METU, Spring 2020, Math 366.

Exercise Set 2

1. Let G be a group and let $\text{Tor}(G)$ be the subset of G consisting of elements of finite order.

   (a) If A is abelian then show that $\text{Tor}(A)$ is a subgroup of A. Find an example where $\text{Tor}(A)$ is infinite.

   (b) Give an example of a group G, such that $\text{Tor}(G)$ is not a subgroup of G.

2. Let C_1 and C_2 be the cubics given by the following equations:

$$C_1 : x^3 + 2y^3 - x - 2y = 0, \qquad C_2 : 2x^3 - y^3 - 2x + y = 0.$$

   Find the nine points of intersection of C_1 and C_2.

3. The elliptic curve $E : y^2 = x^3 + 17$ has precisely 8 points with integer coordinates and $y > 0$. Find as many as you can. Show that none of these points is of finite order.

4. For each of the following elliptic curves, determine all of the rational points of finite order (don't forget ∞). Make a group table which shows all possible group operations between these points and determine the group structure of $\text{Tor}(E(\mathbb{Q}))$:

   - $y^2 = x^3 - x,$
   - $y^2 = x^3 + 4,$
   - $y^2 = x^3 + 4x.$

5. The elliptic curve $y^2 = x^3 - 5x + 4$ has points $P = (0, 2), Q = (1, 0)$ and $R = (3, 4)$. Show that $(P + Q) + R = P + (Q + R)$ without using the fact that $E(\mathbb{Q})$ is a group.

6. Consider the point $P = (0, 1)$ on the elliptic curve $E = y^2 = x^3 + 1$. Show that the order of P is 3. Show that P is an inflection point on the curve E.

7. Consider the cubic equation $u^3 + v^3 = m$ where m is a fixed integer. Consider the change of variables

$$x = \frac{12m}{u+v}, \qquad y = 36m\frac{u-v}{u+v}.$$

   Show that x and y satisfy the relation $y^2 = x^3 - 432m^2$.

8. Show that there are infinitely many right triangles whose edges are of rational length and whose area is 6. For example (3,4,5), (7/10, 120/7, 1201/70), etc...