$p = x^2+y^2$ — a descent method

Prop. $p \equiv 1 \pmod 4$ prime $\Rightarrow$ $\exists\, x,y \in \mathbb{Z}$ $\quad x^2+y^2=p$

Pf: — " — $\Rightarrow \exists\, a,b \in \mathbb{Z}$ $\quad a^2+1 = pb$

Basic identity: $\boxed{(x^2+y^2)(x'^2+y'^2) = (xx'+yy')^2 + (-xy'+yx')^2}$

$(x+iy)(x'+iy') = (xx'+yy') + i(-xy'+yx')$

assume: $x^2+y^2 = pm$, $x,y \in \mathbb{Z}$, $p \nmid m$, $m>1$ (e.g. $x=a, y=1, m=b$)

construction of x'', y'' with $x''^2+y''^2 = pm' < pm$:

take $x', y' \in \mathbb{Z}$ such that $\left\{\begin{array}{l} x' \equiv x \pmod m \\ y' \equiv y \pmod m \\ |x'|, |y'| \le \frac{m}{2} \end{array}\right\} \Rightarrow x' \neq 0$ or $y' \neq 0$ (since $m^2 \nmid p$)

$\Rightarrow -xy'+yx' \equiv -xy+yx \equiv 0 \pmod m$, $xx'+yy' \equiv x^2+y^2 \equiv 0 \pmod m$

$\Rightarrow x'^2+y'^2 \equiv x^2+y^2 \equiv 0 \pmod m$, $x'^2+y'^2 = mm'$, $1 \le m' \le \frac{1}{m}\left(\left(\frac{m}{2}\right)^2+\left(\frac{m}{2}\right)^2\right) < m$

$\Rightarrow \underbrace{\frac{x^2+y^2}{m}\,\frac{x'^2+y'^2}{m}}_{pm'} = \left(\frac{xx'+yy'}{m}\right)^2 + \left(\frac{-xy'+yx'}{m}\right)^2 = x''^2+y''^2$ $\quad x'', y'' \in \mathbb{Z}$

Repeat until $m'=1 \Rightarrow$ Prop.

Exercise: p prime, $\left(\frac{\pm 2}{p}\right) = 1 \Rightarrow \exists\, x,y \in \mathbb{Z}$ $\quad x^2 \mp 2y^2 = p$ (by this method)

Thm. (Lagrange) $1 \le n \in \mathbb{Z} \Rightarrow \exists\, x,y,z,t \in \mathbb{Z}$ $\quad x^2+y^2+z^2+t^2 = n$.

Lemma $(x^2+y^2+z^2+t^2)(x'^2+y'^2+z'^2+t'^2) = (x''^2+y''^2+z''^2+t''^2)$,

$x'' = xx'+yy'+zz'+tt'$, $y'' = -xy'+yx'-zt'+tz'$, $z'' = -xz'+yt'+zx'-ty'$, $t'' = -xt'-yz'+zy'+tx'$

[Where does this formula come from? $q = x+iy+jz+kt \in \mathbb{H}$ quaternion ($ij=-ji=k$, $i^2=j^2=-1$), $\overline{q} = x-iy-jz-kt$, $N(q) = q\overline{q} = x^2+y^2+z^2+t^2$, $q\overline{q'} = q''$]

Enough to consider, therefore, $n=p$ prime. We know that $\exists\, a,b \in \mathbb{Z} \ni$ $a^2+b^2+1^2+0^2 = pm$. In general, if $x^2+y^2+z^2+t^2 = pm$ with $m>1$,

- if $2 \mid m$: can assume $x \equiv y \pmod 2$, $z \equiv t \pmod 2$ $\Rightarrow \left(\frac{x+y}{2}\right)^2+\left(\frac{x-y}{2}\right)^2+\left(\frac{z+t}{2}\right)^2+\left(\frac{z-t}{2}\right)^2 = p\frac{m}{2}$.
- if $2 \nmid m$: take $x', y', z', t' \in \mathbb{Z}$, $x' \equiv x \pmod m$, $y' \equiv y \pmod m$, $z' \equiv z \pmod m$, $t' \equiv t \pmod m$, $|x'|, |y'|, |z'|, |t'| < \frac{m}{2}$ ($\Rightarrow$ not all x', y', z', t' are 0, as $m^2 \nmid p$)

$\Rightarrow x'', y'', z'', t'' \equiv 0 \pmod m$, $x'^2+y'^2+z'^2+t'^2 = pmm'$

$pm' = \left(\frac{x''}{m}\right)^2+\left(\frac{y''}{m}\right)^2+\left(\frac{z''}{m}\right)^2+\left(\frac{t''}{m}\right)^2$, $\quad mm' < 4\left(\frac{m}{2}\right)^2 = m^2 \Rightarrow m' < m$.

Repeat until $m'=1 \Rightarrow$ Thm.

Geometric reformulation (Minkowski)

Ex: $p \equiv 1 \pmod 4$, $a^2+1 = pb$ $(a,b \in \mathbb{Z})$

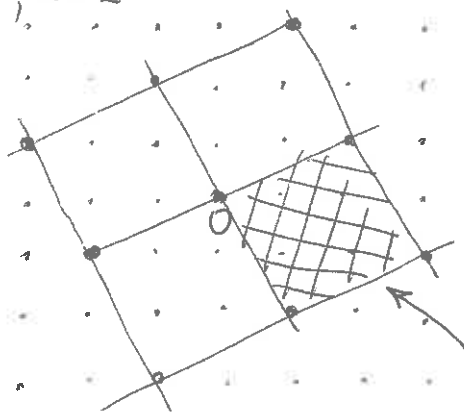
Goal: find $(x,y) \in \mathbb{Z}^2 \setminus \{(0,0)\}$ such that (1) $x \equiv ay \pmod p$ (2) $\|(x,y)\|^2 = x^2+y^2$ is small $(< 2p)$

(1) $\Rightarrow$ $x^2+y^2 \equiv (a^2+1)y^2 \equiv 0 \pmod p$

(2) $\Rightarrow 0 < x^2+y^2 < 2p \Rightarrow x^2+y^2 = p$

What is $L = \{(x,y) \in \mathbb{Z}^2 \mid x \equiv ay \pmod p\} \subset \mathbb{Z}^2$?

Ex: $p=5$, $a=2$



$$L = \ker\left(\alpha: \mathbb{Z}^2 \longrightarrow (\mathbb{Z}/p\mathbb{Z})^2 \longrightarrow \mathbb{Z}/p\mathbb{Z}\right)$$

$$(x,y) \longmapsto (x,y)\pmod p \longmapsto x - ay \pmod p$$

$\mathbb{Z}^2/L \xrightarrow{\sim} \mathrm{Im}(\alpha) = \mathbb{Z}/p\mathbb{Z}$

$L \subset \mathbb{Z}^2$ is a sublattice of index p

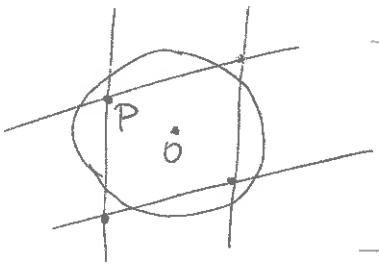
$\Downarrow$

$\underbrace{\mathrm{vol}(\mathbb{R}^2/L)}_{\text{volume of the fundamental domain}} = p\,\underbrace{\mathrm{vol}(\mathbb{R}^2/\mathbb{Z}^2)}_{1} = p$

Thm (Minkowski) (special case) $L \subset \mathbb{R}^2$ lattice, $2^2\,\mathrm{vol}(\mathbb{R}^2/L) \le \pi R^2 = \mathrm{vol}(\{P \in \mathbb{R}^2 \mid \|P\| \le R\})$

$\Downarrow$

$\exists\, P \in L \setminus \{0\}$, $\|P\| \le R$



Our case: minimal value of R satisfies

$$4p = \pi R^2$$

$$\Rightarrow \exists (x,y) \in L \setminus \{(0,0)\} \quad x^2+y^2 \le R^2 = \frac{4p}{\pi} < 2p$$

the general result is the following.

Thm (Minkowski) $L \subset V$ lattice, $V = \mathbb{R}$-vector space, $\dim_{\mathbb{R}}(V) = n > 0$, $0 \in K \subset V$ centrally symmetric and convex.

If $2^n\,\mathrm{vol}(V/L) < \mathrm{vol}(K) \Rightarrow \exists\, x \in L \cap K$, $x \neq 0$.

If K is compact, the same holds if $2^n\,\mathrm{vol}(V/L) = \mathrm{vol}(K)$.

Ex: p prime, $\left(\frac{\pm 2}{p}\right) = 1 \Rightarrow \exists a \in \mathbb{Z}$ $a^2 \equiv \pm 2 \pmod p$

$L = \{(x,y) \in \mathbb{Z}^2 \mid x \equiv ay \pmod p\} \ni (x,y) \Rightarrow x^2 \mp 2y^2 \equiv 0 \pmod p$

$K = K_r = \{(x,y) \in \mathbb{R}^2 \mid x^2+2y^2 \le r^2\}$, $\mathrm{vol}(K_r) = \frac{\pi}{\sqrt{2}} r^2$, $\mathrm{vol}(\mathbb{R}^2/L) = p$

If $4p = \frac{\pi}{\sqrt{2}} r^2 \Rightarrow \exists (x,y) \in (L \cap K_r) \setminus \{(0,0)\}$, $0 < x^2+2y^2 \le r^2 = \frac{4\sqrt{2}}{\pi} p < 2p$

$\Rightarrow 0 < |x^2 \mp 2y^2| < 2p$ divisible by p $\Rightarrow$ $\begin{cases} x^2-2y^2 = \pm p \Rightarrow \exists x',y' \; x'^2-2y'^2 = p \\ x^2+2y^2 = p \end{cases}$

$(1+\sqrt{2})(x+y\sqrt{2}) = (x+2y)+(x+y)\sqrt{2} \Rightarrow (x+2y)^2 - 2(x+y)^2 = -x^2+2y^2$

Invertible matrices

R = commutative ring

(1) $A \in M_n(R)$ ($n \times n$-matrix over R)

$\mathrm{adj}(A) \in M_n(R)$ the adjoint matrix $\quad \mathrm{adj}(A)_{ij} = (-1)^{i+j} \det(A \text{ without } \begin{matrix} i\text{-th column} \\ j\text{-th row} \end{matrix})$

$A \cdot \mathrm{adj}(A) = \mathrm{adj}(A) \cdot A = \det(A) \cdot I_n$ (Cramer's rule)

(2) $GL_n(R) = \{ A \in M_n(R) \mid \exists\, B \in M_n(R) \quad AB = I_n \}$ $\quad (\Rightarrow \det(A)\det(B) = 1$

$= \{ - " - \mid \det(A) \in R^* \}$ $\quad \det(A) \in R^*)$

$(B = \det(A)^{-1} \mathrm{adj}(A) \Rightarrow AB = BA = I_n)$

Subgroups of $\mathbb{Z}^n$

Prop. (Smith normal form of matrices over $\mathbb{Z}$) $\forall A \in M_{n\times m}(\mathbb{Z})\ \exists g \in GL_n(\mathbb{Z})\ \exists h \in GL_m(\mathbb{Z})$

$$gAh = A' = \begin{pmatrix} d_1 & & & & \\ & \ddots & & 0 & \\ & & d_r & & \\ & 0 & & \ddots & \\ & & & & 0 \end{pmatrix}$$

$r \geq 0,\ 1 \leq d_1 | d_2 | \cdots | d_r$ $\quad r \leq \min(m,n)$

uniquely determined by A

$d_1 \cdots d_k = \gcd(\text{ } k\times k \text{ minors of } A)$

Subgroups $Y \subset X = \mathbb{Z}^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \sum_{i=1}^n x_i e_i \mid x_1, \dots, x_n \in \mathbb{Z} \right\}$: Y is finitely generated

If $v_1, \dots, v_m \in \mathbb{Z}^n$ generate $Y = \mathbb{Z}v_1 + \cdots + \mathbb{Z}v_m$, consider (also follows from the proof)

the matrix $A = (v_1 | \cdots | v_m) \in M_{n\times m}(\mathbb{Z})$ and apply the above Proposition to it:

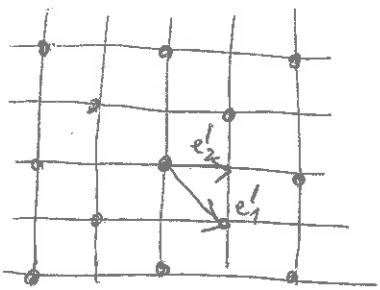
$A' = gAh = (gv_1 | \cdots | gv_m)h$. Action of h: replaces $\{v_j\}$ by another system of generators of Y

$- " -\ g$: change of basis of X

let $e_i' = g^{-1}e_i = g^{-1}\begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \leftarrow i\text{th place} \in \mathbb{Z}^n$. Then

$$\boxed{\begin{aligned} X &= \mathbb{Z}e_1' \oplus \cdots \oplus \mathbb{Z}e_n' & 1 \leq d_1 | d_2 | \cdots | d_r \\ Y &= \mathbb{Z}d_1e_1' \oplus \cdots \oplus \mathbb{Z}d_re_r' & (0 \leq r \leq n) \end{aligned}}$$

Ex:



$d_1 = 1$
$d_2 = 2$

Cor (1) $X/Y = \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_r\mathbb{Z} \oplus \mathbb{Z}^{n-r}$

(2) X/Y is finite $\Leftrightarrow r = n$; if true, then the index

$$(X:Y) = |X/Y| = \prod_{i=1}^n d_i = |\det(A')| = |\det(A)|$$

(if $m = n$)

(2') reformulation: if $m = n$, then

X/Y is finite $\Leftrightarrow \det(v_1 | \cdots | v_m) \neq 0$; if true, then

$$(X:Y) = |\ - " - \ |.$$

Exercise (subgroups of $\mathbb{Z}^2 = \binom{\mathbb{Z}}{\oplus}{\mathbb{Z}} = \left\{\binom{x}{y} \mid x,y \in \mathbb{Z}\right\}$ of a given index).

Recall that $\left(\mathbb{Z}^2 : \left(\mathbb{Z}\binom{a}{c} \oplus \mathbb{Z}\binom{b}{d}\right)\right) = \begin{cases} |ad-bc| & \text{if } ad-bc \neq 0 \\ \infty & \text{if } ad-bc = 0 \end{cases}$

Let $L \subset \mathbb{Z}^2$ be a subgroup such that $m = (\mathbb{Z}^2 : L) = |\mathbb{Z}^2/L| < \infty$.

(1) $L \cap \binom{\mathbb{Z}}{\oplus}{0} = \mathbb{Z}\binom{a}{0}$, for (a unique) $a \geq 1$.

(2) The projection of $L \subset \mathbb{Z}^2$ under $p_2 : \mathbb{Z}^2 \to \mathbb{Z}$, $p_2\left(\binom{x}{y}\right) = y$, satisfies $p_2(L) = d\mathbb{Z}$, for (a unique) $d \geq 1$

(3) $L = \mathbb{Z}\binom{a}{0} \oplus \mathbb{Z}\binom{b}{d}$, $a, d \geq 1$, $ad = m$, $0 \leq b < a$ (a, b, d unique).

(4) The number of subgroups $L \subset \mathbb{Z}^2$ of index $m \in \mathbb{N}_+$ is equal to

$$\sum_{ad=m} a = \sum_{a|m} a = \sigma_1(m)$$ (sum of the positive divisors of m)

Exercise. (1) Subgroups $L \subset \mathbb{Z}^n$ of index $(\mathbb{Z}^n : L) = m < \infty$ are given by

$$L = \mathbb{Z}\begin{pmatrix} a_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \oplus \mathbb{Z}\begin{pmatrix} b_{1,2} \\ a_2 \\ 0 \\ \vdots \\ 0 \end{pmatrix} \oplus \cdots \oplus \mathbb{Z}\begin{pmatrix} b_{1,n} \\ \vdots \\ b_{n-1,n} \\ a_n \end{pmatrix},$$

where $a_1, \dots, a_n \geq 1$, $a_1 \cdots a_n = m$, $0 \leq b_{i,j} < a_i$ $(1 \leq i < j \leq n)$

(2) The integers $\{a_i\}$ and $\{b_{i,j}\}$ satisfying ↗ are uniquely determined by L.

(3) The number of subgroups $L \subset \mathbb{Z}^n$ of index $m < \infty$ is equal to

$$c(n,m) = \sum_{\substack{a_1 \cdots a_n = m \\ a_i > 0}} a_1^{n-1} a_2^{n-2} \cdots a_{n-1}$$

---

(4) $$\sum_{m \geq 1} \frac{c(n,m)}{m^s} = \prod_{p \text{ prime}} \left(\sum_{r \geq 1} \frac{c(n,p^r)}{p^{rs}} \right)$$ $\left(\iff c(n, m_1 m_2) = c(n,m_1)c(n,m_2) \text{ if } (m_1, m_2) = 1\right)$

---

(5) p prime $\implies$ $$\sum_{r \geq 1} c(n,p^r) X^r = \frac{1}{(1-X)(1-pX)\cdots(1-p^{n-1}X)}$$

---

(6) $$\sum_{m \geq 1} \frac{c(n,m)}{m^s} = \zeta(s)\zeta(s-1)\cdots\zeta(s-(n-1))$$

Discrete subgroups of $\mathbb{R}^n$

$V = \mathbb{R}$-vector space, $\dim_{\mathbb{R}}(V) = n > 0 \quad (n < \infty)$

If $(\ ,\ ) : V \times V \to \mathbb{R}$ is a (positive definite) scalar product, then $\|x\| = \sqrt{(x,x)}$ is a norm on V and $d(x,y) = \|x-y\|$ a metric on V

Open balls: $B(x,r) = \{ y \in V \mid \|y-x\| < r \} \qquad x \in V,\ 0 < r \in \mathbb{R}$

If $(\ ,\ )'$ is another scalar product, then $\sqrt{(x,x)}' = \|x\|'$ satisfies $C_1\|\cdot\| \le \|\cdot\|' \le C_2\|\cdot\|$ for some constants $0 < C_1 < C_2 \Rightarrow$ the following notions do not depend on $(\ ,\ )$:

Recall: a subset $X \subset V$ is bounded if $\exists C > 0\ \forall x \in X\ \|x\| < C$;

open if $\forall x \in X\ \exists r > 0\ X \supset B(x,r)$; closed if $V \smallsetminus X$ is open;

discrete if ——" —— $X \cap B(x,r) = \{x\}$; compact if every open covering $\bigcup_\alpha U_\alpha \supset X$ contains a finite subcovering $U_{\alpha_1} \cup \dots \cup U_{\alpha_n} \supset X$.

Facts: (1) X is discrete and compact $\Leftrightarrow$ X is finite.

(2) X is compact $\Leftrightarrow$ X is closed and bounded.

Prop. A discrete subgroup $L \subset V = (V,+)$ is closed. [False for sets: $\{\frac{1}{n}\}_{n\ge 1} \subset \mathbb{R}$ discrete, not closed]

Pf: If not, $\exists\, a \in V \smallsetminus L$, $\{a_n\} \subset L$ $\lim\limits_{n\to\infty} a_n = a$.

$a \in V \smallsetminus L \Rightarrow$ after replacing a_n by a subsequence, we can assume that $m \ne n \Rightarrow a_m \ne a_n$.

$\forall \varepsilon > 0\ \exists\, c(\varepsilon)\ \forall\, m \ge c(\varepsilon)\ \|a_m - a\| < \frac{\varepsilon}{2}$ $\quad (\Rightarrow \forall\, n > m \ge c(\varepsilon)\ 0 < \|a_n - a_m\| < \varepsilon)$.

let $N_1 = c(1)$, $b_1 = a_{1+N_1} - a_{N_1}$; $0 < \|b_1\| < 1$, $b_1 \in L$

$N_2 = c(\|b_1\|)$, $b_2 = a_{1+N_2} - a_{N_2}$; $0 < \|b_2\| < \|b_1\|$, $b_2 \in L$ etc. $\Rightarrow \forall r > 0\ |B(0,r) \cap L| = \infty$ contradiction

---

Cor. A subgroup $L \subset V$ is discrete $\Leftrightarrow \forall X \subset V$ bounded $|X \cap L| < \infty$

$\Leftrightarrow \exists$ —— " —— .

Pf: L discrete subgroup, X compact $\Rightarrow$ $L \cap X$ closed, bounded $\Rightarrow$ compact, discrete $\Rightarrow$ finite

$L \subset V$ subgroup, X compact, $X \cap L$ finite $\Rightarrow \exists r > 0$ $L \cap B(0,r) = \{0\} \Rightarrow \forall a \in L$ $L \cap B(a,r) = \{a\}$

Def. A subgroup $L \subset V$ is a lattice if $L = \mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_n$, $\{v_i\}$ = basis of V $(n = \dim_{\mathbb{R}}(V))$

Ex: $\mathbb{Z}^n \subset \mathbb{R}^n$ is a lattice.

Thm. A (non-zero) subgroup $L \subset V$ is discrete $\Leftrightarrow$ it is a lattice in $\mathbb{R}L = \left\{ \sum_{i=1}^{N} t_i a_i \mid N \ge 0,\ t_i \in \mathbb{R},\ a_i \in L \right\} \Leftrightarrow L = \mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_m$, $v_i \in V$ linearly independent over $\mathbb{R}$ $(m = \dim_{\mathbb{R}} \mathbb{R}L \le n)$

$\Rightarrow V/L \simeq (\mathbb{R}/\mathbb{Z})^m \times \mathbb{R}^{n-m}$; L lattice $\Leftrightarrow V/L$ compact

---

Pf. Replace V by $\mathbb{R}L$. Assume $L \subset V$ is discrete and $\exists\, u_1, \dots, u_n \in L$ $(n = \dim_{\mathbb{R}} V)$ linearly independent over $\mathbb{R}$. Consider $L' = \mathbb{Z}u_1 \oplus \dots \oplus \mathbb{Z}u_n \subset L \subset V$ (discrete subgroup) and $A = \left\{ \sum_{i=1}^{n} t_i u_i \mid 0 \le t_i \le 1 \right\} \subset V$ (compact). Then $L \cap A = \{p_1, \dots, p_r\}$ is finite,

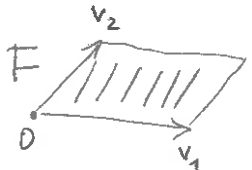
$L \subset V = L' + A \Rightarrow L \subset L' + (L \cap A) = \bigcup_{j=1}^{r} (L' + p_j) \Rightarrow d = (L : L') < \infty$. Theorem of Lagrange: $d(L/L') = 0 \Rightarrow dL \subset L' \Rightarrow L' \subset L \subset \frac{1}{d}L' = \bigoplus_{i=1}^{n} \mathbb{Z}\frac{u_i}{d}$, $\left(\frac{1}{d}L' : L\right) \le \left(\frac{1}{d}L' : L'\right) = d^n$

$\Rightarrow L = \mathbb{Z}v_1 \oplus \dots \oplus \mathbb{Z}v_n$ $\left(\overset{L' \subset L}{\Rightarrow} v_1, \dots, v_n \text{ basis of } V\right) \Rightarrow$ L lattice in V.

Volume, covolume

Fix a volume element on V: e.g., fix a basis of $V \Rightarrow$ isomorphism $V \xrightarrow{\sim} \mathbb{R}^n$ of vector spaces; we can then take $C\cdot$ the Lebesgue measure on $\mathbb{R}^n$ (for a fixed $C>0$) and transport it to V. We get a measure $\mu = \mu_{vol}$ on reasonable subsets $X \subset V$. It is translation invariant: $\mu(a+X) = \mu(X)$ $(a \in V,\ X \subset V)$ and unique up to multiplication by a constant $c>0$.

$L \subset V$ lattice: choose a basis $L = \mathbb{Z}v_1 \oplus \cdots \oplus \mathbb{Z}v_n$ and consider the fundamental domain $F = \left\{ \sum_{i=1}^n \lambda_i v_i \;\middle|\; 0 \le \lambda_i < 1 \right\}$. Then



$$V = \coprod_{a \in L} (a+F)$$ disjoint union

The covolume of L is $\mu(V/L) = \mu(F)$

For example, if $V = \mathbb{R}^n$, $\mu = dx_1 \cdots dx_n$, then $\mu(V/L) = \left| \det \underbrace{\left(v_1 \middle| \cdots \middle| v_n\right)}_{A} \right|$

This is well-defined: another basis $\{v_i'\}$ of L gives a matrix $A' = \left(v_1' \middle| \cdots \middle| v_n'\right) = Ah$ for some $h \in GL_n(\mathbb{Z}) \Rightarrow |\det(A')| = |\det(A)|$

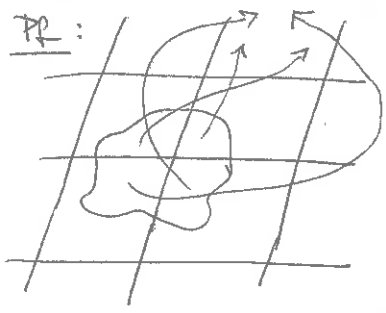
Equivalently, $\mu(\mathbb{R}^n/L) = \sqrt{\det({}^tAA)}$, ${}^tAA$ = the Gram matrix of scalar products $(x,y) = \sum_{i=1}^n x_i y_i$ $\quad ({}^tAA)_{ij} = {}^t v_i v_j = (v_i, v_j)$

Recall: (1) A subset $X \subset V$ is centrally symmetric if $0 \in X$ and $(x \in X \Rightarrow -x \in X)$

(2) — " — is convex if $x, y \in X \Rightarrow \forall \lambda\ 0 \le \lambda \le 1\ \ \lambda x + (1-\lambda) y \in X$

Lemma (Blichfeldt) If $L \subset V$ is a lattice and $U \subset V$ is measurable, $\mu(U) > \mu(V/L) \Rightarrow \exists\ x, y \in U,\ 0 \ne x - y \in L$.

Pf:



$$U = \coprod_{a \in L} \underbrace{U \cap (a+F)}_{a + ((-a+U) \cap F)}$$

F = fundamental domain

If all $(-a+U) \cap F \subset F$ were disjoint, then

$$\underbrace{\mu(F)}_{\mu(V/L)} \ge \sum_{a \in L} \mu((-a+U) \cap F) = \sum_{a \in L} \mu(U \cap (a+F)) = \mu(U)$$

contradiction. So $\exists\ a, b \in L\ (a \ne b),\ \exists\ x, y \in U \quad -a+x = -b+y \in F$

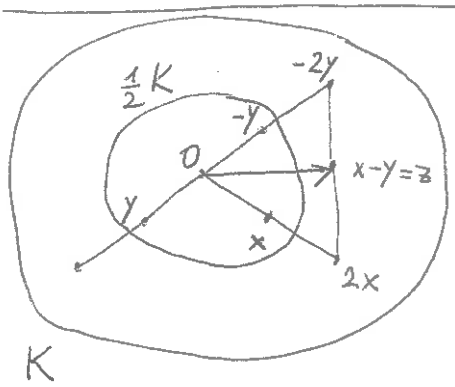
$\Rightarrow \quad 0 \ne x - y = a - b \in L$.

Exercise: If $k \in \mathbb{Z}_{\ge 1}$, $\mu(U) > k\,\mu(V/L) \Rightarrow x_0, \ldots, x_k \in U$ distinct

$\forall\ 0 \le i < j \le k \quad x_i - x_j \in L$.

Minkowski's Theorem

Thm (Minkowski) $L \subset V$ lattice, $n = \dim_{\mathbb{R}}(V) \geq 1$, $K \subset V$ centrally symmetric convex.
If $\mu(K) > 2^n \mu(V/L)$ (or if $\mu(K) \geq 2^n \mu(V/L)$ and K is compact), then
$\exists \quad 0 \neq z \in L \cap K$.



Pf: If $\mu(K) > 2^n \mu(V/L)$

$\Downarrow$

$\mu(\frac{1}{2}K) > \mu(V/L)$

$\Downarrow$ Blichfeldt

$\exists\, x, y \in \frac{1}{2}K$, $0 \neq \underbrace{x-y}_{z} \in L$

But $z = x - y = \frac{1}{2}(2x + (-2y)) \in K$, since K is convex

$2x \in K$, $2y \in K \Rightarrow -2y \in K$ (K centrally symmetric).

If K compact and $\mu(K) = 2^n \mu(V/L)$: $\forall i \geq 1 \quad \exists\, z_i \in \underbrace{(L \cap (1+\frac{1}{i})K) \setminus \{0\}}_{\text{finite}} \subset \underbrace{2K}_{\text{bounded}}$

One element z appears infinitely many times

$\Rightarrow 0 \neq z \in L \cap \bigcap_{i \geq 1} (1+\frac{1}{i})K$

the closure of K $= K$

Rmk (Successive minima) If K is, in addition, compact, Minkowski defined

$\lambda_1 \leq \lambda_2 \leq \cdots \leq \lambda_n$ by $\lambda_i = \inf \{ t > 0 \mid L \cap tK$ contains i elements linearly independent over $\mathbb{R} \}$

$(= \min \{ \text{---} \text{---} (\cdots) \})$

and proved that $\lambda_1 \cdots \lambda_n \mu(K) \leq 2^n \mu(V/L)$

(the above thm implies that $\lambda_1 \leq t$ if $\mu(tK) = 2^n \mu(V/L) \Rightarrow \lambda_1^n \mu(K) \leq 2^n \mu(V/L)$)

Ex: (1) $x^2+y^2=m$. Assume that $m \in \mathbb{Z}$, $m \geq 1$ and that $\exists r \in \mathbb{Z} \quad r^2+1 \equiv 0 \pmod m$.

Let $V = \mathbb{R}^2$, $\mu = dx_1 dx_2$, $L = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{Z}^2 \mid x \equiv ry \pmod m \right\} = \mathbb{Z}\begin{pmatrix} m \\ 0 \end{pmatrix} \oplus \mathbb{Z}\begin{pmatrix} r \\ 1 \end{pmatrix}$

$\mathrm{vol}(V/L) = \mu(\mathbb{R}^2/L) = \left| \det \begin{pmatrix} m & r \\ 0 & 1 \end{pmatrix} \right| = m$, $\begin{pmatrix} x \\ y \end{pmatrix} \in L \Rightarrow x^2+y^2 \equiv y^2(r^2+1) \equiv 0 \pmod m$

Let $K = K_R = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} \in \mathbb{R}^2 \mid x^2+y^2 \leq R^2 \right\}$, $\mu(K) = \pi R^2$.

If $\pi R^2 = 4m \underset{\text{Minkowski}}{\Longrightarrow} \exists \begin{pmatrix} x \\ y \end{pmatrix} \in L \setminus \{(0)\}$, $0 < x^2+y^2 \leq R^2 = \frac{4}{\pi} m < 2m \Rightarrow x^2+y^2 = m$.

---

(2) $x^2+y^2+z^2+t^2=m$. Assume that $m \in \mathbb{Z}$, $m \geq 1$ and that $\exists r, s \in \mathbb{Z} \quad r^2+s^2+1 \equiv 0 \pmod m$ (*)

$V = \mathbb{R}^4$, $\mu = dx_1 dx_2 dx_3 dx_4$, $L = \left\{ \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} \in \mathbb{Z}^4 \;\middle|\; \begin{array}{l} x \equiv rz+st \pmod m \\ y \equiv sz-rt \pmod m \end{array} \right\} = \mathbb{Z}\begin{pmatrix} m \\ 0 \\ 0 \\ 0 \end{pmatrix} \oplus \mathbb{Z}\begin{pmatrix} 0 \\ m \\ 0 \\ 0 \end{pmatrix} \oplus \mathbb{Z}\begin{pmatrix} r \\ s \\ 1 \\ 0 \end{pmatrix} \oplus \mathbb{Z}\begin{pmatrix} s \\ -r \\ 0 \\ 1 \end{pmatrix}$

$\mu(V/L) = m^2$

$K = K_R = \left\{ \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} \in \mathbb{R}^4 \mid x^2+y^2+z^2+t^2 \leq R^2 \right\}$, $\mu(K) = R^4 \frac{\pi^{4/2}}{\Gamma(4/2+1)} = \frac{\pi^2 R^4}{2}$

If $\frac{\pi^2 R^4}{2} = 2^4 m^2 \underset{\text{Minkowski}}{\Longrightarrow} \exists\, 0 \neq \begin{pmatrix} x \\ y \\ z \\ t \end{pmatrix} \in L \cap K \Rightarrow 0 < \underbrace{x^2+y^2+z^2+t^2}_{\equiv 0 \pmod m} \leq R^2 = \frac{2^2\sqrt{2}}{\pi} m < 2m$

$\Rightarrow x^2+y^2+z^2+t^2 = m$

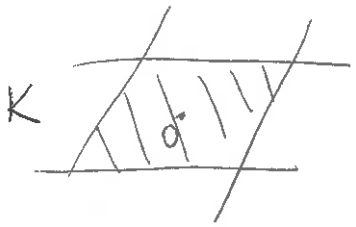
$\Rightarrow$ Every $m \geq 1$ is a sum of 4 squares (Lagrange)

Exercise: (*) is satisfied if $m = 2^\lambda m_0$, $2 \nmid m_0$, $\lambda \in \{0, 1\}$

Example: Minkowski's thm for parallelopipeds

Prop. Let $A = (A_{ij})_{1 \le i,j \le n} \in GL_n(\mathbb{R})$. If $t_1, \dots, t_n > 0$ are real numbers such that $t_1 \cdots t_n \ge |\det(A)|$, then there exist integers $x_1, \dots, x_n \in \mathbb{Z}$ (not all equal to zero) such that $\forall i = 1, \dots, n \quad \left| \sum_{j=1}^{n} A_{ij} x_j \right| \le t_i$.

Pf: $K = \{(x_1, \dots, x_n) \in \mathbb{R}^n \mid \forall i = 1, \dots, n \quad \left| \sum_{j=1}^{n} A_{ij} x_j \right| \le t_i\}$



is a compact centrally symmetric convex subset of $\mathbb{R}^n$ with volume $\mu(K) = \dfrac{2^n \prod_{1}^{n} t_i}{|\det(A)|}$.

Exercise. Show that, under the same assumptions, $\forall i_0 \in \{1, \dots, n\}$ there exist integers $x_1, \dots, x_n \in \mathbb{Z}$ (not all equal to zero) such that $\forall i = 1, \dots, n$

$$\left| \sum_{j=1}^{n} A_{ij} x_j \right| \begin{cases} \le t_i & \text{if } i = i_0 \\ < t_i & \text{if } i \ne i_0. \end{cases}$$

[**Hint:** consider, for all $k = 1, 2, \dots$, $t_i' = \begin{cases} t_i & i = i_0 \\ \left(1 + \frac{1}{k}\right) t_i & i \ne i_0 \end{cases}$.]

Volume calculations

(1) **Γ-function**: $\Gamma(a) = \int_0^\infty x^a e^{-x} \frac{dx}{x} = \int_0^\infty x^{a-1} e^{-x}\, dx$ $\quad (a>0)$

$(x^a e^{-x})' = a x^{a-1} e^{-x} - x^a e^{-x} \Rightarrow \boxed{\Gamma(a+1) = a\Gamma(a)}$; $\boxed{\Gamma(1)=1}$ $(\Rightarrow \Gamma(n+1)=n!$ $\forall n \in \mathbb{Z}_{\geq 0} = \mathbb{N})$

(2) **Beta-function**: $B(a,b) = \int_0^1 u^{a-1}(1-u)^{b-1}\, du$ $\quad (a,b>0)$ $= \int_0^\infty \frac{z^{a-1} dz}{(1+z)^{a+b}}$ $\quad \left(u = \frac{z}{1+z}\right)$

$\Gamma(a)\Gamma(b) = \int_{x,y\geq 0} x^a y^b e^{-(x+y)} \frac{dx}{x}\frac{dy}{y} \overset{(x=yz)}{=} \int_{y,z\geq 0} y^{a+b} z^a e^{-y(1+z)} \frac{dy}{y}\frac{dz}{z} \overset{t=y(1+z)}{=} \underbrace{\left(\int_0^\infty t^{a+b} e^{-t} \frac{dt}{t}\right)}_{\Gamma(a+b)} \underbrace{\left(\int_0^\infty \frac{z^{a-1} dz}{(1+z)^{a+b}}\right)}_{B(a,b)}$

$\Rightarrow \boxed{B(a,b) = \frac{\Gamma(a)\Gamma(b)}{\Gamma(a+b)}}$

(3) $I(b_1,\dots,b_n) = \int_{x_1,\dots,x_n\geq 0,\ x_1+\dots+x_n\leq 1} x_1^{b_1}\cdots x_n^{b_n} \frac{dx_1}{x_1}\cdots\frac{dx_n}{x_n} = \int_{x_i\geq 0,\ \sum x_i\leq 1} x_1^{b_1-1}\cdots x_n^{b_n-1}\, dx_1\cdots dx_n$ $\quad (b_i>0)$ $\quad \boxed{I(b_1) = \frac{1}{b_1}}$

$I'(b_1,\dots,b_n) = \int_{y_1,\dots,y_{n-1}\geq 0,\ y_1+\dots+y_{n-1}\leq 1} y_1^{b_1-1}\cdots y_{n-1}^{b_{n-1}-1}(1-y_1-\dots-y_{n-1})^{b_n-1} dy_1\cdots dy_{n-1}$ $\quad \boxed{I'(b_1,b_2) = B(b_1,b_2)}$

(4) $x_i = t y_i$ $(i<n)$, $x_n = t(1-y_1-\dots-y_{n-1})$, $t = \sum_{i=1}^n x_i$, $dx_1\cdots dx_n = t^{n-1}\, dt\, dy_1\cdots dy_{n-1}$

$I(b_1,\dots,b_n) = \int_{0\leq t\leq 1} \int_{y_1,\dots,y_{n-1}\geq 0,\ y_1+\dots+y_{n-1}\leq 1} t^{n-1} t^{(b_1-1)+\dots+(b_n-1)} y_1^{b_1-1}\cdots y_{n-1}^{b_{n-1}-1}(1-y_1-\dots-y_{n-1})^{b_n-1}\, dt\, dy_1\cdots dy_{n-1}$

$= I(b_1+\dots+b_n)\, I'(b_1,\dots,b_n) = \frac{I'(b_1,\dots,b_n)}{b_1+\dots+b_n}$

(5) **n=2**: $I(b_1,b_2) = \frac{B(b_1,b_2)}{b_1+b_2} = \frac{\Gamma(b_1)\Gamma(b_2)}{\Gamma(b_1+b_2+1)}$

(6) **Induction on n**: $I(b_1,\dots,b_n) = \frac{\Gamma(b_1)\cdots\Gamma(b_n)}{\Gamma(b_1+\dots+b_n+1)}$, $I'(b_1,\dots,b_n) = \frac{\Gamma(b_1)\cdots\Gamma(b_n)}{\Gamma(b_1+\dots+b_n)}$

(7) $\int_{\substack{x_1,\dots,x_n\geq 0 \\ \left(\frac{x_1}{a_1}\right)^{\rho_1}+\dots+\left(\frac{x_n}{a_n}\right)^{\rho_n}\leq 1}} x_1^{p_1}\cdots x_n^{p_n} \frac{dx_1}{x_1}\cdots\frac{dx_n}{x_n} = \left(\prod_i \frac{a_i^{p_i}}{\rho_i}\right) \int_{\substack{y_1,\dots,y_n\geq 0 \\ y_1+\dots+y_n\leq 1}} y_1^{p_1/\rho_1}\cdots y_n^{p_n/\rho_n} \frac{dy_1}{y_1}\cdots\frac{dy_n}{y_n} = \frac{\prod_{i=1}^n (a_i^{p_i}\Gamma(\frac{p_i}{\rho_i})/\rho_i)}{\Gamma(\frac{p_1}{\rho_1}+\dots+\frac{p_n}{\rho_n}+1)}$

$(\lambda_i = a_i y_i^{1/\rho_i}$, $\frac{dx_i}{x_i} = \frac{1}{\rho_i}\frac{dy_i}{y_i})$

$J(\underline{a};\underline{p};\underline{\rho})$ $\qquad I(\frac{p_1}{\rho_1},\dots,\frac{p_n}{\rho_n})$ $\qquad (a_i,p_i,\rho_i>0)$

(8) $\mathrm{vol}\left\{x\in\mathbb{R}^n \,\middle|\, \sum_{i=1}^n |x_i/a_i|^{\rho_i} \leq 1\right\} = \left(\prod_{i=1}^n 2a_i\Gamma(\frac{1}{\rho_i})/\rho_i\right) / \Gamma\left(\frac{1}{\rho_1}+\dots+\frac{1}{\rho_n}+1\right)$ $\quad (a_i,\rho_i>0)$

(9) $\mathrm{vol}\left\{x\in\mathbb{R}^n \,\middle|\, \sum_{i=1}^n |x_i|^p \leq r^p\right\} = r^n \left(2\Gamma(\frac{1}{p})/p\right)^n / \Gamma(\frac{n}{p}+1)$ $\quad (p,r>0)$

(10) $\mathrm{vol}\left\{x\in\mathbb{R}^n \,\middle|\, \sum_{i=1}^n |x_i|^2 \leq r^2\right\} = r^n \Gamma(\frac{1}{2})^n / \Gamma(\frac{n}{2}+1)$ $\quad \boxed{n=2 \Rightarrow \Gamma(\frac{1}{2}) = \sqrt{\pi}}$ $\quad (r>0)$

(11) $\mathrm{vol}\left\{(x,z)\in\mathbb{R}^s\times\mathbb{C}^t \,\middle|\, \sum_1^s |x_j| + 2\sum_1^t |z_k| \leq R\right\} = 2^s(2\pi)^t \int_{\substack{x_j,r_k\geq 0 \\ \sum x_j + 2\sum r_k \leq R}} r_1\cdots r_k\, dx_1\cdots dx_j\, dr_1\cdots dr_k =$ $\quad \boxed{z_k = r_k e^{i\theta_k},\ 0\leq\theta_k\leq 2\pi}$

$= 2^s(2\pi)^t \underbrace{J\left(\mathbb{R}^s \oint (\mathbb{R}/2)^t ; \underline{1}^s \underline{2}^t ; \underline{1}^{s+t}\right)}_{R^s\left(\frac{R}{2}\right)^{2t} I(\underbrace{1,\dots,1}_{s},\underbrace{2,\dots,2}_{t})} = 2^s\left(\frac{\pi}{2}\right)^t R^{s+2t} \frac{\Gamma(1)^s\Gamma(2)^t}{\Gamma(s+2t+1)} = 2^s\left(\frac{\pi}{2}\right)^t \frac{R^{s+2t}}{(s+2t)!}$

Equation $ax^2+by^2+cz^2=0$

Theorem (Legendre) Assume: $a,b,c \in \mathbb{Z}\setminus\{0\}$ square-free, $\gcd(a,b)=\gcd(b,c)=\gcd(c,a)=1$,
$\exists x,y,z \in \mathbb{Z}$ $x^2 \equiv -bc \pmod a$, $y^2 \equiv -ca \pmod b$, $z^2 \equiv -ab \pmod c$, $a>0>c$
$\Rightarrow$ $\exists x,y,z \in \mathbb{Z}^3\setminus\{(0,0,0)\}$ $ax^2+by^2+cz^2=0$.

Variant: Assume $a,b,c \in \mathbb{Z}\setminus\{0\}$, abc square-free; write $abc = 2^\lambda p_1 \cdots p_r$, $\lambda \in \{0,1\}$, $p_i \neq 2$ prime. If $\forall p=p_i$ $\exists$ solution of $ax_p^2+by_p^2+cz_p^2 \equiv 0 \pmod p$ with $\gcd(x_p,y_p,z_p,p)=1$
(no assumption about positivity/negativity) and for $p=2$ $ax_2^2+by_2^2+cz_2^2 \equiv 0 \pmod{2^{2+\lambda}}$ — " —),
then $\exists x,y,z \in \mathbb{Z}^3\setminus\{(0,0,0)\}$ $\underbrace{ax^2+by^2+cz^2}_{f(x,y,z)}=0$.

Pf: **Step 1**. We construct linear forms $l_i = l_i(x,y,z)$ $(1 \le i \le r)$, l', l'' with coeff. in $\mathbb{Z}$ such that the congruences

(*) $l_i \equiv 0 \pmod{p_i}$ $(1 \le i \le r)$, $l' \equiv 0 \pmod{2^{\lambda+1}}$, $l'' \equiv 0 \pmod 2$

imply $f(x,y,z) \equiv 0 \pmod{4|abc|}$

$p=p_i$: say, $p \mid c \Rightarrow p \nmid ab \Rightarrow \exists r_p \in \mathbb{Z}$ $ar_p^2+b \equiv 0 \pmod p$; take $l_i(x,y,z) = x - r_p y$

$p=2$: if $\lambda=0$: $2 \nmid abc$; we cannot have $a \equiv b \equiv c \pmod 4$; after permuting them, we can assume $a \equiv -b \pmod 4$; take $l'(x,y,z) = x-y$, $l''(x,y,z) = z$

if $\lambda=1$: say, $2 \mid c \Rightarrow 2 \nmid ab$, $2 \nmid x_2 y_2 \Rightarrow a+b+ct^2 \equiv 0 \pmod 8$ for $t=0$ or 1;
take $l'(x,y,z) = x-y$, $l''(x,y,z) = z - ty$

Step 2. $L = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{Z}^3 \mid (*) \text{ holds} \right\} \subset \mathbb{Z}^3$, $(\mathbb{Z}^3 : L) = 2^{\lambda+2} \prod_{i=1}^r p_i = 4|abc|$.

Step 3. So $L \subset \mathbb{R}^3$ is a lattice with $\mu(\mathbb{R}^3/L) = 4|abc|$. Consider

$K = K_R = \left\{ \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in \mathbb{R}^3 \mid |a|x^2+|b|y^2+|c|z^2 < R^2 \right\}$, $\mu(K_R) = |abc|^{-1/2} \frac{4}{3}\pi R^3$

When is $\mu(K_R) > \underbrace{2^3 \mu(\mathbb{R}^3/L)}_{32|abc|}$? If $\frac{4}{3}\pi R^3 > 32|abc|^{3/2} \iff R^2 > \left(\frac{24}{\pi}\right)^{2/3} |abc|$

But $\frac{24}{\pi} < \frac{24}{3} = 8 \Rightarrow \left(\frac{24}{\pi}\right)^{2/3} < 4$, so $R^2 = 4|abc| \Rightarrow \mu(K_R) > 2^3 \mu(\mathbb{R}^3/L)$.

Minkowski: $\exists 0 \neq \begin{pmatrix} x \\ y \\ z \end{pmatrix} \in K_R \cap L$ for $\Rightarrow$ $\underbrace{|f(x,y,z)|}_{\equiv 0 \pmod{4|abc|}} \le |a|x^2+|b|y^2+|c|z^2 < \underbrace{R^2}_{4|abc|}$

$\Rightarrow$ $f(x,y,z) = 0$.

Rk: Thm implies that the form $f(x,y,z)$ satisfying the assumptions is necessarily indefinite. This yields certain cases of QRL (Legendre).

Ex: $2 \neq p \neq q \neq 2$ primes, $f = x^2+py^2+qz^2$ is definite

If $q \equiv 3 \pmod 4$, $\left(\frac{-q}{p}\right) = 1$, $\left(\frac{-p}{q}\right) = 1$ $\Rightarrow$ the assumptions are satisfied $(a=1, b=p, c=q)$ } contradiction.

So $q \equiv 3 \pmod 4$, $\left(\frac{-p}{q}\right) = 1 \Rightarrow \left(\frac{-q}{p}\right) = -1$.

Remarks on "Legendre's Theorem"

In fact, Legendre proved a slightly different result, namely: ($\square$ = square)

Thm. Let $a,b,c \in \mathbb{Z}\setminus\{0\}$ be not of the same sign, abc $\square$-free. Then:

$(*)$ $ax^2+by^2+cz^2=0$ has a solution $(x,y,z)\in\mathbb{Z}^3\setminus\{(0,0,0)\}$

$\Updownarrow$

$(**)$ $-bc\equiv\square \pmod a$, $-ca\equiv\square\pmod b$, $-ab\equiv\square\pmod c$.

More generally, if we replace the condition "abc $\square$-free" by "$(a,b)=(b,c)=(c,a)=1$", then $[(**)\Rightarrow(*)]$. Note: $3x^2-y^2-z^2=0$ has a solution, but $-1\not\equiv\square \pmod 3$

(descent)

Legendre's proof followed a reduction procedure due to Lagrange. In other words, it proceeded by induction on the size of the coefficients.

Here is an example of the induction step for

$x^2-Ay^2=Bz^2$, $1\le|A|<|B|$, $\gcd(A,B)=1$.

the assumption $(**)\iff$ $A\equiv\square\pmod B$, $B\equiv\square\pmod A$.

$\Rightarrow \exists\, s,u\in\mathbb{Z}$ $\quad s^2=A+Bu$, $|s|\le|B|/2 \Rightarrow |u|<|B|/4+1\le|B|/2$.

We are looking for solutions (x,y,z) with $x\equiv sy\pmod B \Rightarrow sx\equiv Ay\pmod B$

$(x+y\sqrt{A})(s-\sqrt{A})=B(x_1+y_1\sqrt{A})$, $\quad x_1=(sx-Ay)/B$, $\quad y_1=(sy-x)/B$

$N(x+y\sqrt{A})=x^2-Ay^2\equiv Bz^2$, $\quad N(s-\sqrt{A})=s^2-A=Bu \Rightarrow N(x_1+y_1\sqrt{A})=x_1^2-Ay_1^2=uz^2$

As $A\equiv s^2\pmod u$, new equation with $|u|<|B|/2$

$B\equiv\square\pmod A$, $Bu\equiv\square\pmod A$ $\Longrightarrow^{(A,B)=1}$ $u\equiv\square\pmod A$, the new equation also satisfies $(**)$.

If $\gcd(u,A)=1$ $\Rightarrow$ we can conclude by induction that $\exists$ solution (x_1,y_1,z)

$\Rightarrow \exists$ solution (x,y,z) of $(*)$.

---

this descent argument is, in principle, effective - it produces a non-trivial solution of $(*)$, provided we solve at each step the congruence $s^2\equiv A\pmod B$. this is a very time-consuming process, since it requires factorisation of each B into a product of primes. Cremona and Ruskin (2002) found a clever modification of the descent argument that requires only factorisation of the initial a,b and c (~~~~ and an explicit solution of $-bc\equiv r^2\pmod a$, $-ca\equiv s^2\pmod b$, $-ab\equiv t^2\pmod c$). they also showed how to produce a parametric description of all solutions

$x=Q_1(u,v)$, $y=Q_2(u,v)$, $z=Q_3(u,v)$, where Q_i are quadratic forms with not too big coefficients (relative to $|a|,|b|,|c|$).

A proof of Legendre's thm (in its original form $(*) \Leftarrow (**)$) using geometry of numbers for an indefinite quadratic form $x^2+y^2-z^2$ is due to Davenport and Marshall Hall (1948). The argument given in the text (with the definite quadratic form $|a|x^2+|b|y^2+|c|z^2$) is due to Cassels (1959).

Holzer (1950) showed that, for abc $\square$-free, $(**)$ implies that there exists a non-trivial solution $(x,y,z) \in \mathbb{Z}^3$ with $\max(|a|x^2, |b|y^2, |c|z^2) \leq |abc|$.
His proof relied on a generalisation of Dirichlet's thm on primes in arithmetic progressions to an analogous statement in imaginary quadratic fields (proved by Hecke).

More elementary proofs of Holzer's result were given by Mordell (1969) – completed by Williams (1988) – and Cochrane – Mitchell (1998).
