

On Giuga numbers

Florian Luca, Carl Pomerance and Igor Shparlinski

Received November 18, 2007; Revised May 29, 2008

Abstract

A Giuga number is a composite integer n satisfying the congruence $\sum_{j=1}^{n-1} j^{n-1} \equiv -1 \pmod{n}$. We show that the counting function $\#\mathcal{G}(x)$ of the Giuga numbers $n \leq x$ satisfies the estimate $\#\mathcal{G}(x) = o(x^{1/2})$ as $x \rightarrow \infty$, improving upon a result of V. Tipu.

Keywords: Giuga numbers, Carmichael numbers.

2000 Mathematics Subject Classification: 11A41, 11N25.

1 Introduction

1.1 Background

Fermat's Little Theorem immediately implies that for n prime,

$$\sum_{j=1}^{n-1} j^{n-1} \equiv -1 \pmod{n}. \quad (1.1)$$

Giuga [3], conjectured that there are no composite integers n fulfilling (1.1); a counterexample is called a *Giuga number*. With \mathcal{G} the set of all Giuga numbers, it is known that $n \in \mathcal{G}$ if and only if n is composite and

$$p^2(p-1) \mid n-p \quad (1.2)$$

for all prime factors p of n . In particular, n is squarefree. Furthermore, it is also a *Carmichael number*; that is, the congruence $a^n \equiv a \pmod{n}$ holds for all integers a .

We refer the reader to [5, pages 21-22] and the introduction to [7] for more properties of the Giuga numbers. In [1], the relation (1.2) is relaxed to $p^2 \mid n-p$, and it is shown that this property is equivalent to the sum of the reciprocals of the prime factors of n being $1/n \pmod{1}$. Call such a composite number a *weak Giuga number*. There are several examples known, the smallest one being 30 (see sequence A007850 in [6]).

During the preparation of this paper, F. L. was supported in part by Grant SEP-CONACyT 46755, C. P. by NSF Grant DMS-0703850, and I. S. by ARC Grant DP0556431

1.2 Our result

For a positive real number x we put $\mathcal{G}(x) = \mathcal{G} \cap [1, x]$. While Giuga's conjecture asserts that \mathcal{G} is empty, the best known upper bound on $\#\mathcal{G}(x)$ is

$$\#\mathcal{G}(x) = O\left(x^{1/2} \log x\right) \quad (1.3)$$

and is due to V. Tipu [7]. Here, we obtain an improvement of (1.3), which in particular shows that $\#\mathcal{G}(x)$ is of a smaller order of magnitude than $x^{1/2}$.

Theorem. *The following estimate holds:*

$$\#\mathcal{G}(x) = O\left(\frac{x^{1/2}}{(\log x)^2}\right).$$

We follow the approach from [7], which in turn is an adaptation of some arguments due to Erdős [2] and Pomerance, Selfridge and Wagstaff [4] which have been used to find an upper bound for the number of Carmichael numbers up to x . However, we also complement it with some new arguments which lead us to a better upper bound. We note that it is easy to show that the counting function of the weak Giuga numbers $n \leq x$ is $O(x^{2/3})$.

2 Proof

2.1 Notation

For a natural number n let $\tau(n)$, respectively $\omega(n)$, be the number of divisors of n , the number of prime divisors of n . We use p and q for prime numbers and the Landau and Vinogradov symbols O , o , \ll and \gg with their usual meanings.

2.2 Preparation

We assume that x is large. To prove the theorem it is sufficient to show $\#\mathcal{G}(x) - \#\mathcal{G}(x/2) \ll x^{1/2}/(\log x)^2$, since we can then apply the same estimate with x replaced by $x/2, x/4, \dots$, and add these estimates. Let

$$n = \prod_{j=1}^k p_j \in \mathcal{G}(x) \setminus \mathcal{G}(x/2),$$

where $p_1 > p_2 > \dots > p_k$ are prime numbers ordered decreasingly. For a squarefree positive integer m we write $\lambda(m) = \text{lcm}[p-1 : p \mid m]$. This function is referred to as the Carmichael function of m (or the universal exponent modulo m). If n is a Giuga number we have $p-1 \mid n-1$ for each prime $p \mid n$, so that $\gcd(n, \lambda(n)) = 1$. Thus, for any integer d , those possible Giuga numbers n with $d \mid n$ are in (at most) a single residue class modulo

$d^2\lambda(d)$, and in the case that $d = p$ is prime, we also have $n > p^2(p-1)$, since the residue class is $p \pmod{p^2(p-1)}$ and $n > p$.

2.3 Large values of p_1

We first consider the case when $p_1 > x^{1/4}$. For a fixed value of p_1 , the number of Giuga numbers $n \leq x$ divisible by p_1 is $\leq x/p_1^2(p_1-1)$. Summing this for $p_1 > x^{1/4} \log x$ gives the estimate $O(x^{1/2}/(\log x)^3)$, so we may assume $x^{1/4} < p_1 \leq x^{1/4} \log x$. Suppose $d \mid n$ with $d \neq p_1$. Then n is in a residue class modulo $p_1^2 d^2 \lambda(p_1 d)$, and in particular is in a residue class modulo $p_1^2 d^2 (p_1-1)$. If d is in the interval

$$I = [\log x, x^{1/4}/(\log x)^2],$$

then the number of Giuga numbers $n \leq x$ with $p_1 d \mid n$ is at most

$$\begin{aligned} & \sum_{\substack{x^{1/4} < p_1 \leq x^{1/4} \log x \\ d \in I}} \left(1 + \frac{x}{p_1^2 d^2 (p_1-1)} \right) \\ & \leq \pi(x^{1/4} \log x) \frac{x^{1/4}}{(\log x)^2} + \sum_{\substack{p_1 > x^{1/4} \\ d > \log x}} \frac{x}{p_1^2 d^2 (p_1-1)} \ll \frac{x^{1/2}}{(\log x)^2}. \end{aligned}$$

Thus, we may assume that n has no divisors in I . As a consequence, the largest divisor d of n composed of primes less than $\log x$ has $d < \log x$, since if not, $d \in I$. Since $x/2 < n \leq x$, we thus have

$$n = p_1 p_2 p_3 p_4 d, \quad x^{1/4} \log x \geq p_1 > p_2 > p_3 > p_4 > \frac{x^{1/4}}{(\log x)^2}, \quad 1 \leq d < \log x.$$

Then $x^{1/2}/(\log x)^4 < p_3 p_4 < x^{1/2}$, and since n is in a residue class modulo $p_3^2 p_4^2 (p_3-1)$, the number $p_3 p_4$ determines at most one Giuga number $n \leq x$ divisible by $p_3 p_4$. Since $p_4 < x/p_3^3$, the number of choices for p_4 given p_3 is $O(x/(p_3^3 \log x))$, which when summed over $p_3 > x^{1/4}$ gives the estimate $O(x^{1/2}/(\log x)^2)$. But if $p_3 \leq x^{1/4}$, then the number of choices for $p_3 p_4$ is at most $\pi(x^{1/4})^2 \ll x^{1/2}/(\log x)^2$.

2.4 Small values of p_1

We now assume that $p_1 \leq x^{1/4}$. Let $d_j(n) = p_1 p_2 \cdots p_j$ for $j \leq k = \omega(n)$, and choose $m = m(n)$ as the least number ≥ 2 with

$$d_m(n) \geq x^{m/(2m+2)}/(\log x)^2. \tag{2.1}$$

Such an index m exists, since we are assuming that $n > x/2$. By the minimality of m , we have

$$d_{m-1}(n) < x^{(m-1)/2m}/(\log x)^2 \text{ if } m \geq 3. \tag{2.2}$$

Our idea is to fix a number d and count the number of Giuga numbers $n \leq x$ with $d_m(n) = d$. This count is at most $1 + x/(d^2 \lambda(d))$, and so it remains to sum this expression over allowable values of d . That is, denoting by $\mathcal{D}(x)$ the set of all such values of d , we now need to estimate the sum

$$\sum_{d \in \mathcal{D}(x)} \left(1 + \frac{x}{d^2 \lambda(d)}\right) = \#\mathcal{D}(x) + L(x), \quad (2.3)$$

say. The estimate for $\#\mathcal{D}(x)$ is easy. If $m = 2$, then the number of choices for $d = p_1 p_2$ is at most $\pi(x^{1/4})^2 \ll x^{1/2}/(\log x)^2$. If $m \geq 3$, then by (2.2),

$$d_m(n) < d_{m-1}(n)^{m/(m-1)} < x^{1/2}/(\log x)^{2m/(m-1)} < x^{1/2}/(\log x)^2. \quad (2.4)$$

Thus, we have the acceptable estimate

$$\#\mathcal{D}(x) \ll \frac{x^{1/2}}{(\log x)^2}. \quad (2.5)$$

To estimate $L(x)$, let $L_m(x)$ be the contribution corresponding to a choice for $m \geq 2$. Let $u = \gcd(p_1 - 1, p_2 - 1)$ so that

$$\lambda(d) \geq \lambda(p_1 p_2) = (p_1 - 1)(p_2 - 1)/u.$$

We have by (2.1) that $L_m(x)$ is at most

$$x \sum_{u \geq 1} u \sum_{\substack{p_1 > p_2 \\ u|p_1-1, u|p_2-1}} \frac{1}{p_1^2(p_1-1)p_2^2(p_2-1)} \sum_{\substack{p_3 \cdots p_m \geq \frac{x^{2m+2}}{p_1 p_2 (\log x)^2}}} \frac{1}{(p_3 \cdots p_m)^2},$$

where the final sum does not appear when $m = 2$. Using (2.1) we have

$$p_1 p_2 \geq d_m(n)^{2/m} \geq x^{1/(m+1)}/(\log x)^2 = y_m,$$

say. Thus,

$$\begin{aligned} L_m(x) &\ll x \sum_{u \geq 1} u \sum_{\substack{p_1 > p_2 \\ p_1 p_2 \geq y_m \\ u|p_1-1, u|p_2-1}} \frac{1}{p_1^3 p_2^3} \frac{p_1 p_2 (\log x)^2}{x^{m/(2m+2)}} \\ &\leq x^{(m+2)/(2m+2)} (\log x)^2 \sum_{u \geq 1} \frac{1}{u^3} \sum_{\substack{p_1 > p_2 \\ p_1 p_2 \geq y_m \\ p_1-1=uv, p_2-1=uw}} \frac{1}{v^2 w^2}. \end{aligned} \quad (2.6)$$

We have written $p_1 - 1 = uv, p_2 - 1 = uw$ and so writing $z = vw$, we have

$$z = vw \geq p_1 p_2 / (2u^2) \geq y_m / (2u^2).$$

If $u^2 \leq y_m$, then the contribution to $L_m(x)$ in (2.6) is at most

$$\begin{aligned} & x^{(m+2)/(2m+2)} (\log x)^2 \sum_{u^2 \leq y_m} \frac{1}{u^3} \sum_{z \geq y_m/(2u^2)} \frac{\tau(z)}{z^2} \\ & \ll x^{(m+2)/(2m+2)} (\log x)^2 \sum_{u^2 \leq y_m} \frac{1}{u^3} \frac{u^2 \log x}{y_m} \ll x^{1/2-1/(2m+2)} (\log x)^6. \end{aligned}$$

And if $u^2 > y_m$, the contribution to $L_m(x)$ in (2.6) is at most

$$\begin{aligned} & x^{(m+2)/(2m+2)} (\log x)^2 \sum_{u^2 > y_m} \frac{1}{u^3} \sum_{z \geq 1} \frac{\tau(z)}{z^2} \\ & \ll x^{(m+2)/(2m+2)} (\log x)^2 \sum_{u^2 > y_m} \frac{1}{u^3} \ll x^{1/2-1/(2m+2)} (\log x)^4. \end{aligned}$$

If $m \leq (\log x)^{1/2}$, these last two estimates give an acceptable bound for $L_m(x)$. In particular,

$$\sum_{m \leq (\log x)^{1/2}} L_m(x) \ll x^{1/2} \exp\left(-\frac{1}{3}\sqrt{\log x}\right). \quad (2.7)$$

To conclude, we consider the case $m > (\log x)^{1/2}$. We have

$$\sum_{\substack{d \leq x \\ \omega(d)=m}} \frac{1}{d} \leq \frac{1}{m!} \left(\sum_{p \leq x} \sum_{\nu=1}^{\infty} \frac{1}{p^\nu} \right)^m \leq \frac{1}{m!} (\log \log x + c)^m \leq \left(\frac{e \log \log x + ec}{m} \right)^m,$$

where c is an absolute constant. Thus, using (2.1) and (2.4),

$$\begin{aligned} \sum_{m > (\log x)^{1/2}} L_m(x) & \leq \sum_{m > (\log x)^{1/2}} \sum_{\substack{d \geq x^{m/(2m+2)}/(\log x)^2 \\ \omega(d)=m}} \frac{x}{d^2} \\ & \leq \sum_{m > (\log x)^{1/2}} x^{(m+2)/(2m+2)} (\log x)^2 \sum_{\substack{d \leq x \\ \omega(d)=m}} \frac{1}{d} \ll x^{1/2} \exp\left(-\sqrt{\log x}\right). \end{aligned}$$

Putting this estimate together with (2.7), we obtain $L(x) = o(x^{1/2}/(\log x)^2)$ which after substitution in (2.3) and using (2.5) completes the proof.

Acknowledgements

The authors thank the referee for a careful reading of the manuscript and Jean-Marie De Koninck for useful discussions. This work started during a pleasant visit of I. S. to the Mathematical Institute of the UNAM in Morelia, México. This author thanks this Institution for its hospitality.

References

- [1] D. Borwein, J. M. Borwein, P. B. Borwein and R. Girgensohn, *Giuga's conjecture on primality*, Amer. Math. Monthly **103** (1996), 40–50.
- [2] P. Erdős, *On pseudoprimes and Carmichael numbers*, Publ. Math. Debrecen **4** (1956), 201–206.
- [3] G. Giuga, *Su una presumibile proprietà caratteristica dei numeri primi*, Ist. Lombardo Sci. Lett. Rend. Cl. Sci. Mat. Nat. **14(83)** (1950), 511–528.
- [4] C. Pomerance, J. L. Selfridge and S. S. Wagstaff, Jr., *The pseudoprimes to $25 \cdot 10^9$* , Math. Comp. **35** (1980), 1003–1026.
- [5] P. Ribenboim, *The little book of bigger primes*, 2nd ed., Springer, New York, 2004.
- [6] N. J. A. Sloane, *On-Line Encyclopedia of Integer Sequences*, <http://research.att.com/~njas/sequences/>.
- [7] V. Tipu, *A note on Giuga's conjecture*, Canad. Math. Bull. **50** (2007), 158–160.

Florian Luca: Mathematical Institute, UNAM, Ap. Postal 61-3 (Xangari), CP 58089, Morelia, Michoacán, Mexico

E-mail address: fluca@matmor.unam.mx

Carl Pomerance: Department of Mathematics, Dartmouth College, Hanover, NH 03755-3551, USA

E-mail address: carlp@gauss.dartmouth.edu

Igor Shparlinski: Department of Computing, Macquarie University, Sydney, NSW 2109, Australia

E-mail address: igor@ics.mq.edu.au