

GETTING INTEGER SOLUTIONS FROM RATIONAL ONES

DAVID SAVITT

With a simple example, we can illustrate the difficulties of passing from *rational* solutions of a quadratic Diophantine equation to *integer* solutions. Consider the equations

$$x^2 + y^2 = N$$

and

$$x^2 + 4y^2 = N.$$

Evidently the first has a rational solution if and only if the second does: for if (x, y) is a solution of the first, then $(x, y/2)$ is a solution of the second, and conversely. On the other hand, to say that the second equation has a solution with x and y integers amounts to saying that the first equation has a solution with at least one of x and y even, in other words, that $N \not\equiv 2 \pmod{4}$. Thus, for the second equation to have an integer solution, we need to impose not only the usual local conditions that primes which are $3 \pmod{4}$ divide N an even number of times, but also the additional condition that $N \not\equiv 2 \pmod{4}$ – in other words, that 2 divides N either not at all or at least twice.

For larger coefficients n of y^2 , the problems passing from rational to integer solutions become even more subtle, to the point where congruence conditions cannot completely describe the integers represented by $x^2 + ny^2$. For more on the sort of math that goes into this, see the excellent book by David Cox, “Primes of the form $x^2 + ny^2$ ”. (Highly suggested, but very mature subject matter. Parental guidance recommended!)

In some cases, we are fortunate in our ability to pass from rational solutions to integer solutions. We now provide a result which will help us in a few cases.

Theorem 0.1 (Davenport-Cassels). *Let A be a k -by- k symmetric matrix with integer entries, and define*

$$f(X_1, \dots, X_k) = (X_1 \ \dots \ X_k) A \begin{pmatrix} X_1 \\ \vdots \\ X_k \end{pmatrix}.$$

(For example, if A is the 3-by-3 matrix

$$\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix}$$

then

$$f(X_1, X_2, X_3) = (X_1 \ X_2 \ X_3) \begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \\ 1 & 1 & 0 \end{pmatrix} \begin{pmatrix} X_1 \\ X_2 \\ X_3 \end{pmatrix} = X_1^2 + 2X_1X_3 + X_2^2 + 2X_2X_3.$$

Suppose the function f is positive definite, i.e. $f(X_1, \dots, X_k) \geq 0$ with equality if and only if $X_1 = \dots = X_k = 0$. Suppose also that for every $(c_1, \dots, c_k) \in \mathbb{Q}^k$ (in other words, (c_1, \dots, c_k) is a k -tuple of rational numbers) there exists a k -tuple $(N_1, \dots, N_k) \in \mathbb{Z}^k$ so that $f(c_1 - N_1, \dots, c_k - N_k) < 1$. Then if the equation $f(X_1, \dots, X_k) = n$ with n an integer has a rational solution, it also has an integer solution.

As an example, let

$$A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

so that $f(X_1, X_2, X_3) = X_1^2 + X_2^2 + X_3^2$ and f is plainly positive definite. Given (c_1, c_2, c_3) , let N_i be the integer nearest to c_i . Then $|c_i - N_i| \leq 1/2$, so $f(c_1 - N_1, c_2 - N_2, c_3 - N_3) \leq (1/2)^2 + (1/2)^2 + (1/2)^2 < 1$ and f satisfies the hypotheses of the theorem. Hence, according to the theorem, every integer that is representable as the sum of three

rational squares is also representable as the sum of three integer squares. An analogous choice of A would evidently prove the same statement for the sum of two squares. Similar for the quadratic form $x^2 + 2y^2$ as well.

However, for *four* squares, the theorem can't help us, because then $f(1/2, 1/2, 1/2, 1/2) = 1 \not\leq 1$. In this case, there's a trick. We now know that an integer is the sum of three integer squares if and only if it is not of the form $4^a(8b + 7)$ for integers a, b . So for any n either n or $n - 1$ is the sum of three squares, and therefore any n is the sum of four squares! We even have the extra information that one of these squares can be taken to be 0 or 1. As a side note, using modular forms, one can prove a beautiful result on the number of different ways of representing an integer as the sum of four squares.

I still owe you a proof of the Davenport-Cassels theorem above. Here we go:

Proof. Suppose $f(c_1, \dots, c_k) = n$. Let D be the common denominator of the c_i 's. Then Dc_1, \dots, Dc_k is a k -tuple of integers with the property that $f(Dc_1, \dots, Dc_k) = D^2n$. Let t be the smallest integer so that there exist integers x_1, \dots, x_k with $f(x_1, \dots, x_k) = t^2n$.

By the preceding paragraph, we have $t \leq D$; we wish to prove $t = 1$. The hypotheses of the theorem guarantee that there exists a k -tuple of integers (N_1, \dots, N_k) with

$$f\left(\frac{x_1}{t} - N_1, \dots, \frac{x_k}{t} - N_k\right) < 1.$$

Let $z_i = \frac{x_i}{t} - N_i$. If $z_i = 0$ for all i , we're done, so assume not. Now assign

$$\begin{aligned} \Delta &= (x_1 \quad \cdots \quad x_k) A \begin{pmatrix} N_1 \\ \vdots \\ N_k \end{pmatrix}, \\ a &= f(N_1, \dots, N_k) - n, \\ b &= 2(nt - \Delta), \\ t' &= at + b, \\ x'_i &= ax_i + bN_i. \end{aligned}$$

One calculates

$$\begin{aligned} f(x'_1, \dots, x'_k) &= a^2 f(x_1, \dots, x_k) + 2ab\Delta + b^2 f(N_1, \dots, N_k) \\ &= a^2 t^2 n + ab(2nt - b) + b^2(n + a) \\ &= n(a^2 t^2 + 2abt + b^2) \\ &= (t')^2 n \end{aligned}$$

and

$$\begin{aligned} tt' &= at^2 + bt \\ &= t^2 f(N_1, \dots, N_k) - nt^2 + 2nt^2 - 2t\Delta \\ &= t^2 f(N_1, \dots, N_k) - 2t\Delta + f(x_1, \dots, x_k) \\ &= f(x_1 - tN_1, \dots, x_k - tN_k) \\ &= t^2 f(z_1, \dots, z_k). \end{aligned}$$

Hence $0 < t' = tf(z_1, \dots, z_k) < t$, contradicting the minimality of t' . This proves the theorem. \square

This proof is taken directly from "A Course in Arithmetic" by J.-P. Serre.