[4] C. G. J. Jacobi, *Über die Kreistheilung und ihre Andwendung auf die Zahlentheorie*, J. Reine Angew. Math. 30 (1846), pp. 166–182.
[5] Ernst Jacobsthal, *Über die Darstellung der Primzahlen der Form $4n+1$ als Summe zweier Quadrate*, ibid. 132 (1907), pp. 238–245.
[6] Emma Lehmer, *Criteria for cubic and quartic residuacity*, Mathematika 5 (1958), pp. 20–29.
[7] — *On Euler's criterion*, J. Austral. Math. Soc. 1 (1959), pp. 64–70.
[8] Horst von Lienen, *Primzahlen als achte Potenzreste*, J. Reine Angew. Math. 266 (1974), pp. 107–117.
[9] Lothar von Schrutka, *Ein Beweis für die Zerlegbarkeit der Primzahlen von dre Form $6n+1$ in ein einfaches und ein dreifaches Quadrat*, ibid. 140 (1911), pp. 252–265.
[10] M. Stern, *Eine Bemerkung zur Zahlentheorie*, ibid. 32 (1846), pp. 89–90.
[11] A. E. Western, *Some criteria for the residues of eighth and other powers*, Proc. London Math. Soc. 9 (1911), pp. 244–272.
[12] Albert L. Whiteman, *Theorems analogous to Jacobsthal's theorem*, Duke Math. J. 16 (1949), pp. 619–626.
[13] — *Cyclotomy and Jacobsthal sums*, Amer. J. Math. 74 (1952), pp. 89–99.

DEPARTMENT OF MATHEMATICS AND STATISTICS
UNIVERSITY OF SOUTH CAROLINA
Columbia, South Carolina, U.S.A.

DEPARTMENT OF MATHEMATICS AND STATISTICS
CARLETON UNIVERSITY
Ottawa, Ontario, Canada

Received on 2.6.1980 (1209)

ACTA ARITHMETICA
XLI (1982)

A note on recurrent mod p sequences

by

U. ZANNIER (Pisa)

Important arithmetical functions, namely the integral valued linear combinations of polynomials multiplied by exponentials 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: $\mathbf{N}\to\mathbf{Z}$. Suppose that*

(i) *for every prime $p > p_0$, f satisfies a non trivial recurrence equation in $\mathbf{Z}/p\mathbf{Z}$, of length $r_p \leqslant p^k$, for some fixed k.*

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

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

Proof. We recall the following Siegel's classical lemma (see for example [1]): "Let M, N denote integers, $N > M > 0$, and let u_{ij} ($1 \leqslant i \leqslant M$, $1 \leqslant j \leqslant N$), denote integers satisfying $|u_{ij}| \leqslant U$. 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

$$|x_j| \leqslant (NU)^{M/(N-M)}."$$

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 $M = [N/2]$, using Siegel's Lemma, we can choose integers $x_1, \ldots, x_N$, not all zero, such that:

$$F(h) = 0 \quad \text{for} \quad 0 < h \leqslant M \tag{1}$$

and subject to the estimate

$$|x_j| \leqslant N \max_{\substack{0<h\leqslant M\\ 1\leqslant r\leqslant N}} |f(r+h)| \leqslant C_1 N^{B+1},$$

obtaining thus the following bound

$$|F(r)| \leqslant C_2 N^{B+1}(N+r)^B. \tag{2}$$

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

Let us argue by induction, and suppose that:

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

By (1) r may be chosen $\geqslant M$.

Let p be a prime number such that $p > p_0$ and $r_p < r$. From our hypothes f satisfies a difference equation of the type:

$$f(m+r_p) \equiv \sum_{h=0}^{r_p-1} a_{h,p} f(m+h) \pmod p,$$

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

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

$$|F(r)| \geqslant \prod_{\substack{p_0<p\\ r_p<r}} p \geqslant \prod_{\substack{p_0<p\\ p\leqslant r^{1/k}}} p \geqslant C_3 \exp(C_4 r^{1/k}) \tag{3}$$

for N large enough, where $C_3, C_4 > 0$. (We have used the prime number theorem.)

Now (2) and (3) are contradictory for N large and for $r \geqslant M$, 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 $r_p \leqslant p+B$ and $|f(n)| \leqslant Ca^n$, provided $a < \exp(3-2\sqrt{2})$.

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

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

The following construction provides such an example: let $a_n = \prod_{p\leqslant n} p$ and $f(m) = \sum_{r=0}^{m} a_r \binom{m}{r}$. It is easy to verify the congruence $f(n+p) \equiv f(n) \pmod p$, for every prime p, and the bound $|f(n)| \leqslant A^n$ for some A. Our sequence does not satisfy recurrence relations in $\mathbf{Z}$, 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

$$f(n+p) \equiv f(n) \pmod p$$

In this case the bound $|f(n)| < C(e-1)^{ln}$, $0 < l < 1$, 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 $f\colon \mathbf{N}\to\mathbf{Z}$ is a solution of a finite difference equation with integral coefficients, then f is of the form:*

$$f(n) = \sum_{j=1}^{s} P_j(n) r_j^n \tag{4}$$

with $P_j \in \mathbf{Q}(r_1, \ldots, r_s)[x]$ 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 $P_j \in \mathbf{Q}(r_1, \ldots, r_s)[x]$, and that $r_j^n = H_n/D_n$, where H_n is an algebraic integer and D_n a polynomial with algebraic integer coefficients, which is nonzero.

If $\mathfrak{p}$ is a prime ideal which divides the denominator of r_j, $\mathfrak{p}^n$ would divide D_n and we should obtain:

$$|N(D_n)| \geqslant |N(\mathfrak{p})|^n$$

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

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

Let now W be a normal extension of $\mathbf{Q}$, containing $\mathbf{Q}(r_1, \ldots, r_s)$, and let $\sigma \in \mathrm{Gal}(W/\mathbf{Q})$.

Since $f(n) \in \mathbf{Z}$ for every n, we have:

$$\sum_{j=1}^{s} \sigma(P_j(n))\,\sigma(r_j)^n = \sum_{j=1}^{s} P_j(n)\,r_j^n.$$

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 σ.

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

$$|f(n)| \geqslant \max_{P_j \neq 0} |r_j|^n \quad \text{for an infinity of } n$$

and, since f is assumed to have polynomial growth, we conclude that $\max\limits_{P_j\neq 0}|r_j| \leqslant 1$, and, by the preceding observation, we have also:

$$\max_{\sigma} \max_{P_j \neq 0} |\sigma(r_j)| \leqslant 1.$$

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

References

[1] A. Baker, *Transcendental number theory*, Cambridge Univ. Press, 1974.

[2] A. O. Gelfond, *Calcul des differences finies*, Dunod, 1963.

[3] A. Perelli et U. Zannier, *Su un teorema di Pólya*, Boll. U. M. I., (5) 18-A (1981), pp. 305–307.

Received on 8. 7. 1980
and in revised form on 15. 10. 1980 (1215)

ACTA ARITHMETICA
XLI (1982)

Selberg's sieve estimate with a one sided hypothesis

by

DANIEL A. RAWSTHORNE (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 λ-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 $\mathfrak{A}$ 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 $\mathscr{P}$ be a set of primes and define (the empty product being 1)

$$P(z) = \prod_{\substack{p\in\mathscr{P}\\ p<z}} p. \tag{1}$$

Define the sifting function $\mathscr{S}(\mathfrak{A};\mathscr{P},z)$ for any z to be

$$\mathscr{S}(\mathfrak{A};\mathscr{P},z) = \left|\{a \in \mathfrak{A}:\ (a, P(z)) = 1\}\right|; \tag{2}$$

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

In order to study the function $\mathscr{S}(\mathfrak{A};\mathscr{P},z)$ 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.