Isogeny-based Cryptography School **Summer 2021**

Lecture 7: Applications of class group computations

Lecturer: Jean-François Biasse *TA: R. Erukulangara and W. Youmans*

Disclaimer: *These notes have not been subjected to the usual scrutiny reserved for formal publications. They may be distributed outside this class only with the permission of the Instructor.*

7.1 Ideal decomposition in $\mathrm{Cl}(-d)$

One of the direct applications of the class group computation that impact isogeny computations the most is the decomposition of the class of an ideal with respect to a generating set for $\mathrm{Cl}(-d)$. Here we assume that computations happen in the class group of an imaginary quadratic order. Following our description of the Hafner and McCurley technique for computing $\mathrm{Cl}(-d)$, we represent ideal classes by reduced quadratic forms of discriminant $-d$. In particular, at the end of the class group computation algorithm, we have a generating set of size $n^{1+o(1)}$ of the lattice $\Lambda \subseteq \mathbb{Z}^n$ of vectors $\vec{x}$ such that

$$f_1^{x_1} \cdots f_n^{x_n} = 1_{\mathrm{Cl}(-d)},$$

where $\mathcal{B} = (f_i)_{i \leq n}$ is the set of prime form corresponding to the split primes $p \leq L(d)^{1/\sqrt{8}}$. We have that $n = L(d)^{1/\sqrt{8}+o(1)}$. On a technicality, we did not need a basis of Λ to compute $\mathrm{Cl}(-d)$. However, to perform ideal decomposition and solve related problems (such as the Discrete Logarithm Problem), we need a proper basis. This is obtained easily in time $n^{3+o(1)}$ by using the same modular Gaussian elimination strategy (Hermite Normal Form) presented by Hafner and McCurley in [3, Sec. 4]. The run time is guaranteed by the fact that we work modulo $h = |\mathrm{Cl}(-d)|$ whose bit size is polynomial in $\log d$. We can now assume that we have a matrix $M \in \mathbb{Z}^{n \times n}$ such that

- For all $i \leq n$, $\prod_{j \leq n} f_j^{m_{i,j}} = 1_{\mathrm{Cl}(-d)}$.
- M is lower triangular.
- For each $j > i$, $m_{i,i} > m_{i,j}$ (diagonal terms are dominant).
- $M = \begin{pmatrix} H & (0) \\ * & I \end{pmatrix}$ for $H \in \mathbb{Z}^{n_0 \times n_0}$ where $n_0 = \log^{2+o(1)} d$ (small essential part).

The last point is due to the fact that (under the GRH), the prime forms corresponding to ideals of norm up to $12 \log^2 d$ generate $\mathrm{Cl}(-d)$. This means that the rows of index $i > n_0$ represent a relation of the form $f_i = \prod_{j \leq n_0} f_j^{-m_{i,j} \bmod h}$, i.e. they show the decomposition of f_i with respect to the generators $f_1, \ldots, f_{n_0}$ of $\mathrm{Cl}(-d)$.

Now given an input reduced form f, we can decompose f according to $f_1, \ldots, f_{n_0}$ by following the two-step process:

1. Find $\vec{x} \in \mathbb{Z}^n$ such that $f = \prod_i f_i^{x_i}$ by the methods of Section 6.2.
2. For each $i > n_0$, perform the reduction $\vec{x} \leftarrow \vec{x} - x_i \vec{m}_i \bmod h$ where $\vec{m}_i$ is the i-th row of M.

Step 1 runs in time $L(d)^{1/\sqrt{2}+o(1)}$. Step 2 uses the matrix M to re-write each component f_i, $i > n_0$ of the decomposition of f with respect to the small generating set $f_1, \ldots, f_{n_0}$. Note that since $\vec{x}$ has polynomial ℓ_1-norm, the cost of this step is polynomial. In the end, we obtain the desired decomposition. Note that the entries of $\vec{x} \in \mathbb{Z}^{n_0}$ we created are potentially as large as h which is of the order of $\sqrt{d}$. This is not good for isogeny evaluation, because to evaluate the action of f on the isogeny class of an elliptic curve, one has to pay a price proportional to the ℓ_1-norm of the vector of exponent, in this case $\sqrt{d}$, which is inefficient.

However, we know from the expander graph properties of the Cayley graph that a decomposition vector with length at most $\log d$ should exist. We just need to find it. We can view Λ as a sublattice of $\mathbb{Z}^{n_0}$ by restricting ourselves to the lattice generated by the rows of H. In terms of lattice problems, we are looking for $\vec{y} \in \Lambda$ such that $\|\vec{x} - \vec{y}\|$ is small. In this case, the small vector $\vec{z} = \vec{x} - \vec{y}$ satisfies

$$\prod_i f_i^{z_i} = \prod_i f_i^{x_i} \cdot \underbrace{\prod_i f_i^{-v_i}}_{=1_{\mathrm{Cl}(-d)}} = \prod_i f_i^{x_i}.$$

Therefore we are facing an instance of the bounded distance decoding problem. One way to solve it is to find a reduced basis for Λ and then to use a round-off technique. More elaborate methods exist, but what they all have in common is that it is asymptotically computationally difficult to solve BDD when the dimension increases. Here $n_0 = \log^{2+o(1)} d$ is already a fairly high dimension to obtain asymptotically good results. If we resort to aggressive unproven heuristics such as in [1], then we can prove a better run time. As long as the dimension remains moderate, practical implementations relying on LLL or BKZ can produce interesting results (see [1] for a detailed treatment).

7.2 Computations in non-maximal orders

The complexity of the Hafner-McCurley approach for computing $\mathrm{Cl}(-d)$ and solving related problems such as ideal decomposition is in $L(d)^{3/\sqrt{8}+o(1)}$ where $-d$ is the discriminant of the order we work in. However, this can become rapidly inefficient as the conductor grows, even when the fundamental discriminant corresponding to the maximal order is small. Typically, computations done in the class group of the non-maximal order $\mathbb{Z}[\sqrt{d}]$ can be required in the context of isogeny computation. In particular, when it comes to computing endomorphism rings via the Bisson-Sutherland method [2].

There is however a way to compute class groups in suborders and to solve related problems relevant to isogeny evaluation such as ideal class decomposition by reducing the problem to computations in the class group of the maximal order. Let $-d_K$ be the fundamental discriminant corresponding to the maximal order of the quadratic field K, and let $-d = -f^2 d_K$ be the discriminant of a suborder $\mathcal{O}$ of the maximal order $\mathcal{O}_K$. Then Pauli and Klueners proved that

$$1 \to \mathcal{O}^* \to {\mathcal{O}_K}^* \to \bigoplus_{\mathfrak{p}|f} {\mathcal{O}_{K\mathfrak{p}}}^* / \mathcal{O}_{\mathfrak{p}}^* \to \mathrm{Cl}(-d) \to \mathrm{Cl}(-d_K) \to 1, \tag{7.1}$$

where $\mathcal{O}_{\mathfrak{p}}$ denotes the localization of $\mathcal{O}$ at $\mathfrak{p}$. What this means is that $\mathrm{Cl}(-d_K)$ is a quotient of $\mathrm{Cl}(-d)$ by the image of $\bigoplus_{\mathfrak{p}|f} {\mathcal{O}_{K\mathfrak{p}}}^* / \mathcal{O}_{\mathfrak{p}}^*$. We can retrieve a complete generating set for the relations between generators of $\mathrm{Cl}(-d)$ by using the relations between generators of $\mathrm{Cl}(-d_K)$ (which we obtain from class group computation in the maximal order) and their relationship with the images of generators of $\bigoplus_{\mathfrak{p}|f} {\mathcal{O}_{K\mathfrak{p}}}^* / \mathcal{O}_{\mathfrak{p}}^*$. We summarize this procedure in Algorithm 1

Let's explain Algorithm 1 a little more. It starts from the observation that the generators of $\mathrm{Cl}(-d)$ are that of $\mathrm{Cl}(-d_K)$, and those of $\bigoplus_{\mathfrak{p}|f} {\mathcal{O}_{K\mathfrak{p}}}^* / \mathcal{O}_{\mathfrak{p}}^*$ since $\mathrm{Cl}(-d) \to \mathrm{Cl}(-d_K)$ is surjective, and its kernel is the image of $\bigoplus_{\mathfrak{p}|f} {\mathcal{O}_{K\mathfrak{p}}}^* / \mathcal{O}_{\mathfrak{p}}^*$. This means that $\mathrm{Cl}(-d)$ is generated by $g_1, \cdots, g_k, \mathfrak{g}_1, \cdots, \mathfrak{g}_l$, and we now need to find

Algorithm 1 Computing $\mathrm{Cl}(\mathcal{O})$ from $\mathrm{Cl}(\mathcal{O}_K)$ (high level description)

```
Require: Order $\mathcal{O} \subseteq \mathcal{O}_K$ of conductor $f$, generators and relations for $\mathrm{Cl}(\mathcal{O}_K)$.
Ensure: Generators and relations for $\mathrm{Cl}(\mathcal{O})$.
  Compute generators $(g_i)_{i\leq k}$ and a relation matrix $M_1 \in \mathbb{Z}^{k\times k}$ for $\bigoplus_{\mathfrak{p}|f} {\mathcal{O}_K}_{\mathfrak{p}}{}^* / \mathcal{O}_{\mathfrak{p}}^*$.
  Let $(\mathfrak{g}_i)_{i\leq l}$ be generators of $\mathrm{Cl}(\mathcal{O}_K)$ and $d_i, \alpha_i$ such that $\mathfrak{g}_i^{d_i} = (\alpha_i)\mathcal{O}_K$. $M_2 \leftarrow \mathrm{diag}(d_i)$.
  For each $\alpha_i$, find $\vec{v}_i$ such that $\overline{\alpha_i} = (g_j)_{j\leq k}^{\vec{v}_i}$ where $\overline{\alpha_i}$ is the image of $\alpha_i$ in $\bigoplus_{\mathfrak{p}|f} {\mathcal{O}_K}_{\mathfrak{p}}^*/\mathcal{O}_{\mathfrak{p}}^*$.
  $M_3 \leftarrow (-\vec{v}_i)_{i\leq l}$. $M \leftarrow \begin{pmatrix} M_1 & (0) \\ M_3 & M_2 \end{pmatrix}$.
  Let $G_1, \cdots, G_k \leftarrow g_1, \cdots, g_k$. $G_{k+1}, \cdots, G_{k+l} \leftarrow \mathfrak{g}_1, \cdots, \mathfrak{g}_l$.
  return $(G_i)_{i\leq k+l}$, $M$.
```

relations between them. Moreover, according to the exact sequence of (7.1), the image of $\bigoplus_{\mathfrak{p}|f} {\mathcal{O}_K}_{\mathfrak{p}}{}^* / \mathcal{O}_{\mathfrak{p}}^*$ is the kernel of $\mathrm{Cl}(-d) \to \mathrm{Cl}(-d_K)$. This means that products $\prod_i g_i^x$ are mapped to (classes of) principal ideals of the form $\prod_j \mathfrak{g}_j^{y_j}$. The only way to form a relation involving the $(g_i)_{i\leq k}$ and the $(\mathfrak{g}_j)_{j\leq l}$ is therefore to have a relation of the form $\prod_j \mathfrak{g}_j^{y_j} = (\alpha)$ (from $\mathrm{Cl}(-d_K)$), and to decompose the class $\overline{\alpha}$ of α in $\bigoplus_{\mathfrak{p}|f} {\mathcal{O}_K}_{\mathfrak{p}}{}^* / \mathcal{O}_{\mathfrak{p}}^*$ with respect to $g_1, \ldots, g_k$ thus giving that $\prod_i g_i^{x_i} = \prod_j \mathfrak{g}_j^{y_j}$ (the equality being considered in $\mathrm{Cl}(-d)$). This means that $\vec{x} - \vec{y}$ is a relation between generators of $\mathrm{Cl}(-d)$. The submatrix $(M_1 \mid (0))$ corresponds to the choice of $\vec{y} = \vec{0}$ (in which case we just take relations between the $(g_i)_{i\leq k}$). The rows of $(M_3 \mid M_2)$ correspond to choices of $\vec{y}$ that span the lattice of relations between the $\mathfrak{g}_i$, i.e. such that $\prod_j \mathfrak{g}_j^{y_j} = (\alpha)$ for some α. Altogether, the rows of $\begin{pmatrix} M_1 & (0) \\ M_3 & M_2 \end{pmatrix}$ span the lattice of relations between the generators of $\mathrm{Cl}(-d)$.

Now we move to the estimation of the cost of this procedure. To compute $\mathfrak{g}_1, \ldots, \mathfrak{g}_k$, one needs to compute $\mathrm{Cl}(-d_K)$. As we've seen in Section 7.1, this comes with a relation matrix $H \in \mathbb{Z}^{n_0 \times n_0}$ between the prime forms of norm less than $\log^{2+o(1)} d$. Then a polynomial time procedure can yield unimodular matrices U, V such that $UHV = \mathrm{diag}(d_i)$. Then the coefficients of V^{-1} give us the generators of the $\mathfrak{g}_j$ according to the following procedure.

Lemma 7.1 *Let U, V such that $UHV = \mathrm{diag}(d_i)$ where $H \in \mathbb{Z}^{n_0\times n_0}$ is a basis of the lattice of relations between the prime forms of norm less than $\log^{2+o(1)} d$. Then each generator $\mathfrak{g}_k$ of order d_k is obtained by using the coefficients of the k-th row of V^{-1}:*

$$\mathfrak{g}_k = f_1^{v_{k,1}^{-1}} f_2^{v_{k,2}^{-1}} \ldots f_{n_0}^{v_{k,n_0}^{-1}}.$$

Proof: We start by proving that HV is a relation matrix for the $\mathfrak{g}_k$ we just defined, that is to say, we want to show that each row of HV is a relation. We denote by $HV_{i,k}$ the coefficient i, k of HV. From the definition of the $\mathfrak{g}_k$, we have that the coefficients of the i-th row of HV satisfy

$$\begin{aligned}\prod_k \mathfrak{g}_k^{HV_{i,k}} &= \prod_k \prod_j \mathfrak{p}_j^{HV_{i,k} V_{k,j}^{-1}} = \prod_j \mathfrak{p}_j^{\sum_k HV_{i,k} V_{k,j}^{-1}} \\ &= \prod_j \mathfrak{p}_j^{(HVV^{-1})_{i,j}} = \prod_j \mathfrak{p}_j^{H_{i,j}} = 1_{\mathrm{Cl}(\mathcal{O}_K)}\end{aligned}$$

The last equality simply derives from the fact that the row i of H is a relation for the $\mathfrak{p}_j$. Now since U is unimodular, the rows of $UHV = \mathrm{diag}(d_i)$ generate the same lattice of relations as the rows of HV.

Finally, there cannot be more relations between the $(\mathfrak{g}_k)_{k\leq n_0}$ because the transformation between the $\mathfrak{p}_j$ and the $\mathfrak{g}_k$ is invertible. Therefore $\langle([\mathfrak{p}_j])_{j\leq n_0}\rangle = \langle([\mathfrak{g}_k])_{k\leq n_0}\rangle$, and in particular, we know that the determinant of the lattice of relations between the $\mathfrak{p}_j$ is the same as the determinant of the lattice of relations between the $\mathfrak{g}_k$ (i.e. the class number). Therefore, the $\mathfrak{g}_k$ must be the generators of the cycles of order d_k in the decomposition $\mathrm{Cl}(-d_k) = \bigoplus_i \mathbb{Z}/d_i\mathbb{Z}$. ■

We can drop the $\mathfrak{g}_j$ where $d_j = 1$ from the list as they are trivial and therefore keep only $k \leq n_0$ of them. The creation of $\bigoplus_{\mathfrak{p}|f} {\mathcal{O}_K}_{\mathfrak{p}}^{\ *} /\mathcal{O}_{\mathfrak{p}}^*$ requires the factorization of the conductor f. Finally, for each $\vec{v}_i$ in Step 3 comes at the cost of solving discrete logarithms with respect to the generators of $(\mathcal{O}_K/\mathfrak{p})^*$ for each of the polynomially many divisors $\mathfrak{p}$ of f.

Proposition 7.2 *The cost of Algorithm 1 is given by*

$$\mathrm{Cost}(\textit{Class Group of } \mathrm{Cl}(-d_K)) + \mathrm{Cost}(\textit{Factorization of } f) + \mathrm{Cost}(\textit{DLP in } (\mathcal{O}_K/\mathfrak{p})^*).$$

A similar procedure giving the decomposition of a given class of ideal with respect to the generators of $\mathrm{Cl}(-d)$ can be derived from the work of Klueners and Pauli as well.

Algorithm 2 Finding the class of $\mathfrak{a} \subseteq \mathcal{O}$ in $\mathrm{Cl}(\mathcal{O})$

```
Require: Ideal $\mathfrak{a}$ in $\mathcal{O} \subseteq \mathcal{O}_K$ of conductor $f$, generators $(G_i)_{i\leq k+l}$ and relations $M$ for $\mathrm{Cl}(\mathcal{O})$. Generators
    $(\mathfrak{g}_j)_{j\leq l}$ for $\mathrm{Cl}(\mathcal{O}_K)$.
Ensure: Vector $\vec{v} \in \mathbb{Z}^{l+k}$ such that $(G_i)_{i\leq k+l}^{\vec{v}}$ is the class of $\mathfrak{a}$.
  Decompose $\mathfrak{a}$ in $\mathrm{Cl}(\mathcal{O}_K)$. Find $\alpha, (x_i)_{i\leq k}$ such that $\mathfrak{a} = (\alpha)\prod_i \mathfrak{g}_i^{x_i}$.
  Decompose $\alpha$ in $\bigoplus_{\mathfrak{p}|f} {\mathcal{O}_K}_{\mathfrak{p}}^{*}/\mathcal{O}_{\mathfrak{p}}^*$. Find $(y_j)_{j\leq l}$ such that $\overline{\alpha} = \prod_j g_j^{y_j}$.
  Let $\vec{v} = (x_1, \cdots, x_k, y_1, \cdots, y_l)$.
  return $\vec{v}$.
```

References

[1] J.-F. Biasse, C. Fieker, and M. Jacobson. Fast heuristic algorithms for computing relations in the class group of a quadratic order, with applications to isogeny evaluation. *LMS Journal of Computation and Mathematics*, 19(A):371–390, 2016.

[2] G. Bisson and A. Sutherland. Computing the endomorphism ring of an ordinary elliptic curve over a finite field. *Journal of Number Theory*, 131(5):815 – 831, 2011. Elliptic Curve Cryptography.

[3] J.L. Hafner and K.S. McCurley. A rigorous subexponential algorithm for computation of class groups. *J. Amer. Math. Soc.*, 2:837–850, 1989.