QUADRATIC FORMS OVER GLOBAL FIELDS

PETE L. CLARK

Contents

1. The Hasse Principle(s) For Quadratic Forms Over Global Fields 1
1.1. Reminders on global fields 1
1.2. Statement of the Hasse Principles 2
2. The Hasse Principle Over $\mathbb{Q}$ 3
2.1. Preliminary Results: Reciprocity and Approximation 3
2.2. $n \leq 1$ 6
2.3. $n = 2$ 6
2.4. $n = 3$ 6
2.5. $n = 4$ 8
2.6. $n \geq 5$ 9
3. The Hasse Principle Over a Global Field 9
3.1. $n = 2$ 10
3.2. $n = 3$ 10
3.3. $n = 4$ 11
3.4. $n \geq 5$ 12
4. Some Applications to Integral Forms 12
4.1. The Aubry-Davenport-Cassels Lemma 12
4.2. Two, Three and Four Squares 14
4.3. More on Euclidean Forms and ADC Forms 15
References 16

1. The Hasse Principle(s) For Quadratic Forms Over Global Fields

All quadratic forms and quadratic spaces will be assumed nondegenerate unless otherwise noted.

1.1. Reminders on global fields.

A **number field** is a field K which is a finite-dimensional field extension of $\mathbb{Q}$.

Let k be a field. A **function field over k** is a field K which can be expressed as a finite degree separable extension of the rational function field $k(t)$. (By the **Separable Noether Normalization Theorem**, it follows that the class of function fields over k is not enlarged if the word "separable" is omitted.)

A **global field** is a field which is either a number field or a function field over

Thanks to France Dacar, Timo Keller and Danny Krashen for helpful comments.

a finite field $\mathbb{F}$.

To any global field K we associate the set Σ_K of **places** of K, namely equivalence classes of absolute values on K.

BIG OSTROWSKI

1.2. Statement of the Hasse Principles.

Let q be a quadratic form over the global field K, and let v be a place of K. We write q_v for the base change of q to a quadratic form over K_v.

Now we can state one of the most important and influential results in quadratic forms theory and number theory.

Theorem 1. *(Hasse Principle) For a quadratic form q over the global field K, the following are equivalent:*
(i) q is isotropic.
*(ii) q is **locally isotropic**: for all places v of K, q_v is isotropic.*

It will take us most of the chapter to give a complete proof of Theorem 1. For now we assume it and derive further "Hasse Principles".

For a quadratic space (V, B) over a global field K and $v \in \Sigma_K$, write V_v for $(V \otimes_K K_v, B \otimes_K K_v)$.

Theorem 2. *(Hasse Principle for Isometric Embedding) For quadratic spaces V, W over a global field K, TFAE:*
(i) There is an isometric embedding $V \hookrightarrow W$.
(ii) For all $v \in \Sigma_K$, there are isometric embeddings $V_v \hookrightarrow W_v$.

Proof. (i) $\implies$ (ii) is immediate.
(ii) $\implies$ (i): We go by induction on $\dim V$. The case $\dim V = 0$ being trivial, suppose $n \geq 1$, that the result holds in dimension $n-1$, and write $V = \langle \alpha \rangle \oplus V'$. For $v \in \Sigma_K$, we have $\langle \alpha \rangle_v \hookrightarrow V_v \hookrightarrow W_v$, i.e., W_v represents α. By the First Representation Theorem, the space $W \oplus \langle -\alpha \rangle$ is locally isotropic, so by the Hasse Principle it is isotropic, and thus we may write $W = \langle \alpha \rangle \oplus W'$. However, for all $v \in \sigma_K$, since V_v is a nondegenerate subspace of W_v, we may write

$$\langle \alpha \rangle \oplus W'_v = W_v = V_v \oplus X_v = \langle \alpha \rangle \oplus V'_v \oplus X_v.$$

Applying Witt Cancellation, we get isometric embeddings $V'_v \hookrightarrow W'_v$ for all $v \in \Sigma_K$. We are done by induction. □

The case of $\dim V = \dim W$ is important enough to be stated separately.

Theorem 3. *(Hasse Principle for Isomorphism) For quadratic forms q, q' over the global field K, the following are equivalent:*
(i) $q \cong_K q'$.
*(ii) q and q' are **locally isomorphic**: for all places v of K, $q_v \cong_{K_v} q'_v$.*

For a quadratic form $q_{/K}$ and $v \in \Sigma_K$, we define the **v-adic Hilbert symbol** simply as the Hilbert symbol of the base change: $H_v(q) = H(q_v)$.

Corollary 4. *(Classification of Quadratic Forms Over Global Fields) For quadratic forms q, q' over a global field K, the following are equivalent:*
(i) $q \cong q'$,
(ii) All of the following hold:
(a) $\dim q = \dim q'$.
(b) $\operatorname{disc} q = \operatorname{disc} q'$.
(c) For all places $v \in \Sigma_K$, $H_v(q) = H_v(q')$.

Proof. This follows immediately from the Hasse Principle for Isomorphism and the fact that for all $v \in \Sigma_K$, quadratic forms over K_v are classified by their dimension, discriminant and Hasse invariant (XXX). □

Exercise: Show that Corollary 4 gives an explicit procedure for testing isomorphism of quadratic forms over global fields.

Recall that we say a rational quadratic form q is **indefinite** if $q_{\mathbb{R}}$ is isotropic: i.e., neither positive nor negative definite.

Corollary 5. *(Meyer) For $n \geq 5$, an indefinite n-ary quadratic form $q_{\mathbb{Q}}$ is isotropic.*

Proof. This follows from the Hasse Principle together with the fact that for all primes p, every quadratic form in at least five variables over $\mathbb{Q}_p$ is isotropic. □

Corollary 6. *For a global field K, the following are equivalent:*
(i) The u-invariant of K is 4.
(ii) K has no real places.

Exercise: Prove Corollary 6. (Don't forget to show that $u(K) \geq 4$, i.e., that K admits an anisotropic quaternary form.)

Exercise: Prove (that the Hasse Principle implies) the **Hasse Principle for Hyperbolicity**: if q is a quadratic form over a global field K, then q is hyperbolic iff q_v is hyperbolic for all $v \in \Sigma_K$.

2. The Hasse Principle Over $\mathbb{Q}$

2.1. Preliminary Results: Reciprocity and Approximation.

Let $a, b \in \mathbb{Q}^\times$. Then for all $v \in \Sigma_{\mathbb{Q}}$ we have the Hilbert symbol $(a,b)_v$. One of the key ideas in this subject is to examine relations among the various $(a,b)_v$.

Lemma 7. *Let $a, b \in \mathbb{Q}^\times$.*
a) For all odd primes $p \nmid ab$, $(a,b)_p = 1$.
b) In particular, $\{v \in \Sigma_{\mathbb{Q}} \mid (a,b)_v = -1\}$ is finite.

Exercise: Prove Lemma 7.

Exercise: Let $a, b \in \mathbb{Q}^\times$. Show that if the quadratic form $ax^2 + by^2 - z^2 = 0$ is isotropic, $(a,b)_v = 1$ for all $v \in \Sigma_{\mathbb{Q}}$.

Theorem 8. *(Hilbert Reciprocity Law) For $a, b \in \mathbb{Q}^\times$, we have*

$$\prod_{v \in \Sigma_{\mathbb{Q}}} (a,b)_v = 1. \tag{1}$$

Proof. Because of the bilinearity of Hilbert symbols, it suffices to prove the result when each of a and b is either -1 or a prime number. Moreover, of course what we are trying to establish is that in each case, $\#\{v \in \Sigma_{\mathbb{Q}} \mid (a,b)_v = -1\}$ is even.
Case 1: $a = b = -1$. We have $(-1,-1)_v = -1$ iff $v \in \{2, \infty\}$.
Case 2: $a = -1, b = 2$. Since $-(1)^2 + 2(1)^2 - (1)^2 = 0$, by Exercise X.X we have $(-1,2)_v = 1$ for all $v \in \Sigma_{\mathbb{Q}}$.
Case 3: $a = -1$, $b = \ell$ an odd prime. We have $(-1,\ell)_v = 1$ except possibly for $v \in \{2, \ell\}$ and $(-1,\ell)_2 = (1,\ell)_\ell = (-1)^{\frac{\ell-1}{2}}$.
Case 4: $a = b = p$ is a pime (possibly 2). By X.X, for all $v \in \Sigma_{\mathbb{Q}}$, $(a,a)_v = (-1,a)_v$, so we are reduced to Cases 2 and 3.
Case 5: $a = 2$, $b = \ell$ an odd prime. We have $(2,\ell)_v = 1$ except possibly for $v \in \{2, \ell\}$. Further, we have

$$(2,\ell)_2 = 1 \iff \ell \equiv \pm 1 \pmod 8,$$
$$(2,\ell)_\ell = 1 \iff \left(\frac{2}{\ell}\right) = 1 \iff \ell \equiv \pm 1 \pmod 8,$$

where we have used the second supplement to the Quadratic Reciprocity Law.
Case 5: $a = \ell_1$, $b = \ell_2$ are distinct odd primes. Then $(\ell_1,\ell_2)_v = 1$ except possibly for $v \in \{2, \ell_1, \ell_2\}$. Further:

$$(\ell_1,\ell_2)_2 = (-1)^{\frac{(\ell_1-1)}{2}\frac{(\ell_2-1)}{2}},$$
$$(\ell_1,\ell_2)_{\ell_1} = \left(\frac{\ell_2}{\ell_1}\right),$$
$$(\ell_1,\ell_2)_{\ell_2} = \left(\frac{\ell_1}{\ell_2}\right).$$

Thus the fact that $(\ell_1,\ell_2)_2(\ell_1,\ell_2)_{\ell_1}(\ell_1,\ell_2)_{\ell_2} = 1$ follows from – indeed, *is* – the Quadratic Reciprocity Law. □

Exercise: If you haven't realized it already, verify that Theorem 8 is equivalent to quadratic reciprocity together with its first and second supplements. However, for the study of quadratic forms over global fields it is an especially graceful formulation of these classical results: as we will see later, Hilbert's Reciprocity Law extends verbatim to any global field.

Theorem 9. *(Global Existence Theorem) Let $a_1, \ldots, a_N \in \mathbb{Q}^\times$. For each $1 \leq i \leq N$ and $v \in \Sigma_{\mathbb{Q}}$, let $\epsilon_{i,v} \in \{\pm 1\}$. The following are equivalent:*
(i) There is $\alpha \in \mathbb{Q}^\times$ such that for all $1 \leq i \leq N$ and all $v \in \Sigma_{\mathbb{Q}}$,

$$(\alpha, a_i)_v = \epsilon_{i,v}.$$

(ii) All of the following hold:
(a) $\{(i,v) \mid \epsilon_{i,v} = -1\}$ is finite.
(b) For $1 \leq i \leq N$, we have $\prod_{v \in \Sigma_{\mathbb{Q}}} \epsilon_{i,v} = 1$.
(c) For all $v \in \Sigma_{\mathbb{Q}}$, there is $\alpha_v \in \mathbb{Q}_v^\times$ such that $(\alpha_v, a_i)_v = \epsilon_{i,v}$.

Proof. (i) $\implies$ (ii): Condition (a) follows from Lemma 7, condition (b) follows from Theorem 8, and condition (c) is obvious: take $\alpha_v = \alpha$ for all v.
(ii) $\implies$ (i): It is no loss of generality to assume that $a_i \in \mathbb{Z}$ for all i. Let $S \subset \Sigma_{\mathbb{Q}}$ consist of 2,∞ and all primes dividing at least one a_i, and let $T \subset \Sigma_{\mathbb{Q}}$ be the set of all places such that $\epsilon_{i,v} = -1$ for some i: these are finite sets.
Case 1 ($S \cap T = \varnothing$):

Let $a = \prod_{\ell \in T \setminus \{\infty\}} \ell$ and $m = 8 \prod_{\ell \in S \setminus \{2,\infty\}} \ell$. Since S and T are disjoint, a and m are coprime, so by Dirichlet's Theorem on Primes in Arithmetic Progression there is a prime number $p \equiv a \pmod{m}$ and $p \notin S \cup T$. We may take $\alpha = ap$. The verification of this is left to the reader as an exercise (or see [Se, pp. 25-26]).
Case 2 (General Case):
For $v \in \Sigma_{\mathbb{Q}}$, $\mathbb{Q}_v^{\times 2}$ is open in $\mathbb{Q}_v^{\times}$. By Artin-Whaples Approximation, there is $\alpha' \in \mathbb{Q}^{\times}$ such that for all $v \in S$, $\frac{\alpha'}{\alpha_v} \in \mathbb{Q}_v^{\times 2}$ and thus

$$(\alpha', a_i)_v = (\alpha_v, a_i)_v = \epsilon_{i,v} \ \forall v \in S.$$

Let $\eta_{i,v} = \epsilon_{i,v}(\alpha', a_i)_v$; then the family $(\eta_{i,v})$ satisfies conditions (a), (b) and (c) and $\eta_{i,v} = 1$ for all $v \in S$. By Case 1 above, there is $\beta \in \mathbb{Q}^{\times}$ such that $(\beta, a_i)_v = \eta_{i,v}$ for all i and all $v \in \Sigma_{\mathbb{Q}}$. We may take $\alpha = \beta\alpha'$. □

Exercise: Fill in the details of Case 1 in the proof of Theorem 9.

Let R be a Dedekind domain with fraction field R. Then the discrete valuations on K with valuation ring containing R are precisely the $\mathfrak{p}$-adic valuations $v_{\mathfrak{p}}$ for $\mathfrak{p}$ a nonzero prime ideal of R. For each such $\mathfrak{p}$, let $| \cdot |_{\mathfrak{p}}$ denote a corresponding non-Archimedean absolute value on R, say $x \mapsto e^{-v_{\mathfrak{p}}(x)}$.

Theorem 10. *(Dedekind Approximation Theorem) Let R be a Dedekind domain with fraction field K. Let $\mathcal{P}$ be a finite set of nonzero prime ideals of R. For each $\mathfrak{p} \in \mathcal{P}$ we give ourselves $n_{\mathfrak{p}} \in \mathbb{Z}$ and $x_{\mathfrak{p}} \in K$. Then there is $x \in K$ such that:*
(i) For all $\mathfrak{p} \in \mathcal{P}$, $v_{\mathfrak{p}}(x - x_{\mathfrak{p}}) = n_{\mathfrak{p}}$ and
(ii) $v_{\mathfrak{q}}(x) \geq 0$ for all nonzero prime ideals $\mathfrak{q} \notin \mathcal{P}$.

Proof. Step 1: For $\mathfrak{p} \in \mathcal{P}$, the set $U_{\mathfrak{p}}$ of elements $y \in K_{\mathfrak{p}}$ such that $v_{\mathfrak{p}}(y - x_{\mathfrak{p}}) = n_{\mathfrak{p}}$ is nonempty and (cl)open. Applying Artin-Whaples Approximation to the set $\{| \cdot |_{\mathfrak{p}}\}_{\mathfrak{p} \in \mathcal{P}}$, we get $y \in K$ such that $v_{\mathfrak{p}}(y - x_{\mathfrak{p}}) = n_{\mathfrak{p}}$ for all $\mathfrak{p} \in \mathcal{P}$.
Step 2: Let $\mathcal{Q}$ be the finite set of prime ideals $\mathfrak{q} \notin \mathcal{P}$ such that $v_{\mathfrak{q}}(y) < 0$. If $\mathcal{Q} = \varnothing$, then we're done – take $x = y$ – so assume $\mathcal{Q} \neq \varnothing$. For each $\mathfrak{p} \in \mathcal{P}$, there exists a positive integer $a_{\mathfrak{p}}$ such that for all $z \in R$ with $z \equiv 1 \pmod{\mathfrak{p}^{a_{\mathfrak{p}}}}$, $v_{\mathfrak{p}}(yz - x_i) = n_{\mathfrak{p}}$. Applying the Chinese Remainder Theorem to the set $\{\mathfrak{p}^{a_{\mathfrak{p}}} \mid \mathfrak{p} \in \mathcal{P}\} \coprod \mathcal{Q}$ of pairwise comaximal ideals of R, we get $z \in R$ such that for all $\mathfrak{p} \in \mathcal{P}$ $v_{\mathfrak{p}}(yz - x_{\mathfrak{p}}) = n_{\mathfrak{p}}$ and for all $\mathfrak{q} \in \mathcal{Q}$, $v_{\mathfrak{q}}(yz) = 0$. So we may take $x = yz$. □

Theorem 11. *Let $\mathcal{P}$ be a finite subset of $\Sigma_{\mathbb{Q}}$. Suppose given $t_p \in \mathbb{Q}_p^{\times 2}$ for all $v \in \mathcal{P}$. Then there is $t \in \mathbb{Q}^{\times}$ such that*
(i) $t \equiv t_p \pmod{\mathbb{Q}_p^{\times 2}}$ for all $v \in \mathcal{P}$, and
(ii) $|t|_p = 1$ for all but possibly at most one finite prime $p \notin \mathcal{P}$.

Proof. Let $\mathcal{P}_f = \mathcal{P} \setminus \{\infty\}$. Let $\epsilon \in \{\pm 1\}$ have the same sign as p_∞ if $\infty \in \mathcal{P}$; if $\infty \notin \mathcal{P}$, put $\epsilon = 1$. Put

$$\beta = \epsilon \prod_{p \in \mathcal{P}_f} p^{v_p(t_p)}.$$

Then for all $p \in \mathcal{P}_f$, we may write $\beta = u_p t_p$ for some $u_p \in \mathbb{Z}_p^{\times}$; if $2 \notin \mathcal{P}$, put $u_2 = 1$. By the Dedekind Approximation Theorem, there is $z \in \mathbb{Z}$ such that $z \equiv u_p \pmod{p}$ for all odd $p \in \mathcal{P}_f$ and $z \equiv u_2 \pmod{8}$. By the Local Square Theorem, $z \equiv u_p \pmod{\mathbb{Q}_p^{\times 2}}$ for all $p \in \mathcal{P}_f$. Since $\gcd(z, 8\prod_{p \in \mathcal{P}_f} p) = 1$, by Dirichlet's Theorem there is a prime $p_0 \equiv z \pmod{8 \prod_{p \in \mathcal{P}_f} p}$. We may take $t = p_0\beta$. □

2.2. $n \leq 1$.

These cases are absolutely trivial, as every quadratic form over a field in at most one variable is anisotropic!

2.3. $n = 2$.

Recall that a binary form q over any field K is isotropic iff $-\operatorname{disc} q \in K^{\times 2}$.

Let q be a binary form over $\mathbb{Q}$ – we may assume that q has $\mathbb{Z}$-coefficients – such that $q_v = q_{/\mathbb{Q}_v}$ is isotropic for all $v \in \Sigma_{\mathbb{Q}}$. By the above remark, for all $v \in \Sigma_{\mathbb{Q}}$, $-\operatorname{disc} q \in \mathbb{Q}_v^{\times 2}$. For $v = \infty$ this says $-\operatorname{disc} q > 0$. For $v = p$ a finite prime it certainly implies that $v_p(-\operatorname{disc} q)$ is even. By unique factorization in $\mathbb{Z}$, this implies that $-\operatorname{disc} q = n^2$ for some $n \in \mathbb{Z}$, so $\operatorname{disc} q \equiv -1 \pmod{\mathbb{Q}^{\times 2}}$ and q is isotropic.

2.4. $n = 3$.

The Hasse Principle for ternary forms over $\mathbb{Q}$ is equivalent to the following classical theorem of Legendre. Let $q_{\mathbb{Q}}$ be a locally isotropic ternary quadratic form. Via a change of variables, we may take q to have the form

$$q(x, y, z) = ax_1^2 + bx_2^2 + cx_3^2,$$

with a, b, c nonzero *squarefree* integers. If a, b, c were all positive or all negative, $q_{/\mathbb{R}}$ would be anisotropic. Thus, up to relabeling and multiplying through by -1, we may – and shall – assume that a is positive and b and c are negative.

Finally, we may reduce to the case in which a, b, c are coprime in pairs, or equivalently that abc is squarefree. We leave this as a simple but enlightening exercise for the reader. Thus we are led to consider the **Legendre equation**

$$ax^2 + by^2 + cz^2 = 0, \tag{2}$$

with $a > 0$, $b, c < 0$ and abc squarefree.

We can "remove the p-adic numbers" via the following observation: $q_{\mathbb{Q}_p}$ is isotropic for all primes p iff $q_{\mathbb{Z}_p}$ is isotropic for all primes p iff $q_{\mathbb{Z}/p^n\mathbb{Z}}$ is isotropic for all p and n iff $q_{/\mathbb{Z}/n\mathbb{Z}}$ is isotropic for all $n \in \mathbb{Z}^+$.

We claim that if $q(x, y, z)$ is isotropic, then $-bc$ is a square modulo a, $-ac$ is a square modulo b, and $-ab$ is a square modulo c. Indeed, suppose there are $x, y, z \in \mathbb{Q}$, not all zero, such that $ax^2 + by^2 + cz^2 = 0$. By rescaling, we may assume that $(x, y, z) \in \mathbb{Z}^3$ and $\gcd(x, y, z) = 1$.

Let p be a prime dividing a. Reducing 2 modulo a gives

$$by^2 + cz^2 \equiv 0 \pmod{p}.$$

If y and z were both divisible by p, then since $ax^2 + by^2 + cz^2 = 0$, $p \mid ax^2$. Since $p \mid a$ and $\gcd(a, c) = 1$, $p \mid x^2$ and thus $p \mid x$, contradicting $\gcd(x, y, z) = 1$. So we may assume that at least one of y and z is invertible modulo p; with no real loss of generality we assume y is invertible modulo p. Then $by^2 \equiv -cz^2 \pmod{p}$, so

$$-bc \equiv \left(\frac{cz}{y}\right)^2 \pmod{p},$$

i.e., $-bc$ is a square modulo p. Since this argument holds for every prime dividing the squarefree integer a, by the Chinese Remainder Theorem $-bc$ is a square modulo a. And of course a perfectly symmetrical argument shows that $-ac$ is a square modulo b and that $-ab$ is a square modulo c.

This was easy. Remarkably, Legendre showed that these easy necessary conditions are also sufficient for the existence of a nontrivial solution to 2.

Theorem 12. *(Legendre) The Legendre Equation*

$$q(x, y, z) = ax^2 + by^2 + cz^2 = 0$$

has a nontrivial integer solution iff $-bc$ is a square modulo a, $-ac$ is a square modulo b and $-ab$ is a square modulo c.

We will give a geometry of numbers proof of Theorem 12. For an even more elementary proof, see [NT, §17.2].

Lemma 13. *Let $m \in \mathbb{Z}^+$ and let $\epsilon_1, \epsilon_2, \epsilon_3 \in \mathbb{R}^{>0}$ be such that $\epsilon_1\epsilon_2\epsilon_3 \geq m$. Let $\ell(x, y, z) = \alpha x + \beta y + \gamma z \in \mathbb{Z}[x, y, z]$ be any linear polynomial. Then there are $(x, y, z) \in (\mathbb{Z}^3)^\bullet$ such that*

$$\ell(x, y, z) \equiv 0 \pmod{m} \tag{3}$$

and $|x| \leq \epsilon_1$, $|y| \leq \epsilon_2$, $|z| \leq \epsilon_3$.

Exercise: Prove Lemma 13. (Suggestion: show that (3) defines a sublattice $\Lambda \subset \mathbb{Z}^3$ of index dividing m, and apply Minkowski's Linear Forms Theorem [GoN, §9.2].)

We now begin the proof of Legendre's Theorem. First, we may assume that b and c are not both -1. Indeed, if $b = c = -1$, then the condition $-bc$ is a square modulo a gives that -1 is a square modulo a and thus a is a sum of two integer squares, yielding a nontrivial solution to $ax^2 - y^2 - z^2 = 0$.

We claim that our congruence conditions force $q(x, y, z)$ are necessary and sufficient for the existence of linear forms $L_1(x, y, z), L_2(x, y, z) \in \mathbb{Z}[x, y, z]$ such that

$$q(x, y, z) \equiv L_1(x, y, z)L_2(x, y, z) \pmod{abc}.$$

Since a, b, c are coprime in pairs, it is sufficient to show the factorization of q into linear forms modulo a, modulo b and modulo c; then by the Chinese Remainder Theorem we may choose $L_1, L_2 \in \mathbb{Z}[x, y, z]$ which reduce modulo a, b and c to the linear factors of q. So: let r be such that $r^2 \equiv -bc \pmod{a}$, and let c' be such that $cc' \equiv 1 \pmod{a}$. Then

$$q(x, y, z) = ax^2 + by^2 + cz^2 \equiv by^2 + cz^2 \equiv cc'(by^2 + cz^2) \equiv c'(bcy^2 + c^2z^2)$$
$$\equiv c'(c^2z^2 - r^2y^2) \equiv c'(cz + ry)(cz - ry) \equiv L_1(x, y, z)L_2(x, y, z) \pmod{a}.$$

By symmetry similar arguments can be made modulo b and c. So we get

$$q(x, y, z) \equiv L_1(x, y, z)L_2(x, y, z) = (\alpha x + \beta y + \gamma z)(\alpha' x + \beta' y + \gamma' z) \pmod{abc}.$$

Now apply Lemma 13 with $m = abc$, $\epsilon_1 = \sqrt{|bc|}$, $\epsilon_2 = \sqrt{|ac|}$, $\epsilon_3 = \sqrt{|ab|}$: there are $(x_1, y_1, z_1) \in (\mathbb{Z}^3)^\bullet$ with

$$|x_1| \leq \sqrt{bc},\ |y_1| \leq \sqrt{ac},\ |z_1| \leq \sqrt{ab}$$

and

$$L_1(x_1, y_1, z_1) \equiv 0 \pmod{abc}.$$

Since $q \equiv L_1 L_2 \pmod{abc}$, this implies

$$q(x_1, y_1, z_1) \equiv 0 \pmod{abc}.$$

Note that we have

$$x_1^2 \leq bc, \ y_1^2 \leq -ac, \ z_1^2 \leq -ab.$$

In fact, since bc is squarefree and greater than 1, we must have $x_1^2 < bc$. Similarly, if $y_1^2 = -ac$ then $a = 1$ and $c = -1$, and if $z_1^2 = -ab$ then $a = 1$ and $b = -1$, so at least one of the two inequalities must be strict and thus

$$-2abc < by_1^2 + cz_1^2 \leq ax_1^2 + by_1^2 + cz_1^2 \leq ax_1^2 < abc.$$

Thus either $q(x_1, y_1, z_1) = 0$ – great! – or $q(x_1, y_1, z_1) = -abc$. In the latter case, the ternary form q represents $-\operatorname{disc}(q)$ hence is isotropic by [NCA, Cor. 95].[1] If one wants to avoid this result, here is a completely elementary finish: put

$$x_2 = -by_1 + x_1 z_1,$$

$$y_2 = ax_1 + y_1 z_1,$$

$$z_2 = z_1^2 + ab.$$

Then

$$q(x_2, y_2, z_2) = ab(ax_1^2 + by_1^2 + cz_1^2) + z_1^2(ax_1^2 + by_1^2 + cz_1^2) + abcz_1^2 + a^2b^2c$$
$$= ab(-abc) - abcz_1^2 + abcz_1^2 + a^2b^2c = 0,$$

so (x_2, y_2, z_2) satisfies 2. If $z_2 = z_1^2 + ab = 0$ then $a = 1$, $b = -1$, and $(1, 1, 0)$ is a nontrivial solution of 2.

Before moving on we record the following strengthening of the ternary Hasse Principle over $\mathbb{Q}$.

Theorem 14. *Let q be a ternary rational quadratic form, and let $p_0 \in \Sigma_{\mathbb{Q}}$. If for all $p \in \Sigma_{\mathbb{Q}} \setminus \{p_0\}$, q_p is isotropic, then q is isotropic.*

Proof. Since an/isotropy is not affected by scaling, we may assume $q = \langle a, b, -1 \rangle$, so for any $v \in \Sigma_{\mathbb{Q}}$, q_v is isotropic iff $(a, b)_v = 1$. By Hilbert Reciprocity we have $1 = \prod_{v \in \Sigma_{\mathbb{Q}}} (a, b)_v = (a, b)_{v_0}$. Thus q_{v_0} is also isotropic, i.e., q is locally isotropic, and by the ternary Hasse Princile q is isotropic. □

2.5. $n = 4$.

After consulting the literature, we were not able to choose between two different proofs of the $n = 4$ case. We will give both of them: the first is taken from [Se], the second from [C] and [G].

First proof: Let $q = \langle a, b \rangle - \langle c, d \rangle$ be locally isotropic. By the Isotropy Criterion, for each $v \in \Sigma_{\mathbb{Q}}$, since q_v is isotropic, there is $\alpha_v \in \mathbb{Q}_v^\times$ which is $\mathbb{Q}_v$-represented by both $ax_1^2 + bx_2^2$ and $cx_3^2 + dx_4^2$. By [QF4, Lemma 9], for all $v \in \Sigma_{\mathbb{Q}}$,

$$(\alpha_v, -ab)_v = (a, b)_v, \ (\alpha_v, -cd)_v = (c, d)_v.$$

We may now apply Theorem 7 to get $\alpha \in \mathbb{Q}^\times$ such that

$$(\alpha, -ab)_v = (a, b)_v, \ (\alpha, -cd)_v = (c, d)_v \ \forall v \in \Sigma_{\mathbb{Q}}.$$

[1] I am indebted to Danny Krashen for pointing out this simplification of the end of the proof.

By [QF4, Lemma 9] the binary form $\langle a, b\rangle$ K_v-represents α for all $v \in \Sigma_{\mathbb{Q}}$; equivalently, the ternary form $\langle a, b, -\alpha\rangle$ is locally isotropic and thus isotropic by the previous section; equivalently, $\langle a, b\rangle$ represents α. Similarly, $\langle a, b\rangle$ repesents α, and thus by the Isotropy Condition q is isotropic.

Second proof: We may take q of the form $\langle a_1, a_2, a_3, a_4\rangle$, with each a_i a squarefree integer. Let $\mathcal{P} = \{p \mid p \mid 2 \operatorname{disc} q\} \cup \{\infty\}$. Then for all $p \notin \mathcal{P}$, we have $(a_i, a_j)_p = 1$ for all $1 \leq i, j \leq 4$. For $p \in \Sigma_{\mathbb{Q}}$, since q_p is isotropic, by the Isotropy Criterion there is $t_p \in \mathbb{Q}_p^{\times}$ such that $\langle a_1, a_2\rangle_p$ and $\langle a_3, a_4\rangle_p$ both $\mathbb{Q}_p$-represent t_p. Apply Theorem 11 to get $t \in \mathbb{Z}$ and a prime number p_0. Then $\langle a_1, a_2, -t\rangle_p$ and $\langle a_3, a_4, -t\rangle_p$ are isotropic for all $p \in \mathcal{P}$. Further, for all $p \notin (\mathcal{P} \cup \{p_0\})$, $\langle a_1, a_2, -t\rangle_p$ and $\langle a_3, a_4, -t\rangle_p$ are isotropic since their entries are p-adic units. Thus the ternary forms $\langle a_1, a_2, -t\rangle$ and $\langle a_3, a_4, -t\rangle$ are locally isotropic except possibly at p_0, so by Theorem 14 they are both isotropic. Then $\langle a_1, a_2\rangle$ and $\langle a_3, a_4\rangle$ both $\mathbb{Q}$-represent t, so $q = \langle a_1, a_2\rangle - \langle a_3, a_4\rangle$ is isotropic.

2.6. $n \geq 5$.

Since every quadratic form in at least five variables over a CDVR with finite residue field is isotropic, in this case the Hasse Principle for isotropy amounts to: if q is indefinite, then q is isotropic. An indefinite form in more than five variables has an indefinite subform in exactly five variables, so it suffices to treat the case $n = 5$.

Now write $h = \langle a_1, a_2\rangle - \langle a_3, a_4, a_5\rangle$. Let $\mathcal{V}$ be ∞ together with the set of primes dividing $2a_1 \cdots a_5$. For each $v \in \mathcal{V}$, h_v is isotropic, so by the Isotropy Criterion there is $\alpha_v \in \mathbb{Q}_v^{\times}$ such that $\langle a_1, a_2, -\alpha_v\rangle$ and $\langle a_3, a_4, a_5, -\alpha_v\rangle$ are both isotropic. In particular, for each $v \in \mathcal{V}$ there are $b_{1,v}, b_{2,v} \in \mathbb{Q}_v$ such that

$$\alpha_v = a_1 b_{1,v}^2 + a_2 b_{2,v}^2.$$

By Artin-Whaples Approximation, there are $b_1, b_2 \in \mathbb{Q}^{\times}$ such that for all $v \in \mathcal{V}$,

$$a_1 b_1^2 + a_2 b_2^2 \equiv \alpha_v \pmod{\mathbb{Q}_v^{\times 2}} \ \forall v \in \mathcal{V}.$$

Put $\alpha = a_1 b_1^2 + a_2 b_2^2$. It follows that $\langle a_3, a_4, a_5, -\alpha\rangle$ is $\mathbb{Q}_v$-isotropic for all $v \in \mathcal{V}$. It also $\mathbb{Q}_v$-isotropic for all other v – indeed, the ternary subform $\langle a_3, a_4, a_5\rangle$ already has this property – so by the $n = 4$ case $\langle a_3, a_4, a_5, -\alpha\rangle$ is $\mathbb{Q}$-isotropic: there are $x_3, x_4, x_5, y \in \mathbb{Q}$, not all 0, such that

$$a_3 x_3^2 + a_4 x_4^2 + a_5 x_5^2 = \alpha y^2 = a_1 (b_1 y)^2 + a_2 (b_2 y)^2,$$

and thus h is $\mathbb{Q}$-isotropic.

3. The Hasse Principle Over a Global Field

We now wish to prove the Hasse Principle for Isotropy for quadratic forms over an *arbitrary* global field K. Here are the main ideas of the proof: the case $n \leq 1$ is still trivial, of course. Each of the cases $n = 2$ and $n = 3$ turns out to follow from a big theorem in algebraic number theory, as we will explain (and then outsource to standard works). On the other hand, via a dirty trick it will turn out that knowing the $n = 3$ case of the Hasse Principle for *all* global fields allows for an easier proof of the $n = 4$ case of the Hasse Principle over our fixed global field K! Finally, the case of $n \geq 5$ goes exactly as in the case of $K = \mathbb{Q}$.

3.1. $n = 2$.

Let q be a binary form over K. As in the case $K = \mathbb{Q}$, it comes down to the following: given that $-\operatorname{disc} q \in K_v^{\times 2}$ for all $v \in \Sigma_K$, we must show that $-\operatorname{disc} q \in K^{\times 2}$. The following theorem accomplishes this.

Theorem 15. *(Global Square Theorem) For $a \in K^\times$, the following are equivalent:*
(i) a is a square in K: there exists $b \in K$ with $b^2 = a$.
(ii) a is a local square*: for all $v \in \Sigma_v$, there is $b_v \in K_v$ with $b_v^2 = a$.*

Proof. (i) $\implies$ (ii) is immediate.
$\neg$ (i) $\implies$ $\neg$ (ii): suppose that $a \in K^\times \setminus K^{\times 2}$: then $L = K(\sqrt{a})$ is a quadratic field extension (and even a Galois extension, since we are "globally" excluding the case of characteristic 2). We may therefore apply a case of the celebrated Cebotarev Density Theorem: the set of finite places v of K which split in the extension L/K has density equal to $\frac{1}{[L:K]}$. In particular, there are infinitely many places v which *do not* split in L, which means that $K_v \otimes_K L = K_v(\sqrt{a})$ is a quadratic field extension of K_v, so $a \in K_v^\times \setminus K_v^{\times 2}$. □

Exercise: Let K be a global field. Show that the natural map

$$K^\times / K^{\times 2} \to \prod_{v \in \Sigma_K} K_v^\times / K_v^{\times 2}$$

is injective.

Exercise: Let $q_{/K}$ be a binary quadratic form, and let $S_q = \{ v \in \Sigma_K \mid q_v \text{ is isotropic } \}$.
a) Show that if q is isotropic, $S_q = \Sigma_K$.
b) Show that if q is anisotropic, S_q has density $\frac{1}{2}$.

3.2. $n = 3$.

Proposition 16. *For a global field K, the following are equivalent:*
(i) The Hasse Principle holds for ternary quadratic forms over K.
(ii) The Hasse Principle holds for Hilbert Symbols over K: for $a, b \in K^\times$, we have $(a, b) = 1$ iff $(a, b)_v = 1$ for all $v \in \Sigma_K$.
(iii) The Hasse Principle holds for plane conics over K: if $C_{/K}$ is a smooth plane conic such that $C(K_v) \neq \varnothing$ for all $v \in \Sigma_K$, then $C(K) \neq \varnothing$.
(iv) The Hasse Principle holds for quaternion algebras over K: if $B_{/K}$ is a quaternion algebra such that $B_v = B \otimes_K K_v \cong M_2(K_v)$ for all $v \in \Sigma_K$.
(v) The Hasse Principle holds for quaternary quadratic forms over K of square discriminant.

Proof. First observe that a form q is isotropic iff any *similar* form αq (for $\alpha \in K^\times$ is isotropic.
(i) $\implies$ (ii): This is immediate, since the Hilbert symbol (a, b) tracks the an/isotropy of the ternary form $ax^2 + by^2 - z^2 = 0$.
(ii) $\implies$ (i): Every ternary quadratic form is similar to some $ax^2 + by^2 - z^2 = 0$.
(i) $\iff$ (iii) is immediate.
(iii) $\iff$ (iv) follows from the equivalence between conics and quaternion algebras.
(iv) $\iff$ (v): A quadratic form is quaternary of square discriminant iff it is similar to the norm form of a quaternion algebra. □

Proposition 16 gives us several possible avenues of attack. For instance, to show that (ii) holds, we may reason as follows: for any field K, the Hilbert symbol $(a, b) = 1$ – i.e., the quadratic form $ax^2 + by^2 - z^2 = 0$ is isotropic – iff a is a norm from the quadratic extension $K(\sqrt{b})/K$. So if $(a, b)_v = 1$ for all $v \in \Sigma_K$, then for all $v \in \Sigma_K$, a is a norm from the quadratic algebra $L_v = K(\sqrt{b}) \otimes_K K_v$. Now we invoke the following deep result.

Theorem 17. *(Hasse Norm Theorem) Let L/K be a cyclic Galois extension of global fields. For $a \in K^\times$, TFAE:*
(i) $a \in N_{L/K}(L)$.
(ii) a is a local norm: for all $v \in \Sigma_K$, $a \in N_{L \otimes_K K_v/K_v}(L \otimes_K K_v)$.

Proof. See e.g. [M-CFT, Thm. VIII.1.4]. □

This works! On the other hand, (iv) gives us a chance to apply an even deeper theorem to get a slightly (but usefully!) stronger result.

Theorem 18. *(Albert-Brauer-Hasse-Noether)*
a) There is an exact sequence

$$0 \longrightarrow \operatorname{Br} K \longrightarrow \bigoplus_{v \in \Sigma_K} \operatorname{Br}(K_v) \xrightarrow{\text{inv}} \mathbb{Q}/\mathbb{Z} \longrightarrow 0. \tag{4}$$

b) Every element of $\operatorname{Br}(K)[2]$ *and* $\operatorname{Br}(K_v)[2]$ *is a quaternion algebra, and there is an exact sequence*

$$0 \longrightarrow (\operatorname{Br} K)[2] \longrightarrow \bigoplus_{v \in \Sigma_K} (\operatorname{Br} K_v)[2] \xrightarrow{\text{inv}} \mathbb{Z}/2\mathbb{Z} \longrightarrow 0. \tag{5}$$

Proof. See [P, Ch. 18]. □

In more down to earth terms, part b) asserts that the Hasse principle holds for Hilbert symbols together with the following result.

Theorem 19. *(Hilbert Reciprocity Law) For $a, b \in K^\times$, we have $\prod_{v \in \Sigma_K} (a, b)_v = 1$.*

From this we deduce the following result.

Theorem 20. *Let q be a ternary quadratic form over a global field K. Let $v_0 \in \Sigma_K$. If for all $v \neq v_0$, q_v is isotropic, then q is isotropic.*

3.3. $n = 4$.

Let q be a locally isotropic quadratic form over K. If $\operatorname{disc} q = 1$, then by the work of the previous section – and, especially, by Proposition 16(v) – q is isotropic. The case in which $\operatorname{disc} q \neq 1$ really is different.

Exercise: Let q be a quaternary form over a global field.
a) Suppose that there is $v_0 \in \Sigma_K$ such that q_v is isotrpic for all $v \neq v_0$. Show that q is isotropic.
b) Show that the quadratic form $q = \langle 1, 1, 1, 7 \rangle$ over $\mathbb{Q}$ is anisotropic at $v = \infty$ and at no finite place.

To get around this dichotomy we do something sneaky: we **extend the base**. This is justified by the following result.

Theorem 21. *Let K be a field, $\alpha \in K^\times \setminus K^{\times 2}$, and put $L = K(\sqrt{\alpha})$. For an anisotropic form q over K, TFAE:*
(i) q_L is isotropic.
(ii) q contains a binary subform f of discriminant $-\alpha$.

Proof. (i) $\implies$ (ii): Let $q = \langle a_1, \ldots, a_n \rangle$. Since q_L is isotropic, there are $x_1, \ldots, x_n, y_1, \ldots, y_n \in K$, not all zero, such that $\sum_{i=1}^n a_i(x_i + y_i\sqrt{\alpha})^2 = 0$. Resolving this equation into its rational and irrational parts, we get

$$\sum_{i=1}^n a_i x_i^2 + \alpha \sum_{i=1}^n a_i y_i^2 = 0, \tag{6}$$

$$\sum_{i=1}^n a_i x_i y_i = 0. \tag{7}$$

Equation (7) tells us that $x = (x_1, \ldots, x_n)$ and $y = (y_1, \ldots, y_n)$ are orthgonal in the quadratic space (K^n, q), whereas (6) tells us that $q(x) = -\alpha q(y)$, which, since q anisotropic, implies that *both* x and y are nonzero vectors. Since α is not a square, $q(x)$ and $q(y)$ lie in different square classes, so the vectors x and y are a basis for a two-dimensional subspace on which q restricts to the quadratic form $f = \langle q(x), q(y) \rangle$, of discriminant $q(x)q(y) = -\alpha$.
(ii) $\implies$ (i): Since $\operatorname{disc} f = -\alpha$, $\operatorname{disc} f_L = -1$. Thus $f_L \cong \mathbb{H}$ is a subform of q_L, so q_L is isotropic. □

Corollary 22. *Let K be a field, and let q be a quaternary quadratic form over K with* $\operatorname{disc} q = \alpha \neq 1$. *Put $L = K(\sqrt{\alpha})$. If q_L is isotropic, then q is isotropic. Then q_L is anisotropic.*

Proof. By Theorem 21, $q = f \oplus g$, with $\dim f = 2$ and $\operatorname{disc} f = -\alpha$. But then g is a binary form of discriminant -1, i.e., $g \cong \mathbb{H}$ is a subform of q, so q is isotropic. □

It should now be clear how to complete the proof of the Hasse Principle for quaternary forms: let q is a locally isotropic quaternary form, and let $L = K(\sqrt{\operatorname{disc} q})$. Then q_L is locally isotropic of square discriminant, so it is isotropic, hence by Corollary 22 so is q.

3.4. $n \geq 5$.

The proof that we gave in the case $K = \mathbb{Q}$ carries over verbatim to the case of an arbitrary global field K, as we invite the reader to check.

4. Some Applications to Integral Forms

4.1. The Aubry-Davenport-Cassels Lemma.

Theorem 23. *(Aubry-Davenport-Cassels) Let $q(x) = q(x_1, \ldots, x_n) \in \mathbb{Z}[x]$ be an integral quadratic form. We suppose that for any $y = (y_1, \ldots, y_n) \in \mathbb{Q}^n \setminus \mathbb{Z}^n$, there exists $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ such that*

$$0 < |q(x - y)| < 1.$$

Then, for any integer d, q represents d rationally iff q represents d integrally.

Proof. For $x, y \in \mathbb{Q}^n$, put $x \cdot y := \frac{1}{2}(q(x+y) - q(x) - q(x))$. Then $(x, y) \mapsto x \cdot y$ is bilinear and $x \cdot x = q(x)$. Note that for $x, y \in \mathbb{Z}^n$, we need not have $x \cdot y \in \mathbb{Z}$, but certainly we have $2(x \cdot y) \in \mathbb{Z}$. Our computations below are parenthesized so as to emphasize this integrality property.

Let $d \in \mathbb{Z}$, and suppose that there exists $x \in \mathbb{Q}^n$ such that $q(x) = d$. Equivalently, there exists $t \in \mathbb{Z}$ and $x' \in \mathbb{Z}^n$ such that $t^2 d = x' \cdot x'$. We choose x' and t such that $|t|$ is minimal, and it is enough to show that $|t| = 1$.

Applying the hypothesis to $x = \frac{x'}{d}$, there is $y \in \mathbb{Z}^n$ such that if $z = x - y$, we have $0 < |q(z)| < 1$. Now put

$$a = y \cdot y - d,$$

$$b = 2(dt - x' \cdot y),$$

$$T = at + b,$$

$$X = ax' + by.$$

Then $a, b, T \in \mathbb{Z}$, and $X \in \mathbb{Z}^n$.

Claim: $X \cdot X = T^2 d$.

Indeed,

$$X \cdot X = a^2(x' \cdot x') + ab(2x' \cdot y) = b^2(y \cdot y) = a^2t^2d + ab(2dt - b) + b^2(d + a)$$

$$= d(a^2t^2 + 2abt + b^2) = T^2 d.$$

Claim: $T = t(z \cdot z)$.

Indeed,

$$tT = at^2 + bt = t^2(y \cdot y) - dt^2 + 2dt^2 - t(2x' \cdot y)$$

$$= t^2(y \cdot y) - t(2x' \cdot y) + x' \cdot x' = (ty - x') \cdot (ty - x') = (-tz) \cdot (-tz) = t^2(z \cdot z).$$

Since $0 < |z \cdot z| < 1$, we have $0 < |T| < |t|$, contradicting the minimality of $|t|$. □

Remark: Theorem 23 has a curious history. So far as I know there is no paper of Davenport and Cassels which contains it: it is more folkloric. The attribution of this result is due to J.-P. Serre in his influential text [Se]. Later, André Weil pointed out [W] that in the special case of $f(x) = x_1^2 + x_2^2 + x_3^2$, the result goes back to a 1912 paper of the amateur mathematician L. Aubry [Au12].

Let us say an integral quadratic form q is **Euclidean** if for all $y = (y_1, \ldots, y_n) \in \mathbb{Q}^n \setminus \mathbb{Z}^n$, there is $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$ such that $0 < |q(x - y)| < 1$. An integral quadratic form is **ADC** if for all $d \in \mathbb{Z}$, if q $\mathbb{Q}$-represents d, then q $\mathbb{Z}$-represents d.

With this new terminology, we get a pithy restatement of Theorem 23.

Theorem 24. *(Aubry-Davenport-Cassels) Every Euclidean integral form is ADC.*

Exercise: a) Suppose that $q(x) \in \mathbb{Z}[x]$ is an anisotropic quadratic form. Show that q is Euclidean iff for all $x \in \mathbb{Q}^n$, there exists $y \in \mathbb{Z}^n$ such that $|q(x - y)| < 1$.

b) Show that the criterion of part a) does not work for isotropic forms by considering $q(x, y) = x^2 - y^2$.

Proposition 25. *Let $n, a_1, \ldots, a_n \in \mathbb{Z}^+$. Then the integral quadratic form $q(x) = a_1x_1^2 + \ldots + a_nx_n^2$ is Euclidean iff $\sum_i a_i < 4$.*

Exercise: Prove Proposition 25.

4.2. **Two, Three and Four Squares.**

Our goal in this section is to prove the following celebrated classical results.

Theorem 26. *(Fermat-Euler Two Squares Theorem)*
For $n \in \mathbb{Z}^+$, the following are equivalent:
(i) For every prime $p \equiv 3 \pmod 4$, $v_p(n)$ is even.
(ii) n is a sum of two integer squares: there are $x, y \in \mathbb{Z}$ with $x^2 + y^2 = n$.

Theorem 27. *(Legendre-Gauss Three Squares Theorem) For $n \in \mathbb{Z}^+$, the following are equivalent:*
(i) n is not *of the form $4^a(8k+7)$ for any $a \in \mathbb{N}$ and $k \in \mathbb{Z}$.*
(ii) n is a sum of three integer squares: there are $x, y, z \in \mathbb{Z}$ with $x^2 + y^2 + z^2 = n$.

Theorem 28. *(Lagrange Four Squares Theorem)*
For all $n \in \mathbb{Z}^+$, there are $x, y, z, w \in \mathbb{Z}^+$ such that $n = x^2 + y^2 + z^2 + w^2$.

4.2.1. *Proof of the Two Squares Theorem.*

Let $q = \langle 1, 1 \rangle$ and $n \in \mathbb{Z}^+$. Since $1 + 1 < 4$, by Proposition 25 q is Euclidean, and thus by Theorem 23 q $\mathbb{Z}$-represents an integer n iff it $\mathbb{Q}$-represents n. Further, q $\mathbb{Q}$-represents $n \in \mathbb{Z}^\bullet$ iff the ternary form $\langle 1, 1, -n \rangle$ is isotropic, which holds iff $(-1, n) = 1$, which by the Hasse Principle plus the Reciprocity law holds iff $(-1, n)_\infty = 1$ and for all odd primes ℓ, $(-1, n)_\ell = 1$. Clearly $(-1, n)_\infty = 1 \iff n > 0$, which we assume henceforth. Further, for every odd prime ℓ we have $(-1, p)_\ell = 1$ if $\ell \neq p$ and $(-1, \ell)_\ell = (-1)^{\frac{\ell-1}{2}}$, i.e., 1 iff $\ell \equiv 1 \pmod 4$. Now write

$$n = 2^a p_1^{b_1} \cdots p_r^{b_r} q_1^{c_1} \cdots q_s^{c_s},$$

where the p_i's are primes which are 1 modulo 4, the q_j's are primes which are three modulo 4 and $a, b_i, c_j \in \mathbb{N}$. Now:
(i) $\implies$ (ii): if each $c_i = 2C_i$ is even, for every odd prime ℓ,

$$(-1, n)_\ell = (-1, 2)_\ell^a (-1, p_1)_\ell^{b_1} \cdots (-1, p_r)_\ell^{b_r} ((-1, q_1)_\ell^{C_1})^2 \cdots ((-1, q_s)_\ell^{C_s})^2 = 1.$$

(ii) $\implies$ (i): if for some $1 \leq j \leq s$ we have c_j is odd, then

$$(-1, n)_{q_j} = (-1, q_j)_{q_j}^{c_j} = -1,$$

so q does not $\mathbb{Q}$-represent n.

4.2.2. *Proof of the Three Squares Theorem.*

Proposition 29. *For $n \in \mathbb{Z}^+$ the following are equivalent:*
(i) n is not *of the form $4^a(8k+7)$.*
(ii) n is $\mathbb{Q}$-represented by q.

Proof. Let $n \in \mathbb{Z}^\bullet$. In particular $n \in \mathbb{Q}$, so by Hasse-Minkowski, q $\mathbb{Q}$-represents n iff q $\mathbb{Q}_v$-represents n for all $v \in \Sigma_{\mathbb{Q}}$. (Conversely, if we know which integers q $\mathbb{Q}$-represents, then we know which raitonal numbers it $\mathbb{Q}$-represents, since q $\mathbb{Q}$-represents $\frac{a}{b}$ iff it $\mathbb{Q}$-represents ab.) As usual, we write q_v for $q_{\mathbb{Q}_v}$.
Step 1: If q_v is isotropic, then it is universal, i.e., there is no condition at v for q to represent n. For $v \in \Sigma_{\mathbb{Q}}$, q_v is isotropic iff $(-1, -1)_v = -1$ iff $v \in \{2, \infty\}$. Indeed, with no calculation we know that $(-1, -1)_p = 1$ for all odd p and $(-1, -1)_\infty = -1$,

so by the Hilbert Reciprocity Law we conclude $(-1,-1)_2 = -1$.[2]
Step 2: Let $v = \infty$. Clearly $q_\infty = x^2 + y^2 + z^2$ $\mathbb{R}$-represents $n \in \mathbb{Z}$ iff $n \geq 0$.
Step 3: Let $v = 2$. By [QF-LOCAL, §2.3] the anisotropic ternary form q_2 $\mathbb{Q}_2$-represents every square class in $\mathbb{Q}_2$ except $-\operatorname{disc} q = -1$. Further, $n \equiv -1 \pmod{\mathbb{Q}_2^{\times 2}}$ iff $v_2(n)$ is even and $\frac{n}{2^{v_2(n)}} \equiv -1 \pmod 8$. We're done. □

Now consider $q = \langle 1,1,1 \rangle$ as an integral form. Since $1+1+1 < 4$, by Proposition 25 q is Euclidean, hence by Theorem 23 it is ADC, so the Legendre-Gauss Three Squares Theorem follows immediately from Proposition 29.

4.2.3. *Proof of the Four Squares Theorem.*

Exercise (Square-squarefree decomposition): For all $n \in \mathbb{Z}^+$, there are unique $a, m \in \mathbb{Z}^+$ with m squarefree such that $n = a^2 m$.

Let $q = \langle 1,1,1,1 \rangle$. If for some $x \in \mathbb{Z}^4$, $q(x) = m$, then $q(ax) = a^2 m$. So it suffices to show that q $\mathbb{Z}$-represents every squarefree positive integer m. By the Three Squares Theorem, m is a sum of three integer squares unless $m = 8k+7$. But if $m = 8k+7$, then $m - 1 = 8k+6$. Now $\operatorname{ord}_2(8k+6) = 1$, so $8k+6$ is not of the form $4^a(8k+7)$, hence $8k+6 = x^2+y^2+z^2$ and $m = 8k+7 = x^2+y^2+z^2+1^2$.

Similar ideas can be used to prove the following mild generalization.

Theorem 30. *For $d \in \mathbb{Z}^+$, the following are equivalent:*
(i) The quadratic form $q = \langle 1,1,1,d \rangle$ $\mathbb{Z}$-represents all positive integers.
(ii) $1 \leq d \leq 7$.

Exercise: Prove Theorem 30.

Exercise: Show that for $n \in \mathbb{Z}^+$, the following are equivalent:
(i) There are integers x, y, z, w such that $n = x^2 + y^2 + z^2 + 8w^2$.
(ii) $n \not\equiv 7 \pmod 8$.

Exercise: Prove or disprove the following claims:
a) If d is a positive integer which is not divisible by 8, then the quadratic form $x^2 + y^2 + z^2 + dw^2$ integrally represents all sufficiently large positive integers.
b) If $d = 8d'$ is a positive integer, then the quadratic form $x^2 + y^2 + z^2 + dw^2$ integrally represents all sufficiently large positive integers which are *not* $7 \pmod 8$.

Exercise: Let $n \geq 4$, and let $q \in \mathbb{Z}[x]$ a positive definite n-ary form. Show TFAE:
(i) q is an ADC form.
(ii) q $\mathbb{Z}$-represents every positive integer.

4.3. **More on Euclidean Forms and ADC Forms.**

We will report on the main results of [ADCII]...as soon as that paper is complete!

[2] This is a circular argument in the sense that we needed to evaluate $(-1,-1)_2$ to prove the Hilbert Reciprocity Law, but it is nice to be able to make quick calculations.

References

[ADCII] P.L. Clark and W.C. Jagy, *Euclidean quadratic forms and ADC forms II*, preprint.

[Au12] L. Aubry, Sphinx-Œdipe 7 (1912), 81–84.

[C] J.W.S. Cassels, *Rational quadratic forms.* London Mathematical Society Monographs, 13. Academic Press, Inc. [Harcourt Brace Jovanovich, Publishers], London-New York, 1978.

[Cop] W.A. Coppel, *Number theory. An introduction to mathematics. Part B.* Revised printing of the 2002 edition. Springer, New York, 2006.

[G] L.J. Gerstein, *Basic Quadratic Forms.*

[GoN] P.L. Clark, *Geometry of numbers and applications to number theory.* Notes available at `www.math.uga.edu/∼pete/geometryofnumbers.pdf`

[L] T.Y. Lam, *Introduction to quadratic forms over fields.* Graduate Studies in Mathematics, 67. American Mathematical Society, Providence, RI, 2005.

[M-CFT] J. Milne, *Class Field Theory.* `http://www.jmilne.org/math/CourseNotes/CFT310.pdf`

[NCA] P.L. Clark, *Non-commutative algebra.* Lecture notes available at `http://www.math.uga.edu/∼pete/noncommutativealgebra.pdf`.

[NZM] I. Niven, H.S. Zuckerman and H.L. Montgomery, *An introduction to the theory of numbers.* Fifth edition. John Wiley & Sons, Inc., New York, 1991.

[NT] P.L. Clark, *Number theory: A Contemporary Introduction.* Notes available at `http://math.uga.edu/∼pete/4400FULL.pdf`

[OM] T.O. O'Meara, *Introduction to quadratic forms.* Reprint of the 1973 edition. Classics in Mathematics. Springer-Verlag, Berlin, 2000.

[P] R.S. Pierce, *Associative algebras.* Graduate Texts in Mathematics, 88. Studies in the History of Modern Science, 9. Springer-Verlag, New York-Berlin, 1982.

[S] W. Scharlau, *Quadratic and Hermitian forms.* Grundlehren der Mathematischen Wissenschaften 270. Springer-Verlag, Berlin, 1985.

[Se] J.-P. Serre, *A course in arithmetic.* Graduate Texts in Mathematics, No. 7. Springer-Verlag, New York-Heidelberg, 1973.

[Ste] E. Steinitz, *Algebraische Theorie der Körper.* J. Reine Angew. Math. 137 (1910), 167-309.

[W] A. Weil, *Number theory. An approach through history from Hammurapi to Legendre.* Reprint of the 1984 edition. Modern Birkhäuser Classics, Boston, MA, 2007.

[Wit] E. Witt, *Theorie der quadratischen Formen in beliebigen Körpern.* J. Reine Angew. Math. 176 (1937), 31-44.