MATH 3270 Assignment # 1 Solutions

(1) Let p_n denote the n^{th} prime number. Prove that for every $n \in \mathbb{Z}^+$, $p_{n+1} \leq p_1 p_2 \cdots p_n + 1$. (Hint: use ideas from the proof that there are infinitely many primes.)
$p_1 p_2 \cdots p_n + 1$ leaves a remainder of 1 when divided by p_i for $1 \leq i \leq n$ and therefore is not divisible by p_i for $1 \leq i \leq n$. Therefore its prime factors are of the form p_j for $j > n$. Therefore $p_{n+1} \leq p_1 p_2 \cdots p_n + 1$.

(2) Let a and n be positive integers such that $n > 1$ and $a^n - 1$ is prime.
  (a) Prove that $a = 2$.
  $a^n - 1 = (a-1)(a^{n-1} + a^{n-2} + \cdots + a + 1)$ so if $a > 2$, then the two factors are greater than 1 so that $a^n - 1$ is composite– contradiction. Therefore $a = 2$.
  (b) Prove that n must be prime. If $n = xy$ where x and y are greater than 1, then $a^n - 1 = (a^x)^y - 1 = (a^x - 1)(a^{x(y-1)} + a^{x(y-2)} + \cdots + a^x + 1)$ where the two factors are greater than 1 and thus $a^n - 1$ is composite–contradiction. Therefore n must be prime.

(3) (a) Find $(1331, 2431)$ by finding the prime factorizations.
  $1331 = 11^3$
  $2431 = 11 \times 13 \times 17$
  Therefore $(1331, 2431) = 11$.
  (b) Find $(1331, 2431)$ by applying the Euclidean algorithm.

$$\begin{aligned}
2431 &= 1331(1) + 1100 \\
1331 &= 1100(1) + 231 \\
1100 &= 231(4) + 176 \\
231 &= 176(1) + 55 \\
176 &= 55(3) + 11 \\
55 &= 11(5)
\end{aligned}$$

  Therefore $(1331, 2431) = 11$.
  (c) Express $(1331, 2431)$ in the form $1331m + 2431n$.

$$\begin{aligned}
11 &= 176 - (3)55 \\
&= 176 - (3)(231 - 176(1)) = (-3)231 + (4)176 \\
&= (-3)231 + (4)(1100 - 231(4)) = (4)1100 - 19(231) \\
&= (4)1100 - 19(1331 - 1100) = (-19)1331 + 23(1100) \\
&= (-19)1331 + 23(2431 - 1331) = (23)2431 - (42)1331
\end{aligned}$$

(4) Let a and b be positive integers. Prove that $gcd(a, b) = lcm(a, b)$ if and only if $a = b$.
Let $a = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_k^{b_k}$ be prime factorizations of a and b. Then

$$gcd(a, b) = \prod_{i=1}^{k} p_i^{\min(a_i, b_i)}$$

while

$$lcm(a, b) = \prod_{i=1}^{k} p_i^{\max(a_i, b_i)}.$$

Therefore $gcd(a, b) = lcm(a, b)$ if and only if $\min(a_i, b_i) = \max(a_i, b_i)$ for $1 \leq i \leq k$. This is true if and only if $a_i = b_i$ for each $1 \leq i \leq k$ which is true if and only if $a = b$.

(5) Prove that if $p > 3$ is prime, then $12|p^2 - 1$.
We need to show that 3 and 4 divide $p^2 - 1$.
Since $p > 3$, p is not divisible by 3, so $p = 3k + 1$ or $3k + 2$.
$(3k + 1)^2 - 1 = 9k^2 + 6k$ is divisible by 3.
$(3k + 2)^2 - 1 = 9k^2 + 12k + 3$ is divisible by 3.
Thus $3|p^2 - 1$.
Since $p > 3$, p is not divisible by 2, so $p = 4k + 1$ or $4k + 3$.
$(4k + 1)^2 - 1 = 16k^2 + 8k$ is divisible by 4.
$(4k + 3)^2 - 1 = 16k^2 + 24k + 8$ is divisible by 4.
Therefore $4|p^2 - 1$.
Therefore $12|p^2 - 1$.

(6) Bonus: Use the Euclidean algorithm to prove that $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.
WOLOG, assume $m \leq n$. Then $n = mq + r$ where $0 \leq r < m$. $q = \lfloor \frac{n}{m} \rfloor$. Then

$$a^n - 1 = (a^m - 1)(a^{n-m} + a^{n-2m} + \cdots + a^{n-\lfloor \frac{n}{m} \rfloor m}) + a^{n-\lfloor \frac{n}{m} \rfloor m} - 1 = (a^m - 1)(a^{n-m} + a^{n-2m} + \cdots + a^{n-qm}) + a^r - 1.$$

Thus if the Euclidean algorithm for m, n is:

$$\begin{aligned}
n &= mq_1 + r_1 \\
m &= r_1 q_2 + r_2 \\
r_1 &= r_2 q_3 + r_3 \\
\ldots &= \ldots \\
r_{j-2} &= r_{j-1} q_j + r_j \\
r_{j-1} &= r_j q_{j+1}
\end{aligned}$$

where $(m, n) = r_j$, then the Euclidean algorithm for $a^m - 1, a^n - 1$ is:

$$\begin{aligned}
a^n - 1 &= (a^m - 1)Q_1 + a^{r_1} - 1 \\
a^m - 1 &= (a^{r_1} - 1)Q_2 + a^{r_2} - 1 \\
a^{r_1} - 1 &= (a^{r_2} - 1)Q_3 + a^{r_3} - 1 \\
\ldots &= \ldots \\
a^{r_{j-2}} - 1 &= (a^{r_{j-1}} - 1)Q_j + a^{r_j} - 1 \\
a^{r_{j-1}} - 1 &= (a^{r_j} - 1)Q_{j+1} = (a^{(m,n)} - 1)Q_{j+1}.
\end{aligned}$$

Thus $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.