# Math 312 Section 951 Final Exam Solutions

August 18, 2023

1a Recall that $\tau(n) = \prod_i (a_i+1)$ with $n = \prod_i p_i^{a_i}$. Since $\tau(n) = 1\times 15 = 3\times 5$, we conclude that $n = p_1^{14}$ or $n = p_1^2 p_2^4$. The smallest postive $n = 3^2 \times 2^2 = 144$.

1b Recall that $\phi(n) = \prod_i p_i^{a_i-1}(p_i - 1)$. By considering the possible factorization of 12, we reach that $n = 13, 21, 26, 28, 36, 42$.

2 If $(c_i, m) = 1$,then $(m - c_i, m) = 1$ and $c_i \not\equiv m - c_i \mod m$. Furthermore, notice that since $n \neq 2, \phi(n)$ is always even. WLOG, let's assume for all $c_i$, $1 \leq c_i \leq m-1$ and $c_1 < c_2 < \cdots < c_{\phi(m)}$, then

$$\begin{aligned}
&c_1 + c_2 + \cdots + c_{\phi(m)} \\
&= c_1 + c_{\phi(m)-1} + c_2 + c_{\phi(m)-2} + \cdots + c_{\frac{\phi(m)}{2}} + c_{\frac{\phi(m)}{2}+1} \\
&= c_1 + m - c_1 + c_2 + m - c_2 + \cdots + c_{\frac{\phi(m)}{2}} + m - c_{\frac{\phi(m)}{2}} \\
&\equiv 0 \mod m
\end{aligned}$$

3a Since

$$\begin{aligned}
2^{2047-1} = (2^{11})^{186} \equiv 1 \mod 2047 \\
2^{1023} = (2^{11})^{93} \equiv 1 \mod 2047
\end{aligned}$$

2047 passes Miller's test to the base 2.

3b Since $2821 = 7 \times 13 \times 31$ is square free and $(7-1)|(2821-1)$, $(13-1)|(2821-1)$, $(31-1)|(2821-1)$, we conclude that 2821 is a Carmichael number by Korselt's criterion.

4 The scenario in the question is equivelant to solving the following Diophantine equation

$$63x + 7 = 23y$$

The general solution is

$$x = 28 + 23t, y = 77 + 63t$$

The smallest positive solution is

$$x = 5, y = 14$$

There are 5 plantains in each of the 63 piles.

5 By Euler's theorem, we have $2^{\phi(77)} = 2^{60} \equiv 1 \mod 77$. Thus,

$$2^{94338} = (2^{60})^{1572} \times 2^{18} \equiv 36 \mod 77$$

6 By Euler's theorem, we have $a^{\phi(b)} \equiv 1 \mod b$. And it is obvious $b^{\phi(a)} \equiv 0 \mod b$. Thus,

$$a^{\phi(b)} + b^{\phi(a)} \equiv 1 \mod b$$

Similarly, $a^{\phi(b)}+b^{\phi(a)} \equiv 1 \mod a$. Since $a|(a^{\phi(b)}+b^{\phi(a)}-1)$ and $b|(a^{\phi(b)}+b^{\phi(a)}-1)$, it must be $\mathrm{lcm}(a,b) = ab|(a^{\phi(b)} + b^{\phi(a)} - 1)$, therefore

$$a^{\phi(b)} + b^{\phi(a)} \equiv 1 \mod ab$$

7a Since

$$2^{62} = (2^6)^{10} \times 2^2 \equiv 4 \mod 63$$

63 is not a pseudoprime to the base $b = 2$.

7b Since

$$2^{\frac{1387-1}{2}} = 2^{693} \equiv 512 \mod 1387$$
$$2^{1387-1} \equiv (512)^2 \equiv 1 \mod 1387$$

1387 is a pseudoprime but not a strong pseudoprime to the base $n = 2$.

8 From theorem 2.1, we see that every positive integer can be represented uniquely in base 3, i.e., $n = \sum_{i=0}^{k} b_i 3^i$ with $b_i \in \{0, 1, 2\}$. To construct the required representation in the question, we replace any $2 \times 3^i$ with $3^{i+1} - 3^i$ untill all coefficients are $-1, 0, 1$. For negative integer $n$, we first obtain the representation of $-n$, then add a minus sign for each coefficient. To prove uniqueness, suppose there are two representations of $n = \sum_{i=0}^{k} b_i 3^i = \sum_{i=0}^{k} a_i 3^i$. Subtract $\sum_{i=0}^{k} b_i 3^i$ from $\sum_{i=0}^{k} a_i 3^i$, we have

$$\sum_{i=0}^{k} (a_i - b_i) 3^i = 0$$

Let $j$ be the smallest index such that $a_j \neq b_j$, then

$$\sum_{i=j}^{k} (a_i - b_i) 3^i = 0$$

$$3^j \sum_{i=j}^{k} (a_i - b_i) 3^{i-j} = 0$$

It must be that $\sum_{i=j}^{k} (a_i - b_i) 3^{i-j} = 0$ and

$$\sum_{i=j+1}^{k} (a_i - b_i) 3^{i-j} = -(a_j - b_j)$$

It must be that $3|(a_j - b_j)$. However $-2 \leq a_j - b_j \leq 2$, which is a contradiction.

9a A primitive root $r \mod n$ is a positive integer such that $(r, n) = 1$ and $\text{ord}_n r = \phi(n)$. Since $\phi(29) = 28$, the possible divisors of 28 is $1, 2, 4, 7, 14, 28$. Check that

$$3^2 = 9 \mod 29$$

$$3^4 = 23 \mod 29$$

$$3^7 = 12 \mod 29$$

$$3^{14} = 28 \mod 29$$

We conclude that 3 is a primitive root of 29.

9b There are $\phi(\phi(29)) = 12$ incongruent roots of 29.

9c Recall that a number of the form $2, 4, p^t, 2p^t$ has at least one primitive root. Since $34 = 2 \times 17$, it has a primitive root. Try 3 and follow the same method in 9a. We conclude that 3 is a primitive root of 34.

10a To find $d$, we solve

$$ed = 3d \equiv 1 \mod \phi(33)$$

$$d \equiv 7 \mod 20$$

10b To decipher, we apply

$$P = C^d \mod n$$

to get

$$04^7 \equiv 16 \mod 33$$

$$23^7 \equiv 23 \mod 33$$

$$00^7 \equiv 00 \mod 33$$

$$12^7 \equiv 12 \mod 33$$

So the plain text is QXAM