BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 61, No. 2, 2013

NUMBER THEORY

On Sums of Four Coprime Squares

by

A. SCHINZEL

Summary. It is proved that all sufficiently large integers satisfying the necessary congruence conditions mod 24 are sums of four squares prime in pairs.

P. Turán asked (see [2, p. 204]) for a characterization of positive integers that are sums of four squares prime in pairs. In this direction we shall prove

THEOREM 1. *A positive integer n has a decomposition*

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

where

(2) $$(x_i, x_j, 6) = 1 \quad \text{for all } 1 \le i < j \le 4$$

if and only if

(3) $$n \equiv 3, 4, 7, 12, 15 \text{ or } 19 \pmod{24}.$$

THEOREM 2. *If* (3) *holds and n is large enough, then n has a decomposition* (1) *with x_1, x_2 odd primes and*

(4) $$(x_i, x_j) = 1 \quad \text{for } 1 \le i < j \le 4.$$

It seems likely that the condition (2) can be replaced in Theorem 1 by (4) for $n \ne 100, 268$, and also that Theorem 2 holds for $n > 268$. Prof. J. Browkin has checked that all positive integers n satisfying (3) up to $5 \cdot 10^4$ have a decomposition (1) with (4) and $x_4 = 1$ except $n = 100$, 247 and 268.

Proof of Theorem 1. Necessity is well known, see [2, p. 204]. In order to prove sufficiency notice that by (3),

(5) $$n - 1 \equiv 2, 3, 6, 11, 14 \text{ or } 18 \pmod{24},$$

2010 *Mathematics Subject Classification*: Primary 11E25.
Key words and phrases: sum of squares.

hence, by Gauss's theorem, $n-1\equiv x_1^2+x_2^2+x_3^2$, where $(x_1,x_2,x_3)=1$. Thus, by (5) at most one x_i is even and at most one divisible by 3. Taking $x_4=1$ we obtain (2).

LEMMA 1. *The number $r(n)$ of representations of n as the sum of two squares satisfies $r(n)=O(n^\varepsilon)$ for every $\varepsilon>0$.*

Proof. We have $r(n)\le 4d(n)$, where $d(n)$ is the number of divisors of n, and the relation $d(n)=O(n^\varepsilon)$ is well known. ■

LEMMA 2. *For n satisfying* (3) *let $R(n)$ be the number of pairs $\langle p,q\rangle$ of primes such that*

$$2<p\le\sqrt{n/2},\qquad 2<q\le\sqrt{n/2} \tag{6}$$

and $n-p^2-q^2$ is representable as x^2+y^2, where $(x,y)=1$. Then

$$R(n)>A\frac{n}{(\log n)^{5/2}}\left(1+O\left(\frac{\log\log n}{(\log n)^{1/10}}\right)\right), \tag{7}$$

where $A>0$.

Proof. If n satisfies (3), then in the notation of [1, p. 264], $q\le 1$, $h=0$, $K\,|\,2$. By Lemmas 8 and 10 of [1] the number of pairs $\langle p,q\rangle$ of primes satisfying (6) and such that $(n-p^2-q^2)/K$ has no prime factor $\equiv 3 \pmod 4$ is at least

$$A\frac{n}{(\log n)^{5/2}}\left(1+O\left(\frac{\log\log n}{(\log n)^{1/10}}\right)\right).$$

Since $n-p^2-q^2\not\equiv 0 \bmod 4$, it follows that $n-p^2-q^2=x^2+y^2$, where $(x,y)=1$. Thus (7) holds. ■

LEMMA 3. *The number of solutions $\langle p,q,x,y\rangle$ of the equation*

$$n=p^2+q^2+p^2x^2+y^2,$$

where p,q,x,y are integers and $p>0$, is $O(n^{1/2+\varepsilon})$ for every $\varepsilon>0$.

Proof. By Lemma 1 the number in question equals

$$\sum_{0<p\le\sqrt n}\ \sum_{|x|\le\frac1p\sqrt n} r(n-p^2-p^2x^2)\le\sum_{0<p\le\sqrt n}\left(\frac{2\sqrt n}{p}+1\right)O(n^{\varepsilon/2})$$

$$=O(n^{1/2+\varepsilon/2})\sum_{0<p\le\sqrt n}\frac1p+O(n^{1/2+\varepsilon/2})=O(n^{1/2+\varepsilon/2}\log n)=O(n^{1/2+\varepsilon}).\ ■$$

Proof of Theorem 2. We estimate the number N of pairs $\langle x_1,x_2\rangle$ of odd primes x_1,x_2 such that $n=x_1^2+x_2^2+x_3^2+x_4^2$, $(x_3,x_4)=1$ and neither

$$x_1=x_2 \tag{8}$$

nor

$$x_i\,|\,x_j\quad \text{for any } i=1,2;\ j=3,4. \tag{9}$$

The number of pairs of odd primes in question such that (8) holds is $O(n^{1/2})$. The number of pairs of odd primes in question such that (9) holds is, by Lemma 3, $O(n^{1/2+\varepsilon})$. Thus, by Lemma 2

$$N > A\frac{n}{(\log n)^{5/2}}\left(1 + O\left(\frac{\log\log n}{(\log n)^{1/10}}\right)\right) + O(n^{1/2+\varepsilon}) > 0$$

for all sufficiently large n satisfying (3). ∎

By an easy modification of this argument we find that every sufficiently large integer $n \not\equiv 0, 1, 5 \pmod 8$ is representable as $x_1^2 + x_2^2 + x_3^2 + x_4^2$, where x_1, x_2 are odd primes, x_3, x_4 are integers and $(x_1, x_3) = (x_2, x_4) = 1$.

Since the constant in the O-symbol in (7) is ineffective, one cannot determine from the proof here or in Theorem 2 the greatest n for which the assertion does not hold.

References

[1] G. Greaves, *On the representation of a number in the form $x^2 + y^2 + p^2 + q^2$ where p, q are odd primes*, Acta Arith. 29 (1976), 257–274.

[2] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Springer, 2004.

A. Schinzel
Institute of Mathematics
Polish Academy of Sciences
Śniadeckich 8
00-956 Warszawa, Poland
E-mail: schinzel@impan.pl

Received April 11, 2013 (7927)