

(Bas Edixhoven).

Leiden, 2011/10/24.

1.

Gauss's theorem on sums of 3 squares via group schemes.

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

Theorem (Gauss) Let $n \in \mathbb{Z}_{>0}$ be square free. Then:

$$\#\{x \in \mathbb{Z}^3: x_1^2 + x_2^2 + x_3^2 = n\} = \begin{cases} 0 & \text{if } n \equiv 7 \pmod{8} \\ 48 \cdot \frac{\#\text{Pic}(O_{-n})}{\#\mathcal{O}_{-n}^\times} & \text{if } n \equiv 3 \pmod{8} \\ 24 \cdot \frac{\#\text{Pic}(O_{-4n})}{\#\mathcal{O}_{-4n}^\times} & \text{if } n \equiv 1, 2 \pmod{4}. \end{cases}$$

[page 336-337 article 291.

Reference: (page 339 of (english) Springer edition of *Disquisitiones*, art. 292.
There formulated in terms of equiv. classes of quadr. forms. Probably
Gauss even wrote it for the # of primitive solutions without
the assumption that n be square free. (We assume n square free.)
Anyway, I find his text hard to read. Goal of this talk:
understand why such a result is true, with all methods allowed.

I see two ways. 1: $\left(\sum_{m \in \mathbb{Z}} q^{m^2} \right)^3 = \sum_{n \geq 0} r_3(n) \cdot q^n \dots$ modular
forms of wt. $3/2$,

This is "well known" but I do not know it. on $\Gamma_1(4)$.

2. Using the action of SO_3 , group scheme / \mathbb{Z} . That's what we
will do. Shimura did this: *Bull. AMS*, 43, July 2006, but not really.
(see p. 291, lines 7-8). (

3. Follow Gauss: for $x \in \mathbb{Z}^3$ with $\|x\|^2 = n$, $(x^\perp, \text{inner pr., orientation})$
is a pos. def. symm. bil. form, of discr. n . Find out which ones
occur, and how often. (A lot of work..., 200 pages of *Disq.*)

Gauss considered the example $n = 770 = 2 \cdot 5 \cdot 7 \cdot 11$.

Then $\# \text{Pic}(\mathcal{O}_{-4n}) = 32$ $\text{Pic}(\mathcal{O}_{-4n}) \cong \mathbb{Z}/8\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$.

$770 = 27^2 + 5^2 + 4^2 = 25^2 + 9^2 + 8^2 = 25^2 + 12^2 + 1^2 = 24^2 + 13^2 + 5^2 =$
 $23^2 + 15^2 + 4^2 = 20^2 + 19^2 + 3^2 = 20^2 + 17^2 + 9^2 = 17^2 + 16^2 + 15^2,$

that is: $8 \cdot 6 \cdot 8$ ways, and $8 \cdot 6 \cdot 8 = 12 \cdot 32 = \frac{24}{2} \cdot 32$ indeed

But: $(27, 5, 4)^\perp \cong (24, 13, 5)^\perp \cong (20, 19, 3)^\perp \cong (20, 17, 9)^\perp : 19x^2 + 6xy + 41y^2$
and $(25, 9, 8)^\perp \cong (25, 12, 1)^\perp \cong (23, 15, 4)^\perp \cong (17, 16, 15)^\perp : 6x^2 + 4xy + 129y^2$

Now we start our proof, using group schemes.

But first, we need the existence of a solution ($n \equiv 7(8)$ is very easy).

Assume: n square free, ≥ 1 , $n \not\equiv 7(8)$.

Then: $\exists (x, y, z) \in \mathbb{Q}^3$ s.t. $x^2 + y^2 + z^2 = n$: use Hasse principle

(for $p \neq 2$: lift a smooth \mathbb{F}_p -point to a \mathbb{Z}_p -point, \mathbb{R} : clear

for $p=2$: $\{x^2 : x \in \mathbb{Z}_2^\times\} = 1 + 8\mathbb{Z}_2$, then easy).

From \mathbb{Q} -point to a \mathbb{Z} -point: (Cassels) do exercise 4.11 on p. 359

of Cassels-Fröhlich; take in \mathbb{Z}^3 a closest pt. to your \mathbb{Q} -point, then

chord method leads to a \mathbb{Z} -point of the sphere. on the sphere.

closed subscheme.

note: \mathbb{Z} -pt. primitive bec. n sq. free.

So: $X_n := V(x^2 + y^2 + z^2 - n) \xrightarrow{\iota} \mathbb{A}_{\mathbb{Z}}^3 - V(x, y, z)$

zero section.

and let $P \in X_n(\mathbb{Z})$ be a (primitive) solution.

Let $G := SO_3$, grp. scheme / \mathbb{Z} : $\forall \mathbb{Z} \rightarrow A: G(A) = \left\{ \begin{array}{l} g \in GL_3(A) : \\ \left(\begin{array}{l} \text{Equations for } SO_3: \|g_1\|^2 = 1, \|g_2\|^2 = 1, \langle g_1, g_2 \rangle = 0, \\ g_3 = g_1 \times g_2; \text{ 6 equations, complete int'n.} \end{array} \right) \left\{ \begin{array}{l} g^6 \cdot g = 1 \\ \det(g) = 1 \end{array} \right\} \end{array} \right.$

Let $H \rightarrow G$ (closed subgrp. scheme) be the stabilizer of P :

$\forall \mathbb{Z} \rightarrow A, H(A) = \{g \in G(A) : g \cdot P = P \text{ in } A^3\}$. Clearly given by equations, although we do not know P .

For every $Q \in X_n(\mathbb{Z})$ we have $G_{P,Q} \rightarrow G$ given by:
 $\forall \mathbb{Z} \rightarrow A, G_{P,Q}(A) = \{g \in G(A) : g \cdot P = Q\}$, the transporter.

Proposition. $\forall Q \in X_n(\mathbb{Z})$, $G_{P,Q}$ is an H -torsor on $(\text{Spec } \mathbb{Z})_{\text{Zar}}$
 that is: $\forall U \subset \text{Spec } \mathbb{Z}$ open: $H(U)$ acts freely and transitively on $G_{P,Q}(U)$,
 and $\forall p$ prime $\exists U \ni \text{Spec}(\mathbb{F}_p)$ s.t. $G_{P,Q}(U) \neq \emptyset$.

Proof. Use symmetries, for $\forall v \in \mathbb{Q}^3$: $s_v: \mathbb{Q}^3 \rightarrow \mathbb{Q}^3, x \mapsto x - \frac{\langle x, v \rangle}{\langle v, v \rangle} v$,
 and study the denominators. ... \square . reference: P. Gille + L. Moret-Bailly, "Actions algébriques de gr. alg.", See home page P. Gille.

This gives an "exact sequence":

$$G(\mathbb{Z}) \backslash X_n(\mathbb{Z}) \xrightarrow{c} H^1(\text{Spec}(\mathbb{Z})_{\text{Zar}}, H) \rightarrow H^1(\text{Spec}(\mathbb{Z})_{\text{Zar}}, G)$$

$$Q \longmapsto [G_{P,Q}], \quad \mathcal{J} \longmapsto \mathcal{J} \otimes_H G = (\mathcal{J} \times G) / H$$

Now $G = \text{Aut}(\mathbb{Z}^3, b, d)$, hence $H^1(\text{Spec}(\mathbb{Z})_{\text{Zar}}, G)$ is the set of isom. classes of (M, b_M, d_M) that are locally isom. to $(\mathbb{Z}^3, \frac{1}{2}d)$.
 For such (M, b_M, d_M) : $\text{discr}(b_M) = 1$, Minkowski: shortest non zero $m \in M$ has $b_M(m, m) = 1$, $M = \mathbb{Z} \oplus m^\perp$, etc. No nontriv. twists,
 $H^1(\text{Spec } \mathbb{Z}, G)$ is a one point set.

Bad things over \mathbb{F}_2 . 1. H need not be flat. Example: $n \equiv 3 \pmod{8}$,
 then $P = (1, 1, 1)$ in \mathbb{F}_2^3 , $H_{\mathbb{F}_2} = G_{\mathbb{F}_2}$, whereas $H_{\mathbb{Z}[\frac{1}{n}]} = \text{Aut}(P^\perp, b, d)$
 $(\mathbb{Z}[\frac{1}{n}]^3 = \mathbb{Z}[\frac{1}{n}] \cdot P \oplus P^\perp)$. 1-dim'l fibres.

Actually, this is not a big problem, one can work with H^b , the closure in H of H_α .

I think H is flat / \mathbb{Z}_2 , but

2. When $n \equiv 2 \pmod{4}$, then $H_{\mathbb{F}_2} \rightarrow \text{Aut}(P^\perp, b, d)_{\mathbb{F}_2}$ is not injective.
 $(P_{\mathbb{F}_2} = (1, 1, 0) \text{ in } \mathbb{F}_2^3)$ (kernel $\cong G_{\alpha, \mathbb{F}_2}$.)

$$(g, Q) \mapsto (gQ, Q)$$

Good things over $\mathbb{Z}[1/2]$. $G \times X_n \rightarrow X_n \times X_n$ is smooth & surjective, $H_{\mathbb{Z}[1/2]}$ is smooth, $G_{p, Q}$ is H -tensor on $\text{Spec}(\mathbb{Z}[1/2])_{\text{et}}$ (ad hoc arguments no longer necessary).

(P^\pm, b) is positive def., primitive, with discr. n . (even at z primitive, ...)

Let $\mathcal{O} :=$ ring of integers of $\mathbb{Q}(\sqrt{-n})$.

$$T := \text{Res}_{\mathcal{O}/\mathbb{Z}}(G_{m, \mathcal{O}}), \text{ Norm}: T \rightarrow G_{m, \mathbb{Z}}, T_1 := \ker(\text{Norm}).$$

$$T_1^\circ \subset T_1 \rightarrow \Phi, \Phi = \bigoplus_{i \neq j} \mathbb{F}_2, \text{ over } z \neq p|n.$$

Example: for $n \neq 3(8)$: $\mathcal{O} = \mathbb{Z}[\sqrt{-n}]$, $T_1 \sim x^2 + ny^2 = 1$, hence $(T_1)_{\mathbb{F}_p}$ not connected at $p|n, p \neq 2$.

Prop. $\underline{\text{Aut}}(P^\pm, b, d) \cong T_1$ over $\mathbb{Z}[1/2]$ (argument: etale bc.)
($(P^\pm, b) \cong (1, n)$)

$$H_{\mathbb{Z}[1/2]} \xrightarrow[\text{open imm.}]{} (T_1)_{\mathbb{Z}[1/2]} \text{ with image } (T_1^\circ)_{\mathbb{Z}[1/2]}$$

Other good things: $G(\mathbb{Z}[1/2]) = G(\mathbb{Z}), X_n(\mathbb{Z}[1/2]) = X_n(\mathbb{Z})$.
($v_2(x^2 + y^2 + z^2) \leq 1 + \min\{v_2(x), v_2(y), v_2(z)\}$) (x, y, z in \mathbb{Q}_2 , say).

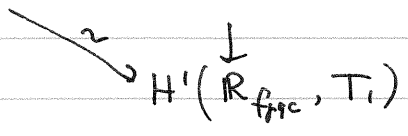
Prop. $G(\mathbb{Z}) \setminus X_n(\mathbb{Z}) = G(\mathbb{Z}[1/2]) \setminus X_n(\mathbb{Z}[1/2]) \xrightarrow{c} H^1(\mathbb{Z}[1/2]_{\text{et}}, T_1^\circ)$

$$\text{im}(c) = \ker \left(H^1(\mathbb{Z}[1/2]_{\text{et}}, T_1^\circ) \rightarrow H^1(\mathbb{Q}_2 \times \mathbb{R}_{\text{et}}, T_1^\circ) \right) \downarrow H^1(\mathbb{Z}[1/2]_{\text{et}}, G)$$

(Tool: $\{\text{affine schemes}/\mathbb{Z}\} \rightarrow \{\text{aff.}/(\mathbb{Z}_2 \times \mathbb{Z}[1/2]) + \text{glueing}/\mathbb{Q}_2\}$ is an equivalence of cat's; just do it for \mathbb{Z} -modules).
(well known for coherent modules, Artin, Algebraization of formal moduli II, thm. 2.6).

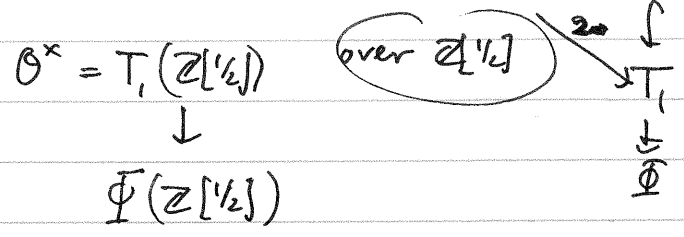
Relation with Pic(O). $T_1 \rightarrow T \rightarrow \text{Gm} / \mathbb{Z}$,

induces: $\mathbb{Z}^x \rightarrow H^1(\mathbb{Z}_{\text{Frac}}, T_1) \rightarrow \text{Pic}(O)$.



$$H^1(\mathbb{Z}, T_1) \xrightarrow{\text{isom. if } n \neq 3(8)} H^1(\mathbb{Z}[1/2], T_1) \twoheadrightarrow H^1(\mathbb{Q}_2, T_1) = \mathbb{F}_2 \quad n \equiv 3(8)$$

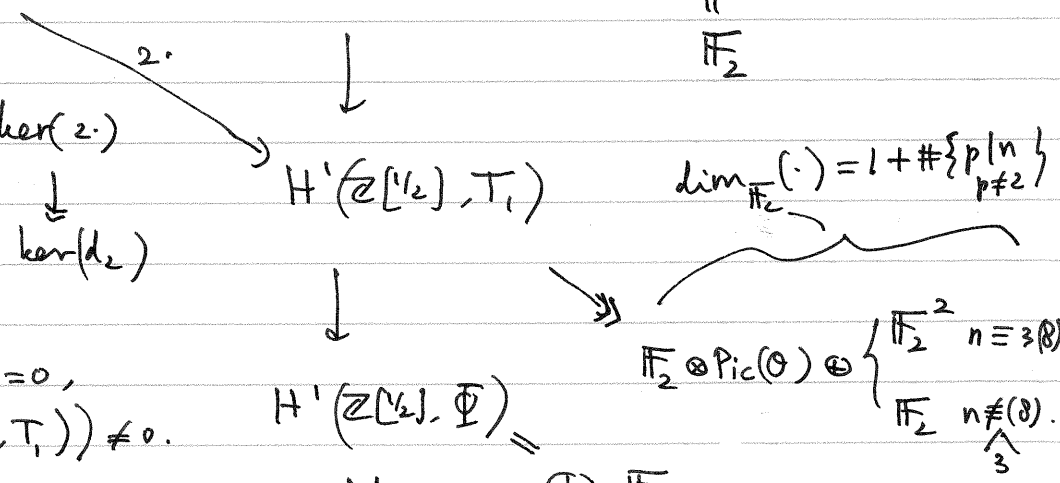
And now the diagram that finishes it all: $\mathbb{P}_2 \hookrightarrow T_1 \rightarrow T_1^0$



$$H^1(\mathbb{Z}[1/2], T_1) \longrightarrow H^1(\mathbb{Z}[1/2], T_1^0) \longrightarrow H^2(\mathbb{Z}[1/2], \mathbb{P}_2) \xrightarrow{d_2} \dots$$

\parallel
 \mathbb{F}_2

We have an exact sequence $\ker(d_1) \rightarrow \text{coker}(2) \rightarrow \dots$
Now look at the dimensions.



Conclusions: $d_1=0, d_2=0,$
 $(H^1(\mathbb{Z}[1/2], T_1^0) \rightarrow H^1(\mathbb{R}, T_1)) \neq 0.$

$$\# H^1(\mathbb{Z}[1/2], T_1^0) = \# \text{Pic}(O) \cdot 2 \cdot \begin{cases} 1 & \text{if } n \not\equiv 3(8) \\ 0 & \text{if } n \equiv 3(8) \end{cases} \cdot \begin{cases} 2 & \text{if } p|n \\ 1 & \text{if } \Phi = 0 \\ 1 & \text{if } \Phi \neq 0 \end{cases}$$