Math 370 Number Theory
Assignment # 7

1. For this problem do not use prime factorization. They first couple should look familiar to you.
   (a) Suppose that $k, m, n \in \mathbb{N}$ such that $\gcd(m, n) = 1$. Let $a = \gcd(k, m)$ and $b = \gcd(k, n)$ and $k|mn$. Show that :
      i. $\gcd(a, b) = 1$.
      ii. $ab|k$.
      iii. Show that $k|ab$ and hence k=ab. (Hint: Use Bézout's theorem for both a and b).
   (b) Show if m, n are relatively prime natural numbers then $k|mn$ if and only if $k = ab$ where $a|m$ and $b|n$ and $\gcd(a, b) = 1$.
   (c) Show that σ is multiplicative.
2. Continuing on with the last problem:
   (a) Show if $n_1, \ldots n_r$ are pairwise relatively prime then $k|n_1 n_2 \ldots n_r$ if and only if $k = a_1 a_2 \ldots a_r$ where $a_i|n_i$ and $a_1, a_2, \ldots a_r$ are pairwise relatively prime.
   (b) Suppose $n = p_1^{\alpha_1} p_2^{\alpha_2} \ldots p_r^{\alpha_r}$ with $1 \leq \alpha_i$ and p_i prime, is the unique prime factorization of n. Show that $a|n$ if and only if $a = p_1^{\beta_1} p_2^{\beta_2} \ldots p_r^{\beta_r}$ where $0 \leq \beta_i \leq \alpha_i$. This shows that the unique factorization of a must included only primes in the factorization on n and must have smaller (or equal) powers of each of those primes.
3. Let p be an odd prime and $a \in \mathbb{Z}$ with $p \not| a$. Show that if $x^2 = a \pmod p$ has a solution, then it has exactly 2 solutions. (Hint let b be a solution and then show there will be exactly 2).