1071 Cryptography Homework #2
Due 10/30

1. Let a and $n > 1$ be integers with $gcd(a, n) = 1$. The **order** of $a \pmod{n}$, $ord_n(a)$, is the smallest positive integer r such that $a^r \equiv 1 \pmod{n}$.
   (a) Show that $r \leq \phi(n)$.
   (b) Show that if $m = rk$ is a multiple of r, then $a^m \equiv 1 \pmod{n}$.
   (c) If $a^t \equiv 1 \pmod{n}$, where $t = qr + s$ with $0 \leq s < r$, show that $a^s \equiv 1 \pmod{n}$. Also, show that the definition of r implies that $s = 0$ and thus $r|t$.
   (d) Show that $ord_n(a)|\phi(n)$.
   (e) Show that any prime order group **G** (not necessarily a group of integers) is indeed cyclic.

2. (a) Show that if gcd(e, 24) = 1, then $e^2 \equiv 1 \pmod{24}$.
   (b) Show that if n = 35 is used as an RSA modulus, then the encryption exponent e always equals the decryption exponent d.

3. Suppose that there are two users in a network. Let their RSA moduli be n_1 and n_2, with n_1 not equal to n_2. If you are told that n_1 and n_2 are not relatively prime, how would you break their schemes? (In Asiacrypt 2013, the paper "Factoring RSA keys from certified smart cards: Coppersmith in the wild" showed that there is a devastated security loophole in Taiwan's "Citizen Digital Certificate".)

4. Show that the quotients in the Euclidean algorithm for $gcd(a, b)$ are exactly the numbers $a_0, a_1, \ldots$ that appear in the continued fraction of $\frac{a}{b}$.

5. In order to increase security, Bob chooses n and two encryption exponents e_1, e_2. He asks Alice to encrypt her message m to him by first computing $c_1 = m^{e_1} \pmod{n}$, then encrypting c_1 to get $c_2 = {c_1}^{e_2} \pmod{n}$. Alice then sends c_2 to Bob. Does this double encryption increase security over single encryption? Why or why not?