Math 173A - Greatest Common Divisors and Modular Arithmetic

1. Prove that if p is a prime number and $p \mid a_1 a_2 \dots a_k$ for integers $a_1, \dots, a_k$, then p divides at least one of the a_i's.

2. In this exercise we'll prove that prime factorization is unique, i.e. that any integer a may be written
$$a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r} \tag{1}$$
for primes $p_1, \dots, p_r$ and nonnegative integers $e_1, \dots, e_r$ where the p_i are unique up to rearrangement.

   A common way to prove that some way of doing something is unique is to do it in two ways and then argue that they're the same. To this end, suppose we could write
$$a = p_1 p_2 \cdots p_s = q_1 q_2 \cdots q_t, \tag{2}$$
where the p_i and q_j are all primes, not necessarily distinct and s may be different from t.

   (a) Where did the e_i's go when we moved from (1) to (2)?

   (b) Argue that p_1 must divide $q_1 \cdots q_t$. Use this to conclude that p_1 is equal to one of the q_i's. Now reorder so that this is q_1.

   (c) Now divide both sides of (2) by p_1. What are you left with? Repeat this argument.

   (d) Put the previous pieces together into a short, well-written proof for the uniqueness of prime factorization.

3. Prove that there are infinitely many prime numbers. *Hint: what if there were only finitely many?*

4. Compute $\gcd(291, 252)$ and find integers u and v such that
$$291u + 252v = \gcd(291, 252).$$