**Práctica2:**

**Transformada Rápida**

**De Fourier**

****

Contenido

[1. Estructura de datos utilizada. 3](#_Toc376963345)

[1.1 Estructura de datos con Números Complejos. 3](#_Toc376963346)

[Estructura de datos. 3](#_Toc376963347)

[Base y Formato de Entrada de los coeficientes. 3](#_Toc376963348)

[1.2 Estructura de datos en Zp. 3](#_Toc376963349)

[Estructura de datos. 3](#_Toc376963350)

[Base y Formato de Entrada de los coeficientes. 3](#_Toc376963351)

[2. Comparación de los algoritmos. 4](#_Toc376963352)

[2.1 Comparación de los algoritmos sobre los números complejos. 4](#_Toc376963353)

[Explicación de la eficiencia 4](#_Toc376963354)

[Tiempos aumentando el número de coeficientes de ambos polinomios. 4](#_Toc376963355)

[Tiempos aumentando el número de coeficientes de ambos polinomios, buscando favorecer a FFT. 4](#_Toc376963356)

[Tiempos aumentando el número de coeficientes de un solo polinomio. 4](#_Toc376963357)

[2.2 Comparación de los algoritmos sobre Zp. 5](#_Toc376963358)

[Explicación de la eficiencia 5](#_Toc376963359)

[Tiempos aumentando el número de coeficientes de ambos polinomios. 5](#_Toc376963360)

[Tiempos aumentando el número de coeficientes de ambos polinomios, buscando favorecer a FFT. 5](#_Toc376963361)

[Tiempos aumentando el número de coeficientes de un solo polinomio. 5](#_Toc376963362)

[3. Manual de usuario. 7](#_Toc376963363)

# 1. Estructura de datos utilizada.

## 1.1 Estructura de datos con Números Complejos.

### Estructura de datos.

La estructura de datos que usamos para operar con los polinomios sobre C es la siguiente:

* Los polinomios se representan de forma densa, es decir, los coeficientes nulos también se guardan y valdrán 0.
* Estructura de datos de un polinomio de grado ‘n’:

Ese número será guardado en un vector de ‘n+1’ posiciones, cada coeficiente del polinomio ocupará una posición del vector.

La posición 0 del vector tendrá el coeficiente menos significativo.

La posición n-1 del vector tendrá el coeficiente más significativo.

* Cada coeficiente del polinomio será un vector de dos posiciones:

La posición 0 del coeficiente, es la parte real.

La posición 1 del coeficiente, es la parte imaginaria.

### Base y Formato de Entrada de los coeficientes.

Los coeficientes se introducirán de uno en uno separados por espacios. El primer coeficiente será el menos significativo, y el último el más significativo.

Cada coeficientes se introducen como una pareja con el formato: “(x, y)” siendo x la parte real e y la parte imaginaria.

Ejemplo:

Introducimos: (3,4) (5,6) (7,0)

Polinomio introducido: (3+4i)+ (5+6i)x^1 + (7+0i)x^2

## 1.2 Estructura de datos en Zp.

### Estructura de datos.

La estructura de datos que usamos para operar con los polinomios en Zp es la siguiente:

* Los polinomios se representan de forma densa, es decir, los coeficientes nulos también se guardan y valdrán 0.
* Estructura de datos de un polinomio de grado ‘n’:

Ese número será guardado en un vector de ‘n+1’ posiciones, cada coeficiente del polinomio ocupará una posición del vector.

La posición 0 del vector tendrá el coeficiente menos significativo.

La posición n-1 del vector tendrá el coeficiente más significativo.

### Base y Formato de Entrada de los coeficientes.

Los coeficientes se introducirán de uno en uno separados por espacios. El primer coeficiente será el menos significativo, y el último el más significativo.

Ejemplo:

Introducimos: 20 30 40

Polinomio introducido: 20 + 30x + 40x^2

# 2. Comparación de los algoritmos.

## 2.1 Comparación de los algoritmos sobre los números complejos.

### Explicación de la eficiencia

La multiplicación escuela empieza teniendo los mejores tiempos cuando los números tienen

### Tiempos aumentando el número de coeficientes linealmente.

|  |  |  |
| --- | --- | --- |
| **Suma de los Grados de los polinomios** | **Escuela (ms)** | **FFT (ms)** |
| 1 | 0,0023 | 0,12 |
| 10 | 0,0087 | 12,4 |
| 20 | 0,0210 | 27 |
| 30 | 0,0312 | 31,2 |
| 40 | 0,098 | 75 |
| 50 | 0,1145 | 81 |
| 60 | 0,1223 | 88 |
| 70 | 0,134 | 268 |
| 80 | 0,1223 | 277 |
| 90 | 0,176 | 280 |
| 100 | 0,21 | 281 |
| 110 | 0,24 | 290 |
| 120 | 0,2834 | 294 |

### 

### Tiempos aumentando el número de coeficientes exponencialmente.

|  |  |  |
| --- | --- | --- |
| **Suma de los Grados de los polinomios** | **Escuela (ms)** | **FFT (ms)** |
| 1 | 0,0023 | 0,12 |
| 2 | 0,0038 | 5,31 |
| 4 | 0,0083 | 7,9 |
| 7 | 0,0192 | 10,6 |
| 15 | 0,0212 | 12,6 |
| 31 | 0,0328 | 29 |
| 63 | 0,0968 | 92,3 |
| 127 | 0,2995 | 297,8 |
| 255 | 1,0886 | 624,43 |
| 511 | 4,2829 | 895,7 |
| 1023 | 17,1991 | 1058 |
| 2047 | 68,898 | 1256,44 |
| 4095 | 293,9 | 1626 |
| 8191 | 1163 | 6599,5 |
| 16383 | 5104,8 | 26882 |
| 32767 | 22155,7 | 104079 |
| 65535 | 94564,2 | 438347,27 |

## 

## 2.2 Comparación de los algoritmos sobre Zp.

### Explicación de la eficiencia

La multiplicación escuela empieza teniendo los mejores tiempos cuando los números tienen

### Tiempos aumentando el número de coeficientes linealmente.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Suma de los Grados de los polinomios** | **Escuela z41 (ms)** | **FFT z41(ms)** | **Escuela z257 (ms)** | **FFT z257 (ms)** | **Escuela z65537 (ms)** | **FFT z65537 (ms)** |
| 1 | 0,01 | 0,1 | 0,02 | 0,8 | 0,23 | 7,5 |
| 10 | --- | --- | 0,16 | 76,1 | 9,4 | 265 |
| 20 | --- | --- | 0,24 | 189,5 | 23,4 | 936 |
| 30 | --- | --- | 0,4 | 181,4 | 51,5 | 967 |
| 40 | --- | --- | 0,57 | 541,5 | 81,1 | 3167 |
| 50 | --- | --- | 0,92 | 545,1 | 126,4 | 3190 |
| 60 | --- | --- | 1,2 | 551,3 | 145,1 | 3206 |
| 70 | --- | --- | 1,7 | 1787,7 | 251,6 | 11092 |
| 80 | --- | --- | 2,05 | 1795,2 | 329,1 | 11107,33 |
| 90 | --- | --- | 2,57 | 1894,5 | 432,1 | 11115 |
| 100 | --- | --- | 3,21 | 1909,27 | 620,9 | 11154,5 |
| 110 | --- | --- | 3,95 | 2115,78 | 784,7 | 11138,58 |
| 120 | --- | --- | 4,48 | 2323,3 | 975 | 22480 |

### 

### Tiempos aumentando el número de coeficientes exponencialmente.

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **Suma de los Grados de los polinomios** | **Escuela z41 (ms)** | **FFT z41(ms)** | **Escuela z257 (ms)** | **FFT z257 (ms)** | **Escuela z65537 (ms)** | **FFT z65537 (ms)** |
| 1 | 0,01 | 0,1 | 0,02 | 0,8 | 0,23 | 7,5 |
| 2 | 0,01 | 9,7 | 0,05 | 1,43 | 1,6 | 31 |
| 4 | 0,02 | 20,6 | 0,07 | 21,3 | 3,1 | 62,75 |
| 7 | 0,03 | 28,76 | 0,09 | 33,2 | 7,8 | 93,6 |
| 15 | --- | --- | 0,17 | 69,7 | 18,75 | 265 |
| 31 | --- | --- | 0,53 | 192 | 51,89 | 978,5 |
| 63 | --- | --- | 1,25 | 513,4 | 163,8 | 3221,66 |
| 127 | --- | --- | 5,07 | 2510,11 | 1121,6 | 23255,7 |
| 255 | --- | --- | 18,88 | 5608,3 | 4642,6 | 41847 |
| 511 | --- | --- | --- | --- | 16854,25 | 66098 |
| 1023 | --- | --- | --- | --- | 67950,67 | 256248 |
| 2047 | --- | --- | --- | --- | 278846 | 1704558 |
| 4095 | --- | --- | --- | --- | 1104229 | 8522790 |
| 8191 | --- | --- | --- | --- | --- | --- |
| 16383 | --- | --- | --- | --- | --- | --- |
| 32767 | --- | --- | --- | --- | --- | --- |
| 65535 | --- | --- | --- | --- | --- | --- |

# 3. Manual de usuario.

Haremos una breve descripción de cómo se ejecuta el programa para poder hacer las multiplicaciones con los distintos algoritmos.

1. El programa nos preguntará sobre que cuerpo queremos multiplicar polinomios:

*Desea multiplicar polinomios sobre:*

*1. Numeros Complejos*

*2. Z\_41*

*3. Z\_257*

*4. Zp*

1. El programa nos preguntará como queremos introducir los polinomios:

*Desea introducir los polinomios:*

*1. A mano*

*2. Aleatoriamente*

1. Si elegimos aleatoriamente tendremos que decir el número de coeficientes que va a tener cada polinomio, y diremos una semilla para el generador de números aleatorios:

*Cuantos coeficientes quiere que tenga el primer polinomio:*

*4*

*Cuantos coeficientes quiere que tenga el segundo polinomio:*

*3*

*Diga una semilla para generar el numero aleatorio:*

*3*

1. Nos preguntará que algoritmo de multiplicación deseamos usar:

*Diga que multiplicacion quiere usar:*

*1.Escuela*

*2.Multiplicacion mediante FFT*

*3.Las dos anteriores para comparar los tiempos*

1. Mostrará los resultados del algoritmo que elijamos, y el tiempo empleado:

*Ejemplo caso 3:*

*Resultado en Z257 de multiplicacion ESCUELA:*

*242x^5 + 141x^4 + 147x^3 + 201x^2 + 95x^1 + 243*

*Tiempo empleado en la multiplicacion escuela: 1 ms*

*Resultado en Z257 de multiplicacion mediante FFT:*

*242x^5 + 141x^4 + 147x^3 + 201x^2 + 95x^1 + 243*

*Tiempo empleado en la multiplicacion mediante FFT: 1 ms*

1. Finalmente nos preguntará si deseamos hacer más multiplicaciones o terminar:

*¿Desea hacer mas multiplicaciones?*

*1. Si*

*2. No*