Rennes, 2012/06/19
(conference for Moret-Bailly)
(1 hour)

Bas Edixhoven, Univ. Leiden.

Gauss's theorem on sums of 3 squares, via groupschemes.

I think that the topic of this talk is suitable: Laurent likes number theory, groupschemes, cohomology.

Let us first state Gauss's result.

Notation: for $d \in \mathbb{Z}$ not a square, $d \equiv 0, 1\ (4)$, let $\mathcal{O}_d := \mathbb{Z}\left[\frac{\sqrt{d}+d}{2}\right]$, the quadratic order of discriminant d.

Thm (Gauss) $\xleftarrow{}$ he's proud of it, mentions it in the introduction of Disquisitiones

Let $n \in \mathbb{Z}_{\geq 1}$, then:

$$\#\left\{(x,y,z)\in\mathbb{Z}^3 : \begin{array}{l} x^2+y^2+z^2=n \\ \gcd(x,y,z)=1\end{array}\right\} = \begin{cases} 0 & \text{if } n\equiv 0,4,7\ (8) \\ 48\cdot\dfrac{\#\operatorname{Pic}(\mathcal{O}_{-n})}{\#(\mathcal{O}_{-n}^\times)} & \text{if } n\equiv 3\,(8) \\ 24\cdot\dfrac{\#\operatorname{Pic}(\mathcal{O}_{-4n})}{\#(\mathcal{O}_{-4n}^\times)} & \text{if } n\equiv 1,2\ (4)\end{cases}$$

$\Big(I \underset{\longmapsto}{\text{inv. }\mathcal{O}\text{-module}}\ x \longmapsto \frac{x\bar{x}}{N(I)} = \#(I/\mathcal{O}\cdot x)\Big)$

Rem. Gauss in terms of quadratic forms in 2 var's.

Reference article 291 (p. 336 – 339) of english Springer edition of Disquisitiones. There, the result comes after ≥ 200 pages of a detailed study of quadratic forms in 2 and 3 variables, not easy to read (I didn't) (Andrew Granville is working on an interpretation in modern terminology.)

Gauss's method, I think, sketched in a few lines (thanks Hendrik Lenstra). For $P \in \mathbb{Z}^3$ with $\|P\|^2 = n$, $(P^\perp, \langle\cdot,\cdot\rangle|_{P^\perp}, \text{orientation})$ is a pos. def. oriented symm. bil. form $/\mathbb{Z}$, rank 2, discr. n, primitive. Find out which ones can occur, and how often (the (M,b) s.t. $(M,b) \overset{\perp}{\oplus} (\mathbb{Z},n)$ admits an "overlattice" of index n; exactly one "genus", use a "Goursat lemma").

I find the result much nicer than the proof suggests.

Goal: to give a more direct proof, using symmetry, not quadr. forms: the action of SO_3. This is work in progress, I do explain the # of solutions & given the existence of one.

uses same idea, but adelic methods, not groupschemes / $\mathbb{Z}$.

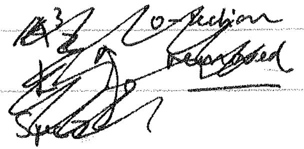
Rem. See also Shimura, Bull. AMS. 43, July 2006. He doesn't give a full proof, see p. 291, lines 7–8: "The proof is not so short, but conceptually straightforward, and at least not as painful as that of Gauss".

Rem. An alternative way is to use modular forms of weight 3/2 on $\Gamma_1(4)$:

$$\Big(\sum_{n\in\mathbb{Z}} q^{n^2}\Big)^3 = \sum_{n\geq 0} r_3(n)\cdot q^n.$$

(hence $n \equiv 1,2,3,5,6\ (8)$)

Assumptions. $n \in \mathbb{Z}_{\geq 1}$, $P \in \mathbb{Z}^3$ a primitive sol'n of $x^2+y^2+z^2=n$.



Def. $X := V(x^2+y^2+z^2-n) \rightarrowtail (\mathbb{A}^3_{\mathbb{Z}})$.
$S := \operatorname{Spec}\mathbb{Z}$

We want: $\# X(\mathbb{Z})^{\text{prim}}$, note: $P \in X(\mathbb{Z})^{\text{prim}}$.

GGX.

Let $G := SO_3$, grp. sch. / $\mathbb{Z}$, equations in Gl_3: $g^t\cdot g = 1$, $\det(g)=1$. Then

Let $H := G_P$, stab. of P in G: $\forall\, \mathbb{Z}\to A$: $H(A) = \{g\in G(A) : g\cdot P = P$ in ~~$X(A)$~~ $\mathbb{A}^3\}$ closed subgroupscheme of G. **Note:** ~~the~~ $H(\mathbb{R})$ = rotations with axis $\mathbb{R}\cdot P$.

We have: $H \rightarrowtail G \longrightarrow X$.
$g \longmapsto g\cdot P$

for some topology

$$\begin{tikzcd} & & & \operatorname{Pic}(..) \arrow[d, "\wr"] & \{1\} \arrow[d, equal] \\ H(S) \arrow[r, tail] & G(S) \arrow[r] & X(S) \arrow[r] & H^1(S,H) \arrow[r] & H^1(S,G) \end{tikzcd}$$

We would like to say: $X = G/H$ and: exact seq. of pointed sets.

But there are problems: / $\mathbb{F}_2$, if $P_{\mathbb{F}_2} = (1,1,1)$ then $H_{\mathbb{F}_2} = G_{\mathbb{F}_2}$,

/ $\mathbb{F}_p$, $p\mid n$: , remove the origin.

what topology to use?

Our solution: consider the sheaves on $S_{\text{Zar}} = \operatorname{Spec}\mathbb{Z}$ + Zariski topology (small site) induced by X, G, H, and denote them by the same symbols, and prove directly that we have the sequence.

Def. $\forall\, Q\in X(S)^{\text{prim}}$ let $G_{P,Q} \rightarrowtail G$: $\forall\, \mathbb{Z}\to A$, $G_{P,Q}(A) = \{g\in G(A) : g\cdot P = Q$ in $\mathbb{A}^3\}$

Prop. $\forall\, Q\in X(S)^{\text{prim}}$, $G_{P,Q}$ is a right H-torsor on S_{Zar}, that is, $\forall\, U\subset S$ open, $G_{P,Q}(U) \circlearrowleft H(U)$ is free and transitive, and $\forall\, p$ prime, $\exists\, U \ni \operatorname{Spec}\mathbb{F}_p$ s.t. $G_{P,Q}(U) \neq \emptyset$.

Proof. Elementary, use pairs of symmetries s_v, $\overset{\neq 0}{v} \in \mathbb{Q}^3$, $s_v : \mathbb{Q}^3 \to \mathbb{Q}^3$, $x \mapsto x - \frac{2\langle x,v\rangle}{\langle v,v\rangle} . v$, and control denominators.

Example: for $v \in \mathbb{Z}^3$ primitive, $4 \nmid \langle v,v\rangle$, hence $s_v : \mathbb{Z}_{(2)}^3 \longrightarrow \mathbb{Z}_{(2)}^3$. $\boxtimes$

(if $Q \neq P$, take $v = Q-P$, then $s_v : P \mapsto Q$. This works in $\mathbb{Q}^3$. To make it work at p, first choose a suitable w s.t. $\langle s_w P - Q, s_w P - Q\rangle \neq 0$ in $\mathbb{F}_p$.)

(to prove existence of such a w took me about 1 page). $\boxtimes$

(this implies that $\boxed{G(\mathbb{Z}_{(2)}) = G(\mathbb{Q}), \quad G(\mathbb{Z}) = G(\mathbb{Z}[1/2])}$

So we have $c : X(S)^{\mathrm{prim}} \longrightarrow H^1(S, H)$

Lemma. $c(Q_1) = c(Q_2) \iff \exists\, g \in G(S)$ s.t. $gQ_1 = Q_2$.

Proof. $\Leftarrow$: $g\cdot : G_{P,Q_1} \xrightarrow{\sim} G_{P,Q_2}$

$\Rightarrow$: Let $\varphi : G_{P,Q_1} \xrightarrow{\sim} G_{P,Q_2}$ isom. of H-torsors on S_{Zar}.

For $t \in G_{P,Q_1}(U)$, $(\varphi t) \cdot t^{-1} \in G_{Q_1,Q_2}(U)$, and indep. of t: $t' = th$, $(\varphi t')(t')^{-1} = (\varphi t) h h^{-1} t^{-1}$. Hence an elmt. in $G_{Q_1,Q_2}(S)$. $\boxtimes$

Lemma Let Z be a right H-torsor. Then $[Z] \in \mathrm{im}(c) \iff Z \otimes_H G \overset{\mathrm{def}}{=} (Z \times G)/H$ is trivial as G-torsor.

$(z,g) \cdot h = (zh, h^{-1}g)$.

Proof. $\Leftarrow$. Let $s \in (Z \otimes_H G)(S)$.

Locally, $s \leftarrow (z, g) \in (Z \times G)(U)$, unique up to $(z', g') = (zh, h^{-1}g)$, $h \in H(U)$. Gives $Q := g^{-1}P \in X(U)$, indep. of g, hence $Q \in X(S)$. Then $Z \to G_{P,Q}$, $z \mapsto g^{-1}$. $\boxtimes$ (we do not use $\Rightarrow$).

Lemma $H^1(S, G) = \{1\}$.

Proof. Note: $G = \underline{\mathrm{Aut}}(\mathbb{Z}^3, \langle\cdot,\cdot\rangle, d)$, $d : \mathbb{Z} \xrightarrow{\sim} \Lambda^3 \mathbb{Z}^3$.

$H^1(S, G)$ is the set of twists of $(\mathbb{Z}^3, \langle\cdot,\cdot\rangle, d)$ on S_{Zar}.

Let (M, b_M, d_M) be a twist. Then $(M_{\mathbb{Q}}, b_{M\mathbb{Q}}) \cong (\mathbb{Q}^3, \langle\cdot,\cdot\rangle)$ hence b_M pos. def.

Note: $\left\{ \begin{array}{l} M \cong \mathbb{Z}^3. \\ \mathrm{discr}(b_M) = 1, \ \mathrm{Vol}(M_{\mathbb{R}}/M) = 1. \end{array} \right.$ Minkowski: $\lambda_1 > 1 \Rightarrow \lambda_1 \geqslant \sqrt{2} \Rightarrow \frac{4}{3}\pi\left(\frac{1}{2}\sqrt{2}\right)^3 \leqslant 1$ ↯.

Hence $\exists\, m \in M$, $b(m,m) = 1$, $M = \mathbb{Z}\cdot m \oplus m^{\perp}$, etc. $\boxtimes$

We have: $G(S)\backslash X(S)^{\mathrm{prim}} \xrightarrow{\sim} H^1(S, H)$.

Last step: determine H. (but that will be enough)
I only know it over $\mathbb{Z}[1/2]$.

<u>Lemma</u> H does not depend on P: $\forall Q \in X(S)^{\mathrm{prim}}$, $G_Q = H$. (can. isom. of gr. sch., <u>not</u> with emb. in G)

<u>Proof.</u> Locally $Q = gP$, $g \in G(U)$.
Then $H = G_P \xrightarrow{\sim} G_Q$, $h \mapsto ghg^{-1}$, the isom. is indep. of $g' = gh'$ because H is <u>commutative</u>. $\boxtimes$

<u>Rem.</u> Can even determine H by descent.

<u>Def.</u> Let $T := \mathrm{Res}_{\mathbb{Z}[\frac{1}{2}, \sqrt{-n}]/\mathbb{Z}[1/2]} \mathbb{G}_m$: $T(A) = (A[u]/(u^2+n))^\times$
$= \{a_1 + a_2 u : a_1^2 + n a_2^2 \in A^\times\}$,

$T = \mathrm{Spec}\left(\mathbb{Z}[\frac{1}{2}][x,y]/(x^2+ny^2)\right)$. $\mathbb{G}_m \longrightarrow T$: $a \mapsto a + 0.u$

$N : T \longrightarrow \mathbb{G}_m$ $a_1 + a_2 u \mapsto a_1^2 + n a_2^2$.

<u>Prop.</u> We have $\mathbb{G}_m \rightarrowtail T \twoheadrightarrow H_{\mathbb{Z}[1/2]}$ exact sequence of gr. sch. / $\mathbb{Z}[1/2]$, for the Zariski topology (big site).

<u>**Proof.**</u> Over $\mathbb{Z}[\frac{1}{2n}, \sqrt{n}]$: $P' = (\sqrt{n}, 0, 0)$, $G_{P'} = (SO_2)_{\mathbb{Z}[\frac{1}{2n}, \sqrt{n}]}$,
1-dim. torus with char. grp. $\mathbb{Z}$ + quadr. char. $\mathbb{Q} \to \mathbb{Q}(i)$.

Descent to $\mathbb{Z}[\frac{1}{2n}]$: $\overline{P'} = (-\sqrt{n}, 0, 0) \rightsquigarrow H_{\mathbb{Z}[\frac{1}{2n}]} = (T_1)_{\mathbb{Z}[\frac{1}{2n}]} := \ker(N : —)$.

Main steps of the rest: <u>étale loc.</u>: x^2+ny^2 (it is primitive)

- $\underline{\mathrm{Aut}}(P^\perp)_{\mathbb{Z}[1/2]} = T_1$ $\quad T_1^0 \hookrightarrow T_1 \twoheadrightarrow \Phi = \bigoplus_{2 \neq p | n} i_{p,*} \mathbb{F}_2 : (\underline{a_1^2 + 0a_2^2 = 1}) / \mathbb{F}_p$.
- $H_{\mathbb{Z}[1/2]} \longrightarrow T_1$ via action on $P^\perp$,
  gives $H_{\mathbb{Z}[1/2]} \xrightarrow{\sim} T_1^0$.
- $T \twoheadrightarrow T_1^0$, $a_1 + a_2 u \mapsto \frac{a_1 + a_2 u}{a_1 - a_2 u}$, kernel $\mathbb{G}_m$. $\boxtimes$

Consequence: = for both numerator and denominator.

$$G(\mathbb{Z})\backslash X(\mathbb{Z})^{\text{prim}} \underset{\downarrow}{=} G(\mathbb{Z}[\tfrac{1}{2}])\backslash X(\mathbb{Z}[1/2])^{\text{prim}} \xrightarrow{\sim} H^1(\operatorname{Spec}\mathbb{Z}[1/2], H) = \operatorname{Pic}\left(\mathbb{Z}[\tfrac{1}{2}, \sqrt{-n}]\right)$$

and $H^2(\operatorname{Spec}\mathbb{Z}[\tfrac{1}{2}], \mathbb{G}_m) = 0$ bec. of dimension 1 and Zariski topology.

indeed: $H^1(\operatorname{Spec}\mathbb{Z}[1/2], G) = \{1\}$.

(each elmt. extends over $\mathbb{Z}$, and so is trivial)

cover $\mathbb{Z}$ with $\mathbb{Z} \to \mathbb{Z}[1/2] \times \mathbb{Z}_{(2)}$, "int." $\mathbb{Q}$.

$$M_{\mathbb{Q}} \xleftarrow[\sim]{\varphi} \mathbb{Q}^3 \supset \mathbb{Z}_{(2)}^3 \quad \text{take } M := M_{\mathbb{Z}[1/2]} \cap \varphi\,\mathbb{Z}_{(2)}^3$$

$b_M \qquad \langle\cdot,\cdot\rangle \qquad$ to extend $M_{\mathbb{Z}[1/2]}$.

We have proved:

if $X(\mathbb{Z})^{\text{prim}} \neq \emptyset$ then

$$\# X(\mathbb{Z})^{\text{prim}} = \frac{\# G(\mathbb{Z}[1/2])}{\# H(\mathbb{Z}[1/2])} \cdot \# \operatorname{Pic}\left(\mathbb{Z}[\tfrac{1}{2}, \sqrt{-n}]\right)$$

$$= \frac{24}{\boxed{\# \mathbb{Z}[\tfrac{1}{2}, \sqrt{-n}]^{\times,0}_{\text{tors}}}} \cdot \# \operatorname{Pic}\left(\mathbb{Z}[\tfrac{1}{2}, \sqrt{-n}]\right)$$

$$= \{ t = a_1 + a_2\sqrt{-n} \in \mathbb{Z}[\tfrac{1}{2}, \sqrt{-n}]^{\times} : \text{torsion}, \forall \underset{\neq 2}{p} \mid n : a_1 \equiv 1\ (p) \}$$

$$= \underline{\{1\} \text{ if } n > 3}$$

<u>About existence</u>: can follow Gauss, or: Hasse principle ⇝ $X(\mathbb{Q}) \neq \emptyset$, then a very funny argument (Cassels-Fröhlich exercise 4.11 p. 359) take in $\mathbb{Z}^3$ a point closest to our $\mathbb{Q}$-point in X, then chord method leads to a $\mathbb{Z}$-point on the sphere. (maybe only known to be primitive if n square-free).

Or also: (after Weil, in an article for Siegel) if one "knows" the formula then one can prove it by relating it to Θ^4: sum of 4 squares.