Japan. J. Math. 5, 183–189 (2010)
DOI: 10.1007/s11537-010-1023-9

JAPANESE JOURNAL OF MATHEMATICS
SINCE 1924

Generalizations of Arnold's version of Euler's theorem for matrices

Marcin Mazur · Bogdan V. Petrenko

Received: 2 July 2010 / Revised: 21 July 2010 / Accepted: 30 July 2010
Published online: 25 December 2010

Communicated by: Takeshi Saito

To the memory of Vladimir Igorevich Arnold (1937–2010),
for his vision and inspiration.

Abstract. A recent result, conjectured by Arnold and proved by Zarelua, states that for a prime number p, a positive integer k, and a square matrix A with integral entries one has $\mathrm{tr}(A^{p^k}) \equiv \mathrm{tr}(A^{p^{k-1}}) \pmod{p^k}$. We give a short proof of a more general result, which states that if the characteristic polynomials of two integral matrices A, B are congruent modulo p^k then the characteristic polynomials of A^p and B^p are congruent modulo p^{k+1}, and then we show that Arnold's conjecture follows from it easily. Using this result, we prove the following generalization of Euler's theorem for any 2×2 integral matrix A: the characteristic polynomials of $A^{\Phi(n)}$ and $A^{\Phi(n)-\phi(n)}$ are congruent modulo n. Here ϕ is the Euler function, $\prod_{i=1}^{l} p_i^{\alpha_i}$ is a prime factorization of n and $\Phi(n) = (\phi(n) + \prod_{i=1}^{l} p_i^{\alpha_i - 1}(p_i + 1))/2$.

Keywords and phrases: Euler congruences, Euler's theorem, Fermat's little theorem, congruences for traces

Mathematics Subject Classification (2010): 05A10, 11A07, 11C20

M. MAZUR
Department of Mathematics, Binghamton University, P.O. Box 6000, Binghamton, NY 13892-6000, USA
(e-mail: mazur@math.binghamton.edu)

B.V. PETRENKO
Department of Mathematics, SUNY Brockport, 350 New Campus Drive, Brockport, NY 14420, USA
(e-mail: bpetrenk@brockport.edu)