Radical Isogenies

Frederik Vercauteren, joint work with Wouter Castryck and Thomas Decru

imec-COSIC, KU Leuven, Belgium

Radical isogenies are a novel approach to computing isogenies which is efficient for chains of **small degree** N isogenies, such as required in CSIDH [4]. As such it is complementary to the Vélu-sqrt approach described in [1] which only requires $\widetilde{O}(\sqrt{\ell})$ operations in $\mathbb{F}_p$ instead of $O(\ell)$ and is most efficient for larger degree isogenies, say degree > 100.

Radical isogenies are given by explicit formulae, are deterministic and completely avoid generating N-torsion points. Given an elliptic curve E with a point P of order N, one can use Vélu's formulae to compute a defining equation for $E' = E/\langle P \rangle$. Radical isogenies then give formulae for the coordinates of a point P' on E' again of order N, such that the composition

$$E \to E' \to E'/\langle P' \rangle \tag{1}$$

is a cyclic isogeny of degree N^2. These formulae are algebraic expressions in the coefficients of E and the coordinates of P, and one radical (an Nth root) of another algebraic expression in the coefficients of E and the coordinates of P.

An important implication of this construction is that the same formulae now apply to E' and P', which allows us to compute chains of N-isogenies of arbitrary length without needing to generate an N-torsion point in every step.

To derive these formulae you will use the following approach:

1. Is there a natural parametrized elliptic curve model that represents an elliptic curve together with an N-torsion point (wlog we can assume the point P to be $(0,0)$)? If so, we can use this model to derive explicit formulae that depend on the parameters of the model.
   Approach: To solve this, we will use the Tate normal form
   $$E : y^2 + (1-c)xy - by = x^3 - bx^2 \qquad P = (0,0),\ b, c \in K\,.$$
   which represents an elliptic curve E over a field K together with a K-rational point $P = (0,0)$ of order $N \geq 4$. The fact that P has order exactly N imposes an algebraic relation between b, c which we denote $F_N(b,c) = 0$. Define $\mathbb{Q}_N(b,c)$ the function field of the curve $F_N(b,c)$, i.e.
   $$\mathbb{Q}_N(b,c) := \mathrm{Frac}\,\frac{\mathbb{Q}[b,c]}{(F_N(b,c))}\,.$$
2. Given such a model, we will derive an equation for $E' = E/\langle P \rangle$.
   Approach: Use Vélu's formulae to derive an explicit equation for the curve E'. This step is straightforward.

3. Given the equation for E' we can now look for an N-torsion point P' on E', such that
$$E \to E' \to E'/\langle P' \rangle \tag{2}$$
is a cyclic isogeny of degree N^2. This simply means that the kernel of the composition has to be generated by a single N^2-torsion point on E (and not e.g. full N-torsion).
Approach: You will show that the point P' has to satisfy
$$\hat{\varphi}(P') = \lambda P \text{ for some } \lambda \in (\mathbb{Z}/N)^*, \tag{3}$$
with $\hat{\varphi} : E' \to E$ the dual of φ.
4. Since we know the equation of E' explicitly, and we are looking for an N-torsion point on E', satisfying the above equation, how will we find it?
Approach: Find a root of the N-th division polynomial on E', which by definition has as its roots the x-coordinates of the N-torsion points. Note that E' is parametrized by (b, c), the parameters of E, and thus the N-th division polynomial has coefficients which are also parametrized by (b, c).
5. We can factor the N-th division polynomial over $\mathbb{Q}_N(b, c)$, but this typically results in a product of irreducible factors of degree > 1. To find a correct root, we need to determine the correct factor of the N-th division polynomial, and we also have to determine the smallest algebraic extension of $\mathbb{Q}_N(b, c)$ where such a root is defined.
Approach: We show that it is sufficient to adjoin a single N-th root of an algebraic expression in (b, c). More in detail, the central observation is that P' is defined over $\mathbb{Q}_N(b, c, \sqrt[N]{\rho}\,)$ for some $\rho \in \mathbb{Q}_N(b, c)$ and we prove that one can take $\rho = t_N(P, -P)$ where t_N denotes the Tate pairing.
6. Once we know the correct field extension, we can explicilty find a root of (a factor of) the division polynomial defined over this extension. This root gives the x-coordinate of P' explicitly, and the y-coordinate follows easily by solving a degree 2 equation coming from the curve equation.
Approach: Use a standard root finding algorithm.
7. The fact that we only require one Nth root explains the name "radical isogenies". By rewriting (E', P') again in Tate normal form with coefficients b' and c', we are ready for another iteration. The formulae we derive in fact express b' and c' directly as elements of $\mathbb{Q}_N(b, c, \sqrt[N]{\rho}\,)$, and can simply be applied as many times as required without the need to generate N-torsion points explicitly as one would do in the more classical approaches.
Approach: Move the point P' to $(0, 0)$ again and transform the curve into Tate normal form. This gives the new b', c' which can be repeated indefinitely.

An important application is where we apply these formula for an elliptic curve over a finite field $\mathbb{F}_q$, with $\gcd(q - 1, N) = 1$. In this case, we immediately obtain that the radical $\sqrt[N]{\rho}$ is again defined over $\mathbb{F}_q$, since Nth powering is a field automorphism in this case. This can be applied in the setting of CSIDH, since there we need to take a number of steps in one direction, i.e. a cyclic isogeny.

We will now proceed to go through each of these steps to derive explicit radical isogenies for the case $N = 5$.

1 Step 1: The Tate normal form

We will be interested in elliptic curves E over K with a distinguished point $P \in E(K)$ of some finite order N. By translating this point to $(0,0)$ and requiring that the tangent line is horizontal, and with proper scaling, one can easily prove the following lemma.

Lemma 1. *Let E be an elliptic curve over K and let $P \in E(K)$ be a point of order $N \geq 4$, then (E, P) is isomorphic to a unique pair of the form*

$$E : y^2 + (1-c)xy - by = x^3 - bx^2, \qquad P = (0,0) \tag{4}$$

with $b, c \in K$ and

$$\Delta(b,c) = b^3(c^4 - 8bc^2 - 3c^3 + 16b^2 - 20bc + 3c^2 + b - c) \neq 0\,.$$

Exercise 1 *Prove the above lemma, i.e. that (b,c) are unique given that $P = (0,0)$.*

The resulting curve-point pair is said to be in Tate normal form.

Exercise 2 *Using your favorite computer algebra package, show that on the Tate normal form, the first few scalar multiples of $P = (0,0)$ are given by simple expressions in b and c, e.g.*

$$2P = (b, bc),\ 3P = (c, b-c), \qquad -P = (0,b),\ -2P = (b,0),\ -3P = (c, c^2)\,.$$

Using these multiples, for each $N \geq 4$ one can write down an irreducible polynomial $F_N(b,c) \in \mathbb{Z}[b,c]$ whose vanishing, along with the non-vanishing of $\Delta(b,c)$ and of $F_m(b,c)$ for $4 \leq m < N$, expresses that P has exact order N.

Exercise 3 *Using the previous exercise, show that the first few values of F_N are given by $F_4(b,c) = c = 0$, $F_5(b,c) = c - b = 0$ and $F_6(b,c) = c^2 + c - b = 0$.*

Alternatively, the polynomial $F_N(b,c)$ can be recovered as a factor of the constant term of the N-division polynomial (see Step 4 for their definition) of the curve (4), when considered over the rational function field $\mathbb{Q}(b,c)$. This is the approach taken in [9, §2], to which we refer for more details.

Remark 2. Up to birational equivalence, $F_N(b,c)$ is a defining polynomial for the modular curve $X_1(N)$. See again [9] for more background.

Following the previous exercises, we now know that for $N = 5$, we have the following Tate normal form:

$$E : y^2 + (1-b)xy - by = x^3 - bx^2, \qquad P = (0,0) \tag{5}$$

as long as $b \neq 0$ nor a root of $b^2 - 11b - 1$.

2 Step 2: Isogenies and Vélu's formulae

Let E and E' be elliptic curves over K. An isogeny $\varphi : E \to E'$ is a non-constant morphism such that $\varphi(\mathcal{O}_E) = \mathcal{O}_{E'}$, where $\mathcal{O}_E, \mathcal{O}_{E'}$ denote the respective points at infinity. The degree of φ is its degree as a morphism and there always exists a dual isogeny $\hat{\varphi} : E' \to E$ such that $\hat{\varphi} \circ \varphi = [\deg(\varphi)]$, where as usual $[\cdot]$ denotes scalar multiplication. The kernel of φ is a finite subgroup of E, more precisely its size is a divisor of $\deg(\varphi)$, where equality holds if and only if φ is separable (which is automatic if $\operatorname{char} K \nmid \deg(\varphi)$). Conversely, given a finite subgroup $C \subset E$, there exists a unique[1] separable isogeny φ having C as its kernel. Concrete formulae for this isogeny were given by Vélu:

Theorem 3. *Let C be a finite subgroup of the elliptic curve*

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

over K. Fix a partition $C = \{\mathcal{O}_E\} \cup C_2 \cup C^+ \cup C^-$, where C_2 are the order 2 points of C, and C^+ and C^- are such that for any $P \in C^+$ it holds that $-P \in C^-$. Write $S = C^+ \cup C_2$, and for $Q \in S$ define

$$\begin{aligned}
g_Q^x &= 3x(Q)^2 + 2a_2x(Q) + a_4 - a_1y(Q), \\
g_Q^y &= -2y(Q) - a_1x(Q) - a_3, \\
u_Q &= (g_Q^y)^2, \quad v_Q = \begin{cases} g_Q^x & \text{if} \quad 2Q = \mathcal{O}_E, \\ 2g_Q^x - a_1g_Q^y & \text{else,} \end{cases} \\
v &= \sum_{Q\in S} v_Q, \quad w = \sum_{Q\in S}(u_Q + x(Q)v_Q), \\
A_1 &= a_1, \quad A_2 = a_2, \quad A_3 = a_3, \\
A_4 &= a_4 - 5v, \quad A_6 = a_6 - (a_1^2 + 4a_2)v - 7w.
\end{aligned}$$

Then the separable isogeny φ with domain E and kernel C has codomain $E' = E/C$ with Weierstrass equation

$$E' : y^2 + A_1xy + A_3y = x^3 + A_2x^2 + A_4x + A_6 \tag{6}$$

over $\overline{K}$. Furthermore, for $P \in E$ we can compute the image of P as

$$\begin{aligned}
x(\varphi(P)) &= x(P) + \sum_{Q\in C\setminus\{\mathcal{O}_E\}} (x(P+Q) - x(Q)) \\
y(\varphi(P)) &= y(P) + \sum_{Q\in C\setminus\{\mathcal{O}_E\}} (y(P+Q) - y(Q)).
\end{aligned}$$

Proof. See [10]. ∎

[1] Up to post-composition with an isomorphism.

Exercise 4 *Using your favorite computer algebra package, apply Vélu's formulae to E and P and compute an equation for E'. You can for instance use the* `IsogenyFromKernel` *command in Magma for this where you first have to derive the kernel polynomial (which is easy given the multiples of P you computed before). If everything went correct, you should end up with a curve isomorphic to*

$$y^2+(-b+1)*x*y-b*y = x^3-b*x^2+(-5*b^3-10*b^2+5*b)*x+(-b^5-10*b^4+5*b^3-15*b^2+b)\,. \blacksquare$$

3 Step 3: finding a kernel generator on E'

Now that we have determined E', we need to find a point P' on E' such that the composition

$$E \to E' \to E'/\langle P'\rangle \tag{7}$$

is a cyclic isogeny of degree N^2. This simply means that the kernel of the composition has to be generated by a single N^2-torsion point on E (and not e.g. full N-torsion).

Exercise 5 *Show that the point P' has to satisfy*

$$\hat{\varphi}(P') = \lambda P \text{ for some } \lambda \in (\mathbb{Z}/N)^*, \tag{8}$$

with $\hat{\varphi} : E' \to E$ the dual of φ.

In particular, there are $N\phi(N)$ such points, generating N distinct subgroups of E', where ϕ denotes Euler's totient function. The points corresponding to $\lambda = 1$ will be called P-distinguished; they can be viewed as a set of canonical generators for these subgroups.

4 Step 4: Division polynomials

Let E/K be defined by $y^2+a_1xy+a_3y = x^3+a_2x^2+a_4x+a_6$, and let $b_2 = a_1^2+4a_2$, $b_4 = 2a_4 + a_1a_3$, $b_6 = a_3^2 + 4a_6$, $b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2$. For all integers $N \geq 0$, the N-division polynomial is given by

$$\Psi_{E,0} = 0, \quad \Psi_{E,1} = 1, \quad \Psi_{E,2} = 2y+a_1x+a_3, \quad \Psi_{E,N} = t\cdot \prod_{Q\in(E[N]\setminus E[2])/\pm} (x-x(Q)),$$

where $t = N$ if N is odd and $t = \frac{N}{2}\cdot\Psi_{E,2}$ if N is even. By definition, we have that for any non-trivial $P \in E[N]$, $\Psi_{E,N}(P) = 0$. The division polynomials satisfy the following recurrence relation which allows them to be computed efficiently:

$$\begin{aligned}
\Psi_{E,3} &= 3x^4 + b_2x^3 + 3b_4x^2 + 3b_6x + b_8\\
\frac{\Psi_{E,4}}{\Psi_{E,2}} &= 2x^6 + b_2x^5 + 5b_4x^4 + 10b_6x^3 + 10b_8x^2 + (b_2b_8 - b_4b_6)x + (b_4b_8 - b_6^2)\\
\Psi_{E,2N+1} &= \Psi_{E,N+2}\Psi_{E,N}^3 - \Psi_{E,N-1}\Psi_{E,N+1}^3 \text{ if } N \geq 2\\
\Psi_{E,2N} &= \frac{\Psi_{E,N}}{\Psi_{E,2}}(\Psi_{E,N+2}\Psi_{E,N-1}^2 - \Psi_{E,N-2}\Psi_{E,N+1}^2) \text{ if } N \geq 3.
\end{aligned}$$

Note that $\Psi_{E,2}^2 = 4x^3 + (a_1^2 + 4a_2)x^2 + (2a_1a_3 + 4a_4)x + a_3^2 + 4a_6$, i.e. a univariate polynomial in x.

If one is interested in points of exact order N (so not just in $E[N]$), then one can use the reduced N-division polynomial $\psi_{E,N}$ defined as

$$\psi_{E,N} = \frac{\Psi_{E,N}}{\mathrm{lcm}_{d|N, d \neq N}\{\Psi_{E,d}\}}.$$

For all primes ℓ, we have that $\Psi_{E,\ell} = \psi_{E,\ell}$. Note that for $N > 2$, the reduced N-division polynomial of an elliptic curve E is a univariate polynomial in x.

The multiplication by N-map can be expressed explicitly using division polynomials as follows [8, Exercise 3.6]:

$$[N]P = \left(\frac{\phi_{E,N}(P)}{\Psi_{E,N}(P)^2}, \frac{\omega_{E,N}(P)}{\Psi_{E,N}(P)^3} \right), \tag{9}$$

with $\phi_{E,N} = x\Psi_{E,N}^2 - \Psi_{E,N+1}\Psi_{E,N-1}$ and $\omega_{E,N} = \frac{1}{2\Psi_{E,N}}(\Psi_{E,2N} - \Psi_{E,N}(a_1\phi_{E,N} + a_3\Psi_{E,N}^2))$.

Exercise 6 *Using a computer algebra package, compute the* 5*-th division polynomial for the curve*

$$E : y^2 + (1 - c)xy - by = x^3 - bx^2\,.$$

What is the constant term of this polynomial? How does this related to F_5 *you have derived before?*

Exercise 7 *Using a computer algebra package, compute the* 5*-th division polynomial for the curve* E'*. The answer is given in the appendix.*

Exercise 8 *Using a computer algebra package, compute the factorisation of the* 5*-th division polynomial on the curve* E' *as irreducible polynomials over the funciton field* $\mathbb{Q}(b)$*. Which degrees do you see? Can you relate one of the factors with the dual isogeny?*

5 Step 5: Constructing the correct algebraic extension via the Tate pairing

Given an elliptic curve E/K and an integer $N \geq 2$, the Tate pairing is a bilinear map

$$t_N : E(K)[N] \times E(K)/NE(K) \to K^*/(K^*)^N : (P_1, P_2) \mapsto t_N(P_1, P_2)$$

which can be computed as follows. Consider a Miller function f_{N,P_1}, i.e., a function on E with divisor $N(P_1) - N(\mathcal{O}_E)$. Let D be a K-rational divisor on E that is linearly equivalent with $(P_2) - (\mathcal{O}_E)$ and whose support is disjoint from $\{P_1, \mathcal{O}_E\}$. Then $t_N(P_1, P_2) = f_{N,P_1}(D)$. If $P_1 \neq P_2$ and the Miller function is normalized, i.e., the leading coefficient of its expansion around $\mathcal{O}_E$ with respect to the uniformizer x/y equals 1 (we are assuming that E is in Weierstrass form), then one can simply compute $t_N(P_1, P_2)$ as $f_{N,P_1}(P_2)$.

For certain instances of K, the Tate pairing is known to be non-degenerate, meaning that for each $P_1 \in E(K)[N] \setminus \{\mathcal{O}_E\}$ there exists a $P_2 \in E(K)/NE(K)$ such that $t_N(P_1, P_2) \neq 1$, and vice versa. Most notably, this is true if $K = \mathbb{F}_q$ is a finite field containing a primitive Nth root of unity ζ_N [6], i.e., for which $N \mid q - 1$.

Another important feature is that the Tate pairing is compatible with isogenies, in the following sense: if $\varphi : E \to E'$ is an isogeny over K then the rule $t_N(\varphi(P_1), P_2') = t_N(P_1, \hat{\varphi}(P_2'))$ applies. For a proof of this compatibility we refer to [2, Thm. IX.9], which assumes $\zeta_N \in K$, but this condition can be discarded (it is not used in the proof).

Exercise 9 *Show that the above implies that*

$$t_N(\varphi(P_1), \varphi(P_2)) = t_N(P_1, P_2)^{\deg(\varphi)}$$

for all $P_1 \in E(K)[N]$ and $P_2 \in E(K)/NE(K)$.

Exercise 10 *Using the fact that $\hat{\varphi}(P') = P$ and exploiting the compatibility of the Tate pairing with isogenies, show that the field of definition of P' must contain $\sqrt[N]{t_N(P, -P)}$. Why do you think $-P$ was chosen and not just P?*

Exercise 11 *Using a computer algebra package, compute a representant of the Tate pairing $t_5(P, -P)$ on E. In this case the result can simply be taken as b. Note the multiplying with any 5-th power in $\mathbb{Q}_N(b, c)^*$ is an equally valid answer since the Tate pairing is only determined modulo 5-th powers.*

The above exercise shows that the field of definition of P' contains at least the field $\mathbb{Q}_N(b, c, \sqrt[N]{\rho})$, but it does not directly imply that both are equal. Adjoining an N-th root is an instance of a simple radical extension.

Following [5], we say that a field extension $K \subset L$ is simple radical of degree $N \geq 2$ if there exists an $\alpha \in L$ such that *(i)* $L = K(\alpha)$, *(ii)* $\rho := \alpha^N \in K$, and *(iii)* $x^N - \rho \in K[x]$ is irreducible. Property *(iii)* can be verified easily using the following theorem.

Theorem 4. *Let K be a field, consider an integer $N \geq 2$, and let $\rho \in K^*$. Assume that for all primes $m \mid N$ we have $\rho \notin K^m$. If $4 \mid N$, assume moreover that $\rho \notin -4K^4$. Then the polynomial $x^N - \rho \in K[x]$ is irreducible.*

Proof. See [7, Thm. VI.9.1]. ■

Although you have only shown an inclusion of fields, it is possible to show an equality as in the following theorem. For a proof we refer to the original paper [3].

Theorem 5. *Let $P' \in E'$ be a point satisfying (3). Then the field extension $\mathbb{Q}_N(b,c) \subset \mathbb{Q}_N(b,c)(P')$, obtained by adjoining the coordinates of P', is simple radical of degree N. More precisely, $\mathbb{Q}_N(b,c)(P') = \mathbb{Q}_N(b,c)(\sqrt[N]{\rho})$ for an appropriately chosen Nth root $\sqrt[N]{\rho}$ of $\rho = f_{N,P}(-P)$.*

Remark 1. Our choice of radicand $\rho = f_{N,P}(-P)$ is somewhat arbitrary: any representant of $t_N(P, \mu P)$ for any $\mu \in (\mathbb{Z}/N)^*$ would have worked equally well, with the same proofs. This reflects the fact that scaling ρ by Nth powers, or raising ρ to an exponent that is coprime with N, results in the same simple radical extension.

6 Step 6: finding the coordinates of P'

Following Theorem 5 we know it is sufficient to consider the field extension $\mathbb{Q}_N(b,c)(\sqrt[N]{\rho})$ for an appropriately chosen Nth root $\sqrt[N]{\rho}$ of $\rho = f_{N,P}(-P)$ to find the field of definition of P'.

Exercise 12 *Using a computer algebra package, find the coordinates of P' on E' by first finding its x-coordinate as a root of a well chosen factor of the 5-th division polynomial on E' over the field extension $\mathbb{Q}_N(b,c)(\sqrt[N]{b})$.*

In particular, if you choose the factor

$$
\begin{aligned}
z^5 + 10bz^4 + (-5b^3 - 5b^2 + 55b)z^3 + (-85b^4 - 120b^3 - 230b^2 + 35b)z^2 \\
+(-5b^6 - 310b^5 - 770b^4 + 325b^3 - 95b^2 + 10b)z \\
-b^8 + 19b^7 - 777b^6 + 757b^5 - 755b^4 - 2b^3 - 17b^2 + b
\end{aligned}
$$

you will end up with the x-coordinate of a P-distinguished point. If we denote $\omega = \sqrt[5]{b}$, then the result you should obtain is given by

$$
\begin{aligned}
P' := [5\omega^4 + (b-3)\omega^3 + (b+2)\omega^2 + (2b-1)\omega - 2b, \\
5\omega^4 + (b-3)\omega^3 + (b^2 - 10b + 1)\omega^2 + (-b^2 + 13b)\omega - b^2 - 11b]
\end{aligned}
$$

Given the coordinates of a P-distinguished point P', all other P-distinguished points are found by varying the choice of $\sqrt[N]{\rho}$:

Lemma 6. *Let $\lambda \in (\mathbb{Z}/N)^*$ and consider formulae expressing the coordinates of a point P' such that $\hat{\varphi}(P') = \lambda P$. Then, by varying the choice of the Nth root $\sqrt[N]{\rho}$, i.e., by scaling it with ζ_N^i for $i = 0, 1, \ldots, N-1$, these formulae compute the coordinates of all points P' for which $\hat{\varphi}(P') = \lambda P$.*

7 Step 7: transforming back to Tate normal form

Now that you have found the coordinates of the point P', you are almost done in deriving the radical isogeny formulae for $N = 5$. The final step is simply to transform the curve equation for E' back into a Tate normal form, the coefficients of which are the radical isogeny formulae.

Exercise 13 *Using the result of the previous exercise, transform the curve E' into Tate normal form*

$$E' : y^2 + (1 - b')xy - b'y = x^3 - b'x^2, \qquad P' = (0,0)\,.$$

One possible answer is given by

$$b' = \omega \frac{\omega^4 + 3\omega^3 + 4\omega^2 + 2\omega + 1}{\omega^4 - 2\omega^3 + 4\omega^2 - 3\omega + 1}$$

8 Other examples

Below you can find some other examples that were computed in a similar method as you did for $N = 5$. Note that the table only contains a representative of the radicand. The corresponding formulae expressing b', c' as a function of $b, c, \omega = \sqrt[N]{\rho}$ become too complex to nicely display here. All formulae for $N = 2, \ldots, 13$ can be found online at https://github.com/KULeuven-COSIC/Radical-Isogenies. ■

N	Polynomial relation $F_N(b,c) = 0$	Radicand $\rho = f_{N,P}(-P)$
4	$c = 0$	$-b$
5	$c - b = 0$	b
6	$c^2 + c - b = 0$	$-b^2/c$
7	$c^3 + cb - b^2 = 0$	b^3/c^2
8	$c^2b - c^2 + 3cb - 2b^2 = 0$	$-b^3/(b-c)$
9	$c^5 + c^4 - c^3b + c^3 - 3c^2b + 3cb^2 - b^3 = 0$	$b^3c^2/(b-c)^2$
10	$c^5 + c^4b + 3c^3b - 3c^2b^2$ $+ c^2b - 2cb^2 + b^3 = 0$	$-b^3c/(c^2 + c - b)$
11	$c^7b + 3c^6b - c^6 - 3c^5b^2 + 6c^5b - 9c^4b^2$ $+ 4c^3b^3 + c^3b^2 - 3c^2b^3 + 3cb^4 - b^5 = 0$	$b^3(b-c)^2/(c^2 + c - b)^2$
12	$c^6 + c^4b + c^4 - 5c^3b - c^2b^3$ $+ 10c^2b^2 - 9cb^3 + 3b^4 = 0$	$-b^4(b-c)/(b^2 - bc - c^3)$
13	$c^{10} - c^9b^2 - 6c^8b^2 + 6c^8b + 5c^7b^3 - 21c^7b^2$ $+ 3c^7b + 24c^6b^3 - 13c^6b^2 + c^6b - 9c^5b^4$ $+ 21c^5b^3 - 6c^5b^2 - 15c^4b^4 + 15c^4b^3 + 4c^3b^5$ $- 20c^3b^4 + 15c^2b^5 - 6cb^6 + b^7 = 0$	$b^5(c^2 + c - b)^2/(b^2 - bc - c^3)^2$

Table 1: Relations $F_N(b,c) = 0$ and radicands ρ for small $N \geq 4$

A similar reasoning can be made for $N > 5$, but a direct factorization of the reduced N-division polynomial of E' over $\mathbb{Q}_N(b,c)(\sqrt[N]{\rho})$ quickly becomes unwieldy, for several reasons: the coefficients of E' become more involved, the degree of $\psi_{E',N}$ grows quadratically, and both ρ and the base field $\mathbb{Q}_N(b,c)$ become increasingly complicated, see Table 1. For instance, from $N=7$ onwards it is no longer possible to eliminate one of the variables b,c using the relation $F_N(b,c)=0$. As long as the modular curve $X_1(N)$ has genus 0, it is possible to get around this by using a different parametrization, but for $N=11$ and $N\geq 13$ this is no longer the case.

An approach that already works much better is to use number fields, i.e. assign a large enough integer value to b, construct the number field defined by $F_N(b,c)=0$ and the degree N extension by adjoining $\sqrt[N]{\rho}$. The root of $\psi_{E',N}(x)$ is an expression in c and $\sqrt[N]{\rho}$ with rational coefficients. We know that each such coefficient is a rational function in b, so if b is large enough, this function can be found using lattice reduction. The most effective method is similar to the previous method, but uses p-adic fields instead of number fields. Again we need to choose a "large enough" value for b and a large enough precision with which we represent the p-adic field, to be able to reconstruct the rational function in b. We followed this approach for $N=13$, since Magma struggles to find the formulae using direct root finding.

9 Appendix

The 5-th division polynomial on E'

```
5z^12 + (5b^2 - 30b + 5)z^11 + (b^4 - 322b^3 - 551b^2 + 267b + 1)z^10 + (-480b^5 - 3390b^4 + 3030b^3 -
    6335b^2 + 470b)z^9 + (-285b^7 - 3765b^6 + 8265b^5 - 20355b^4 + 35910b^3 - 8040b^2 + 285b)z^8 + (-90b^9 -
    870b^8 + 27060b^7 + 20850b^6 + 62910b^5 - 72060b^4 + 20220b^3 - 3150b^2 + 90b)z^7 + (-15b^11 + 405b^10 +
    42195b^9 + 128310b^8 + 266625b^7 - 228315b^6 - 293925b^5 + 172200b^4 - 28125b^3 - 225b^2 + 15b)z^6 +
    (-b^13 + 289b^12 + 27558b^11 + 199127b^10 + 511270b^9 - 280879b^8 + 477816b^7 + 1713587b^6 - 1578322b^5 +
    418067b^4 - 28098b^3 + 199b^2 + b)z^5 + (65b^14 + 9915b^13 + 112205b^12 + 669245b^11 - 352475b^10 +
    538435b^9 + 6828385b^8 - 3948605b^7 + 4751805b^6 - 2247405b^5 + 252920b^4 - 11135b^3 + 60b^2)z^4 + (5b^16
    + 2060b^15 + 33060b^14 + 331020b^13 + 334630b^12 - 730470b^11 + 8809165b^10 - 14385960b^9 + 14356630b^8 -
    6234590b^7 + 5800370b^6 - 1060370b^5 + 75310b^4 - 2310b^3 + 5b^2)z^3 + (250b^17 + 4615b^16 + 94755b^15 +
    113915b^14 - 32065b^13 + 7027425b^12 - 19811600b^11 - 400635b^10 - 11570105b^9 + 10204120b^8 - 7585240b^7 +
    2059970b^6 - 256090b^5 + 11175b^4 - 265b^3)z^2 + (20b^19 + 160b^18 + 13080b^17 + 55555b^16 - 478150b^15 +
    4484205b^14 - 6832915b^13 - 20657360b^12 + 7663700b^11 - 31325575b^10 - 7101825b^9 + 9341380b^8 - 1331150b^7
    + 385260b^6 - 28745b^5 + 675b^4 - 20b^3)z + b^21 - 9b^20 + 520b^19 + 8515b^18 - 59980b^17 + 160118b^16 +
    2573598b^15 - 13562315b^14 + 15424734b^13 - 34652931b^12 + 15685472b^11 - 13788354b^10 - 8269780b^9 +
    266981b^8 - 133579b^7 + 28334b^6 - 935b^5 + 11b^4 - b^3
```

Its corresponding factorisation in irreducible polynomials over $\mathbb{Q}(b)$:

```
<z^2 + (b^2 - b + 1)z + 1/5b^4 + 3/5b^3 - 26/5b^2 - 8/5b + 1/5, 1>,
<z^5 - 15bz^4 + (-55b^3 + 45b^2 + 5b)z^3 + (-35b^5 - 65b^4 + 65b^3 - 100b^2)z^2 + (-10b^7 - 25b^6 -
    30b^5 - 980b^4 + 495b^3 - 5b^2)z - b^9 - 7b^8 + 62b^7 - 605b^6 + 127b^5 - 1177b^4 - 14b^3 - b^2, 1>,
<z^5 + 10bz^4 + (-5b^3 - 5b^2 + 55b)z^3 + (-85b^4 - 120b^3 - 230b^2 + 35b)z^2 + (-5b^6 - 310b^5 -
    770b^4 + 325b^3 - 95b^2 + 10b)z - b^8 + 19b^7 - 777b^6 + 757b^5 - 755b^4 - 2b^3 - 17b^2 + b, 1>
```

References

[1] Daniel J Bernstein, Luca De Feo, Antonin Leroux, and Benjamin Smith. Faster computation of isogenies of large prime degree. In *ANTS-XIV*, volume 4 of *Open Book Series*, pages 39–55. Mathematical Sciences Publishers, 2020.

[2] Ian F. Blake, Gadiel Seroussi, and Nigel P. Smart, editors. *Advances in elliptic curve cryptography*, volume 317 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 2005.

[3] Wouter Castryck, Thomas Decru, and Frederik Vercauteren. Radical isogenies. In Shiho Moriai and Huaxiong Wang, editors, *Advances in Cryptology - ASIACRYPT 2020 - Part II*, volume 12492 of *Lecture Notes in Computer Science*, pages 493–519. Springer, 2020.

[4] Wouter Castryck, Tanja Lange, Chloe Martindale, Lorenz Panny, and Joost Renes. CSIDH: An efficient post-quantum commutative group action. In *Asiacrypt 2018 (3)*, volume 11274 of *Lecture Notes in Computer Science*, pages 395–427. Springer, 2018.

[5] Keith Conrad. Simple radical extensions. Expository paper. https://kconrad.math.uconn.edu/blurbs/galoistheory/simpleradical.pdf.

[6] Florian Hess. A note on the Tate pairing of curves over finite fields. *Archiv der Mathematik*, 82:28–32, 2004.

[7] Serge Lang. *Algebra*, volume 211 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, third edition, 2002.

[8] Joseph H Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer, second edition, 2009.

[9] Marco Streng. Generators of the group of modular units for $\Gamma_1(N)$ over the rationals. *Cornell University*, arXiv:1503.08127v2, 2019. https://arxiv.org/abs/1503.08127v2.

[10] Jacques Vélu. Isogénies entre courbes elliptiques. *Comptes-Rendus de l'Académie des Sciences, Série I*, 273:238–241, 1971.