Arithmetic on Abelian and Kummer varieties

2014/12/18 — **Séminaire de Théorie des Nombres** — Caen

David Lubicz, **Damien Robert**

Differential addition

- Notations: $x, y, X = x + y, Y = x - y$, $0_A = (a_i)$;
- $$z_i^{\chi} = \Big(\sum_{t \in Z(\overline{2})} \chi(t) x_{i+t} x_t\Big)\Big(\sum_{t \in Z(\overline{2})} \chi(t) y_{i+t} y_t\Big) / \Big(\sum_{t \in Z(\overline{2})} \chi(t) a_{i+t} a_t\Big).$$
- $$\begin{aligned} 4X_{00}Y_{00} &= z_{00}^{00} + z_{00}^{01} + z_{00}^{10} + z_{00}^{11}; \\ 4X_{01}Y_{01} &= z_{00}^{00} - z_{00}^{01} + z_{00}^{10} + z_{00}^{11}; \\ 4X_{10}Y_{10} &= z_{00}^{00} + z_{00}^{01} - z_{00}^{10} - z_{00}^{11}; \\ 4X_{11}Y_{11} &= z_{00}^{00} - z_{00}^{01} - z_{00}^{10} + z_{00}^{11}; \end{aligned}$$

$\Rightarrow$ $7M + 12S + 9M_0$ for the differential addition (here we neglect multiplications by constants).

Remark

$\left(\sum_t \chi(t) a_{i+t} a_t\right)$ is simply the classical theta null point $\vartheta\left[\begin{smallmatrix}\chi/2 \\ i/2\end{smallmatrix}\right](0, \Omega)^2$.

Normal additions

- $$\begin{aligned}
2(X_{10}Y_{00}+X_{00}Y_{10}) &= z_{10}^{00}+z_{10}^{01};\\
2(X_{11}Y_{01}+X_{01}Y_{11}) &= z_{10}^{00}-z_{10}^{01};\\
2(X_{01}Y_{00}+X_{00}Y_{01}) &= z_{01}^{00}+z_{01}^{10};\\
2(X_{11}Y_{10}+X_{10}Y_{11}) &= z_{01}^{00}-z_{01}^{10};\\
2(X_{11}Y_{00}+X_{00}Y_{11}) &= z_{11}^{00}+z_{11}^{11};\\
2(X_{01}Y_{10}+X_{10}Y_{01}) &= z_{11}^{00}-z_{11}^{11};
\end{aligned}$$

$\Rightarrow$ $(4M+8S+3M_0)+3\times(2M+4S+2M_0)=10M+20S+9M_0$ to compute all the κ_{ij}.

Normal additions, explicit coordinates

- $\mathfrak{P}_\alpha(Z) = Z^2 - 2\frac{\kappa_{\alpha 0}}{\kappa_{00}} Z + \frac{\kappa_{\alpha\alpha}}{\kappa_{00}}$ whose roots are $\{\frac{X_\alpha}{X_0}, \frac{Y_\alpha}{Y_0}\}$;
- We can recover the coordinates X_i, Y_i by solving the equation

$$\begin{pmatrix} 1 & 1 \\ Z & Z' \end{pmatrix} \begin{pmatrix} Y_i/Y_0 \\ X_i/X_0 \end{pmatrix} = \begin{pmatrix} 2\kappa_{0i}/\kappa_{00} \\ 2\kappa_{\alpha i}/\kappa_{00} \end{pmatrix};$$

- We find

$$X_i = \frac{X_\alpha \kappa_{0i} - X_0 \kappa_{\alpha i}}{X_\alpha \kappa_{00} - X_0 \kappa_{\alpha 0}}.$$

$\Rightarrow$ $(10M + 20S + 9M_0) + 8M = 18M + 20S + 9M_0$ to compute X once we know Z.

Compatible additions

- Let $P_1 = X^2 + aX + b$ and $P_2 = X^2 + cX + d$. Then P_1 and P_2 have a common root iff $(ad - bc)(c - a) = (d - b)^2$, in this case this root is $(d - b)/(a - c)$.
- A compatible addition amount to computing a normal addition $x + y$, and finding a root of $\mathfrak{P}_\alpha$ as a common root of the polynomial $\mathfrak{P}'_\alpha$ coming from the addition of $(x + t, y + t)$;
- So for a compatible addition we need the extra computation of $\mathfrak{P}'_\alpha$ $\Rightarrow 6M + 12S + 5M_0$;
- The common root is

$$\frac{\kappa'_{\alpha\alpha}\kappa'_{00} - \kappa_{\alpha\alpha}\kappa_{00}}{2(\kappa'_{\alpha 0} - \kappa_{\alpha 0})};$$

$\Rightarrow$ $28M + 32S + 14M_0$;

- In the $(x, x + t)$ representation, once we have computed $x + y$ via a compatible addition, we can reuse some operations in the computation of $x + y + t$;
- Still, it is more efficient to use a three way addition to compute $x + y + t$ rather than another compatible addition.
- Possible improvements: find better normalisations, use the equation of the Kummer surface ...