Giuga's conjecture on primality

D. Borwein[*], J. M. Borwein[‡], P. B. Borwein[*], R. Girgensohn[§]

Abstract. G. Giuga conjectured that if an integer n satisfies $\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \mod n$, then n must be a prime. We survey what is known about this interesting and now fairly old conjecture.

Giuga proved that n is a counterexample to his conjecture if and only if each prime divisor p of n satisfies $(p-1) \mid (n/p-1)$ and $p \mid (n/p-1)$. Using this characterization, he proved computationally that any counterexample has at least 1,000 digits; equipped with more computing power, E. Bedocchi later raised this bound to 1,700 digits. By improving on their method, we determine that any counterexample has at least 13,800 digits.

We also give some new results on the second of the above conditions. This leads, in our opinion, to some interesting questions about what we call Giuga numbers and Giuga sequences.

Keywords: Primality, Carmichael numbers, Computational number theory.
AMS (1991) subject classification: Primary 11A41, 11Y11, Secondary 11Y50.

[*]Research supported by NSERC

[‡]Research supported by NSERC and the Shrum Endowment at Simon Fraser University.

[§]Research supported by a DFG fellowship

1 Introduction

In 1950, G. Giuga formulated the following conjecture ([3]).

Conjecture. For each integer n it is true that

$$n \text{ is prime} \quad \Longleftrightarrow \quad s_n := \sum_{k=1}^{n-1} k^{n-1} \equiv -1 \bmod n.$$

Fermat's little theorem says that if p is a prime, then $k^{p-1} \equiv 1 \bmod p$ for $k = 1, \ldots, p-1$. Therefore, for each prime p, $s_p \equiv -1 \bmod p$. The question becomes:

Does there exist a non-prime n such that $s_n \equiv -1 \bmod n$?

This question has resisted solution for more than forty years. After surveying what is known about the conjecture, we will give several new results here which might suggest directions of further investigations.

The key to dealing with Giuga's conjecture is the following theorem, which was proved by Giuga in his original paper. A proof can also be found in [5]. For the sake of completeness, we give the proof here.

Theorem 1. *$s_n \equiv -1 \bmod n$ if and only if for each prime divisor p of n we have $(p-1) \mid (n/p-1)$ and $p \mid (n/p-1)$.*

Proof. It is well-known and an easy consequence of considering residue classes (see [5], p. 16) that for a prime p, we have

$$\sum_{k=1}^{p-1} k^{n-1} \equiv \begin{cases} -1 \mod p & \text{if } (p-1) \mid (n-1), \\ 0 \mod p & \text{if } (p-1) \not\mid (n-1). \end{cases}$$

Therefore, for each prime divisor p of n with $n = p \cdot q$, we get

$$\sum_{k=1}^{n-1} k^{n-1} \equiv q \sum_{k=1}^{p-1} k^{n-1} \equiv \begin{cases} -q \mod p & \text{if } (p-1) \mid (n-1), \\ 0 \mod p & \text{if } (p-1) \not\mid (n-1). \end{cases} \tag{1}$$

Assume that $s_n \equiv -1 \mod n$. Then for each prime divisor p of n, $n = p \cdot q$, we have

$$-1 \equiv \begin{cases} -q \mod p & \text{if } (p-1) \mid (n-1), \\ 0 \mod p & \text{if } (p-1) \not\mid (n-1). \end{cases} \tag{2}$$

This is only possible if $(p-1) \mid (n-1) = q(p-1)+(q-1)$. So $(p-1) \mid (q-1)$. It then also follows from (2) that $-1 \equiv -q \mod p$, or $p \mid (q-1)$.

On the other hand, assume that $p \mid (q-1)$ and $(p-1) \mid (q-1)$. It then follows from (1) that $s_n \equiv -q \mod p$; since $q \equiv 1 \mod p$, we have that $s_n \equiv -1 \mod p$ for each prime divisor p of n. Now, n must be squarefree: If it were not, then there would exist a prime divisor p of n with $p \mid q$; this contradicts $p \mid (q-1)$. Since each of the distinct prime divisors of n divides $s_n + 1$, this is also true for n. In other words, $s_n \equiv -1 \mod n$. ☺

As noted in the proof, every counterexample to Giuga's conjecture must be squarefree. Squarefree composite numbers which satisfy the first of these two conditions have been investigated in their own right: they are called *Carmichael numbers*. They were introduced by Carmichael in 1910. Carmichael numbers are of interest because they are "pseudo-prime" in the following sense (Korselt's criterion, 1899): *n divides $a^n - a$ for all integers a if and only if n is squarefree and $p-1$ divides $n/p-1$ for all prime divisors p of n.* The Carmichael condition

$$(p-1) \mid (n/p-1) \text{ for all prime divisors } p \text{ of } n$$

is equivalent to the condition

$$(p-1) \mid (n-1) \text{ for all prime divisors } p \text{ of } n.$$

Note that any Carmichael number is odd. (Assume that n is even. It has at least one other prime factor p besides 2. Then the even number $p-1$ divides the odd number $n-1$, which is a contradiction.) The smallest Carmichael number is $561 = 3 \cdot 11 \cdot 17$. The next two Carmichael numbers are $1105 = 5 \cdot 13 \cdot 17$ and $1729 = 7 \cdot 13 \cdot 19$. It has only recently been proved that there are infinitely many Carmichael numbers (see [1]).

In order to refer easily to the second condition as well, we will call any composite number n with $p \mid (n/p-1)$ for all prime divisors p of n a *Giuga number*. As we saw in the proof of Theorem 1, any Giuga number is squarefree. Moreover, one can prove the following equivalence along the lines of that proof (with $n-1$ replaced by $\varphi(n)$, where φ is the Euler (totient) function): *n is a Giuga number if and only if $\sum_{k=1}^{n-1} k^{\varphi(n)} \equiv -1 \mod n$.* In his original paper, Giuga proved another equivalence: *n is a Giuga number if and only if*

$$\sum_{p \mid n} \frac{1}{p} - \prod_{p \mid n} \frac{1}{p} \in \mathbb{N}.$$

This equivalence will be of great importance throughout this paper. We will give a slightly generalized version of Giuga's proof below. The smallest Giuga number is 30: $1/2 + 1/3 + 1/5 - 1/30 = 1$. The next two Giuga numbers are 858: $1/2 + 1/3 + 1/11 + 1/13 - 1/858 = 1$, and 1722: $1/2 + 1/3 + 1/7 + 1/41 - 1/1722 = 1$. We do not know if there are infinitely many Giuga numbers.

Giuga's theorem can now be restated as

Theorem. *A composite integer n satisfies $s_n \equiv -1 \bmod n$ if and only if it is both a Carmichael number and a Giuga number.*

Giuga's conjecture is that such a number cannot exist.

The smallest odd Giuga number has at least 9 prime factors, since with a smaller number of prime factors the sum $1/p_1 + \ldots + 1/p_m - 1/n$ is smaller than 1. However, this lower bound for a counterexample increases dramatically if we take into account that it must also be a Carmichael number. Any Carmichael number n has the following property: If p is a prime factor of n, then for no k is $kp + 1$ a prime factor of n. (If it were, then we would have $(kp + 1) - 1 = kp \mid (n - 1)$ and $p \mid n$, which is a contradiction.) So, for example, no Carmichael number has the prime factors 3 and 7 at the same time. This property was used by Giuga to prove computationally that each counterexample has at least 1000 digits. Later, E. Bedocchi ([2]) used the same method to prove that each counterexample has at least 1700 digits. We will describe the method in Section 2 of this article. We have been able to improve on this method by reducing the number of cases to be looked at and have shown computationally that any counterexample has no less than $13,800$ digits.

We believe that an approach to prove or refute Giuga's conjecture in general is to study Giuga numbers in more depth; we will do this in Section 3 of this paper. It turns out that there is much more structure to be studied if we drop the condition that the numbers p in the definition be prime. This leads us to the following definition.

Definition. *A finite, increasing sequence of integers, $[n_1, \ldots, n_m]$, is called a Giuga sequence if*

$$\sum_{i=1}^{m} \frac{1}{n_i} - \prod_{i=1}^{m} \frac{1}{n_i} \in \mathbb{N}.$$

The proof of the following equivalence is due to Giuga in the case that the n_i are primes.

Theorem 2. *A finite, increasing sequence* $[n_1, \ldots, n_m]$ *is a Giuga sequence if and only if it satisfies* $n_i \mid (n_1 \cdots n_{i-1} \cdot n_{i+1} \cdots n_m - 1)$ *for* $i = 1, \ldots, m$.

Proof. Write $n := n_1 \cdots n_m$ and $q_i := n/n_i$. Note that the sequence is a Giuga sequence if and only if $n \mid (q_1 + \ldots + q_m - 1)$.

The "only if" part of the asserted equivalence now follows immediately from this.

On the other hand, assume that $n_i \mid (q_i - 1)$ or $n_i^2 \mid (n - n_i)$ for all i. Multiplying leads to $n^2 \mid (n - n_1) \cdots (n - n_m)$. In evaluating this product we can drop all multiples of n^2. We therefore get $n^2 \mid (n\,(q_1 + \ldots + q_m) - n_1 \cdots n_m) = n\,(q_1 + \ldots + q_m - 1)$. Therefore, $n \mid (q_1 + \ldots + q_m - 1)$, which means that $[n_1, \ldots, n_m]$ is a Giuga sequence. ☺

Note that each two distinct elements n_i, n_j in a Giuga sequence are relatively prime ($n_i \mid (n/n_i - 1)$, but $n_j \mid n/n_i$). When n is a Giuga number, it gives rise to a Giuga sequence (its prime factors), but in general it is conceivable that an integer n can have two different factorizations, both of which are Giuga sequences. However, we know of no example of this. We do know that there is an infinity of Giuga sequences; we will show this in Section 3 of this article.

In the same way, Carmichael numbers can be generalized to Carmichael sequences: *A finite, increasing sequence,* $[a_1, \ldots, a_m]$*, is called a Carmichael sequence if* $(a_i - 1) \mid (a_1 \cdots a_m - 1)$ *for* $i = 1, \ldots, m$. Note that a Carmichael sequence has either exclusively odd or exclusively even elements and that its elements need not be relatively prime. As with Carmichael numbers, any two distinct factors a_i, a_j in a Carmichael sequence satisfy $a_i \not\equiv 1 \bmod a_j$ (or, equivalently, $a_j \nmid (a_i - 1)$). Carmichael sequences occur in much greater profusion than Giuga sequences. At the end of Section 3 we will construct some infinite families of Carmichael sequences.

Giuga's conjecture would be proved if one were to show that no Giuga sequence can be a Carmichael sequence. This, in turn, would be proved if it can be shown that any Giuga sequence must contain two factors n_i, n_j with $n_j \mid (n_i - 1)$. It might even be true that every Giuga sequence contains an even factor; Giuga's conjecture would follow from this. We have found no Giuga sequence which consists of odd factors only, but this is probably a consequence of the size of the problem.

In Section 4 of this article, we will give a list of open questions concerning Giuga sequences and Giuga's conjecture.

2 Computing lower bounds for a counterexample

As we have seen, any counterexample to Giuga's conjecture must be a squarefree odd number with prime factorization $n = q_1 \cdots q_k$ such that

(i) $q_i \not\equiv 1 \bmod q_j$ for all i, j, and

(ii) $1/q_1 + \ldots + 1/q_k > 1$.

Giuga and Bedocchi used these two properties to compute lower bounds for a counterexample in the following way. For $m \in \mathbb{N}$, denote by p_m the m-th odd prime. A finite set of odd primes, $\{q_1, \ldots, q_k\}$, is called *normal* if condition (i) obtains. For each $m \in \mathbb{N}$, let S_m be the set of all normal sets with maximum element smaller than p_m. For each $S \in S_m$, $S = \{q_1, \ldots, q_k\}$, define the set

$$T_m(S) = \{q_1, \ldots, q_k,\ q_{k+1}, \ldots, q_r\}$$

to be the smallest set of odd primes which contains S, and is such that $q_j \geq p_m$ and $S \cup \{q_j\}$ is normal for $j > k$, and $\sum_{j=1}^{r} 1/q_j > 1$. Let $r_m(S)$ be the number of elements of $T_m(S)$. For example,

$$T_6(\{3,5\}) = \{3, 5,\ 17, 23, 29, 47, 53, \ldots, 7919, 7937\},\ r_6(\{3,5\}) = 383$$

and

$$T_1(\{\}) = \{3, 5, 7, 11, 13, 17, 19, 23, 29\},\ r_1(\{\}) = 9.$$

Now define the sequence $(i_m)_{m \in \mathbb{N}}$ by

$$i_m = \min\{r_m(S) \mid S \in S_m\}.$$

As Giuga observed, this sequence is non-decreasing; we will see shortly why this is the case.

Now, the number of prime factors of a counterexample to Giuga's conjecture exceeds i_m for each $m \in \mathbb{N}$. Indeed, the prime factors form a normal set, and the subset S of the factors smaller than p_m is a member of S_m. Since any normal set of primes which contains S and satisfies condition (ii) above must contain at least $r_m(S)$ elements, we have that n has at least $r_m(S) \geq i_m$ prime factors; this is true for any $m \in \mathbb{N}$. So, any counterexample is bigger than $\prod_{j=1}^{i_m} p_j$, and therefore has at least the same number of digits as this product. Giuga estimated $i_9 > 361$, this yields more than 1000 digits;

Bedocchi computed $i_9 = 554$, this yields more than 1700 digits. (Note that Giuga and Bedocchi used a slightly different definition for i_m; this is why their numbers differ from our numbers by 1.)

To compute i_m, one has to find $r_m(S)$ for all $S \in S_m$. Since the number of elements of S_m increases geometrically with m, the time needed to compute i_m gets out of hand quickly. With our R4000 Challenge server and the symbolic manipulation package Maple, we were able, with considerable effort, to compute $i_{19} = 825$. At this point in time we started looking for a better algorithm, something which allows us to look at only some sets in S_m, not all of them. Fortunately enough, we found just such an algorithm. It is based on the following observation. Consider a set $S \in S_m$ and the associated value $r_m(S)$. Now, S has at most two "successors" in the set S_{m+1}, namely S itself and the set $S' = S \cup \{p_m\}$. We will now show that $r_{m+1}(S) \geq r_m(S)$ and $r_{m+1}(S') \geq r_m(S)$. In fact, there are two cases:

Case (i): $S \cup \{p_m\}$ is normal. Then S has the two successors S and S' in S_{m+1}. Also, we have $p_m \in T_m(S)$. However, $p_m \notin T_{m+1}(S)$, but every other element of $T_m(S)$ is contained in $T_{m+1}(S)$. So, $T_{m+1}(S)$ must contain at least one higher prime for the sum $\sum_{q \in T_{m+1}(S)} 1/q$ to exceed 1. Therefore, $r_{m+1}(S) \geq r_m(S)$. As regards S', the set $T_m(S)$ may contain primes which are congruent to 1 mod p_m. These are missing in $T_{m+1}(S')$, since $p_m \in S'$. For each of these we need at least one higher prime for the sum $\sum_{q \in T_{m+1}(S')} 1/q$ to exceed 1. Again, $r_{m+1}(S') \geq r_m(S)$.

Case (ii): $S \cup \{p_m\}$ is not normal. Then the only successor of S in S_{m+1} is S itself. Also, $T_m(S) = T_{m+1}(S)$; the prime p_m is not contained in either set. Therefore, $r_m(S) = r_{m+1}(S)$.

This shows that the sequence i_m is indeed non-decreasing. But it shows more: the values $r_{k+1}, r_{k+2}, \ldots$ for all of the successors in $S_{k+1}, S_{k+2}, \ldots$ of a given set $S \in S_k$ do not fall below $r_k(S)$. If we want to compute i_m and already know an upper bound $I \geq i_m$, then we do not have to look at any successor in the sets $S_{k+1}, \ldots, S_m$ of a set $S \in S_k$ with $r_k(S) > I$. So the natural way to do this is to do it iteratively: Start with $A_1 := S_1$, and let A_{k+1} consist of the successors in S_{k+1} of all $S \in A_k$ with $r_k(S) \leq I$. Then $i_m = \min\{r_m(S) \mid S \in A_m\}$. If I is close to i_m, then this significantly reduces the number of sets to consider.

The bound I can of course be chosen as the value $r_m(S)$ for some $S \in S_m$. The iterative method saves the most time if one correctly guesses which

sets have low values. By looking at preliminary computational results, we discovered that the following rule seems to hold. Let $L_5 := \{5, 7\}$, and define

$$L_{k+1} := \begin{cases} L_k \cup \{p_k\} & \text{if } L_k \cup \{p_k\} \text{ is normal,} \\ L_k & \text{otherwise.} \end{cases}$$

Then it seems that for $m \geq 5$, $r_m(L_m) = i_m$. We have no proof that this is always true, but having discovered that the sets L_m yield good upper bounds for i_m, we employed our iterative method with these upper bounds to compute all values i_m for $m \leq 100$ in Maple and later for $m \leq 135$ in C. We always found that $r_m(L_m) = i_m$.

It was, by the way, surprisingly difficult to translate what was a fairly straight-forward Maple program into C. While Maple handled the data structures we required (lists of sets of variable length) easily, it was a non-trivial problem to implement these in C. We gained a speed-up of a factor of around 5 (for m around 100), though. Even with this speed-up, the last case ($m = 135$) took 303 cpu hours, and the "curse of exponentiality" makes further computation close to impracticable. We thank Gerald Kuch (now a graduate student at the University of Waterloo) for doing this conversion from Maple to C.

Here are some of the i_m (the first nine of these are also given by Bedocchi in [2]): $i_1 = 9$, $i_2 = 27$, $i_3 = 65$, $i_4 = 114$, $i_5 = 127$, $i_6 = 202$, $i_7 = 278$, $i_8 = 323$, $i_9 = i_{10} = i_{11} = 554$, $i_{12} = i_{13} = i_{14} = i_{15} = i_{16} = 704$, $i_{17} = i_{18} = 751$, $i_{19} = i_{20} = 825$, $\ldots$, $i_{49} = i_{50} = 2121$, $\ldots$, $i_{74} = i_{75} = 2657$, $\ldots$, $i_{99} = i_{100} = i_{101} = 3050$, $\ldots$, $i_{131} = i_{132} = i_{133} = i_{134} = i_{135} = 3459$. $i_{100} = 3050$ implies that any counterexample to Giuga's conjecture has at least 12055 digits, $i_{135} = 3459$ implies that any counterexample has at least 13887 digits.

As Bedocchi points out in [2], this method is inherently incapable of showing that Giuga's conjecture holds for all integers: the set L_{27692} is normal, has 8135 elements and satisfies $\sum_{q \in L_{27692}} 1/q > 1$. Therefore, $i_m \leq 8135$ for all $m \geq 27692$.

3 Giuga sequences

Recall that a Giuga sequence is a finite, increasing sequence of integers, $[n_1, \ldots, n_m]$, such that

$$\sum_{i=1}^{m} \frac{1}{n_i} - \prod_{i=1}^{m} \frac{1}{n_i} \in \mathbb{N}.$$

When dealing with Giuga's conjecture, we are mainly interested in Giuga sequences which consist exclusively of primes; we will call these *proper* Giuga sequences. However, Giuga sequences, proper or not, are interesting objects in their own right; in this section we will give some of their properties.

We have computed all Giuga sequences up to length 7 and some of length 8. There is no Giuga sequence of length 2; one sequence of length 3 ($[2, 3, 5]$); two sequences of length 4 ($[2, 3, 7, 41]$ and $[2, 3, 11, 13]$); three sequences of length 5 ($[2, 3, 7, 43, 1805]$, $[2, 3, 7, 83, 85]$ and $[2, 3, 11, 17, 59]$); 17 sequences of length 6; 27 sequences of length 7; and hundreds of sequences of length 8.

So far, we know only 11 Giuga numbers (or proper Giuga sequences). They are

3 factors:

$30 = 2 \cdot 3 \cdot 5$

4 factors:

$858 = 2 \cdot 3 \cdot 11 \cdot 13$
$1722 = 2 \cdot 3 \cdot 7 \cdot 41$

5 factors:

$66198 = 2 \cdot 3 \cdot 11 \cdot 17 \cdot 59$

6 factors:

$2214408306 = 2 \cdot 3 \cdot 11 \cdot 23 \cdot 31 \cdot 47057$
$24423128562 = 2 \cdot 3 \cdot 7 \cdot 43 \cdot 3041 \cdot 4447$

7 factors:

$432749205173838 = 2 \cdot 3 \cdot 7 \cdot 59 \cdot 163 \cdot 1381 \cdot 775807$
$14737133470010574 = 2 \cdot 3 \cdot 7 \cdot 71 \cdot 103 \cdot 67213 \cdot 713863$
$550843391309130318 = 2 \cdot 3 \cdot 7 \cdot 71 \cdot 103 \cdot 61559 \cdot 29133437$

8 factors:

$$244197000982499715087866346 =$$
$$2 \cdot 3 \cdot 11 \cdot 23 \cdot 31 \cdot 47137 \cdot 28282147 \cdot 3892535183$$
$$554079914617070801288578559178 =$$
$$2 \cdot 3 \cdot 11 \cdot 23 \cdot 31 \cdot 47059 \cdot 2259696349 \cdot 110725121051$$

For all of these examples, the 'sum minus product' value is 1; to reach any higher value, the sequence would have to have at least 59 factors. To find all Giuga sequences of a given length, one could check all sequences of this length whose elements are not too large (the sum over their reciprocals must be greater than 1). However, the number of these grows exponentially; even for length 7 there are too many to check them all. Fortunately, we have the following theorem which tells us how to find all Giuga sequences of length m with a given initial segment of length $m-2$.

Theorem 3. *(a) Take an initial sequence of length $m-2$, $[n_1, \ldots, n_{m-2}]$. Let*

$$P = n_1 \cdots n_{m-2},\ S = 1/n_1 + \ldots + 1/n_{m-2}.$$

Fix an integer $v > S$ (this will be the sum minus product value). Take any integers a, b with $a \cdot b = P(P + S - v)$ and $b > a$. Let

$$n_{m-1} := (P + a)/P(v - S),\ n_m := (P + b)/P(v - S).$$

Then

$$S + 1/n_{m-1} + 1/n_m - 1/Pn_{m-1}n_m = v.$$

The sequence $[n_1, \ldots, n_{m-1}, n_m]$ is a Giuga sequence if and only if n_{m-1} is an integer.

(b) Conversely, if $[n_1, \ldots, n_{m-1}, n_m]$ is a Giuga sequence with sum minus product value v, and if we define

$$a := n_{m-1}P(v - S) - P,\ b := n_m P(v - S) - P$$

(with P and S the product and the sum of the first $m-2$ terms) then a and b are integers and $a \cdot b = P(P + S - v)$.

Proof. (a) First we have to check that with these definitions for n_{m-1} and n_m we have in fact $S + 1/n_{m-1} + 1/n_m - 1/Pn_{m-1}n_m = v$. These are straight-forward calculations:

$$S + P(v-S)/(P+a) + P(v-S)/(P+b) - P^2(v-S)^2/P(P+a)(P+b) = v$$

if and only if

$$P/(P+a) + P/(P+b) - P(v-S)/(P+a)(P+b) = 1$$

if and only if

$$P/(P+a) + P/(P+b) - (P^2-ab)/(P+a)(P+b) = 1,$$

which is true.

This means that the completed sequence is a Giuga sequence if and only if both n_{m-1} and n_m are integers. It remains to be shown that n_{m-1} is integer if and only if n_m is. Because of the symmetry, it is enough to prove the implication in one direction. If

$$P(v-S) \mid (P+a)$$

then

$$P(v-S) \mid (P+a)(P+b) = 2P^2 + (a+b)P - (v-S)P,$$

so

$$P(v-S) \mid (2P^2 + (a+b)P) = P(P+a+P+b),$$

so

$$P(v-S) \mid P(P+b)$$

(since $P(v-S)$ divides $P+a$).

The assertion follows if we show that $\gcd(P(v-S), P) = 1$. Assume that there is a prime p with $p \mid P(v-S)$ and $p \mid P$, $p \mid n_i$, say. Since $\gcd(n_i, n_j) = 1$ for i not equal to j, p does not divide any of the other factors. Since p divides

$$P(v-S) = vP - (n_2 \cdots n_{m-2} + \ldots + n_1 \cdots n_{m-3}),$$

we can drop all terms on the right-hand side with a factor n_i to get

$$p \mid n_1 \cdots n_{i-1} \cdot n_{i+1} \cdots n_{m-2},$$

which is a contradiction.

(b) It is clear that these a and b are integers. It remains to be checked that $a \cdot b = P(P+S-v)$. We have

$$\begin{aligned} a \cdot b &= -P^2(v-S)(n_{m-1}+n_m) + P^2 n_{m-1} n_m (v-S)^2 + P^2 \\ &= P^2(S-v)n_{m-1}n_m \cdot (1/n_{m-1} + 1/n_m + S - v) + P^2 \\ &= P^2(S-v)n_{m-1}n_m \cdot 1/(n_{m-1}n_m P) + P^2 \\ &= P(P+S-v). \end{aligned}$$

☺

We used this theorem to compute our Giuga sequences; this works well for sequences up to length 7, but for length 8 and higher there are still too many possible initial segments to check.

All Giuga sequences we have found so far contain an even factor (it is usually the factor 2, but there are two sequences of length 9 which contain 4 instead). So far, we have not been able to find a sequence with only odd factors. Since any counterexample to Giuga's conjecture would be an odd Giuga number, it would be of some interest to find at least one such sequence. Let $n := n_1 \cdots n_m$. The Giuga equation $1/n_1 + \ldots + 1/n_m - 1/n = v$ is equivalent to $n/n_1 + \ldots n/n_m - 1 = nv$; by considering this equation modulo 4, it is quite straightforward to show that if all factors n_i are odd, then necessarily $m - v \equiv 1 \bmod 4$. (In fact, assume that the first k factors are congruent to -1 modulo 4, and the other $m - k$ factors are congruent to 1 modulo 4. Then the equation reduces to

$$-1 \equiv v(-1)^k - k(-1)^{k-1} - (m-k)(-1)^k = (-1)^k(v - m + 2k) \mod 4,$$

from which $m - v \equiv 1 \bmod 4$ follows.) If we look for odd sequences with value $v = 1$, then we only have to check sequences of length $m \equiv 2 \bmod 4$. The cases $m = 2$ and $m = 6$ can be ruled out because we need at least nine relatively prime odd integers for the sum of their reciprocals to exceed 1. Now, $m = 10$ can be ruled out computationally, with the use of Theorem 3. But this is where computational feasibility ends. For $m = 14$, there are just too many initial segments to check; another approach is needed here.

We asserted in the introduction that there are infinitely many Giuga sequences. As the following proposition tells us, it is possible to generate longer Giuga sequences out of shorter ones with certain properties.

Theorem 4. *Take a Giuga sequence of length m, $[n_1, \ldots, n_{m-1}, n_m]$, which satisfies*

$$n_m = n_1 \cdots n_{m-1} - 1. \tag{3}$$

Let

$$\tilde{n}_m := n_1 \cdots n_{m-1} + 1,\ \tilde{n}_{m+1} := n_1 \cdots n_{m-1}\tilde{n}_m - 1.$$

Then $[n_1, \ldots, n_{m-1}, \tilde{n}_m, \tilde{n}_{m+1}]$ is also a Giuga sequence with the same sum minus product value.

Proof. Let $P := n_1 \ldots n_{m-1}$, $S := 1/n_1 + \ldots + 1/n_{m-1}$. Then $n_m = P - 1$, $\tilde{n}_m = P + 1$ and $\tilde{n}_{m+1} = P^2 + P - 1$. Both sequences have the same sum

minus product value if and only if

$$S+\frac{1}{P-1}-\frac{1}{P(P-1)}=S+\frac{1}{P+1}+\frac{1}{P^2+P-1}-\frac{1}{P(P+1)(P^2+P-1)};$$

the latter equation is true for all S and P. ☺

Note that if the shorter Giuga sequence has property (3), then so has the longer one. Since the sequence $[2,3,5]$ also has this property, this proves that there are Giuga sequences of any length. (Note also that each of the sequences which occur in such a recursion will contain an even factor.) However, the sequences arrived at by this recursion are not the only Giuga sequences there are. In each step from length m to $m+1$, other Giuga sequences seem to pop out of thin air, some of them with property (3) (and thus leading to new recursions), some without.

Explicitly, two infinite families are

(a) $n_1=2$, $n_k=n_1\cdots n_{k-1}+1$ for $k=2,\ldots,m-1$, $n_m=n_1\cdots n_{m-1}-1$;

(b) $n_1=2$, $n_2=3$, $n_3=11$, $n_4=23$, $n_5=31$, $n_k=n_1\cdots n_{k-1}+1$ for $k=6,\ldots,m-1$, $n_m=n_1\cdots n_{m-1}-1$.

Recall that a Carmichael sequence is a finite increasing sequence of integers, $[a_1,\ldots,a_m]$, such that

$$(a_i-1)\mid\left(\prod_{j=1}^{m}a_j-1\right)\ \text{for } i=1,\ldots,m.$$

At the end of the introduction we stated that there is a profusion of Carmichael sequences; in fact, there are infinitely many of them with any number of factors. A trivial example would be the sequence $[a,\ldots,a]$ for any $a\in\mathbb{N}$, but this is too cheap. We now conclude this section by giving a somewhat less trivial construction. We omit the computations here, since they are essentially simple but would enlarge this side remark unduly.

There are infinitely many Carmichael sequences of length 3; in fact, the following construction gives us *all* 3-factor Carmichael sequences. Take three integers $b1,b2,b3\in\mathbb{N}$ which are pairwise co-prime. Let $c\in\mathbb{N}$ be the solution of the congruence $(b_1b_2+b_1b_3+b_2b_3)\,c\equiv-(b_1+b_2+b_3) \bmod b_1b_2b_3$. (Such a solution exists and is unique modulo $b_1b_2b_3$, because the integers

are pairwise co-prime. Equivalently, one can also solve the system of congruences $b_2b_3c \equiv -b_2-b_3 \bmod b_1$, $b_1b_3c \equiv -b_1-b_3 \bmod b_2$, $b_1b_2c \equiv -b_1-b_2 \bmod b_3$.) Then $a_1 := cb_1 + 1$, $a_2 := cb_2 + 1$, $a_3 := cb_3 + 1$ is always a Carmichael sequence, and every 3-factor Carmichael sequence is of this form. For example, if we choose $b_1 = 1$, $b_2 = 2$ and $b_3 = 3$, then we get Chernick's observation (see [1]) that $a_1 := 6k+1$, $a_2 := 12k+1$, $a_3 := 18k+1$ is always a Carmichael sequence.

The following two recursions produce Carmichael sequences of length $m+1$ and $m+2$ out of the Carmichael sequence $[a_1, \ldots, a_m]$.

(a) Let $a_{m+1} := \prod_{j=1}^{m} a_j$. Then $[a_1, \ldots, a_m, a_{m+1}]$ is a Carmichael sequence.

(b) Let $a_{m+1} := \prod_{j=1}^{m} a_j$ and $a_{m+2} := d(a_{m+1} - 1) + 1$ where d is a divisor of $a_{m+1} + 1$. Then $[a_1, \ldots, a_m, a_{m+1}, a_{m+2}]$ is a Carmichael sequence.

In particular, if we start with an odd 3-factor Carmichael sequence, then we can extend it to arbitrary length by iterating the step (b) with $d = 2$.

4 Open problems

1. Giuga's conjecture: *Show that no integer exists which is both a Giuga number and a Carmichael number.*
   More general: *Show that no Giuga sequence can be a Carmichael sequence.* (This would imply the truth of Giuga's conjecture.)

2. Does every Giuga sequence contain two factors n_i, n_j with $n_j \mid (n_i-1)$? If this were true, then Giuga's conjecture is proved.

3. Find a Giuga sequence which consists of odd factors (or odd primes) only, or prove that none exist. If there were none, then Giuga's conjecture would be proved.

4. Are there infinitely many proper Giuga sequences?

5. Is it true that, in the notation of Section 2, $r_m(L_m) = i_m$ for $m = 5, \ldots, 27692$? If so, then this would prove that a counterexample to Giuga's conjecture has at least 36069 digits.

6. Find a fast way to generate all Giuga sequences of a given length.

7. Are there Giuga sequences with a sum minus product value higher than 1?

8. Are there two distinct Giuga sequences whose elements have the same product?

9. Can each integer be a factor in a Giuga sequence? If this were true then it would answer the previous two questions positively. In fact, take any integer n which is the product of a Giuga sequence, $n = n_1 \cdots n_m$ with $1/n_1 + \ldots + 1/n_m - 1/n = v$. If we can find a second Giuga sequence which contains n as a factor, e.g., $1/n + 1/\tilde{n}_1 + \ldots + 1/\tilde{n}_k - 1/n\tilde{n}_1 \cdots \tilde{n}_k = w$, then we can combine the two of them and get the Giuga sequence $1/n_1 + \ldots + 1/n_m + 1/\tilde{n}_1 + \ldots 1/\tilde{n}_k - 1/n_1 \cdots n_m \tilde{n}_1 \cdots \tilde{n}_k = v + w$. It has the same product as the previous one, but a higher sum minus product value.

10. Agoh's conjecture: *Let B_k denote the kth Bernoulli number. Then $nB_{n-1} \equiv -1 \bmod n$ if and only if n is a prime?* Note that the denominator of the number nB_{n-1} can be greater than 1, but since the denominator of any Bernoulli number is squarefree, the denominator of nB_{n-1} is invertible modulo n. As Takashi Agoh (Science University of Tokyo) has informed us, this recent conjecture of his is equivalent to Giuga's conjecture: Every counterexample to Giuga's conjecture is also a counterexample to Agoh's conjecture and vice versa. This can be seen from the well-known formula

$$s_{n-1} = \sum_{i=1}^{n} \binom{n}{i} n^{i-1} B_{n-i}$$

after some analysis involving von Staudt-Clausen's theorem: *The denominator of B_{2k} is given by* $\prod_{\substack{p \text{ prime} \\ (p-1)|2k}} p$. (See [4], pp. 91–93; this also implies that the denominator of B_{2k} is squarefree.)
Incidentally, it is possible to use a similar argument to characterize Giuga numbers in the following way: *n is a Giuga number if and only if* $nB_{\varphi(n)} \equiv -1 \bmod n$.

Finally, we would like to thank Hugh Edgar for originally making us aware of Giuga's conjecture and challenging us to extend what was known computationally.

References

[1] W.R. Alford, A. Granville, C. Pomerance, There are infinitely many Carmichael numbers, *Ann. of Math.* **140** (1994), 1–20.

[2] E. Bedocchi, Nota ad una congettura sui numeri primi, *Riv. Mat. Univ. Parma* **11** (1985), 229–236

[3] G. Giuga, Su una presumibile proprietà caratteristica dei numeri primi, *Ist. Lombardo Sci. Lett. Rend. A* **83** (1950), 511–528

[4] G.H. Hardy, E.M. Wright, *An Introduction to the Theory of Numbers*, Oxford University Press, Oxford 1959

[5] P. Ribenboim, *The Book of Prime Number Records,* Springer-Verlag 1989.

D. Borwein, Department of Mathematics, University of Western Ontario, London, Ontario N6A 5B7, Canada; dborwein@uwo.ca.

J.M. Borwein, Department of Mathematics and Statistics, Simon Fraser University, Burnaby, BC V5A 1S6, Canada; jborwein@cecm.sfu.ca.

P. Borwein, Department of Mathematics and Statistics, Simon Fraser University, Burnaby, BC V5A 1S6, Canada; pborwein@cecm.sfu.ca.

R. Girgensohn, Department of Mathematics and Statistics, Simon Fraser University, Burnaby, BC V5A 1S6, Canada; girgen@cecm.sfu.ca.

```
# p(i) is the i-th prime.

# Que(m,bound) returns all sets for the index m (i.e., subsets of the set of
# the first m-1 odd primes such that no element divides another element-1)
# whose estimate is below the bound.

Que := proc(m,bound) local i,n,S,Q,q,Sp;

if m=1 then RETURN({{}}); fi;     # If m=1 then the empty set is the only
                                  # "feasible" set.
S:=Que(m-1,bound);                # Collect the "feasible" sets for the index
                                  # m-1 in S.
                                  # "feasible": has an estimate below the bound.
n:=nops(S);                       # n is the number of sets Que returned for m-1.
Q:={};                            # We will collect all feasible sets for the
                                  # index m in Q.
for i from 1 to n do              # Now go through all sets in S.
   q:=convert(S[i],`*`);          # There are two cases:
   if gcd(q,p(m)-1)>1 then        # 1st case: The (m-1)st odd prime can't enter
      Q:=Q union {S[i]};          # the set S[i]. Then S[i] is in Q; its
                                  # estimate doesn't change.
   else                           # 2nd case: The (m-1)st odd prime can enter
                                  # the set S[i].
      if Est(S[i],m,bound+1)<=bound
                                  # Compute the estimate of the set S[i].
         then Q:=Q union {S[i]}; # If the estimate is below the bound, put
      fi;                         # S[i] into Q.
      Sp:=S[i] union {p(m)};
      if Est(Sp,m,bound+1)<=bound
                                  # Compute the estimate of the set S[i] u {p(m)}
         then Q:=Q union {Sp};    # If the estimate is below the bound, put
      fi;                         # S[i] u {p(m)} into Q.
   fi;
od;
Q;                                # Return all feasible sets for the index m.
end;


# Est(S,m,bound) adds the reciprocals of the primes in S and then
```

```
# continues to add the reciprocals of all primes greater or equal
# to the m-th odd prime which are not congruent to 1 mod any prime
# in S.
# Est stops adding when the sum exceeds 1 or when the number of primes
# added exceeds the bound.
# Est returns the number of primes it added.

Est:=proc(S,m,bound) local c,n,q,t,s,k,j,L;
n:=m+1;k:=nops(S);
s:=evalf(sum(1/S[j],j=1..k));
q:=product(S[j],j=1..k);
while k<bound and s<1 do
c:=char(p(n)-1,q);s:=s+c/p(n); k:=k+c;
        n:=n+1;
od;
k;
end;

char:=proc(a,b) local s;
s:=1; if gcd(a,b)>1 then s:=0;fi;s;
end;
```

CARMICHAEL SEQUENCES

David Borwein

November 10, 1994 carmichl.tex

Proposition 1. *Let $b_1, b_2, b_3 \in N$ be pairwise co-prime and let $B := b_2b_3 + b_3b_1 + b_1b_2$. Let $b \in N$ be such that*

$$bB \equiv -1 - B \ mod\ b_1b_2b_3.$$

(Since B and $b_1b_2b_3$ are co-prime such a b exists and is unique modulo $b_1b_2b_3$.) Then the four integers a_0, a_1, a_2, a_3 defined by

$$\begin{aligned} a_0 &:= b + 1 \\ a_1 &:= bb_2b_3 + 1 \\ a_2 &:= bb_3b_1 + 1 \\ a_3 &:= bb_1b_2 + 1 \end{aligned}$$

form a Carmichael sequence.

Proof. Let $L := b_1b_2b_3, A_0 := b, A_1 := bb_2b_3, A_2 := bb_3b_1, A_3 := bb_1b_2$. Then

$$\begin{aligned} a_0a_1a_2a_3 - 1 &= (A_0 + 1)(A_1 + 1)(A_2 + 1)(A_3 + 1) - 1 \\ &= A_0A_1A_2A_3 + A_0A_1A_2 + A_0A_1A_3 + A_0A_2A_3 + A_1A_2A_3 \\ &\quad + A_0A_1 + A_0A_2 + A_0A_3 + A_1A_2 + A_1A_3 + A_2A_3 \\ &\quad + A_0 + A_1 + A_2 + A_3. \end{aligned}$$

By removing the terms that are divisible by L, we reduce the right-hand side of the above expression modulo L to

$$\begin{aligned} &A_0A_1 + A_0A_2 + A_0A_3 + A_0 + A_1 + A_2 + A_3 \\ &\quad = b^2B + b(1 + B) = b(bB + 1 + B) \equiv 0 \bmod L. \end{aligned}$$

It follows that $a_0a_1a_2a_3 - 1 \equiv 0 \bmod L$, and hence that each $a_i - 1 \mid a_0a_1a_2a_3 - 1$. □

Example 1. $b_1 = 1, b_2 = 2, b_3 = 3, B = 2 + 6 + 3 = 11$
$11b \equiv -12 \mod 6 \implies b = 0 \mod 6.$
$(b+1)(2b+1)(3b+1)(6b+1)$ is Carmichael.
$b = 6:$ $\quad 7 \cdot 13 \cdot 19 \cdot 37 = 63973$ is proper.

Example 2. $b_1 = 2, b_2 = 3, b_3 = 5, B = 6 + 15 + 10 = 31$
$31 \equiv -32 \mod 30 \implies b = 28 \mod 30.$
$(b+1)(6b+1)(10b+1)(15b+1)$ is Carmichael.
$b = 28:$ $\quad 29 \cdot 169 \cdot 281 \cdot 421 = 579793201$ is not proper.

Proposition 2. *Let $b_1, b_2, b_3, b_4 \in \mathbb{N}$, let $(b_1+1), (b_2+1), (b_3+1), (b_4+1)$ be a Carmichael sequence, let $L := \operatorname{lcm}(b_1, b_2, b_3, b_4)$, let c be the hcf of the coefficients of the quartic polynomial $(b_1x+1)(b_2x+1)(b_3x+1)(b_4x+1)-1$, let $a := \operatorname{hcf}(c, L)$, and let $b \equiv 1 \mod L/a$. Then the four integers*

$$(b_1b+1), (b_2b+1), (b_3b+1), (b_4b+1)$$

form a Carmichael sequence.

Proof. We have

$$(b_1x+1)(b_2x+1)(b_3x+1)(b_4x+1) - 1 = xB(x),$$

where

$$B(x) := B_1x^3 + B_2x^2 + B_3x + B_4.$$

Now

$$\begin{aligned} B\left(1 + k\frac{L}{a}\right) &= k^3\frac{L^3}{a^3}B_1 + k^2\frac{L^2}{a^2}(3B_1 + B_2) \\ &\quad + k\frac{L}{a}(3B_1 + 2B_2 + B_3) + B_1 + B_2 + B_3 + B_4 \\ &\equiv B_1 + B_2 + B_3 + B_4 \mod L, \end{aligned}$$

since $a \mid L$ and $a \mid \operatorname{hcf}(B_1, B_2, B_3, B_4)$. But

$$B_1 + B_2 + B_3 + B_4 = (b_1+1)(b_2+1)(b_3+1)(b_4+1) - 1 \equiv 0 \mod L,$$

since $(b_1+1), (b_2+1), (b_3+1), (b_4+1)$ form a Carmichael sequence. The desired conclusion follows. □

Example 3. $b_1 = 6, b_2 = 10, b_3 = 12, b_4 = 40, L = 120, c = a = 4,$
$b = 1 \mod 30.$
$(6b+1)(10b+1)(12b+1)(40b+1)$ is Carmichael.
$b = 1:$ $\quad 7 \cdot 11 \cdot 13 \cdot 41 = 41041$ is proper.
$b = 31:$ $\quad 187 \cdot 311 \cdot 373 \cdot 1241 = 26920468201$ is not proper.

Example 4. $b_1 = 4, b_2 = 8, b_3 = 44, b_4 = 88, L = 88, c = 16, a = 8,$
$b = 1 \mod 11.$
$(4b+1)(8b+1)(44+1)(88b+1)$ is Carmichael.
$b = 1:$ $\quad 5 \cdot 9 \cdot 45 \cdot 89 = 180225$ is not proper.
$b = 12:$ $\quad 49 \cdot 97 \cdot 529 \cdot 1057 = 2657654209$ is not proper.

REMARKS. Proposition 1 generates Carmichael sequences of length 4 starting from any pair-wise coprime integers b_1, b_2, b_3. Proposition 2 starts with a Carmichael sequence and generates new ones. Evidently Proposition 2 holds for any length of Carmichael sequence. All the Carmichael sequences listed by Andrew Granville in his survey paper (September 1992 Notices of the AMS) can be generated by means of Proposition 2 (extended).