Math 312 Section 951 Test #5 Solutions

August 10, 2023

1 We proceed to prove this statement by taking the contrapositive. Assume n is composite and let $n = pm$ where p is a prime factor. Then

$$\begin{aligned} M_n &= 2^n - 1 \\ &= 2^{pm} - 1 \\ &= (2^p - 1)\sum_{k=0}^{m-1} 2^{pk} \end{aligned}$$

Since $2^p - 1 \geq 3, \sum_{k=0}^{m-1} 2^{pk} \geq 5$, M_n is composite.

2 Assume $n = \prod_{k=1}^{m} p_k^{n_k}$, then

$$\phi(n) = n\prod_{k=1}^{m}\left(1 - \frac{1}{p_k}\right)$$

Since n is a composite number, each prime factor $p_k \leq \sqrt{n}$. We have

$$\phi(n) \leq n\prod_{k=1}^{m}\left(1 - \frac{1}{\sqrt{n}}\right) \leq n\left(1 - \frac{1}{\sqrt{n}}\right) = n - \sqrt{n}$$

Alternative proof: Since n is composite, there exists a prime number p such that $p \leq \sqrt{n}$ and $n = pq$. Notice that $q \geq \sqrt{n}$. It is obvious that $p, 2p, \cdots, qp$ are not coprime to n. So $\phi(n) \leq n - q \leq n - \sqrt{n}$.

3a Use the following decipher method

$$P = C - 3 \mod 26$$

we reach ICAME ISAWI CONQU ERED.

3b

plaintext	encryption	ciphertext
B	$2 \times 1 + 4 = 6 \mod 26$	G
I	$2 \times 8 + 4 = 20 \mod 26$	U
T	$2 \times 19 + 4 = 16 \mod 26$	Q
C	$2 \times 2 + 4 = 8 \mod 26$	I
O	$2 \times 14 + 4 = 6 \mod 26$	G
I	$2 \times 8 + 4 = 20 \mod 26$	U
N	$2 \times 13 + 4 = 4 \mod 26$	E

4

plaintext	encryption	ciphertext
DR	$0317^7 = 1579 \mod 2627$	1579
AM	$0012 = 2155 \mod 2627$	2155
AS	$0018^7 = 0309 \mod 2627$	0309

5a Assume $n = \prod_{k=1}^{m} p_k^{n_k}$, then

$$\sigma(n) = \prod_{k=1}^{m} \left(\frac{p_k^{n_k+1} - 1}{p_k - 1} \right) = \prod_{k=1}^{m} \left(\sum_{l=0}^{n_k} p_k^l \right)$$

Consider $m = 1$. Since

$$\sigma(n) = \sum_{l=0}^{n_1} p_1^l = 1 + p_1 + \cdots + p_1^{n_1} = 24$$

$p_1 \neq 2$ and n_1 must be odd. If $n_1 = 1$, $n = 23$. If $n_1 \geq 3$, since $1 + p_1 + p_1^2 + p_1^3 \geq 1 + 3 + 3^2 + 3^3 > 24$, there is no such n.
Consider $m = 2$, then

$$\sigma(n) = \left(\sum_{l=0}^{n_1} p_1^l \right) \left(\sum_{l=0}^{n_2} p_2^l \right) = (1 + p_1 + \cdots + p_1^{n_1})\,(1 + p_2 + \cdots + p_2^{n_2}) = 24$$

Since for $i \in \{1, 2\}$, $1 + p_i + \cdots + p_i^{n_i} \geq 3$, the possible scenarios are $3 \times 8 = 24$ and $4 \times 6 = 24$. For the first case, we have $p_1 = 2, n_1 = 1, p_2 = 7, n_2 = 1$ and $n = 14$ while for the latter case we have $p_1 = 3, n_1 = 1, p_2 = 5, n_2 = 1$ and $n = 15$.
Consider $m \geq 3$, then

$$\sigma(n) = \prod_{k=1}^{m} \left(\sum_{l=0}^{n_k} p_k^l \right) \geq 3^3 > 24$$

There is no such n.
In conclusion, $n = 14, 15, 23$.

5b Assume $n = \prod_{k=1}^{m} p_k^{n_k}$, then

$$\tau(n) = \prod_{k=1}^{m} (n_k + 1) = 14$$

The possible scenarios are $1 \times 14 = 14$ and $2 \times 7 = 14$. In the first case, we have $n_1 = 13$ and $n = p_1^{13}$ while in the latter case we have $n_1 = 1, n_2 = 6$ and $n = p_1 p_2^6$. The smallest positive integer $n = 3 \times 2^6 = 192$.