Homework 24, due December 4

(1) (Problem 5, page 370) Show that the point $Q = (2, 3)$ on the curve $y^2 = x^3 + 1$ satisfies $6Q = \infty$. Show that the points $\infty, Q, 2Q, 3Q, 4Q, 5Q$ are distinct.
(2) Consider the point $P = (3, 8)$ on the curve $y^2 = x^3 - 43x + 166$ defined over the rational numbers. Compute $2P, 4P$, and $8P$.
(3) (from Problem 2, page 370)
    - List the points on the elliptic curve $E : y^2 \equiv x^3 - 2 \pmod 7$.
    - Write down the addition table for this elliptic curve.
(4) (Problem 5, page 375) Compute the difference $(5, 9) - (1, 1)$ on the elliptic curve $y^2 \equiv x^3 - 11x + 11 \pmod{593899}$.