Analiza rzeczywista i zespolona

Notatki do wykładu[1]

9 Transformata Fouriera

Będziemy używali przeskalowanej miary Lebesgue'a na prostej $\mathbb{R}$:

$$m = (2\pi)^{-1/2}\lambda,$$

dzięki czemu otrzymamy prostsze wzory. Przyjmujemy

$$\|f\|_p = \left(\int_{-\infty}^{\infty} |f(x)|^p \, m(dx)\right)^{1/p} \qquad (1 \le p < \infty),$$

$$(f * g)(x) = \int_{-\infty}^{\infty} f(x-y)g(y)\, m(dy) \qquad (x \in \mathbb{R}),$$

$$\hat{f}(t) = \mathcal{F}f(x) = \int_{-\infty}^{\infty} f(x)e^{-ixt}\, m(dx) \qquad (t \in \mathbb{R}).$$

Ostatnią funkcję nazywamy *transformatą Fouriera* funkcji $f : \mathbb{R} \to \mathbb{C}$. Jest ona dobrze określona dla funkcji $f \in L^1(\mathbb{R})$. Przekształcenie $\mathcal{F}$ przyporządkowujące każdej funkcji f jej transformatę Fouriera $\hat{f}$ nazywamy *transformacją Fouriera.*

Twierdzenie **1.** *Niech $1 \le p \le \infty$. Jeśli $f \in L^1(\mathbb{R})$ oraz $g \in L^p(\mathbb{R})$, to splot $f * g$ jest prawie wszędzie dobrze określony oraz $f * g \in L^p(\mathbb{R})$.*

Dowód. Na ćwiczeniach. □

Przypomnijmy, że dla funkcji $f : \mathbb{R} \to \mathbb{R}$ określmy jej przesunięcie o $h \in \mathbb{R}$ wzorem

$$\tau_h f(x) = f(x-h), \quad (x \in \mathbb{R}).$$

Twierdzenie **2.** *(a) Transformacja Fouriera jest ograniczonym operatorem liniowym z $L^1(\mathbb{R})$ w $L^\infty(\mathbb{R})$, ponadto*

$$\|\hat{f}\|_\infty \le \|f\|_1 \qquad (f \in L^1(\mathbb{R})).$$

(b) Niech $f \in L^1(\mathbb{R})$, $h \in \mathbb{R}$ oraz $g(x) = f(x)e^{ihx}$. Wówczas

$$(\tau_h f)\hat{}(t) = \hat{f}(t)e^{-iht} \quad \text{oraz} \quad \hat{g}(t) = \tau_h(\hat{f})(t) = \hat{f}(t-h) \qquad (t \in \mathbb{R}).$$

(c) Jeśli $f, g \in L^1(\mathbb{R})$, to $(f * g)\hat{}(t) = \hat{f}(t)\hat{g}(t)$.

[1] skompilował Bartłomiej Dyda

(d) *Jeśli* $f \in L^1(\mathbb{R})$, *to* $\hat{f} \in C_0(\mathbb{R}) := \{g \in C(\mathbb{R}) : \lim_{|x|\to\infty} g(x) = 0\}$.

(e) *Jeśli* $g(x) = -ixf(x)$ *oraz* $f, g \in L^1(\mathbb{R})$, *to* $\hat{f}$ *jest funkcją różniczkowalną oraz* $(\hat{f})'(t) = \hat{g}(t)$.

Dowód. Części (a), (b), (c) udowodnimy na ćwiczeniach.

(d) Jeśli $t_n \to t$, to

$$|\hat{f}(t_n) - \hat{f}(t)| \le \int_{-\infty}^{\infty} |f(x)||e^{-it_nx} - e^{-itx}|\, m(dx).$$

Funkcja podcałkowa jest ograniczona przez $2|f(x)|$ i dla każdego $x \in \mathbb{R}$ dąży do zera, gdy $n \to \infty$. Wobec tego $\hat{f}(t_n) \to \hat{f}(t)$ na mocy twierdzenia Lebesgue'a o zbieżności ograniczonej. Zatem $\hat{f} \in C(\mathbb{R})$.

Ponieważ $e^{-\pi i} = -1$, więc

$$\hat{f}(t) = -\int_{-\infty}^{\infty} f(x)e^{-it(x+\pi/t)}\, m(dx) = -\int_{-\infty}^{\infty} f(x-\pi/t)e^{-itx}\, m(dx).$$

Wobec tego

$$2\hat{f}(t) = \int_{-\infty}^{\infty} (f(x) - f(x-\pi/t))e^{-itx}\, m(dx),$$

a zatem

$$2|\hat{f}(t)| \le \|f - \tau_{\pi/t}f\|_1.$$

Z zadania z ćwiczeń wynika, że prawa strona powyższej nierówności dąży do zera, gdy $|t| \to \infty$.

(e) Niech $t_n \ne t$ oraz $t_n \to t$, gdy $n \to \infty$. Zachodzi

$$\begin{aligned}
\frac{\hat{f}(t_n) - \hat{f}(t)}{t_n - t} &= \int_{-\infty}^{\infty} f(x)\frac{e^{-ixt_n} - e^{-ixt}}{t_n - t}\, m(dx) \\
&= \int_{-\infty}^{\infty} f(x)e^{-ixt}\frac{e^{-ix(t_n-t)} - 1}{t_n - t}\, m(dx) \\
&= \int_{-\infty}^{\infty} f(x)e^{-ixt}\phi(x, t_n - t)\, m(dx),
\end{aligned}$$

gdzie

$$\phi(x,u) = \frac{e^{-ixu} - 1}{u} = \frac{1}{u}\int_0^{xu} (e^{-iy})'\, dy.$$

Ponieważ $|\phi(x,u)| \le |x|$ dla każdego $u \ne 0$ oraz $\phi(x, t_n - t) \to -ix$, gdy $n \to \infty$, więc możemy zastosować twierdzenie Lebesgue'a o zbieżności ograniczonej i wywnioskować, że

$$\lim_{n\to\infty} \frac{\hat{f}(t_n) - \hat{f}(t)}{t_n - t} = \int_{-\infty}^{\infty} f(x)e^{-ixt}(-ix)\, m(dx) = \hat{g}(t).$$

Z definicji Heinego granicy wynika, że $(\hat{f})'(t) = \hat{g}(t)$. □

10 Odwrotna transformacja Fouriera[2]

Niech $f \in L^1(\mathbb{R})$. Naszym celem będzie wyrażenie funkcji f za pomocą $\hat{f}$.

Lemat 3. *Niech* $f(x) = e^{-\varepsilon|x|}$, *gdzie* $\varepsilon > 0$. *Wówczas*

$$\hat{f}(t) = \sqrt{\frac{2}{\pi}} \cdot \frac{\varepsilon}{\varepsilon^2 + t^2} \quad (t \in \mathbb{R}).$$

Dowód. Bezpośredni rachunek – na ćwiczeniach. $\square$ — 18 XI 2021

11 Jedność aproksymatywna

Odejdziemy na chwilę od głównego wątku, żeby udowodnić pewne pomocnicze fakty.

Niech funkcja $h \in L^1(\mathbb{R})$ będzie nieujemna oraz $\int_{\mathbb{R}} h(x)\, m(dx) = 1$. Określamy

$$h_\lambda(x) = \frac{1}{\lambda} h(\frac{x}{\lambda}) \quad (\lambda > 0).$$

Łatwo sprawdzić, że $\int_{\mathbb{R}} h_\lambda(x)\, m(dx) = 1$. Rodzinę $(h_\lambda)_{\lambda>0}$ nazywamy *jednością aproksymatywną.*

Twierdzenie 4. *Niech h i h_λ będą takie jak wyżej. Jeśli $g \in L^\infty(\mathbb{R})$ i g jest ciągła w punkcie x, to*

$$\lim_{\lambda \to 0} (g * h_\lambda)(x) = g(x).$$

Dowód. Zachodzi

$$\begin{aligned}(g * h_\lambda)(x) - g(x) &= \int_{\mathbb{R}} (g(x-y) - g(x)) h_\lambda(y)\, m(dy) \\ &= \int_{\mathbb{R}} (g(x-y) - g(x)) \lambda^{-1} h(y/\lambda)\, m(dy) \\ &= \int_{\mathbb{R}} (g(x-\lambda s) - g(x)) h(s)\, m(ds).\end{aligned}$$

Ostatnia z funkcji podcałkowych jest ograniczona przez $2\|g\|_\infty h(s)$ i dąży do zera, gdy $\lambda \to 0$ dla każdego punktu s. Teza twierdzenia wynika więc z twierdzenia Lebesgue'a o zbieżności ograniczonej. $\square$

Twierdzenie 5. *Niech h i h_λ będą takie jak wyżej. Jeśli $1 \le p < \infty$ oraz $f \in L^p(\mathbb{R})$, to*

$$\lim_{\lambda \to 0} \|f * h_\lambda - f\|_p = 0.$$

Dowód. Z twierdzenia 1 splot $f * h_\lambda$ jest prawie wszędzie dobrze określony i jest elementem $L^p(\mathbb{R})$. Zachodzi

$$(f * h_\lambda)(x) - f(x) = \int_{\mathbb{R}} (f(x-y) - f(x)) h_\lambda(y)\, m(dy),$$

więc z nierówności Jensena wynika, że

$$|(f * h_\lambda)(x) - f(x)|^p \le \int_{\mathbb{R}} |f(x-y) - f(x)|^p h_\lambda(y)\, m(dy).$$

[2] Przedwczesne, lepiej było zacząć od rozdziału 11.

Całkując powyższą nierówność względem zmiennej x i stosując twierdzenie Fubiniego otrzymujemy

$$\|f * h_\lambda - f\|_p^p \leq \int_{\mathbb{R}} \|\tau_y f - f\|_p^p h_\lambda(y)\, m(dy).$$

Jeśli $g(y) = \|\tau_{-y} f - f\|_p^p$, to g jest funkcją ograniczoną i ciągłą na mocy zadania z ćwiczeń, a prawa strona powyższej nierówności przybiera postać

$$\int_{\mathbb{R}} \|\tau_y f - f\|_p^p h_\lambda(y)\, m(dy) = \int_{\mathbb{R}} g(-y) h_\lambda(y)\, m(dy) = g * h_\lambda(0).$$

Ale z twierdzenia 4 $g * h_\lambda(0) \to g(0) = 0$, gdy $\lambda \to 0$, co kończy dowód. $\square$

Uwaga **6.** *Powyższe twierdzenie wyjaśnia nazwę* jedności aproksymatywnej*: gdyby zachodziło $\|f * h_\lambda - f\|_p = 0$, to moglibyśmy powiedzieć, że h_λ jest jednością (elementem neutralnym) dla działania splotu. Jednak równość ta zachodzi tylko w granicy przy $\lambda \to 0$.*

Twierdzenie **7.** *Niech h i h_λ będą takie jak wyżej, ale dodatkowo załóżmy, że $h \in AC[-N, N]$ dla dowolnego $N \in \mathbb{N}$, $h(x) = h(-x)$ oraz że h jest malejąca na $[0, \infty)$. Wówczas jeśli $1 \leq p \leq \infty$ oraz $f \in L^p(\mathbb{R})$, to*

$$\lim_{\lambda \to 0} f * h_\lambda(x) = \tilde{f}(x)$$

dla każdego punktu Lebesgue'a x funkcji f.

Dowód. Wybierzmy dowolny $\varepsilon > 0$ oraz punkt Lebesgue'a x funkcji f. Istnieje więc $\eta > 0$ taka, że

$$\frac{1}{2r} \int_{|y|<r} |f(x-y) - \tilde{f}(x)|\, m(dy) < \varepsilon \qquad (0 < r \leq \eta).$$

Zachodzi

$$\begin{aligned} |(f * h_\lambda)(x) - \tilde{f}(x)| &= \left| \int_{\mathbb{R}} (f(x-y) - \tilde{f}(x)) h_\lambda(y)\, m(dy) \right| \\ &\leq \left| \int_{|y|<\eta} (f(x-y) - \tilde{f}(x)) h_\lambda(y)\, m(dy) \right| \\ &\quad + \left| \int_{|y|\geq\eta} (f(x-y) - \tilde{f}(x)) h_\lambda(y)\, m(dy) \right| \\ &=: I_1 + I_2. \end{aligned}$$

Dla $|y| < \eta$ zachodzi

$$h_\lambda(y) = h_\lambda(|y|) = \int_{|y|}^{\eta} (-h'_\lambda(t))\, dt + h_\lambda(\eta) =: \int_{[0,\eta]} \mathbf{1}_{(|y|,\infty)}(t) \nu(dt), \qquad (1)$$

gdzie miara $\nu(A) = \int_A \mathbf{1}_{[0,\eta]}(t)(-h'_\lambda(t))\, dt + h_\lambda(\eta)\delta_{\{\eta\}}(A)$ jest sumą części absolutnie ciągłej względem miary Lebesgue'a (z gęstością $\mathbf{1}_{[0,\eta]} \cdot (-h'_\lambda)$) oraz delty Diraca w punkcie η pomnożonej przez liczbę $h_\lambda(\eta)$. Zauważmy, że miara ν zależy od λ i η, czego nie uwzględniamy notacji.

Zatem

$$\begin{aligned}
I_1 &\le \int_{|y|<\eta} |f(x-y) - \tilde{f}(x)| \int_{[0,\eta]} \mathbf{1}_{(|y|,\infty)}(t)\nu(dt)\, m(dy) \\
&= \int_{[0,\eta]} \int_{|y|<\eta} |f(x-y) - \tilde{f}(x)| \mathbf{1}_{(|y|,\infty)}(t)\, m(dy)\nu(dt) \\
&= \int_{[0,\eta]} 2t \cdot \frac{1}{2t} \int_{|y|<t} |f(x-y) - \tilde{f}(x)|\, m(dy)\nu(dt) \le \int_{[0,\eta]} 2t\varepsilon\, \nu(dt).
\end{aligned}$$

Dalej,

$$\begin{aligned}
\int_{[0,\eta]} t\varepsilon\, \nu(dt) &= \eta\varepsilon h_\lambda(\eta) + \varepsilon \int_0^\eta t(-h_\lambda'(t))\, dt \\
&= \eta\varepsilon h_\lambda(\eta) + \varepsilon \left([t(-h_\lambda(t))]_0^\eta + \int_0^\eta h_\lambda(t)\, dt \right) \\
&= \varepsilon \int_0^\eta h_\lambda(t)\, dt \le \varepsilon\sqrt{2\pi} \int_0^\infty h_\lambda(t)\, m(dt) = \frac{\sqrt{2\pi}}{2}\varepsilon.
\end{aligned}$$

Wobec tego $I_1 \le \sqrt{2\pi}\varepsilon$.

Teraz przejdziemy do oszacowania I_2. Niech q będzie wykładnikiem sprzężonym do p, tj. $1/p + 1/q = 1$. Niech $A = \{y : |y| \ge \eta\}$. Zachodzi

$$\begin{aligned}
I_2 &\le \int \mathbf{1}_A(y)|f(x-y) - \tilde{f}(x)|h_\lambda(y)\, m(dy) \\
&\le \|f\|_p \cdot \|\mathbf{1}_A h_\lambda\|_q + |\tilde{f}(x)| \cdot \|\mathbf{1}_A h_\lambda\|_1.
\end{aligned}$$

Ale

$$\|\mathbf{1}_A h_\lambda\|_1 = \int_{|y|\ge\eta} \frac{1}{\lambda} h\Big(\frac{y}{\lambda}\Big)\, m(dy) = \int_{|y|\ge\eta/\lambda} h(y)\, m(dy) \to 0,$$

przy $\lambda \to 0$ (wynika to z ciągłości miary skończonej $h(y)\, m(dy)$ w dół lub z twierdzenia Lebesgue'a o zbieżności ograniczonej). Ponadto

$$\begin{aligned}
\|\mathbf{1}_A h_\lambda\|_\infty &= \sup_{|y|\ge\eta} \left| \frac{1}{\lambda} h\Big(\frac{y}{\lambda}\Big) \right| = \frac{1}{\lambda} h\Big(\frac{\eta}{\lambda}\Big) = \frac{2}{\eta} \cdot \frac{\eta}{2\lambda} h\Big(\frac{\eta}{\lambda}\Big) \\
&\le \frac{2}{\eta} \int_{\frac{\eta}{2\lambda}}^{\frac{\eta}{\lambda}} h(y)\, dy \le \frac{2}{\eta} \int_{\frac{\eta}{2\lambda}}^{\infty} h(y)\, dy \to 0,
\end{aligned}$$

przy $\lambda \to 0$. W przypadku $q \in \{1, \infty\}$ wykazaliśmy już więc, że $I_2 \to 0$, gdy $\lambda \to 0$. Jeśli zaś $q \in (1, \infty)$, to $q = 1 + q/p$, więc z nierówności Höldera,

$$\begin{aligned}
\|\mathbf{1}_A h_\lambda\|_q &= \left(\int_A h_\lambda h_\lambda^{q/p} \right)^{1/q} \le \|\mathbf{1}_A h_\lambda\|_1^{1/q} \cdot \|\mathbf{1}_A h_\lambda^{q/p}\|_\infty^{1/q} \\
&= \|\mathbf{1}_A h_\lambda\|_1^{1/q} \cdot \|\mathbf{1}_A h_\lambda\|_\infty^{1/p} \to 0,
\end{aligned}$$

przy $\lambda \to 0$, bo jak wcześniej pokazaliśmy, każdy z powyższych czynników zbiega do zera.

Stąd dla dostatecznie małych liczb λ zachodzi $I_2 < \varepsilon$, a więc $I_1 + I_2 < (\sqrt{2\pi} + 1)\varepsilon$. To kończy dowód. □

Uwaga 8. *Równość (1) pozwala napisać*

$$h_\lambda(y) = \int_{[0,\eta]} \mathbf{1}_{(|y|,\infty)}(t)\nu(dt) = \int_{[0,\eta]} \mathbf{1}_{(-t,t)}(y)\nu(dt),$$

a więc pozwala wyrazić funkcję h_λ za pomocą „ciągłej sumy” (całki) funkcji postaci $\mathbf{1}_{(-t,t)}(y)$. To pozwoliło nam zamienić całkę z funkcji

$$y \mapsto (f(x-y) - \tilde{f}(x))h_\lambda(y)$$

na pewne wyrażenie zawierające całki z funkcji

$$y \mapsto (f(x-y) - \tilde{f}(x))\mathbf{1}_{(-t,t)}(y),$$

a takie właśnie całki występują w definicji punktu Lebesgue'a.

Równość (1) można otrzymać również bez założenia absolutnej ciągłości funkcji h, istotne za to były warunki $h(x) = h(-x)$ oraz fakt, że h maleje na $[0,\infty)$. W konsekwencji założenie $h \in AC[-N,N]$ można usunąć z twierdzenia 7. — 25 XI 2021

12 Odwrotna transformacja Fouriera – ciąg dalszy

Niech

$$h(x) = \sqrt{\frac{2}{\pi}} \cdot \frac{1}{1+x^2}.$$

Wówczas $h \geq 0$, $\int_\mathbb{R} h(x)\, m(dx) = 1$ oraz

$$h_\lambda(x) = \sqrt{\frac{2}{\pi}} \cdot \frac{\lambda}{\lambda^2 + x^2} = \int_\mathbb{R} e^{-\lambda|t|} e^{itx}\, m(dt),$$

na mocy lematu 3.

Twierdzenie 9. *Jeśli $f \in L^1(\mathbb{R})$, to*

$$(f * h_\lambda)(x) = \int_\mathbb{R} e^{-\lambda|t|} \hat{f}(t) e^{ixt}\, m(dt)$$

dla każdego $x \in \mathbb{R}$.

Dowód. Dowód polega na zastosowaniu twierdzenia Fubiniego

$$\begin{aligned}
(f * h_\lambda)(x) &= \int_\mathbb{R} f(x-y) h_\lambda(y)\, m(dy) \\
&= \int_\mathbb{R} f(x-y) \int_\mathbb{R} e^{-\lambda|t|} e^{ity}\, m(dt)\, m(dy) \\
&= \int_\mathbb{R} e^{-\lambda|t|} \int_\mathbb{R} f(x-y) e^{ity}\, m(dy)\, m(dt) \\
&= \int_\mathbb{R} e^{-\lambda|t|} \int_\mathbb{R} f(y) e^{it(x-y)}\, m(dy)\, m(dt) \\
&= \int_\mathbb{R} e^{-\lambda|t|} \hat{f}(t) e^{itx}\, m(dy)\, m(dt).
\end{aligned}$$

□

Lemat **10.** *Jeśli $f \in L^1_{loc}(\mathbb{R})$ jest ciągła w punkcie x, to punkt ten jest jej punktem Lebesgue'a oraz $f(x) = \tilde{f}(x)$.*

Dowód. Niech $\varepsilon > 0$. Dobierzmy $\delta > 0$ tak, aby $|f(y) - f(x)| < \varepsilon$ dla $|x - y| < \delta$. Wówczas dla $0 < r < \delta$ zachodzi

$$\frac{1}{2r}\int_{x-r}^{x+r} |f(y) - f(x)|\, dy \leq \frac{1}{2r}\int_{x-r}^{x+r} \varepsilon\, dy = \varepsilon,$$

a zatem

$$\lim_{r\to 0} \frac{1}{2r}\int_{x-r}^{x+r} |f(y) - f(x)|\, dy = 0.$$

Z powyższego wynika również, że

$$\lim_{r\to 0} \frac{1}{2r}\int_{x-r}^{x+r} f(y)\, dy = f(x),$$

a to oznacza, że $f(x) = \tilde{f}(x)$ oraz że x jest punktem Lebesgue'a funkcji f. $\square$

Twierdzenie **11** (o transformacji odwrotnej)**.** *Jeżeli $f \in L^1(\mathbb{R})$, to dla każdego punktu Lebesgue'a x funkcji f zachodzi*

$$\tilde{f}(x) = \lim_{\lambda\to 0} \int_{\mathbb{R}} e^{-\lambda|t|} \hat{f}(t) e^{ixt}\, m(dt).$$

Jeżeli dodatkowo $\hat{f} \in L^1(\mathbb{R})$, to

$$\tilde{f}(x) = \int_{\mathbb{R}} \hat{f}(t) e^{ixt}\, m(dt),$$

dla każdego punktu $x \in \mathbb{R}$, ponadto $\tilde{f} \in C_0(\mathbb{R})$.

Dowód. Na mocy poprzedniego twierdzenia zachodzi

$$(f * h_\lambda)(x) = \int_{\mathbb{R}} e^{-\lambda|t|} \hat{f}(t) e^{ixt}\, m(dt).$$

Przechodząc do granicy $\lambda \to 0$ i stosując twierdzenie 7 widzimy, że lewa strona zbiega do $\tilde{f}(x)$ dla każdego punktu Lebesgue'a x funkcji f. To daje pierwszą część twierdzenia. Druga część wynika z pierwszej i z tego, że jeśli $\hat{f} \in L^1(\mathbb{R})$, to z twierdzenia Lebesgue'a o zbieżności ograniczonej,

$$\lim_{\lambda\to 0} \int_{\mathbb{R}} e^{-\lambda|t|} \hat{f}(t) e^{ixt}\, m(dt) = \int_{\mathbb{R}} \hat{f}(t) e^{ixt}\, m(dt).$$

Ostatnia część wynika stąd, że

$$\int_{\mathbb{R}} \hat{f}(t) e^{ixt}\, m(dt) = \int_{\mathbb{R}} \hat{f}(-t) e^{-ixt}\, m(dt) = \hat{g}(x),$$

gdzie $g(t) = \hat{f}(-t)$. Ponieważ $g \in L^1(\mathbb{R})$, więc z własności transformacji Fouriera $\hat{g} \in C_0(\mathbb{R})$. Skoro $\hat{g}$ jest ciągła oraz $\tilde{f} = \hat{g}$ p.w., to każdy punkt $x \in \mathbb{R}$ jest punktem Lebesgue'a funkcji f, a więc $\tilde{f} = \hat{g}$ *wszędzie.* $\square$

Twierdzenie **12** (o jednoznaczności)**.** *Jeżeli $f \in L^1(\mathbb{R})$ i $\hat{f}(t) = 0$ dla każdego $t \in \mathbb{R}$, to $f = 0$ p.w.*

Dowód. Wynika natychmiast z poprzedniego twierdzenia. $\square$

WNIOSEK **13.** *Niech $f \in L^1(\mathbb{R})$ oraz $\hat{f} \geq 0$. Wówczas jeśli f jest ciągła w zerze, to $\hat{f} \in L^1(\mathbb{R})$ oraz*

$$f(0) = \int_{\mathbb{R}} \hat{f}(t)\, m(dt),$$

Dowód. Jeśli f jest ciągła w zerze, to zero jest punktem Lebesgue'a funkcji f oraz $\tilde{f}(0) = f(0)$, wobec czego z twierdzenia 11

$$f(0) = \lim_{\lambda \to 0} \int_{\mathbb{R}} e^{-\lambda|t|} \hat{f}(t)\, m(dt). \tag{2}$$

Stąd i z lematu Fatou

$$\begin{aligned} \int_{\mathbb{R}} \hat{f}(t)\, m(dt) &= \int_{\mathbb{R}} \lim_{\lambda \to 0} e^{-\lambda|t|} \hat{f}(t)\, m(dt) \\ &\leq \liminf_{\lambda \to 0} \int_{\mathbb{R}} e^{-\lambda|t|} \hat{f}(t)\, m(dt) = f(0) < \infty. \end{aligned}$$

Zatem $\hat{f} \in L^1(\mathbb{R})$, druga część wniosku wynika z (2). $\square$

13 Transformacja Fouriera na $L^2(\mathbb{R})$

TWIERDZENIE **14.** *Jeśli $f \in L^1(\mathbb{R}) \cap L^2(\mathbb{R})$, to $\hat{f} \in L^2(\mathbb{R})$ oraz $\|f\|_2 = \|\hat{f}\|_2$.*

Dowód. Niech $g(x) = \overline{f(-x)}$. Oczywiście $g \in L^1(\mathbb{R})$, a ponieważ również $f \in L^1(\mathbb{R})$, więc z twierdzenia 1 wynika, że $\varphi = f * g \in L^1(\mathbb{R})$. Z twierdzenia 2 dostajemy $\hat{\varphi} = \hat{f}\hat{g}$. Ale

$$\begin{aligned} \hat{g}(t) &= \int_{\mathbb{R}} \overline{f(-x)} e^{-ixt}\, m(dx) = \int_{\mathbb{R}} \overline{f(x)} e^{ixt}\, m(dx) \\ &= \overline{\int_{\mathbb{R}} f(x) e^{-ixt}\, m(dx)} = \overline{\hat{f}(t)}, \end{aligned}$$

zatem $\hat{h} = \hat{f} \cdot \overline{\hat{f}} = |\hat{f}|^2 \geq 0$. Z zadania z ćwiczeń, ponieważ $f, g \in L^2(\mathbb{R})$, więc splot $\varphi = f * g$ jest funkcją jednostajnie ciągłą. Możemy więc skorzystać z wniosku 13 dla funkcji φ; otrzymujemy, że $\hat{\varphi} \in L^1(\mathbb{R})$ oraz

$$\varphi(0) = \int_{\mathbb{R}} \hat{\varphi}(t)\, m(dt) = \int_{\mathbb{R}} |\hat{f}(t)|^2\, m(dt) = \|\hat{f}\|_2^2,$$

w szczególności $\hat{f} \in L^2(\mathbb{R})$. Z drugiej strony,

$$\varphi(0) = \int_{\mathbb{R}} f(x) g(0 - x)\, m(dx) = \int_{\mathbb{R}} f(x) \overline{f(x)}\, m(dx) = \|f\|_2^2. \qquad \square$$

TWIERDZENIE **15.** *Niech $f \in L^2(\mathbb{R})$. Wówczas*

$$\lim_{R \to \infty} \|f \mathbf{1}_{[-R,R]} - f\|_2 = 0$$

oraz istnieje funkcja $g \in L^2(\mathbb{R})$ taka, że

$$\lim_{R \to \infty} \|\mathcal{F}(f \mathbf{1}_{[-R,R]}) - g\|_2 = 0.$$

Jeśli dodatkowo $f \in L^1(\mathbb{R})$, to $g = \hat{f}$.

Dowód. Pierwsza część jest treścią zadania z ćwiczeń. Z pierwszej części wynika, że ciąg $(f\mathbf{1}_{[-R,R]})_R$ jest ciągiem Cauchy'ego w $L^2(\mathbb{R})$, a ponieważ $f\mathbf{1}_{[-R,R]} \in L^1(\mathbb{R}) \cap L^2(\mathbb{R})$, więc z twierdzenia 14 otrzymujemy, że również ciąg $(\mathcal{F}(f\mathbf{1}_{[-R,R]}))_R$ jest ciągiem Cauchy'ego w $L^2(\mathbb{R})$. Jest więc on zbieżny do pewnej funkcji $g \in L^2(\mathbb{R})$.

Jeśli dodatkowo $f \in L^1(\mathbb{R})$, to ciąg $(f\mathbf{1}_{[-R,R]})_R$ jest zbieżny w $L^1(\mathbb{R})$ do funkcji f, zatem z ograniczoności transformacji Fouriera $\mathcal{F} : L^1(\mathbb{R}) \to L^\infty(\mathbb{R})$ wynika, że ciąg $(\mathcal{F}(f\mathbf{1}_{[-R,R]}))_R$ jest zbieżny w $L^\infty(\mathbb{R})$ do funkcji $\hat{f}$. Stąd z zadania z ćwiczeń $\hat{f} = g$. □

Definicja 16. *Dla funkcji $f \in L^2(\mathbb{R})$ określamy $\hat{f}$ jako granicę w $L^2(\mathbb{R})$ funkcji $\mathcal{F}(f\mathbf{1}_{[-R,R]})$, przy $R \to \infty$,*

$$\lim_{R\to\infty} \|\mathcal{F}(f\mathbf{1}_{[-R,R]}) - \hat{f}\|_2 = 0.$$

Używamy też oznaczenia $\hat{f} = \mathcal{F}(f)$.

Twierdzenie 15 orzeka, że definicja ta jest zgodna z wcześniejszą definicją transformacji Fouriera na $L^1(\mathbb{R})$.

Twierdzenie **17.** *Dla $f \in L^2(\mathbb{R})$ niech*

$$\Psi(f)(x) = \mathcal{F}(f)(-x).$$

Wówczas Ψ oraz $\mathcal{F}$ są izometriami $L^2(\mathbb{R})$, ponadto $\Psi\mathcal{F} = \mathcal{F}\Psi = \mathrm{Id}$, w szczególności $\mathcal{F} : L^2(\mathbb{R}) \to L^2(\mathbb{R})$ jest surjekcją.

Dowód. Dla $f \in L^2(\mathbb{R})$ zachodzi

$$\mathcal{F}(f) = L^2\text{-}\lim_{R\to\infty} \mathcal{F}(f\mathbf{1}_{[-R,R]}),$$

skąd z ciągłości normy (zadanie z ćwiczeń)

$$\|\mathcal{F}(f)\|_2 = \lim_{R\to\infty} \|\mathcal{F}(f\mathbf{1}_{[-R,R]})\|_2 = \lim_{R\to\infty} \|f\mathbf{1}_{[-R,R]}\|_2 = \|f\|_2,$$

po drodze skorzystaliśmy m.in. z twierdzenia 14. Zatem $\mathcal{F}$ jest izometrią $L^2(\mathbb{R})$, w konsekwencji Ψ również. — 2 XII 2021

Niech $f \in L^1(\mathbb{R}) \cap L^2(\mathbb{R})$ oraz $\hat{f} \in L^1(\mathbb{R}) \cap L^2(\mathbb{R})$. Wówczas z twierdzenia 11 o transformacji odwrotnej

$$\Psi\mathcal{F}(f) = f.$$

Kładąc powyżej $f(-\cdot)$ w miejsce f otrzymamy

$$\Psi\Psi(f) = f(-\cdot),$$

skąd

$$\mathcal{F}\Psi(f)(x) = \Psi\Psi(f)(-x) = f(x).$$

Podsumowując, otrzymaliśmy, że

$$\Psi\mathcal{F}(f) = \mathcal{F}\Psi(f) = f, \qquad (f, \hat{f} \in L^1(\mathbb{R}) \cap L^2(\mathbb{R})). \tag{3}$$

Załóżmy teraz, że $f \in L^1(\mathbb{R}) \cap L^2(\mathbb{R})$. Wówczas $f * h_\lambda \in L^1(\mathbb{R}) \cap L^2(\mathbb{R})$. Ponadto $\mathcal{F}(f * h_\lambda) = \mathcal{F}(f)\mathcal{F}(h_\lambda)$, przy czym $\mathcal{F}(f) \in L^\infty(\mathbb{R})$ oraz $\mathcal{F}(h_\lambda)(t) =$

$e^{-\lambda|t|}$, więc $F(h_\lambda) \in L^1(\mathbb{R}) \cap L^2(\mathbb{R})$. Stąd również $\mathcal{F}(f * h_\lambda) \in L^1(\mathbb{R}) \cap L^2(\mathbb{R})$. Wobec tego możemy skorzystać z równości (3) dla funkcji $f * h_\lambda$, otrzymujemy

$$\Psi\mathcal{F}(f * h_\lambda) = \mathcal{F}\Psi(f * h_\lambda) = f * h_\lambda.$$

Przechodząc z $\lambda \to 0$ i korzystając z faktu, że $f * h_\lambda \to f$ w $L^2(\mathbb{R})$, oraz że $\mathcal{F}$ i Ψ są izometriami $L^2(\mathbb{R})$,

$$\Psi\mathcal{F}(f) = \mathcal{F}\Psi(f) = f. \tag{4}$$

Przypomnijmy, że powyższą równość otrzymaliśmy dla $f \in L^1(\mathbb{R}) \cap L^2(\mathbb{R})$. Ponieważ jednak przestrzeń $L^1(\mathbb{R}) \cap L^2(\mathbb{R})$ leży gęsto w $L^2(\mathbb{R})$, a operatory $\Psi\mathcal{F}$ oraz $\mathcal{F}\Psi$ są izometriami $L^2(\mathbb{R})$, więc

$$\Psi\mathcal{F}(f) = \mathcal{F}\Psi(f) = f, \qquad (f \in L^2(\mathbb{R})). \qquad \square$$

Twierdzenie **18.** *Zachodzi następująca* tożsamość Parsevala

$$\int_{\mathbb{R}} f(x)\overline{g(x)}\, m(dx) = \int_{\mathbb{R}} \hat{f}(x)\overline{\hat{g}(x)}\, m(dx), \qquad (f, g \in L^2(\mathbb{R})).$$

Dowód. Oznaczając przez $\langle f, g\rangle = \int_{\mathbb{R}} f(x)\overline{g(x)}\, m(dx)$ iloczyn skalarny w $L^2(\mathbb{R})$ możemy zapisać tezę równoważnie,

$$\langle f, g\rangle = \langle \hat{f}, \hat{g}\rangle.$$

Wynika ona ze wzoru polaryzacyjnego

$$\begin{aligned}
\langle f, g\rangle &= \tfrac{1}{4}\left(\|f+g\|_2^2 - \|f-g\|_2^2 + i\|f+ig\|_2^2 - i\|f-ig\|_2^2\right)\\
&= \tfrac{1}{4}\left(\|\hat{f}+\hat{g}\|_2^2 - \|\hat{f}-\hat{g}\|_2^2 + i\|\hat{f}+i\hat{g}\|_2^2 - i\|\hat{f}-i\hat{g}\|_2^2\right)\\
&= \langle \hat{f}, \hat{g}\rangle.
\end{aligned} \qquad \square$$

Uwaga **19.** *Udowodniliśmy, że $\mathcal{F} : L^2(\mathbb{R}) \to L^2(\mathbb{R})$ jest izomorfizmem przestrzeni Hilberta $L^2(\mathbb{R})$* na *siebie.*

14 Transformacja Fouriera na $\mathbb{Z}_N$

Transformacja Fouriera może być określona w dużo ogólniejszym kontekście niż rozważany poprzednio. Nie będziemy jednak rozwijać ogólnej teorii, tylko skupimy się na pewnym prostym przykładzie.

Niech $\mathbb{Z}_N = \mathbb{Z}/(N\mathbb{Z})$, jest to grupa z dodawaniem (modulo N), jest to też przestrzeń metryczna (z metryką dyskretną). Na tej grupie rozważamy miarę liczącą μ, każda funkcja $f : \mathbb{Z}_N \to \mathbb{C}$ jest mierzalna i całkowalna względem tej miary, przy czym

$$\int_{\mathbb{Z}_N} f(k)\, \mu(dk) = \sum_{k=0}^{N-1} f(k).$$

Definicja **20.** *Dla funkcji $f : \mathbb{Z}_N \to \mathbb{C}$, czyli $f = (f(0), f(1), \ldots, f(N-1)) \in \mathbb{C}^N$, określamy jej* transformatę Fouriera *wzorem*

$$\hat{f}(t) = \sum_{k=0}^{N-1} f(k) e^{-\frac{2\pi i k t}{N}}.$$

Używamy również oznaczenia $\mathcal{F}(f) = \hat{f}$.

Uwaga **21.** *W przypadku $\mathbb{R}$ określaliśmy transformację Fouriera na $L^1(\mathbb{R})$ (a później na $L^2(\mathbb{R})$), tutaj jednak $L^1(\mathbb{Z}_N, \mu) = L^2(\mathbb{Z}_N, \mu) = \mathbb{C}^N$ – innymi słowy, nie musimy niczego zakładać o funkcji f, aby definicja $\hat{f}$ miała sens.*

Przykład **22.** *Na $\mathbb{Z}_1$*[3] *transformacja Fouriera jest identycznością,*

$$\mathbb{C} \ni (f(0)) \mapsto (f(0)) \in \mathbb{C},$$

a więc nie jest to ciekawy przykład. Na $\mathbb{Z}_2$ transformacja Fouriera działa następująco

$$\mathbb{C}^2 \ni (f(0), f(1)) \mapsto (f(0) + f(1), f(0) - f(1)) \in \mathbb{C}^2.$$

Na $\mathbb{Z}_3$:

$$\begin{aligned}\mathbb{C}^3 \ni (f(0), f(1), f(2)) \mapsto (&f(0) + f(1) + f(2),\\ &f(0) + f(1)e^{-\frac{2\pi i}{3}} + f(2)e^{-\frac{4\pi i}{3}},\\ &f(0) + f(1)e^{-\frac{4\pi i}{3}} + f(2)e^{-\frac{8\pi i}{3}}) \in \mathbb{Z}_3.\end{aligned}$$

W $\mathbb{Z}_4$:

$$\begin{aligned}\mathbb{Z}_4 \ni (f(0), f(1), f(2), f(3)) \mapsto (&f(0) + f(1) + f(2) + f(3),\\ &f(0) - if(1) - f(2) + if(3),\\ &f(0) - f(1) + f(2) - f(3),\\ &f(0) + if(1) - f(2) - if(3)) \in \mathbb{Z}_4.\end{aligned}$$

Na przykład ciąg $(1, 3, 5, 8) \in \mathbb{C}^4$ zostanie przekształcony na ciąg $(17, -4 + 5i, -5, -4 - 5i) \in \mathbb{C}^4$.

Twierdzenie **23.** *(o transformacji odwrotnej) Jeśli $f : \mathbb{Z}_N \to \mathbb{C}$, to*

$$f(n) = \frac{1}{N} \sum_{t=0}^{N-1} \hat{f}(t) e^{\frac{2\pi i n t}{N}} \quad (n = 0, 1, \ldots, N - 1).$$

Dowód. Zachodzi

$$\begin{aligned}\frac{1}{N} \sum_{t=0}^{N-1} \hat{f}(t) e^{\frac{2\pi i n t}{N}} &= \frac{1}{N} \sum_{t=0}^{N-1} \sum_{k=0}^{N-1} f(k) e^{-\frac{2\pi i k t}{N}} e^{\frac{2\pi i n t}{N}}\\ &= \frac{1}{N} \sum_{k=0}^{N-1} f(k) \sum_{t=0}^{N-1} e^{\frac{2\pi i (n-k) t}{N}}.\end{aligned} \tag{5}$$

Jeśli $n = k$, to $\sum_{t=0}^{N-1} e^{\frac{2\pi i (n-k) t}{N}} = \sum_{t=0}^{N-1} 1 = N$. Jeśli zaś $n \neq k$, to

$$\sum_{t=0}^{N-1} e^{\frac{2\pi i (n-k) t}{N}} = \sum_{t=0}^{N-1} \left(e^{\frac{2\pi i (n-k)}{N}}\right)^t = \frac{\left(e^{\frac{2\pi i (n-k)}{N}}\right)^N - 1}{e^{\frac{2\pi i (n-k)}{N}} - 1} = \frac{e^{2\pi i (n-k)} - 1}{e^{\frac{2\pi i (n-k)}{N}} - 1} = 0.$$

Wracając do ostatniej sumy w (5), składniki dla $k \neq n$ znikają, a więc

$$\frac{1}{N} \sum_{t=0}^{N-1} \hat{f}(t) e^{\frac{2\pi i n t}{N}} = f(n). \qquad \square$$

[3] W zasadzie transformacja Fouriera nie jest określona na $\mathbb{Z}_N$, tylko na $L^1(\mathbb{Z}_N) = \mathbb{C}^N$.

Uwaga **24.** *Podobnie jak w przypadku $\mathbb{R}$ można by uzyskać bardziej symetryczne wzory rozważając przeskalowaną miarę liczącą.*

Definicja **25.** *Dla $f, g : \mathbb{Z}_N \to \mathbb{C}$ określamy splot $f * g : \mathbb{Z}_N \to \mathbb{C}$ wzorem*

$$(f * g)(n) = \sum_{k=0}^{N-1} x(n-k)y(k), \quad (n = 0, 1, \dots, N-1).$$

W powyższym wzorze $n - k$ jest obliczane w $\mathbb{Z}_N$, czyli modulo N.

Przykład **26.** *Dla $f, g : \mathbb{Z}_N \to \mathbb{C}$ piszmy w skrócie $f_k = f(k)$ oraz $g_k = g(k)$. Wówczas np. w przypadku $N = 3$,*

$$f * g = (f_0g_0 + f_2g_1 + f_1g_2,\ f_1g_0 + f_0g_1 + f_2g_2,\ f_2g_0 + f_1g_1 + f_0f_2).$$

Twierdzenie **27.**

$$\mathcal{F}(f * g)(t) = \mathcal{F}(f)(t) \cdot \mathcal{F}(g)(t).$$

Dowód. Na ćwiczeniach. □

15 Algorytm FFT[4]

Niech $f : \mathbb{Z}_N \to \mathbb{C}$. Dla obliczenia $\hat{f}(t)$ bezpośrednio z definicji potrzebujemy wykonać $O(N)$ operacji (bo mamy sumę N składników), a więc do znalezienia $\hat{f}$ potrzebujemy $O(N^2)$ operacji. Można jednak obliczyć $\hat{f}$ znacznie efektywniej, bo używając $O(N \log N)$ operacji, jeśli N jest potęgą dwójki[5].

Wprowadźmy następujące oznaczenie: dla $f : \mathbb{Z}_N \to \mathbb{C}$ niech

$$\mathcal{F}_{\mathbb{Z}_N}(f)(t) = \hat{f}(t) = \sum_{k=0}^{N-1} f(k)e^{-\frac{2\pi ikt}{N}}, \quad (t \in \mathbb{Z}).$$

Powyżej rozważamy $t \in \mathbb{Z}$, jednak prawa strona jest N-okresowa, więc otrzymamy takie same wartości $\mathcal{F}_{\mathbb{Z}_N}(f)(t)$ dla t różniących się o całkowitą wielokrotność N.

Niech $N = 2M$ oraz $f : \mathbb{Z}_N \to \mathbb{C}$, piszemy $f_k = f(k)$. Wówczas

$$\begin{aligned}\mathcal{F}_{\mathbb{Z}_N}(f)(t) &= \sum_{k=0}^{M-1} f_{2k}e^{-\frac{2\pi i2kt}{2M}} + \sum_{k=0}^{M-1} f_{2k+1}e^{-\frac{2\pi i(2k+1)t}{2M}} \\ &= \mathcal{F}_{\mathbb{Z}_M}((f_0, f_2, \dots, f_{2M-2}))(t) + e^{-\frac{2\pi it}{N}}\mathcal{F}_{\mathbb{Z}_M}((f_1, f_3, \dots, f_{2M-1}))(t),\end{aligned}$$

gdzie $t = 0, 1, \dots, N-1$ (!). Jeśli N jest potęgą dwójki, to powyższego wzoru możemy używać rekurencyjnie do obliczania dalej $\mathcal{F}_{\mathbb{Z}_M}$.

[4]Cooley i Tukey (1965) spopularyzowali ten algorytm i pokazali, że ma złożoność $O(N \log N)$. Sam pomysł, bez oszacowania złożoności, pojawiał się jednak wcześniej, np. u Gaussa (1805).

[5]Podany sposób można rozszerzyć na przypadek, gdy N rozkłada się na iloczyn małych liczb pierwszych; istnieją też algorytmy o takiej samej złożoności $O(N \log N)$ działające dla dowolnych liczb N, też pierwszych.

Zobaczmy dla przykładu rachunek dla $f : \mathbb{Z}_8 \to \mathbb{C}$. Mamy

$$\begin{aligned}
&\mathcal{F}_{\mathbb{Z}_8}((f_0, f_1, f_2, f_3, f_4, f_5, f_6, f_7))(t) \\
&\quad = \mathcal{F}_{\mathbb{Z}_4}((f_0, f_2, f_4, f_6))(t) + e^{-\frac{2\pi it}{8}} \mathcal{F}_{\mathbb{Z}_4}((f_1, f_3, f_5, f_7))(t) \\
&\quad = \mathcal{F}_{\mathbb{Z}_2}((f_0, f_4))(t) + e^{-\frac{2\pi it}{4}} \mathcal{F}_{\mathbb{Z}_2}((f_2, f_6))(t) \\
&\qquad + e^{-\frac{2\pi it}{8}} \Big(\mathcal{F}_{\mathbb{Z}_2}((f_1, f_5)) + e^{-\frac{2\pi it}{4}} \mathcal{F}_{\mathbb{Z}_2}((f_3, f_7))(t) \Big).
\end{aligned}$$

W ostatnim kroku obliczamy transformaty $\mathcal{F}_{\mathbb{Z}_2}$.

Rachunki można przeprowadzić w następujący sposób. Zaczynamy od pewnej funkcji $f : \mathbb{Z}_8 \to \mathbb{C}$,

$$(f_0, f_1, f_2, f_3, f_4, f_5, f_6, f_7).$$

Aby obliczyć jej transformatę, grupujemy osobno wyrazy parzyste i nieparzyste i dla nich będziemy liczyć transformaty $\mathcal{F}_{\mathbb{Z}_4}$:

$$(f_0, f_2, f_4, f_6,\ f_1, f_3, f_5, f_7).$$

Aby obliczyć te transformaty, znowu w każdej czwórce grupujemy wyrazy parzyste i nieparzyste i dla nich będziemy liczyć transformaty $\mathcal{F}_{\mathbb{Z}_2}$:

$$(f_0, f_4,\ f_2, f_6,\ f_1, f_5,\ f_3, f_7).$$

Teraz dla każdej grupki dwóch elementów obliczamy $\mathcal{F}_{Z_2}$ bezpośrednio lub ze wzoru rekurencyjnego (co na jedno wychodzi), tj. obliczamy

$$\begin{aligned}
&(\mathcal{F}_{\mathbb{Z}_2}(f_0, f_4), \mathcal{F}_{\mathbb{Z}_2}(f_2, f_6), \mathcal{F}_{\mathbb{Z}_2}(f_1, f_5), \mathcal{F}_{\mathbb{Z}_2}(f_3, f_7)) \\
&\quad = (f_0 + f_4, f_0 - f_4,\ f_2 + f_6, f_2 - f_6,\ f_1 + f_5, f_1 - f_5,\ f_3 + f_7, f_3 - f_7) \\
&\quad =: (g_0, g_1,\ g_2, g_3,\ g_4, g_5,\ g_6, g_7).
\end{aligned} \tag{6}$$

Tutaj (g_0, g_1) oraz (g_2, g_3) to transformacje $\mathcal{F}_{Z_2}$ odpowiednio (f_0, f_4) oraz (f_2, f_6). Zatem ze wzoru rekurencyjnego (dla $N = 4$ oraz $t = 0, 1, 2, 3$),

$$\mathcal{F}_{\mathbb{Z}_4}((f_0, f_2, f_4, f_6))(t) = \mathcal{F}_{\mathbb{Z}_2}((f_0, f_4))(t) + e^{-\frac{2\pi it}{4}} \mathcal{F}_{\mathbb{Z}_2}((f_2, f_6))(t),$$

skąd

$$\begin{aligned}
\mathcal{F}_{\mathbb{Z}_4}((f_0, f_2, f_4, f_6)) &= (g_0, g_1, g_0, g_1) + (e^{-\frac{\pi i0}{2}} g_2, e^{-\frac{\pi i1}{2}} g_3, e^{-\frac{\pi i2}{2}} g_2, e^{-\frac{\pi i3}{2}} g_3) \\
&= (g_0, g_1, g_0, g_1) + (g_2, -ig_3, -g_2, +ig_3) \\
&= (g_0 + g_2, g_1 - ig_3, g_0 - g_2, g_1 + ig_3).
\end{aligned}$$

Podobny rachunek można przeprowadzić dla drugiej czwórki elementów $(g_4, g_5,\ g_6, g_7)$. Wobec tego kolejnym krokiem po (6) jest obliczenie

$$\begin{aligned}
&(g_0 + g_2, g_1 - ig_3,\ g_0 - g_2, g_1 + ig_3,\ g_4 + g_5, g_5 - ig_7,\ g_4 - g_6, g_5 + ig_7) \\
&\quad =: (h_0, h_1,\ h_2, h_3,\ h_4, h_5,\ h_6, h_7).
\end{aligned} \tag{7}$$

Po raz ostatni korzystamy ze wzoru rekurencyjnego (dla $N = 8$ oraz $t = 0, 1, \ldots 7$),

$$\begin{aligned}
&\mathcal{F}_{\mathbb{Z}_8}((f_0, f_1, f_2, f_3, f_4, f_5, f_6, f_7)) \\
&\quad = (h_0, h_1,\ h_2, h_3,\ h_0, h_1,\ h_2, h_3) \\
&\quad + (\omega_0 h_4, \omega_1 h_5,\ \omega_2 h_6, \omega_3 h_7,\ \omega_4 h_4, \omega_5 h_5,\ \omega_6 h_6, \omega_7 h_7),
\end{aligned} \tag{8}$$

gdzie $\omega_k = e^{-\frac{2\pi i k}{8}}$. — 9 XII 2021

Podsumowując, wykonaliśmy następujące operacje:

$$
\begin{array}{cccccccc}
(f_0, & f_1, & f_2, & f_3, & f_4, & f_5, & f_6, & f_7) \\
 & & & \downarrow & & & & \\
(f_0, & f_4, & f_2, & f_6, & f_1, & f_5, & f_3, & f_7) \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
(f_0+\omega_0 f_4, & f_0+\omega_4 f_4, & f_2+\omega_0 f_6, & f_2+\omega_4 f_6, & f_1+\omega_0 f_5, & f_1+\omega_4 f_5, & f_3+\omega_0 f_7, & f_3+\omega_4 f_7) \\
\parallel & \parallel & \parallel & \parallel & \parallel & \parallel & \parallel & \parallel \\
(g_0, & g_1, & g_2, & g_3, & g_4, & g_5, & g_6, & g_7) \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
(g_0+\omega_0 g_2, & g_1+\omega_2 g_3, & g_0+\omega_4 g_2, & g_1+\omega_6 g_3, & g_4+\omega_0 g_5, & g_5+\omega_2 g_7, & g_4+\omega_4 g_6, & g_5+\omega_6 g_7) \\
\parallel & \parallel & \parallel & \parallel & \parallel & \parallel & \parallel & \parallel \\
(h_0, & h_1, & h_2, & h_3, & h_4, & h_5, & h_6, & h_7) \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
(h_0+\omega_0 h_4, & h_1+\omega_1 h_5, & h_2+\omega_2 h_6, & h_3+\omega_3 h_7, & h_0+\omega_4 h_4, & h_1+\omega_5 h_5, & h_2+\omega_6 h_6, & h_3+\omega_7 h_7)
\end{array}
$$

Policzmy wykonane operacje postaci „$a + bc$” dla liczb $a, b, c \in \mathbb{C}$. Wykonaliśmy je w trzech wierszach powyżej, za każdym razem ośmiokrotnie. Łącznie daje to $8 \cdot 3 = 8 \cdot \log_2(8)$ operacji.

16 Algorytm szybkiego mnożenia liczb całkowitych

Wyjaśnimy zasadę działania takiego algorytmu[6] na przykładzie mnożenia $423 \cdot 57$. Mamy

$$
\begin{aligned}
423 &= 3 + 2 \cdot 10^1 + 4 \cdot 10^2 = P(10), \quad \text{dla } P(x) = 3 + 2x + 4x^2; \\
57 &= 7 + 5 \cdot 10^1 = Q(10), \quad \text{dla } Q(x) = 7 + 5x.
\end{aligned}
$$

Zatem

$$423 \cdot 57 = PQ(10),$$

wystarczy więc obliczyć iloczyn wielomianów PQ. Pisząc wielomiany jako ich ciąg współczynników,

$$
\begin{aligned}
P &= (3, 2, 4, 0, 0, \ldots) =: (p_0, p_1, \ldots), \\
Q &= (7, 5, 0, 0, \ldots) =: (q_0, q_1, \ldots),
\end{aligned}
$$

otrzymujemy

$$
\begin{aligned}
PQ &= (p_0, p_1, \ldots) * (q_0, q_1, \ldots) \\
&:= (p_0 q_0, p_0 q_1 + p_1 q_0, p_0 q_2 + p_1 q_1 + p_2 q_0, \ldots). \qquad (9)
\end{aligned}
$$

[6] Pierwszy algorytm tego typu jest autorstwa Schönhage–Strassena (1971). Używa on funkcji i FFT o wartościach w pewnym pierścieniu $\mathbb{Z}_q$. Tutaj dla uproszczenia prezentujemy wersję używającą funkcji zespolonych.

Ponieważ ciągi $(p_0, p_1, \ldots)$ oraz $(q_0, q_1, \ldots)$ są od pewnego miejsca zerowe, więc biorąc odpowiednio duże N, splot obcięcia tych ciągów $(p_0, \ldots, p_{N-1})$ oraz $(q_0, \ldots, q_{N-1})$ (liczony jako splot funkcji na $\mathbb{Z}_N$) będzie taki sam jak początkowy fragment (9). Dokładniej, jeśli mnożone czynniki mają odpowiednio po m i n cyfr, to wielomiany P, Q są stopnia odpowiednio $m-1$ oraz $n-1$, więc ich iloczyn PQ ma stopień $m+n-2$. Wystarczy więc wziąć $N > m+n-2$.

W naszym przykładzie $N > 3+2-2 = 3$, więc weźmiemy $N = 4$, potrzebujemy zatem obliczyć splot funkcji na $\mathbb{Z}_4$,

$$(3, 2, 4, 0) * (7, 5, 0, 0).$$

Pomysł polega na tym, żeby obliczyć transformaty Fouriera tych ciągów (co można zrobić szybko, jeśli weźmiemy N będące potęgą dwójki),

$$\begin{aligned}
\mathcal{F}_{\mathbb{Z}_4}((3,2,4,0)) &= (3+2+4, 3-2i-4, 3-2+4, 3+2i-4) \\
&= (9, -1-2i, 5, -1+2i), \\
\mathcal{F}_{\mathbb{Z}_4}((7,5,0,0)) &= (7+5, 7-5i, 7-5, 7+5i) \\
&= (12, 7-5i, 2, 7+5i).
\end{aligned}$$

Teraz obliczamy iloczyn transformat,

$$\begin{aligned}
\mathcal{F}_{\mathbb{Z}_4}((3,2,4,0))\mathcal{F}_{\mathbb{Z}_4}((7,5,0,0)) &= (9, -1-2i, 5, -1+2i)(12, 7-5i, 2, 7+5i) \\
&= (108, -17-9i, 10, -17+9i).
\end{aligned}$$

W pierwszym wierszu powyżej jest mnożenie funkcji na $\mathbb{Z}_4$:

$$(a_0, a_1, a_2, a_3)(b_0, b_1, b_2, b_3) = (a_0b_0, a_1b_1, a_2b_2, a_3b_3).$$

Następnie obliczamy tranformatę odwrotną, co ze względu na podobieństwo do $\mathcal{F}$ również można zrobić za pomocą algorytmu FFT,

$$\begin{aligned}
&\mathcal{F}_{\mathbb{Z}_4}^{-1}((108, -17-9i, 10, -17+9i)) \\
&\quad = \tfrac{1}{4}(108 - 17 - 9i + 10 - 17 + 9i, \\
&\qquad 108 + i(-17-9i) - 10 - i(-17+9i), \\
&\qquad (108 + 17 + 9i + 10 + 17 - 9i, \\
&\qquad 108 - i(-17-9i) - 10 + i(-17+9i)) \\
&\quad = \tfrac{1}{4}(84, 116, 152, 80) \\
&\quad = (21, 29, 38, 20).
\end{aligned}$$

Ostatecznie

$$423 \cdot 57 = PQ(10) = 21 + 29 \cdot 10 + 38 \cdot 10^2 + 20 \cdot 10^3 = 24111.$$

Literatura

[1] W. Rudin. *Analiza rzeczywista i zespolona.* 1986.

[2] E. M. Stein and G. Weiss. *Introduction to Fourier analysis on Euclidean spaces.* Princeton Mathematical Series, No. 32. Princeton University Press, Princeton, N.J., 1971.