The Hasse–Minkowski Theorem

Akshatha Arunkumar

Independent Research Project

The Guiding Question

Goal

Given a quadratic equation with rational coefficients, can we decide whether it has a **non-trivial** rational solution?

Motivating examples

- $x^2 + 3y^2 = z^2$ (conjecture: no)
- $x^2 + y^2 = 2z^2$ (conjecture: yes)

Brute-force search is hopeless — we need prime-by-prime invariants.

Why Quadratic Forms?

- Appear in Diophantine equations, coding theory, lattice physics.
- Degree 2 $\Rightarrow$ rich structure *and* complete classification.
- Central notion: isotropy — does $Q(\mathbf{x}) = 0$ have $\mathbf{x} \neq 0$?

Basic Definitions (quick)

Definition (Quadratic form)

$Q(\mathbf{x}) = \mathbf{x}^\top A\mathbf{x}$ with $A = A^\top \in M_n(\mathbb{Q})$.

Definition (Discriminant)

$\mathrm{disc}(Q) = (-1)^{n(n-1)/2} \det A \mod (\mathbb{Q}^\times)^2$.

Definition (Isotropic)

Q is isotropic if $Q(\mathbf{x}) = 0$ for some $\mathbf{x} \neq 0$.

Diagonalising Quickly

Brief algorithm (one sweep).

- *Pick* an off-diagonal entry $2b$ in row i, col j.
- *Complete the square:* $b\,x_i x_j \;\rightsquigarrow\; \dfrac{b}{a_i}(a_i x_i^2) + \left(x_j + \dfrac{b}{a_i}x_i\right)^2$ if $a_i \neq 0$.
- *Replace* $x_j \leftarrow x_j - \dfrac{b}{a_i}x_i$ to cancel the term.
- *Repeat* until all cross terms are gone; char $\mathbb{Q} \neq 2$ keeps denominators manageable.

Start with $3x^2 + 4xy + 5y^2$.

$$3\left(x + \tfrac{2}{3}y\right)^2 + \tfrac{11}{3}y^2 = 3u^2 + \tfrac{11}{3}v^2.$$

Moral: any non-degenerate form is $\langle a_1, \ldots, a_r \rangle$ after a change of coordinates.

Enter the p-adics

Definition

Write $x = p^k a/b$ ($p \nmid ab$). Define $v_p(x) = k$, $|x|_p = p^{-k}$ and complete to get $\mathbb{Q}_p$.

Enter the p-adics

Definition

Write $x = p^k a/b$ $(p \nmid ab)$. Define $v_p(x) = k$, $|x|_p = p^{-k}$ and complete to get $\mathbb{Q}_p$.

Example

$x = \frac{14}{75} = 2 \cdot 7/3 \cdot 5^2$ $v_5(x) = -2$ so $|x|_5 = 25$ (huge!).

Real vs p-adic Distance

Real norm: $|10^n + 1|_\infty \to \infty$.

3-**adic norm:** $|10^n + 1|_3 = |1|_3 = 1$ (because $3 \nmid 10^n + 1$).

In $\mathbb{Q}_3$ the sequence 10^n *converges* to -1!
Intuition: carries propagate infinitely far to the left.

Hensel's Lemma – Our Workhorse

Lemma (Simple form)

If $f \in \mathbb{Z}_p[x]$, $a_0 \in \mathbb{Z}_p$ with $f(a_0) \equiv 0 \pmod p$ and $f'(a_0) \not\equiv 0 \pmod p$, then f has a unique root $\tilde{a} \in \mathbb{Z}_p$ lifting a_0.

Hensel's Lemma – Our Workhorse

Lemma (Simple form)

If $f \in \mathbb{Z}_p[x]$, $a_0 \in \mathbb{Z}_p$ with $f(a_0) \equiv 0 \pmod{p}$ and $f'(a_0) \not\equiv 0 \pmod{p}$, then f has a unique root $\tilde{a} \in \mathbb{Z}_p$ lifting a_0.

Newton–Hensel iteration. Set

$$a_{n+1} = a_n - \frac{f(a_n)}{f'(a_n)}.$$

- Each step doubles the p-adic precision: if $f(a_n) \equiv 0 \pmod{p^k}$, then $f(a_{n+1}) \equiv 0 \pmod{p^{2k}}$.
- Geometric convergence: the error term gains an extra factor p (often p^2) per iteration.
- Termination in practice: a few iterations usually reach the desired modulus p^m.

Example – Lifting $x^2 = 2$ in $\mathbb{Q}_7$

Mod 7: $3^2 = 2$ $a_0 = 3$. Newton step mod 49:

$$a_1 = 3 - \frac{3^2 - 2}{2 \cdot 3} = 10 \pmod{49}, \qquad 10^2 \equiv 2 \pmod{49}.$$

Iterating yields $\sqrt{2} \in \mathbb{Z}_7$.

Legendre Symbol Recap

$$\left(\frac{a}{p}\right) = a^{(p-1)/2} \pmod{p} \in \{\pm 1\}.$$

Quadratic reciprocity flips (a/p) and (p/a); invaluable for local checks.

The Hasse–Minkowski Theorem

Theorem

A non-degenerate quadratic form Q is isotropic over $\mathbb{Q}$ $\iff$ isotropic over $\mathbb{R}$ and every $\mathbb{Q}_p$.

Local checks at finitely many places $=$ global answer.

Key Idea 1 — Local Classification

Task. Classify a quadratic form Q over a local field $\mathbb{Q}_v$.

- Invariants: $\big(n, \operatorname{disc} Q, \epsilon_v(Q)\big)$
  - $n = \dim Q$
  - $\operatorname{disc} Q = (-1)^{n(n-1)/2} \det A \pmod{(\mathbb{Q}_v^\times)^2}$
  - $\epsilon_v(Q) = \prod_{i<j}(a_i, a_j)_v$ (Hasse invariant)
- Two forms are isometric over $\mathbb{Q}_v \iff$ their triples match.

Key Idea 2 — Four-Variable Core $\leftrightarrow$ Quaternion Algebras

- A diagonal 4-tuple $\langle a, b, c, d \rangle$ with $abcd \in (\mathbb{Q}^\times)^2$ corresponds to a quaternion algebra (a, b).
- **Albert–Brauer–Hasse–Noether:** that algebra splits over $\mathbb{Q}$ iff it splits over every completion $\mathbb{Q}_v$.
- Splitting $\Longrightarrow$ Q is isotropic in dimension 4.

Key Idea 3 — Dimension Induction

- Attach (or peel off) a hyperbolic plane $H = \langle 1, -1 \rangle$.
- If $Q \perp H$ is isotropic, either Q already is, or a 2-dimensional isotropic subspace lets us reduce $\dim Q$ by 2.
- Repeatedly strip planes until reaching the $n = 4$ core where isotropy is settled.

Key Idea 4 — Hilbert Product Formula

$$\prod_v (a,b)_v = 1 \qquad (a, b \in \mathbb{Q}^\times).$$

- At most an *even* number of places can contribute -1.
- Ensures local Hasse invariants are globally compatible: any single obstruction must be cancelled elsewhere.

Key Idea 5 — Weak–Chinese Approximation

- $\mathbb{Q}$ is dense in every $\mathbb{Q}_v$.
- Choose a vector that is almost a zero everywhere, then adjust coordinates using the Chinese Remainder Theorem to satisfy finitely many congruence conditions simultaneously.
- Continuity in each $|\cdot|_v$ promotes the "almost-zero" to an actual global isotropic vector.

Worked Example 1 – $x^2 + 3y^2 = z^2$

Real solution: $(1, 0, 1)$.
$p = 3$: only trivial $\Rightarrow$ obstruction.

No rational solution.

Worked Example 2 – $x^2 + y^2 = 2z^2$

Locally solvable everywhere global solution, e.g. $(3, 1, 2)$.

Hilbert Symbol & Product Formula

$$(a, b)_v = \begin{cases} 1 & \exists (x, y, z) \in \mathbb{Q}_v \text{ such that } x^2 = ay^2 + bz^2, \\ -1 & \text{otherwise.} \end{cases}$$

Key identity: $\prod_v (a, b)_v = 1 \Rightarrow$ "obstruction parity".

Applications

- **Lagrange 1770:** every $n \in \mathbb{N}$ is a sum of 4 squares.
- Checking rational points on conics $ax^2 + by^2 = z^2$.
- Classification of forms: two forms are $\mathbb{Q}$-equivalent iff they match at all places.

When Local isn't Global

- Cubic Selmer curve: everywhere locally solvable, no global point.
- Open territory: higher-degree forms, Brauer–Manin obstructions.

Quadratic forms are a rare "Goldilocks" case where everything works.

Take-aways

- Think **locally** to solve **global** problems.

Thank you for listening!