Elliptic Curves - Example Sheet 1

1. $Dw^2 = uv(u-v)(u+v)$

D	u	v	w	$\frac{u^2-v^2}{w}$	$\frac{2uv}{w}$	$\frac{u^2+v^2}{w}$
6	2	1	1	3	4	5
15	4	1	2	$15/2$	4	$17/2$
21	4	3	2	$7/2$	12	$25/2$
210	5	2	1	21	20	29

2. Putting $y = t(x+1)$ gives $(x,y) = \left(\frac{1-3t^2}{1+t+3t^2}, \frac{2t+t^2}{1+t+3t^2}\right)$

Putting $y = tx$ gives $(x,y) = (t^2-1, t^3-t)$

3. (i) $C_3 = \{U^3+V^3=W^3\} \subset \mathbb{P}^2$

Hessian = const. UVW

There are 9 points of inflection

$(U:V:W) = (\zeta_3^i : 0 : 1), (0 : \zeta_3^i : 1), (\zeta_3^i : -1 : 0)$ $\quad i = 0,1,2.$

$U^3+V^3=W^3 \iff (9Z-Y)^3 + Y^3 = (3X)^3$

$\iff Y^2Z - 9YZ^2 = X^3 - 27Z^3$

Dehomogenising gives $\quad y^2 - 9y = x^3 - 27$

Completing the square gives $\quad y^2 = x^3 - 432$

(N.B. we are free to scale a_6 by a 6^{th} power)

(ii) $y^2 - x^3 + x = \dfrac{(V^4 - W^4 + U^4)W^2}{U^6} = 0$

If $E: y^2 = x^3 - x$ then $E(\mathbb{Q}) = \{0, (0,0), (\pm 1, 0)\}$

(proved in lectures)

So if $(U:V:W) \in C(\mathbb{Q})$ then $UVW = 0$

$\therefore C_4(\mathbb{Q}) = \{(1:0:\pm 1), (0:1:\pm 1)\}$

4. $C_0 = \{y^2 = f(x)\} \subset \mathbb{A}^2$

$(x,y) \in C_0$ singular $\iff \begin{cases} y^2 = f(x) \\ 2y = 0 \\ f'(x) = 0 \end{cases} \iff$ $(x,y) = (\alpha, 0)$ with α a repeated root of f.

Write $f(x) = a_n x^n + \ldots + a_1 x + a_0 \quad a_n \neq 0, \; n \geq 2.$

C_0 has projective closure $C \subset \mathbb{P}^2$ with equation

$Y^2 Z^{n-2} = a_n X^n + \ldots + a_1 X Z^{n-1} + a_0 Z^n$

Putting $Z = 0$ gives $0 = a_n X^n \implies X = 0$

i.e. only point at infinity is $(X:Y:Z) = (0:1:0)$

This is a smooth point if $n = 3$ & singular if $n > 3$.

5. The multiples of $P = (0,0)$ are

$(0,0), (1,0), (-1,-1), (2,-3), \left(\frac{1}{4}, \frac{-5}{8}\right), (6,14)$

$\left(\frac{-5}{9}, \frac{8}{27}\right), \left(\frac{21}{25}, \frac{-69}{125}\right)$

These points are of the form $\left(\frac{r}{t^2}, \frac{s}{t^3}\right) \quad r,s,t \in \mathbb{Z} \quad \begin{matrix}(r,t)=1 \\ (s,t)=1\end{matrix}$

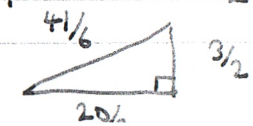
i.e. the denominators are squares & cubes.

6. $Dy^2 = x^3 - x \rightsquigarrow D\left(\frac{y}{D^2}\right)^2 = \left(\frac{x}{D}\right)^3 - \frac{x}{D}$

$\iff y^2 = x^3 - D^2 x$

Some solutions to $5w^2 = uv(u-v)(u+v)$			Corresponding points on $E: y^2 = x^3 - 25x$	
u	v	w	$x = \frac{5u}{v}$	$y = \frac{25w}{v^2}$
5	4	6	$25/4$	$75/8$
-4	5	6	-4	6
9	1	12	45	300
-1	9	12	$-5/9$	$100/27$

These all give the same triangle



If $P = \left(\frac{5u}{v}, \frac{25w}{v^2}\right)$ $\quad 2P = (\xi, \eta)$

$$\xi = \left(\frac{3\left(\frac{5u}{v}\right)^2 - 25}{2\left(\frac{25w}{v^2}\right)}\right)^2 - 2\left(\frac{5u}{v}\right)$$

$$= \frac{(3u^2-v^2)^2 - 8u^2(u^2-v^2)}{4w^2} = \left(\frac{u^2+v^2}{2w}\right)^2$$

We get $\xi = \frac{41^2}{12^2}$ $\quad \eta = \frac{7^2.31.41}{12^3}$

Side lengths $\frac{\eta}{\xi} = \frac{7^2.31}{12.41} = \frac{1519}{492}$

$$\frac{10\xi}{\eta} = \frac{10.12.41}{7^2.31} = \frac{4920}{1519}$$

$$\frac{\xi^2+25}{\eta} = \frac{41^4+25.12^4}{12.7^2.31.41} = \frac{3344161}{747348}$$

7 (i) $E_d : \quad dy^2 = f(x) = x^3 + a_2x^2 + a_4x + a_6$

Replacing x, y by $\frac{x}{d}, \frac{y}{d^2}$ gives

$$d\left(\frac{y}{d^2}\right)^2 = \left(\frac{x}{d}\right)^3 + a_2\left(\frac{x}{d}\right)^2 + a_4\left(\frac{x}{d}\right) + a_6$$

$$\iff \quad y^2 = x^3 + (da_2)x^2 + (d^2a_4)x + (d^3a_6)$$

(ii) $E : \; y^2 = x^3 + ax + b \qquad a, b \in \mathbb{Q}$

$E' : \; y^2 = x^3 + a'x + b' \qquad a', b' \in \mathbb{Q}$

If these curves are twists then $\exists\, u \in \overline{\mathbb{Q}}^*$ s.t.

$a' = u^4 a \qquad j(E) \neq 0, 1728 \implies ab \neq 0$

$b' = u^6 b \qquad \therefore \; u^2 = \frac{ab'}{a'b} \in \mathbb{Q}$

Now $E' \cong E_d$ over $\mathbb{Q}$ $\iff \begin{cases} a' = \lambda^4 d^2 a \\ b' = \lambda^6 d^3 b \end{cases}$ for some $\lambda \in \mathbb{Q}^*$

$$\iff \quad d \equiv u^2 \mod (\mathbb{Q}^*)^2$$

The square free integers form a set of coset reps. for $\mathbb{Q}^*/(\mathbb{Q}^*)^2$.

8. We claim that $j(\lambda) = j(\lambda')$ iff λ and λ' belong to the same orbit when S_3 acts on $\mathbb{P}^1$ via Möbius maps permuting $0, 1, \infty$, i.e. iff

$$\lambda' \in \left\{\lambda, 1-\lambda, \frac{1}{\lambda}, \frac{\lambda-1}{\lambda}, \frac{\lambda}{\lambda-1}, \frac{1}{1-\lambda}\right\}$$

(i) It is easy to check $j(\lambda) = j(1-\lambda) = j\left(\frac{1}{\lambda}\right)$

(ii) An orbit of size 6, containing λ_0 say, accounts for all the roots of the degree 6 polynomial

$$2^8(x^2-x+1)^3 - j(\lambda_0)\, x^2(x-1)^2 = 0$$

(iii) The orbits of size < 6 are $\{-\zeta_3, -\zeta_3^2\}, \{\frac{1}{2}, 2, -1\}$ and $\{0, 1, \infty\}$ corresponding to $j = 0, 1728, \infty$.

9. (i) Using the formula sheet we get (after some calculation)

$$x(2P) = \frac{x^4 - 2ax^2 - 8bx + a^2}{(2y)^2}$$

$$y(2P) = \frac{x^6 + 5ax^4 + 20bx^3 - 5a^2x^2 - 4abx - a^3 - 8b^2}{(2y)^3}$$

(ii) $x(2P) = x(-P)$

$$\iff x^4 - 2ax^2 - 8bx + a^2 = 4x(x^3+ax+b)$$

$$\iff \underbrace{3x^4 + 6ax^2 + 12bx - a^2}_{= g(x)} = 0$$

(iii) $g'(x) = 12(x^3 + ax + b)$

So for a repeated root we would have $2P = 3P = O_E$

$\implies P = O_E$ $\times$

10. (i) Let $E = \left\{ \begin{array}{r} au+bv+cw=0 \\ uvw=t^3 \end{array} \right\} \subset \mathbb{P}^3_{u,v,w,t}$

Eliminating w gives $uv(au+bv) = -ct^3$

Renaming variables $y\left(\frac{-cz}{a}\right)\left(ay+b\left(\frac{-cz}{a}\right)\right) = -cx^3$

$\iff \quad y^2z - \frac{bc}{a^2}yz^2 = x^3$

Dehomogenising: $y^2 - \frac{bc}{a^2}y = x^3$

Multiplying a_3 by a cube: $y^2 - abcy = x^3$

Completing the square: $y^2 = x^3 + 16(abc)^2$

(ii) $\phi : C \to E;\ (X:Y:Z) \mapsto (X^3 : Y^3 : Z^3 : XYZ)$

is a non constant morphism of smooth projective curves

$\therefore \quad \mathrm{Im}(\phi) = E$

(iii) If $P = (x:y:z) \in C$ with $xyz \neq 0$

and $\phi(P) = Q$ then

$\phi^{-1}(Q) = \{(x:y:z), (x:\zeta_3 y:\zeta_3^2 z), (x:\zeta_3^2 y:\zeta_3 z)\}$

$\therefore \deg \phi = 3.$

11. Let $(x,y) \mapsto (u^2x+r,\ u^3y+u^2sx+t)$

be an automorphism of E.

From the formula sheet we have (putting $a_1=a_2=a_4=a_6=0$ & $a_3=1$)

$0 = 2s$

$0 = 3r - s^2$

$u^3 = 1+2t$

$0 = -s+3r^2-2st$

$0 = r^3 - t - t^2$

In characteristic 2 these simplify to

$r = s^2, \quad s = r^2, \quad u^3 = 1, \quad r^3 = t^2+t.$

Solutions: $u = 1, \omega, \omega^2$ (3 choices)

$(r,s,t) = (0,0,0), (0,0,1)$
or $(\omega^i, \omega^{2i}, \omega^j)$ $i=0,1,2$ $j=1,2$ } 8 choices

$\therefore \quad \# \mathrm{Aut}(E) = 24$

Let $\alpha : (x,y) \mapsto (\omega x, y)$

$\beta : (x,y) \mapsto (x+1,\ y+x+\omega)$

We compute $\alpha\beta\alpha^{-1} : (x,y) \mapsto (x+\omega,\ y+\omega^2 x+\omega)$

$\alpha\beta\alpha^{-1} \neq \beta \implies \mathrm{Aut}(E)$ is non-abelian.

12. $K = \mathbb{Q}(\sqrt{d})$, $\mathrm{Gal}(K/\mathbb{Q}) = \{1, \sigma\}$
where $\sigma(\sqrt{d}) = -\sqrt{d}$.

Let $P \in C(K)$. If $\sigma(P) = P$ then $P \in C(\mathbb{Q})$ and we're done. Otherwise draw the line ℓ through P and $\sigma(P)$. Let Q be the third point of intersection of ℓ and C.
Then $\sigma(Q) = Q$ and so $Q \in C(\mathbb{Q})$.