

## On the $l$ -Adic Expansion of Certain Gauss Sums and Its Applications\*)

Hiroo Miki

### Introduction

In the present paper, we shall give a new explicit formula on the  $l$ -adic expansion (mod  $\pi^l$ ) of certain Gauss sums (see Theorem 1 in Section 1).

Let  $p$  be any prime number and let  $m > 1$  be a natural number which is not divisible by  $p$ . Let  $\zeta_m$  be a primitive  $m$ -th root of unity in the field of complex numbers  $C$ . Let  $Q$  be the field of rational numbers and let  $Z$  be the ring of rational integers. Fix a prime ideal  $\mathfrak{p}$  of  $Q(\zeta_m)$  lying above  $p$  and put  $N\mathfrak{p} = q$ , where  $N\mathfrak{p}$  is the absolute norm of  $\mathfrak{p}$ . Note that  $m | (q-1)$ . Let  $F_q$  be the finite field of  $q$  elements. Let

$$\chi_{\mathfrak{p}}(x \bmod \mathfrak{p}) = \left( \frac{x}{\mathfrak{p}} \right)_m$$

be the  $m$ -th power residue symbol in  $Q(\zeta_m)$ , i.e.,

$$\chi_{\mathfrak{p}}(x \bmod \mathfrak{p}) \equiv x^{(q-1)/m} \pmod{\mathfrak{p}}$$

for  $x \in Z[\zeta_m]$ .  $\chi_{\mathfrak{p}}$  induces a homomorphism of the multiplicative group  $F_q^\times$  of  $F_q$  to  $C^\times$  of order  $m$  and  $\chi_{\mathfrak{p}}(0) = 0$ . Here we identify  $F_q$  and  $Z[\zeta_m]/\mathfrak{p}$ . Let  $T$  be the trace of  $F_q$  to  $F_p$  and put

$$\psi(x) = \zeta_p^{T(x)}$$

for  $x \in F_q$ . Then  $\psi$  is a homomorphism of the additive group  $F_q$  to the multiplicative group  $C^\times$ .

**Definition.** For each  $a \in Z$ , put

---

Received May 29, 1986.

\*) This is the details of my lecture in Symp. on Algebraic Number Theory, October 1985 at the Research Institute for Mathematical Sciences Kyoto Univ., which is a revised and extended version of my intensive lectures at Kanazawa Univ. and Tokyo Institute of Technology in Jan.-Feb. 1985. I also gave my intensive lecture related to this subject at Kyushu Univ. in Dec. 1985 and at Nagoya Univ. in July 1986.