M343L: HOMEWORK SET 7 PROOFS

ANDREW TSENG: ART2589

Problem 6.1

1: $P \bigoplus Q = P$
2: $P \bigoplus P = P \quad Q \bigoplus Q = Q$
3: $P \bigoplus P \bigoplus P = P \quad Q \bigoplus Q \bigoplus Q = Q$

Problem 6.4

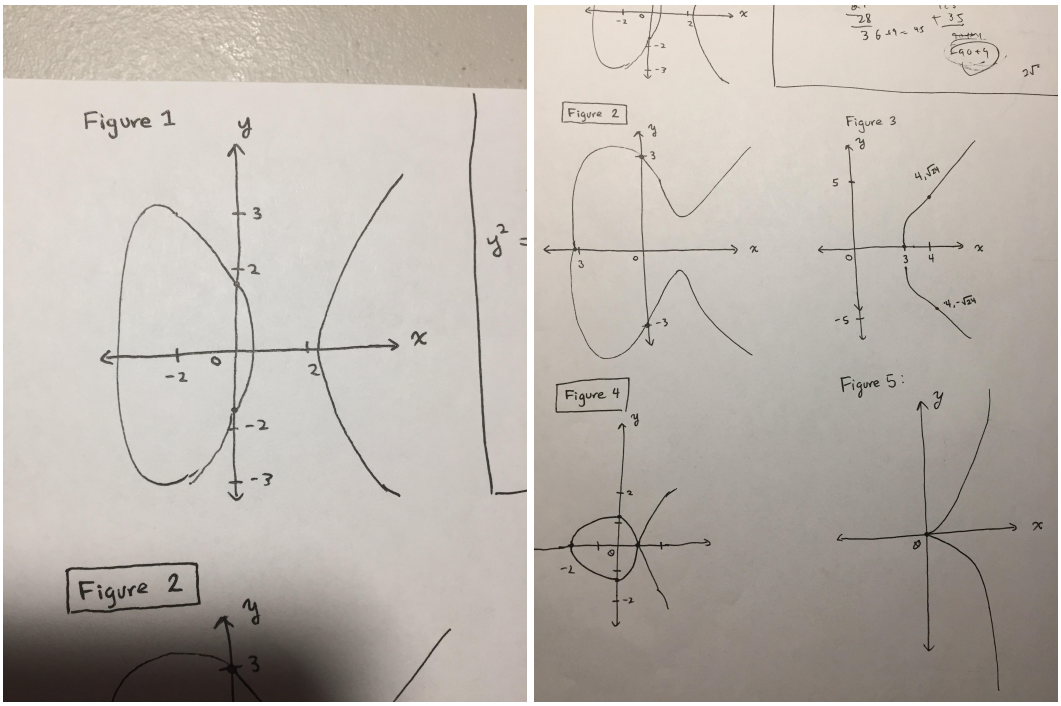

Figure 4: $4(-3)^3 + 27(2)^2 = 0$, which indicates the the $\Delta E = 0$, which indicates the the curve is not an elliptical curve.
Figure 5 is not an elliptical curve because $4A^3 + 27B^2 = 0$ which means all the roots of the curve not distint (in fact they are all 0).

Problem 6.8

Solving the DLP:

$$E : y^2 = x^3 + x + 1 \in F_5$$

Using the program **ecdlp.py**, with **ecdlp.in** as the input file, we find that $n = 4$ satsifies the DLP equation on E.
The program uses elliptical addition to solve nP and finds a match to Q.
We find that: List of $k_j P = (3, 4), (2, 4), (0, 4), (0, 1)$
Thus when $k = 4$, $kP = Q \in E$.

Problem 6.10

$P = n_1 P_1 + n_2 P_2$.

Problem 6.13