Problem class 5

1. Let $C : Y^2Z = X^3 + A\,XZ^2 + B\,Z^3$ be a Weierstrass equation over a field k of characteristic not 2. Suppose $\Delta = 0$. Show that $(3B : 0 : -2A)$ is a singular point in $C(k)$ and hence C is not smooth.

Solution: The characteristic of k is not 2, therefore $\Delta = -16 \cdot (4A^3 + 27B^2) = 0$ implies $4A^3 + 27B^2 = 0$. We claim this point $(3B : 0 : -2A)$ lies in $C(k)$:

$$\begin{aligned} 0 = Y^2Z = X^3 + A\,XZ^2 + B\,Z^3 &= (3B)^3 + A(3B)(-2A)^2 + B(-2A)^3 \\ &= B(27B^2 + 12A^3 - 8A^3) = 0 \end{aligned}$$

We claim this is a singular point. The three partial derivatives confirm this

$$\begin{aligned} \partial X : &\qquad 0 = 3X^2 + A\,Z^2 = 3(3B)^2 + A\,(-2A)^2 = 0; \\ \partial Y : &\qquad 2YZ = 0; \\ \partial Z : &\qquad 0 = Y^2 = 2AXZ + 3BZ^2 = 2A(3B)(-2A) + 3B(-2A)^2 = 0. \end{aligned}$$

2. a) Let $E : y^2 = x^3 + A\,x + B$ be a Weierstrass equation defined over k. Let $D \in k^\times$. Show that there is a transformation between E and the curve $E' : y^2 = x^3 + D^4A\,x + D^6B$.

   b) Determine the discriminant Δ' of E' in terms of the discriminant of E. Define the quantity $j = -1728\,(4A)^3/\Delta$ called the **j-invariant**. Prove that this quantity is invariant under this transformation.

   c) Show that every Weierstrass equation E defined over $k = \mathbb{Q}$ can be transformed into a Weierstrass equation with A and B integers.

Solution:

a) We start by multiplying the Weierstrass equation by D^6:

$$D^6y^2 = D^6x^3 + D^6A\,x + BD^6$$

Now using $y' = D^3y$ and $x' = D^2x$, we find

$$y'^2 = (D^3\,y)^2 = D^6y^2 = (D^2\,x)^3 + D^4A\,(D^2x) + BD^6 = x'^3 + D^4A\,x' + D^6B.$$

b) The discriminant of E' is

$$\Delta' = -16 \cdot \big(4(D^4\,A)^3 + 27(D^6\,B)^2\big) = -16(D^{12}\,4A^3 + D^{12}\,27B^2) = D^{12} \cdot \Delta.$$

Now the j-invariant of E' is

$$j' = -1728\frac{(4D^4A)^3}{\Delta'} = -1728\frac{D^{12}(4A)^3}{D^{12}\Delta} = -1728\frac{(4A)^3}{\Delta} = j.$$

c) Suppose $E : y^2 = x^3 + A\,x + B$ is a Weierstrass equation with A and B in $\mathbb{Q}$. Let d be the common denominator of A and B. Then $E' : y^2 = x^3 + d^4 A\,x + d^6\,B$ is a Weierstrass equation with $d^4 A$ and $d^6 B$ integers.

3. Let E be the cubic curve given by

$$Y^2 Z + a_1\,XYZ + a_3\,YZ^2 = X^3 + a_2\,X^2 Z + a_4\,XZ^2 + a_6\,Z^3$$

with $a_1, a_2, a_3, a_4, a_6 \in k$. Suppose that it is non-singular. Let $O = (0 : 1 : 0) \in E(k)$. Let $P = (x_P : y_P : 1)$ and $Q = (x_Q : y_Q : 1)$.

a) Prove that O is the unique point of E at infinity and that it is an inflection point.

b) Show that $-P = (x_P, -y_P - a_1\,x_P - a_3)$.

c) Spell out the procedure to compute $P + Q$.

d) Do the same for $2\,P$.

Solution:

a) Taking $Z = 0$, we find the equation $X^3 = 0$. This shows that the line at infinity intersects E only at $O = (0 : 1 : 0)$. Since the intersection multiplicity is 3, this is an inflection point.

b) Since O is an inflection point, we have $\hat{O} = O$. Just as for the Weierstrass equation, this shows that the lines through O have affine form $x = c$ for a constant $c \in k$. Therefore the x-coordinate of $-P$ is the same as P. It follows that y_P and y_{-P} are solutions to the equation

$$0 = y^2 + (a_1\,x_P + a_3)\,y + (-x_P^3 - a_2 x_P^2 - a_4 x_P - a_6) = (y - y_P)(y - y_{-P}).$$

From the linear term, we deduce $a_1 x_P + a_3 = -y_P - y_{-P}$ which gives the desired statement.

c) The line $y = \lambda\,x + \nu$ through P and Q still can be determined with

$$\lambda = \frac{y_P - y_Q}{x_P - x_Q} \qquad \text{and} \qquad \nu = y_P - \lambda\,x_P.$$

Then we intersect with the given equation

$$\begin{aligned}(\lambda x + \nu)^2 + a_1(\lambda x + \nu)x + a_3(\lambda x + \nu) &= x^3 + a_2 x^2 + a_4 x + a_6 \\ 0 &= x^3 + (a_2 - \lambda^2 - a_1\lambda)\,x^2 + \cdots \\ &= (x - x_P)(x - x_Q)(x - x_R)\end{aligned}$$

and we consider the quadratic coefficient to find

$$x_{P+Q} = x_R = \lambda^2 + a_1\lambda - a_2 - x_P - x_Q.$$

Then $y_R = \lambda x_R + \nu$ gives R and the formula found in the previous part combines to

$$y_{P+Q} = -y_R - a_1\,x_R - a_3 = -(\lambda + a_1)\,x_R - a_3 - \nu.$$

d) The duplication formula is only different in that we need to find the slope λ of the tangent $T_P(E)$. The tangent is

$$(3x_P^2 + 2\,a_2x_P + a_4 - a_1y_P)\,X + (-2\,y_P - a_1x_P - a_3)\,Y + (\cdots)\,Z = 0$$

which gives

$$\lambda = \frac{3x_P^2 + 2\,a_2x_P + a_4 - a_1y_P}{2y_P + a_1x_P + a_3}.$$

4. Let C_1 and C_2 be the cubics defined over $\mathbb{R}$ by

$$C_1\colon\ X^3 + 2\,Y^3 - XZ^2 - 2\,YZ^2 = 0 \text{ and } C_2\colon\ 2\,X^3 - Y^3 - 2\,XZ^2 + YZ^2 = 0.$$

a) Find the nine points $\{P_1, P_2, \ldots, P_9\}$ of intersection of C_1 and C_2.

b) (Long!) Set $P_1 = (0:0:1)$. Prove that if a cubic passes through P_2, P_3, $\ldots$, P_9 then it also passes through P_1.

Solution:

a) Subtracting the second equation C_2 from twice the first C_1 gives $0 = 5Y^3 - 5YZ^2 = 5\,Y(Y+Z)(Y-Z)$. The other way, subtracting the first from twice the second yields $0 = 5\,X(X+Z)(X-Z)$. Hence $Z \neq 0$, we can take $Z = 1$ and then $X \in \{-1, 0, 1\}$ and $Y \in \{-1, 0, 1\}$. An indeed all nine choices give points in the intersection:

$$\begin{aligned} C_1 \cap C_2 = \big\{&(0:0:1), (0:1:1), (0:-1:1),\\ &(1:0:1), (1:1:1), (1:-1:1), (-1:0:1), (-1:1:1), (-1:-1:1)\big\} \end{aligned}$$

b) A general cubic can be written as

$$\begin{aligned} b_0\,X^3 + b_1\,X^2Y + b_2\,X^2Z + b_3\,XY^2 + b_4\,XYZ +\\ + b_5\,XZ^2 + b_6\,Y^3 + b_7\,Y^2Z + b_8\,YZ^2 + b_9\,Z^3 = 0 \end{aligned}$$

When we intersect with the line $Y = Z$, we must see the three intersection points $(1:1:1)$, $(0:1:1)$ and $(-1:1:1)$. Therefore we get

$$\begin{aligned} b_0\,X^3 + (b_1 + b_2)\,X^2Y + (b_3 + b_4 + b_5)\,XY^2 + (b_6 + b_7 + b_8 + b_9)\,Y^3 =\\ = cX(X+Y)(X-Y) = cX^3 - cXY^2 \end{aligned}$$

for some constant c. Therefore $b_1 + b_2 = 0$, $b_6 + b_7 + b_8 + b_9 = 0$ and $b_0 = -(b_3 + b_4 + b_5)$. We can do the same with the line $Y = -Z$.

$$\begin{aligned} b_0\,X^3 + (b_1 - b_2)\,X^2Y + (b_3 - b_4 + b_5)\,XY^2 + (b_6 - b_7 + b_8 - b_9)\,Y^3 =\\ = c'X(X+Y)(X-Y) \end{aligned}$$

gives us $b_1 - b_2 = 0$, $b_6 - b_7 + b_8 - b_9 = 0$ and $b_0 = -(b_3 - b_4 + b_5)$.

So far we have learnt that $b_1 = b_2 = 0$, $b_8 = -b_6$, $b_9 = -b_7$, $b_4 = 0$ and $b_5 = -b_0 - b_3$.

$$b_0\,(X^3 - XZ^2) + b_3\,(XY^2 - XZ^2) + b_6\,(Y^3 - YZ^2) + b_7\,(Y^2Z - Z^3) = 0$$

We intersect now with the line $Y = 0$. Here we know that $(1 : 0 : 1)$ and $(-1 : 0 : 1)$ are solutions, but we do not know the third intersection yet. Therefore $b_0\,(X^3 - XZ^2) - b_3XZ^2 - b_7Z^3$ is zero for $(X : Z) = (1 : 1)$, giving $-b_3 - b_7 = 0$, and for $(X : Z) = (-1 : 1)$, giving $b_3 - b_7 = 0$. Adding these two gives $b_3 = b_7 = 0$. We conclude that any cubic passing through these 8 points is of the form

$$b_0\,(X^3 - XZ^2) + b_6\,(Y^3 - YZ^2) = 0.$$

They indeed all pass through $(0 : 0 : 1)$. The three curves in Figure 20 in the notes are from this family of curves.