Number Theory, Lecture 9

Sums of squares

Jan Snellman[1]

[1]Matematiska Institutionen
Linköpings Universitet

TEKNISKA HÖGSKOLAN
LINKÖPINGS UNIVERSITET

Summary

1. Sums of two squares
2. Sums of four squares

Summary

1. Sums of two squares
2. Sums of four squares

Theorem

Let n be a positive integer. If $n \equiv 3 \mod 4$ then n can not be written as the sum of two squares (of integers).

Proof.

		x	0	1	2	3
		x^2	0	1	0	1
y	y^2					
0	0		0	1	0	1
1	1		1	2	1	2
2	0		0	1	0	1
3	1		1	2	1	2

$\square$

Composites

Lemma

If m, n are sums of two squares, then so is mn.

Proof.

Suppose $m = a^2 + b^2$, $n = c^2 + d^2$. Then

$$mn = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$$

$\square$

Note that if we put $z = a + ib$, $w = c + id$, then $|z|^2 = z\overline{z} = a^2 + b^2$, $|w|^2 = w\overline{w} = c^2 + d^2$, $|z|^2|w|^2 = (a^2 + b^2)(c^2 + d^2)$, $|zw|^2 = (ac + bd)^2 + (ad - bc)^2$.

Theorem

Every prime p, $p \equiv 1 \mod 4$, can be written as a sum of two squares.

Proof.

Deferred. $\square$

Note that $2 = 1^2 + 1^2$, and that primes congruent to 3 mod 4 can not be written as a sum of two squares.

Lemma

If p prime, $p = 4m + 1$, m integer, then exists x, y, k pos integers with $x^2 + y^2 = kp$, $k < p$.

Proof.

$$\left(\frac{-1}{p}\right) \equiv (-1)^{(p-1)/2} = (-1)^{2m} = 1 \mod p$$

so -1 is a QR mod p. Thus exists $0 < a < p$, $a^2 \equiv -1 \mod p$. Thus $p|(a^2 + 1)$, so $a^2 + 1 = a^2 + 1^2 = kp$ some k. Since

$$kp = x^2 + 1^2 \leq (p-1)^2 + 1 < p^2$$

it follows that $k < p$. □

Proof (that $p = 4k + 1$ is sum of two squares)

- Let m be smallest such that $mp = x^2 + y^2$. We will show that $m = 1$.
- Suppose $m > 1$, and put $a \equiv x \mod m$, $b \equiv y \mod m$, $-m/2 < a \leq m/2$, $-m/2 < b \leq m/2$. Then $a^2 + b^2 \equiv x^2 + y^2 = mp \equiv 0 \mod m$.
- So exists k s.t. $a^2 + b^2 = km$.
- We have $(a^2 + b^2)(x^2 + y^2) = (km)(mp) = kmp^2$.
- We also have that $(a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2$
- Furthermore $ax + by \equiv x^2 + y^2 \equiv 0 \mod m$, $ay - bx \equiv xy - yx \equiv 0 \mod m$.
- $\left(\frac{ax+by}{m}\right)^2 + \left(\frac{ay-bx}{m}\right)^2 = km^2p/m^2 = kp$ (misprint in Rosen)
- Will show $0 < k < m$, a contradiction (hence $m > 1$ was false)

Proof (contd)

- $a^2 + b^2 = km$, $-m/2 < a \leq m/2$, $-m/2 < b \leq m/2$.
- So $a^2 \leq m^2/4$, $b^2 \leq m^2/4$.
- Thus $0 \leq km = a^2 + b^2 \leq m^2/4 + m^2/4 = m^2/2$.
- Hence $0 \leq k \leq m/2$. So $k < m$. Remains to show that $k > 0$.
- But if $k = 0$ then $a^2 + b^2 = 0$, so $a = b = 0$, so $x \equiv y \equiv 0 \mod m$, so $m|x$ and $m|y$. Furthermore $x^2 + y^2 = mp$, hence $m^2|mp$, hence $m|p$. But $m < p$, so must have $m = 1$.

Theorem

The positive integer $n = \prod_p p^{a_p}$ can be written as a sum of two squares iff a_p is even for all $p \equiv 3 \mod 4$.

Proof

- 2 sum of two squares
- Every $p = 4k + 1$ sum of two squares
- Every product of integers that are sums of two squares is a sum of two squares
- Every square is the sum of two squares
- Hence, if a_p even every $p = 4k + 1$, then n product of integers which are sums of two squares, hence a sum of two squares

Proof (contd)

- Now suppose $p \equiv 3 \mod 4$, $a_p = 2j+1$. Will show that n not the sum of two squares.
- Suppose not, $n = x^2 + y^2$
- $d = \gcd(x,y)$, $a = x/d$, $b = y/d$, $m = n/d^2$, $\gcd(a,b) = 1$, $a^2 + b^2 = m$.
- $a_p = 2j+1 = v_p(n)$, $k = v_p(d)$, $v_p(m) = 2j+1-2k \geq 0$, hence ≥ 1. So $p|m$.
- $\gcd(a,b) = 1$, $m = a^2 + b^2$, $p|m$, so $p \not| a$.
- So $aX \equiv b \mod p$ solvable, with soln $X = z$ say
- $a^2 + b^2 \equiv a^2 + (az)^2 = a^2(1+z^2) \mod p$
- But $a^2 + b^2 = m$, $p|m$, so $a^1(1+z^2) \equiv 0 \mod p$
- $\gcd(a,p) = 1$ so by cancellation $1 + z^2 \equiv 0 \mod p$. So $z^2 \equiv -1 \mod p$. But $\left(\frac{-1}{p}\right) = -1$ since $p \equiv 3 \mod 4$. Contradiction.

Example

- $2^3 * 3^5 = 1944$ can not be written as a sum of two squares
- $2^3 * 13^3 = 17576$ can be written as a sum of two squares;

$$
\begin{aligned}
2 &= 1^2 + 1^2 \\
2^2 &= 2^2 + 0^2 \\
2^3 &= (1 * 2 + 0)^2 + (1 * 0 - 1 * 2)^2 = 2^2 + 2^2 \\
13 &= 2^2 + 3^2 \\
13^2 &= 13^2 + 0^2 \\
13^3 &= (2 * 13 + 3 * 0)^2 + (2 * 0 - 3 * 13)^2 = 26^2 + 39^2 \\
2^3 * 13^3 &= (2 * 26 + 2 * 39)^2 + (2 * 39 - 2 * 26)^2 = 130^2 + 26^2
\end{aligned}
$$

3 squares not enough

Example

7 can not be written as a sum of 3 squares: modulo 8, a square takes the values $0, 1, 4$, thus (assume $x^2 \geq y^2 \geq z^2$)

x^2	y^2	z^2	$x^2 + y^2 + z^2$
0	0	0	0
1	0	0	1
4	0	0	4
1	1	0	2
4	1	0	5
4	4	0	0
1	1	1	3
4	1	1	6
4	4	1	1
4	4	4	4

Composites

Theorem

If m, n are sums of fours squares, then so is mn.

Proof.

Suppose $m = a^2 + b^2 + c^2 + d^2$, $n = e^2 + f^2 + g^2 + h^2$. Then

$$mn = (a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2) = R^2 + S^2 + T^2 + U^2$$

with

$$\begin{aligned} R &= ae + bf + cg + dh \\ S &= af - be + ch - dg \\ T &= ag - bh - ce + df \\ U &= ah + bg - cf - de \end{aligned}$$

$\square$

As in the case of two squares, where the formula for compunding sums of two squares was given by multiplication of Gaussian integers, this formula can be remembered/derived by making use of the “Hamiltonian integers”

$$\alpha = a + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}$$
$$\beta = e + f\mathbf{i} + g\mathbf{j} + h\mathbf{k}$$

and their norms.
Recall:

$$\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1,$$

$$\mathbf{ij} = \mathbf{k}, \quad \mathbf{jk} = \mathbf{i}, \quad \mathbf{ki} = \mathbf{j},$$

and the $\mathbf{i}, \mathbf{j}, \mathbf{k}$ anti-commute pairwise.

Lemma

If $p > 2$ is prime, then exists integer $0 < k < p$ such that

$$x^2 + y^2 + z^2 + w^2 = kp$$

has an integer solution (x, y, z, w).

Proof

- First we find integer solns to $x^2 + y^2 + 1 \equiv 0 \mod p$, with $0 \leq x < p/2$, $0 \leq y < p/2$.
- Put $S = \left\{ j^2 \middle| 0 \leq j \leq (p-1)/2 \right\}$, $T = \left\{ -1 - j^2 \middle| 0 \leq j \leq (p-1)/2 \right\}$. All elems in S non-congruent mod p, since $j_1^2 \equiv j_2^2 \mod 2$ implies $0 \equiv j_1^2 - j_2^2 = (j_1 + j_2)(j_1 - j_2) \mod p$, hence $j_1 \equiv j_2 \mod p$ or $j_1 \equiv -j_2 \mod p$, contradicts $0 \leq j \leq (p-1)/2$.
- Similarly, all elems in T non-congruent mod p.

Proof (contd)

- S, T disjoint, both contain $(p+1)/2$ elems, so $S \cup T$ has $p+1$ elems
- Only p congruence classes mod p
- Pigeonhole principle (and above): exists $0 \le x, y \le (p-1)/2$, $x^2 \in S$, $-1-y^2 \in T$, and $x^2 \equiv -1-y^2 \mod p$
- So $x^2 + y^2 + 1 \equiv 0 \mod p$
- So $x^2 + y^2 + 1 = kp$ for some integer $k > 0$
- But $kp = x^2 + y^2 + 1 \le 2\left((p-1)/2\right)^2 + 1 < p^2$, so $k < p$.

Theorem

Every prime p can be written as $p = x^2 + y^2 + z^2 + w^2$ with $x, y, z, w \in \mathbb{Z}$.

Proof (sketch)

- Similar to proof that every $p = 4k + 1$ is sum of two squares: use lemma to assert that $mp = x^2 + y^2 + z^2 + w^2$ some m, let m be minimal, show $m = 1$.
- We'll do half of the proof, the rest is in Rosen
- To start, $p = 2$ OK since $2 = 1^2 + 1^2 + 0^2 + 0^2$
- m smallest positive integer such that $mp = x^2 + y^2 + z^2 + w^2$
- Assume, toward contradiction, that $m > 1$.

Proof (contd)

- Maybe m is even?
- Among x, y, z, w, and even number of even integers
- Permute, then $x \equiv y \mod 2$, $z \equiv w \mod 2$
- $a = (x-y)/2$, $b = (x+y)/2$, $c = (z-w)/2$, $d = (z+w)/2$ all integers
- $a^2 + b^2 + c^2 + d^2 = \frac{1}{4}\left((x-y)^2 + (x+y)^2 + (z-w)^2 + (z+w)^2\right) = \frac{1}{2}(x^2 + y^2 + z^2 + w^2) = \frac{1}{2}mp$
- Contradicts minimality of m
- Maybe m is odd?
- Check Rosen why impossible

Theorem

Every positive integer n can be written as the sum of four squares.

Proof.

- $n = \prod_p p^{a_p}$
- Each p sum of four squares
- By lemma on composites, each p^{a_p} sum of four squares
- By same lemma, n is the sum of four squares

$\square$

Example

$$
\begin{aligned}
3 &= 1^2 + 1^2 + 1^2 + 0^2 \\
5 &= 2^2 + 1^2 + 0^2 + 0^2 \\
4 &= 2^2 + 0^2 + 0^2 + 0^2 = 1^2 + 1^2 + 1^2 + 1^2 \\
15 &= 3^2 + 2^2 + 1^2 + 1^2 \\
20 &= 4^2 + 2^2 + 0^2 + 0^2 = 3^2 + 3^2 + 1^2 + 1^2
\end{aligned}
$$

Generating functions

Theorem

$$\prod_j \frac{1}{1 - st^{j^2}} = \sum_n t^n \sum_v (c_{n,v} s^v)$$

where $c_{n,v}$ counts the number of ways of writing n as a sum of v squares. If we want to find these ways, they are encoded in the correspinding monomial in

$$\prod_j \frac{1}{1 - st^{j^2} u_j}$$

Example

The coefficent of t^{20} in

$$\prod_j (1 - st^{j^2} u_j)^{-1}$$

is

$$s^{20}u_1^{20} + s^{17}u_1^{16}u_2 + s^{14}u_1^{12}u_2^2 + s^{12}u_1^{11}u_3 + s^{11}u_1^8u_2^3 + \\ s^9u_1^7u_2u_3 + s^8u_1^4u_2^4 + s^6u_1^3u_2^2u_3 + \left(u_2^5 + u_1^4u_4\right)s^5 + s^4u_1^2u_3^2 + s^2u_2u_4$$

from which we extract the information that

- 20 can be written uniquely as a sum of two squares as $2^2 + 4^2$
- 20 can be written uniquely as a sum of four sqaures as $1^2 + 1^2 + 3^2 + 3^2$
- 20 can be written as a sum of five squares in precisely two ways, namely $2^2 + 2^2 + 2^2 + 2^2 + 2^2$ and $1^2 + 1^2 + 1^2 + 1^2 + 4^2$

Example

The taylor expansion of order 3 of

$$\prod_j (1 - st^{j^2})^{-1}$$

is a formal power series in t, which starts as

$$\begin{aligned} s^2t^{20} + s^3t^{19} + \left(s^3 + s^2\right)t^{18} + \left(s^3 + s^2\right)t^{17} + \\ st^{16} + s^3t^{14} + s^2t^{13} + s^3t^{12} + s^3t^{11} + s^2t^{10} + \\ \left(s^3 + s\right)t^9 + s^2t^8 + s^3t^6 + s^2t^5 + s^3t^3 + st^4 + s^2t^2 + st + 1 \end{aligned}$$

We see that t^3, t^7, t^{15} are missing: $3, 5$ are primes congruent to 3 mod 4, and 15 contains one such prime to an odd exponent.