Problems on Canvas.

Work until ~3:20

$\in \mathbb{Q}$

1. Let L be the line $m(x+2)+3$ of slope m going through the point $(-2,3)$. This line intersects the elliptic curve $E_1 : y^2 = x^3+17$ in the point $(-2,3)$ and in two other points. If all three of these points have rational coordinates, show that the quantity

$$m^4 + 12m^2 + 24m - 12$$

must be the square of a rational number.

$L: y = m(x+2)+3$

$E: y^2 = x^3+17$

Find intersection $E \cap L$

$(m(x+2)+3)^2 = x^3+17$

$m^2(x+2)^2 + 6m(x+2)+9 = x^3+17$

$m^2(x^2+4x+4) + 6m(x+2)+9 = x^3+17$

$(*)$ $0 = x^3 - m^2x^2 - (4m^2+6m)x - (4m^2+12m-8)$

we know $(-2,3) \in L \cap E$

$\Rightarrow -2$ solves $(*)$

$\Rightarrow x+2$ divides the RHS of $(*)$

$$
\begin{array}{r l}
 & x^2 + (-m^2-2)x + (-2m^2-6m+4) \\
\hline
x+2 \,\big) & x^3 - m^2x^2 - (4m^2+6m)x - (4m^2+12m-8) \\
- & x^3 + 2x^2 \\
\hline
 & (-m^2-2)x^2 - (4m^2+6m)x \\
- & (-m^2-2)x^2 \; (-2m^2-4)x \\
\hline
 & (-2m^2-6m+4)x - (4m^2+12m-8) \\
 & (-2m^2-6m+4)x + (-4m^2-12m+8) \\
\hline
 & 0
\end{array}
$$

$$\Longrightarrow 0 = (x+2)\left(x^2 - (m^2+2)x - (2m^2+6m-4)\right)$$

roots are -2, roots r_+, r_-

$$r_\pm = \frac{m^2+2 \pm \left[(m^2+2)^2 + 4(2m^2+6m-4)\right]^{1/2}}{2}$$

$$= \frac{1}{2}\left[m^2+2 \pm \left(m^4+12m^2+24m-12\right)^{1/2}\right] \in \mathbb{Q}$$

$$\Longrightarrow \left(m^4+12m^2+24m-12\right)^{1/2} \in \mathbb{Q}$$

$\Longrightarrow$ $m^4+12m^2+24m-12$ is the square of a rational

4. Show that the only integer point on $y^2 = x^3 - 1$ is $(1, 0)$.

$$x^3 = y^2 + 1 \qquad \text{factor in } \mathbb{Z}[i]$$
$$= (y+i)(y-i)$$

Claim: if $y+i$ & $y-i$ are relatively prime, then they must both be cubes.

suppose $\gcd(y+i, y-i) = 1$

$\Rightarrow$ $y \pm i$ are cubes.

Suppose $y + i = (m+in)^3 \quad m, n \in \mathbb{Z}$
$$= m^3 + 3m^2(in) + 3m(in)^2 + (in)^3$$
$$= (m^3 - 3mn^2) + (3m^2n - n^3)i$$

$\Rightarrow y = m^3 - 3mn^2 = m(m^2 - 3n^2)$, $\quad 3m^2n - n^3 = 1$

$n(3m^2 - n^2) = 1$

$\Rightarrow n = \pm 1$

if $n = 1 \Rightarrow 3m^2 - 1 = 1 \Rightarrow 3m^2 = 2$

$\Rightarrow m^2 = 2/3$

no solns $\Rightarrow n \neq 1$

if $n=-1 \Rightarrow 3m^2-1=-1$

$\Rightarrow 3m^2=0 \Rightarrow m=0$

$\Rightarrow y = m(m^2-3n^2) = 0$

$y^2 = x^3 - 1 \Rightarrow x = 1$

need to show $\gcd(y+i, y-i) = 1$

suppose $\delta \in \mathbb{Z}[i]$ is a common divisor

$\Rightarrow \delta$ divides $(y+i)-(y-i) = 2i$

$\Rightarrow N(\delta) \mid N(2i) = 4$

$N(y+i) = (y+i)(y-i) = y^2+1 = x^3$

which is odd

$y^2 = x^3 - 1 \Rightarrow x^3 = y^2+1$ (look mod 8)

$N(\delta) \mid N(y+i) \Rightarrow N(\delta)$ odd

$\Rightarrow N(\delta) = 1$, so δ is a unit $\boxtimes$