A VON STAUDT-TYPE FORMULA FOR $\sum_{z\in\mathbb{Z}_n[i]} z^k$

P. FORTUNY AYUSO, JOSÉ MARÍA GRAU, AND ANTONIO M. OLLER-MARCÉN

Abstract. In this paper we study the sum of powers in the Gaussian integers $\mathbf{G}_k(n) := \sum_{a,b\in[1,n]}(a+bi)^k$. We give an explicit formula for $\mathbf{G}_k(n) \pmod n$ in terms of the prime numbers $p \equiv 3 \pmod 4$ with $p \,||\, n$ and $p-1 \mid k$, similar to the well known one due to von Staudt for $\sum_{i=1}^n i^k \pmod n$. We apply this formula to study the set of integers n which divide $\mathbf{G}_n(n)$ and compute its asymptotic density with six exact digits: $0.971000\ldots$.

AMS 2010 Mathematics Subject Classification 11B99, 11A99, 11A07
Keywords: Power sum, Erdös-Moser equation, Asymptotic density

1. Introduction

The sum of powers of integers of the form

$$S_k(n) := 1^k + 2^k + 3^k + \cdots + n^k$$

is a well-studied problem in arithmetic (see e.g., [20] and [21]). Finding formulas for these sums has interested mathematicians for more than 300 years since the time of James Bernoulli (1665-1705). If we call B_i and $B_i(x)$ the i-th Bernoulli number and Bernoulli polynomial, respectively, then (see, e.g., [1])

$$S_k(m) = \frac{B_{k+1}(m+1) - B_{k+1}}{k+1}. \tag{1}$$

The sum of powers modulo n was studied by von Staudt in 1840 in [11], where he gave the following result for even k:

Theorem 1. *Let $k, n \geq 1$ be integers with k even, then,*

$$S_k(n) \equiv -\sum_{\substack{p\mid n\\ p-1\mid k}} \frac{n}{p_i} \pmod n.$$

L. Carlitz [2] considered the case k odd and claimed that $n \mid S_k(n)$ in that case. P. Moree [7] pointed out that this is false, but that $S_k(n) = rn/2$ for integer r. The following lemma from a preprint of [4] gives the parity of r:

Lemma 1. *Let $k > 2$ be odd. There is an integer r such that $S_k(n) = rn/2$. If $n \equiv 2 \pmod 4$ then r is odd, otherwise it is even.*

TABLE 1. $\mathbf{G}_k(n) \pmod n$ for $1 \le k, n \le 24$; whit $\epsilon := (1+i)$.

$k \diagdown n$	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24
1	**0**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
2	0	**0**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
3	0	ϵ	**0**	0	0	3ϵ	0	0	0	5ϵ	0	0	0	7ϵ	0	0	0	9ϵ	0	0	0	11ϵ	0	0
4	0	0	0	**0**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
5	0	ϵ	0	0	**0**	3ϵ	0	0	0	5ϵ	0	0	0	7ϵ	0	0	0	9ϵ	0	0	0	11ϵ	0	0
6	0	0	0	0	0	**0**	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
7	0	ϵ	0	0	0	3ϵ	**0**	0	0	5ϵ	0	0	0	7ϵ	0	0	0	9ϵ	0	0	0	11ϵ	0	0
8	0	0	2	0	0	2	0	**0**	0	0	0	8	0	0	5	0	0	0	0	0	14	0	0	8
9	0	ϵ	0	0	0	3ϵ	0	0	**0**	5ϵ	0	0	0	7ϵ	0	0	0	9ϵ	0	0	0	11ϵ	0	0
10	0	0	0	0	0	0	0	0	0	**0**	0	0	0	0	0	0	0	0	0	0	0	0	0	0
11	0	ϵ	0	0	0	3ϵ	0	0	0	5ϵ	**0**	0	0	7ϵ	0	0	0	9ϵ	0	0	0	11ϵ	0	0
12	0	0	0	0	0	0	0	0	0	0	0	**0**	0	0	0	0	0	0	0	0	0	0	0	0
13	0	ϵ	0	0	0	3ϵ	0	0	0	5ϵ	0	0	**0**	7ϵ	0	0	0	9ϵ	0	0	0	11ϵ	0	0
14	0	0	0	0	0	0	0	0	0	0	0	0	0	**0**	0	0	0	0	0	0	0	0	0	0
15	0	ϵ	0	0	0	3ϵ	0	0	0	5ϵ	0	0	0	7ϵ	**0**	0	0	9ϵ	0	0	0	11ϵ	0	0
16	0	0	2	0	0	2	0	0	0	0	0	8	0	0	5	**0**	0	0	0	0	14	0	0	8
17	0	ϵ	0	0	0	3ϵ	0	0	0	5ϵ	0	0	0	7ϵ	0	0	**0**	9ϵ	0	0	0	11ϵ	0	0
18	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**0**	0	0	0	0	0	0
19	0	ϵ	0	0	0	3ϵ	0	0	0	5ϵ	0	0	0	7ϵ	0	0	0	9ϵ	**0**	0	0	11ϵ	0	0
20	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**0**	0	0	0	0
21	0	ϵ	0	0	0	3ϵ	0	0	0	5ϵ	0	0	0	7ϵ	0	0	0	9ϵ	0	0	**0**	11ϵ	0	0
22	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	**0**	0	0
23	0	ϵ	0	0	0	3ϵ	0	0	0	5ϵ	0	0	0	7ϵ	0	0	0	9ϵ	0	0	0	11ϵ	**0**	0
24	0	0	2	0	0	2	0	0	0	0	0	8	0	0	5	0	0	0	0	0	14	0	0	**8**

On the other hand, in [3] the pairs (k, n) with $k, n \ge 1$ such that $n \mid S_k(n)$ were characterized. In particular:

Theorem 2. *Let $k, n \ge 1$ be integers. Then, $n \mid S_k(n)$ if and only if one of the following holds:*

i) *n is odd and $p - 1 \nmid k$ for every prime divisor p of n.*
ii) *n is a multiple of 4 and $k > 1$ is odd.*

Much research has been carried out regarding divisibility properties of power sums (see for instance [5, 6, 9, 10]).

In this work, we deal with power sums of Gaussian integers, an extension that has not been considered yet. Instead of the sum of the k-th powers of the first n positive integers, we are concerned with the sum of the k-th powers of all Gaussian integers in the $n \times n$ base square of the first quadrant. Namely, this paper deals with power sums of the form:

$$\mathbf{G}_k(n) := \sum_{1 \le a, b \le n} (a + bi)^k.$$

Table 1 lists the values of $\mathbf{G}_k(n) \pmod n$ for $1 \le k, n \le 24$.

A cursory look at Table 1 supports the idea that when $\mathrm{Im}(\mathbf{G}_k(n)) \not\equiv 0 \pmod n$ (i.e., when $\mathbf{G}_k(n)$ is not real modulo n) then $\mathrm{Re}(\mathbf{G}_k(n)) \equiv \mathrm{Im}(\mathbf{G}_k(n)) \equiv n/2 \pmod n$. The large proportion of pairs (k, n) for which $n \mid \mathbf{G}_k(n)$ is also remarkable.

The main goal of this paper is to give an analogue of Carlitz-von Staudt formula in this Gaussian setting. In particular we prove the following result:

Theorem. *Let $k, n \ge 1$ be integers and consider the set*

$$\mathcal{P}(k, n) := \{\text{prime } p : p \,||\, n, p^2 - 1 \mid k, p \equiv 3 \pmod 4\}.$$

Then:

$$\mathbf{G}_k(n) \equiv \begin{cases} \frac{n}{2}(1+i) \pmod{n}, & \text{if } k>1 \text{ is odd and } n \equiv 2 \pmod 4; \\ -\sum\limits_{p\in\mathcal{P}(k,n)} \dfrac{n^2}{p^2} \pmod{n}, & \text{otherwise.} \end{cases}$$

As an application of this result, we study the asymptotic density of the set of integers n such that $n \mid \mathbf{G}_n(n)$, (i.e., the density of zeros in the diagonal of Table 1). We prove that this set has indeed an asymptotic density and compute its value up to the sixth decimal digit $0.971000\ldots$. This value is in contrast with that of the classical integral setting [3], where the asymptotic density of the set of integers n such that $n \mid S_n(n)$ is exactly $1/2$.

2. Auxiliary results on sums of binomial coefficients

In order to prove our main theorem we use some technical results involving sums of binomial coefficients. The first one is due to Hermite [13], although Bachman [14] gave it in a more general form:

Lemma 2. *Let k be a positive integer and p be a prime. Then:*

$$\sum_{0<j(p-1)<k} \binom{k}{j(p-1)} \equiv 0 \pmod p.$$

The second technical result we use is more recent and is due to Dilcher [12]. It involves alternating lacunary sums of binomial coefficients:

Lemma 3. *Let k be a positive integer and let p be an odd prime. Then*

$$\sum_{j=0}^{k}(-1)^j\binom{k(p-1)}{j(p-1)} \equiv \begin{cases} 0 \pmod p, & \text{if } k \text{ is odd;} \\ 2 \pmod p, & \text{if } k \text{ is even and } p+1 \nmid k; \\ 1 \pmod p, & \text{if } p+1 \mid k. \end{cases}$$

The following proposition will also play a key role in the proof of our main theorem. It is a direct consequence of the lemmata above.

Proposition 1. *Let p be an odd prime and n a positive integer such that $p-1 \mid n$. Then:*

$$\sum_{j=1}^{\frac{n}{(p-1)}-1} (-1)^{\frac{j(p-1)}{2}} \binom{n}{j(p-1)} \equiv \begin{cases} -1 \pmod p, & \text{if } p\equiv 3 \pmod 4 \text{ and } p+1 \mid \frac{n}{(p-1)}; \\ 0 \pmod p, & \text{otherwise.} \end{cases}$$

Proof. Write $n = k(p-1)$. then the sum in the statement is

$$S = \sum_{j=1}^{k-1}(-1)^{\frac{j(p-1)}{2}}\binom{k(p-1)}{j(p-1)}.$$

If $p \equiv 1 \pmod 4$, then $\frac{p-1}{2}$ is even and the sum S does not alternate so that Lemma 2 applies and $S \equiv 0 \pmod p$ in this case.

On the other hand, if $p \equiv 3 \pmod 4$ S alternates then

$$S = \sum_{j=0}^{k}(-1)^j\binom{k(p-1)}{j(p-1)} - \binom{k(p-1)}{0} - (-1)^k\binom{k(p-1)}{k(p-1)}$$

and the result follows by Lemma 3. □

3. Proof of the main theorem

Recall that

$$\mathbf{G}_k(n) := \sum_{1\leq a,b\leq n} (a+bi)^k.$$

Writing $z = a + bi$, the binomial theorem gives:

$$\mathbf{G}_k(n) \equiv \sum_{1\leq a\leq n}\sum_{1\leq b\leq n}\sum_{1\leq m\leq k}\binom{k}{m}a^{k-m}b^m i^m \pmod{n}.$$

Consequently, from the definition of the power sum $S_k(n)$ we obtain the following:

Lemma 4. *Let k, n be positive integers. Then:*

i) $Re(\mathbf{G}_k(n)) \equiv \sum_{j=0}^{\lfloor k/2\rfloor}(-1)^j\binom{k}{2j}S_{2j}(n)S_{k-2j}(n) \pmod{n}$.

ii) $Im(\mathbf{G}_k(n)) \equiv \sum_{j=0}^{\lfloor (k-1)/2\rfloor}(-1)^j\binom{k}{2j+1}S_{2j+1}(n)S_{k-2j-1}(n) \pmod{n}$.

This result allows us to study $\mathrm{Re}(\mathbf{G}_k(n))$ and $\mathrm{Im}(\mathbf{G}_k(n))$ separately. We start with the imaginary part:

Proposition 2. *For any integers n, k, $Im(\mathbf{G}_k(n)) \equiv 0 \pmod{n}$ unless $n \equiv 2 \pmod 4$ and $k > 1$ is odd in which case $Im(\mathbf{G}_k(n)) \equiv n/2 \pmod{n}$.*

Proof. We examine different cases and use Lemma 4 ii) extensively.

- If n is odd, then $p - 1$ is even for every $p \mid n$ and we can apply part i) of Theorem 2 to get $S_{2j+1}(n) \equiv 0 \pmod{n}$ for every $0 \leq j \leq \lfloor k/2\rfloor + 1$. Hence $\mathrm{Im}(\mathbf{G}_k(n)) \equiv 0 \pmod{n}$ in this case.
- If $4 \mid n$ then Theorem 2 ii) implies that $S_{2j+1}(n) \equiv 0 \pmod{n}$ for every $j > 1$. Consequently, $\mathrm{Im}(\mathbf{G}_k(n)) \equiv k\frac{n(n-1)}{2}S_{k-1}(n) \pmod{n}$ and four cases arise:
  i) If $k = 1$, then $\mathrm{Im}(\mathbf{G}_k(n)) \equiv n\frac{n(n-1)}{2} \equiv 0 \pmod{n}$.
  ii) If $k = 2$, then $\mathrm{Im}(\mathbf{G}_k(n)) \equiv 2\left(\frac{n(n-1)}{2}\right)^2 \equiv 0 \pmod{n}$.
  iii) If $k > 2$ is even, then $S_{k-1}(n) \equiv 0 \pmod{n}$ due to Theorem 2 ii) and hence $\mathrm{Im}(\mathbf{G}_k(n)) \equiv 0 \pmod{n}$.
  iv) If $k > 1$ is odd, then [3, Lemma 3] $S_{k-1}(n) \equiv \frac{n}{2}S_{k-1}(2) \equiv 0 \pmod 2$ so that $\mathrm{Im}(\mathbf{G}_k(n)) \equiv 0 \pmod{n}$.
- For $n \equiv 2 \pmod 4$ we consider the following cases:
  i) If $k = 1$, since $S_0(n) = n$ then $\mathrm{Im}(\mathbf{G}_k(n)) \equiv 0 \pmod{n}$ trivially.
  ii) If k is even, then $\binom{k}{2j+1}$ is also even for every $j \geq 0$. Moreover, we know [3] that in this case $S_{2j+1}(n) \equiv 0 \pmod{n/2}$ from which follows that $\mathrm{Im}(\mathbf{G}_k(n)) \equiv 0 \pmod{n}$.
  iii) If $k > 1$ is odd, it is easy to see that $\sum_{j=0}^{\frac{k-1}{2}}\binom{k}{2j+1} \equiv 1 \pmod 2$. Thus, since $S_m(2) \equiv 1 \pmod 2$ for every positive m, it follows that $\mathrm{Im}(\mathbf{G}_k(n)) \equiv 1 \pmod 2$. Just like in the previous case, $\mathrm{Im}(\mathbf{G}_k(n)) \equiv 0 \pmod{n/2}$ and then $\mathrm{Im}(\mathbf{G}_k(n)) \equiv n/2 \pmod{n}$.

□

We now consider the real part, which requires a finer analysis. Notice that $S_k(1) = 1 \equiv 0 \pmod 1$, so that in what follows we assume $n > 1$.

Proposition 3. *If $n \equiv 2 \pmod 4$ and $k > 1$ is odd, then $Re(\mathbf{G}_k(n)) \equiv n/2 \pmod n$.*

Proof. Since k is odd, $k - 2j$ is odd for every $0 \leq j \leq \lfloor k/2 \rfloor$. Consequently [3] $S_{k-2j}(n) \equiv 0 \pmod{n/2}$ and due to Lemma 4 i), $\mathrm{Re}(\mathbf{G}_k(n)) \equiv 0 \pmod{n/2}$. Moreover, since $S_0(2) \equiv 0 \pmod 2$ and $S_m(2) \equiv 1 \pmod 2$ for every $m > 1$, it follows that $\mathrm{Re}(\mathbf{G}_k(n)) \equiv \dfrac{n^2}{4}\displaystyle\sum_{j=1}^{\frac{k-1}{2}} \binom{k}{2j} \pmod 2$. To conclude, it is enough to observe that $\displaystyle\sum_{j=1}^{\frac{k-1}{2}} \binom{k}{2j} \equiv 1 \pmod 2$ and $n^2/4 \equiv 1 \pmod 2$. □

Proposition 4. *If $k > 1$ is odd and $n \not\equiv 2 \pmod 4$, or if $k = 1$, then $Re(\mathbf{G}_k(n)) \equiv 0 \pmod n$.*

Proof. The case $k = 1$ is trivial, since $\mathrm{Re}(\mathbf{G}_k(n)) \equiv S_0(n)S_1(n) = nS_1(n) \equiv 0 \pmod n$.

Now, assume that $k > 1$ is odd and $n \not\equiv 2 \pmod 4$. We distinguish two cases:

i) If n is odd, then $S_{k-2j}(n) \equiv 0 \pmod n$ for every $0 \leq j \leq \lfloor k/2 \rfloor$ because $k - 2j$ is odd and Theorem 2 i) applies. The result follows from Lemma 4 i).

ii) If $4 \mid n$, then $S_{k-2j}(n) \equiv 0 \pmod n$ for every $0 \leq j < \lfloor k/2 \rfloor = \frac{k-1}{2}$. Hence, $\mathrm{Re}(\mathbf{G}_k(n)) \equiv (-1)^{\frac{k-1}{2}}\binom{k}{k-1}S_0(n)S_1(n) \equiv 0 \pmod n$ because $S_0(n) = n$.

□

Proposition 5. *Let $k > 1$ and $n = p_1^{r_1} \cdots p_s^{r_s}$ be integers. Then*

$$Re(\mathbf{G}_k(n)) \equiv \begin{cases} -\frac{n^2}{p_i^2} \pmod{p_i}, & \text{if } r_i = 1,\ p_i^2 - 1 \mid k \text{ and } p_i \equiv 3 \pmod 4; \\ 0 \pmod{p_i^{r_i}}, & \text{otherwise.} \end{cases}$$

Proof. Since k is even and $S_0(n) = 0$, by Lemma 4 i), for every $1 \leq i \leq s$:

$$\mathrm{Re}(\mathbf{G}_k(n)) \equiv \sum_{j=1}^{\frac{k}{2}-1} (-1)^j \binom{k}{2j} S_{2j}(n)S_{k-2j}(n) \pmod{p_i^{r_i}}.$$

As usual in this section, we study different cases:

- If $p_i = 2$, as $2j$ and $k - 2j$ are even for every j we have that [3] $S_{2j}(n) \equiv \frac{n}{2^{r_i}}S_{2j}(2^{r_i}) \equiv \frac{n}{2^{r_i}}2^{r_i-1} \equiv n/2 \pmod{2^{r_i}}$ and, in the same way $S_{k-2j}(n) \equiv n/2 \pmod{2^{r_i}}$. Hence, $\mathrm{Re}(\mathbf{G}_k(n)) \equiv \frac{n^2}{4}\sum_{j=1}^{\frac{k}{2}-1}(-1)^j\binom{k}{2j} \pmod{2^{r_i}}$. Now:
  i) If $r_i > 1$, clearly $n^2/4 \equiv 0 \pmod{2^{r_i}}$ because $2r_i - 2 \geq r_i$ and thus $\mathrm{Re}(\mathbf{G}_k(n)) \equiv 0 \pmod{2^{r_i}}$.
  ii) If $r_i = 1$, we have that $\sum_{j=1}^{\frac{k}{2}-1}(-1)^j\binom{k}{2j} \equiv \sum_{j=1}^{\frac{k}{2}-1}\binom{k}{2j} \equiv 0 \pmod 2$ so, again, $\mathrm{Re}(\mathbf{G}_k(n)) \equiv 0 \pmod{2^{r_i}}$.

- If p_i is an odd prime, then [3]:

$$S_m(p_i^{r_i}) \equiv \begin{cases} -p_r^{r_i-1} \pmod{p_i^{r_i}}, & \text{if } p_i - 1 \mid m; \\ 0 \pmod{p_i^{r_i}}, & \text{otherwise.} \end{cases}$$

Which gives:

i) If $r_i > 1$, then every term in the expression of $\mathrm{Re}(\mathbf{G}_k(n))$ is $0 \pmod{p_i^{r_i}}$:
   a) If either $p_i - 1 \nmid 2j$ or $p_i - 1 \nmid k - 2j$, then either $S_2 j(n) \equiv 0 \pmod{p_i^{r_i}}$ or $S_{k-2j}(n) \equiv 0 \pmod{p_i^{r_i}}$.
   b) If $p_i - 1$ divides both $2j$ and $k - 2j$, then $S_{2j}(n)S_{k-2j}(n) \equiv p^{2r_i-2} \equiv 0 \pmod{p_i^{r_i}}$.

ii) If $r_i = 1$ and $p_i - 1 \nmid k$, then, for every $1 \leq j \leq k/2 - 1$, either $p_i - 1 \nmid 2j$ or $p_i - 1 \nmid k - 2j$. Thus, every term in the expression of $\mathrm{Re}(\mathbf{G}_k(n))$ is $0 \pmod{p_i}$.

iii) If $r_i = 1$ and $p_i - 1 \mid k$, then, for every $1 \leq j \leq k/2 - 1$ either $p_i - 1 \mid 2j$ or $p_i - 1 \nmid 2j$. If $p_i - 1 \nmid 2j$, then the corresponding term is $0 \pmod{p_i}$. If $p_i - 1 \mid 2j$, so that $p_i - 1 \mid k - 2j$ and thus $S_{2j}(n) \equiv S_{k-2j}(n) \equiv n/p_i \pmod{p_i}$. Consequently,

$$\mathrm{Re}(\mathbf{G}_k(n)) \equiv \frac{n^2}{p_i^2} \sum_{\substack{1 \leq j \leq k/2-1 \\ p_i - 1 \mid 2j}} (-1)^j \binom{k}{2j} = \sum_{j=1}^{\frac{k}{p_i-1}-1} (-1)^{\frac{j(p_i-1)}{2}} \binom{k}{j(p_i-1)}.$$

But this latter sum can be evaluated using Proposition 1 to complete the proof in this case.

□

Theorem 3. *Let $k, n \geq 1$ be integers. Define the set*

$$\mathcal{P}(k,n) := \{\text{prime } p : p \,||\, n, p^2 - 1 \mid k, p \equiv 3 \pmod 4\}.$$

Then:

$$\mathbf{G}_k(n) \equiv \begin{cases} \frac{n}{2}(1+i) \pmod n, & \text{if } k > 1 \text{ is odd and } n \equiv 2 \pmod 4; \\ -\sum\limits_{p \in \mathcal{P}(k,n)} \frac{n^2}{p^2} \pmod n, & \text{otherwise.} \end{cases}$$

Proof. From Propositions 2 and 3, we know that $\mathbf{G}_k(n) \equiv \frac{n}{2}(1+i) \pmod n$ if $k > 1$ is odd and $n \equiv 2 \pmod 4$.

In the remaining cases, $\mathrm{Im}(\mathbf{G}_k(n)) \equiv 0 \pmod n$ by Proposition 2.

Define $n' = \prod\limits_{p \in \mathcal{P}(k,n)} p$. Clearly $n = \frac{n}{n'} \cdot n'$ and $\gcd(n/n', n') = 1$. Propositions 4 and 5 imply that:

$$\mathrm{Re}(\mathbf{G}_k(n)) \equiv 0 \pmod{n/n'},$$

$$\mathrm{Re}(\mathbf{G}_k(n)) \equiv -n^2/p^2 \pmod p, \text{ for every } p \in \mathcal{P}(k,n).$$

And the result follows applying the Chinese Remainder Theorem. □

4. On the congruence $\mathbf{G}_k(n) \equiv 0 \pmod{n}$

In this section we focus on the solutions to $\mathbf{G}_k(n) \equiv 0 \pmod{n}$; i.e. numbers n such that $0 = \sum_{z\in\mathbb{Z}_n[i]} z^k$. In particular, we study the sets

$$\mathcal{N}_k := \{n \in \mathbb{N} : \mathbf{G}_k(n) \equiv 0 \pmod{n}\},$$

$$\mathcal{K}_n := \{k \in \mathbb{N} : \mathbf{G}_k(n) \equiv 0 \pmod{n}\}.$$

In other words, we are interested in the zeros of each row and column in Table 1.

The following result is a simple consequence of Theorem 3:

Corollary 1. *Let $k, n \geq 1$ be integers. Then $\mathbf{G}_k(n) \not\equiv 0 \pmod{n}$ if and only if there exists a prime p dividing n such that:*

i) $p \equiv 3 \pmod 4$.
ii) $p^2 - 1 \mid k$.
iii) $p^2 \nmid n$.

This corollary will allow us to explicitly describe the complements of $\mathcal{N}_k$ and $\mathcal{K}_n$ and, furthermore, to obtain information about their density.

Proposition 6. *Let p be a prime a define the set $\mathbb{F}(p) := \{p(ps+r) : s \in \mathbb{N}$ and $0 < r < p\}$. Then:*

$$\mathbb{N} \setminus \mathcal{N}_k = \begin{cases} 4\mathbb{N} + 2, & \text{if } k > 1 \text{ is odd;} \\ \bigcup\limits_{\substack{p^2-1\mid k \\ p\equiv 3 \pmod 4}} \mathbb{F}(p), & \text{otherwise.} \end{cases}$$

Proposition 7. *Let p be a prime and define the set $\mathbb{G}(p) := \{h(p^2 - 1) : h \in \mathbb{N}\}$. Then:*

$$\mathbb{N} \setminus \mathcal{K}_n = \begin{cases} 2\mathbb{N} + 1, & \text{if } n \equiv 2 \pmod 4; \\ \bigcup\limits_{\substack{p\| n \\ p\equiv 3 \pmod 4}} \mathbb{G}(p), & \text{otherwise.} \end{cases}$$

In what follows, given a set $A \subseteq \mathbb{N}$, we denote by $\delta(A)$ its asymptotic density.

Theorem 4. *For very positive integer k, the asymptotic density of $\mathcal{N}_k$ is:*

$$\delta(\mathcal{N}_k) = \begin{cases} 3/4, & \text{if } k > 1 \text{ is odd;} \\ \prod\limits_{\substack{p^2-1\mid k \\ p\equiv 3 \pmod 4}} \dfrac{p^2 - p + 1}{p^2}, & \text{otherwise.} \end{cases}$$

Proof. For any non-empty finite family of primes $\mathcal{P}$, the system of congruences

$$\{x \equiv pr \pmod{p^2} : p \in \mathcal{P}\}$$

has solutions. An easy inductive argument shows that

$$\delta\left(\bigcap_{p\in\mathcal{P}} \mathbb{F}(p)\right) = \frac{\prod\limits_{p\in\mathcal{P}} p - 1}{\operatorname{lcm}\{p^2 : p \in \mathcal{P}\}} = \prod_{p\in\mathcal{P}} \frac{p-1}{p^2}.$$

Proposition 6 and the inclusion-exclusion principle lead to

$$\delta(\mathbb{N} \setminus \mathcal{N}_k) = 1 - \prod_{\substack{p^2-1 \mid k \\ p \equiv 3 \pmod 4}} (1 - \frac{p-1}{p^2})$$

and we are done. □

This result has the following somewhat remarkable consequence:

Corollary 2. *For every $\epsilon > 0$, there exists $k \in \mathbb{N}$ such that $\delta(\mathcal{N}_k) < \epsilon$.*

Proof. It is enough to observe that

$$\prod_{p \equiv 3 \pmod 4} \frac{p^2 - p + 1}{p^2} = 0.$$

□

Remark. Corollary 2 means that, despite great amount of zeros in Table 1, there are rows such that the density of zeros on them is as close to 0 as desired.

Proposition 8. *Let n be a positive integer. If $3 \mid n$ but $9 \nmid n$, then $8\mathbb{N} \subseteq \mathbb{N} \setminus \mathcal{K}_n$. If, in addition, $n \not\equiv 2 \pmod 4$, then $8\mathbb{N} = \mathbb{N} \setminus \mathcal{K}_n$.*

Proof. If $8 \mid k$, then $k \in \mathbb{G}(3)$. Hence, if $3 \mid n$ and $9 \nmid n$, Proposition 7 implies that $k \in \mathbb{N} \setminus \mathcal{K}_n$.

I we furthermore assume that $n \not\equiv 2 \pmod 4$, then Proposition 7 implies that, if $k \in \mathbb{N} \setminus \mathcal{K}_n$, then $p^2 - 1 \mid k$ for some $p \mid n$ such that $p \equiv 3 \pmod 4$. But in this case, $p^2 - 1 \equiv 0 \pmod 8$ and the proof is complete. □

5. On the congruence $\mathbf{G}_n(n) \equiv 0 \pmod n$}

We consider in this section the case $k = n$; i.e., we are concerned with those n such that $n \mid \mathbf{G}_n(n)$. In other words: the zeros in the diagonal of Table 1.

The following result is just a version of Corollary 1 when $k = n$.

Corollary 3. *Let $n > 1$ be an integer. Then, $\mathbf{G}_n(n) \not\equiv 0 \pmod n$ if and only if there exists a prime p such that:*

i) $p \equiv 3 \pmod 4$.
ii) $p^3 - p \mid n$.
iii) $p^2 \nmid n$.

As a consequence we obtain a result similar to Proposition 8:

Proposition 9. *Let n be a positive integer. If $\mathbf{G}_n(n) \not\equiv 0 \pmod n$, then $24 \mid n$.*

Proof. By Corollary 3, if $\mathbf{G}_n(n) \not\equiv 0 \pmod n$ then $n = hp(p+1)(p-1)$ for some prime $p \equiv 3 \pmod 4$, so that $8 \mid (p+1)(p-1)$. Moreover, one of -1, p or $p+1$ is a multiple of 3 and we are done. □

Define the following set:

$$\mathfrak{M} := \{n \in \mathbb{N} : \mathbf{G}_n(n) \equiv 0 \pmod n\}$$

The rest of the paper is devoted to computing the asymptotic density of $\mathfrak{M}$. Note that Proposition 9 implies that this density (if it exists) is, at least, $\frac{23}{24} = 0.958\overline{3}$. In

fact we show that it is quite close to this value computing $\delta(\mathfrak{M})$ up to five decimal places.

For a prime p, define the following set:

$$\mathfrak{U}_p := \{n \in \mathbb{Z} : p^3 - p \mid n, p^2 \nmid n\}.$$

Proposition 10. *The set $\mathfrak{M}$ satisfies the following conditions:*

i) $\mathbb{N} \setminus \mathfrak{M} = \bigcup_{\substack{p \text{ prime} \\ p\equiv 3 \pmod 4}} \mathfrak{U}_p$.

ii) *$\mathfrak{M}$ has an asymptotic density.*

Proof. The first assertion is a straightforward consequence of Corollary 3.
In order to prove ii), let $u_p = p^3 - p$ and observe that $u_p = \min(\mathfrak{U}_p)$. Then, $\mathfrak{U}_p = u_p\mathbb{Z} \setminus pu_p\mathbb{Z}$ and, consequently,

$$\delta(\mathfrak{U}_p) = \frac{1}{u_p} - \frac{1}{pu_p} = \frac{1}{p^2(1+p)}.$$

Since $\sum_p \delta(\mathfrak{U}_p) < \infty$, it follows that $\mathbb{N} \setminus \mathfrak{M}$ has an asymptotic density and so has $\mathfrak{M}$, as claimed. □

In order to compute bounds for the asymptotic density of $\mathfrak{M}$ (now we know it exists) we present a couple of technical lemmata.

Lemma 5. *Let $2 < q < p$ be two prime numbers and $0 < s < p$, $0 < t < q$ two integers. The Diophantic equation*

$$(p^3 - p)(Yp + s) = (q^3 - q)(Xq + t)$$

has a solution if and only if $q^2 \nmid p^2 - 1$.

Proof. Rewriting the equality as

$$Kp^2(p^2-1) + sp(p^2-1) = K'q^2(q^2-1) + tq(q^2-1)$$

and taking the gcd:

$$p^2 - 1 = m\bar{p}, \;\; q^2 - 1 = m\bar{q}$$

the original equation simplifies to

$$Kp^2\bar{p} + sp\bar{p} = K'q^2\bar{q} + tq\bar{q}.$$

There are three cases to consider, depending on $\gcd(\bar{p}, q^2)$ (notice that $2 < q$ implies $p \nmid \bar{q}$ because $p \nmid (q+1)(q-1)$).

- If $\gcd(\bar{p}, q^2) = 1$ then the same happens with $p^2\bar{p}$ and $q^2\bar{q}$, so that the equality is of the form

$$Kp_1 = K'p_2 + b \tag{2}$$

  for p_1 and p_2 coprime, which has an infinite number of solutions for any b.
- If $\gcd(\bar{p}, q^2) = q$ then one can divide by q both sides of the equation to get

$$Kp^2\tilde{p} + sp\tilde{p} = K'q\bar{q} + t\bar{q},$$

  with, again, $p^2\tilde{p}$ and $q\bar{q}$ coprime and we have another equation like (2).
- Finally, if $\gcd(\bar{p}, q^2) = q^2$ then, dividing both sides by q the equation becomes

$$Kp^2q\tilde{p} + spq\tilde{p} = K'q\bar{q} + t\bar{q},$$

  which has no solutions because $t < q$.

□

Lemma 6. *For p, s integers, define $\mathfrak{F}(p,s) := \{p(p-1)(p+1)(Kp+s) : K \in \mathbb{N}\}$. If $\mathcal{P}$ is a finite family of primes and $\{s_q\}_{q\in\mathcal{P}}$ satisfies $0 < s_q < q$, then:*

$$\delta\left(\bigcap_{q\in\mathcal{P}} \mathfrak{F}(q,s_q)\right) = \begin{cases} 0, & \text{if there exist } p,q \in \mathcal{P} \text{ with } p^2 \mid q^2-1; \\ \dfrac{1}{\operatorname{lcm}\{q^4-q^2 : q\in\mathcal{P}\}}, & \text{otherwise.} \end{cases}$$

Proof. If there exist $p, q \in \mathcal{P}$ with $p^2 \mid q^2-1$, Lemma 5 implies that $\mathfrak{F}(p,s_p)\bigcap\mathfrak{F}(q,s_q) = \emptyset$ and hence $\bigcap_{q\in\mathcal{P}}\mathfrak{F}(q,s_q) = \emptyset$.

In the other case, by the Chinese Remainder Theorem, the set of solutions of the system of simultaneous congruences given by:

$$\{x \equiv s_p(p^3-p) \pmod{p^4-p^2} : p \in \mathcal{P}\}$$

determines an arithmetic progression of difference $\operatorname{lcm}\{p^4-p^2 : p\in\mathcal{P}\}$. Consequently its asymptotic density is $1/\operatorname{lcm}\{q^4-q^2 : q\in\mathcal{P}\}$ as claimed. □

We return to the sets $\mathfrak{U}_p$ previously defined.

Proposition 11. *Let $\mathcal{P}$ be a finite family of primes. Then:*

$$\delta\left(\bigcap_{q\in\mathcal{P}} \mathfrak{U}_q\right) = \begin{cases} 0, & \text{if there are } p,q \in \mathcal{P} \text{ with } p^2 \mid q^2-1; \\ \dfrac{\prod_{q\in\mathcal{P}} q-1}{\operatorname{lcm}\{q^4-q^2 : q\in\mathcal{P}\}}, & \text{otherwise.} \end{cases}$$

Proof. By induction on the number of elements in $\mathcal{P}$ and using Lemma 6 it can be shown that the intersection $\bigcap_{q\in\mathcal{P}}\mathfrak{U}_q$ (when non-empty) is the union of $\prod_{q\in\mathcal{P}} q-1$ disjoint arithmetic progressions of difference $\operatorname{lcm}\{q^4-q^2 : q\in\mathcal{P}\}$. □

If $w(m)$ denotes the number of different prime factors of m, ϕ is the Euler totient function and defining

$$\vartheta(m) := \begin{cases} 0, & \text{if there exist } p,q \mid m \text{ such that } p^2 \mid q^2-1; \\ \dfrac{\phi(m)}{\operatorname{lcm}\{p^4-p^2 : p\mid m\}}, & \text{otherwise,} \end{cases}$$

then, the inclusion-exclusion principle together with the last Proposition let us state the following result:

Proposition 12. *Let $\mathcal{P}$ be a finite set of Gaussian primes and $\Theta := \prod_{p\in P}$, then:*

$$\delta\left(\bigcup_{p\in\mathcal{P}} \mathfrak{U}_p\right) = -\sum_{1<d\mid\Theta} (-1)^{w(d)}\vartheta(d)$$

These results allow us to approximate the asymptotic density of $\mathfrak{M}$ which is given by the following sum:

$$\delta(\mathfrak{M}) = \sum_{m\in\Upsilon} (-1)^{w(m)}\vartheta(m)$$

where Υ is the set of square-free integers whose prime factors are all Gaussian.

Theorem 5. *The asymptotic density of $\mathfrak{M}$ is* $0.971000\ldots$

Proof. Let $\mathcal{P}$ be the set of the first thirty Gaussian primes. Namely,

$$\mathcal{P} := \{p \text{ prime} : p \equiv 3 \pmod 4, p \leq 263\}.$$

Then:

$$\delta\left(\bigcup_{p\in\mathcal{P}} \mathfrak{U}_p\right) \leq \delta(\mathbb{N}\setminus\mathfrak{M}) \leq \delta\left(\bigcup_{p\in\mathcal{P}} \mathfrak{U}_p\right) + \sum_{\substack{p>263\\ p\equiv 3 \pmod 4}} \frac{1}{p^3+p^2}.$$

Applying the inclusion-exclusion principle, and taking into account Proposition 11, we have been able to compute, using PARI/GP:

$$\ell := \delta\left(\bigcup_{p\in\mathcal{P}} \mathfrak{U}_p\right) = \frac{52832172344...086951451}{1821843350513...659697280} = 0.0289992947691577872...$$

where the numerator has 117 digits and the denominator has 119. We know (see A085992 in the OEIS or [15]) that

$$\sum_{\substack{p \text{ prime}\\ p\equiv 3 \pmod 4}} \frac{1}{p^3} =: \Theta = 0.041007556566473031928886548851960025924 3\ldots$$

Moreover, if $\mathfrak{p} := 1299689$ is the 99999-th prime, then one can compute

$$\sum_{\substack{\mathfrak{p}<p \text{ prime}\\ p\equiv 3 \pmod 4}} \frac{1}{p^2+p^3} < \sum_{\substack{\mathfrak{p}<p \text{ prime}\\ p\equiv 3 \pmod 4}} \frac{1}{p^3} = \sum_{\substack{\mathfrak{p}\geq p \text{ prime}\\ p\equiv 3 \pmod 4}} \frac{-1}{p^3} + \Theta < 2\times 10^{-14},$$

$$\sum_{\substack{263<p\leq\mathfrak{p}\\ p\equiv 3 \pmod 4}} \frac{1}{p^3+p^2} < 5.3539\times 10^{-7},$$

Consequently:

$$0.0289992947 < \ell < \delta(\mathbb{N}\setminus\mathfrak{M}) < \ell + 5.354\times 10^{-7} < 0.0289998302,$$

and hence:

$$0.971000169 < \delta(\mathfrak{M}) < 0.97100071.$$

□

Remark. The computation of the asymptotic density of $\mathfrak{M}$ up to 6 decimal digits has required over 24 hours. Albeit the implementation does not use either parallelism or caching, the fact that the computational complexity of the problem is essentially $\mathcal{O}(2^n)$ (due to the underlying inclusion-exclusion principle), trying to get to the 57 Gaussian primes required for the next decimal digit has been seen by us as not not worth the effort, as we do not have access either to massively parallel hardware or large amounts of RAM.

6. Conclusions and future perspectives

We have started with this work an interesting new research area on the sum of powers on the ring $\mathbb{Z}[i]/n\mathbb{Z}[i]$. The formulas in Theorem 3 allow a fast computation of that sum from the Gaussian prime factors of n, in an analogue way as von Staudt's formula for $\mathbb{Z}_n$. There are also two areas of interest that this work opens before us:

6.1. **Sums of powers in more general rings.** A more general framework might be described as follows: given a finite ring $\mathcal{A}$, find a formula for the value of $\sum_{a\in\mathcal{A}} a^k$. Natural first steps might $\mathcal{A}$ being the ring of square matrices of a given order with coefficients in $\mathbb{Z}_n$ or the ring of Hamilton quaternions over $\mathbb{Z}_n$, $\mathbb{H}(\mathbb{Z}_n)$. However, these cases might prove too complicated due to their non-commutativity and the lack of results similar to those of Section 2. At the same time, conjectures are not easy to come up with, as computations soon become unfeasible for n a little large. As a matter of fact, we have found no pair (k,n) such that the sum of the $k-$th powers of the elements of $\mathbb{H}(\mathbb{Z}_n)$ be nonzero. On the other hand, the first numbers n for which the sum of of the n-th powers of all 2×2 matrices over $\mathbb{Z}/n\mathbb{Z}$ is non-zero are

$$6, 18, 30, 42, 54, 66, 78, 90, 102, 114, 126, 138, 150, 162, 174, 186, ...$$

All of them are of congruent with 6 (mod 12), but this is not something we would conjecture as a fact for all $n \in \mathbb{N}$.

6.2. **The *Erdős-Moser equation* in Gaussian stage.** We would like to finish this paper posing in the Gaussian context a topic related to power sums of integers as the *Erdős-Moser equation*, which is the Diophantine equation

$$S_k(m-1) = m^k. \tag{3}$$

In a 1950 letter to Moser, Erdős conjectured that solutions to this equation do not exist except for the trivial one $1^1 + 2^1 = 3^1$. Three years later, Moser [16] proved the conjecture for odd k or $m < 10^{10^6}$. Since then, much work on this equation has been carried out, but the conjecture has not been completely solved. For surveys of research on this and related problems, see [17, 18] and [19, Section D7].

For power sums of Gaussian integers, a reasonable analogue Diophantine equation could be

$$\mathbf{G}_k(m-1) = (m+mi)^k$$

for which, after performing computations for $k, m < 100$, we state the following

Conjecture 1. *The equation above has only the solution* $(k,m) = (2,3)$*:*

$$(1+i)^2 + (1+2i)^2 + (2+i)^2 + (2+2i)^2 = 18i = (3+3i)^2$$

References

[1] A. F. Beardon. Sums of powers of integers. *Amer. Math. Monthly*, 103(3):201–213, 1996.

[2] L. Carlitz. The Staudt-Clausen theorem. *Math. Mag.*, 34:131–146, 1960-1961.

[3] J. M. Grau, P. Moree and A. M. Oller-Marcén. About the congruence $\sum_{k=1}^{n} k^{f(n)} \equiv 0 \pmod{n}$. Preprint, 2013, http://arxiv.org/abs/1304.2678.

[4] B.C. Kellner. On the theorems of Von Staudt and Clausen. in preparation

[5] T. Lengyel. On divisibility of some power sums. *Integers*, 7:A41, 6, 2007.

[6] K. MacMillan and J. Sondow. Divisibility of power sums and the generalized Erdős-Moser equation. *Elem. Math.*, 67(4):182–186, 2012.

[7] P. Moree. On a theorem of Carlitz-von Staudt. *C. R. Math. Rep. Acad. Sci. Canada*, 16(4):166–170, 1994.

[8] N. J. A. Sloane. The On-Line Encyclopedia of Integer Sequences. https://oeis.org.

[9] J. Sondow and K. MacMillan. Reducing the Erdős-Moser equation $1^n+2^n+\cdots+k^n = (k+1)^n$ modulo k and k^2. Preprint, 2010, http://arxiv.org/abs/1011.2154.

[10] J. Sondow and K. MacMillan. Reducing the Erdős-Moser equation $1^n+2^n+\cdots+k^n = (k+1)^n$ modulo k and k^2. *Integers*, 11:A34, 8, 2011.

[11] K. G. C. von Staudt. Beweis eines Lehrsatzes die Bernoullischen Zahlen betreffend. *J. Reine Angew. Math*, 21:372–374, 1840.

[12] K. Dilcher, Congruences for a class of alternating lacunary sums of binomial coeficients, J. Integer Seq. 10 (2007) Article 07.10.1.
[13] Ch. Hermite, Extrait d'une lettre a M. Borchardt J. Reine Angew. Math. 81 (1876) 93-95.
[14] P. Bachmann, Niedere Zahlentheorie. Part 2, Teubner, Leipzig, 1910; Parts 1 and 2 reprinted in one volume, Chelsea, New York, 1968.
[15] R. J. Mathar. Table of Dirichlet L-Series and Prime Zeta Modulo Functions for Small Moduli. arXiv:1008.2547 2010.
[16] L. Moser. On the Diophantine equation $1^n + 2^n + 3^n + \cdots + (m-1)^n = m^n$. *Scripta Math.*, 19:84–88, 1953.
[17] W. Butske, L. M. Jaje, and D. R. Mayernik. On the equation $\sum_{P|N} \frac{1}{P} + \frac{1}{N} = 1$, pseudoperfect numbers, and perfectly weighted graphs. *Math. Comp*, 69:407–420, 2000.
[18] P. Moree. Moser's mathemagical work on the equation $1^k + 2^k + \ldots + (m-1)^k = m^k$. *Rocky Mountain J. Math.*, no. 5 (2013), 1707-1737.
[19] R. Guy. *Unsolved problems in number theory*. 2nd ed. Springer, New York, 2004.
[20] H.J. Schultz. The sums of the kth powers of the first n integers Amer. Math. Monthly 87 (1980), 478–481.
[21] C. B. Boyer. Pascal's formula for the sums of powers of the integers. Scripta Math. 9 (1943), 237-244.

Departamento de Matemáticas, Universidad de Oviedo, Avda. Calvo Sotelo s/n, 33007 Oviedo, Spain
E-mail address: fortunypedro@uniovi.es

Departamento de Matemáticas, Universidad de Oviedo, Avda. Calvo Sotelo s/n, 33007 Oviedo, Spain
E-mail address: grau@uniovi.es

Centro Universitario de la Defensa de Zaragoza, Ctra. Huesca s/n, 50090 Zaragoza, Spain
E-mail address: oller@unizar.es