Applied Mathematics 3B

Assignment #7 **Solution**

---

1. We have

$$F_6 = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & e^{2\pi i/6} & e^{4\pi i/6} & e^{6\pi i/6} & e^{8\pi i/6} & e^{10\pi i/6} \\ 1 & e^{4\pi i/6} & e^{8\pi i/6} & e^{12\pi i/6} & e^{16\pi i/6} & e^{20\pi i/6} \\ 1 & e^{6\pi i/6} & e^{12\pi i/6} & e^{18\pi i/6} & e^{24\pi i/6} & e^{30\pi i/6} \\ 1 & e^{8\pi i/6} & e^{16\pi i/6} & e^{24\pi i/6} & e^{32\pi i/6} & e^{40\pi i/6} \\ 1 & e^{10\pi i/6} & e^{20\pi i/6} & e^{30\pi i/6} & e^{40\pi i/6} & e^{50\pi i/6} \end{pmatrix} = \begin{pmatrix} 1 & 1 & 1 & 1 & 1 & 1 \\ 1 & e^{\pi i/3} & e^{2\pi i/3} & -1 & -e^{\pi i/3} & -e^{2\pi i/3} \\ 1 & e^{2\pi i/3} & -e^{\pi i/3} & 1 & e^{2\pi i/3} & -e^{\pi i/3} \\ 1 & -1 & 1 & -1 & 1 & -1 \\ 1 & -e^{\pi i/3} & e^{2\pi i/3} & 1 & -e^{\pi i/3} & e^{2\pi i/3} \\ 1 & -e^{2\pi i/3} & -e^{\pi i/3} & -1 & e^{2\pi i/3} & e^{\pi i/3} \end{pmatrix}.$$

Notice that row j has the entry $e^{2\pi ijk/n}$ in column k (where $n = 6$). Since $\cos(4\omega) = \cos\omega$ we expect a periodicity of 3. Similarly $\sin(4\omega) = \sin\omega$. We also have

$$\begin{pmatrix} \cos(\omega) \\ \cos(2\omega) \\ \cos(3\omega) \\ \cos(4\omega) \\ \cos(5\omega) \\ \cos(6\omega) \end{pmatrix} = \frac{1}{2}\begin{pmatrix} -1 \\ -1 \\ 2 \\ -1 \\ -1 \\ 2 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} \sin(\omega) \\ \sin(2\omega) \\ \sin(3\omega) \\ \sin(4\omega) \\ \sin(5\omega) \\ \sin(6\omega) \end{pmatrix} = \frac{1}{2}\begin{pmatrix} \sqrt{3} \\ -\sqrt{3} \\ 0 \\ \sqrt{3} \\ -\sqrt{3} \\ 0 \end{pmatrix}.$$

It follows that

$$F_6\begin{pmatrix} \cos(\omega) \\ \cos(2\omega) \\ \cos(3\omega) \\ \cos(4\omega) \\ \cos(5\omega) \\ \cos(6\omega) \end{pmatrix} = \frac{1}{2}\begin{pmatrix} -1-1+2-1-1+2 \\ -1-e^{\pi i/3}+2e^{2\pi i/3}+1+e^{\pi i/3}-2e^{2\pi i/3} \\ -1-e^{2\pi i/3}-2e^{\pi i/3}-1-e^{2\pi i/3}-2e^{\pi i/3} \\ -1+1+2+1-1-2 \\ -1+e^{\pi i/3}+2e^{2\pi i/3}-1+e^{\pi i/3}+2e^{2\pi i/3} \\ -1+e^{2\pi i/3}-2e^{\pi i/3}+1-e^{2\pi i/3}+2e^{\pi i/3} \end{pmatrix} = 3\begin{pmatrix} 0 \\ 0 \\ -\frac{1}{2}-\frac{\sqrt{3}}{2}i \\ 0 \\ -\frac{1}{2}+\frac{\sqrt{3}}{2}i \\ 0 \end{pmatrix}$$

The non-zero coefficients are at coordinate 2 and 4. The underlying period is then $6/2 = 3$. The fraction $6/4$ is not a valid period. Similarly

$$F_6\begin{pmatrix} \sin(\omega) \\ \sin(2\omega) \\ \sin(3\omega) \\ \sin(4\omega) \\ \sin(5\omega) \\ \sin(6\omega) \end{pmatrix} = \frac{1}{2}\begin{pmatrix} \sqrt{3}-\sqrt{3}+\sqrt{3}-\sqrt{3} \\ \sqrt{3}-\sqrt{3}e^{\pi i/3}-\sqrt{3}+\sqrt{3}e^{\pi i/3} \\ \sqrt{3}-\sqrt{3}e^{2\pi i/3}+\sqrt{3}-\sqrt{3}e^{2\pi i/3} \\ \sqrt{3}+\sqrt{3}-\sqrt{3}-\sqrt{3} \\ \sqrt{3}+\sqrt{3}e^{\pi i/3}+\sqrt{3}+\sqrt{3}e^{\pi i/3} \\ \sqrt{3}+\sqrt{3}e^{2\pi i/3}-\sqrt{3}-\sqrt{3}e^{2\pi i/3} \end{pmatrix} = 3\begin{pmatrix} 0 \\ 0 \\ \frac{\sqrt{3}}{2}-\frac{i}{2} \\ 0 \\ \frac{\sqrt{3}}{2}+\frac{i}{2} \\ 0 \end{pmatrix}$$

Once again the period is 3. Another way to see this is to note that

$$\begin{pmatrix} \cos(\omega) \\ \cos(2\omega) \\ \cos(3\omega) \\ \cos(4\omega) \\ \cos(5\omega) \\ \cos(6\omega) \end{pmatrix} = \frac{1}{2}\begin{pmatrix} e^{i\omega}+e^{-i\omega} \\ e^{i2\omega}+e^{-i2\omega} \\ e^{i3\omega}+e^{-i3\omega} \\ e^{i4\omega}+e^{-i4\omega} \\ e^{i5\omega}+e^{-i5\omega} \\ e^{i6\omega}+e^{-i6\omega} \end{pmatrix}.$$

Thus the m-th entry (counting from 0) is $\frac{1}{2}(e^{i2\pi(2(m+1))/6} + e^{-i2\pi(2(m+1))/6})$. Thus for the j-th entry of $F_6(\cos\omega, \ldots, \cos(6\omega))^T$ we find

$$\begin{aligned} \sum_{k=0}^{5} e^{2\pi ijk/6}\frac{1}{2}\left(e^{i2\pi(2(k+1))/6} + e^{-i2\pi(2(k+1))/6}\right) &= \frac{1}{2}\sum_{k=0}^{5} e^{i2\pi(jk+2(k+1))/6} + \frac{1}{2}\sum_{k=0}^{5} e^{i2\pi(jk-2(k+1))/6} \\ &= e^{i2\pi/3}\frac{1}{2}\sum_{k=0}^{5} e^{i2\pi(jk+2k)/6} + e^{-i2\pi/3}\frac{1}{2}\sum_{k=0}^{5} e^{i2\pi(jk-2k)/6} \end{aligned}$$

$$
\begin{aligned}
&= e^{i2\pi/3}\frac{1}{2}\sum_{k=0}^{5}\left[e^{i2\pi(j+2)/6}\right]^k + e^{-i2\pi/3}\frac{1}{2}\sum_{k=0}^{5}\left[e^{i2\pi(j-2)/6}\right]^k \\
&= 3e^{i2\pi/3}\delta_{j,4} + 3e^{-i2\pi/3}\delta_{j,2} \\
&= \begin{cases} 3\left(-\frac{1}{2}+\frac{\sqrt{3}}{2}i\right) & j=4 \\ 3\left(-\frac{1}{2}-\frac{\sqrt{3}}{2}i\right) & j=2 \\ 0 & \text{otherwise} \end{cases}.
\end{aligned}
$$

From

$$
\begin{pmatrix} \sin(\omega) \\ \sin(2\omega) \\ \sin(3\omega) \\ \sin(4\omega) \\ \sin(5\omega) \\ \sin(6\omega) \end{pmatrix} = -\frac{i}{2}\begin{pmatrix} e^{i\omega} - e^{-i\omega} \\ e^{i2\omega} - e^{-i2\omega} \\ e^{i3\omega} - e^{-i3\omega} \\ e^{i4\omega} - e^{-i4\omega} \\ e^{i5\omega} - e^{-i5\omega} \\ e^{i6\omega} - e^{-i6\omega} \end{pmatrix}
$$

we find that the j-th entry of $(\sin\omega,\ldots,\sin(6\omega))^T$ is $-\frac{i}{1}2(e^{i2\pi(2(m+1))/6} - e^{-i2\pi(2(m+1))/6})$ and for the j-th entry of $F_6(\sin\omega,\ldots,\sin(6\omega))^T$

$$
\begin{aligned}
\sum_{k=0}^{5} e^{2\pi ijk/6}\left(-\frac{i}{2}\right)\left(e^{i2\pi(2(k+1))/6} - e^{-i2\pi(2(k+1))/6}\right) &= -\frac{i}{2}\sum_{k=0}^{5} e^{i2\pi(jk+2(k+1))/6} + \frac{i}{2}\sum_{k=0}^{5} e^{i2\pi(jk-2(k+1))/6} \\
&= -e^{i2\pi/3}\frac{i}{2}\sum_{k=0}^{5} e^{i2\pi(jk+2k)/6} + e^{-i2\pi/3}\frac{i}{2}\sum_{k=0}^{5} e^{i2\pi(jk-2k)/6} \\
&= -e^{i2\pi/3}\frac{i}{2}\sum_{k=0}^{5}\left[e^{i2\pi(j+2)/6}\right]^k + e^{-i2\pi/3}\frac{i}{2}\sum_{k=0}^{5}\left[e^{i2\pi(j-2)/6}\right]^k \\
&= -3ie^{i2\pi/3}\delta_{j,4} + 3ie^{-i2\pi/3}\delta_{j,2} \\
&= \begin{cases} 3\left(\frac{\sqrt{3}}{2}+\frac{i}{2}\right) & j=4 \\ 3\left(\frac{\sqrt{3}}{2}-\frac{i}{2}\right) & j=2 \\ 0 & \text{otherwise} \end{cases}.
\end{aligned}
$$

2. For $a = 5$ we find (for each power we calculate the remainder after division by 21)

$$
\begin{array}{llrlrlrll}
a^0 & \equiv & 1 & \equiv & & \equiv & 1 & \bmod & 21 \\
a^1 & \equiv & 5 & \equiv & 1\times 5 & \equiv & 5 & \bmod & 21 \\
a^2 & \equiv & 25 & \equiv & 5\times 5 & \equiv & 4 & \bmod & 21 \\
a^3 & \equiv & 125 & \equiv & 4\times 5 & \equiv & 20 & \bmod & 21 \\
a^4 & \equiv & 625 & \equiv & 20\times 5 & \equiv & 16 & \bmod & 21 \\
a^5 & \equiv & 3125 & \equiv & 16\times 5 & \equiv & 17 & \bmod & 21 \\
a^6 & \equiv & 15625 & \equiv & 17\times 5 & \equiv & 1 & \bmod & 21
\end{array}
$$

Thus we find $r = 6$, $\gcd(5^3-1, 21) = \gcd(124, 21) = 1$. **The algorithm fails to find a non-trivial factor in this case (omission in the textbook).** The gcd can be found using the Euclidean algorithm:

$$
124/21 = 5 \quad \text{rem} \quad 19, \qquad 21/19 = 1 \quad \text{rem} \quad 2, \qquad 19/2 = 9 \quad \text{rem} \quad 1, \qquad 2/\mathbf{1} = 2 \quad \text{rem} \quad \mathbf{0}.
$$

For $a = 8$ we find (for each power we calculate the remainder after division by 21)

$$
\begin{array}{llrlrll}
a^0 & \equiv & 1 & \equiv & 1 & \bmod & 21 \\
a^1 & \equiv & 8 & \equiv & 8 & \bmod & 21 \\
a^2 & \equiv & 64 & \equiv & 1 & \bmod & 21
\end{array}
$$

Thus we find $r = 2$, $\gcd(8^1-1, 21) = \gcd(7, 21) = 7$. The gcd can be found using the Euclidean algorithm:

$$
21/\mathbf{7} = 3 \quad \text{rem} \quad \mathbf{0}.
$$

Thus the factors are 7 and $21/7 = 3$.

For $a = 4$ we find (for each power we calculate the remainder after division by 21)

$$\begin{array}{rcrcrll} a^0 & \equiv & 1 & \equiv & 1 & \mod & 21 \\ a^1 & \equiv & 4 & \equiv & 4 & \mod & 21 \\ a^2 & \equiv & 16 & \equiv & 16 & \mod & 21 \\ a^3 & \equiv & 64 & \equiv & 1 & \mod & 21 \end{array}$$

Thus we find $r = 3$. Since r is odd, we cannot apply the method.

Note that for $r = 6$ we also have $a^r = 1 \mod 21$, however $a^{\frac{r}{2}} - 1 = 4^3 - 1 \equiv 0 \mod 21$ and we cannot apply the method.