Notes to the Feit-Thompson conjecture. II

By Kaoru Motose

Emeritus Professor, Hirosaki University[†)]

(Communicated by Shigefumi Mori, M.J.A., Sept. 13, 2010)

Abstract: Feit and Thompson conjectured for distinct primes $p < q$ that $(q^p - 1)/(q - 1)$ never divides $(p^q - 1)/(p - 1)$. This paper is a record on partial solutions to this conjecture for small primes 3 and 5.

Key words: Odd order theorem; power residue symbol; Eisenstein reciprocity.

We set for primes $p < q$,

$$F = \frac{q^p - 1}{q - 1} \text{ and } T = \frac{p^q - 1}{p - 1}.$$

Feit and Thompson [2] conjectured that F never divides T. If it would be proved, their odd order theorem [3] would be greatly simplified (see [1,4]). In this paper, partial solutions to this conjecture are given for $p = 3$ and $p = 5$ (see also [6,7]).

Throughout this paper, we set $\zeta = e^{\frac{2\pi i}{p}}$ and $\lambda = 1 - \zeta$. In case $q \equiv 1 \bmod p$, $F \equiv 0$ and $T \equiv 1 \bmod p$ and so F never divides T. Thus we assume $q \not\equiv 1 \bmod p$ in this paper. Hence $p > 2$ and there exists a positive integer c with $c(q-1) \equiv 1 \bmod p$.

We set $\eta = \zeta^c(\zeta - q)$ and let D_p be the ring of algebraic integers in $\mathbf{Q}(\zeta)$. Then η is primary (see [5, p.206]) by the next Lemma (1) and F is the norm $N(\eta)$ of η in D_p.

Let $\chi_A = \left(\frac{}{A}\right)_p$ be the pth power residue symbol where A is an ideal of D_p with $A \not\ni p$ (see [5, p.205]). We write simply χ_α in case $A = \alpha D_p$ for $\alpha \in D_p$.

The next Lemma (2) holds for odd mth power residue symbols and (3) holds for an arbitrary m.

Lemma. *We have the next assertions.*

(1) $\eta \equiv 1 - q \bmod \lambda^2$, *namely, η is primary.*

(2) $\chi_\eta(-1) = 1$ *and if a, b are real, then* $\chi_a(b) = 1$.

(3) $\chi_A(\zeta) = \zeta^{\frac{N(A)-1}{p}}$. *In particular,* $\chi_\eta(\zeta) = \zeta^{\frac{F-1}{p}}$.

Proof. (1) Since $p = \lambda^{p-1}u$ for some $u \in D_p$ and so $c(q-1) \equiv 1 \bmod \lambda^2$,

$$\begin{aligned}\eta &= (1-\lambda)^c(1-\lambda-q) \\ &\equiv (1-c\lambda)(1-q-\lambda) \\ &\equiv 1 - q + \lambda(c(q-1)-1) \equiv 1 - q \bmod \lambda^2.\end{aligned}$$

(2) We have $\chi_\eta(-1) = \chi_\eta(-1)^p = 1$ for an odd p. Since $\zeta \to \bar{\zeta}$ is the automorphism of $\mathbf{Q}(\zeta)$, where $\bar{\zeta}$ is the complex conjugate of ζ, it follows from [5, p.206, Proposition 14.2.4] that

$$\overline{\chi_a(b)} = \chi_{\bar{a}}(\bar{b}) = \chi_a(b)$$

and so $\chi_a(b)$ is real. Our assertion follows since p is odd and $\chi_a(b)$ is a pth root of 1.

(3) If $a \equiv 1$ and $b \equiv 1 \bmod p$, then it follows from $(a-1)(b-1) \equiv 0 \bmod p^2$ that

$$\frac{ab-1}{p} \equiv \frac{a-1}{p} + \frac{b-1}{p} \bmod p.$$

Thus if $\chi_B(\zeta) = \zeta^{\frac{N(B)-1}{p}}$ and $\chi_C(\zeta) = \zeta^{\frac{N(C)-1}{p}}$, then $\zeta^{\frac{N(BC)-1}{p}} = \chi_{BC}(\zeta)$ by $N(BC) = N(B)N(C)$. In case A is prime, (3) is clear by $A \not\ni p$ and in general case, it follows from the above. □

The next is a key in this paper. However I can not compute $\chi_\eta(u)$ for $p > 5$.

Proposition. *Assume F divides T. Then we obtain the following assertions.*

(1) $\chi_\eta(p) = 1$.

(2) $\chi_\eta(u) = \chi_\eta(\zeta - 1)$ *for a unit* $u = \prod_{t=2}^{p-1} \frac{\zeta^t - 1}{\zeta - 1}$.

(3) $\chi_\eta(\zeta + \epsilon)^{2(q-1)} = \chi_m(\zeta)^{q+1}$ *where $\epsilon = \pm 1$ and $q + \epsilon = p^\ell m$ with $p \nmid m$. In particular, $\chi_\eta(\zeta + \epsilon) = 1$ if p divides $q + 1$.*

Proof. (1) In virtue of $F \mid T$, we can see $\chi_\eta(p) = 1$ from $(q, p) = 1$ and the equation

$$\chi_\eta(p)^q = \chi_\eta(p^q) = \chi_\eta(1) = 1.$$

2000 Mathematics Subject Classification. Primary 11A07, 20D05.

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

doi: 10.3792/pjaa.86.131

(2) It follows from $p = (\zeta - 1)^{p-1}u$ and the next equation by (1) that

$$1 = \chi_\eta(p) = \chi_\eta((\zeta - 1)^{p-1}u) = \chi_\eta(\zeta - 1)^{-1}\chi_\eta(u).$$

(3) Since each pair of η, m and p is relatively prime and η is primary, using (1) and the Eisenstein reciprocity law (see [5, p.207, Theorem 1]), we have

$$\begin{aligned}\chi_\eta(\zeta + \epsilon) &= \chi_\eta(q + \epsilon) = \chi_\eta(p)^\ell \chi_\eta(m) = \chi_m(\eta) \\ &= \chi_m(\zeta^c)\chi_m(\zeta + \epsilon).\end{aligned}$$

We have our result by $2(q-1)$th power of two sides in this equation. In fact, we obtain from Lemma (2)

$$\begin{aligned}\chi_\eta(\zeta + \epsilon)^{2(q-1)} &= \chi_m(\zeta^{c(q-1)})^2 \chi_m(\zeta^2 + 2\epsilon\zeta + 1)^{q-1} \\ &= \chi_m(\zeta)^{q+1}\chi_m(\zeta + \bar{\zeta} + 2\epsilon)^{q-1} \\ &= \chi_m(\zeta)^{q+1}\end{aligned}$$

because $c(q-1) \equiv 1 \mod p$ and $\zeta + \bar{\zeta} + 2\epsilon$ is real. □

Corollary. *F never divides T in either case of the following*

(a) $p = 3$ *and* $q \not\equiv -1 \mod 9$

(b) $p = 5$ *and* $q = 5\ell - 1$ *with* $5 \nmid \ell$.

Proof. We use notations in Proposition and we assume F divides T. Then $q \not\equiv 1 \mod p$ as in the first notice. Thus we have $q \equiv -1 \mod p$ in any case (a) or (b). Thus we have $1 = \chi_\eta(\zeta + \epsilon) = \chi_\eta(u)$ from Proposition (3) and (2).

(a) We have $\chi_\eta(\zeta) = 1$ from the next equation by Lemma (2).

$$1 = \chi_\eta(\zeta + 1) = \chi_\eta(-\zeta^2) = \chi_\eta(-1)\chi_\eta(\zeta)^2 = \chi_\eta(\zeta)^2.$$

The equation $q \equiv -1 \mod 9$ follows from

$$1 = \chi_\eta(\zeta) = \zeta^{\frac{F-1}{3}} = \zeta^{q\frac{q+1}{3}} \text{ by Lemma (3).}$$

(b) Noting $1 = \chi_\eta(u) = \chi_\eta(\zeta + 1)$ and $u = \zeta^2(\zeta + 1)^2$, we have

$$1 = \chi_\eta(u) = \chi_\eta(\zeta)^2\chi_\eta(\zeta + 1)^2 = \chi_\eta(\zeta)^2.$$

Hence, by Lemma (3),

$$1 = \chi_\eta(\zeta) = \zeta^{\frac{F-1}{5}} = \zeta^{q(q^2+1)\frac{q+1}{5}}.$$

Thus $q \equiv -1 \mod 25$. □

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] 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.

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

[4] R. K. Guy, *Unsolved problems in number theory*, Third edition, Springer, New York, 2004.

[5] K. Ireland and M. Rosen, *A classical introduction to modern number theory*, Second edition, Springer, New York, 1990.

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

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