PART III ELLIPTIC CURVES
FORMULA SHEET

A Weierstrass equation, over a field K, is an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

with coefficients $a_1, \dots, a_6$ in K. If $\mathrm{char}(K) \neq 2$ then we may replace y by $\frac{1}{2}(y - a_1x - a_3)$ to obtain an equation of the form

$$y^2 = 4x^3 + b_2x^2 + 2b_4x + b_6$$

where

$$b_2 = a_1^2 + 4a_2, \quad b_4 = 2a_4 + a_1a_3, \quad b_6 = a_3^2 + 4a_6.$$

If further $\mathrm{char}(K) \neq 3$ then we may replace x by $\frac{1}{36}(x - 3b_2)$ and y by $\frac{1}{108}y$ to obtain

$$y^2 = x^3 - 27c_4x - 54c_6$$

where

$$c_4 = b_2^2 - 24b_4, \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6.$$

The discriminant $\Delta \in \mathbb{Z}[a_1, \dots, a_6]$ is defined by

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$$

where

$$b_8 = a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2.$$

It can be shown that (1) defines a smooth projective curve (and hence an elliptic curve, with origin the point at infinity) if and only if $\Delta \neq 0$. If $\mathrm{char}(K) \neq 2$ then this already follows from the usual formula for the discriminant of a cubic polynomial. A separate argument is required in the case $\mathrm{char}(K) = 2$.

The following relations may also be verified

$$4b_8 = b_2b_6 - b_4^2, \quad c_4^3 - c_6^2 = 1728\Delta.$$

The j-invariant is $j = c_4^3/\Delta$.

If $\mathrm{char}(K) \neq 2, 3$ it suffices to consider elliptic curves of the form

$$y^2 = x^3 + ax + b \tag{2}$$

in which case

$$\Delta = -16(4a^3 + 27b^2), \quad j = \frac{1728(4a^3)}{4a^3 + 27b^2}.$$

Date: 26th January 2024.

Any two Weierstrass equations for the same elliptic curve E over K are related by substitutions of the form

$$\begin{aligned} x &= u^2x' + r \\ y &= u^3y' + u^2sx' + t \end{aligned}$$

where $u, r, s, t \in K$ with $u \neq 0$. The coefficients a_i' of the new Weierstrass equation are related to the coefficients a_i of the old via

$$\begin{aligned} ua_1' &= a_1 + 2s \\ u^2a_2' &= a_2 - sa_1 + 3r - s^2 \\ u^3a_3' &= a_3 + ra_1 + 2t \\ u^4a_4' &= a_4 - sa_3 + 2ra_2 - (rs+t)a_1 + 3r^2 - 2st \\ u^6a_6' &= a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1. \end{aligned} \tag{3}$$

The various associated quantities are transformed by

$$\begin{aligned} u^2b_2' &= b_2 + 12r \\ u^4b_4' &= b_4 + rb_2 + 6r^2 \\ u^6b_6' &= b_6 + 2rb_4 + r^2b_2 + 4r^3 \\ u^8b_8' &= b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \end{aligned} \tag{4}$$

and $u^4c_4' = c_4$, $u^6c_6' = c_6$, $u^{12}\Delta' = \Delta$, $j' = j$.

Let $P_1 = (x_1, y_1)$ and $P_2 = (x_2, y_2)$ be points on (1) with $P_1, P_2, P_1 + P_2 \neq 0_E$. Then $P_3 = P_1 + P_2 = (x_3, y_3)$ is given by

$$\begin{aligned} x_3 &= \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_3 &= -(\lambda + a_1)x_3 - \nu - a_3 \end{aligned}$$

where if $x_1 \neq x_2$ then

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}, \quad \nu = \frac{y_1x_2 - y_2x_1}{x_2 - x_1},$$

and if $x_1 = x_2$ then

$$\lambda = \frac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, \quad \nu = \frac{-x_1^3 + a_4x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}.$$

It is sometimes convenient to work with formulae in x only. Specialising to the shorter Weierstrass form (2), assuming $P_1 \neq P_2$, and putting $P_4 = P_1 - P_2 = (x_4, y_4)$, we obtain

$$\begin{aligned} x_3 + x_4 &= \frac{2(x_1x_2 + a)(x_1 + x_2) + 4b}{(x_1 - x_2)^2}, \\ x_3x_4 &= \frac{x_1^2x_2^2 - 2ax_1x_2 - 4b(x_1 + x_2) + a^2}{(x_1 - x_2)^2}. \end{aligned}$$