On an inverse problem to Frobenius' theorem

JIANGTAO SHI

This is a joint work with Wei Meng

School of Mathematical Sciences, Peking University

E-mail: shijt@math.pku.edu.cn

Let G be a finite group and e a positive integer dividing $|G|$, the order of G.

Denoting $L_e(G) = \{x \in G \mid x^e = 1\}$.

Frobenius' Theorem (1895):

For every $e \mid |G|$, there exists a positive integer k such that $|L_e(G)| = ke$.

Inverse Problem to Frobenius' Theorem:

For a small positive integer k, give a complete classification of all finite groups G with $|L_e(G)| \leq ke$ for every $e \mid |G|$.

It is easy to prove that $|L_e(G)| = e$ for every $e \mid |G|$ if and only if G is a cyclic group.

In this talk, we give a complete classification of finite groups G with $|L_e(G)| \leq 2e$ for every $e \mid |G|$.

Lemma 1.1 Let G be a p-group of order p^n for a prime p. Then $|L_{p^i}(G)| \leq 2p^i$ $(0 \leq i \leq n)$ if and only if one of the following holds:

(1) G is a cyclic group;

(2) $G \cong Z_{2^{n-1}} \times Z_2$, where $n \geq 2$;

(3) $G \cong Q_8$;

(4) $G \cong \langle a,\, b \mid a^{2^{n-1}} = b^2 = 1,\, b^{-1}ab = a^{1+2^{n-2}} \rangle$, where $n \geq 4$.

Lemma 1.2 Let G be a finite group whose order has at least two distinct prime divisors and e a positive integer dividing $|G|$. Then $|L_e(G)| \leq 2e$ if and only if one of the following holds:

(1) G is a cyclic group;

(2) $G \cong Z_m \times T$, where $m > 1$ is an odd integer and $T \cong Z_{2^{n-1}} \times Z_2\, (n \geq 2)$ or Q_8 or $\langle a,\, b \mid a^{2^{t-1}} = b^2 = 1,\, b^{-1}ab = a^{1+2^{t-2}} \rangle\, (t \geq 4)$;

(3) $G \cong Z_m \times T$, where $T \cong \langle a,\, b \mid\ a^3 = b^{2^n} = 1,\, b^{-1}ab = a^{-1} \rangle$, $n \geq 1$ and $(m,\, 6) = 1$.

By Lemmas 1.1 and 1.2, our main result is as follows:

Theorem 1.3 Let G be a finite group and e a positive integer dividing $|G|$. Then $|L_e(G)| \leq 2e$ for every $e \mid |G|$ if and only if one of the following statements holds:

(1) G is a cyclic group;

(2) $G \cong Z_m \times T$, where $m \geq 1$ is an odd integer and $T \cong Z_{2^{n-1}} \times Z_2\,(n \geq 2)$ or Q_8 or $\langle a,\, b \mid a^{2^{t-1}} = b^2 = 1,\, b^{-1}ab = a^{1+2^{t-2}} \rangle\,(t \geq 4)$;

(3) $G \cong Z_m \times T$, where $T \cong \langle a,\, b \mid\ a^3 = b^{2^n} = 1,\, b^{-1}ab = a^{-1} \rangle$, $n \geq 1$ and $(m,\, 6) = 1$.

Corollary 1.4 Let G be a finite group and e a positive integer dividing $|G|$. Then $|L_e(G)| = 2e$ for every proper divisor e of $|G|$ if and only if G is isomorphic to one of the following groups:

(1) $G \cong Z_{2^{n-1}} \times Z_2$, where $n \geq 2$;

(2) $G \cong \langle a,\, b \mid a^{2^{n-1}} = b^2 = 1,\, b^{-1}ab = a^{1+2^{n-2}} \rangle$, where $n \geq 4$.

Corollary 1.5 Let G be a finite group of odd order and e a positive integer dividing $|G|$. Then $|L_e(G)| \leq 2e$ for every $e \mid |G|$ if and only if G is a cyclic group.

Corollary 1.5' Let G be a finite group of odd order and e a positive integer dividing $|G|$. If $|L_e(G)| \leq 2e$ for every $e \mid |G|$, then $|L_e(G)| = e$ for every $e \mid |G|$.

The classification of finite groups G with $|L_e(G)| \leq 3e$ for every $e \mid |G|$, is almost finished by W. Meng and J.T. Shi.

Problem 1 When $k = 4, 5, 6, \ldots$, give a complete classification of finite groups G with $|L_e(G)| \leq ke$ for every $e \mid |G|$.

Is there an upper bound for k such that a finite group G is solvable if $|L_e(G)| \leq ke$ for every $e \mid |G|$?

Theorem 1.6 Let G be a finite group. If $|L_e(G)| \leq 7e$ for every $e \mid |G|$, then G is solvable.

The alternating group A_5 of degree 5 shows that a finite group G with $|L_e(G)| \leq 8e$ for every $e \mid |G|$ may be non-solvable.

Problem 2 Classify finite non-solvable groups G with $|L_e(G)| \leq 8e$ for every $e \mid |G|$.

Proposition 1.7 Let G be a characteristically simple group. If $|L_e(G)| \leq 8e$ for every $e \mid |G|$, then $G \cong A_5$.

Problem 3 For any positive integer k, does there always exist a finite group G such that $|L_e(G)| = ke$ for some $e \mid |G|$?

Problem 4 Denoting $\mathcal{K} = \{k \mid |L_e(G)| = ke \text{ for some } e \mid |G|\}$.

(1) If $\mathcal{K} = \{1, m\}$ consists of two distinct positive integers, what can we say about G?

(2) If $\mathcal{K} = \{1, 2, 3, \ldots, n\}$ consists of continuous positive integers, is there an upper bound for n?

Thank you!