F. Beukers

Congruence properties of coefficients of solutions of Picard/Fuchs equations

Groupe de travail d'analyse ultramétrique, tome 14 (1986-1987), exp. nº 11, p. 1-6
<http://www.numdam.org/item?id=GAU_1986-1987__14__A5_0>

Groupe d'Etude d'Analyse
ultramétrique. (1986/87)
n° 11, 6 pages

Le 26 janvier 1987

Exposé n° 11

CONGRUENCE PROPERTIES OF COEFFICIENTS OF SOLUTIONS OF PICARD/FUCHS EQUATIONS

by F.Beukers

Let

(1) $$F(t) = \sum_{n=1}^{\infty} f(n)t^{n-1}, \quad f(n) \in \mathbb{Z}_p$$

be a power series which is a solution of a p-adic differential equation coming from algebraic geometry. It is a well-known fact that F(t) can be approximated p-adically by algebraic functions. A theorem of J.Denef and L.Lipschitz [DL] states that the coefficients of an algebraic function mod p^s can be generated by a p^s-automaton, in other words:

(2) $\forall s \in \mathbb{N}, \exists r \in \mathbb{N}, \forall i \in \mathbb{Z}$ with $0 \leq i < p^r$ we find $r' \in \mathbb{N}$ with $r' < r$ and $i' \in \mathbb{Z}$ with $0 \leq i' < p^r$ such that $\forall m \in \mathbb{N}$ we have

$$f(mp^r+i) \equiv f(mp^{r'}+i') \pmod{p^s}$$

It turns out that in special examples of (1) the statement (2) can be remarkably refined in certain cases. The purpose of this paper is to study a number of such examples. A number of the results mentioned here are due M.Coster, and they will appear in his thesis.

The examples we have in mind fall roughly under two headings (Case I and II).

Case I. Suppose F(t)dt is the differential of a formal group law of height one over $\mathbb{Z}_p$.

Let A be the Hasse-Witt coefficient of this formal group. An alternative way of describing Case I is,

$$\exists A \in \mathbb{Z}_p, \ \vartheta(t) \in \mathbb{Z}_p[[t]] \text{ such that } F(t)dt = AF(t^p)t^{p-1}dt + d\vartheta(t).$$

(see [LH]). Comparison of coefficients yields the following equivalent statement,

$$\exists A \in \mathbb{Z}_p \text{ such that } f(mp^r) \equiv Af(mp^{r-1}) \pmod{p^r} \quad \forall m, r \in \mathbb{N}.$$

Examples of this case are f(n) = a(n), b(n), c(n), where

$$a(n) = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k}{k}, \quad b(n) = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}, \quad c(n) = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2 \quad ..$$

These numbers arise as denominators for approximations in the irrationality proofs of log 2, $\zeta(2)$ and $\zeta(3)$ respectively (see [P], [B1]). Since

$$\frac{dt}{\sqrt{1-6t+t^2}} = \sum_{n=1}^{\infty} a(n-1)t^{n-1}dt$$

and $dt/\sqrt{1-6t+t^2}$ is a rational differential, the corresponding formal group is just the multiplicative one for every odd prime p. Hence

$$a(mp^r-1) \equiv a(mp^{r-1}-1) \pmod{p^r} \quad \forall m,r \in \mathbb{N}.$$

In [B2] it is shown that the same congruence also holds for b(n), c(n). However, it turns out that for $p \geq 5$ we have

$$b(mp^r-1) \equiv b(mp^{r-1}-1) \pmod{p^{3r}} \quad \forall m,r \in \mathbb{N}$$

and the same congruence holds for c(n) as well. As far as we know this stronger congruence cannot be explained yet om the basis of a general theory. Subsequent generalisations are given by M.Coster [C2].

Let p be a prime $\equiv 1 \pmod 4$. Then the canonical differential form $dt/\sqrt{1-6t^2+t^4}$ on the elliptic curve E: $y^2 = t^4-6t^2+1 \simeq \mathbb{C}/\mathbb{Z}[i]$ corresponds to the formal addition law on E with Hasse invariant $\not\equiv 0 \pmod p$ since $p \equiv 1 \pmod 4$. As a consequence we find

$$(3) \qquad a\left(\frac{mp^r-1}{2}\right) \equiv (\alpha+\beta i)a\left(\frac{mp^{r-1}-1}{2}\right) \pmod{p^r} \quad \forall m,r \in \mathbb{N}, m \text{ odd}.$$

where $p = \alpha^2+\beta^2$, $\alpha \equiv 1 \pmod 4$. Numerical experience suggests however the following conjecture,

CONJECTURE: Congruence (3) is true mod p^{2r} .

It was proved by Van Hamme for m=r=1. A similar, non-conjectural, statement is

THEOREM. Let p, α, β be as in (3). Then

$$\binom{-1/2}{\frac{mp^r-1}{4}} \equiv (\alpha+\beta i)\binom{-1/2}{\frac{mp^{r-1}-1}{4}} \pmod{p^{2r}} \quad \forall m,r \in \mathbb{N}, \; m \equiv 1 \pmod 4.$$

The proof , given by Chowla, Dwork, Evans for m=r=1 [CDE] and by Van Hamme and M.Coster in general, consists of showing that

$$\binom{-1/2}{\frac{mp^r-1}{4}} \Big/ \binom{-1/2}{\frac{mp^{r-1}-1}{4}} \equiv \Gamma_p^2(1/4)/\Gamma_p(1/2) \pmod{p^{2r}}$$

and then noticing that the latter number is a Jacobi sum equal to $\alpha+\beta i$, [GK]. Using the same line of argument it is possible to prove similar congruences for other binomial coefficients (M.Coster [C3]).

We now turn our attention to b(n) and c(n).

THEOREM (Stienstra-Beukers [SB]) Let notations be as in (3). Then

$$b\left(\frac{mp^r-1}{2}\right) \equiv (\alpha+\beta i)^2 b\left(\frac{mp^{r-1}-1}{2}\right) \pmod{p^r} \quad \forall\, m,r \in \mathbb{N},\ m \text{ odd.} \tag{4}$$

CONJECTURE. Congruence (4) is true mod p^{2r}.

This conjecture was proved by Van Hamme for the case m=r=1.

Now take p an odd prime and let

$$\sum_{n=1}^{\infty} \gamma_n q^n = q \prod_{n=1}^{\infty} (1-q^{2n})^4 (1-q^{4n})^4$$

Let $\pi \in \mathbb{Z}_p$ be the zero of $X^2 - \gamma_p X + p^3$ such that $|\pi|_p = 1$ (if it exists). Then

THEOREM (Beukers [B3])

$$c\left(\frac{mp^r-1}{2}\right) \equiv \pi\, c\left(\frac{mp^{r-1}-1}{2}\right) \pmod{p^r} \qquad \forall\, m,r \in \mathbb{N},\ m \text{ odd.} \tag{5}$$

CONJECTURE. Congruence (5) is true mod p^{2r}.

In all conjectures there seems to be no known explanation of why these stronger congruences should occur.

We now describe the second class of examples.

<u>Case</u> II. Suppose p prime and $F(t) \equiv Q(t)Q(t^p)Q(t^{p^2})\ldots \pmod{p}$ where $Q(t) \in \mathbb{Z}_p[t]$, $\deg Q \leq p-1$.

Put $Q(t) = \sum_{n=0}^{p-1} q(n)t^n$, then, as a consequence of (6), we find that if $n = n_0 + n_1 p + n_2 p^2 + \ldots + n_t p^t$ is the expansion of n in base p, then $f(n) \equiv q(n_0)q(n_1)\ldots q(n_t) \pmod{p}$. In particular, if $p \mid q(n_i)$ for some i, then $f(n) \equiv 0 \pmod{p}$. In many examples the factorisation (6) exists. Let $\mu_p(d,n)$ be the number of digits d occurring in n in base p. It turns out that often the occurrence of $p \mid q(n_i)$ for some i implies a much stronger divisibility property when $\mu_p(n_i,n)$ increases. For example, let f(n)= c(n), where c(n) is as above. Then we have a factorisation of type mentioned above. If p=5 then $Q(t)=1-2t^2+t^4$, i.e. $5 | q(1)$, $5 | q(3)$.

CONJECTURE: let $q = \mu_5(1,n) + \mu_5(3,n)$, then $5^q | c(n)$.

For p=11 we have similarly,

CONJECTURE: Let $q=\mu_{11}(5,n)$, then $11^q | c(n)$.

Both conjectures were positively verified for all $n \leq 1000$.

Now let b(n) be as above. Then, for any p we have a factorisation of the form above [SB]. Moreover, if $p \equiv 3 \pmod 4$ then $b(\frac{p-1}{2}) \equiv 0 \pmod p$ [SB], i.e. the (p-1)/2-th coefficient of Q(t) is zero mod p. This suggests the following conjecture, which was verified for a large number of cases,

CONJECTURE: Let p be a prime and $p \equiv 3 \pmod 4$. Let $q=\mu_p(\frac{p-1}{2},n)$. Then $p^q | b(n)$.

Now consider the a(n) which can also be defined by

$$\sum_{n=0}^{\infty} a(n)t^n = \frac{1}{\sqrt{1-6t+t^2}}$$

We deal with the more general

$$\sum_{n=0}^{\infty} u(n)t^n = (1 + \alpha_1 t + \ldots + \alpha_{p-1}t^{p-1})^{\frac{1}{1-p}}$$

where $\alpha_i \in \mathbb{Z}_p$ and p is an odd prime.

THEOREM (M.Coster) Let $J = \{1 \leq j \leq p-1 \mid p \text{ divides } \alpha_j\}$ (set of relevant digits). Let

$$q = \sum_{j \in J} \mu_p(j,n).$$

Then

$$p^{\left[\frac{q+1}{2}\right]} \text{ divides } u(n).$$

COROLLARY. Let $p \equiv 3 \pmod 4$, and $q=\mu_p(\frac{p-1}{2},n)$. Then $p^{\left[\frac{q+1}{2}\right]}$ divides a(n).

<u>Proof</u> of the Corollary. According to Coster's theorem we have to show that the coefficient of $x^{\frac{1}{2}(p-1)}$ in $(x^2-6x+1)^{\frac{1}{2}(p-1)}$ is divisible by p. Since the elliptic curve $y^2 = x^4-6x^2+1$ is isomorphic to $\mathbb{C}/\mathbb{Z}[i]$, its Hasse-invariant is zero if $p\equiv 3 \pmod 4$. This is equivalent to saying that the coefficient of x^{p-1} in $(x^4-6x^2+1)^{\frac{1}{2}(p-1)}$ is divisible by p, as asserted.

In special cases Coster's theorem can be strenghtened.

THEOREM (M.Coster). Suppose $p \mid \alpha_j$ for $j=s,s+1,\dots,p-1$. Let

$$q = \sum_{j=s+1}^{p-1} \mu_p(j,n).$$

Then p^q divides $u(n)$.

EXAMPLE. Notice that $(1-t)^{-\frac{1}{2}} = ((1-t)^{\frac{1}{2}(p-1)})^{1/1-p}$. So $p\mid\alpha_j$ for $j=\frac{1}{2}(p+1),\dots,p-1$.

On the other hand

$$(1-t)^{-\frac{1}{2}} = \sum_{n=0}^{\infty} \binom{-\frac{1}{2}}{n}(-t)^n.$$

Let $\alpha\in\mathbb{Z}_p$, $n\in\mathbb{N}$ have p-adic expansions $a_0+a_1p+a_2p^2+\dots$ and $n_0+n_1p+n_2p^2+\dots+a_tp^t$ respectively. Then it is an elementary excercise to show that the number of factors p in $\binom{\alpha}{n}$ equals the number of occurrences of $n_i > \alpha_i$. Note that this implies the above theorem for this particular case.

The proof of the last two theorems is elementary but very tedious. One expands $(1+\alpha_1t+\dots+\alpha_{p-1}t^{p-1})^{1/1-p}$ as a powerseries in t to obtain

$$u(n) = \sum_{\sum ib_i=n} \binom{1/(1-p)}{b_1\dots b_{p-1}} \prod_1^{p-1} \alpha_i^{b_i}$$

and then study the divisibility properties of the multinomial coefficients

$$\binom{1/(1-p)}{b_1\dots b_{p-1}} = \frac{\frac{1}{1-p}\left(\frac{1}{1-p}-1\right)\dots\left(\frac{1}{1-p}-b+1\right)}{b_1!\,b_2!\,\dots\,b_{p-1}!}, \quad b=\sum_i b_i .$$

We hope that by these examples we have motivated the following question.

QUESTION. Are the above divisibility properties and congruences special cases of an unrecognised overall p-adic structure of coefficients of solutions of Picard-Fuchs equations ?

-REFERENCES-

[B1] F.Beukers, A note on the irrationality of $\zeta(3)$, Bull.London Math.Soc.11(1979),268-272.

[B2] F.Beukers, Some congruences for the Apéry numbers, J.Number Theory 21(1985),141-155

[B3] F.Beukers, Another congruence for the Apéry numbers, J.Number Theory 25(1987),201-210.

[C1] M.Coster, Congruence properties of coefficients of certain power series, submitted to Compositio Math.

[C2] M.Coster, Some congruences for generalised Apéry numbers, preprint.

[C3] M.Coster, Generalisation of a congruence of Gauss, submitted to J.Number Theory.

[CDE] S.Chowla, B.Dwork, R.Evans, On the mod p^2 determination of $\binom{(p-1)/2}{(p-1)/4}$, J.Number Theory 24(1986), 188-196.

[DL] J.Denef, L.Lipschitz, Algebraic power series and diagonals, preprint.

[H] M.Hazewinkel, Formal Groups and Applications, Academic Press, New York 1978.

[GK] B.Gross, N.Koblitz, Gauss sums and the p-adic Γ-function, Ann.Math.109(1979), 569-581.

[P] A.J.van der Poorten, A proof that Euler missed..., Apéry's proof of the irrationality of $\zeta(3)$, Math.Intelligencer 1 (1979), 195-203.

[SB] J.Stienstra, F.Beukers, On the Picard-Fuchs equation and the formal Brauer group of certain elliptic K3-surfaces, Math.Annalen 271 (1985), 269-304.

F.Beukers
Department of Mathematics
University of Utrecht
P.O.Box 80.010
3508 TA Utrecht
Netherlands