

**Zeitschrift:** L'Enseignement Mathématique  
**Herausgeber:** Commission Internationale de l'Enseignement Mathématique  
**Band:** 38 (1992)  
**Heft:** 1-2: L'ENSEIGNEMENT MATHÉMATIQUE

**Artikel:** REAL NUMBERS WITH BOUNDED PARTIAL QUOTIENTS: A SURVEY  
**Autor:** Shallit, Jeffrey  
**Kapitel:** 14. PSEUDO-RANDOM NUMBER GENERATION  
**DOI:** <https://doi.org/10.5169/seals-59489>

### **Nutzungsbedingungen**

Die ETH-Bibliothek ist die Anbieterin der digitalisierten Zeitschriften. Sie besitzt keine Urheberrechte an den Zeitschriften und ist nicht verantwortlich für deren Inhalte. Die Rechte liegen in der Regel bei den Herausgebern beziehungsweise den externen Rechteinhabern. [Siehe Rechtliche Hinweise.](#)

### **Conditions d'utilisation**

L'ETH Library est le fournisseur des revues numérisées. Elle ne détient aucun droit d'auteur sur les revues et n'est pas responsable de leur contenu. En règle générale, les droits sont détenus par les éditeurs ou les détenteurs de droits externes. [Voir Informations légales.](#)

### **Terms of use**

The ETH Library is the provider of the digitised journals. It does not own any copyrights to the journals and is not responsible for their content. The rights usually lie with the publishers or the external rights holders. [See Legal notice.](#)

**Download PDF:** 02.04.2025

**ETH-Bibliothek Zürich, E-Periodica, <https://www.e-periodica.ch>**

if the limit exists. Then Veech showed that  $\mu_\theta(I)$  exists for all  $I \subseteq [0, 1)$  if and only if the partial quotients of  $\theta$  are bounded.

For other connections with ergodic theory, see the papers of Stewart [286]; del Junco [154]; Dani [70, 72]; and Baggett and Merrill [14, 15].

#### 14. PSEUDO-RANDOM NUMBER GENERATION

Lehmer [183] introduced the *linear congruential method* for pseudo-random number generation. Let  $X_0, m, a, c$  be given, and define

$$X_{k+1} = aX_k + c \pmod{m},$$

for  $k \geq 0$ . For this to be a good source of “random” numbers, we want the sequence  $X_k$  to be uniformly distributed, as well as the sequence of pairs  $(X_k, X_{k+1})$ , triples, etc.

A test for randomness called the *serial test* on pairs  $(X_k, X_{k+1})$  amounts to the two-dimensional version of the discrepancy mentioned above in Section 12. This turns out to be essentially the function  $\rho(\mathbf{g}, m)$  defined in Section 10. Thus linear congruential generators that pass the pairwise serial test arise from rationals  $a/m$  having small partial quotients in their continued fraction expansion. See the papers of Dieter [87, 88]; Niederreiter [219, 220, 222]; Knuth [170, Section 3.3.3]; and Borosh and Niederreiter [42].

#### 15. FORMAL LANGUAGE THEORY

Let  $w = w_0w_1w_2 \cdots$  be an infinite word over a finite alphabet. We say that the finite word  $x = x_0x_1 \cdots x_n$  is a *subword* of  $w$  if there exists  $m \geq 0$  such that  $w_{m+i} = x_i$ , for  $0 \leq i \leq n$ . We say that  $w$  is *k-th power free* if  $x^k$  is never a subword of  $w$ , for all nonempty words  $x$ . Here is a classical example: let  $s(n)$  denote the number of 1's in the binary expansion of  $n$ . Then the infinite word of Thue-Morse

$$t = t_0t_1t_2 \cdots = 0110100110010110 \cdots,$$

defined by  $t_n = s(n) \pmod{2}$ , is cube-free.

Another way to define infinite words is as the fixed point of a homomorphism on a finite alphabet. For example, the Thue-Morse word  $t$  is a fixed point of  $\varphi$ , where  $\varphi(0) = 01$  and  $\varphi(1) = 10$ .