PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 100, Number 2, June 1987

SOME ARITHMETIC PROPERTIES OF THE MINIMAL POLYNOMIALS OF GAUSS SUMS

WAN DAQING

ABSTRACT. For the minimal polynomial $f(x) = x^k + b_1 x^{k-1} + \cdots + b_k$ of $\sum_{n=0}^{p-1} \exp(2\pi i n^k/p)$ over Q, where p is a prime $\equiv 1 \pmod{k}$, we evaluate b_1, b_2 and prove $p|b_i$ $(i = 1, \ldots, k)$ but $p^2 \nmid b_j$ $(j = 2, k)$. Also, we raise the interesting conjecture that $p^2 \nmid b_j$ for $k \geq j \geq 2$.

1. Introduction. Define the Gauss sum $G(k,p) = G(k)$ by

$$G(k) = \sum_n \exp\left(\frac{2\pi i n^k}{p}\right),$$

where k is a prime with $p \equiv 1 \pmod{k}$, and $\sum_n$ indicates that the sum on n is over an arbitrary complete residue system $(\bmod p)$. The Gauss sums and their minimal polynomials have been extensively studied (see the survey article [1]).

For $k = 2$, the minimal polynomial of $G(2)$ is

$$f_2(x) = x^2 - (-1)^{(p-1)/2} p.$$

For $k = 3$, in his monumental Disquistiones Arthmeticae, Gauss [5] exhibited the minimal polynomial $f_3(x)$ of $G(3)$,

$$f_3(x) = x^3 - 3px - pr,$$

where $4p = r^2 + 27t^2$, $r \equiv 1 \pmod 3$.

For $k = 4$, Gauss, Legendre, Lebesgue, Caley, Sylvester, Scott, Pellet, and Carey determined the minimal polynomial $f_4(x)$ of $G(4)$. Using the formula of $G(4)$ in [1], we can easily obtain $f_4(x)$,

$$f_4(x) = x^4 - 2p\left(1 + 2\left(\frac{2}{p}\right)\right)x^2 + 8pax + p\left[p\left(5 - 4\left(\frac{2}{p}\right)\right) - 4a^2\right],$$

where $p = a^2 + b^2$, $a \equiv -1 \pmod 4$.

With the increase of k, the formula for $f_k(x)$ becomes increasingly complicated. Here we only give the historical background on the topic. For $k = 5$, Legendre, Carey, Scott, Tanner, Carey, Clashan, and Burnside determined the minimal polynomial $f_5(x)$ of $G(5)$. For $k = 6$, the minimal polynomial of $G(6)$ was first exhibited by Smith in 1880 with no proof. A proof was given somewhat later by Carey, also by D. H. and E. Lehmer [3] in 1984. For $k = 8$, the minimal polynomial of $G(8)$ was recently obtained by R. J. Evans [4]. For $k = 12, 16$ and 24, the minimal polynomial $f_k(x)$ can also be obtained by using the formulae of the corresponding Gauss sums, but they would be very troublesome.

Received by the editors Decembr 14, 1985 and, in revised form, April 16, 1986.
1980 *Mathematics Subject Classification* (1985 *Revision*). Primary 15G05.

In this paper, along another direction we investigate arithmetic properties of the minimal polynomial $f_k(x)$ for arbitrary k. As well, we give an interesting conjecture concerning the coefficients, which might lead to new research topics on Gauss sums.

2. Main result. In this section, we prove the following divisible properties of the coefficients of the minimal polynomial $f_k(x)$.

THEOREM. *Let the minimal polynomial of $G(k)$ over Q be*

$$f_k(x) = x^k + b_1 x^{k-1} + \cdots + b_k.$$

Then

(1) $b_1 = 0$, $b_2 = (k/2)p$ *or* $(k/2)p(1-k)$ *according as* $\chi(-1) = 1$ *or not, where* χ *is the multiplicative character of* F_p^* *with order* k.

(2) $p|b_i$ $(i = 1, \ldots, k)$, $p^2 \nmid b_j$ $(j = 2, k)$.

PROOF. Let χ be a multiplicative character of F_p^* with order k; define

$$G_a = G_a(k) = \sum_n \exp\left(\frac{2\pi i a n^k}{p}\right), \qquad a \neq 0.$$

It is obvious that $G_a = G_b$ if $\chi(a) = \chi(b)$, also $G_a \in Z[\xi_p]$, where $\xi_p = e^{2\pi i/p}$. For given $a, b \in F_p^*$, there exists an element σ of $\mathrm{Gal}(Q(\xi_p)/Q)$ such that $\sigma(G_a) = G_b$. Let g be a primitive root of F_p^*, then we have

$$\begin{array}{llll} G_1 & = G_{g^k} & = G_{g^{2k}} & = \cdots \\ G_g & = G_{g\cdot g^k} & = g_{g\cdot g^{2k}} & = \cdots \\ \vdots & & & \\ G_{g^{k-1}} & = G_{g^{k-1}\cdot g^k} & = G_{g^{k-1}\cdot g^{2k}} & = \cdots . \end{array}$$

Thus, we have proved that any root of the minimal polynomial $f_k(x)$ of $G(k) = G_1$ is among $\{G_1, G_g, \ldots, G_{g^{k-1}}\}$.

Let $F(x) = \prod_{i=0}^{k-1}(x - G_{g^i}) = x^k + b_1 x^{k-1} + \cdots + b_k$; by Galois theory we know that $F(x) \in Z[x]$. We now prove that $F(x) = f_k(x)$ and $f_k(x)$ has the desired properties.

Let N_s denote the number of solutions of congruence

$$x_1^k + x_2^k + \cdots + x_s^k \equiv 0 \pmod{p}, \qquad s \geq 1. \tag{1}$$

Then

$$\begin{aligned} H_s &\triangleq \sum_{i=0}^{k-1} G_{g^i}^s = \frac{k}{p-1}\sum_{a=1}^{p-1} G_a^s \\ &= \frac{k}{p-1}\sum_{x_1=0}^{p-1}\cdots\sum_{x_s=0}^{p-1}\sum_{a=1}^{p-1}\exp\left(\frac{2\pi i(x_1^k + \cdots + x_s^k)a}{p\cdot}\right) \\ &= \frac{k}{p-1}\{(p-1)N_s - (p^s - N_s)\} = \frac{k}{p-1}(pN_s - p^2) \equiv 0 \pmod{p}. \end{aligned} \tag{2}$$

By Newton's formulae, we have

$$
\begin{aligned}
0 &= H_1 + b_1, \\
0 &= H_2 + b_1 H_1 + 2b_2, \\
0 &= H_3 + b_1 H_2 + b_2 H_1 + 3b_3, \\
&\vdots \\
0 &= H_k + b_1 H_{k-1} + \cdots + b_{k-1} H_1 + k b_k.
\end{aligned} \tag{3}
$$

(2) and (3) together imply

$$
\begin{aligned}
b_1 &\equiv 0 \pmod{p}, \\
b_2 &\equiv 0 \pmod{p}, \\
&\vdots \\
b_k &\equiv 0 \pmod{p},
\end{aligned}
$$

that is, $p|b_i$ $(i = 1, \ldots, k)$.

Since $N_1 = 1$, (2) gives $H_1 = 0$ and (3) gives $b_1 = 0$. From $H_2 + b_1 H_1 + 2b_2 = 0$, and $b_1 = 0$, we obtain

$$
\begin{aligned}
b_2 &= -\frac{1}{2} H_2 = -\frac{1}{2} \frac{k}{p-1} (pN_2 - p^2), \\
N_2 &= N(x^k + y^k \equiv 0 \pmod{p}) \\
&= 1 + (p-1)(1 + \chi(-1) + \cdots + \chi^{k-1}(-1)) \\
&= p + (p-1)(\chi(-1) + \cdots + \chi^{k-1}(-1)),
\end{aligned}
$$

$$
\begin{aligned}
b_2 &= -\frac{1}{2} \frac{k}{p-1} p(p-1)(\chi(-1) + \cdots + \chi^{k-1}(-1)) \\
&= \begin{cases} \frac{k}{2} p, & \text{if } \chi(-1) \neq 1, \\ \frac{k}{2} p(1-k), & \text{if } \chi(-1) = 1. \end{cases}
\end{aligned} \tag{4}
$$

Next, we show $p^2 \nmid b_k$. From (2) and $0 = H_k + b_1 H_{k-1} + \cdots + b_{k-1} H_1 + k b_k$, we deduce

$$
p^2 \nmid b_k \Leftrightarrow p^2 \nmid H_k \Leftrightarrow p \nmid N_k.
$$

Now,

$$
\begin{aligned}
N_k &= N(x_1^k + \cdots + x_k^k \equiv 0 \pmod{p}) \\
&\equiv \sum_{x_1, \ldots, x_{k-1}} \sum_{i=0}^{k-1} (-x_1^k - \cdots - x_{k-1}^k)^{(p-1)i/k} \pmod{p}.
\end{aligned} \tag{5}
$$

We notice that

$$
\sum_{x_i \bmod p} x_1^{u_1} \cdots x_{k-1}^{u_{k-1}} \equiv 0 \pmod{p} \quad \text{if some } u_i < p-1.
$$

Expanding (5)

$$N_k \equiv \sum_{x_1,\ldots,x_{k-1}} (-x_1^k - \cdots - x_{k-1}^k)^{(p-1)(k-1)/k}$$

$$\equiv \sum_{x_1,\ldots,x_{k-1}} (-1)^{(p-1)(k-1)/k} \begin{pmatrix} \dfrac{p-1}{k}(k-1) \\ \dfrac{p-1}{k} \quad \dfrac{p-1}{k} \quad \cdots \quad \dfrac{p-1}{k} \end{pmatrix} x_1^{p-1} \cdots x_{k-1}^{p-1}$$

$$\equiv (-1)^{k-1} \cdot (-1)^{(p-1)/k} \begin{pmatrix} \dfrac{p-1}{k}(k-1) \\ \dfrac{p-1}{k} \quad \dfrac{p-1}{k} \quad \cdots \quad \dfrac{p-1}{k} \end{pmatrix} \not\equiv 0 \pmod{p}.$$

Therefore, $p^2 \nmid b_k$. By the Eisenstein criteria, we deduce that $F(x)$ is an irreducible polynomial over Q, $F(x) = f_k(x)$, and $f_k(x)$ has the desired properties.

The theorem is completely proved.

3. Further discussion. The above theorem shows that $f_k(x)$ is p-Eisensteinian. Observing the formulae in §1 and the known formulae for $f_k(x)$, we find the remarkable possibility that $p^2 \nmid b_j$ $(j = 2, \ldots, k)$. Thus, we give the following

CONJECTURE. *Let $f_k(x) = x^k + b_1 x^{k-1} + \cdots + b_k$ be the minimal polynomial of $G(k)$ over Q; then $p^2 \nmid b_j$ for $j = 2, \ldots, k$.*

Our theorem shows that the conjecture is valid for $j = 2$ and k.

REMARK. According to the referee, arithmetic in $Q(\exp(2\pi i/p^k))$ can be used to delve more deeply, also the result $p|b_i$ $(i = 1, \ldots, k)$ was generalized by D. H. and E. Lehmer [**2**, p. 106].

REFERENCES

1. D. C. Berdt and R. J. Evans, *The determination of Gauss sums*, Bull. Amer. Math. Soc. (N.S.) **5** (1981), 107–121.
2. D. H. Lehmer and E. Lehmer, *The cyclotomy of hyper-Kloosterman sums*, Acta Arith. **14** (1968), 89–111.
3. ——, *The sextic period polynomial*, Pacific J. Math. **111** (1984), 341–355.
4. R. J. Evans, *The octic period polynomial*, Proc. Amer. Math. Soc. **87** (1983), 380–393.
5. C. F. Gauss, *Disquisitiones arithmeticae*, Yale Univ. Press, New Haven, Conn., 1966.

DEPARTMENT OF MATHEMATICS, SICHUAN UNIVERSITY, CHENGDU, SICHUAN, PEOPLE'S REPUBLIC OF CHINA

Current address: Department of Mathematics, University of Washington, Seattle, Washington 98195