Homework 39, due December 9

(1) Write down the addition table for the elliptic curve $E : y^2 + xy \equiv x^3 + 1 \pmod{2}$.

(2) Choose a message of at least five characters. Let $p = 102957830214234598523542370111119$. Encode your message as a point on the curve $E : y^2 \equiv x^3 + 23x + 17 \pmod{p}$. Use one extra character at the end of your message to make sure it encodes as a point.

(3) Let $p = 102957830214234598523542370111119$. Define the elliptic curve $E$ by $E : y^2 \equiv x^3 + 4x + 4 \pmod{p}$. Let $A$ be the point $(1, 3)$ and $B$ be the point $(69191178569848326160572708363740, 69345928396974443058108559876130)$. You receive the message $y_1 = (2712221111077269330209558694853, 56731441929119870413208632138532)$, $y_2 = (10202465621849293104116721682861, 101431596619654710328174830883350)$ and know that the private key for this cryptosystem is $a = 1995$. Decrypt into a message in English.