REPRESENTATIONS OF INTEGERS BY QUADRATIC FORMS

PETE L. CLARK

As we have seen, if

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

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 $q(x_1, \ldots, x_n)$, we now know how to determine the set of all integers (or even rational numbers) d such that

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

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

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

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

Proof. For $x, y \in \mathbb{Q}^n$, put $x \cdot y := \frac{1}{2}(q(x + y) - q(x) - q(x))$. Then $(x, y) \mapsto x \cdot y$ is bilinear and $x \cdot x = q(x)$. Note that for $x, y \in \mathbb{Z}^n$, we need not have $x \cdot y \in \mathbb{Z}$, but certainly we have $2(x \cdot y) \in \mathbb{Z}$. Our computations below are parenthesized so as to emphasize this integrality property.
Let $d \in \mathbb{Z}$, and suppose that there exists $x \in \mathbb{Q}^n$ such that $q(x) = d$. Equivalently, there exists $t \in \mathbb{Z}$ and $x' \in \mathbb{Z}^n$ such that $t^2 d = x' \cdot x'$. We choose x' and t such that $|t|$ is minimal, and it is enough to show that $|t| = 1$.

Applying the hypothesis (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

$$a = y \cdot y - d,$$
$$b = 2(dt - x' \cdot y),$$
$$T = at + b,$$
$$X = ax' + by.$$

Then $a, b, T \in \mathbb{Z}$, and $X \in \mathbb{Z}^n$.
Claim: $X \cdot X = T^2 d$.
Indeed,

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

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

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

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

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 $x - y \neq (0, \ldots, 0)$, so since q is anistropic, 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 belived 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

$$|(r_x - n_x)^2 - d(r_y - n_y)^2| < 1 \tag{1}$$

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

[1] A 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. The Three Squares Theorem

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

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

2.1. Proof of the Three Squares Theorem.

The strategy of proof is as follows: the quadratic form $q(x, y, z) = x^2 + y^2 + z^2$ satisfies the hypotheses of the Davenport-Cassels Lemma (Lemma 1) of the previous section. Therefore, to show that an integer n is a sum of three integer squares it suffices to show the *a priori* much weaker assertion that it is a sum of three rational squares. It is traditional to establish the latter assertion using the Hasse-Minkowski theory of quadratic forms over $\mathbb{Q}$ in terms of quadratic forms over the p-adic numbers. But since in these notes we have not even officially introduced the p-adic numbers, we need to do something more elementary. Instead we follow the second half of a short and clever argument of J. Wójcik, which succeeds in replacing the Hasse-Minkowski Theory with an appeal to (i) Fermat's Two Squares Theorem, (ii) Legendre's Theorem on homogeneous ternary quadratic equations and (iii) Dirichlet's Theorem on Primes in Arithmetic Progressions.[2]

The following result takes care of the implication (i) $\implies$ (ii) of Theorem 2 (the easy direction!).

Lemma 3. *Let n be an integer of the form $4^a(8k+7)$ for some $a \in \mathbb{N}$, $k \in \mathbb{Z}$. Then n is* not *the sum of three rational squares.*

Proof. Step 0: Suppose on the contrary that $4^a(8k+7)$ is a sum of three rational squares. We may take our rational numbers to have a common deminator $d > 0$ and thus

$$\left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2 + \left(\frac{z}{d}\right)^2 = 4^a(8k+7).$$

Clearing denominators, we get

$$x^2 + y^2 + z^2 = d^2 4^a(8k+7).$$

[2]That we have indeed given complete proofs of all of these theorems previously is something of a happy coincidence: I did not learn about W ojcik's argument until 2011, more than four years after these notes were first written.

Write $d = 2^b d'$ with d' odd. Since $1^2, 3^2, 5^2, 7^2 \equiv 1 \pmod 8$, we find that $d'^2 \equiv 1 \pmod 8$ and thus

$$d^2 4^a(8k+7) = (2^b)^2(d'^2)4^a(8k+7) = 4^{a+b}(8k'+7).$$

In other words, to show that no integer of the form $4^a(8k+7)$ is a sum of 3 rational squares, it suffices to show that no integer of the form $4^a(8k+7)$ is a sum of three integral squares. So let us now show this.
Step 1: We observe that $x^2 + y^2 + z^2 \equiv 7 \pmod 8$ has no solutions. Indeed, since the squares mod 8 are $0, 1, 4$, this is a quick mental calculation. (In particular this disposes of the $a = 0$ case.)
Step 2: we observe that if $n \equiv 0, 4 \pmod 8$ then the congruence

$$x^2 + y^2 + z^2 \equiv n \pmod 8$$

has no *primitive solutions*, i.e., no solutions in which at least one of x, y, z is odd. Indeed, since the squares mod 8 are $0, 1, 4$, so in particular the only odd square is 1. Since 4 and 0 are both even, if x, y, z are not all even, then exactly one two of them must be odd, say x and y, so $x^2 \equiv y^2 \equiv 1 \pmod 8$ and thus $z^2 \equiv 4 - 2 \pmod 8$ or $z^2 \equiv 8 - 2 \pmod 8$, and neither 2 nor 6 is a square modulo 8.
Step 3: Now suppose that there are integers x, y, z such that $x^2+y^2+z^2 = 4^a(8k+7)$. If $a = 0$ then by Step 1 reducing modulo 8 gives a contradiction. If $a = 1$, then $4^a(8k+7) \equiv 4 \pmod 8$, so by Step 2 any representation $x^2 + y^2 + z^2 = 4(8k+7)$ must have x, y, z all even, and then dividing by 4 gives $(\frac{x}{2})^2+(\frac{y}{2})^2+(\frac{z}{2})^2 = (8k+7)$, a contradiction. If $a \geq 2$, then $4^a(8k+7) \equiv 0 \pmod 8$, and again by Step 2 in any representation $x^2 + y^2 + z^2 = 4^a(8k+7)$ we must have x, y, z all even. Thus writing $x = 2X$, $y = 2Y$, $z = 2Z$ we get an integer representation $X^2 + Y^2 + Z^2 = 4^{a-1}(8k+7)$. We may continue in this way until we get a representation of $4(8k+7)$ as a sum of three integral squares, which we have just seen is impossible. □

Lemma 4. *Suppose that every squarefree positive integer $n \not\equiv 7 \pmod 8$ is a sum of three integral squares. Then every positive integer $n \neq 4^a(8k+7)$ is a sum of three integral squares.*

Proof. Let n be a positive integer which is *not* of the form $4^a(8k+7)$. As for any positive integer, we may write n as $n = 2^a n_1^2 n_2$, where $a \geq 0$, n_1 is odd and n_2 is odd and squarefree.
Case 1: $0 \leq a \leq 1$, $n_2 \not\equiv 7 \pmod 8$. Then $2^a n_2$ is squarefree and not $7 \pmod 8$, so by assumption there exist $x, y, z \in \mathbb{Z}$ such that $x^2 + y^2 + z^2 = 2^a n_2$, and thus $(n_1 x)^2 + (n_1 y)^2 + (n_1 z)^2 = 2^a n_1^2 n_2 = n$.
Case 2: $n_2 \not\equiv 7 \pmod 8$. In such a case n is of the form $(2^b)^2$ times an integer n of the type considered in Case 1. Since such an integer n is a sum of three integreal squares, so is any square times n.
Case 3: $n_2 \equiv 7 \pmod 8$. For n not to be of the form $4^a(8k+7)$, the power of a must be odd; in other words, we may write n as a square times $2n_2$ where n_2 is squarefree and of the form $8k_+7$. Thus $2n_2$ is squarefree and not of the form $8k+7$, so by assumption $2n_2$ is a sum of three squares, hence so is n. □

Lemma 5. *Let $m \in \mathbb{Z}^+$, $n \equiv 3 \pmod 8$, and write $m = p_1 \cdots p_r$. Then the number of i such that $p_i \equiv 3, 5 \pmod 8$ is even.*

Exercise: Prove Lemma 5. (Suggestion: one way to do it would be by using the evaluation of the Jacobi symbol $\left(\frac{-2}{m}\right)$. But a completely elementary proof is also

possible.)

Since $x^2 + y^2 + z^2$ rationally represents an integer n iff it integrally represents an integer n, the following result completes the proof of Theorem 2.

Proposition 6. *Let n be a squarefree integer, $n \not\equiv 7 \pmod 8$. Then n is a sum of three rational squares.*

Proof. To fix ideas we will first give the argument under certain additional congruence conditions and then explain how to modify it to deal with the other cases. Filling in the details for these latters cases would be a good exercise for the interested reader.
Case 1: Let us suppose that $m = p_1 \cdots p_r$ is squarefree and $m \equiv 1 \pmod 4$. Thus each p_i is odd and the number of $p_i \equiv 3 \pmod 4$ is even. By Dirichlet's Theorem on Primes in Arithmetic Progressions, there is a prime number q such that
• $\left(\frac{q}{p_i}\right) = \left(\frac{-1}{p_i}\right)$ for all $1 \leq i \leq p_i$ and
• $q \equiv 1 \pmod 4$.
(Indeed, each of the first conditions restricts q to a nonempty set of congruence classes modulo the distinct odd primes p_i, whereas the last condition is a condition modulo a power of 2. By the Chinese Remainder Theorem this amounts to a set of congruence conditions modulo $4p_1 \cdots p_r$ and all of the resulting congruence classes are relatively prime to $4p_1 \cdots p_r$, so Dirichlet's Theorem applies.)
It follows that for all $1 \leq i \leq r$,

$$\left(\frac{-q}{p_i}\right) = \left(\frac{-1}{p_i}\right)\left(\frac{q}{p_i}\right) = 1,$$

and

$$\left(\frac{m}{q}\right) = \left(\frac{p_1}{q}\right) \cdots \left(\frac{p_r}{q}\right) = \left(\frac{q}{p_1}\right) \cdots \left(\frac{q}{p_r}\right) = \left(\frac{-1}{p_1}\right) \cdots \left(\frac{-1}{p_r}\right) = 1.$$

The last equality holds because the number of factors of -1 is the number of primes $p_i \equiv 3 \pmod 4$, which as observed above is an even number.
since $-q$ is a square modulo each of the distinct primes p_i, by the Chinese Remainder Theorem it is also a square modulo $m = p_1 \cdots p_r$. Therefore by the Chinese Remainder Theorem there is an integer x such that

$$x^2 \equiv -q \pmod m$$

$$x^2 \equiv m \pmod q.$$

But according to Legendre's Theorem, these are precisely the congruence conditions necessary and sufficient for the homogeneous equation

$$qu^2 + z^2 - mt^2 = 0$$

to have a solution in integers (u, z, t), not all zero. Indeed, we must have $t \neq 0$, for otherwise $qu^2 + z^2 = 0 \implies u = z = 0$. Moreover, since $q \equiv 1 \pmod 4$, by Fermat's Two Squares Theorem there are $x, y \in \mathbb{Z}$ such that $qu^2 = x^2 + y^2$. Therefore

$$mt^2 - z^2 = qu^2 = x^2 + y^2,$$

so

$$m = \left(\frac{x}{t}\right)^2 + \left(\frac{y}{t}\right)^2 + \left(\frac{z}{t}\right)^2$$

and m is a sum of three rational squares, completing the proof in this case.
Case 2: Suppose $m = 2m_1 = 2p_1 \cdots p_r$ with $m_1 = p_1 \cdots p_r$ squarefree and odd. In this case we may proceed exactly as above, except that we require $q \equiv 1 \pmod 8$.
Case 3: Suppose $m = p_1 \cdots p_r$ is squarefree and $m \equiv 3 \pmod 8$. By Lemma 5, the number of prime divisors p_i of m which are either 5 or 7 modulo 8 is even. By Dirichlet's Theorem there exists a prime q such that

- $\left(\frac{q}{p_i}\right) = \left(\frac{-2}{p_i}\right)$ for all $1 \leq i \leq p_i$ and
- $q \equiv 5 \pmod 8$.

It follows that for all $1 \leq i \leq r$,

$$\left(\frac{-2q}{p_i}\right) = \left(\frac{-2}{p_i}\right)\left(\frac{q}{p_i}\right) = 1,$$

and

$$\left(\frac{m}{q}\right) = \left(\frac{p_1}{q}\right) \cdots \left(\frac{p_r}{q}\right) = \left(\frac{q}{p_1}\right) \cdots \left(\frac{q}{p_r}\right) = \left(\frac{-2}{p_1}\right) \cdots \left(\frac{-2}{p_r}\right) = 1.$$

The last equality holds because the number of factors of -1 is the number of primes $p_i \equiv 5, 7 \pmod 8$, which as observed above is an even number.
Therefore there is an integer x such that

$$x^2 \equiv -2q \pmod m$$
$$x^2 \equiv m \pmod q,$$

so by Legendre's Theorem the equation

$$2qu^2 + z^2 - mt^2 = 0$$

has a solution in integers (u, z, t) with $t \neq 0$. Since $q \equiv 1 \pmod 4$, there are $x, y \in \mathbb{Z}$ such that $2qu^2 = x^2 + y^2$, so

$$mt^2 - z^2 = 2qu^2 = x^2 + y^2,$$

and thus once again

$$m = \left(\frac{x}{t}\right)^2 + \left(\frac{y}{t}\right)^2 + \left(\frac{z}{t}\right)^2.$$

□

2.2. **Some applications of the Three Squares Theorem.**

Knowing exactly which integers are represented by $x^2 + y^2 + z^2$ turns out to be a powerful weapon for analyzing representation of integers by certain quaternary quadratic forms.

Proposition 7. *The three squares theorem implies the four squares theorem.*

Proof. In order to show the Four Squares Theorem it suffices to show that every squarefree positive integer m is a sum of four integer squares. By the Three Squares Theorem, m is even a sum of three integer squares unless $m = 8k + 7$. But if $m = 8k+7$, then $m-1 = 8k+6$. Now $\mathrm{ord}_2(8k+6) = 1$, so $8k+6$ is not of the form $4^a(8k + 7)$, hence $8k + 6 = x^2 + y^2 + z^2$ and $m = 8k + 7 = x^2 + y^2 + z^2 + 1^2$. □

More generally:

Theorem 8. *For any $1 \leq d \leq 7$, the quadratic form $q = x^2 + y^2 + z^2 + dw^2$ integrally represents all positive integers.*

Proof. As above it is enough to show that q represents all squarefree positive integers. Moreover, if $m \neq 8k+7$ is a squarefree positive integer then m is represented already by $x^2+y^2+z^2$ so certainly by q. It remains to dispose of $m = 8k+7$.
Case 1: Suppose $d = 1, 2, 4, 6$. Then $m - d \cdot 1^2 = m - d$ is:
• $m - 1 = 8k + 6$, if $d = 1$. This is a sum of 3 squares.
• $m - 2 = 8k + 5$, if $d = 2$. This is a sum of 3 squares.
• $m - 4 = 8k + 3$, if $d = 3$. This is a sum of 3 squares.
• $m - 5 = 8k + 2$, if $d = 5$. This is a sum of 3 squares.
• $m - 6 = 8k + 1$, if $d = 6$. This is a sum of 3 squares.
Case 2: If $d = 3$, then

$$m - d \cdot 2^2 = m - 12 = 8k - 5 = 8(k-1) + 3.$$

Thus, so long as $m - 12$ is positive, it is a sum of three squares. We need to check separately that positive integers less than 12 are still represented by q, but this is easy: the only one which is not already a sum of 3 squares is $7 = 2^2+0^2+0^2+3\cdot 1^2$.
Case 3: If $d = 7$, then

$$m - d \cdot 2^2 = m - 28 = 8(k-3) + 5.$$

Thus, so long as $m - 28$ is positive, it is a sum of three squares. Again we must separately check that positive integers less than 28 are represented by q, and again this comes down to checking 7: $7 = 0^2 + 0^2 + 0^2 + 7 \cdot 1^2$. □

If we are looking for quaternary quadratic forms $q = x^2 + y^2 + z^2 + dw^2$ which represent *all* positive integers, then we have just found all of them: if $d > 7$, then such a q cannot integrally represent 7. Nevertheless we can still use the Gauss-Legendre Theorem to analyze these forms. For instance.

Proposition 9. *For a positive integer n, TFAE:*
(i) There are integers x, y, z, w such that $n = x^2 + y^2 + z^2 + 8w^2$.
(ii) $n \not\equiv 7 \pmod 8$.

Proof. (i) $\implies$ (ii): For any integers x, y, z, w, reducing $n = x^2 + y^2 + z^2 + 8w^2$ modulo 8 gives $n \equiv x^2 + y^2 + z^2 \pmod 8$, and we already know that this has no solutions when $n \equiv 7 \pmod 8$.
(ii) $\implies$ (i): Write $n = 2^a m$ with m odd. If m is not of the form $8k+7$ then both m and $2m$ are sums of three integer squares, and since n is an even power of 2 times either m or $2m$, n must be a sum of three intege squares. So we are reduced to the case $n = 2^a(8k+7)$ with $a \geq 1$. If $a = 1$ then $\operatorname{ord}_2(n) = 1$ and again n is a sum of three integer squares. Suppose $a = 2$, so $n = 32k + 28$ and thus $n - 8 \cdot 1^2 = 32k + 20 = 4(8k+5)$ is of the form $x^2 + y^2 + z^2$ and thus $n = x^2 + y^2 + z^2 + 8w^2$. If $a \geq 3$ is odd, then n is a sum of three squares. If $a \geq 4$ is even, then $n = (2^{\frac{a-2}{2}})^2(4 \cdot (8k+7))$ is a square times an integer represented by q, so n is also represented by q. □

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

3. Approximate local-global principle

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

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

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 $q(x_1, \ldots, x_n) = N$ 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 $q(x_1, \ldots, x_n) = N$ 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 10. *(Hecke, Eichler, Tartakowsky, Kloosterman, Deligne, ...) Suppose $q(x_1, \ldots, x_n)$ 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 $q(x_1, \ldots, x_n) = N$ 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 11. *Let q be a positive-definite quadratic form in $n \geq 4$ variables. Then there exists N_0 such that if $N \geq N_0$, $q(x_1, \ldots, x_n) = N$ 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 $q(x_1, \ldots, x_n) = N$ 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 12. *(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 10 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 10 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 Schneeburger proved the following:

Theorem 13. *(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:

$d = 1$: $1^2 + 1^2 + 1^2 + 1 \cdot 2^2 = 7$.
$d = 2$: $2^2 + 1^2 + 0^2 + 2 \cdot 1^2 = 7$.
$d = 3$: $2^2 + 1^2 + 1^2 + 3 \cdot 1^2 = 7$.
$d = 4$: $1^2 + 1^2 + 1^2 + 4 \cdot 1^2 = 7$.
$d = 5$: $1^2 + 1^2 + 0^2 + 5 \cdot 1^2 = 7$.
$d = 6$: $1^2 + 0^2 + 0^2 + 6 \cdot 1^2 = 7$.
$d = 7$: $0^2 + 0^2 + 0^2 + 7 \cdot 1^2 = 7$.

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):

$x^2 + y^2 + z^2$ does not represent 7.
$x^2 + y^2 + 2z^2$ does not represent 14.
$x^2 + y^2 + 3z^2$ does not represent 6.
$x^2 + 2y^2 + 2z^2$ does not represent 7.
$x^2 + 2y^2 + 3z^2$ does not represent 10.
$x^2 + 2y^2 + 4z^2$ does not represent 14.
$x^2 + 2y^2 + 5z^2$ 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.[3] 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 Schneeburger 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

[3]It 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!

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 14. *(Bhargava's Master Theorem) Let $S \subset \mathbb{Z}^+$. 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, Bhargava showed that 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 $N \in \{1, \ldots, N_0\}$ then it represents every positive integer.

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 15. *(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.