

Zinnowitz, 2016/04/05 1 hour

1.

Gauss composition and primitive integral points on spheres.
 (details: Albert Gunaman's thesis, openaccess.beiden.univ.nl)

Let $n \equiv 3(8), n > 3$. $X_n(\mathbb{Z}) := \left\{ (x, y, z) \in \mathbb{Z}^3 : \begin{array}{l} x^2 + y^2 + z^2 = n \\ \gcd(x, y, z) = 1 \end{array} \right\}$

$$\mathcal{O}_{-n} := \mathbb{Z} \left[\frac{1 + \sqrt{-n}}{2} \right].$$

Thm (Gauss) $\# X_n(\mathbb{Z}) = 24 \cdot \# \text{Pic}(\mathcal{O}_{-n})$.

My interest: $\left(\sum_{m \in \mathbb{Z}} q^{m^2} \right)^d$, modular forms, weight $d/2$.

Zagier: proof using modular forms (1975), not so easy, leads to mock mod. f.
 $v := P^{-n}Q$

Gauss's proof. For $P \in X_n(\mathbb{Z})$: $P^\perp \hookrightarrow \mathbb{Z}^3 \xrightarrow{\langle \cdot, \cdot \rangle} \mathbb{Z}$
 $\uparrow \quad \quad \quad \uparrow$
 $P^\perp \oplus \mathbb{Z} \cdot P \rightarrow n\mathbb{Z}$
 $n^2 \langle Q, Q \rangle = \langle v, v \rangle + n$
 $b := \langle \cdot, \cdot \rangle|_{P^\perp \times P^\perp}$
 disc. n , represents $-n \pmod{n^2}$.

Then work backwards: count

such b up to isom., and use: $V(L, b')$ L free \mathbb{Z} -module rank 3,
 b' pos. def. sym. bil. form disc. 1, $(L, b') \cong (\mathbb{Z}^3, \langle \cdot, \cdot \rangle)$.

The counting is a bit complicated: $24 \cdot 2^{t-1} \# \text{Pic}(\mathcal{O}_{-n}) / 2^{t-1}$.

Goal: use SO_3 -action and Hasse-Minkowski to give a new proof, and
 get more: $SO_3(\mathbb{Z}) \backslash X_n(\mathbb{Z})$ is a $\text{Pic}(\mathcal{O}_{-n})$ -torsor.

(Rem: earlier work by Shimura & Gross, adelicly.)

$$X_n := V(x^2 + y^2 + z^2 - n) \hookrightarrow \mathbb{A}^3 - V(x, y, z).$$

$$\bigcup G := SO_3 \quad (g, x) \mapsto (x, gx)$$

Over $\mathbb{Z}[1/2]$: $G \times X_n \rightarrow X_n \times X_n$ is surjective & smooth, action transitive

$$/\mathbb{F}_2: \mathbb{F}_2^3 = \mathbb{F}_2 \cdot \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \oplus \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix}^\perp \quad \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix}$$

$$\text{So } G_{\mathbb{F}_2} \supset SO_{2, \mathbb{F}_2}, \text{ dim. } 3.$$

for étale top.

stab: 1-dim. comm.

Surprise: X_n, G on $\text{Spec}(\mathbb{Z}) + \text{Zar}$, then $G \curvearrowright X_n$ transitive!
 for $v \in \mathbb{Z}^3$ primitive

Use symmetries: $S_v: x \mapsto x - 2 \frac{\langle x, v \rangle}{\langle v, v \rangle} \cdot v$, $\uparrow \langle v, v \rangle$.

$$\forall p: G(\mathbb{Z}_p) \curvearrowright X_n(\mathbb{Z}_p).$$

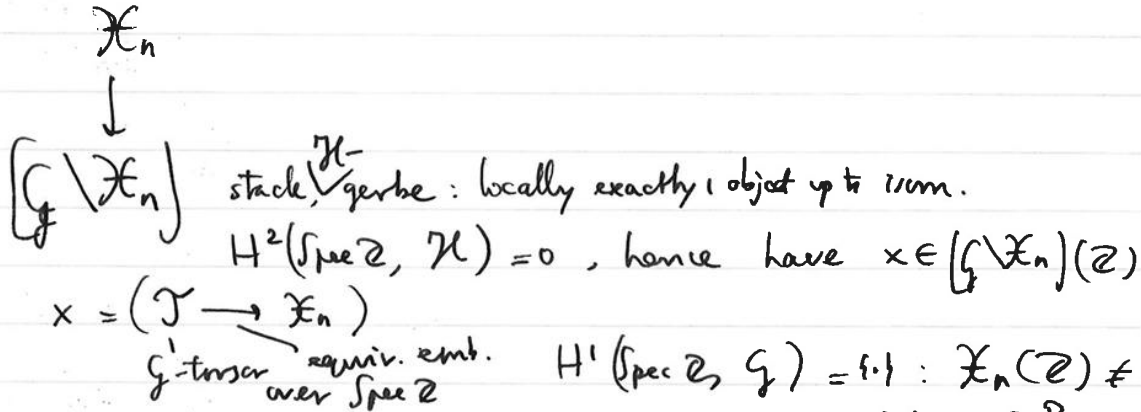
Now we can use non-ab. cohomology.

1st aim now: $\mathcal{X}_n(\mathbb{Z}) \neq \emptyset$.

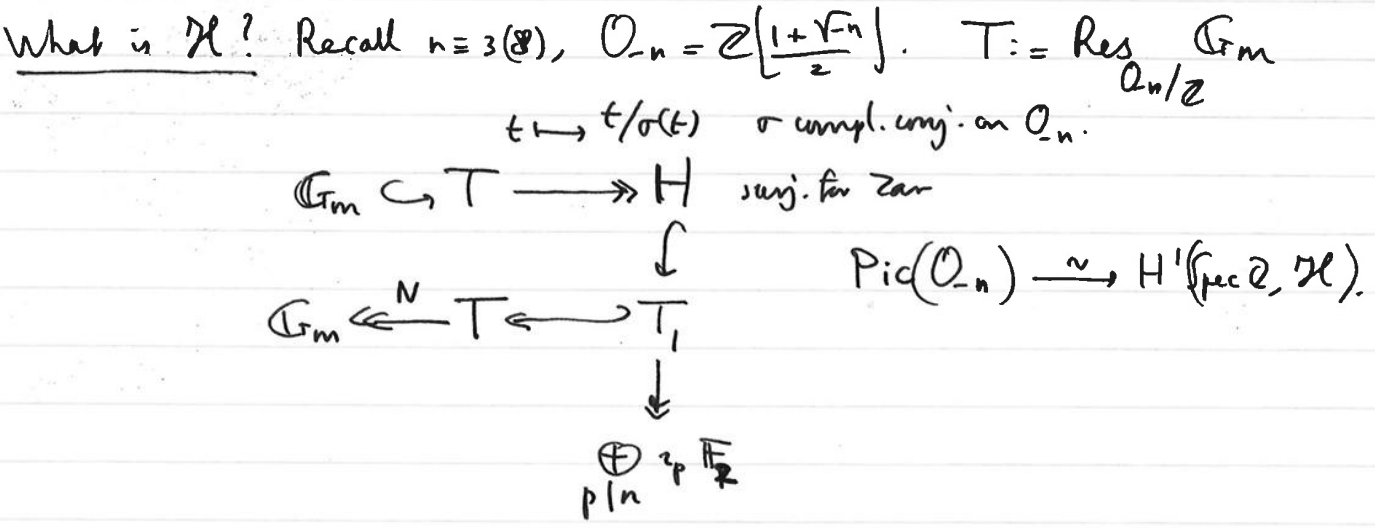
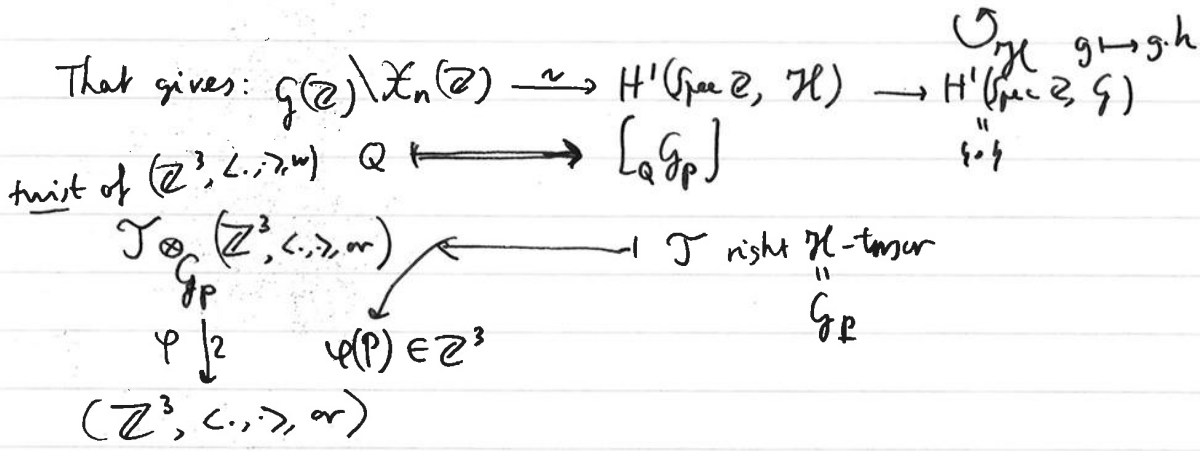
Hans-Minkowski: $\mathcal{X}_n(\mathbb{Q}) \neq \emptyset$.

Using $s, v \in \mathbb{Q}$: $\forall p \mathcal{X}_n(\mathbb{Z}_{(p)}) \neq \emptyset$.

$\forall U \subset \text{Spec } \mathbb{Z}$: category (groupoid) $\mathcal{G}(U) \subset \mathcal{X}_n(U)$, $\forall x, y: \text{Aut}(x) = \text{Aut}(y)$.
 $\mathcal{H} :=$ the stabiliser, sheaf of comm. grps on $\text{Spec } \mathbb{Z}$. bec. ~~sheaf~~ $\mathcal{G}(U)_x$ comm.



2nd aim $\text{Pic}(\mathcal{O}_{-n})$ -action. Let $P \in \mathcal{X}_n(\mathbb{Z})$. $\mathcal{G} \rightarrow \mathcal{X}_n$ "fibration".



Explicit action of $\text{Pic}(\mathcal{O}_n)$

Let I be an invertible \mathcal{O}_n -module, $P \in \mathcal{X}_n(\mathbb{Z})$.

$\mathbb{Q} \otimes P^\perp$ is a $\mathbb{Q}(\sqrt{-n})$ -vect. space: $v \mapsto P \times v = \sqrt{-n} \cdot v$

$$\underline{I}^x \otimes_{\underline{\mathcal{O}_n}}^x \mathbb{Z}^3 = \left(\mathbb{Z} \cdot P \oplus I \cdot \sigma(I)^{-1} \cdot P^\perp \right) \subset \mathbb{Q}^3$$

$$+ \frac{N(\epsilon)}{N(I)} \cdot (t \cdot \sigma(\epsilon)^{-1}) \cdot \mathbb{Z}^3$$

where $t \in I$ generates I/nI . $\in \text{SO}_3(\mathbb{Q})_P$

$\varphi \swarrow$
 $[I] \cdot P = \varphi(P) \cdot \mathbb{Z}^3$

The action of $\text{Pic}(\mathcal{O}_n)$ on P^\perp 's: $\varphi(P)^\perp \cong I \cdot \sigma(I)^{-1} \cdot P^\perp$
 note: $[I \cdot \sigma(I)^{-1}] = [I^2]$. Forms that occur: 1 coset under 2 $\cdot \text{Pic}(\mathcal{O}_n)$.

Another way to see it:

$$\{\pm 1\} \hookrightarrow \bigoplus_{P|n} \mathbb{F}_2 \longrightarrow H^1(\text{Spec}(\mathbb{Z})_{2n}, \mathbb{H}) \longrightarrow H^1(\text{Spec}(\mathbb{Z})_{\text{et}}, T_1)$$

$$\searrow \quad \quad \quad \nearrow$$

$$H^1(\text{Spec}(\mathbb{Z})_{2n}, \mathbb{H})$$

(To put it a bit in perspective: Bhargava & Gross, Arithmetic invariant theory, ask for such an approach...)