Canad. Math. Bull. Vol. **50** (1), 2007 pp. 158–160

A Note on Giuga's Conjecture

Vicentiu Tipu

Abstract. Let $G(X)$ denote the number of positive composite integers n satisfying $\sum_{j=1}^{n-1} j^{n-1} \equiv -1 \pmod{n}$. Then $G(X) \ll X^{1/2} \log X$ for sufficiently large X.

1 Introduction

Fermat's theorem states that if $(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$. Thus

$$\sum_{j=1}^{p-1} j^{p-1} \equiv -1 \pmod{p}.$$

Giuga [7] conjectured that there are no composite numbers n satisfying $\sum_{j=1}^{n-1} j^{n-1} \equiv -1 \pmod{n}$. The truth of his conjecture would imply an interesting characterization of prime numbers, just like Wilson's theorem. It is not hard to show [11, pp. 21–22] that every counterexample n to Giuga's conjecture (which will henceforth be called a "Giuga number") satisfies

$$p^2(p-1) \mid (n-p), \tag{1}$$

for every prime $p \mid n$. In particular, this implies that n is squarefree and every Giuga number is a Carmichael number (a number m is Carmichael if $a^m \equiv a \pmod{m}$ $\forall a \in \mathbb{N}$) since, by Korselt's criterion [8], m is Carmichael if and only if m is squarefree and $p(p-1) \mid (m-p)$ for every $p \mid m$. Giuga [7] showed that a number n is Giuga if and only if it is Carmichael and

$$\sum_{p \mid n} \frac{1}{p} - \frac{1}{n} \in \mathbb{N}. \tag{2}$$

This last condition implies that every Giuga number has at least 9 prime factors and enabled Giuga to estimate that the least Giuga number, if it exists, has at least 1000 digits. This was improved by Bedocchi [3] to 1700 digits, and by Borwein, Borwein, Borwein and Girgensohn [4] to more than 13000 digits. It seems that no one has estimated the size of the exceptional set in Giuga's conjecture. Here we prove the following:

Received by the editors October 25, 2004.
AMS subject classification: 11A51.

https://doi.org/10.4153/CMB-2007-016-8 Published online by Cambridge University Press

Theorem 1 *Let $G(X)$ denote the number of exceptions $n \le X$ to Giuga's conjecture. Then for X larger than an absolute constant which can be made explicit, $G(X) \ll X^{\frac{1}{2}} \log X$*

Alford, Granville, and Pomerance [2] proved that there are infinitely many Carmichael numbers. In fact, the number of Carmichael numbers less than X is expected to be $\gg X^{1-\epsilon}$ for all $\epsilon > 0$, and for all sufficiently large X. If this last statement is true, as the heuristic arguments in [6] and [9] indicate, then our result shows that Giuga numbers are a lot sparser than Carmichael numbers.

2 Proof of the Theorem

The proof consists of a careful adaptation of the method used by Erdős [6] and by Pomerance, Selfridge, and Wagstaff [10] in estimating an upper bound for the number of Carmichael numbers less than X.

Note that condition (1) insures that no Giuga number less than X can have a prime factor greater than $X^{1/3}$. If $n < X$ is squarefree, write $n = \prod_{j=1}^{k} p_j$, where $p_1 > p_2 > \cdots > p_k$. Define $f(n)$ to be the least common multiple of $p_j - 1$ for $j = 1, \ldots, k$. Given a squarefree d, note that the number of Giuga numbers $< X$ and divisible by d is at most $1 + \frac{X}{d^2 f(d)}$.

If $p_1 \ge X^{1/4}$, then the number of Giuga numbers less than X and divisible by such primes $\ge X^{1/4}$ is

$$< X \sum_{p \ge X^{1/4}} \frac{1}{p^2(p-1)} \ll X \sum_{m \ge X^{1/4}} \frac{1}{m^3} \ll X \int_{X^{1/4}}^{\infty} \frac{dt}{t^3} = X^{1/2}.$$

If not, then $p_1 < X^{1/4}$, so therefore $p_1 p_2 < X^{1/2}$. If $p_1 p_2 \ge X^{1/3}$, then evidently $f(p_1 p_2) \ge p_1 - 1 \gg X^{1/6}$. Thus the number of Giuga numbers $< X$ and divisible by such p_1 and p_2 is

$$\ll \sum_{X^{1/3} \le d < X^{1/2}} \left(1 + \frac{X}{d^2 X^{1/6}}\right) < X^{1/2} + X^{5/6} \sum_{d \ge X^{1/3}} \frac{1}{d^2} \ll X^{1/2}.$$

All we need is to estimate the number of Giuga numbers $< X$ which are divisible by $p_1 p_2 < X^{1/3}$, and where $p_1 < X^{1/4}$. Note that $p_2 < X^{1/6}$, so the product of the three largest primes $p_1 p_2 p_3 < X^{1/2}$. If $p_1 p_2 p_3 \ge X^{3/8}$, then clearly $f(p_1 p_2 p_3) \gg X^{1/8}$, so the number of Giuga numbers divisible by such primes is

$$\ll \sum_{X^{3/8} \le d < X^{1/2}} \left(1 + \frac{X}{d^2 X^{1/8}}\right) < X^{1/2} + X^{7/8} \sum_{d \ge X^{3/8}} \frac{1}{d^2} \ll X^{1/2}.$$

This process can be continued; at each step, we need to estimate the number of Giuga numbers divisible by $p_1 p_2 \cdots p_m$, where $\prod_{j=1}^{m-1} p_j < X^{\frac{m-1}{2m}}$. Note that $\prod_{j=1}^{m} p_j < X^{1/2}$, because p_m is the smallest prime factor in the product. If $\prod_{j=1}^{m} p_j \ge$

$X^{\frac{m}{2m+2}}$, then $f(\prod_{j=1}^{m} p_j) \geq p_1 - 1 \gg X^{\frac{1}{2m+2}}$. So the number of Giuga numbers divisible by $\prod_{j=1}^{m} p_j$, where the p_j satisfy the above constraints is

$$\ll \sum_{X^{\frac{m}{2m+2}} \leq d < X^{1/2}} \left(1 + \frac{X}{d^2 X^{\frac{1}{2m+2}}}\right) < X^{1/2} + X^{\frac{2m+1}{2m+2}} \sum_{d \geq X^{\frac{m}{2m+2}}} \frac{1}{d^2} \ll X^{1/2}.$$

After $\ll \log X$ steps, all the possibilities are exhausted, *i.e.,* there cannot be any divisors of any other form which divide a Giuga number $< X$. Therefore the number of exceptions to Giuga's conjecture is $\ll X^{1/2} \log X$, and the theorem is proved. ∎

3 Further Ideas

Our estimate of $G(X)$ depends crucially on estimates of $f(d)$. Even if one can prove the sharpest possible bound for $f(d)$, namely $f(d) \gg d$ for almost all d, it will still not be possible, using only this method, to prove anything stronger than $G(X) \ll X^{1/3}$.

Further ideas are needed for the proof of the full Giuga conjecture, involving perhaps Bernoulli numbers [1], or Giuga sequences [4, 5].

Acknowledgement The author would like to thank his supervisor, Prof. John Friedlander, for many helpful discussions.

References

[1] T. Agoh, *On Giuga's conjecture.* Manuscripta Math. **87**(1995), no. 4, 501–510.
[2] W. R. Alford, A. Granville, and C. Pomerance, *There are infinitely many Carmichael numbers.* Ann. of Math. **139**(1994), no. 3, 703–722.
[3] E. Bedocchi, *Note on a conjecture about prime numbers.* (Italian), Riv. Mat. Univ. Parma **11**(1985), 229–236.
[4] D. Borwein, J. M. Borwein, P. B. Borwein, and R. Girgensohn, *Giuga's conjecture on primality.* Amer. Math. Monthly **103**(1996), no. 1, 40–50.
[5] J. M. Borwein, E. Wong, *A survey of results relating to Giuga's conjecture on primality.* In: Advances in Mathematical Sciences: CRM's 25 years. CRM Proc. Lecture Notes 11, American Mathematical Society, Providence, RI, 1997, pp. 13–27.
[6] P. Erdős, *On pseudoprimes and Carmichael numbers.* Publ. Math. Debrecen **4**(1956), 201–206.
[7] G. Giuga, *Su una presumibile proprietá caratteristica dei numeri primi.* Ist. Lombardo Sci. Lett. Rend. Cl. Sci. Mat. Nat. **14(83)**(1950). 511–528.
[8] A. Korselt, *Problème chinois.* L'intermediaire des mathematiciens **6**(1899), 142-143.
[9] C. Pomerance, *Two methods in elementary analytic number theory.* In: Number Theory and Applications. NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., Kluwer, Dordrecht, 1989, pp. 135-161.
[10] C. Pomerance, J. L. Selfridge, and S. Wagstaff, *The pseudoprimes to* $25 \cdot 10^9$. Math. Comp. **35**(1980), no. 151, 1003–1026.
[11] P. Ribenboim, *The little book of bigger primes.* Second edition. Springer-Verlag, New York, 2004.

Department of Mathematics
University of Toronto
Toronto, ON
M5S 2E4
e-mail: vtipu@math.utoronto.ca