MAC260 Elliptic Curves

Week 8 Problem Class

2. $E: y^2 = x^3 - x + 1$.

Recall if $p/q \in \mathbb{Q}$ with $\gcd(p,q) = 1$

then $H(p/q) = \max\{|p|, |q|\}$

If $P \in E(\mathbb{Q})$ then

$$h_x(P) = \ln H(x(P))$$

Start by guessing a point on E:

Take $P = (1,1)$.

Then $h_x(P) = \ln(H(1)) = \ln(1)$

$= 0$.

So we double.

Week 3 Formulas give

$$x(2P) = m^2 - 2x(P)$$

slope of tangent at P

$$= \left(\frac{3x^2-1}{2y}\right)^2\Big|_P - 2x(P)$$

Using curve eq. $y^2 = x^3 - x + 1$

we can write this as

$$x(2P) = \left.\frac{(3x^2-1)^2}{4(x^3-x+1)}\right|_P - 2x(P)$$

Plugging $x(P) = 1$ I get

$$x(2P) = -1$$

So $h_x(2P) = 0$ still.

Keep doubling & applying the formula above again I get

$$x(4P) = \left.\frac{(3x^2-1)^2}{4(x^3-x+1)}\right|_{2P} - 2x(2P)$$

$$= 3$$

So $h_x(4P) = \ln(3) > 1$.

So this answers (a) and (b)

To answer (c) we keep going:

find

$$x(8P) = \left.\frac{(3x^2-1)^2}{4(x^3-x+1)}\right|_{4P} - 2x(4P)$$

$$= 19/25$$

So $h_x(8P) = \ln(H(19/25))$

$$= \ln 25 \approx 3 \cdot 22$$

Finally $h_x(16P)$

$$= \left.\frac{(3x^2-1)^2}{4(x^3-x+1)}\right|_{8P} - 2x(8P)$$

$$= -\frac{350701}{265225}$$

So $h_x(16P) = \ln(350701)$

$$\approx 12 \cdot 77$$

So $h_x(16P) > 10$ as req'd.

1. $E: \quad y^2 = x^3 + ax + b \quad (a, b \in \mathbb{Z})$

$(x, y) \in E(\mathbb{Q})$

Show x & y are of the form

$$x = \frac{m}{d^2} \quad y = \frac{n}{d^3}$$

for integers m, n, d $\quad \gcd(m, d) = \gcd(n, d) = 1$.

Proof: Do this for each prime individually.

Let p be any prime: write

$$x = p^k \frac{r}{s} \quad \text{with } p \nmid r, \ p \nmid s$$

and $k \in \mathbb{Z}$.

So $x^3 = p^{3k} r^3/s^3$

So RHS of our eqn becomes

$$p^{3k} \frac{r^3}{s^3} + a p^k \frac{r}{s} + b$$

$$= p^{3k} \left(\frac{r^3 + ap^{-2k} rs^2 + bp^{-3k} s^3}{s^3} \right)$$

Let $t = r^3 + ap^{-2k} rs^2 + bp^{-3k} s^3$

$$= p^{3k} \frac{t}{s^3}$$

Now suppose p is one of the primes dividing <u>denominator</u> of x, i.e. $k<0$.

Then

$$t = r^3 + ap^{-2k} rs^2 + bp^{-3k} s^3$$

is an integer.

Moreover p divides the last 2 terms in t but not the first $\therefore$

$p \nmid t$.

So $x^3 + ax + b = p^{3k} \dfrac{t}{s^3}$

where $k<0$ and $\gcd(p,t), \gcd(p,s) = 1$.

Now look at the right-hand side:

Write $y = p^{l}\, u/v$ $\quad \gcd(p,u) = \gcd(p,v) = 1$

$$\therefore\ y^2 = p^{2l} \frac{u^2}{v^2}.$$

So setting LHS = RHS we get

$$p^{2l} \frac{u^2}{v^2} = p^{3k} \frac{t}{s^3}$$

Since u, v, t, s are all coprime to p, this implies

$$p^{2l} = p^{3k}$$

$$\therefore 2l = 3k$$

So $k = 2j$ $\quad l = 3j$ for some j

So we get

$$x = p^k \, r/s = p^{2j} \, r/s$$

$$y = p^l \, u/v = p^{3j} \, u/v$$

where $j < 0$ and r, s, u, v coprime to p.

If we repeat this for every p dividing denominator of x we get

$$x = \frac{m}{d^2} \qquad y = \frac{n}{d^3}$$

where $d = p_1^{-j_1} \cdots p_r^{-j_r}$

where the j_i are exponents as above, m, n coprime to d.