Contemporary Mathematics

# A New Look at Sums of Squares

Larry J. Gerstein

Let $R$ be an integral domain. Among the most basic problems in the theory of quadratic forms over $R$ is the determination of which nonzero elements in $R$ can be expressed as a sum of $n$ squares in $R$, where $n$ is a positive integer. When $R = \mathbb{Z}$, the classics of this genre are the two-square, four-square, and three-square theorems of Fermat, Lagrange, and Gauss, respectively (listed here in chronological order). Of more recent vintage (1964) is this theorem of Cassels: If $k$ is a field of characteristic not 2, then a polynomial in $k[x]$ is a sum of $n$ squares of polynomials if and only if it is a sum of $n$ squares of rational functions in $k(x)$. (In slightly more general form this result is known as the Cassels–Pfister theorem, a cornerstone of the algebraic theory of quadratic forms.) My first goal in this paper is to present a unified approach to all these results. Having done this, I will begin the process of extending this approach to a wider class of problems on representations by quadratic forms. At the end of the paper I will raise some questions that arise naturally along the way.

For a ring $R$, the symbol $\square_n$ will denote the set of nonzero elements in $R$ that can be written as a sum of $n$ squares of elements of $R$.

From now on we will assume $R$ is a principal ideal domain whose quotient field $F$ has characteristic not 2. (In fact our main rings of interest will be $\mathbb{Z}$ and $k[x]$.) We now sketch a bit of background; for more details see [G2] or [O]. Let $V$ be a regular quadratic $F$-space with $B : V \times V \to F$ its symmetric bilinear form, and let $Q : V \to F$ defined by $Q(v) = B(v, v)$ be its associated quadratic form. An **$R$-lattice** $L$ in $V$ is a free $R$-module of finite rank; and $L$ is said to be **on** $V$ if it spans $V$. Given a basis $\mathbb{B} = \{v_1, \ldots, v_n\}$ for $L$, the matrix $A = (B(v_i, v_j))$ is the **Gram matrix** of $L$ with respect to $\mathbb{B}$. An expression of the form $X \cong Y$ will have one of several meanings, depending on the context: if $X$ and $Y$ are both spaces or both lattices, it means $X$ and $Y$ are isometric; if $X$ is a space or lattice and $Y$ is a matrix, it means $Y$ is the Gram matrix of $X$ with respect to a suitable basis; if $X$ and $Y$ are both matrices, it means $X$ and $Y$ are congruent over the relevant ring—that is, $X = {}^tTYT$ for some invertible matrix $T$. The determinant $\det A$ is the **discriminant** of $L$, denoted $dL$; it is well-defined up to squares in $R^*$. The fractional $R$-ideal $vL := (dL)$ is the **volume** of $L$. Two other important fractional ideals associated with $L$ are the **scale** $sL$ and the **norm** $nL$, which are generated respectively by

$$\{B(x, y) \mid x, y \in L\} \quad \text{and} \quad \{Q(x) \mid x \in L\}.$$

We will say $L$ is **integral** if $sL \subseteq R$. The inclusions $2sL \subseteq nL \subseteq sL$ hold, and hence $nL = sL$ if $2 \in R^*$. Also, from the definition of the determinant it follows that $vL \subseteq (sL)^n$; moreover, if $I$ is a fractional ideal and $Q(L) \subseteq I$, then $vL \subseteq (\frac{1}{2}I)^n$. Lattice volumes increase in accord with inclusions; that is, $L \subset L' \Rightarrow vL \subset vL'$. If $I = (\alpha)$, a lattice $L$ is **$I$-modular** if $L \cong \alpha U$, with $U$ a unimodular $R$-matrix; and $L$ is said to be **unimodular** if it is $R$-modular. A lattice $M$ is **$I$-maximal** if $Q(M) \subseteq I$ and $M$ is maximal (among the lattices on the space spanned by $M$) with respect to this property. From the several inclusions stated in this paragraph, it follows that every lattice $L$ in a space $V$ satisfying $Q(L) \subseteq I$ is contained in an $I$-maximal lattice on $V$.

Each nontrivial prime spot (equivalence class of valuations) $\mathfrak{p}$ on $F$ yields a completion $F_\mathfrak{p}$, and then $V$ extends (via tensor product) to a quadratic $F_\mathfrak{p}$-space $V_\mathfrak{p} \supset V$; again $\mathbb{B}$ is a basis. If $\mathfrak{p}$ is determined by a nonzero prime ideal of $R$, then $R_\mathfrak{p}$ denotes the closure of $R$ in $F_\mathfrak{p}$, and then $L_\mathfrak{p}$ is the $R_\mathfrak{p}$-lattice $R_\mathfrak{p}L$ in $V_\mathfrak{p}$. Similarly, if $I$ is a fractional $R$-ideal, we write $I_\mathfrak{p}$ for the fractional $R_\mathfrak{p}$-ideal $R_\mathfrak{p}I$ in $F_\mathfrak{p}$. It can be shown—with the help of the invariant factor theorem—that an $R$-lattice $L$ on $V$ is $I$-maximal if and only if for all $\mathfrak{p}$ the lattice $L_\mathfrak{p}$ is $I_\mathfrak{p}$-maximal on $V_\mathfrak{p}$.

We will say that $R$-lattices $L$ and $L'$ on $V$ are in the same **genus** if there is an isometry $L_\mathfrak{p} \cong L'_\mathfrak{p}$ for all nonzero prime ideals $\mathfrak{p}$ of $R$. It was shown by Eichler in 1952 that for a given fractional $R$-ideal $I$, all $I$-maximal $R$-lattices on a given quadratic $F$-space $V$ are in the same genus. In particular, if one $R$-maximal $R$-lattice on $V$ is unimodular, then they all are.

From now on, if $\mathfrak{p}$ is the $p$-adic spot for some prime $p$ of $R$, we will usually subscript with $p$ instead of $\mathfrak{p}$.

Now we turn our attention to $\mathbb{Z}$-lattices and $k[x]$-lattices. It has long been known that every positive definite unimodular $\mathbb{Z}$-lattice of rank $n \leq 7$ has an orthonormal basis. When $n \leq 5$ this result was a consequence of Hermite's inequality (from 1850) bounding the **minimum** of a lattice: the smallest absolute value of a nonzero element represented by the lattice. We state the inequality here, first for $\mathbb{Z}$-lattices, as Hermite did it; and then we state its adaption to $k[x]$-lattices, when the "minimum" means the smallest degree of a nonzero element represented by the lattice. (So over $k[x]$ "size" is measured by degree instead of absolute value.) The proofs in the two settings are similar, the main difference being the nonarchimedian behavior of the degree function. See [G2, §7.2] for the details.

Hermite's Inequalities. (i) *Let $V$ be an anisotropic $\mathbb{Q}$-space of dimension $n$, and let $L$ be an integral $\mathbb{Z}$-lattice on $V$. Then*

$$\min L \leq \left(\frac{4}{3}\right)^{\frac{n-1}{2}} |dL|^{\frac{1}{n}}.$$

(ii) *Let $L$ be an integral $k[x]$-lattice on an anisotropic quadratic $k(x)$-space $V$ of dimension $n$. Then*

$$\min L \leq \frac{1}{n}\partial(dL).$$

We now have two corollaries for $k[x]$-lattices. The proof of the first one is immediate in the anisotropic case; the isotropic case needs a short additional argument, which we omit.

COROLLARY 1 (Harder's Theorem). *Let $L$ be a unimodular $k[x]$-lattice of rank $n$. Then there exist $\alpha_1, \dots, \alpha_n \in k^*$ such that $L \cong \langle \alpha_1, \dots, \alpha_n \rangle$.*

(Here we have used the bracket notation $\langle \dots\dots\dots \rangle$ for a diagonal matrix.)

COROLLARY 2 (Cassels–Pfister Theorem). *Let $f \in k[x]$ and suppose $\alpha_1, \dots, \alpha_n \in k$. If $f = \sum_i \alpha_i r_i^2$ for some $r_i \in k(x)$, then $f = \sum_i \alpha_i p_i^2$ for some $p_i \in k[x]$. In particular,*

$$f \in \square_n \text{ over } k[x] \iff f \in \square_n \text{ over } k(x).$$

PROOF. Only "$\Longleftarrow$" requires proof. Let $V \cong \langle \alpha_1, \dots, \alpha_n \rangle$ with respect to some basis $\{v_1, \dots, v_n\}$. We're given $f \in k[x]$ and the assumption that $Q(v) = f$ for some $v \in V$. Then $v$ is contained in a $k[x]$-maximal lattice $M$ on $V$. The $k[x]$-lattice

$$L = k[x]v_1 \perp \cdots \perp k[x]v_n$$

is unimodular, and it is also $k[x]$-maximal. (Here we use the fact that $2 \in k[x]^*$.) By Eichler's Theorem $L_p \cong M_p$ for all primes $p$. Therefore $M$ is unimodular, and so $L \cong \langle \alpha_1, \dots, \alpha_n \rangle$ by Harder's Theorem. □

Now let's turn to the theory over $\mathbb{Z}$. Here, since 2 is not a unit, more is required than for the proof of Cassels–Pfister, because in general a unimodular $\mathbb{Z}$-lattice need not be $\mathbb{Z}$-maximal. But the main idea of the present proof is is to show that the particular unimodular lattices under scrutiny in the theorem are in fact $\mathbb{Z}$-maximal.

THEOREM. *Let $1 \le n \le 4$, and let $m \in \mathbb{N}$. Then*

$$m \in \square_n \text{ over } \mathbb{Z} \iff m \in \square_n \text{ over } \mathbb{Q}$$

PROOF SKETCH OF "$\Longleftarrow$". The case $n = 1$ is trivial, so we will assume that $2 \le n \le 4$. Let $L \cong \langle 1, \dots 1 \rangle$ on a $\mathbb{Q}$-space $V$, and suppose $v \in V$ satisfies $Q(v) = m$. Then $v$ is contained in a $\mathbb{Z}$-maximal lattice $M$. If we can show that $L$ is also $\mathbb{Z}$-maximal, then by Eichler we would know that $M_p \cong L_p$ for all $p$, and hence that $M$ is unimodular. Therefore we would know by Hermite's inequality that $M \cong \langle 1, \dots 1 \rangle$, from which the result would follow. Thus it is enough to prove that the lattice $L \cong \langle 1, \dots, 1 \rangle$ is $\mathbb{Z}$-maximal; equivalently, that for all primes $p$ the $\mathbb{Z}_p$-lattice $L_p = \mathbb{Z}_p L$ is $\mathbb{Z}_p$-maximal. (Here $\mathbb{Z}_p$ denotes the ring of 2-adic integers.)

This is clear for all $p \neq 2$, since then $nL_p = sL_p = vL_p = \mathbb{Z}_p$, and a lattice $J$ on $V_p$ containing $L_p$ would necessarily have $nJ \supset \mathbb{Z}_p$. (Here we have used the several inclusions of scale, norm, and volume listed earlier in the paper.) Therefore it suffices to show that the lattice $L_2 = \mathbb{Z}_2 L$ is $\mathbb{Z}_2$-maximal in $V_2$.

In each dimension the arguments involve discriminants and Hasse symbols. We illustrate with the case $n = 3$. Lattices over $\mathbb{Z}_2$ with biggest possible volume and norm $\subseteq \mathbb{Z}_2$ on a $\mathbb{Q}_2$-space of discriminant 1 would have the form

$$\begin{pmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{pmatrix} \perp \langle -1 \rangle \text{ or } \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix} \perp \langle 3 \rangle$$

But in both of these cases the underlying $\mathbb{Q}_2$-space would have Hasse symbol $-1$, hence no such lattice is on $\mathbb{Q}_2 L_2$. Therefore $L_2$ is $\mathbb{Z}_2$-maximal.

Now we get the classical theorems over $\mathbb{Z}$ as immediate corollaries.

COROLLARY 1 (Lagrange's Four-Square Theorem). *In $\mathbb{Z}$,*

$$\square_4 = \mathbb{N}.$$

PROOF. Apply the preceding theorem and the Hasse–Minkowski theorem. □

COROLLARY 2 (Fermat's Two-Square Theorem). *If $m \in \mathbb{N}$, then in $\mathbb{Z}$*

$$m \in \square_2 \Longleftrightarrow ord_p\, m \equiv 0 \pmod 2 \text{ for all } p \equiv 3 \pmod 4.$$

PROOF. From the theorem, we can (and will) assume $m$ is square-free. We must determine which $m$ satisfy $m \longrightarrow \langle 1,1\rangle$ over $\mathbb{Q}$; equivalently, $m \longrightarrow \langle 1,1\rangle$ over $\mathbb{Q}_p$ for all primes $p$. Such a representation is clear if $p$ is an odd prime not dividing $m$ or if $p \equiv 1 \pmod 4$, since in these cases there is an isometry $\langle 1,1\rangle \cong \langle m,m\rangle$ over $\mathbb{Q}_p$. (Recall: If $p \equiv 1 \pmod 4$ then $-1 \in \mathbb{Q}_p^{*2}$.) If $p \equiv 3 \pmod 4$ and $p \mid m$ (giving $\operatorname{ord}_p m = 1$), a representation $m \longrightarrow \langle 1,1\rangle$ over $\mathbb{Q}_p$ would force an isometry $\langle 1,1,-m\rangle \cong \langle 1,-1,-m\rangle$; but a Hasse symbol calculation shows this to be impossible. So no such prime exists. Therefore, either $m \equiv 1 \pmod 4$ or $m = 2k$ with $k \equiv 1 \pmod 4$. In both these cases a Hasse symbol calculation shows that $\langle 1,1\rangle \cong \langle m,m\rangle$ over $\mathbb{Q}_2$. □

COROLLARY 3 (Gauss's Three-Square Theorem). *Let $m \in \mathbb{N}$. Then*

$$m \in \square_3 \Longleftrightarrow m \neq 4^\nu k \text{ with } k \equiv 7 \pmod 8.$$

PROOF SKETCH. First note that $\langle 1,1,1\rangle$ is universal over $\mathbb{Q}_p$ for all $p \neq 2$. And $m \longrightarrow \langle 1,1,1\rangle$ over $\mathbb{Q}_2$ if and only if $\langle 1,1,1,-m\rangle$ is isotropic; equivalently (since $\langle 1,1,1,1\rangle$ is the unique 4-dimensional anisotropic $\mathbb{Q}_2$-space), $-m \notin \mathbb{Q}_2^2$. Finally, this is equivalent to $m \neq 4^\nu(7+8a)$. □

What about nonunimodular representations? Our results on sums of squares have centered on showing that a given lattice $L$ of interest represents all the elements of its coefficient ring $R$ represented by the ambient quadratic space. We did this by showing that $L$ was $R$-maximal and belonged to a genus containing only one isometry class. Since in each case $L$ was unimodular, the $R_\mathfrak{p}$-lattice $L_\mathfrak{p}$ was automatically $R_\mathfrak{p}$-maximal whenever $2 \in R_\mathfrak{p}^*$, so there was extra work proving $R$-maximality only when $R = \mathbb{Z}$ and $\mathfrak{p} = (2)$. From the local theory it is easy to show that if the discriminant $dL$ is square-free then $L_\mathfrak{p}$ is $R_\mathfrak{p}$-maximal whenever $\mathfrak{p}$ is nondyadic. For example, if $dL$ is square-free and $R = k[x]$ then $L$ is $R$-maximal.

In the material that follows, we will have several occasions to compute the Hasse symbol of a quadratic space over a local field. In this computation we follow [S] in computing the Hasse invariant of the space $\langle \alpha_1, \dots, \alpha_n\rangle$ as the product $\prod_{i<j} (\alpha_i, \alpha_j)_p$. Here $(\cdot,\cdot)_p$ is the associated Hilbert symbol with respect to the prime $p$, and it can be calculated by formulas in [S, p. 20] or [G2, pp. 82-83] over $\mathbb{Q}_p$; and, since all nontrivial spots on $\mathbb{F}_q(x)$ are nondyadic, over completions of $\mathbb{F}_q(x)$ Hilbert symbols can be computed essentially as over $\mathbb{Q}_p$ when $p$ is odd.

We begin our consideration of nonunimodular representations by considering some results on lattices over $\mathbb{F}_q[x]$.

PROPOSITION. *Let $L$ be an integral $\mathbb{F}_q[x]$-lattice on a regular quadratic $\mathbb{F}_q(x)$-space, and suppose the discriminant $dL$ has degree $\leq 1$. Then $L$ is $\mathbb{F}_q[x]$-maximal and has class number 1.*

PROOF. Write $R = \mathbb{F}_q[x]$, $F = \mathbb{F}_q(x)$, and "$\partial$" for degree. If $\partial(dL) = 0$ then $L$ is unimodular, and the result follows immediately from Harder's theorem and the classification of $\mathbb{F}_q$-spaces. If $\partial(dL) = 1$, say $dL = \alpha(x+\beta)$, with $\alpha, \beta \in \mathbb{F}_q$,

then $L$ is $R$-maximal, from our earlier discussion. Write $p_0 = x + \beta$. By Hermite's inequality (ii) there is a splitting

$$L \cong \langle 1, \dots, 1, \lambda \rangle \perp \langle \mu p_0 \rangle$$

with $\lambda, \mu \in \mathbb{F}_q^*$. If $J \in \operatorname{gen} L$ then $dJ = dL$, so there is also a splitting

$$J \cong \langle 1, \dots, 1, \lambda' \rangle \perp \langle \mu' p_0 \rangle$$

with $\lambda', \mu' \in \mathbb{F}_q^*$. Now $L$ and $J$ are on the same quadratic $F$-space, so there is a Hilbert symbol equality $(\lambda, \mu p_0)_p = (\lambda', \mu' p_0)_p$ for all primes $p$. In particular, when $p = p_0$ it follows from this that $\lambda$ and $\lambda'$ are in the same square class in $\mathbb{F}_q$. Hence, since $dL = dJ$, the same is true of $\mu$ and $\mu'$. □

Remark. The case $\partial(dL) = 0$ in the preceding proposition is just a restatement of the Cassels–Pfister theorem when $k = \mathbb{F}_q$.

When $\partial(dL) \geq 2$, the determination of class numbers is a more cumbersome process, even when $dL$ is irreducible, as the following two-part example shows.

Example. In this example we will usually write $R$ for $\mathbb{F}_3[x]$ and $F$ for $\mathbb{F}_3(x)$.
(i) Suppose $L \cong \begin{pmatrix} x+1 & 1 \\ 1 & x+2 \end{pmatrix}$ in the basis $\{v_1, v_2\}$ over $R$. We claim that $L$ is maximal and has class number 1. Because $dL = x^2 + 1 = p_0$, a prime in $R$, we know from our previous discussion that $L$ is $R$-maximal. An orthogonally split lattice in $\operatorname{gen} L$ would have form $J_1 = \langle 1, x^2 + 1 \rangle$ or $J_2 = \langle 2, 2(x^2 + 1) \rangle$. For both of these possibilities, when localized at $p_0$ the Hasse symbol of the ambient $F_{p_0}$-space would be $+1$, because $2 \in F_{p_0}^{*2}$; while meanwhile the space $FL \cong \langle x + 1, (x + 1)(x^2 + 1) \rangle$ has Hasse symbol $-1$ at $p_0$, because $x + 1 \notin F_{p_0}^{*2}$. Therefore $\operatorname{gen} L$ contains no split lattices, so (by binary reduction) any $J \in \operatorname{gen} L$ must have a Gram matrix of the form $A = \begin{pmatrix} ax+b & c \\ c & ex+f \end{pmatrix}$ for some $a, b, c, e, f \in \mathbb{F}_3$ with $ace \neq 0$. Because $dJ = dL = x^2 + 1$, elementary arithmetic tells us that for $J$'s Gram matrix we need to consider only the matrices

$$A_1 = \begin{pmatrix} x+1 & 1 \\ 1 & x+2 \end{pmatrix}, \quad A_2 = \begin{pmatrix} x+1 & 2 \\ 2 & x+2 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 2x+1 & 1 \\ 1 & 2x+2 \end{pmatrix},$$

$$A_4 = \begin{pmatrix} 2x+1 & 2 \\ 2 & 2x+2 \end{pmatrix}.$$

But if $J \cong A_1$ in $\{v_1, v_2\}$, then $J \cong A_2$ in $\{v_1, 2v_2\}$, and similarly $A_3 \cong A_4$. And if $J \cong A_3$ in $\{w_1, w_2\}$ then $J \cong A_1$ in $\{w_1' = 2w_1 + w_2, w_2' = w_1 + w_2\}$. Therefore in all cases $J \cong A_1 \cong L$, so $L$ has class number 1, as claimed.
(ii) One might suspect, based on the proposition and part (i) of this example, that an integral $R$-lattice with prime discriminant must have class number 1 (as well as being $R$-maximal). But the lattices

$$J_1 = \langle 1, x^2 + 1 \rangle \quad \text{and} \quad J_2 = \langle 2, 2(x^2 + 1) \rangle$$

mentioned in part (i) are $R$-maximal and in the same genus, yet $J_1 \ncong J_2$ by Corollary 2 in [G1]. (In brief: $J_1$ does not represent 2.) In fact the class of the lattice $L$ discussed in part (i) is the only other class of binary integral definite (i.e., anisotropic at $\infty$) $R$-lattices of discriminant $x^2 + 1$, and it is on a different space from $FJ_1$ and $FJ_2$. Therefore $J_1$ and $J_2$ belong to a genus of class number 2.

For nonunimodular representations over $\mathbb{Z}$, we give new proofs of two results of Fermat cited on the first page of Cox's book [C].

THEOREM (Fermat). *Let $l$ be an odd prime number. Then in $\mathbb{Z}$*
(I) *$l = x^2 + 2y^2$ is solvable if and only if $l \equiv 1$ or $3 \pmod 8$.*
(II) *$l = x^2 + 3y^2$ is solvable if and only if $l = 3$ or $l \equiv 1 \pmod 3$.*

PROOF. (I) Consider a $\mathbb{Z}$-lattice $L \cong \langle 1, 2\rangle$ on a quadratic $\mathbb{Q}$-space $V$, and let $m \in \mathbb{Z}$. We claim

$$m \longrightarrow L \quad \Longleftrightarrow \quad m \longrightarrow V.$$

Only "$\Longleftarrow$" requires proof. Whenever $p \neq 2$, the lattice $L_p$ is unimodular and hence $\mathbb{Z}_p$-maximal; and the $\mathbb{Z}_2$-lattice $L_2$ is $\mathbb{Z}_2$-maximal because any $\mathbb{Z}_2$-lattice properly containing it will have a Jordan component $\langle \lambda \rangle$ with $\lambda \notin \mathbb{Z}_2$. Therefore $L$ is $\mathbb{Z}$-maximal. Now (and here we are imitating our Cassels–Pfister argument) if $v \in V$ and $Q(v) = m$ then $v$ is contained in a $\mathbb{Z}$-maximal lattice $M$ on $V$. By Eichler's theorem, $M$ and $L$ are in the same genus, and hence $dM = dL = 2$. So Hermite's inequality (or the reduction theory of binary quadratic forms) gives $M \cong \langle 1, 2\rangle \cong L$, and hence a representation $m \longrightarrow L$, as claimed.

To finish the proof of (I), we must determine for which odd primes $l$ the isometry

$$\langle 1, 2, -l\rangle \cong \langle 1, -1, 2l\rangle$$

holds over $\mathbb{Q}_p$ for every prime $p$. Existence of such an isometry over $\mathbb{Q}_p$ is clear if $p \notin \{2, l\}$, by the triviality of the Hilbert symbol on $p$-adic units.

("$\Longrightarrow$") Suppose $l \equiv 1 \pmod 8$. Then $l \in \mathbb{Z}_2^{*2}$ by the local square theorem, and so $l \longrightarrow \langle 1, 2\rangle$ (and the equivalent isometry) holds over $\mathbb{Q}_2$. And the desired isometry holds over $\mathbb{Q}_l$ because the $\mathbb{Q}_l$-space on the left has Hasse symbol

$$(2, -l)_l = (2, l)_l = \left(\frac{2}{l}\right) = (-1)^{\frac{l^2-1}{8}} = 1,$$

while the space on the right has Hasse symbol

$$(-1, 2l)_l = (-1, l)_l = \left(\frac{-1}{l}\right) = 1.$$

Now suppose $l \equiv 3 \pmod 8$. Then $l \in 3\mathbb{Q}_2^{*2}$ by the local square theorem; and since trivially $3 \longrightarrow \langle 1, 2\rangle$ over $\mathbb{Q}_2$, so also $l \longrightarrow \langle 1, 2\rangle$ over $\mathbb{Q}_2$. Finally, the reader can check that the isometry $\langle 1, 2, -l\rangle \cong \langle 1, -1, 2l\rangle$ holds over $\mathbb{Q}_l$ by a Hasse symbol computation similar to that in the case $l \equiv 1 \pmod 8$.

("$\Longleftarrow$") If $l \equiv 5$ or $7 \pmod 8$, then the Hasse symbols of the two spaces of interest are different when $p = l$, hence the essential representation over $\mathbb{Q}_l$ fails, so the required representation over $\mathbb{Q}$ fails as well.

(II) Paralleling the argument in part (i), we begin by considering a lattice $L \cong \langle 1, 3\rangle$ with respect to a basis $\{v_1, v_2\}$ on a $\mathbb{Q}$-space $V$, with the goal of showing that for all $m \in \mathbb{Z}$ the equivalence $m \to L \Longleftrightarrow m \to V$ holds. Hermite's inequality and binary reduction shows that every integral lattice of discriminant 3 on $V$ must be isometric to $\langle 1, 3\rangle$ or $\begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$. These are in different genera, since over $\mathbb{Z}_2$ the latter lattice represents no odd integers. Therefore $L$ has class number 1. But now define $w_2 = \dfrac{v_1 + v_2}{2}$ and consider the lattice

$$M = \mathbb{Z}v_1 + \mathbb{Z}w_2 \cong \begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}.$$

Then $L \subsetneq M$ (in fact, $L_p = M_p$ for all $p \neq 2$, but $L_2 \subset M_2$), and $Q(M) \subseteq \mathbb{Z}$. So $L$ is not $\mathbb{Z}$-maximal; but $M$ is, and $M$ has class number 1. It follows that $m \to M \iff m \to V$. At first glance it may seem that the determination of the numbers represented by $L$ is no longer in sight; but fortunately it turns out that $L$ and $M$ represent the same integers, as we now show. Let $v \in M$; say $v = av_1 + bw_2$, with $a, b \in \mathbb{Z}$. If $2 \mid b$ then $v \in L$. But now suppose $b$ is odd (and so $v \notin L$). Then

$$Q(av_1 + bw_2) = \begin{cases} Q\big(-av_1 + (a+b)w_2\big) \text{ if } a \equiv 1 \pmod 2 \\ Q(bv_1 + aw_2) \text{ if } a \equiv 0 \pmod 2 \end{cases}$$

Therefore in all cases $Q(v) \in Q(L)$, as claimed. To sum up the argument in part (II) up to here: $L$ and $V$ represent exactly the same integers. Of course 3 is one of those integers. So to complete the proof of Fermat's theorem it remains to determine which odd primes $l \neq 3$ satisfy the Hilbert symbol equality

$$(3, -l)_p = (-1, 3l)_p \quad \text{for all primes } p;$$

equivalently,

$$(l, -3)_p = 1 \quad \text{for all primes } p.$$

Now, if this condition holds, then in particular $(l, -3)_3 = 1$, and therefore $l \equiv 1 \pmod 3$.

Conversely, suppose $l \equiv 1 \pmod 3$. Then $(l, -3)_p = 1$ for all $p \notin \{2, l\}$, by the triviality of the Hilbert symbol on $p$-adic units when $p$ is odd. Therefore by Hilbert reciprocity it suffices to show that $(l, -3)_2 = 1$ or (equivalently) that $(l, -3)_l = 1$. Since $l \equiv 1 \pmod 3$ and $l$ is odd, we actually have $l \equiv 1 \pmod 6$; say $l = 1 + 6k$.

If $k \equiv 0 \pmod 4$ then $l \equiv 1 \pmod 8$ and hence $(l, -3)_2 = 1$ by the local square theorem.

If $k \equiv 2 \pmod 4$ then $l \equiv 1 \pmod 4$, and then (since also $l \equiv 1 \pmod 3$)

$$(l, -3)_l = (l, -1)_l (l, 3)_l = (l, 3)_l = \left(\frac{3}{l}\right) = \left(\frac{l}{3}\right) = 1.$$

Finally, suppose $k$ is odd, and so $l \equiv 3 \pmod 4$. We have $(l, -3)_l = (l, 3)_l (l, -1)_l$. And now

$$(l, 3)_l = \left(\frac{3}{l}\right) = -\left(\frac{l}{3}\right) = -1 \quad \text{and} \quad (l, -1)_l = \left(\frac{-1}{l}\right) = -1.$$

Therefore $(l, -3)_l = 1$, as desired. □

**Problems**.

(1) Our example in which we discuss class numbers of lattices over $\mathbb{F}_3[x]$ is painfully ad hoc. Is there a more systematic approach to class numbers of $\mathbb{F}_q[x]$-lattices; and, in particular, is there a way to efficiently identify the lattices of class number 1 with a given discriminant?

(2) Under what conditions on a quadratic $\mathbb{Q}$-space $V$ is there an integral lattice $L$ on $V$ that represents all the integers represented by $V$? Clearly a lattice on $V$ that is $\mathbb{Z}$-maximal and also has a one-class genus will have this property. But, as we have seen in the lattice $\langle 1, 3 \rangle$, this pair of properties is not essential.

(3) Let us call two $\mathbb{Z}$-lattices on the same $\mathbb{Q}$-space **spectrally similar** if they represent exactly the same elements. For example, we have seen that $\langle 1, 3 \rangle$ and

$\begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}$ are spectrally similar. It would be interesting to develop tests for spectral similarity of lattices. Note that spectrally similar matrices need not be "isospectral" in the sense of Conway and Sloane [C–S]. For instance, the lattice $\langle 1, 3 \rangle$ represents 1 only twice, while $\begin{pmatrix} 1 & \frac{1}{2} \\ \frac{1}{2} & 1 \end{pmatrix}$ represents 1 six times.

(4) For which $\mathbb{Z}$ lattices $L$ is there a completely decomposable lattice (that is, a lattice with an orthogonal basis) spectrally similar to $L$ ?

(5) Given a $\mathbb{Z}$-lattice $L$, how can we determine a *minimal* lattice spectrally similar to $L$ ? If we restrict the search to sublattices of $L$, does it make the problem easier?

(6) Go beyond the reproof of Fermat's theorem given here to consider representations by a broader range of lattices, including lattices of higher rank.

(7) Reconsider the preceding questions over more general rings; e.g., over the rings of integers of algebraic number fields or global function fields.

## References

[C–S] J. H. Conway and N. J. A. Sloane, *Four-Dimensional Lattices with the Same Theta Series*, Duke Math. J. 66 (International Mathematics Research Notices 4 (1992), pp. 93–96.

[C] D. A. Cox, *Primes of the Form $x^2 + ny^2$*, John Wiley and Sons, 1997.

[G1] L. J. Gerstein, *Definite quadratic forms over $\mathbb{F}_q[x]$*, J. Algebra 268 (2003), 252–263.

[G2] L. J. Gerstein, *Basic Quadratic Forms*, Graduate Studies in Mathematics 90, Amer. Math. Soc., 2008.

[O] O. T. O'Meara, *Introduction to Quadratic Forms* (reprint of the 1973 edition), Springer-Verlag, 2000.

[S] J.-P. Serre, *A Course in Arithmetic*, Springer-Verlag, 1973.

Dept. of Mathematics, University of California, Santa Barbara, CA 93106-3080
E-mail address: **gerstein@math.ucsb.edu**