

**Zeitschrift:** L'Enseignement Mathématique  
**Herausgeber:** Commission Internationale de l'Enseignement Mathématique  
**Band:** 36 (1990)  
**Heft:** 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

**Artikel:** GAUSS SUMS AND THEIR PRIME FACTORIZATION  
**Autor:** Brinkhuis, Jan  
**Kapitel:** 5. The prime factorization of the Gauss sum: proof of the result  
**DOI:** <https://doi.org/10.5169/seals-57901>

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften auf E-Periodica. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. Das Veröffentlichen von Bildern in Print- und Online-Publikationen sowie auf Social Media-Kanälen oder Webseiten ist nur mit vorheriger Genehmigung der Rechteinhaber erlaubt. [Mehr erfahren](#)

### **Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. La reproduction d'images dans des publications imprimées ou en ligne ainsi que sur des canaux de médias sociaux ou des sites web n'est autorisée qu'avec l'accord préalable des détenteurs des droits. [En savoir plus](#)

### **Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. Publishing images in print and online publications, as well as on social media channels or websites, is only permitted with the prior consent of the rights holders. [Find out more](#)

**Download PDF:** 06.03.2026

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

“sometimes” there is, once one has determined  $v(\alpha) \bmod e_0$ , a relatively easy method to determine moreover  $v(\alpha)$  itself. It would take us too far to give a formal account of this method, so in this matter we will restrict ourselves to the special case of Gauss sums.

(4.6) For general insight it is of interest to know how  $e_0$  depends on  $\gamma$ . We will give the answer under the assumptions that the residual characteristic of  $v$  is a prime number, say  $l$ , and that  $\gamma$  has finite order, say  $e$ . For each  $n \in \mathbf{N}$  we can write  $n = l^r n'$  with  $r \in \mathbf{N} \cup \{0\}$ ,  $n' \in \mathbf{N}$  and  $l \nmid n'$ ; then we call  $n'$  the  $l$ -free part of  $n$ . Now we give the desired result.

(4.7) The number  $e_0$  is the  $l$ -free part of  $e$ .

We omit the proof of this fact, as we will not make use of it: in our application it will be obvious what  $e_0$  is, once we have computed the class of  $\pi^{\gamma-1}$  in  $F(v)$  which is something that we have to do anyway.

## 5. THE PRIME FACTORIZATION OF THE GAUSS SUM: PROOF OF THE RESULT

Now we are ready to prove theorem (3.3). We will do this by proving the statements in (3.4).

*Proof of (3.4).* By proposition (1.2) (i), (iii) and (iv) only primes of  $\mathbf{Q}(pm)$  above  $p$  can occur in the prime factorization of  $G$ . Let  $i \in \mathbf{Z}$  with  $0 < i < m$  and  $(i, m) = 1$ . We have to determine the integer  $k_i$  defined by (3.1). We are first going to determine  $k_i$  modulo  $p-1$  by using lemma (4.3). We apply this lemma to  $F = \mathbf{Q}(pm)$ ,  $v = v_{\mathfrak{P}}$ ,  $\alpha = G^{\tau_i}$ ,  $\pi = \zeta_p - 1$  and  $\gamma = \sigma_g$  where  $g \in \mathbf{Z}$  with  $0 < g < p$  is such that  $g \pmod{p}$  generates  $(\mathbf{Z}/p\mathbf{Z})^* = \mathbf{F}_p^*$ ; then  $k = k_i$  and the residue class field  $F(v)$  is  $\mathbf{F}_p$ . This choice satisfies the requirements of the lemma as  $\sigma_g$  lies in  $\text{Gal}(\mathbf{Q}(p)/\mathbf{Q})$  which is the inertia group of  $\mathfrak{P}$  in the extension  $\mathbf{Q}(pm)/\mathbf{Q}$ . Now let us calculate the left and right hand side of the equality  $l(\rho(\alpha)) = (0, z^k)$  which holds by lemma (4.3). On the one hand  $\rho(\alpha) = G^{\tau_i(\sigma_g^{-1})}$  which is by proposition (1.2) (ii) equal to

$$\chi(\bar{g})^{\tau_i} = \chi(\bar{g})^i \quad \text{where} \quad \bar{g} = g \bmod p$$

and this is by (2.1) congruent to  $g^{\frac{p-1}{m}i} \bmod \mathfrak{P}$ . Therefore

$$l(\rho(\alpha)) = (0, \bar{g}^{\frac{p-1}{m}i}).$$

On the other hand,

$$z = (\zeta_p - 1)^{\sigma_g^{-1}} = \sum_{i=0}^{g-1} \zeta_p^i$$

which is congruent to  $g \pmod{\mathfrak{P}}$  and so  $(0, z^k) = (0, \bar{g}^{k_i})$ . Therefore the equality  $l(\rho(\alpha)) = (0, z^k)$  amounts here to the following congruence

$$g^{\frac{p-1}{m}i} \equiv g^{k_i} \pmod{p}$$

that is, by the choice of  $g$ ,

$$k_i \equiv \frac{p-1}{m}i \pmod{p-1}.$$

Thus  $k_i$  has been determined modulo  $p-1$ . In fact one may replace in (5.4) the congruence sign by the equality sign as on the one hand clearly  $0 < \frac{p-1}{m}i < p-1$  and on the other hand by proposition (1.2) (iii) and (iv) one has  $0 \leq k_i \leq v_{\mathfrak{P}}(p) = p-1$ . Therefore one gets

$$k_i = \frac{p-1}{m}i,$$

This finishes the proof of the theorem.

## 6. ANNIHILATORS OF THE IDEAL CLASS GROUP OF A CYCLOTOMIC FIELD

In this section we give an account of the annihilation of the ideal class group of a cyclotomic field by the Stickelberger ideal. For each commutative ring  $R$  with unit element, each  $R$ -module  $M$  and each  $\lambda \in R$ , one says that  $\lambda$  annihilates  $M$  or that  $\lambda$  is an annihilator of  $M$  if  $\lambda r = 0$  for all  $r \in M$ ; the set  $\text{Ann}_R M$  of all annihilators of an  $R$ -module  $M$  clearly forms an ideal in the ring  $R$ .

Let  $m > 1$ . The structure of  $Cl_{\mathbf{Q}(m)}$ , the ideal class group of the cyclotomic field  $\mathbf{Q}(m)$ , and the action of the Galois group  $\Gamma = \text{Gal}(\mathbf{Q}(m)/\mathbf{Q})$  on it, are of great interest. Information on this structure is contained in  $\text{Ann}_{Z\Gamma} Cl_{\mathbf{Q}(m)}$ .