Formulas for elliptic curves

Shahed Sharif

June 11, 2009

Given

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

we define

$$\begin{array}{l} b_2{=}a_1^2 + 4a_2 \\ b_4{=}2a_4 + a_1a_3 \\ b_6{=}a_3^2 + 4a_6 \\ b_8{=}a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 \\ \hline c_4{=}b_2^2 - 24b_4 \\ c_6{=}-b_2^3 + 36b_2b_4 - 216b_6 \\ \hline \Delta{=}b_2^2b_8 - 8b_4^3 - 27b_6^3 + 9b_2b_4b_6 \\ j{=}c_4^3/\Delta \end{array}$$

Then E is also given by $y^2 = x^3 - 27c_4x - 54c_6$. In the original equation, the duplication formula is

$$x([2]P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 + b_2x^2 + 2b_4x + b_6}.$$

Now suppose E is given by $y^2 = x^3+ax^2+bx$, with discriminant $16b^2(a^2-4b)$. Let $T = (0, 0)$. Consider the quadratic extension over the base field given by adjoining $\sqrt{d}$ for some non-square d, and let σ denote the nontrivial automorphism. Let ξ be the cocycle over this extension given by $\xi_\sigma = T$. Then the corresponding torsor has equation

$$C : dw^2 = d^2 - 2adz^2 + (a^2 - 4b)z^4.$$