Homework 18, due October 16

(1) If $(n, e) = (1484884039, 61229153)$, factor n using the low decryption exponent continued fraction attack.

(2) Use the continued fraction attack to find the decryption exponent for the public key $(n, e) = (60842791409, 50073749237)$.

(3) (Page 194, problem 19) Let $n = pq$ be a product of two distinct primes.
   (a) Let m be a multiple of $\phi(n)$. Show that if $\gcd(a, n) = 1$, then $a^m \equiv 1 \pmod{p}$ and $\pmod{q}$.
   (b) For the same m, let a be an arbitrary integer $\pmod{n}$, so that possibly $\gcd(a, n) \neq 1$. Show that $a^{m+1} \equiv a \pmod{p}$ and $\pmod{q}$.
   (c) Let e and d be encryption and decryption exponents for RSA with modulus n. Show that $a^{ed} \equiv a \pmod{n}$ for all a. This shows that we do not need to assume $\gcd(a, n) = 1$ for RSA to work.
   (d) If p and q are large, why is it likely that $\gcd(a, n) = 1$ for a randomly chosen a?