

1. Classify the torsion subgroup of the rational points on the elliptic curve

$$y^2 = x^3 + 2x^2 - 3x.$$

The discriminant of the polynomial  $x^3 + 2x^2 - 3x$  is  $D = 144$ . By the Lutz-Nagell theorem, if  $P = (x, y)$  is a rational point on the elliptic curve of finite order, then either  $y = 0$ , or  $y$  divides 144.

Running through the divisors of 144, we find that the points of finite order are  $(0, 0)$ ,  $(1, 0)$ ,  $(-3, 0)$ ,  $(-1, 2)$ ,  $(-1, -2)$ ,  $(3, 6)$ , and  $(3, -6)$ . So, including the point at infinity, the group of finite rational points on the elliptic curve is

$$E(\mathbb{Q})_T = \{\infty, (0, 0), (1, 0), (-3, 0), (-1, 2), (-1, -2), (3, 6), (3, -6)\}$$

This is a finite Abelian group of order 8, so it must be isomorphic to  $\mathbb{Z}_8$ ,  $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ , or  $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ .

We consider the points  $(0, 0)$ ,  $(1, 0)$  and  $(-3, 0)$ . These three points lie on the  $x$ -axis, and the tangent lines to the curve at these points are all vertical. Thus, the third point of intersection is the point at infinity. So the orders of each of these points is 2. So the group has at least three points of order two, namely  $(0, 0)$ ,  $(1, 0)$ , and  $(-3, 0)$ .

The group  $\mathbb{Z}_8$  has only 1 element of order two, namely the element 4, since  $\langle 4 \rangle = \{0, 4\}$ . So the group  $E(\mathbb{Q})_T$  cannot be  $\mathbb{Z}_8$ .

So we are left with  $G = \mathbb{Z}_4 \oplus \mathbb{Z}_2$  and  $H = \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ . One main difference is that the group  $G$  has elements of order 4, whereas the group  $H$  has no elements of order 4.

Consider the element  $(-1, 2)$  on the elliptic curve. The tangent line to the curve at the point  $(-1, 2)$  intersects the curve at  $(1, 0)$ , which when reflected over the  $x$ -axis is  $(-1, 0)$ . So  $(-1, 2) + (-1, 2) = (1, 0)$ . At any rate, the point  $(-1, 0)$  is not a point of order 2. So the group cannot be  $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$ .

Therefore, the group is  $\mathbb{Z}_4 \oplus \mathbb{Z}_2$ .