ADSP: HW3

Lo Chun, Chou
R13922136

April 24, 2025

(1)

(2)

(a)

By Fermat's little theorem, since 67 is a prime number, we have:

$$2^{66} \equiv 1 \pmod{67}$$

Then using the fact that:

$$\text{if } a \equiv b \pmod{n} \text{ then } a^k \equiv b^k \pmod{n} \text{ for any integer } k \in \mathbb{Z}^+$$

we have:

$$\begin{aligned} &(2^{66})^{10} \equiv 1^{10} \pmod{67} \\ \Rightarrow\ &2^{660} \equiv 1 \pmod{67} \end{aligned}$$

And using the property:

$$\text{If } a \equiv b \pmod{n} \text{ and } c \equiv d \pmod{n} \text{ then } a \cdot c \equiv b \cdot d \pmod{n}$$

We can calculate 2^{40}:

$$\begin{aligned} &2^6 \equiv 64 \equiv -3 \pmod{67} \\ \Rightarrow\ &(2^6)^6 \equiv (-3)^6 \equiv 243 \times 3 \equiv 42 \times 3 \equiv 126 \equiv -8 \pmod{67} \\ \Rightarrow\ &2^{40} \equiv 2^{36} \times 2^4 \equiv (-8) \times 16 \equiv -128 \equiv 6 \pmod{67} \end{aligned}$$

and combine 2^{40} with 2^{660}, and we'll get the required result:

$$\begin{aligned}
2^{700} \pmod{67} &\equiv 2^{660} \cdot 2^{40} \pmod{67} \\
&\equiv 1 \cdot 6 \pmod{67} \\
&\equiv 6 \pmod{67} \qquad \square
\end{aligned}$$

(b)

We're given the following congruences and are required to find $x \in \mathbb{Z}^+, \quad x \in [0, 2800]$:

$$\begin{aligned}
x &\equiv 4 \pmod{43} \\
x &\equiv 15 \pmod{67}
\end{aligned}$$

Since $\gcd(43, 67) = 1$, we can use the Chinese Remainder Theorem.

Let $n_1 = 43$ and $n_2 = 67$, then we'll have:

$$\begin{aligned}
n &= n_1 \cdot n_2 = 2881 \\
N_1 &= \frac{n}{n_1} = 67 \\
N_2 &= \frac{n}{n_2} = 43
\end{aligned}$$

And we'll need to solve:

$$\begin{aligned}
N_1 x_1 \equiv 1 \pmod{n_1} &\implies 67x_1 \equiv 1 \pmod{43} \\
N_2 x_2 \equiv 1 \pmod{n_2} &\implies 43x_2 \equiv 1 \pmod{67}
\end{aligned}$$

Using the Extended Euclidean Algorithm:

$$\begin{aligned}
67 &= 1 \cdot 43 + 24 &&\Rightarrow 24 = 67 - 1 \cdot 43 \\
43 &= 1 \cdot 24 + 19 &&\Rightarrow 19 = 43 - 1 \cdot 24 \\
24 &= 1 \cdot 19 + 5 &&\Rightarrow 5 = 24 - 1 \cdot 19 \\
19 &= 3 \cdot 5 + 4 &&\Rightarrow 4 = 19 - 3 \cdot 5 \\
5 &= 1 \cdot 4 + 1 &&\Rightarrow 1 = 5 - 1 \cdot 4
\end{aligned}$$

then we'll get:

$$
\begin{aligned}
1 &= 5 - 1 \cdot 4 \\
&= 5 - 1 \cdot (19 - 3 \cdot 5) \\
&= 5 - 1 \cdot 19 + 3 \cdot 5 \\
&= 4 \cdot 5 - 1 \cdot 19 \\
&= 4 \cdot (24 - 1 \cdot 19) - 1 \cdot 19 \\
&= 4 \cdot 24 - 5 \cdot 19 \\
&= 4 \cdot 24 - 5 \cdot (43 - 1 \cdot 24) \\
&= 9 \cdot 24 - 5 \cdot 43 \\
&= 9 \cdot (67 - 1 \cdot 43) - 5 \cdot 43 \\
&= 9 \cdot 67 - 14 \cdot 43
\end{aligned}
$$

Thus, $x_1 = 9,\ x_2 = -14$ (or $x_2 = 53$).

And the solution $\bar{x}$ is:

$$
\begin{aligned}
\bar{x} &\equiv N_1 \cdot x_1 \cdot 4 + N_2 \cdot x_2 \cdot 15 \pmod{n} \\
&\equiv 67 \cdot 9 \cdot 4 + 43 \cdot (-14) \cdot 15 \pmod{2881} \\
&\equiv 2412 - 9030 \pmod{2881} \\
&\equiv -6618 \pmod{2881} \\
&\equiv 2025 \pmod{2881} \qquad \square
\end{aligned}
$$

(c)

By Wilson's theorem, we knew that if p is a prime, then:

$$(p-1)! \equiv -1 \pmod{p}$$

Thus, since 43 is a prime, we have:

$$
\begin{aligned}
& 42! \equiv -1 \pmod{43} \\
\Rightarrow\ & 39! \times 40 \times 41 \times 42 \equiv 42 \pmod{43}
\end{aligned}
$$

By another property of modular arithmetic, we have:

$$\text{If } ca \equiv cb \pmod{n} \text{ and } \gcd(c, n) = 1 \text{ then } a \equiv b \pmod{n}$$

Therefore, since $\gcd(42, 43) = 1$, we can divide 42 on both sides:

$$39! \times 40 \times 41 \equiv 1 \pmod{43}$$

Thus, this means that 39! is the inverse of $40 \times 41 \pmod{43}$.

$$40 \times 41 \equiv (-3) \times (-2) \equiv 6 \pmod{43}$$

Solving this using the Extended Euclidean Algorithm:

$$43 = 6 \cdot 7 + 1 \quad \Rightarrow \; 1 = 43 - 6 \cdot 7$$

So we found that the inverse of 6 is -7 or $36 \pmod{43}$. And hence the solution is:

$$39! \equiv 36 \pmod{43} \qquad \square$$

(3)

(4)

(5)

(6)

(7)

Extra problems