AN ELEMENTARY PROOF OF A THEOREM ON QUADRATIC FORMS OVER THE RATIONAL NUMBERS

Autor(en): **Leep, David B.**

Objekttyp: **Article**

Zeitschrift: **L'Enseignement Mathématique**

Band (Jahr): **35 (1989)**

Heft 1-2: **L'ENSEIGNEMENT MATHÉMATIQUE**

PDF erstellt am: **26.05.2024**

Persistenter Link: https://doi.org/10.5169/seals-57371

Nutzungsbedingungen

Die ETH-Bibliothek ist Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Inhalten der Zeitschriften. Die Rechte liegen in der Regel bei den Herausgebern.
Die auf der Plattform e-periodica veröffentlichten Dokumente stehen für nicht-kommerzielle Zwecke in Lehre und Forschung sowie für die private Nutzung frei zur Verfügung. Einzelne Dateien oder Ausdrucke aus diesem Angebot können zusammen mit diesen Nutzungsbedingungen und den korrekten Herkunftsbezeichnungen weitergegeben werden.
Das Veröffentlichen von Bildern in Print- und Online-Publikationen ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. Die systematische Speicherung von Teilen des elektronischen Angebots auf anderen Servern bedarf ebenfalls des schriftlichen Einverständnisses der Rechteinhaber.

Haftungsausschluss

Alle Angaben erfolgen ohne Gewähr für Vollständigkeit oder Richtigkeit. Es wird keine Haftung übernommen für Schäden durch die Verwendung von Informationen aus diesem Online-Angebot oder durch das Fehlen von Informationen. Dies gilt auch für Inhalte Dritter, die über dieses Angebot zugänglich sind.

Ein Dienst der *ETH-Bibliothek*
ETH Zürich, Rämistrasse 101, 8092 Zürich, Schweiz, www.library.ethz.ch

http://www.e-periodica.ch

L'Enseignement Mathématique, t. 35 (1989), p. 191-202

AN ELEMENTARY PROOF OF A THEOREM ON QUADRATIC FORMS OVER THE RATIONAL NUMBERS

by David B. Leep

Introduction

It is well known, and easy to prove, that each positive rational number is a sum of four rational squares. The main idea of the proof is that the set of nonzero rational numbers which are sums of four squares forms a group under multiplication.

Let F be a field of characteristic $\neq 2$, $F^\times$ the nonzero elements of F, and let $\langle a_1, ..., a_n\rangle$ denote the quadratic form $a_1x_1^2 + ... + a_nx_n^2$ where $a_i \in F^\times$. Let

$$D_F(\langle a_1, ..., a_n\rangle) = \{c \in F^\times \mid c = \sum_{i=1}^{n} a_i x_i^2, x_i \in F\}.$$

Then $D_F(\langle 1, a, b, ab\rangle)$ is a multiplicative subgroup of $F^\times$. (See Lemma 1.3.) Let $\mathbf{Q}$ be the field of rational numbers. The goal of this paper is to give a new and elementary proof of the following theorem of which the result above is a special case.

Main Theorem. *Let* $a, b \in \mathbf{Q}^\times$. *Then*

$$D_{\mathbf{Q}}(\langle 1, a, b, ab\rangle) = \begin{cases} \mathbf{Q}^\times_{>0} \text{ (positive rationals)} & \text{if } a, b > 0 \\ \mathbf{Q}^\times & \text{otherwise.} \end{cases}$$

There are essentially three ways to prove the Main Theorem at present. One way is to use the Hasse-Minkowski theorem ([La], p. 168). This is, however, a difficult theorem to prove. Proofs of the Hasse-Minkowski theorem rely on Dirichlet's theorem on primes in an arithmetic progression ([Se], [BS]), class field theory ([Om]), or Gauss' theory on the existence of certain types of binary quadratic forms ([Ca]). (Actually, Skolem showed in [Sk] that a weaker analytic result than Dirichlet's theorem suffices to give a proof of the Hasse-Minkowski theorem.) A second way to prove the Main Theorem is to use Meyer's theorem that an indefinite 5-dimensional quadratic form over $\mathbf{Q}$ is isotropic. This theorem was originally proved using

the classical integral theory of quadratic forms over the integers and also depends on Dirichlet's theorem or Gauss' theory mentioned above. A third way is to use the so called weak Hasse-Minkowski theorem. A proof of this can be found in [La], p. 174-178, but knowledge is required of Witt rings, local fields, exact sequences, and Springer's theory for quadratic forms over local fields.

Until now, no proof of the Main Theorem, much less an elementary one, has appeared exploiting the fact that $D_{\mathbf{Q}}(\langle 1, a, b, ab\rangle)$ is a multiplicative subgroup of $\mathbf{Q}^\times$. We present a truly elementary proof below using nothing more exotic than the notion of quadratic residues and the Möbius function.

We follow basic terminology and notation as found in [La]. In particular, a quadratic form $\langle a_1, ..., a_n\rangle$ is isotropic over F if there exist $x_1, ..., x_n \in F$, not all zero, such that $\sum_{i=1}^{n} a_i x_i^2 = 0$. We have the orthogonal sum $\langle a_1, ..., a_m\rangle \perp \langle b_1, ..., b_n\rangle = \langle a_1, ..., a_m, b_1, ..., b_n\rangle$ and $\langle\langle a, b\rangle\rangle$ stands for $\langle 1, a, b, ab\rangle$.

I wish to thank T.Y. Lam for the proof of Proposition 1.4 which is much simpler than my original proof.

§ 1. Reductions to prove the Main Theorem

1.1. Main Theorem. *Let* $a, b \in \mathbf{Q}^\times$. *Then*

$$D_{\mathbf{Q}}(\langle 1, a, b, ab\rangle) = \begin{cases} \mathbf{Q}^\times_{>0} & \text{if } a, b > 0 \\ \mathbf{Q}^\times & \text{otherwise.} \end{cases}$$

We begin by stating some basic results needed to prove Theorem 1.1.

1.2. Lemma. *Let* $q = \langle a_1, ..., a_n\rangle$, $a_i \in F^\times$.

(a) *If* q *is isotropic over* F, *then* $D_F(q) = F^\times$.

(b) *Let* $c \in F^\times$. *Then* $q \perp \langle c\rangle$ *is isotropic over* F *if and only if* $-c \in D_F(q)$.

Proof. (a) Let $c \in F^\times$ be given. An appropriate linear change of variable lets us assume $q(1, 0, ..., 0) = 0$. Then

$$q(x_1, ..., x_n) = x_1(\sum_{i=2}^{n} b_i x_i) + Q(x_2, ..., x_n)$$

where some $b_i \neq 0$. Choose $a_2, ..., a_n \in F$ such that $\sum_{i=2}^{n} b_i a_i \neq 0$ and let

$a_1 = \dfrac{c - Q(a_2, ..., a_n)}{b_2 a_2 + ... + b_n a_n}$. Then $q(a_1, a_2, ..., a_n) = c$.

(b) Suppose $q(a_1, ..., a_n) + ca_{n+1}^2 = 0$ where some $a_i \neq 0$. If $a_{n+1} \neq 0$, then $q\left(\dfrac{a_1}{a_{n+1}}, ..., \dfrac{a_n}{a_{n+1}}\right) = -c$. If $a_{n+1} = 0$, then q is isotropic and (a) implies $-c \in D_F(q)$. The converse is trivial.

1.3. LEMMA. *Let* $a, b \in F^\times$. *Then* $D_F(\langle\langle a, b\rangle\rangle)$ *is a subgroup of* $F^\times$.

Proof. Clearly $1 \in D_F(\langle\langle a, b\rangle\rangle)$ and the following formula shows $D_F(\langle\langle a, b\rangle\rangle)$ is closed under multiplication.

$$\begin{aligned}&(x_1^2 + ax_2^2 + bx_3^2 + abx_4^2)(y_1^2 + ay_2^2 + by_3^2 + aby_4^2)\\ &= (x_1y_1 - ax_2y_2 - bx_3y_3 - abx_4y_4)^2 + a(x_1y_2 + x_2y_1 + bx_3y_4 - bx_4y_3)^2\\ &\quad + b(x_1y_3 + x_3y_1 + ax_4y_2 - ax_2y_4)^2 + ab(x_1y_4 + x_4y_1 + x_2y_3 - x_3y_2)^2\end{aligned}$$

If $c \in D_F(\langle\langle a, b\rangle\rangle)$ then $\dfrac{1}{c} = c\left(\dfrac{1}{c}\right)^2 \in D_F(\langle\langle a, b\rangle\rangle)$.

1.4. PROPOSITION. *Let* $a, b, c \in F^\times$. *If* $\langle\langle a, b\rangle\rangle \perp \langle c\rangle$ *is isotropic over* F *then* $\langle\langle b, c\rangle\rangle \perp \langle a\rangle$ *is isotropic over* F.

Proof. We can assume $\langle\langle b, c\rangle\rangle$ and hence $\langle 1, b, c\rangle$ is not isotropic over F otherwise we are done. By Lemma 1.2 (b), there exists $x_i \in F$ such that $-c = x_1^2 + ax_2^2 + bx_3^2 + abx_4^2$. Then $x_1^2 + bx_3^2 + c = -a(x_2^2 + bx_4^2)$ and both sides are nonzero since $\langle 1, b, c\rangle$ is not isotropic over F. It follows $-a = \dfrac{x_1^2 + bx_3^2 + c}{x_2^2 + bx_4^2} \in D_F(\langle\langle b, c\rangle\rangle)$ since $D_F(\langle\langle b, c\rangle\rangle)$ is a subgroup of $F^\times$ by Lemma 1.3. Therefore $\langle\langle b, c\rangle\rangle \perp \langle a\rangle$ is isotropic over F by Lemma 1.2 (b).

We see from Lemma 1.2 (b) that the Main Theorem is equivalent to the following more convenient formulation.

1.1′. THEOREM. *Let* $a, b, c \in \mathbf{Q}^\times$. *If* a, b, c *are not all positive, then* $\langle\langle a, b\rangle\rangle \perp \langle c\rangle$ *is isotropic over* $\mathbf{Q}$.

We begin now setting up the proof of the Main Theorem. We can assume $a, b, c \in \mathbf{Z}$ since a, b, c can be replaced by $a\alpha^2, b\beta^2, c\gamma^2$ for any nonzero $\alpha, \beta, \gamma \in \mathbf{Z}$. Suppose the Main Theorem is false. Then there exist nonzero $a, b, c \in \mathbf{Z}$, not all positive, such that $\langle\langle a, b\rangle\rangle \perp \langle c\rangle$ is not isotropic over $\mathbf{Q}$. We can assume $|a| + |b| + |c|$ is minimal among all such counter-examples and we can assume $|a| \leqslant |b| \leqslant |c|$ by Proposition 1.4.

1.5. LEMMA. *Continue the assumptions from above. Then* $|b| < |c|$ *and* $|c|$ *is an odd prime number.*

Proof. If $|c| = 1$, then $|a| = |b| = 1$ and $\langle\langle a, b\rangle\rangle \perp \langle c\rangle$ is isotropic over $\mathbf{Q}$ since a, b, c are not all positive. Thus $|c| > 1$.

Suppose $|b| = |c|$. If $c = -b$ then $\langle\langle a, b\rangle\rangle \perp \langle c\rangle$ is isotropic over Q, a contradiction. If $b = c$ then $\langle\langle a, b\rangle\rangle \perp \langle b\rangle$ is not isotropic over $\mathbf{Q}$. Then Proposition 1.4 implies $\langle\langle b, b\rangle\rangle \perp \langle a\rangle \cong \langle\langle 1, b\rangle\rangle \perp \langle a\rangle$ is not isotropic over $\mathbf{Q}$. But $1 + |b| + |a| < |a| + |b| + |c|$ and a, b are not both positive (since $b = c$). This contradicts the minimality assumption and therefore $|b| < |c|$.

Suppose $|c|$ is not a prime number and let $-c = (-c_1)(-c_2)$ where $|c_1|, |c_2| < |c|$. If $c < 0$, we can assume in addition that $c_1, c_2 < 0$. Then $\langle\langle a, b\rangle\rangle \perp \langle c_i\rangle$, $i = 1, 2$, both have at least one of a, b, c_i negative. Since $|a| + |b| + |c_i| < |a| + |b| + |c|$, it follows $\langle\langle a, b\rangle\rangle \perp \langle c_i\rangle$ is isotropic over $\mathbf{Q}$, $i = 1, 2$. Then $-c_1, -c_2 \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$ by Lemma 1.2 (b) and $-c \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$ by Lemma 1.3. This implies $\langle\langle a, b\rangle\rangle \perp \langle c\rangle$ is isotropic over $\mathbf{Q}$ by Lemma 1.2 (b), a contradiction. Therefore $|c|$ is a prime number.

If $|c| = 2$, then $|a| = |b| = 1$. If $a = -1$ or $b = -1$ then $\langle\langle a, b\rangle\rangle \perp \langle c\rangle$ is isotropic over $\mathbf{Q}$. If $a = b = 1$, then $c = -2$ and $\langle\langle 1, 1\rangle\rangle \perp \langle -2\rangle$ is isotropic over $\mathbf{Q}$. These contradictions imply $|c| \neq 2$ and therefore $|c|$ is an odd prime.

To finish the proof of the Main Theorem we are reduced to proving Theorem 1.6:

1.6. THEOREM. *Suppose* p *is an odd prime,* $a, b \in \mathbf{Z}$, *and* $0 < |a|, |b| < p$. *Then there exists* $m \in \mathbf{Z}$, $0 < |m| < p$, *such that* $2mp \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$.

We shall assume Theorem 1.6 has been proved and finish the proof of the Main Theorem now. We apply Theorem 1.6 with $|c|$ in place of p. Then there exists $m \in \mathbf{Z}$, $0 < |m| < |c|$, such that $2m|c| \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$. Our minimality assumption implies $\langle\langle a, b\rangle\rangle \perp \langle -|m|\rangle$ and $\langle\langle a, b\rangle\rangle \perp \langle -2\rangle$ are both isotropic over $\mathbf{Q}$. Then $2, |m|$ and hence $2|m|$ all lie in $D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$. If $a, b > 0$ then $c < 0$ and it must be that $-c \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$. If either $a < 0$ or $b < 0$ then $-1 \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$ since $\langle\langle a, b\rangle\rangle \perp \langle 1\rangle$ is isotropic over $\mathbf{Q}$ by our minimality assumption. Therefore $-c \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$ in both cases and $\langle\langle a, b\rangle\rangle \perp \langle c\rangle$ is isotropic over $\mathbf{Q}$. This contradicts our assumption that a counterexample to the Main Theorem exists and finishes the proof of the Main Theorem.

Remark. A natural attempt to finish the proof of the Main Theorem would be a version of Theorem 1.6 where one finds $M \in \mathbf{Z}$, $0 < |M| < p$, such that $Mp \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$. But according to [Mo], p. 169, one can only guarantee $|M| \leqslant \sqrt{2|ab|} < \sqrt{2p^2} = \sqrt{2}\,p$. If one could also make M even, then this result in [Mo] would give a proof of Theorem 1.6.

It remains to prove Theorem 1.6. If p is an odd prime, let $\left(\frac{c}{p}\right)$ be the Legendre symbol: If $(c, p) = 1$, then $\left(\frac{c}{p}\right) = \pm -1$ where $c^{\frac{p-1}{2}} \equiv \left(\frac{c}{p}\right) \bmod p$. In the course of proving Theorem 1.6 we will use the following result.

1.7. THEOREM. *Let p be an odd prime, $p \neq 5$, and let a, b be integers such that $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$. Then there exist $x, y \in \mathbf{Z}$ such that $\left(\frac{ax^2 + by^2}{p}\right) = -1$ and $x^2 + y^2 < p$.*

We shall assume Theorem 1.7 has been proved and give now the

Proof of Theorem 1.6. If $\langle\langle a, b\rangle\rangle$ is isotropic over Q then we are done by Lemma 1.2(a). Now assume $\langle\langle a, b\rangle\rangle$ is not isotropic over Q. First assume at least one of $-a, -b, -ab$ is a quadratic residue mod p. Let $\alpha \in \{-a, -b, -ab\}$ where $\left(\frac{\alpha}{p}\right) = 1$. There exists β, $1 \leqslant \beta \leqslant p-1$, such that $p \mid \beta^2 - \alpha$ and $\beta^2 - \alpha$ is even (replace β by $p - \beta$ if necessary). Then $|\beta^2 - \alpha| \leqslant \beta^2 + |\alpha| < p^2 + p^2 = 2p^2$. Therefore, $\beta^2 - \alpha = 2mp$ where $0 < |m| < p$ and $2mp \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$.

If $p \equiv 1 \bmod 4$ then at least one of $-a, -b, -ab$ is a quadratic residue mod p since $\left(\frac{-1}{p}\right) = 1$ and $p \nmid ab$. Now suppose $p \equiv 3 \bmod 4$. Then at least one of $-a, -b, -ab$ is a quadratic residue mod p unless $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$. Suppose $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$ and choose x, y as in Theorem 1.7. Since $p \equiv 3 \bmod 4$, we have $-(ax^2+by^2)$ is a quadratic residue mod p and hence there exists β, $1 \leqslant \beta \leqslant p-1$, such that $p \mid \beta^2 + ax^2 + by^2$ and $\beta^2 + ax^2 + by^2$ is even. Then $|\beta^2 + ax^2 + by^2| \leqslant \beta^2 + |a|x^2 + |b|y^2 < p^2 + p(x^2+y^2) < 2p^2$. Therefore, $\beta^2 + ax^2 + by^2 = 2mp$ where $0 < |m| < p$ and $\beta^2 + ax^2 + by^2 \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$.

The proof of Theorem 1.7 is given in the next section. Although we need Theorem 1.7 only when $p \equiv 3 \bmod 4$ we give a complete proof since very little additional work is required.

§ 2. The proof of Theorem 1.7

In this section p denotes an odd prime number. We begin by recalling a result about sequences of quadratic residues and nonresidues mod p.

2.1. Lemma. *The number of pairs* $(n, n+1)$ *in the set* $\{1, 2, ..., p-1\}$ *such that* $\left(\frac{n}{p}\right) = 1, \left(\frac{n+1}{p}\right) = -1$ *is equal to* $\dfrac{p - \left(\frac{-1}{p}\right)}{4}$.

Proof. This elementary result is proved completely in [Ha], p. 157-158. (See also [An], Chapter 10.)

The next two lemmas give a way to count the number of lattice points $(x, y) \in \mathbf{Z} \times \mathbf{Z}$, $x, y > 0$, satisfying the conditions of Theorem 1.7.

Let

$$\mathscr{S}(x) = \{(\alpha, \beta) \in \mathbf{Z} \times \mathbf{Z} \mid \alpha, \beta > 0, \alpha^2 + \beta^2 < x^2\}$$

and let $\mathscr{P}(x) = \{(\alpha, \beta) \in \mathscr{S}(x) \mid (\alpha, \beta) = 1\}$. Let $S(x) = |\mathscr{S}(x)|$ and $P(x) = |\mathscr{P}(x)|$. (It will be clear from context whether we mean the point (α, β) or the greatest common divisor of α, β.)

2.2. Lemma. *Let* R *be the set of nonzero squares* mod p.

(a) *The function* $\theta : \mathscr{P}(\sqrt{p}) \to R$ *given by* $\theta(x, y) = \dfrac{y^2}{x^2} \bmod p$ *is an injection.*

(b) $P(\sqrt{p}) \leqslant \frac{1}{2}(p-1)$.

Proof. Clearly (a) implies (b) since $|R| = \frac{1}{2}(p-1)$. If (a) is false then there exist two distinct points $(x_1, y_1), (x_2, y_2)$ in $\mathscr{P}(\sqrt{p})$ such that $\dfrac{y_1^2}{x_1^2} \equiv \dfrac{y_2^2}{x_2^2} \bmod p$. Then $y_1^2 x_2^2 - x_1^2 y_2^2 = (y_1 x_2 + x_1 y_2)(y_1 x_2 - x_1 y_2) \equiv 0 \bmod p$. We have $y_1 x_2 + x_1 y_2 \neq 0$ since $x_i, y_i > 0$ and $y_1 x_2 - x_1 y_2 \neq 0$ otherwise $\dfrac{y_1}{x_1} = \dfrac{y_2}{x_2}$ and

then the points $(x_1, y_1), (x_2, y_2)$ would be equal since $(x_i, y_i) = 1$, $i = 1, 2$. We have

$$\begin{aligned}(x_1^2+y_1^2)(x_2^2+y_2^2) &= (x_1x_2+y_1y_2)^2 + (y_1x_2-x_1y_2)^2 \\ &= (x_1x_2-y_1y_2)^2 + (y_1x_2+x_1y_2)^2 .\end{aligned}$$

Either $(y_1x_2-x_1y_2)^2$ or $(y_1x_2+x_1y_2)^2$ is $\geqslant p^2$ since both are nonzero and one of them is divisible by p^2. Therefore $(x_1^2+y_1^2)(x_2^2+y_2^2) \geqslant p^2$ and then either $x_1^2 + y_1^2 \geqslant p$ or $x_2^2 + y_2^2 \geqslant p$. This is a contradiction since both (x_1, y_1) and (x_2, y_2) lie in $\mathscr{P}(\sqrt{p})$.

Remark. Although (b) in the preceeding lemma is not needed in what follows it was included since it gives a fairly good upper bound for $P(\sqrt{p})$ that is valid for all primes. It can be shown using Lemmas 2.4, 2.5 below (see also [HW], p. 268) that $\lim_{p\to\infty} \frac{P(\sqrt{p})}{p} = \frac{3}{2\pi} \approx .477$. It is unusual to obtain, with so little work, such a good estimate that is valid for all prime numbers.

2.3. LEMMA. *Assume* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = 1$. *Let* $\tau: R \to \{0, 1, -1\}$ *where* $\tau(z^2) = \left(\frac{a+bz^2}{p}\right)$. *Then* $\left|\tau^{-1}(-1)\right| = \dfrac{p - \left(\frac{-1}{p}\right)}{4}$.

Proof. Since $\left(\frac{a}{p}\right) = 1$, we have $\tau(z^2) = -1 \Leftrightarrow \left(\frac{1+\frac{b}{a}z^2}{p}\right) = -1$. Since $\left(\frac{b/a}{p}\right) = 1$, by Lemma 2.1 this happens if and only if $\frac{b}{a}z^2$ is one of the $\dfrac{p - \left(\frac{-1}{p}\right)}{4}$ elements β in R such that $\left(\frac{\beta}{p}\right) = 1, \left(\frac{\beta+1}{p}\right) = -1$. Therefore, there are exactly $\dfrac{p - \left(\frac{-1}{p}\right)}{4}$ elements z^2 in R such that $\tau(z^2) = -1$.

Since $\left(\frac{a + b\frac{y^2}{x^2}}{p}\right) = -1 \Leftrightarrow \left(\frac{ax^2+by^2}{p}\right) = -1$ when $p \nmid x$, it follows from Lemmas 2.2, 2.3 that proving Theorem 1.7 is equivalent to finding (x, y)

$\in \mathscr{P}(\sqrt{p})$ such that $\tau \circ \theta(x, y) = -1$. This is equivalent to showing $\theta(\mathscr{P}(\sqrt{p}))$ $\cap \tau^{-1}(-1)$ is nonempty. Since θ is injective, $|\tau^{-1}(-1)| = \dfrac{p - \left(\dfrac{-1}{p}\right)}{4}$, and $|R| = \dfrac{p-1}{2}$, it is sufficient to show $P(\sqrt{p}) + \dfrac{p - \left(\dfrac{-1}{p}\right)}{4} > \dfrac{p-1}{2}$. Thus to prove Theorem 1.7, we are reduced to showing

$$P(\sqrt{p}) > \frac{p-1}{2} - \frac{p - \left(\frac{-1}{p}\right)}{4} = \begin{cases} \dfrac{p-3}{4} & \text{if } p \equiv 3 \bmod 4 \\ \dfrac{p-1}{4} & \text{if } p \equiv 1 \bmod 4 . \end{cases}$$

As pointed out earlier, $\lim\limits_{p \to \infty} \dfrac{P(\sqrt{p})}{p} \approx .477$. Thus it is clear that for all but finitely many primes p we have $\dfrac{P(\sqrt{p})}{p} > \dfrac{1}{4}$, i.e., $P(\sqrt{p}) > \dfrac{p-1}{4}$. Since we need to check this result for all primes p, $p \neq 5$, it is necessary to give rather careful estimates. We now compute $P(x)$ and compare it to $\dfrac{x^2-1}{4}$.

Let μ be the Möbius function: If $n \in \mathbf{Z}$, $n = \prod\limits_{i=1}^{t} p_i^{e_i}$, then

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ (-1)^t & \text{if each } e_i = 1 \\ 0 & \text{if some } e_i > 1 . \end{cases}$$

Let [ ] denote the greatest integer function.

2.4. LEMMA. $P(x) = \sum\limits_{i=1}^{\infty} \mu(i)\, S\left(\dfrac{x}{i}\right) = \sum\limits_{i=1}^{\left[\frac{x}{\sqrt{2}}\right]} \mu(i)\, S\left(\dfrac{x}{i}\right)$.

Proof. Since $S(\sqrt{2}) = 0$, we have $S\left(\dfrac{x}{i}\right) = 0$ if $i \geqslant \left[\dfrac{x}{\sqrt{2}}\right] + 1$. In order to count how many times each lattice point is counted in the sum $\sum\limits_{i=1}^{\infty} \mu(i)\, S\left(\dfrac{x}{i}\right)$ we partition the lattice points in $\mathscr{S}(x)$ into the rays passing through the origin. Let $(\alpha, \beta) \in \mathscr{P}(x)$ and consider all multiples $(m\alpha, m\beta)$

that lie in $\mathscr{S}(x)$. Let n be the unique positive integer such that $(n\alpha, n\beta) \in \mathscr{S}(x)$ but $((n+1)\alpha, (n+1)\beta) \notin \mathscr{S}(x)$. Then for a given positive integer i, we have $(j\alpha, j\beta) \in \mathscr{S}\left(\frac{x}{i}\right)$ precisely for $\left[\frac{n}{i}\right]$ values of j since if $\left(\left[\frac{n}{i}\right]+1\right)(\alpha, \beta) \in \mathscr{S}\left(\frac{x}{i}\right)$ then $i\left(\left[\frac{n}{i}\right]+1\right)(\alpha, \beta) \in \mathscr{S}(x)$. But $i\left(\left[\frac{n}{i}\right]+1\right) \geqslant n+1$. Therefore exactly $\left[\frac{n}{i}\right]$ points on the ray through (α, β) lie in $\mathscr{S}\left(\frac{x}{i}\right)$. It follows that in the sum to be evaluated, the points on the ray through (α, β) contribute $\sum_{i=1}^{\infty} \mu(i)\left[\frac{n}{i}\right] = 1$. To prove this last equality we start with the well known fact $\sum_{i|m} \mu(i) = \begin{cases} 1 & \text{if } m = 1 \\ 0 & \text{if } m > 1. \end{cases}$ Then $1 = \sum_{m=1}^{n} \sum_{i|m} \mu(i) = \sum_{i=1}^{n} \mu(i)\left[\frac{n}{i}\right]$ since $\left[\frac{n}{i}\right]$ is the number of multiples of i that are $\leqslant n$. Therefore the sum to be evaluated counts the number of points in $\mathscr{P}(x)$ and this completes the proof.

2.5. LEMMA. *For all* $x \geqslant 1, \frac{\pi}{4}x^2 - 2x + 1 < S(x) < \frac{\pi}{4}x^2$.

Proof. To each point $(\alpha, \beta) \in \mathscr{S}(x)$ associate the lattice square for which (α, β) is the lower left corner. Let M_1 denote the region covered by these squares. Then $S(x) =$ area of M_1. Let M_2, M_3 be the two strips of length x, width 1, parallel to the axes where $M_2 = \{(x_1, y_1) \mid 0 \leqslant x_1 \leqslant x, 0 \leqslant y_1 \leqslant 1\}$, and $M_3 = \{(x_1, y_1) \mid 0 \leqslant x_1 \leqslant 1, 0 \leqslant y_1 \leqslant x\}$. When $x \geqslant 1$, these strips cover a combined area of $2x - 1$. Since the quarter circle of radius x is contained in $M_1 \cup M_2 \cup M_3$, it follows $\frac{\pi}{4}x^2 < S(x) + 2x - 1$.

Now to each point (α, β) in $\mathscr{S}(x)$ associate the lattice square for which (α, β) is the upper right corner. These lattice squares lie entirely in the first quadrant and inside the circle of radius x. Therefore $S(x) < \frac{\pi}{4}x^2$.

2.6. LEMMA. *Let* $m > n \geqslant 1, m, n \in \mathbf{Z}$. *Then*

$$\frac{1}{(n+1)^2} + \frac{1}{(n+2)^2} + \ldots + \frac{1}{m^2} < \frac{1}{n} - \frac{1}{m}.$$

Proof. Apply the integral test to $\int_n^m \frac{1}{t^2}\,dt$ or observe

$$\sum_{i=n}^{m-1} \frac{1}{(i+1)^2} < \sum_{i=n}^{m-1} \left(\frac{1}{i} - \frac{1}{i+1}\right) = \frac{1}{n} - \frac{1}{m}.$$

We now use Lemmas 2.4, 2.5 to estimate $P(x)$. We need to determine values of x for which $P(x) > \dfrac{x^2-1}{4}$. First assume $x > 10$. Then $\dfrac{x}{\sqrt{2}} > 7$ so $\left[\dfrac{x}{\sqrt{2}}\right] \geqslant 7$.

$$P(x) = \sum_{i=1}^{\infty} \mu(i)\, S\left(\frac{x}{i}\right) = \sum_{i=1}^{\left[\frac{x}{\sqrt{2}}\right]} \mu(i)\, S\left(\frac{x}{i}\right)$$

$$\geqslant S(x) - S\left(\frac{x}{2}\right) - S\left(\frac{x}{3}\right) - S\left(\frac{x}{5}\right) + S\left(\frac{x}{6}\right) - \sum_{i=7}^{\left[\frac{x}{\sqrt{2}}\right]} S\left(\frac{x}{i}\right)$$

$$> \left(\frac{\pi}{4}x^2 - 2x + 1\right) - \frac{\pi}{4}\left(\frac{x}{2}\right)^2 - \frac{\pi}{4}\left(\frac{x}{3}\right)^2 - \frac{\pi}{4}\left(\frac{x}{5}\right)^2$$

$$+ \left(\frac{\pi}{4}\left(\frac{x}{6}\right)^2 - 2\left(\frac{x}{6}\right) + 1\right) - \frac{\pi}{4}x^2\left(\frac{1}{7^2} + \ldots + \frac{1}{\left[\frac{x}{\sqrt{2}}\right]^2}\right)$$

$$> \frac{\pi}{4}x^2\left(1 - \frac{1}{4} - \frac{1}{9} - \frac{1}{25} + \frac{1}{36} - \frac{1}{6} + \frac{1}{\left[\frac{x}{\sqrt{2}}\right]}\right) - 2x\left(1 + \frac{1}{6}\right) + 2 \text{ (by Lemma 2.6)}$$

$$= \frac{\pi}{4}x^2\left(\frac{46}{100}\right) + \frac{\pi}{4}x^2\left(\frac{1}{\left[\frac{x}{\sqrt{2}}\right]}\right) - \frac{7}{3}x + 2$$

$$\geqslant \frac{23\pi}{200}x^2 + \left(\frac{\sqrt{2}\pi}{4} - \frac{7}{3}\right)x + 2, \text{ since } \frac{x^2}{\left[\frac{x}{\sqrt{2}}\right]} \geqslant \sqrt{2}x\,.$$

Let $f(x) = \dfrac{23\pi}{200}x^2 + \left(\dfrac{\sqrt{2}\pi}{4} - \dfrac{7}{3}\right)x + 2$, $g(x) = \dfrac{x^2-1}{4}$. One can check that $f(10) > g(10)$, $f'(10) > g'(10)$, $f''(10) > g''(10)$. Therefore $P(x) > f(x) > g(x)$ for all $x > 10$. This implies $P(\sqrt{p}) > \dfrac{p-1}{4}$ if $\sqrt{p} > 10$, i.e., $p > 100$. It remains to show $P(\sqrt{p}) > \dfrac{p-1}{4}$ if $p < 100$, $p \neq 5$.

At this point we simply count lattice points directly and construct the table below. The table shows $P(\sqrt{p}) > \frac{p-1}{4}$ for all primes $p < 100$ except $p = 5$. This completes the proof of Theorem 1.7 and hence the Main Theorem has been proved completely.

p	$P(\sqrt{p})$	Range of primes where $P(\sqrt{p}) > \frac{p-1}{4}$
59	27	$59 \leqslant p \leqslant 97$
31	15	$31 \leqslant p \leqslant 53$
19	9	$19 \leqslant p \leqslant 29$
11	5	$11 \leqslant p \leqslant 17$
7	3	$p = 7$
3	1	$p = 3$
5	1	$1 \not> \frac{5-1}{4}$

§ 3. Consequences of the Main Theorem

In this section we derive some consequences of the Main Theorem that have applications to the algebraic theory of quadratic forms. The results in this section are well known ([La], Chapter 6). The point is that we have new and more elementary proofs.

Let $\langle\langle a, b, c\rangle\rangle$ denote the 3-fold Pfister form

$$\langle 1, a\rangle \otimes \langle 1, b\rangle \otimes \langle 1, c\rangle = \langle 1, a, b, c, ab, ac, bc, abc\rangle .$$

3.1. Proposition. *Let* $a, b, c \in \mathbf{Q}^{\times}$. *Then* $\langle\langle a, b, c\rangle\rangle$ *is hyperbolic over* $\mathbf{Q}$ *if and only if* a, b, c *are not all positive.*

Proof. If $\langle\langle a, b, c\rangle\rangle$ is hyperbolic, then consideration of $\langle\langle a, b, c\rangle\rangle$ over the field of real numbers shows at least one of a, b, c is negative.

Now suppose $a < 0$. Then the Main Theorem implies $-c \in D_{\mathbf{Q}}(\langle\langle a, b\rangle\rangle)$ and $\langle\langle a, b\rangle\rangle \perp \langle c\rangle$ is isotropic over $\mathbf{Q}$ by Lemma 1.2(b). A theorem of Pfister ([La], p. 279] implies $\langle\langle a, b, c\rangle\rangle$ is hyperbolic over $\mathbf{Q}$.

3.2. PROPOSITION. *Let* $a, b, c \in \mathbf{Q}^\times$, $a, b, c > 0$. *Then*

$$\langle\langle a, b, c\rangle\rangle \cong \langle\langle 1, 1, 1\rangle\rangle = 8\langle 1\rangle .$$

Proof. Calculating in the Witt ring WF we have

$$\langle\langle a, b, 1\rangle\rangle \perp (-1)\langle\langle a, b, c\rangle\rangle = \langle\langle a, b\rangle\rangle(\langle 1, 1\rangle \perp (-1)\langle 1, c\rangle)$$
$$= \langle\langle a, b\rangle\rangle\langle 1, -c\rangle = \langle\langle a, b, -c\rangle\rangle = 0 \text{ by Proposition 3.1.}$$

Therefore $\langle\langle a, b, 1\rangle\rangle \cong \langle\langle a, b, c\rangle\rangle$. Repeating the same calculation with a, b in place of c yields the result.

3.3. COROLLARY. *Let* $a, b, c \in \mathbf{Q}^\times$ *and let* $\mathbf{H} = \langle 1, -1\rangle$. *Then*

$$\langle\langle a, b, c\rangle\rangle \cong \begin{cases} \langle\langle 1, 1, 1\rangle\rangle & \text{if } a, b, c > 0 \\ 4\mathbf{H} & \text{otherwise .} \end{cases}$$

3.4. THEOREM. $I^3\mathbf{Q}$ *is torsion-free.*

Proof. Corollary 3.3 shows that the only nonzero 3-fold Pfister form in $I^3\mathbf{Q}$ is $\langle\langle 1, 1, 1\rangle\rangle$. Therefore $I^3\mathbf{Q} \cong \mathbf{Z}$ and $I^3\mathbf{Q}$ is torsion-free.

REFERENCES

[An] ANDREWS, G. *Number Theory*. W.S. Saunders, Philadelphia, 1971.

[BS] BOREVICH, Z. I. and I. R. SHAFAREVICH. *Number Theory*. Academic Press, New York, 1966.

[Ca] CASSELS, J. W. S. *Rational Quadratic Forms*. Academic Press, New York, 1978.

[Ha] HASSE, H. *Vorlesungen Über Zahlentheorie*. Springer-Verlag, Berlin, 1964.

[HW] HARDY, G. H. and E. M. WRIGHT. *An Introduction to the Theory of Numbers*. Oxford University Press, 4th ed., 1960.

[La] LAM, T. Y. *The Algebraic Theory of Quadratic Forms*. Benjamin, 1973.

[Mo] MORDELL, L. J. *Diophantine Equations*. Academic Press, New York, 1969.

[Om] O'MEARA, O. T. *Introduction to Quadratic Forms*. Springer-Verlag, Berlin, 1963.

[Se] SERRE, J.-P. *A Course in Arithmetic*. Springer-Verlag, 1973.

[Sk] SKOLEM, Th. On the Diophantine Equation $ax^2 + by^2 + cz^2 + dv^2 = 0$. *Norske Videnskabers Selsk. Forh. 21* (1948), 76-79.

(Reçu le 10 avril 1989)

David B. Leep

Department of Mathematics
University of Kentucky
Lexington, KY 40506
(USA)