****
BANACH CENTER PUBLICATIONS, VOLUME **
INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
WARSZAWA 201*

SUMS OF TWO NUMBERS HAVING ONLY PRIME FACTORS CONGRUENT TO ONE MODULO FOUR

RAINER DIETMANN
Department of Mathematics
Royal Holloway, University of London
Egham, Surrey, TW20 0EX, United Kingdom
Email: rainer.dietmann@rhul.ac.uk

CHRISTIAN ELSHOLTZ
Institute of Analysis and Number Theory, Graz University of Technology
Kopernikusgasse 24/II, A-8010 Graz, Austria
Email: elsholtz@math.tugraz.at

Abstract. We show that every sufficiently large positive integer congruent to 2 modulo 4 can be written as the sum of two positive integers, each having only prime factors congruent to 1 modulo 4.

Responding to a question of Euler we show how the following result can be quickly deduced from results in the modern literature:

Theorem. Every sufficiently large positive integer congruent to 2 modulo 4 can be written as the sum of two positive integers, each having only prime factors congruent to 1 modulo 4.

This asymptotically answers a question of Euler ([2], letter to Goldbach) which has been repeatedly enquired about by Lemmermeyer on mathematical websites [5, 6]. As Lemmermeyer [6, 7] describes, Euler considered a result like this a possible path to prove the four squares theorem, which he seriously attempted, but which was eventually proved by Lagrange. Important partial results towards Euler's question are due to R. D. James [4], who in the ternary case proved that every positive integer congruent to 3 modulo 4 can be written as the sum of three numbers composed only of prime factors congruent to

2010 *Mathematics Subject Classification*: Primary 1N25; Secondary 11E25, 11N36, 11P32
Key words and phrases: binary additive problem, question of Euler, sums of integers with multiplicative constraints
The paper is in final form and no version of it will be published elsewhere.

1 modulo 4. Moreover, using Brun's sieve, he obtained an approximation to the binary case to the effect that each large positive integer congruent to 2 modulo 4 can be written as the sum of two integers each having at most two prime factors not congruent to 1 modulo 4. The ternary case allows for an elementary proof, based on Gauß' theorem on the sum of three triangular numbers: any positive integer k can be written as

$$k = \frac{x(x-1)}{2} + \frac{y(y-1)}{2} + \frac{z(z-1)}{2}$$

and therefore

$$4k+3 = [x^2+(x-1)^2] + [y^2+(y-1)^2] + [z^2+(z-1)^2].$$

Observe that $x^2+(x-1)^2$, $y^2+(y-1)^2$ and $z^2+(z-1)^2$ are each a sum of two adjacent squares, and thus cannot be divisible by any prime $p \equiv 3 \pmod 4$. [1]

We now show that the theorem is a consequence of a well known result of the late George Greaves [3] that uses Iwaniec's half dimensional sieve. Independently of our work and also based on Greaves' result, Schinzel [8] proved a related conjecture of Turán on representing integers as sums of four squares being *coprime* in pairs. By Greaves [3], each sufficiently large n with $n \equiv 2 \pmod 4$ can be written in the form

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

for primes p, q and integers x, y, and the number of such representations is at least

$$A\frac{n}{(\log n)^{5/2}} + o\left(\frac{n}{(\log n)^{5/2}}\right)$$

for an absolute constant $A > 0$. Clearly the contribution coming from $p = 2$ or $q = 2$ is of a smaller order of magnitude: if say $p = 2$, then there are $O(n^{1/2})$ many possibilities for q, and using the familiar bound $r(n) \ll_\varepsilon n^\varepsilon$ for the number of representations of a positive integer n as a sum of two squares of integers, as $r(n-4-q^2) \ll_\varepsilon n^\varepsilon$ the total number of possibilities for q, x and y in case of $p = 2$ is $O_\varepsilon(n^{1/2+\varepsilon})$. So we may assume that both p and q are odd primes. Then $n \equiv 2 \pmod 4$ implies that both x and y are even. Writing

$$a = p^2 + x^2 \text{ and } b = q^2 + y^2$$

both a and b are odd. Taking multiplicities into account, we conclude with $r(a), r(b) = O_\varepsilon(n^\varepsilon)$ that there are at least

$$n^{1-3\varepsilon} \tag{1}$$

many pairs (a, b) of odd positive integers a, b, such that $n = a + b$ and both a and b are the sum of the square of a prime and the square of an integer. Now suppose that w is a prime with $w \equiv 3 \pmod 4$ and w divides $a = p^2 + x^2$, say. The footnote, with $s = p$ being prime, implies that $p = w$ and x is divisible by w. There are at most $O(1 + n^{1/2}/w^2)$ many values of a divisible by w^2, and for any such a there will be only one corresponding b since $a + b = n$. The same argument applies if w divides b. Moreover, clearly w can be at most $n^{1/2}$. Summing over all such w we conclude that the number of pairs (a, b)

[1] Here and in the following we make use of the following simple observation following immediately from the Two Squares Theorem: if a prime $p \equiv 3 \pmod 4$ divides a sum $s^2 + t^2$, then p divides both s and t.

with $a+b=n$ and a, b of the form above, where one of a and b is divisible by *any* prime congruent to 3 mod 4, is at most $O(n^{1/2})$, which is of smaller order of magnitude than (1). Since we have excluded all prime factors p of a and b with $p=2$ or $p \equiv 3 \pmod 4$, this finishes the proof.

Remark. As in [8] our argument based on [3] is ineffective regarding "sufficiently large n". Using the circle method with a Kloosterman refinement instead, Brüdern [1] in particular obtained an effective version of Schinzel's result. It should be possible to apply the same strategy to our problem here but it was our intention to keep the exposition brief.

A quite different asymptotic solution of Euler's problem was posted by the mathoverflow user with pseudonym Lucia (see [6]).

One could also ask the corresponding question of writing every sufficiently large positive integer congruent to 2 modulo 4 as the sum of two integers composed only of prime factors congruent to 3 modulo 4, but this problem seems to be out of reach of existing methods.

References

[1] Brüdern, J. *Sums of Squares Coprime in Pairs*, Bull. Polish Acad. Sci. Math. 62 (2014), 215–231.

[2] Euler, L. Letter to Goldbach, 6th May 1747, available at:
`http://eulerarchive.maa.org/correspondence/correspondents/Goldbach.html`

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

[4] James, R. D., *A problem in additive number theory*, Transactions of the American Mathematical Society 43, No. 2 (1938), 296–302.

[5] Lemmermeyer, F. post on "nmbthry", 10 September 2009
`https://listserv.nodak.edu/cgi-bin/wa.exe?A2=NMBRTHRY;1ab10435.0909`

[6] Lemmermeyer, F., Question 37278 on "mathoverflow", 31 August 2010, `https://mathoverflow.net/questions/37278`, answers by Lucia, and Rainer Dietmann & Christian Elsholtz.

[7] Lemmermeyer, F. Euler, Goldbach and "Fermat's theorem",
`https://arxiv.org/abs/1310.6605`

[8] Schinzel, A., *On sums of four coprime squares*, Bull. Polish Acad. Sci. Math. 61 (2013), 109–111.