Funct. Anal. Other Math. (2009) 2: 249–250
DOI 10.1007/s11853-008-0026-z

FAOM

Extended Euler congruence

Pierre Deligne

Received: 6 September 2007 / Accepted: 2 October 2007 / Published online: 29 November 2008

Abstract The matricial Euler congruence $\mathrm{Tr}(A^{p^n}) \equiv \mathrm{Tr}(A^{p^{n-1}})$ modulo p^n, previously announced in Arnold, Japanese J. Math. 1(1), 1–24, 2006 for $A \in M_N(\mathbb{Z})$, is given a proof based on extending it to the ring of Witt vectors of length n.

Keywords Euler congruence · Witt vector

Mathematics Subject Classification (2000) 11A07 · 05B20 · 13K05

The matricial Euler congruence

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

which was announced in [1] for $A \in M_N(\mathbb{Z})$, can be extended as follows. We replace $\mathbb{Z}$ with $\mathbb{Z}/p^n\mathbb{Z}$ and consider $\mathbb{Z}/p^n\mathbb{Z}$ as being $W_n(\mathbb{F}_p)$ (the ring of Witt vectors of length n). As geometers, we dislike considering the case of the field $\mathbb{F}_p$ alone: the main part of the following proof depends on the discovery of an extension to the case of $W_n(R)$, where R is of characteristic p.

Proposition *Let R be an $\mathbb{F}_p$ algebra (commutative with unity). The endomorphism $F: x \mapsto x^p$ of R defines by functoriality an endomorphism F of $W_n(R)$. For A in $M_N(W_n(R))$, the equality*

$$\mathrm{Tr}(A^{p^n}) = F(\mathrm{Tr}(A^{p^{n-1}})) \tag{2}$$

holds in $W_n(R)$.

Proof It suffices to consider the universal case, where R is the ring of the polynomials of N^2n variables $X^i_j(k)$ over $\mathbb{F}_p$ and A^i_j is the Witt vector whose components are $X^i_j(k)$. We

P. Deligne (✉)
School of Mathematics, Institute for Advance Studies, Einstein Drive, Princeton, NJ 08540, USA
e-mail: deligne@math.ias.edu

must prove a polynomial identity in these variables. It suffices to prove it in $W_n(R(1/D))$, where D is the discriminant of the characteristic polynomial of $\left(X^i_j(0)\right)$. If k is an algebraically closed field containing $R[1/D]$, it suffices to prove (2) in $W_n(k)$: we may and shall assume that $R = k$ is algebraically closed and that the image of A in $M_N(k)$ is a matrix with distinct eigenvalues.

To simplify, we may also suppose that the image of A in $M_N(k)$ is invertible. In this case, the matrix A is conjugate to a diagonal matrix. It remains to prove that for $a_i \in W_n(k)^*$ $(1 \le i \le n)$, we have

$$\sum a_i^{p^n} = F\left(\sum a_i^{p^{n-1}}\right) \quad \left(= \sum F\left(a_i^{p^{n-1}}\right)\right).$$

As F is an endomorphism, the task is thus reduced to the case $N = 1$.

It remains to show that for $a \in W_n(k)$, the element $a^{p^{n-1}}$ is a multiplicative representative (i.e., a Witt vector of the form $(\lambda, 0, 0, \ldots, 0)$). Indeed, F acts on a multiplicative representative by raising it to the p-th power.

Writing $a = \alpha u$, where α is a multiplicative representative and $u \to 1$ in k, we must prove that $u^{p^{n-1}} = 1$.

The ring $W(k)$ of the Witt vectors is a complete discrete valuation ring with residue field k and maximal ideal p, and $W_n(k)$ is its quotient by p^n. We have

$$u \equiv 1 \pmod{p},$$

whence $u^{p^a} \equiv 1 \ (p^{a+1})$ follows inductively, as can be seen from the development of $(1 + p^{a-1}x)^p$.

And, finally, (1) follows from (2) because F is the identity of $\mathbb{F}_p$. □

References

1. Arnold VI (2006) On the matricial version of Fermat–Euler congruences. Japanese J Math 1(1):1–24. Publisher's erratum 1(2):469