Title: Gauss Congruences in Algebraic Number Fields

Author: Paweł Gładki , Mateusz Pulikowski

Citation style: Gładki Paweł, Pulikowski Mateusz. (2022). Gauss Congruences in Algebraic Number Fields. „Annales Mathematicae Silesianae” (08 Jan 2022), DOI: 10.2478/amsil-2022-0002

Annales Mathematicae Silesianae (2022),
DOI: 10.2478/amsil-2022-0002

GAUSS CONGRUENCES IN ALGEBRAIC NUMBER FIELDS

Paweł Gładki, Mateusz Pulikowski

Abstract. In this miniature note we generalize the classical Gauss congruences for integers to rings of integers in algebraic number fields.

Recall that the classical Gauss congruence for integers states that, for $a \in \mathbb{Z}$ and $n \in \mathbb{N}$, the following identity holds true:

$$\sum_{d|n} \mu\left(\frac{n}{d}\right) a^d \equiv 0 \pmod{n},$$

where $\mu\colon \mathbb{N} \to \{-1, 0, 1\}$ is the Möbius function defined by

$$\mu(n) = \begin{cases} 1, & \text{if } n = 1, \\ (-1)^m, & \text{if } n \text{ is a product of } m \text{ different primes}, \\ 0, & \text{otherwise.} \end{cases}$$

The abovestated identity generalizes in a surprisingly easy and natural way to rings of integers in algebraic function fields.

Let K be an algebraic number field and denote by $\mathcal{O}_K$ its ring of integers. Denote by $\mathcal{I}(\mathcal{O}_K)$ the family of all ideals of $\mathcal{O}_K$ and by $\operatorname{Spec} \mathcal{O}_K$ its prime

Received: 22.09.2021.Accepted: 08.01.2022.
(2020) Mathematics Subject Classification: 12F05, 12J15.
Key words and phrases: Gauss congruences, algebraic number fields.

spectrum. Further, denote by $N\colon \mathcal{I}(\mathcal{O}_K) \to \mathbb{N}$ the absolute norm function defined by the size of the (necessarily finite) quotient ring:

$$N(\mathfrak{n}) = |\mathcal{O}_K/\mathfrak{n}|.$$

Here and later on, for $a, b \in \mathcal{O}_K$ and $\mathfrak{n} \in \mathcal{I}(\mathcal{O}_K)$, by $a \equiv b (\operatorname{mod} \mathfrak{n})$ we shall understand $a - b \in \mathfrak{n}$.

As $\mathcal{O}_K$ is a Dedeking domain, every nonzero ideal $\mathfrak{n}$ of $\mathcal{O}_K$ can be uniquely represented as a product of prime ideals of $\mathcal{O}_K$, so that one can consider the following generalization of the Möbius fuction, which is due to Shapiro ([1]):

$$\mu(\mathfrak{n}) = \begin{cases} 1, & \text{if } \mathfrak{n} = 0, \\ (-1)^m, & \text{if } \mathfrak{n} \text{ is a product of } m \text{ different prime ideals,} \\ 0, & \text{otherwise.} \end{cases}$$

With this definition of the function $\mu\colon \mathcal{I}(\mathcal{O}_K) \to \{-1, 0, 1\}$, we shall prove the following version of the Gauss identity for number fields:

Theorem 1. *Let $a \in \mathcal{O}_K$, $\mathfrak{n} \in \mathcal{I}(\mathcal{O}_K)$. Then*

$$\sum_{\mathfrak{d}|\mathfrak{n}} \mu\left(\frac{\mathfrak{n}}{\mathfrak{d}}\right) a^{N(\mathfrak{d})} \equiv 0 \ (\operatorname{mod} \mathfrak{n}).$$

For the proof we will use a version of Euler's Theorem for number fields. We shall state it here together with a proof for the sake of the completeness of our exposition, however there is no claim to its originality whatsoever.

Proposition 2 (Euler's Theorem). *Let $a \in \mathcal{O}_K$, $\mathfrak{p} \in \operatorname{Spec} \mathcal{O}_K$ and $k \in \mathbb{N}$. Then*

$$a^{N(\mathfrak{p})^k} \equiv a^{N(\mathfrak{p})^{k-1}} \ (\operatorname{mod} \mathfrak{p}^k).$$

Proof. One needs to evaluate the number of units in the ring $\mathcal{O}_K/\mathfrak{p}^k$. The canonical map $\mathcal{O}_K/\mathfrak{p}^k \to \mathcal{O}_K/\mathfrak{p}$ given by $x + \mathfrak{p}^k \mapsto x + \mathfrak{p}$ is a well-defined ring homomorphism whose kernel is equal to $\mathfrak{p}/\mathfrak{p}^k$. As $\mathcal{O}_K$ is a Dedekind domain, the prime ideal $\mathfrak{p}$ is also maximal and hence $\mathcal{O}_K/\mathfrak{p}$ is a field, so that the ideal $\mathfrak{p}/\mathfrak{p}^k$ is maximal. Since $\sqrt{\mathfrak{p}^k} = \sqrt{\mathfrak{p}} = \mathfrak{p}$ is a maximal ideal, $\mathcal{O}_K/\mathfrak{p}^k$ is local, and thus $\mathfrak{p}/\mathfrak{p}^k$ is equal precisely to the set of non-units of $\mathcal{O}_K/\mathfrak{p}^k$. Considering the chain of additive Abelian groups $\mathfrak{p}^k \subseteq \mathfrak{p}^{k-1} \subseteq \ldots \mathfrak{p}^2 \subseteq \mathfrak{p}$ and using the isomorphism theorem combined with the Lagrange theorem, we get

$$|\mathfrak{p}/\mathfrak{p}^k| = (\mathfrak{p} : \mathfrak{p}^2) \cdot (\mathfrak{p}^2 : \mathfrak{p}^3) \cdot \ldots \cdot (\mathfrak{p}^{k-1} : \mathfrak{p}^k).$$

Each quotient group $\mathfrak{p}^i/\mathfrak{p}^{i+1}$, $i \in \{1, \ldots, k-1\}$, has a structure of a $\mathcal{O}_K/\mathfrak{p}$-vector space, and its dimension is equal to 1. Indeed, let $x \in \mathfrak{p}^i \setminus \mathfrak{p}^{i+1}$ and $\mathfrak{a} = (x) + \mathfrak{p}^{i+1}$. Then $\mathfrak{p}^i \supseteq \mathfrak{a} \supsetneq \mathfrak{p}^{i+1}$, and, consequently, $\mathfrak{a} = \mathfrak{p}^i$, for otherwise $\frac{\mathfrak{a}}{\mathfrak{p}^i}$ would be a proper divisor of $\mathfrak{p} = \frac{\mathfrak{p}^{i+1}}{\mathfrak{p}^i}$. Hence $x + \mathfrak{p}^{i+1}$ is a basis of the $\mathcal{O}_K/\mathfrak{p}$-vector space $\mathfrak{p}^i/\mathfrak{p}^{i+1}$.

Therefore the number of units of the ring $\mathcal{O}_K/\mathfrak{p}^k$ is equal to:

$$|\mathcal{O}_K/\mathfrak{p}^k| - |\mathfrak{p}/\mathfrak{p}^k| = N(\mathfrak{p}^k) - |\mathcal{O}_K/\mathfrak{p}|^{k-1} = N(\mathfrak{p}^k) - N(\mathfrak{p})^{k-1}.$$

As the absolute norm is multiplicative, $N(\mathfrak{p}^k) = N(\mathfrak{p})^k$ and hence

$$(a + \mathfrak{p}^k)^{N(\mathfrak{p})^k - N(\mathfrak{p})^{k-1}} = a^{N(\mathfrak{p})^k - N(\mathfrak{p})^{k-1}} + \mathfrak{p}^k = 1 + \mathfrak{p}^k,$$

or, equivalently, $a^{N(\mathfrak{p})^k} \equiv a^{N(\mathfrak{p})^{k-1}} (\operatorname{mod} \mathfrak{p}^k)$. □

We can now proceed to the proof of Theorem 1:

PROOF. Fix $a \in \mathcal{O}_K$ and $\mathfrak{n} \in \mathcal{I}(\mathcal{O}_K)$. Let $\mathfrak{n} = \mathfrak{p}_1^{k_1} \cdot \ldots \cdot \mathfrak{p}_m^{k_m}$ be the unique factorization of $\mathfrak{n}$ into a product of prime ideals. By the definition of the function μ, the set of divisors of $\mathfrak{n}$ whose value of μ is nonzero is equal to:

$$\{\mathfrak{p}_{j_1} \cdot \ldots \cdot \mathfrak{p}_{j_l} \mid 1 \leqslant j_1 < \ldots < j_l \leqslant m, l \in \{0, \ldots, m\}\},$$

where by product of 0 ideals we understand the zero ideal 0. Thus

$$\begin{aligned}
\sum_{\mathfrak{d}|\mathfrak{n}} \mu\left(\frac{\mathfrak{n}}{\mathfrak{d}}\right) a^{N(\mathfrak{d})} &= \sum_{l=0}^{m} \sum_{1 \leqslant j_1 < \ldots < j_l \leqslant m} (-1)^l a^{N\left(\frac{\mathfrak{p}_1^{k_1} \cdot \ldots \cdot \mathfrak{p}_m^{k_m}}{\mathfrak{p}_{j_1} \cdot \ldots \cdot \mathfrak{p}_{j_l}}\right)} \\
&= \sum_{l=0}^{m} \sum_{1 \leqslant j_1 < \ldots < j_l \leqslant m} (-1)^l a^{\frac{N(\mathfrak{p}_1)^{k_1} \cdot \ldots \cdot N(\mathfrak{p}_m)^{k_m}}{N(\mathfrak{p}_{j_1}) \cdot \ldots \cdot N(\mathfrak{p}_{j_l})}} \\
&= \sum_{l=0}^{m-1} \sum_{2 \leqslant j_1 < \ldots < j_l \leqslant m} \Bigg[(-1)^l a^{N(\mathfrak{p}_1)^{k_1} \frac{N(\mathfrak{p}_2)^{k_2} \cdot \ldots \cdot N(\mathfrak{p}_m)^{k_m}}{N(\mathfrak{p}_{j_1}) \cdot \ldots \cdot N(\mathfrak{p}_{j_l})}} \\
&\quad - (-1)^l a^{N(\mathfrak{p}_1)^{k_1 - 1} \frac{N(\mathfrak{p}_2)^{k_2} \cdot \ldots \cdot N(\mathfrak{p}_m)^{k_m}}{N(\mathfrak{p}_{j_1}) \cdot \ldots \cdot N(\mathfrak{p}_{j_l})}} \Bigg].
\end{aligned}$$

By Proposition 2, $a^{N(\mathfrak{p}_1)^{k_1}} \equiv a^{N(\mathfrak{p}_1)^{k_1-1}} (\operatorname{mod} \mathfrak{p}_1^{k_1})$. Consequently,

$$(-1)^l a^{N(\mathfrak{p}_1)^{k_1} \frac{N(\mathfrak{p}_2)^{k_2}\cdot\ldots\cdot N(\mathfrak{p}_m)^{k_m}}{N(\mathfrak{p}_{j_1})\cdot\ldots\cdot N(\mathfrak{p}_{j_l})}} \equiv (-1)^l a^{N(\mathfrak{p}_1)^{k_1-1} \frac{N(\mathfrak{p}_2)^{k_2}\cdot\ldots\cdot N(\mathfrak{p}_m)^{k_m}}{N(\mathfrak{p}_{j_1})\cdot\ldots\cdot N(\mathfrak{p}_{j_l})}} (\operatorname{mod} \mathfrak{p}_1^{k_1}),$$

for $2 \leqslant j_1 < \ldots < j_l \leqslant m$, $l \in \{0, \ldots, m-1\}$, and hence

$$\sum_{\mathfrak{d}|\mathfrak{n}} \mu\left(\frac{\mathfrak{n}}{\mathfrak{d}}\right) a^{N(\mathfrak{d})} \equiv 0 \ (\operatorname{mod} \mathfrak{p}_1^{k_1}).$$

Repeating the argument for the ideals $\mathfrak{p}_2, \ldots, \mathfrak{p}_m$ we get

$$\sum_{\mathfrak{d}|\mathfrak{n}} \mu\left(\frac{\mathfrak{n}}{\mathfrak{d}}\right) a^{N(\mathfrak{d})} \equiv 0 \ (\operatorname{mod} \mathfrak{p}_i^{k_i}),$$

for $i \in \{1, \ldots, m\}$, so that

$$\sum_{\mathfrak{d}|\mathfrak{n}} \mu\left(\frac{\mathfrak{n}}{\mathfrak{d}}\right) a^{N(\mathfrak{d})} \equiv 0 \ (\operatorname{mod} \mathfrak{n}). \qquad \square$$

Remark 3. We note that taking $K = \mathbb{Q}$ with $\mathcal{O}_K = \mathbb{Z}$ Theorem 1 yields the classical version of the Gauss congruence.

References

[1] H.N. Shapiro, *An elementary proof of the prime ideal theorem*, Comm. Pure Appl. Math. **2** (1949), 309–323.

Institute of Mathematics
University of Silesia in Katowice
Bankowa 14
40-007 Katowice
Poland
e-mail: pawel.gladki@us.edu.pl
e-mail: mateusz.pulikowski@us.edu.pl