COSC581 - Algorithms
Spring 2023
Homework #8 Solutions

1. Let ω be an n^{th} root of unity, and let k be a fixed integer. Evaluate:

$$1 + \omega^k + \omega^{2k} + \cdots + \omega^{(n-1)k}$$

The sum of a closed form geometric formula: $a + ar^2 + ... + ar^n = \sum^n_{k=0}(ar^k) = a((1 - r^{n+1}) / (1 - r))$.
source: https://en.wikipedia.org/wiki/Geometric_series.

Therefore, a=1, r=ω, and k=0→n-1. Thus,
$1 + \omega^k + \omega^{2k} + ... + \omega^{k(n-1)} = 1((1 - \omega^n) / (1 - \omega)) = 1((1 - 1) / (1 - e^{2\pi i/n})) = 0$.
□

---

2. Use the FFT to compute $C(x)$ as the product of $A(x)$ and $B(x)$, where $A(x) = x^2 + 3x + 1$ and $B(x) = x + 7$.
   a. Find the value of $A(x)$ at the complex fourth roots of unity (1, -1, i, -i).

$A^{[0]}(x) = 1 + x$
$A^{[1]}(x) = 3$
So, $A(x) = A^{[0]}(x^2)+x(A^{[1]}(x^2))$

$A(1) = 1^2+3(1)+1 = 5$
$A(-1) = (-1)^2+3(-1)+1 = -1$
$A(i) = i^2+3(i)+1 = 3i$
$A(-i) = (-i)^2+3(-i)+1 = -3i$

   b. Find the value of $B(x)$ at the complex fourth roots of unity.

$B^{[0]}(x) = 7$
$B^{[1]}(x) = 1$
So, $B(x) = B^{[0]}(x^2)+x(B^{[1]}(x^2))$

$B(1) = 1+7 = 8$
$B(-1) = -1+7 = 6$
$B(i) = i+7$
$B(-i) = -i+7$

c. Use the results of (a) and (b) to find the value of $C(x)$ at the complex fourth roots of unity.

$C(1) = A(1)*B(1) = 5*8 = 40$
$C(-1) = A(-1)*B(-1) = -1*6 = -6$
$C(i) = A(i)*B(i) = 3i(i+7) = 3i^2+21i = 21i - 3$
$C(-i) = A(-i)*B(-i) = -3i(-i+7) = 3i^2 - 21i = -21i - 3$

d. Use these results to find the coefficients of $C(x)$.

$$C = \tfrac{1}{4}\begin{Vmatrix} 1 & 1 & 1 & 1 \\ 1 & -i & -1 & i \\ 1 & (-i)^2 & (-1)^2 & i^2 \\ 1 & (-i)^3 & (-1)^3 & i^3 \end{Vmatrix} \begin{Vmatrix} 40 \\ 21i-3 \\ -6 \\ -21i-3 \end{Vmatrix} = \tfrac{1}{4}\begin{Vmatrix} 40-6+21i-3-21i-3 \\ 40-i(21i-3)+6+i(-21i-3) \\ 40-1(21i-3)-6-1(-21i-3) \\ 40+i(21i-3)+6-i(-21i-3) \end{Vmatrix} = \begin{Vmatrix} 7 \\ 22 \\ 10 \\ 1 \end{Vmatrix}$$

So, $C(x) = 7 + 22x + 10x^2 + x^3$.
□

---

3. What is the totient of 3044?

Recall $\varphi(n) = n(1-1/p_1)(1-1/p_2)...(1-1/p_k)$, where $p_1 \rightarrow p_k$ are primes that divide n=3044.

The primes of 3044 are: 2, and 761 (determined programmatically). Thus,

$\varphi(n) = 3044(1-(½))(1-(1/761)) = 1520$.
□

---

4. Consider an RSA crypto scheme with n=21 and D=5.
   a. What is a possible value(s) of E?

$\varphi(n) = (p-1)(q-1) = (7-1)(3-1) = 6*2 = 12$

E can be any value such that:

- DE mod $\varphi(n) \equiv 1$
- $1 < E < \varphi(n)$
- $\gcd(E, \varphi(n)) = 1$

So, if $E = 5 \Rightarrow DE = 5*5 = 25 \% 12 = 1$.

b. Encode two messages of your choosing.

1) $M=3 \Rightarrow c \equiv 3^5 \% 21 = 12$
2) $M=9 \Rightarrow c \equiv 9^5 \% 21 = 18$

c. Name three messages that are unencodable.

M=0 and M=1 are always unencodable. Other messages include:

1) $M=6 \Rightarrow 6^5 = 7776 \% 21 = 6$
2) $M=7 \Rightarrow 7^5 = 16807 \% 21 = 7$
3) $M=8 \Rightarrow 8^5 = 32768 \% 21 = 8$

---

5. Given a finite simple undirected graph *G* and a positive integer *k*, explain how you would reduce the problem of finding in *G* an independent set of size *k* to the problem of merely deciding whether such a set exists.

Call the decision algorithm and assume it reports “yes,” since otherwise there is no search to be performed.

Two methods below:

Deleting vertices. Consider each vertex in turn by deleting it and calling again the decision algorithm. Whenever the decision algorithm reports “yes,” we know the graph still contains one or more Independent Sets so simply continue. Should the decision algorithm return “no,” however, we know the vertex just deleted is required in any remaining Independent Sets so restore it (and of course its incident edges) to the graph. Once this has been done, the resultant graph is an independent set of size k.

Adding edges. Iteratively attempt to add every edge missing from the original graph, retaining an edge iff the decision algorithm reports “yes.” Once this has been done, vertices with degree less than n-1 form an independent set of size k.