Arithmetic on Abelian and Kummer varieties

2014/04/16 — **Institut Fourier** — Grenoble

David Lubicz, **Damien Robert**

Differential addition

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

$\Rightarrow$ $8S + 4M + 4I = 14M + 8S$ for the differential addition (here we neglect multiplications by constants).

Remark

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

Normal additions

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

$\Rightarrow$ $(8S+4M)+3\times(4M+2M)=22M+8S$ to compute all the κ_{ij}.

Normal additions, explicit coordinates

- We work with the polynomial $\mathfrak{P}_\alpha = Z^2 - 2\kappa_{\alpha 0} Z + \kappa_{\alpha\alpha}\kappa_{00}$, whose roots are $Z = X_\alpha Y_0$ and $Z' = X_0 Y_\alpha$;
- We can as well assume that $Y_0 = 1$ (projective coordinates);
- The equation to solve is then

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

- We get $X_i = (-\kappa_{0i} + \kappa_{00}\kappa_{\alpha i})/(Z' - Z)$;

$\Rightarrow$ $24M + 8S + I = 26M + 8S$ 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 $\mathfrak{P}'_\alpha \Rightarrow 10M + 8S$;
- The common root is

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

$\Rightarrow$ $36M + 16S + 2M + 1I = 41M + 16S$;

- 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 $x + y + t$, we gain $-4S - 6M - 4S - 2M$ for a cost of $33M + 8S$;
- Still, it may be more efficient to use a three way addition to compute $x + y + t$ rather than another compatible addition, since this cost $12M + 8I = 32M$;
- I have not used the projectivity all the time, probably a lot to gain...