \sigma(2\alpha P_1 + P_2) = 3\alpha P_1 + P_2$$

hence $3\alpha \equiv 0 \pmod{m}$. Moreover, the three distinct points P_2 , $\sigma(P_2)$ and $\sigma^2(P_2)$ are on the line $y = y_2$. Thus their sum is zero, i.e.,

$$O = P_2 + \sigma(P_2) + \sigma^2(P_2) = 3\alpha P_1 + 3P_2.$$

Since $3\alpha \equiv 0 \pmod{m}$, we deduce $3P_2 = O$, contradicting $m \geq 4$.

If the order of σ is 2: as above $P_2 = \sigma^2(P_2)$ yields $2\alpha \equiv 0 \pmod{m}$. If m is odd this implies $\alpha \equiv 0 \pmod{m}$, i.e., σ is the identity on $\mathcal{E}[m]$, a contradiction. If m is even the only possibility is $\alpha = \frac{m}{2}$.

The last statement for m even follows from the fact that σ acts trivially on $2P_1$ and $2P_2$. $\square$

Corollary 3.2. *Let $p \geq 5$ be an odd prime, then $[K_p : K(\zeta_p, y_1, y_2)]$ is odd.*

Proof. Assume there is a $\sigma \in \text{Gal}(K_p/K(\zeta_p, y_1, y_2))$ of order 2. Since $y_i \neq 0$ (because $p \neq 2$), one has $\sigma(P_i) \neq -P_i$. Then $\sigma(P_i) + P_i$ is a nontrivial p -torsion point lying on the line $y = -y_i$. The point $\sigma(P_i) + P_i$ is on the line $y = -y_i$ so, if $\sigma(P_i) + P_i$ is not a multiple of P_j ($i \neq j$), then we consider the basis $\{P_j, \sigma(P_i) + P_i = (\tilde{x}_i, -y_i)\}$. Now σ is the identity on $K(\zeta_p, \tilde{x}_i, y_i, y_j) = K_p$ (by Theorem 3.1): a contradiction. Therefore $\sigma(P_1) = -P_1 + \beta_1 P_2$ and $\sigma(P_2) = \beta_2 P_1 - P_2$ which, together with $\sigma^2 = \text{Id}$, yield $\beta_1 \beta_2 = 0$. Hence either P_1 or P_2 is mapped to its opposite, a contradiction. $\square$

Remark 3.3. The identity $K_2 = K(x_1, \zeta_2, y_1, y_2)$ does not hold in general. A counterexample is again provided by the curve $\mathcal{E} : y^2 = x^3 - 1$ with $P_1 = (1, 0)$ (as in Remark 2.8 any other choice would yield the equality $K_2 = K(x_1)$).

Theorem 3.4. *Let $p \equiv 2 \pmod{3}$ be an odd prime, then $K_p = K(x_1, y_1, y_2)$ or $K_p = K(x_1, y_1, \zeta_p)$.*

Proof. The degree of x_2 over $K(y_2)$ is at most 3, hence $[K_p : K(x_1, y_1, y_2)] \leq 3$. By Theorem 3.1 we know $K_p = K(x_1, \zeta_p, y_1, y_2)$ and the hypothesis ensures that $[\mathbb{Q}(\zeta_p) : \mathbb{Q}]$ is not divisible by 3, so the same holds for $[K_p : K(x_1, y_1, y_2)]$. Then either $K_p = K(x_1, y_1, y_2)$ or $[K_p : K(x_1, y_1, y_2)] = 2$. If the second case occurs, take the nontrivial element σ of $\text{Gal}(K_p/K(x_1, y_1, y_2))$. Since σ fixes x_1, y_1 and y_2 , its representation in $\text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ (expressing the action of σ on $\mathcal{E}[p]$ with respect to the $\mathbb{Z}$ -basis P_1, P_2) yields

$$\sigma = \begin{pmatrix} 1 & b \\ 0 & d \end{pmatrix} \quad \text{and} \quad \sigma^2 = \begin{pmatrix} 1 & b(1+d) \\ 0 & d^2 \end{pmatrix}.$$

Since p is an odd prime, $\sigma^2 = \text{Id}$ leads either to $d = 1$ (hence $b = 0$ and $\sigma = \text{Id}$, a contradiction) or to $d = -1$. Hence $\sigma(P_2) = bP_1 - P_2$ (with $b \neq 0$ otherwise σ would fix x_2 as well), i.e., bP_1 lies on the line $y = -y_2$. Thus $K(y_2) \subseteq K(x_1, y_1)$ and so $K_p = K(x_1, y_1, \zeta_p)$. $\square$

Corollary 3.5. *Let $p \equiv 2 \pmod{3}$ be an odd prime. Assume there is a nontrivial K -rational p -torsion point P_1 and take any $P_2 \in \mathcal{E}[p] - \mathcal{E}(K)$ (if there is no such P_2 , then $K_p = K$). Then either $K_p = K(\zeta_p)$ or $K_p = K(y_2)$.*

Proof. Just apply Theorem 3.4 to the basis $\{P_1, P_2\}$. $\square$

Theorem 3.6. *If $m \geq 4$ and $K_m = K(x_1, \zeta_m, y_1, y_2)$, then $K_m = K(x_1, \zeta_m, y_2)$.*

Proof. The hypothesis implies $K_m = K(x_1, y_2, \zeta_m)(y_1)$ so $[K_m : K(x_1, y_2, \zeta_m)] \leq 2$. Take $\sigma \in \text{Gal}(K_m/K(x_1, \zeta_m, y_2))$, then $\sigma(x_1) = x_1$ yields $\sigma(P_1) = \pm P_1$. If $\sigma(P_1) = P_1$, then $y_1 \in K(x_1, \zeta_m, y_2)$ and $K_m = K(x_1, \zeta_m, y_2)$. Assume now that $\sigma(P_1) = -P_1$ and let

$$\sigma = \begin{pmatrix} -1 & a \\ 0 & b \end{pmatrix}.$$

Then

$$\zeta_m = \sigma(\zeta_m) = \zeta_m^{-b}$$

yields $b \equiv -1 \pmod{m}$ and

$$\sigma^2 = \begin{pmatrix} 1 & -2a \\ 0 & 1 \end{pmatrix} = \text{Id}$$

leads to $2a \equiv 0 \pmod{m}$.

Case $a \equiv 0 \pmod{m}$: we have $\sigma = [-1]$. Then $\sigma(P_2) = -P_2$, i.e., $\sigma(x_2) = x_2 \in K(x_1, \zeta_m, y_2)$. By Theorem 2.5, this yields $K_m = K(x_1, \zeta_m, y_2)$ and contradicts $\sigma \neq \text{Id}$.

Case $a \equiv \frac{m}{2} \pmod{m}$: we have $\sigma(P_2) = \frac{m}{2}P_1 - P_2$, i.e., $\sigma(P_2) + P_2 - \frac{m}{2}P_1 = O$. Since P_2 and $\sigma(P_2)$ lie on the line $y = y_2$ and are distinct, $-\frac{m}{2}P_1$ must be the third point of $\mathcal{E}$ on that line. Since $-\frac{m}{2}P_1$ has order 2 this yields $y_2 = 0$, contradicting $m \geq 4$. $\square$

To provide generators for a more general m we can use the following result of Reynolds (see [5, Lemma 2.2]).

Lemma 3.7. *Assume that $P \in E(K)$ is not a 2-torsion point and that $\phi : E \rightarrow E$ is a K -rational isogeny with $\phi(R) = P$. Then $K(x(R), y(R)) = K(x(R))$.*

Proof. Put $F = K(x(R))$ and $F' = K(x(R), y(R))$, then $[F' : F] \leq 2$ and we take $\sigma \in \text{Gal}(F'/F)$. Since σ fixes $x(R)$, one has $\sigma(R) = \pm R$. Moreover $\sigma(\phi(R)) - \phi(R) = O$ yields $\phi(\sigma(R) - R) = O$ as well. Now $\sigma(R) = -R$ would yield $O = \phi(-2R) = -2P$ a contradiction to $P \notin \mathcal{E}[2]$. Hence $\sigma(R) = R$ and $F' = F$. $\square$

Lemma 3.8. *If P is a point in $\mathcal{E}(\bar{K})$ and $n \geq 1$, then we have $x(nP) \in K(x(P))$.*

Proof. For any $\sigma \in \text{Gal}(\bar{K}/K(x(P)))$ one has $\sigma(P) = \pm P$ and $\sigma(nP) = \pm nP$. Hence $\sigma(x(nP)) = x(nP)$, i.e., $x(nP) \in K(x(P))$. $\square$

Corollary 3.9. *Let m be divisible by $d \geq 3$ and let R be a point of order m . Then*

$$K(x(R), y(R)) = K\left(x(R), y\left(\frac{m}{d}R\right)\right).$$

In particular, if $K = K(\mathcal{E}[d])$ and if R is a point of order m , then $K(x(R), y(R)) = K(x(R))$.

Proof. Apply the previous lemmas to the field $K(P)$, with $P = \frac{m}{d}R$ and $\phi = [\frac{m}{d}]$. $\square$

Corollary 3.10. *Let $m \geq 5$ be divisible for at least an odd number $d \geq 5$. Then*

$$K_m = K\left(x(P_1), x(P_2), \zeta_d, y\left(\frac{m}{d}P_2\right)\right).$$

Proof. By Corollary 3.9, $K_m = K_d(x(P_1), x(P_2))$. Obviously $\{\frac{m}{d}P_1, \frac{m}{d}P_2\}$ is a $\mathbb{Z}$ -basis for $\mathcal{E}[d]$, hence Theorems 3.1 and 3.6 (applied with $m = d$) yield

$$K_d = K\left(x\left(\frac{m}{d}P_1\right), \zeta_d, y\left(\frac{m}{d}P_2\right)\right).$$

By Lemma 3.8, we have $x(\frac{m}{d}P_1) \in K(x(P_1))$ and the thesis follows. $\square$

The previous result leaves out only integers m of the type $2^s 3^t$. For the case $t = 1$ we mention the following

Proposition 3.11. *The coordinates of the points of order dividing $3 \cdot 2^n$ can be explicitly computed by radicals out of the coefficients of the Weierstrass equation.*

Proof. By the Weierstrass equation, we can compute the y -coordinates out of the x -coordinate. Then by the addition formula, it suffices to compute the x -coordinate of two $\mathbb{Z}$ -independent points of order 3 (done in Section 4), and the x -coordinate of two $\mathbb{Z}$ -independent points of order 2^n (found in Section 5 for $n = 1, 2$). Now it suffices to show that for a point P of order 2^n with $n \geq 3$ the coordinate x_P can be computed out of x_{2P} . Indeed, we have $y_P \neq 0$ (because the order of P is not 2) and so by the duplication formula

$$x_{2P} = \frac{x_P^4 - 2Ax_P^2 - 8Bx_P + A^2}{4y_P^2} = \frac{x_P^4 - 2Ax_P^2 - 8Bx_P + A^2}{4x_P^3 + 4Ax_P + 4B}$$

(a polynomial equation of degree 4 with coefficients coming from the Weierstrass equation). It suffices to solve two such equations, by choosing $2P$ as two generators for $\mathcal{E}[2^{n-1}]$. $\square$

Proposition 3.12. *If $m > 2$ is divisible by 3 (resp. 4), then*

$$K_m = K_{x,m} \cdot L$$

where L is the field generated by the y -coordinates of any two $\mathbb{Z}$ -independent points of order 3 (resp. 4).

Proof. Just apply Corollary 3.9 with $d = 3$ (resp. $d = 4$). $\square$

We conclude this section with some remarks on the Galois group $\text{Gal}(K_p/K)$ for a prime $p \geq 5$, which led us to believe that the generating set $\{x_1, \zeta_p, y_2\}$ is often minimal.

Lemma 3.13. *For any prime $p \geq 5$ one has $[K_p : K(x_1, \zeta_p)] \leq 2p$. Moreover the Galois group $\text{Gal}(K_p/K(x_1, \zeta_p))$ is cyclic, generated by a power of $\eta = \begin{pmatrix} -1 & 1 \\ 0 & -1 \end{pmatrix}$.*

Proof. By Theorem 3.6, $K_p = K(x_1, \zeta_p, y_2)$. Let $\sigma \in \text{Gal}(K_p/K(x_1, \zeta_p))$, then $\sigma(P_1) = \pm P_1$ and $\det(\sigma) = 1$ yield $\sigma = \begin{pmatrix} \pm 1 & \alpha \\ 0 & \pm 1 \end{pmatrix}$ (for some $0 \leq \alpha \leq p-1$). The powers of η are

$$\eta^n = \begin{cases} \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} & \text{if } n \text{ is even} \\ \begin{pmatrix} -1 & n \\ 0 & -1 \end{pmatrix} & \text{if } n \text{ is odd} \end{cases}$$

and its order is obviously $2p$, hence it suffices to show that any such σ is a power of η . One easily checks that, for even α ,

$$\begin{pmatrix} -1 & \alpha \\ 0 & -1 \end{pmatrix} = \eta^{\alpha+p} \quad \text{and} \quad \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} = \eta^{(p-1)\alpha}$$

while, for odd α ,

$$\begin{pmatrix} -1 & \alpha \\ 0 & -1 \end{pmatrix} = \eta^\alpha \quad \text{and} \quad \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix} = \eta^{p-\alpha}.$$

□

Since the p -th division polynomial has degree $\frac{p^2-1}{2}$ and, obviously, $[K(x_1, \zeta_p) : K(x_1)] \leq p-1$ one immediately finds

$$[K(x_1, \zeta_p, y_2) : K] \leq \frac{p^2-1}{2} \cdot (p-1) \cdot 2p = (p^2-1)(p^2-p) = |\text{GL}_2(\mathbb{Z}/p\mathbb{Z})|$$

and can provide conditions for the equality to hold.

Theorem 3.14. *Let $p \geq 5$ be a prime, then $\text{Gal}(K_p/K) \simeq \text{GL}_2(\mathbb{Z}/p\mathbb{Z})$ if and only if the following holds:*

1. $K \cap \mathbb{Q}(\zeta_p) = \mathbb{Q}$;
2. the p -th division polynomial φ_p is irreducible in $K(\zeta_p)[x]$;
3. there exists a basis P_1, P_2 of $\mathcal{E}[p]$ and an element $\eta \in \text{Gal}(K_p/K)$ such that $\eta(P_1) = -P_1$ and $\eta(P_2) = P_1 - P_2$.

Proof. The conditions lead to the equality $[K_p : K] = |\text{GL}_2(\mathbb{Z}/p\mathbb{Z})|$. □

Remark 3.15. By Serre's open image theorem, when $\mathcal{E}$ has no complex multiplication, one expects the equality to hold for almost all primes p . Hence for a general number field K (not containing ζ_p or any coordinate of any generator of $\mathcal{E}[p]$) one expects x_1, y_2 and ζ_p to be a minimal set of generators for K_p over K .

4. NUMBER FIELDS $K(\mathcal{E}[3])$

In this section we generalize the classification of the number fields $\mathbb{Q}(\mathcal{E}[3])$, appearing in [2], to the case when the base field is a general number field K .

We recall that the four x -coordinates of the 3-torsion points of $\mathcal{E}$ are the roots of the polynomial $\varphi_3 := x^4 + 2Ax^2 + 4Bx - A^2/3$. Solving φ_3 with radicals, we get explicit expressions for the x -coordinates and we recall that for $m=3$ being $\mathbb{Z}$ -independent is equivalent to having different x -coordinates. Let $\Delta := -432B^2 - 64A^3$ be the discriminant of the elliptic curve and let

$$\gamma := \frac{\sqrt[3]{-\Delta} - 4A}{3}, \quad \delta := \frac{(-\gamma - 4A)\sqrt{\gamma} - 8B}{\sqrt{\gamma}} \quad \text{and} \quad \delta' := \frac{(-\gamma - 4A)\sqrt{\gamma} + 8B}{\sqrt{\gamma}}$$

(where we have chosen one square root of γ and one cubic root for Δ , since $\zeta_3 \in K_3$ the degree $[K_3 : K]$ will not depend on this choice).

If $B \neq 0$, the roots of φ_3 are

$$x_1 = -\frac{1}{2}(\sqrt{\delta} + \sqrt{\gamma}) \quad , \quad x_2 = \frac{1}{2}(\sqrt{\delta} + \sqrt{\gamma}) \quad , \quad x_3 = -\frac{1}{2}(\sqrt{\delta'} - \sqrt{\gamma}) \quad \text{and} \quad x_4 = \frac{1}{2}(\sqrt{\delta'} - \sqrt{\gamma}) \quad .$$

The corresponding points, by arbitrarily choosing the sign for the y -coordinate, have order 3 and are pairwise $\mathbb{Z}$ -independent. For completeness, we show the expressions of y_1, y_2, y_3 and y_4 in terms of A, B, γ, δ and δ' :

$$y_1 = \sqrt{\frac{(-\gamma\sqrt{\gamma} + 4B)\sqrt{\delta} + \gamma\delta}{4\sqrt{\gamma}}} \quad , \quad y_2 := \sqrt{\frac{(\gamma\sqrt{\gamma} - 4B)\sqrt{\delta} + \gamma\delta}{4\sqrt{\gamma}}} \quad ,$$

$$y_3 = \sqrt{\frac{(-\gamma\sqrt{\gamma} - 4B)\sqrt{\delta'} - \gamma\delta'}{4\sqrt{\gamma}}} \quad \text{and} \quad y_4 = \sqrt{\frac{(\gamma\sqrt{\gamma} + 4B)\sqrt{\delta'} - \gamma\delta'}{4\sqrt{\gamma}}} \quad .$$

If $B = 0$, then $\gamma = 0$ too and the formulas provided above do not hold anymore. The x -coordinates are now the roots of $\varphi_3 = x^4 + 2Ax^2 - A^2/3$. Let

$$\beta := -\left(\frac{2\sqrt{3}}{3} + 1\right)A \quad ,$$

then two solutions of φ_3 are $x_1 = \sqrt{\beta}$ and $x_2 = -\sqrt{\beta}$. Furthermore

$$y_1 = \sqrt{\frac{-2A\sqrt{\beta}}{\sqrt{3}}} = \sqrt{\frac{-2A}{3}} \sqrt{-2A\sqrt{3} - 3A} \quad .$$

Using the results of the previous sections and the explicit formulas, we can now give a “minimal” description of K_3 in terms of generators.

Proposition 4.1. *In any case $K_3 = K(x_1, y_2, y_1)$. Moreover*

1. *if $B \neq 0$, then $K_3 = K(\sqrt{\gamma}, \zeta_3, y_1)$;*
2. *if $B = 0$, then $K_3 = K(\zeta_3, y_1)$.*

Proof. If $B \neq 0$, then

$$y_1^2 + y_2^2 = -4B - \frac{\gamma^2}{2\sqrt{\gamma}} - 2A\sqrt{\gamma} \quad .$$

Therefore $x_1 + x_2 = \sqrt{\gamma} \in K(y_1^2, y_2^2)$ and $x_2 \in K(x_1, y_1^2, y_2^2)$, which immediately yields $K_3 = K(x_1, y_1, y_2)$. Moreover, by Theorem 2.7, $K_3 = K(x_1 + x_2, x_1x_2, \zeta_3, y_1)$ so, since

$$x_1x_2 = \frac{\gamma}{4} + A + \frac{2B}{\sqrt{\gamma}} \in K(x_1 + x_2) = K(\sqrt{\gamma}) \quad ,$$

one has $K_3 = K(\sqrt{\gamma}, \zeta_3, y_1)$.

If $B = 0$, then $x_1 = \sqrt{\beta} = -x_2$ so $K_3 = K(x_1, y_1, y_2)$ is obvious. The final statement follows from $x_1 + x_2 = 0$, $K(x_1x_2) = K(\sqrt{3}) \subseteq K(y_1)$ and Theorem 2.7. $\square$

We shall use the statements of Proposition 4.1 to describe the number fields K_3 in terms of the degree $[K_3 : K]$ and the Galois groups $\text{Gal}(K_3/K)$.

4.1. **The degree** $[K_3 : K]$. Because of the well known embedding $\text{Gal}(K_n/K) \hookrightarrow \text{GL}_2(\mathbb{Z}/n\mathbb{Z})$ one has that $[K_3 : K]$ is a divisor of $|\text{GL}_2(\mathbb{Z}/3\mathbb{Z})| = 48$ (in particular, if $B = 0$, then $K_3 = K(\zeta_3, y_1)$ and y_1 has degree at most 8 over K so $d := [K_3 : K]$ divides 16). Therefore $d \in \Omega := \{1, 2, 3, 4, 6, 8, 12, 16, 24, 48\}$. In [2], we proved that the minimal set for $[\mathbb{Q}(\mathcal{E}[3]) : \mathbb{Q}]$ is $\tilde{\Omega} := \{2, 4, 6, 8, 12, 16, 48\}$. For a general base field K , it is easy to see that the minimal set for d is the whole Ω .

Theorem 4.2. *With notations as above let $d := [K_3 : K]$, then $d \in \Omega$ and this set is minimal. Consider the following conditions for $B \neq 0$*

$$\begin{array}{lll} \text{A1. } \sqrt[3]{\Delta} \notin K; & \text{B1. } \sqrt{\delta} \notin K(\sqrt{\gamma}); & \text{C. } \zeta_3 \notin K(\sqrt{\gamma}, y_1); \\ \text{A2. } \sqrt{\gamma} \notin K(\sqrt[3]{\delta}); & \text{B2. } y_1 \notin K(\sqrt{\delta}); & \end{array}$$

and the corresponding ones for $B = 0$

$$\begin{array}{ll} \text{D1. } \sqrt{3} \notin K; & \text{E. } \zeta_3 \notin K(y_1); \\ \text{D2. } \sqrt{\beta} \notin K(\sqrt{3}); & \\ \text{D3. } y_1 \notin K(\sqrt{\beta}). & \end{array}$$

Then the degrees are the following (the conditions not appearing in the third and sixth column are assumed not to hold, obviously $d = 1 \iff$ none of the conditions hold)

B	d	holding conditions	B	d	holding conditions
$B \neq 0$	48	A1, A2, B1, B2, C	$B \neq 0$	4	A2, B1
$B \neq 0$	24	A1, B1, B2, C	$B \neq 0$	4	A2, B2
$B \neq 0$	24	A1, A2, B1, B2	$B \neq 0$	4	B1, B2
$B \neq 0$	16	A2, B1, B2, C	$B \neq 0$	3	A1
$B \neq 0$	12	A1, A2, B1	$B \neq 0$	2	<i>1 among A2, B1, B2</i>
$B \neq 0$	12	A1, A2, B2	$B = 0$	16	D1, D2, D3, E
$B \neq 0$	12	A1, B1, B2	$B = 0$	8	D2, D3, E
$B \neq 0$	8	B1, B2, C	$B = 0$	4	D1, D3
$B \neq 0$	8	A2, B1, B2	$B = 0$	4	D2, D3
$B \neq 0$	6	A1 and 1 among A2, B1, B2	$B = 0$	2	D1
			$B = 0$	2	D3

Proof. Everything follows from Proposition 4.1 and the explicit description of the generators of K_3 , just note that all conditions (except **A1** which provides an extension of degree 3) yield extensions of degree 2. We remark that not all possible combinations appear in the table because there are certain relations between the conditions. Indeed, for $B = 0$, condition **D2** implies condition **D3** (since $y_1 = \sqrt{\frac{2A}{\sqrt{3}}} \sqrt[4]{\beta}$), while, if **D2** does not hold, then $x_1 \in K(\sqrt{3})$ and $x_3 =$

$\sqrt{\left(\frac{2\sqrt{3}}{3} - 1\right)A} \in K(\sqrt{3})$ as well. Since $x_1 x_3 = \frac{A\sqrt{-3}}{3}$, this implies that **E** does not hold.

In the same way one sees that if **B1** does not hold then δ and δ' are both squares in $K(\sqrt{\gamma})$. Therefore $x_i \in K(\sqrt{\gamma})$ for $1 \leq i \leq 4$ and, by Proposition 2.3, $\zeta_3 \in K(\sqrt{\gamma})$ as well, i.e., **C** does not hold. Moreover if **B2** does not hold, then y_1^2 , which is of the form $u + v\sqrt{\delta}$ for some $u, v \in K(\sqrt{\gamma})$, is a square in $K(\sqrt{\delta})$, hence $y_2^2 = u - v\sqrt{\delta}$ is a square as well. In this case we have $\sqrt{\gamma}, \sqrt{\delta}, y_1, y_2 \in K(\sqrt{\delta})$, i.e., $K_3 = K(x_1, y_1, y_2) = K(\sqrt{\delta})$ (in particular again **C** does not hold). The only thing left to prove is that for every d , there exists an elliptic curve with $[K_3 : K] = d$. In [2], we have already shown explicit examples of such curves when $d \neq 1, 3$ and 24. For

the remaining ones it suffices to take examples from there with $d = 2, 6$ and 48 and put $K = \mathbb{Q}(\zeta_3)$. $\square$

4.2. Galois groups. We now list all possible Galois groups $\text{Gal}(K_3/K)$ via a case by case analysis (one can easily connect a Galois group to the conditions in Theorem 4.2, so we do not write down a summarizing statement here).

4.2.1. $\mathbf{B} = \mathbf{0}$. The degree $[K_3 : K]$ divides 16 hence $\text{Gal}(K_3/K)$ is a subgroup of the 2-Sylow subgroup of $\text{GL}_2(\mathbb{Z}/3\mathbb{Z})$ which is isomorphic to SD_8 (the semidihedral group of order 16). Hence, if $d = 16$, $\text{Gal}(K_3/K) \simeq SD_8$ and, by [2, Theorem 3.1], it is generated by the elements

$$\varphi_{6,1} \begin{cases} y_1 \mapsto y_3 \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{cases} \quad \text{and} \quad \varphi_{2,1} \begin{cases} y_1 \mapsto y_1 \\ \sqrt{-3} \mapsto -\sqrt{-3} \end{cases}$$

(here and in what follows the notations for the $\varphi_{i,j}$ are taken from [2, Appendix A]).

Obviously if $d = 2$, then $\text{Gal}(K_3/K) \simeq \mathbb{Z}/2\mathbb{Z}$ and $d = 1$ yields a trivial group. Hence we are left with $d = 4$ and 8 .

If $d = 8$: then $\sqrt{3} \in K$ but $\sqrt{-3} \notin K$ which yields $i \notin K$. Letting φ be any element of the Galois group one has $\varphi(y_1^2) = \pm y_1^2$, i.e., $\varphi(y_1) = \pm y_1, \pm i y_1$. Then

$$\text{Gal}(K_3/K) = \langle \varphi_{6,1}^2, \varphi_{2,1} : \varphi_{6,1}^8 = \varphi_{2,1}^2 = \text{Id}, \varphi_{2,1} \varphi_{6,1}^2 \varphi_{2,1} = \varphi_{6,1}^6 \rangle \simeq D_4$$

(the dihedral group of order 8).

If $d = 4$: then there are two cases

- a.** $\sqrt{3} \notin K$, $\sqrt{\beta}, \zeta_3 \in K(\sqrt{3})$ and $y_1 \notin K(\sqrt{3})$, or
- b.** $\sqrt{3} \in K$, $[K(y_1) : K] = 4$ and $\zeta_3 \in K(y_1)$.

In case **a** there are elements sending $\sqrt{3}$ to $-\sqrt{3}$, hence x_1 to x_3 and y_1^2 to $\pm y_3^2$. There are no such elements of order 2, so $\text{Gal}(K_3/K) \simeq \mathbb{Z}/4\mathbb{Z}$ and it is generated by $\varphi_{6,1} \varphi_{2,1}$ or $\varphi_{6,1}^3 \varphi_{2,1}$ (note that both fix ζ_3 hence one can also deduce that this case happens if ζ_3 belongs to K and i does not).

In case **b** (as in $d = 8$) one has $\varphi(y_1^2) = \pm y_1^2$: if $\zeta_3 \in K$, then $i \in K$ as well and the Galois group is $\langle \varphi_{6,1}^2 \rangle \simeq \mathbb{Z}/4\mathbb{Z}$. If $\zeta_3 \notin K$, then the Galois group must contain elements moving i and, among them, the ones sending y_1^2 to $\pm y_1^2$ all have order 2. Therefore $\text{Gal}(K_3/K) \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and the generators are $\{\varphi_{6,1}^4, \varphi_{2,1}\}$ or $\{\varphi_{6,1}^4, \varphi_{2,1} \varphi_{6,1}^6\}$.

4.2.2. $\mathbf{B} \neq \mathbf{0}$. The degree is a divisor of 48. Looking at the subgroups of $\text{GL}_2(\mathbb{Z}/3\mathbb{Z})$ one sees that certain orders do not leave any choice: indeed $d = 1, 2, 3, 12, 16, 24$ and 48 give $\text{Gal}(K_3/K) \simeq \text{Id}, \mathbb{Z}/2\mathbb{Z}, \mathbb{Z}/3\mathbb{Z}, D_6, SD_8, \text{SL}_2(\mathbb{Z}/3\mathbb{Z})$ and $\text{GL}_2(\mathbb{Z}/3\mathbb{Z})$ respectively. The remaining orders are $d = 4, 6$ and 8 .

If $d = 8$: then there are two cases

- a.** $K = K(\sqrt{\gamma})$, $[K(y_1) : K] = 4$ and $K_3 = K(y_1, \zeta_3)$, or
- b.** $K = K(\sqrt[3]{\delta})$ and $K_3 = K(\sqrt{\gamma}, y_1)$.

In case **a**, since all elements of the Galois group fix $\sqrt{\gamma}$, one has $\varphi(\sqrt{\delta}) = \pm \sqrt{\delta}$, which yields $\varphi(y_1) \in \{\pm y_1, \pm y_2\}$. Therefore φ has order 1, 2 or 4 and, since $(\mathbb{Z}/2\mathbb{Z})^3$ is not a subgroup of $\text{GL}_2(\mathbb{Z}/3\mathbb{Z})$, we have some elements of order 4 (the ones with $\varphi(y_1) = \pm y_2$). Moreover there is $\sigma \in \text{Gal}(K_3/K(y_1))$ with $\sigma(\zeta_3) = \zeta_3^2$. Note that in this case $x_1 \in K(y_1)$ so $y_2 \notin K(y_1)$ (otherwise

$K_3 = K(y_1)$ by Proposition 4.1, a contradiction to $[K_3 : K] = 8$, hence $\sigma(y_2) = -y_2$. Now it is easy to check that $\text{Gal}(K_3/K) = \langle \varphi, \sigma : \varphi^4 = \sigma^2 = \text{Id}, \sigma\varphi\sigma = \varphi^3 \rangle \simeq D_4$, with

$$\varphi \begin{cases} y_1 \mapsto y_2 \\ \zeta_3 \mapsto \zeta_3 \end{cases} \quad \text{and} \quad \sigma \begin{cases} y_1 \mapsto y_1 \\ \zeta_3 \mapsto \zeta_3^2 \end{cases}.$$

In case **b**, since $\sqrt{\gamma}$ is no longer fixed, $\varphi(\delta) \in \{\delta, \delta'\}$ and therefore the image of y_1 can be any of the other y_i 's. Moreover, once $\varphi(\sqrt{\gamma})$ and $\varphi(\sqrt{\delta})$ are fixed, $\varphi(y_1) = \pm y_i$ yields $\varphi(y_i) = \pm y_1$ so, again, we have no elements of order 8 (and, as above, they cannot all be of order 2). Since there is no “special” y coordinate, all elements with $\varphi(y_1) = y_i$ ($i \neq 1$) have order 4 and $\text{Gal}(K_3/K)$ is the quaternion group Q_8 with generators of order 4

$$\varphi_2 \begin{cases} y_1 \mapsto y_2 \\ \sqrt{\gamma} \mapsto \sqrt{\gamma} \end{cases}, \quad \varphi_3 \begin{cases} y_1 \mapsto y_3 \\ \sqrt{\gamma} \mapsto -\sqrt{\gamma} \end{cases} \quad \text{and} \quad \varphi_4 \begin{cases} y_1 \mapsto y_4 \\ \sqrt{\gamma} \mapsto -\sqrt{\gamma} \end{cases},$$

and the element

$$\varphi_1 \begin{cases} y_1 \mapsto -y_1 \\ \sqrt{\gamma} \mapsto \sqrt{\gamma} \end{cases}$$

of order 2.

If $d = 6$: then there is the cubic extension $K(\sqrt[3]{\Delta})$ and K_3 must contain its Galois closure. Hence if $\zeta_3 \in K$, we have $\text{Gal}(K_3/K) \simeq \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$, otherwise $K_3 = K(\sqrt[3]{\Delta}, \zeta_3)$ with $\text{Gal}(K_3/K) \simeq S_3$.

If $d = 4$: then there are three cases

- a.** $K = K(\sqrt[3]{\Delta})$ and $K_3 = K(\sqrt{\delta})$, or
- b.** $K = K(\sqrt[3]{\Delta})$ and $K_3 = K(\sqrt{\gamma}, y_1)$, or
- c.** $K = K(\sqrt{\gamma})$ and $K_3 = K(y_1)$.

In all these cases K_3 contains a quadratic subextension K' which is $K(\sqrt{\gamma})$ (cases **a** and **b**) or $K(\sqrt{\delta})$ (case **c**). If $\zeta_3 \notin K'$ then $K_3 = K'(\zeta_3)$ and $\text{Gal}(K_3/K') \simeq \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. If $\zeta_3 \in K'$, then K' is the unique quadratic subextension, $\text{Gal}(K_3/K)$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ and it is generated by

$$\mathbf{a} : \varphi \begin{cases} \sqrt{\gamma} \mapsto -\sqrt{\gamma} \\ \sqrt{\delta} \mapsto \sqrt{\delta'} \end{cases}, \quad \mathbf{b} : \varphi \begin{cases} \sqrt{\gamma} \mapsto -\sqrt{\gamma} \\ y_1 \mapsto y_3 \end{cases} \quad \text{or} \quad \mathbf{c} : \varphi \begin{cases} \sqrt{\delta} \mapsto -\sqrt{\delta} \\ y_1 \mapsto y_2 \end{cases}.$$

5. NUMBER FIELDS $K(\mathcal{E}[4])$

In this section we briefly describe the case $m = 4$. Let α, β and γ be the roots of $x^3 + Ax + B = 0$. These roots are the abscissas of the points of order 2 of $\mathcal{E}$. The points of exact order 4 of $\mathcal{E}$ are

$\pm P_1, \pm P_2, \pm P_3, \pm P_4, \pm P_5, \pm P_6$, where

$$\begin{aligned} P_3 &= (\alpha - \sqrt{(\alpha - \beta)(\alpha - \gamma)}, (\alpha - \beta)\sqrt{\alpha - \gamma} - (\alpha - \gamma)\sqrt{\alpha - \beta}), \\ P_4 &= (\beta - \sqrt{(\beta - \alpha)(\beta - \gamma)}, (\beta - \alpha)\sqrt{\beta - \gamma} - (\beta - \gamma)\sqrt{\beta - \alpha}), \\ P_5 &= \left(\gamma + \sqrt{(\alpha - \gamma)(\beta - \gamma)}, \frac{(\alpha - \gamma)(\beta - \gamma)}{\sqrt{\gamma - \alpha}} + \frac{(\alpha - \gamma)(\beta - \gamma)}{\sqrt{\gamma - \beta}} \right), \\ P_6 &= \left(\gamma - \sqrt{(\alpha - \gamma)(\beta - \gamma)}, \frac{(\alpha - \gamma)(\beta - \gamma)}{\sqrt{\gamma - \alpha}} - \frac{(\alpha - \gamma)(\beta - \gamma)}{\sqrt{\gamma - \beta}} \right). \end{aligned}$$

In particular, the points $P_1 = (\alpha + \sqrt{(\alpha - \beta)(\alpha - \gamma)}, (\alpha - \beta)\sqrt{\alpha - \gamma} + (\alpha - \gamma)\sqrt{\alpha - \beta})$ and $P_2 = (\beta + \sqrt{(\beta - \alpha)(\beta - \gamma)}, (\beta - \gamma)\sqrt{\beta - \alpha} + (\beta - \alpha)\sqrt{\beta - \gamma})$ form a basis of the 4-torsion subgroup of $\mathcal{E}$. With the explicit formulas for the coordinates of the 4-torsion points it's easy to see that $K_4 = K(\sqrt{-1}, \sqrt{\alpha - \beta}, \sqrt{\beta - \gamma}, \sqrt{\gamma - \alpha})$ (see [3]). Another quick way to find this extension is by applying Theorem 2.5.

5.1. The degree $[K_4 : K]$. By definition $K(\alpha, \beta)$ is the splitting field of $x^3 + Ax + B$, hence $[K(\alpha, \beta) : K] \leq 6$. Then $K_4 = K(\sqrt{\alpha - \beta}, \sqrt{\alpha - \gamma}, \sqrt{\beta - \gamma}, i)$ has degree at most $16 \cdot [K(\alpha, \beta) : K] \leq 96$ which is, as expected, the cardinality of $\text{GL}_2(\mathbb{Z}/4\mathbb{Z})$.

Theorem 5.1. *Let K be a number field and let $\mathcal{E}$ be an elliptic curve with Weierstrass form $y^2 = x^3 + Ax + B$ defined over K . Let K' be the splitting field of $x^3 + Ax + B$: put $d' := [K' : K]$ and $d := [K_4 : K]$. Consider the conditions*

$$\begin{aligned} \text{A1. } & \sqrt{\alpha - \beta} \notin K', & \text{A2. } & \sqrt{\alpha - \gamma} \notin K'(\sqrt{\alpha - \beta}), \\ \text{A3. } & \sqrt{\beta - \gamma} \notin K'(\sqrt{\alpha - \beta}, \sqrt{\alpha - \gamma}), & \text{A4. } & i \notin K(\sqrt{\alpha - \beta}, \sqrt{\alpha - \gamma}, \sqrt{\beta - \gamma}). \end{aligned}$$

Then the degrees are the following (the conditions not appearing in the third and sixth column are assumed not to hold, obviously $d = 1 \iff d' = 1$ and none of the conditions hold)

d	d'	holding conditions	d	d'	holding conditions
96	6	A1, A2, A3, A4	12	3	<i>2 among A1, A2, A3, A4</i>
48	6	<i>3 among A1, A2, A3, A4</i>	8	2	<i>2 among A1, A2, A3, A4</i>
48	3	A1, A2, A3, A4	8	1	<i>3 among A1, A2, A3, A4</i>
32	2	A1, A2, A3, A4	6	6	<i>none</i>
24	6	<i>2 among A1, A2, A3, A4</i>	6	3	<i>1 among A1, A2, A3, A4</i>
24	3	<i>3 among A1, A2, A3, A4</i>	4	2	<i>1 among A1, A2, A3, A4</i>
16	2	<i>3 among A1, A2, A3, A4</i>	4	1	<i>2 among A1, A2, A3, A4</i>
16	1	A1, A2, A3, A4	3	3	<i>none</i>
12	6	<i>1 among A1, A2, A3, A4</i>	2	2	<i>none</i>
			2	1	<i>1 among A1, A2, A3, A4</i>

Proof. The computations are straightforward (any of the conditions provides a degree 2 extension). $\square$

We provide some examples over $\mathbb{Q}$ which describe the cases $A = 0$ or $B = 0$ and a few more (obviously, since $i \in \mathbb{Q}_4 = \mathbb{Q}(\mathcal{E}[4])$ we cannot obtain extension of degree 1 or 3).

Example 5.2. A=0. Consider, for example, $\mathcal{E} : y^2 = x^3 - 25$: it is easy to see that $\mathbb{Q}' = \mathbb{Q}(\zeta_3, \sqrt[3]{5})$ and

$$\mathbb{Q}_4 = \mathbb{Q}(\zeta_3, \sqrt[3]{5}, i, \sqrt{1 - \zeta_3}).$$

Looking at ramification of primes (over 2, 3 and 5) and with some direct computations, one finds $[\mathbb{Q}_4 : \mathbb{Q}] = 24$. In general, the same computations for $\mathcal{E} : y^2 = x^3 - B$ lead to

$$\mathbb{Q}_4 = \mathbb{Q}(\zeta_3, \sqrt[3]{B}, i, \sqrt{1 - \zeta_3}) .$$

Hence, if we exclude obvious particular cases like $B \in (\mathbb{Q}^*)^3$, the degree turns out to be 24 (i.e., seems to be “almost” independent from B).

Example 5.3. B=0. For $\mathcal{E} : y^2 = x^3 + Ax$ we have a rational root, hence we can only obtain degrees which are a power of 2.

The curve $\mathcal{E} : y^2 = x^3 - 9x$ (A is the opposite of a square in $\mathbb{Q}$), with $\alpha = 0$, $\beta = 3$ and $\gamma = -3$, yields

$$\mathbb{Q}' = \mathbb{Q} \quad \text{and} \quad \mathbb{Q}_4 = \mathbb{Q}(\sqrt{3}, \sqrt{2}, i)$$

with $[\mathbb{Q}_4 : \mathbb{Q}] = 8$.

The curve $\mathcal{E} : y^2 = x^3 - 4x$ (again the opposite of a square, but 2 has a special role as one sees looking at $\sqrt{\beta - \gamma}$) yields

$$\mathbb{Q}' = \mathbb{Q} \quad \text{and} \quad \mathbb{Q}_4 = \mathbb{Q}(\sqrt{2}, i)$$

with $[\mathbb{Q}_4 : \mathbb{Q}] = 4$.

The curve $\mathcal{E} : y^2 = x^3 - 3x$ (A is not a square in $\mathbb{Q}$) yields

$$\mathbb{Q}' = \mathbb{Q}(\sqrt{3}) \quad \text{and} \quad \mathbb{Q}_4 = \mathbb{Q}(\sqrt{2}, \sqrt[4]{3}, i)$$

with $[\mathbb{Q}_4 : \mathbb{Q}] = 16$.

We give a few more examples just to complete the list of 2-powers degrees. The remaining degrees (divisible by 3), are harder to obtain (over $\mathbb{Q}$) because of the formulas for the roots of $x^3 + Ax + B$; obviously they should be easily accessible via computer calculation.

Example 5.4. The curve

$$y^2 = x^3 - \frac{481}{3}x + \frac{9658}{27} = \left(x - \frac{34}{3}\right) \left(x - \frac{7}{3}\right) \left(x + \frac{41}{3}\right)$$

provides $\sqrt{\alpha - \beta} = 3$, $\sqrt{\alpha - \gamma} = 5$ and $\sqrt{\beta - \gamma} = 4$. Hence $\mathbb{Q}_4 = \mathbb{Q}(i)$ has degree 2 over $\mathbb{Q}$.

The curve

$$y^2 = x^3 - 22x - 15 = (x - 5)(x^2 + 5x + 3)$$

yields

$$\mathbb{Q}' = \mathbb{Q}(\sqrt{13}) \quad \text{and} \quad \mathbb{Q}_4 = \mathbb{Q} \left(\sqrt{\frac{5 + \sqrt{13}}{2}}, \sqrt{\frac{5 - \sqrt{13}}{2}}, \sqrt[4]{5}, i \right)$$

which has degree 32 over $\mathbb{Q}$ (again by means of ramification and direct computations).

5.2. Galois groups. One can find descriptions for $\text{GL}_2(\mathbb{Z}/4\mathbb{Z})$ in [1, Section 5.1] or [4, Section 3]: the most suitable for our goals is the exact sequence coming from the canonical projection $\text{GL}_2(\mathbb{Z}/4\mathbb{Z}) \rightarrow \text{GL}_2(\mathbb{Z}/2\mathbb{Z})$ whose kernel we denote by H_2^4 . Obviously

$$H_2^4 = \left\{ \begin{pmatrix} 1 + 2a & 2b \\ 2c & 1 + 2d \end{pmatrix} \in \text{GL}_2(\mathbb{Z}/4\mathbb{Z}) \right\}$$

and it is easy to check that it is an abelian group of order 16 and exponent 2, i.e., isomorphic to $(\mathbb{Z}/2\mathbb{Z})^4$. Thanks to the natural embedding $\text{GL}_2(\mathbb{Z}/2\mathbb{Z}) \hookrightarrow \text{GL}_2(\mathbb{Z}/4\mathbb{Z})$, the sequence

$$H_2^4 \hookrightarrow \text{GL}_2(\mathbb{Z}/4\mathbb{Z}) \twoheadrightarrow \text{GL}_2(\mathbb{Z}/2\mathbb{Z})$$

splits and, for any K , we have a commutative diagram

$$\begin{array}{ccccc} H_2^4 & \hookrightarrow & \mathrm{GL}_2(\mathbb{Z}/4\mathbb{Z}) & \twoheadrightarrow & \mathrm{GL}_2(\mathbb{Z}/2\mathbb{Z}) \\ \downarrow & & \downarrow & & \downarrow \\ \mathrm{Gal}(K_4/K') & \hookrightarrow & \mathrm{Gal}(K_4/K) & \twoheadrightarrow & \mathrm{Gal}(K'/K) . \end{array}$$

The structure of $\mathrm{Gal}(K_4/K)$ can be derived from the lower sequence (which splits as well) checking the conditions of Theorem 5.1 to compute d' (which immediately identifies $\mathrm{Gal}(K'/K)$ as one among Id , $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/3\mathbb{Z}$ or S_3) and the $i \in \{0, \dots, 4\}$ for which $\mathrm{Gal}(K_4/K') \simeq (\mathbb{Z}/2\mathbb{Z})^i$.

REFERENCES

- [1] C. ADELMANN, *The decomposition of primes in torsion point fields*, Lecture Notes in Mathematics, 1761. Springer-Verlag, Berlin, 2001.
- [2] A. BANDINI - L. PALADINO, *Number fields generated by the 3-torsion points of an elliptic curve*, Monatshefte für Mathematik **168** (2012), 157–181.
- [3] DVORNICICH R., ZANNIER U., *An analogue for elliptic curves of the Grunwald-Wang example*, C. R. Acad. Sci. Paris, Ser. I **338** (2004), 47-50.
- [4] C. HOLDEN, *Mod 4 Galois representations and elliptic curves*, Proc. Amer. Math. Soc. **136**, no. 1 (2008), 31–39.
- [5] J. REYNOLDS, *On the pre-image of a point under an isogeny and Siegel's theorem*, New York J. Math. **17** (2011), 163–172.
- [6] J.H. SILVERMAN, *The arithmetic of elliptic curves, 2nd edition*, **GTM 106** Springer-Verlag, Heidelberg, 2009.

DIPARTIMENTO DI MATEMATICA E INFORMATICA, UNIVERSITÀ DEGLI STUDI DI PARMA, PARCO AREA DELLE SCIENZE, 53/A - 43124 PARMA (PR), ITALY

E-mail address: andrea.bandini@unipr.it

DIPARTIMENTO DI MATEMATICA E INFORMATICA- UNIVERSITÀ DELLA CALABRIA, PONTE PIETRO BUCCI - CUBO 31 B - 87036 ARCAVACATA DI RENDE (CS) - ITALY

E-mail address: paladino@mat.unical.it