# RATIONAL QUADRATIC FORMS AND THE LOCAL-GLOBAL PRINCIPLE

PETE L. CLARK

A **form** of degree $k$ is a polynomial $P(x_1, \ldots, x_n)$ which is homogeneous of degree $k$: in each monomial term $cx_1^{i_1} \cdots x_n^{i_n}$, the *total degree* $i_1 + \ldots + i_n$ is $k$. E.g.

$$F_n(x, y, z) = x^n + y^n - z^n$$

is a form of degree $n$, such that the study of solutions to $F_n(x, y, z) = 0$ is equivalent to Fermat's Last Theorem.

For the most part we will concentrate here on **quadratic forms** ($k = 2$):

$$\sum_{1 \leq i \leq j \leq n} a_{ij} x^i x^j,$$

where the coefficients $a_{ij}$ are usually either integers or rational numbers (although we shall also be interested in quadratic forms with coefficients in $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{R}$). For instance, a **binary** quadratic form is any expression of the form

$$q(x, y) = ax^2 + bxy + cy^2.$$

As for most Diophantine equations, quadratic forms were first studied over the integers, meaning that the coefficients $a_{ij}$ are integers and only integer values of $x_1, \ldots, x_n$ are allowed to be plugged in. At the end of the 19th century it was realized that by allowing the variables $x_1, \ldots, x_n$ to take *rational* values, one gets a much more satisfactory theory. (In fact one can study quadratic forms with coefficients and values in any field $F$. This point of view was developed by Witt in the 1930's, expanded in the middle years of this century by, among others, Pfister and Milnor, and has in the last decade become especially closely linked to one of the deepest and most abstract branches of contemporary mathematics: "homotopy K-theory.") However, a wide array of firepower has been constructed over the years to deal with the complications presented by the integral case, culminating recently in some spectacular results. In this handout we will concentrate on what can be done over the rational numbers, and also on what statements about integral quadratic forms can be directly deduced from the theory of rational quadratic forms.

Let us distinguish two types of problems concerning a quadratic form $q(x_1, \ldots, x_n)$, which we will allow to have *either* integral or rational coefficients $a_{ij}$.

**Homogeneous problem** (or **isotropy problem**): Determine whether there exist integers, $x_1, \ldots, x_n$, not all zero, such that $q(x_1, \ldots, x_n) = 0$. A quadratic form such that $q(x) = 0$ has a nontrivial integral solution is said to be **isotropic**; if there is no nontrivial solution it is said to be **anisotropic**.

Example 0: The sum of squares forms $x_1^2 + \ldots + x_n^2$ are all anisotropic. Indeed, for any real numbers $x_1, \ldots, x_n$, not all zero, $x_1^2 + \ldots + x_n^2 > 0$: a form with this property is said to be **positive definite**.

Example 1: The $\mathbb{Z}$-quadratic form $x^2 - ny^2$ is isotropic iff $n$ is a perfect square.

**Inhomogeneous problem**: For a given integer $n$, determine whether the equation $q(x_1, \ldots, x_n) = n$ has an integer solution (if so, we say "$q$ **represents** $n$"). More generally, for fixed $q$, determine all integers $n$ represented by $q$.

Example 2: We determined all integers $n$ represented by a $x_1^2 + x_2^2$, and stated without proof the results for the quadratic forms $x_1^2+x_2^2+x_3^2$ and $x_1^2+x_2^2+x_3^2+x_4^2$; in the latter case, all positive integers are represented.

In general the inhomogeneous problem is substantially more difficult than the homogeneous problem. One reason why the homogeneous problem is easier is that, even if we originally state it in terms of the integers, it can be solved using rational numbers instead:

**Proposition 1.** *(Principle of homogeneous equivalence) Let $P(x_1, \ldots, x_n)$ be a homogeneous polynomial with integral coefficients. Then $P(x_1, \ldots, x_n)$ has a nontrivial solution with $x_1, \ldots, x_n \in \mathbb{Z}$ iff it has a nontrivial solution with $x_1, \ldots, x_N \in \mathbb{Q}$.*

Proof: Of course a nontrivial integral solution is in particular a nontrivial rational solution. For the converse, assume there exist $\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}$, not all 0, such that $P(\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}) = 0$. Suppose $P$ is homogeneous of degree $k$. Then for any $\alpha \in \mathbb{R}^\times$, we have

$$P(\alpha x_1, \ldots, \alpha x_n) = \alpha^k P(x_1, \ldots, x_n),$$

since we can factor out $k$ $\alpha$'s from every term. So let $N = \operatorname{lcm}(q_1, \ldots, q_n)$. Then

$$P(N\frac{p_1}{q_1}, \ldots, N\frac{p_n}{q_n}) = N^k P(\frac{p_1}{q_1}, \ldots, \frac{p_n}{q_n}) = N^k \cdot 0 = 0,$$

so that $(N\frac{p_1}{q_1}, \ldots, N\frac{p_n}{q_n})$ is a nontrivial integral solution.

Thus the homogeneous problem for integral forms (of any degree) is really a problem about *rational* forms.

Remark: The inhomogeneous problem still makes sense for forms of higher degree, but to solve it – even for rational forms – is generally extremely difficult. For instance, Selmer conjectured in 1951 that a prime $p \equiv 4,\ 7,\ 8 \pmod 9$ is of the form $x^3 + y^3$ for two *rational* numbers $x$ and $y$. A proof of this in the first two cases was announced (but not published) by Noam Elkies in 1994; more recently, Dasgupta and Voight have carefully written down a proof of a slightly weaker result. The case of $p \equiv 8 \pmod 9$ remains open. In this case (i.e., that of binary cubic forms) the rich theory of rational points on elliptic curves can be fruitfully applied. Even less is known about (say) binary forms of higher degree.

## 1. Rational quadratic forms

In this section, we work with quadratic forms $q$ with coefficients $a_{ij}$ lying in $\mathbb{Q}$. (In fact, everything we say works over an arbitrary field $F$ whose characteristic is different from 2.) This gives many advantages, which we state mostly without proof:

Fact 1: Every rational quadratic form can be diagonalized.

In general, two quadratic forms $q$ and $q'$ should be regarded as **equivalent** if there is an invertible linear change of variables $(x_1', \ldots, x_n') = A(x_1, \ldots, x_n)$ carrying one to the other. In particular, equivalent quadratic forms represent the same values, and equivalence preserve an/isotropy.

Any quadratic form $q(x_1, \ldots, x_n)$ can be represented by a symmetric matrix $Q$, such that

$$q(x_1, \ldots, x_n) = xQx^T,$$

where $x = (x_1, \ldots, x_n)$. However, there is a slight annoyance here which is seen by calculating the quadratic form associated to the symmetric matrix

$$\begin{bmatrix} a & b \\ b & d \end{bmatrix}$$

; it is

$$q(x_1, x_2) = ax_1^2 + 2bx_1x_2 + bx^{.}_2$$

So to get the "general" binary quadratic form of XX, we need to use the matrix

$$\begin{bmatrix} a & \frac{b}{2} \\ \frac{b}{2} & d, \end{bmatrix}$$

and in general, the symmetric matrix $M$ corresponding to the quadratic form $\sum_{i \leq j} a_{ij} X^i X^j$ is

$m_{ij} = a_{ij}$, $i = j$,
$m_{ij} = \frac{a_{ij}}{2}$, $i \neq j$,

so the representing matrix $M$ of an integral quadratic form $q$ will in general have only half-integral entries.

Now the matrix interpretation of equivalence is as follows: the form with representing matrix $M$ is equivalent to the quadratic form with representing matrix $AMA^T$ for any invertible matrix $A$. If we are working with rational quadratic forms, then $M$ and $A$ can have rational entries and the condition for invertibility is that $\det(A) \neq 0$. However, if we are working with integral quadratic forms, then $A$ must have integral entries and its inverse must have integral entries, which means that $\det(A) = \pm 1$.

Recall from linear algebra that every real symmetric matrix $M$ is similar to a diagonal matrix via a matrix $A$ which is orthogonal: $A^{-1} = A^T$. In fact, for every symmetric matrix $M$ with entries in a subfield $F$ of $\mathbb{C}$, there exists an invertible matrix $A$ such that $AMA^T$ is diagonal: this amounts to saying that we can "rationally diagonalize" a symmetric matrix by performing simultaneous row and column operations. We omit the proof.

In particular, every rational quadratic form is equivalent to a quadratic form of the shape

$$\langle a_1, \ldots, a_n \rangle = a_1x_1^2 + \ldots + a_nx_n^2.$$

Example: Consider the integral quadratic form $q(x,y) = xy$, with associated matrix $M = \begin{bmatrix} 0 & \frac{1}{2} \\ \frac{1}{2} & 0 \end{bmatrix}$. Note that we have $\det(M) = -\frac{1}{4}$. If there exists an integrally invertible matrix $A$ with $AMA^T = D$ diagonal, then

$$\det(D) = \det(A)\det(M)\det(A^T) = \det(M)\det(A)^2 = \det(M) = -\frac{1}{4}.$$

But the diagonal entries of the matrix defining an integral quadratic form must be integers, so the determinant of any integrally diagonalizable quadratic form must be an integer. So $q(x,y) = xy$ is not integrally diagonalizable.

Fact 2: Every isotropic rational quadratic form is universal.

There is a special quadratic form

$$H = \langle 1, -1 \rangle = x_1^2 - x_2^2,$$

called the **hyperbolic plane**. By diagonalizing the form $q(x,y) = xy$, one sees that it is equivalent, over $\mathbb{Q}$, to $H$. In particular the hyperbolic plane $H$ is isotropic – indeed take $x_1 = x_2$ – and moreover it represents every nonzero scalar $x \in \mathbb{Q}^\times$: take $y = 1$. One can show that if $q$ is any isotropic rational quadratic form, then

$$q \cong x_1^2 - x_2^2 + q'(x_3, \ldots, x_n),$$

so that every isotropic form "contains" the hyperbolic plane. In particular, every quadratic form which is isotropic *rationally* represents every rational number.

This is not true over $\mathbb{Z}$: the isotropic quadratic form $x^2 - y^2$ does not represent every integer. Indeed, $x^2 - y^2 \equiv 2 \pmod 4$ has no solution, so $x^2 - y^2$ does not represent any integer which is $2 \pmod 4$.

Fact 3: Over $\mathbb{Q}$, the representation problem can be reduced to the isotropy problem.

More precisely, one has the following result:

**Theorem 2.** *Let $q(x_1, \ldots, x_n)$ be a quadratic form over $\mathbb{Q}$ (or over any field $F$ of characteristic different from 2), and let $a \in \mathbb{Q}^\times$ (or $a \in F^\times$). The following are equivalent:*
*a) The quadratic form $q(x_1, \ldots, x_n) + (-a)x_{n+1}^2$ is isotropic.*
*b) The quadratic form $q$ rationally represents $a$.*

Proof: If $q$ represents $a$, then there exist $x_1, \ldots, x_n \in \mathbb{Q}$, not all 0, such that $q(x_1, \ldots, x_n) = a$, but then rewriting gives

$$q(x_1, \ldots, x_n) + (-a)(1)^2 = 0.$$

Conversely, suppose there are $x_1, \ldots, x_n, x_{n+1}$ in $\mathbb{Q}$, not all 0, such that $q(x_1, \ldots, x_n) + (-a)x_{n+1}^2 = 0$. If $x_{n+1} \neq 0$, then we can move it to the other side and divide by it (thank goodness we are over $\mathbb{Q}$!) to get

$$q(\frac{x_1}{x_{n+1}}, \ldots, \frac{x_n}{x_{n+1}}) = a.$$

Otherwise, we have $q(x_1, \ldots, x_n) = 0$, for $x_1, \ldots, x_n$ not all zero, which means that $q$ is isotropic, and we averred above that this implies that $q$ "contains" the hyperbolic plane $H$ and therefore represents *every* element of $\mathbb{Q}^\times$, in particular $a$.

Thus, if we had an algorithm for deciding whether a given rational quadratic form is isotropic, then applying it to the form $q + (-a)x_{n+1}^2$, we can equally well decide whether it rationally represents any given number $a$.

Remark: There is, to the best of my knowledge, absolutely nothing like "Fact 3" for forms of higher degree.

## 2. Legendre's Theorem

We can now give a complete solution to a problem we first considered early on in the course: given $a, b, c \in \mathbb{Z}$, how do we know whether the (quadratic) form

$$ax^2 + by^2 + cz^2 = 0$$

has a nontrivial solution?

Note that, by the discussion of the last section, if we can solve this problem we can completely solve the homogeneous problem for ternary *integral* quadratic forms $q(x, y, z) = 0$. Indeed, by Proposition 1 it is enough to decide whether or not $q(x, y, z) = 0$ has a nontrivial rational solution, and working rationally we can diagonalize $q$ to get an equation of the above form.

The answer is given by the following beautiful theorem of Legendre. To state it, we will employ some *ad hoc* notation: for nonzero integers $a$ and $b$, we will write $a\square\, b$ to mean that $a$ is a square (possibly zero) modulo $|b|$. Note that, if $b$ is odd, $a\square\, b$ implies that the Jacobi symbol $\left(\frac{a}{b}\right) = 1$, but not conversely. A small lemma:

**Lemma 3.** *Let $b, c \in \mathbb{Z} \setminus \{0\}$, with $\gcd(b, c) = 1$. Then $a\square\, bc \iff a\square\, b$ and $a\square\, c$.*

If there exists an integer $x$ such that $a \equiv x^2 \pmod{bc}$, then certainly $a \equiv x^2 \pmod{b}$ and $a \equiv x^2 \pmod{c}$, giving the forward implication. Conversely, if $a \equiv x^2 \pmod{b}$ and $a \equiv y^2 \pmod{c}$, then since $b$ and $c$ are relatively prime, by CRT there exists a $z \pmod{bc}$ such that $z \equiv x \pmod{b}$ and $z \equiv y \pmod{c}$, hence $a \equiv z^2 \pmod{b}$ and $a \equiv z^2 \pmod{c}$, so $a \equiv z^2 \pmod{bc}$.

**Theorem 4.** *(Legendre) Let a, b, c be nonzero integers, squarefree, relatively prime in pairs, and neither all positive nor all negative. Then*

$$ax^2 + by^2 + cz^2 = 0$$

*has a nontrivial integral solution iff all of the following hold:*
*(i) $-ab\square\, c$.*
*(ii) $-bc\square\, a$.*
*(iii) $-ca\square\, b$.*

Some remarks on the conditions: if $a$, $b$ and $c$ are all positive or all negative, the quadratic form is definite over $\mathbb{R}$ and has no nontrivial real solutions. Because integral isotropy is equivalent to rational isotropy, we may adjust $a$, $b$ and $c$ by any rational square, and therefore we may assume that they are squarefree integers. Moreover, if two of them are divisible by a prime $p$, then they are both exactly divisible by $p$, and by a simple $\text{ord}_p$ argument the equation certainly has no solutions unless $p$ divides $c$. But then we may divide through $a$, $b$ and $c$ by $p$.

Let us prove the easy half of this theorem now, namely showing that these conditions are necessary. In fact, let us show that they are precisely the conditions obtained by postulating a primitive integral solution $(x, y, z)$ and going modulo $a$, $b$ and $c$. Indeed, go modulo $c$: we get

$$ax^2 \equiv -by^2 \pmod{c};$$

multiplying by $-b$, which is coprime to $c$, we get the equivalent condition

$$-abx^2 \equiv (by)^2 \pmod{c}.$$

Suppose first that there exists some prime $p \mid c$ such that $p \mid x$. Then since $\gcd(b, c) = 1$, we get $p \mid y$, and that implies $p^2 \mid -ax^2 - by^2 = cz^2$. Since $c$ is squarefree, this implies $p \mid z$, contradicting primitivity. Therefore $x$ is nonzero modulo every prime $p$ dividing $c$, so $x$ is a unit modulo $c$, and we can divide, getting

$$-ab \equiv (byx^{-1})^2 \pmod{c},$$

which is condition (i). By symmetry, reducing modulo $a$ we get (ii) and reducing modulo $b$ we get (iii).

Following Ireland and Rosen, to prove the sufficiency we will state the theorem in an equivalent form, as follows:

**Theorem 5.** *(Legendre's theorem restated) For $a$ and $b$ positive squarefree integers, the equation*

$$ax^2 + by^2 = z^2$$

*has a nontrivial integral solution iff all of the following hold:*
*(i) $a\Box\ b$.*
*(ii) $b\Box\ a$.*
*(iii) $-\frac{ab}{d^2}\Box\ d$, where $d = \gcd(a, b)$.*

We leave it as a (not difficult, but somewhat tedious) exercise to the reader to check that Theorem 5 is equivalent to Theorem 4.

Now we prove the sufficiency of the conditions of Theorem 5.

The result is obvious if $a = 1$.

Case 1: $a = b$. The theorem asserts that $ax^2 + ay^2 = z^2$ has a solution iff $-1$ is a square modulo $a$. By the first supplement to QR, this is last condition is equivalent to: no prime $p \equiv 3 \pmod{4}$ divides $a$. If this condition holds then by the two squares theorem we have $a = r^2+s^2$, and then we can take $x = r,\ y = s,\ z = r^2+s^2$. On the other hand, if there exists $p \mid a$, $p \equiv 3 \pmod{4}$, then taking $\operatorname{ord}_p$ of both sides of the equation $z^2 = a(x^2 + y^2)$ gives a contradiction, since $\operatorname{ord}_p(z^2) = 2\operatorname{ord}_p(z)$ is even, and $\operatorname{ord}_p(a(x^2 + y^2)) = \operatorname{ord}_p(a) + \operatorname{ord}_p(x^2 + y^2) = 1 + \operatorname{ord}_p(x^2 + y^2)$ implies $\operatorname{ord}_p(x^2 + y^2)$ is odd, contradicting the Two Squares Theeorem.

If $b > a$, we can interchange $a$ and $b$, so we may now assume that $a > b$.

We will now prove the theorem by a descent-type argument, as follows: assuming the hypotheses of Theorem 5 we will construct a new form $Ax^2+by^2 = z^2$ satisfying the same hypotheses, with $0 < A < a$, and such that if this latter equation has a nontrivial solution then so does $ax^2 + by^2 = z^2$. We perform this reduction process repeatedly, interchanging $A$ and $b$ if $A < b$. Since each step reduces $\max(A, b)$, eventually we will be in the case $A = 1$ or $A = b$, in which we have just shown the equation has a solution. Reversing our sequence of reductions shows that the original equation has a solution.

Now, since $b\Box\ a$, there exist $T$ and $c$ such that

$$c^2 - b = aT, \tag{1}$$

for $T \in \mathbb{Z}$. Applying the square/squarefree decomposition, we may write $T = Am^2$ with $A$ squarefree. Choosing $c$ minimally, we may assume that $|c| \le \frac{a}{2}$.

Claim: $0 < A < a$.

Proof: Since $0 \le c^2 = aAm^2 + b < a(Am^2 + 1)$ and $a > 0$, $Am^2 > -1$; since $b$ is squarefree, $T = am^2 \neq 0$, hence $Am^2 \ge 1$ and thus $A > 0$. Also

$$aAm^2 < c^2 \le \frac{a^2}{4},$$

so

$$A \le Am^2 < \frac{a}{4} < a.$$

Claim: $A\Box\ b$.

Recalling $d = \gcd(a, b)$, write $a = a_1 d$, $b = b_1 d$, so that $\gcd(a_1, b_1) = 1$; since $a$ and $b$ are squarefree, this implies $\gcd(a_1, d) = \gcd(b_1, d) = 1$. Then (1) reads

$$c^2 - b_1 d = a_1 d A m^2 = aAm^2.$$

So $d \mid c^2$, and since $d$ is squarefree, $d \mid c$. Put $c = c_1 d$ and cancel:

$$dc_1^2 - b_1 = Aa_1 m^2. \tag{2}$$

So $Aa_1m^2 \equiv -b_1 \pmod{d}$; multiplying through by $a_1$, we get

$$Aa_1^2 m^2 \equiv -a_1 b_1 \pmod{d}. \tag{3}$$

Now, any common prime factor $p$ of $m$ and $d$ would divide both $b_1$ and $d$, a contradiction; so $\gcd(m, d) = 1$. Since $\frac{-ab}{d^2} = -a_1 b_1$ is a square modulo $d$ by (iii) and $a_1$ and $m$ are units modulo $d$, (3) implies that $A\Box\ d$. Moreover, $c^2 \equiv aAm^2 \pmod{b_1}$. Since $a\Box\ b$, $a\Box\ b_1$. Also $\gcd(a, b_1) = 1$ – a common divisor would divide $d$, but $\gcd(b_1, d) = 1$ – and similarly $\gcd(m, b_1) = 1$. So

$$A \equiv c^2(am^2)^{-1} \pmod{b_1},$$

and hence $A\Box\ b_1$. Since $A\Box\ b_1$ and $A\Box\ d$, by Lemma 3 $A\Box\ b$.

Next, put $r = \gcd(A, b)$ and $A = rA_1$, $b = rb_2$, so that $\gcd(A_1, b_2) = \gcd(r, b_2) = 1$. We claim that $-A_1b_2\Box\ r$. Using (1) we have

$$c^2 - rb_2 = c^2 - rb = aAm^2 = arA_1m^2. \tag{4}$$

Since $b$ is squarefree, so is $r$, hence $r \mid c$. So if a prime $p$ divides both $am$ and $r$, then $p^2 \mid c^2 - aAm^2 = rb_2 \implies p^2 \mid r$, a contradiction. So $\gcd(am, r) = 1$. Putting $c = rc_1$,

$$arA_1m^2 \equiv -rb_2 \pmod{r^2},$$

so

$$aA_1m^2 \equiv -b_2 \pmod{r}.$$

Since $a\square\ b$ and $r \mid b$, $a\square\ r$. Multiplying through by $b_2$, we get

$$-aA_1b_2m^2 \equiv b_2^2 \pmod{r},$$

and since $\gcd(am, r) = 1$, we conclude $-A_1b_2\square\ r$.

Now assume that $AX^2 + bY^2 = Z^2$ has a nontrivial solution. Then

$$AX^2 = Z^2 - bY^2. \tag{5}$$

Multiplying (5) by (1), we have

$$a(AXm)^2 = (Z^2 - bY^2)(c^2 - b) = (Zc + bY)^2 - b(cY + Z)^2.$$

Note that this unlikely-looking identity can be interpreted as

$$N(Z + Y\sqrt{b})N(c + \sqrt{b}) = N(Zc + bY + (cY + Z)\sqrt{b}).$$

Putting $x = AXm$, $y = cY + Z$, $z = Zc + bY$, this gives a solution to $ax^2 + by^2 = z^2$, which is nontrivial since $x \neq 0$. Thus we have completed our "descent" argument, which proves that the equation has a solution.

## 3. Hilbert's reciprocity law

As we mentioned, Legendre's theorem has the following consequence: a ternary quadratic form

$$q_{a,b} : aX^2 + bY^2 - Z^2$$

has a nontrivial integral solution iff there is a real solution and for every prime $p$ and every positive integer $a$ the congruence

$$aX^2 + bY^2 \equiv Z^2 \pmod{p^a} \tag{6}$$

has a nontrivial solution. As $a$ increases, each of these congruences is stronger than the last, so it makes some sense to bundle up the infinitely many questions of whether any of these $p$-power congruences has a solution into a single question. Let us introduce the following terminology:

An integral quadratic form $q(x_1, \ldots, x_n)$ is **p-isotropic** if for all $a \in \mathbb{Z}^+$, the congruence $q(x_1, \ldots, x_n) \equiv 0 \pmod{p^a}$ has a nontrivial solution. Otherwise we will say that it is **p-anisotropic**. We will say that $q$ is **$\infty$-isotropic** if it has a real solution.[1]

Considering the case of $q_{a,b}$, for each prime $p$ and for $\infty$ we are asking a yes/no question – "Is $q_{a,b}$ $p$-isotropic?" so it makes some vague sense to denote "yes" by $+1$ and "no" by $-1$, so we define **symbols** $\langle a, b\rangle_p$ for all primes $p$ and $\langle a, b\rangle_\infty$ in this way: i.e., $+1$ if $q_{a,b}$ is $p$-isotropic and $-1$ if it is $p$-anisotropic (and the same for $\infty$). So Legendre's theorem can be rephrased by saying that $q_{a,b}$ is istropic iff $\langle a, b\rangle_p = 1$ for all $p \leq \infty$.

But now that we've defined the notation, a further question occurs to us: if $q_{a,b}$ is

[1] Don't ask why we have introduced the symbol $\infty$ to describe the real solutions. It is just traditional to do so. Moreover, we will eventually get tired of saying "(and $\infty$)" and start writing $p \leq \infty$. There is no need to read anything deep into this, at least not today.

isotropic, the answers to our questions are always yes; but if it isn't, at least some of the answers are no. So which combinations of yes and no are possible?

**Theorem 6.** *(Hilbert) a) For every pair of nonzero integers $a, b$, the symbol $\langle a, b\rangle_p$ is equal to $+1$ except possibly for finitely many values of $p \leq \infty$.*
*b) Two integral ternary quadratic forms $q_{a,b}$ and $q_{c,d}$ are* rationally equivalent *– i.e., one can be obtained from the other by a $3 \times 3$ invertible matrix $A$ with rational entries – iff $\langle a, b\rangle_p = \langle c, d\rangle_p$ for all $p \leq \infty$.*
*c) The finite set of $p \leq \infty$ for which $\langle a, b\rangle_p = -1$ has an* even *number of elements.*
*d) For every subset $S$ of the primes union $\infty$ which is finite and of even order, there exist $a$ and $b$ such that $\langle a, b\rangle_p = -1$ iff $p \in S$.*

We admit that this is a mouthful. In particular parts b) and d) solve yet a third problem on rational quadratic forms: their *classification* up to equivalence. We advise the reader to concentrate on the following consequence: for any $q_{a,b}$, by part a) we can consider the infinite product $\prod_{p\leq\infty}\langle a, b\rangle_p$ (since it equals 1 except possible finitely many times), and by part c) we get the following relation, the **Hilbert reciprocity law**:

$$\prod_{p\leq\infty}\langle a, b\rangle_p = 1 \tag{7}$$

This has the extremely useful upshot that instead of having to check congruences modulo all powers of all primes and a sign condition, it suffices to omit any one $p \leq \infty$ from these checks. In particular, we could omit "$p = \infty$" from the checking and get the following result which looks hard to believe based upon the proof we gave: if $ax^2 + by^2 = z^2$ has a solution modulo $p^a$ for all $p$ and $a$, then it necessarily has an integral solution: in particular the condition that $a$ and $b$ are not both positive *follows automatically* from all the congruence conditions, although it is certainly independent of any finite number of them!

In fact, with a bit of hindsight one can see that the condition of whether or not there is going to be a solution modulo all powers of 2 is the most complicated one. This is taken into account in the statement of Legendre's theorem: the congruence conditions on their own would not imply that $\langle a, b\rangle_2 = +1$ without the sign conditions ("conditions at $\infty$"), so somehow Legendre's clean conditions exploit this slight redundancy. To see this, consider the case of $a = b = -1$, which has solutions modulo every power of an odd prime, but no nontrivial solutions modulo 4 (and also no real solutions).

Hilbert also found explicit formulae for $\langle a, b\rangle_p$ in terms of Legendre symbols. For the sake of concision we do not state it here. However, we cannot help but mentioning that if one knows these formulae (which are not so hard to prove), then the relation (7) is equivalent to knowing quadratic reciprocity together with its first and second supplements! It turns out that all aspects of the theory rational quadratic forms can be generalized to the case where the coefficients lie not in $\mathbb{Q}$ but in an arbitrary algebraic number field $K$. In particular, a suitable version of Hilbert's reciprocity law holds over $K$, and this is a very clean way to phrase quadratic reciprocity over number fields.

## 4. The local-global principle

We are now in a position to state what is surely one of the most important and influential results in all of number theory.

**Theorem 7.** *(Hasse-Minkowski) Let $q(x_1, \ldots, x_n)$ be an integral quadratic form. The following are equivalent:*
*a) $q$ is isotropic (over $\mathbb{Z} \iff$ over $\mathbb{Q}$).*
*b) $q$ is isotropic over $\mathbb{R}$, and for all $n \in \mathbb{Z}^+$, there are nontrivial solutions to the congruence $q(x_1, \ldots, x_n) \equiv 0 \pmod{n}$.*

It is clear that a) $\implies$ b). Indeed, in contrapositive form, this has been our favorite "easy" method for showing that an equation *does not* have a solution: any integral solution also gives a real solution and a solution to every possible congruence. The matter of it is in the converse, which asserts that if a quadratic form $q(x_1, \ldots, x_n) = 0$ does not have an integral solution, we can always detect it via congruences and/or over the real numbers.

This turns out to be the master theorem in the area of rational quadratic forms. It is not (yet) stated in a form as explicit as Legendre's theorem for ternary quadratic forms – which, recall, did not just assert that isotropy modulo $n$ for all $n$ implied isotropy over $\mathbb{Z}$ (or equivalently, over $\mathbb{Q}$) but actually said explicitly, in terms of the coefficients, a finite list of congruence conditions to check. Indeed one knows such explicit conditions in all cases, and we will return to mention them in the next section, but for now let us take a broader approach.

First, even in its "qualitative form" the theorem gives an algorithm for determining whether any quadratic form is isotropic. Namely, we just have to search in parallel for one of the two things:

(i) Integers $x_1, \ldots, x_n$, not all 0, such that $q(x_1, \ldots, x_n) = 0$.
(ii) An integer $N$ such that the congruence $q(x_1, \ldots, x_n) \equiv 0 \pmod{N}$ has only the all-zero solution.

For any given $N$, (ii) is a finite problem: we have exactly $N^n - 1$ values to plug in and see whether we get 0. Similarly, if we wanted to check all tuples of integers $(x_1, \ldots, x_n)$ with $\max_i |x_i| \leq M$, then that too is obviously a finite problem. Conceivably we could search forever and never find either a value of $M$ as in (i) or a value of $N$ as in (ii) – for sure we will never find both! – but the Hasse-Minkowksi theorem asserts that if we search long enough we will find either one or the other. This then is our algorithm!

In point of fact the situation is better for part (ii): it can be shown that for any degree $k$ form $P(x_1, \ldots, x_n)$ with integer coefficients, there is a recipe (algorithm!) for computing a *single* value of $N$ such that if $P(x_1, \ldots, x_n) \equiv 0 \pmod{N}$ has a nontrivial solution, then *for all* $N$ the congruence has a solution. Moreover, one can determine whether or not there are any real solutions (using methods from calculus). For this the two essential tools are:

(i) The Weil bounds for points on curves over $\mathbb{Z}/p\mathbb{Z}$, which allows one to compute a finite set of primes $S$ such that for all $p > S$ the congruence $P \equiv 0 \pmod{p}$ automatically has nontrivial solutions (in fact, a number of solutions which tends to $\infty$ with $p$).

This is a serious piece of mathematics dating from around the 1940's.

(ii) Hensel's Lemma, which gives sufficient conditions for lifting a solution $(x_1, \ldots, x_n)$ to $P \equiv 0 \pmod{p}$ to solutions modulo all higher powers $p^a$ of $p$.

This turns out to be surprisingly similar to Newton's method for finding roots of equations, and the proof is relatively elementary.

Alas, we do not have time to say more about either one.

So in finite time we can determine whether or not there is any value of $N$ for which $P(x_1, \ldots, x_n) \equiv 0$ has only the trivial solution, and we can also tell whether there are real solutions. Of course, if $P = 0$ fails to have congruential solutions and/or real solutions, then we know it cannot have nontrivial integral (equivalently, rational) solutions. But suppose we find that our form $P$ passes all these tests? Can we then assert that it has a nontrivial integral solution?

As we have just seen (or heard), the answer is a resounding "yes" when $P$ is a **quadratic** form. In general, whenever the answer to this question is "yes", one says that the **local-global principle**, or **Hasse principle**, holds for $P$. Of course the big question is: does the Hasse principle hold for all forms of higher degree?

One can also ask whether the Hasse principle holds for not-necessarily homogeneous polynomials, like $x^2 + y^3 + z^7 = 13$. The following remarkable result shows that it could not possibly hold for all polynomials in several variables over the integers.

**Theorem 8.** *(Davis-Matijasevic-Putnam-Robinson) There is no algorithm that will accept as input a polynomial $P(x_1, \ldots, x_n)$ with integral coefficients and output* 1 *if $P(x_1, \ldots, x_n) = 0$ has an integral solution, and* 0 *otherwise.*

Since we just said that there is an algorithm which determines if a polynomial (not necessarily homogeneous, in fact) has congruential solutions and real solutions, there must therefore be some polynomials which pass these tests and yet still have no solutions.

Remark: It is unknown whether there exists an algorithm to decide if a polynomial with rational coefficients has a rational solution.

One might think that such counterexamples to the Hasse principle might be in some sense nonconstructive, but this is not at all the case:

**Theorem 9.** *The following equations have congruential solutions and real solutions, but no nontrivial integral solutions:*

*a) (Selmer)* $3X^3 + 4Y^3 + 5Z^3 = 0$*;*
*b) (Bremner)* $5w^3 + 9x^3 + 10y^3 + 12z^3 = 0$.

These are just especially nice examples. It is known (if not "well-known") that for every $k > 2$ there is a form $P(x, y, z) = 0$ of degree $k$ which violates the local-global principle. In fact some of my own work has been devoted to constructing large (in particular, infinite) sets of counterexamples to the local-global principle.

There are however some further positive results, the most famous and important being the following:

**Theorem 10.** *(Birch) Let $k$ be a positive integer. Then there exists an $n_0(k)$ with the following property:*
*a) If $k$ is odd, then every degree $k$ form $P(x_1, \ldots, x_n) = 0$ in $n \geq n_0$ variables has a nontrivial integral solution.*
*b) If $k$ is odd and $P(x_1, \ldots, x_n)$ is a degree $k$ form in $n \geq n_0$ variables with "low-dimensional singularities", then $P$ has a nontrivial integral solution iff it has a nontrivial real solution.*

Remark: The condition of low-dimensional singularities is a bit technical. Let us rather define what it means for an equation to have no singularities at all, which is a special case. A nontrivial **complex** solution $(x_1, \ldots, x_n)$ to $P(x_1, \ldots, x_n)$ at which all the partial derivatives $\frac{\partial P}{\partial x_i}$ vanish is called a **singular point**. (Perhaps you remember from multivariable calculus these are the points at which a curve or surface can be "not so nice": i.e., have self-intersections, cusps, or other pathologies.) $P$ is said to be **nonsingular** if there are no singular points. In particular, one immediately checks that a diagonal form $P(x_1, \ldots, x_n) = a_1 x_1^k + \ldots + a_k x_n^k$ is nonsingular, so Birch's theorem applies to diagonal forms, and in particular to quadratic forms. (As far as I know it is an open problem whether the theorem holds for forms of even degree without any additional hypotheses.)

Thus morally, if only there are enough variables compared to the degree, then all congruence conditions are automatically satisfied and moreover th. However, in the proof $n_0$ does indeed have to be very large compared to $k$, and it is quite an active branch of analytic number theory to improve upon these bounds.

Another idea, which we shall be able to express only vaguely and see an example of in the case of the inhomogeneous problem for integral quadratic forms, is that if one asks as a yes/no question whether or not the existence of congruential solutions and real solutions is enough to ensure the existence of integral solutions, then one has to take rather drastic measures – e.g., enormously many variables compared to the degree, as above – to ensure that the answer is "yes" rather than "no" most of the time. However, if one can somehow **quantify** the failure of a local-global phenomenon, then one can hope that in any given situation it fails only to a *finite* extent.

## 5. Local Conditions for Isotropy of Quadratic Forms

(ii) Although the result is not phrased in explicit form, part of the point is that one can easily determine whether the condition of part b) holds. For instance, there will be real solutions unless, when the quadratic form is diagonalized (over $\mathbb{Q}$), all of the diagonal entries have the same sign. It is less obvious but still true that given *any* equation $P(x_1, \ldots, x_n)$, there is an algorithm to check in a finite amount of time whether for *all* $N$, $P(x_1, \ldots, x_n) \equiv 0 \pmod N$ has nontrivial solutions. Explicit conditions will be given in the case of ternary quadratic forms ($n = 3$), coming up soon. Such conditions are known for all $n$ (for $n = 2$, they are the restrictions coming from quadratic reciprocity that we have already seen).

(iii) In fact as the number of variables increases it becomes much easier to satisfy the congruence conditions, until we get to $n = 5$: every quadratic form $q(x_1, \ldots, x_n)$ in 5 or more variables has nontrivial solutions modulo every integer $N$! This has a remarkable corollary:

**Theorem 11.**
*a) Let $q(x_1, \ldots, x_n)$ be an integral quadratic form in at least 5 variables. Then $q(x) = 0$ has a nontrivial integral solution iff it has a nontrivial* real solution*, i.e., unless $q$ is positive or negative definite.*
*b) Let $q$ be a quadratic form in at least 4 variables which is not negative (resp. positive) definite – i.e., over $\mathbb{R}$ it takes on some positive (resp. negative) values. Then $q$ rationally represents all positive (resp. negative) rational numbers.*

Proof: Part a) follows immediately from the Hasse-Minkowksi theorem and the assertion that there are no "congruential" obstructions to a quadratic form in at least 5 variables being isotropic. Part b) follows morally by applying Theorem 2, although to see it one needs to know that there is a field $\mathbb{Q}_p$ of characteristic 0 with the property that $q$ is isotropic over $\mathbb{Q}_p$ iff $q$ is isotropic modulo $p^a$ for all $a$.

So in particular we deduce that every positive rational number is a sum of four rational squares. This is of course weaker than Lagrange's Theorem, and it must be, because the theorem also applies e.g. to $2x_1^2 + 3x_2^2 + 4x_3^2 + 5x_4^2$, which visibly does not represent 1 over $\mathbb{Z}$.