Homework 21, due October 25

(1) Let $p = 37$. Evaluate $L_2(24)$.
(2) Alice and Bob perform Diffie-Hellman key exchange with the prime $p = 257$ and the primitive root $\alpha = 3$. If Alice chooses $x = 32$ and Bob chooses $y = 189$, compute Alice and Bob's shared secret mod p. Show your work.
(3) Fix an odd prime p and an integer g with $\gcd(g, p) = 1$. In this problem we find a method to test whether g is a primitive root mod p.
   (a) Let k be the least positive integer with $g^k \equiv 1 \pmod{p}$ (note that k exists by Fermat's little theorem). Prove that $k \mid (p-1)$ via the following steps. Assume for contradiction that $k \nmid (p-1)$. Show that $p - 1 = kq + r$ for an integer r with $1 \leq r < k$. Raise both sides of the equation $g^k \equiv 1 \pmod{p}$ to the q-th power power and use Fermat's little theorem to prove $g^r \equiv 1 \pmod{p}$. Explain why this contradicts the minimality of k.
   (b) Let $p - 1 = q_1^{a_1} \cdots q_t^{a_t}$ be the factorization of $p - 1$ into primes, where the primes q_i are distinct and the a_i are positive integers. Show that if g is not a primitive root mod p, then $g^{(p-1)/q_i} \equiv 1 \pmod{p}$ for some $1 \leq i \leq t$. (Hint: Show that if g is not a primitive root mod p then $g^k \equiv 1 \pmod{p}$ for some $k < p - 1$. By part (a) we have $k \mid (p-1)$. Show that $k \mid \frac{p-1}{q_i}$ for some i, and raise both sides of $g^k \equiv 1 \pmod{p}$ to an appropriate power.)
   (c) Deduce from part (b) that if $g^{(p-1)/q_i} \not\equiv 1 \pmod{p}$ for all $1 \leq i \leq t$ then g is a primitive root mod p.
   (d) Let $p = 2251799813687339$. Factor $p - 1$ (using Sage, say) to see that $p - 1 = 2q$, where q is a prime. Use the test in part (c) to prove that $g = 2$ is a primitive root mod p.