Bas Edixhoven, Universiteit Leiden.

Bordeaux, 2011/11/15.
45 minutes.

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

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

Thm (Gauss) Let $n \in \mathbb{Z}_{\geq 1}$, then:

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

Reference: pages 336–339 (article 291) of (english) Springer edition of Disquisitiones. There, this result comes after more than 200 pages of detailed study of quadratic forms in 2 & 3 variables. Those pages are not easy to read (I didn't). I think his method is as follows:

For (x,y,z) a solution, $((x,y,z)^\perp$, restr. of b (standard symm. bil. form on $\mathbb{Z}^3$), orientation$)$ is an oriented pos. def. symm. bil. form $/\mathbb{Z}$ of rank 2, primitive, discriminant n. Find out which ones occur (the (M,b) such that $(M,b) \overset{\perp}{\oplus} (\mathbb{Z},n)$ admits an "overlattice" of index n, (exactly one "genus"; use a "Goursat lemma")) and how often.
(Hendrik Lenstra explained this to me)
I find the result nicer looking than the proof suggests.

Goal: to give a "simpler" proof (better: more direct), using symmetry instead of quadratic forms: the action of SO_3, grp. scheme $/\mathbb{Z}$. This is work in progress. I have now a satisfactory proof for the number of solutions, given that there is one. But not (yet!) for that existence.

<u>Rem.</u> See also Shimura, Bull. AMS., 43, July 2006. He doesn't really give a full proof; see p. 291, lines 7–8.

<u>Rem.</u> An alternative way is to use modular forms of weight 3/2 on $\Gamma_1(4)$,
$$\Big(\sum_{n\in\mathbb{Z}} q^{n^2}\Big)^3 = \sum_{n\geq 0} r_3(n).q^n.$$

<u>Assumptions:</u> $n\in\mathbb{Z}_{\geq 1}$, $P\in\mathbb{Z}^3$ a primitive solution of $x^2+y^2+z^2=n$.

Let $X_n := V(x^2+y^2+z^2-n) \rightarrowtail \mathbb{A}^3_{\mathbb{Z}} - V(x,y,z)$ $\quad\left(\begin{array}{c}\mathbb{A}^3_{\mathbb{Z}}\\ \downarrow \uparrow 0\\ \operatorname{Spec}\mathbb{Z}\end{array}\right)$

We want to know $\# X_n(\mathbb{Z})$. Note: $P\in X_n(\mathbb{Z})$.

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

(Equations: $\|g_1\|^2=1$, $\|g_2\|^2=1$, $g_3 = g_1\times g_2$, $\langle g_1,g_2\rangle = 0$: 6 eqn's, <u>complete int'n</u>.)

Let $H\subset G$ be the stabiliser of P: $H(A) = \{g\in G(A) : g\cdot P = P \text{ in } A^3\}$, given by equations, closed subgrp. scheme of G.

<u>Our tool:</u> "short exact sequence" $H \rightarrowtail G \twoheadrightarrow X_n$, $g\longmapsto g\cdot P$, and the "exact cohomology sequence":
$$H(\mathbb{Z}) \rightarrowtail G(\mathbb{Z}) \longrightarrow X_n(\mathbb{Z}) \longrightarrow H^1(\operatorname{Spec}\mathbb{Z}, H) \longrightarrow H^1(\operatorname{Spec}\mathbb{Z}, G)$$

First question: what topology to use? $G\to X_n$ should be surjective as morphism of sheaves.

Answer: the Zariski topology is already strong enough!

<u>Def.</u> $\forall\, Q\in X_n(\mathbb{Z})$, let $G_{P,Q}\rightarrowtail G$ be given by:
$$G_{P,Q}(A) = \{g\in G(A) : g\cdot P = Q \text{ in } A^3\},$$ it is the "transporteur".

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

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

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

So, we really have an exact sequence of pointed sets:

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

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

$H^1((\mathrm{Spec}\,\mathbb{Z})_{\mathrm{Zar}}, G)$: $G = \underline{\mathrm{Aut}}(\mathbb{Z}^3, b, d)$, hence this H^1 is the set of isomorphism classes of (M, b_M, d_M) that are locally isomorphic to $(\mathbb{Z}^3, b, d)$. For such (M, b_M, d_M): $\mathrm{discr}(b_M) = 1$, and Minkowski shows that a shortest non-zero $m \in M$ has $b_M(m,m) = 1$, so $M = \mathbb{Z}\cdot m \oplus m^\perp$, etc. So this H^1 is a one point set.

<u>H, what is it!</u> Nice fact: as H is commutative, it does not depend on P: $\forall Q$, we have a given isom. from H to the stab. of Q.
I do not really know H, but I know $H_{\mathbb{Z}[1/2]}$, its restr. to $\mathrm{Spec}\,\mathbb{Z}[1/2]$.

Let $T := \mathrm{Res}_{\mathbb{Z}[1/2,\sqrt{-n}]/\mathbb{Z}[1/2]}\, \mathbb{G}_m$, so $T(A) = \left(A[u]/(u^2+n)\right)^\times$,
$T = \mathrm{Spec}\,\mathbb{Z}[x, y, 1/(x^2+ny^2)]$.

Then we have $\mathbb{G}_m \rightarrowtail T$, $A^\times \hookrightarrow (A[u]/(u^2+n))^\times$, and over $\mathbb{Z}[1/2]$ we have

$$\mathbb{G}_{m,\mathbb{Z}[1/2]} \rightarrowtail T_{\mathbb{Z}[1/2]} \twoheadrightarrow H_{\mathbb{Z}[1/2]}, \quad \text{\underline{exact} on } (\mathrm{Spec}\,\mathbb{Z}[1/2])_{\mathrm{Zar}}.$$

(this requires some work)

Consequence: $\mathbb{Z}[1/2]^\times \rightarrowtail \mathbb{Z}[1/2, \sqrt{-n}]^\times \twoheadrightarrow H(\mathbb{Z}[1/2])$

$$\mathrm{Pic}\,(\mathbb{Z}[1/2, \sqrt{-n}]) \xrightarrow{\sim} H^1(\mathrm{Spec}(\mathbb{Z}[1/2]), H)$$

$$\Big\uparrow 2 \quad c$$

$$G(\mathbb{Z}[1/2]) \backslash X_n(\mathbb{Z}[1/2])$$

$$\| \leftarrow \text{elementary.}$$

$$G(\mathbb{Z}) \backslash X_n(\mathbb{Z})$$

<u>Conclusion</u>: if $X_n(\mathbb{Z}) \neq \emptyset$, then

$$\# X_n(\mathbb{Z}) = \frac{\# G(\mathbb{Z}[1/2])}{\# H(\mathbb{Z}[1/2])} \cdot \# \mathrm{Pic}\ \mathbb{Z}[\tfrac{1}{2}, \sqrt{-n}]$$

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

where $\mathbb{Z}[\frac{1}{2}, \sqrt{-n}]^{\times,0}_{\mathrm{tors}} = \left\{ \begin{array}{l} t = t_0 + t_1\sqrt{-n} \in \mathbb{Z}[\frac{1}{2}, \sqrt{-n}]^\times, \text{ torsion,} \\ \text{s.t. } \forall \underset{\neq 2}{p} \mid n : \ t_0 \equiv 1 \ (p) \end{array} \right\}$

$\|$

$\{1\}$ if $n > 3$.