COMP2711 Homework3

LIU, Jianmeng 20760163

Question 1:

From $32b - 21a = 19$, we have:

$$\begin{aligned} 32b - 21a &\equiv 19 (\text{mod } 21) \\ 32b &\equiv 19 (\text{mod } 21) \quad (*) \end{aligned}$$

To solve this congruence, we need to find a multiple inverse of 32 modulo 21. Notice that $\gcd(32, 21) = 1$, so by using the Euclidean algorithm, we have:

$$\begin{aligned} 32 &= 1 \cdot 21 + 11 \\ 21 &= 1 \cdot 11 + 10 \\ 11 &= 1 \cdot 10 + 1 \end{aligned}$$

Reverse the steps, we have:

$$\begin{aligned} 1 &= 11 - 1 \cdot 10 \\ &= 11 - 1 \cdot (21 - 1 \cdot 11) \\ &= 2 \cdot 11 - 1 \cdot 21 \\ &= 2 \cdot (32 - 1 \cdot 21) - 1 \cdot 21 \\ &= 2 \cdot 32 - 3 \cdot 21 \end{aligned}$$

Thus,

$$\begin{aligned} 2 \cdot 32 - 3 \cdot 21 &\equiv 1 (\text{mod } 21) \\ 2 \cdot 32 &\equiv 1 (\text{mod } 21) \end{aligned}$$

which means 2 is a multiple inverse of 32 modulo 21. To solve $(*)$, we multiply 2 on both sides,

$$\begin{aligned} 2 \cdot 32b &\equiv 2 \cdot 19 (\text{mod } 21) \\ b &\equiv 38 (\text{mod } 21) \equiv 17 (\text{mod } 21) \end{aligned}$$

Thus, $b = 17 + 21k$, where $k \in \mathbb{Z}$. Since $b \in \mathbb{Z}_{42}$, only $k = 0$ and $k = 1$ are valid, which gives $b = 17$ or $b = 38$.

- When $b = 17$, $32 \cdot 17 - 21a = 19$, we get $a = 25 \in \mathbb{Z}_{42}$.
- When $b = 38$, $32 \cdot 38 - 21a = 19$, we get $a = 57 \notin \mathbb{Z}_{42}$.

Therefore, there exists only one pair of a, b, where $a = 25, b = 17$.

Question 2:

Question 3:

We first let $m = 9 \cdot 14 \cdot 5 = 630$, $M_1 = m/9 = 70, M_2 = m/14 = 45, M_3 = m/5 = 126$.

By using extended Euclidean algorithm, we know:

4 is an inverse of M_1 modulo 9, since $4 \cdot 70 \equiv 4 \cdot 7 \equiv 1 (\text{mod } 9)$

5 is an inverse of M_2 modulo 14, since $5 \cdot 45 \equiv 5 \cdot 3 \equiv 1 (\text{mod } 14)$

1 is an inverse of M_3 modulo 5, since $1 \cdot 126 \equiv 1 \cdot 1 \equiv 1 (\text{mod } 5)$

So the solutions to the system are those x such that:

$$\begin{aligned} x &\equiv 4 \cdot 70 \cdot 4 + 8 \cdot 45 \cdot 5 + 3 \cdot 126 \cdot 1 \\ &= 3298 \\ &\equiv 148 (\text{mod } 630) \end{aligned}$$

Therefore, the solutions are those x such that $x \equiv 148 (\text{mod } 630)$, which can also be written as $x = 148 + 630k, k \in \mathbb{Z}$.

Question 4:

Note that $1027_{10} = 2^{10} + 2^1 + 2^0 = (100\ 0000\ 0011)_2$, compute:

$$\begin{aligned} 8^{2^0} &\equiv 8 (\text{mod } 22) \\ 8^{2^1} &\equiv (8^2) \equiv 20 (\text{mod } 22) \\ 8^{2^2} &\equiv (20^2) \equiv 4 (\text{mod } 22) \\ 8^{2^3} &\equiv (4^2) \equiv 16 (\text{mod } 22) \\ 8^{2^4} &\equiv (16^2) \equiv 14 (\text{mod } 22) \\ 8^{2^5} &\equiv (14^2) \equiv 20 (\text{mod } 22) \\ 8^{2^6} &\equiv (20^2) \equiv 4 (\text{mod } 22) \\ 8^{2^7} &\equiv (4^2) \equiv 16 (\text{mod } 22) \\ 8^{2^8} &\equiv (16^2) \equiv 14 (\text{mod } 22) \\ 8^{2^9} &\equiv (14^2) \equiv 20 (\text{mod } 22) \\ 8^{2^{10}} &\equiv (20^2) \equiv 4 (\text{mod } 22) \end{aligned}$$

According to repeated squaring method, we know that

$$
\begin{aligned}
8^{1027} &= 8^{2^{10}} \cdot 8^{2^1} \cdot 8^{2^0} \\
&\equiv 4 \cdot 20 \cdot 8 (\bmod 22) \\
&\equiv 2 (\bmod 22)
\end{aligned}
$$

Therefore, $8^{1027} \equiv 2 (\bmod 22)$

Question 5: