MATHEMATICS OF COMPUTATION
Volume 67, Number 222, April 1998, Pages 863–866
S 0025-5718(98)00928-4

# CHECKING THE ODD GOLDBACH CONJECTURE UP TO $10^{20}$

YANNICK SAOUTER

Abstract. Vinogradov's theorem states that any sufficiently large odd integer is the sum of three prime numbers. This theorem allows us to suppose the conjecture that this is true for all odd integers. In this paper, we describe the implementation of an algorithm which allowed us to check this conjecture up to $10^{20}$.

## 1. Introduction

Goldbach stated in 1742 that every even integer greater than 2 is the sum of two prime numbers. This problem is now known as the Goldbach conjecture. This is still unsolved and the closest related results are that: (i) there exists an integer $S$ such that every integer is the sum of at most $S$ primes [6], and (ii) every sufficiently large even integer may be written as the sum of a prime number and of the product of at most two prime numbers [3]. On the other hand, this conjecture has been numerically verified up to $4 \times 10^{11}$ [7]. This conjecture, if true, would also imply the following property: every odd number greater than or equal to 7 is the sum of three prime numbers. This latter conjecture seems easier to deal with and it gives some results. For instance, Vinogradov [8] proved that it is true for all integer values greater than $3^{3^{15}}$. This bound was then reduced to $10^{43000}$. In this paper we investigate this conjecture numerically and prove it to be true for all integers less than $10^{20}$.

## 2. Principle of the algorithm

Because of the huge size of the set of odd integers considered, systematic verification for all integers is impossible. But it is in fact possible to use partial results of the Goldbach conjecture. Indeed if $N$ is an odd integer, $p$ a prime number and $N-p$ is the sum of two prime numbers, then $N$ is obviously the sum of three prime numbers. Then by virtue of the results of [7], if $N$ is odd and if there is a prime number $p$ such that $N - p < 4.10^{11}$, then $N$ is the sum of three prime numbers. So our algorithm just amounts to exhibiting a sequence of increasing prime numbers $p_i$, $0 \leq i \leq P$, such that $p_0 < 4.10^{11}$, $p_{i+1} - p_i < 4.10^{11}$ for all $0 \leq i \leq P-1$ and $p_P > 10^{20}$. The problem then is to have an efficient prime certificate. Indeed we need at least $250.10^6$ prime numbers. If we use for instance Morain's prover ECPP [1], we see that numbers of 20 decimal digits are certified in approximately 1 second on Sun stations. Thus with forty machines (the number we used) the verification

Received by the editor March 19, 1996 and, in revised form, October 16, 1996.
1991 *Mathematics Subject Classification.* Primary 11P32.
*Key words and phrases.* Odd Goldbach conjecture, primality tests.

would have lasted more than two months. The next section describes the technique we used to avoid this problem.

## 3. Prime certificate

The prime certificate we used was an implementation of Theorem 5 of [2].

**Lemma 1.** *Let $N = RF+1$ be an odd integer where the entire factorization of $F$ is known, $F$ is even and $\gcd(R, F) = 1$. We suppose that there exists an integer $a$ such that $a^{N-1} \equiv 1 \pmod N$ and, for all prime factors $p_i$ of $F$, $\gcd(a^{(N-1)/p_i} - 1, N) = 1$. We pose then $R = 2Fs + r$ with $0 \leq r < 2F$. We suppose $N < 2F^3$, then $N$ is a prime number if and only if either $s = 0$ or $r^2 - 8s$ is not a perfect square.*

In practice, if we directly use this criterion on any integer $N$ possible, we need to factorize $N-1$ to a sufficient part of it. Although it is quite feasible for 20 digit numbers, it would have slowed down the algorithm a great deal. So we decided to search for prime numbers of a special form:

**Theorem 1.** *Let $N = 2^{22}.R + 1$ with $N < 10^{20}$ and $R$ odd. Suppose that there exists an integer $a$ such that $a^{(N-1)/2} \equiv -1 \pmod N$. Then $N$ is prime if and only if either $s = 0$ or $r^2 - 8s$ is not a perfect square, $r$ and $s$ defined as above.*

*Proof.* Application of the previous lemma. Firstly we have indeed $2.(2^{22})^3 > 10^{20} \geq N$. If $a^{(N-1)/2} \equiv -1 \pmod N$, then $a^{(N-1)} \equiv 1 \pmod N$ and

$$\gcd(a^{(N-1)/2} - 1, N) = \gcd((a^{(N-1)/2} + 1) - 2, N) = \gcd(2, N) = 1.$$

Hence the result follows from Lemma 1. □

Now we have:

**Lemma 2.** *Let $N$ be a prime number of the form $10.k + 3$. Then $5^{(N-1)/2} \equiv -1 \pmod N$.*

*Proof.* By application of Euler's criterion and quadratic reciprocity law, we have $5^{(N-1)/2} \equiv (\frac{5}{N}) = (\frac{N}{5}) = (\frac{3}{5}) = -1 \pmod N$, since 3 is a nonquadratic residue modulo 5. □

We then obviously have:

**Theorem 2.** *Let $N = 2^{22}.R + 1$ with $N < 10^{20}$, $N \equiv 3 \pmod{10}$ and $R$ odd. Suppose that $5^{(N-1)/2} \equiv -1 \pmod N$. Then $N$ is prime if and only if either $s = 0$ or $r^2 - 8s$ is not a perfect square, $r$ and $s$ defined as above.*

The least prime number of the forms $2^{22}.R+1$, with $R$ odd, and $10.k+3$ at the same time is equal to $138412033 = 33 \times 2^{22} + 1$. You may note that if you increment or decrement any such number with a multiple of $10.2^{22}$, then this number will still be of the desired form (with the exception of the fact that it is not necessarily a prime number).

Then our algorithm was the following:

(1) Let $p_0 = 138412033$.
(2) If $p_i$ is a prime number according to Theorem 2, increment $i$ by one and set $p_{i+1}$ to $p_i$ plus $95360.2^{22}$ and go on with step 2.
(3) If $p_i$ is not a prime number decrement $p_i$ by $10.2^{22}$ and go on to step 2.
(4) Repeat while $p_i < 10^{20}$.

The nominal value $95360.2^{22}$ is in fact the largest multiple of $10.2^{22}$ smaller than $4.10^{11}$. Then if the latter algorithm ends, the odd Goldbach conjecture is true up to $10^{20}$. You may note that the converse is false.

## 4. Implementations and results

The algorithm was not in fact implemented exactly this way. First, before applying Theorem 2, a partial sieving was effected to discard the numbers having small divisors. The sieve used the first ten prime numbers and was very efficient: a great part of the remaining integers proved to be prime and thus it is quite clear that a larger sieve might have slowed down the algorithm.

The second difference is that the research area was split into 40 subparts and distributed in parallel on 40 Sun stations. The code was written using the GMP multiprecision library [5] and the computations took approximately four days. The first prime of the sequence was 138412033 and the last one was 100000000209366024193. Table 1 gives the first 100 values $k$, giving the prime numbers $N = 5.2^{23}.k+1258213$ used in the derivation.

Table 1. First 100 prime numbers

| | | | | |
|---|---|---|---|---|
| 3 | 9537 | 19059 | 28575 | 38107 |
| 47622 | 57147 | 66651 | 76182 | 85713 |
| 95230 | 104764 | 114297 | 123819 | 133347 |
| 142879 | 152415 | 161950 | 171471 | 181003 |
| 190501 | 200022 | 209541 | 219066 | 228594 |
| 238104 | 247624 | 257157 | 266683 | 276219 |
| 285727 | 295258 | 304785 | 314305 | 323839 |
| 333355 | 342882 | 352405 | 361941 | 371467 |
| 381000 | 390522 | 400048 | 409575 | 419098 |
| 428604 | 438132 | 447663 | 457194 | 466710 |
| 476242 | 485761 | 495291 | 504813 | 514347 |
| 523878 | 533397 | 542932 | 552466 | 561991 |
| 571519 | 581038 | 590565 | 600090 | 609625 |
| 619159 | 628675 | 638196 | 647704 | 657232 |
| 666751 | 676285 | 685821 | 695353 | 704887 |
| 714405 | 723936 | 733452 | 742983 | 752485 |
| 761989 | 771520 | 781054 | 790588 | 800116 |
| 809623 | 819151 | 828679 | 838198 | 847726 |
| 857232 | 866748 | 876268 | 885804 | 895333 |
| 904851 | 914377 | 923910 | 933445 | 942973 |

## 5. Conclusion

This method can clearly be adapted for computing bounds in problems involving four or more prime numbers. However, reaching the bound of $10^{43000}$ encountered in Vinogradov's theorem seems practically unfeasible. But under the assumption of generalized Riemann hypothesis, it has been proved [9] that this bound can be lowered to $3.2 \times 10^{49}$. Such a bound is much more practicable and using the method described above, it should be possible to reach this bound for at most 7 prime numbers in quite a reasonable amount of time and whence to establish the property in its generality under Riemann's hypothesis. It is also conceivable that

more powerful computational resources could also permit to reach this bound for 6 or maybe 5 prime numbers only.

## 6. Acknowledgement

The author wishes to especially thank the referee of the article whose advice on the first version was very helpful and who directed me to the reference [9].

## 7. Late note

During the year 1996, Zinoviev [10] proved under the assumption of the Generalized Riemann Hypothesis, that any odd number greater than $10^{20}$ is the sum of three prime numbers. Thus the current work fills the gap of the remaining cases. It has also to be quoted that Deshouillers et al. [4], also performed a complete verification, by checking the binary Goldbach conjecture up to $1.615 \times 10^{12}$, which allows to deduce the truth of the odd Goldbach conjecture up to $10^{20}$ by a theorem of Schoenfeld, again, under the assumption of the GRH.

## References

[1] A.O.L. Atkin and F. Morain, *Elliptic curves and primality proving*, Math. Comp. **61** (1993), no. 203, 29–68. MR **93m:**11136

[2] J. Brillhart, D.H. Lehmer, and J.L. Selfridge, *New primality criteria and factorizations of* $2^m \pm 1$, Math. Comp. **29** (1975), no. 130, 620–647. MR **52:**5546

[3] J.R. Chen, *On the representation of a large even integer as the sum of a prime and the product of at most two primes*, Kexue Tongbao (1966), no. 17, 385–386.

[4] J.M. Deshouillers, G.Effinger, H. te Riele, and D.Zinoviev, *A complete Vinogradov* 3*-primes theorem under the Riemann Hypothesis*, Preprint, 1997.

[5] T. Grandlung, *The GNU multiple precision arithmetic library*, Technical documentation, 1993.

[6] L. Schnirelmann, *Über additive Eigenschaften von Zahlen*, Math. Ann. (1933), no. 107, 649–660.

[7] M.K. Sinisalo, *Checking the Goldbach conjecture up to* $4.10^{11}$, Math. Comp. **61** (1993), no. 204, 931–934. MR **94a:**11157

[8] I.M. Vinogradov, *Representation of an odd number as the sum of three primes*, Dokl. Akad. Nauk SSSR (1937), no. 15, 169–172.

[9] T.Z. Wang and J.R. Chen, *On odd Goldbach problem under general Riemann hypothesis*, Sci. China Ser. A **36** (1993), no. 6, 682–691. MR **95a:**11090

[10] D.Zinoviev, *On Vinogradov's constant in Goldbach's ternary problem*, J. Number Theory **65** (1997), 334–358. CMP 97:16

IRISA, Campus de Beaulieu, F-35042 Rennes Cédex, France
*E-mail address*: Yannick.Saouter@irit.fr