THE HASSE-MINKOWSKI LOCAL-GLOBAL PRINCIPLE

ENDER MINYARD

1. Introduction

This note serves to provide an exposition of the proof of the following theorem:

Theorem 1.1 (Hasse-Minkowski)**.** *Let $f \in \mathbb{Q}[x_1, \ldots, x_n]$ be a rational quadratic form. Then $\exists X \in \mathbb{Q}^n$ with $f(X) = 0$ if and only if $\exists Y \in \mathbb{R}^n$ with $f(Y) = 0$ and for all primes $p, \exists Z \in \mathbb{Q}_p^n$ with $f(Z) = 0$.*

We will introduce $\mathbb{Q}_p$ and the rest of the characters next section, but for now, are happy to note the definition of a quadratic form:

Definition 1. *Let K be a field. A quadratic form over K is a degree-two polynomial in n variables of the form*

$$f(X) = f(x_1, \ldots, x_n) = \sum_{1 \le i,j \le n} a_{ij} x_i x_j$$

with $a_{ij} \in K^*$ for each i, j. The group $\mathrm{GL}_n(K)$ of invertible $n \times n$ matrices acts on such an f by

$$A \cdot f(X) = f(AX).$$

It is standard [1] *that f can be "diagonalized," i.e. there is some $A \in \mathrm{GL}_n(K)$ such that*

$$f(AX) = a_1 x_1^2 + \cdots + a_n x_n^2,$$

and we will always assume this is the case. The number $\#\{i : a_i \neq 0\}$ is called the rank of f. We define discriminant of f to be

$$d(f) = a_1 \cdots a_n.$$

For $a \in K$, we say f represents a if there exists $(X_1, ..., X_N) \in K^n$ with $(X_1, ..., X_N) \neq (0, ..., 0)$ such that

$$f(X_1, ..., X_N) = a.$$

Remark 1. *We note that if one writes $f = g - h$ where g and h are also quadratic forms over K, then f represents 0 over K iff there is some $b \in K$ such that both f and g represent*

Date: December 9, 2025.

(just take $b := g(X) = h(X) \in K$, where $X \in K^n$ is such that $f(X) = 0$). We use this freely throughout proofs.

The author finds this work interesting because of the relationship between quadratic forms and post-quantum cryptography. If it were possible to determine the lowest integer value represented by an arbitrary quadratic form corresponding to a lattice, for example, this would undermine many lattice-based cryptographic protocols. Guaranteeing that 0 is represented by a quadratic form with rational (equivalently, integer) coefficients can be seen as the first step towards investigating these matters.

2. First Definitions

Definition 2. *A field is a set $\mathbb{F}$ together with two binary operations on $\mathbb{F}$, addition and multiplication, that interact "reasonably." We let $\mathbb{F}^* := \mathbb{F} \setminus \{0\}$.*

The following axioms are required to hold for all elements a, b, c of the field $\mathbb{F}$:

- Additive and multiplicative identity: There exist two distinct elements 0 and 1 in $\mathbb{F}$ such that $a + 0 = a$ and $a * 1 = a$.
- Associativity of addition and multiplication: $a+(b+c) = (a+b)+c$, and $a*(b*c) = (a*b)*c$.
- Commutativity of addition and multiplication: $a + b = b + a$, and $a * b = b * a$.
- Additive inverses: For every a in $\mathbb{F}$, there exists an element in $\mathbb{F}$, denoted $-a$, called the additive inverse of a, such that $a + (-a) = 0$.
- Multiplicative inverses: For every $a \neq 0$ in $\mathbb{F}$, there exists an element in $\mathbb{F}$, denoted by a^{-1} or $1/a$, called the multiplicative inverse of a, such that $a * a^{-1} = 1$.
- Distributivity of multiplication over addition: $a * (b + c) = (a * b) + (a * c)$.

Example 1. *In $\mathbb{Q}$, take 2 and $\frac{1}{2}$. Adding 2 to $\frac{1}{2}$ produces another element of $\mathbb{Q}$, $\frac{5}{2}$. Subtracting $\frac{1}{2}$ from 2 produces an element of $\mathbb{Q}$, $\frac{3}{2}$. Multiplying 2 by $\frac{1}{2}$ produces the identity element, 1, while staying inside the field.*

Example 2. *In $\mathbb{R}$, take 3 and $\frac{1}{3}$. Adding 3 to $\frac{1}{3}$ produces another element of $\mathbb{R}$, $\frac{10}{3}$. Subtracting $\frac{1}{3}$ from 3 produces an element of $\mathbb{Q}$, $\frac{8}{3}$. Multiplying 3 by $\frac{1}{3}$ produces the identity element, 1, while staying inside the field $\mathbb{R}$.*

Example 3. *In $\mathbb{C}$, take i. Adding i to i produces another element of $\mathbb{C}$, $0 + 2i$. Subtracting i from i produces another element of $\mathbb{C}$, $0 + 0i$. Multiplying i^2 by i^2 produces the identity element, 1, while staying inside the field $\mathbb{C}$.*

Example 4. *$\mathbb{Z}/p\mathbb{Z} := \mathbb{F}_p$ is a field because elements of this field which are added together and multiplied by each other stay in the field. Also, members of $\mathbb{Z}/p\mathbb{Z}$ can possess a multiplicative inverse which can be found using the Euclidean algorithm.*

Definition 3. *Fix a prime number $p \in \mathbb{Z}$. The p-adic valuation on $\mathbb{Z}$ is the function*

$$\nu_p : \mathbb{Z} - \{0\} \to \mathbb{R}$$

defined as follows: for each integer $n \in \mathbb{Z}, n \neq 0$, let $\nu_p(n)$ be the unique positive integer satisfying

$$n = p^{\nu_p(n)} n'$$

with

$$p \nmid n'.$$

We extend ν_p to the field of rational numbers as follows: if $x = \frac{a}{b} \in \mathbb{Q}^*$, then

$$\nu_p(x) = \nu_p(a) - \nu_p(b)$$

.

Definition 4. *For any nonzero $x \in \mathbb{Q}$, we define the p-adic absolute value at x by*

$$|x|_p = p^{-\nu_p(x)}.$$

We extend this to all of $\mathbb{Q}$ by defining $|0|_p = 0$. [2]

Example 5. *The 3-adic absolute value at 9 is $\frac{1}{3^{\nu_3(9)}} = \frac{1}{9}$.*

Definition 5. *The p-adic rational numbers $\mathbb{Q}_p$ consist of all numbers of the form*

$$x = \sum_{n \geq -n_0} a_n p^n$$

with

$$0 \leq a_n \leq p - 1$$

and

$$-n_0 = \nu_p(x) \in \mathbb{Z},$$

where the series may contain infinitely many terms.

The p-adic expansion for a positive integer replaces the number 10 in the base 10 number system (in other words, decimals) with a prime number p.

Example 6. *Since $320 = 5 + 3 * 7 + 6 * 7^2$ in base 7, we can see that $\frac{320}{49} = 5 * 7^{-2} + 3 * 7^{-1} + 6$ is a rational number, but can be considered in $\mathbb{Q}_7$ as well.* [2]

Since $\mathbb{Q}_p$ is a field, every non-zero element of $\mathbb{Q}_p$ is a unit, meaning that it has a multiplicative inverse. The same cannot be said for the following subset:

Definition 6. *The ring of p-adic integers is the subset of $\mathbb{Q}_p$ defined by*

$$\mathbb{Z}_p = \left\{ \sum_{n=0}^{\infty} a_n p^n : 0 \leq a_n \leq p-1 \right\} = \{x \in \mathbb{Q}_p : \nu_p(x) \geq 0\} = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$$

.

Notice that using the definition $\mathbb{Z}_p = \{x \in \mathbb{Q}_p : |x|_p \leq 1\}$, $\mathbb{Z}_p$ is the p-adic analog of the unit disk in $\mathbb{C}$, where the norm there would be the usual, Euclidean absolute value. We note that both $\mathbb{Q}_p$ and $\mathbb{Z}_p$ have many other, equivalent definitions, but the basic, set-theoretic one given above will be sufficient for the proof we give!

3. Useful Lemmata

Theorem 3.1 (Chevalley-Warning (Weak Version))**.** *If $\mathbb{F}_p$ is a finite field and $f \in \mathbb{F}_p[x_1, \ldots, x_n]$ is such that $n > \deg f$, then p divides $\#\{X \in \mathbb{F}_p^n : f(X) = 0\}$. In particular, if $\deg f = 2$ and $n \geq 3$, then since $p \geq 2$, we always have a nonzero $X \in \mathbb{F}_p^n$ solving $f(X) = 0$.*

Proof.

$$\begin{aligned}
\#\{X \in \mathbb{F}_p^n : f(X) = 0\} &= \sum_{X \in \mathbb{F}_p^n} \left(1 - f^{p-1}(X)\right) && \text{by Fermat's Little Theorem} \\
&= \#\mathbb{F}_p^n - \sum_{X \in \mathbb{F}_p^n} f^{p-1}(X) \\
&\equiv 0 - 0 = 0 && \text{since } \sum_{x \in \mathbb{F}_p} x^i = 0 \text{ for } i < p-1
\end{aligned}$$

□

Lemma 3.2 (Hensel's)**.** *Let $f(x)$ be a one variable polynomial with integer coefficients and fix $k \geq 1$. Suppose that there is an integer $a \in \mathbb{Z}$ such that $f(a) \equiv 0 \mod p^k$ and $f'(a) \not\equiv 0 \mod p^k$. Then there is some $a' \in \mathbb{Z}$ such that $f(a') \equiv 0 \mod p^{k+1}$, and this a' is unique when taken with $0 \leq a' \leq p^{k+1}$ and $a \equiv a' \mod p^k$. As a corollary, if $f(x) \equiv 0 \mod p$ has a solution $a \in \mathbb{Z}$ with $f'(a) \not\equiv 0 \mod p$, there is a unique $a \in \mathbb{Q}_p$ (in fact in $\mathbb{Z}_p$) solving $f(a) = 0$.*

Hensel's Lemma allows us to determine, in many circumstances, whether a polynomial has roots in $\mathbb{Z}_p$ with relative ease [2].

Theorem 3.3 ([3, pg. 24]). *Let $(a_i)_{i\in I}$ be a finite family of elements in $\mathbb{Q}^*$ and let $(\epsilon_{i,v})_{i\in I, v\in V}$ be a family of numbers equal to ± 1. Then there exists $x \in \mathbb{Q}^*$ such that $(a_i, x)_v = \epsilon_{i,v}$ for all $i \in I, v \in V$ if and only if*

1. *Almost all the $\epsilon_{i,v}$ are equal to 1.*
2. *For all $i \in I$ we have $\prod_{v\in V} \epsilon_{i,v} = 1$, and*
3. *For all $v \in V$ there exists $x_v \in \mathbb{Q}_v^*$ such that $(a_i, x_v)_v = \epsilon_{i,v}$ for all $i \in I$.*

This is a topological theorem which explores simultaneously approximating $x_1 \in \mathbb{Q}_{p_1}, \ldots, x_n \in \mathbb{Q}_{p_n}$ by some $x \in \mathbb{Q}$, analogous to the Chinese Remainder Theorem.

Proposition 3.1 ([4, Proposition 15]). *Let f be a quadratic form over the field K, let $a \in K^*/K^{*2}$, let $d = d(f)$, and let $\epsilon = \epsilon(f)$. Then f represents a if and only if*

- *f is rank 2 and $(a, -d) = \epsilon$*
- *f is $\geq$ rank 4.*

4. The Hilbert Symbol and the Product Formula

Definition 7. *Let $a, b \in K^*$ where $K = \mathbb{Q}_p$ or $\mathbb{R}$ (corresponding to $p = \infty$). We define $(a, b)_p$ if $z^2 - ax^2 - by^2 = 0$ has a solution $(0, 0, 0) \neq (x, y, z)$ in K^3, and $(a, b)_p = -1$ otherwise. We call $(a, b)_p = \pm 1$ the Hilbert symbol of a and b relative to K. Whenever it does not cause confusion, we simply write (a, b).*

The Hilbert symbol generalizes the Legendre symbol and can be expressed in terms of the Legendre symbol (see [3]). Given the above definition, it makes sense to treat ∞ as if it were not only a number, but a prime one. There are many philsophical reasons for this as well, but exploring them would lead us astray.

Proposition 4.1. *Let $K = \mathbb{Q}_p$ or $\mathbb{R}$, $a, a', b, c \in K^*$, and in the formulas (2) and (3) below, suppose $a \neq 0$. The Hilbert symbol satisfies the following formulas:*

1. $(a, b) = (b, a)$ *and* $(a, c^2) = 1$,
2. $(a, -a) = 1$ *and* $(a, 1 - a) = 1$,
3. $(a, b) = 1 \to (aa', b) = (a', b)$,
4. $(a, b) = (a, -ab) = (a, (1 - a)b)$.

Proof. (1) Formula (1) is clear from the definition of the Hilbert Symbol.

(2) If $b = -a$, then,

$$0 = z^2 - ax - by^2 = z^2 - ax - ay^2$$

has the zero $(z, x, y) = (0, 1, 1)$. Similarly, if $b = 1-a$, the defining quadratic equation has the zero $(z, x, y) = (1, 1, 1)$.

(3) See [4, Proposition 8(iii)].
(4) Follows from proofs of formulas (1) through (3).

□

Proposition 4.2 (Product Formula)**.** *If $a, b \in \mathbb{Q}^*$ we have $(a,b)_p = 1$ for all but finitely many primes p, and*

$$(a,b)_\infty \prod_{p \text{ prime}} (a,b)_v = 1$$

Proof. The Hilbert symbol is bilinear, thus it suffices to prove the theorem when a and b are equal to -1 or to a prime number. We thus consider the cases and apply Theorem 9 [4] to each.

(1) If $a = b = -1$, then $(-1,-1)_\infty = (-1,-1)_2 = -1$, and one can see that if $p \neq 2, \infty$ then $(-1,-1)_p = 1$. Since there are an even number of p such that $(a,b)_p = -1$, the product of the Hilbert symbols equals 1.
(2) Suppose that $a = 1, b = l$ where l is a prime. If $l = 2$, then $(-1,2)_v = 1$ for all $v \in V$, which can easily be seen since the solution $(1,1,1)$ exists:

$$1^2 + 1 * 1^2 - 2 * 1^2 = 0$$

If $l \neq 2$, then if $v \neq 2$, l then in applying Theorem 9 [4] to $(a,b)_v$ we have $\alpha = \beta = 0$, hence $(a,b)_v = 1$. Otherwise, $v = 2$ or l, and Theorem 9 [4] yields $(-1,l)_2 = (-1,l)_l = (-1)^{\epsilon(l))}$. Taking the product of these Hilbert symbols yields 1.
(3) Suppose now that $a = l, b = l'$ with l, l' primes. If $l = l'$, then by formula (iv) of Proposition 4.1 we have $(l,l')_v - (l,-1)_v$ for each $v \in V$, and the formula follows from case 2 above. Otherwise, we have $l \neq l'$.

Suppose $l' = 2$. Then α and β in Theorem 9 [4] are equal to 0 when $v \neq 2, l$, giving $(l,2)_v = 1$. If $l' \neq 2$, by Theorem 9 [4] we have

$$(l,2)_2 = (-1)^{\omega(l)}$$

and

$$(l,2)_l = (2/l) = (-1)^{\omega(l)}$$

by the properties of the Legendre symbol. Taking the product of the Hilbert symbols yields 1.

If l and l' are distinct odd primes, then $(l,l')_v = 1$ for $v \neq 2, l, l'$ and Theorem 9 [4] yields

$$(l,l')_2 = (-1)^{\epsilon(l)\epsilon(l')}$$

and

$$(l, l')_l = (l'/l), (l, l')_V = (l/l').$$

By quadratic reciprocity, $(l'/')(l/l') = (-1)^{\epsilon(l)\epsilon(l')}$, and taking the product suffices.

□

5. Proof of Hasse-Minkowski

A majority of the following proof (excluding the $n \geq 5$ case), is taken from either [4] or [5], which have been inspired by [3]. Note that we can always assume that our quadratic form f is diagonalized with no coefficients equal to zero. The case where $\text{rank}(f) = n = 1$ is trivial, so we continue for $n \geq 2$:

(1) Case $n = 2$: In this case, we have $x_1^2 - ax_2^2$ for some nonzero $a \in \mathbb{Q}$. Now, we know that f has a nontrivial root in $Q_\infty = \mathbb{R}$, hence $a > 0$. Since a is a rational number, it has a "factorization" which may include negative powers of prime numbers. Thus, we may write

$$a = \prod_p p^{\nu_p(a)}$$

where the product runs over all (finite) primes. Since each f_p represents 0, we have

$$a = \frac{x_1}{x_2}^2$$

in each $\mathbb{Q}_p$, so a is a square in each $\mathbb{Q}_p$. This implies that $\nu_p(a)$ is even for every p, hence a is a square in $\mathbb{Q}$, and so f represents 0 in $\mathbb{Q}$

(2) Case $n = 3$: In this case, our quadratic form looks like $x^2 - ax_2^2 - bx_3^2$. By taking all square factors into the squares, we can assume that $v_p(a)$ and $v_p(b)$ are either 1 or 0 for all primes. Without loss of generality, assume that $|a| \leq |b|$. If this is not the case, simply flip a and b.

The proof is done by induction on the integer $m = |a| + |b|$. The base case has $m = 2$. Then f can be one of four different forms: $x_1^2 \pm x_2^2 \pm x_3^2$. The form must represent 0 in $\mathbb{R}$, so we do not have to consider the case $x_1^2 + x_2^2 + x_3^2$. In all other cases, the form represents 0, either by the element $(1, 1, 0)$ or $(1, 0, 1)$. This proves the base case.

For induction, assume $m > 2$. Since $|a| \leq |b|$ and $|b| \geq 2$ the number b has a prime factorization. It is also square-free, so $b = \pm p_1 p_2 ... p_k$. Take a specific p_i. If $a \equiv 0 \bmod p$, then a is a square modulo p. If $a \not\equiv 0 \bmod p$, then a is in U, the set of p-adic units. By assumption, f_{p_i} represents 0, so there is a triplet (x', y', z') with the

property that $(z')^2 = a(x')^2 - b(y')^2$ is 0. By Theorem 2.9 [5] we assume this triplet is primitive. Therefore, $(z')^2 - a(x')^2 \equiv 0 \bmod p_i$. If $x' \equiv 0 \bmod p_i$, this reduces to $(z')^2 \equiv 0 \bmod p_i$, which implies that z would be divisible by p_i. This contradicts the fact that (x', y', z') is primitive. So we can assume that $x' \not\equiv 0 \bmod p_i$. We conclude that a is a square mod p, otherwise we cannot have $(z')^2 - a(x')^2 \equiv 0 \bmod p_i$.

By the Chinese Remainder Theorem, we know $\mathbb{Z}/b\mathbb{Z} = \prod_{j=1}^{k} \mathbb{Z}/p_j\mathbb{Z}$. We can assume that a is a square in all the factors of $\mathbb{Z}/b\mathbb{Z}$, hence a square in $\mathbb{Z}/b\mathbb{Z}$ itself. There exist integers c and d such that $d^2 = a + bc$ because a and b are square-free. We choose d such that $|d| \leq \frac{|b|}{2}$ and rewrite this equation, finding that $bc = d^2 - a$, and a and d^2 are squares. Since $|bc| = |b||c|$, f represents 0 if and only if the form $g - x_1^2 - ax_2^2 - cx_3^2$ represents 0. Because f represents 0 in all $\mathbb{Q}_v$, so does g. Also note that $|c| = |\frac{d^2-a}{b}| \leq \frac{|b|}{4} + 1 < |b|$. The first inequality follows from the fact that $|b| \geq 2$.

Finally, write c as $c'u^2$, with c' square-free. Then we can use the inductive hypothesis by noting that $|c'| < |b|$. This means that $h = x_1^2 - ax_2^2 - c'x_3^2$ represents 0 and is equivalent to g by taking the square root of u out of x_3^2. So g represents 0, which was equivalent to f representing 0.

(3) Case $n = 4$: We can write our quadratic form as

$$f = ax_1^2 + bx_2^2 - (cx_3^2 + dx_4^2)$$

for some nonzero $a, b, c, d \in \mathbb{Q}$. Let $p \in V$. By hypothesis, f_p represents 0, so there exists some $x_p \in \mathbb{Q}_p^*$ which is represented by both $g = ax_1^2 + bx_2^2$ and $h = cx_3^2 + dx_4^2$.

Recalling the definitions of both $d(f)$ and $\epsilon(f)$, we have

$$d(g) = ab, \epsilon(g) = (a, b), d(h) = cd, \text{ and } \epsilon(h) = (c, d).$$

Thus, by Proposition 3.1 we have $(x_p, -ab)_p = (a, b)_p$ and $(x_p, -cd)_p = (c, d)_p$ for primes p and $p = \infty$. By the Product Formula we have

$$(a, b)_\infty \prod_p (a, b)_p = (c, d)_\infty \prod_p (c, d)_p = 1,$$

so the conditions of Theorem 3.3 are satisfied. Hence there exists $x \in \mathbb{Q}^*$ such that

$$(x, -ab)_p = (a, b)_p \text{ and } (x, -cd)_p = (c, d)_p \text{ for all primes } p \text{ and } \infty.$$

If z is a variable, then the quadratic forms $g - xz^2$ and $h - xz^2$ both represent 0 in each $\mathbb{Q}_p$ by Proposition 3.1 and since we have already proven this theorem for rank 3 forms, this implies that g and h both represent 0 in $\mathbb{Q}$. But $f = g - h = (g - xz^2) - (h - xz^2)$, hence f represents 0.

(4) Case $n = 5$: Suppose that $q(X)$ is a rational quadratic form in $n \geq 5$ variables, such that for all primes p, $q(X) = 0$ has a solution $X \in \mathbb{Q}_p^n$, and also $q(X) = 0$ has a solution $X \in \mathbb{R}^n$. We can assume that $q(X)$ is given by a diagonal equation

$$q(X) = \sum_{j=1}^{n} a_j x_j^2,$$

where $a_j \in \mathbb{Z} \setminus \{0\}$. Let us define $q_1(x_1, x_2) := a_1 x_1^2 + a_2 x_2^2$ and $q_2(x_3, \ldots, x_n) := q_1 - q$, so that $q = q_1 - q_2$ as polynomials. Note that q_2 is a quadratic form in ≥ 3 variables. Furthermore, since q has a real zero, it is an indefinite quadratic form (i.e. $\exists X_1, X_2$ with $q(X_2) < 0 < q(X_1)$), so by relabelling coefficients, we can assume that q_2 is indefinite as well.[1]

By assumption, for all primes p, there is some $x_p = (x_{p,1}, \ldots, x_{p,n}) \in \mathbb{Q}_p^n$ such that

$$q(x_p) = q_1(x_{p,1}, x_{p,2}) - q_2(x_{p,3}, \ldots, x_{p,n}) = 0.$$

Multiplying through by a sufficiently high power of p, we can assume that $x_p \in \mathbb{Z}_p^n$ as well. Let S be the set of primes such that $\nu_p(\mathrm{disc}(q_2)) \neq 0$. Note that $\mathrm{disc}(q_2)$ is just some number, so $\nu_p(\mathrm{disc}(q_2)) = 0$ for all but finitely many p. Thence S is a finite set. By the Chinese remainder theorem, we can find some $(z_1, z_2) \in \mathbb{Z}^2$ such that for $i = 1, 2$, also

$$\begin{aligned} z_i &\equiv x_{p,i} \bmod p^{1+\nu_p(q_1(x_p))}, \quad \text{for } p \in S \setminus \{2\} \\ z_i &\equiv x_{2,i} \bmod 8^{1+\nu_2(q_1(x_2))}, \quad \text{for } p = 2. \end{aligned}$$

Moreover, by adding $8 \prod_{p \in S} p$ to each z_i, we can assume $q_1(z_1, z_2) \neq 0$.[2] We show that $q_2(X) = q_1(z_1, z_2)$ has a solution $(y_3, \ldots, y_n) \in \mathbb{Q}^{n-2}$. This will suffice, since then

$$q(z_1, z_2, y_3, \ldots, y_n) = q_1(z_1, z_2) - q_2(y_3 \ldots, y_n) = 0.$$

and $(z_1, z_2, y_3, \ldots, y_n) \in \mathbb{Q}^n$. We will use previously-proven cases of Hasse Minkowski and induction on $\mathrm{rank}(q_2) = n - 2 \geq 3$. Therefore we just need to prove that $q_2(X) = q_1(z_1, z_2)$ has solutions everywhere locally, i.e. in $\mathbb{Q}_p^{n-2}$ for all primes p and in $\mathbb{R}^{n-2}$.

First, note that $q_2(y_3, \ldots, y_n) \bmod p$ is a quadratic form in ≥ 3 variables over $\mathbb{F}_p$ if $p \neq 2$, with duplicate roots iff p divides $\mathrm{disc}(q_2)$. In particular, for $p \notin S \cup \{2\}$,

[1] This is important, since any quadratic form Q over $\mathbb{R}$ is indefinite iff it has a nontrivial $\mathbb{R}$-zero iff for all $d \in \mathbb{R}$, also $d = Q(X)$ has a solution X in $\mathbb{R}$ (often called Sylvester's Law of Inertia).

[2] A priori, it seems like it could be that $q_1(z_1 + n \cdot 8 \prod_{p \in S} p, z_2 + n \cdot 8 \prod_{p \in S} p) = 0$ for any $n \in \mathbb{Z}$, but we know that $q_1(x_1 + A, x_2 + A) = a_1(x_1 + A)^2 + a_2(x_1 + A)^2 = q_1(x_1, x_2) + 2A(a_1 x_1 + a_2 x_2) + A^2(a_1 + a_2)$, which one can use to rule this out.

Chevalley-Warning plus Hensel's Lemma gives a solution $Y \in \mathbb{Q}_p^{n-2}$ to $q_1(z_1, z_2) = q_2(Y)$. Second, since q_2 is assumed to be indefinite and $q_1(z_1, z_2) \neq 0$, we have a nontrivial $\mathbb{R}$-solution. Therefore we need to ensure our equation has solutions for $p \in S \cup \{2\}$, which I claim was the purpose of imposing congruences on (z_1, z_2).

If, for any field k, we define $k^{\times 2} := \{x^2 : x \in k^\times\} \subset k$ to be the subset of nonzero squares, we claim that the congruences given force $q_1(z_1, z_2)/q_1(x_{p,1}, x_{p,2}) \in \mathbb{Q}_p^{\times 2}$ for $p \in S \cup \{2, \infty\}$. Indeed if this is true, then for $p \in S$, we have some $t_p \in \mathbb{Q}_p^{\times 2}$ such that

$$q_1(z_1, z_2) = t_p^2 q_1(x_{p,1}, x_{p,2}) = t_p^2 q_2(x_{p,3}, \ldots, x_{p,n}) = q_2(t_p x_{p,3}, \ldots, t_p x_{p,n}).$$

Since $t_p \neq 0$, this gives the desired, local representation of $q_1(z_1, z_2)$ for $p \in S \cup \{2\}$.

To this end, note that if $n \in \mathbb{Z}_{\geq 2}$, then $z_i \equiv a_i \mod n$ enforces $q_1(z_1, z_2) \equiv q_1(a_1, a_2) \mod n$ (literally, write out $z_1 = a_1 + m_1 n, z_2 = a_2 + m_2 n$). Therefore our congruences enforce

$$\begin{array}{ll} q_1(z_1, z_2) \equiv q_1(x_{p,1}, x_{p,2}) \mod p^{1+\nu_p(q_1(x_p))}, & \text{for } p \in S \setminus \{2\} \\ q_1(z_1, z_2) \equiv q_1(x_{2,1}, x_{2,2}) \mod 8^{1+\nu_2(q_1(x_2))}, & \text{for } p = 2. \end{array}.$$

Hence for $p \neq 2$, also

$$\nu_p(q_1(z_1, z_2) - q_1(x_{p,1}, x_{p,2})) \geq 1 + \nu_p(q_1(x_p)) = 1 + \nu_p(q_1(x_{p,1}, x_{p,2})).$$

By the ultrametric inequality, this enforces that $\nu_p(q_1(x_{p,1}, x_{p,2})) = \nu_p(q_1(z_1, z_2))$.[3] In particular, we can write the p-adic expansion

$$q_1(z_1, z_2)/q_1(x_{p,1}, x_{p,2}) = \sum_{k=0}^{\infty} a_i p^i$$

with $0 \leq a_i \neq\leq p - 1$ and $a_0 \neq 0$. Since $q_1(z_1, z_2)/q_1(x_{p,1}, x_{p,2}) \equiv 1 \mod p$, we moreover know that $a_0 = 1$.

If $p \neq 2$, then apply Hensel's Lemma to $f(x) = x^2 - q_1(z_1, z_2)/q_1(x_{2,1}, x_{2,2})$. Mod p, we get that this is $x^2 - 1 \equiv 0 \mod p$, which obviously has a ± 1, and since $f'(\pm 1) = \pm 2 \not\equiv 0 \mod p$, Hensel's Lemma gives a solution to $f(x) = x^2 - q_1(z_1, z_2)/q_1(x_{2,1}, x_{2,2})$ in $\mathbb{Q}_p^\times$; giving the desired square-ness. For $p = 2$, you can do the same argument, with a slightly "fancier" version of Hensel's lemma to see that $q_1(z_1, z_2)/q_1(x_{2,1}, x_{2,2}) \equiv$

[3]It is worth convincing oneself that if $A = p^r \cdot n$ and $B = p^e \cdot m$ with $e > r$ and $\gcd(p, n) = \gcd(p, m) = 1$, then $\nu_p(A) = r$.

1 mod 8 suffices.[4] Alternatively, this is a formal consequence of the fact that

$$(1+8t)^{1/2} = \sum_{i=0}^{\infty} \binom{1/2}{i} (8t)^i,$$

and one can check that $\left|\binom{1/2}{i} \cdot 8^i\right|_2 \to 0$ as $i \to \infty$, so this power series "converges" to a number in $\mathbb{Z}_2$, which is necessarily a root of $1+8t$, if $t \in \mathbb{Z}_2$.

Acknowledgements

I offer my sincerest gratitude to Hunter Handley.

References

[1] T. Y. Lam. Introduction to quadratic forms over fields. 2004.
[2] Fernando Q. Gouvêa. P-adic numbers: An introduction. 2020.
[3] Jean-Pierre Serre. A course in arithmetic. 1973.
[4] Jeffrey Hatley. Hasse-minkowski and the local-to-global principle. 2009.
[5] Tim Bredek. The hasse-minkowski theorem, 2022.
[6] Keith Conrad. Hensel's lemma.

[4] See [6, THM 4.4] or [4, THM 4].