Homework 13, due October 20

(1) (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?

(2) (a) Does 48382 have a square root modulo 83987? Explain.
   (b) Let $n = 213523 \cdot 304687$. Find x and y with $x^2 \equiv y^2 \pmod{n}$ but $x \not\equiv \pm y \pmod{n}$.

(3) Suppose you know that

$$271610257949550853120^2 \equiv 689562347736325759112749577741079678616245489330498^2$$

$$\pmod{64654102357758919410799483670936470498512529871913 49}.$$

Use this information to factor 6465410235775891941079948367093647049851252987191349.

(4) (Page 108, problem 27) Alice designs a cryptosystem (following Rabin) as follows. She chooses two distinct primes p and q congruent to 3 (mod 4) and keeps them secret. She makes $n = pq$ public. When Bob wants to send Alice a message m, he computes $x = m^2 \pmod{n}$ and sends x to Alice. She makes a decryption machine that does the following: When the machine is given a number x, it computes the square roots of $x \pmod{n}$ since it knows p and q. There is usually more than one square root. It chooses one at random and gives it to Alice. When Alice receives x from Bob, she puts it into her machine. If the output from the machine is a meaningful message, she assumes it is the correct message. If it is not meaningful, she puts x into the machine again. She continues until she gets a meaningful message.
   (a) Why should Alice expect to get a meaningful message fairly soon?
   (b) If Eve intercepts x (she already knows n), why should it be hard for her to determine m?
   (c) If Eve breaks into Alice's office and can try a few chosen ciphertext attacks on Alice's decryption machine, how can she determine the factorization of n?