Math 416

Worksheet 9. Roots of unity and polynomial multiplication

Euler's Formula. $e^{i\theta} = \cos\theta + i\sin\theta$ (which remember represents the point $(\cos\theta, \sin\theta)$ on the unit circle in $\mathbb{C}$.)

Definition. An *nth root of unity* is a solution (in $\mathbb{C}$) to $z^n = 1$.

Problem 1.

(a) Prove that for any integer k, the number $e^{2\pi ik/n}$ is a complex n^{th} root of unity. Where does it appear on the unit circle?
(b) Find all solutions $\theta \in \mathbb{R}$ to $e^{i\theta} = 1$.
(c) Prove that, for any $n \in \mathbb{N}$, the numbers

$$e^{2\pi ik/n},\ k = 0, 1, \ldots, n-1,$$

are the complex n^{th} roots of unity. (In particular, you must show that this is a list of n distinct numbers!) Draw a picture and indicate where these n points appear in the plane.
(d) Write $\zeta = e^{2\pi i/n}$. Prove that

$$1, \zeta, \zeta^2, \ldots, \zeta^{n-1}$$

is also a complete list of the n^{th} roots of unity.
(e) Prove that if n is even, then squaring the n^{th} roots of unity gives a list (with repetitions) of the $(n/2)^{\text{th}}$ roots of unity.
(f) Prove that if n is even, then the n^{th} roots of unity come in $\pm$ pairs: ξ is an n^{th} root of unity iff $-\xi$ is. What about when n is odd?

Polynomial multiplication Given two polynomials $A(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n$ and $B(x) = b_0 + b_1x + b_2x^2 + \cdots + b_nx^n$, we would like to compute the coefficients of the product

$$\begin{aligned} A(x)B(x) &= a_0b_0 + (a_0b_1 + a_1b_0)x + \cdots + a_nb_nx^{2n} \\ &= c_0 + c_1x + \cdots + c_{2n}x^{2n}. \end{aligned}$$

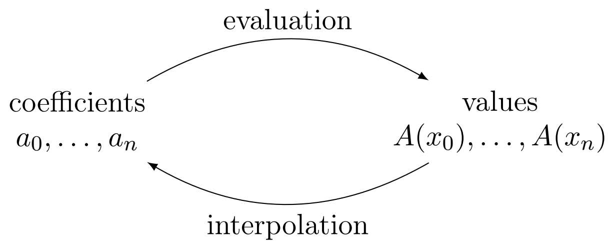
Problem 2. Find an explicit formula for the coefficient c_k of x^k in $A(x)B(x)$, for $k = 0, 1, \ldots, 2n$.

Problem 3. Briefly discuss with your groupmates a naïve algorithm to multiply two degree n polynomials in $O(n^2)$ time.

Our goal is to find a D&C solution that runs in $O(n \log n)$ time. The main idea is to convert the polynomial to **point–value form**.

Problem 4. Discuss with your groupmates the assertion, *a polynomial of degree n is determined by $n+1$ of its values.* Can you interpret this in terms of linear algebra?

So we need to translate between coefficient form and point–value form efficiently:



Problem 5. Show how evaluation at a single value x can be performed in linear time using *Horner's Rule*:

$$A(x) = a_0 + x(a_1 + x(a_2 + \cdots + x(a_{n-2} + x(a_{n-1} + a_n x)) \cdots)$$

Do a small example, say a degree-3 polynomial.

So we need a way to interpolate quickly. The trick will be to choose the interpolation points x_k cleverly. But actually we won't worry much about interpolation yet; it will turn out by some magic that if we find a nice evaluation algorithm, then interpolation will fall right out of it.

Problem 6. Explain how, if we could both interpolate polynomials in $O(n \log n)$ and evaluate at n points in $O(n \log n)$ time, then we could multiply polynomials in $O(n \log n)$ time. Draw a diagram.

A preview: Choose the n points for interpolation in $\pm$ pairs, so that the even powers of $\pm x_k$ are the same:

$$\pm x_0, \pm x_1, \dots, \pm x_{n/2-1}.$$

Then we can split $A(x)$ up as a sum $A(x) = A_E(x^2) + xA_O(x^2)$, where A_E and A_O are each polynomials of degree $\frac{n}{2} - 1$. These lower-degree polynomials have to be evaluated at $n/2$ points each:

$$(x_0)^2, (x_1)^2, \dots, (x_{n/2-1})^2.$$

But, (uh-oh!), these $n/2$ points no longer come in $\pm$ pairs! How do we continue the recursion?! **Answer:** By evaluating at the n^{th} roots of unity in $\mathbb{C}$ (!), which we will explore on the next worksheet.

In case you're fast, like last time:

We want to interpolate! That is, we still want to be able to take n values of a polynomial $A(x_0)$, $A(x_1)$, …, $A(x_{n-1})$ and return its coefficients a_0, a_1,…, a_{n-1}. This problem can be thought of in terms of matrices:

$$\begin{bmatrix} A(x_0) \\ A(x_1) \\ \vdots \\ A(x_{n-1}) \end{bmatrix} = \begin{bmatrix} 1 & x_0 & {x_0}^2 & \cdots & {x_0}^{n-1} \\ 1 & x_1 & {x_1}^2 & \cdots & {x_1}^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_{n-1} & {x_{n-1}}^2 & \cdots & {x_{n-1}}^{n-1} \end{bmatrix} \begin{bmatrix} a_0 \\ a_1 \\ \vdots \\ a_{n-1} \end{bmatrix}.$$

Problem 7 (Challenging!)**.** The large $n \times n$ matrix M is called a **Vandermonde matrix**. Prove that if the x_is are distinct, then the Vandermonde matrix is invertible.