Quadratic forms and the local global principle

Lecture 2: Quadratic forms over finite fields and Fourier transforms

Part 1: Classification of quadratic forms / $\mathbb{F}_q$

Part 2: Fourier transforms / $\mathbb{F}_q$

Part 3: Counting rational points on spheres / $\mathbb{F}_q$

# of solns to $Q(v) = a$

Vaguely speaking:

Oftentimes we can think of problems in 3 levels of increasing complexity.

$$\mathbb{F}_p \rightsquigarrow \mathbb{Q}_p \rightsquigarrow \mathbb{Q}$$

local-global principle

① $\mathbb{F}_p \rightsquigarrow \mathbb{F}_p[[t]] := \{ \sum_{i \geq 0} a_i t^i : a_i \in \mathbb{F}_p \}$

$$\mathbb{F}_p \ni a_0 \qquad \underbrace{a_0 + \cdots + a_0}_{p} = 0$$

If somehow I could "carry" this term

$$\text{"} \underbrace{a_0 + \cdots + a_0}_{p} = a_0 t \text{"}$$

One can do this! (Witt constructi)

Resulting ring: $\mathbb{Z}_p$, the ring of p-adic integers.

the fraction field of $\mathbb{Z}_p$ is $\mathbb{Q}_p$

$\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad\quad //$

compl. of $\mathbb{Q}$ under p-adic topology.

$\mathbb{F}_p((t))$ $\mathbb{Q}_p$

$\mathbb{Q}$

$\mathbb{F}_p(X)$

~~Lecture~~

<u>Lemma</u>. Every nondegenerate quad. form (V, Q) of dim 2 is either isom to the hyperbolic plane H_2

<u>OR</u> to $(L, a\,\mathrm{Nm}_{L/k})$, where L/k is a separable quad ext^n & $a \in k^\times$.

<u>Pf</u>: Assume (V, Q) is anisotropic.

Pick any basis of V. Then

$$Q(x,y) = Ax^2 + Bxy + Cy^2.$$

WLOG $A \neq 0$. $= A(x+\alpha y)(x+\beta y)$

for some $\alpha, \beta \in \bar{k}$

$$= A\big(x^2 + \underbrace{(\alpha+\beta)}_{\in k} xy + \underbrace{\alpha\beta}_{\in k} y^2\big)$$

so $\alpha, \beta \in \bar{k} \setminus k$, and $\alpha+\beta \in k$, $\alpha\beta \in k$

$\Rightarrow k(\alpha)/k$ quadr. extn, α, β are conj.

Moreover

$$Q(x,y) = A(x+\alpha y)(x+\bar{\alpha} y)$$
$$= A\, Nm_{k(\alpha)/k}(x+\alpha y). \qquad \square$$

Part 1: Classification of quadratic forms / $\mathbb{F}_q$ ($k = \mathbb{F}_q$)

$q = p^n$, p odd, $n \in \mathbb{Z}_{>0}$

- $\mathbb{F}_q^\times$ is cyclic
- $Nm: \mathbb{F}_{q^2} \to \mathbb{F}_q$, $x \mapsto x \cdot x^q = x^{q+1}$ is surjective.

Lemma. Every anisotropic quad space $(V, Q)/\mathbb{F}_q$ of dim 2 is $(\mathbb{F}_{q^2}, Nm)$.

Pf. By prev lemma, we know that every anisotropic quad space of dim 2 is $(\mathbb{F}_{q^2}, a \cdot Nm)$ for some $a \in \mathbb{F}_q^\times$.
Since Nm is surj. $\exists\, \alpha \in \mathbb{F}_{q^2}^\times$ s.t. $Nm(\alpha) = a$.
Then mult by α is an isometry $(\mathbb{F}_{q^2}, a \cdot Nm) \xrightarrow{\sim} (\mathbb{F}_{q^2}, Nm)$ $\square$

<u>Prop.</u> Any anisotropic quadratic space is 1 dim'l or is $(\mathbb{F}_{q^2}, Nm)$.

<u>Pf.</u> Could be 1-dim'l: $(\mathbb{F}_q, ax^2)$ for some $a \in \mathbb{F}_q^\times$

Could be 2-dim'l: $(\mathbb{F}_{q^2}, Nm)$

What about 3-dim'l?

Suppose (V, Q) is a 3-dim'l quad space, <u>anisotropic</u>

Pick any nonzero $v \in V$. Then $Q(v) \neq 0$.

Now by result from last week

$$\underbrace{V}_{3\text{ dim'l}} = \underbrace{\mathbb{F}_q v}_{1\text{ dim'l}} \oplus \underbrace{v^\perp}_{\underline{2\text{-dim'l}}}.$$

anisotropic

$\Rightarrow v^\perp \cong (\mathbb{F}_{q^2}, Nm)$ by prev lemma.

Since Nm is surj., $\exists\, \alpha \in \mathbb{F}_{q^2}$ s.t. $Nm(\alpha) = -Q(v)$.

<u>Now</u>: $(v, \alpha) \in \mathbb{F}_q v \oplus v^\perp = V$

and $Q(\underbrace{v, \alpha}_{\text{nonzero!}}) = Q(v) + Q(\alpha) = Q(v) - Q(v) = 0.$

$\Rightarrow (v, \alpha)$ is isotropic $\times$.

What about 4-dim?

use induction! $\square$

IT FOLLOWS: (Fix $a \in \mathbb{F}_q^\times$, which is not a square in $\mathbb{F}_q^\times$ — i.e. $\nexists\, b \in \mathbb{F}_q^\times$ s.t. $b^2 = a$)

Every anisotropic quad space is of one of the following forms:

(V, Q)	dim	disc
✩ $(\mathbb{F}_q, x^2)$	1	1
✩ $(\mathbb{F}_q, ax^2)$	1	-1
✩ $(\mathbb{F}_{q^2}, \mathrm{Nm})$ $\begin{pmatrix} 1 & \\ & -a \end{pmatrix}$	2	$\omega(-a) = -\omega(-1)$

Note: $\omega(-1) = 1 \iff -1$ is a square in $\mathbb{F}_q^\times$

Recall: discriminant $\in (k^\times)/(k^\times)^2 = \underbrace{(\mathbb{F}_q^\times)/(\mathbb{F}_q^\times)^2}_{\text{size } 2}$!

More precisely, can consider

$$\omega : \mathbb{F}_q^\times \longrightarrow \mathbb{C}^\times$$

$$x \longmapsto \begin{cases} +1 & \text{if } x \in (\mathbb{F}_q^\times)^2 \\ -1 & \text{if } x \notin (\mathbb{F}_q^\times)^2 \end{cases}$$

Then $\ker(\omega) = (\mathbb{F}_q^\times)^2$ and so ω allows us to identify $(\mathbb{F}_q^\times)/(\mathbb{F}_q^\times)^2$ with $\{\pm 1\} = \mu_2$.

✩ One more: $\operatorname{disc}(H_2) = \omega(-1)$

Main thm from week 1 $\Rightarrow$ (V,Q) any nondegen quad space is $H_{2r} \oplus$ anisotropic part

So every nondegen quad space must be one of the following

(V,Q)	dim	disc
$(\mathbb{F}_q^{\oplus 2r}, H_{2r})$	$2r$	$\omega(-1)^r$
$(\mathbb{F}_q^{\oplus 2r-2}, H_{2r-2}) \oplus (\mathbb{F}_{q^2}, Nm)$	$2r$	$-\omega(-1)^r$
$(\mathbb{F}_q^{\oplus 2r}, H_{2r}) \oplus (\mathbb{F}_q, x^2)$	$2r+1$	$\omega(-1)^r$
$(\mathbb{F}_q^{\oplus 2r}, H_{2r}) \oplus (\mathbb{F}_q, ax^2)$	$2r+1$	$-\omega(-1)^r$

<u>Thm</u> (classificatn of quad. spaces over $\mathbb{F}_q$)

The isomorphism class of a nondegen quad space (V,Q) over $\mathbb{F}_q$ is determined by:

- $\dim(V)$
- $\operatorname{disc}(Q)$.

Part 2. Fourier transforms over finite fields

Ex.: Homomorphisms $(\mathbb{F}_p,+) \to \mathbb{C}^\times$

$$\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} \qquad \mathrm{Im} \subset \mu_p := \{z \in \mathbb{C}^\times : z^p = 1\}.$$

Set $\psi_0 : \mathbb{F}_p \to \mathbb{C}^\times$

$$1 \mapsto e^{2\pi i/p}$$

$$x \mapsto e^{2\pi i x/p}$$

What about any other homomorphism?

$\psi_0' : \mathbb{F}_p \to \mathbb{C}^\times$

$$1 \mapsto e^{2\pi i a/p}$$

$$x \mapsto e^{2\pi i a x/p}$$

$$\psi_0'(x) = e^{2\pi i a x/p} = \psi_0(ax)$$

So: ψ_0' can be written in terms of ψ_0!

Set $\psi : \mathbb{F}_q \to \mathbb{C}^\times$, $x \mapsto e^{2\pi i \, \mathrm{Tr}(x)/p}$

where $\mathrm{Tr} : \mathbb{F}_q \to \mathbb{F}_p$, $x \mapsto x + x^p + \cdots + x^{p^{n-1}}$

$$\mathbb{F}_q = \mathbb{F}_{p^n}$$

Fact: Every $\underbrace{\text{homomorphism } \mathbb{F}_q \to \mathbb{C}^\times}_{\text{"characters of } \mathbb{F}_q\text{"}}$ is of the form $\psi_a : \mathbb{F}_q \to \mathbb{C}^\times$, $x \mapsto \psi(ax)$, for some $a \in \mathbb{F}_q$.

Lemma. For $y \in \mathbb{F}_q$:

$$\sum_{x \in \mathbb{F}_q} \psi(xy) = \begin{cases} q & \text{if } y = 0 \\ 0 & \text{otherwise.} \end{cases}$$

Pf. If $y=0$: $\sum_{x \in \mathbb{F}_q} \psi(xy) = \sum_{x \in \mathbb{F}_q} \psi(0) = q$ ✓

If $y \neq 0$: $\exists\, a \in \mathbb{F}_q^\times$ s.t. $\psi(ay) \neq 1$.

$$\psi(ay)(\text{LHS}) = \psi(ay) \sum_{x \in \mathbb{F}_q} \psi(xy) = \sum_{x \in \mathbb{F}_q} \psi((a+x)y)$$

$$= \sum_{x \in \mathbb{F}_q} \psi(xy) = \text{LHS}$$

$$\Rightarrow \text{LHS} = 0. \qquad \square$$

Def. The Fourier transform of a functn $f: \mathbb{F}_q \to \mathbb{C}$ is the fn

$$\mathrm{FT}(f): \mathbb{F}_q \to \mathbb{C}, \quad y \mapsto \frac{1}{\sqrt{q}} \sum_{x \in \mathbb{F}_q} f(x)\psi(-xy).$$

Two important properties: For any $f: \mathbb{F}_q \to \mathbb{C}$,

① (Fourier inversion) $\mathrm{FT}(\mathrm{FT}(f))(x) = f(-x)$

② (Plancherel formula) $\sum_{x \in \mathbb{F}_q} |f(x)|^2 = \sum_{y \in \mathbb{F}_q} |\mathrm{FT}(y)|^2$.

KEY Example. FT of any character of $\mathbb{F}_q$
$\underbrace{\text{any character of } \mathbb{F}_q}$ Ψ_a for some $a \in \mathbb{F}_q$.

- Compute $FT(\Psi_a)$

$$FT(\Psi_a)(y) = \frac{1}{\sqrt{q}} \sum_{x\in\mathbb{F}_q} \overbrace{\Psi_a(x)}^{\Psi(ax)} \Psi(-xy) = \frac{1}{\sqrt{q}} \sum_{x\in\mathbb{F}_q} \Psi((a-y)x)$$

$$= \begin{cases} \frac{1}{\sqrt{q}}\cdot q & \text{if } a-y=0 \iff y=a \\ 0 & \text{otherwise} \end{cases}$$

$$= \sqrt{q}\cdot \delta_a(y)$$

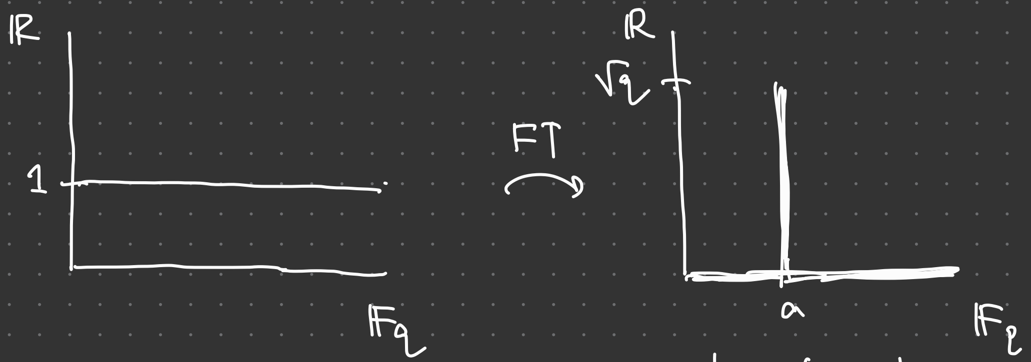
- Compute $FT(FT(\Psi_a))$

$$FT(FT(\Psi_a))(x) = FT\left(\sqrt{q}\cdot \delta_a\right)(x)$$

$$= \frac{\cancel{\sqrt{q}}}{\cancel{\sqrt{q}}} \sum_{y\in\mathbb{F}_q} \delta_a(y)\Psi(-xy) = \Psi(-ax) = \Psi_a(-x)$$

So. $\boxed{FT(FT(\Psi_a))(x) = \Psi_a(-x)}$ (matches 1)

Pictorially:



$|\psi_a|$ $\qquad$ $|FT(\psi_a)|$ $= \sqrt{q} \cdot \delta_a$

Observe: $\boxed{\sum_{x \in \mathbb{F}_q} |\psi_a(x)|^2 = q = (\sqrt{q})^2 = \sum_{y \in \mathbb{F}_q} |FT(\psi_a)(y)|^2.}$

(matches ②)

Part 3: Gauss sums and rational points on spheres

<u>Def.</u> $v_Q(x) := \#\{v \in V : Q(v) = x\}$

(V, Q) nondegen quad sp / $\mathbb{F}_q$

$$\gamma_Q(y) = \sum_{x \in \mathbb{F}_q} v_Q(x) \cdot \psi(-xy)$$

Key to why γ_Q is useful:

<u>Prop.</u> If $(V, Q) = (V_1, Q_1) \oplus (V_2, Q_2)$, then

$$\gamma_Q = \gamma_{Q_1} \cdot \gamma_{Q_2}$$

Strategy to compute v_Q: any nonsquare $\in \mathbb{F}_q^\times$

Step 1. Compute v_Q for $(\mathbb{F}_q, x^2)$, $(\mathbb{F}_q, ax^2)$, $(\mathbb{F}_q^{\oplus 2}, H_2)$, $(\mathbb{F}_{q^2}, Nm)$

Step 2. Deduce γ_Q in these 4 cases.

Step 3. Use multiplicative prop of γ_Q to obtain γ_Q in general.

Step 4. Use Fourier inversion to recover v_Q.

$$v_Q(x) = \frac{1}{q} \sum_{x \in \mathbb{F}_q} \gamma_Q(y)\,\psi(xy).$$

We will compute Step 1 & 2.

<u>FIRST</u>: $\gamma_Q(0) = \sum_{x \in \mathbb{F}_q} v_Q(x) = \#V = q^{\dim(V)}$

$\boxed{\text{dim } 1}$ $(\mathbb{F}_q, ax^2)$ where $a \in \mathbb{F}_q^\times$ arbitrary.

$$v_Q(x) = \begin{cases} 1 & x = 0 \\ 2 & \text{if } x \neq 0 \text{ \& } x/a \text{ is a square in } \mathbb{F}_q^\times \\ 0 & \text{otherwise} \end{cases}$$

$az^2 = 0$

$az^2 = x \neq 0$

$z^2 = \frac{x}{a}$

$$= 1 + \operatorname{sgn}\left(\frac{x}{a}\right).$$

Let $\underline{\mathrm{sgn}}: \mathbb{F}_q \to \mathbb{C}^\times$

$$x \mapsto \begin{cases} 0 & \text{if } x = 0 \\ 1 & \text{if } x \text{ is a square in } \mathbb{F}_q^\times \\ -1 & \text{otherwise.} \end{cases}$$

So: for $y \in \mathbb{F}_q^\times$

$$r_Q(y) = \sum_{x \in \mathbb{F}_q} \left(1 + \mathrm{sgn}\left(\tfrac{x}{a}\right)\right) \psi(-xy)$$

$$= \underbrace{\left(\sum_{x \in \mathbb{F}_q} \psi(-xy)\right)}_{=0} + \underline{\left(\sum_{x \in \mathbb{F}_q} \mathrm{sgn}\left(\tfrac{x}{a}\right) \psi(-xy)\right)}$$

So:

$$\boxed{r_Q(y) = \begin{cases} \displaystyle\sum_{x \in \mathbb{F}_q} \mathrm{sgn}\left(\tfrac{x}{a}\right)\psi(-xy) & \text{if } y \neq 0 \\ \underline{q} & \text{if } y = 0 \end{cases}}$$

$\boxed{\text{dim } 2}$ in either $Q = H_2$ or N_m

$$\boxed{r_Q(y) = \begin{cases} \mathrm{disc}(Q) \cdot q & \text{if } y \neq 0 \\ q^2 & \text{if } y = 0. \end{cases}}$$

Fact (see Lemma 2.15 & Observation 2.16)

$$\left| \sum_{x \in \mathbb{F}_q} \operatorname{sgn}\left(\frac{x}{a}\right) \psi(-xy) \right| = q^{1/2}$$

Point: For (V, Q) nondegen. $n = \dim V$

$$|\gamma_Q(y)| = \begin{cases} q^{n/2} & \text{if } y \neq 0 \\ q^n & \text{if } y = 0 \end{cases}$$

Prop. If a quad space (V, Q) has dim $n \geq 3$,

then $v_Q(0) > 1$.

i.e. (V, Q) has at least one nonzero isotropic vector.

Pf. $v_Q(0) = \frac{1}{q} \sum_{y \in \mathbb{F}_q} \gamma_Q(y)$

$$= \underbrace{\frac{1}{q} \gamma_Q(0)}_{q^{n-1}} + \frac{1}{q} \sum_{y \in \mathbb{F}_q^\times} \gamma_Q(y)$$

By Cauchy-Schwarz

$$|v_Q(0) - q^{n-1}| \leq \frac{1}{q} \sum_{y \in \mathbb{F}_q^\times} |\gamma_Q(y)|$$

$$= \frac{1}{q} \sum_{y \in \mathbb{F}_q^\times} q^{n/2} = \frac{(q-1)}{q} \cdot q^{n/2}.$$

$$\Rightarrow q^{n-1} - \left(\frac{q-1}{q}\right) q^{n/2} \leq \nu_Q(0) \leq q^{n-1} + \left(\frac{q-1}{q}\right) q^{n/2}.$$

<u>Check</u>: If $n \geq 3$, then

$$q^{n-1} - \left(\frac{q-1}{q}\right) q^{n/2} > 1$$

$$\Rightarrow \quad 1 < \nu_Q(0) \qquad \square$$