THE EXAMPLE BY STEPHENS

KAORU MOTOSE

Abstract. Concerning the Feit-Thompson Conjecture, Stephens found the serious example. Using Artin map (see [9]), we shall show that numbers 17 and 3313 in the example by Stephen are common index divisors of some subfields of a cyclotomic field $\mathbb{Q}(\zeta_r)$ where $r = 112643$ and $\zeta_r = e^{\frac{2\pi i}{r}}$, and some results in [7, 8] shall be again proved.

Key Words: Artin map, common index divisors, Gauss sums.
2000 *Mathematics Subject Classification*: Primary 11A15, 11R04; Secondary 20D05.

Let $p < q$ be primes and we set

$$f := \frac{q^p - 1}{q - 1} \text{ and } t := \frac{p^q - 1}{p - 1}.$$

Feit and Thompson [3] conjectured that f never divides t. If it would be proved, the proof of their odd order theorem [4] would be greatly simplified (see [1] and [5]).

Throughout this note, we assume that *r is a common prime divisor of f and t.* Using computer, Stephens [10] found the example about r as follows: for $p = 17$ and $q = 3313$, $r = 112643 = 2pq + 1$ is the greatest common divisor of f and t. This example is so far the only one.

In this note, using the Artin map, we shall show that both 17 and 3313 are common index divisors (gemeinsamer ausserwesentlicher Discriminantenteiler) of some subfields of a cyclotomic field $\mathbb{Q}(\zeta_r)$ where $r = 112643$ and $\zeta_r = e^{\frac{2\pi i}{r}}$, and some results in [7, 8] shall be again proved from our Theorem.

The assumption on r yields from [7, Lemma, (1) and (3)] that p and q are orders of q mod r and p mod r, respectively. Thus $r \equiv 1 \bmod 2pq$ since r is odd.

We set $q^*q := r - 1$ and $\zeta = e^{\frac{2\pi i}{r}}$. Let n be a divisor of q^*, let L_n be a subfield of $K = \mathbb{Q}(\zeta)$ with $[L_n : \mathbb{Q}] = n$ and let $\mathbb{O}_n$ be the algebraic integer ring of L_n. Using the exact sequence by the Artin map (see [9, p.99 and section 2.16]) and Kummer's theorem.

We have $d(\mu) = I(\mu)^2 d(L_n)$ for $\mu \in \mathbb{O}_n$ where $I(\mu) \in \mathbb{Z}$, $d(\mu)$ and $d(L_n)$ are discriminants of μ and of the field L_n, respectively.

The example by Stephens shows from the next Theorem that $p = 17$ and $q = 3313$ are common index divisors of L_{34} and of L_{6626}, respectively, since we can exchange p for q.

The detailed version of this paper will be submitted for publication elsewhere.

Theorem. *Assume r is a common prime divisor of f and t, and n is a divisor of q^*, where $q^*q = r-1$. Then p splits completely in $\mathbb{O}_n$ and if there exists $\mu \in \mathbb{O}_n$ such that p does not divide $I(\mu)$, then $n \leqq p$. In particular, for $n > p$, p is a common index divisor of $\mathbb{O}_n$ namely, p divides $I(\gamma)$ for all $\gamma \in \mathbb{O}_n$.*

Let c be a primitive root for r, let χ be a character of order n defined by $\chi(c) = \omega$ where $\omega = e^{\frac{2\pi i}{n}}$ and let $g(\chi) = \sum_{a\in\mathbb{F}_r} \chi(a)\zeta^a$ be the Gauss sum of χ where $\mathbb{F}_r$ is a finite field of order r. Let $\sigma(\zeta) = \zeta^c$ be a generator of the Galois group G of K over $\mathbb{Q}$ and set $T_n := \langle \sigma^n \rangle$.

For simplicity, we set $g_0 = -1$, $g_k = g(\chi^k)$ for $n > k > 0$ and $\theta_k = \theta^{\sigma^k}$ for $n > k \geqq 0$ where $\theta = \sum_{\tau\in T_n} \zeta^\tau$ is a trace of ζ.

It is known that $L_n = \mathbb{Q}(\theta)$ and θ is a normal basis element of $\mathbb{O}_n$ over $\mathbb{Z}$ (see [9, p.61, p.74])

The next Lemma is useful to our object. It only needs to assume r is prime and n is a divisor of $r-1$ in this Lemma. This proof is essentially in the first equation of (1) due to [9, p.62]. This idea of classifying primitive roots goes back to Gauss; the regular 17 polygon construction by ruler and compass.

Lemma.

(1) *$g_k = \sum_{s=0}^{n-1} \omega^{ks}\theta_s$ for $0 \leqq k < n$ and $n\theta_k = \sum_{s=0}^{n-1} \bar{\omega}^{ks} g_s$ for $0 \leqq k < n$ where $\bar{\omega}$ is the complex conjugate of ω.*

(2) *Using (1), determinants of cyclic matrices A_n, B_n are given by*

$$|A_n| := \begin{vmatrix} \theta_0 & \theta_1 & \dots & \theta_{n-1} \\ \theta_{n-1} & \theta_0 & \dots & \theta_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ \theta_1 & \theta_2 & \dots & \theta_0 \end{vmatrix} = \prod_{k=0}^{n-1} g_k \quad \text{and} \quad |B_n| := \begin{vmatrix} g_0 & g_1 & \cdots & g_{n-1} \\ g_{n-1} & g_0 & \cdots & g_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ g_1 & g_2 & \cdots & g_0 \end{vmatrix} = n^n \prod_{k=0}^{n-1} \theta_k.$$

(3) *We have*

$$d(L_n) = \begin{cases} r^{n-1} & \text{if } n \text{ is odd,} \\ (-1)^{\frac{r-1}{2}} r^{n-1} & \text{if } n \text{ is even.} \end{cases}$$

Some results in [7, 8] are proved again in the next

Corollary. *Let r be a common prime divisor of f and t. Then we have*
(1) *$p \equiv 1$ or $r \equiv 1 \bmod 4$* (see [7, Lemma, (4)]).
(2) *$q \equiv -1 \bmod 9$ in case $p = 3$ and f divides t* (see [8, Corollary, (a)]).

Proof of (2). We consider the case $n = p = 3$. If f is composite, then f does not divide t. Thus we may assume f is prime and so $r = f$ (see [7]). f has a primary prime decomposition $f = \eta\bar{\eta}$ in $\mathbb{Z}[\omega]$ where $\omega = e^{\frac{2\pi i}{3}}$ and $\eta = \omega(\omega - q)$, (see [6, 8]). In this case, we set χ is the cubic residue character modulo η. Let $h(x)$ be the minimal polynomial of θ over $\mathbb{Q}$.

$$h(x) := x^3 + a_1x^2 + a_2x + a_3 = (x - \theta_0)(x - \theta_1)(x - \theta_2).$$

where $a_1 = -\theta_0 - \theta_1 - \theta_2 = 1$. If 3 does not divide $I(\theta)$, then $h(x) \equiv x^3 - x \bmod 3$ by Kummer's theorem and our Theorem. This contradicts to $a_1 = 1$. Thus $d(\theta) \equiv 0 \bmod 3$. Using $g_1g_2 = g_1\bar{g_1} = |g_1|^2 = r$, we have

$$f = r = -|A_3| = -(\theta_0 + \theta_1 + \theta_2)\begin{vmatrix} 1 & \theta_1 & \theta_2 \\ 1 & \theta_0 & \theta_1 \\ 1 & \theta_2 & \theta_0 \end{vmatrix} = \theta_0^2 + \theta_1^2 + \theta_2^2 - a_2 = 1 - 3a_2.$$

Thus we obtain $3a_2 = 1 - f = -q(q + 1)$. On the other hand, using $g_2 = \bar{g_1},\ f = \eta\bar{\eta}$ and the Stickelberger relation $g_1^3 = r\eta = f\eta$ (see [6]), we have

$$\begin{aligned} -27a_3 &= 27\theta_0\theta_1\theta_2 = |B_3| = \begin{vmatrix} g_0 & g_1 & g_2 \\ g_2 & g_0 & g_1 \\ g_1 & g_2 & g_0 \end{vmatrix} = g_0^3 + g_1^3 + g_2^3 - 3g_0g_1g_2 \\ &= -1 + f(\eta + \bar{\eta}) + 3f = -1 + f(q - 1) + 3f = (q + 1)^3. \end{aligned}$$

Thus we have $3^3q^3a_3 = (-q(q + 1))^3 = 3^3a_2^3$ and so $a_2 + a_3 \equiv a_2^3 - q^3a_3 = 0 \bmod 3$. Noting $h'(\theta) \equiv a_2 - \theta \bmod 3$ where $h'(x)$ is the derivation of $h(x)$, we obtain

$$0 \equiv -d(\theta) = N_{L_3/\mathbb{Q}}(h'(\theta)) \equiv h(a_2) \equiv a_2 - a_2^2 + a_3 \equiv -a_2^2 \bmod 3.$$

Thus we have $0 \equiv 3a_2 = -q(q + 1) \bmod 9$. □

Remark. Using only the quadratic reciprocity law, we can prove

$$q \equiv -1 \bmod 8 \text{ in case } p = 3 \text{ and } f \text{ divides } t.$$

It simplifies the proof of Proposition 3.2 by Lemma 3.3 on p.172 in the paper
K. Dilcher and J. Knauer, *On a conjecture of Feit and Thompson,* pp.169-178 in the book, *High primes and misdemeanours,* edited by A. van der Poorten, A. Stein, Fields Institute Communications **41**, Amer. Math. Soc., 2004.

We can understand their proof through the next some results in this order :

- Ex. 11 on p.231, and p.103 in the book, B. C. Berndt, R.J. Evans, K. S. Williams, *Gauss and Jacobi Sums,* Wiley, New York, 1998.
- Proof of Theorem 2 on p.139 in the paper, R. Hudson and K. S. Williams, *Some new residuacity criteria,* Pacific J. of Math. **91**(1980), 135-143.
- The tables for the cyclotomic numbers of order 6 and p.68 in the paper, A. L. Whiteman, *The cyclotomic numbers of order twelve,* Acta. Arithmetica **6** (1960), 53-76.

References

[1] Apostol, T. M., *The resultant of the cyclotomic polynomials $F_m(ax)$ and $F_n(bx)$*, Math. Comput. **29** (1975), 1-6.

[2] Artin, E., *Theory of algebraic numbers*, notes by Gerhard Würges, Göttingen, Germany (1956).

[3] Feit, W. and Thompson, J. G., *A solvability criterion for finite groups and some consequences*, Proc. Nat. Acad. Sci. USA **48** (1962), 968-970.

[4] Feit, W. and Thompson, J. G.,*Solvability of groups of odd order*, Pacific J. Math. **13** (1963), 775-1029.

[5] Guy, R. K., *Unsolved problems in number theory*, Springer, 3rd ed., 2004.

[6] Ireland, K. and Rosen, M., *A classical introduction to modern number theory.* Springer, 2nd ed., 1990.

[7] Motose, K., *Notes to the Feit-Thompson conjecture*, Proc. Japan, Acad., ser A, **85**(2009), 16-17.

[8] Motose, K., *Notes to the Feit-Thompson conjecture. II*, Proc. Japan, Acad., ser A, **86**(2010), 131-132.

[9] Ono, T., *An introduction to algebraic number theory*, Plenum Press 1990 (a translation of Suron Josetsu, Shokabo, 2nd ed., 1988).

[10] Stephens, N. M., *On the Feit-Thompson conjecture*, Math. Comput. **25** (1971), 625.

Emeritus Professor, Hirosaki University
Toriage 5-13-5, Hirosaki, 036-8171, JAPAN
E-mail address: moka.mocha_no_kaori@snow.ocn.ne.jp