

REPRESENTATIONS OF INTEGERS BY QUADRATIC FORMS

PETE L. CLARK

As we have seen, if

$$P(x_1, \dots, x_n) = d$$

is an inhomogeneous polynomial equation (i.e., $d \neq 0$), then the determination of whether it has an integer solution is considerably more subtle than whether it has a rational solution. Perhaps the best single example of this is the proven nonexistence of an algorithm to determine whether a polynomial equation has an integral solution. In contrast, the question of whether a homogeneous polynomial equation must have a nontrivial solution is equivalent to the issue of whether polynomial equations must have rational solutions, and this is a wide open problem (although some experts think that it too will turn out to be algorithmically undecidable).

We have just surveyed the complete theory of homogeneous quadratic equations in any number of variables. One of the great miracles of the quadratic case is that, over \mathbb{Q} , the inhomogeneous problem reduces to the homogeneous problem, so that given a quadratic form $q(x_1, \dots, x_n)$, we now know how to determine the set of all integers (or even rational numbers) d such that

$$q(x_1, \dots, x_n) = d$$

has a *rational* solution. Two of the more striking consequences we derived from this Hasse-Minkowski theory were the following:

Fact 1: A quaternary quadratic form $q = ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2$ rationally represents all integers allowed by sign considerations:

- (i) if a, b, c, d are all positive, q represents all $d \in \mathbb{Q}^{>0}$;
- (ii) if a, b, c, d are all negative, q represents all $d \in \mathbb{Q}^{<0}$;
- (iii) otherwise q represents all $d \in \mathbb{Q}^\times$.

Fact 2: The three squares form $x^2 + y^2 + z^2$ rationally represents an integer d iff $d > 0$ and $d \neq 4^a(8k + 7)$.

These are strongly reminiscent of two results we stated but not did prove for integral quadratic forms, namely that $x_1^2 + x_2^2 + x_3^2 + x_4^2$ *integrally* represents all positive integers and $x_1^2 + x_2^2 + x_3^2 + x_4^2$ *integrally* represents all positive integers except precisely those of the form $4^a(8k + 7)$.

It seems clear that we cannot hope to recover general integral representability results from the Hasse-Minkowski theory. For instance, Fact 1 does not distinguish between the Four Squares form and a form in which a, b, c, d are all at least 2: such a form clearly cannot represent 1 integrally! Morally speaking, “local conditions”

of congruence and sign do not take into account the *size* of the coefficients of the quadratic form, whereas one clearly wants some or all of the coefficients to be small in order for a positive definite quadratic form to have a fighting chance at representing small positive integers.

So what to do?

Let us describe some of the ways that various mathematicians have reacted to this question over the years.

1. THE DAVENPORT-CASSELS LEMMA

Here is a beautiful observation which allows us to solve the representation problem for $x^2 + y^2 + z^2$:

Lemma 1. (*Davenport-Cassels*) *Let $q(x) = f(x_1, \dots, x_n) = \sum_{i,j=1}^n a_{ij}x_i x_j$ be a quadratic form with $a_{ij} = a_{ji} \in \mathbb{Z}$. We suppose **condition (DC)**: that for any $y = (y_1, \dots, y_n) \in \mathbb{Q}^n \setminus \mathbb{Z}^n$, there exists $x = (x_1, \dots, x_n) \in \mathbb{Z}^n$ such that*

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

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

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

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

Applying the hypothesis (DC) $x = \frac{x'}{d}$, there exists a $y \in \mathbb{Z}^n$ such that if $z = x - y$ we have

$$0 < |q(z)| < 1.$$

Now put

$$\begin{aligned} a &= y \cdot y - d, \\ b &= 2(dt - x' \cdot y), \\ T &= at + b, \\ X &= ax' + by. \end{aligned}$$

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

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

Indeed,

$$\begin{aligned} X \cdot X &= a^2(x' \cdot x') + ab(2x' \cdot y) + b^2(y \cdot y) = a^2 t^2 d + ab(2dt - b) + b^2(d + a) \\ &= d(a^2 t^2 + 2abt + b^2) = T^2 d. \end{aligned}$$

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

Indeed,

$$\begin{aligned} tT &= at^2 + bt = t^2(y \cdot y) - dt^2 + 2dt^2 - t(2x' \cdot y) \\ &= t^2(y \cdot y) - t(2x' \cdot y) + x' \cdot x' = (ty - x') \cdot (ty - x') = (-tz) \cdot (-tz) = t^2(z \cdot z). \end{aligned}$$

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

Remark 1: Suppose that the quadratic form q is anisotropic. Then condition (DC) is equivalent to the following more easily verified one: for all $x \in \mathbb{Q}^n$, there exists $y \in \mathbb{Z}^n$ such that $|q(x - y)| < 1$. Indeed, since $x \notin \mathbb{Z}^n$ and $y \in \mathbb{Z}^n$, $x - y \notin \mathbb{Z}^n$. In particular $x - y \neq (0, \dots, 0)$, so since q is anisotropic, necessarily $|q(x - y)| > 0$.

Remark 2: Lemma 1 has a curious history. So far as I know there is no paper of Davenport and Cassels (two eminent 20th century number theorists) which contains it: it is more folkloric. The attribution of this result seems to be due to J.-P. Serre in his influential 1970 text *A Course in Arithmetic*. More recently, André Weil pointed out that in a special case – indeed the case of $f(x) = x_1^2 + x_2^2 + x_3^2$, the one of most interest to us here – the result goes back to a 1912 paper of the amateur mathematician L. Aubry.

There is also more than the usual amount of variation in the hypotheses of this result. Serre’s text makes the additional hypothesis that f is positive definite – i.e., $x \neq 0 \implies f(x) > 0$. Many of the authors of more recent number theory texts that include this result follow Serre and include the hypothesis of positive definiteness. Indeed, when I first wrote these notes in 2006, I did so myself (and included a place-holder remark that I believed that this hypothesis was superfluous).¹ To get from Serre’s proof to ours requires only (i) inserting absolute values where appropriate, and (ii) noting that whenever we need $x \cdot y$ to be integral, we have an extra factor of 2 in the expression to make it so. The result is also stated and proved (in a mildly different way) in Weil’s text.

Remark 3: In the isotropic case, the stronger hypothesis $0 < |q(x - y)| < 1$ is truly necessary. Consider for instance $q(x, y) = x^2 - y^2$: we ask the reader to show that 2 is represented rationally but not integrally.

One might call a quadratic form **Euclidean** if it satisfies (DC). For example, the quadratic form $q(x, y) = x^2 - dy^2$ is Euclidean iff given rational numbers r_x, r_y , we can find integers n_x, n_y such that

$$(1) \quad |(r_x - n_x)^2 - d(r_y - n_y)^2| < 1$$

Since we know that we can find an integer within $\frac{1}{2}$ of any rational number (and that this estimate is best possible!), the quantity in question is at most $(\frac{1}{2})^2 + |d|(\frac{1}{2})$ if $d < 0$ and at most $\frac{d}{4}$ when $d > 0$. So the values of d for which (1) holds are precisely $d = -1, -2, 2, 3$. This should be a familiar list: these are precisely the values of d for which you proved that $\mathbb{Z}[\sqrt{d}]$ is a PID. Whenever $\mathbb{Z}[\sqrt{d}]$ is a PID, one can use Euclid’s Lemma to solve the problem of which primes (and in fact which integers, with more care) are integrally represented by $x^2 - dy^2$. The Davenport-Cassels Lemma allows for a slightly different approach: for these values of d , $x^2 - dy^2 = N$ has an integral solution iff it has a rational solution iff $x^2 - dy^2 - Nz^2 = 0$ is isotropic, which we can answer using Legendre’s Theorem.

Also $x^2 + y^2 + z^2$ satisfies the hypotheses of the Davenport-Cassels lemma: given

¹A notable exception is Lam’s 2005 text on quadratic forms, which states the result for anisotropic forms, simplified as in Remark 1.

rational numbers x, y, z , find integers n_1, n_2, n_3 at most $\frac{1}{2}$ a unit away, and then

$$(x - n_1)^2 + (x - n_2)^2 + (x - n_3)^2 \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} < 1.$$

Therefore the Hasse-Minkowski theory gives the three square theorem!

Note however that the Davenport-Cassels Lemma applies only to an extremely limited number of quadratic forms: e.g., it does not even apply to $x_1^2 + x_2^2 + x_3^2 + x_4^2$: take $x_1 = x_2 = x_3 = x_4 = \frac{1}{2}$. (This is not in itself so tragic, because, recall, one can easily deduce the Four Squares Theorem from the Three Squares Theorem.) We leave it as an exercise for the reader to find other quadratic forms to which the lemma applies.

2. A COUNTEREXAMPLE TO THE LOCAL-GLOBAL PRINCIPLE FOR REPRESENTABILITY BY QUADRATIC FORMS

In general we cannot hope that a local-global principle will tell us which integers can be represented. For instance, for “most” negative squarefree d , there are infinitely many primes p which are *not* of the form $x^2 - dy^2$ even though the equation $x^2 - dy^2 = p$ has congruential solutions.

Example: $x^2 + 17y^2 = 257$.

First we observe that this equation cannot have integral solutions. Indeed, we consider $257 - 17 \cdot 0^2$, $257 - 17 \cdot 1^2$, $257 - 17 \cdot 2^2$, $257 - 17 \cdot 3^2$, and none of these integers are perfect squares. If we took $|y| > 3$, then $257 - 17y^2 \leq 257 - 17 \cdot 16 = -15 < 0$.

Unfortunately it is not quite within the means of the theory we have developed to show that this equation has solutions modulo N for *all* N . But notice that there are no obstructions if we reduce modulo the “usual” values of N : going mod 257 we get the condition that $\left(\frac{-17}{257}\right)$ must be 1, and going mod 17 we get that $\left(\frac{257}{17}\right)$ must be 1. These conditions are easily seen to be equivalent to each other using quadratic reciprocity, and a Legendre symbol calculation shows that they both do hold. Moreover if we reduce modulo 16 we get the equation $x^2 + 1 \equiv 1 \pmod{16}$, which evidently does have a solution, $x \equiv 0 \pmod{16}$. It can be shown using elementary counting arguments that modulo any prime $p \neq 2, 17, 257$ there is always a solution. However, we must also show that there are solutions when N is an arbitrary prime *power* p^k . An important result called **Hensel’s Lemma** says that if an equation has solutions modulo a sufficiently large power of a prime, then it automatically has solutions modulo *all* powers of the prime. In the case at hand it turns out that modulo all odd primes already having a solution modulo p is enough to guarantee solutions modulo all p^k , whereas for $p = 2$ we need (in the case of quadratic forms with odd coefficients) to know – as we do – that we have a solution modulo 2^4 .

The above argument is couched in relatively modern language (Hensel’s theory dates from circa 1900), but the great number theorists of the early 1800’s had quite a good understanding of this phenomenon, albeit from a different perspective.

There is a notion of two quadratic forms being *locally equivalent* at p : this means

that one can be brought to the other by an invertible matrix M with rational entries and such that all entries of both M and M^{-1} have $\text{ord}_p \geq 0$. Similarly there is a much more classical notion of quadratic forms being equivalent at ∞ , which is just a simple sign condition. Then the general principle is that if

$$q(x_1, \dots, x_n) = N$$

has solutions everywhere locally, then there is some form q' which is everywhere locally equivalent to q and such that q' integrally represents N .

The collection of all equivalence classes of quadratic forms everywhere locally equivalent to q is called the **genus** of q . Then the local-global principle holds for $q(x_1, \dots, x_n) = N$ (for all N) iff the genus of q is the one element set $\{q\}$. This occurs for the three and four squares form, but is a rather rare condition among positive definite forms: there are, for instance, only a finite number of positive definite quaternary quadratic forms which are unique in their genus.

A fuller description of this “genus theory” of Lagrange, Legendre and Gauss would require a course in and of itself – it is closely related to, but not subsumed by, the more modern algebraic number theory than one invariably (and rightfully) meets in a more advanced course. Let us pass to the discussion of some more easily described modern developments.

3. APPROXIMATE LOCAL-GLOBAL PRINCIPLE

From now on we restrict to the case of positive-definite integral quadratic forms $q(x_1, \dots, x_n)$. For such a form, the equation

$$q(x_1, \dots, x_n) = N$$

can have at most finitely many integral solutions. Indeed, if we define $r_q(N)$ to be the number of solutions, then the summatory function

$$R_q(N) = \sum_{i=1}^N r_q(i)$$

is counting lattice points lying on or inside the ellipsoid $q(x_1, \dots, x_n) = N$ in n -dimensional Euclidean space. Recalling our previous study of this sort of problem, we know that there exists a constant V such that

$$R_q(N) \sim V \cdot N^{n/2},$$

so that the average value of $r_q(N)$ is asymptotically $N^{\frac{n}{2}-1}$.

To say that $q(x_1, \dots, x_n) = N$ has an integral solution is to say that $r_q(N) > 0$. It turns out to be a good strategy to exchange our problem for a seemingly harder problem: what can one say about the order of magnitude of $r_q(N)$?

One has the following theorem, thanks to the combined work of many leading mathematicians over a period of about 50 years:

Theorem 2. (Hecke, Eichler, Tartakowsky, Kloosterman, Deligne, ...) *Suppose $q(x_1, \dots, x_n)$ is positive definite and $n \geq 4$. There exists a decomposition*

$$r_q(N) = r_E(N) + r_C(N)$$

with the following properties:

- a) $r_E(N) > 0$ iff the equation $q(x_1, \dots, x_n) = N$ has solutions everywhere locally.
 b) There exist effectively computable positive constants C_1, C_2 (depending on q) such that:

$$r_E(N) > 0 \implies r_E(N) \geq C_1 N^{n/2-1}.$$

$$|r_C(N)| \leq C_2 d(N) N^{\frac{n}{4}-\frac{1}{2}}.$$

Here $d(N)$ is the divisor function, which recall, grows slower than any positive power of N . One can interpret this result as saying that a local-global principle for $r_q(N)$ holds *asymptotically*, with **almost square root error!**

The proof of this theorem requires lots of techniques from 20th century number theory, and in particular the introduction of objects which are a lot less elementary and quaint than quadratic polynomials with integer coefficients. Notably the proof first associates to a quadratic form a **modular form** – a certain especially nice kind of function of a complex variable – and the result follows from a bound on the coefficients of a power series expansion of this function. In particular, one uses results on the number of solutions to much more general systems of equations over finite fields established by fundamental work of Pierre Deligne in the 1970's (work that justly landed him the Fields Medal).

Corollary 3. *Let q be a positive-definite quadratic form in $n \geq 4$ variables. Then there exists N_0 such that if $N \geq N_0$, $q(x_1, \dots, x_n) = N$ satisfies the local-global principle (has integral solutions iff it has congruential solutions).*

Again, the theory of congruential solutions is sufficiently well-developed so as to enable one to determine (with some work, to be sure) precise conditions on N such that solutions exist everywhere locally. Therefore the corollary gives a method for solving the representation problem for integral quadratic forms in at least four variables: (i) explicitly compute the value of N_0 in the Corollary; (ii) explicitly compute the local conditions for solvability; (iii) check each of the finitely many values of N , $1 \leq N \leq N_0$ to see whether $q(x_1, \dots, x_n) = N$ has a solution.

Thus the representation problem is reduced to a finite calculation. Of course not all finite problems can be solved in a reasonable (or even unreasonable) amount of time in practice, so quite a lot of technique and ingenuity is necessary to apply this method. Here is a success story:

Theorem 4. *(Hanke, 2004) The quadratic form $x^3 + 3y^2 + 5z^2 + 7w^2$ integrally represents all positive integers except 2 and 22.*

This result was conjectured by M. Kneser in 1961.

Note that in Theorem 2 the number of variables has to be at least 4. When $n = 2$ or 3, the above corollary is false: we already mentioned this in the case of 2 variables, which is in some sense the hardest but also the best understood in terms of pure algebraic number theory. The case of ternary quadratic forms brings several new features and remains fascinatingly open. If you want to hear more, you will have to wait until 2008 and ask Prof. Hanke about it.

4. THE 15 AND 290 THEOREMS

The constants in Theorem 2 most definitely depend on the quadratic form q in question. A greater challenge is to prove results about integral representability that are in some sense independent of the particular quadratic form. For instance, a positive-definite quadratic form is said to be **universal** if it integrally represents every positive integer. (So the four squares form is universal.) The preceding section asserts the existence of a complicated procedure that can determine whether a given form is universal. Is there some easy way to determine whether a quadratic form is universal?

Indeed. In the 1990's Conway and Schneeberger proved the following:

Theorem 5. (*Fifteen theorem*) *A positive definite quadratic form with integral defining matrix integrally represents every positive integer iff it integrally represents the integers 1 through 15.*

Example: We will determine all positive integers d for which the form

$$x^2 + y^2 + z^2 + dw^2$$

is universal. We know that by taking $w = 0$ we can get every positive integer except those of the form $4^a(8k + 7)$; but since we need only go up to 15 it suffices to check whether we can represent 7. Let's check:

$$d = 1: 1^2 + 1^2 + 1^2 + 1 \cdot 1^2 = 7.$$

$$d = 2: 2^2 + 1^2 + 0^2 + 2 \cdot 1^2 = 7.$$

$$d = 3: 2^2 + 1^2 + 1^2 + 3 \cdot 1^2 = 7.$$

$$d = 4: 1^2 + 1^2 + 1^2 + 4 \cdot 1^2 = 7.$$

$$d = 5: 1^2 + 1^2 + 0^2 + 5 \cdot 1^2 = 7.$$

$$d = 6: 1^2 + 0^2 + 0^2 + 6 \cdot 1^2 = 7.$$

$$d = 7: 0^2 + 0^2 + 0^2 + 7 \cdot 1^2 = 7.$$

We cannot represent 7 if $d \geq 8$: taking $w \neq 0$ would make the form too large.

In fact, let us consider the problem of which quadratic forms

$$q(x_1, x_2, x_3, x_4) = ax_1^2 + bx_2^2 + cx_3^2 + dx_4^2$$

with $a \leq b \leq c \leq d$ represent all positive integers. A case-by-case analysis shows that in order for the integers 1, 2, 3 and 5 to all be represented, we need (a, b, c) to be one of: (1, 1, 1), (1, 1, 2), (1, 1, 3), (1, 2, 2), (1, 2, 3), (1, 2, 4), (1, 2, 5). As it happens, no ternary quadratic form can represent all positive integers. In the cases at hand, the smallest exceptions are (as you can readily check):

$$x^2 + y^2 + z^2 \text{ does not represent } 7.$$

$$x^2 + y^2 + 2z^2 \text{ does not represent } 14.$$

$$x^2 + y^2 + 3z^2 \text{ does not represent } 6.$$

$$x^2 + 2y^2 + 2z^2 \text{ does not represent } 7.$$

$$x^2 + 2y^2 + 3z^2 \text{ does not represent } 10.$$

$$x^2 + 2y^2 + 4z^2 \text{ does not represent } 14.$$

$$x^2 + 2y^2 + 5z^2 \text{ does not represent } 10.$$

Now one can go through a similar analysis for the other 6 cases as we did for the first case, and determine a complete list of diagonal positive definite quaternary universal quadratic forms: there are precisely 54 of them.² In fact this investigation was originally done by S. Ramanujan in 1917, except that not having the 15 theorem he was forced to come up with “empirical” (i.e., conjectural) rules for which integers are represented by the above ternary quadratic forms, so that he did not supply proofs for his results.

Remark 4: Given the stories that have been told about Ramanujan and his unearthly intuition, it is interesting to remark that his paper lists a 55th universal quadratic form: $x^2 + 2y^2 + 5z^2 + 5w^2$. Ironically, this form does not represent 15, as Dickson observed ten years later.

The 15 theorem was discovered in a graduate seminar that Conway was teaching at Princeton, in which Schneeberger was an attending student. The original proof was quite computationally onerous, and it was never written down. Indeed, by the time Manjul Bhargava became a graduate student at Princeton and heard about the theorem, some of the details of the proof had been forgotten.

Manjul was doubly stunned by this: that such a wonderful theorem could have been discovered, and also that it had met such a disappointing fate. He found a new proof of the 15 theorem which is, truly, one of the most beautiful mathematical arguments I have ever seen. It quite cleverly manages to avoid any serious computations. In fact he proved the following generalization:

Theorem 6. (*Manjul’s Master Theorem*) *Let S be any subset of the positive integers. There exists a finite subset S_0 of S such that a positive definite integer-matrix quadratic form represents all integers in S iff it represents all integers in S_0 .*

Example: Taking S to be the prime numbers, one may take S_0 to be the primes less than or equal to 73.

The proof gives an algorithm for determining S_0 , but whether or not it is practical seems to depend very much on the choice of S : it gets much harder if S does not contain several very small integers.

Indeed, let us now recall that we have been saying “integer matrix” quadratic forms for the last few results, but a quadratic form is represented by a polynomial with integer coefficients iff its defining matrix satisfies the slightly weaker condition that its diagonal entries are integers and its off-diagonal entries are half-integers (e.g. $q(x, y) = xy$). However, if q is any integral quadratic form, then the matrix entries of $2q$ are certainly integers, and q represents an integer N iff $2q$ represents $2N$. Thus, applying Manjul’s Master Theorem to the subset of positive *even* integers, one deduces the existence of an integer N_0 such that if a positive-definite integral matrix represents every $N \in \{1, \dots, N_0\}$ then it represents every positive integer.

²It can now be told that I put this as an extra credit problem on the final exam. Moreover, I hinted that I might do so, and in fact there was a student who practiced this type of calculation and was able to give the complete solution!

Already in Conway's course it was suggested that N_0 could be taken to be 290. However, the calculations necessary to establish this result were Herculean: Manjul's method requires one to show that each of a set of about 6,000 quadratic forms is universal. Some of these forms can be proven universal in relatively slick and easy ways, but about 1,000 of them are seriously hard. So Manjul enlisted the help of Jonathan Hanke, and after several years of intense work (including extremely intensive and carefully checked computer calculations), they were able to show the following result.

Theorem 7. (*Bhargava-Hanke 290 Theorem*) *If a positive-definite integral quadratic form represents each of:*

1, 2, 3, 5, 6, 7, 10, 13, 14, 15, 17, 19, 21, 22, 23, 26, 29, 30, 31, 34, 35, 37, 42, 58, 93, 110, 145, 203, 290,
then it represents all positive integers.