Homework 25, due December 8

(1) (Problem 6, page 370) Factor $n = 35$ by the elliptic curve method by using the elliptic curve $y^2 \equiv x^3 + 26$ and calculating 3 times the point $P = (10, 9)$. Factor $n = 35$ by the elliptic curve method by using the elliptic curve $y^2 \equiv x^3 + 5x + 8$ and the point $P = (1, 28)$.
(2) (Problem 8, page 370) Devise an analog of the procedure in exercise 8(a) in Chapter 7 that uses elliptic curves.
(3) (Problem 3, page 375) Factor 3900353 using elliptic curves. Try to factor 3900353 using the $p-1$ method. Using the knowledge of the prime factors from the elliptic curve factorization, explain why the $p - 1$ method does not work well for this problem.
(4) 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.