ORIENTING SUPERSINGULAR ISOGENY GRAPHS

Notes for the Isogeny-based Cryptography School 2020

Leonardo Colò, Aix-Marseille University, France

July 2021

These short lecture notes aims at giving an overview on the framework of orienting supersingular elliptic curves, that is exploiting the use of embeddings of imaginary quadratic orders into endomorphism rings of supersingular Elliptic curves. They try to provide all the information necessary to understand the general ideas behind the key exchage protocol OSIDH. Further detail could be found in [CK].

1 Basic Definitions

Definition. A *K-orientation* on a supersingular elliptic curve E/k is a homomorphism $\iota : K \hookrightarrow \mathrm{End}^0(E)$. An *$\mathcal{O}$-orientation* on E is a K-orientation such that the image of the restriction of ι to $\mathcal{O}$ is contained in $\mathrm{End}(E)$. We write $\mathrm{End}((E,\iota))$ for the order $\mathrm{End}(E)\cap\iota(K)$ in $\iota(K)$. An $\mathcal{O}$-orientation is *primitive* if ι induces an isomorphism of $\mathcal{O}$ with $\mathrm{End}((E,\iota))$.

Remark. The supersingular isogeny path problem takes place in a geometric category of supersingular elliptic curves. In the equivalent category of left ideals for a quaternion order, primitive orientations are usually referred to as optimal embeddings and they have been introduced by Eichler [Eic] (also see [Voi, Ch. 30-31]).

Remark. Orientations (and optimal embeddings) can be used to p-adically lift supersingular elliptic E curves, that is, construct an elliptic curve over (an extension of) $\mathbb{Q}_p$ whose reduction modulo p is exactly E. This process brings us in the characteristic 0 realm meaning that the p-adic lifting of a supersingular curve is not supersingular anymore. For more detail one could refer to [Bel].

Remark. (Primitive) Orientations are in bijection with the (primitive) representations of the discriminant of $\mathcal{O}$ by normic ternary quadratic form associated associated to the endomorphism ring of the elliptic curve (See [AB], [Mil]).

Example. The elliptic curve E_0 over $\mathbb{F}_p$ with j-invariant 0 is supersingular for $p \equiv 2 \mod 3$. In these cases, its endomorphism ring its known to be isomorphic to the maximal quaternion order

$$\mathrm{End}(E_0) \simeq \mathbb{Z} + \mathbb{Z}\left[\frac{1+i}{2}\right] + \mathbb{Z}[j] + \mathbb{Z}\left[\frac{3+i+3j+k}{6}\right] \subseteq \mathfrak{A}_{p,\infty}$$

where $i^2 = -3$, $j^2 = -p$ and $\mathfrak{A}_{p,\infty}$ is the quaternion algebra ramified at p and ∞.

We know that E_0 admits an endomorphism of degree 3 (we could check that it is a root of $\Phi_3(X,X)$, the classical modular polynomial of degree 3) given by $\rho : (x,y) \to (\zeta_3 x, y)$ for a primitive cube root of unity ζ_3.

We can show that there is a unique optimal embedding $\mathcal{O}_K = \mathbb{Z}[\omega] \hookrightarrow \mathcal{O}$ where $\mathcal{O}_K$ is the ring of integers of the number field $K = \mathbb{Q}(\sqrt{-3})$ of discriminant -3. (Exercise?) and this is given by $w \to (1+i)/2$ resulting in a unique primitive orientation $w \to \rho$.

Let $\phi : E \to F$ be an isogeny of degree ℓ. A K-orientation $\iota : K \hookrightarrow \mathrm{End}^0(E)$ determines a K-orientation $\phi_*(\iota) : K \hookrightarrow \mathrm{End}^0(F)$ on F, defined by

$$\phi_*(\iota)(\alpha) = \frac{1}{\ell}\,\phi \circ \iota(\alpha) \circ \hat{\phi}.$$

Conversely, given K-oriented elliptic curves (E, ι_E) and (F, ι_F) we say that an isogeny $\phi : E \to F$ is K-oriented if $\phi_*(\iota_E) = \iota_F$, i.e. if the orientation on F is induced by ϕ.

If E admits a primitive $\mathcal{O}$-orientation by an order $\mathcal{O}$ in K, $\phi : E \to F$ is an isogeny then F admits an induced primitive $\mathcal{O}'$-orientation for an order $\mathcal{O}'$ satisfying

$$\mathbb{Z} + \ell\mathcal{O} \subseteq \mathcal{O}' \text{ and } \mathbb{Z} + \ell\mathcal{O}' \subseteq \mathcal{O}.$$

We say that an isogeny $\phi : E \to F$ is an $\mathcal{O}$-oriented isogeny if $\mathcal{O} = \mathcal{O}'$.

Remark. Orientations permits one to recover some terminology usually associated with CM elliptic curves (see [Koh]);

- $\mathcal{O} = \mathcal{O}'$ and we say that ϕ is *horizontal*,
- $\mathcal{O} \subset \mathcal{O}'$ with index ℓ and we say that ϕ is *ascending*,
- $\mathcal{O}' \subset \mathcal{O}$ with index ℓ and we say that ϕ is *descending*.

Definition. We define an ℓ-*isogeny chain* of length n from E_0 to E to be a sequence of isogenies of degree ℓ:

$$E_0 \xrightarrow{\phi_0} E_1 \xrightarrow{\phi_1} E_2 \xrightarrow{\phi_2} \dots \xrightarrow{\phi_{n-1}} E_n = E.$$

We say that the ℓ-isogeny chain is *without backtracking* if $\ker(\phi_{i+1} \circ \phi_i) \neq E_i[\ell]$ for each $i = 0, \dots, n-1$, and say that the isogeny chain is *descending* (or *ascending*, or *horizontal*) if each ϕ_i is descending (or ascending, or horizontal, respectively).

Remark. The orientation by an imaginary quadratic number field K differentiates vertices in the descending paths from a starting elliptic curve, determining an infinite graph.

2 Class Group Action

Suppose that (E_i, ϕ_i) is an ℓ-isogeny chain, with E_0 equipped with an $\mathcal{O}_K$-orientation $\iota_0 : \mathcal{O}_K \to \mathrm{End}(E_0)$. For each i, let $\iota_i : K \to \mathrm{End}^0(E_i)$ be the induced K-orientation on E_i, and we note $\mathcal{O}_i = \mathrm{End}(E_i) \cap \iota_i(K)$ with $\mathcal{O}_0 = \mathcal{O}_K$. In particular, if (E_i, ϕ_i) is a descending ℓ-chain, then ι_i induces an isomorphism

$$\iota_i : \mathbb{Z} + \ell^i\mathcal{O}_K \longrightarrow \mathcal{O}_i.$$

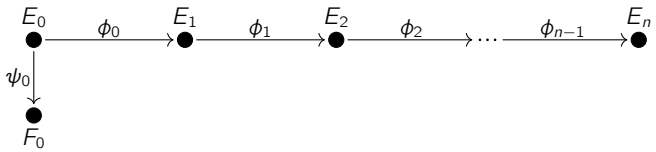
Let q be a prime different from p and ℓ that splits in $\mathcal{O}_K$, let $\mathfrak{q}$ be a fixed prime over q. For each i we set $\mathfrak{q}_{(i)} = \iota_i(\mathfrak{q}) \cap \mathcal{O}_i$, and define

$$C_i = E_i[\mathfrak{q}_{(i)}] = \{P \in E_i[q] \mid \psi(P) = 0 \text{ for all } \psi \in \mathfrak{q}_{(i)}\}.$$

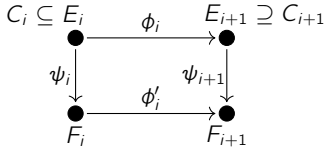
We define $F_i = E_i/C_i$, and let $\psi_i : E_i \to F_i$, an isogeny of degree q. By construction, it follows that $\phi_i(C_i) = C_{i+1}$ for all $i = 0, \dots, n-1$. In particular, if (E_i, ϕ_i) is a descending ℓ-ladder, then ι_i induces an isomorphism

$$\iota_i : \mathbb{Z} + \ell^i\mathcal{O}_K \longrightarrow \mathcal{O}_i.$$

The isogeny $\psi_0 : E_0 \to F_0 = E/C_0$ gives the following diagram of isogenies:

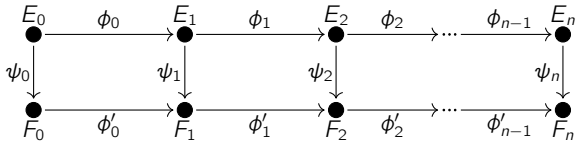


and for each $i = 0, \dots, n-1$ there exists a unique $\phi'_i : F_i \to F_{i+1}$ with kernel $\psi_i(\ker(\phi_i))$ such that the following diagram commutes:



The isogenies $\psi_i : E_i \to F_i$ induce orientations $\iota'_i : \mathcal{O}'_i \to \mathrm{End}(F_i)$. This construction motivates the following definition.

Definition. An *ℓ-ladder* of length n and degree q is a commutative diagram of ℓ-isogeny chains (E_i, ϕ_i) and (F_i, ϕ'_i) of length n connected by q-isogenies $(\psi_i : E_i \to F_i)$:



We also refer to an ℓ-ladder of degree q as a *q-isogeny* of ℓ-isogeny chains, which we express as $\psi : (E_i, \phi_i) \to (F_i, \phi'_i)$.

We say that an ℓ-ladder is ascending (or descending, or horizontal) if the ℓ-isogeny chain (E_i, ϕ_i) is ascending (or descending, or horizontal, respectively). We say that the ℓ-ladder is *level* if ψ_0 is a horizontal q-isogeny. If the ℓ-ladder is descending (or ascending), then we refer to the length of the ladder as its *depth* (or, respectively, as its *height*).

We introduce the following notation:

- $\mathrm{SS}(p) = \{\text{Supersingular elliptic curves over } \bar{\mathbb{F}}_p \text{ up to isomorphism}\}$
- $\mathrm{SS}_{\mathcal{O}}(p) = \{\mathcal{O}\text{-oriented supersingular elliptic curves over } \bar{\mathbb{F}}_p \text{ up to } K\text{-isomorphism}\}$
- $\mathrm{SS}^{pr}_{\mathcal{O}}(p) = \{\text{Primitive } \mathcal{O}\text{-oriented upersingular elliptic curves over } \bar{\mathbb{F}}_p \text{ up to isomorphism}\}$

Integral $\mathcal{O}$-ideals act on $\mathrm{SS}^{pr}_{\mathcal{O}}(p)$ via

$$j(E) \longrightarrow [\mathfrak{a}] \cdot j(E) = j(E/E[\mathfrak{a}])$$

where, as usual, the group $E[\mathfrak{a}]$ consists of all the points annihilated by all the endomorphisms in $\mathfrak{a} \hookrightarrow \mathrm{End}(E)$. Since principal ideals act trivially, this action factors through the class group

$$\begin{aligned} \mathcal{Cl}(\mathcal{O}) \times \mathrm{SS}_{\mathcal{O}}(p) &\longrightarrow \mathrm{SS}_{\mathcal{O}}(p) \\ ([\mathfrak{a}], E) &\longmapsto [\mathfrak{a}] \cdot E = E/E[\mathfrak{a}] \end{aligned}$$

Theorem 2.1. *The class group $\mathcal{Cl}(\mathcal{O})$ acts faithfully and transitively on the set of $\mathcal{O}$-isomorphism classes of primitive $\mathcal{O}$-oriented elliptic curves.*

3 Modular approach

We recall that the modular curve $X(1) \cong \mathbb{P}^1$ classifies elliptic curves up to isomorphism, and the function j generates its function field. The family of elliptic curves

$$E : y^2 + xy = x^3 - \frac{36}{(j - 1728)}x - \frac{1}{(j - 1728)}$$

covers all isomorphism classes $j \neq 0, 12^3$ or ∞, such that the fiber over $j_0 \in k$ is an elliptic curve of j-invariant j_0. The curves $y^2 + y = x^3$ and $y^2 = x^3 + x$ deal with the cases $j = 0$ and $j = 1728$.

The modular polynomial $\Phi_m(X, Y)$ defines a correspondence in $X(1) \times X(1)$ such that $\Phi_m(j(E), j(E')) = 0$ if and only if there exists a cyclic m-isogeny ϕ from E to E', possibly over some extension field.

Definition. A *modular ℓ-isogeny chain* of length n over k is a finite sequence $(j_0, j_1, \ldots, j_n)$ in k such that $\Phi_\ell(j_i, j_{i+1}) = 0$ for $0 \leq i < n$. A *modular ℓ-ladder* of length n and degree q over k is a pair of modular ℓ-isogeny chains

$$(j_0, j_1, \ldots, j_n) \text{ and } (j'_0, j'_1, \ldots, j'_n),$$

such that $\Phi_q(j_i, j'_i) = 0$.

Given any modular ℓ-isogeny chain (j_i), elliptic curve E_0 with $j(E_0) = j_0$, and isogeny $\psi_0 : E_0 \to F_0$, it follows that we can construct an ℓ-ladder $\psi : (E_i, \phi_i) \to (F_i, \phi'_i)$ and hence a modular ℓ-isogeny ladder. In fact the ℓ-ladder can be efficiently constructed recursively from the modular ℓ-isogeny chain $(j_0, \ldots, j_n)$ and $(j'_0, \ldots, j'_n)$, by solving the system of equations

$$\Phi_\ell(j'_i, Y) = \Phi_q(j_{i+1}, Y) = 0,$$

for $Y = j'_{i+1}$.

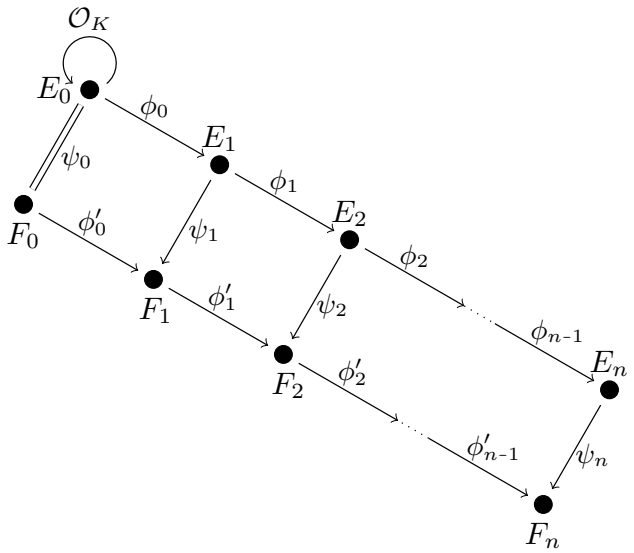
4 OSIDH Protocol

In this framework, we could try to construct a key-exchange cryptographic protocol. Suppose we fix an elliptic curve E_0/k ($k = \mathbb{F}_{p^2}$) which is primitively oriented by O_K, the ring of integers of a class number one imaginary quadratic field K. We construct a descending ℓ-isogeny chain (in the infinite oriented volcano) $E_0 \to E_1 \to \ldots \to E_n$. The orientation on E_0 yields an orientation on E_i by an order of conductor ℓ^i:

$$\iota_i : \mathbb{Z} + \ell^i \mathcal{O}_K \to \mathcal{O}_i \subset \mathrm{End}(E_i),$$

and we set $\mathcal{O} = \mathcal{O}_n$. By hypothesis on E_0/k (the class number of $\mathcal{O}_K$ is 1), any horizontal isogeny $\psi_0 : E_0 \to F_0$ is, up to isomorphism $F_0 \cong E_0$, an endomorphism.

For a set of small primes $q_1, \ldots, q_t$ splitting in $\mathcal{O}_K$, both parties choose exponents $(e_1, \ldots, e_t)$ and push forward a $q_1^{e_1} \cdot \ldots \cdot q_t^{e_t}$-endomorphism $\phi_0 \in \mathrm{End}(E_0)$, to an isogeny $\psi : (E_i, \phi_i) \to (F_i, \phi'_i)$.



At this point the idea is to exchange curves F_n (final Alice's curve) and G_n (final Bob's curve) and to apply the same process again starting from the elliptic curve received from the other party. Unfortunately, this is not enough to get to the same final elliptic curve. Once Alice receives the unoriented curve G_n computed by Bob she also needs additional information for each prime q_i, namely which directions - out of $q_i + 1$ total q_i-isogenies - to take as $\mathfrak{q}_i$ and $\bar{\mathfrak{q}}_i$ (the two primes above q_i in $\mathcal{O}_i$).

Exercises

Exercise 1. Show that, for an odd prime $p \equiv 2 \mod 3$ there exists a unique primitive orientation (up to conjugation) of $E(j = 0)$ by $\mathcal{O}_K$, the ring of integers of $K = \mathbb{Q}(\sqrt{-3})$.

What happens for $p = 2$?

Exercise 2. Verify the commutativity of the squares in a ladder: let G_1 and G_2 be two subgroups of E and suppose $\phi_i : E \to F_i = E/G_i$. Check that $F_1/\phi_1(G_2) = F_2/\phi_2(G_1)$.

Exercise 3. Class group action. We fix $p = 10007$, $\ell = 2$ and $\Delta_K = -3$.

- Describe the class group $\mathcal{O}_i = \mathbb{Z} + \ell^i \mathcal{O}_K$.

- Compute the class number of $\mathcal{O}_i = \mathbb{Z} + \ell^i \mathcal{O}_K$.
- Construct the oriented volcano up to depth 5.
- For $q = 7, 13, 19$ compute the class group action of the two primes above them on one of the elliptic curves at level 4 (oriented by $\mathcal{O}_4$).

Exercise 4. Class group. We characterize the initialization phase of ladder construction (= construction q-isogenies of ℓ-isogeny chains). The initialization step is problematic at 2-torsion elements of $\mathcal{Cl}(\mathcal{O}_i)$ as such elements are primes whose square is a principal ideal, that is, the action of $\mathfrak{q}$ and $\bar{\mathfrak{q}}$ is the same.

- Work out the two torsion part of $\mathcal{Cl}(\mathcal{O}_i)$ for $\Delta_K = -3$ and $\ell = 2$ and give a rough estimate on the number of steps to be done in order to differentiate the action of all the primes above $q < 1024$.

  Remark. This could be done using both the notation of ideals and that of quadratic forms, since we have a correspondence

$$\mathcal{O} \trianglerighteq \mathfrak{a} = (\alpha, \beta) \longrightarrow \frac{\mathrm{Nm}(\alpha x + \beta y)}{\mathrm{Nm}(\mathfrak{a})} = \langle a, b, c \rangle$$
$$\mathcal{O} \trianglerighteq \mathfrak{a} = (a, \frac{-b + \sqrt{\Delta}}{2}) \longleftarrow \langle a, b, c \rangle$$

- What are the problematic primes $p \in \mathbb{Z}$, i.e., primes that split in ideals lying in the 2-torsion subgroup?

Exercise 5. Modular approach. A square of isogenies in a ladder can be represented by a point on the modular curve $X_0(\ell q)$. This, together with the 2 maps $X_0(\ell q) \to X_0(\ell)$ (one is obtained from the other by composing with the Atkin Lehner involution) and the two maps $X_0(\ell q) \to X_0(q)$ (once again conjugated by Atkin-Lehner involution) give full description of the 4 isogenies determining the sides of the square.

Constructing a ladder consist in completing the right and bottom side of a square (determining the bottom right corner). One could hope to pre-construct a rational function $F(j_0, j_1, j_0')$ representing the image of $X_0(\ell q)$ in the product $X_0(\ell) \times X_0(\ell) \times X_0(q)$ such that, evaluated in the triple $(j(E_i), j(E_{i+1}), j(F_i))$, gives the j-invariant completing the ladder.

- Suppose $p = 2689$. Prove that elliptic curves over $\mathbb{F}_{p^2}$ can be oriented by $K = \mathbb{Q}(\sqrt{-19})$.
- We will fix $\ell = 3$ and $q = 7$. Construct the parameters t_ℓ and t_q for the modular curves $X_0(\ell)$ and $X_0(q)$ in terms of the Dedekind η-function (see [Mcm2] for some more details) as well as the maps $X_0(\ell) \to X(1)$ and $X_0(q) \to X(1)$ (One could refer to [Mcm1] for some explicit choices).
- Compute the correspondence $X_0(\ell q) \to X_0(\ell) \times X_0(\ell)$ by comparing the q expansions of $t_3(q)$ and $t_3(q^7)$ (see the Appendix for some precomputations).

  Remark. This is the analogous of the classical modular polynomial of degree 7 with some $\Gamma_0(3)$ level structure. Although, one could notice that the size of the coefficients is much smaller.

- Consider the isogeny $375\omega + 1883 \to 332\omega + 1282$ and compute the 8 squares for which it is the top map.
- Construct the modular correspondence $X_0(\ell q) \to X_0(\ell) \times X_0(\ell) \times X_0(q)$ and complete the ladder

$$\begin{array}{ccccccccc} 2634 & \longrightarrow & 359\omega + 800 & \longrightarrow & 375\omega + 1883 & \to & 332\omega + 1282 & \to & 1521\omega + 334 \to 1720\omega + 2265 \\ \downarrow & & \downarrow & & \downarrow & & & & \\ 2634 & \longrightarrow & 469\omega + 268 & \to & 2526\omega + 2057 & & & & \end{array}$$

  here ω is a root of $x^2 + x + 5$.

  Remark. Notice that a choice has been made at the second step where the two 7-isogenies differentiate.

Remark. For very small prime p this procedure might not work. The reason is that the map $\mathrm{SS}_{\mathcal{O}}(p) \to \mathrm{SS}(p)$ becomes quite rapidly non-surjective meaning that the same j-invariant appears multiple times in the same level or in two adjacent levels. This is problematic when doing examples but it is marginal in real cryptographic applications where p is usually big.

- One could repeat the exercise working with ℓ^2 instead of ℓ, i.e., adding $\Gamma_0(9)$ level structure. This means consider rectangles where the top and bottom sides are chains of 3 isogenies of length 3 and the vertical maps represent 7-isogenies between them. A nice feature of this is that the size of the modular polynomials tends to get smaller when we go up in the modular tower.

Exercise 6. Division polynomials: We fix $q = p^2 = 10007^2$. Observe that $p \equiv 2 \bmod 3$ which tells us that the elliptic curve E_0 of j-invariant 0 is supersingular. We consider the embedding $\mathbb{Z}[\omega] \hookrightarrow \mathrm{End}(E_0)$ where $\omega^2 - \omega + 1 = 0$. Consider the 2-isogeny chain

$$E_0 \to E_1 \to E_2 \to E_3 \to E_4 \to E_5$$

where $j(E_0) = 0$, $j(E_1) = 3965$, $j(E_2) = 7778$, $j(E_3) = 8545$, $j(E_4) = 377 + 1623\omega$, and $j(E_5) = 2602 + 656\omega$. On E_0 we have a 7-isogeny given by the action of $2(1 - \omega) - 1$. Construct its kernel polynomial and push it through the given isogeny chain.

References

[AB] M. Alsina and P. Bayer. *Quaternion Orders, Quadratic Forms, and Shimura Curves*. CRM monograph series. American Mathematical Society, 2004.

[Bel] J.V. Belding. "Number Theoretic Algorithms for Elliptic Curves". PhD Thesis. University of Maryland at College Park, 2008.

[CK] L. Colò and D. Kohel. "Orienting supersingular isogeny graphs". In: *Journal of Mathematical Cryptology* 14.1 (Oct. 2020), pp. 414–437. URL: `http://dx.doi.org/10.1515/jmc-2019-0034`.

[Eic] M. Eichler. "Zur Zahlentheorie der Quaternionen-Algebren." In: *Journal für die reine und angewandte Mathematik* 195 (1955), pp. 127–151.

[Koh] D. Kohel. "Endomorphism rings of elliptic curves over finite fields". PhD Thesis. U.C. Berkeley, 1996.

[Mcm1] K. Mcmurdy. *Explicit Equations for $X_0(N)$*. `https://phobos.ramapo.edu/~kmcmurdy/research/Models/index.html`.

[Mcm2] K. Mcmurdy. "A Splitting Criterion for Galois Representations Associated to Exceptional Modular Forms". PhD Thesis. University of California, Berkeley, 2001.

[Mil] P. Milione. "CM points on Shimura curves and p-adic binary quadratic forms". In: *Acta Arithmetica* 183.3 (Jan. 2018), pp. 237–256.

[Voi] J. Voight. *Quaternion Algebras*. `https://math.dartmouth.edu/~jvoight/quat-book.pdf`.

Appendix

```
> PS<q> := LaurentSeriesRing(QQ);
> f3 := DedekindEta(PS,[<1,12>,<3,-12>],200);
> f7:=DedekindEta(PS,[<1,4>,<7,-4>],200);
> f9 := DedekindEta(PS,[<1,3>,<9,-3>],200);
> f37 := Evaluate(f3,q^7 + O(q^200));
> f97 := Evaluate(f9,q^7 + O(q^200));
> B:=AlgebraicRelations([f3,f37],[8,8]);
> P<X,Y> := Universe(B);
> B;

[
X^8 - X^7*Y^7 - 84*X^7*Y^6 - 2646*X^7*Y^5 - 38332*X^7*Y^4 - 249501*X^7*Y^3 - 589680*X^7*Y^2
- 254996*X^7*Y - 84*X^6*Y^7 + 76482*X^6*Y^6 + 3324664*X^6*Y^5 - 59876628*X^6*Y^4
- 2305419732*X^6*Y^3 + 5415347854*X^6*Y^2 - 429876720*X^6*Y - 2646*X^5*Y^7 + 3324664*X^5*Y^6
- 1467398205*X^5*Y^5 - 45085572*X^5*Y^4 - 698263874840*X^5*Y^3 - 1680650984628*X^5*Y^2
- 132595060941*X^5*Y - 38332*X^4*Y^7 - 59876628*X^4*Y^6 - 45085572*X^4*Y^5
+ 3625600210414*X^4*Y^4 - 32867381988*X^4*Y^3 - 31820895060948*X^4*Y^2 - 14850602184348*X^4*Y
- 249501*X^3*Y^7 - 2305419732*X^3*Y^6 - 698263874840*X^3*Y^5 - 32867381988*X^3*Y^4
- 779835569463405*X^3*Y^3 + 1288042952640696*X^3*Y^2 - 747308553528726*X^3*Y
- 589680*X^2*Y^7 + 5415347854*X^2*Y^6 - 1680650984628*X^2*Y^5 - 31820895060948*X^2*Y^4
+ 1288042952640696*X^2*Y^3 + 2160077580913984 2*X^2*Y^2 - 1729485509595051 6*X^2*Y
- 254996*X*Y^7 - 429876720*X*Y^6 - 132595060941*X*Y^5 - 14850602184348*X*Y^4
- 747308553528726*X*Y^3 - 1729485509595051 6*X*Y^2 - 150094635296999121*X*Y + Y^8
]

> AlgebraicRelations([f9,f97],[8,8]);

[
X^8 - X^7*Y^7 - 21*X^7*Y^6 - 189*X^7*Y^5 - 910*X^7*Y^4 - 2415*X^7*Y^3 - 3213*X^7*Y^2
- 1547*X^7*Y - 21*X^6*Y^7 - 441*X^6*Y^6 - 4193*X^6*Y^5 - 22470*X^6*Y^4 - 70875*X^6*Y^3 -
121877*X^6*Y^2 - 86751*X^6*Y - 189*X^5*Y^7 - 4193*X^5*Y^6 - 43785*X^5*Y^5 - 262710*X^5*Y^4
- 946379*X^5*Y^3 - 1913625*X^5*Y^2 - 1760535*X^5*Y - 910*X^4*Y^7 - 22470*X^4*Y^6 -
262710*X^4*Y^5 - 1757630*X^4*Y^4 - 7093170*X^4*Y^3 - 16380630*X^4*Y^2 - 17911530*X^4*Y
- 2415*X^3*Y^7 - 70875*X^3*Y^6 - 946379*X^3*Y^5 - 7093170*X^3*Y^4 - 31919265*X^3*Y^3 -
82530819*X^3*Y^2 - 100442349*X^3*Y - 3213*X^2*Y^7 - 121877*X^2*Y^6 - 1913625*X^2*Y^5
- 16380630*X^2*Y^4 - 82530819*X^2*Y^3 - 234365481*X^2*Y^2 - 301327047*X^2*Y - 1547*X*Y^7
- 86751*X*Y^6 - 1760535*X*Y^5 - 17911530*X*Y^4 - 100442349*X*Y^3 - 301327047*X*Y^2
- 387420489*X*Y + Y^8
]

> C:=AlgebraicRelations([f3,f7,f37],[4,5,1]);
> P<X,Y,Z>:=Universe(C);
> C[4];

X^4*Y^3*Z - 10808/142185*X^4*Y^3 + 409346/28437*X^4*Y^2*Z + 157829/47395*X^4*Y^2
+ 8417906/142185*X^4*Y*Z - 10982174/47395*X^4*Y - 412477394/142185*X^4
+ 206215137/202708415*X^3*Y^5 + 10761264509/405416830*X^3*Y^4*Z
- 3185404308/202708415*X^3*Y^4 - 143739504193/173750070*X^3*Y^3*Z
+ 3777859611/11583338*X^3*Y^3 - 335576313359/57916690*X^3*Y^2*Z
+ 183804248439/57916690*X^3*Y^2 + 425441848006/5791669*X^3*Y*Z
+ 67929410677527/57916690*X^3*Y + 16835336602/28437*X^3*Z
+ 66289712821038/5791669*X^3 - 11166681339/405416830*X^2*Y^5*Z
- 8930061332037/81083366*X^2*Y^4*Z - 8117865083142/40541683*X^2*Y^4
- 250177208371983/57916690*X^2*Y^3*Z - 521545410239013/28958345*X^2*Y^3
```

```
- 327329959362210/5791669*X^2*Y^2*Z - 12426596976215583/28958345*X^2*Y^2
- 9113611103561853/28958345*X^2*Y*Z - 124454881180005327/28958345*X^2*Y
- 3730332029345271/5791669*X^2*Z - 482147712509876217/28958345*X^2
+ 22536219856257/202708415*X*Y^5*Z - 400200100425117/405416830*X*Y^4*Z
- 3945282430407012/202708415*X*Y^4 - 1867348135853793/57916690*X*Y^3*Z
- 14687557924511007/57916690*X*Y^3 - 13310935795806327/57916690*X*Y^2*Z
+ 8523296326054251/57916690*X*Y^2 - 14563587862879524/28958345*X*Y*Z
+ 191970035808768441/11583338*X*Y - 4181256894541608/28958345*X*Z
- 254011356343402686/28958345*X + 1789968614624487/405416830*Y^5*Z
+ 767519611709931/31185910*Y^4*Z - 79891969215741993/202708415*Y^4
+ 156588438217599/4455130*Y^3*Z + 84993591563161524/28958345*Y^3
+ 105793984316286/28958345*Y^2*Z
```