SOME CONGRUENCES CONCERNING FINITE GROUPS

KAORU MOTOSE

ABSTRACT. In this paper, we present a lemma about orders of normal subgroups in a transitive group of prime degree. This lemma has an application to prove simplicity of the alternative group A_5 of degree 5, and 4-transitive Mathieu groups $M_{11}, M_{12}, M_{23}, M_{24}$. Please use this lemma for your lecture to your students about group theory or Galois theory. I present some comments to Feit-Thompson conjecture. I think also it is not so popular, to mathematician, even to finite group theorists and number theorists.

Key Words: Sylow theorem, Alternative groups, Mathieu groups,

2000 *Mathematics Subject Classification*: Primary 20B20 ; Secondary 20B05, 20B35.

Sylow theorem states that the number of distinct p-Sylow subgroups is congruent to 1 modulo p. In this paper, we call it Sylow congruence and using this, we shall present a lemma to prove the simplicity of the alternative group A_5 and Mathieu groups $M_{11},\ M_{12},\ M_{23},\ M_{24}$. Moreover, we shall give some comments to Feit-Thompson Conjecture. The part up to Theorem 9 was written in considering for education to students.

Congruences in finite groups are important between group theory and number theory. It is the most important congruence in group theory that the order $|H|$ of subgroup H of a group G is a divisor of $|G|$. For the proof of this, we use all conditions in the definition of the group. Apply this to the unit group of the residue ring $\mathbb{Z}/n\mathbb{Z}$, we have Fermat little theorem and Euler theorem.

Let Γ_n be the set of complex numbers of order n and we define cyclotomic polynomial $\Phi_n(x) = \prod_{\eta\in\Gamma_n}(x-\eta)$. Then formula $x^n - 1 = \prod_{d|n}\Phi_d(x)$ yields form classifying orders in the group of roots of $x^n - 1 = 0$, which is equivalent to the definition of the cyclotomic polynomial $\Phi_m(x)$. It follows from this formula that the group $\mathbb{F}_q^*$ is cyclic, where $\mathbb{F}_q$ is a finite field of order q and $\mathbb{F}_q^* = \mathbb{F}_q \setminus \{0\}$. Usually, we prove this using orders of two elements in the abelian group $\mathbb{F}_q^*$.

From Sylow congruence, non cyclic groups of order pq with primes $p < q$ have a normal q-Sylow subgroup and q distinct p-Sylow subgroups. Groups of this kind are there infinite many for a fixed prime p by the Dirichlet theorem which can be proved by cyclotomic polynomials in case $q \equiv 1 \bmod p$. These groups suggest Burnside's p^sq^t theorem.

1. Some notations and elementary results

In this section we shall give some notations and elementary well known results. Let G be a finite group and let Δ be a finite set. We say Δ is a G-set if satisfying the following

The detailed version of the rest from Lemma 10 will be submitted for publication elsewhere.

conditions

$$\alpha^h \in \Delta,\ (\alpha^g)^h = \alpha^{gh} \text{ and } \alpha^1 = \alpha \text{ for } \alpha \in \Delta \text{ and } g, h \in G.$$

We set $G_\Gamma = \{g \in G \mid \alpha^g = \alpha \text{ for all } \alpha \in \Gamma\}$ for a subset Γ of Δ. In case $G_\Delta = \{1\}$, we say Δ is a faithful G-set or G is a permutation group on Δ. We can classify elements in G-set Δ by orbits $\alpha^G = \{\alpha^g \mid g \in G\}$ for $\alpha \in \Delta$ and we obtain

$$\Delta = \bigcup_k \alpha_k^G, \text{ and } |\Delta| = \sum_k |\alpha_k^G|.$$

We set $G_\alpha = \{g \in G \mid \alpha^g = \alpha\}$ for $\alpha \in \Delta$. Then G_α is a subgroup of G. Since $\alpha^g = \alpha^h$ is equivalent to $G_\alpha g = G_\alpha h$, we have

$$|G| = |\alpha^G||G_\alpha|.$$

Let G be a permutation group on Δ. G is transitive if there exists $g \in G$ with $\alpha^g = \beta$ for arbitrary $\alpha, \beta \in \Delta$. G is k-transitive ($k \geq 2$) if G_α is $(k-1)$-transitive on $\Delta \setminus \{\alpha\}$.

Lemma 1. *Let G be 2-transitive on a finite set Δ and let $\{1\} \neq N$ be a normal subgroup of G. Then we have*

(1) *$G = G_\alpha \cup G_\alpha x G_\alpha$ for $x \notin G_\alpha$.*
(2) *$G = G_\alpha N$ and N is transitive on Δ.*

Proof. (1) Let $g \in G \setminus G_\alpha$ then $\alpha \neq \alpha^g$ and $\alpha \neq \alpha^x$. Since G is 2-transitive, there exists $h \in G_\alpha$ such that $\alpha^g = \alpha^{xh}$. Thus $g(xh)^{-1} \in G_\alpha$ and so $g \in G_\alpha xh \subset G_\alpha x G_\alpha$.

(2) If $N \subset G_\alpha$, then we have a contradiction

$$N \subset \bigcap_{g \in G} g^{-1} G_\alpha g = \bigcap_{g \in G} G_{\alpha^g} = G_\Delta = \{1\}.$$

Hence we have $N \not\subset G_\alpha$ and there exists $n \in N \setminus G_\alpha$. Since G is 2-transitive,

$$G = G_\alpha \bigcup G_\alpha n G_\alpha \subset G_\alpha N G_\alpha = G_\alpha N \text{ and } \Delta = \alpha^G = \alpha^{G_\alpha N} = \alpha^N.$$

A transitive group G is regular on Δ if $G_\alpha = 1$ for some $\alpha \in \Delta$. Moreover, for subset T of G, we set normalizer $\mathcal{N}_G(T) = \{g \in G \mid g^{-1}Tg = T\}$ of T and centralizer $\mathcal{C}_G(T) = \{g \in G \mid gt = tg \text{ for all } t \in T\}$ of T.

Lemma 2. *Let G be 2-transitive on a finite set Δ and let $N \neq \{1\}$ be a regular normal subgroup of G.*

(1) *N is elementary abelian and $|\Delta| = |N|$ is a power of a prime.*
(2) *If G_α is simple, then G_α is a subgroup of $\mathrm{Aut}(N) = \mathrm{GL}(s, \mathbb{F}_p)$ where $\mathrm{Aut}(N)$ is a automorphism group of N, $|\Delta| = |N| = p^s$, and $\mathrm{GL}(s, \mathbb{F}_p)$ is the general linear group over a prime field $\mathbb{F}_p$.*

Proof. (1) We prove that G_α is transitive on $N \setminus \{1\}$ by the action $n^g = g^{-1}ng$ for $n \in N \setminus \{1\}$ and $g \in G_\alpha$. Let $s \neq t$ be arbitrary elements of $N \setminus \{1\}$. Then $\alpha^s, \alpha^t \in \Delta \setminus \{\alpha\}$ and there exists $g \in G_\alpha$ such that $\alpha^{sg} = \alpha^t$ because G_α is transitive on $\Delta \setminus \{\alpha\}$. Hence we have $gtg^{-1} = s$ from $\alpha^{sg} = \alpha^t = \alpha^{gt}$ and $gtg^{-1}s^{-1} \in N_\alpha = \{1\}$.

Thus $x^p = 1$ for all $x \in N$ since N contains an element of a prime order p and G_α is transitive on $N \setminus \{1\}$ by the action $a^g = gag^{-1}$ for $a \in N$ and $g \in G_\alpha$.

Thus N is a p-group and the center $Z \neq 1$ of N is normal in G (see the paragraph before Lemma 8). Hence it follow from the next that $N = Z$, namely, N is elementary.

$$G_\alpha Z = G = G_\alpha N,\ G_\alpha \cap Z = \{1\} = G_\alpha \cap N$$

On the other hand,

$$p^e = |N| = |N_\alpha||\alpha^N| = |\alpha^N| = |\Delta|.$$

(2) If $G_\alpha \cap \mathcal{C}_G(N) \neq \{1\}$, then $G_\alpha = G_\alpha \cap \mathcal{C}_G(N)$ since G_α is simple and $\mathcal{C}_G(N)$ is normal. Thus $G_\alpha \subset \mathcal{C}_G(N)$ which is a contradiction to that G_α is transitive on $N \setminus \{1\}$. Thus it follows from the above that

$$|\mathcal{C}_G(N)| = |\alpha^{\mathcal{C}_G(N)}| = |\Delta| = |\alpha^N| = |N|$$

Thus this implies $N = \mathcal{C}_G(N)$ from $N \subset \mathcal{C}_G(N)$. Hence we have

$$G_\alpha \cong G_\alpha N/N = G/N = \mathcal{N}_G(N)/\mathcal{C}_G(N)$$

is a subgroup of the automorphism $\mathrm{Aut}(N)$ of N by considering map $n \to g^{-1}ng$ for $n \in N$ and $g \in G$.

In the next well known theorem concerning the simplicity of groups, (1) is useful for multiply transitive groups. (2) is useful for linear groups. As the corollary of (2), (3) is useful for A_5 and $\mathrm{PSL}(2, K)$, where K is a field with $|K| \geq 4$. In this theorem, it is unnecessary to assume Δ is finite and G is finite.

Theorem 3. *Let G be 2-transitive on a set Δ. Then we have*

(1) (see [7, p.22] and [8, p. 263]) *If G_α is simple and G has no regular normal subgroups $\neq \{1\}$, then G is simple.*

(2) (Iwasawa, 1941, see [8, p. 263]) *If $G = G'$ and G_α has a normal solvable subgroup H such that $G = \langle x^{-1}Hx \mid x \in G\rangle$, then G is simple.*

(3) (Corollary of (2)) *If $G = G'$ and $G_\alpha \neq \{1\}$ is solvable, then G is simple.*

Proof. Let $N \neq \{1\}$ be a normal subgroup of G.

(1) We have $G = G_\alpha N$ from Lemma 1 (2) and $G_\alpha \bigcap N \neq \{1\}$ since G has no regular normal subgroups. $G_\alpha \bigcap N \neq \{1\}$ is normal in G_α and so $G_\alpha = G_\alpha \bigcap N \subset N$ from the assumption. Hence we have $G = G_\alpha N = N$ because G is 2-transitive.

(2) HN is normal in G by $G = G_\alpha N$. Hence we have

$$G = \langle x^{-1}Hx \mid x \in G\rangle \subset HN \text{ and } G = HN$$

Thus we have a contradiction such that a non solvable group $(G/N)' = G/N = HN/N$ and a solvable group $H/H \cap N$ are isomorphic.

(3) We set $L = \langle G_\alpha \mid \alpha \in \Delta\rangle$. If $L = G_\beta$ for some $\beta \in \Delta$, then $L = G_\alpha$ for all $\alpha \in \Delta$ because these are conjugate and L is normal. Hence we have a contradiction $L = \bigcap_{\alpha\in\Delta} G_\alpha = \{1\}$. Since G_α is maximal from Lemma 1 (2), we have

$$L = \langle x^{-1}G_\alpha x \mid x \in G\rangle = G$$

Thus G is simple from (2).

Another proof. We have $G = G_\alpha N$ from Lemma 1 (2). G_α has a normal subgroup H such that G_α/H is abelian. Noting HN is normal in G, Hence $G/HN = G_\alpha N/HN$ is abelian because this is a homomorphic image of abelian group G_α/H. Thus $G = G' \subset HN$ and $G = HN$. H has a normal subgroup K such that H/K is abelian and $G/KN = HN/KN$ is abelian. Thus $G = G' \subset KN$ and $G = KN$. We continue this process and we have $G = N$.

The next (1) is trivial and is needless to prove. However it is very important to obtain all conjugate classes of the symmetric group S_n. If students don't know (1), then it needs much calculations to prove (2).

Remark 4. (1) $(k^\tau)^{\tau^{-1}\sigma\tau} = k^{\sigma\tau}$ *for* $k \in \Delta$, *namely, we have*

$$\tau^{-1}(i_1 i_2 \cdots i_r)(j_1 j_2 \cdots j_s)\cdots(k_1 k_2 \cdots k_t)\tau = (i_1^\tau i_2^\tau \cdots i_r^\tau)(j_1^\tau j_2^\tau \cdots j_s^\tau)\cdots(k_1^\tau k_2^\tau \cdots k_t^\tau)$$

and

$$\tau^{-1}\sigma\tau = \begin{pmatrix} 1^\tau & 2^\tau & \cdots & n^\tau \\ 1^{\sigma\tau} & 2^{\sigma\tau} & \cdots & n^{\sigma\tau} \end{pmatrix}.$$

(2) *Using the above, we have* $\tau^{-1}(12)(34)\tau = (1^\tau 2^\tau)(3^\tau 4^\tau)$ *for* $\sigma = (12)(34)$. *Thus subgroup* $V = \{(1), (12)(34), (13)(24), (14)(23)\}$ *is normal in the symmetric group* S_4 *of degree* 4.

The next are well known and appears in many text books for students. Note that product of permutation should be left hand in this paper because actions on Δ is right hand.

Remark 5. *We may write here* $1, 2, 3, 4, 5$ *instead of arbitrary* $k_1, k_2, k_3, k_4, k_5 \in \Delta$, *respectively, in* (2) *and* (3).

(1) $A_n (n \geq 3)$ *is (n-2)-transitive on* $\Delta = \{1, 2, \ldots, n\} = \{a_1, a_2, \ldots, a_n\}$ *since either* σ *or* $\tau = \sigma(a_{n-1}a_n)$ *is an even permutation for* $k^\sigma = a_k$ *for all* k.

(2) $A_n (n \geq 3)$ *is generated by 3-cycles in virtue of* $(12)(23) = (132)$ *and* $(12)(34) = (12)(23)(23)(34) = (132)(243)$.

(3) $A_n (n \geq 5)$ *is perfect, namely* $A_n = A_n'$ *by* (2) *and*

$$(123) = (23)(45)(123)\{(23)(45)\}^{-1}(123)^{-1}$$

2. Some proofs of simplicity of A_5

The simplicity of the alternative group A_5 is important for history of mathematics and education on students studying group theory and Galois theory. There are many proofs about this.

Method 1: A_5 is 3-transitive and generated by 3-cycles. Non trivial normal subgroup contains a 3-cycles.

Method 2: The numbers of elements in five conjugate classes are $1, 12, 12,$
$20, 15$ and any partial sums of these containing 1 is not a divisor of 60.

We shall give another two proofs using the above lemmas and theorem.

Theorem 6. *A_5 is simple.*

Proof 1. Stabilizer A_4 of 5 is solvable because A_4 has a normal subgroup $V = \{(1), (12)(34), (13)(24), (14)(23)\}$ such that A_4/V and V are abelian (see Remark 1 (2)). A_5 is perfect by Remark 2 (3) and 3-transitive by Remark 2 (1). Thus A_5 is simple by Theorem 1 (3).

Proof 2. Let $\{1\} \neq N$ be a normal subgroup of A_5.

If $5 \mid |N|$ then N contains all 5-cycles from Sylow theorem and so $|N| \geq 4! = 24$. If N is regular then $|N| = 5$ and so we have a contradiction from the above.

Thus N is not regular, namely, $M = A_4 \cap N \neq \{1\}$. Since A_5 and A_4 are 2-transitive, $A_5 = A_4N$ and $A_4 = A_3M$, and so $A_5 = A_4N = A_3MN = A_3N$. In case $A_3 \cap N = \{1\}$, we have $|N| = 20$ contradicts to the first statement in this proof. Hence $A_3 = A_3 \cap N \neq \{1\}$ from $|A_3| = 3$ and $A_5 = N$.

Theorem 7. *$A_n (n \geq 5)$ is simple.*

Proof. We may assume $n \geq 6$. Let $\{1\} \neq N$ be a normal subgroup of A_n. In case N is regular, $n = p^s$ from Lemma 2 (1) where p is prime, and A_{n-1} is a subgroup of $\mathrm{GL}(s, p)$ from Lemma 2 (2). Thus we have the next contradiction from $p^s = n > 4$.

$$\frac{(p^s-1)!}{2} = |A_{n-1}| \leq |\mathrm{GL}(s,p)| = \prod_{k=0}^{s-1}(p^s - p^k) < \frac{(p^s-1)!}{2}$$

Thus N is not regular, namely, $N \cap A_{n-1} \neq \{1\}$. We may assume inductively A_{n-1} is simple. Hence $A_{n-1} = A_{n-1} \cap N \subset N$ and so $A_n = A_{n-1}N = N$
(see also Theorem 1 (1)).

3. Transitive groups of prime degrees

We set $\Delta_T = \{\alpha \in \Delta \mid \alpha^t = \alpha \text{ for all } t \in T\}$ for a subset T of G. Considering G-set G for p-group G by conjugation, (1) in the next shows that the center G_G of p-group G is non trivial. (2) is also proved by elementary number theory or as the special case to cyclic group of order $p^e r$ in the following proof of Sylow theorem. However, the next proof is very simple.

Lemma 8. (1) $|\Delta| \equiv |\Delta_G| \bmod p$ *for a p-group G and G-set Δ.*
(2) $\binom{p^e r}{p^e} \equiv r \bmod p$ *for a prime p.*

Proof. (1) It follows from $|G| = |G_{\alpha_k}||\alpha_k^G|$ that

$$|\Delta| = |\Delta_G| + \sum_{|\alpha_k^G|>1} |\alpha_k^G| \equiv |\Delta_G| \bmod p.$$

(2) Compare coefficients of x^{p^e} in both sides of the next equation.

$$(x+1)^{p^e r} = (x^{p^e} + 1)^r \text{ in } \mathbb{F}_p[x].$$

The following is the proof of Sylow theorem by H. Wielandt. This is useful to the order of non trivial normal subgroup of a transitive group of a prime degree.

Theorem 9 (Sylow). *We set $|G| = p^e r$ with $(p, r) = 1$, and $n_p \geq 0$ is the number of distinct p-Sylow subgroups. Then $n_p \equiv 1 \bmod p$, in particular, there exists a p-Sylow subgroup, and a p-subgroup is contained in $t^{-1}St$ for $t \in G$ and a p-Sylow subgroup S. In particular, p-Sylow subgroups are mutually conjugate.*

Proof. We set $\Delta = \{S \subset G \mid |S| = p^e\}$. Then Δ is G-set by $S^g = Sg$ for $g \in G$. We also consider $S \in \Delta$ is $G_{\{S\}}$-set by $s^h = sh$ for $s \in S$ and $h \in G_{\{S\}}$. We can see that $G_{\{S\}}$ is a p-subgroup because $|s^{G_{\{S\}}}| = |sG_{\{S\}}| = |G_{\{S\}}|$ for all $s \in S$ and so $|G_{\{S\}}|$ is a divisor of $|S|$. Using $|G| = |G : G_{\{S\}}||G_{\{S\}}|$, we can see $G_{\{S\}}$ is a p-Sylow subgroup if and only if $p \not| |G : G_{\{S\}}|$. Hence we have

$$0 \not\equiv r \equiv \binom{p^e r}{p^e} = |\Delta| = \sum_{S \in \Delta} |G : G_{\{S\}}| \equiv n_p r \bmod p.$$

From this congruence, we have $n_p \equiv 1 \bmod p$.

Let H be a p-subgroup and let G/S be the set of right cosets of a p-Sylow subgroup S. G/S is H-set by $(Sg)^h = Sgh$.

$$0 \not\equiv r = |G/S| \equiv |(G/S)_H| \bmod p.$$

Hence $|(G/S)_H| \neq 0$ implies there exists St with $StH = St$ and so $tH \subset StH = St$.

In the next lemma, $|\mathcal{N}_G(P)| = pr$ is the foundation on the proof of simplicity of multiply transitive groups $A_5, M_{11}, M_{12}, M_{23}, M_{24}$.

Lemma 10. *Let p be a prime and let G be a transitive group on a set Δ, where $|\Delta| = p+s$ with $s < p$. We set $|G|/p \equiv r \bmod p$, where $0 < r < p$. Then for a p-Sylow subgroup P of G, we have*

$$\mathcal{C}_G(P) = P, \ r \mid p-1 \text{ and } |\mathcal{N}_G(P)| = pr.$$

The following lemma gives structure of normal subgroups in a transitive group of prime degree. The assertion $|G/G'| \mid r$ follows from Lemma 10.

Lemma 11 (5, p. 607). *Let G be a transitive group of odd prime degree p on a set Δ and let $G' \neq \{1\}$ be the commutator group of G. We set $|G|/p \equiv r \bmod p$, where $0 < r < p$. Then we have*

(1) *G' is contained in all non trivial normal subgroups.*
(2) *G/G' is cyclic, $|G/G'| \mid r$ and $r \mid p-1$.*

Corollary 12. (1) *Let G be transitive on a set Δ of a prime degree $p > 3$ and $|G|/p \equiv r \bmod p$, where $0 < r < p$. Then $r \mid p-1$.*
If N is a non trivial normal subgroup of G, then $|G|/r \mid |N|$.
If G be 3-transitive and $(r, \frac{|G|}{p-1}) = 1$, then G is simple.

(2) *Let G be 2-transitive on a set Δ of a degree $p+1$, where $p > 3$ is prime but not a Mersenne prime and $|G|/p \equiv r \bmod p$, where $0 < r < p$. Then $r \mid p-1$.*
If N is a non trivial normal subgroup of G, then $|G|/r \mid |N|$.
If G is 4-transitive and $(r, \frac{|G|}{p-1}) = 1$, then G is simple.

Example 13. (1) Simplicity of groups $A_5, M_{11}, M_{12}, M_{23}, M_{24}$ follows from Corollary 12, founded on Lemma 10, because A_5, M_{11}, M_{23} are 3-transitive and these orders are 60, $11 \cdot 10 \cdot 9 \cdot 8$, $23 \cdot 22 \cdot 21 \cdot 20 \cdot 48$, respectively and because M_{12}, M_{24} are 4-transitive and these orders are $12 \cdot |M_{11}|$, $24 \cdot |M_{23}|$, respectively (see [6, p.303], [7, p. 298] and [8, p. 292]).

(2) If M_{12} has a transitive extension $G = M_{13}$, then we set $p = 13$ and $\frac{|G|}{13} = 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8 \equiv (-1)^5 5! \equiv 10 \bmod 13$. Thus $r = 10$ is not a divisor of $12 = p - 1$. Hence there does not exists M_{13} (see [6, p. 302] and [8, p. 298]).

The next is well known and shows that transitive groups of odd prime degrees are closed to simple groups.

Theorem 14. *Let G be a transitive group of odd prime degree p on a set Δ and let G' be the commutator group of G. Then we have*

(1) *If $G' = 1$, then $|G| = p$.*
(2) (Galois) *If $G' \neq 1$ and $G'' = 1$, then G is an affine group over a prime field $\mathbb{F}_p$.*
(3) *If $G'' \neq 1$, then G' is simple. In particular, $G = G'$ implies G is simple.*

Proof. (1) We have $G = \mathcal{C}_G(P) = P$ from Lemma 10 (1).

(2) G' is transitive, abelian and of degree p. Hence $G' = P$ from (1) and P can be identified to the additive group $(\mathbb{F}_p, +)$ of $\mathbb{F}_p$. A subgroup $G_\alpha P$ has the order $p|G_\alpha| = |G|$ since $G_\alpha \cap P = P_\alpha = 1$. Hence $G = G_\alpha P$ Since $G' = P = \mathcal{C}_G(P)$, $G = \mathcal{N}_G(P)$, we have $G_\alpha \cong G/P$ is a cyclic subgroup of

$$\mathrm{Aut}((\mathbb{F}_p, +)) = \{x \to sx \mid s \in \mathbb{F}_p^*\}$$

and the action of G_α to P by conjugation is the same with the multiplication in $\mathbb{F}_p$.

(3) We have $G' = G''$ from $G \quad G'' \neq \{1\}$ and Lemma 11 (1). Let $H \neq \{1\}$ be normal in G'. Then $H \supset G'' = G'$ from Lemma 11 (1) since G' is transitive and of degree p.

4. Some comments to Feit-Thompson Conjecture

In this paper we shall give some comments to Feit-Thompson Conjecture (see below Conjectures 1 [2] and 2 [9]). For distinct primes p and q, we set

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

Conjecture 1. *A does not divide B for $A < B$ (see [2]).*

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]).

(1) in the next is fundamental to consider Conjecture 1 because of $B > A$ for $q > p \geq 2$.

(2) is very easy but it is slightly useful for using computer and a starting point for Conjecture 1. As a special case of (2), we may assume p and q are odd for Conjecture 1.

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

Comment 1. (1) $\dfrac{m^n-1}{m-1} > \dfrac{n^m-1}{n-1}$ *for integers* $n > m \geq 2$.
(2) *In case* $q \equiv 1 \bmod p$, *then* A *does not divide* B.
(3) *In case* $p = 3 < q$ *and* A *is composite, then* A *does not divide* B.
(4) *In case* $p = 3, 7 < q$ *and* $q \equiv 2$ *or* $4 \bmod 7$, *then* A *does not divide* B.

Conjecture 2. A *and* B *are relatively prime* (*see* [9]).

If a prime number r divides both A and B then $r = 2\lambda pq + 1$ for some integer λ (see Comment 3 (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 conjecture 1 unresolved (see [9]).

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).

Comment 2. *If* $p = 17$ *and* $q = 3313$, *then we have*
(1) (Stephens [9]) $(\Phi_p(q), \Phi_q(p)) = 2pq + 1$.
(2) $p^{\frac{q-1}{2}} \equiv 1 \bmod q$.
(3) $q^{\frac{p-1}{2}} \equiv 1 \bmod p^2$.

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

a	2	3	17	3313
$3 < p < 131077$	3511 ($p < 6 \times 10^9$)	11 ($p < 10^7$)	46021, 48947	7, 17

(1) and (2) in the next are not useful to the computer but may be useful to consider Conjectures. Here the notation $|c|_d$ means the order of $c \bmod d$ for natural numbers c and d with $(c, d) = 1$.

The conjecture 1 is now open in case $p \equiv 3 \bmod 4$ and $q \equiv 3 \bmod 4$ though there are another unsolved cases.

Comment 3. *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* $\Phi_p(q)$ *and* $\Phi_q(p)$. *Then the following hold.*
(1) $p = |q|_d$ *and* $q = |p|_d$.
(2) $a^p \equiv p$, $a^q \equiv q \bmod d$ *and* $pq = |a|_d$ *namely,* $\Phi_{pq}(a) \equiv 0 \bmod d$.
(3) $2pq \mid \varphi(d)$.
(4) *If* $p \equiv 3 \bmod 4$, *then* $d \equiv 1 \bmod 4$.
(5) *If* $p \equiv 3$ *and* $q \equiv 1 \bmod 4$, *then* A *does not divide* B.

References

[1] Apostol, T. M., *The Resultant of the Cyclotomic Polynomials* $F_m(ax)$ *and* $F_n(bx)$, Math. Comput. **29** (1975), 1-6.
[2] Feit, W. and Thompson, J. G., *A Solvability Criterion for Finite Groups and Some Consequences* , Proc. Nat. Acad. Sci. USA **48** (1962), 968-970.

[3] Feit, W. and Thompson, J. G., *A Solvability of Groups of odd order*, Pacific J. Math. **13** (1963), 775-1029.
[4] Guy, R. K., *Unsolved Problems in Number Theory,* 3rd ed., 2004, New York Springer.
[5] Huppert, B., *Endliche Gruppen I*, Grundlehren, **134** (1967), Springer.
[6] Huppert, B. and Blackburn, N., *Finite Groups III*, Grundlehren, **243** (1982), Springer.
[7] Passman, D. S., *Permutation Groups* , 1968, Benjamin.
[8] Rotman, J. J., *An Introduction to the Theory of Groups* , 4th ed., GTM **148**, 1994, Springer.
[9] Stephens, N. M., *On the Feit-Thompson Conjecture*, Math. Comput. **25** (1971), 625.

Emeritus Professor of Hirosaki University
Toriage 5-13-5, Hirosaki, 036-8171, Japan
E-mail address: moka.mocha_no_kaori@snow.ocn.ne.jp