A note on recurrent mod $p$ sequences

by

U. ZANNIER (Pisa)

Important arithmetical functions, namely the integral valued linear combinations of polynomials multiplied by exponential functions, have the striking property of being periodic mod $p$ for all sufficiently large primes $p$.

In this paper we are concerned with the following problem: which other sequences, apart from the above mentioned ones, satisfy some periodicity condition mod $p$ for almost all primes $p$?

Our result is that no other such sequence exists, provided a certain kind of growth condition is satisfied.

We consider sequences satisfying a more general property, i.e. those which are solutions of recurrence equations mod $p$ for large $p$. (Periodicity is actually a special kind of recurrence.)

In the sequel $C_1, C_2, \ldots$ will denote numbers which depend only on the sequence.

We have the following

**Theorem.** Let $f: \mathbb{N} \to \mathbb{Z}$. Suppose that

(i) for every prime $p > p_0$, $f$ satisfies a non-trivial recurrence equation in $\mathbb{Z}[p\mathbb{Z}]$, of length $r_p < p^k$, for some fixed $k$.

(ii) $|f(n)| \leq n^B$ for some constant $B$.

Then $f$ satisfies a non-trivial recurrence equation over $\mathbb{Z}$.

**Proof.** We recall the following Siegel's classical lemma (see for example [1]): "Let $M, N$ denote integers, $N > M > 0$, and let $u_j$ $(1 \leq i \leq M, 1 \leq j \leq N)$, denote integers satisfying $|u_{ij}| \leq U$. Then there exists a non trivial integral solution $x_1, x_2, \ldots, x_N$, of the linear system

$$\sum_{j=1}^{N} u_{ij} x_j = 0 \quad \text{for} \quad i = 1, 2, \ldots, M$$

such that $|x_i| \leq (NU)^{M(N-M)}$.

Let now $N$ be a large integer, and consider the auxiliary function

$$F(t) = x_1 f(t+1) + \ldots + x_N f(t+N).$$
Setting \( M = \lfloor N/2 \rfloor \), using Siegel’s Lemma, we can choose integers \( x_1, \ldots, x_N \), not all zero, such that:

\[
F(h) = 0 \quad \text{for} \quad 0 < h \leq M
\]

and subject to the estimate

\[
|x_j| \leq N \max_{0 < h \leq N} |f(r+h)| \leq C_1 N^{E+1},
\]

obtaining thus the following bound

\[
|F(r)| \leq C_1 N^{E+1}(N+r)^\mu.
\]

We want to show that, when \( N \) has been chosen large enough, we have \( F(r) = 0 \) for all \( r \in \mathbb{N} \).

Let us argue by induction, and suppose that:

\[
F(1) = F(2) = \ldots = F(r-1) = 0.
\]

By (1) \( r \) may be chosen \( \geq M \).

Let \( p \) be a prime number such that \( p > p_0 \) and \( r < r \). From our hypothesis \( f \) satisfies a difference equation of the type:

\[
f(m + r_p) = \sum_{h=0}^{r_p-1} a_{0, p} f(m + h) \quad (\text{mod } p),
\]

and so the same holds for \( F \). But then the induction hypothesis clearly implies \( F(r) = 0 \) (mod \( p \)).

Suppose \( F(r) \neq 0 \). Then the above congruences imply:

\[
|F(r)| \gg \prod_{p < \sqrt{C_2}} p \gg \prod_{p \leq \sqrt{C_2}} p \geq C_3 \exp(C_4 \sqrt{r})
\]

for \( N \) large enough, where \( C_2, C_4 > 0 \). (We have used the prime number theorem.)

Now (3) and (4) are contradictory for \( N \) large and for \( r \geq M \), and the contradiction proves the theorem.

Remarks. 1. For simplicity we have given only a particular form of a more general theorem of the same kind; in fact one may relax the bound for \( f \), at the cost of reducing the order of growth admitted for \( r_p \).

We may prove for example that the conclusion remains true, assuming \( r_p \leq p + B \) and \( |f(n)| \leq C a^n \), provided \( a < \exp(3 - 2y \sqrt{2}) \).

The only modification required consists in a different use of Siegel’s Lemma: we choose \( M = \lfloor y N \rfloor \), \( 0 < y < 1 \), and then optimize the choice of \( y \). (In fact the best one is \( y = \sqrt{2} - 1 \).)

We point out that, though \( \exp(3 - 2y \sqrt{2}) \) could be probably replaced by a larger number, there are exponentially growing sequences, periodic mod \( p \), with \( r_p \leq p \), that do not satisfy the conclusion.

The following construction provides such an example: let \( a_n = \prod_{p \leq n} p \) and \( f(m) = \sum_{p \leq m} a_p \cdot (\frac{m}{p}) \). It is easy to verify the congruence \( f(n+1) \equiv f(n) \) (mod \( p \)), for every prime \( p \), and the bound \( |f(n)| \leq A^h \) for some \( A \). Our sequence does not satisfy recurrence relations in \( Z \), otherwise it would be of the form stated in the lemma below, and, since its period mod \( p \) divides \( p \), it would be a polynomial. But this would imply \( a_n = 0 \) for large \( n \), thus obtaining a contradiction.

2. A better result may be obtained assuming the recurrence to be

\[
f(n+1) \equiv f(n) \quad (\text{mod } p)
\]

In this case the bound \( |f(n)| \leq C(e-1)^l, 0 < l < 1 \), is sufficient to imply that \( f \) is a polynomial (see [3]).

We now sketch the proof that, under the conditions of our theorem \( f \) is of the following type:

\[
f(n) = \sum_{j=1}^s P_j(n) r_j^n
\]

where the \( P_j \) are polynomials and the \( r_j \) are roots of unity.

We tacitly assume some known lemmas from the theory of finite difference equations (see for example [2]).

We require the following

**Lemma.** If \( f: \mathbb{N} \rightarrow \mathbb{Z} \) is a solution of a finite difference equation with integral coefficients, then \( f \) is of the form:

\[
f(n) = \sum_{j=1}^s P_j(n) r_j^n
\]

with \( P_j \in \mathbb{Q}(r_1, \ldots, r_s)[x] \) and where the \( r_j \) are algebraic integers.

**Proof.** It is well known that \( f \) has an expression of the form (4) where the \( P_j \) are polynomials and the \( r_j \) are algebraic numbers. Using a determinant argument one can easily show that in fact \( f \in \mathbb{Q}(r_1, \ldots, r_s)[x] \), and that \( r_j^p = H_n D_n \), where \( H_n \) is an algebraic integer and \( D_n \) a polynomial with algebraic integer coefficients, which is nonzero.

If \( p \) is a prime ideal which divides the denominator of \( r_j \), \( p^a \) would divide \( D_n \) and we should obtain:

\[
|N(D_n)| > |N(p)|^a
\]

where \( N \) is the norm from \( \mathbb{Q}(r_1, \ldots, r_s) \), over \( Q \).

But, since \( |N(p)| > 1 \), we have a contradiction.

Let now \( W \) be a normal extension of \( Q \), containing \( Q(r_1, \ldots, r_s) \), and let \( \sigma \in \text{Gal}(W/Q) \).
Since \( f(n) \in \mathbb{Z} \) for every \( n \), we have:

\[
\sum_{j=1}^{g} \sigma(P_j(n)) \sigma(r_j)^n = \sum_{j=1}^{g} P_j(n) r_j^n.
\]

But it is well known that the expression of \( f \) in the form (4) is unique, and it follows that the \( \sigma(r_j) \) are a permutation of the \( r_j \), and this happens for every \( \sigma \).

Thus, if in the formula for \( f \) some \( r_j \) has a polynomial coefficient which is nonzero, then all of its conjugates have the same property. But

\[
|f(n)| \geq \max_{P_j > 0} |r_j|^n \quad \text{for an infinity of } n
\]

and, since \( f \) is assumed to have polynomial growth, we conclude that

\[
\max_{P_j > 0} |r_j| < 1,
\]

and, by the preceding observation, we have also:

\[
\max_{\sigma} \max_{P_j > 0} |\sigma(r_j)| \leq 1.
\]

Since the \( r_j \) are algebraic integers, a well known theorem of Kronecker implies that they are roots of unity.

References


Received on 8.7.1989
and in revised form on 15.10.1980 (1215)

Selberg's sieve estimate with a one sided hypothesis

by

DANIEL A. RAWSTORNE (Wheaton, Md.)*

1. Introduction. It has been found in many interesting number theory problems that the most successful techniques involve a small sieve. One of the best small sieve techniques known is that of Selberg [8]. This sieve has been investigated by Ankeny-Onishi [1] and Halberstam-Richert [2], among others. The results they obtain using the Selberg sieve rely on assumptions made about the function \( \omega(d) \) (defined in Section 2), and the aim of this paper is to obtain similar results with less stringent assumptions.

2. The basis of the sieve and Selberg’s \( \lambda \)-method. We follow the notation of Halberstam-Richert ([2]) and ([4]).

Let \( \mathfrak{A} \) be a finite sequence of integers, and let \( \mathfrak{A}_d \) denote the subsequence of \( \mathfrak{A} \) of all of whose elements are divisible by \( d \). We use \( |\mathfrak{A}| \) and \( |\mathfrak{A}_d| \) to denote the number of elements of \( \mathfrak{A} \) and \( \mathfrak{A}_d \), respectively.

Let \( \mathfrak{P} \) be a set of primes and define (the empty product being 1)

\[
P(z) = \prod_{\mathfrak{p} \in \mathfrak{P}} \mathfrak{p}^{-z}.
\]

Define the sifted function \( \mathcal{S}(\mathfrak{A}; \mathfrak{P}, z) \) for any \( z \) to be

\[
\mathcal{S}(\mathfrak{A}; \mathfrak{P}, z) = |\{ a \in \mathfrak{A} : \{ a, P(z) \} = 1 \}|;
\]

in other words, \( \mathcal{S}(\mathfrak{A}; \mathfrak{P}, z) \) is the number of elements of \( \mathfrak{A} \) remaining after we have removed all those with prime factors less than \( z \) that belong to \( \mathfrak{P} \).

In order to study the function \( \mathcal{S}(\mathfrak{A}; \mathfrak{P}, z) \) we need some notation. We choose a convenient approximation to \( |\mathfrak{A}| \), call it \( X \), and define

\[
R_1 = |\mathfrak{A}| - X.
\]

* This work is a portion of the author's PhD thesis. Thanks go to Harold Diamond and to the University of Illinois at Urbana, Ill. This work was partially supported by a University of Illinois Fellowship.