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: ?????

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)

1. Introduction

In a series of papers [1]–[8] Arnold investigated dynamical aspects of the arithmetic modulo n. In particular, he observed many congruences for traces of powers of an integral matrix and he considered them as generalizations of Fermat's little theorem and Euler's theorem. It is remarkable that Arnold arrived at these congruences in an experimental way typical in natural sciences (but also fundamental in mathematics of Wallis, Newton, and many others) by gathering extensive experimental data and extrapolating from it general results. His most striking discovery is perhaps the following congruence:

$$\operatorname{tr}(A^{p^n}) \equiv \operatorname{tr}(A^{p^{n-1}}) \pmod{p^n}, \tag{1}$$

where p is a prime and n is a positive integer. Arnold proved (1) for $n = 1, 2, 3$ and conjectured it in general. Arnold's conjecture was subsequently proved by Zarelua [13] and Vinberg [12], and in fact this result can be found already in papers by Jänichen [9] and Schur [11]. For an excellent exposition of the history of these questions and some applications to topology and dynamics we refer to a recent paper by Zarelua [14].

In the present note we give a surprisingly simple proof of a more general result contained in the following theorem:

Theorem 1.1. *Let $A, B \in \mathrm{M}_n(\mathbb{Z})$, and let p be a prime and k a positive integer.*

(i) If the characteristic polynomials of A and B are congruent modulo p^k, then the characteristic polynomials of A^p and B^p are congruent modulo p^{k+1}.

(ii) The characteristic polynomials of A^{p^k} and $A^{p^{k-1}}$ are congruent modulo p^k.

As (ii) is essentially Arnold's extension of Euler's theorem, part (i) should be thought of as a generalization of the following simple but very useful fact in elementary number theory: if a, b are integers such that $a \equiv b \pmod{p^k}$ then $a^p \equiv b^p \pmod{p^{k+1}}$.

As another generalization of Euler's theorem to matrices Arnold suggested the following congruence:

$$\operatorname{tr}(A^n) \equiv \operatorname{tr}(A^{n-\phi(n)}) \pmod{n},$$

where A is an integral matrix, n a positive integer and ϕ is the Euler's function. Unfortunately, Arnold himself pointed out that this is false already for $n = 6$ and some 2×2 integral matrices. On the other hand, it is an old but relatively unknown result that (1) for all prime powers implies that

$$\sum_{d|n} \mu\Big(\frac{n}{d}\Big)\operatorname{tr}(A^d) \equiv 0 \pmod{n},$$

where μ is the Möbius function (just prove it separately modulo each prime power in n by pairing the summands appropriately to apply (1)). See [14] for more about the history of this congruence. In the last section of this note we use Theorem 1.1 to prove a different extension of Euler's theorem, much closer in spirit to Arnold's attempt, but only for 2×2 integral matrices. To formulate this result consider a positive integer $n > 1$, whose prime factorization is $n = \prod_{i=1}^{l} p_i^{\alpha_i}$, and define $\Phi(n)$ by

$$\Phi(n) = \frac{1}{2}\Big(\phi(n) + \prod_{i=1}^{l} p_i^{\alpha_i - 1}(p_i + 1)\Big),$$

where ϕ is the Euler function. Note that $\Phi(n) = n$ if n is a prime power and $\Phi(n) > n$ otherwise.

Theorem 1.2. *Let $n > 1$ be a positive integer and let $A \in \mathrm{M}_2(\mathbb{Z})$. Then the characteristic polynomials of $A^{\Phi(n)}$ and $A^{\Phi(n)-\phi(n)}$ are congruent modulo n.*

Note that Euler's theorem is indeed a simple consequence of Theorem 1.2 applied to matrices of the form $\left(\begin{smallmatrix} a & 0 \\ 0 & 0 \end{smallmatrix}\right)$.

2. Main result

Lemma 2.1. *Let p be a prime and n a positive integer. For any symmetric polynomial $f \in \mathbb{Z}[x_1, \ldots, x_n]$ there exists a symmetric polynomial $h \in \mathbb{Z}[x_1, \ldots, x_n]$ such that*

$$f(x_1^p, x_2^p, \ldots, x_n^p) = f(x_1, \ldots, x_n)^p + ph(x_1, \ldots, x_n).$$

Proof. The polynomial $f(x_1^p, x_2^p, \ldots, x_n^p) - f(x_1, \ldots, x_n)^p$ is symmetric, has integer coefficients, and its reduction modulo p is 0. □

Let $s_i = s_i(x_1, \ldots, x_n)$ be the i-th elementary symmetric polynomial (see Section 6 of Chapter IV in [10] for basic facts about symmetric polynomials). The fundamental theorem about symmetric polynomials [10, Theorem IV.6.1] implies that for every positive integer m there exist unique polynomials $T_{m,i} \in \mathbb{Z}[x_1, \ldots, x_n]$, $i = 1, 2, \ldots, n$, such that

$$s_i(x_1^m, \ldots, x_n^m) = T_{m,i}(s_1(x_1, \ldots, x_n), \ldots, s_n(x_1, \ldots, x_n))$$

for $i = 1, \ldots, n$. Lemma 2.1 yields the following corollary:

Corollary 2.2. *Let p be a prime. Then $T_{p,i}(x_1, \ldots, x_n) \equiv x_i^p \pmod{p}$ for $i = 1, 2, \ldots, n$.*

The following lemma was suggested to us by Takeshi Saito.

Lemma 2.3. *Let p be a prime. The polynomials $T_{p,i}(x_1 + y_1, \ldots, x_n + y_n) \in \mathbb{Z}[x_1, \ldots, x_n, y_1, \ldots, y_n]$, $i = 1, \ldots, n$, satisfy*

$$T_{p,i}(x_1 + y_1, \ldots, x_n + y_n) \equiv T_{p,i}(x_1, \ldots, x_n) \pmod{pI + I^2},$$

where I is the ideal $(y_1, \ldots, y_n)$.

Proof. The Taylor expansion yields

$$\begin{aligned} &T_{p,i}(x_1 + y_1, \ldots, x_n + y_n) \\ &\equiv T_{p,i}(x_1, \ldots, x_n) + \sum_{j=1}^{n} \frac{\partial}{\partial x_j} T_{p,i}(x_1, \ldots, x_n) y_j \pmod{I^2}. \end{aligned}$$

The lemma follows now immediately from the congruences

$$\frac{\partial}{\partial x_j} T_{p,i}(x_1, \ldots, x_n) \equiv 0 \pmod{p},$$

which hold for every $i, j = 1, \ldots, n$ by Corollary 2.2. □

Consider now a commutative ring S. For a monic polynomial $f = x^n + \sum_{i=1}^{n} (-1)^i a_i x^{n-i}$ of degree n in $S[x]$ and a positive integer m define the polynomial $T_m(f)$ by

$$T_m(f) = x^n + \sum_{i=1}^{n} (-1)^i T_{m,i}(a_1, \ldots, a_n) x^{n-i}.$$

It follows directly from the definition of the polynomials $T_{m,i}$ that if $f(x) = (x - u_1) \cdots (x - u_n)$ then $T_m(f) = (x - u_1^m) \cdots (x - u_n^m)$. This implies that if f is the characteristic polynomial of a matrix $A \in \mathrm{M}_n(S)$ then $T_m(f)$ is the characteristic polynomial of A^m (this is clear when S is a domain and in general follows from the functorial properties of characteristic polynomials).

Remark 2.4. Takeshi Saito pointed out the following natural construction of the operations T_m. The ring $S[x]$ can be considered as an algebra over itself via the substitution homomorphism $x \mapsto x^m$. This makes $S[x]$ a free $S[x]$ module of rank m and therefore the norm $N_m : S[x] \longrightarrow S[x]$ is defined in the usual way ($N_m(f)$ is the determinant of multiplication by f). It is multiplicative ($N_m(fg) = N_m(f) N_m(g)$) and satisfies $N_m(ax - b) = (-1)^{m-1}(a^m x - b^m)$. In fact, these two properties and functoriality with respect to change of the coefficient ring characterize N_m. It follows that $N_m(f) = (-1)^{n(m-1)} T_m(f)$ for any monic polynomial f of degree n.

An immediate corollary of Lemma 2.3 is the following theorem:

Theorem 2.5. *Let p be a prime, S a commutative ring and I and ideal of S. If $f, g \in S[x]$ are monic polynomials of the same degree such that $f \equiv g \pmod{I}$ then $T_p(f) \equiv T_p(g) \pmod{pI + I^2}$. In particular, for any positive integer k, and any monic polynomials $f, g \in \mathbb{Z}[x]$ such that $f \equiv g \pmod{p^k}$ we have $T_p(f) \equiv T_p(g) \pmod{p^{k+1}}$.*

Proposition 2.6. *Let p be a prime and $f \in \mathbb{Z}[x]$ a monic polynomial of degree n. Then $T_p(f) \equiv f \pmod{p}$.*

Proof. Corollary 2.2 and Fermat's little theorem yield

$$T_{p,i}(a_1, \ldots, a_n) \equiv a_i^p \equiv a_i \pmod{p}$$

for $i = 1, \ldots, n$ and any integers $a_1, \ldots, a_n$. □

We are ready to prove our main result.

Proof of Theorem 1.1. Let f and g be the characteristic polynomials of A and B respectively. Then the characteristic polynomials of A^p and B^p are $T_p(f)$ and $T_p(g)$. Thus (i) follows from Theorem 2.5 and (ii) follows from Proposition 2.6 when $k = 1$ and from (i) and obvious induction in general. □

3. An analog of Euler's theorem for $\mathrm{M}_2(\mathbb{Z})$

If q is a power of a prime, we denote by $\mathbb{F}_q$ a finite field with q elements.

Lemma 3.1. *Let p be a prime. The following conditions for positive integers a, b are equivalent:*

(i) A^a and A^b have the same characteristic polynomial for any $A \in \mathrm{M}_2(\mathbb{F}_p)$.
(ii) $\mathrm{tr}(A^a) = \mathrm{tr}(A^b)$ for any $A \in \mathrm{M}_2(\mathbb{F}_p)$.
(iii) Either $(p^2 - 1)|(a - b)$ or $(p^2 - 1)|(pa - b)$.

Proof. It is clear that (i) implies (ii). Suppose that (ii) holds. Taking for A the matrix $\left(\begin{smallmatrix} u & 0 \\ 0 & 0 \end{smallmatrix}\right)$, where u is a generator of the multiplicative group $\mathbb{F}_p^\times$, we see that $u^a = u^b$, hence $(p-1)|(a-b)$. Let w be a generator of the multiplicative group $\mathbb{F}_{p^2}^\times$ and let $x^2 - sx + t$ be the minimal polynomial of w over $\mathbb{F}_p$. The matrix $A = \left(\begin{smallmatrix} 0 & -t \\ 1 & s \end{smallmatrix}\right)$ has eigenvalues w and w^p. It follows that $w^a + w^{pa} = w^b + w^{pb}$. Since $(p-1)|(a-b)$, we also have $w^a w^{pa} = t^a = t^b = w^b w^{pb}$. This implies that either $w^a = w^b$ or $w^{pa} = w^b$. In the former case we have $(p^2-1)|(a-b)$ and in the latter case we have $(p^2 - 1)|(pa - b)$. Thus (ii) implies (iii).

Suppose now that (iii) holds. Then $(p-1)|(a-b)$. It follows that A^a and A^b have the same determinant for any $A \in \mathrm{M}_2(\mathbb{F}_p)$. Let $A \in \mathrm{M}_2(\mathbb{F}_p)$. It suffices to show that A^a and A^b have equal traces. Let $u, w \in \mathbb{F}_{p^2}$ be the eigenvalues

of A. If one of u, w is in $\mathbb{F}_p$, then both are in $\mathbb{F}_p$. It follows that $u^a = u^b$ and $w^a = w^b$, hence A^a and A^b have equal traces. If neither one of u, w is in $\mathbb{F}_p$, then $w = u^p$ and $u^{p^2-1} = 1$. If $(p^2-1)|(a-b)$ then $u^a = u^b$ and $w^a = w^b$ so again A^a and A^b have equal traces. Finally, if $(p^2-1)|(pa-b)$ then $u^a = w^b$ and $w^a = u^b$ hence $\mathrm{tr}(A^a) = \mathrm{tr}(A^b)$. □

Corollary 3.2. *Let p be a prime. If a, b are positive integers such that $(p+1)|(a+b)$, $(p-1)|(a-b)$, and the numbers $(a+b)/(p+1)$ and $(a-b)/(p-1)$ are of the same parity, then A^a and A^b have equal characteristic polynomials for any $A \in \mathrm{M}_2(\mathbb{F}_p)$.*

Proof. Since

$$pa - b = (p^2-1)\Big(\frac{a+b}{2(p+1)} + \frac{a-b}{2(p-1)}\Big),$$

the result follows from Lemma 3.1. □

Proof of Theorem 1.2. Let $n = \prod_{i=1}^{l} p_i^{\alpha_i}$ be a prime power factorization of n. Fix $j \in \{1, 2, \ldots, l\}$ and set $a = \frac{1}{2}\prod_{i\neq j} p_i^{\alpha_i-1}(\prod_{i=1}^{l}(p_i+1)+\prod_{i=1}^{l}(p_i-1))$ and $b = \frac{1}{2}\prod_{i\neq j} p_i^{\alpha_i-1}(\prod_{i=1}^{l}(p_i+1)-\prod_{i=1}^{l}(p_i-1))$. Note that the numbers a, b satisfy the assumptions of Corollary 3.2 for the prime $p = p_j$. It follows from Corollary 3.2 that for any matrix $A \in \mathrm{M}_2(\mathbb{Z})$ the characteristic polynomials of the matrices A^a and A^b are congruent modulo p_j. Theorem 1.1(i) implies now that the characteristic polynomials of $A^{p^{\alpha_j-1}a}$ and $A^{p^{\alpha_j-1}b}$ are congruent modulo $p_j^{\alpha_j}$. Since $p^{\alpha_j-1}a = \Phi(n)$ and $p^{\alpha_j-1}b = \Phi(n) - \phi(n)$, we see that for each j the characteristic polynomials of the matrices $A^{\Phi(n)}$ and $A^{\Phi(n)-\phi(n)}$ are congruent modulo $p_j^{\alpha_j}$. □

A straightforward modification of the proof of Theorem 1.2 yields the following result.

Theorem 3.3. *For $n = \prod_{i=1}^{l} p_i^{\alpha_i}$ define $u = \mathrm{lcm}\{p_i^{\alpha_i-1}(p_i+1) : 1 \le i \le l\}$ and $w = \mathrm{lcm}\{p_i^{\alpha_i-1}(p_i-1) : 1 \le i \le l\}$ (here* lcm *stands for the least common multiple). Let s and t be positive integers such that $su > tw$. Then, for any $A \in \mathrm{M}_2(\mathbb{Z})$, the characteristic polynomials of the matrices A^{su+tw} and A^{su-tw} are congruent modulo n. If, in addition, for each $i \in \{1, \ldots, l\}$ the numbers $su/p_i^{\alpha_i-1}(p_i+1)$ and $tw/p_i^{\alpha_i-1}(p_i-1)$ have the same parity, then the characteristic polynomials of the matrices $A^{(su+tw)/2}$ and $A^{(su-tw)/2}$ are congruent modulo n.*

Acknowledgements. We are grateful to Takeshi Saito for his suggestions which not only shortened our original proof of Theorem 1.1 but also made the argument aesthetically more pleasing and more conceptual. We thank Hendrik W. Lenstra for pointing out an error in an earlier version of Theorem 3.3.

References

[1] V.I. Arnold, Fermat–Euler dynamical systems and the statistics of arithmetics of geometric progressions, Funct. Anal. Appl., **37** (2003), 1–15.

[2] V.I. Arnold, The topology of algebra: Combinatorics of squaring, Funct. Anal. Appl., **37** (2003), 177–190.

[3] V.I. Arnold, Topology and statistics of formulae of arithmetics, Russian Math. Surveys, **58** (2003), 637–664.

[4] V.I. Arnold, Fermat dynamics, matrix arithmetics, finite circles, and finite Lobachevsky planes, Funct. Anal. Appl., **38** (2004), 1–13.

[5] V.I. Arnold, The matrix Euler–Fermat theorem, Izv. Math., **68** (2004), 1119–1128.

[6] V.I. Arnold, Geometry and dynamics of Galois fields, Russian Math. Surveys, **59** (2004), 1029–1046.

[7] V.I. Arnold, Ergodic and arithmetical properties of geometrical progression's dynamics and of its orbits, Mosc. Math. J., **5** (2005), 5–22.

[8] V.I. Arnold, On the matricial version of Fermat–Euler congruences, Jpn. J. Math., **1** (2006), 1–24.

[9] W. Jänichen, Über die Verallgemeinerung einer Gaussschen Formel aus der Theorie der höhern Kongruenzen, Sitzungsber. Berlin. Math. Ges., **20** (1921), 23–29.

[10] S. Lang, Algebra, Grad. Texts in Math., **211**, Springer-Verlag, 2002.

[11] I. Schur, Arithmetische Eigenschaften der Potenzsummen einer algebraischen Gleichung, Compos. Math., **4** (1937), 432–444.

[12] E.B. Vinberg, On some number-theoretic conjectures of V. Arnold, Jpn. J. Math., **2** (2007), 297–302.

[13] A.V. Zarelua, On matrix analogs of Fermat's little theorem, Math. Notes, **79** (2006), 783–796.

[14] A.V. Zarelua, On congruences for the traces of powers of some matrices, Proc. Steklov Inst. Math., **263** (2008), 78–98.