[5] H. Rademacher, *On the Phragmén–Lindelöf theorem and some applications*, Math. Z. 72 (1959), pp. 192–204.

[6] K. Ramachandra, *Riemann zeta function — Introductory lectures* (unpublished).

[7] E. C. Titchmarsh, *The theory of the Riemann zeta function*, Oxford 1951.

SCHOOL OF MATHEMATICS
TATA INSTITUTE OF FUNDAMENTAL RESEARCH
HOMI BHABHA ROAD
BOMBAY 400 005 (INDIA)

Received on 2.4.1984 (1417)

ACTA ARITHMETICA
XLVI (1986)

Automata and the arithmetic of formal power series

by

M. Mendès France (Talence) and A. J. van der Poorten (Macquarie)

1. Let p be a prime and denote by $\boldsymbol{F}$ a field of characteristic p. Then $\boldsymbol{F}((X))$ is the field of formal Laurent series

$$f = f(X) = \sum_{h=m}^{\infty} f_h X^h, \quad f_h \in \boldsymbol{F};\ m \in \boldsymbol{Z}.$$

The element f is said to be *algebraic* (over the field $\boldsymbol{F}(X)$ of rational functions over $\boldsymbol{F}$) if for some $s \in \boldsymbol{N}$ there are polynomials $a_0, a_1, \ldots, a_s \in \boldsymbol{F}[X]$ not all zero, so that

$$a_0 f^s + a_1 f^{s-1} + \ldots + a_s = 0.$$

Denote by $\boldsymbol{Z}_p$ the domain of p-adic integers. Each $\lambda \in \boldsymbol{Z}_p$ has a unique representation

$$\lambda = \sum_{k=0}^{\infty} \lambda_k p^k, \quad \lambda_k \in \{0, 1, \ldots, p-1\}.$$

For each nonnegative rational integer $n = \sum_{k=0}^{\infty} n_k p^k$ we define the binomial coefficients

$$\binom{\lambda}{n} := \prod_{k=0}^{\infty} \binom{\lambda_k}{n_k}.$$

Since $n_k = 0$ for all sufficiently large k, the product on the right is finite. Further, we define

$$(1+X)^{\lambda} := \sum_{n=0}^{\infty} \binom{\lambda}{n} X^n.$$

Of course our definitions are theorems in characteristic p as one sees by arguing naively:

$$(1+X)^{\lambda} = (1+X)^{\Sigma \lambda_k p^k} = \prod (1+X)^{\lambda_k p^k} = \prod (1+X^{p^k})^{\lambda_k}$$
$$= \prod_{k=0}^{\infty} \sum_{h=0}^{\infty} \binom{\lambda_k}{h} X^{hp^k} = \sum_{n=0}^{\infty} \prod_{k=0}^{\infty} \binom{\lambda_k}{n_k} X^n.$$

In this spirit, given a formal power series

$$f = f(X) = \sum_{h=0}^{\infty} f_h X^h,$$

thus an element of $F[[X]]$, with $f_0 = 1$, we have

$$f^{\lambda} = \prod_{k=0}^{\infty} (1+(f-1)^{p^k})^{\lambda_k} = \sum_{n=0}^{\infty} \binom{\lambda}{n}(f-1)^n.$$

Our definition of $\binom{\lambda}{n}$ is a well-known congruence (see for example [7]).

One notices readily that the map $\lambda \mapsto f^{\lambda}$ is continuous (in that elements p-adically near to one another in the domain yield power series near to one another in the formal power series topology); it follows that we have defined a proper exponentiation.

We shall make a simple appeal to the theory of finite automata to show:

THEOREM. *Let F be a finite field of characteristic p and suppose $f = \sum_{h \geqslant 0} f_h X^h$ is in $F[[X]]$ with $f_0 = 1$ and $f \neq f_0$. Let λ be a p-adic integer. If both f and f^{λ} are algebraic then λ is rational.* (If λ is irrational and f is non-constant algebraic then f^{λ} is transcendental over $F[X]$.)

2. Finite automata. Formally, an *m-automaton*, $m \geqslant 2$, consists of a finite set S of states containing a distinguished element i: the initial state, and a subset F of acceptance or final states, related by a map σ

$$\{0, 1, 2, \ldots, m-1\} \times S \to S$$

known as the transition function. A word $\mu \in \bigcup_{n=0}^{\infty} \{0, 1, \ldots, m-1\}^n$ is said to be *accepted* by the automaton if μ sends the state i to a state in F. This is to say: set $i = x_0$, $\mu = \mu_0 \mu_1 \ldots \mu_{t-1}$ ($\mu_j \in \{0, 1, \ldots, m-1\}$) and define $x_{k+1} = \sigma(\mu_k, x_k)$. Then μ is accepted by the automaton if and only if $x_t \in F$. The language $\mathscr{L}$ of all words accepted by the automaton is described as generated by the automaton. The words of $\mathscr{L}$ may be interpreted as natural numbers presented in the base m, so one might speak of a formal power series

$$L(X) = \sum_{n \in \mathscr{L}} X^n$$

as generated by the automaton. Moreover one might associate a symbol χ_j with each state x_j, in which case each integer $h \geqslant 0$ becomes a symbol, say f_h, on being read by the m-automaton. Then the formal power series

$$f(X) = \sum_{h \geqslant 0} f_h X^h,$$

or the sequence (f_h), is appropriately described as m-automatic. L is the case where the states in F have the symbol 1 and the states in $S \setminus F$ have the symbol 0.

Suppose now that m is a power of some prime p and that the symbols are chosen to be elements of some finite field F of characteristic p. Then it is a theorem of Christol, Kamae, Mendès France and Rauzy [3] that *f is algebraic over $F(X)$ if and only if the sequence (f_h) is m-automatic.* It follows readily from a theorem of Furstenberg [6] that the manner of choice of symbols from F is irrelevant.

The following well-known result (see [1], [5]) is easily seen:

LEMMA. *If the sequence $f = (f_h)$ is p-automatic then the subsequence (f_{p^h}) is (ultimately) periodic.*

Proof. Consider words $p^h = 100\ldots000$ with h greater than $|S|$, the number of states of the automaton. On reading p^h the automaton must reach some state more than once. Hence the sequence (f_{p^h}) is periodic with period of length at most $|S|$.

COROLLARY. *If f is algebraic over $F(X)$, where F is a finite field of characteristic p, then the subsequence (f_{p^h}) of the sequence of coefficients is periodic.*

For a quite informal introduction to finite automata see FOLDS! [4]; note also the uncited additional references.

3. Proof of the theorem. Were

$$(1+X)^{\lambda} = \sum_{n=0}^{\infty} \binom{\lambda}{n} X^n$$

algebraic, then the sequence $(\binom{\lambda}{n})$ would be p-automatic, so by the Lemma the sequence $(\binom{\lambda}{p^n}) = (\binom{\lambda_n}{1}) = (\lambda_n)$ is periodic. But then $\lambda = \sum \lambda_n p^n$ is rational. Conversely if λ is rational then of course $(1+X)^{\lambda}$ is algebraic.

For convenience, change notation to set

$$f = \sum_{h=1}^{\infty} f_h X^h$$

and suppose that both f and $(1+f)^{\lambda}$ are algebraic with $f \neq 0$. Write $h(X) = (1+X)^{\lambda}$. We claim that if $h \circ f = g$ and both f and g are algebraic, then so is h. Indeed f has a right inverse, j say, with $j(X)$ a formal power series in some fractional power of X. But since f is algebraic so is j, and then so is $g \circ j$. Thus we have $h \circ (f \circ j) = h = g \circ j$ is algebraic (and since a priori $h(X)$ is a power series in X, the power series $g \circ j$ has no fractional powers). But as already shown, h algebraic implies λ rational.

4. Remarks. The authors had conjectured (a special case of) the theorem in [9]. There we note that in characteristic 2 one has

$$(1+X)^{\lambda} = \sum_{n \in \mathscr{L}(\lambda)} X^n$$

with $\mathscr{L}(\lambda)$ the language of all integers $\mu = \prod_{k=0}^{\infty} \mu_k 2^k$ with $0 \leqslant \mu_k \leqslant \lambda_k$ (and $\mu_k = 0$ for all sufficiently large k). Thus: $\mathscr{L}(\lambda)$ is the language of all nonnegative integers ‘under’ $\lambda = \sum_{k=0}^{\infty} \lambda_k 2^k$. Here we have shown that whenever $\lambda \in Z_2$ is irrational then the language $\mathscr{L}(\lambda)$ under λ is not recognisable by a finite automaton.

Our present theorem can of course be proved without appeal to the theory of finite automata. Indeed the referee points out that λ may be approximated by a rational a/b:

$$|\lambda - a/b|_p < p^{-2k} \quad \text{with} \quad |a|, |b| < p^k.$$

Then

$$(1+X)^{\lambda b} \equiv (1+X)^a \ (\mathrm{mod}\ X^{p^{2k}})$$

and given a polynomial $P(X, Y)$ with zero $Y = (1+X)^\lambda$ one readily shows that, with k sufficiently large, the polynomial one constructs to vanish at $(1+X)^{\lambda b}$ also vanishes at $(1+X)^a$. Of course this is a significantly less elegant argument than the one we present.

References

[1] J.-P. Allouche, *Somme des chiffres et transcendance*, Bull. Soc. Math. France 110 (1982), pp. 279–285 (see lemma at p. 281).

[2] A. Blanchard et M. Mendès France, *Symmètrie et transcendance*, Bull. Sci. Math. (2) 106 (1982), pp. 325–335.

[3] G. Christol, T. Kamae, M. Mendès France et G. Rauzy, *Suites algèbriques, automates et substitutions*, Bull. Soc. Math. France 108 (1980), pp. 401–419.

[4] F. M. Dekking, M. Mendès France and A. J. van der Poorten, *FOLDS!* The Mathematical Intelligencer 4 (1982), pp. 130–138; II *Symmetry disturbed*, ibid., pp. 173–181; III *More Morphisms*, ibid., pp. 190–195.

[5] S. Eilenberg, *Automata, Languages and Machines*, Vol. A, Academic Press, 1974, (see proposition 5.1, p. 24).

[6] H. Furstenberg, *Algebraic functions over finite fields*, J. Algebra 7 (1967), pp. 271–277.

[7] N. Koblitz, *P-adic analysis; a short course on recent work*, Cambridge U.P.; LMS Lecture Notes 46, 1980 (note p. 15).

[8] J. H. Loxton and A. J. van der Poorten, *Arithmetic properties of the solutions of a class of functional equations*, J. Reine Angew. Math. 330 (1982), pp. 159–172.

[9] M. Mendès France, A. J. van der Poorten, *Automata and p-adic numbers*, in: *Théorie des nombres, Colloque de Luminy, 1983*, (Unpublished manuscript).

U.E.R. DE MATHÉMATIQUES ET D'INFORMATIQUE
UNIVERSITÉ DE BORDEAUX I
TALENCE, FRANCE

SCHOOL OF MATHEMATICS AND PHYSICS
MACQUARIE UNIVERSITY
NORTH RYDE, NEW SOUTH WALES, AUSTRALIA

Received on 17.7.1984
and in revised form on 21.2.1985

ACTA ARITHMETICA
XLVI (1986)

An iteration problem involving the divisor function*

by

CLAUDIA SPIRO (Buffalo, N.Y.)

1. Introduction. Let $d(n)$ denote the number of positive integers dividing the positive integer n. For every integer $I \geqslant 3$, recursively define an integer sequence $S(I) = \{a_k\}_{k=0}^{\infty}$ by

$$(1) \qquad a_0 = I; \quad a_{k+1} = a_k + (-1)^k d(a_k) \quad \text{for } k \geqslant 0.$$

For example, the sequence $S(275)$ is

$$(2) \qquad 275, \overline{281, 279, 285, 277, 279, 273},$$

where the bar indicates that the sequence becomes periodic immediately after the term 275, and that one full period consists, in order, of the terms 281, 279, 285, 277, 279, 273. We will show that every sequence contains only integers exceeding 2 (see Proposition 1). If a sequence $S(I)$ is eventually periodic, we call the period a *cycle*. If there are n terms in the cycle, we say that it is an *n-cycle*, or a *cycle of length n*. Thus, the cycle in (2) has length 6.

At the West Coast Number Theory Conference, held in Los Angeles in December of 1977, we stated the following conjectures about these sequences:

CONJECTURE 1. *For every I, the sequence $S(I)$ is eventually periodic.*

CONJECTURE 2. *For each n, there are infinitely many 2n-cycles.*

CONJECTURE 3. *The series $\sum 1/n$, summed over all positive integers which are elements of at least one cycle, diverges.*

CONJECTURE 4. *Every element of a given cycle has the same parity.*

In this paper, we establish that there are infinitely many 2-cycles (see Theorem 1). This is Conjecture 2 for $n = 1$. In addition, we show (see Theorem 3) that Conjecture 2 follows from the Prime k-tuples Conjecture.

2. Elementary properties of the sequences $S(I)$. Throughout this paper, m and n will denote positive integers, and p will denote a prime. Proposition 1,

* This investigation was supported in part by a Research Development Fund Award from the State University of New York Research Foundation.