11. Warings Problem

In 1770, E. Waring asserted without proof that every natural number is a sum of at most 4 squares, 9 cubes, 16 biquadrates, and so on.

Waring's Problem: For $k \in \mathbb{N}$ with $k \geq 2$, there exists a number $s = s(k)$ such that every natural number n is a sum of at most s k^{th} powers of natural numbers, i.e.

$$n = x_1^k + \cdots + x_s^k \text{ with } x_i \in \mathbb{N} \cup \{0\} \ (1 \leq i \leq s).$$

Let $g(k)$ denote the least s such that the above statement holds. Then Waring's problem states that

$$g(2) = 4, \ g(3) = 9, \ g(4) = 19, \ldots, \ g(k) < \infty.$$

In 1770, Lagrange proved $g(2) = 4$. By 1909, only known cases are $k = 2, 3, 4, 5, 6, 7, 8, 10$. In 1909, by a combinatorial method, Hilbert proved that $g(k) < \infty$ for every $k \geq 2$. By the work of Vinogradov, we now have an almost complete solution to $g(k)$. Consider the integer

$$n = 2^k \left\lfloor \left(\tfrac{3}{2}\right)^k \right\rfloor - 1 < 3^k.$$

The most efficient representation for n is to use $\left\lfloor \left(\frac{3}{2}\right)^k \right\rfloor - 1$ many 2^k and

$$n = 2^k \left(\left\lfloor \left(\tfrac{3}{2}\right)^k \right\rfloor - 1 \right) + 1^k (2^k - 1).$$

Thus we obtain a result of Euler that

$$g(k) \geq 2^k + \left\lfloor \left(\tfrac{3}{2}\right)^k \right\rfloor - 2.$$

Indeed, the equality holds for all but finitely many k. The equality holds only if

$$2^k \left\{ \left(\tfrac{3}{2}\right)^k \right\} + \left\lfloor \left(\tfrac{3}{2}\right)^k \right\rfloor \leq 2^k.$$

In 1957, Mahler showed that the above inequality holds for all but finitely many k.

2015 11 23(3)

In the following, we'll establish $g(2)=4$. Observe that as x runs over $\mathbb{Z}/p\mathbb{Z}$, $x^2 \equiv 0,1,4 \pmod 8$. Since $x_1^2+x_2^2+x_3^2 \not\equiv 7 \pmod 8$, we see that $g(2) \geq 4$.

2015 11 25

63? → Theorem 62: If p is an odd prime, there exist $x,y \in \mathbb{Z}$ such that $1+x^2+y^2 = mp$, where $m \in \mathbb{Z}$ satisfying $1 \leq m \leq p-1$. Huh? Why?

Proof: Consider the sets

$$S_1 = \{x^2 + p\mathbb{Z} ; x \in \mathbb{Z} \text{ and } 0 \leq x \leq \tfrac{p-1}{2}\}$$

and

$$S_2 = \{-1-y^2 + p\mathbb{Z} ; y \in \mathbb{Z} \text{ and } 0 \leq y \leq \tfrac{p-1}{2}\}.$$

Note that $x_1^2 \equiv x_2^2 \pmod p$ if and only if $x_1 \equiv \pm x_2 \pmod p$. Since $0 \leq x \leq \frac{p-1}{2}$, all elements in S_1 are distinct, so are S_2. Since $|S_1| = |S_2| = \frac{p-1}{2}$, we have $S_1 \cap S_2 \neq \varnothing$. Thus there exist $x,y \in \mathbb{Z}$ with $0 \leq x,y \leq \frac{p-1}{2}$ such that

$$x^2 \equiv -1-y^2 \pmod p \Rightarrow 1+x^2+y^2 \equiv 0 \pmod p.$$

Thus $1+x^2+y^2 = mp$ for some $m \in \mathbb{Z}$. Also, we have

$$0 < m < \frac{1+x^2+y^2}{p} \leq \frac{1+(\frac{p-1}{2})^2+(\frac{p-1}{2})^2}{p} < p. \qquad \blacksquare$$

64 → Theorem 63 (Lagrange's Theorem): We have $g(2)=4$. In other words, every natural number can be expressed as a sum of four squares.

Proof: We have the Lagrange identity

$$\begin{aligned}&(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)\\ &= (x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2 + (x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2\\ &\quad + (x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2 + (x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2.\end{aligned}$$

We see that the product of two numbers which are representable as a sum of four squares is also representable as a sum of four squares. Thus to prove the theorem, it suffices to show that all primes are representable as a sum of four squares. Note that

$$2 = 1^2+1^2+0^2+0^2.$$

Let p be an odd prime. By theorem 62, there exist $x_1,x_2,x_3,x_4 \in \mathbb{Z}$ such that $x_1^2+x_2^2+x_3^2+x_4^2 = mp$ with $1 \leq m \leq p-1$. Let m_0 be the

smallest natural number such that $m_0 p$ is a sum of four squares. It remains to show that $m_0 = 1$. Suppose that m_0 is even. Note that

$$(x_1+x_2+x_3+x_4)^2 = x_1^2+x_2^2+x_3^2+x_4^2+2\sum_{1\le i<j\le 4} x_i x_j.$$

Since $x_1^2+x_2^2+x_3^2+x_4^2 = m_0 p$ is even, we see that $x_1+x_2+x_3+x_4$ is even. Thus either all x_1, x_2, x_3, x_4 are even, all x_1, x_2, x_3, x_4 are odd, or two are even (say x_1 and x_2) and two are odd (say x_3 and x_4). In all cases,

$$x_1+x_2,\ x_1-x_2,\ x_3+x_4,\ x_3-x_4$$

are all even. It follows that

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

This contradicts the minimality of m_0. Thus m_0 is odd. Suppose that $m_0 > 1$. Since $x_1^2+x_2^2+x_3^2+x_4^2 = m_0 p$ and $1 \le m_0 \le p-1$, not all of x_1, x_2, x_3, x_4 are divisible by m_0 for otherwise $m_0^2 \mid m_0 p$ and thus $m_0 \mid p$, a contradiction. Thus there exist $b_1, b_2, b_3, b_4 \in \mathbb{Z}$ such that $y_i = x_i - b_i m_0$ and $|y_i| < \frac{m_0}{2}$ $(1 \le i \le 4)$ and not all of the y_i's are zero. Then

$$0 < y_1^2+y_2^2+y_3^2+y_4^2 < 4\left(\frac{m_0}{2}\right)^2 = m_0^2$$

and

$$y_1^2+y_2^2+y_3^2+y_4^2 \equiv 0 \pmod{m_0}.$$

Thus there exists $m_1 \in \mathbb{Z}$ with $m_1 < m_0$ such that

$$y_1^2+y_2^2+y_3^2+y_4^2 = m_0 m_1.$$

We recall that

$$x_1^2+x_2^2+x_3^2+x_4^2 = m_0 p.$$

Multiply the above two equalities together. By the Lagrange identity, there exist $z_1, z_2, z_3, z_4 \in \mathbb{Z}$ such that

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

where $z_1 = x_1 y_1 + x_2 y_2 + x_3 y_3 + x_4 y_4$ and etc. Since

$$z_1 = \sum_{i=1}^{4} x_i(x_i - b_i m_0) = \sum_{i=1}^{4} x_i^2 + m_0 K$$

for some $K \in \mathbb{Z}$, and since $x_1^2+x_2^2+x_3^2+x_4^2 = m_0 p$, we have

$$z_1 \equiv 0 \pmod{m_0}.$$

2015 11 25 (2)

Similarly, z_2, z_3, z_4 are divisible by m_0. Let $t_i = \frac{z_i}{m_0}$ $(1 \le i \le 4)$. Then

$$t_1^2 + t_2^2 + t_3^2 + t_4^2 = m_1 p$$

and $1 \le m_1 < m_0$, which contradicts the minimality of m_0. Thus $m_0 = 1$ for all odd primes p. Thus we see that all primes are representable as a sum of four squares. ∎

2015 11 27

65 → Theorem 64: We have $g(4) \le 53$.

Proof: We have the identity

$$6(a^2+b^2+c^2+d^2)^2 = \quad \text{(64)}$$

$$(a+b)^4 + (a-b)^4 + (c+d)^4 + (c-d)^4 + (a+c)^4 + (a-c)^4 + (b+d)^4 + (b-d)^4 + (a+d)^4 + (a-d)^4 + (b+c)^4 + (b-c)^4.$$

Combining the above identity with theorem 63, we see that every integer of the form $6x^2$ can be expressed as a sum of 12 fourth powers. Note that every natural number can be written in the form $6k+r$ with $k \in \mathbb{N} \cup \{0\}$ and $0 \le r \le 5$. Then by theorem 63, we can write k as a sum of 4 squares, say $k = x_1^2 + x_2^2 + x_3^2 + x_4^2$. Then $6k = 6x_1^2 + 6x_2^2 + 6x_3^2 + 6x_4^2$. Since each term in the above sum is a sum of 12 fourth powers, $6k$ can be expressed as a sum of 48 fourth powers. Finally, r is a sum of r fourth powers ($r = 1^4 + \cdots + 1^4$). Since $0 \le r \le 5$, $6k+r$ is a sum of 53 fourth powers. ∎

← 64