(Bas Edixhoven). Leiden, 2011/10/24.

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

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

Theorem (Gauss) Let $n \in \mathbb{Z}_{\geq 1}$ be square free. Then:

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

Reference: {page 336–337 article 291. / 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: $\left(\sum_{m \in \mathbb{Z}} q^{m^2}\right)^3 = \sum_{n \geq 0} r_3(n) \cdot q^n$ ... modular forms of wt. 3/2, on $\Gamma_1(4)$.
This is "well known" but I do not know it.

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 $\|x\|^2 = n$, ($x^\perp$, 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 $\#\mathrm{Pic}(\mathcal{O}_{-4n}) = 32$ $\quad \mathrm{Pic}(\mathcal{O}_{-4n}) \cong \mathbb{Z}/8\mathbb{Z} \times (\mathbb{Z}/2\mathbb{Z})^2$.

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

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 <u>existence of a solution</u> ($n \equiv 7\ (8)$ is very easy).

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

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. $\quad$ on the sphere.

<u>note</u>: $\mathbb{Z}$-pt. primitive bec. n sq. free.

closed subscheme.

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

zero section.

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

Let $G := SO_3$, grp. scheme $/\mathbb{Z}$: $\forall\, \mathbb{Z}\to A$: $G(A) = \left\{ g \in GL_3(A) : \begin{matrix} g^t\cdot g = 1 \\ \det(g) = 1 \end{matrix} \right\}$

(Equations for SO_3: $\|g_1\|^2 = 1$, $\|g_2\|^2 = 1$, $\langle g_1, g_2\rangle = 0$, $g_3 = g_1 \times g_2$; 6 equations, complete int'n.)

Let $H \rightarrowtail G$ (closed subgr. scheme) be the stabiliser of P:

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

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

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

<u>Proof</u>. Use symmetries, for $\overset{\circ}{\nparallel}\, v \in \mathbb{Q}^3$: $s_v : \mathbb{Q}^3 \to \mathbb{Q}^3$, $x \mapsto x - 2\frac{\langle x,v\rangle}{\langle v,v\rangle}\cdot v$,
and study the denominators. ... $\boxtimes$.

This gives an "exact sequence": reference: P. Gille + L. Moret-Bailly, "Actions algébriques de gr. alg.", See home page P. Gille.

$$G(\mathbb{Z})\backslash X_n(\mathbb{Z}) \xrightarrow{\ c\ } H^1\big(\operatorname{Spec}(\mathbb{Z})_{\mathrm{Zar}}, H\big) \longrightarrow H^1\big((\operatorname{Spec}\mathbb{Z})_{\mathrm{Zar}}, G\big)$$
$$Q \longmapsto [G_{P,Q}], \qquad T \longmapsto T \otimes_H G = (T \times G)/H$$

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

<u>Bad things over $\mathbb{F}_2$</u>. <u>1.</u> H need not be flat. Example: $n \equiv 3\ (8)$,
then $P = (1,1,1)$ in $\mathbb{F}_2^3$, $H_{\mathbb{F}_2} = G_{\mathbb{F}_2}$; whereas $H_{\mathbb{Z}[1/n]} = \mathrm{Aut}(P^\perp, b, d)$
$(\mathbb{Z}[1/n]^3 = \mathbb{Z}[1/n]\cdot P \overset{\perp}{\oplus} P^\perp)$. 1-dim'l fibres.
Actually, this is not a big problem, one can work with H^b, the closure in H of $H_{\mathbb{Q}}$.

<u>2.</u> When $n \equiv 2\ (4)$, then I think H is flat $/\mathbb{Z}_2$, but $H_{\mathbb{F}_2} \longrightarrow \mathrm{Aut}(P^\perp, b, d)_{\mathbb{F}_2}$ is <u>not injective</u>.
$(P_{\mathbb{F}_2} = (1,1,0)$ in $\mathbb{F}_2^3)$ (kernel $\cong \mathbb{G}_{a,\mathbb{F}_2}$.)

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

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

$(P^\perp, b)$ is positive def., primitive, with discr. n. (even at 2 primitive, ...)

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

$T := \mathrm{Res}_{\mathcal{O}/\mathbb{Z}}(\mathbb{G}_{m,\mathcal{O}})$, Norm: $T \longrightarrow \mathbb{G}_{m,\mathbb{Z}}$, $T_1 := \ker(\mathrm{Norm})$.

$T_1^\circ \hookrightarrow T_1 \twoheadrightarrow \Phi$, $\Phi = \bigoplus i_{p*}\mathbb{F}_2$, over $2 \neq p \mid n$.

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

Prop. $\mathrm{Aut}(P^\perp, b, d) \cong T_1$ over $\mathbb{Z}[1/2]$ (argument: etale loc. $(P^\perp, b) \cong \begin{pmatrix}1 & \\ & n\end{pmatrix}$)

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

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. $G(\mathbb{Z})\backslash X_n(\mathbb{Z}) = G(\mathbb{Z}[1/2])\backslash X_n(\mathbb{Z}[1/2]) \overset{c}{\hookrightarrow} H^1(\mathbb{Z}[1/2]_{et}, T_1^\circ)$

$$\downarrow$$

$$H^1(\mathbb{Z}[1/2]_{et}, G)$$

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

(Tool: $\{\text{affine schemes}/\mathbb{Z}\} \longrightarrow \{\text{aff.}/(\mathbb{Z}_2 \times \mathbb{Z}[1/2]) + \text{glueing}/\mathbb{Q}_2\}$ 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 $\mathrm{Pic}(\mathcal{O})$. $T_1 \rightarrowtail T \twoheadrightarrow \mathbb{G}_m \;/\mathbb{Z}$,

induces:
$$\begin{tikzcd} \mathbb{Z}^\times \arrow[r, tail] \arrow[dr, "\sim"'] & H^1(\mathbb{Z}_{fpqc}, T_1) \arrow[r, two heads] \arrow[d] & \mathrm{Pic}(\mathcal{O}) \\ & H^1(\mathbb{R}_{fpqc}, T_1) & \end{tikzcd}$$

$$\begin{tikzcd} H^1(\mathbb{Z}, T_1) \arrow[r, tail, "\text{isom. if } n \not\equiv 3(8)"'] & H^1(\mathbb{Z}[1/2], T_1) \arrow[r, two heads, shift left] & H^1(\mathbb{Q}_2, T_1) \arrow[l, shift left] \end{tikzcd} = \mathbb{F}_2 \quad n \equiv 3\,(8)$$

And now the diagram that finishes it all: $\mu_2 \rightarrowtail T_1 \twoheadrightarrow T_1^\circ$

$$\begin{tikzcd} & T_1^\circ \arrow[d, hook] \\ T_1 \arrow[ur, two heads] \arrow[r, "2\cdot"] & T_1 \arrow[d, two heads] \\ & \Phi \end{tikzcd}$$

over $\mathbb{Z}[1/2]$

$$\begin{tikzcd}[column sep=small] & \mathcal{O}^\times = T_1(\mathbb{Z}[1/2]) \arrow[d] & \\ & \Phi(\mathbb{Z}[1/2]) \arrow[d] & \\ H^1(\mathbb{Z}[1/2], T_1) \arrow[r] \arrow[dr, "2\cdot"] & H^1(\mathbb{Z}[1/2], T_1^\circ) \arrow[r] \arrow[d] & H^2(\mathbb{Z}[1/2], \mu_2) \arrow[r, "d_1"] & \cdots \\ & H^1(\mathbb{Z}[1/2], T_1) \arrow[d] \arrow[dr, two heads] & \mathbb{F}_2 \arrow[u, equal] \\ & H^1(\mathbb{Z}[1/2], \Phi) \arrow[d, "d_2"] & \mathbb{F}_2 \otimes \mathrm{Pic}(\mathcal{O}) \oplus \begin{cases} \mathbb{F}_2^2 & n \equiv 3(8) \\ \mathbb{F}_2 & n \not\equiv 3(8) \end{cases} \\ & {} & \end{tikzcd}$$

$$\dim_{\mathbb{F}_2}(\cdot) = 1 + \#\{p \mid n,\ p \neq 2\}$$

$$H^1(\mathbb{Z}[1/2], \Phi) = \bigoplus_{2 \neq p \mid n} \mathbb{F}_2$$

We have an exact sequence $\ker(d_1) \to \mathrm{coker}(2\cdot) \twoheadrightarrow \ker(d_2)$.

Now look at the dimensions.

Conclusions: $d_1 = 0$, $d_2 = 0$,

$\left(H^1(\mathbb{Z}[1/2], T_1^\circ) \to H^1(\mathbb{R}, T_1)\right) \neq 0$.

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