

Homework 2 Solutions - Sri Raga Velagapudi

1. **Given:** Two finite cyclic groups  $G_1$  and  $G_2$  such that  $|G_1| = |G_2| = n$  for some  $n \in \mathbb{Z}$ .

**Prove:**  $G_1 \cong G_2$

**Proof:** Let  $a \in G_1$  be the element that generates  $G_1$  and let  $b \in G_2$  be the element that generates  $G_2$ . Then every element in  $G_1$  is for the form  $a^i$  where  $0 \leq i < n$ . Similarly, every element  $G_2$  is for the form  $b^i$  where  $0 \leq i < n$ .

We can define an a function  $\varphi$  such that  $\varphi(a^i) \rightarrow b^i$  and  $\varphi^{-1}(b^i) \rightarrow a^i$ .

Now we have  $\varphi(a^0) = \varphi(a^n) = \varphi(1_1) \rightarrow 1_2 = b^n = b^0$ .

We also have that  $\varphi(a^i) \cdot \varphi(a^j) = b^i \cdot b^j = b^{i+j} = \varphi(a^{i+j}) = \varphi(a^i \cdot a^j)$  for  $0 \leq i, j < n$ . Also,  $\varphi$  is bijective because any two distinct elements  $a^i$  and  $a^j$  in  $G_1$  would map to  $b^i$  and  $b^j$  and if  $b^i = b^j$  then  $i = j$  implying that  $a^i = a^j$ .

2. **Given:** The fundamental theorem of abelian groups states that any group  $G$  of order  $n$  is isomorphic to the direct sum  $\mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \dots \mathbb{Z}_{p_{k-1}^{e_{k-1}}} \oplus \mathbb{Z}_{p_k^{e_k}}$  where  $p_i$  is a prime and  $e_i$  is a positive integer.

**Find:** Express  $\mathbb{F}_7^*$ , the multiplicative group of the field  $\mathbb{F}_7$ , in the above form.

**Solution:**  $\mathbb{F}_7^* = \{1, 2, 3, 4, 5, 6\}$ .  $|\mathbb{F}_7^*| = 6$ . By the above theorem,  $\mathbb{F}_7^* \cong \mathbb{Z}_3 \oplus \mathbb{Z}_2$ . The following is the mapping:-

$$1 \mapsto (0, 0)$$

$$2 \mapsto (1, 0)$$

$$3 \mapsto (2, 1)$$

$$4 \mapsto (2, 0)$$

$$5 \mapsto (1, 1)$$

$$6 \mapsto (0, 1)$$

Note that every element in  $\mathbb{F}_7^*$  is mapped to the corresponding element in  $\mathbb{Z}_3 \oplus \mathbb{Z}_2$  of the same order. That is, for each  $a \in \mathbb{F}_7^*$  and the smallest possible positive integer  $k$  such that  $a^k = 1$ , the corresponding element  $(x, y)$  in  $\mathbb{Z}_3 \oplus \mathbb{Z}_2$  satisfied  $(kx, ky) = (0, 0)$ .

**Find:** Express the multiplicative group of  $\mathbb{F}_7[x]/\langle x^2 + 1 \rangle$  in the above form.

**Solution:**  $x^2 + 1$  is irreducible over  $\mathbb{F}_7[x]$  therefore  $\mathbb{F}_7[x]/\langle x^2 + 1 \rangle$  is also a field. As a result the multiplicative group of  $\mathbb{F}_7[x]/\langle x^2 + 1 \rangle$ ,  $G$ , is the set  $\{ax + b | a, b \in \mathbb{F}_7\} - \{0\}$ . This is because only the 0 element lacks an inverse in a field.

$|G| = |\mathbb{F}_7[x]/\langle x^2 + 1 \rangle| - 1 = 48$ . Satisfying the representation in the theorem, all the potential direct sum representations of  $G$  are as follows:

$$(1) \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$$

$$(2) \mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$$

$$(3) \mathbb{Z}_{2^3} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3$$

$$(4) \mathbb{Z}_{2^4} \oplus \mathbb{Z}_3$$

$$(5) \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_3$$

Note that for a given direct sum group from the list above, the largest possible order of an element in the group is the least common multiple of the orders of the modulo groups involved. The largest possible order for group (1) is 6, for group (2) is 12, for group (3) is 24, for group (4) is 48 and group (5) is 12.

By the theorem, we know that  $G$  MUST be isomorphic to only one of the five direct sum

groups above.  $G$  has an element,  $2x + 6$ , of order 48. The following shows the calculation of the order of  $2x + 6$ :

$$\begin{aligned}(2x + 6)^2 &= 4x^2 + 1 + 3x = 4 + 3x \text{ (since } x^2 = -1 \text{ in this field)} \\ \implies (2x + 6)^4 &= (4 + 3x)^2 = 2x^2 + 2 + 3x = 3x \\ \implies (2x + 6)^{48} &= (3x)^{12} = (3^{12}) \cdot (x^{12}) = 1\end{aligned}$$

Note that no power  $k$  less than 12 exists such that  $(3x)^k = 1$  because 3 in  $\mathbb{F}_7^*$  is of order 6 and  $x$  is of order 4 ( $x^2 = -1$ ). Therefore no power  $k'$  less than 48 exists such that  $(2x + 6)^{k'} = 1$ .

Since  $2x + 6$  must map to an element in the direct sum of the same order, we know that the direct sum isomorphic to  $G$  must be (4). Thus  $G \cong \mathbb{Z}_{2^4} \oplus \mathbb{Z}_3$ .

**Find:** Express the multiplicative group of  $\mathbb{F}_7[x]/\langle x^2 - 1 \rangle$  in the above form.

**Solution:**  $x^2 - 1$  is reducible over  $\mathbb{F}_7[x]$ . Therefore, by CRT,  $\mathbb{F}_7[x]/\langle x^2 - 1 \rangle \cong \mathbb{F}_7[x]/\langle x - 1 \rangle \oplus \mathbb{F}_7[x]/\langle x + 1 \rangle$ . Note that  $\mathbb{F}_7[x]/\langle x - 1 \rangle \oplus \mathbb{F}_7[x]/\langle x + 1 \rangle$  is a ring and not a field. Some non-zero elements in it, for example  $(0,1)$ , do not have multiplicative inverses because no ordered pair  $(a,b)$  when multiplied by  $(0,1)$  gives the multiplicative identity  $(1,1)$ . Therefore a multiplicative group,  $G$ , defined for this ring would only include elements of the form  $(a,b)$  with  $a, b \in \mathbb{F}_7$  and  $a, b \neq 0$ . Note that we can rewrite  $G$  as  $\mathbb{F}_7^*[x]/\langle x - 1 \rangle \oplus \mathbb{F}_7^*[x]/\langle x + 1 \rangle$ .  $|G| = |\mathbb{F}_7^*[x]/\langle x - 1 \rangle \oplus \mathbb{F}_7^*[x]/\langle x + 1 \rangle| = 36$ . The following are the orders of elements in  $\mathbb{F}_7^*$ :

- 1 is of order 1.
- 2 is of order 3.  $2^3 \bmod 7 = 1$
- 3 is of order 6.  $3^6 \bmod 7 = 1$
- 4 is of order 3.  $4^3 \bmod 7 = 1$
- 5 is of order 6.  $5^6 \bmod 7 = 1$
- 6 is of order 2.  $6^2 \bmod 7 = 1$

Then an element in  $\mathbb{F}_7^*[x]/\langle x - 1 \rangle \oplus \mathbb{F}_7^*[x]/\langle x + 1 \rangle$  would have an order of at most 6 (since 6 is the largest possible least common multiple of any two given elements of  $\mathbb{F}_7^*$ ).

Therefore the direct sum representation of  $G$  must also have elements of order at most 6. By the theorem above we have,  $G \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$ .

**Given:** Two commutative groups  $G_1 = \mathbb{Z}_{d_1} \oplus \dots \oplus \mathbb{Z}_{d_m}$  and  $G_2 = \mathbb{Z}_{e_1} \oplus \dots \oplus \mathbb{Z}_{e_n}$  where  $d_i, e_i \in \mathbb{Z}$ .

**Find:** An efficient algorithm to determine if  $G_1 \cong G_2$ .

**Solution:** This algorithm and proof assume that  $G_1$  and  $G_2$  are of the same order. Determining if the order is the same is a trivial process. We would multiply all the  $d_i$ s together and all the  $e_i$ s together and compare the results of the two products. This would take  $O(m+n)$  operations.

This proof also assumes that the direct sums in neither  $G_1$  nor  $G_2$  contain the trivial modulo group  $\mathbb{Z}_1$ .

Per the theorem outline at the beginning of this section, we have that the given group  $G_1$

must be isomorphic to a direct sum  $G_p = \mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \dots \mathbb{Z}_{p_{k-1}^{e_{k-1}}} \oplus \mathbb{Z}_{p_k^{e_k}}$  where  $p_i^{e_i}$  is a power of a prime. However, there is no guarantee that all  $p_i^{e_i}$  are co-prime to each other. In order for  $G_1 \cong G_2$ , both groups must be isomorphic to the same prime direct sum representation,  $G_p$  mentioned above. Note that direct sum groups isomorphic to  $G_p$  do not need to be identical to the direct sum representation of  $G_p$ . They can be permutations of the modulo groups in the direct sum representation or even combine one or more co-prime modulo groups together. Two modulo groups  $\mathbb{Z}_m$  and  $\mathbb{Z}_n$  are considered co-prime if  $\gcd(m, n) = 1$ . Therefore the key to an algorithm that determines whether or not  $G_1$  is isomorphic to  $G_2$  is determining whether for each element  $\mathbb{Z}_{d_i}$  in  $G_1$  there is atleast one element  $\mathbb{Z}_{e_j}$  in  $G_2$  such that the following is true:

- (A) If  $d_i > e_j$ , then  $d_i \bmod e_j = 0$  and  $\gcd(e_j, d_i/e_j) = 1$ .
- (B) Or if  $d_i \leq e_j$ , then  $e_j \bmod d_i = 0$  and  $\gcd(d_i, e_j/d_i) = 1$ .

The above mod condition ensures that a group element,  $\mathbb{Z}_x$ , from one group is mapped to a multiple of the same group element,  $\mathbb{Z}_{kx}$ , in the other group. The gcd check ensures that  $k$  is co-prime to  $x$ . This latter check is crucial because if for a given  $d_i$  all possible  $e_j$ s that satisfied the mod condition had  $\gcd(k, x) > 1$  then it would imply that there is a prime power,  $p^y$ , that is that largest power of prime  $p$  to divide  $d_i$  which is not the largest to divide any  $e_j$ . This would mean that two or more modulo group elements of the direct sum in  $G_1$  (or  $G_2$ ) that were not co-prime were combined together in  $G_2$  (or  $G_1$ ). As a result the two direct sum groups,  $G_1$  and  $G_2$  in this case would not be isomorphic to each other.

For clarity, lets define two elements  $d_i$  and  $e_j$  as potential matches if they satisfy either of the conditions A or B mentioned above.

Based on the above logic, the algorithm to determine if  $G_1 \cong G_2$  would be as follows:

- (1) For each  $d_i$  find potential matching  $e_j$ s and mark  $d_i$  and its corresponding  $e_j$  matches. If no potential matches are found for  $d_i$  then output that  $G_1$  is not isomorphic to  $G_2$ .
- (2) Once all  $d_i$ s are matched, check each  $e_j$  to see if it is marked. If there exists some  $e_h$  that is not marked then it means  $e_h$  did not make the list of potential matchings of any of the  $d_i$ . Then output that  $G_1$  is not isomorphic to  $G_2$ .
- (3) Else output that  $G_1 \cong G_2$ .

The total time taken by this algorithm would be  $m * n * 3 * (\log d_m) * (\log e_n) + n$  where  $m * n$  is for the number pairs of elements that are compared.  $(\log d_m) * (\log e_n)$  is the time taken to do division, gcd or mod. 3 is the maximum number of mod, division or gcd operations needed in determining if two elements are potential matches. The '+n' is for the time taken by step 2. This algorithm is a polynomial time algorithm.

3. **Given:**  $\omega = e^{2\pi i/m}$  is the  $m^{\text{th}}$  root of infinity.

**Prove:**  $\bar{\omega} = \omega^{-1}$ .

**Proof:**  $\bar{\omega}$  is the conjugate of  $\omega$  and therefore equal to  $e^{-2\pi i/m}$ .

In order for  $\bar{\omega}$  to be  $\omega^{-1}$ ,  $\bar{\omega} \cdot \omega$  must equal 1.

$$\bar{\omega} \cdot \omega = e^{-2\pi i/m} \cdot e^{2\pi i/m} = e^0 = 1.$$

Therefore,  $\bar{\omega} = \omega^{-1}$ .

**Show:**  $\sum_{k=1}^m (\omega^i)^k \cdot (\bar{\omega}^j)^k$  is  $m$  if  $j=i$  and  $0$  otherwise.

**Proof:** We can simplify  $\sum_{k=1}^m (\omega^i)^k \cdot (\bar{\omega}^j)^k$  to  $\sum_{k=1}^m (\omega^i \cdot \bar{\omega}^j)^k$ . We know that  $\bar{\omega} = \omega^{-1}$ . When  $i = j$

we have  $\sum_{k=1}^m (1)^k = m$ . When  $i \neq j$ , then without loss of generality, we can assume  $i > j$ .

Then  $\sum_{k=1}^m (\omega^i \cdot \bar{\omega}^j)^k = \sum_{k=1}^m (\omega^{i-j})^k$ . Note that  $\omega^{i-j}$  is also an  $m$ th root of unity.  $\sum_{k=1}^m (\omega^{i-j})^k =$

$$\sum_{k=0}^{m-1} (\omega^{i-j})^k = \frac{(\omega^{i-j})^m - 1}{\omega^{i-j} - 1} = 0.$$

**Given:** Matrix  $M$  is defined as follows:

$$\begin{pmatrix} 1 & \omega & \omega^2 & \dots & \omega^{(m-2)} & \omega^{(m-1)} \\ 1 & \omega^2 & \omega^4 & \dots & \omega^{2(m-2)} & \omega^{2(m-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \omega^{m-1} & \omega^{(m-1)2} & \dots & \omega^{(m-1)(m-2)} & \omega^{(m-1)(m-1)} \\ 1 & 1 & 1 & \dots & 1 & 1 \end{pmatrix}$$

**Prove:**  $\bar{M}^T \cdot M = m \cdot I_{m \times m}$ .

**Proof:**  $\bar{M}$  is the following matrix:

$$\begin{pmatrix} 1 & \bar{\omega} & \bar{\omega}^2 & \dots & \bar{\omega}^{(m-2)} & \bar{\omega}^{(m-1)} \\ 1 & \bar{\omega}^2 & \bar{\omega}^4 & \dots & \bar{\omega}^{2(m-2)} & \bar{\omega}^{2(m-1)} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 1 & \bar{\omega}^{m-1} & \bar{\omega}^{(m-1)2} & \dots & \bar{\omega}^{(m-1)(m-2)} & \bar{\omega}^{(m-1)(m-1)} \\ 1 & 1 & 1 & \dots & 1 & 1 \end{pmatrix}$$

$\bar{M}^T$  would then be the following:

$$\begin{pmatrix} 1 & 1 & \dots & 1 & 1 \\ \bar{\omega} & \bar{\omega}^2 & \dots & \bar{\omega}^{(m-1)} & 1 \\ \bar{\omega}^2 & \bar{\omega}^4 & \dots & \bar{\omega}^{(m-1)2} & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \bar{\omega}^{(m-2)} & \bar{\omega}^{2(m-2)} & \dots & \bar{\omega}^{(m-1)(m-2)} & 1 \\ \bar{\omega}^{(m-1)} & \bar{\omega}^{2(m-1)} & \dots & \bar{\omega}^{(m-1)(m-1)} & 1 \end{pmatrix}$$

Given the above, the  $(i, j)$  entry of  $\overline{M}^T.M$  is defined by  $\sum_{k=1}^m (\omega^{(i-1)k}).(\overline{\omega}^{(j-1)k})$ . By the earlier proof, we have that  $\sum_{k=1}^m (\omega^i)^k.(\overline{\omega}^j)^k$  is  $m$  if  $i = j$  and  $0$  otherwise. Since in this proof,  $i$  and  $j$  were arbitrary, this proof will also hold for  $i-1$  and  $j-1$ . Therefore we have,  $\sum_{k=1}^m (\omega^{i-1})^k.(\overline{\omega}^{j-1})^k$  is  $m$  if  $i-1 = j-1$ , i.e.  $i = j$  and  $0$  otherwise. This results in the following matrix for  $\overline{M}^T.M$ :

$$\begin{pmatrix} m & & & & \\ & m & & & \\ & & \ddots & & \\ & & & m & \\ & & & & m \end{pmatrix}$$

Thus, we have  $\overline{M}^T.M = m.I_{m \times m} \Rightarrow \frac{1}{m}.\overline{M}^T = M^{-1}$ .

**Given:** Assume the following:

$$M. \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{m-2} \\ a_{m-1} \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{m-2} \\ \alpha_{m-1} \end{pmatrix}$$

**Prove:**

$$M^{-1}. \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{m-2} \\ a_{m-1} \end{pmatrix} = \frac{1}{m}. \begin{pmatrix} \omega^m.\alpha_{m-1} \\ \omega^{m-1}.\alpha_{m-2} \\ \vdots \\ \omega^2.\alpha_1 \\ \omega.\alpha_0 \end{pmatrix}$$

**Proof:** From the given equation we can conclude the following:

$$M. \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{m-2} \\ a_{m-1} \end{pmatrix} = \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{m-2} \\ \alpha_{m-1} \end{pmatrix} \Rightarrow \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{m-2} \\ a_{m-1} \end{pmatrix} = M^{-1}. \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{m-2} \\ \alpha_{m-1} \end{pmatrix}$$

Then we need to prove that

$$M^{-1}.M^{-1} \cdot \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{m-2} \\ \alpha_{m-1} \end{pmatrix} = \frac{1}{m} \cdot \begin{pmatrix} \omega^m.\alpha_{m-1} \\ \omega^{m-1}.\alpha_{m-2} \\ \vdots \\ \omega^2.\alpha_1 \\ \omega.\alpha_0 \end{pmatrix}$$

Since  $M^{-1} = \frac{1}{m}.\overline{M}^T$ , we have  $M^{-1}.M^{-1} = \frac{1}{m^2}.\overline{M}^T.\overline{M}^T$ . Then we have

$$M^{-1}.M^{-1} \cdot \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{m-2} \\ \alpha_{m-1} \end{pmatrix} = \frac{1}{m^2}.\overline{M}^T.\overline{M}^T \cdot \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{m-2} \\ \alpha_{m-1} \end{pmatrix}$$

$$\overline{M}^T.\overline{M}^T = \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ \overline{\omega} & \overline{\omega}^2 & \cdots & \overline{\omega}^{(m-1)} & 1 \\ \overline{\omega}^2 & \overline{\omega}^4 & \cdots & \overline{\omega}^{(m-1)^2} & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \overline{\omega}^{(m-2)} & \overline{\omega}^{2(m-2)} & \cdots & \overline{\omega}^{(m-1)(m-2)} & 1 \\ \overline{\omega}^{(m-1)} & \overline{\omega}^{2(m-1)} & \cdots & \overline{\omega}^{(m-1)(m-1)} & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 & \cdots & 1 & 1 \\ \overline{\omega} & \overline{\omega}^2 & \cdots & \overline{\omega}^{(m-1)} & 1 \\ \overline{\omega}^2 & \overline{\omega}^4 & \cdots & \overline{\omega}^{(m-1)^2} & 1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \overline{\omega}^{(m-2)} & \overline{\omega}^{2(m-2)} & \cdots & \overline{\omega}^{(m-1)(m-2)} & 1 \\ \overline{\omega}^{(m-1)} & \overline{\omega}^{2(m-1)} & \cdots & \overline{\omega}^{(m-1)(m-1)} & 1 \end{pmatrix}$$

The  $(i, j)$  entry in the above  $\overline{M}^T.\overline{M}^T$  matrix product is of the form  $\sum_{k=1}^m (\overline{\omega}^{(i-1)})^k . (\overline{\omega}^{(j)})^{k-1}$ .

This can be reduced to  $\overline{\omega}^{(i-1)} \sum_{k=1}^m (\overline{\omega}^{(i-1)}.\overline{\omega}^{(j)})^{k-1}$ . In cases where  $j = n - i + 1$ , the summation equals  $\overline{\omega}^{(i-1)}.m = \omega^{(m-1)(i-1)}.m$  since  $\overline{\omega} = \omega^{-1} = \omega^{(m-1)}$ . Note that  $\omega^{(m-1)(i-1)}.m$  further reduces to  $\omega^{m(i-1)}.\omega^{-1(i-1)}$ .  $\omega^{m(i-1)} = 1$  since  $\omega^m = 1$ .  $\omega^{-1(i-1)} = \omega^{-1(i-1)} * \omega^m = \omega^{m-(i-1)}$ . For all other cases of  $(i, j)$ , we have that  $\overline{\omega}^{(i-1)} \sum_{k=1}^m (\overline{\omega}^{(i-1)}.\overline{\omega}^{(j)})^{k-1}$  is reduced to

$\overline{\omega}^{(i-1)} \sum_{k=0}^{m-1} (\overline{\omega}^{(i-1+j)})^k = 0$  since  $\overline{\omega}^{(i-1+j)}$  is also an  $m^{th}$  root of unity. Therefore, we have

$$\frac{1}{m^2}.\overline{M}^T.\overline{M}^T \cdot \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{m-2} \\ \alpha_{m-1} \end{pmatrix} = \frac{1}{m^2} \cdot \begin{pmatrix} & & & & m.\omega^m \\ & & & m.\omega^{(m-1)} & \\ & & \ddots & & \\ & m.\omega^2 & & & \\ m.\omega & & & & \end{pmatrix} \begin{pmatrix} \alpha_0 \\ \alpha_1 \\ \vdots \\ \alpha_{m-2} \\ \alpha_{m-1} \end{pmatrix}$$

$$= \frac{1}{m} \cdot \begin{pmatrix} \omega^m \cdot \alpha_{m-1} \\ \omega^{(m-1)} \cdot \alpha_{m-2} \\ \vdots \\ \omega^2 \cdot \alpha_1 \\ \omega \cdot \alpha_0 \end{pmatrix}$$

Thus we have

$$M^{-1} \cdot \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{m-2} \\ a_{m-1} \end{pmatrix} = \frac{1}{m} \cdot \begin{pmatrix} \omega^m \cdot \alpha_{m-1} \\ \omega^{m-1} \cdot \alpha_{m-2} \\ \vdots \\ \omega^2 \cdot \alpha_1 \\ \omega \cdot \alpha_0 \end{pmatrix}$$

**Given:** Vector  $\vec{a} \in \mathbb{C}^m$  and we can compute  $(M \cdot \vec{a})$  in  $O(m \log m)$ .

**Prove:**  $M^{-1} \cdot \vec{a}$  can be computed in  $O(m \log m)$ .

**Proof:** Let  $(M \cdot \vec{a}) = \vec{a}$ , then per previous findings, we have that

$$M^{-1} \cdot \vec{a} = \frac{1}{m} \cdot \begin{pmatrix} \omega^m \cdot \alpha_{m-1} \\ \omega^{m-1} \cdot \alpha_{m-2} \\ \vdots \\ \omega^2 \cdot \alpha_1 \\ \omega \cdot \alpha_0 \end{pmatrix}$$

Therefore, given  $\vec{a}$  we can take  $m$  operations to compute  $\omega, \omega^2, \dots, \omega^{(m-2)}, \omega^{(m-1)}$ , then another  $m$  operations to calculate the entries  $\omega^{(m-i)} \cdot \alpha_{(m-i-1)}$  of the RHS above and finally another  $m$  operations to multiply each entry above by  $\frac{1}{m}$ . The total number of operations to calculate  $M^{-1} \cdot \vec{a}$  would then be  $O(m \log m) + 3m = O(m \log m)$ .

**Given:**  $f(x) \in \mathbb{C}[x]$  is a monic polynomial of degree  $d$  with roots  $\alpha_1, \alpha_2, \dots, \alpha_d$ .  $g(x) = f(\theta \cdot x)$ .

**Show:** Roots of  $g(x)$  are precisely  $\theta^{-1} \cdot \alpha_1, \dots, \theta^{-1} \cdot \alpha_d$ .

**Proof:** Since  $g(x) = f(\theta \cdot x)$ , the roots of  $g(x)$  would satisfy the equation  $(\theta \cdot x - \alpha_i) = 0$  where  $\alpha_i$  is some root of  $f(x)$ . Then we have  $x = \alpha_i \cdot \theta^{-1}$ . Therefore, the roots of  $g(x)$  are  $\theta^{-1} \cdot \alpha_1, \theta^{-1} \cdot \alpha_2, \dots, \theta^{-1} \cdot \alpha_d$ .

**Given:**  $f(x) \in \mathbb{C}[x]$  is a monic polynomial of degree  $d$  with roots  $\alpha_1, \alpha_2, \dots, \alpha_d$ .  $g(x) = f(\theta \cdot x)$  and its roots are precisely  $\theta^{-1} \cdot \alpha_1, \dots, \theta^{-1} \cdot \alpha_d$ .

**Deduce:** The problem of evaluating a given polynomial  $a(x) \in \mathbb{C}[x]$  at the roots of  $g(x)$  is equivalent to the problem of evaluating the polynomial  $b(x)$  where  $b(x) = a(\theta^{-1} \cdot x)$  at the roots of  $f(x)$ .

**Proof:** Let  $\alpha_i$  be an arbitrary root of  $f(x)$ . Then  $\theta^{-1} \cdot \alpha_i$  is the corresponding root of  $g(x)$ . If  $a(x)$  were evaluated at  $\theta^{-1} \cdot \alpha_i$  we would have  $a(\theta^{-1} \cdot \alpha_i)$ . If  $b(x)$  were evaluated at  $\alpha_i$  we would

have  $b(\alpha_i)$  which by definition is also  $a(\theta^{-1}.\alpha_i)$ . Since  $i$  is arbitrary, this applies to every root of  $f(x)$  and the corresponding  $g(x)$ . Thus, the problem of evaluating a given polynomial  $a(x) \in \mathbb{C}[x]$  at the roots of  $g(x)$  is equivalent to the problem of evaluating the polynomial  $b(x)$  where  $b(x) = a(\theta^{-1}.x)$  at the roots of  $f(x)$ .