Michigan Math. J. 50 (2002)

On Gaussian Periods That Are Rational Integers

F. Thaine

1. Preliminaries

Let $p \geq 3$ be a prime number, ζ_p a pth primitive root of 1, and Δ the Galois group of $\mathbb{Q}(\zeta_p)/\mathbb{Q}$. Let $q \neq p$ be a prime number, ζ_q a qth primitive root of 1, and n the order of q modulo p. Assume that $q \not\equiv 1 \bmod p$. Hence $n \geq 2$, $p(q-1) \mid q^n - 1$, and $n \mid p-1$. Set $f = (q^n - 1)/p$ and $e = (p-1)/n$. Let Q be a prime ideal of $\mathbb{Z}[\zeta_p]$ above q and let $\mathbb{F} = \mathbb{Z}[\zeta_p]/Q$. Thus $\mathbb{F} \simeq \mathbb{F}_{q^n}$, the finite field with q^n elements. Let $\alpha \in \mathbb{Z}[\zeta_p]$ be a generator of $\mathbb{F}^\times$ such that $\alpha^f \equiv \zeta_p \bmod Q$, and let T be the trace from $\mathbb{F}$ to $\mathbb{F}_q$. In this paper we study the Gaussian periods η_i $(0 \leq i \leq p-1)$ defined by

$$\eta_i = \sum_{j=0}^{f-1} \zeta_q^{T(\alpha^{i+pj})}, \tag{1}$$

as well as the Gauss sum

$$G = \sum_{i=0}^{q^n-2} \zeta_p^i \zeta_q^{T(\alpha^i)} = \sum_{i=0}^{p-1} \eta_i \zeta_p^i. \tag{2}$$

Some basic definitions and results are given in this section. A short review of the cyclotomic numbers of order e corresponding to p is given in Section 2. Those numbers will play an important role in Section 4. In Section 3 we show applications of the periods η_i to the study of indices of cyclotomic units in $\mathbb{Z}[\zeta_p]$ (with respect to Q and α) and of the orders of certain components of the ideal class group of $\mathbb{Q}(\zeta_p)$. More precisely, let A be the p-part of the ideal class group of $\mathbb{Q}(\zeta_p)$, $\mathbb{Z}_p$ the ring of p-adic integers, and $\omega\colon \Delta \to \mathbb{Z}_p^\times$ the Teichmüller character; in Section 3 we study the ω^{p-ln}-components of A for n and l odd, $1 \leq l \leq e-1$ (see the definitions in Section 3). In Section 4 we show an efficient method to calculate the periods η_i, based on the Gross–Koblitz formula and on properties of the cyclotomic numbers of order e corresponding to p; in Section 5 we give a MAPLE program to perform such calculations. I am grateful to Hershy Kisilevsky and John McKay for some valuable comments.

We start with a simple proof of the known result (see [6, Thm. 4]) that, under the stated hypothesis, the η_i are rational integers and so $G \in \mathbb{Z}[\zeta_p]$. In fact, G belongs to the only subfield of degree e of $\mathbb{Q}(\zeta_p)$ and is divisible by a (sometimes large) power of q.

Received March 15, 2001. Revision received December 17, 2001.

This work was supported in part by grants from NSERC and FCAR.