BULLETIN BRAZILIAN MATHEMATICAL SOCIETY

Bull Braz Math Soc, New Series 33(2), 225-229

On a Conjecture of Finotti

John Tate

— *Dedicated to IMPA on the occasion of its* 50^{th} *anniversary*

Abstract. We prove a conjecture of Luis Finotti about cubic polynomials of one variable in characteristic p. He checked it by computer for primes $p < 890$ and uses it to define and study the minimal degree lift of the generic point of an ordinary elliptic curve in characteristic p to the canonical lift mod p^3 of the curve.

Keywords: congruence, residue, cubic polynomial, elliptic curve, canonical lift.

1 Statement and proof of the conjecture

The theorem below is a slight generalization of a discovery of Luis Finotti, who conjectured the corollary below and checked it by computer for all primes $p \leq 877$, [1], [2].

Finotti's conjecture involves what I will call the *leading coefficient of the remainder* of the division of a polynomial $f(X)$ by a polynomial $g(X)$ of degree n. By this I mean the coefficient of X^{n-1} in the remainder, even if it be 0. Fernando Villegas remarked that if $g(x)$ is monic this quantity is the negative of the residue at $X = \infty$ of the differential $f(X)dX/g(X)$, i.e., is the coefficient of X^{-1} in the expansion of the rational function $f(X)/g(X)$ in powers of X^{-1}. Once pointed out, this is obvious:

$$\frac{f(X)}{g(X)} = q(X) + \frac{r(X)}{g(X)} = q(X) + \frac{cX^{n-1} + \cdots}{X^n + \cdots} = q(X) + cX^{-1} + \cdots .$$

I thank Villegas for this observation, which was a big help to me in finding a first proof of the Theorem below.

Let $p = 2m + 1$ be a prime ≥ 3 and let k be a field of characteristic p. Note that a polynomial $F = \sum a_\nu X^\nu \in k[X]$ is the derivative of another polynomial if and only if $a_\nu = 0$ for $\nu \equiv -1 \pmod p$.

Received 5 June 2002.

Theorem. *Let $F_1, F_2, F_3 \in k[X]$ be monic cubic polynomials. For $i = 1, 2, 3$ let A_i be the coefficient of X^{p-1} in F_i^m, and let $G_i \in k[X]$ be a polynomial of degree $3m+1$ such that $G_i' = F_i^m - A_i X^{p-1}$, where $'$ denotes differentiation with respect to X. Let c_i be the leading coefficient of the remainder of the division of $G_j G_k$ by $X^p F_i^{m+1}$, where $\{i, j, k\} = \{1, 2, 3\}$. Then $c_1 + c_2 + c_3 = 0$.*

Proof. We show that $c_1 + c_2 + c_3$ is the coefficient of X^{4p-1} in the derivative $(G_1 G_2 G_3)'$ and is therefore 0. By hypothesis, there are polynomials $q_i, r_i \in k[X]$ such that

$$G_j G_k = q_i X^p F_i^{m+1} + r_i\ , \qquad \deg r_i \leq 5m + 3\ ,$$

and c_i is the coefficient of X^{5m+3} in r_i. Then

$$\begin{aligned}
(G_1 G_2 G_3)' &= G_1 G_2 G_3' + G_1 G_3 G_2' + G_2 G_3 G_1' \\
&= \sum_{i=1}^{3} (q_i X^p F_i^{m+1} + r_i)(F_i^m - A_i X^{p-1}) \\
&= \sum_{i=1}^{3} \Big(q_i X^p F_i^p - q_i A_i X^{2p-1} F_i^{m+1} + r_i (F_i^m - A_i X^{p-1}) \Big)\ .
\end{aligned}$$

The degree of q_i is $m - 2 < p - 1$. Hence the monomials X^{np-1}, in particular X^{4p-1}, do not appear in $q_i X^p F_i^p$. The degree of $q_i A_i X^{2p-1} F_i^{m+1}$ is $4p - 2$. The coefficient of X^{4p-1} in $r_i (F_i^m - A_i X^{p-1})$ is c_i. Hence $\sum_{i=1}^{3} c_i$ is the coefficient of X^{4p-1} in $(G_1 G_2 G_3)'$ as claimed. $\square$

Corollary. *Suppose $p \geq 5$. Let $F \in k[X]$ be a monic cubic polynomial. Let A be the coefficient of X^{p-1} in F^m. Let $G \in k[X]$ be a polynomial of degree $3m + 1$ such that $G' = F^m - AX^{p-1}$. Then the remainder in the division of G^2 by $X^p F^{m+1}$ has degree $\leq 5m + 2 = \frac{5p-1}{2}$.*

Proof. The theorem with $F_1 = F_2 = F_3 = F$ shows that 3 times the remainder is of degree $\leq \frac{5p-1}{2}$, and we have assumed $p \neq 3$.

One can also prove the corollary directly using Villegas's interpretation in terms of residues. We have

$$\begin{aligned}
\frac{3G^2\, dX}{X^p F^{m+1}} = \frac{3G^2 G'\, dX}{X^p F^{m+1} G'} &= \frac{dG^3}{X^p F^{m+1}(F^m - AX^{p-1})} \\
&= \frac{d(G^3/(X^p F^p))}{(1 - AX^{p-1}/F^m)}.
\end{aligned}$$

At $X = \infty$, the function G^3/X^pF^p has a pole of order $m-1$ and AX^{p-1}/F^m has a zero of order m. Hence the residue at $X = \infty$ of the differential $3G^2\,dX/X^pF^{m+1}$ is the same as that of the exact differential $d(G^3/X^pF^p)$, and is therefore 0. $\square$

2 Origin of the conjecture

Finotti was led to conjecture the corollary by his study of the Teichmueller points in canonical lifts of elliptic curves. Let

$$E : y^2 = x^3 + ax + b = f(x)$$

be an ordinary elliptic curve defined over k. Let

$$\mathbf{a} = (a, a_1, a_2), \quad \mathbf{b} = (b, b_1, b_2) \in W_3(k)$$

be Witt vectors of length three, so that

$$\mathbf{E} : \mathbf{y}^2 = \mathbf{x}^3 + \mathbf{ax} + \mathbf{b}$$

is a lift of E mod p^3. Suppose F_1, F_2, G_1, G_2 are polynomials with coefficients in k such that

$$(\mathbf{x}, \mathbf{y}) = \tau(x, y) := ((x, F_1(x), F_2(x)), (y, yG_1(x), yG_2(x)))$$

defines a map τ from the affine part of E to the affine part of **E**. It was shown by J.F. Voloch and J. Walker [4] in the corresponding situation mod p^2 that $\deg(F_1)$ takes on its minimum value, which is $(3p-1)/2$, if and only if **E** is the canonical lift of E and τ is the Teichmueller lift of points mod p^2. Finotti uses the corollary, applied to the cubic $f(x)$, to show that if $\deg(F_1) = (3p-1)/2$, then the minimum possible degree of F_2 is $(3p^2-1)/2$, and that this occurs only if **E** is the canonical lift of $E \pmod{p^3}$. However the corresponding τ is not the Teichmueller lift of points mod p^3. It is defined on the affine part of E, but does not extend to the point O at infinity. He calls that τ the "minimal degree" lift. It is useful for computing the canonical lift of E and also the Teichmuller lift of points mod p^3. The Teichmueller F_2 is of degree $2p^2 - p$, has the same derivative as the minimal degree F_2, and is characterized by $\deg(4x^{p^2}F_2 - 3F_1^{2p})$ taking its minimum value, which is $(5p^2-1)/2$, cf. [3], [2].

3 An example

To end this note we mention an easily stated congruence which can be proved with the corollary.

Proposition. *Let* $p = 2m + 1$ *be a prime* ≥ 5. *Then*

$$\sum_{\substack{1 \leq \mu, \nu \leq m \\ \mu + \nu \geq m+1}} \frac{1}{\mu\nu} \equiv 0 \pmod{p}$$

Proof. With notation as in the corollary, we can take $F = X^2(X+1)$, $A = 1$, and

$$G = X^p \sum_{\mu=1}^{m} (X+1)^\mu / \mu \ ,$$

for then

$$G' = X^p \sum_{\mu=1}^{m} (X+1)^{\mu-1} = X^{p-1}((X+1)^m - 1) = F^m - AX^{p-1}.$$

By the corollary, the leading coefficient of the remainder on dividing

$$G^2 = X^{2p} \sum_{1 \leq \mu, \nu \leq m} (X+1)^{\mu+\nu} / \mu\nu$$

by $X^p F^{m+1} = X^{2p+1}(X+1)^{m+1}$ is zero. Terms of degree $\leq 2p+m$ in G^2 do not affect that leading coefficient. Dropping them and cancelling $X^{2p}(X+1)^{m+1}$, we find that the leading coefficient in question is the remainder on dividing

$$\sum_{\substack{1 \leq \mu, \nu \leq m \\ \mu + \nu \geq m+1}} (X+1)^{\mu+\nu-m-1} / \mu\nu$$

by X. $\square$

On seeing the congruence just proved, Matilde Lalin noted that

$$\sum_{\substack{1 \leq \mu, \nu \leq m \\ \mu + \nu \geq m+1}} \frac{1}{\mu\nu} = \sum_{k=1}^{m} \frac{1}{k^2}$$

is an identity in rational numbers for every integer $m > 0$, provable by induction on m. If $p = 2m + 1$ is prime, the right side of Lalin's identity is the sum of all mth roots of unity in characteristic p, hence is 0 if $p > 3$, giving another proof of the proposition.

References

[1] L.R.A. Finotti. *Canonical and Minimal Degree Lifting of Curves*, Ph.D. thesis, The University of Texas at Austin, 2001.

[2] L.R.A. Finotti. *Minimal Degree Liftings of Hyperelliptic Curves,* submitted (preprint available at `http://www.math.ucsb.edu/~finotti/`).

[3] L.R.A. Finotti. *Degrees of the Elliptic Teichmueller Lift,* submitted (preprint available at `http://www.math.ucsb.edu/~finotti/`)

[4] J.F. Voloch and J.L. Walker. *Euclidean weights of codes from elliptic curves over rings,* Trans. Amer. Math. Soc., **352**(11) (2000), 5063–5076.

John Tate
Department of Mathematics
The University of Texas at Austin
Austin, TX 78712
USA

E-mail: tate@math.utexas.edu