Practice

From Math 20630

HW 7: Some Number Theory

1. Use 168.

2. (a) n is divisible by p, so it can be written as $n = ap$ for some a. Now since p is prime, if q divides ap, then a must be divisible by q. Rewriting, we have $n = bqp$ for some $a = bq$, and so n is divisible by pq.

   (b) Take the starting point of the above argument except $p = q$. We have $n = ap$, and since $p = q$, then n is divisible by both p and q. However, consider the case when $ap < p^2$. In this case, n is not divisible by p^2. So n need not be divisible by pq if $p = q$.

3. (a)
$$x^n - 1 = (x-1)(1 + x + x^2 + \cdots + x^{n-1})$$
$$= (x + x^2 + \cdots + x^n) + (-1 - x - x^2 - \cdots - x^{n-1})$$
   Cancelling terms, we get $x^n - 1$ as desired.

   (b) If n is not prime, then it can be written as pa where p is some prime number. Then, $2^n - 1$ becomes $2^{pa} - 1$, or $(2^p)^a - 1$. Using the above,
$$(2^p)^a - 1 = (2^p - 1)(1 + 2^p + 2^{2p} + \cdots + 2^{p(a-1)})$$
   Notice $2^p - 1 < 2^n - 1$, and $p \leq 2$ in order for p to be prime. As such, $2^p - 1 > 1$, and we have factored our expression into a product of which at least one factor is greater than 1, so $2^n - 1$ is not prime for non-prime n.

   (c) $n = 11$ is a prime number which does not result in a Mersenne prime. The converse is false.

4. (a) According to the Euclidean algorithm, the gcd of two numbers can be written as a linear combination of those two numbers. The gcd of p and a, however, is 1 since a and p are coprime. So $\gcd(p, a) = mp + na = 1$

   (b) Say $p|a$. If so, we are done. Otherwise, since p does not divide a, then $\gcd(p, a) = mp + na = 1$ for some m, n. Multiplying by b, we get $bmp + bna = b$. bmp is obviously divisible by p, and bna is divisible by p since we are given that $p|ab$.