Werk

Titel: On Giuga's Conjecture.

Autor: Agoh, Takashi

Jahr: 1995

PURL: https://resolver.sub.uni-goettingen.de/purl?365956996_0087|log37

Kontakt/Contact

Digizeitschriften e.V.
SUB Göttingen
Platz der Göttinger Sieben 1
37073 Göttingen

info@digizeitschriften.de

manuscripta math. 87, 501 - 510 (1995)

manuscripta mathematica
©Springer-Verlag 1995

On Giuga's Conjecture

Takashi Agoh

Department of Mathematics, Science University of Tokyo, Noda, Chiba 278, Japan
E-mail address: agoh@ma.noda.sut.ac.jp

Received April 11, 1995

To the memory of Suzuko Koshiba-Takamiya

In this paper we shall investigate Giuga's conjecture which asserts an interesting characterization of prime numbers, just as Wilson's Theorem. Some variations and consequences of the Giuga congruence are discussed by means of Bernoulli numbers. In addition, we shall study various quotients relating to the integers satisfying the Giuga congruence.

1. Introduction

In 1950, Giuga asked in his paper [7] whether if the congruence

$$\text{(G)} \qquad 1^{n-1} + 2^{n-1} + \cdots + (n-1)^{n-1} \equiv -1 \pmod{n}$$

holds for $n \geq 2$, then n is a prime. Conversely, if n is a prime, then by Fermat's little theorem this congruence obviously holds.

This problem has been also introduced in the books of Ribenboim [11, 12] and Sierpiński [13].

We now present the following definition:

Definition 1. *The composite number n satisfying* (G) *will be called a Giuga number.*

According to this definition, we may state the following

Conjecture (Giuga). *There is no Giuga number.*

If this conjecture is true, then the congruence (G) provides an interesting characterization of prime numbers, just as Wilson's Theorem.

In the same paper Giuga confirmed himself that this conjecture is true for $n \leq 10^{1000}$. Also, Bedocchi [5] verified the same statement for $n \leq 10^{1700}$.

Recently, it has been reported in [6] that any counterexample for this conjecture has at least 12055 digits.

In this paper we shall investigate some variations and consequences of the Guiga congruence (G) by means of Bernoulli numbers. In addition, special quotients relating to the integers n satisfying (G) are discussed.

2. Basic properties of n satisfying (G)

In this section, we extract from Giuga's paper [7] some basic and important properties of an integer n satisfying (G).

Define $\Sigma = \{n \geq 2 \mid n \text{ satisfies (G)}\}$. At first, we shall introduce a characterization of an integer $n \in \Sigma$.

Proposition 1. *Let $n \geq 2$. Then $n \in \Sigma$ if and only if $p^2(p-1) \mid n-p$ for any prime factor p of n.*

The proof can be easily given by elementary method (see e.g. Ribenboim [11], Chapter 2, II-C).

By this proposition we know that if $n \in \Sigma$, then n is odd and square-free. Hence, we may assume that

$$n = p_1 p_2 \cdots p_s \quad \text{and} \quad 3 \leq p_1 < p_2 < \cdots < p_s$$

with s distinct odd primes $p_1, p_2, \cdots, p_s$.

It is also easy to show from Proposition 1 that

Proposition 2. *Let $n \geq 2$. Then $n \in \Sigma$ if and only if $p-1 \mid n-1$ for any prime factor p of n and*

$$n \sum_{p \mid n} \frac{1}{p} \equiv 1 \pmod{n}.$$

By this proposition we see that if $n \in \Sigma$, then for $k = 1, 2, \cdots, s-1$

$$n < n+1 \leq n \sum_{p \mid n} \frac{1}{p} = n\left(\sum_{i=1}^{k} \frac{1}{p_i} + \sum_{i=k+1}^{s} \frac{1}{p_i}\right) \leq n \sum_{i=1}^{k} \frac{1}{p_i} + (s-k)\frac{n}{p_{k+1}} < s\frac{n}{p_1},$$

which shows

$$\sum_{p \mid n} \frac{1}{p} > 1,$$

and further

$$s < p_1 \quad \text{and} \quad s > k + p_{k+1}\left(1 - \sum_{i=1}^{k} \frac{1}{p_i}\right) \ (k = 1, 2, \cdots, s-1).$$

Proposition 3. *If $n \in \Sigma$, then $(\varphi(n), n) = 1$, where φ is the Euler totient function.*

This result is an easy consequence of Proposition 1. In fact, if we assume that n is a composite and $p \equiv 1 \pmod{q}$ for different prime factors p and q of n, then $0 \equiv (n-1)+(1-p) = n-p = (n-q)+(q-p) \equiv -p \pmod{q}$, which is contrary to $p \neq q$.

The following statement is also immediate from Proposition 1.

Proposition 4. *If $n \in \Sigma$, then*

(i) $a^{n-1} \equiv 1 \pmod{n}$ *for any integer a with $(a,n)=1$,*

(ii) $a^{n-p} \equiv 1 \pmod{p^3}$ *for any prime factor p of n and integer a with $p \nmid a$.*

Here, the composite number $n > 0$ satisfying the congruence (i) of this proposition is called a *Carmichael number*. It can be easily shown that n is a Carmicheal number if and only if $p(p-1) \mid n-p$ for any prime factor p of n. Therefore we see, in view of Proposition 1, that a Giuga number requires much stronger condition than that of a Carmichael number.

Note that the smallest Carmichael number is $561 = 3 \cdot 11 \cdot 17$. Recently, in the ingenious paper [4] of Alford, Granville and Pomerance, it was shown that there exist infinitely many Carmichael numbers.

3. Some variations and consequeces of (G)

In this section we shall discuss some variations and consequences of (G) by means of Bernoulli numbers and derive specific properties of an integer $n \in \Sigma$.

For $m \geq 0$ and $k \geq 1$, we let

$$S_m(k) = \sum_{a=1}^{k} a^m \quad \text{and} \quad S_m^*(k) = \sum_{\substack{a=1 \\ (a,k)=1}}^{k} a^m,$$

and denote by B_m $(m \geq 0)$ the Bernoulli numbers defined by

$$\frac{x}{e^x - 1} = \sum_{m=0}^{\infty} \frac{B_m}{m!} x^m,$$

thus $B_0 = 1, B_1 = -1/2, B_2 = 1/6, B_3 = 0$, and so on.

We now present some fundamental properties relating to the above sums and Bernoulli numbers which will be needed later:

(I) (Euler-MacLaurin Summation Formula). *If $m \geq 0$ and $k \geq 1$, then*

$$S_m(k) = \sum_{i=1}^{m+1} \frac{1}{i} \binom{m}{i-1} (k+1)^i B_{m+1-i}.$$

(II) (cf. Agoh [1], Theorem 1). *If $m \geq 0$ and $k \geq 1$, then*

$$S_m^*(k) = \sum_{i=1}^{m+1} \frac{1}{i} \binom{m}{i-1} k^i H_{m+1-i}(k),$$

where

$$H_i(k) = \prod_{p|k}(1 - p^{i-1})B_i \quad (0 \le i \le m)$$

with the product taken over all prime factors p of k.

(III) (von Staudt-Clausen's Theorem). *If $m \ge 2$ is even, then*

$$B_m + \sum_{p-1|m} \frac{1}{p}$$

is an integer, where the sum is taken over all primes p such that $p - 1 \mid m$.

For a prime p, let $\mathbb{Z}_p$ be the ring of all rational numbers which are p-integral. By (III) we know that if $p - 1 \nmid m$, then $B_m \in \mathbb{Z}_p$. Also, if $p - 1 \mid m$, then $pB_m \in \mathbb{Z}_p$, more precisely $pB_m \equiv -1 \pmod{p}$.

Proposition 5. *Let $n \ge 2$. Then $n \in \Sigma$ if and only if $nB_{n-1} \equiv -1 \pmod{n}$.*

Proof. When n is a prime, the assertion is trivial. So suppose that n is a composite number. Take m, $k = n - 1$ in (I). Since n is odd ≥ 9, $B_{n-2} = 0$. Also, $nB_{n-i} \in \mathbb{Z}_p$ $(i = 3, 4, \cdots, n)$ for any prime factor p of n. Hence we can derive

$$S_{n-1}(n-1) = \sum_{i=1}^{n} \frac{1}{i}\binom{n-1}{i-1} n^i B_{n-i} \equiv nB_{n-1} \pmod{n},$$

which shows that the proposition follows. □

Note that the Carmichael condition $p(p-1) \mid n - p$ is equivalent to

$$nB_{n-1} \equiv -n \sum_{p|n} \frac{1}{p} \pmod{n}.$$

Therefore we may deduce the above result also from Proposition 2.

Proposition 6. *If n is a Giuga number, then for any prime factor p of n*

(i) $pB_{n-p} \equiv p - 1 \pmod{p^3}$,

(ii) $pB_{(n/p)-1} \equiv p - 1 \pmod{p^2}$,

(iii) $pB_{((n/p)-1)/p} \equiv p - 1 \pmod{p}$.

Proof. Take $m = n - p$ and $k = p - 1$ in (I):

$$S_{n-p}(p-1) = \sum_{i=1}^{n-p+1} \frac{1}{i}\binom{n-p}{i-1} p^i B_{n-p+1-i}.$$

By Proposition 4-(ii) we have $S_{p-1}(p-1) \equiv p - 1 \pmod{p^3}$. Also, $B_{n-p-1} = 0$ and for $i \ge 3$

$$\frac{1}{i}\binom{n-p}{i-1}p^{i-1} \equiv 0 \pmod{p^3}.$$

Thus we obviously see that n satisfies the congruence (i). Similarly, the other assertions can be also deduced by the same argument as done for (i). □

Let Λ be any non-empty subset of the set of prime factors p of a fixed integer $n \in \Sigma$. Then we can state

Proposition 7. *Let $M = M(\Lambda) = \prod_{p\in\Lambda} p$ and $t = t(\Lambda)$ be the number of elements of Λ. If $n \in \Sigma$, then*

$$\left(\sum_{p\in\Lambda}\frac{M}{p}\right)\left(\prod_{p\in\Lambda}\frac{1-p^{n-2}}{1-p}\right) \equiv (-1)^{t-1} \pmod{M}.$$

In particular,

$$\prod_{p|n}\frac{1-p^{n-2}}{1-p} \equiv (-1)^{s-1} \pmod{n},$$

where s is the number of prime factors of n.

Proof. By Proposition 2, $p-1 \mid n-1$ for any $p \in \Lambda$. Therefore, we obtain from (III)

$$MB_{n-1} \equiv -M\sum_{p\in\Lambda}\frac{1}{p} \pmod{M}.$$

Taking $m = n-1$ and $k = M$ in (II),

$$S^*_{n-1}(M) = \sum_{i=1}^{M}\frac{1}{i}\binom{n-1}{i-1}M^iH_{n-i}(M).$$

Since $S^*_{n-1}(M) \equiv \varphi(M) \pmod{M}$ and

$$\frac{1}{i}\binom{n-1}{i-1}M^{i-1} \equiv 0 \pmod{M}$$

for $i \geq 2$, it follows that

$$\varphi(M) \equiv MH_{n-1}(M) \equiv -\left(\prod_{p\in\Lambda}(1-p^{n-2})\right)\left(M\sum_{p\in\Lambda}\frac{1}{p}\right) \pmod{M},$$

which proves the first congruence, because $(\varphi(M), M) = 1$ by Proposition 3. When $M = n$, use Proposition 2. Then the second congruence is immediately deduced from the first. □

4. Special quotients relating to $n \in \Sigma$

In this section we will deal with special quotients relating to an integer $n \in \Sigma$ and describe some arithmetic properties of them.

Let denote by Γ the set of Carmichael numbers. For an integer $n \geq 2$ and a prime p, we now define various quotients with base a:

Definition 2. *We define*

(i) $q_p(a) = \dfrac{a^{p-1}-1}{p}$ $(p \nmid a)$, *the Fermat quotient of* p,

(ii) $q(a,n) = \dfrac{a^{\varphi(n)}-1}{n}$ $((a,n)=1)$, *the Euler quotient of* n,

(iii) $C(a,n) = \dfrac{a^{n-1}-1}{n}$ $(n \in \Gamma,\ (a,n)=1)$, *the Carmichael quotient of* n,

(iv) $G_p(a,n) = \dfrac{a^{n-p}-1}{p^3}$ $(n \in \Sigma,\ p \mid n,\ p \nmid a)$, *the Giuga quotient of* n.

It is easily seen that all of these quotients are integers and satisfy the following "*logarithmic property*":

Proposition 8. *For* p, n, a *and* b *approved in Definition* 2, *it follows that*

(i) $q_p(ab) \equiv q_p(a) + q_p(b) \pmod{p}$,

(ii) $q(ab,n) \equiv q(a,n) + q(b,n) \pmod{n}$,

(iii) $C(ab,n) \equiv C(a,n) + C(b,n) \pmod{n}$,

(iv) $G_p(ab,n) \equiv G_p(a,n) + G_p(b,n) \pmod{p^3}$.

Note that Giuga's conjecture is the same as the assertion $G_p(a,n) = 0$ for all bases a with $p \nmid a$.

In his papers [9, 10], Lerch gave the following expression for $q(a,n)$ modulo n:

Proposition 9. *If* $n \geq 2$ *and* a *are integers with* $(a,n)=1$, *then*

$$q(a,n) \equiv \sum_{\substack{k=1 \\ (k,n)=1}}^{n-1} \frac{1}{ak}\left[\frac{ak}{n}\right] \pmod{n},$$

where $[x]$ *denotes the greatest integer* $\leq x$. *In particular, if* p *is a prime and* $p \nmid a$, *then*

$$q_p(a) \equiv \sum_{k=1}^{p-1} \frac{1}{ak}\left[\frac{ak}{p}\right] \pmod{p}.$$

Many interesting properties of Fermat and Euler quotients can be deduced in connection with Wilson quotients (for primes and composites) and Bernoulli numbers. Expositions and details are found in the papers of Agoh [2], Agoh, Dilcher and Skula [3], Lehmer [8] and Lerch [9, 10].

We introduce here the definition of Wilson quotients for prime and composite numbers:

Definition 3. *For $m \geq 2$, let*

$$J(m) = \prod_{\substack{j=1 \\ (j,m)=1}}^{m} j$$

and

$$\varepsilon_m = \begin{cases} -1 & \text{when } m = 2,\ 4,\ q^\alpha,\ 2q^\alpha \ (q \text{ is an odd prime, } \alpha \geq 1), \\ 1 & \text{otherwise.} \end{cases}$$

Then we denote by

(i) $W_p = \dfrac{(p-1)!+1}{p}$ *(p is a prime), the Wilson quotient of p,*

(ii) $W(m) = \dfrac{J(m) - \varepsilon_m}{m}$ $(m \geq 2)$, *the generalized Wilson quotient of m.*

According to Wilson's Theorems for primes and composites, we clearly see that W_p and $W(m)$ both are integers. For these quotients we have the following expressions modulo p (cf. [3], Proposition 8):

Proposition 10. *For an integer $m \geq 2$, it follows that*

$$\varepsilon_m \varphi(m) W(m) \equiv \sum_{\substack{a=1 \\ (a,m)=1}}^{m-1} q(a,m) \pmod{m}.$$

In particular, if p is an odd prime, then

$$W_p \equiv \sum_{a=1}^{p-1} q_p(a) \pmod{p}.$$

Lemma 1 (Voronoï's Congruence). *Let $t \geq 1$, $m \geq 2$ and a be integers with $(a,m) = 1$. Then*

$$\frac{(a^t-1)S_t^*(m)}{m} \equiv t \sum_{\substack{k=1 \\ (k,m)=1}}^{m-1} (ak)^{t-1} \left[\frac{ak}{m}\right] \pmod{m}.$$

Proof. For each k $(1 \leq k \leq m-1)$ with $(k,m) = 1$, there exists an integer r_k such that

$$ak = \left[\frac{ak}{m}\right] m + r_k, \quad 1 \leq r_k \leq m-1.$$

Hence we have

$$(ak)^t = \left(\left[\frac{ak}{m}\right] m + r_k\right)^t \equiv tm \left[\frac{ak}{m}\right] r_k^{t-1} + r_k^t \pmod{m^2}.$$

Noting that $\{r_k \mid 1 \le k \le m-1\} = \{k \mid (k,m) = 1, 1 \le k \le m-1\}$ and $r_k \equiv ak \pmod{m}$, sum over the k's with $(k,m) = 1$ and $1 \le k \le m-1$. Then we get

$$(a^t - 1)S_t^*(m) \equiv tm \sum_{\substack{k=1 \\ (k,m)=1}}^{m-1} (ak)^{t-1} \left[\frac{ak}{m}\right] \pmod{m^2},$$

which proves the lemma. □

Using the above lemma we may state

Proposition 11. (i) *If $n \in \Gamma$ and $(a,n) = 1$, then*

$$\varphi(n)C(a,n) \equiv (n-1)q(a,n) \pmod{n}.$$

(ii) *If $n \in \Sigma$, $p \mid n$ and $p \nmid a$, then*

$$(p-1)G_p(a,n) \equiv \frac{n-p}{p^2} q_p(a) \pmod{p}.$$

Proof. (i) Take $m = n$ and $t = n-1$ in Lemma 1:

$$C(a,n)S_{n-1}^*(n) \equiv (n-1) \sum_{\substack{k=1 \\ (k,m)=1}}^{m-1} (ak)^{n-2} \left[\frac{ak}{n}\right] \pmod{n}.$$

Since $n \in \Gamma$, we have $S_{n-1}^*(n) \equiv \varphi(n) \pmod{n}$ and

$$(ak)^{n-2} \equiv \frac{1}{ak} \pmod{n}.$$

Hence, the congruence (i) follows from Proposition 9.

(ii) Similarly, take $m = p^3$ and $t = n-p$ in Lemma 1:

$$G_p(a,n)S_{n-p}^*(p^3) \equiv (n-p) \sum_{\substack{k=1 \\ (k,p)=1}}^{p^3-1} (ak)^{n-p-1} \left[\frac{ak}{p^3}\right] \pmod{p^3}.$$

Since $n \in \Sigma$, we have $S_{n-p}^*(p^3) \equiv p^2(p-1) \pmod{p^3}$ and

$$(ak)^{n-p-1} \equiv \frac{1}{ak} \pmod{p^3}.$$

Therefore, by using Proposition 9 the above congruence yields

$$(p-1)G_p(a,n) \equiv \frac{n-p}{p^2} q(a,p^3) \pmod{p}.$$

Here, we shall show that $q(a,p^3) \equiv q_p(a) \pmod{p}$. Since p is odd and so

$$\binom{p^2}{i} p^{i-3} \equiv 0 \pmod{p}$$

for each $i \geq 2$, it follows that

$$\begin{aligned} q(a,p^3) &= \frac{a^{\varphi(p^3)}-1}{p^3} = \frac{1}{p^3}\sum_{i=1}^{p^2}\binom{p^2}{i}(a^{p-1}-1)^i \\ &= \sum_{i=1}^{p^2}\binom{p^2}{i}p^{i-3}(q_p(a))^i \equiv q_p(a) \pmod{p}, \end{aligned}$$

which completes the proof. □

For $n \in \Gamma$, we have $(\varphi(n), n) = (n-1, n) = 1$, which implies that $C(a,n) \equiv 0 \pmod{n}$ if and only if $q(a,n) \equiv 0 \pmod{n}$.

Here, the following questions for Carmichael quotients arise naturally:

(1) *For a given $n \in \Gamma$, does there exist a base a such that $(a,n) = 1$ and $C(a,n) \equiv 0 \pmod{n}$?*

(2) *For a given base a, does there exist an integer $n \in \Gamma$ such that $(a,n) = 1$ and $C(a,n) \equiv 0 \pmod{n}$?*

On the other hand, for a given prime p and an integer a with $p \nmid a$, it follows that

$$q_p(p-a) \equiv q_p(a) + \frac{1}{a} \pmod{p}.$$

This shows that $p \mid q_p(a)$ and $p \mid q_p(p-a)$ do not hold simultaneously. Therefore, there exists an integer a, $p \nmid a$, such that $p \nmid q_p(a)$. For such an integer a and $n \in \Sigma$ the congruence (ii) of Proposition 11 implies that $G_p(a,n) \equiv 0 \pmod{p}$ if and only if $n \equiv p \pmod{p^3}$.

The following proposition is an immediate consequence of Propositions 10 and 11:

Proposition 12. (i) *If $n \in \Gamma$, then*

$$\sum_{\substack{a=1 \\ (a,n)=1}}^{n-1} C(a,n) \equiv -\varepsilon_n W(n) \pmod{n}.$$

(ii) *If $n \in \Sigma$, then for any prime factor p of n*

$$\sum_{a=1}^{p-1} G_p(a,n) \equiv -\frac{n-p}{p^2} W_p \pmod{p}.$$

We do not enter into details, but it may be also possible to deduce various properties of Carmichael and Giuga numbers by means of Euler numbers.

Acknowledgement. Thanks to Karl Dilcher and Ladislav Skula for many useful discussions.

References

1. T. Agoh, On Bernoulli and Euler numbers, manuscripta math. **61** (1988), 1-10
2. T. Agoh, On Fermat and Wilson quotients, Preprint (1995)
3. T. Agoh, K. Dilcher and L. Skula, Fermat and Wilson quotients for composite moduli, Preprint (1995)
4. W.R. Alford, A. Granville and C. Pomerance, There are infinitely many Carmichael numbers, Ann. of Math. **140** (1994), 1-20
5. E. Bedocchi, Nota ad una congettura sui numeri primi, Riv. Mat. Univ. Parma **11** (1985), 229-236
6. D. Borwein, J.M. Borwein, P.B. Borwein and R. Girgensohn, Giuga's conjecture on primality, Preprint (1994)
7. G. Giuga, Su una presumibile proprietà caratteristica dei numeri primi, Ist. Lombardo Sci. Lett. Rend. Cl. Sci. Mat. Nat. **83** (1950), 511-528
8. E. Lehmer, On congruences involving Bernoulli numbers and the quotients of Fermat and Wilson, Ann. of Math. **39** (1938), 350-360
9. M. Lerch, Zur Theorie des Fermatschen Quotienten $\frac{a^{p-1}-1}{p} = q(a)$, Math. Annalen **60** (1905), 471-490
10. M. Lerch, Sur les théorèmes de Sylvester concernant le quotient de Fermat, C. R. Acad. Sci. Paris **142** (1906), 35-38
11. P. Ribenboim, The book of prime number records, Springer-Verlag, New York, 1988
12. P. Ribenboim, The little book of big primes, Springer-Verlag, New York, 1991
13. W. Sierpiński, Elementary number theory, Hafner, New York, 1964

This article was processed by the author using the LaTeX style file *cljour1* from Springer-Verlag.