UDC 512.5

José María Grau (Univ. de Oviedo, Spain),
A. M. Oller-Marcén (Centro Univ. de la Defensa, Zaragoza, Spain)

VARIATIONS ON GIUGA NUMBERS AND GIUGA'S CONGRUENCE

ВАРІАЦІЇ ЧИСЕЛ ТА КОНГРУЕНЦІЇ ГЮГА

A k-strong Giuga number is a composite integer such that $\sum_{j=1}^{n-1} j^{n-1} \equiv -1 \pmod{n}$. We consider the congruence $\sum_{j=1}^{n-1} j^{k(n-1)} \equiv -1 \pmod{n}$ for each $k \in \mathbb{N}$ (thus extending Giuga's ideas for $k = 1$). In particular, it is proved that a pair (n, k) with composite n satisfies this congruence if and only if n is a Giuga number and $\lambda(n) \mid k(n-1)$. In passing, we establish some new characterizations of Giuga numbers and study some properties of the numbers n satisfying $\lambda(n) \mid k(n-1)$.

k-Сильне число Гюга — це складене ціле число таке, що $\sum_{j=1}^{n-1} j^{n-1} \equiv -1 \pmod{n}$. Ми розглядаємо конгруенцію $\sum_{j=1}^{n-1} j^{k(n-1)} \equiv -1 \pmod{n}$ для кожного $k \in \mathbb{N}$ (таким чином ми розширюємо ідеї Гюга на випадок $k = 1$). Як частинний випадок доведено, що пара (n, k) зі складеним n задовольняє цю конгруенцію тоді і тільки тоді, коли n — число Гюга та $\lambda(n) \mid k(n-1)$. Крім того, встановлено деякі нові характеристики чисел Гюга та вивчено властивості чисел n, що задовольняють $\lambda(n) \mid k(n-1)$.

1. Preliminaries. The starting point of this paper is the following definition.

Definition 1. i) *A Giuga number is a composite integer n such that $p \mid (n/p - 1)$ for every p, prime divisor of n.*

ii) *A strong Giuga number is a composite integer n such that $p(p-1) \mid (n/p - 1)$ for every p, prime divisor of n.*

Strong Giuga numbers are counterexamples to Giuga's conjecture [8]; i.e., they are composite integers such that

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

There are several equivalent ways to define Giuga numbers [1, 5, 8, 10]. In particular we focus on the following characterization of Giuga numbers [5, p. 41] that, in some sense, is analogue to the one given in (1) for strong Giuga numbers.

Proposition 1. *Let n be an integer. Then n is a Giuga number if and only if*

$$\sum_{j=1}^{n-1} j^{\phi(n)} \equiv -1 \pmod{n},$$

where ϕ is Euler's totient function.

Clearly strong Giuga numbers are also Giuga numbers and, in fact, using the so-called Korselt's criterion [14] it can be seen that:

Proposition 2. *An integer n is a strong Giuga number if and only if it is both a Giuga and a Carmichael number.*

Much work has been done regarding these numbers [1, 3, 10, 13, 16, 17] and several generalizations and/or variations are possible [6, 9]. In this paper some new characterizations of Giuga numbers will be established. This characterizations will lead to a generalization of both strong Giuga numbers and Carmichael numbers.

2. New characterizations of Giuga numbers. This section is devoted to give a familiy of characterizations of Giuga numbers that include Proposition 1. The following lemma will be our main tool.

Lemma 1. *For every natural numbers A, B and N we have that*

$$\sum_{j=1}^{N-1} j^{A\lambda(N)} \equiv \sum_{j=1}^{N-1} j^{B\phi(N)} \pmod{N}.$$

Proof. Put $N = 2^a p_1^{r_1} \ldots p_s^{r_s}$ with p_i distinct odd primes. Choose $i \in \{1, \ldots, s\}$. We have that

$$\sum_{j=1}^{N-1} j^{A\lambda(N)} \equiv \frac{N}{p_i^{r_i}} \sum_{j=1}^{p_i^{r_i}-1} j^{A\lambda(N)} \pmod{p_i^{r_i}},$$

$$\sum_{j=1}^{N-1} j^{B\phi(N)} \equiv \frac{N}{p_i^{r_i}} \sum_{j=1}^{p_i^{r_i}-1} j^{B\phi(N)} \pmod{p_i^{r_i}}.$$

Now, since both $A\lambda(N),\ B\phi(N) \geq r_i$, we get

$$\sum_{j=1}^{p_i^{r_i}-1} j^{A\lambda(N)} = \sum_{\substack{1 \leq j \leq p_i^{r_i}-1 \\ (p_i, j)=1}} j^{A\lambda(N)} + \sum_{\substack{1 \leq j \leq p_i^{r_i}-1 \\ p_i \mid j}} j^{A\lambda(N)} \equiv \phi(p_i^{r_i}) + 0 \pmod{p_i^{r_i}},$$

$$\sum_{j=1}^{p_i^{r_i}-1} j^{B\phi(N)} = \sum_{\substack{1 \leq j \leq p_i^{r_i}-1 \\ (p_i, j)=1}} j^{B\phi(N)} + \sum_{\substack{1 \leq j \leq p_i^{r_i}-1 \\ p_i \mid j}} j^{A\lambda(N)} \equiv \phi(p_i^{r_i}) + 0 \pmod{p_i^{r_i}}.$$

Consequently,

$$\sum_{j=1}^{N-1} j^{A\lambda(N)} \equiv \sum_{j=1}^{N-1} j^{B\phi(N)} \pmod{p_i^{r_i}} \quad \text{for every} \quad i = 1, \ldots, s.$$

Clearly if N is odd the proof is complete. If n is even we have that

$$\sum_{j=1}^{N-1} j^{A\lambda(N)} \equiv \frac{N}{2^a} \sum_{j=1}^{2^a-1} j^{A\lambda(N)} \equiv \frac{N}{2^a} \left(\sum_{\substack{1 \leq j \leq 2^a-1 \\ j \text{ even}}} j^{A\lambda(N)} + 2^{a-1} \right) \pmod{2^a},$$

$$\sum_{j=1}^{N-1} \equiv \frac{N}{2^a} \left(\sum_{\substack{1 \leq j \leq 2^a-1 \\ j \text{ even}}} j^{B\phi(N)} + 2^{a-1} \right) \pmod{2^a}.$$

Now, if $a = 1, 2$ or 3 it can be easily verified that

$$\sum_{\substack{1 \le j \le 2^a - 1 \\ j \text{ even}}} j^{A\lambda(N)} \equiv \sum_{\substack{1 \le j \le 2^a - 1 \\ j \text{ even}}} j^{B\phi(N)} \pmod{2^a}.$$

On the other hand, if $a \ge 4$ we have that $\phi(N) \ge \lambda(N) \ge a$ and, consequently, $j^{A\lambda(N)} \equiv j^{B\phi(N)} \equiv 0 \pmod{2^a}$ for every $1 \le j \le 2^{a-1}$ even. Thus

$$\sum_{j=1}^{N-1} j^{A\lambda(N)} \equiv \sum_{j=1}^{N-1} j^{B\phi(N)} \pmod{2^a}.$$

Lemma 1 is proved.

The following result extends Proposition 1. In particular it shows that we can replace Euler's totient function $\phi(n)$ by Carmichael's function $\lambda(n)$ or by any multiple of $\phi(n)$ or $\lambda(n)$.

Proposition 3. *Let n be any composite integer. Then the following are equivalent*:

i) *n is a Giuga number*;

ii) *for every positive integer K, $\sum_{j=1}^{n-1} j^{K\lambda(n)} \equiv \sum_{j=1}^{n-1} j^{K\phi(n)} \equiv -1 \pmod{n}$*;

iii) *there exists a positive integer K such that $\sum_{j=1}^{n-1} j^{K\lambda(n)} \equiv \sum_{j=1}^{n-1} j^{K\phi(n)} \equiv -1 \pmod{n}$.*

***Remark* 1.** If n is a Carmichael number, then $\lambda(n)|(n-1)$. If we put $k = \dfrac{n-1}{\lambda(n)}$, then we have

$$S := \sum_{j=1}^{n-1} j^{n-1} = \sum_{j=1}^{n-1} j^{k\lambda(n)}.$$

If, in addition, n is a Giuga number, we can apply Lemma 1 with $A = k$ and $B = 1$ to get $S \equiv -1 \pmod{n}$. Hence, we have a new proof of Proposition 2 which avoids the use of Korselt's criterion replacing it by Carmichael's criterion [7].

3. *k*-strong Giuga numbers and *k*-Carmichael numbers. As a clear consequence of Proposition 3 we have the following result.

***Corollary* 1.** *Let n be a strong Giuga number. Then*

$$\sum_{j=1}^{n-1} j^{k(n-1)} \equiv -1 \pmod{n}$$

for every positive integer k.

Proof. If n is a strong Giuga number, then it is both a Carmichael and a Giuga number. Being a Carmichael number, we have that $\lambda(n) \mid (n-1)$, so if $\dfrac{k(n-1)}{\lambda(n)} = k' \in \mathbb{N}$ we get

$$S := \sum_{j=1}^{n-1} j^{k(n-1)} = \sum_{j=1}^{n-1} j^{k\lambda(n)\frac{(n-1)}{\lambda(n)}} = \sum_{j=1}^{n-1} j^{k'\lambda(n)},$$

and, since n is a Giuga number, it is enough to apply Corollary 1 and Proposition 3 to get $S \equiv -1 \pmod{n}$.

Corollary 1 is proved.

This result motivates the definitions below. In some sense we are *stratifying* strong Giuga numbers and Carmichael numbers. A similar idea was used in [11] in the context of Lehmer numbers [15].

Definition 2. *Let $k \in \mathbb{N}$.*

i) *A composite number n is a k-strong Giuga number if*

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

ii) *An integer n is a k-Carmichael number if $\lambda(n)$ divides $k(n-1)$.*

***Remark* 2.** Observe that for $k = 1$ we recover the classical Carmichael and strong Giuga numbes.

It is well-known that Carmichael numbers are square-free. This is no longer true for k-Carmichael numbers with $k > 1$. Nevertheless we have the following result.

Proposition 4. *Let n be a square-free positive composite integer and let $k \in \mathbb{N}$. The following are equivalent*:

i) *n is a k-Carmichael number*,

ii) *for every prime divisor p of n, $p-1$ divides $k(n-1)$*,

iii) *for every integer a, $a^{kn} \equiv a^k \pmod{n}$.*

Proof. If n is a square-free k-Carmichael number, then $\lambda(n) = \mathrm{lcm}\{p-1 \mid p \text{ divides } n\}$ divides $k(n-1)$. This proves that i) implies ii).

Now, if $p-1$ divides $k(n-1)$ for every prime divisor p of n and given any integer a, it follows that $a^{k(n-1)} \equiv 1 \pmod{p}$ for every prime divisor p of n such that p does not divide a. If p divides a the same congruence follows trivially and this proves that ii) implies iii).

Finally, to see that iii) implies i) it is enough to consider an integer a coprime to n.

Proposition 4 is proved.

We are now in the condition give an analogue of Proposition 2.

Theorem 1. *Let n be a composite integer. Then n is a k-strong Giuga number if and only if n is both a Giuga number and a k-Carmichael number.*

Proof. Assume that n is a Giuga number and a k-Carmichael number. Since $\lambda(n)$ divides $k(n-1)$ we have that

$$\sum_{j=1}^{n-1} j^{k(n-1)} = \sum_{j=1}^{n-1} j^{k'\lambda(n)} \equiv -1$$

due to Proposition 3.

Conversely, assume that n is a k-strong Giuga number, i.e., $\sum_{j=1}^{n-1} j^{k(n-1)} \equiv -1 \pmod{n}$. As a consequence (see [18], Theorem 2.3) we have that $p-1$ divides $k\left(n/p-1\right)$, that p divides $n/p-1$ for every p, prime divisor of n and, moreover, that n is square-free. Since n is square-free, $\lambda(n) = lcm\{p-1 \mid p \text{ prime dividing } n\}$. Thus, $\lambda(n)$ divides $k(n-1)$ and n is a k-Carmichael number. To get that n is also a Giuga number, due to Proposition 2, it is enough to apply Lemma 1 with $B = 1$ and $A = \dfrac{k(n-1)}{\lambda(n)}$.

Theorem 1 is proved.

Associated to the idea of k-strong Giuga numbers, let us define the following sets:

$$\mathcal{G}_k := \{n \in \mathbb{N} \mid n \text{ is } k\text{-strong Giuga number}\},$$

$$\mathcal{K}_n := \{k \in \mathbb{N} \mid n \text{ is } k\text{-strong Giuga number}\}.$$

Taking into account that the condition $\lambda(n) \mid k(n-1)$ is equivalent to $\dfrac{\lambda(n)}{gcd(\lambda(n), n-1)} \mid k$, Theorem 1 gives a complete description of the set $\mathcal{K}_n$ for every n as stated in the following corollary.

***Corollary* 2.** *Let n be any composite positive integer. Then*

$$\mathcal{K}_n = \begin{cases} \left\{ t \cdot \dfrac{\lambda(n)}{gcd(\lambda(n), n-1)} \;\middle|\; t \in \mathbb{N} \right\}, & \textit{if} \quad n \quad \textit{is a Giuga number}, \\ \varnothing, & \textit{otherwise.} \end{cases}$$

Moreover, since it is clear that $n \in \mathcal{G}_k$ if and only if $k \in \mathcal{K}_n$ we also have the following result.

***Corollary* 3.** *$\mathcal{G}_k$ is nonempty if and only if $\lambda(n)$ divides $k(n-1)$ for some Giuga number n.*

This last result can be used to find values of k such that $\mathcal{G}_k$ is nonempty. To do so, we evaluate $k_n := \dfrac{\lambda(n)}{gcd(\lambda(n), n-1)}$ for every of the thirteen known Giuga numbers $g_1, \ldots, g_{13}$ (see A007850 in the *On-line Encyclopedia of Integer Sequences*). Thus, we will have thirteen values of k for which $\mathcal{G}_{tk}$ is known to be nonempty for any t:

$$\begin{aligned}
k_{g_1} &= 4, \\
k_{g_2} &= 60, \\
k_{g_3} &= 120, \\
k_{g_4} &= 2320, \\
k_{g_5} &= 1552848, \\
k_{g_6} &= 10080, \\
k_{g_7} &= 139714902540, \\
k_{g_8} &= 93294624780, \\
k_{g_9} &= 228657996794220, \\
k_{g_{10}} &= 4756736241732916394976, \\
k_{g_{11}} &= 20024071474861042488900, \\
k_{g_{12}} &= 2176937111336664570375832140, \\
k_{g_{13}} &= 15366743578393906356665002406454800354974137359272 \\
&\quad\; 445859047945613961394951904884493965220.
\end{aligned}$$

For these values and $t = 1$ one gets:

$$\begin{aligned}
\mathcal{G}_{k_{g_1}} &= \{g_1, \ldots\}, \\
\mathcal{G}_{k_{g_2}} &= \{g_1, g_2, \ldots\}, \\
\mathcal{G}_{k_{g_3}} &= \{g_1, g_2, g_3, \ldots\}, \\
\mathcal{G}_{k_{g_4}} &= \{g_1, g_4, \ldots\},
\end{aligned}$$

$$\mathcal{G}_{k_{g_5}} = \{g_1, g_5, \dots\},$$
$$\mathcal{G}_{k_{g_6}} = \{g_1, g_2, g_6, \dots\},$$
$$\mathcal{G}_{k_{g_7}} = \{g_1, g_7, \dots\},$$
$$\mathcal{G}_{k_{g_8}} = \{g_1, g_2, g_8, \dots\},$$
$$\mathcal{G}_{k_{g_9}} = \{g_1, g_2, g_9, \dots\},$$
$$\mathcal{G}_{k_{g_{10}}} = \{g_1, g_{10}, \dots\},$$
$$\mathcal{G}_{k_{g_{11}}} = \{g_1, g_{11}, \dots\},$$
$$\mathcal{G}_{k_{g_{12}}} = \{g_1, g_2, g_{12}, \dots\},$$
$$\mathcal{G}_{k_{g_{13}}} = \{g_1, g_2, g_{13}, \dots\}.$$

Finally observe that, with this notation, Giuga's conjecture can be stated as $\mathcal{G}_1 = \varnothing$.

1. *Takashi Agoh.* On Giuga's conjecture // Manuscr. Math. – 1995. – **87**, № 4. – P. 501 – 510.
2. *William D. Banks, C. Wesley Nevans, Carl Pomerance.* A remark on Giuga's conjecture and Lehmer's totient problem // Alban. J. Math. – 2009. – **3**, № 2. – P. 81 – 85.
3. *Edmondo Bedocchi.* Note on a conjecture about prime numbers // Riv. mat. Univ. Parma. – 1985. – **11**, № 4. – P. 229 – 236.
4. *Beeger N. G. W. H.* On composite numbers n for which $a^{n-1} \equiv (\bmod\, n)$ for every a prime to n // Scr. Math. – 1950. – **16**. – P. 133 – 135.
5. *Borwein D., Borwein J. M., Borwein P. B., Girgensohn R.* Giuga's conjecture on primality // Amer. Math. Mon. – 1996. – **103**, № 1. – P. 40 – 50.
6. *Borwein J. M., Wong E.* A survey of results relating to Giuga's conjecture on primality // Adv. Math. Sci.: CRM's 25 years (Montreal, PQ, 1994). – Providence, RI: Amer. Math. Soc., 1997. – **11**. – P. 13 – 27.
7. *Carmichael R. D.* On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \bmod P$ // Amer. Math. Mon. – 1912. – **19**, № 2. – P. 22 – 27.
8. *Giuseppe Giuga.* Su una presumibile proprietá caratteristica dei numeri primi // Ist. Lombardo Sci. Lett. Rend. Cl. Sci. Mat. Nat. – 1950. – **14/83**, № 3. – P. 511 – 528.
9. *José María Grau, Florian Luca, Antonio M. Oller-Marcén.* On a variant of Giuga numbers // Acta Math. Sinica. – 2011. – **28**, № 4. – P. 653 – 660.
10. *José María Grau, Antonio M. Oller-Marcén.* Giuga numbers and the arithmetic derivative // J. Integer Sequences. – 2012. – **15**, № 4. – Article 12.4.1.
11. *José María Grau, Antonio M. Oller-Marcén.* On k-Lehmer numbers // Integers. – 2012. – **12**, № 5. – P. 1081 – 1089.
12. *Glyn Harman.* On the number of Carmichael numbers up to x // Bull. London Math. Soc. – 2005. – **37**, № 5. – P. 641 – 650.
13. *Bernd C. Kellner.* The equivalence of giuga's and agoh's conjectures // arXiv:math/0409259v1 [math.NT].
14. *Alwin R. Korselt.* Problè me chinois // Interméd. math. – 1996. – **6**. – P. 142 – 143.
15. *Lehmer D. H.* On Euler's totient function // Bull. Amer. Math. Soc. – 1932. – **38**, № 10. – P. 745 – 751.
16. *Florian Luca, Carl Pomerance, Igor Shparlinski.* On Giuga numbers // Int. J. Mod. Math. – 2009. – **4**, № 1. – P. 13 – 18.
17. *Vicentiu Tipu.* A note on Giuga's conjecture // Can. Math. Bull. – 2007. – **50**, № 1. – P. 158 – 160.
18. *Erick Wong.* Computations on normal families of primes: M. Sc. Thesis. – Simon Fraser Univ., 1997.

Received 20.11.13