Canad. Math. Bull. Vol. **43** (2), 2000 pp. 236–238

On a Question of Buium

José Felipe Voloch

Abstract. We prove that $\{(n^p - n)/p\}_p \in \prod_p \mathbf{F}_p$, with p ranging over all primes, is independent of 1 over the integers, assuming a conjecture in elementary number theory generalizing the infinitude of Mersenne primes. This answers a question of Buium. We also prove a generalization.

For an integer n and a prime p, the quantity $\delta_p(n) = (n^p - n)/p (\mathrm{mod}\ p)$, has been considered classically. In fact $\delta_p(n)/n$, when p does not divide n, is known as the Fermat quotient. Recently this quantity has been reconsidered as part of the quest for finding a substitute, in the number field case, for the derivations in the function field case (see [B1,2], [I], [Sm]), since it satisfies the Leibniz rule, that is $\delta_p(mn) = m\delta_p(n) + n\delta_p(m)$.

Let R be the ring $\prod_p \mathbf{F}_p$, where the product is taken over all primes, then R is a ring of characteristic zero (not a domain) and the integers $\mathbf{Z}$ sit in R. Also, given an integer n, $\delta(n) = \big(\delta_p(n)\big)_p$ is an element of R. Buium asked the following question: decide if $\delta(n)$ is in $\mathbf{Z}$ for all n. Clearly $\delta(n) = 0, n = 0, 1$ and $2\delta(-1) = 0$. If there are infinitely many Mersenne primes we will show that $1, \delta(2)$ are linearly independent over $\mathbf{Z}$. Assuming a generalization of this conjecture, we will prove more. Namely, if $n_1, \ldots, n_r$ are multiplicatively independent integers then $1, \delta(n_1), \ldots, \delta(n_r)$ are linearly independent over $\mathbf{Z}$.

Consider the following statements:

(A) If $m > n \geq 1$ are coprime integers, such that m/n is not a perfect power, then there are infinitely many primes of the form $(m^l - n^l)/(m - n)$.

(B) If $m, n \neq 0$ are integers, $m/n \neq \pm 1$, then $1, m\delta(n) - n\delta(m)$ are linearly independent over $\mathbf{Z}$.

(C) If $n_1, \ldots, n_r$ are multiplicatively independent non-zero integers then $1, \delta(n_1), \ldots, \delta(n_r)$ are linearly independent over $\mathbf{Z}$.

The statement (A), at least when $n = 1$, is a well-known open problem in elementary number theory and it is widely believed to be true, although no cases of it has been proved. The special case $m = 2, n = 1$ corresponds to Mersenne primes and there there is ample numerical evidence. The case $m = 10$, $n = 1$ corresponds to the so-called repunits and there there is also some numerical evidence. The statement (B), with $n = 1$, is an answer to Buium's question, while (C) generalizes (B). We prove:

Theorem *(A) implies (B) and (B) implies (C).*

Proof Assume m, n are integers as in (A) and assume (A) holds. Let $p = (m^l - n^l)/(m - n)$ be prime. Then $m^l = n^l + p(m - n)$. If l does not divide $p - 1$, then $x \mapsto x^l$ is a bijection in $\mathbf{Z}/p$ and from $m^l \equiv n^l (\mathrm{mod}\ p)$, we conclude that $p | (m - n)$ which will be false for p large.

Received by the editors April 8, 1998; revised August 11, 1998.
AMS subject classification: 11A07.

https://doi.org/10.4153/CMB-2000-031-6 Published online by Cambridge University Press

Assume that is not the case, so that $l|(p-1)$. Then

$$m^{p-1} = \left(n^l + p(m-n)\right)^{(p-1)/l} \equiv n^{p-1} - \frac{(m-n)p}{ln^l} (\text{mod } p^2).$$

Thus,

$$n\delta_p(m) - m\delta_p(n) \equiv -\frac{(m-n)nm}{ln^l} (\text{mod } p).$$

If (B) is false, there exists a, b integers not both zero with $a\big(n\delta(m) - m\delta(n)\big) + b = 0$ so, for p as above we get $aln^l - bnm(m-n) \equiv 0 (\text{mod } p)$. For p going to infinity of the form $(m^l - n^l)/(m-n)$ we have $ln^l = o(p)$, since $m > n$. So, for p large, the last congruence implies that $aln^l - bmn(m-n) = 0$, but that bounds l and therefore p, unless $a = 0$. But in this case, the last congruence reads $bmn(m-n) \equiv 0 (\text{mod } p)$, which also bounds p. As (A) implies that p cannot be bounded, we conclude that (A) implies (B) if m, n are integers as in (A).

Suppose now that $m, n \neq 0$ are arbitrary integers and $a\big(n\delta(m) - m\delta(n)\big) + b = 0$ for some a, b. If m, n are not coprime and $m = dm'$, $n = dn'$, m', n' coprime, then $0 = a\big(n\delta(m) - m\delta(n)\big) + b = ad^2\big(n'\delta(m') - m'\delta(n')\big) + b$, which reduces (B) to the case m, n coprime. If $m = m_1^r, n = n_1^r$, then $0 = a\big(n\delta(m) - m\delta(n)\big) + b = r(n_1 m_1)^{r-1}\big(n_1\delta(m_1) - m_1\delta(n_1)\big) + b$, which reduces (B) to the case m/n is not a perfect power, so (A) implies (B) in general.

If $\sum a_i\delta(m_i) = b$ assume, replacing m_i by $-m_i$ and a_i by $-a_i$ if necessary, that the m_i are all positive. Let

$$m = \prod_{a_i > 0} m_i^{a_i m_i}, \quad n = \prod_{a_i < 0} m_i^{-a_i m_i}$$

then

$$\delta(m) = \sum_{a_i > 0} a_i m \delta(m_i), \quad \delta(n) = \sum_{a_i < 0} -a_i n \delta(m_i).$$

Therefore $n\delta(m) - m\delta(n) = mn \sum a_i \delta(m_i) = mnb$, thus by (B) we conclude that $m/n = \pm 1$ and therefore the m_i's are multiplicatively dependent. So (B) implies (C).

Remarks (i) Note that to prove (B) for a given pair m, n satisfying the hypotheses of (A) we only need (A) for the same pair m, n.

(ii) Some of the calculations in the proof that (A) implies (B) generalize some results of Johnson [J].

(iii) The fact that $b\delta(2) \neq 0$ for all $b \in \mathbf{Z}$, $b \neq 0$ is equivalent to there being infinitely many primes p with $2^p \not\equiv 2 (\text{mod } p^2)$, which is an open problem and indicates that (B) is likely to be out of reach of present techniques. However, one could get by with something weaker than (A) when $n = 1$, namely that $(m^l - 1)/(m-1)$ has a large prime factor for infinitely many l.

(iv) One may conjecture that, under the hypotheses of (C), that $d(n_1), \ldots, d(n_r)$ are actually algebraically independent over $\mathbf{Z}$. We can prove that, for $r = 1$, this is also implied by (A). In fact, if $P\big(\delta(m)\big) = 0$, for a polynomial P with integer coefficients, we get as before $P\big(-m(m-1)/l\big) \equiv 0 (\text{mod } p)$, for $p = (m^l - 1)/(m-1)$, prime. Again we can use an estimate to get $P\big(-m(m-1)/l\big) = 0$ and complete the proof as before. Note that irreducible polynomials in one variable over **Z** and of degree bigger than one have no roots in R, by the Chebotarev density theorem, but some reducible polynomials do, such as $(x^2-2)(x^2-3)(x^2-6)$, so this extension of the theorem is non-vacuous.

(v) The ring R has many quotients which are fields of characteristic zero, the so-called non-principal ultraproducts of the $\mathbf{F}_p$. One can then ask similar questions for these quotients.

Acknowledgements The author would like to thank A. Buium for the question that inspired this note. This research was started during the first Arizona winter school on Arithmetical Algebraic Geometry, at the Southwestern Center for Arithmetical Algebraic Geometry, and finished at MSRI. The author would also like to thank the TARP (grant ARP-006) and the NSA (grant MDA904-97-1-0037) for financial support.

References

[B1] A. Buium, *Geometry of p-jets*. Duke Math. J. **82**(1996), 349–357.

[B2] ———, *Arithmetic analogues of derivations*. J. Algebra **198**(1997), 290–299.

[I] Y. Ihara, *On Fermat quotient and "differentiation of numbers"*. RIMS Kokyuroku **810**(1992) 324–341, In Japanese; English translation by S. Hahn, Univ. of Georgia, (preprint).

[J] W. Johnson, *On the nonvanishing of Fermat quotients* (mod p). J. Reine Angew. Math. **292**(1977), 196–200.

[Sm] A. L. Smirnov, *Hurwitz inequalities for number fields*. St. Petersburg Math. J. **4**(1993), 357–375.

Department of Mathematics
University of Texas
Austin, Texas 78712
U.S.A.
e-mail: voloch@math.utexas.edu