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 $p = 10295783021423459852354237011119$. 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 $p = 10295783021423459852354237011119$. 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

$$(691911785698483261605727083637 40, 693459283969744430581085598761 30).$$

You receive the message

$$y_1 = (271222211110772693302095586948 53, 567314419291198704132086321385 32),$$

$$y_2 = (102024656218492931041167221682861, 101431596619654710328174830883350)$$

and know that the private key for this cryptosystem is $a = 1995$. Decrypt into a message in English.