RC23605 (W0505-077) May 11, 2005
Mathematics

IBM Research Report

A Diophantine Equation - Sums of Squares

Don Coppersmith
IBM Research Division
Thomas J. Watson Research Center
P.O. Box 218
Yorktown Heights, NY 10598

A DIOPHANTINE EQUATION - SUMS OF SQUARES

Don Coppersmith

Mathematical Sciences Department, IBM T.J.Watson Research Center, Yorktown Heights, NY 10598, USA

dcopper@us.ibm.com

Abstract

Given positive integers a, b, c, we solve the diophantine equation $a(x_1^2+x_2^2)+b(x_3^2+x_4^2)+c(x_5^2+x_6^2)=abc$.

The following Diophantine equation was inspired by a question of Poo-Sung Park [Par].

Theorem 1 Given positive integers a, b, c, there exist integers $x_1, \ldots, x_6$ satisfying:

$$a(x_1^2+x_2^2)+b(x_3^2+x_4^2)+c(x_5^2+x_6^2)=abc.$$

Proof. We can assume that a, b, c are squarefree and pairwise relatively prime, in light of the following two reductions:

Reduction 1: Suppose a, b, c are not pairwise relatively prime. Say $p|\gcd(b,c)$. Set $a'=ap$, $b'=b/p$, $c'=c/p$. Solve

$$a'(y_1^2+y_2^2)+b'(y_3^2+y_4^2)+c'(y_5^2+y_6^2)=a'b'c'$$

Set $x_1=py_1$, $x_2=py_2$, and $x_i=y_i, i=3,4,5,6$, and verify that $\{x_i\}$ solves the original problem.

Reduction 2: Suppose the coefficients are not squarefree. Suppose $p^2|c$. Set $a'=a$, $b'=b$, $c'=c/p^2$, and solve

$$a'(y_1^2+y_2^2)+b'(y_3^2+y_4^2)+c'(y_5^2+y_6^2)=a'b'c'$$

Then set $x_i=py_i, i=1,2,3,4$, and $x_5=y_5$ and $x_6=y_6$ to solve the original problem.

In each case the reduced problem has smaller product abc, so that after finitely many steps we reach a point where no further reductions are possible. At this point, each prime p divides at most one of the coefficients a, b, c.

Suppose $p|c$. We know that the sums of squares d^2+e^2 (where d, e are arbitrary integers) achieve each nonzero residue modulo p. In particular, since neither a, b is divisible by p, there are integers d, e, not both divisible by p, satisfying

$$d^2 + e^2 = -b/a \bmod p.$$

Calculate that for any $\{x_i\}$ satisfying the following two linear equations:

$$dx_1 + ex_2 - (d^2 + e^2)x_3 = 0 \bmod p$$

$$ex_1 - dx_2 - (d^2 + e^2)x_4 = 0 \bmod p$$

we have

$$p|a(x_1^2 + x_2^2) + b(x_3^2 + x_4^2)$$

and hence (since $p|c$)

$$p|a(x_1^2 + x_2^2) + b(x_3^2 + x_4^2) + c(x_5^2 + x_6^2).$$

The set of integer lattice points $(x_1, x_2, x_3, x_4, x_5, x_6)$ satisfying these two conditions forms a lattice, which has density $1/p^2$; that is, one of every p^2 integer lattice points satisfies both equations.

Write the corresponding pair of equations for each p dividing a, b or c. The set of integer lattice points satisfying all such equations again forms a lattice, with density $1/\prod p^2 = 1/(abc)^2$. For each such point $(x_1, \ldots, x_6)$, the sum $a(x_1^2 + x_2^2) + b(x_3^2 + x_4^2) + c(x_5^2 + x_6^2)$ is divisible by each prime p dividing abc, so we get

$$abc|a(x_1^2 + x_2^2) + b(x_3^2 + x_4^2) + c(x_5^2 + x_6^2).$$

Dilate the lattice along the six coordinate directions by factors $(\sqrt{a}, \sqrt{a}, \sqrt{b}, \sqrt{b}, \sqrt{c}, \sqrt{c})$, respectively. Now we have a lattice L with density $1/(abc)^3$, that is, one point per $(abc)^3$ six-dimensional volume.

Hermite's constant $\gamma_6 = (64/3)^{1/6} < 1.67$ assures us that there is a nonzero element w of this lattice L whose squared Euclidean length is at most $\gamma_6(\det L)^{2/6} < 1.67abc$; see [Wei1]. This element w is of the form $w = (x_1\sqrt{a}, x_2\sqrt{a}, x_3\sqrt{b}, x_4\sqrt{b}, x_5\sqrt{c}, x_6\sqrt{c})$, with x_i integers, not all zero. The squared Euclidean length of w is

$$M = a(x_1^2 + x_2^2) + b(x_3^2 + x_4^2) + c(x_5^2 + x_6^2).$$

By construction M is a multiple of each p dividing abc, so M is a multiple of abc. M is nonzero because w is nonzero. $M < 1.67abc$. The only positive multiple of abc smaller than $1.67abc$ is abc itself. Thus

$$M = a(x_1^2 + x_2^2) + b(x_3^2 + x_4^2) + c(x_5^2 + x_6^2) = abc.$$

An alternative approach is more intuitive but the bound is slightly weaker, and in fact fails to yield the desired result. Construct a six-dimensional ball with radius $R = \sqrt{abc/2}$ around each point of L. Each ball has six-dimensional volume V_6R^6 where $V_6 = \pi^3/6$; see [Wei2]. So it has volume $(\pi^3/48)(abc)^3 > 0.64(abc)^3$. The centers of these balls occur once per $(abc)^3$ volume. The volume of these balls don't quite account for the volume of 6-dimensional space; we cannot conclude that they overlap. If we could, we would then consider the centers of two overlapping balls. Their distance is strictly less than $2R = 2\sqrt{abc/2}$, so their squared distance is smaller than $2abc$. The difference of the two centers gives a vector

$$(w_1, w_2, w_3, w_4, w_5, w_6) = (x_1\sqrt{a}, x_2\sqrt{a}, x_3\sqrt{b}, x_4\sqrt{b}, x_5\sqrt{c}, x_6\sqrt{c}),$$

with x_i integers, not all zero. As before, the squared distance is

$$M = a(x_1^2 + x_2^2) + b(x_3^2 + x_4^2) + c(x_5^2 + x_6^2),$$

and again we would conclude M is a positive multiple of abc smaller than $2abc$, whence $M = abc$.

The numbers given by Hermite's constant and the lattice basis argument are stronger than those given by the sphere packing argument, and the difference allows one method to succeed where the other fails.

References

[Par] Poo-Sung Park, sci.math.research posting, April 21, 2005.

[Wei1] Eric W. Weisstein. "Hermite Constants." From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/HermiteConstants.html

[Wei2] Eric W. Weisstein. "Ball." From MathWorld–A Wolfram Web Resource. http://mathworld.wolfram.com/Ball.html