Assignment 2: Algorithmic Algebra with Applications
Neeraj Kayal
February 20, 2008

NOTE: Due Date for submission is Thursday, 28th Feb.

Notation
The group $\mathbb{Z}_m$ will mean the additive group of the integers modulo $m$. Thus it is the unique cyclic group of size $m$.

Exercises

1. **Finite cyclic groups.** A cyclic group $(G, \cdot)$ is a group all of whose elements are of the form $a^i$ for some $a \in G, i \in \mathbb{Z}$. Show that any two finite cyclic groups of the same size are isomorphic.

2. **Finite Commutative Groups.** The structure theorem for finite commutative group states that every finite commutative group $G$ is isomorphic to a group of the form

$$\mathbb{Z}_{p_1^{e_1}} \oplus \mathbb{Z}_{p_2^{e_2}} \oplus \ldots \oplus \mathbb{Z}_{p_k^{e_k}}$$

• Consider the multiplicative group of the field $\mathbb{F}_7$. Express $\mathbb{F}_7^*$ in the form (1).

• Consider the multiplicative group of the field $\mathbb{F} \overset{\text{def}}{=} \mathbb{F}_7[x]/\langle x^2 + 1 \rangle$. Express $\mathbb{F}^*$ in the form (1).

• Consider the multiplicative group of the ring $\mathbb{R} \overset{\text{def}}{=} \mathbb{F}_7[x]/\langle x^2 - 1 \rangle$. Express $\mathbb{R}^*$ in the form (1).

• Devise an efficient (polynomial time) algorithm that given two sets of integers \(\{d_1, d_2, \ldots, d_m\}\) and \(\{e_1, \ldots, e_n\}\) determines whether the group

$$G_1 \overset{\text{def}}{=} \mathbb{Z}_{d_1} \oplus \ldots \oplus \mathbb{Z}_{d_m}$$

is isomorphic to the group

$$G_2 \overset{\text{def}}{=} \mathbb{Z}_{e_1} \oplus \ldots \oplus \mathbb{Z}_{e_n}.$$

3. **Fast polynomial multiplication algorithm.** Recall that in devising a fast, $O(d \cdot \log d)$ algorithm for multiplication of two polynomials, we wanted to evaluate a given polynomial
at the $m$-th roots of unity. Let $\omega = e^{2\pi i/m}$ be a primitive $m$-th root of unity and let $M$ be the matrix

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

Then:

(a) Show that $\overline{\omega} = \omega^{-1}$. That is, the conjugate of $\omega$ is also the inverse of $\omega$.

(b) Show that:

$$
\sum_{k=1}^{m} (\omega^i)^k \cdot (\overline{\omega}^j)^k = \begin{cases} m & \text{if } j = i, \\ 0 & \text{otherwise.} \end{cases}
$$

(c) Deduce that $M^T \cdot M = m \cdot I_{m \times m}$, and therefore that $\frac{1}{m} \cdot M^T$ is the inverse of $M$.

(d) Use this to show that if

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

then

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

(e) Deduce that if on input a vector $a \in \mathbb{C}^m$, we can compute $(M \cdot a)$ in time $O(m \cdot \log m)$ then we can also compute $(M^{-1} \cdot a)$ in $O(m \cdot \log m)$ time.

(f) Let $f(x) \in \mathbb{C}[x]$ be a monic polynomial of degree $d$ with roots $\alpha_1, \alpha_2, \ldots, \alpha_d$. That is,

$$
f(x) = (x - \alpha_1) \cdot (x - \alpha_2) \cdot \ldots \cdot (x - \alpha_d).
$$

Let $g(x)$ be the polynomial $f(\theta \cdot x)$. Then show that:

i. The roots of $g(x)$ are precisely $\theta^{-1} \cdot \alpha_1, \ldots, \theta^{-1} \cdot \alpha_d$.

ii. Deduce that 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 $b(x) \overset{\text{def}}{=} a(\theta^{-1} \cdot x)$ at the roots of $f(x)$.