Sums of Squares and Golden Gates

Peter Sarnak

Stanford, May 2015

Sums of Squares:

C.L. Siegel: From his 1934 mass formula book:

“ It is somewhat surprising that in a branch of mathematics as old as the theory of quadratic forms which originated among the ancient Babylonians and has been intensively studied during the last three centuries by a succession of mathematicians of the highest rank, including Fermat, Gauss, Jacobi and Minkowski, any fundamentally new ideas have been left to be discovered. Never the less, it is our aim in these lectures to present a new general theorem in the arithmetical theory of quadratic forms which has several important applications . . . "

SUM OF TWO SQUARES

$$x_1^2 + x_2^2 = p \quad (\text{a prime})$$

p	(x_1, x_2)	p	(x_1, x_2)
2	(1, 1)	43	NS
3	NS : NO SOLUTION	47	NS.
5	(2, 1)	53	(7, 2)
7	NS.	59	NS
11	NS	61	(6, 5)
17	(4, 1)	67	NS
19	NS	71	NS
23	NS	73	(8, 3)
29	(5, 2)	79	NS
31	NS	83	NS
41	(5, 4)	89	(8, 5)
		97	(9, 4)

APPARENTLY SIMPLE RULE: WHEN p GIVES REMAINDER 3 WHEN DIVIDED BY 4; NO SOLUTION WHEN p GIVES REMAINDER 1 WHEN DIVIDED BY 4, THERE IS A SOLUTION.

Sums of Two Squares (Fermat):

$$x^2+y^2=p \quad , \ p \text{ an odd prime}$$

has a solution in integers

$$\text{if and only if} \qquad p \equiv 1(4).$$

(can one find the solutions quickly - later).
A necessary condition to solve

$$x^2+y^2=m$$

is that the (local) congruences be met $q \geqslant 1$

$$x^2+y^2 \equiv m \pmod{q} \qquad \text{——(1)}$$

(These are easy to check, involve only finitely many q's.) If $m \geqslant 0$ and (1) holds then
$x^2+y^2=m$ has a solution!
This is called the "local to global" principle.

SUM OF THREE SQUARES

$$x^2 + y^2 + z^2 = m \geq 0$$

m	(x,y,z)	m	(x,y,z)
1	$(1,0,0),\cdots$	16	$(4,0,0),\cdots$
2	$(1,1,0),\cdots$	17	$(4,1,0),\cdots$
3	$(1,1,1),\cdots$	18	$(4,1,1),\cdots$
4	$(2,0,0),\cdots$	19	$(3,3,1),\cdots$
5	$(2,1,0),\cdots$	20	$(4,2,0),\cdots$
6	$(2,1,1),\cdots$	21	$(4,2,1),\cdots$
7	NS	22	$(3,3,2),\cdots$
8	$(2,2,0),\cdots$	23	NS
9	$(2,2,1),\cdots$	24	$(4,2,2),\cdots$
10	$(3,1,0),\cdots$	25	$(5,0,0),\cdots$
11	$(3,1,1),\cdots$	26	$(5,1,0),\cdots$
12	$(2,2,2),\cdots$	27	$(5,1,1),\cdots$
13	$(3,2,0),\cdots$	28	NS
14	$(3,2,1),\cdots$	29	$(5,2,0),\cdots$
15	NS	30	$(5,2,1),\cdots$

APPARENTLY NO SOLUTIONS IF $m \equiv 7(8)$ AND ALSO $m = 28, \ldots$

Sums of Three Squares (Gauss 1800)

$$x^2+y^2+z^2=m \quad ,m \geqslant 0$$

Local congruence obstructions

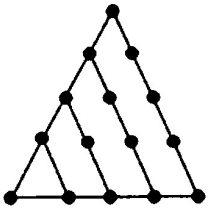
$$m \neq 4^a(8b+7) \qquad \text{——(2)}$$

Theorem (Local to global)
If (2) holds then m is a sum of three squares!

Sums of Four Squares (Lagrange)
Every positive integer is a sum of four squares.

Gauss in his diary: July 10, 1796

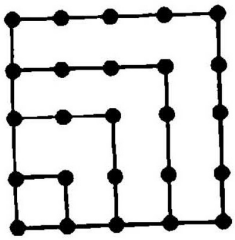
$$\text{EYPHKA! num} = \Delta + \Delta + \Delta$$

$\triangle =$ 

$$\frac{n(n+1)}{2}$$

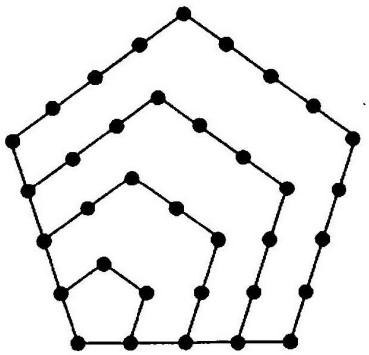
Triangular numbers arise by counting the number of points in a triangular array.

The sequence of triangular numbers is thus 1, 3, 6, 10, 15, ...



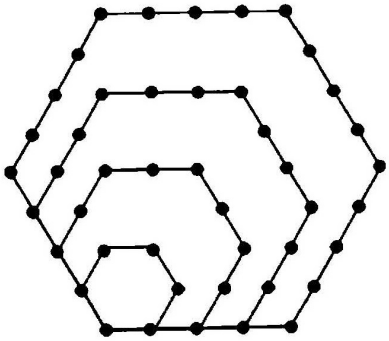
n^2

Similarly, the sequence of squares is 1, 4, 9, 16, 25, ...



$$\frac{n(3n-1)}{2}$$

Pentagonal numbers: 1, 5, 12, 22, 35, ...



$$n(2n-1)$$

Hexagonal numbers: 1, 6, 15, 28, 45, ...

Legendre (1830): Every integer larger than 1791 is a sum of four hexagonal numbers.

H. Iwaniec, W. Duke, R. Schulze-Pillot (1990): Every sufficiently large number is a sum of three hexagonal numbers (Ineffective!).

In 1900, Hilbert proposed 23 problems for the 20th century (**of which Paul Cohen solved the first**). Siegel worked on Hilbert's 11th problem: to develop a theory (local to global) for solving

$$F(x_1, x_2, \ldots, x_n) = m \qquad \text{——(3)}$$

for a quadratic form F (e.g., a sum of squares) and either

(i) x_j, m are in a quadratic number field K,

(ii) x_j, m are in the "integers" O_K of K.

Examples of quadratic fields:

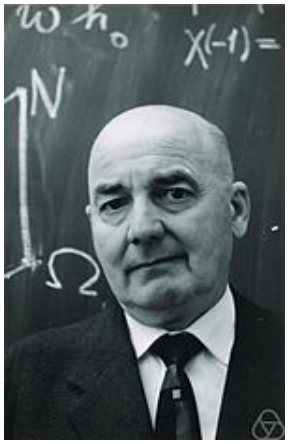
$$K = \mathbb{Q}(\sqrt{2}) := \{x = a + b\sqrt{2} : a, b \in \mathbb{Q}\}$$

and

$$O_{\mathbb{Q}(\sqrt{2})} = \mathbb{Z}[\sqrt{2}] := \{a + b\sqrt{2} : a, b \in \mathbb{Z}\}$$

$$\alpha = a + b\sqrt{2}, \alpha' = a - b\sqrt{2}$$

- Over K, Hasse solved the problem completely: has a solution iff it has a solution locally (over all “completions" K_v).

The “Hasse-Minkowski Theorem".

Over the “integers” O_K of K the problem is much more difficult.

Siegel Mass Formula: Quadratic forms F and G are **equivalent** over O_K if

$$F(Ax) = G(x),$$

for some $n \times n$ matrix A with coefficients in O_K and whose inverse also has coefficients in O_K.

Such F and G represent the same integers in K.

The **genus** $\mathfrak{F}$ of an "integral" quadratic form F consists of all integral quadratic forms G that are locally in congruences (and at the real places) equivalent to F.

Hermite's theorem: Any such genus $\mathfrak{F}$ consists of a **finite** number of inequivalent forms $F_1, F_2, \ldots, F_h$; we call h the **class number**.

Mass Formula: (Assume F is definite)

Let $r_{F_j}(m)$ be the number of representations of m by F_j,

there are $W_j > 0$ depending only on the genus such that

$\sum_{j=1}^{h} W_j r_{F_j}(m) =$ product of local densities.

The densities depend only on $\mathfrak{F}$ which count solutions in congruences.

The product of local densities is positive precisely when there are no local obstructions to solving $F(x) = m$.

If $h = 1$ then positivity holds, so Siegel's formula gives a complete solution! For example,

$$x_1^2 + x_2^2, \quad x_1^2 + x_2^2 + x_3^2, \quad x_1^2 + x_2^2 + x_3^2 + x_4^2$$

all have $h = 1$, explaining the results of Fermat, Gauss, and Lagrange.

But $h = 1$ is very rare, and if $h > 1$ then there are exceptions (i.e. m's that should be represented but are not).

$n \geqslant 5$ (Siegel): For quadratic K as above,

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 + x_5^2 = m$$

with $m > 0$ and $m' > 0$ (called totally positive) has a solution if and only if there are no local obstructions **except for finitely many m's** (up to units)

$n = 4$ (Kneser 1974): Same is true for $n = 4$. (His proof is elementary given Hasse's theorem).

One can also prove Kneser's result using the Ramanujan conjectures (Deligne's theorem).

$n = 3$ (Cogdell-Piatetsky Shapiro-S, 2000)

Same is true for sums of 3 squares, but this is ineffective.

Example: Maass proved that for $\mathbb{Q}(\sqrt{5})$, the genus of $x_1^2 + x_2^2 + x_3^2$ is a singleton and *every* $m > 0$ is a sum of 3 squares. (This is the only such case!)

Example: Using $\mathbb{Z}[\sqrt{3}]$, one such genus of quadratic forms is:

$$x_1^2 + x_2^2 + x_3^2 \quad , x_1^2 + 2x_2^2 + 2\sqrt{3}x_2x_3 + 2x_3^2$$

Here, the class number h is 2.

Consider $D \equiv 5(8)$ and $K = \mathbb{Q}(\sqrt{D})$.

Here there are no (finite) local obstructions to being a sum of 3 squares, so every m such that m and m' are sufficiently large (in an explicit sense, such as perhaps $mm' > 10^D$) is a sum of 3 squares **with at most one exception**.

So the problem is not completely resolved.

For $n = 2$ there is no simple local to global principle (class field theory)

IN WHAT FOLLOWS WE WILL WORK WITH 2×2 MATRICES

$$A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}, \quad a, b, c, d \text{ ARE COMPLEX NUMBERS}$$

$$A^* := \begin{bmatrix} \bar{a} & \bar{c} \\ \bar{b} & \bar{d} \end{bmatrix} \quad (\text{OR } A^\dagger)$$

if $a = x + iy$
$\bar{a} = x - iy$

A IS UNITARY IF $A^* A = I$.

THE SET OF 2×2 UNITARY MATRICES FORM A "GROUP" CALLED THE UNITARY GROUP, DENOTED $U(2)$.

Golden gates:

Classical Computing:
A single bit state is $\{0,1\}$. Gates for classical circuits achieve any Boolean

$$f : \{0,1\}^n \to \{0,1\}$$

via $\wedge, \backsim$ etc., complexity = length of circuit.
Theoretical Quantum Computing: Single qubit states are points $u = (u_1, u_2) \in \mathbb{C}^2$

$$|u|^2 = |u_1|^2 + |u_2|^2 = 1.$$

A 1-bit *quantum gate* is a 2×2 unitary matrix A. There is a natural notion of "distance" $d(A,B)$ between such matrices:

$$d(A,B) := \sqrt{1 - \frac{|\text{trace}(A^* \cdot B)|}{2}}$$

A set of gates $\{A_1, A_2, \ldots, A_n\}$ is **universal** if any 1-bit quantum state A is approximated arbitrarily closely (for this distance) by "circuits" in the A_j's.

We seek universal gates whose circuits to approximate any 2×2 unitary matrix A are *short*.

Textbook Gates:

Hadamard	H	$\frac{1}{\sqrt{2}}\begin{bmatrix} 1 & 1 \\ 1 & -1 \end{bmatrix}$
Pauli-X	X	$\begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$
Pauli-Y	Y	$\begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$
Pauli-Z	Z	$\begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$
Phase	S	$\begin{bmatrix} 1 & 0 \\ 0 & i \end{bmatrix}$
$\pi/8$	T	$\begin{bmatrix} 1 & 0 \\ 0 & e^{i\pi/4} \end{bmatrix}$

The gates H and S generate exactly 24 gates, called the *Clifford gates*.
Remarkably, using H and T instead, we can approximate **any** A as close as we wish; Solavay and Kitaev proved that such "universality" with H and T can be achieved **efficiently**!

Ross - Selinger (2014)

$$d\left(U, \begin{bmatrix} e^{i\pi/128} & 0 \\ 0 & e^{-i\pi/128} \end{bmatrix}\right) < 10^{-10} = \varepsilon$$

with the word

$$U = HTSHTSHT \ldots\ldots\ldots\ldots\ldots HTH$$

T-count is 102 (100 is optimal).

$\varepsilon = 10^{-20}$, T-count 200 (198 optimal).

$\varepsilon = 10^{-2000}$, T-count 19942 (19934 optimal)

Run time 383 seconds.

Back to sums of squares

$K = \mathbb{Q}(\sqrt{2}), O_K = \mathbb{Z}[\sqrt{2}].$

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 2^h, \quad h \geqslant 0.$$

for

$$x_j \in O_K. \qquad \text{——(1)}$$

One can show (Kliuchnikov-Maslov-Mosca) (2013) that the solutions to (1) with $h \leq t$ give rise via

$$(x_1, x_2, x_3, x_4) \mapsto \begin{bmatrix} \frac{x_1 + ix_2}{2^{h/2}} & \frac{x_3 + ix_4}{2^{h/2}} \\ \\ \frac{-x_3 + ix_4}{2^{h/2}} & \frac{x_1 - ix_2}{2^{h/2}} \end{bmatrix}$$

to the circuits with T-count at most t, using the gates H, S, T.

So the question of approximating and A by a word in these is: for $x_1, \ldots, x_4$ in O_K satisfying $x_1^2 + x_2^2 + x_3^2 + x_4^2 = 2^h$, how well do the scaled points

$$\frac{1}{2^{h/2}}(x_1, x_2, x_3, x_4)$$

cover the unit sphere in 4-dimensional space? There are about 2^h such points, so they can pack with radius $\varepsilon \approx 2^{-h/3}$ (vol ball radius ε in S^3 is ε^3).

One can show (Lubotzky-Phillips-S 1988) using modular forms (and among other things the Ramanujan conjectures) that these points cover most points of S^3 with such an optimally small ε!

“Golden" … if we can find them quickly!

To be truly golden, one needs to find these short circuits quickly (i.e., poly t steps).

Side note: K. Manders and L. Adleman(1978) The problem of deciding if

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

has a solution in natural numbers x and y, given a, b, c, is NP-complete!

Ross-Selinger(2014) gave a random algorithm (to find the x_i's) whose expected running time(assuming various heuristics) is poly(t) and which if it stops produces essentially the best approximation to a given diagonal element $\left[\begin{smallmatrix} \alpha & 0 \\ 0 & \bar{\alpha} \end{smallmatrix}\right]$.

It runs very well in practice, and by writing a general 2×2 unitary matrix A as a product of three diagonal matrices we get a circuit 3 times longer than what we know exists and is optimal.

The Algorithm:

Step 1: Find an integral solution to

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = 5^h, \quad h \leq t$$

with (x_1, x_2, x_3, x_4) doing the approximation to diagonal A; i.e., $x_1 \sim \alpha, x_2 \sim \beta, x_3 \sim 0, x_4 \sim 0$ with integers α and β satisfying $\alpha^2 + \beta^2 = 5^h$.

Step 2: Choose x_1 close to $\alpha(\lfloor \alpha \rfloor + k)$ and x_2 close to $\beta(\lfloor \beta \rfloor + \ell)$. Then check if

$$x_3^2 + x_4^2 = 5^h - (x_1^2 + x_2^2)$$

has a solution: if the right side is prime $p \equiv 1(4)$ then we can find x_3 and x_4 (by Fermat!)

According to an algorithm of R. Schoof (using elliptic curves with “CM") such x_3 and x_4 can be found in poly(log p) steps!

Now vary k, ℓ a little until this succeeds (i.e., we get such a prime); in practice it does succeed!

Step 3: Once (x_1, x_2, x_3, x_4) are found, there is a tree structure (coming from the factorization theory of integral Hamilton quaternions) to the solutions representing 5^h (or $2^h \ldots$). A variant of this works using x_j in $\mathbb{Z}[\sqrt{2}]$ with H, S, T gates!

The above algorithm finds the (short) circuit encoding such an (x_1, x_2, x_3, x_4) that gives a close approximation of a diagonal A.

So remarkably, even in the 21st century, understanding the finer features of sums of squares is of interest, and may supply the basic building block of a quantum computer! Fermat, Gauss, and Siegel might be very surprised.

References

M. Nielsen and I. Chuang “Quantum computation and quantum information" CUP (2000)

N. Ross and P. Selinger arXiv 1403.2975 (2014)

V. Kliuchnikov, D. Maslov and M. Mosca arXiv 1212/6964 (2012)

A. Lubotzky, R. Phillips and P. Sarnak, CPAM 39, 149-186 (1986)

P. Sarnak Letter on Solovay Kitaev and Golden Gates *http://publications.ias.edu/sarnak/paper/2637*

W. Duke and R. Schulze-Pilot, Invent. Math. 99 (1990), no. 1, 49-57.

J. Cogdell “On sums of three squares" J. Theor. Nombres Bordeaux 15 (2003), no. 1 33-44.

K. Manders and L. Adleman “NP complete decision problems for quadratic polynomials"

J. Ellenberg and A. Venkatesh, Local-global principles for representations of quadratic forms. Invent. Math. 171 (2008), no. 2, 257-279.