FFT (coeffi $\rightleftarrows$ value)

$\xrightarrow{}$ IFFT $\xrightarrow{}$

$f = (f_0, f_1, \dots f_{n-1}) \xrightarrow{FFT} \overbrace{f(1),\ f(3^1),\ f(3^2),\ \dots}^{n}$

$\sum f_i x^i$

$g = (g_0, g_1, \dots g_{n-1}) \xrightarrow{FFT} g(1),\ g(3),\ g(3^2),\ \dots$

$(f \cdot g)(a) = f(a) \cdot g(a) \longrightarrow (\ f(1)g(1),\ f(3^1)g(3^1),\ f(3^2)g(3^2),\ \dots$

$\therefore \underset{n\log n}{2\,FFT} + (O(n) \times mult) + \underset{n\log n}{IFFT} = O(n\log n)$

우리 동형 암호는 이미 오른쪽 Table 있어서

$n^2 \rightarrow n$

$6, 3, 2, 1 \longleftrightarrow 11,\ 3+2i,\ 3,\ 3-2i$

- 왜 $n \log n$ 인가?

$S(n)$: FFT complex of polydes = n

$$S(n) = 2\,\underline{S\left(\tfrac{n}{2}\right)} + n$$

↳ b_e, b_o

$n/2$

```
for j in range(n/2)
    b[j] = b_e + w^j · b_o
    b[j+n/2] b_e - w^j b_o
return b
```

$$= 2\left(2 \cdot S\left(\tfrac{n}{4}\right) + \tfrac{n}{2}\right) + n$$

$$= 2^2 \times S\left(\tfrac{n}{4}\right) + n + n$$

$$= 2^2 \cdot S\left(\tfrac{n}{4}\right) + 2n$$

$$= 2^2 \times \left(2 \cdot S\left(\tfrac{n}{8}\right) + \tfrac{n}{4}\right) + 2n$$

$$= 2^3\, S\left(\tfrac{n}{8}\right) + 3n$$

$\vdots$

$$= 2^k S\left(n/2^k\right) + kn$$

$2^k = n$ 이 마지막 라인

$$\therefore \ = n\,S(1) + \log_2 n \times n$$

↓ degree 1 이면 값 1

$$\therefore \ S(n) = n \log n$$

FFT 코드로 이해하기

def FFT(P)

  n = len(P)

  if n == 1 :

    return P) base condition

  $w = e^{\frac{2\pi i}{n}}$ // 복소평면 위 원 n등분 $\Rightarrow w = \frac{1}{n} e^{-\frac{2\pi i}{n}}$ (IFFT 공식)

  $P_e = [P_0, P_2, \dots, P_{n-2}]$ // P[::2]
  $P_o = [P_1, P_3, \dots, P_{n-1}]$ // P[1::2])→ 홀수 짝수 나눔

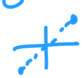
  b_e = FFT(P_e), b_o = FFT(P_o)

  b = [0] × n → b 초기화

  for j in range (n/2) : (j값 0부터 $\frac{n}{2}-1$ 까지)

    $b[j] = b_e[j] + w^j b_o[j]$
    $b[j + n/2] = b_e[j] - w^j b_o[j]$)→ 원점 대칭 이용

  $w^1 = -w^0$



  return b.

---

ex) $P(x) = 5 + 3x + 2x^2 + x^3$

• n = 1 FFT(5) → [5], FFT(2) → [2], FFT(3) → [3], FFT(1) → [1]

• n = 2 $P(x) = 5 + 2x$

$w = e^{\pi i} = -1$

$b_e = 5$ $b[0] = b_e[0] + 1 \cdot b_o[0] = 7$ (1 = w^0) ∴ [7, 3]

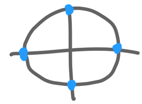
$b_o = 2$ $b[1] = b_e[0] - 1\, b_o[0] = 3$

↳ same way $3 + x \Rightarrow [4, 2]$

- $n=4$

$p(x) = 5 + 3x + 2x^2 + x^3$

$w = e^{\frac{\pi}{2}i} = i$ $\quad w^0 = 1 \quad w^2 = -1$ $\quad w^1 = i \quad w^3 = -i$



$y_e = [7, 3]$

$y_o = [4, 2]$

$b[0] = [7, 3] + 1\,[4, 2] = [11, 5]$

$b[2] = [7, 3] - 1\,[4, 2] = [3, 1]$

$b[1] = [7, 3] + i\,[4, 2] = [7+4i, 3+2i]$

$b[3] = [7, 3] - i\,[4, 2] = [7-4i, 3-2i]$

$[11, 3+2i, 3, 3-2i]$

$p(x) = 1 + x + x^2 + x^3$

$\Rightarrow$ FFT$(1) \to [1]$ $\quad$ FFT$(1+x) \to [2, 0]$

when $n=4$

$w = i$

$b[0] = [2, 0] + 1\,[2, 0] = [4, 0]$

$b[2] = [2, 0] - 1\,[2, 0] = [0, 0]$

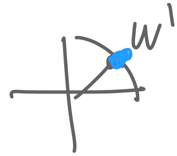
$b[1] = [2, 0] + i\,[2, 0] = [2+2i, 0]$

$b[3] = [2, 0] - i\,[2, 0] = [2-2i, 0]$

$n=8$

$P_e \Rightarrow [\,11,\ -1+9i,\ 0,\ -1-9i\,]$

$P_o \Rightarrow\ \Rightarrow [\,22,\ 11+11i,\ 0,\ 11-11i\,]$



for $j = 0 \sim 3$

$w = e^{\frac{\pi}{4}i} = (\sqrt{2}, \sqrt{2}i)$

$b[0] = 11 + (\sqrt{2}, \sqrt{2}i)\,22 = ?$

$b[4] = 11 - (\sqrt{2}, \sqrt{2}i)\,22 = ?$

??

$b[1] = (-1+9i) + i(11+11i) = -12+20i$

$b[5] = (-1+9i) - i(11+11i) = 10-2i$

$b[2] = \qquad = 0$

$b[6] = \qquad = 0$

$b[3] = (-1-9i) - 1(11-11i) = -12+2i$

$b[7] = (-1-9i) + (11-11i) = 10-20i$

$\therefore \Rightarrow [\,?,\ -12+20i,\ 0,\ -12+2i,\ ?,\ 10-2i,\ 0,\ 10-20i\,]$

$A(x) = 5 + 3x + 2x^2 + x^3 \Rightarrow [11,\ 3+2i,\ 3,\ 3-2i]$ ①

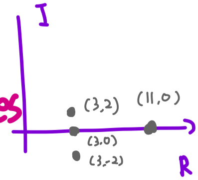
$B(x) = 1 + x + x^2 + x^3 \Rightarrow [4,\ 0,\ 0,\ 0]$ ②

$C(x) = A(x)B(x) = 5 + 8x + 10x^2 + 11x^3 + 6x^4 + 3x^5 + x^6 + 0x^7$

$\hookrightarrow [\ ?,\ -12+20i,\ 0,\ -12+2i,\ ?,\ 10-2i,\ 0,\ 10-20i\ ]$ ③

---

1. A의 식이 로 바뀌 주었는데 계수로 표현된식 → 좌표로 으로 알고 있습니다. 이는 다항식 $A(x)$ → 복소평면의 점 4개 (11, 0), (3, 2), (3, 0), (3, −2) 로 표현 한것 인가요? yes (1-1)



그렇다면 복소평면에서 저 4개의 점을 지나는 그래프는 실제 실수로 이루어진 다항식 $A(x)$의 그래프와 같은 것인가요? (1-2) yes

또한 복소평면에서 저 4개의 점을 연결하면 실수가 3 인지점에서 허수 값이 3개인데 복소 평면이여서 가능한 것인가요? (1-3) yes

→ 파란 물결로 표시 해두었 습니다.

2. 이전 page 에서 b[0], b[4] 를 업데이트 해줄때 $w' = (\sqrt{2}, \sqrt{2}i)$ 이기 때문에 계산은 $11 + (\sqrt{2}, \sqrt{2}i)\ 22 = (22\sqrt{2} + 11,\ 22\sqrt{2}i)$ 이런식으로 해줄수 있는 것인가요? (2-1) yes

3. A × B ⇒ n^2이 걸리기 때문에 A → 점으로 ①, B → 점으로 ② 해서 ① ⊙ ② = ③ 으로 $O(n)$ 해주서 ③ 을 IFFT 로 다시 C 로 만들어 줘서 $O(n \lg n)$ 이 걸려 많이 시간이 단축된다 고 이해 하였습니다. 이것이 맞나요? (3-1)

$\hookrightarrow 3n\lg n + n$

len 4, 4 다항식 곱하면
7개되니 처음 다항식을
4등분을 한 것이 아니라
A, B를 7등분해서
점 7개를 생성하고
그것을 곱해서 C의 점
7개를 생성한후 다시
원래대로 IFFT를 해줘

① ⊙ ② = ③ $O(n)$ 만에 얻는 과정은 각각 점들은 어떤 연산을 해주어야 하나요? (점4개 ⊛ 점4개 = 점 8개 이과정이 궁금 합니다!) (3-2)

Reducible Youtube FFT => Very Good

짝수 차수 => $(1,1)\ (-1,1)\ \ (-2,4)\ (2,4)$ 등등 짝을 이룸
└> 그래서 이렇게 묶음 $P(x) = P_e(x^2) + x\,P_o(x^2)$
└> even └> odd

하지만 또 근을 $(3,x)(-3,x)$ 이런식이 항상 근재 X

=> 복소 평면으로 확장 ($i^2 = -1$ 성질이 있기 때문에

$\boxed{\text{IFFT}}$ (점) => (계수) => (코드 FFT에서 $w = \frac{1}{n} e^{-\frac{2\pi i}{n}}$)
로만 바꿔주면됨

└> $P(x) = p_0 + p_1 x + p_2 x^2 + \dots + p_{n-1} x^{n-1}$

$$\begin{bmatrix} P(w^0) \\ P(w^1) \\ \vdots \\ P(w^{n-1}) \end{bmatrix} = \begin{bmatrix} 1 & 1 & & 1 \\ 1 & w & w^2 & w^{n-1} \\ 1 & w^2 & w^4 \ \dots & \\ & & & w^{(n-1)(n-1)} \end{bmatrix} \begin{bmatrix} p_0 \\ p_1 \\ p_2 \\ \vdots \\ p_{n-1} \end{bmatrix}$$

$$\begin{bmatrix} p_0 \\ p_1 \\ \vdots \\ p_{n-1} \end{bmatrix} = \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & w & w^2 & \dots & w^{n-1} \\ \vdots & w^2 & w^4 & \dots & w^{2(n-1)} \\ \vdots & & & \cdot & \vdots \\ 1 & \dots & & & w^{(n-1)(n-1)} \end{bmatrix}^{-1} \begin{bmatrix} P(w^0) \\ P(w^1) \\ P(w^2) \\ \vdots \\ P(w^{n-1}) \end{bmatrix}$$

$$= \frac{1}{n} \begin{bmatrix} 1 & 1 & 1 & \dots & 1 \\ 1 & w^{-1} & w^{-2} & \dots & w^{-(n-1)} \\ 1 & w^{-2} & w^{-4} & & \vdots \\ & & & & w^{-(n-1)(n-1)} \end{bmatrix} \begin{bmatrix} P(w^0) \\ P(w^1) \\ \vdots \\ P(w^{n-1}) \end{bmatrix}$$