The example by Stephens

Dedicated to the memory of Professor Goro Azumaya

By Kaoru MOTOSE[†)]

Emeritus Professor, Hirosaki University

(Communicated by Masaki KASHIWARA, M.J.A., Feb. 13, 2012)

Abstract: Concerning the Feit-Thompson conjecture, Stephens found an example for primes 17 and 3313. In this paper, using the Artin map, these primes are common index divisors of subfields of a cyclotomic field, and some results in [7,8] shall be again proved.

Key words: Odd order theorem; Artin map; common index divisor.

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 paper, 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 paper, 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 $\mathbf{Q}(\zeta_r)$ where $r = 112643$ and $\zeta_r = e^{\frac{2\pi i}{r}}$, and some results in [7,8] shall be again proved.

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 and $r \equiv 1 \bmod 2pq$.

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 $K = \mathbf{Q}(\zeta)$ with $[L_n : \mathbf{Q}] = n$ and let $\mathbf{O}_n$ be the algebraic integer ring of L_n. The next exact sequence using the Artin map α follows from [9, p. 99 and section 2.16] where $\alpha = \alpha_{L_n/\mathbf{Q}}$ and $\alpha(s) = (\frac{L_n/\mathbf{Q}}{s})$ (the Artin symbol, see [9, p. 96]).

$$1 \longrightarrow H_n(r) \longrightarrow I_{\mathbf{Q}}(r) \xrightarrow{\alpha} G_n \longrightarrow 1$$

where G_n is the Galois group of L_n over $\mathbf{Q}$, $I_{\mathbf{Q}}(r)$ is the fractional ideal group of $\mathbf{Q}$ prime to r, namely,

$$I_{\mathbf{Q}}(r) := \left\{ \frac{s}{t} \;\middle|\; 0 < s, t \in \mathbf{Z}, (st, r) = 1 \right\} \text{ and}$$

$$H_n(r) := \left\{ \frac{s}{t} \in I_{\mathbf{Q}}(r) \;\middle|\; s \equiv tx^n \bmod r,\ x \in \mathbf{Z} \right\}.$$

We have $d(\mu) = I(\mu)^2 d(L_n)$ for $\mu \in \mathbf{O}_n$ where $I(\mu) \in \mathbf{Z}$, $d(\mu)$ 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, because we can exchange p for q.

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* $\mathbf{O}_n$ *and if there exists* $\mu \in \mathbf{O}_n$ *such that* p *does not divide* $I(\mu)$*, then* $n \leqq p$*.*

In particular, for $n > p$*,* p *is a common index divisor of* $\mathbf{O}_n$ *namely,* p *divides* $I(\gamma)$ *for all* $\gamma \in \mathbf{O}_n$*.*

Proof. First we show p splits completely in $\mathbf{O}_n$.

It is well known that $x^{q^*} \equiv p \bmod r$ is solvable in $\mathbf{Z}$ from $p^q \equiv 1 \bmod r$ (see [6, p. 45]). Thus $p \in H_n(r)$ and $\alpha(p) = 1$. Hence $\nu = \nu^{\alpha(p)} \equiv \nu^p \bmod P$ for all $\nu \in \mathbf{O}_n$, where P is a prime ideal in $\mathbf{O}_n$ containing p. This means degree of P is 1. Hence p has the prime ideal decomposition $p = P_1 P_2 \cdots P_n$ in $\mathbf{O}_n$, where P_j are all distinct prime ideals.

Next we shall show $n \leqq p$. Let $h(x)$ be the minimal polynomial of μ over $\mathbf{Q}$. Using decomposition of p and the assumption p does not divide

2000 Mathematics Subject Classification. Primary 11A07; Secondary 20D05.

[†)] Present address: Toriage 5-13-5, Hirosaki, Aomori 036-8171, Japan.

doi: 10.3792/pjaa.88.35

$I(\mu)$, by Kummer's theorem in [2, p. 141–145], we obtain $h(x) \equiv \phi_1(x)\phi_2(x)\cdots\phi_n(x) \bmod p$ where $\phi_j(x) = x - a_j$, $a_j \in \mathbf{Z}$ and $a_j \bmod p$ are all distinct. Thus we have $p \geqq |\{a_j \bmod p\}| = n$. □

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 $g(\chi) = \sum_{a \in \mathbf{F}_r} \chi(a)\zeta^a$ be the Gauss sum of χ where $\mathbf{F}_r$ is a finite field of order r.

Let $\sigma(\zeta) = \zeta^c$ be a generator of the Galois group G of K over $\mathbf{Q}$ 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 $L_n = \mathbf{Q}(\theta)$ and θ is a normal basis element of $\mathbf{O}_n$ over $\mathbf{Z}$ (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) *We set cyclic matrices A_n, B_n of the degree n as follows*:

$$A_n := \begin{pmatrix} \theta_0 & \theta_1 & \dots & \theta_{n-1} \\ \theta_{n-1} & \theta_0 & \dots & \theta_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ \theta_1 & \theta_2 & \dots & \theta_0 \end{pmatrix}$$

and

$$B_n := \begin{pmatrix} g_0 & g_1 & \cdots & g_{n-1} \\ g_{n-1} & g_0 & \cdots & g_{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ g_1 & g_2 & \cdots & g_0 \end{pmatrix}.$$

Then A_n has eigenvalues g_k and column eigenvectors $v_k = (\omega^{kj})$, respectively and B_n has also eigenvalues $n\theta_k$ and column eigenvectors $v_k = (\bar{\omega}^{kj})$, respectively.

(3) *$|A_n| = \prod_{k=0}^{n-1} g_k$ and $|B_n| = n^n \prod_{k=0}^{n-1} \theta_k$ where $|A_n|$ and $|B_n|$ are determinants of A_n and B_n, respectively.*

(4) *We set $\epsilon = (-1)^{\frac{(r-1)(n-2)}{8}+1}$ for even n and λ is the quadratic character. Then we have*

$$|A_n| = \begin{cases} -r^{\frac{n-1}{2}} & \textit{if } n \textit{ is odd,} \\ \epsilon r^{\frac{n-2}{2}} g(\lambda) & \textit{if } n \textit{ is even.} \end{cases}$$

Thus we have

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

Proof. (1) First equations follow essentially from

$$\begin{aligned} g(\chi) &= \sum_{a \in \mathbf{F}_r} \chi(a)\zeta^a = \sum_{\ell=1}^{r-1} \chi(c^\ell)\zeta^{c^\ell} \\ &= \sum_{t=0}^{n-1} \sum_{s=1}^{\frac{r-1}{n}} \chi(c^{ns})\chi(c^t)(\zeta^{c^{ns}})^{c^t} \\ &= \sum_{t=0}^{n-1} \chi(c^t)\Big(\sum_{\tau \in T_n} \zeta^\tau\Big)^{\sigma^t} = \sum_{t=0}^{n-1} \omega^t \theta_t. \end{aligned}$$

On second equations, we can easily solve linear equations $g_k = \sum_{s=0}^{n-1} \omega^{ks}\theta_s$ for $0 \leqq k < n$ about the unknowns θ_s.

(2) is easily checked from (1).

(3) follows easily from (2).

(4): It is easy to see $\chi(-1) = 1$ for odd n. In general, it follows from

$$\chi(-1) = \chi(c^{\frac{r-1}{2}}) = \omega^{\frac{r-1}{2}} = (e^{\pi i})^{\frac{r-1}{n}} = (-1)^{\frac{r-1}{n}}.$$

(4) follows from $g_k g_{n-k} = \chi(-1)^k |g_k|^2 = \chi(-1)^k r$ for $1 \leqq k \leqq \frac{n-1}{2}$. □

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

Corollary.

(1) *If r is a common prime divisor of f and t, then $p \equiv 1$ or $r \equiv 1 \bmod 4$ (see [7, Lemma, (4)]).*

(2) *If $p = 3$ and f divides t, then $q \equiv -1 \bmod 9$ (see [8, Corollary, (a)]).*

Proof. Let n be a divisor of q^* where $q^* q = r - 1$.

(1) We set here $n = 2$. We have $d(L_2) = (-1)^{\frac{r-1}{2}} r$ by Lemma and $d(\theta) = (\theta - \theta_1)^2 = d(L_2)$ because $\theta = \mathrm{Tr}_{K/L_2}(\zeta)$ and so $\theta + \theta_1 = -1$. Thus Kummer's theorem asserts $h(x) \equiv (x - b)(x + b + 1) \bmod p$ for the minimal polynomial $h(x)$ of θ.

$$(2b+1)^2 \equiv (\theta - \theta_1)^2 = d(L_2) \equiv (-1)^{\frac{r-1}{2}} \not\equiv 0 \bmod p.$$

Thus we have by Fermat's theorem.

$$1 \equiv ((2b+1)^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}\frac{r-1}{2}} \bmod p.$$

(2) We consider the case $n = p = 3$. If f is composite, then f does not divide t. Thus f is prime

and so $r = f$ (see [7]), where r is as in (1). f has a primary prime decomposition $f = \eta\bar{\eta}$ in $\mathbf{Z}[\omega]$ 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 $\mathbf{Q}$.

$$\begin{aligned} h(x) &:= x^3 + a_1x^2 + a_2x + a_3 \\ &= (x - \theta_0)(x - \theta_1)(x - \theta_2), \end{aligned}$$

where $a_1 = -\theta_0 - \theta_1 - \theta_2 = 1$. If 3 does not divide $I(\theta)$, then $h(x) \equiv x^3 - x \bmod 3$ contradicts to $a_1 = 1$. Thus $d(\theta) \equiv 0 \bmod 3$.

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

Thus we have $3a_2 = 1 - f = -q(q+1)$. 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

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

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

Remark. The minimal polynomials of θ and prime ideal decompositions of p in cases (1) and (2) can be explicitly determined.

References

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

[2] E. Artin, *Theory of algebraic numbers*, Notes by Gerhard Würges from lectures held at the Mathematisches Institut, Göttingen, Germany, in the Winter Semester, 1956/7, translated by George Striker, Schildweg 12, Göttingen, 1959.

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

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

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

[6] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, 2nd ed., Grad. Texts in Math., 84, Springer, New York, 1990.

[7] K. Motose, Notes on the Feit-Thompson conjecture, Proc. Japan Acad. Ser. A Math. Sci. **85** (2009), no. 2, 16–17.

[8] K. Motose, Notes to the Feit-Thompson conjecture. II, Proc. Japan Acad. Ser. A Math. Sci. **86** (2010), no. 8, 131–132.

[9] T. Ono, *An introduction to algebraic number theory*, translated by the author from the second Japanese edition of Suron Josetsu, Plenum Press, New York, 1990.

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