ACTA ARITHMETICA
LXVII.1 (1994)

On the roots of certain sequences of congruences

by

Daniel Berend (Beer Sheva)

1. Introduction and main theorems. Put

$$P_k = p_1 p_2 \ldots p_k, \qquad k = 1, 2, \ldots,$$

where $p_1 < p_2 < \ldots$ is the sequence of all primes in increasing order. Denote by x_k the least positive integer x such that $x(x+1) \equiv 0 \pmod{P_k}$. Erdős [E] opined that

$$(1) \qquad \frac{x_k}{P_k} \to 0 \quad \text{and} \quad \frac{x_k}{\sqrt{P_k}} \to \infty \qquad \text{as } k \to \infty,$$

and similarly for $k!$ instead of P_k (x_k being defined correspondingly). In this paper we deal with the first convergence, along with various strengthenings and generalizations. The second convergence, which Erdős estimated as "hopeless", is left open.

As partial motivation to look at these questions, let us mention the diophantine equations

$$(2) \qquad x(x+1) = P_k,$$

studied by Nelson, Penney and Pomerance [NPP], and

$$(3) \qquad x(x+1) = k!,$$

posed by Erdős at one of the Western Number Theory Conferences ([G, Problems 301–305]). It is unknown whether these equations have finitely many solutions or not, although (3) is known to have "few" solutions [BO]. Proving the second convergence in (1) would show in particular that (2) has only finitely many solutions.

Theorem 1. $\lim_{k\to\infty} x_k/P_k = 0$.

We shall actually obtain a stronger result. To state it we use the following notation. Let (A_k) be a sequence of subsets of $[0,1)$. Then (A_k) *converges to* $[0,1)$ (in the Hausdorff metric), and we write $A_k \to [0,1)$ as $k \to \infty$, if for every $\varepsilon > 0$ the sets A_k are eventually ε-dense in $[0,1)$ (i.e., intersect every subinterval of length ε).

Theorem 2. *Let $q_1 < q_2 < \ldots$ be a sequence of primes satisfying $\sum_{l=1}^{\infty} 1/q_l = \infty$. Put $Q_k = q_1 q_2 \ldots q_k$, $k \in \mathbb{N}$. Let S_k be the set of all solutions of the congruence*

$$x(x+1) \equiv 0 \pmod{Q_k}$$

in the interval $[0, Q_k - 1]$. Define

$$R_k = \{x/Q_k : x \in S_k\} \subseteq [0,1).$$

Then $R_k \to [0,1)$ as $k \to \infty$.

Now Theorem 2 admits the following (stronger) finite version.

Theorem 2′. *Given $\varepsilon > 0$ there exists an $M = M(\varepsilon)$ having the following property. Let Q be a positive integer factorizing as $Q = q_1^{e_1} q_2^{e_2} \ldots q_k^{e_k}$, with $\sum_{i=1}^{k} q_i^{-e_i} > M$, and let $S(Q)$ be the set of all solutions of the congruence $x(x+1) \equiv 0 \pmod{Q}$ in the interval $[0, Q-1]$. Then the set*

$$R = \{x/Q : x \in S(Q)\} \subseteq [0,1)$$

is ε-dense in $[0,1)$.

Example 1. Theorems 2 and 2′ do not apply to obtain the analogue of Theorem 1 when P_k is replaced by other "natural" sequences, such as $k!$ or even $[1, 2, \ldots, k]$. The reason is that in these cases "too many" of the exponents e_i are greater than 1:

$$k! = \prod_{i=1}^{\pi(k)} p_i^{[k/p_i] + [k/p_i^2] + \ldots}, \qquad [1, 2, \ldots, k] = \prod_{i=1}^{\pi(k)} p_i^{[\log_{p_i} k]},$$

where $\pi(k)$ denotes the number of primes not exceeding k. On the other hand, Theorem 2′ does apply to the sequence

$$Q_k = \prod_{i=1}^{\pi(k)} p_i^{[\log \log_{p_i}(k+1)]}.$$

Theorem 3 will take care of the first two sequences, although we do not obtain the density result of Theorem 2.

Denote by $P(Q)$ the number of distinct prime divisors of a positive integer Q.

Theorem 3. *Let Q_k be a sequence of positive integers satisfying $P(Q_k) \to \infty$ as $k \to \infty$. Let x_k be the least positive solution of the congruence*

$$x(x+1) \equiv 0 \pmod{Q_k}.$$

Then $x_k/Q_k \to 0$.

Again, Theorem 3 admits a finite version, which this time we can make quantitative.

Theorem 3′. *Let Q be a positive integer and x be the smallest positive solution of the congruence $x(x+1) \equiv 0 \pmod{Q}$. Then*

$$x \le \frac{Q}{P(Q)}.$$

For Theorem 2 we have the following converse.

Theorem 4. *Given any $\varepsilon > 0$, there exists a sequence of primes $(q_k)_{k=1}^{\infty}$ such that $R_k \subseteq [0,\varepsilon) \cup (1-\varepsilon, 1)$ for each k, where R_k is as in Theorem 2.*

The following theorem shows in particular that Theorem 3′ is essentially best possible.

Theorem 5. *Given any $\varepsilon > 0$, there exists a sequence of primes $(q_k)_{k=1}^{\infty}$ such that, denoting by x_k the least positive solution of the congruence*

$$x(x+1) \equiv 0 \pmod{Q_k},$$

where $Q_k = q_1 q_2 \ldots q_k$, we have

$$x_k \ge (1-\varepsilon)\frac{Q_k}{k}, \qquad k = 1, 2, \ldots$$

In the next section we prove some extraneous results that will serve us in proving the main (positive) results, but seem to be of independent interest. The proofs of Theorems 1–5 are given in Section 3.

I would like to express my gratitude to P. Erdős for long and interesting discussions on these problems.

2. Dense parallelepipeds on the circle. Given a (finite or infinite) sequence (α_n) in some additive semigroup, the *parallelepiped based on* (α_n) is denoted by IP-(α_n) and defined as the algebraic sum of the sets $\{0, \alpha_n\}$:

$$\begin{aligned} IP\text{-}(\alpha_n) &= \{0, \alpha_1\} + \{0, \alpha_2\} + \ldots \\ &= \{\alpha_{n_1} + \alpha_{n_2} + \ldots + \alpha_{n_j} : j \ge 0,\ 1 \le n_1 < n_2 < \ldots < n_j\}. \end{aligned}$$

(Our notation derives from the concept of an IP-set; see [B, Def. 2.3].) The parallelepiped is *d-dimensional* if the sequence (α_n) is of finite length d, and *infinite-dimensional* if the sequence is infinite. (Thus, for example, the set $\{0\}$ may be considered as a parallelepiped of any finite dimension or even of infinite dimension.)

We shall be interested in finite parallelepipeds in the circle group $\mathbb{T} = \mathbb{R}/\mathbb{Z}$. It will be convenient to identify $\mathbb{T}$ with the interval $[0,1)$. Denote by $\|x\|$ the distance of $x \in \mathbb{R}$ (or $x \in \mathbb{T}$) from the nearest integer. In [B, Prop. 2.1(1)] the following condition was shown to be sufficient for an infinite-dimensional parallelepiped IP-$(\alpha_n)_{n=1}^{\infty}$ to be dense in $\mathbb{T}$:

$$\sum_{n=1}^{\infty} \|h\alpha_n\| = \infty, \qquad h = 1, 2, \ldots$$

Our main result in this section (Proposition 2) consists of an analogue for finite-dimensional parallelepipeds, namely a sufficient condition for such parallelepipeds to be ε-dense. First we present

PROPOSITION 1. *A d-dimensional parallelepiped in $\mathbb{T}$ contains a non-trivial point x with $\|x\| \le 1/(d+1)$.*

Here a point $x \in IP\text{-}(\alpha_n)_{n=1}^d$ is *non-trivial* if it is a sum of a non-zero number of generators α_n. (Note that we may well have $x = 0$.)

Proof. Consider the following $d+1$ points:

$$y_i = \sum_{n=0}^{i} \alpha_n, \qquad i = 0, 1, \ldots, d.$$

Obviously, we can find two of them, say y_i and y_j, $0 \le i < j \le d$, with $\|y_j - y_i\| \le 1/(d+1)$. But then

$$\Big\| \sum_{n=i+1}^{j} \alpha_n \Big\| \le \frac{1}{d+1},$$

which proves the proposition.

Remark 1. As a d-dimensional parallelepiped contains $2^d - 1$ non-trivial points, one could expect to have in it usually a point whose distance from 0 is of the same order of magnitude as 2^{-d}. In general, however, the proposition cannot be improved, as the simple example $\alpha_1 = \alpha_2 = \ldots = \alpha_d = 1/(d+1)$ shows. Moreover, taking a small perturbation of these α_n's we obtain basically the same example, with the parallelepiped containing 2^d distinct points.

PROPOSITION 2. *For any $\varepsilon > 0$ there exists a $B = B(\varepsilon) \in \mathbb{N}$ such that for every sequence $(\alpha_n)_{n=1}^d$ in $\mathbb{T}$ satisfying*

$$\sum_{n=1}^{d} \|h\alpha_n\| > B, \qquad h = 1, 2, \ldots, B,$$

the parallelepiped $IP\text{-}(\alpha_n)_{n=1}^d$ is ε-dense.

Proof. Suppose, to the contrary, that there exists some $\varepsilon > 0$ such that for every $B \in \mathbb{N}$ there exists a finite sequence $\boldsymbol{\alpha}_B = (\alpha_{Bn})_{n=1}^{d_B}$ with

$$\sum_{n=1}^{d_B} \|h\alpha_{Bn}\| > B, \qquad h = 1, 2, \ldots, B,$$

the d_B-dimensional parallelepiped $\mathcal{P}_M = IP\text{-}\boldsymbol{\alpha}_B$ being not ε-dense.

Call a point $x \in \mathbb{T}$ a *multi-limit point of* $(\boldsymbol{\alpha}_B)_{B=1}^{\infty}$ if for every $\varepsilon > 0$ and positive integer N there exists a B such that the interval $(x-\varepsilon, x+\varepsilon)$ contains at least N points of $\boldsymbol{\alpha}_B$. Denote by $\mathcal{L}$ the set of all multi-limit points of $(\boldsymbol{\alpha}_B)$. Clearly, since $d_B \to \infty$ as $B \to \infty$, the set $\mathcal{L}$ is non-empty.

Take a point $x \in \mathcal{L}$. Taking a B for which $\boldsymbol{\alpha}_B$ contains sufficiently many points very close to x, one sees that the corresponding $\mathcal{P}_B$ contains modulo 1 a small perturbation of the set $\{nx : 1 \le n \le N\}$, where N can be made arbitrarily large by choosing B appropriately. Now the closure of the set $\{nx : n \in \mathbb{N}\}$ is a subgroup of $\mathbb{T}$, which is $\mathbb{T}$ itself if x is irrational, and $\{0, 1/g, 2/g, \ldots, (g-1)/g\}$ if x is rational with denominator g (in reduced form). Hence our assumption implies that $\mathcal{L}$ is a finite set of rationals, say $\mathcal{L} = \{0, 1/g, 2/g, \ldots, (g-1)/g\}$. Split each $\boldsymbol{\alpha}_B$ into $2g$ subsequences $\boldsymbol{\alpha}_B^{(j)}$, $1 \le j \le g$, placing in $\boldsymbol{\alpha}_B^{(j)}$ those elements of $\boldsymbol{\alpha}_B$ belonging to $[(j-1)/(2g), j/(2g))$. For each B select $j_0 = j_0(B)$ as the j for which $\sum_{x \in \boldsymbol{\alpha}_B^{(j)}} \|gx\|$ is maximal. Passing to a subsequence of $(\boldsymbol{\alpha}_B)_{B=1}^{\infty}$ we may assume $j_0(B)$ to be constant. Denote the sequence $\boldsymbol{\alpha}_B^{(j_0)}$ by $\boldsymbol{\beta}_B = (\beta_{Bn})_{n=1}^{d'_B}$. Define $\boldsymbol{\gamma}_B = (\gamma_{Bn})_{n=1}^{[d'_B/g]}$ by

$$\gamma_{Bn} = \sum_{i=1}^{g} \beta_{B,(g-1)n+i}, \qquad n = 1, 2, \ldots, [d'_B/g].$$

Passing to a subsequence again, we may assume that $\|\gamma_{Bn}\| < \varepsilon$ for every B and n. Our construction guarantees that $\sum_n \|\gamma_{Bn}\| \ge 1$ for sufficiently large B, so that IP-$\boldsymbol{\gamma}_B$ is ε-dense in $\mathbb{T}$. Since IP-$\boldsymbol{\alpha}_B \supseteq IP$-$\boldsymbol{\gamma}_B$, the original parallelepiped is ε-dense as well. This completes the proof.

3. Proofs. Proof of Theorem 2′. Take a positive integer $Q = q_1^{e_1} q_2^{e_2} \ldots q_k^{e_k}$. It will be slightly more convenient to consider, instead of S, the set $S' = S(Q) + 1$, consisting of all solutions of

$$x(x-1) \equiv 0 \pmod{Q}. \tag{4}$$

Define integers y_i, $1 \le i \le k$, in the range $[0, Q-1]$ by the requirements

$$y_i \equiv 1 \pmod{q_i^{e_i}}, \qquad y_i \equiv 0 \pmod{q_j^{e_j}}, \qquad 1 \le j \le k,\ j \ne i.$$

View the set $\{0, 1, \ldots, Q-1\}$ as the additive group $\mathbb{Z}/Q\mathbb{Z}$. It is readily verified that

$$S' = \{0, y_1\} + \{0, y_2\} + \ldots + \{0, y_k\}.$$

Put $r_i = y_i/Q$, $1 \le i \le k$. Note that r_i is (in reduced form) a rational with denominator $q_i^{e_i}$ for each i. Putting

$$R' = \{x/Q' : x \in S'\} \subseteq [0, 1),$$

and viewing $[0,1)$ again as the circle group $\mathbb{T}$, we obtain

$$R' = \{0, r_1\} + \{0, r_2\} + \ldots + \{0, r_k\}.$$

We have to show that, if $\sum_{i=1}^k q_i^{-e_i}$ is sufficiently large, then R' is ε-dense in $\mathbb{T}$. In fact, take B as in Proposition 2 and suppose that $\sum_{i=1}^k q_i^{-e_i} > B + \log B + 1$. Then for $1 \le h \le B$ we have

$$\begin{aligned}\sum_{i=1}^k \|hr_i\| &\ge \sum_{i:q_i^{e_i}>h} \|hr_i\| \ge \sum_{i:q_i^{e_i}>h} q_i^{-e_i}\\ &\ge \sum_{i=1}^k q_i^{-e_i} - \sum_{n=1}^B n^{-1} \ge (B + \log B + 1) - (\log B + 1) \ge B\,.\end{aligned}$$

By Proposition 2, this proves the theorem.

Proof of Theorem 3′. We proceed as in the proof of Theorem 2′. It has to be shown that (4) has a solution in the range $[2, Q/P(Q)+1]$. Let

$$\begin{aligned}S_1 &= \{0, y_1\} + \{0, y_2\} + \ldots + \{0, y_{k-1}\} \subset S',\\ R_1 &= \{0, r_1\} + \{0, r_2\} + \ldots + \{0, r_{k-1}\} \subset R'.\end{aligned}$$

By Proposition 1, R_1 contains a point $r = \sum_{i\in I} r_i$ $(\emptyset \ne I \subseteq \{1,2,\ldots,k-1\})$ with $\|r\| \le 1/k$. If $r \in [0, 1/k]$, then consider the number $s = rQ = \sum_{i\in I} y_i$ (mod Q). Clearly, s solves (4) and $|s| \le Q/k = Q/P(Q)$. Since $I \ne \emptyset$ we have $r \ne 0$, so that $s \ne 0$. Since $I \ne \{1,2,\ldots,k\}$ we have $s \ne 1$. Therefore, in this case s furnishes a solution of (4) as desired. If $r \in [1-1/k, 1)$, then take $J = \{1,2,\ldots,k\} - I$ and $r' = \sum_{i\in J} r_i$. Then

$$r' = 1 + \frac{1}{Q} - r \in \left(\frac{1}{Q}, \frac{1}{Q} + \frac{1}{k}\right].$$

Hence the corresponding solution of (4), namely $s' = r'Q = \sum_{i\in J} y_i$, is again in the required range. This completes the proof.

Proof of Theorem 4. Choose q_1 arbitrarily. Assume that $q_1, q_2, \ldots$ $\ldots, q_{k-1}$ have been chosen. The system of congruences

$$(5)\qquad q_1 q_2 \ldots q_{i-1} q_{i+1} \ldots q_{k-1} x \equiv 1 \pmod{q_i}, \qquad i = 1, 2, \ldots, k-1,$$

clearly has a solution x modulo $q_1 q_2 \ldots q_{k-1} = Q_{k-1}$. Any such solution is relatively prime to Q_{k-1}. By Dirichlet's theorem on the existence of primes in arithmetic progressions there exist infinitely many primes in the progression $x + Q_{k-1}\mathbb{N}$. Take one of these as q_k.

For each k, define integers (depending on k) y_i, $1 \le i \le k$, in the range $[0, Q_k - 1]$ by the requirements

$$(6)\qquad \begin{aligned}y_i &\equiv 1 \pmod{q_i},\\ y_i &\equiv 0 \pmod{q_j}, \qquad 1 \le j \le k,\ j \ne i.\end{aligned}$$

Our construction guarantees that

$$y_i = q_1 q_2 \ldots q_{i-1} q_{i+1} \ldots q_k, \qquad i = 1, 2, \ldots, k-1,$$
$$y_k \equiv Q_k + 1 - \sum_{j=1}^{k-1} y_j \pmod{Q_k}.$$

Putting

$$r_i = y_i / Q_k, \qquad 1 \le i \le k, \tag{7}$$

we consequently have

$$r_i = \frac{1}{q_i}, \qquad i = 1, 2, \ldots, k-1,$$
$$r_k \equiv 1 + \frac{1}{Q_k} - \sum_{j=1}^{k-1} \frac{1}{q_j} \pmod{1}.$$

Hence, setting $R'_k = \{0, r_1\} + \{0, r_2\} + \ldots + \{0, r_k\}$, we obtain

$$R'_k \subseteq \Bigg[0, \sum_{i=1}^{k-1} \frac{1}{q_i}\Bigg] \cup \Bigg[1 + \frac{1}{Q_k} - \sum_{i=1}^{k-1} \frac{1}{q_i}, 1\Bigg),$$

and therefore

$$R_k = R'_k - \frac{1}{Q_k} \subseteq \Bigg[0, \sum_{i=1}^{k-1} \frac{1}{q_i}\Bigg] \cup \Bigg[1 - \sum_{i=1}^{k-1} \frac{1}{q_i}, 1\Bigg).$$

Since, by our construction, the sequence q_k may clearly be chosen with $\sum_{k=1}^{\infty} 1/q_k$ arbitrarily small, this concludes the proof.

Proof of Theorem 5. Basically, the idea is to get close to the situation of the example given in Remark 1. We start as in the proof of Theorem 4, but instead of (5) require upon selecting each q_k that it satisfies the system

$$q_1 q_2 \ldots q_{i-1} \left\lceil \frac{q_i}{k} \right\rceil q_{i+1} \ldots q_k \equiv 1 \pmod{q_i}, \qquad i = 1, 2, \ldots, k-1.$$

Defining y_i and r_i, $1 \le i \le k$, by (6) and (7), we obtain

$$y_i = q_1 q_2 \ldots q_{i-1} \left\lceil \frac{q_i}{k} \right\rceil q_{i+1} \ldots q_k, \qquad i = 1, 2, \ldots, k-1,$$
$$y_k \equiv Q_k + 1 - \sum_{j=1}^{k-1} y_j \pmod{Q_k},$$

and therefore

$$r_i = \frac{\lceil q_i/k \rceil}{q_i}, \qquad i = 1, 2, \ldots, k-1,$$

$$r_k = 1 + \frac{1}{Q_k} - \sum_{j=1}^{k-1} \frac{\lceil q_i/k \rceil}{q_j}.$$

It follows that

$$\left| r_i - \frac{1}{k} \right| \le \frac{1}{q_i}, \qquad i = 1, 2, \ldots, k-1,$$

whence

$$\left| \sum_{i \in I} r_{ki} - \frac{|I|}{k} \right| \le \sum_{j=1}^{k-1} \frac{1}{q_j} + \frac{1}{Q_k}, \qquad I \subseteq \{1, 2, \ldots, k\}$$

(where $|I|$ denotes the cardinality of I). Consequently, if $s \ne 0, 1$ is any solution of (4), then $s = \sum_{i \in I} y_i$, with

$$\left| s - \frac{Q_k |I|}{k} \right| \le \left(\sum_{j=1}^{k-1} \frac{1}{q_j} + \frac{1}{Q_k} \right) Q_k.$$

Again, the sequence q_k may clearly be chosen with $\sum_{k=1}^{\infty} 1/q_k$ arbitrarily small, whence the theorem follows.

References

[B] D. Berend, *IP-Sets on the circle*, Canad. J. Math. 42 (1990), 575–589.

[BO] D. Berend and C. F. Osgood, *On the equation $P(x) = n!$ and a question of Erdős*, J. Number Theory 42 (1992), 189–193.

[E] P. Erdős, personal communication.

[F] H. Furstenberg, *Recurrence in Ergodic Theory and Combinatorial Number Theory*, Princeton University Press, Princeton, N.J., 1981.

[G] R. K. Guy, *Problems from Western Number Theory Conferences*, 1981, unpublished.

[NPP] C. Nelson, D. E. Penney and C. Pomerance, *714 and 715*, J. Recreational Math. 7 (1974), 87–89.

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE
BEN-GURION UNIVERSITY
BEER SHEVA 84105, ISRAEL

Received on 4.10.1993 (2501)