Problem class 6

1. Let E be the elliptic curve defined over $\mathbb{Q}$ given by $y^2 = x^3 + x + 3$. Let $P = (-1 : 1 : 1)$. Compute $-P$, $2\,P$, $3\,P$ and $4\,P$.

Solution: The equation is in Weierstrass form so the inverse $-P$ is simply $(-1 : -1 : 1)$.

To compute $2\,P$ we use the formulae for duplication.

$$\lambda = \frac{3x_P^2 + A}{2y_P} = \frac{3 \cdot (-1)^2 + 1}{2 \cdot 1} = 2 \quad \text{and} \quad \nu = y_P - \lambda x_P = 1 - 2 \cdot (-1) = 3.$$

Then R is

$$x_R = \lambda^2 - 2x_P = 2^2 - 2 \cdot (-1) = 6 \quad \text{and} \quad y_R = \lambda x_R + \nu = 2 \cdot 6 + 3 = 15.$$

This yields $2\,P = (6 : -15 : 1)$.

To evaluate $3\,P$ we will sum $2\,P$ and P.

$$\lambda = \frac{y_{2P} - y_P}{x_{2P} - x_P} = \frac{-15 - 1}{6 - (-1)} = -\frac{16}{7} \quad \text{and}$$
$$\nu = y_P - \lambda x_P = 1 - \left(-\tfrac{16}{7}\right) \cdot (-1) = -\frac{9}{7}$$

which allows us to get the point R as

$$x_R = \lambda^2 - x_{2P} - x_P = \left(-\frac{16}{7}\right)^2 - 6 - (-1) = \frac{256 - 5 \cdot 49}{49} = \frac{11}{49}$$
$$y_R = \lambda x_R + \nu = -\frac{16}{7} \cdot \frac{11}{49} - \frac{9}{7} = -\frac{617}{343}$$

and thus $3\,P = \left(\frac{11}{49} : -\frac{617}{343} : 1\right) = (77 : -617 : 343)$.

To find $4\,P$ we can either add P to $3\,P$ or multiply $2\,P$ by 2. We do the latter:

$$\lambda = \frac{3 \cdot 6^2 + 1}{2 \cdot (-15)} = -\frac{109}{30} \quad \text{and} \quad \nu = (-15) - \left(-\frac{109}{30}\right) \cdot 6 = \frac{34}{5}$$

which tells us that the point R is determined by

$$x_R = \left(-\frac{109}{30}\right)^2 - 2 \cdot 6 = \frac{1081}{900} \quad \text{and} \quad y_R = -\frac{109}{30} \cdot \frac{1081}{900} + \frac{34}{5} = \frac{65771}{27000}$$

and hence $4\,P = \left(\frac{1081}{900} : -\frac{65771}{27000} : 1\right) = (32430 : -65771 : 27000)$.

2. Let E be the elliptic curve $y^2 = x^3 + 2\,x - 1$ defined over $\mathbb{F}_5$.

a) Find all points in $E(\mathbb{F}_5)$. (The number of them will be a prime.)

b) Pick a point P as a generator of this cyclic group and write all other points as a multiple of your P.

Solution:

a) There is the point $O = (0 : 1 : 0)$ at infinity. Then for $x = 0$, we find $y^2 = -1$ which has two solutions namely $y = 2$ and $y = 3$. This gives the points $(0 : 2 : 1)$ and $(0 : 3 : 1)$. For $x = 1$, the equation is $y^2 = 2$ which has no solution in $\mathbb{F}_5$. For $x = 2$ it is $y^2 = 1$ which adds the points $(2 : 1 : 1)$ and $(2 : 4 : 1)$. When $x = 3$ there are no solutions to $y^2 = 2$. Finally when $x = -1$ then $y^2 = 1$ give the last two points $(-1 : 1 : 1)$ and $(-1 : -1 : 1)$. In summary we have

$$E(\mathbb{F}_5) = \Big\{O,\ (0:2:1),\ (0:3:1),\ (2:1:1),\\ (2:4:1),\ (4:1:1),\ (4:4:1)\Big\}$$

b) The solution for this part depends on the choice of P. Here we pick $P = (0 : 2 : 1)$. We know that $7\,P = O$ so the points found must be of the form $j\,P$ for $0 \leqslant j \leqslant 6$.

First $-P = 6\,P$ is simply $(0 : -2 : 1) = (0 : 3 : 1)$.

Now we compute $2\,P$:

$$\begin{aligned} \lambda &= \frac{3\,0^2 + 2}{2 \cdot 2} = \frac{1}{2} = 3 \\ \nu &= 2 - 3 \cdot 0 = 2 \\ x_R &= 3^2 - 2 \cdot 0 = 4 \\ y_R &= 3 \cdot 4 + 2 = 4 \end{aligned}$$

Therefore $2\,P = (4, -4) = (4 : 1 : 1)$. For free we gain $-2\,P = 5\,P = (4 : 4 : 1)$.

Next, we need $3\,P$. We add $P = (0, 2)$ and $2\,P = (4, 1)$:

$$\begin{aligned} \lambda &= \frac{2 - 1}{0 - 4} = \frac{1}{1} = 1 \\ \nu &= 2 - 1 \cdot 0 = 2 \\ x_R &= 1^2 - 0 - 4 = 2 \\ y_R &= 1 \cdot 2 + 2 = 4 \end{aligned}$$

Therefore $3\,P = (2, -4) = (2 : 1 : 1)$. Also $-3\,P = 4\,P = (2 : 4 : 1)$ which gives us the complete list:

$$E(\mathbb{F}_5) = \Big\{0\,P = O,\ 1\,P = (0:2:1),\ 2\,P = (4:1:1),\ 3\,P = (2:1:1),\\ 4\,P = (2:4:1),\ 5\,P = (4:4:1),\ 6\,P = (0:3:1)\Big\}$$

3. Let a be an element in a field k of characteristic different from 2 and 3. Consider the cubic

$$C: \qquad Y^2Z + XYZ = X^3 + a\,XZ^2$$

which contains the point $O = (0:1:0)$ and the point $P = (0:0:1)$.

a) For which a is the cubic smooth.

b) Write out the formula for the point $P + Q$ where $Q = (x_Q : y_Q : 1) \neq P$.

c) Use this to verify that $(Q + P) + P = Q$.

Solution:

a) Let $(X : Y : Z)$ be a singular point on C. The three partial derivatives give the equations

$$\begin{aligned} YZ &= 3X^2 + a\,Z^2 \\ 2YZ + XZ &= 0 \\ Y^2 + XY &= 2a\,XZ \end{aligned}$$

From the middle equation we learn that either $Z = 0$ or $X = -2Y$. If $Z = 0$, then C tells us that $X = 0$ and therefore we are at the point O. However the third equation above is not valid for O; therefore O is non-singualar.

Hence we have $X = -2Y$. The third equation then becomes $Y^2 - 2Y^2 = -4a\,YZ$. Either $Y = 0$ or $Y = 4a\,Z$. If $Y = 0$ then $X = 0$ and we are at P. However the partial derivative with respect to X is zero at P only if $a = 0$.

Instead if $Y \neq 0$, then $X = -2 \cdot 4aZ = -8aZ$ and we are at the point $(-8a : 4a : 1)$. For this point to satisfy the first of the above equation, we would have $4a = 3(-8)^2 + a$. If $a = 0$, we rediscover the previous case, otherwise $a = 1/64$.

Conclusion: C is smooth if $a \neq 0$ and $a \neq 1/64$. If $a = 0$ then $(0:0:1)$ is singular and if $a = 1/64$ the point $(-1/8 : 1/16 : 1) = (-2 : 1 : 16)$ is singular.

b) The line through $P = (0,0)$ and $Q = (x_Q, y_Q)$ is $y = \lambda x$ with $\lambda = y_Q/x_Q$. This makes sense as $x_Q \neq 0$ since $Q \neq P$. If R is the third point that this line meets the curve then

$$-(\lambda x)^2 - x(\lambda x) + x^3 + a\,x = x(x - x_Q)(x - x_R).$$

The quadratic terms gives $-\lambda^2 - \lambda = -x_Q - x_R$, therefore

$$x_R = \lambda^2 + \lambda - x_Q = \frac{y_Q^2}{x_Q^2} + \frac{y_Q}{x_Q} - x_Q = \frac{y_Q^2 + x_Q y_Q - x_Q^3}{x_Q^2} = \frac{a\,x_Q}{x_Q^2} = \frac{a}{x_Q}.$$

Using $y_R = \lambda x_R$ we find that

$$R = \left(\frac{a}{x_Q}, \frac{a\,y_Q}{x_Q^2}\right).$$

Now we need to find $P+Q=-R$. First of all we have $x_{P+Q}=x_R=a/x_Q$. Then $y^2+x_R\,y-x_R^3-a\,x_R$ must factor as $(y-y_R)(y-y_{P+Q})$. Looking at the linear term in these two expressions, we find $x_R=-y_R-y_{P+Q}$. Therefore $y_{P+Q}=-x_R-y_R$. Hence

$$P+Q=\Big(\frac{a}{x_Q},-\frac{a}{x_Q}-\frac{a\,y_Q}{x_Q^2}\Big)=\Big(\frac{a}{x_Q},-a\frac{x_Q+y_Q}{x_Q^2}\Big).$$

c) By the above formula

$$\begin{aligned}(Q+P)+P&=\Big(\frac{a}{x_{P+Q}},-a\frac{x_{P+Q}+y_{P+Q}}{x_{P+Q}^2}\Big)\\&=\Big(\frac{a}{a/x_Q},-a\frac{a/x_Q-a(x_Q+y_Q)/x_Q^2}{(a/x_Q)^2}\Big)\\&=\Big(x_Q,-a\frac{ax_Q-ax_Q-ay_Q}{a^2}\Big)=(x_Q,y_Q)=Q.\end{aligned}$$

4. Consider the cubic $Y^2Z=X^3$ over a field k with its unique singular point $(0:0:1)$. There is a map $\varphi\colon k\to\mathbb{P}^2(k)$ sending u to $(u:1:u^3)$ that has its image in $C(k)$.

   a) Show that the image is precisely all non-singular point in $C(k)$.

   b) Prove that the map is a group homomorphism from $\langle k,+\rangle$ to the group of non-singular points in $C(k)$.

   [Hint: start by checking $\varphi(-u)=-\varphi(u)$ and that $\varphi(u)$, $\varphi(v)$ and $\varphi(-u-v)$ lie on one line.]

Solution:

a) It is clear that the image of φ is contained in $C(k)\setminus\{(0:0:1)\}$. Conversely, let $P=(X:Y:Z)$ be a point in $C(k)$ which is not equal to $(0:0:1)$. If $Y=0$, then the equation C leads to $X=0$ and so to the point $(0:0:1)$. Therefore $Y\neq 0$ and we can write $P=(X/Y:1:Z/Y)$. Set $u=X/Y\in k$. Then $Z/Y=X^3/Y^3=u^3$. Hence $P=(u:1:u^3)$ is in the image of φ.

b) Recall that it is enough to check that $\varphi(-u)=-\varphi(u)$ for all $u\in k$ and that $u+v+w=0$ implies $\varphi(u)+\varphi(v)+\varphi(w)=0$ for all $u,v,w\in k$.

First $\varphi(-u)=(-u:1:-u^3)=(u:-1:u^3)$. This indeed the reflection of $\varphi(u)$ along the x-axis and hence $\varphi(-u)=-\varphi(u)$ for all $u\in k$.

Let u and v be two distinct elements in k. We wish to check that $\varphi(u)=(u:1:u^3)$ and $\varphi(v:1:v^3)$ and $\varphi(-u-v)=(-u-v:1:(-u-v)^3)$ lie on one

line. This is equivalent to show that the following determinant is zero.

$$\det \begin{pmatrix} u & 1 & u^3 \\ v & 1 & v^3 \\ -u-v & 1 & -u^3-3u^2v-3uv^2-v^3 \end{pmatrix} =$$
$$u \cdot (-u^3-3u^2v-3uv^2-v^3) + v^3 \cdot (-u-v) + u^3 \cdot v$$
$$- u \cdot v^3 - v \cdot (-u^3-3u^2v-3uv^2-v^3) - u^3 \cdot (-u-v)$$

and this cancels indeed to 0. Therefore $\varphi(u) + \varphi(v) + \varphi(-u-v) = O$.

Finally, we have to check that $\varphi(-2u)$ lies on the tangent through $\varphi(u)$ to verify the above equality also in the case when $u = v$. The tangent at $\varphi(u)$ is $3u^2\,X - 2u^3\,Y - Z = 0$. The point $\varphi(-2u) = (-2u : 1 : -8u^3)$ does indeed satisfy this equation.