Lattices In Cryptography
Winter 2026

Lecture 8
Real Fourier Analysis

Instructor: Chris Peikert
Scribe: Prateek Bhakta

1   Fourier Transform

We begin with some basic definitions.

Definition 1.1 (L^1 function). The function class $L^1(\mathbb{R})$ is the set of all functions $f\colon \mathbb{R} \to \mathbb{C}$ for which

$$\int_{\mathbb{R}} |f(x)|\,\mathrm{d}x < \infty.$$

Definition 1.2 (Fourier transform). Given $f \in L^1(\mathbb{R})$, its Fourier Transform $\hat{f}\colon \mathbb{R} \to \mathbb{C}$ is defined as

$$\hat{f}(w) := \int_{\mathbb{R}} f(x)e^{-2\pi ixw}\,\mathrm{d}x.$$

Note that

$$|\hat{f}(w)| \le \int_{\mathbb{R}} |f(x)e^{-2\pi ixw}|\,\mathrm{d}x \le \int_{\mathbb{R}} |f(x)| \cdot |e^{-2\pi ixw}|\,\mathrm{d}x = \int_{\mathbb{R}} |f(x)|\,\mathrm{d}x < \infty$$

for all $w \in \mathbb{R}$, thus $\hat{f}(w)$ is finite for all w. (The second to last step uses the fact that $|e^{-2\pi ixw}| = 1$.)

Example 1.3. The Fourier transform of the Gaussian function $f(x) = e^{-\pi x^2}$ is

$$
\begin{aligned}
\hat{f}(w) &= \int_{\mathbb{R}} e^{-\pi x^2} \cdot e^{-2\pi ixw}\,\mathrm{d}x \\
&= \int_{\mathbb{R}} e^{-\pi((x+iw)^2 + w^2)}\,\mathrm{d}x \\
&= e^{-\pi w^2} \int_{\mathbb{R}} e^{-\pi(x+iw)^2}\,\mathrm{d}x \\
&= e^{-\pi w^2} \int_{\mathbb{R}} e^{-\pi x^2}\,\mathrm{d}x^{[1]} \\
&= e^{-\pi w^2}{}^{[2]} \\
&= f(w),
\end{aligned}
$$

i.e., the Gaussian is its own Fourier transform.

---

[1] This step follows from applying Cauchy's integral formula to the contour integral around the closed path $R \to R - iw \to -R - iw \to -R \to R$, as $R \to \infty$. Since $e^{-\pi x^2}$ is "nice enough" (holomorphic), this integral must be 0. As $R \to \infty$, the integrals from $[R \to R - iw]$ and $[-R - iw \to -R]$ are each bounded in absolute value by $e^{-\pi wR^2}$, hence they both approach 0. Therefore,

$$0 = \lim_{R\to\infty} \int_{-R}^{R} e^{-\pi x^2}\,\mathrm{d}x + \int_{R-iw}^{-R-iw} e^{-\pi x^2}\,\mathrm{d}x = \lim_{R\to\infty} \int_{-R}^{R} e^{-\pi x^2}\,\mathrm{d}x + \int_{R}^{-R} e^{-\pi(u+iw)^2}\,\mathrm{d}u.$$

The result follows by swapping the bounds of integration in the second integral, and taking $R \to \infty$.

[2] This follows from integrating the square in polar coordinates:

$$\int_{\mathbb{R}} e^{-\pi x^2}\,\mathrm{d}x = \sqrt{\int_{\mathbb{R}^2} e^{-\pi x^2} e^{-\pi y^2}\,\mathrm{d}x\,\mathrm{d}y} = \sqrt{\int_{\theta=0}^{2\pi} \int_{r=0}^{\infty} e^{-\pi r^2} \cdot r\,\mathrm{d}r\,\mathrm{d}\theta} = \sqrt{\int_{\theta=0}^{2\pi} \frac{-1}{2\pi}(0-1)\,\mathrm{d}\theta} = 1.$$

Basic facts. We recall some important facts about the Fourier transform.

Fact 1.4 (Linearity). *For all $f, g \in L^1(\mathbb{R})$ and all $a \in \mathbb{R}$, $\widehat{f + g} = \hat{f} + \hat{g}$ and $\widehat{a \cdot f} = a\hat{f}$.*

Fact 1.5 (Time shift). *Let $f \in L^1(\mathbb{R})$ and $h(x) = f(x - c)$ for some $c \in \mathbb{R}$. Then $\hat{h}(w) = e^{-2\pi icw} \cdot \hat{f}(w)$:*

$$\hat{h}(w) = \int_{\mathbb{R}} f(x - c)e^{-2\pi ixw}\,\mathrm{d}x = \int_{\mathbb{R}} f(u)e^{-2\pi i(u+c)w}\,\mathrm{d}u = e^{-2\pi icw} \cdot \hat{f}(w).$$

Fact 1.6 (Time scale). *Let $f \in L^1(\mathbb{R})$ and $h(x) = f(x/s)$ for some $s > 0$. Then $\hat{h}(w) = s\hat{f}(sw)$:*

$$\hat{h}(w) = \int_{\mathbb{R}} f(x/s)e^{-2\pi ixw}\,\mathrm{d}x = s\int_{\mathbb{R}} f(u)e^{-2\pi isuw}\,\mathrm{d}u = s\int_{\mathbb{R}} f(u)e^{-2\pi iu(sw)}\,\mathrm{d}u = s\hat{f}(sw).$$

Fact 1.7 (Transform inversion). *For any $f \in L^1(\mathbb{R})$,*

$$f(x) = \int_{\mathbb{R}} \hat{f}(w)e^{2\pi ixw}\,\mathrm{d}w.$$

In words, this says that $f(x)$ is a linear combination of "character" functions of the form $e^{2\pi ixw}$ for $w \in \mathbb{R}$, each weighted by the Fourier coefficient $\hat{f}(w)$. Each component $e^{2\pi ixw}$ is periodic with period $1/w$ (for $w \neq 0$), hence frequency w. Note that Fact 1.7 implies that $\hat{\hat{f}}(x) = f(-x)$.

2 Fourier Series for Periodic Functions

Now consider a function $g\colon \mathbb{R} \to \mathbb{C}$ (not necessarily in $L^1(\mathbb{R})$) that is periodic with unit period, i.e., $g(x) = g(x + z)$ for any $z \in \mathbb{Z}$. We call such a function $\mathbb{Z}$-*periodic*. Equivalently, we can work with the function $g\colon (\mathbb{R}/\mathbb{Z}) \to \mathbb{C}$, since the original g is constant over any fixed coset $c + \mathbb{Z}$. Such an g can be decomposed as a linear combination of character functions with *integer* frequencies.

Definition 2.1 (Fourier series). For $g\colon (\mathbb{R}/\mathbb{Z}) \to \mathbb{C}$, its Fourier series $\hat{g}\colon \mathbb{Z} \to \mathbb{C}$ is

$$\hat{g}(w) = \int_{\mathbb{R}/\mathbb{Z}} g(x + \mathbb{Z})e^{-2\pi ixw}\,\mathrm{d}x.$$

Equivalently, the integral can be taken over any fundamental region of $\mathbb{Z}$; often it is convenient to use $[0, 1)$.

Facts 1.4 to 1.6 also apply to the Fourier series, by essentially the same proofs. But there is a slightly different inversion formula.

Fact 2.2 (Series inversion).

$$g(x + \mathbb{Z}) = \sum_{w \in \mathbb{Z}} \hat{g}(w)e^{2\pi ixw}.$$

Example 2.3. The Fourier series of $g(x) = e^{2\pi ixk}$, where $k \in \mathbb{Z}$ (so g is $\mathbb{Z}$-periodic), can be derived in two different ways. First, we calculate the Fourier series directly: for any $w \in \mathbb{Z}$,

$$\hat{g}(w) = \int_{[0,1)} e^{2\pi ixk}e^{-2\pi ixw}\,\mathrm{d}x$$

$$= \int_{[0,1)} e^{2\pi ix(k-w)}\,\mathrm{d}x.$$

2

When $w \neq k$, $e^{2\pi i x(k-w)} \, \mathrm{d}x$ completes a nonzero integer number of revolutions around the unit circle (as x goes from 0 to 1), and thus the above integral is 0. When $k = w$, the integral is simply $\int_{[0,1)} e^0 \, \mathrm{d}x = 1$. Therefore $\hat{g}(w) = \delta_{k,w}$, where $\delta_{k,w}$ is the Kronecker delta function.

Alternatively, we can match coefficients for each character function $e^{2\pi i x w}$ in the series inversion formula. We observe that if $e^{2\pi i x k} = \sum_{w \in \mathbb{Z}} \hat{g}(w) e^{2\pi i x w}$, we must have $\hat{g}(w) = \delta_{k,w}$.

Example 2.4. The Fourier series of $g(x) = \cos(2\pi x)$ can be obtained by recalling that $\cos(2\pi x) = \frac{1}{2} e^{2\pi i x} + \frac{1}{2} e^{-2\pi i x}$. So by matching coefficients in the series inversion formula, we have that $\hat{g}(1) = \hat{g}(-1) = \frac{1}{2}$, and $\hat{g}(w) = 0$ for $w \notin \{-1, 1\}$.

Periodization. Let $f \in L^1(\mathbb{R})$, so it has a Fourier transform. For a countable set S, define the notation $f(S) = \sum_{x \in S} f(x)$. Now "$\mathbb{Z}$-periodize" f by summing all its $\mathbb{Z}$-translates, i.e., define $g \colon (\mathbb{R}/\mathbb{Z}) \to \mathbb{C}$ as

$$g(x + \mathbb{Z}) := f(x + \mathbb{Z}) = \sum_{z \in \mathbb{Z}} f(x + z). \tag{2.1}$$

Lemma 2.5. *The Fourier series of g is $\hat{g}(w) = \hat{f}(w)$.*

Intuitively, this says that periodization by $\mathbb{Z}$ "zeroes out" all the non-integer frequencies, and preserves all the integer ones.

Proof. For any $w \in \mathbb{Z}$, we have

$$
\begin{aligned}
\hat{g}(w) &= \int_{\mathbb{R}/\mathbb{Z}} g(x + \mathbb{Z}) e^{-2\pi i x w} \, \mathrm{d}x \\
&= \int_{[0,1)} \sum_{z \in \mathbb{Z}} f(x + z) e^{-2\pi i x w} \, \mathrm{d}x \\
&= \int_{[0,1)} \sum_{z \in \mathbb{Z}} f(x + z) e^{-2\pi i (x+z) w} \, \mathrm{d}x && (z, w \text{ are integers}) \\
&= \int_{\mathbb{R}} f(u) e^{-2\pi i u w} \, \mathrm{d}u && (u = x + z \text{ runs over } \mathbb{R}) \\
&= \hat{f}(w).
\end{aligned}
$$
$\square$

Poisson summation. We can use the above to get an interesting formula involving the sum of a function evaluated at the integers.

Theorem 2.6 (Poisson summation formula). *For any $f \in L^1(\mathbb{R})$, we have $f(\mathbb{Z}) = \hat{f}(\mathbb{Z})$.*

Proof. Define $g \colon (\mathbb{R}/\mathbb{Z}) \to \mathbb{C}$ to be the $\mathbb{Z}$-periodization of f, as in Equation (2.1). By Fact 2.2 and Lemma 2.5, it follows that

$$f(\mathbb{Z}) = g(0 + \mathbb{Z}) = \sum_{w \in \mathbb{Z}} \hat{g}(w) e^{2\pi i 0 w} = \sum_{w \in \mathbb{Z}} \hat{g}(w) = \sum_{w \in \mathbb{Z}} \hat{f}(w) = \hat{f}(\mathbb{Z}).$$
$\square$

More generally, to sum a function over a scaling of the integers $s^{-1}\mathbb{Z}$ (i.e., a general one-dimensional lattice) for some real $s > 0$, we can use Fact 1.6 to rescale: defining $h(x) = f(x/s)$, by Theorem 2.6 (Poisson summation) and Fact 1.6, we have

$$f(s^{-1}\mathbb{Z}) = h(\mathbb{Z}) = \hat{h}(\mathbb{Z}) = s\hat{f}(s\mathbb{Z}). \tag{2.2}$$

Example 2.7. Define $f(x) = e^{-\pi x^2}$, and $f_s(x) := f(x/s) = e^{-\pi(x/s)^2}$. We approximate $f_s(\mathbb{Z})$ for somewhat large s:

$$
\begin{aligned}
f_s(\mathbb{Z}) = f(s^{-1}\mathbb{Z}) &= s\hat{f}(s\mathbb{Z}) && \text{(Equation (2.2))} \\
&= sf(s\mathbb{Z}) && (\hat{f} = f \text{ for the Gaussian}) \\
&\approx sf(0) && (f(sz) = e^{-\pi(sz)^2} \approx 0 \text{ for } z \in \mathbb{Z} \setminus \{0\}) \\
&= s.
\end{aligned}
$$