Notes for the course p-adic methods in arithmetic Summer school, ELTE (2022)

Gergely Zábrádi

29th June 2022

These are the notes of a minicourse given by the author at ELTE in June 2022. Nothing in these notes are original or new. The text has been influenced by the books of Gouvea and Serre [3, 4]. The goal of the course is to explain the local–global principle in arithmetic through the proof of the Theorem of Hasse and Minkowski.

1 Introduction

Why do diophantine equations have no solutions? We start by the following trivial examples.

Example 1. Consider the equation $x^2 + y^2 = -1$ in $\mathbb{Z}$ (or in $\mathbb{Q}$). It has no solutions *because* it has no solutions over $\mathbb{R}$ either (which contains $\mathbb{Z} \subset \mathbb{Q}$).

Example 2. Consider the equation $x^2 - 3y^2 = -1$ in $\mathbb{Z}$. It has no solutions since there are no solutions modulo 3 either (one could also argue mod 4).

I claim that the above 2 types of obstruction have the same nature! To see this at first investigate whether Example 2 has solutions in $\mathbb{Q}$. Finding a common denominator write $x = \frac{a}{c}$ and $y = \frac{b}{c}$ with $(a, b, c) = 1$ to obtain $a^2 - 3b^2 = -c^2$. We may argue the same way: Since -1 is not a square mod 3, we must have $3 \mid c$ and $3 \mid a$ whence $9 \mid a^2 + c^2 = 3b^2$ deducing $3 \mid b$, as well—contradiction. In fact, we have just shown that this equation has no solutions in the field $\mathbb{Q}_3$ of 3-adic numbers. In order to motivate what those are, let us start with the analogy between arithmetic and $\mathbb{Z}$ and arithmetic in $\mathbb{C}[t]$.

ring	$\mathbb{Z}$	$\mathbb{C}[t]$
UFD	✓	✓
PID	✓	✓
maximal ideals	primes	$\{(t-c) \mid c \in \mathbb{C}\}$
local expansion	$a_0 + a_1 p + \cdots + a_n p^n$	$a_0 + a_1(t-c) + \cdots + a_n(t-c)^n$
	only for nonnegative integers	any polynomial
	$(a_i \in \{0, 1, \ldots, p-1\})$	$(a_i \in \mathbb{C})$
fraction field	$\mathbb{Q}$	$\mathbb{C}(t) = \{\frac{f}{g} \mid f, g \in \mathbb{C}[t], g \neq 0\}$
local expansion of fractions	???	$\sum_{n=-N}^{\infty} a_n (t-c)^n$

Note that the local expansion of fractions $\frac{f}{g}$ at c converges in a punctured neighbourhood of c since "t is close to c", ie. "$(t-c)$ is close to 0" $\Rightarrow (t-c)^n \to 0$ as $n \to +\infty$. Replacing $(t-c)$ with the prime $p \in \mathbb{Z}$ makes us want to have $p^n \to 0$ in some metric.

Definition. For a nonzero rational number $\frac{a_1}{b_1}p^k$ with $p \nmid a_1, b_1$, $k \in \mathbb{Z}$ denote by $|\frac{a_1}{b_1}p^k|_p := p^{-k}$ the *p-adic absolute value*. In other words we have $|\alpha|_p = p^{-v_p(\alpha)}$ where v_p denotes the exponent of p in the prime decomposition of a number. Further, put $|0|_p := 0$.

Lemma 1.1. *For all $x, y \in \mathbb{Q}$ we have*

1. $|x|_p = 0 \Leftrightarrow x = 0$.
2. $|xy|_p = |x|_p|y|_p$.
3. $|x + y|_p \leq \max(|x|_p, |y|_p)(\leq |x|_p + |y|_p)$.

Proof. Left to the reader. □

The third inequality above is called the ultrametric inequality. Absolute values are functions $|\cdot|\colon K \to \mathbb{R}^{\geq 0}$ satisfying the above first 2 conditions and the triangle inequality (third condition with just $\leq |x|+|y|$ on the right). An absolute value is called nonarchimedean if the ultrametric inequality is also satisfied, otherwise we call it archimedean. We call two absolute values $|\cdot|$ and $|\cdot|'$ *equivalent* if there exists a real number $s > 0$ such that $|x|^s = |x|'$ for all $x \in K$. Fact: two absolute values on K are equivalent if and only if they induce the same topology on K.

Theorem 1.2 (Ostrowski)**.** *Any absolute value on $\mathbb{Q}$ is equivalent to one of the following (pairwise inequivalent) absolute values:*

1. *The trivial absolute value* $|x|_1 = \begin{cases} 1 \text{ if } x \neq 0 \\ 0 \text{ if } x = 0 \end{cases}$.
2. *The usual archimedean absolute value $|\cdot|_\infty$.*
3. *The p-adic absolute value $|\cdot|_p$ for some prime p.*

Definition. The field $\mathbb{Q}_p$ of p-adic numbers is the *completion* of $\mathbb{Q}$ with respect to $|\cdot|_p$.

Here by completion we mean the equivalence classes of Cauchy sequences. Two Cauchy sequences are *equivalent* if their merge is also a Cauchy sequence.

We recall some basic facts about $|\cdot|_p$ and $\mathbb{Q}_p$:

1. If $(x_n)_{n\geq 1} \subset \mathbb{Q}$ is Cauchy in $|\cdot|_p$ then $|x_n|_p$ stabilizes or $|x_n|_p \to 0$. Indeed, the range of $|\cdot|_p$ on $\mathbb{Q}$ is $p^{\mathbb{Z}} \cup \{0\}$ which has no limit point other than 0. In particular, the range of $|\cdot|_p$ on $\mathbb{Q}_p$ is the same set as $p^{\mathbb{Z}} \cup \{0\}$ is closed in $\mathbb{R}$.

2. Elements of $\mathbb{Q}_p$ have a *unique* p-adic expansion of the form

$$0 \neq x = \sum_{n=-N}^{\infty} a_n p^n \qquad a_n \in \{0, 1, \ldots, p-1\}, a_{-N} \neq 0 \ .$$

3. One could in fact work with any other set of representatives of $\mathbb{Z}/(p) = \mathbb{F}_p$ instead of $\{0, 1, \ldots, p-1\} \subset \mathbb{Z}$.

4. The closed unit disk

$$\mathbb{Z}_p := \{\alpha \in \mathbb{Q}_p \mid |\alpha|_p \leq 1\} = \{a_0 + a_1 p + \cdots + a_n p^n + \cdots\}$$

is a subring! It is closed under addition due to the ultrametric inequality. $\mathbb{Z}_p$ is called the *ring of p-adic integers.*

5. We have $\mathbb{Z}_p/(p^n) \simeq \mathbb{Z}/(p^n)$. $\mathbb{Z}_p$ is a complete discrete valuation ring , in particular it has unique factorization with single prime p.

Example 3. Let $p = 5$. We compute

$$\frac{35}{31} = \frac{2 \cdot 5 + 5^2}{1 + 5 + 5^2} = \frac{2p + p^2}{1 + p + p^2} = 2p + 4p^2 + 3p^3 + p^4 + 4p^5 + \cdots + 4p^n + \cdots = \\ = 2p + 4p^2 + 3p^3 + p^4 + 3p^5 \frac{1}{1-p} \, .$$

Indeed, one has to "carry over" when multiplying or adding. Further, we have

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + \cdots \, .$$

In particular, there is a p-adic expansion of any not necessarily positive integer.

2 Solving equations in $\mathbb{Z}_p$ (or in $\mathbb{Q}_p$)

Lemma 2.1. *Let $f_1, \ldots, f_k \in \mathbb{Z}_p[x_1, \ldots, x_m]$ be polynomials. The following are equivalent:*

(1) *$f_1, \ldots, f_k$ have a common root in $\mathbb{Z}_p^m$;*

(2) *$f_1, \ldots, f_k$ have a common root in $(\mathbb{Z}/(p^n))^m$ for all $n \geq 1$.*

Sketch of proof. (1) $\Rightarrow$ (2): We may reduce the common root mod p^n and use the fact $\mathbb{Z}_p/(p^n) \simeq \mathbb{Z}/(p^n)$.

(2) $\Rightarrow$ (1): One may argue using the fact that $\mathbb{Z}_p$ is a compact topological space therefore so is $\mathbb{Z}_p^m$. Alternatively, one could use König's lemma: put $A_n \subseteq \mathbb{Z}/(p^n)$ the set of mod p^n solutions. These are finite sets and there is a reduction map $A_{n+1} \to A_n$ for all $n \geq 1$. Further, by assumption $A_n \neq \emptyset$ for any $n \geq 1$. Assume all the elements of A_1 can only be lifted to some finite level. Since A_1 is finite, there is a maximum of these levels, say n. However, A_{n+1} is nonempty, and any element in A_{n+1} reduces to an element in A_1 contradicting that n was the maximum level of all the lifts of elements of A_1. Therefore the subset $B_j \subseteq A_j$ consisting of elements of A_j that can be lifted arbitrarily is nonempty for any $j \geq 1$. Any element in B_1 lifts to an element in B_2 which lifts to an element B_3 and so on, so in the limit we obtain a p-adic common root of $f_1, \ldots, f_k$ as a sequence of compatible elements in A_n ($n \geq 1$). □

Proposition 2.2. *Let $f_1, \ldots, f_k \in \mathbb{Z}_p[x_1, \ldots, x_m]$ be* homogeneous *polynomials. Then the following are equivalent:*

(1) *$f_1, \ldots, f_k$ have a nontrivial common root in $\mathbb{Q}_p^m$;*

(2) *$f_1, \ldots, f_k$ have a nontrivial common root in $\mathbb{Z}_p^m$;*

(3) *$f_1, \ldots, f_k$ have a primitive common root in $(\mathbb{Z}/(p^n))^m$ for all $n \geq 1$.*

Here by trivial root we mean $(0, \ldots, 0)$ and by primitive root we mean a tuple $(\alpha_1, \ldots, \alpha_m)$ with greatest common divisor $\gcd(\alpha_1, \ldots, \alpha_m) = 1$.

Proof. (1) and (2) are equivalent since we may multiply any root in $\mathbb{Q}_p^m$ by the least common multiple of the denominators of the coordinates which is still a solution as $f_1, \ldots, f_k$ are homogeneous. In particular, there is a nontrivial solution if and only if there is a primitive one. (2) and (3) are equivalent by Lemma 2.1. □

Lemma 2.3 (Hensel)**.** *Let $f(x) \in \mathbb{Z}_p[x]$, $n, k \in \mathbb{Z}$ with $0 \leq 2k < n$. Assume $f(\alpha) \equiv 0 \pmod{p^n}$ and $v_p(f'(\alpha)) = k$. Then there is a $\beta \in \mathbb{Z}_p$ such that $f(\beta) \equiv 0 \pmod{p^{n+1}}$, $v_p(f'(\beta)) = k$, and $\beta \equiv \alpha \pmod{p^{n-k}}$.*

Proof. We look for β in the form $\beta = \alpha + p^{n-k}z$ and compute

$$f(\beta) = f(\alpha + p^{n-k}z) = f(\alpha) + p^{n-k}zf'(\alpha) + (p^{n-k}z)^2(\cdots) \equiv f(\alpha) + p^{n-k}zf'(\alpha) \pmod{p^{n+1}}$$

since $p^{n+1} \mid p^{2n-2k}$. On the other hand, $v_p(p^{n-k}f'(\alpha)) = n-k+k = n \leq v_p(f(\alpha))$ whence $z := -\frac{f(\alpha)}{p^{n-k}f'(\alpha)}$ lies in $\mathbb{Z}_p$. □

Theorem 2.4. *Let $f \in \mathbb{Z}_p[x_1, \ldots, x_m]$, $\alpha = (\alpha_1, \ldots, \alpha_m) \in \mathbb{Z}_p^m$, $n, k \in \mathbb{Z}$ with $0 \leq 2k < n$. Assume there exists an index $j \in \{1, \ldots, m\}$ such that $f(\alpha) \equiv 0 \pmod{p^n}$ and $v_p\left(\frac{\partial f}{\partial x_j}(\alpha)\right) = k$. Then there exists a $\beta \in \mathbb{Z}_p^m$ such that $f(\beta) = 0$ and $\beta \equiv \alpha \pmod{p^{n-k}}$.*

Proof. We apply Lemma 2.3 repetitively on the 1-variable polynomial $f(\alpha_1, \ldots, x_j, \ldots, \alpha_m)$ in order to find $\beta = (\beta_1, \ldots, \beta_m)$ such that $\beta_i = \alpha_i$ for all $j \neq i \in \{1, \ldots, m\}$. □

Corollary 2.5. *The polynomial $x^{p-1} - 1$ splits completely over $\mathbb{Z}_p$. In particular, the group $\mathbb{Z}_p^\times$ splits as a direct product $\mathbb{Z}_p^\times = \mu_{p-1} \times (1 + p\mathbb{Z}_p)$ (where μ_{p-1} denotes the group of $p-1$th roots of unity).*

Proof. The polynomial $x^{p-1} - 1$ has $p-1$ distinct roots in $\mathbb{F}_p = \mathbb{Z}/(p)$ which all lift to $\mathbb{Z}_p$ by Lemma 2.3 ($n = 1$, $k = 0$: the value of the derivative $(x^{p-1} - 1)' = (p-1)x^{p-2}$ is not divisible by p at the roots mod p). □

Proposition 2.6. *Assume $p \neq 2$. Then any $u \in 1 + p\mathbb{Z}_p$ has a square root in $\mathbb{Z}_p$.*

Proof. The polynomial $x^2 - u$ has two distinct roots mod p since the derivative $(x^2 - u)' = 2x$ does not vanish mod p at ± 1, so we may apply Lemma 2.3 with $n = 1$, $k = 0$. □

Proposition 2.7. *Assume $p = 2$. Then any $u \in 1 + 8\mathbb{Z}_p$ has a square root in $\mathbb{Z}_2$.*

Proof. The polynomial $x^2 - u$ has the root 1 mod $8 = 2^3$ and the valuation of the derivative $(x^2 - u)' = 2x$ at 1 equals $v_2(2) = 1$, so we may apply Lemma 2.3 with $n = 3$, $k = 1$. □

Corollary 2.8. *We have*

$$\mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 = \begin{cases} \langle p, u\rangle = \{1, p, u, pu\} \simeq C_2 \times C_2 & \text{if } p \neq 2 \\ \langle 2, 5, -1\rangle = \{\pm 1, \pm 2, \pm 5, \pm 10\} \cong C_2 \times C_2 \times C_2 & \text{if } p = 2\ . \end{cases}$$

Here u denotes a quadratic nonresidue mod p, ie. $\left(\frac{u}{p}\right) = -1$.

Proof. The multiplicative group decomposes as a direct product $\mathbb{Q}_p^\times = p^{\mathbb{Z}} \times \mathbb{Z}_p\times \simeq p^{\mathbb{Z}} \times \mu_{p-1} \times (1 + p\mathbb{Z}_p)$. The result follows from Propositions 2.6 and 2.7 noting $(\mathbb{Z}/(8))^\times = \langle -1, 5\rangle$. □

3 Statement and application of Theorem of Hasse and Minkowski

It is nice to have some obstructions to the existence of rational solutions of diophantine equations, but how does one guarantee the existence of such? Hasse's local–global principle is that whenever the polynomials $f_1, \ldots, f_k \in \mathbb{Q}[x_1, \ldots, x_m]$ have a common (nontrivial) root in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all primes p then there should be a common (nontrvial) root in $\mathbb{Q}$, too (if the polynomials are homogeneous). However, the following famous counterexample due to Ernst Selmer (1951) shows that this is, unfortunately, not always the case:

Example 4. The equation $3x^3 + 4y^3 + 5z^3$ has nontrivial solutions in $\mathbb{R}$ and in $\mathbb{Q}_p$ for all primes p, but no nontrivial solutions in $\mathbb{Q}$.

Hint of proof. The existence of real and p-adic solutions is not that hard, one first finds solutions mod p and lifts them using Hensel's lemma (one has to distinguish the cases of $p = 3, 5$). The proof of nonexistence of rational solutions requires some algebraic number theory (arithmetic in the ring $\mathbb{Z}[\sqrt[3]{6}]$) or elliptic curves. See the notes of Keith Conrad [2] and the book of Cassels [1] for details. □

However, for quadratic forms we have the following result of Hasse and Minkowski from the 1920s:

Theorem 3.1 (Hasse–Minkowski)**.** *Assume $f \in \mathbb{Q}[x_1, \dots, x_m]$ is homogeneous of degree 2. The the following are equivalent:*

(1) *there exists an $\alpha \neq 0$ in $\mathbb{Q}^m$ such that $f(\alpha) = 0$;*

(2) *there exists an $\alpha^{(\infty)} \neq 0$ in $\mathbb{R}^m$ such that $f(\alpha^{(\infty)}) = 0$ and for all primes p there exists an $\alpha^{(p)} \neq 0$ in $\mathbb{Q}_p^m$ such that $f(\alpha^{(p)}) = 0$.*

We postpone the proof of Theorem 3.1 until section 6. Let us see some application first to the classical problem of sums of three squares.

Theorem 3.2. *A nonnegative integer n can be represented by a sum of three squares if and only if n is* not *of the form $4^a(8k + 7)$ ($a, k \in \mathbb{Z}^{\geq 0}$).*

Proof. At first we show that $x^2 + y^2 + z^2 = 4^a(8k + 7)$ has no solutions in $\mathbb{Z}$. If $a \geq 1$ then arguing mod 4 we find that all x, y, z must be even. Therefore we may divide the equation by 4 to represent $4^{a-1}(8k + 7)$ as a sum of three squares. Repeating the process we may assume $a = 0$. However, squares have residues $0, 1$, or 4 mod 8, so three squares cannot add up to $8k + 7$.

Step 1: For the converse, we first show that if $n \neq 4^a(8k + 7)$ then n can be written as a sum of the squares of three rational numbers. Consider the quadratic form $x^2 + y^2 + z^2 - nu^2$. We show that it has a local solution at each prime and at infinity. Since $n > 0$, there is a nontrivial root in $\mathbb{R}$. Next we treat $p = 2$:

Lemma 3.3. *Assume $n \not\equiv 0, 4, 7 \pmod 8$, $k \geq 3$. Then there exist $x, y, z \in \mathbb{Z}$ such that $x^2 + y^2 + z^2 \equiv n \pmod{2^k}$.*

Proof. Using Proposition 2.7 we may assume $k = 3$. We check $1 = 0^2 + 0^2 + 1^2$, $2 = 0^2 + 1^2 + 1^2$, $3 = 1^2 + 1^2 + 1^2$, $5 = 0^2 + 1^2 + 2^2$, $6 = 1^2 + 1^2 + 2^2$. □

By Lemma 3.3 the form $x^2 + y^2 + z^2 - nu^2$ has a nontrivial zero in $\mathbb{Q}_2$: whenever $4 \mid n$ we may replace $u = \frac{u_1}{2}$ and once $4 \nmid n$ we will have $n \not\equiv 0, 4, 7 \pmod 8$ by our assumption that $n \neq 4^a(8k + 7)$.

Now we turn to the case $p > 2$.

Lemma 3.4. *Assume $p > 2$ and $k \geq 1$. Then the congruence $x^2 + y^2 + z^2 \equiv n \pmod{p^k}$ is solvable for all $n \in \mathbb{Z}$.*

Proof. We take $z = 1$ if $p \mid n$ and $z = 0$ if $p \nmid n$. So it suffices to show that whenever $p \nmid c$ then the congruence $x^2 + y^2 \equiv c \pmod{p^k}$ has a solution (we take $c = n$ or $n - 1$). For the existence of solutions mod p note that the sets $\{c - y^2 \mid y \in \mathbb{F}_p\}$ (resp. $\{x^2 \mid x \in \mathbb{F}_p\}$) have cardinality $\frac{p+1}{2}$, so they cannot be disjoint as $\mathbb{F}_p$ has cardinality $p < \frac{p+1}{2} + \frac{p+1}{2}$. By the multivariate Hensel's Lemma (Thm. 2.4) the mod p solution can be lifted to mod p^k for all $k \geq 1$ since whenever $x_0^2 + y_0^2 \equiv c \not\equiv 0 \pmod p$, we have $(x_0, y_0) \not\equiv (0, 0) \pmod p$ so at least one of the partial derivatives of $x^2 + y^2 - c$ will not vanish mod p at the point (x_0, y_0). □

By Theorem 3.1 there exists a vector $(0,0,0,0) \neq (x_0, y_0, z_0, u_0) \in \mathbb{Q}^4$ such that $x_0^2 + y_0^2 + z_0^2 = nu_0^2$. However, u_0 cannot be 0 as $x_0^2 + y_0^2 + z_0^2$ can only be 0 for $x_0 = y_0 = z_0 = 0$. So putting $x_1 = x_0/u_0$, $y_1 = y_0/u_0$, $z_1 = z_0/u_0$ we find $n = x_1^2 + y_1^2 + z_1^2$.

Step 2: We show that whenever we have rational solutions of $x^2 + y^2 + z^2 = n$, we also have integral solutions. For this we need the following Lemma in elementary geometry due to Cassels and Davenport.

Lemma 3.5. *Assume that we have a rational point $P_1 = (x_1, y_1, z_1) \in \mathbb{Q}^3$ in the Euclidean 3-space with $x_1^2 + y_1^2 + z_1^2 = n \in \mathbb{Z}$ such that the common denominator of (x_1, y_1, z_1) is $t_1 > 1$. Pick an integral vector $P_2 := (x_2, y_2, z_2) \in \mathbb{Z}^3$ by rounding x_1, y_1, z_1, ie. we have $|x_1 - x_2|_\infty, |y_1 - y_2|_\infty, |z_1 - z_2|_\infty \leq \frac{1}{2}$. Then the line connecting P_1 and P_2 intersects the sphere around the origin of radius $\sqrt{n}$ in another rational point $P_3 = (x_3, y_3, z_3) \in \mathbb{Q}^3$ such that $t_1\|P_1 - P_2\|^2(x_3, y_3, z_3) = t_1((x_1 - x_2)^2 + (y_1 - y_2)^2 + (z_1 - z_2)^2)(x_3, y_3, z_3)$ lies in $\mathbb{Z}^3$.*

Proof. Left to the reader. See Lemma B in the Appendix of Chapter I in [4] for a more general statement and proof. □

Note that $t_1\|P_1 - P_2\|^2 \leq t_1(\frac{1}{4} + \frac{1}{4} + \frac{1}{4}) < t_1$ is an integer since we have

$$t_1\|P_1 - P_2\|^2 = t_1\langle P_1 - P_2, P_1 - P_2\rangle = t_1\|P_1\|^2 + t_1\|P_2\|^2 - 2t_1\langle P_1, P_2\rangle = t_1 n + t_1\|P_2\|^2 - 2\langle t_1 P_1, P_2\rangle$$

and $t_1 P_1, P_2 \in \mathbb{Z}^3$. Iterating the above Lemma we end up with an integral point on the sphere of radius $\sqrt{n}$ as desired. □

4 Hilbert symbol and its local properties

In order to uniformize notation we put $\mathbb{Q}_\infty := \mathbb{R}$ and denote by $P \subset \mathbb{N}$ the set of primes such that v (or ℓ) will often run on $P \cup \{\infty\}$. However, p will still denote a (finite) prime.

Definition. Let K be a field (of characteristic different from 2, but for the minicourse always of characteristic 0) and $a, b \in K^\times$. The Hilber symbol $(a, b)_K \in \{\pm 1\}$ is defined to be 1 if the quadratic form $z^2 - ax^2 - by^2$ has a nontrivial root in K and to be -1 otherwise. If the field K is understood from the context we often omit the subscript K. Further, in case $K = \mathbb{Q}_v$ ($v \in P \cup \{\infty\}$) we just put v in the subscript instead of $\mathbb{Q}_v$.

Note that $(a, b)_K = 1$ if and only if the quaternion algebra defined with constants a, b splits over K. We do not need this fact in the sequel, so do not worry if you do not know what a quaternion algebra is.

Proposition 4.1. *Let $a, b \in K^\times$. We have $(a, b) = 1$ if and only if a is a norm of an element in $K(\sqrt{b})$ if and only if b is a norm of an element in $K(\sqrt{a})$.*

Proof. If $b = c^2$ then $K(\sqrt{b}) = K$ whence any $a \in K^\times$ is a norm. Consequently, $x = 0, y = 1, z = c$ is a nontrivial root. Assume now that b is not a square. Then $x_0 = 0$ is not possible for a nontrivial solution $z_0^2 = ax_0^2 + by_1^2$. Therefore $a = (\frac{z_0}{x_0})^2 - b(\frac{y_0}{z_0})^2 = N(\frac{z_0}{x_0} + \sqrt{b}\frac{y_0}{z_0})$. The converse follows similarly. □

The Hilbert symbol has the following basic properties regardless of the field K:

Proposition 4.2. *For all $a, b, c \in K^\times$ we have*

(*i*) $(a, b) = (b, a)$, $(a, bc^2) = (a, b)$;

(*ii*) $(1, a) = (a, -a) = (a, 1 - a) = 1$;

(iii) $(a, bc) = (a, b)(a, c)$ *if* $(a, c) = 1$.

Proof. *(i)* and *(ii)* are obvious from the definition. For *(iii)* use Proposition 4.1 and note that the norm is multiplicative. □

So far K could have been an arbitrary field of characteristic different from 2. However, in case $K = \mathbb{Q}_v$ ($v \in P \cup \{\infty\}$) we can say more: the hilbert symbol $(a, b)_v$ is bilinear, ie. property *(iii)* holds without the assumption $(a, c)_v = 1$. In case $v = \infty$ one can see this directly: we have $(a, b)_\infty = -1$ if and only if both a and b are negative therefore we indeed have $(a, bc)_\infty = (a, b)_\infty (a, c)_\infty$. The case of finite primes is more involved, we need a couple of Lemmas.

Lemma 4.3. *Assume $p \neq 2$ and $a, b, c \in \mathbb{Z}_p^\times$. Then the equation $ax^2 + by^2 + cz^2 = 0$ has a nontrivial (primitive) solution in $\mathbb{Z}_p$ (hence in $\mathbb{Q}_p$). In particular, we have $(a, b)_p = 1$ if $a, b \in \mathbb{Z}_p^\times$.*

Proof. This is similar to Lemma 3.4, so we leave the details to the reader. We may take $z = 1$. □

Lemma 4.4. *Assume $p \neq 2$ and $u \in \mathbb{Z}_p$ is not a square mod p, ie. $\left(\frac{u}{p}\right) = -1$. Then we have $(u, p)_p = -1$.*

Proof. Assume we have $z^2 - ux^2 - py^2 = 0$ for some $x, y, z \in \mathbb{Q}_p$ not all 0. By rescaling we may assume $x, y, z \in \mathbb{Z}_p$ not all divisible by p. Looking at the equation mod p we find that p must divide x since $\left(\frac{u}{p}\right) = -1$. □

Theorem 4.5. *Assume $p \neq 2$ and put $a = p^\alpha s$, $b = p^\beta t$. Then we have the following formula for the Hilbert symbol at p:*

$$(a, b)_p = (-1)^{\alpha\beta \frac{p-1}{2}} \left(\frac{s}{p}\right)^\beta \left(\frac{t}{p}\right)^\alpha .$$

In particular, $(\cdot, \cdot)_p \colon \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \times \mathbb{Q}_p^\times/(\mathbb{Q}_p^\times)^2 \to \{\pm 1\}$ is bilinear nondegenerate pairing.

Proof. By Proposition 4.2(i) and Corollary 2.8 we are reduced to a finite computation of Hilbert symbols (among $1, u, p, up$). The statement follows from Lemmas 4.3 and 4.4 by a computation using the properties in Proposition 4.2. □

Theorem 4.6. *Let $a = 2^\alpha s, b = 2^\beta t \in \mathbb{Q}_2$ with $s, t \in \mathbb{Z}_2^\times$. Then we have*

$$(a, b)_2 = (-1)^{\varepsilon(s)\varepsilon(t) + \alpha\omega(t) + \beta\omega(s)}$$

where $\varepsilon(s) \equiv \frac{s-1}{2} \pmod 2$ and $\omega(s) \equiv \frac{s^2-1}{8} \pmod 2$. In particular, $(\cdot, \cdot)_2 \colon \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \times \mathbb{Q}_2^\times/(\mathbb{Q}_2^\times)^2 \to \{\pm 1\}$ is bilinear and nondegenerate.

Proof. By Corollary 2.8 we only need to check the above identity when $a, b \in \{\pm 1, \pm 2, \pm 5, \pm 10\}$ which is a tedious, but finite computation that we omit. □

5 Global properties of the Hilbert symbol

The goal of this section is to formulate relations between $(a, b)_p$ for fixed nonzero rational numbers a, b and varying p. This is closely related to Gauss' quadratic reciprocity law. Further, for fixed $a \in \mathbb{Q}$ and signs $\varepsilon_v \in \{\pm 1\}$ for $v \in P \cup \{\infty\}$ we would like to give necessary and sufficient conditions on the existence of $b \in \mathbb{Q}$ with $(a, b)_v = \varepsilon_v$ for all $v \in P \cup \{\infty\}$. The latter involves the existence of primes in arithmetic progressions due to Dirichlet.

Let $p \neq q$ be odd primes. Then by Lemma 4.4 the Hilbert symbol $(p,q)_p$ is equal to 1 if and only $q$is a square mod p. In other words, we have the identity $(p,q)_p = \left(\frac{q}{p}\right)$. Moreover, by Theorem 4.6 we have $(p,q)_2 = (-1)^{\varepsilon(p)\varepsilon(q)} = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}$. By the same argument we also have $(-1,p)_p = (-1)^{\frac{p-1}{2}} = (-1,p)_2$. Therefore Gauss' quadratic reciprocity law reads in this language

Theorem 5.1 (quadratic reciprocity law)**.** *For odd primes $p \neq q$ we have*

$$(p,q)_q = \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{q}{p}\right) = (p,q)_2(p,q)_p \ .$$

On the other hand, we have

$$(2,p)_p = \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = (2,p)_2 \ .$$

Putting all the above information we deduce

Theorem 5.2 (Hilbert's reciprocity law)**.** *For all $a,b \in \mathbb{Q}^\times$ we have*

(i) $(a,b)_p = 1$ *for all but finitely many primes p;*

(ii) $\prod_{v \in P \cup \{\infty\}} (a,b)_v = 1.$

Proof. Whenever $a,b \in \{-1\} \cup P$, the statement follows from the formulae above for the Hilbert symbol and the quadratic reciprocity law. For general a,b we deduce the statement from the bilinearity of the local Hilbert symbols. □

Theorem 5.3. *Let I be a finite index set and $a_i \in \mathbb{Q}^\times$ a nonzero rational number for each $i \in I$. Assume further we are given signs $\varepsilon_{i,v} \in \{\pm 1\}$ for all $i \in I$ and $v \in P \cup \{\infty\}$. There is an $x \in \mathbb{Q}^\times$ such that $(a_i,x)_v = \varepsilon_{i,v}$ for all $i \in I$ and $v \in P \cup \{\infty\}$ if and only if the following three conditions are satisfied:*

(1) $\varepsilon_{i,v} = 1$ *for all but finitely many $v \in P \cup \{\infty\}$.*

(2) *We have $\prod_{v \in P \cup \{\infty\}} \varepsilon_{i,v} = 1$ for all $i \in I$.*

(3) *For all $v \in P \cup \{\infty\}$ there exists an element $x_v \in \mathbb{Q}_v^\times$ such that $(a_i, x_v) = \varepsilon_{i,v}$ for all $i \in I$.*

Proof. The necessity of conditions (1) and (2) follow from Hilbert's reciprocity law (Thm. 5.2). Further, if $x \in \mathbb{Q}^\times$ is a global solution then one can take $x_v = x$ in (3).

For the converse assume we are given $a_i \in \mathbb{Q}^\times$ and $\varepsilon_{i,v} \in \{\pm 1\}$ for all $i \in I$ and $v \in P \cup \{\infty\}$ satisfying (1), (2), and (3). We may assume without loss of generality that all a_i are squarefree integers since $(a_i c_i^2, b)_v = (a_i, b)_v$ for all $v \in P \cup \{\infty\}$ and $b, c_i \in \mathbb{Q}^\times$. Put

$$\begin{aligned} S &:= \{\infty, 2\} \cup \{p \in P \mid \exists i \in I \text{ s.t. } p \mid a_i\} \\ T &:= \{v \in P \cup \{\infty\} \mid \exists i \in I \text{ s.t. } \varepsilon_{i,v} = -1 \ . \end{aligned}$$

By our assumptions both S and T are finite subsets of $P \cup \{\infty\}$.

Case 1: $S \cap T = \emptyset$. In particular note that $\infty \notin T$ as $\infty \in S$. Put

$$a := \prod_{\ell \in T} \ell \qquad \text{and} \qquad m := 8 \prod_{p \in S \setminus \{2,\infty\}} p \ .$$

By our assumption $S \cap T = \emptyset$ the integers a and m are coprime, so we may use Dirichlet's theorem to find a prime $q \notin S \cup T$ such that $q \equiv a \pmod{m}$. We claim that $x := aq$ satisfies $(a_i, x)_v = \varepsilon_{i,v}$ for all $i \in I$ and $v \in P \cup \{\infty\}$. We check this case by case:

1. $v \in S$. In this case we have $\varepsilon_{i,v} = 1$ by the assumption $S \cap T = \emptyset$. For $v = \infty$ we find $(a_i, aq)_\infty = 1$ since $aq > 0$. For $v = p \neq 2 \in S$ we note $q \equiv a \pmod p$ as $p \mid m$, so $x = aq \equiv a^2 \pmod p$, ie. $\left(\frac{x}{p}\right) = 1$ whence $(a_i, x)_p = 1$ by Theorem 4.5. Similarly, for $v = 2 \in S$ we have $x \equiv a^2 \equiv 1 \pmod 8$ showing $(x, a_i)_2 = 1$ by Theorem 4.6.

2. $v = \ell \in T$. So $\ell \notin S$, ie. $\ell \neq \infty, 2$ and $a_i \in \mathbb{Z}_\ell^\times$ for all $i \in I$. Therefore Theorem 4.5 reads in this case
$$(a_i, b)_\ell = \left(\frac{a_i}{\ell}\right)^{v_\ell(b)} \qquad \forall b \in \mathbb{Q}_\ell^\times \ .$$
By condition (3) there exists an $x_\ell \in \mathbb{Q}_\ell^\times$ such that $\left(\frac{a_i}{\ell}\right)^{v_\ell(x_\ell)} = (a_i, x_\ell)_\ell = \varepsilon_{i,\ell}$ for all $i \in I$. Moreover, $\ell \in T$ means there exists an index $i \in I$ with $\varepsilon i, \ell = -1$ showing $v_\ell(x_\ell)$ must be odd. On the other hand, we have $v_\ell(aq) = 1 (\equiv v_\ell(x_\ell) \pmod 2)$ as $q \notin T$ and $\ell \mid a$, but $\ell^2 \nmid a$ by construction. So we have
$$(a_i, x)_\ell = \left(\frac{a_i}{\ell}\right)^{v_\ell(x)} = \left(\frac{a_i}{\ell}\right)^{v_\ell(x_\ell)} = (a_i, x_\ell)_\ell = \varepsilon_{i,\ell}$$
for all $i \in I$ as desired.

3. $\ell \notin S \cup T \cup \{q\}$. In this case we have $\varepsilon_{i,\ell} = 1$, $a_i \in \mathbb{Z}_\ell^\times$ for all $i \in I$ and $x = aq \in \mathbb{Z}_\ell^\times$, too, whence $(a_i, x)_\ell = 1$ by Lemma 4.3.

By the discussion above the only exception where possibly $(a_i, x)_\ell \neq \varepsilon_{i,\ell}$ is $\ell = q$ not treated by the above 3 cases. This is the point where Dirichlet's Theorem—that we could choose $q \equiv a \pmod m$ to be a prime—comes into force. Indeed, by Hilbert's reciprocity law (Thm. 5.2) and condition (2) the equality $(a_i, x)_\ell = \varepsilon_{i,\ell}$ must fail at an even number of places, so it cannot just be the single place $\ell = q$. This shows we have $(a_i, x)_q = \varepsilon_{i,q}$ proving the result in Case 1.

Case 2: This is the general case where we no longer assume $S \cap T = \emptyset$. By assumption (3) there exists an element $x_v \in \mathbb{Q}_v^\times$ for all $v \in S$ such that $(x_v, a_i)_v = \varepsilon_{i,v}$ for all $i \in I$. In order to proceed further we need the following approximation theorem.

Lemma 5.4. *Assume $S \subset P \cup \{\infty\}$ is a finite set. Then the diagonal embedding $\mathbb{Q} \hookrightarrow \prod_{v \in S} \mathbb{Q}_v$ has dense image where the right hand side is given the product topology of the topologies induced by the v-adic absolute values on $\mathbb{Q}_v$ ($v \in S$).*

Proof. We may increase S to have $\infty \in S$, so we may assume $S = \{\infty, p_1, \ldots, p_n\}$. The density in the product topology means that for all $(x_\infty, x_1, \ldots, x_n) \in \prod_{v \in S} \mathbb{Q}_v = \mathbb{R} \times \mathbb{Q}_{p_1} \times \cdots \times \mathbb{Q}_{p_n}$, $\varepsilon > 0$ and $N \in \mathbb{Z}^{>0}$ there exists a rational number $x \in \mathbb{Q}$ such that $|x - x_\infty|_\infty \leq \varepsilon$ and $v_{p_i}(x - x_i) \geq N$ ($\Leftrightarrow |x - x_i|_{p_i} \leq p^{-N}$) ($i = 1, \ldots, n$). Replacing $(x_\infty, x_1, \ldots, x_n)$ by $((p_1 \ldots p_n)^M x_\infty, (p_1 \ldots p_n)^M x_1, \ldots, (p_1 \ldots p_n)^M x_n)$, ε by $\frac{\varepsilon}{(p_1 \ldots p_n)^M}$ and N by $N + M$ for some large enough M we may assume without loss of generality that x_i belongs to $\mathbb{Z}_{p_i}$ for all $i = 1, \ldots, n$. By the Chinese Remainder Theorem there exists an integer $x_0 \in \mathbb{Z}$ such that $x_0 \equiv x_i \pmod{p_i^N}$ for all $i = 1, \ldots, n$ as the prime powers p_i^N are pairwise coprime. Pick a prime q different from $p_1, \ldots, p_n$ and choose $L > 0$ so that $\frac{(p_1 \ldots p_n)^N}{q^L} < \varepsilon$. Then for any integer $u \in \mathbb{Z}$ and $i = 1, \ldots, n$ we have
$$|x_0 + \frac{u(p_1 \ldots p_n)^N}{q^L} - x_i|_{p_i} \leq \max(|x_0 - x_i|_{p_i}, |\frac{u(p_1 \ldots p_n)^N}{q^L}|_{p_i}) \leq p^{-N} \ .$$
On the other hand, we may choose $u \in \mathbb{Z}$ such that $|x_0 - x_\infty + \frac{u(p_1 \ldots p_n)^N}{q^L}|_\infty < \varepsilon$ so that $x := x_0 + \frac{u(p_1 \ldots p_n)^N}{q^L}$ satisfies all the required conditions. □

Note that the square elements $(\mathbb{Q}_v^\times)^2$ form an open subset of $\mathbb{Q}_v$: Indeed, in case $v = \infty$ this is obvious as all positive numbers are squares in $\mathbb{R}$. In case $v = p \neq 2$ is a prime this follows from Proposition 2.6 and in case $v = 2$ from Proposition 2.7. So we may apply Lemma 5.4 to find an element $x' \in \mathbb{Q}^\times$ such that $\frac{x'}{x_v}$ is a nonzero square in $\mathbb{Q}_v$ for all $v \in S$. In particular, we deduce $(a_i, x')_v = (a_i, x_v)_v = \varepsilon_{i,v}$ for all $i \in I$ and $v \in S$. Put $\eta_{i,\ell} := \varepsilon_{i,\ell}(a_i, x')_\ell$ for $\ell \in P \cup \{\infty\}$. The new bunch of signs $(\eta_{i,\ell})_{i\in I, \ell\in P\cup\{\infty\}}$ satisfies $(1), (2), (3)$ by Theorem 5.2 (applied to $(a_i, x')_\ell$) since so does $(\varepsilon_{i,\ell})_{i\in I,\ell\in P\cup\{\infty\}}$. Further, we have $\eta_{i,v} = 1$ for all $v \in S$ by construction. Therefore we may apply Case 1 to find an element $y \in \mathbb{Q}^\times$ satisfying $(a_i, y)_\ell = \eta_{i,\ell}$ for all $i \in I$ and $\ell \in P \cup \{\infty\}$. By the bilinearity of the Hilbert symbol $x := x'y$ satisfies $(a_i, x)_\ell = \varepsilon_{i,\ell}$ for all $i \in I$ and $\ell \in P \cup \{\infty\}$ deducing the theorem in the general case. □

6 Proof of the Hasse–Minkowski Theorem

In order to prove the main theorem in this minicourse we need to recall some generalities on quadratic forms (valid over any field K of characteristic different from 2). Let $f(x_1, \dots, x_n) = \sum_{1\leq i\leq j\leq n} a_{i,j}x_ix_j \in K[x_1, \dots, x_n]$ be a quadratic form, ie. a homogeneous polynomial of degree 2. To f we associate the symmetric matrix $A_f := \begin{pmatrix} a_{1,1} & & & \\ & \ddots & \frac{a_{i,j}}{2} & \\ & \frac{a_{i,j}}{2} & \ddots & \\ & & & a_{n,n} \end{pmatrix}$ so that we have $f(x_1, \dots, x_n) = \begin{pmatrix} x_1 & \cdots & x_n \end{pmatrix} A_f \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$.
We put $\beta_f \colon K^n \times K^n \to K$ for the associated symmetric bilinear form given by the formula $\beta_f(u, w) = u^T A_f w$.

Definition. We call the form β *nondegenerate* if for all $0 \neq w \in K^n$ there is a $u \in K^n$ such that $\beta(u, w) \neq 0$. We call a quadratic form f nondegenerate if the associated symmetric bilinear form β_f is nondegenerate.

By quotienting out by the radical $\operatorname{rad}\beta = \{w \in K^n \mid \beta(u, w) = 0 \ \forall u \in K^n\}$ (or equivalently reducing the number of variables after a suitable change of basis) we may assume from now on that β is nondegenerate.

Definition. We call the symmetric bilinear form β *isotropic* if there exists a nonzero vector $0 \neq w \in K^n$ with $\beta(w, w) = 0$.

Recall that in this language Theorem 3.1 states that a symmetric bilinear form β over $\mathbb{Q}$ is isotropic over $\mathbb{Q}$ if and only if β is isotropic over $\mathbb{Q}_v$ for all $v \in P \cup \{\infty\}$.

Lemma 6.1. *Assume β is isotropic and nondegenerate. Then for all $a \in K$ there is a vector $w \in K^n$ such that $\beta(w, w) = a$ (we say that a is* represented *by the quadratic form $\beta(u, u)$).*

Proof. Since β is isotropic, there is a vector $u \neq 0 \in K^n$ with $\beta(u, u) = 0$. On the other hand, β is nondegenerate, so there is a $y \in K^n$ such that $\beta(u, y) \neq 0$. We look for w in the form $w = cu + y$ ($c \in K$ given later). We compute

$$\beta(cu + y, cu + y) = c^2\beta(u, u) + 2c\beta(u, y) + \beta(y, y) \ .$$

Therefore $c := \frac{a-\beta(y,y)}{2\beta(u,y)}$ will do as $\operatorname{char} K \neq 2$. □

Proposition 6.2. *Let $f(x_1, \dots, x_n)$ be a nondegenerate quadratic form over K with* $\operatorname{char} K \neq 2$. *Then f represents $a \in K$ if and only if the form $f(x_1, \dots, x_n) - ax_0^2$ (in $n + 1$ variables, x_0 being a new variable) is isotropic.*

Proof. Note that $a = 0$ is always represented and $f(x_1, \dots, x_n) - 0x_0^2$ is indeed isotropic by the choice $x_0 = 1$, $x_1 = \cdots = x_n = 0$. Now assume $a \neq 0$. If f is isotropic then by Lemma 6.1 f represents a and in this case $f - ax_0^2$ is also isotropic. So assume f is not isotropic, but $f - ax_0^2$ is. Then there are elements $\alpha_0, \alpha_1, \dots, \alpha_n \in K$, not all zero, such that $f(\alpha_1, \dots, \alpha_n) - a\alpha_0^2 = 0$. Since f is not isotropic, we must have $\alpha_0 \neq 0$ whence $a = f(\frac{\alpha_1}{\alpha_0}, \dots, \frac{\alpha_n}{\alpha_0})$ is represented by f. □

With all this preparation at hand, we can now start the

Proof of Theorem 3.1. Pick a quadratic form f over $\mathbb{Q}$. By the Gram–Schmidt orthogonalization we may assume f is in diagonal form $f = a_1x_1^2 + \cdots + a_nx_n^2$ ($a_1 \dots a_n \neq 0$). Further, by rescaling the variables and multiplying by a constant we may, as well, assume that a_i are square-free integers ($i = 1, \dots, n$) and $a_1 = 1$. We shall proceed by induction on n, but we need to distinguish all $n \leq 4$. The case $n = 1$ is trivial: in this f cannot be isotropic locally either.

1. $n = 2$. Then $f = x_1^2 - ax_2^2$ where $a > 0$ since f is isotropic over $\mathbb{R}$. Further, a is a square in $\mathbb{Q}_p$ therefore $v_p(a)$ is even for all primes p. So a is a square in $\mathbb{Q}$ since all primes are on even exponent in the prime decomposition.

2. $n = 3$, $f = x_1 - ax_2^2 - bx_3^2$ with $a, b \in \mathbb{Z}$ squarefree. We also assume $|a| \leq |b|$ by symmetry. We proceed by induction on $m := |a| + |b|$. The case $m = 2$ is obvious since the form $x_1^2 \pm x_2^2 \pm x_3^2$ has a nontrivial rational root unless both signs are $+$ in which case the form is not isotropic over $\mathbb{R}$, either. So let $m > 2$ whence $|b| \geq 2$. Write $b = \pm p_1 \dots p_k$ in prime decomposition. Since the form $x_1^2 - ax_2^2 - bx_3^2$ is isotropic over $\mathbb{Q}_v$, we have $(a, b)_v = 1$ for all $v \in P \cup \{\infty\}$ by the definition of the Hilbert symbol. So by Theorem 4.5 we have $p_i \mid a$ or $\left(\frac{a}{p_i}\right) = 1$ ($i = 1, \dots, k$) as we have $v_{p_i}(b) = 1$. Either way the congruence $x^2 \equiv a \pmod{p_i}$ has a solution for all $i = 1, \dots, n$. Hence by the Chinese Remainder Theorem a is a square modulo b, too. In particular there exists an integer t with $|t| \leq \frac{|b|}{2}$ such that $t^2 \equiv a \pmod{b}$, ie. $t^2 = a + bb'$ with $|b'| < |b|$. This equation reads $t^2 - a \cdot 1^2 - bb' \cdot 1^2 = 0$ meaning $(a, bb')_v = 1$ for all $v \in P \cup \{\infty\}$. So by the multiplicativity of the local Hilbert symbols we deduce $(a, b')_v = (a, b^2b')_v = (a, b)_v(a, bb')_v = 1$ for all $v \in P \cup \{\infty\}$. Since $|a| + |b'| < |a| + |b|$, using the induction we deduce that the form $x_1^2 - ax_2^2 - b'x_3^2$ is isotropic over $\mathbb{Q}$. In particular, both b' and bb' are norms of elements of $\mathbb{Q}(\sqrt{a})$ by Proposition 4.1. Therefore their quotient b is also a norm from $\mathbb{Q}(\sqrt{a}$ whence $x_1^2 - ax_2^2 - bx_3^2$ is also isotropic over $\mathbb{Q}$ (using Proposition 4.1 again in the reverse direction).

3. $n = 4$, $f = (ax_1^2 + bx_2^2) - (cx_3^2 + dx_4^2)$. We need a common value of the binary forms $ax_1^2 + bx_2^2$ and $cx_3^2 + dx_4^2$.

   Lemma 6.3. *For all $v \in P \cup \{\infty\}$ there exists $0 \neq x_v \in \mathbb{Q}_v$ such that x_v is represented by both forms $ax_1^2 + bx_2^2$ and $cx_3^2 + dx_4^2$.*

   Proof. There is a common value nontrivially as f is isotropic over $\mathbb{Q}_v$. Now if this common value is 0 then at least one of the two binary forms is isotropic over $\mathbb{Q}_v$ (as it represents 0 nontrivially). By Lemma 6.1 isotropic forms represent any element in $\mathbb{Q}_v$ so we just need to pick a nonzero value of the other form which certainly exists. □

   So we pick these elements $x_v \in \mathbb{Q}_v$ for all $v \in P \cup \{\infty\}$. By Proposition 6.2 both forms

$$x_vz^2 - ax_1^2 - bx_2^2 \qquad \text{and} \qquad x_vz^2 - cx_3^2 - dx_4^2$$

are isotropic over $\mathbb{Q}_v$. So we compute

$$1 = \left(\frac{a}{x_v}, \frac{b}{x_v}\right)_v = (ax_v, bx_v)_v = (ax_v, -abx_v^2)_v =$$
$$= (ax_v, -ab)_v = (a, -ab)_v(x_v, -ab)_v = (a, b)_v(x_v, -ab)_v$$

which implies $(x_v, -ab)_v = (a, b)_v$ and by a similar computation $(x_v, -cd)_v = (c, d)_v$ for all $v \in P \cup \{\infty\}$. By Theorem 5.2 we have $\prod_{v\in P\cup\{\infty\}}(a, b)_v = 1 = \prod_{v\in P\cup\{\infty\}}(c, d)_v$ whence we have $\prod_{v\in P\cup\{\infty\}}(x_v, -ab)_v = 1 = \prod_{v\in P\cup\{\infty\}}(x_v, -cd)_v$. Further, $(a, b)_v = -1$ or $(c, d)_v = -1$ for only finitely many places v. Therefore we may apply Theorem 5.3 with $a_1 = -ab$, $a_2 = -cd$, $\varepsilon_{1,v} = (x_v, -ab)_v = (a, b)_v$, $\varepsilon_{2,v} = (x_v, -cd)_v = (c, d)_v$ since condition (3) is also satisfied by the given $x_v \in \mathbb{Q}_v^\times$ ($v \in P \cup \{\infty\}$). So we find an element $x \in \mathbb{Q}^\times$ such that $(x, -ab)_v = (a, b)_v$ and $(x, -cd)_v = (c, d)_v$ for all $v \in P \cup \{\infty\}$. By the same computation as above (x_v replaced by x), we deduce $\left(\frac{a}{x}, \frac{b}{x}\right)_v = 1 = \left(\frac{c}{x}, \frac{d}{x}\right)_v$ for all $v \in P \cup \{\infty\}$. Hence the quadratic forms $ax_1^2 + bx_2^2 - xz^2$ and $cx_3^2 + dx_4^2 - xz^2$ are both isotropic locally everywhere which implies by the case $n = 3$ already proven above that they are also isotropic over $\mathbb{Q}$. By Proposition 6.2 both binary forms $ax_1^2 + bx_2^2$ and $cx_3^2 + dx_4^2$ represent $x \neq 0$ showing f is isotropic over $\mathbb{Q}$.

Finally assume $n \geq 5$. In this case we do induction on n. Pick a form

$$f = a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + \cdots + a_nx_n^2 = h - g$$

where we put $h = a_1x_1^2 + a_2x_2^2$ and $g = -(a_3x_3^2 + \cdots + a_nx_n^2)$ and assume $a_1, \ldots, a_n \in \mathbb{Z}$ are squarefree. As above we look for common values of g and h. Put

$$S := \{\infty, 2\} \cup \{p \in P \mid \exists i \geq 3 \colon p \mid a_i\} ,$$

this is a finite set. As in Lemma 6.3, for all $v \in S$ there exists an element $0 \neq a_v \in \mathbb{Q}_v$ such that a_v is represented by both forms g and h, ie. we have $x_1^v, x_2^v, x_3^v, \ldots, x_n^v \in \mathbb{Q}_v$ such that

$$h(x_1^v, x_2^v) = a_v = g(x_3^v, \ldots, x_n^v) .$$

Since $a_v(\mathbb{Q}_v^\times)^2$ is open in $\mathbb{Q}_v$ and $h \colon \mathbb{Q}_v \times \mathbb{Q}_v \to \mathbb{Q}_v$ is continuous (in the v-adic topology), there exist open neighbourhoods $x_1^v \in U_1^v \subset \mathbb{Q}_v$ and $x_2^v \in U_2^v \subset \mathbb{Q}_v$ such that the image of h on $U_1^v \times U_2^v$ is contained in $a_v(\mathbb{Q}_v^\times)^2$. By Lemma 5.4 (applied twice) there exist $x_1, x_2 \in \mathbb{Q}$ such that $x_j \in U_j^v$ for all $v \in S$ and $j = 1, 2$. We put $a := h(x_1, x_2) \neq 0$ and claim that a is a common value of g and h over $\mathbb{Q}$. By construction a is represented by h over $\mathbb{Q}$ so by Proposition 6.2 we are reduced to showing that the $n - 1$-variable form

$$f_1 = az^2 - g(x_3, \ldots, x_n)$$

is isotropic over $\mathbb{Q}$. By induction, we only need to check that f_1 is isotropic locally everywhere. If v lies in S then $\frac{a}{a_v}$ is a square in $a = h(x_1, x_2) \in h(U_1^v, U_2^v) \subseteq a_v(\mathbb{Q}_v^\times)^2$, ie. there exists $u_v \in \mathbb{Q}_v^\times$ such that $a = a_vu_v^2 = g(x_3^v, \ldots, x_n^v)u_v^2 = g(x_3^vu_v, \ldots, x_n^vu_v)$ is represented by g locally at v. On the other hand if $v \in (P \cup \{\infty\}) \setminus S$ then $a_3, \ldots, a_n$ are v-adic units (ie. lie in $\mathbb{Z}_v^\times$) whence g is isotropic locally at v by Lemma 4.3 and represents a by Lemma 6.1. □

Corollary 6.4. *Let a be in $\mathbb{Q}^\times$ and f be a quadratic form over $\mathbb{Q}$. Then f represents a over $\mathbb{Q}$ if and only if it represents a over $\mathbb{Q}_v$ for all $v \in P \cup \{\infty\}$.*

Proof. We apply Theorem 3.1 on the form $az^2 - f$ and deduce the statement from Proposition 6.2. □

Remark. Assume $n \geq 5$ and p is a prime. Then all nondegenerate forms in n variables are isotropic over $\mathbb{Q}_p$. In particular, if f is a nondegenerate quadratic form over $\mathbb{Q}$ in $n \geq 5$ variables then f is isotropic over $\mathbb{Q}$ if and only if it is isotropic over $\mathbb{R}$ (ie. it is indefinite).

Proof. It suffices to treat the case $n = 5$ so let $f = a_1x_1^2 + \cdots + a_5x_5^2$. By rescaling the variables we may assume $a_1, \ldots, a_5$ are all in $\mathbb{Z}_p$ but not divisible by p^2. Further, there are either at least 3 indices $1 \leq i \leq 5$ with $v_p(a_i) = 0$ or at least 3 indices with $v_p(a_i) = 1$. Note that f is isotropic if and only if so is pf, so we may even assume that there are at least 3 indices i with $v_p(a_i) = 0$. In case $p \neq 2$ the remark follows from Lemma 4.3. In case $p = 2$ one checks by a direct computation that all elements mod 8 are represented by any 4-variable form $a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2$ where a_1, a_2, a_3 are all odd. Finally one applies Proposition 2.7. □

References

[1] John William Scott Cassels. *Lectures on Elliptic Curves.* Number 24. Cambridge University Press, 1991.

[2] Keith Conrad. Selmer's example. *https://kconrad.math.uconn.edu/blurbs/gradnumthy/selmerexample.pdf*, 2017.

[3] F. Q. Gouvêa. *p-adic Numbers, An Introduction.* Springer, Heidelberg, 1997.

[4] J.-P. Serre. *A course in arithmetic.* Springer, New York, 1993.