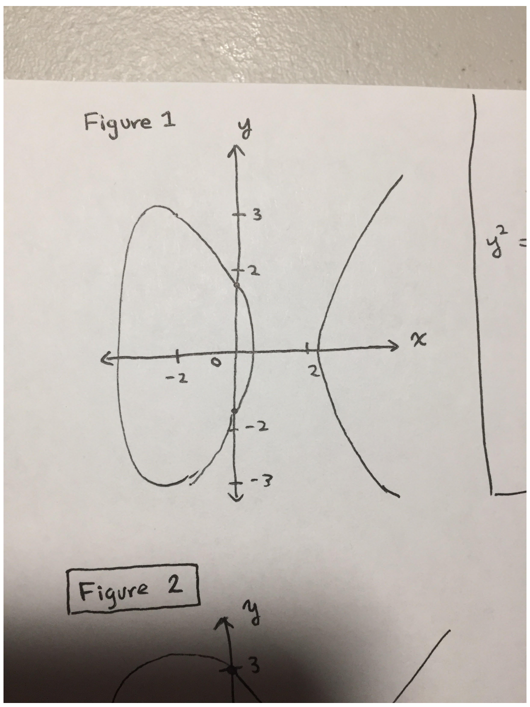
M343L: HOMEWORK SET 7 PROOFS

ANDREW TSENG: ART2589

Problem 6.1

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

Problem 6.4



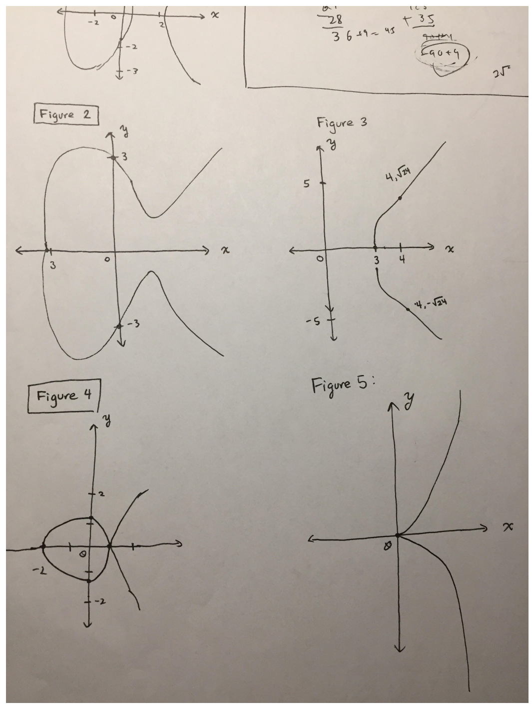


Figure 4: $4(-3)^3 + 27(2)^2 = 0$, which indicates the the $\Delta E = 0$, which indicates the the curve is not an elliptical curve. Figure 5 is not an elliptical curve because $4A^3 + 27B^2 = 0$ which means all the roots of the curve not distint (in fact they are all 0).

Problem 6.8

Solving the DLP:

$$E : y^2 = x^3 + x + 1 \in E_{F5}$$

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

Let the point P be represented by P_X, P_Y. n is the range of numbers from 1 to p (the field value).

$$\begin{bmatrix} P_X \\ P_Y \end{bmatrix} \begin{bmatrix} n_1 & n_2 & \dots & n_r \end{bmatrix} = \begin{bmatrix} P_X n_1 & P_X n_2 & \dots & P_X n_r \\ P_Y n_1 & P_Y n_2 & \dots & P_Y n_r \end{bmatrix}$$

Using the resulting matrix, you can iterate through the matrix to find a pair of $(P_X n, P_Y n)$ that match Q.

Problem 6.13

Using pollard's ρ algorithm to solve ECDLP

Algorithm:

step = 1
while(P does not equal to Q)
  $P = P + P + P$
  $Q = Q + Q$.
step = step + 1

Example:

$P = (1, 8)$, $Q = (12, 11)$
At step 1: $P = (1, 8), Q = (12, 11)$.
At step 2: $P = (9, 6), Q = (1, 5)$.
At step 3: $P = (12, 2), Q = (9, 6)$.
At step 4: $P = (2, 10), Q = (2, 10)$.
At Step 4 P equals to Q, thus $n = 4$ for the ECDLP.