Honam Mathematical J. **20**(1998), No. 1,pp. 21–29

ON THE IRREDUCIBLE QUINTIC POLYNOMIAL OVER THE RATIONAL NUMBER FIELD

DALL-SUN YOON AND SHIN-CHUL HWANG

Dept. of Mathematics, Hanyang University, Seoul 133-791, Korea.

1. Introduction

For an odd prime p , let χ be a multiplicative character of the Galois field F_p of order p where $p = 5f + 1$ (f ; even) and let the order of χ be 5. Define Jacobi sum $J(\chi^i)$, $i = 1, 2, 3, 4$, by

$$J(\chi^i) = \sum_{c=0}^{p-1} \chi^i(c)\chi^i(1-c) = \sum_{c=0}^{p-1} \chi^i\Big(c(1-c)\Big). \tag{1.1}$$

Let g be a primitive element of F_p, β a primitive fifth root of unity and $[k, h]$ the number of sets of values of t and z, each chosen from $0, 1, \cdots, f-1$, for which the congruence relation

$$1 + g^{et+k} \equiv g^{ez+h} \pmod{p}, \quad 0 \le h \le 4, \quad 0 \le z \le f-1,$$

holds where we consider h (as well as k) fixed.

In 1935, Dickson [2, p396] express the Jacobi sum $J(\chi^i)$ using β and $[k, h]$, that is,

$$J(\chi^i) = 2\sum_{k=1}^{2} \beta^{ik} \sum_{h=0}^{4} \beta^{-2ik}[k, h] + \sum_{h=0}^{4} \beta^{-2ik}[0, h] \tag{1.2}$$

Received March 2, 1998.

The first author was supported by Faculty Research Grant of Hanyang University, 1998.

and show the property

$$J(\chi)J(\chi^4) = J(\chi^2)J(\chi^3) = p. \tag{1.3}$$

And, he [2, p402] show that

$$4J(\chi) = x + 5w\sqrt{5} + vi\sqrt{50 - 10\sqrt{5}} + ui\sqrt{50 + 10\sqrt{5}} \tag{1.4}$$

where x, w, u and v are integers such that

$$16p = x^2 + 125w^2 + 50v^2 + 50u^2, \quad xw = v^2 - u^2 - 4uv \tag{1.5}$$

and $x \equiv 1 (\mathrm{mod}\, 5)$ and a solution (x, w, v, u) to (1.5) is "essentially unique" in that there is a simple prescription for obtaining the other solutions from it.

Using Dickson's method, we can obtain the Jacobi sums $J(\chi^i)$, $i = 2, 3, 4$, as following :

$$\begin{aligned} 4J(\chi^2) =& x - 5w\sqrt{5} - ui\sqrt{50 - 10\sqrt{5}} + vi\sqrt{50 + 10\sqrt{5}} \\ 4J(\chi^3) =& x - 5w\sqrt{5} + ui\sqrt{50 - 10\sqrt{5}} - vi\sqrt{50 + 10\sqrt{5}} \\ 4J(\chi^4) =& x + 5w\sqrt{5} - vi\sqrt{50 - 10\sqrt{5}} - ui\sqrt{50 + 10\sqrt{5}}. \end{aligned} \tag{1.6}$$

In this paper, we present the irreducible quintic polynomial of Gauss sum G_5 over the rational number field using the Jacobi sums $J(\chi^i)$, $i = 1, 2, 3, 4$.

2. Preliminaries

Let us recall some definitions and properties, which are necessary for development of the paper.

Let χ be a multiplicative character of F_p, where p is a odd prime such that $p = 5f + 1$, (f ; even). Define two kinds of Gauss sums $G(\chi^i)$ and G_5 of order 5

$$G(\chi^i) = \sum_{c=1}^{p-1} \chi^i(c) e^{2\pi ic/p} \tag{2.1}$$

and

$$G_5 = \sum_{c=1}^{p-1} e^{2\pi i c^5/p}. \tag{2.2}$$

Both of them are intimately linked by the equality [1, p107].

$$G_5 = \sum_{i=1}^{4} G(\chi^i). \tag{2.3}$$

It is easily verified by direct multiplication that

$$G(\chi)G(\chi^4) = G(\chi^2)G(\chi^3) = p. \tag{2.4}$$

There is a very important relation between Jacobi sums and Gauss sums [4, p207]

$$J(\chi^i) = \frac{G^2(\chi^i)}{G(\chi^{2i})}. \tag{2.5}$$

Some combination of Jacobi sums $J(\chi^i)$, $i = 1, 2, 3, 4$ can be evaluated in terms of the parameters x, w, u and v in (1.5);

$$\begin{aligned} J(\chi) + J(\chi^4) &= \frac{1}{2}(x + 5w\sqrt{5}) \\ J(\chi^2) + J(\chi^3) &= \frac{1}{2}(x - 5w\sqrt{5}) \\ \sum_{i=1}^{4} J(\chi^i) &= x. \end{aligned} \tag{2.6}$$

Let t_1 be the real part of $J(\chi)J(\chi^2)$ and let t_2 be the real part of $J(\chi)J(\chi^3)$. Since $J(\chi)J(\chi^2)$ and $J(\chi^4)J(\chi^3)$ is complex conjugate and so is $J(\chi)J(\chi^3)$ and $J(\chi^4)J(\chi^2)$,

$$\begin{aligned} J(\chi)J(\chi^2) + J(\chi^4)J(\chi^3) &= 2t_1, \\ J(\chi)J(\chi^3) + J(\chi^4)J(\chi^2) &= 2t_2. \end{aligned} \tag{2.7}$$

By (1.3) and (2.7), we get four relations of Jacobi sums in terms of t_1, t_2 and p,

$$
\begin{aligned}
J^2(\chi)J(\chi^2) &= 2t_1J(\chi) - pJ(\chi^3),\\
J^2(\chi^2)J(\chi^4) &= 2t_2J(\chi^2) - pJ(\chi),\\
J^2(\chi^3)J(\chi) &= 2t_2J(\chi^3) - pJ(\chi^4),\\
J^2(\chi^4)J(\chi^3) &= 2t_1J(\chi^4) - pJ(\chi^2).
\end{aligned} \tag{2.8}
$$

Then, we get the following relation by addition both sides of (2.8), respectively, and using (2.6)

$$
\begin{aligned}
\sum_{i=1}^{4} J^2(\chi^i)J(\chi^{2i}) &= 2t_1\{J(\chi) + J(\chi^4)\} + 2t_2\{J(\chi^2) + J(\chi^3)\}\\
&\quad - p\{J(\chi) + J(\chi^2) + J(\chi^3) + J(\chi^4)\}\\
&= t_1(x + 5w\sqrt{5}) + t_2(x - 5w\sqrt{5}) - px.
\end{aligned}
$$

From (1.4), (1.5) and (1.6), we get the values of t_1 and t_2:

$$
\begin{aligned}
t_1 &= \frac{1}{16}\Big\{x^2 - 125w^2 - 20\sqrt{5}(v^2 - u^2 + uv)\Big\},\\
t_2 &= \frac{1}{16}\Big\{x^2 - 125w^2 + 20\sqrt{5}(v^2 - u^2 + uv)\Big\}.
\end{aligned}
$$

Hence we get the values of $\sum_{i=1}^{4} J^2(\chi^i)J(\chi^{2i})$, that is,

$$
\sum_{i=1}^{4} J^2(\chi^i)J(\chi^{2i}) = \frac{1}{8}\Big\{x^3 - 625(v^2 - u^2)w\Big\} - px. \tag{2.9}
$$

By (2.1) and (2.2), we get

$$
\{J(\chi) + J(\chi^4)\}\{J(\chi^2) + J(\chi^3)\} = \frac{1}{4}(x^2 - 125w^2). \tag{2.10}
$$

3. The Irreducible Polynomial of G_5

Using (1.3), (2.4), (2.5), (4,6), (2.9) and (2.10). Some combinations of Gauss sums $G(\chi^i)$, $i = 1, 2, 3, 4$ can be evaluated in terms of parameters x, w, u, v and p in (1.5).

LEMMA 1.

$$G^5(\chi^i) = pJ^2(\chi^i)J(\chi^{2i})$$

for $i = 1, 2, 3, 4$.

Proof. By (2, 5) and (2, 4),

$$\begin{aligned} J^2(\chi^i)J(\chi^{2i}) &= \frac{G^4(\chi^i)}{G^2(\chi^{2i})}\,\frac{G^2(\chi^{2i})}{G(\chi^{4i})} \\ &= \frac{G^5(\chi^i)}{G(\chi^{4i})G(\chi^i)}. \end{aligned} \tag{3.1}$$

Since $G(\chi^{4i})G(\chi^i) = p$, then

$$G^5(\chi^i) = pJ^2(\chi^i)J(\chi^{2i}).$$

THEOREM 2.

$$\sum_{i=1}^{4} G^5(\chi^i) = \frac{p}{8}\Big\{x^3 - 625(v^2 - u^2)w - 8px\Big\}.$$

Proof. By (2.9) and Lemma 1, it is true.

LEMMA 3.

$$\sum_{i=1}^{4} G^2(\chi^i)G(\chi^{3i}) = px.$$

Proof. By (2.5) and (2.6)

$$\begin{aligned} J(\chi) + J(\chi^4) &= \frac{G^2(\chi)}{G(\chi^2)} + \frac{G^2(\chi^4)}{G(\chi^3)} \\ &= \frac{G^2(\chi)G(\chi^3) + G^2(\chi^4)G(\chi^2)}{p}. \end{aligned}$$

From (2.6), we have

$$G^2(\chi)G(\chi^3) + G^2(\chi^4)G(\chi^2) = \frac{p}{2}(x + 5w\sqrt{5}). \tag{3.2}$$

$$G^2(\chi^2)G(\chi) + G^2(\chi^3)G(\chi^4) = \frac{p}{2}(x - 5w\sqrt{5}). \tag{3.3}$$

Therefore,

$$\sum_{i=1}^{4} G^2(\chi^i)G(\chi^{2i}) = px.$$

LEMMA 4.

$$\sum_{i=1}^{4} G^3(\chi^i)G(\chi^{2i}) = \frac{p}{4}(x^2 - 125w^2).$$

Proof. Producing both sides of (3.1) and (3.2), respectively, and using (2.6), we have

$$p\sum_{i=1}^{4} G^3(\chi^i)G(\chi^{2i}) = \frac{p^2}{4}(x^2 - 125w^2). \tag{3.4}$$

Hence,

$$\sum_{i=1}^{4} G^3(\chi^i)G(\chi^{2i}) = \frac{p}{4}(x^2 - 125w^2).$$

To obtain the irreducible polynomial of G_5 over the rational number field, We replace G_5 by $\sum_{i=1}^{4} G(\chi^i)$ and expand the fifth

power of $\sum_{i=1}^{4} G(\chi^i)$,

$$
\begin{aligned}
G_5^5 &= \Big(\sum_{i=1}^{4} G(\chi^i)\Big)^5 \\
&= \sum_{i=1}^{4} G^5(\chi^i) + 5\sum_{i=1}^{4} G^4(\chi^i)G(\chi^{2i}) + 5\sum_{i=1}^{4} G^4(\chi^i)G(\chi^{3i}) \\
&\quad + 10\sum_{i=1}^{4} G^3(\chi^i)G^2(\chi^{2i}) + 10\sum_{i=1}^{4} G^3(\chi^i)G^2(\chi^{3i}) \\
&\quad + 25p\sum_{i=1}^{4} G^3(\chi^i) + 50p\sum_{i=1}^{4} G^2(\chi^i)G(\chi^{2i}) \\
&\quad + 50p\sum_{i=1}^{4} G^2(\chi^i)G(\chi^{3i}) + 100p^2\sum_{i=1}^{4} G(\chi^i).
\end{aligned}
$$

In above equation, if we consider p as second degree, all terms of last part of above relation are five degree of $G(\chi^i)$, $i = 1, 2, 3, 4$. So, we make the relations in Lemma 3 and 4 to five degree by producting G_5^2 and G_5, respectively, and p by G_5^3

$$
\begin{aligned}
pxG_5^2 &= \Big\{\sum_{i=1}^{4} G^2(\chi^i)G(\chi^{3i})\Big\}\Big\{\sum_{i=1}^{4} G(\chi^i)\Big\}^2 \\
&= \sum_{i=1}^{4} G^4(\chi^i)G(\chi^{3i}) + \sum_{i=1}^{4} G^3(\chi^i)G^2(\chi^{2i}) \\
&\quad + 2\sum_{i=1}^{4} G^3(\chi^i)G^2(\chi^{3i}) + 2p\sum_{i=1}^{4} G^3(\chi^i) \\
&\quad + 4p\sum_{i=1}^{4} G^2(\chi^i)G(\chi^{3i}) + 3p\sum_{i=1}^{4} G^2(\chi^i)G(\chi^{2i}) \\
&\quad + 3p^2\sum_{i=1}^{4} G^2(\chi^i).
\end{aligned} \tag{3.5}
$$

(3.6)

$$\frac{p^2}{4}(x^2-125w^2)G_5 = \Big\{\sum_{i=1}^{4} G^3(\chi^i)G(\chi^{2i})\Big\}\Big\{\sum_{i=1}^{4} G(\chi^i)\Big\}$$
$$= \sum_{i=1}^{4} G^4(\chi^i)G(\chi^{2i}) + \sum_{i=1}^{4} G^3(\chi^i)G^2(\chi^{2i})$$
$$+ p\sum_{i=1}^{4} G^3(\chi^i) + p\sum_{i=1}^{4} G^2(\chi^i)G(\chi^{2i}).$$

and

$$pG_5^3 = p\Big\{\sum_{i=1}^{4} G(\chi^i)\Big\}^3$$

(3.7)
$$= p\sum_{i=1}^{4} G^3(\chi^i) + 3p\sum_{i=1}^{4} G^2(\chi^i)G(\chi^{2i})$$
$$+ 3p\sum_{i=1}^{4} G^2(\chi^i)G(\chi^{3i}) + 9p^2\sum_{i=1}^{4} G(\chi^i).$$

THEOREM 5. *Let x, w, u and v be integers satisfying the relation (1.5) and let p be an odd prime such that $p = 5f+1$ (f ; even). The irreducible polynomial of G_5 over the rational number field is*

$$p(z) = z^5 - 10pz^2 + \frac{5}{4}p(4p - x^2 + 125w^2)z$$
$$+ \frac{p}{8}\{8px - x^3 + 625w(v^2-u^2)\}.$$

Proof. Using (3.4), (3.5), (3.6), (3.7) and Theorem 2

$$G_5^5 = \sum_{i=1}^{4} G^5(\chi^i) + 10pG_5^3 + 5pxG_5^2 + \frac{5}{4}p^2(x^2-125w^2)G_5 - 5p^2G_5$$
$$= 10pG_5^3 + 5pxG_5^2 + \frac{5}{4}p^2(x^2-125w^2)G_5 - 5p^2G_5$$
$$+ \frac{p}{8}\{x^3 - 625(v^2-u^2)w - 8px\}$$

So, the irreducible polynomial of G_5 is

$$p(z) = z^5 - 10pz^3 - 5pxz^2 + \frac{5}{4}(4p^2 - x^2 + 125w^2)z + \frac{p}{8}\{8px - x^3 + 625w(v^2 - u^2)\}.$$

References

1. B. C. Berndt and R. J. Evans, *The Determination of Gauss sums*,, Bull. Amer. Math. Soci. **5** (1981), 107–129.
2. L. E. Dickson, *Cyclotomy, higher congruences, and Waring's problem*, Amer. J. Math. **57** (1935), 391–424.
3. E. Lehmer, *The quintic character of 2 and 3*, Duke Math. J. **18** (1951), 11–18.
4. L. Lidl and H. Niederreiter, *Finite fields, Encyclopedia Math. Appl. 20*, Cambridge University Press,, Cambridge, 1987.