The Feit-Thompson conjecture and Cyclotomic polynomials

Kaoru Motose

Abstract : We can see that Feit-Thompson conjecture is true using factorizations of cyclotomic polynomials on the finite prime field.

Key Words : Feit-Thompson conjecture, cyclotomic polynomials, finite fields.

2000 *Mathematics Subject Classification* : Primary 12E05,12E10; Secondary11A05.

Feit and Thompson conjectured in [2, p.970, last paragraph]

$$s := \Phi_p(q) = \frac{q^p - 1}{q - 1} \text{ never divides } t := \Phi_q(p) = \frac{p^q - 1}{p - 1} \text{ for distinct primes } p \text{ and } q,$$

where $\Phi_m(x)$ is the m-th cyclotomic polynomial. The utility and the cause of this conjecture are also stated in [1, p.1], and [3, B25]. Stephens [8] found the unique example: for $p = 17$ and $q = 3313$, the prime $r = 2pq + 1 = \gcd(s, t)$ that shows $s \nmid t$ from $r < s$ (see the next page **R1** or [6, p.82]). We show this conjecture is true. The next classical results on cyclotomic polynomials are important for our Theorem.

1. Let ℓ be a prime with $\ell \nmid m$. The m-th cyclotomic polynomial $\overline{\Phi}_m(x) := \Phi_m(x)$ on $\mathbb{F}_\ell$ has square free factors and the root $\bar{\zeta}_m$ of $\overline{\Phi}_m(x)$ is of order m for $\Phi_m(\zeta_m) = 0$ by the equation $x^m - 1 = \prod_{d|m} \overline{\Phi}_m(x)$ since $x^m - 1$ has no multiple roots for $\ell \nmid m$ (see also [4, p.64, 2.45.Theorem]). □

2. Let $|a|_m$ be the order of a mod m for natural numbers a and m with $\gcd(a, m) = 1$. $\overline{\Phi}_m(x)$ factorizes into irreducible polynomials $\bar{u}_k(x) = \prod_{n=0}^{|\ell|_m - 1}(x - \bar{\zeta}_m^{k\ell^n})$ of the same degree $|\ell|_m$, where k satisfy $\gcd(k, \ell m) = 1$ and $1 \le k < m$, since $\bar{u}_k(x)$ are invariant by Frobenius automorphism $\sigma_\ell : \bar{\zeta}_m^k \to \bar{\zeta}_m^{k\ell}$ (see also [4, p.65, 2.47.Theorem.(ii)]). □

By **1** and **2**, $\overline{\Phi}_m(x) := \Phi_m(x)$ on $\mathbb{F}_\ell$ has the minimal splitting field $\mathbb{F}_{\ell^{|\ell|_m}}$ since all square free $\varphi(m)/|\ell|_m$ irreducible factors with the same degree $|\ell|_m$ where $\varphi(m) = \deg \Phi_m(x)$.

Three proofs of our theorem yield from proving contents of Kummer's theorem (see [7, p.84 Theorem 2.17]) and Stephans' examples giving the assertions: a prime $r \mid \gcd(s, t)$ if and only if $|p|_r = q$ and $|q|_r = p$ by $r \equiv 1 \bmod 2pq$.

. **Theorem.** If s divides t, then p is odd and $p = q$.

Proof. We may assume $p < q$, namely, $s < t$ by the next page **R3** or [5, p.16 Remark]. If $p = 2$, then $s \nmid t$ since $s = q + 1$ is even and $t = 2^q - 1$ is odd. Thus we assume $p > 2$.

We also see that s, t are odd and $r \equiv 1 \bmod 2pq$ for any prime divisor r of s by the next page **R2** or [8] or [5, p.16, Lemma.(3)]. We can see $|p|_t = q, |p|_s = q$ and $|q|_s = p$ by $p^q \equiv 1 \bmod t, p^q \equiv 1 \bmod s$ and $q^p \equiv 1 \bmod s$ from $p < q < s$ and $s \mid t$.

p : Both $\Phi_t(x)$ and $\Phi_s(x)$ on $\mathbb{F}_p$ have the splitting field $\mathbb{F}_{p^q}$ from $|p|_t = q = |p|_s$. Thus by the isomorphism $\zeta_t \to \zeta_s$ over $\mathbb{F}_p, s = t$ is contrary to $s < t$. □

q : $\Phi_t(x)$ on $\mathbb{F}_q$ factorizes into $\varphi(t)/|q|_t$ irreducible factors. We have $|q|_s = p$ divides $|q|_t$ by $q^{|q|_t} \equiv 1 \bmod s$ and the inequality $\varphi(t)/|q|_t \ge \varphi(t)/|q|_s = \varphi(t)/p$ by $|q|_s = p$ because $\Phi_s(x)$ on $\mathbb{F}_q$ is already factorize into $\varphi(s)/|q|_s = \varphi(s)/p$ irreducible factors and hence $\overline{\Phi}_t(x)$ factorizes at least into $\varphi(t)/|q|_s = \frac{\varphi(t)}{\varphi(s)} \cdot \frac{\varphi(s)}{p}$ irreducible factors. Thus $|q|_t = p$. If a prime $\ell \mid \gcd(t, (q-1))$, then $q \equiv 1 \bmod \ell$ then we have $|q|_r = 1$ is contray to $p = |q|_t = 1$ by the same method as the above. From this and $t \mid s(q-1), s = t$, contrary to $s < t$. □

p and q : $\Phi_t(x)$ and $\Phi_s(x)$ on $\mathbb{F}_p$ (resp. $\mathbb{F}_q$) has the minimal splitting field $\mathbb{F}_{p^q}$ (resp. $\mathbb{F}_{q^p}$) by $|p|_t = |p|_s = q$. (resp. $|q|_t = |q|_s = p$.)

Since ζ_s on $\mathbb{F}_p$, on $\mathbb{F}_q$, and on $\mathbb{Q}$ have the same order, $\Phi_t(x)$ and $\Phi_s(x)$ has the only one minimal splitting field $\mathbb{Q}(\zeta_t)$, we obtain a cotoradiction $p^q = |\mathbb{F}_{p^q}| = |\mathbb{F}_{q^p}| = q^p$. □

Remarks. We use the same notations and assumptions in the above discussions.

R1 Example of Stephens. Using the program 「MPQSX3」 attached to the package of language UBASIC designed by professor Yuji Kida, we have the prime factorization $s = r_1r_2r_3$ for $p = 17, q = 3313$ where r_1, r_2 and r_3 are primes with $r_k - 1(k = 1, 2, 3)$ are as the next table. We can see $\gcd(s, t) = r_1$ by $q = 3313 \nmid (r_2 - 1)(r_3 - 1)$ in this table.

$$\begin{aligned} r_1 - 1 &= 2 \times 17 \times 3313, \\ r_2 - 1 &= 2 \times 2 \times 5 \times 17 \times 35081 \times 2007623, \\ r_3 - 1 &= 2 \times 17 \times 1609 \times 763897 \times 1869248598543746584721506723. \end{aligned}$$

R2. $r \equiv 1 \bmod 2pq$ for any prime divisor r of s under the conditions $s \mid t$ and $2 < p < q$. If $r \mid s$ and $q \equiv 1 \bmod r$ then $0 \equiv s = q^{p-1} + \cdots + q + 1 \equiv p \bmod r$ and $r = p$. We have a contradiction $0 \equiv t \equiv 1 \bmod r$ by $r = p$. Thus $|q|_r = p$ by $q^p \equiv 1 \bmod r$ and $q \not\equiv 1 \bmod r$. Similarly $|p|_r = q$. Hence we have $r \equiv 1 \bmod 2pq$ by Fermat little theorem.

R3. Since $\frac{x}{\log x}$ is strictly increasing for $3 \le x < y$,

$$\frac{x}{\log x} < \frac{y}{\log y}, \; y^x < x^y \text{ and } \frac{y^x - 1}{y - 1} < \frac{x^y - 1}{y - 1} < \frac{x^y - 1}{x - 1}.$$

Thus we have $s = t$ is equivalent to $p = q$.

References

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

[2] W. Feit and J.G. Thompson, A solvability criterion for finite groups and some consequences, Proc. Natl. Acad. Sci. USA. **48** (1962), 968-970. See p.970, last paragraph.

[3] R. K. Guy, *Unsolved problems in number theory*, 1st ed. 1981, 2nd ed. 1994, 3rd ed. 2004, Springer. See B25.

[4] R. Lidl and H. Niederreiter, Finite fields, Encyclopedia of Mathematics and its applications, 20, 1983, Addison-Wesley Publishing Company, Massachusetts, USA. See p.64, 2.45.Theorem and p.65, 2.47.Theorem. (ii).

[5] K. Motose, Notes to the Feit-Thompson conjecture, Proc. Japan Acad. Ser. A Math. Sci. **85**(2009), no. 2, 16-17. See p.16, Remark and Lemma. (3).

[6] K. Motose, Monologue of triangles (Sankkakei no hitorigoto in Japanese), Hirosaki University Press, 2017. See p.82.

[7] T. Ono, An introduction to algebraic number theory, 1990, Plenum Press. See p.84 Theorem 2.17.

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

Emeritus professor, Hirosaki university

Home post address: Toriage 5-13-5, Hirosaki, 036-8171, JAPAN

Email address: motose@hirosaki-u.ac.jp