Prove/Disprove and Induction

November 17, 2019

Question 1

a) In my solution to HW 7 number 7-20 I mentioned that for any prime p and any integer a, $a^{p-1} \equiv 1$ mod p. What about if n is just any integer, not necessarily a prime? Ie, prove or disprove the following:
For any integer a, and natural number n, $a^{n-1} \equiv 1$ mod n.

b) Suppose gcd(a,b)=1. Show that if $a|n$ and $b|n$ then $ab|n$ for some integer n.

c) Show that the result in part b is false if a and b are not coprime. That is, find some a,b and n such that $a|n$, $b|n$ but $ab \nmid n$

Question 2

a) Prove every positive integer is a product of prime numbers (this justifies my answer to 7-34 for example).
b) For which natural numbers is $2^n < n!$
c) Prove that if p is prime and $p|a_1 \cdots a_n$ then $p|a_i$ for at least one of the a_i

Question 3- Fundamental Theorem of Arithmetic

In 2a) you showed that $n = p_1 \cdots p_n$ for p_i primes. The point of this problem is to show that this expression is unique.
Namely, show that if also $n = q_1 \cdots q_k$ for q_i primes, then we must have n=k, and $p_i = q_j$ for some i,j (that is the primes are all the same).
(For example: 28=2x2x7=2x7x2, ect, ie, the way we can write it as a product

of primes is unique up to the order we write the primes down).

Do this as follows: Assume for the sake of contradiction that $n = p_1 \cdots p_n = q_1 \cdots q_k$ where the list of primes p_i is not the same as the list of primes q_j. Then cancel out the primes that are the common to both sides to get an expression $r_1 \cdots r_m = s_1 \cdots s_z$ for primes r_i, s_j where no $s_j = r_i$. Then use problem 2c to get a contradiction.
Collecting the primes in the factorization of n we can write n uniquely as $n = p_1^{a_1} \cdots p_n^{a_n}$ for $a_i \geq 1, p_i$ primes.

This is a rather innocent looking statement, yet it has profound consequences. Here is a tiny, tiny taste:
Let n be a natural number. Using the fundamental theorem of arithmetic, show that $\sqrt{n} \in \mathbb{Q}$ iff n is a perfect square. (this proves in one fell swoop that $\sqrt{2}, \sqrt{3}, \sqrt{5}, ect$ are not rational numbers).