Totally Goldbach numbers and related conjectures

David van Golstein Brouwers, John Bamberg and Grant Cairns

Goldbach's famous conjecture is that every even integer n greater than 2 is the sum of two primes; to date it has been verified for n up to 10^{17}; see [10, 13]. In order to establish the conjecture for a given even integer n, one optimistic approach is to simply choose a prime $p < n$, and check to see whether $n - p$ is prime. Of course, one has to make a sensible choice of p; if $n - 1$ is prime, one should not choose $p = n - 1$, and there is obviously no point choosing a prime p which is a factor of n. In this paper we examine the set of numbers n for which every "sensible choice" of p works:

Definition 1 A positive integer n is *totally Goldbach* if for all primes $p < n - 1$ with p not dividing n, we have that $n - p$ is prime. We denote by A the set of all totally Goldbach numbers.

It turns out that there are very few totally Goldbach numbers. We find:

$$A = \{1, 2, 3, 4, 5, 6, 8, 10, 12, 18, 24, 30\}.$$

At first sight, it would seem very plausible that A is a small finite set. As everyone knows, the primes tend to become rarer as one proceeds along the real line; if $\pi(n)$ denotes the number of primes no greater than n, then one expects $\pi(n) \le 2\pi(n/2)$ for all $n \ge 6$. Indeed, this was conjectured by Landau and proved by Rosser and Schoenfeld [16]. For n to be a member of A we require as many "sensible" primes p with $p < n/2$ as there are primes p with $n/2 < p < n - 1$. So we would have $n \notin A$ if we could show that $\pi(n)$ is less than $2\pi(n/2)$ minus the number of prime divisors of n. The Prime Number Theorem tells us that the density of the primes falls off on average with $1/\log(n)$. So for big n, there will tend to be considerably more primes between 1 and $n/2$ than there are between $n/2$ and n; in fact, the difference is approximately $(2n \log 2)/(\log n)^2$. The number of prime divisors of n is more difficult to describe, but it grows much more slowly with n [14]. So we expect that large integers n will not belong to A. However, individual numbers seem to care little for expected "average" behaviour. Consistent with the falling frequency of prime numbers, Hardy and Littlewood conjectured (see for example [6]) that $\pi(x + y) \le \pi(x) + \pi(y)$ for all sufficiently large x, y, but there are strongly held contrary views [19].

Before explaining how A can be determined, we first make some connections with three other closely related sets. Consider the set B of positive integers n such that every positive integer $r < n$ which is coprime to n is prime or 1. The members of B are called "very round numbers"; B appears as integer sequence A048597 in Sloane's Integer Sequences web site [17]. Obviously $B \subseteq A$. Knowing A, one finds easily that

$$B = A \backslash \{5, 10\}.$$

According to [12, p. 281], the composition of B was first determined by Schatunowsky (1893) and independently by Wolfskehl (1901). Apparently, it was also obtained by Bonse

This work was commenced while the first author, an undergraduate student at La Trobe University, was a vacation scholar funded by the Australian Mathematical Sciences Institute.

(1907); see [11] for an account of this proof, which is elementary, and makes use of "Bonse's inequality":

$$p_{n+1} < \sqrt{p_1 p_2 \cdots p_n},$$

where p_n denotes the n^{th} prime.

Another closely related set is $C = \{n \in \mathbb{N} : \varphi(n) \leq \tau(n)\}$, where φ is Euler's Totient function and τ is the divisor counting function. Using the simple formulae for φ and τ (see for instance [15, p. 19]), one finds that

$$C = A \backslash \{5\}.$$

This set appears as integer sequence A020490 in Sloane's Integer Sequences web site [17]. Despite the striking similarity between A and C, there is no obvious logical relation between the two sets; is their similarity merely a remarkable coincidence?

When examining Goldbach's conjecture, for a given integer n, it is common to study the number $g(n)$ of ways of representing n as the sum of two primes. Obviously $g(n)$ is less than or equal to the number of primes p with $n/2 \leq p < n-1$. Let the set D consist of those n for which $g(n)$ equals this maximum. Obviously $A \subseteq D$. In [4], Deshouillers, Granville, Narkiewicz and Pomerance showed that the maximum element of D is 210. It is easy to verify then that

$$D = A \cup \{7, 14, 16, 36, 42, 48, 60, 90, 210\}.$$

Of course, the determination of A is a simple consequence of the determination of D; one just checks the elements of D to see which are totally Goldbach.

In their 1993 paper [4], two strategies are given for finding the maximal element n_0 of D. The first strategy relies on the following simple idea: if one can find primes p, q with $n/2 \leq p < n-q$ such that $p \equiv n \pmod{q}$, then $n-p$ would be a multiple of q and $n-p > q$; in this case, $n-p$ would not be prime and so n could not belong to D. According to [4], using estimates for the number of primes $p \leq x$ with $p \equiv a \pmod{q}$, this strategy shows that D is finite and gives $n_0 \leq 10^{520}$. Unfortunately, this leaves too many cases to check, even by computer. Abandoning this approach, the authors of [4] then adopt a different strategy; using an argument involving sieve estimates, they obtain $n_0 \leq 2 \cdot 10^{24}$. Finally, using a computer to check the cases $n \leq 2 \cdot 10^{24}$, they arrive at $n_0 = 210$.

We will show that the first strategy of [4] is sufficient for the determination of our set A; i.e., A can be determined once one has the bound 10^{520}. Our motivation for doing this is two-fold. Firstly, since A is a simpler set, it is only fitting that it have a simpler determination. (This was the original motivation for this work). Secondly, and perhaps more importantly, we will see that this leads us naturally to interesting questions concerning primes in a fixed residue class.

We proceed as follows. First show that A has no element n with $30 < n \leq 2 \cdot 10^6$ by directly applying the definition; this is easily accomplished by computer. Then suppose that $n \in A$ and $n > 2 \cdot 10^6$. Obviously n must be even. Assume first that $n \equiv 1 \pmod{3}$. If q is prime, $q < n-3$ and $q \equiv 1 \pmod{3}$, then $n-q$ is divisible by 3 and hence not prime; as $n \in A$, we conclude that q is a factor of n. Thus

$$n \geq 2 \prod_{\substack{q \text{ prime} \\ q < n-3 \\ q \equiv 1 \bmod 3}} q \;\geq 2 \prod_{\substack{q \text{ prime} \\ q < 2 \cdot 10^6 - 3 \\ q \equiv 1 \bmod 3}} q \;\geq 10^{1000},$$

where the last calculation is performed by computer. Similarly, if $n \equiv 2 \pmod{3}$, then n is at least twice the product of those primes $q < 2 \cdot 10^6 - 3$ for which $q \equiv 2 \pmod{3}$. Once again, one finds that $n \geq 10^{1000}$. So it remains to consider the case where n is divisible by 3 (and hence 6). Arguing as above, for each $a \in \{1, 2, 3, 4\}$,

$$n \geq 6 \prod_{\substack{q \text{ prime} \\ q<n-5 \\ q \equiv a \bmod 5}} q \geq 6 \prod_{\substack{q \text{ prime} \\ q<2\cdot 10^6-5 \\ q \equiv a \bmod 5}} q,$$

for $n \equiv a \pmod 5$ and once again this gives $n \geq 10^{1000}$ in each case. So we may assume that n is divisible by 5 (and hence 30). Proceeding in this manner, we find that for each prime q up to the 351-st prime, 2371, and for each $a = 1, \dots, 2370$, one has $n \geq 10^{1000}$ for $n \equiv a \pmod q$. So we may assume that n is divisible by the product of the first 351 primes; but this also gives $n > 10^{1000}$, as claimed.

In all, the various calculations took less than 24 hours running Maple 9 on a Pentium IV 2.4GHz; the calculations were verified in a little over 2 days, running Mathematica 4 on a Macintosh G3.

Notice that the above argument used the assumption that $n > 2 \cdot 10^6$ to show that $n \geq 10^{1000}$. A complete determination of A, without recourse to [4], would be obtained if the above method could be extended indefinitely and thus turned into an induction argument; that is, assuming that n is greater than some sufficiently large number K, one could try to use the above method to show that n is greater than some larger number K'. Loosely speaking, this approach would work providing the primes q, in any given residue class, are not too sparse. What this asks for is effectively a modular version of Euclid's theorem; recall that Euclid's proof of the infinitude of primes can be rephrased as follows:

$$p_{n+1} < p_1 \cdot p_2 \dots p_n, \text{ for all } n \geq 2$$

where p_i is the i-th prime. This can be regarded as a weak version of Bonse's inequality [11], and a very weak version of Bertrand's postulate [1]. The simplest modular version of Euclid's theorem would be that for all primes q and for all $a = 1, 2, \dots, q-1$,

$$r_{n+1} < r_1 \cdot r_2 \dots r_n, \text{ for all } n \geq 2 \tag{1}$$

where r_i is the i-th prime that is congruent to $a \pmod q$. Unfortunately, this doesn't hold in general. For example, the primes congruent to 3 (mod 13) are $3, 29, 107, \dots$, but $107 \not< 3 \times 29$, and the primes congruent to 5 (mod 61) are $5, 127, 859, \dots$, but $859 \not< 5 \times 127$, etc. In fact, if the twin prime conjecture is true, there are infinitely many counterexamples to (1); indeed, if $q, q+2$ are twin primes, then the first two primes congruent to 2 $\pmod q$ are $r_1 = 2, r_2 = q+2$, and since $2q+2$ is not prime, we must have $r_3 \geq 3q+2$. Hence $r_3 \geq r_1 r_2$.

Nevertheless, computer calculations do seem to show that the following is true for small values of q and n.

Conjecture 1 *For all primes q and for all $a = 1, 2, \dots, q-1$,*

$$r_{n+1} < r_1 . r_2 \dots r_n, \text{ for all } n \geq 3$$

where r_i is the i-th prime that is congruent to a (mod q).

We have been unable to find a statement to this effect in the literature. There are known modular versions of Bertrand's postulate (see [7, 18, 9]), but these results are typically of the form: "for sufficiently large n, ...", and moreover, they are usually not uniform in q and a. The above conjecture is certainly consistent with the prime number theorem modulo q, which gives the asymptotic behaviour of the number $\pi(x; q, a)$ of primes at most x which are congruent to a modulo q:

> "*The expected asymptotic formula* $\pi(x; q, a) \sim x/\varphi(q)\log x$ *as* $x \to \infty$ *has long been known to hold but in all proofs given so far the dependence of the error term on the parameter* q *is rather poorly understood. For all we know it might even be the case that the asymptotic formula begins to represent the true state of affairs only after* x *is (almost) exponentially large compared to* q." from John Friedlander's MathSciNet review of [2].

Notice that Conjecture 1 would follow by induction if we could prove:

Conjecture 2 *For all primes* q *and for all* $a = 1, 2, \dots, q-1$,

(1) $r_4 < r_1 r_2 r_3$,
(2) $r_{n+1} < r_n^2$, *for all* $n \geq 4$,

where r_i *is the* i*-th prime that is congruent to* $a \pmod q$.

Computer calculations appear to support part (1) of Conjecture 2, and in fact for (2), they seem to indicate that $r_{n+1} < r_n^2$, for all $n \geq 3$. Notice that $r_n \geq (2n-3)q + a$. This is simply because the numbers congruent to $a \pmod q$ are:

$$a, q+a, 2q+a, 3q+a, \dots$$

so if a is odd, the smallest possible r_i would be

$$a, 2q+a, 4q+a, 6q+a, \dots$$

while if a is even, the smallest possible r_i would be

$$q+a, 3q+a, 5q+a, \dots$$

if $a \neq 2$ and

$$a, q+a, 3q+a, \dots$$

if $a = 2$. In each case, $r_n \geq (2n-3)q + a$. So, to establish the second part of Conjecture 2, it suffices to show that $r_{n+1} < (2n-3)^2 q^2$, or the somewhat stronger:

Conjecture 3 $r_n < 4(n-3)^2 q^2$, *for all* $n \geq 4$, *all primes* q *and all* $a = 1, \dots, q-1$.

In fact, it is easy to see, using the same kind of elementary arguments used above, that Conjecture 3 also implies the first part of Conjecture 2. So we have

$$\text{Conjecture 3} \Rightarrow \text{Conjecture 2} \Rightarrow \text{Conjecture 1}.$$

Moreover, it is not difficult to show that by the Bombieri–Friedlander–Iwaniec Theorem [3], Conjecture 3 holds "with few exceptions". In fact, computer investigations indicate that the following may be true:

Conjecture 4 $r_n < (n + n\log n)q^2$, *for all* $n \geq 1$, *all primes* q *and all* $a = 1, \dots, q-1$.

This conjecture is a generalization of an old conjecture of Schinzel and Sierpinski (see [12, p. 280 and p. 397]): $r_1 < q^2$ for all primes q and all $a = 1, \dots, q-1$. At present the best result is Meng's improvement of Heath-Brown's version of Linnik's theorem [8]: $r_1 < q^{4.5}$. So Conjecture 4 may be a long way away.

Acknowledgements

We thank Andrew Granville for his communications regarding the estimates which were used in [4], and we are also grateful to the referee for their valuable comments.

References

[1] M. Aigner and G.M. Ziegler, *Proofs from The Book* (Springer-Verlag Berlin 2004).

[2] R.C. Baker and G. Harman, The Brun-Titchmarsh theorem on average, in *Analytic number theory, Vol. 1* (Birkhäuser Boston 1996), 39–103.

[3] E. Bombieri, J.B. Friedlander and H. Iwaniec, *Primes in arithmetic progressions to large moduli. III*, J. Amer. Math. Soc., **2** (1989) 215–224.

[4] J-M. Deshouillers, A. Granville, W. Narkiewicz and C. Pomerance, *An upper bound in Goldbach's problem*, Math. Comp. **61** (1993), 209–213.

[5] P. Dusart, *Inégalités explicites pour* $\psi(X)$, $\theta(X)$, $\pi(X)$ *et les nombres premiers*, C. R. Math. Acad. Sci. Soc. R. Can., **21** (1999), 53–59.

[6] ——, *Sur la conjecture* $\pi(x+y) \leq \pi(x) + \pi(y)$, Acta Arith., **102** (2002) 295–308.

[7] E. Fogels, *On the existence of primes in short arithmetical progressions*, Acta Arith. **6** (1960/1961), 295–311.

[8] Z. Meng, *The distribution of the zeros of* L*-functions and the least prime in some arithmetic progression*, Sci. China Ser. A, **43** (2000), 937–944.

[9] P. Moree, *Bertrand's postulate for primes in arithmetical progressions*, Comput. Math. Appl. **26** (1993), 35–43.

[10] T. Oliveira e Silva, *"Goldbach conjecture verification" web page*, http://www.ieeta.pt/~tos/goldbach.html

[11] H. Rademacher and O. Toeplitz, *The enjoyment of mathematics* (Princeton University Press 1957).

[12] P. Ribenboim, *The new book of prime number records* (Springer-Verlag New York 1996).

[13] J. Richstein, *Verifying the Goldbach conjecture up to* $4 \cdot 10^{14}$, Math. Comp. **70** (2001), 1745–1749.

[14] G. Robin, *Estimation de la fonction de Tchebychef* θ *sur le* k*-ième nombre premier et grandes valeurs de la fonction* $\omega(n)$ *nombre de diviseurs premiers de* n, Acta Arith. **42** (1983), 367–389.

[15] H.E. Rose, *A course in number theory* (Clarendon Press New York 1994).

[16] J.B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. **6** (1962), 64–94.

[17] N.J.A. Sloane, (2004), The On-Line Encyclopedia of Integer Sequences, published electronically at http://www.research.att.com/~njas/sequences/

[18] T. Tatuzawa, *On Bertrand's problem in an arithmetic progression*, Proc. Japan Acad. **38** (1962), 293–294.

[19] A. van der Poorten and T. Ah-Mah, *On the twin prime conjecture*, AustMS Gazette **31** (2004) 36–39.

Department of Mathematics, La Trobe University, Melbourne, VIC 3086
E-mail: dave@purplehades.com

School of Mathematics and Statistics, The University of Western Australia, Crawley, WA 6009
E-mail: john.bam@maths.uwa.edu.au

Department of Mathematics, La Trobe University, Melbourne, VIC 3086
E-mail: G.Cairns@latrobe.edu.au

Received 13 April 2004, accepted 11 June 2004.