The Feit-Thompson conjecture and cyclotomic polynomials

To the memory of professors Kazuo Kishimoto and Yôichi Miyashita

Kaoru Motose

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

Key Words : cyclotomic polynomials, finite fields, splitting fields.

2000 *Mathematics Subject Classification* : Primary 11R18,11A15; Secondary 20E32, 20D10.

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

$$s := \frac{q^p - 1}{q - 1} \text{ never divides } t := \frac{p^q - 1}{p - 1} \text{ for distinct primes } p \text{ and } q.$$

The utility and the cause of this conjecture are also stated in [7], [1, p.1] and [3, B25].

Using a computer, Stephens [7] 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 **R2** or [6, p.82]).This example is a counter example to his view $(s, t) = 1$ but not to Feit Thompson conjecture. However he gave an important congruence to our theorem, in detail see **R1, R2**.

Using the next reviews of classical results, we show this conjecture is true.

Reviews. R1 (Stephens [7]). $r \equiv 1 \bmod 2pq$ for any prime $r | \gcd(t, s)$ and $p < q$. If $p = 2$ then $2^q - 1 \equiv 0 \equiv q+1 \bmod r$, so $q|(r-1)$ by Fermat little theorem and $r|(q+1)$. This yields a contrary $q = r - 1$. Hence $2 < p < q$. If $p \equiv 1 \bmod r$ then $0 \equiv t = p^{q-1} + \cdots + p + 1 \equiv q \bmod r$ and $r = q$. We have a contradiction $0 \equiv s \equiv 1 \bmod r$. Thus $p \not\equiv 1 \bmod r$ and $|p|_r = q$ by $p^q \equiv 1 \bmod r$. Similarly $|q|_r = p$. Hence we have $r \equiv 1 \bmod 2pq$ by Fermat little theorem.

R2. Example of Stephens [7]. Using the program MPQSX3 attached to the package of language UBASIC designed by professor Yuji Kida, we have the prime factorization $s = r_1 r_2 r_3$ for $p = 17, q = 3313$ where r_1, r_2 and r_3 are primes, $r_1 \mid t$ and $r_k - 1$ $(k = 1, 2, 3)$ 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.

$$r_1 - 1 = 2 \times 17 \times 3313, \; r_2 - 1 = 2 \times 2 \times 5 \times 17 \times 35081 \times 2007623,$$
$$r_3 - 1 = 2 \times 17 \times 1609 \times 763897 \times 1869248598543746584721506723.$$

R3. The next shows $s = t$ iff $p = q$. Since $\frac{x}{\log x}$ is strictly increasing for $3 \le x < y$,

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

R4. We define cyclotomic polynomials over $\mathbb{Q}$ by $\Phi_m(x) := \prod_k (x - \zeta_m^k)$ where $\zeta_m = e^{\frac{2\pi i}{m}}$ and k runs over $E_m := \{k \mid 1 \le k < m \text{ with } \gcd(k, m) = 1\}$. $\Phi_m(x)$ is irreducible over $\mathbb{Q}[x]$ since it is minimal invariant by all automorphisms $\sigma_k : \zeta_m \to \zeta_m^k$ for $k \in E_m$.

We assume $\ell \nmid m$ for prime ℓ. All roots of $x^m - 1$ are distinct by its derivation mx^{m-1} and Thus all roots of $x^m - 1$ on $\mathbb{Q}$ or $\mathbb{F}_\ell$ forms the cyclic group $\langle \zeta_m \rangle$ of order m and $x^m - 1 = \prod_{d|m} \Phi_d(x)$ on $\mathbb{Q}$ or on $\mathbb{F}_\ell$ by classifying roots by orders. $\varphi(m) := \deg \Phi_m(x)$ is Euler function. $\Phi_m(x)$ is monic and in $\mathbb{Z}[x]$ by induction on m. (see also [4, p.64, 2.45.Theorem]).

R5. We assume $\ell \nmid m$ for prime ℓ. Let $|a|_m$ be the order of $a \bmod m$ for natural numbers a and m with $\gcd(a,m)=1$. $\Phi_m(x)$ on $\mathbb{F}_\ell$ factorizes into irreducible polynomials $u_{k_i}(x) = \prod_{h=0}^{|\ell|_m-1}(x-\zeta_m^{k_i\ell^h})$ of the same degree $|\ell|_m$ (note $\ell \nmid m$) where $k_i \mod m$ is representatives of cosets $\{Hk_i \mid i = 1\ldots\frac{\varphi(m)}{|\ell|_m}\}$ of subgroup $H = \langle \ell \bmod m\rangle$ in the group $E_m \bmod m$ with order $\varphi(m)$. $u_k(x)$ is irreducible since $u_k(x)$ are minimal invariant by Frobenius automorphism $\sigma_\ell : \zeta_m^{k_i} \to \zeta_m^{k_i\ell}$ (see also [4, p.65, 2.47.Theorem.(ii)]).

Theorem. s never divides t for distinct primes p and q.

Proof. If $p=2$, then $s=q+1$ is even and $t=2^q-1$ is odd, so $s\nmid t$. We shall prove this theorem by reduction to absurdity. Hence we assume $s \mid t$ for $2<p<q$, namely, for odd s,t and $s<t$ by **R3** or [5, p.16, Remark]. We know also $r \equiv 1 \bmod 2pq$ for any prime divisor r of s by **R1**([7]) or [5, p.16, Lemma. (3)]. We can see $|p|_t = q, |p|_s = q$ by $p^q \equiv 1 \bmod t, p^q \equiv 1 \bmod s$ from $p<s$ and $s\mid t$.

Both $\Phi_t(x)$ and $\Phi_s(x)$ on $\mathbb{F}_p$ have the minimal splitting field $\mathbb{F}_{p^q}$ from $|p|_t = q = |p|_s$ and **R5**. The isomorphism $\zeta_t \to \zeta_s$ over $\mathbb{F}_p$ is contrary to $s<t$. □.

Notice. First we show $|q|_t = p$. $\Phi_t(x)$ on $\mathbb{F}_q$ factorizes into $\varphi(t)/|q|_t$ irreducible factors by **R5**, where $\varphi(t) = \deg\Phi_t(x)$. Noting $|q|_s = p$ by $q^p \equiv 1 \bmod s$ from $q<s$ by **R1**, We have $|q|_s = p$ divides $|q|_t$ by $q^{|q|_t} \equiv 1 \bmod s$ and the inequality $\varphi(t)/|q|_t \geq \varphi(t)/|q|_s = \varphi(t)/p$ by $|q|_s = p$ because $\Phi_s(x)$ on $\mathbb{F}_q$ already factorizes into $\varphi(s)/|q|_s = \varphi(s)/p$ irreducible factors and hence $\Phi_t(x)$ on $\mathbb{F}_\ell$ factorizes at least into $\varphi(t)/|q|_s = \frac{\varphi(t)}{\varphi(s)}\cdot\frac{\varphi(s)}{p}$ irreducible factors. Thus $|q|_t = p$. Of course, as the proof in theorem, by $|q|_t = p$ and $|q|_s = p$, we obtain the isomorphism $\zeta_s \to \zeta_t$ over $\mathbb{F}_q$ is contrary to $s<t$.

However the another method exists as follows: If a prime $\ell \mid \gcd(t,(q-1))$, then $q \equiv 1 \bmod \ell$, that is, we have $\Phi_\ell(x)$ on $\mathbb{F}_q$ has the minimal splitting field $\mathbb{F}_q$ from $|q|_\ell = 1$. The minimal splitting fields of $\Phi_t(x)$ on $\mathbb{F}_q$ is also $\mathbb{F}_q$, contrary to $|q|_t = p$. Thus $\gcd(t,(q-1)) = 1$ and $t \mid s(q-1)$, namely, $|q|_t = p$ imply $s=t$, contrary to $s<t$. □

References

[1] T. M. Apostol, The resultant of the cyclotomic polynomials $F_m(ax)$ and $F_n(bx)$, Math. Comp., **129**(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] 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

E-mail address: motose@hirosaki-u.ac.jp