The Hasse–Minkowski Theorem

Lee Dicker
University of Minnesota, REU Summer 2001

The Hasse-Minkowski Theorem provides a characterization of the rational quadratic forms. What follows is a proof of the Hasse-Minkowski Theorem paraphrased from the book, *Number Theory* by Z.I. Borevich and I.R. Shafarevich [1]. Throughout this paper, some familiarity with the p-adic numbers and the Hilbert symbol is assumed and some basic facts about quadratic forms are stated without proof. Also, the proof of the Hasse–Minkowski theorem given here uses the Dirichlet theorem on primes in arithmetic progressions. A proof of Dirichlet's theorem will not be given here (see [1], for a proof of the theorem) due to its length, but the result is stated presently.

Theorem 0 (Dirichlet's theorem). *Every residue class modulo m which consists of numbers relatively prime to m contains an infinite number of prime numbers.*

To begin, we state the definition of a quadratic form over a field $\mathbf{K}$:

Definition 1. *A quadratic form, f, over the field $\mathbf{K}$ is a homogeneous polynomial of degree 2 with coefficients in $\mathbf{K}$ where f can be written*

$$f = \sum_{i,j=1}^{n} a_{ij} x_i x_j,$$

and $a_{ij} = a_{ji}$.

Using the same notation as above, the symmetric matrix $A = (a_{ij})$ completely determines the quadratic form f. We call A the matrix of f and we sometimes refer to $\det A$ as the determinant of f. Let X be the column vector of the variables $x_1, \ \dots \ , x_n$, then we can write

$$f = X^{\mathrm{t}} A X.$$

The quadratic form g is equivalent to $f = X^{\mathrm{t}} A X$ if the matrix of g, A_1, can be written as

$$A_1 = C^{\mathrm{t}} A C,$$

where C is an $n \times n$ invertible matrix with entries in $\mathbf{K}$.

The quadratic form f is said to represent zero in $\mathbf{K}$if there exist values $\alpha_i \in \mathbf{K}$, not all zero such that $f(\alpha_1, \ \dots \ , \alpha_n) = 0$. Likewise, f represents $\gamma \in \mathbf{K}$ if there are values $\alpha_i \in \mathbf{K}$ such that $f(\alpha_1, \ \dots \ , \alpha_n) = \gamma$. It is easily seen that two equivalent quadratic represent the same elements in $\mathbf{K}$. Furthermore, if a nonsingular quadratic form f (i.e. the matrix of f is invertible) represents zero in a field $\mathbf{K}$, then f represents all elements of $\mathbf{K}$.

Additionally, we note that every quadratic form is equivalent to a diagonal quadratic form. That is, if f is a quadratic form in n variables and A is the matrix of f, there exists an invertible matrix C such that the matrix $C^{\mathrm{t}} A C$ is diagonal. This follows immediately from "the Gram-Schmidt"process from linear algebra. Also, it can be shown that if a diagonal quadratic form represents zero in a field $\mathbf{K}$ and the number of elements of $\mathbf{K}$ is greater than five then there is a representation of zero where all the variables take on nonzero values in $\mathbf{K}$.

We are now prepared to state the Hasse–Minkowski Theorem:

Theorem 1 (Hasse–Minkowski). *A quadratic form with rational coefficients represents zero in the field of rational numbers if and only if it represents zero in the field of real numbers and in all fields of p-adic numbers,* $\mathbf{Q}_p$ *(for all primes p).*

The necessity of the condition is clear so we must show its sufficiency.

In light of the facts that every quadratic form is equivalent to a diagonal quadratic form, and that representing zero is preserved when passing between equivalent quadratic forms, only diagonal quadratic forms need be considered in our proof.

Essentially, the proof depends on the number of variables, n, of the quadratic form. For $n = 1$ the theorem is trivial. We divide the proof into four remaining cases. We consider separately when $n = 2, n = 3, n = 4,$ or $n \geq 5$.

When $n = 2$, we first need a lemma pertaining to binary quadratic forms:

Lemma 1. *A binary quadratic form* $f(x, y) = ax^2 + 2bxy + cy^2$ *with determinant* $d = ac - b^2$ *represents zero in a field* $\mathbf{K}$ *if and only if* $-d = \alpha^2$ *for some* $\alpha \in \mathbf{K}$.

Sketch of proof. For the necessity of the condition, when $d = 0$ the proof is trivial. When $d \neq 0$ we note the following two facts: A nonsingular binary quadratic form that represents zero is equivalent to the form $g = y_1 y_2$ (see, for example, [1]). Also, the determinants of equivalent quadratic forms differ by a nonzero factor which is a square in $\mathbf{K}$. For the sufficiency, if $f = ax^2 + by^2$ and $-d = -ab = \alpha^2$, then $f(\alpha, a) = 0$. •

If the binary quadratic form f represents zero in $\mathbf{R}$ and d is the determinant of f, it follows from Lemma 1 that $-d > 0$, hence, $-d = p_1^{k_1} p_2^{k_2} \cdots p_s^{k_s}$ where k_i is a rational integer. If f also represents zero in $\mathbf{Q}_p$ for all primes p, $-d$ must a square in $\mathbf{Q}_{p_i}$ $(i = 1, \ \ldots \ , s)$. Thus, k_i must be even for $i = 1, \ \ldots \ , s$ and $-d$ is a square in $\mathbf{Q}$. By Lemma 1, f represents zero in $\mathbf{Q}$.

Before proving the cases where $n \geq 3$ some things should be noted. The first of these observations follow from the fact that a quadratic form with rational integer coefficients f represents zero if and only if cf represents zero, where c is a nonzero constant in $\mathbf{Q}$: throughout the proof Theorem 1, we may assume that the coefficients of the quadratic form $f(x_1, \ \ldots \ , x_n)$ are rational integers (if necessary, multpily f by the least common multiple of the denominators of the coefficients). Also, it is clear the equation

$$f(x_1, \ \ldots \ , x_n) = 0 \tag{1}$$

is solvable in $\mathbf{Q}$ (or in $\mathbf{Q}_p$) if and only if it is solvable in the rational integers, $\mathbf{Z}$ (respectively, in the p-adic integers, $\mathbf{Z}_p$). We note that (1) is solvable in $\mathbf{R}$ if and only if the form f is indefinite.

Moving on to the case $n = 3$, let $f = a_1 x^2 + a_2 y^2 + a_3 z^2$. Since f represents zero in $\mathbf{R}$, the coefficients a_1, a_2, a_3 do not all have the same sign. We may assume that two coefficients of f are positive and one is negative (if necessary, we may multiply f by -1). We may also assume that a_1, a_2, a_3 are rational integers, square-free (making a change of variables if necessary), and relatively prime. Suppose a_1 and a_2 have a common prime factor p, then multiplying f by p and setting x/p and y/p as new variables, we get a form with coefficients $a_1/p, a_2/p, pa_3$. By repeating this process we obtain a quadratic form whose coefficients are positive rational integers, pairwise relatively prime and square-free:

$$ax^2 + by^2 - cz^2. \tag{2}$$

We now prove a theorem that is relevant to the case at hand and will also be needed again, later, in our proof of the Hasse–Minkowski theorem. We begin with a lemma.

Lemma 2 (Hensel's lemma). *Let $F(x_1, \ldots, x_n)$ be a polynomial whose coefficients are p-adic integers. Let $\gamma_1, \ldots, \gamma_n$ be p-adic integers such that for some i $(1 \leq i \leq n)$ we have*

$$F(\gamma_1, \ldots, \gamma_n) \equiv 0 \ (mod\ p),$$
$$\frac{\partial F}{\partial x_i}(\gamma_1, \ldots, \gamma_n) \not\equiv 0 \ (mod\ p),$$

then there exist p-adic integers $\theta_1, \ldots, \theta_n$ such that

$$F(\theta_1, \ldots, \theta_n) = 0$$

and

$$\theta_i \equiv \gamma_i \ (mod\ p) \ (i = 1, \ldots, n).$$

Proof. Consider the polynomial in x, $f(x) = F(\gamma_1, \ldots, \gamma_{i-1}, x, \gamma_{i+1}, \ldots, \gamma_n)$. We will find $\alpha \in \mathbf{Z}_p$ such that $f(\alpha) = 0$ and $\alpha \equiv \gamma_i \pmod p$. Then set $\theta_j = \gamma_j$ for $i \neq j$, and $\theta_i = \alpha$. It is easily seen that this suffices to prove the lemma. Let $\gamma_i = \gamma$. We construct a sequence of p-adic integers

$$\alpha_0, \alpha_1, \ldots, \alpha_m, \ldots \tag{3}$$

congruent to γ modulo p, such that

$$f(\alpha_m) \equiv 0 \pmod{p^{m+1}}$$

for all $m \geq 0$. For $m = 0$ take $\alpha_0 = \gamma$. We proceed by induction. Suppose for some $m \geq 1$, $\alpha_0, \ldots, \alpha_{m-1}$ have been determined. Then, $\alpha_{m-1} \equiv \gamma \pmod p$ and $f(\alpha_{m-1}) \equiv 0 \pmod{p^m}$. We expand the polynomial $f(x)$ in powers of $x - \alpha_{m-1}$:

$$f(x) = \beta_0 + \beta_1(x - \alpha_{m-1}) + \beta_2(x - \alpha_{m-1})^2 + \ \ldots \quad (\beta_i \in \mathbf{Z}_p).$$

By the induction hypothesis, $\beta_0 = f(\alpha_{m-1}) = p^m A$ where $A \in \mathbf{Z}_p$. Also, since $\alpha_{m-1} \equiv \gamma \pmod p$ and $\frac{\partial F}{\partial x_i}(\gamma_1, \ldots, \gamma_n) \not\equiv 0 \pmod p$, $\beta_1 = f'(\alpha_{m-1}) = B$, where $B \in \mathbf{Z}_p$ and B is not divisible by p. Set $x = \alpha_{m-1} + \xi p^m$ and we get

$$f(\alpha_{m-1} + \xi p^m) = p^m(A + B\xi) + \beta_2 p^{2m}\xi^2 + \ \ldots$$

Since $B \not\equiv 0 \pmod p$ we may choose $\xi = \xi_0 \in \mathbf{Z}_p$ such that $A + B\xi_0 \equiv 0 \pmod p$. Furthermore, since $km \geq 1 + m$ for $k \geq 2$, we have

$$f(\alpha_{m-1} + \xi_0 p^m) \equiv 0 \pmod{p^{m+1}}.$$

In addition $m \geq 1$, so $\alpha_{m-1} + \xi_0 p^m \equiv \gamma \pmod p$ and we see that we may take $\alpha_m = \alpha_{m-1} + \xi_0 p^m$. We now check that the sequence (3) converges p-adically. By construction, $v_p(\alpha_m - \alpha_{m-1}) \geq m$ (here $v_p(\xi)$, $\xi \in \mathbf{Q}_p$ is the p-adic value of ξ) and since the p-adic numbers are complete, (3) converges to a p-adic integer, call it α. Clearly, $\alpha \equiv \gamma \pmod p$. Since $f(\alpha_m) \equiv 0 \pmod{p^{m+1}}$, $\lim_{m\to\infty} f(\alpha_m) = 0$. By the continuity of the polynomial f, $\lim_{m\to\infty} f(\alpha_m) = f(\alpha)$. It follows $f(\alpha) = 0$. •

Now, for the theorem mentioned above:

Theorem 2. *Let $p \neq 2$ and $0 < r < n$. The quadratic form*

$$F = F_0 + pF_1 = \epsilon_1 x_1^2 + \cdots + \epsilon_r x_r^2 + p(\epsilon_{r+1}x_{r+1}^2 + \cdots + \epsilon_n x_n^2),$$

where ϵ_i $(1 \leq i \leq n)$, is a p-adic unit, represents zero in $\mathbf{Q}_p$ if and only if at least one of the forms F_0 or F_1 represents zero.

Proof. The sufficiency of the condition is clear, we prove the necessity. Suppose F represents zero:

$$\epsilon_1\xi_1^2 + \cdots + \epsilon_r\xi_r^2 + p(\epsilon_{r+1}\xi_{r+1}^2 + \cdots + \epsilon_n\xi_n^2) = 0. \tag{4}$$

Without loss of generality, assume that $\xi_i \in \mathbf{Z}_p$ $(1 \leq i \leq n)$ and that at least one ξ_i is not divisible by p. Suppose ξ_1, or some ξ_i among $i = 1, \ \ldots \ , r$, is not divisble by p. Consider equation (4) modulo p, then

$$F_0(\xi_1, \ \ldots \ , \xi_r) \equiv 0 \pmod{p},$$

and

$$\frac{\partial F_0}{\partial x_1}(\xi_1, \ \ldots \ , \xi_r) = 2\epsilon_1\xi_1 \not\equiv 0 \pmod{p}.$$

By Hensel's lemma, F_0 represents zero. Now assume $\xi_1, \ \ldots \ , \xi_r$ are all divisible by p, then some ξ_i $(r+1 \leq i \leq n)$ is not divisible by p and $\epsilon_1\xi_1^2 + \cdots + \epsilon_r\xi_r^2 \equiv 0 \pmod{p^2}$. When looking at equation (4) modulo p^2 we have

$$pF_1(\xi_{r+1}, \ \ldots \ , \xi_n) \equiv 0 \pmod{p^2},$$

or after dividing by p

$$F_1(\xi_{r+1}, \ \ldots \ , \xi_n) \equiv 0 \pmod{p}.$$

We proceed as above, applying Hensel's lemma, and conclude that F_1 represents zero. •

Two useful corollaries follow:

Corollary 1. *If $\epsilon_1, \ \ldots \ , \epsilon_r$ are p-adic units and $p \neq 2$, then the quadratic form $f = \epsilon_1 x_1^2 + \cdots + \epsilon_r x_r^2$ represents zero in $\mathbf{Q}_p$ if and only if the congruence $f(x_1, \ \ldots \ , x_r) \equiv 0 \pmod{p}$ has a nontrivial solution in $\mathbf{Z}_p$.*

Corollary 2. *Let f be the quadratic form from Corollary 1. If $r \geq 3$, then f always represents zero in $\mathbf{Q}_p$.*

Proof. Corollary 1 is an immediate result of Theorem 2. Corollary 2 follows from Chevaley's theorem, which states that if $F(x_1, \ \ldots \ , x_n)$ is a form of degree less than n, then the congruence $F(x_1, \ \ldots \ , x_n) \equiv 0 \pmod{p}$, p a prime, has a nontrivial solution. •

Getting back to the Hasse–Minkowski theorem, we are considering the quadratic form (2) where a, b, c are positive, square-free, rational integers that are pairwise relatively prime. Let $p \neq 2$ be a prime divisor of c. Since (2) represents zero in $\mathbf{Q}_p$ by assumption, we may apply Theorem 2 and Corollary 1 and conclude that the congruence $ax^2 + by^2 \equiv 0 \pmod{p}$ has a nontrivial solution, (x_0, y_0). It follows that the form $ax^2 + by^2$ factors linearly, modulo p: if we assume y_0 is not divisible by p, we have

$$ax^2 + by^2 \equiv ay_0^{-2}(xy_0 + yx_0)(xy_0 - yx_0) \pmod{p}.$$

Thus, since p divides c, (2) factors into linear factors modulo p:

$$ax^2 + by^2 - cz^2 \equiv L^{(p)}(x, y, z)M^{(p)}(x, y, z) \pmod{p},$$

where $L^{(p)}$ and $M^{(p)}$ are integral linear forms. Similarly, for,p', an odd prime divisor of a or b, the quadratic form (2) factors into linear integral forms modulo p'. Also, when $p = 2$ we note that the quadratic form (2) factors linearly modulo 2 since

$$ax^2 + by^2 - cz^2 \equiv (ax + by - cz)^2 \pmod{2}.$$

By the Chinese Remainder theorem we may find integral linear forms $L(x, y, z)$ and $M(x, y, z)$ such that

$$L(x, y, z) \equiv L^{(p)}(x, y, z) \pmod{p},$$
$$M(x, y, z) \equiv M^{(p)}(x, y, z) \pmod{p}$$

for all prime divisors p of a, b, and c. Since a, b, c are square-free and pairwise relatively prime, we have the congruence

$$ax^2 + by^2 - cz^2 \equiv L(x, y, z)M(x, y, z) \pmod{abc}. \tag{5}$$

Now give rational integer values to the variables x, y, z satisfying the inequalities

$$0 \le x < \sqrt{bc},\ 0 \le y < \sqrt{ac},\ 0 \le z < \sqrt{ab}. \tag{6}$$

Without loss of generality, we may exclude the case $a = b = c = 1$, then, since a, b, c are pairwise relatively prime and square-free, $\sqrt{bc}$, $\sqrt{ac}$, and $\sqrt{ab}$ are not integers. It follows that the number of triples (x, y, z) satisfying the inequalities (6) will be strictly greater than $\sqrt{bc} \cdot \sqrt{ac} \cdot \sqrt{ab} = abc$. Since the number of triples is greater than the number of resiue classes modulo abc, there exist distinct triples (x_1, y_1, z_1) and (x_2, y_2, z_2) such that $L(x_1, y_1, z_1) \equiv L(x_2, y_2, z_2) \pmod{abc}$. If we set

$$x_0 = x_1 - x_2,\ y_0 = y_1 - y_2,\ z_0 = z_1 - z_2,$$

it follows from the linearity of L that

$$L(x_0, y_0, z_0) \equiv 0 \pmod{abc}.$$

Looking at the congruence (5) we see that

$$ax_0^2 + by_0^2 - cz_0^2 \equiv 0 \pmod{abc}. \tag{7}$$

Since the triples (x_1, y_1, z_1) and (x_2, y_2, z_2) satisfy the inequalities (6), we have

$$|x_0| < \sqrt{bc},\ |y_0| < \sqrt{ac},\ |z_0| < \sqrt{ab}.$$

Thus,

$$-abc < ax_0^2 + by_0^2 - cz_0^2 < 2abc. \tag{8}$$

Combining (7) and (8) we see that either

$$ax_0^2 + by_0^2 - cz_0^2 = 0, \tag{9}$$

or

$$ax_0^2 + by_0^2 - cz_0^2 = abc. \tag{10}$$

In the first case, (x_0, y_0, z_0) is a nontrivial representation of zero in $\mathbf{Q}$. If the second case holds, we appeal to the following. Since b and c are square-free and relatively prime, bc is not a square. We show that (2) represents zero if and ony if ac is the norm of some element from the field $\mathbf{Q}(\sqrt{bc})$. Supposing (9) holds, we assume without loss of generality that $x_0 \neq 0$, it follows that

$$ac = \Big(\frac{cz_0}{x_0}\Big)^2 - bc\Big(\frac{y_0}{x_0}\Big)^2 = N\Big(\frac{cz_0}{x_0} + \frac{y_0}{x_0}\sqrt{bc}\Big).$$

For the converse, if $ac = N(u + v\sqrt{bc})$, then $ac^2 + b(cv)^2 - cu^2 = 0$. Now suppose (10) holds. Multiplying by c, we get

$$ac(x_0^2 - bc) = (cz_0)^2 - bcy_0^2.$$

Setting $\alpha = x_0 + \sqrt{bc},\ \beta = cz_0 + y_0\sqrt{bc}$, it follows that

$$acN(\alpha) = N(\beta),$$

and

$$ac = N\Big(\frac{\beta}{\alpha}\Big).$$

Thus ac is the norm of $\frac{\beta}{\alpha} \in \mathbf{Q}(\sqrt{bc})$ and (2) represents zero in $\mathbf{Q}$.

In preparation for the last two cases to be proved, that is $n = 4$ and $n \ge 5$, we need another lemma. Before that, we review some properties of the Hilbert symbol.

Definition 2. *For any pair $\alpha \neq 0,\ \beta \neq 0$ of p-adic numbers, the Hilbert symbol $(\alpha, \beta)_p$ is equal to $+1$ or -1 if the form $\alpha x^2 + \beta y^2 - z^2$ represents zero in the field $\mathbf{Q}_p$ or not, accordingly.*

We extend the Hilbert symbol to the real numbers by calling $\mathbf{R}$ the field $\mathbf{Q}_\infty$. Whereas the field $\mathbf{Q}_p$ is the completion of $\mathbf{Q}$ with respect to a finite prime p, we say the real numbers are the completion of $\mathbf{Q}$ with respect to the *infinite prime*.

What follows are some basic properties of the Hilbert symbol (see, for example, [1]):

$$(\alpha, \beta_1\beta_2)_p = (\alpha, \beta_1)_p(\alpha, \beta_2)_p,$$
$$(\alpha, \beta)_p = (\beta, \alpha)_p,\ \ (\alpha, \alpha)_p = (\alpha, -1)_p.$$

For p-adic units ϵ and η, and real numbers a and b,

$$(p, \epsilon)_p = \left(\frac{\epsilon}{p}\right),\quad (\epsilon, \eta)_p = 1 \quad \text{for } p \neq 2, \infty,$$
$$(2, \epsilon)_2 = (-1)^{(\epsilon^2-1)/8},\quad (\epsilon, \eta)_2 = (-1)^{[(\epsilon-1)/2][(\eta-1)/2]},$$
$$(a, b)_\infty = 1, \quad \text{if } a > 0 \text{ or } b > 0,$$
$$(a, b)_\infty = -1, \quad \text{if } a < 0 \text{ and } b < 0,$$

where $\left(\frac{\epsilon}{p}\right)$ is the Legendre symbol.

Lemma 3. *If a rational quadratic form in three variables represents zero in all fields $\mathbf{Q}_p$, where p runs through all primes and ∞, except possibly for $\mathbf{Q}_q$, then it represents zero in $\mathbf{Q}_q$.*

Proof. Consider the rational quadratic form $ax^2 + by^2 - z^2$. It follows from Corollary 2 that $(a, b)_p = 1$ for all p, except possibly when $p = 2, \infty$ or p is in the prime factorization of a or b. Thus, there are only finitely many values of p for which $(a, b)_p = -1$ and the product $\prod_p (a, b)_p$, where p takes on the value of all primes and the symbol ∞, makes sense. To prove the lemma it suffices to show that

$$\prod_p (a, b)_p = 1, \tag{11}$$

that is, the number of p for which $(a, b)_p = -1$ is even.

The basic properties of the Hilbert symbol allow us to reduce the proof of (11) to three cases:
(1) $a = -1,\ b = -1$,
(2) $a = q,\ b = -1$ (q a prime),
(3) $a = q,\ b = q'$ (q and q' primes).

All of the following computations follow from the basic properties of the Hilbert symbol and, in one place, the law of quadratic reciprocity. Case (1):

$$\prod_p (-1, -1)_p = (-1, -1)_2(-1, -1)_\infty = (-1) \cdot (-1) = 1.$$

Case (2):

$$\prod_p (2, -1)_p = (2, -1)_2(2, -1)_\infty = 1 \cdot 1 = 1,$$

$$\prod_p (q, -1)_p = (q, -1)_q(q, -1)_2 = \left(\frac{-1}{q}\right)(-1)^{[(q-1)/2][(-1-1)/2]} = (-1)^{(q-1)/2}(-1)^{[(q-1)/2][(-1-1)/2]} = 1.$$

Case (3):

$$\prod_p (2,q)_p = (2,q)_q(2,q)_2 = \Big(\frac{2}{q}\Big)(-1)^{(q^2-1)/8} = (-1)^{(q^2-1)/8}(-1)^{(q^2-1)/8} = 1,$$

$$\prod_p (q,q')_p = (q,q')_q(q,q')_{q'}(q,q')_2 = \Big(\frac{q'}{q}\Big)\Big(\frac{q}{q'}\Big)(-1)^{[(q-1)/2][(q'-1)/2]}$$

$$= (-1)^{[(q-1)/2][(q'-1)/2]}(-1)^{[(q-1)/2][(q'-1)/2]} = 1.$$

This proves (11), hence, the lemma. •

For the case $n = 4$ of the Hasse–Minkowski theorem we will consider the quadratic form

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 \tag{12}$$

where a_i $(1 \le i \le 4)$ is a square-free integer. The form (12) represents zero in $\mathbf{R}$, thus, we may assume $a_1 > 0,\ a_4 < 0$. Furthermore, let

$$g = a_1x_1^2 + a_2x_2^2 \quad \text{and} \quad h = -a_3x_3^2 - a_4x_4^2.$$

To prove the theorem for $n = 4$, we show that there exists a rational number a, such that both g and h represent a in $\mathbf{Q}$.

Let $p_1, \ \dots\ , p_s$ be all the distinct odd primes that divide a_1, a_2, a_3, a_4. For each of these primes and the prime $p = 2$ choose a representation of zero in $\mathbf{Q}_p$: $a_1\xi_1^2 + a_2\xi_2^2 + a_3\xi_3^2 + a_4\xi_4^2 = 0$. We pick the ξ_i so that $\xi_i \ne 0$ $(1 \le i \le 4)$ (see the review of quadratic forms, above). Set

$$b_p = a_1\xi_1^2 + a_2\xi_2^2 = -a_3\xi_3^2 - a_4\xi_4^2.$$

Choose our ξ_i so that b_p is divisible by at most the first power of p (if $b_p = 0$, then g, h represent zero and thus represent all elements of $\mathbf{Q}_p$). The congruences

$$\begin{aligned} a &\equiv b_2 \pmod{16} \\ a &\equiv b_{p_1} \pmod{p_1^2} \\ &\vdots \\ a &\equiv b_{p_s} \pmod{p_s^2} \end{aligned} \tag{13}$$

determine a rational integer a unique modulo $m = 16p_1^2 \cdots p_s^2$. Since b_{p_i} is divisble by at most the first power of p_i, following congruence holds:

$$b_{p_i}a^{-1} \equiv 1 \pmod{p_i}.$$

Any p-adic unit congruent to 1 modulo p is a square in $\mathbf{Q}_p$ (see [1]), thus $b_{p_i}a^{-1}$ is a square in $\mathbf{Q}_{p_i}$. Similarly, $b_2a^{-1} \equiv 1 \pmod 8$, thus b_2a^{-1} is a square in $\mathbf{Q}_2$ (a 2-adic unit ϵ is a square in $\mathbf{Q}_2$ if and only if $\epsilon \equiv 1 \pmod 8$, see [1]). Note that b_p and a differ by a square in $\mathbf{Q}_p$. Thus, for $p = 2, p_1, \ \dots\ , p_s$ the quadratic forms

$$-ax_0^2 + g \quad \text{and} \quad -ax_0^2 + h \tag{14}$$

represent zero in $\mathbf{Q}_p$.

Choosing $a > 0$, we see that the forms (14) represent zero in $\mathbf{R}$ since $a_1 > 0$ and $a_4 < 0$. Suppose now that $p \ne 2, p_1, \ \dots\ , p_s$ and $p \not| a$, then by Corollary 2 the forms (14) represent zero in $\mathbf{Q}_p$. To summarize our current position, the forms (14) represent zero in $\mathbf{R}$ and all p-adic fields except possibly when p divides

a and $p \neq 2, p_1, \ \ldots \ , p_s$. Thus, if we can choose a positive rational integer a that satisfies the congruences (13) and is divisible by only primes among $2, p_1, \ \ldots \ , p_s$ and possibly one other prime q, we may appeal to Lemma 3 and conclude that (14) represents zero in $\mathbf{Q}_p$ for all primes p including $p = q$. We use Dirichlet's theorem on primes in arithmetic progressions. Pick a rational integer $a^* > 0$ that satisfies the congruences (13). Set $d = \gcd(a^*, m)$, then $\gcd(a^*/d, m/d) = 1$. By Dirichlet's theorem, there exists a $k \in \mathbf{N}$ such that $\frac{a^*}{d} + k\frac{m}{d} = q$ is prime. Take $a = a^* + km = dq$. Hence, the forms (14) represent zero in $\mathbf{R}$ and $\mathbf{Q}_p$ for all primes p.

By the Hasse–Minkowski theorem for three variables, the forms (14) represent zero in $\mathbf{Q}$. It clearly follows that g and h both represent a in $\mathbf{Q}$. This proves the Hasse–Minkowski theorem for quadratic forms in four variables.

Lastly we deal with case $n \geq 5$. Consider the quadratic form

$$a_1x_1^2 + a_2x_2^2 + a_3x_3^2 + a_4x_4^2 + a_5x_5^2. \tag{15}$$

Since the form is indefinite, we may assume $a_1 > 0$ and $a_5 < 0$. We set

$$g = a_1x_1^2 + a_2x_2^2 \quad \text{and} \quad h = -a_3x_3^2 - a_4x_4^2 - a_5x_5^2.$$

Proceeding exactly as in the case $n = 4$, we find a rational integer $a > 0$ such that g and h represent a in $\mathbf{R}$ and $\mathbf{Q}_p$ for all primes p with the possible exception of one prime q. By Lemma 3, g represents a in all p-adic fields including when $p = q$. To show that h represents a in all p-adic fields we note that h represents zero in $\mathbf{Q}_q$ by Corollary 2 (as we saw in the proof of the case $n = 4$, $q \nmid a_i$ $(3 \leq i \leq 5)$). It follows that h represents all elements of $\mathbf{Q}_q$, namely h represents a. Thus g and h represent a in $\mathbf{R}$ and $\mathbf{Q}_p$ for all primes p. Clearly then,

$$-ax_0^2 + g \quad \text{and} \quad -ax_0^2 + h$$

represent zero in $\mathbf{R}$ and $\mathbf{Q}_p$ for all primes p. By the Hasse–Minkowski theorem for forms in three and four variables, $-ax_0^2 + g$ and $-ax_0^2 + h$ both represent zero in $\mathbf{Q}$. Hence, g and h both represent a in $\mathbf{Q}$ and the form (15) represents zero in $\mathbf{Q}$.

In order to generalize to $n > 5$ we first note that any quadratic form over $\mathbf{Q}_p$ with five or more variables always represents zero in $\mathbf{Q}_p$ (see [1]). So the Hasse–Minkowski theorem reads: a quadratic form in five or more variables with rational coefficients represents zero in $\mathbf{Q}$ if and only if it represents zero in $\mathbf{R}$. An indefinite quadratic form in more than five variable is equivalent to an indefinite diagonal quadratic form f, which may be written as $f = f_0 + f_1$ where f_0 is an indefinite quadratic form in five variables. Since we are assured that f_0 represents zero in $\mathbf{Q}_p$ for all p (and in $\mathbf{R}$), by what was just proved f_0 represents zero in $\mathbf{Q}$. It clearly follows that f represents zero in $\mathbf{Q}$.

With that, Theorem 1 has been proved.

References:

[1] Borevich, Z. I. and Shafarevich, I. R. (translated by Greenleaf, Newcomb), *Number Theory*, Academic Press Inc., 1966