Zinnowitz, 2016/04/05 1 hour

Gauss composition and primitive integral points on spheres.
(details: Albert Gunawan's thesis, openaccess.leidenuniv.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) $\# X_n(\mathbb{Z}) = 24 \cdot \# \mathrm{Pic}(\mathcal{O}_{-n})$.

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.

Gauss's proof. For $P \in X_n(\mathbb{Z})$:

$v := P - nQ$

$$\begin{tikzcd} & Q \arrow[r, mapsto] & 1 \\ P^\perp \arrow[r, hook] & \mathbb{Z}^3 \arrow[r, two heads, "\langle P, \cdot \rangle"] & \mathbb{Z} \\ & P^\perp \oplus \mathbb{Z}\cdot P \arrow[u, hook] \arrow[r, two heads] & n\mathbb{Z} \arrow[u, hook] \end{tikzcd}$$

$n^2 \langle Q,Q \rangle = \langle v,v \rangle + n$,
$b := \langle \cdot , \cdot \rangle |_{P^\perp \times P^\perp}$,
discr. n, represents $-n \bmod n^2$.

Then work backwards: count such b up to isom., and use: $\forall (L, b')$ L free $\mathbb{Z}$-module rank 3, b' pos. def. sym. bil. form discr. 1, $(L, b') \cong (\mathbb{Z}^3, \langle \cdot , \cdot \rangle)$.
The counting is a bit complicated: $24 \cdot 2^{t-1} \# \mathrm{Pic}(\mathcal{O}_{-n}) / 2^{t-1}$.

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 $\mathrm{Pic}(\mathcal{O}_{-n})$-torsor.
(Rem: earlier work by Shimura & Gross, adelically.)

$X_n := V(x^2+y^2+z^2-n) \hookrightarrow \mathbb{A}^3 - V(x,y,z)$.
$\circlearrowright G := SO_3 \quad (g,x) \longmapsto (x, gx)$
Over $\mathbb{Z}[1/2]$: $G \times X_n \to X_n \times X_n$ is surjective & smooth, action transitive for étale top.
$/\mathbb{F}_2$: $\mathbb{F}_2^3 = \mathbb{F}_2 \cdot \begin{pmatrix}1\\1\\1\end{pmatrix} \oplus \begin{pmatrix}1\\1\\1\end{pmatrix}^\perp$ $\begin{pmatrix}1\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\1\end{pmatrix}$, $\begin{pmatrix}0 & 1\\1 & 0\end{pmatrix}$
So $G_{\mathbb{F}_2} \supset SL_{2,\mathbb{F}_2}$, dim. 3. stab: 1-dim. comm.

Surprise: $\mathcal{X}_n$, $\mathcal{G}$ on $\mathrm{Spec}(\mathbb{Z})$ + Zar, then $\mathcal{G} \circlearrowright \mathcal{X}_n$ transitive!

Use symmetries: for $v \in \mathbb{Z}^3$ primitive $s_v : x \longmapsto x - \frac{2\langle x, v \rangle}{\langle v, v \rangle} \cdot v$, $4 \nmid \langle v, v \rangle$.
$\forall p$: $\mathcal{G}(\mathbb{Z}_{(p)}) \circlearrowright \mathcal{X}_n(\mathbb{Z}_{(p)})$.
Now we can use non-ab. cohomology.

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

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

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

$\forall U \subset \mathrm{Spec}(\mathbb{Z})$: category (groupoid) $\mathcal{G}(U) \circlearrowright \mathcal{X}_n(U)$, $\forall x,y$: $\mathrm{Aut}(x) = \mathrm{Aut}(y)$.

$\mathcal{H}$:= the stabiliser, sheaf of comm. grps on $\mathrm{Spec}(\mathbb{Z})$. bec. ~~sta~~ $\mathcal{G}(U)_x$ comm.

$$\begin{tikzcd} \mathcal{X}_n \arrow[d] \\ {[\mathcal{G}\backslash\mathcal{X}_n]} \end{tikzcd}$$

stack, $\mathcal{H}$-gerbe : locally exactly 1 object up to isom.

$H^2(\mathrm{Spec}\,\mathbb{Z}, \mathcal{H}) = 0$, hence have $x \in [\mathcal{G}\backslash\mathcal{X}_n](\mathbb{Z})$

$x = (\mathcal{T} \longrightarrow \mathcal{X}_n)$

$\mathcal{G}$-torsor, equiv. emb. over $\mathrm{Spec}\,\mathbb{Z}$

$H^1(\mathrm{Spec}\,\mathbb{Z}, \mathcal{G}) = \{\cdot\}$: $\mathcal{X}_n(\mathbb{Z}) \neq \emptyset$.

<u>2nd aim</u> $\mathrm{Pic}(\mathcal{O}_{-n})$-action. Let $P \in \mathcal{X}_n(\mathbb{Z})$.

$$g \longmapsto g\cdot P$$
$$\mathcal{G} \longrightarrow \mathcal{X}_n \quad \text{"fibration".}$$
$$\circlearrowright_{\mathcal{H}} \quad g \mapsto g\cdot h$$

That gives: $\mathcal{G}(\mathbb{Z})\backslash\mathcal{X}_n(\mathbb{Z}) \xrightarrow{\sim} H^1(\mathrm{Spec}\,\mathbb{Z}, \mathcal{H}) \longrightarrow H^1(\mathrm{Spec}\,\mathbb{Z}, \mathcal{G}) = \{\cdot\}$

<u>twist of</u> $(\mathbb{Z}^3, \langle\cdot,\cdot\rangle, \mathrm{or})$ $\quad Q \longleftrightarrow [{}_Q\mathcal{G}_P]$

$$\mathcal{T} \otimes_{\mathcal{G}_P} (\mathbb{Z}^3, \langle\cdot,\cdot\rangle, \mathrm{or}) \longleftarrow\!\shortmid \mathcal{T} \text{ right } \mathcal{H}\text{-torsor} = \mathcal{G}_P$$

$$\varphi \downarrow \wr \qquad \varphi(P) \in \mathbb{Z}^3$$

$$(\mathbb{Z}^3, \langle\cdot,\cdot\rangle, \mathrm{or})$$

<u>What is $\mathcal{H}$?</u> Recall $n \equiv 3\,(8)$, $\mathcal{O}_{-n} = \mathbb{Z}\left[\frac{1+\sqrt{-n}}{2}\right]$. $T := \mathrm{Res}_{\mathcal{O}_n/\mathbb{Z}}\, \mathbb{G}_m$

$t \longmapsto t/\sigma(t)$ $\quad \sigma$ compl. conj. on $\mathcal{O}_{-n}$.

$$\begin{tikzcd} \mathbb{G}_m \arrow[r, hook] & T \arrow[r, two heads] & H \arrow[d, hook] \\ \mathbb{G}_m & T \arrow[l, two heads, "N"'] & T_1 \arrow[l, hook'] \arrow[d] \\ & & \bigoplus_{p\mid n} i_p \mathbb{F}_2 \end{tikzcd}$$

surj. for Zar

$$\mathrm{Pic}(\mathcal{O}_{-n}) \xrightarrow{\sim} H^1(\mathrm{Spec}\,\mathbb{Z}, \mathcal{H}).$$

Explicit action of $\mathrm{Pic}(\mathcal{O}_{-n})$

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: $v \mapsto P \times v = \sqrt{-n} \cdot v$

$$\underline{I}^\times \otimes_{\underline{\mathcal{O}_{-n}}^\times} \mathbb{Z}^3 = \left(\mathbb{Z}\cdot P \oplus I \cdot \sigma(I)^{-1} \cdot P^\perp + \frac{N(t)}{N(I)} \cdot \underbrace{\left(t \cdot \sigma(t)^{-1}\right)}_{\in SO_3(\mathbb{Q})_P} \cdot \mathbb{Z}^3 \right) \subset \mathbb{Q}^3$$

where $t \in I$ generates I/nI.

$$\xrightarrow[\sim]{\varphi} \quad [I]\cdot P = \varphi(P) . \quad \mathbb{Z}^3$$

The action of $\mathrm{Pic}(\mathcal{O}_{-n})$ 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 $2 \cdot \mathrm{Pic}(\mathcal{O}_{-n})$.

Another way to see it:

$$\begin{tikzcd}
\{\pm 1\} \arrow[r, hook] & \bigoplus_{p \mid n} \mathbb{F}_2 \arrow[dr] & & \\
& & H^1(\mathrm{Spec}(\mathbb{Z})_{\mathrm{Zar}}, \mathbb{H}) \arrow[r] \arrow[dr, two heads] & H^1(\mathrm{Spec}(\mathbb{Z})_{et}, T_1) \\
& & & H^1(\mathrm{Spec}(\mathbb{Z})_{\mathrm{Zar}}, H) \arrow[u, hook]
\end{tikzcd}$$

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