Every Positive Integer is the Sum of Four Squares! (and other exciting problems)

Sophex – University of Texas at Austin

October 18th, 2002

Matilde N. Lalín

1. Lagrange's Theorem

Theorem 1 *Every positive integer is the sum of four squares.*

For instance, $5 = 2^2 + 1^2 + 0^2 + 0^2$, $21 = 4^2 + 2^2 + 1^1 + 0^2$, $127 = 11^2 + 2^2 + 1^2 + 1^2$.

Proof. We will use the following Euler's identity:

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2$$

$$+(x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 + (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2$$

which is very easy to verify.

The conclusion is that the product of two numbers that are sum of four squares is also sum of four squares. Hence, since the case of 1 is trivial, and since every natural number > 1 can be decomposed as a product of prime numbers, it is enough to prove the result for prime numbers. The first case is $p = 2$, but that follows from $2 = 1^2 + 1^2 + 0^2 + 0^2$.

For the case of p odd, we are going to need the following:

Lemma 2 *If p is an odd prime, then there are numbers x, y, and m such that*

$$1 + x^2 + y^2 = mp \qquad 0 < m < p$$

So, for instance, for $p = 3$ we have $1 + 1^2 + 2^2 = 2 \cdot 3$, for $p = 7$ we have $1 + 2^2 + 4^2 = 3 \cdot 7$.

Proof. For $x = 0, 1, \ldots, \frac{p-1}{2}$, the numbers x^2 have all of them different congruences modulo p. This is because if $x_1^2 \equiv x_2^2 \pmod{p}$, then

$$p \mid (x_1 - x_2)(x_1 + x_2) \Rightarrow x_1 \equiv \pm x_2 \pmod{p}$$

which is a contradiction. So we have $\frac{p+1}{2}$ numbers which are incongruent modulo p.

For $y = 0, 1, \ldots, \frac{p-1}{2}$, the numbers $-1 - y^2$ are all incongruent modulo p, using the same idea as before. So we have another set of $\frac{p+1}{2}$ numbers incongruent modulo p.

But there are $p + 1$ numbers altogether in these two sets, and only p possible residues modulo p. Then at least one number x^2 in the first set must be congruent to a number $-1 - y^2$ in the second set. Hence,

$$x^2 \equiv -1 - y^2 \pmod{p} \Rightarrow x^2 + 1 + y^2 = mp$$

Now $x^2 < \left(\frac{p}{2}\right)^2$ and $y^2 < \left(\frac{p}{2}\right)^2$ so,

$$mp = 1 + x^2 + y^2 < 1 + 2 \cdot \left(\frac{p}{2}\right)^2 < p^2$$

then $m < p$. $\square$

It follows from the Lemma that, for p odd prime, there is an $0 < m < p$ such that

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

We are going to see that the least m with that property is $m = 1$. Let m_0 be the least m with the property. If $m_0 = 1$ there is nothing to prove. Then we can suppose $1 < m_0 < p$.

If m_0 is even, then either the x_i are all even, or the x_i are all odd, or two of them are even and the other two are odd. In this case, say x_1, x_2 are even. Then in all the three cases, $x_1 \pm x_2$ and $x_3 \pm x_4$ are all even and we can write

$$\frac{m_0}{2}\, p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2$$

and this contradicts the minimality of m_0.

Now we choose y_i such that

$$y_i \equiv x_i \pmod{m_0}, \qquad |y_i| < \frac{m_0}{2}$$

This can be done, since $-\frac{m_0-1}{2} \le y \le \frac{m_0-1}{2}$ is a complete set of residues. Now observe that the x_i are not all divisible by m_0, since this would imply $m_0^2 \,|\, m_0\, p$ and $m_0 \,|\, p$, a contradiction. As a consequence, we get

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 > 0$$

Then

$$y_1^2 + y_2^2 + y_3^2 + y_4^2 < m_0^2 \quad \text{and} \quad y_1^2 + y_2^2 + y_3^2 + y_4^2 \equiv 0 \pmod{m_0}$$

Therefore,

$$x_1^2 + x_2^2 + x_3^2 + x_4^2 = m_0\, p \qquad (m_0 < p)$$
$$y_1^2 + y_2^2 + y_3^2 + y_4^2 = m_0\, m_1 \qquad (0 < m_1 < m_0)$$

and so,

$$m_1\, m_0^2\, p = z_1^2 + z_2^2 + z_3^2 + z_4^2$$

where the z_i come from Euler's identity. But $z_1 = x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4 \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 0 \pmod{m_0}$ and similarly the other z_i are also divisible by m_0. We can write then $z_i = m_0 w_i$. Dividing by m_0^2, we get

$$m_1\, p = w_1^2 + w_2^2 + w_3^2 + w_4^2$$

and this contradicts again the minimality of m_0. It follows that $m_0 = 1$. $\square$

We should also mention that it is possible to compute the number of such representations. We will state without prove the following

Theorem 3 *Let $Q(n)$ the number of solutions of*

$$n = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

then, writing $n = 2^r(2t+1)$

$$Q(n) = \begin{cases} 8\,S(2t+1) = 8\,S(n) & \text{for } r = 0 \\ 24\,S(2t+1) & \text{for } r \neq 0 \end{cases}$$

where

$$S(n) = \sum_{d|n} d$$

We have seen that four squares are enough to represent any natural number. Three squares are not enough. Indeed, $x_i^2 \equiv 0, 1 \text{ or } 4 \pmod 8$, therefore,

$$x_1^2 + x_2^2 + x_3^2 \not\equiv 7 \pmod 8$$

hence no number of the form $8t+1$ can be represented by three squares.

We have the following Theorem (which we won't prove here).

Theorem 4 *Let* n *be a positive integer. Then* n *can be expressed as the sum of three squares if and only if* n *is not of the form* $4^r(8t+7)$*.*

For the case of two squares,

Theorem 5 *Let* n *be a positive integer. Then* n *can be expressed as the sum of two squares if and only if all prime factors of* n *of the form* $4t+3$ *have even exponents in the factorization of* n*.*

This Theorem can be proved in a similar way as we did for four squares, using the identity

$$(x_1^2 + x_2^2)(y_1^2 + y_2^2) = (x_1y_1 + x_2y_2)^2 + (x_1y_2 - x_2y_1)^2$$

2. Waring's problem

Waring's problem has to do with representing natural numbers as the sum of a fixed number s of k-th powers, namely,

$$n = x_1^k + \ldots + x_s^k$$

If we fix $k > 1$ and s is too small, the problem cannot be solved for every n. Say that $s = 1$, then we won't get solutions unless n is a k-th power.

The first arising question is whether, for a given k, there is any $s = s(k)$ such that

$$n = x_1^k + \ldots + x_s^k$$

is soluble for every n.

In 1770, Waring stated that every number is expressible as a sum of 4 squares, 9 cubes, 19 biquadrates, "and so on", implying that s does exist. Hilbert was the first to prove this assertion for every k, in 1909.

Clearly, given an s that works, any $s' > s$ will work the same. Hence there must be a minimal s that works. It is ussually denoted by $g(k)$. We have just proved that $g(2) = 4$.

It is not hard to prove

Theorem 6 *$g(4)$ does exist and it is ≤ 53.*

Proof. Let us denote by B_s a number which is the sum of s biquadrates. The identity

$$\begin{aligned} 6(a^2+b^2+c^2+d^2)^2 &= (a+b)^4+(a-b)^4+(c+d)^4+(c-d)^4 \\ &+ (a+c)^4+(a-c)^4+(b+d)^4+(b-d)^4 \\ &+ (a+d)^4+(a-d)^4+(b+c)^4+(b-c)^4 \end{aligned}$$

shows us that

$$6(a^2+b^2+c^2+d^2)^2 = B_{12}$$

Because of Lagrange's Theorem, we get

$$6x^2 = B_{12}$$

for every x. Now every positive number is of the form $n = 6t + r$ with $0 \leq r \leq 5$, then using Lagrange's Theorem once again,

$$n = 6(x_1^2 + x_2^2 + x_3^2 + x_4^2) + r$$

implying

$$n = B_{12} + B_{12} + B_{12} + B_{12} + r = B_{48} + r = B_{53}$$

Hence $g(4)$ exists and it is at most 53. $\square$

Theorem 7

$$g(k) \geq 2^k + \left[\left(\frac{3}{2}\right)^k\right] - 2$$

Proof. Write $q = \left[\left(\frac{3}{2}\right)^k\right]$. Consider the number

$$n = 2^k q - 1 < 3^k$$

which can be only represented by terms of the form 1^k and 2^k. Since,

$$n = (q-1)2^k + (2^k - 1)1^k$$

n requires $2^k + q - 2$ powers. $\square$

It has been proved that $g(k) = 2^k + q - 2$ for every but finitely many k. It is conjectured that this equality is always true.

There is another number that in a sense is more interesting that $g(k)$. We define $G(k)$ as the least value of s for which it is true that every positive integer which is large enough can be expressed as a sum of s k-th powers. Thus

$$G(k) \leq g(k)$$

For $k = 2$, we get $G(2) = 4$ since we have proved that four squares are enough and we have exhibited infinitely many numbers, the ones of the form $8t + 7$, that cannot we writen as sum of only three squares.

In general $G(k)$ is much smaller than $g(k)$. Take $k=3$. It is known that $g(3)=9$. Every number can be represented by the sum of nine cubes. Indeed every number but

$$23 = 2\cdot 2^3 + 7\cdot 1^3 \quad \text{and} \quad 239 = 2\cdot 4^3 + 4\cdot 3^3 + 3\cdot 1^3$$

can be expressed by the sum of at most eight cubes. Moreover, there are only 15 integers that require 8 cubes. This implies that $G(3)\le 7$.

$G(k)$ is only known for the cases $k=2,4$. The best currently known bound for $G(k)$ is

$$G(k) < c\,k\log k$$

for some constant c.

On the other hand,

Theorem 8

$$G(k) \ge k+1$$

for $k\ge 2$

Proof. Let $A(N)$ be the number of $n\le N$ which are representable as

$$n = x_1^k + \ldots + x_k^k$$

with $x_i \ge 0$. We may suppose

$$0 \le x_1 \le x_2 \le \ldots \le x_k \le N^{\frac{1}{k}}$$

If $B(N)$ is the number of solutions of the inequality, then $A(N)\le B(N)$. Clearly,

$$B(N) = \binom{[N^{\frac{1}{k}}]+1+k-1}{k} = \frac{\prod_{i=1}^{k}\left([N^{\frac{1}{k}}]+i\right)}{k!} \sim \frac{N}{k!}$$

If $G(k)\le k$, all but finitely many numbers are representable as the sum of k kth powers and

$$A(N) \ge N - c$$

where c is just a constant (independent of N). Then,

$$N - c \le A(N) \le B(N) \sim \frac{N}{k!}$$

and this is impossible when $k>1$. $\square$

Finally, the Table shows what is known for the first 20 values of k.

k	$g(k)$	$G(k)$
2	4	4
3	9	≤ 7
4	19	16
5	37	≤ 18
6	73	≤ 27
7	143	≤ 36
8	279	≤ 42
9	548	≤ 55
10	1079	≤ 63
11	2132	≤ 70
12	4223	≤ 79
13	8384	≤ 87
14	16673	≤ 95
15	33203	≤ 103
16	66190	≤ 112
17	132055	≤ 120
18	263619	≤ 129
19	526502	≤ 138
20	1051899	≤ 146

References

[1] H. Davenport, Analytic Methods for Diophantine Equations and Diophantine inequalities, *The University of Michigan*, Fall Semester (1962)

[2] G. H. Hardy, E. M. Wright, An Introduction to the Theory of Numbers, Fifth Edition, *Oxford University Press*, Oxford (1998)

[3] E. Landau, Elementary Number Theory, *Chelsea Publishing Company*, New York (1958)

[4] Eric Weisstein's World of Mathematics, http://mathworld.wolfram.com/WaringsProblem.html