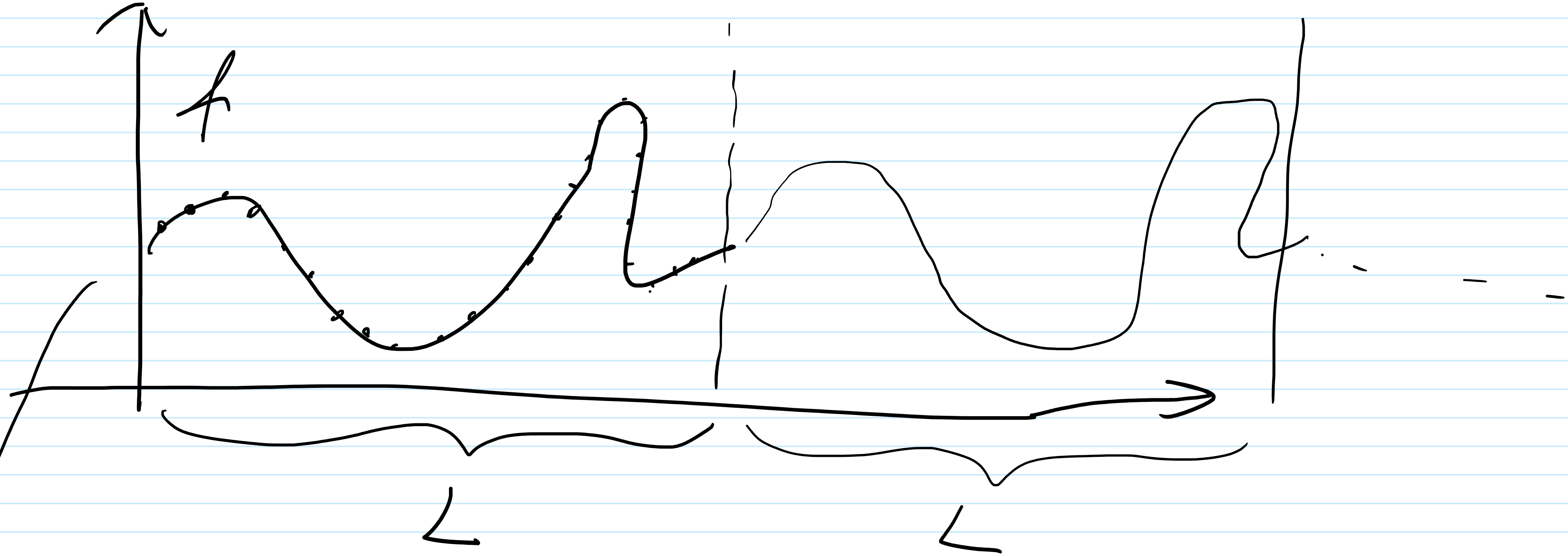
ASD, Wykład 15, 2022.06.09

FFT, szybka transformata Fouriera.

Cooley, Tukey, ±1965.

szybki algorytm służący do:

- mnożenia wielomianów
- podstawa algorytmów szybko mnożących duże liczby naturalne
- przetwarzanie sygnałów.



Rozkładamy f w szereg Fouriera

$$f(x) = a_0 + \sum_{i=1}^{\infty} \underbrace{a_i \sin\left(i x \frac{\pi}{L}\right)} + \sum_{i=1}^{\infty} b_i \underbrace{\cos\left(i x \frac{\pi}{L}\right)}$$

$$\langle a_0, a_1, a_2, \dots, b_1, b_2, \dots \rangle$$

Mnożenie wielomianów

$$W(x) = \cancel{a} \sum_{i=0}^{n} a_i x^i$$

$$U(x) = \sum_{i=0}^{n} b_i \cdot x^i$$

$W(x) \cdot U(x)$ – naiwnie koszt to $O(n^2)$

"

$$\sum_{i=0}^{2n} c_i \cdot x^i \qquad c_i = \sum_{k=0}^{i} a_k \cdot b_{i-k}$$

Gdybyśmy reprezentowali wielomiany jako ciąg wartości

$$W = (W(x_0), W(x_1), \dots, W(x_n))$$

$$U = (U(x_1), \dots\dots, U(x_n))$$

$$W \cdot U = \langle W(x_0) \cdot U(x_0), \dots, W(x_n) \cdot U(x_n) \rangle$$

$$\underbrace{\langle a_0, \dots, a_n \rangle}_{\text{współczynniki}} \xmapsto{FFT} \langle \text{ciąg wartości} \rangle \xmapsto{FFT^{-1}} \langle \text{współczynniki} \rangle$$

FFT szybka tłumacza z jednej

i FFT^{-1} reprezentacji na drugą.

szybko $\approx O(n \log_2(n))$.

Będziemy traktować FFT jako działającą na wielomianach.

WE : ciąg współczynników $a_0, \dots, a_n$

$W(x) = \sum_{i=0}^{n} a_i x^i$

WY : ciąg wartości

$(W(x_0), \dots, W(x_n))$, dla pewnego ustalonego ciągu $x_0 \dots x_n$.

Zakładamy, że $(n+1)$ jest potęgą dwójki.

Jak liczyć FFT?

$x_0 \longmapsto f(x_0) \to O(n)$

$x_n \longmapsto f(x_n) \to O(n)$

$\overline{\qquad O(n^2)}$.

nieefektywne.

Szybciej możemy to zrobić używając metody "dziel i rządź".

Weźmy $f(x) = \sum_{i=0}^{n} f_i \cdot x^i$

$$= f_{even}(x^2) + f_{odd}(x^2) \cdot x$$

$f_{even}(z) = \sum_{i=0,2,4}^{n/2} f_i \cdot z^{i/2}$, $f_{odd}(z) = \sum_{i=1,3,5}^{n/2-1} f_i \, z^{\lfloor i/2 \rfloor}$

$st(f_{even})$, $st(f_{odd}) = \left\lfloor \frac{st(f)}{2} \right\rfloor$

Niech

$T(n, x)$ = koszt obliczenia f na x.

$f(x)$.

$$T(n, x) = 2 \cdot T\left(\frac{n}{2}, x^2\right) + O(n).$$

$$T(n, x) = O(n \cdot \log_2(n)),$$

ale zmieniliśmy po drodze wartości x.

Załóżmy, że chcemy policzyć

$$f(1) = f_{even}(1) + f_{odd}(1) \cdot 1$$

$$f(-1) = f_{even}(1) + f_{odd}(1) \cdot (-1).$$

$$f(a) = f_{even}(a^2) + f_{odd}(a^2) \cdot a$$

$$f(b) = f_{even}(b^2) + f_{odd}(b^2) \cdot b$$

Jak powiązać ze sobą a^2 i b^2?

Chcemy zdefiniować zbiór wartości,
dla których liczymy wartości naszych
wielomianów

$x_0, \ldots, x_n$ $\quad$ $n+1$ - potęga dwójki
$n = 2k+1$,

Chcemy, żeby zbiór

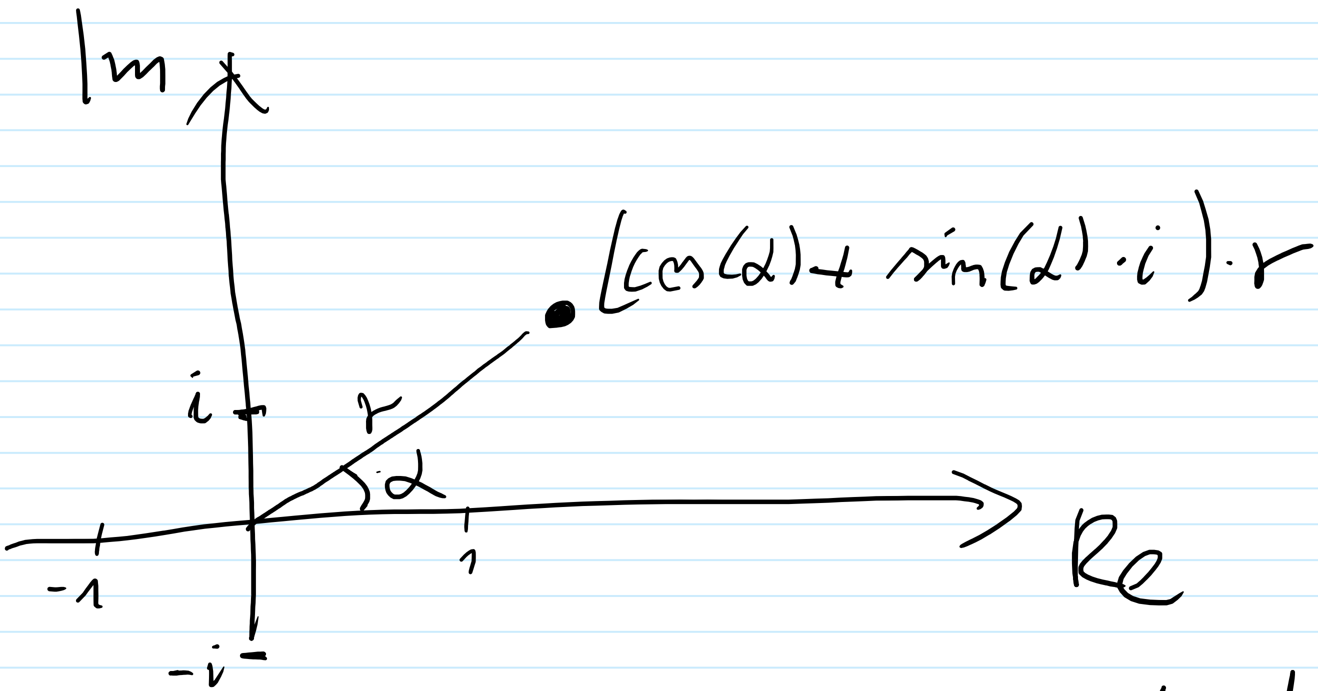
$(x_0)^2, (x_1)^2, \ldots, (x_n)^2$ miał liczność
o połowę mniejszą

i potem, rekurencyjnie,

$(x_0)^4, (x_1)^4 \ldots (x_n)^4$ – liczność 4 razy mniejszą

Skąd wziąć taki ciąg liczb?

Liczby zespolone



Euler

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

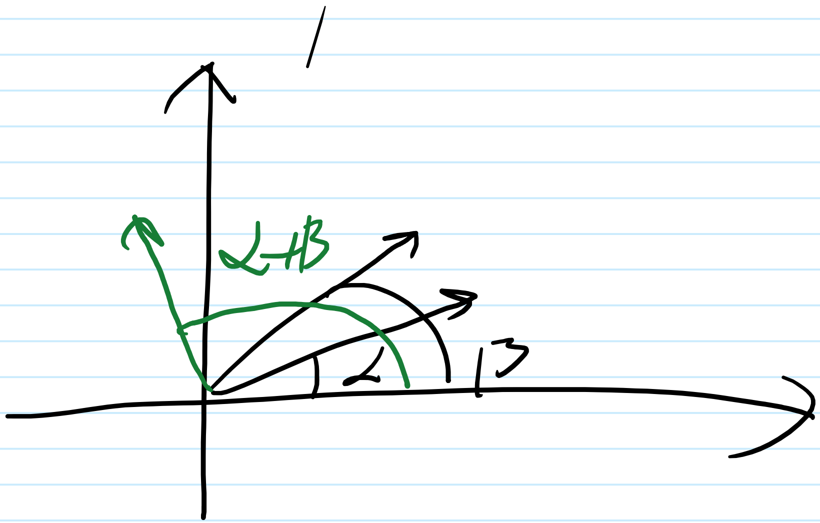
$\cos(\alpha) + \sin(\alpha)\, i = e^{i\alpha}$, α - w radianach

Mnożenie l. zesp.

$$(\cos(\alpha)+i\sin(\alpha))(\cos(\beta)+i\cdot\sin(\beta)) =$$

$$= \cos(\alpha+\beta) + i\sin(\alpha+\beta).$$

$$e^{i\alpha}\cdot e^{i\beta} = e^{i(\alpha+\beta)}$$

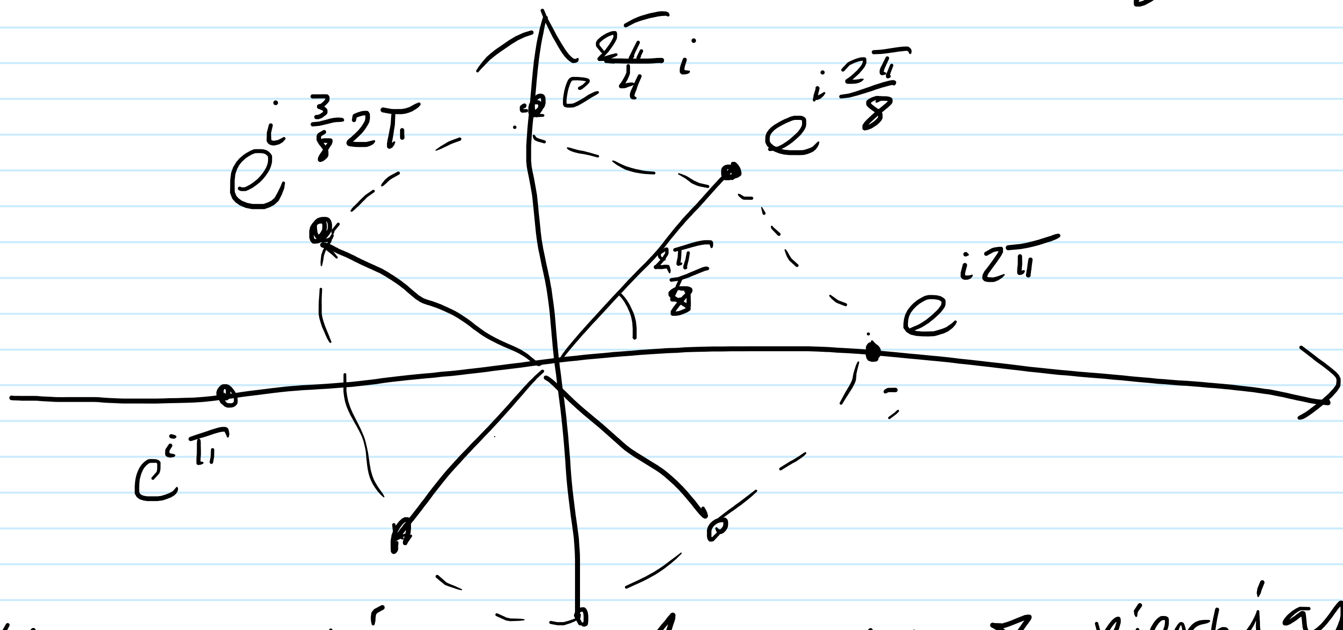


Jak wyglądają pierwiastki z 1 stopnia n.

$$e^{i\left(\frac{2\pi}{n}k\right)}, \quad k = 1, 2, \dots, n$$

$$n = 8$$

$$\left(e^{i\left(\frac{2\pi}{8}\cdot k\right)}\right)^8 = \left[e^{i(2\pi)}\right]^k = 1^k = 1$$

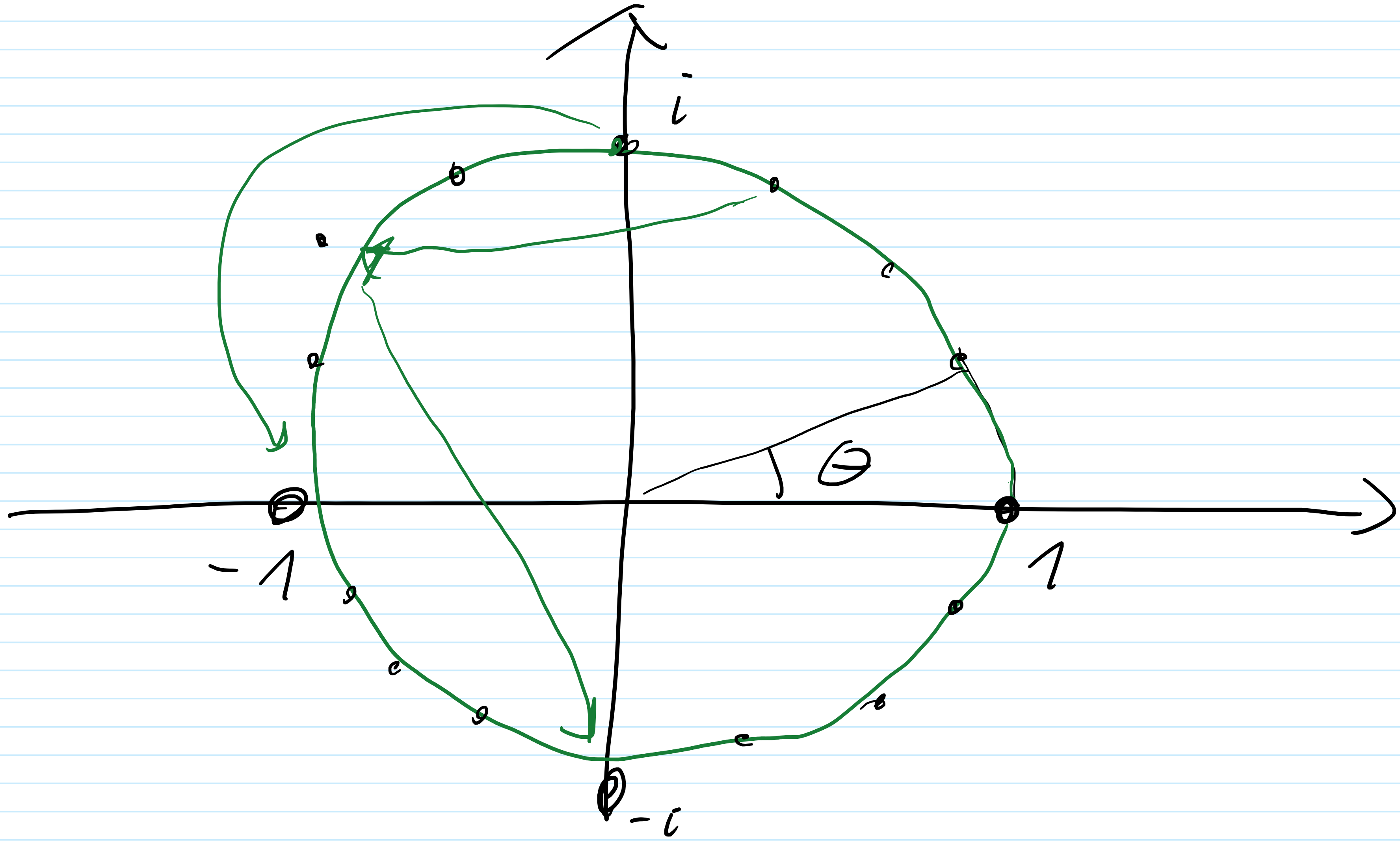


na okręgu o promieniu 1 mamy 8 pierwiastków stopnia 8 z 1.

Ale pierwiastki stopnia 4 to jest dokładnie połowa pierwiastków stopnia 8.

$$\left\{ \left(e^{i\frac{2\pi}{8}}\right)^2, \left(e^{i\frac{2\pi}{8}\cdot 2}\right)^2, \left(e^{i\frac{2\pi}{8}\cdot 3}\right)^2, \ldots, \left(e^{i\frac{2\pi}{8}\cdot 8}\right)^2 \right\} =$$

$$= \left\{ e^{i\frac{2\pi}{4}}, e^{i\frac{2\pi}{4}\cdot 2}, e^{i\frac{2\pi}{4}\cdot 3}, e^{i\frac{2\pi}{4}\cdot 4} \right\}$$


i
θ
-1
1
-i

Musimy policzyć, metodą dziel i rządź, f w wartościach $e^{i\frac{2\pi}{n}\cdot k}$, $k=1,\dots,n$.

Niech $\Theta = e^{i\frac{2\pi}{n}}$,

$\Theta^m = e^{i\frac{2\pi}{n}\cdot m}$

$$V = \begin{vmatrix} 1 & e^{i\Theta} & e^{i\Theta 2} & e^{i\Theta 3} & \dots & e^{i\Theta n} \\ \vdots & e^{i2\Theta} & e^{i2\Theta\cdot 2} & e^{i2\Theta 3} & \dots & \vdots \\ \vdots & \vdots & & & & \vdots \\ 1 & e^{in\theta} & e^{in\Theta 2} & e^{in\Theta 3} & \dots & e^{in\Theta n} \end{vmatrix}$$

$V[k,m]$ = k-ty pierwiastek stopnia n z 1 podniesiony do m-tej potęgi

$$V[k,m] = \left(e^{i k \cdot \frac{2\pi}{n}}\right)^m$$

Niech $f(x) = f_0 + f_1 \cdot x + f_2 \cdot x^2 + \ldots + f_n \cdot x^n$

$$V \cdot \begin{bmatrix} f_0 \\ \vdots \\ f_n \end{bmatrix} = \begin{bmatrix} f(e^{i\theta}) \\ f(e^{i2\theta}) \\ \vdots \\ f(e^{in\theta}) \end{bmatrix}$$

Czyli mamy tłumaczenie w jedną stronę, ze współczynników w ciąg wartości.

Koszt $O(n \log_2(n) \cdot \ldots)$

~~Do~~ Chcemy pomnożyć dwa wielomiany f, g stopnia n

$$f = \langle \overline{f} \rangle \xmapsto{FFT} \langle f(x_0) \ldots f(x_n) \rangle$$

$$g = \langle \overline{g} \rangle \xmapsto[O(n\log(n))]{} \langle g(x_0) \ldots g(x_n) \rangle$$

$$\downarrow$$

$$f \cdot g = \langle \overline{f \cdot g} \rangle \xleftarrow{FFT^{-1}} \langle f(x_0) \cdot g(x_0), \ldots, f(x_n) \cdot g(x_n) \rangle$$

czy to da się zrobić w czasie $O(n \cdot \log_2(n))$!

$$V \cdot A = Y$$

Jeśli mamy macierz odwrotną V^{-1},

$$V^{-1} \cdot V = I$$

to

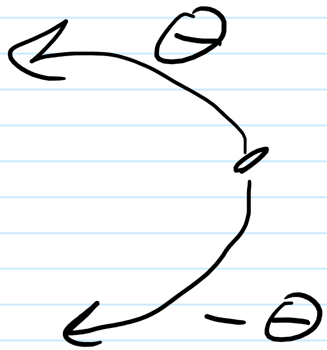
$$V^{-1} \cdot Y = A$$

czyli FFT^{-1} to wymnożenie wektora wartości przez macierz V^{-1}.

Fakt

$$V^{-1} = \frac{1}{n} \cdot \overline{V}$$ – sprzężona V razy $\frac{1}{n}$

$$V^{-1}[m,k] = \frac{1}{n} \cdot e^{i \cdot m(-\theta) \cdot k}$$

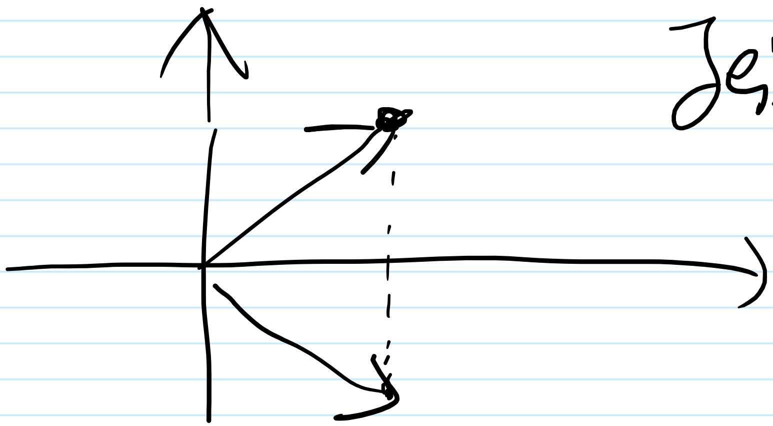


$$e^{i\alpha} = \overline{(\cos(\alpha) + i \cdot \sin(\alpha))} = \cos(\alpha) - i\sin(\alpha)$$

$$= \cos(-\alpha) + i \cdot \sin(-\alpha) = e^{i(-\alpha)}$$

Co z tego wynika?

nV^{-1} to jest permutacja wierszy macierzy V.



Jeśli $e^{i\alpha}$ - to pierwiastek stopnia > 1, to $e^{i(-\alpha)}$ - też jest takim pierwiastkiem.

Więc V^{-1} to macierz V ze spermutowanymi wierszami (i pomnożona przez n).

Więc,

aby pomnożyć wektor wartości $\begin{bmatrix} f(x_0) \\ \vdots \\ f(x_n) \end{bmatrix}$

przez V^{-1} możemy użyć tego samego algorytmu dziel i rządź.

Więc FFT i FFT^{-1} to

ta sama operacja (modulo permutacja ciągu V).