AOA Primary 3

Riley Kopp

November 12, 2019

Application

RSA Encryption

Problem Statement

Use the RSA algorithm. If p=11 and q=17, e = 3.

Answer

$$n = 11 * 17 = 187 \tag{0.1}$$
$$\Phi = 10 * 16 = 160 \tag{0.2}$$
$$e = 3 \tag{0.3}$$
$$e_{invalid} = 32 \tag{0.4}$$
$$\tag{0.5}$$

a	b	r	x	y
3	160	1	-52	-
160	3	1	1	-52
3	1	1	0	1
1	0	1	1	0

$$d = 160 - 52 = 108 \tag{0.6}$$
$$P(x) = x^3 \% 187 \tag{0.7}$$
$$S(x) = x^{108} \% 187 \tag{0.8}$$

Value	Iteration	Math
1	0	1 * 5 % 187 = 5
5	1	5 * 5 % 187 = 25
25	2	25 * 5 % 187 = 125
125	3	Done

$$P(5) = 125$$

DFT

Problem

Compute the DFT (not FFT) of $f(x) = 2x^2 2x + 1$. You must showyour work for credit, and I highly suggest using the table method used in class to track your work as the table makes it easier for me to give partial credit. Your answers must be in a+bi format.

Answer

Table:

	0	1	2
0	1	1	1
1	1	$\frac{-1}{2} + \frac{i\sqrt{3}}{2}$	$\frac{-1}{2} - \frac{i\sqrt{3}}{2}$
2	1	$\frac{-1}{2} - \frac{i\sqrt{3}}{2}$	$\frac{-1}{2} + \frac{i\sqrt{3}}{2}$

Row Summations:

$$1 - 2 + 2 = 1 \tag{0.9}$$

$$1 + 1 - i\sqrt{3} - 1 - i\sqrt{3} = 1 - 2i\sqrt{3} \tag{0.10}$$

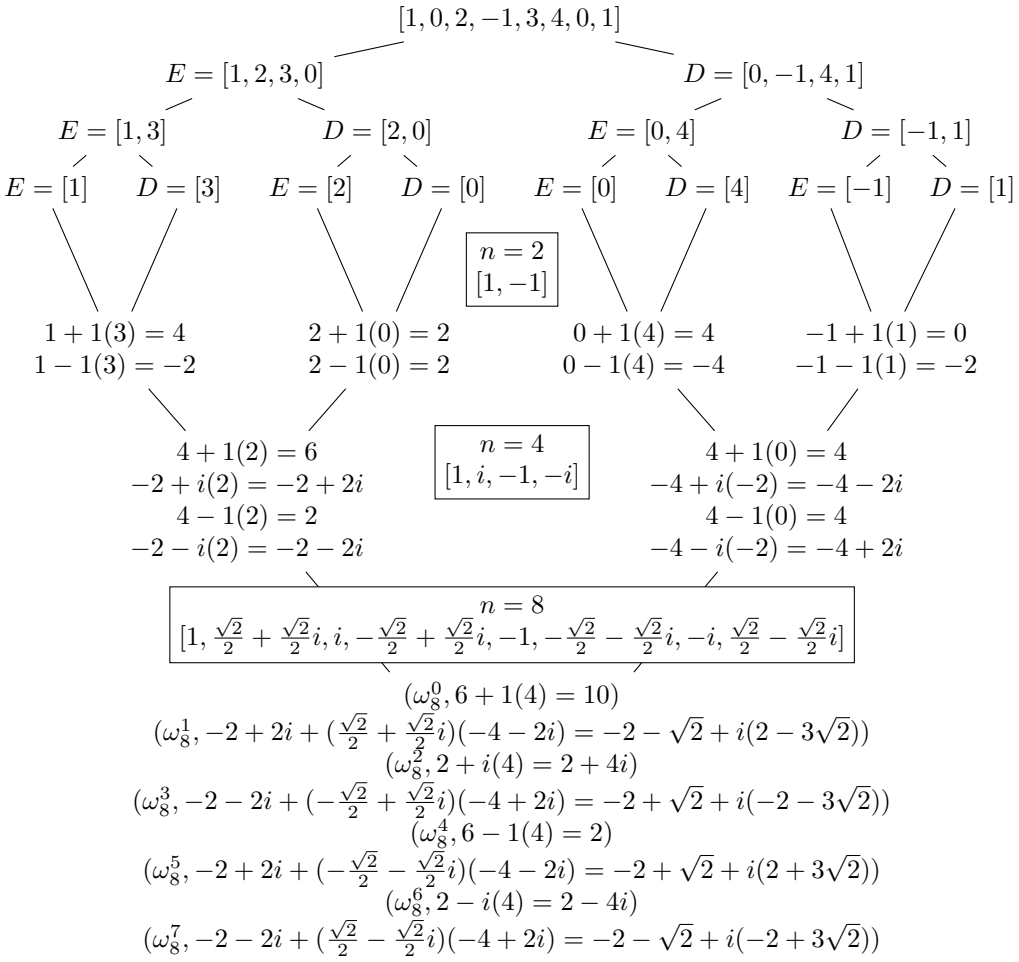
$$1 + 1 + i\sqrt{i} - 1 + i\sqrt{3} = 1 + 2i\sqrt{3} \tag{0.11}$$

FFT

Problem

Compute the FFT for $f(x) = x^7 + 4x^5 + 3x^4x^3 + 2x^2 + 1$. Note the missing powers! It must be clear that this is the FFT and not the DFT (so a tree-like structure would be best). You must show your work for credit. Your answers must be in a+bi format.

Answer



Concepts

The Despeckler

Problem

Suppose you have a black and white image of character to despeckle (0 for white, and 1 for black). To despeckle you can use the example of the convex hull, and then test if setting a black pixel to white will greatly decrease the size. Assume you will remove a pixel if the size decreases by a threshold percentage. Describe an algorithm in pseudocode that would produce the result desired.

Algorithm

Algorithm 1 Solving The Speckle problem in O(i*j)

```
function DESPECKLE(img)
    for i in Rows do
        for j in Cols do
            if !hasNeighbors(img, i, j) then img_ij = 0
            end if
        end for
    end for
    return img
end function
```

RSA Encryption

Problem

We discussed how to encrypt numbers and ACSII characters using the RSA algorithms in class. Describe a method to encrypt an image using the RSA algorithm.

Answer

Simply take the RGB values of each image and encrypt each pixel value. If we were worried about size or runtime I would compress the image first using something like a Huffman compression algorithm and then encrypt the bitstring the compression produces, since both the RSA and Huffman compression algorithms are lossless the data would still be fully recoverable on the receiving side but it would add another layer of complexity.