Notes to the Feit-Thompson conjecture

By Kaoru MOTOSE*)

Emeritus Professor, Hirosaki University

(Communicated by Heisuke HIRONAKA, M.J.A., Jan. 13, 2009)

Abstract: We shall present partial solutions to the conjecture such that $(q^p-1)/(q-1)$ does not divide $(p^q-1)/(p-1)$ for distinct primes $p<q$.

Key words: Odd paper; cyclotomic polynomials; Legendre symbol.

In this paper we shall give partial solutions to the Feit-Thompson conjecture (see [2]) and observations on the Stephans conjecture (see [5]). For distinct primes p and q, we set

$$A=(q^p-1)/(q-1) \text{ and } B=(p^q-1)/(p-1).$$

The Feit-Thompson conjecture.

A does not divide B for $A<B$.

In the paper [1, p.1] and the book [4, p.125], it was mentioned that if it could be proved, it would greatly simplify the very long proof of the Feit-Thompson theorem that every group of odd order is solvable (see [3]).

The next is almost trivial but we cite it here for convenience of readers to know $B>A$ for $q>p\geq 2$.

Remark. $\dfrac{m^n-1}{m-1}>\dfrac{n^m-1}{n-1}$ *for integers* $n>m\geq 2$.

Proof. It is easy for $m=2$ from $2^n>n+2$ for $n\geq 3$. Noting $\dfrac{x}{\log x}$ is strict increasing for $x\geq 3$, we have $\dfrac{n}{\log n}>\dfrac{m}{\log m}$ and hence $m^n>n^m$ for $n>m\geq 3$. Thus we have $\dfrac{m^n-1}{m-1}>\dfrac{m^n-1}{n-1}>\dfrac{n^m-1}{n-1}$ for $n>m\geq 3$. □

(1) and (2) in the next are not useful to the computer but may be useful to consider the conjecture. Here $\Phi_n(x)$ is the cyclotomic polynomial and the notation $|c|_d$ means the order of c mod d for natural numbers c and d with $(c,d)=1$.

Lemma. *Let p, q are distinct primes. We set $pj+qk=1$, $\ell=pj^2+qk^2$, $a=(pq)^\ell$, and $1<d$ is a common divisor of A and B. Then the next hold.*

(1) $p=|q|_d$ *and* $q=|p|_d$.
(2) $a^p\equiv p$, $a^q\equiv q \bmod d$, *and* $pq=|a|_d$.
(3) $2pq\mid\varphi(d)$.
(4) *If* $p\equiv 3$ *or* $q\equiv 3 \bmod 4$, *then* $d\equiv 1 \bmod 4$.

Proof. We may prove one side statement about p or q as conditions on p and q are symmetric.

(1): It is easy to see $q^p\equiv 1 \bmod d$. If $q\equiv 1 \bmod d$, then $0\equiv A=\Phi_p(q)\equiv\Phi_p(1)=p \bmod d$. Hence $d=p$ and we have a contradiction $0\equiv B=\Phi_q(p)\equiv\Phi_q(0)=1 \bmod d$. Thus $p=|q|_d$. Similarly we have $q=|p|_d$.

(2): From setting of ℓ, we have $pj\equiv 1 \bmod q$ and $\ell\equiv j \bmod q$. Thus it follows from $a=(pq)^\ell$, $p\ell\equiv pj\equiv 1 \bmod q$ and (1) that

$$a^p=(pq)^{p\ell}\equiv p^{p\ell}\equiv p\not\equiv 1 \bmod d$$

and similarly $a^q\equiv q\not\equiv 1 \bmod d$. Thus we have $a^{pq}\equiv p^q\equiv 1 \bmod d$ from (1), and so $pq=|a|_d$.

(3): We shall prove that p and q are odd. If $p=2$ then $0\equiv\Phi_2(q)=q+1 \bmod d$ and $0\equiv\Phi_q(2)=2^q-1 \bmod d$ and so $q+1\geq d$ and $2^q\equiv 1 \bmod d$. Thus d is odd and $d-1\geq\varphi(d)\geq|2|_d=q\geq d-1$. Hence $d-1=q$ yields a contradiction $q=2=p$. Similarly, q is odd. It is easy to see $pq\mid\varphi(d)$ from (2) and Euler's theorem. On the other hand $\varphi(d)$ is even for $d>2$. If $d=2$, then we have a contradiction $0\equiv\Phi_p(q)\equiv\Phi_p(1)=p\equiv 1 \bmod 2$.

(4): We may assume that d is prime. We have $d\equiv 1 \bmod p$ from (3), and $p^q\equiv 1 \bmod d$. Thus we obtain $\left(\dfrac{d}{p}\right)=\left(\dfrac{1}{p}\right)=1$ for Legendre symbol and

$$\left(\frac{p}{d}\right)=\left(\frac{p}{d}\right)^q=\left(\frac{p^q}{d}\right)=\left(\frac{1}{d}\right)=1.$$

Hence we have

2000 Mathematics Subject Classification. 11A07, 20D05.
*) Present address: 5-13-5 Toriage, Hirosaki 036-8171, Japan.

©2009 The Japan Academy

$$1 = \left(\frac{p}{d}\right)\left(\frac{d}{p}\right) = (-1)^{\frac{d-1}{2}\frac{p-1}{2}} = (-1)^{\frac{d-1}{2}}.$$

Similarly, we have same result for $q \equiv 3 \mod 4$. □

The next is the partial solution for the conjecture. As a special case of (1) or the proof of Lemma (3), we may assume $2 < p < q$ for the conjecture.

In case $p = 3$, it seems to be very important from [2]. In this case, we may consider $q \equiv -1 \mod 6$ noting (1) and q is odd. Moreover we may assume A is prime from (2) in case $p = 3$.

Proposition. *In either case of the next conditions, A does not divide B.*

(1) $q \equiv 1 \mod p$.
(2) $p = 3 < q$ *and A is composite.*
(3) $p \equiv 3$ *and* $q \equiv 1 \mod 4$.

Proof. Assume $A\ell = B$ for some integer ℓ.

(1) In case $q \equiv 1 \mod p$, we have a contradiction

$$\begin{aligned} 0 &\equiv p\ell = \Phi_p(1)\ell \equiv \Phi_p(q)\ell = A\ell \\ &= B = \Phi_q(p) \equiv \Phi_q(0) = 1 \mod p. \end{aligned}$$

(2) If $\Phi_3(q) = A$ is composite and r is the smallest prime divisor of $\Phi_3(q)$, then we have $6q \mid (r-1)$ by Lemma (3). Thus we have a contradiction $q+1 \geq r \geq 6q+1$ by $(q+1)^2 \geq q^2+q+1 = \Phi_3(q)$.

(3) Since A is a common divisor of A and B, then a congruence $A = q^{p-1} + \cdots + 1 \equiv p \equiv 3 \mod 4$ contradicts to Lemma (4). □

The Stephens conjecture.

A and B are relatively prime.

If a prime number r divides both A and B then $r = 2pq\ell + 1$ for some integer ℓ (see Lemma (3)). Using computer, Stephens found a counterexample $p = 17$, $q = 3313$ and $r = 112643 = 2pq + 1$ and confirmed that r is the greatest common divisor of A and B by computer, so this example leaves the Feit-Thompson conjecture unresolved (see [5]).

At the present, it is known by computer that no other such pairs exist for $p < q < 10^7$ and $p = 3 < q < 10^{14}$ (see [4]).

We don't know that conjectures have some relations with (2) and (3) in the next.

Observation. *If $p = 17$ and $q = 3313$, then we have*

(1) (Stephens) $(\Phi_p(q), \Phi_q(p)) = 2pq + 1 \equiv 3 \mod 4$.
(2) $p^{\frac{q-1}{2}} \equiv 1 \mod q$ *but* $p^{\frac{q-1}{2}} \not\equiv 1 \mod q^2$.
(3) $q^{\frac{p-1}{2}} \equiv 1 \mod p^2$.

In general, there are few prime numbers p satisfying congruence $a^{\frac{p-1}{2}} \equiv 1 \mod p^2$ for a fixed natural number $a > 1$ with $(a, p) = 1$. For example,

a	2	3	17	3313
$3 < p < 10^5$	3511	11	46021, 48947	7, 17

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