ADSP: HW3

Lo Chun, Chou
R13922136

May 7, 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:

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

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)

We're given:

$$M = 11, \; \alpha = 8 + 6i, \; N = 12$$

Since N has factors: $d \in \{1, 2, 3, 4, 6, 12\}$, we can define:

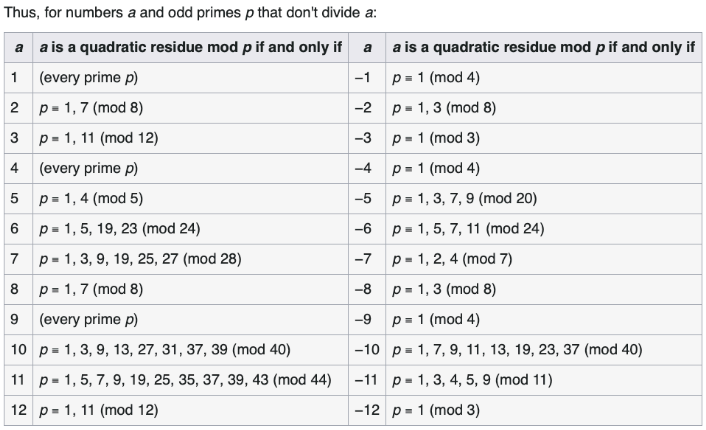
(4)

Using the following properties:

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & p \equiv 1, 7 \pmod{8} \\ -1 & p \equiv 3, 5 \pmod{8} \end{cases} \tag{1}$$

And referencing the following table [1]:

[1] https://en.wikipedia.org/wiki/Quadratic_residue



Thus, for numbers *a* and odd primes *p* that don't divide *a*:

a	***a* is a quadratic residue mod *p* if and only if**	***a***	***a* is a quadratic residue mod *p* if and only if**
1	(every prime *p*)	−1	*p* ≡ 1 (mod 4)
2	*p* ≡ 1, 7 (mod 8)	−2	*p* ≡ 1, 3 (mod 8)
3	*p* ≡ 1, 11 (mod 12)	−3	*p* ≡ 1 (mod 3)
4	(every prime *p*)	−4	*p* ≡ 1 (mod 4)
5	*p* ≡ 1, 4 (mod 5)	−5	*p* ≡ 1, 3, 7, 9 (mod 20)
6	*p* ≡ 1, 5, 19, 23 (mod 24)	−6	*p* ≡ 1, 5, 7, 11 (mod 24)
7	*p* ≡ 1, 3, 9, 19, 25, 27 (mod 28)	−7	*p* ≡ 1, 2, 4 (mod 7)
8	*p* ≡ 1, 7 (mod 8)	−8	*p* ≡ 1, 3 (mod 8)
9	(every prime *p*)	−9	*p* ≡ 1 (mod 4)
10	*p* ≡ 1, 3, 9, 13, 27, 31, 37, 39 (mod 40)	−10	*p* ≡ 1, 7, 9, 11, 13, 19, 23, 37 (mod 40)
11	*p* ≡ 1, 5, 7, 9, 19, 25, 35, 37, 39, 43 (mod 44)	−11	*p* ≡ 1, 3, 4, 5, 9 (mod 11)
12	*p* ≡ 1, 11 (mod 12)	−12	*p* ≡ 1 (mod 3)

$$a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \tag{2}$$

$$\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \tag{3}$$

We can calculate the Legendre sequence for $p = 11$:

$$\left(\frac{1}{11}\right) = 1 \qquad \because 1 \equiv 1^2 \pmod{11}$$
$$\left(\frac{2}{11}\right) = -1 \qquad \because \text{Using (1)},\ 11 \equiv 3 \pmod{8}$$
$$\left(\frac{3}{11}\right) = 1 \qquad \because 3 \equiv 25 \equiv 5^2 \pmod{11}$$
$$\left(\frac{4}{11}\right) = 1 \qquad \because 4 \equiv 81 \equiv 9^2 \pmod{11}$$
$$\left(\frac{5}{11}\right) = 1 \qquad \because 5 \equiv 16 \equiv 4^2 \pmod{11}$$
$$\left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right) = (-1) \times 1 = -1$$
$$\left(\frac{7}{11}\right) = -1 \qquad \text{(Using the table)}$$
$$\left(\frac{8}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{4}{11}\right) = (-1) \times 1 = -1$$
$$\left(\frac{9}{11}\right) = \left(\frac{3}{11}\right)\left(\frac{3}{11}\right) = 1 \times 1 = 1$$
$$\left(\frac{10}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{5}{11}\right) = (-1) \times 1 = -1$$

Thus, the Legendre sequence for $p = 11$ is:

$$\{0, \left(\frac{1}{11}\right), \left(\frac{2}{11}\right), \left(\frac{3}{11}\right), \left(\frac{4}{11}\right), \left(\frac{5}{11}\right), \left(\frac{6}{11}\right), \left(\frac{7}{11}\right), \left(\frac{8}{11}\right), \left(\frac{9}{11}\right), \left(\frac{10}{11}\right)\}$$
$$=\{0, 1, -1, 1, 1, 1, -1, -1, -1, 1, -1\} \qquad \square$$

(5)

(a)

We're given:

$$y[n] = x[n] + 0.4x[n-20] + 0.2x[n-30]$$

And need to find $p[n]$ s.t. $y[n] = x[n] * p[n]$

It is trivial that:

$$p[n] = \delta[n] + 0.4\delta[n-20] + 0.2\delta[n-30] \qquad \square$$

(b)

The lifter is designed to set to 0 when n is a multiple of $N_p = 20$ or 30, and set to 1 otherwise.

Thus, we can design the lifter as:

$$l[n] = \begin{cases} 0 & \text{if } n = 20k \text{ or } 30k \text{ for any } k = 1, 2, 3, \cdots \\ 1 & \text{otherwise} \end{cases} \qquad \square$$

(6)

(a)

It is possible for human to hear voice with freqeuncy $19Hz$.

Even though in theory, the frequency that human can hear is between $20Hz$ and $20000Hz$, by the lower bound of hearing graph in lecture slide p.238, if the sound intensity (P) is high enough, then it is possible for human to hear.

(b)

When we're splitting a signal into segments, where each segment present a word, we are using the property that consonants have smaller energy than vowels, so we can distinguish each word by finding the parts with smaller amplitude. (This can be seen at p.248 of the lecture note.)

However, for some words with <u>double vowels</u>, or there is <u>no consonant</u> in the word, we can not split the signal by this approach.

(c)

A music signal always has a the chord phenomenon because music signal is generated by resonance, for example, brass instruments generate sound by the vibration of a resonator.

Any sound that is generated by resonance has the effect that at freqeuncy values:

$$f = k \cdot f_0 \qquad k \in \mathbb{Z}^+$$

The amplitude of the signal is larger, which is the chord phenomenon.

(7)

(a)

(b)

The first reason why the compression ratio of an image can be higher than an audio signal because image is of dimension $2D$, while audio signal is of dimension $1D$, this causes the redundancy of image to be higher than audio signal.

For example, in an image, if there is a pixel of white color, then it is likely that the pixels surrounding it are also white, and this does not happen only when the pixel is at the edge of an object. This example shows the property of consistency in space domain.

Another reason is also due to consistency but in the frequency domain, if we use intensity to represent amplitude, images tend to concentrate on low-frequency components, thus, the information that needed to be stored is less.

(c)

Extra problem