数理解析研究所講究録
537巻 1984年 18-28

13

Number-theoretic problems in pseudorandom number generation

Harald Niederreiter

Pseudorandom numbers are used for the deterministic simulation of random variables. They are of great importance for general simulation purposes, and in particular for the Monte Carlo method in numerical analysis which is based on simulation. Ideally, we should work with "true" random numbers in a Monte Carlo method. However, if a Monte Carlo method is implemented on a computer, then the use of "true" random numbers becomes problematic, and one prefers to work with numbers that can be generated in the computer by a systematic algorithm, i.e. with pseudorandom numbers. It is an important requirement that pseudorandom numbers can be generated very quickly, since in a typical Monte Carlo calculation we may need about 10^5 pseudorandom numbers.

A sequence of pseudorandom numbers (abbreviated PRN) should satisfy the following properties:

(i) it is generated by a fast deterministic algorithm;

(ii) it possesses good statistical properties similar to those of "true" random numbers, in particular good distribution and statistical independence properties.

A sequence of PRN should simulate a given statistical distribution. There is of course a multitude of interesting distributions, e.g. the normal distribution, the exponential distribution, and so on. Therefore it is more efficient to proceed in the following manner. We select a standard distribution and study methods of simulating this standard distribution by PRN. As a standard distribution we choose a simple one, namely the uniform distribution

$$U(x) = \begin{cases} 0 & \text{for } x < 0, \\ x & \text{for } 0 \leq x \leq 1, \\ 1 & \text{for } x > 1. \end{cases}$$

To simulate this distribution, it suffices to take PRN from the interval $[0,1]$. If one knows how to simulate $U(x)$, then by well-known transformations one can obtain PRN that simulate any other given distribution; see [3, Ch. 5], [6, Ch. 3]. PRN simulating the uniform distribution are called uniform PRN.

/

The most common method of generating uniform PRN is the so-called linear congruential method, which was proposed by D. H. Lehmer [10] in the early days of the Monte Carlo method. If used properly, this method combines simplicity with excellent performance. Let $M \in \mathbb{N}$ be large, let $\lambda \in \mathbb{N}$ with $2 \leq \lambda < M$ and $g.c.d(\lambda,M) = 1$, and let $r \in \mathbb{Z}$. We generate a sequence $y_0,y_1,\ldots$ of integers with $0 \leq y_n < M$ by the recursion

$$y_{n+1} \equiv \lambda y_n + r \bmod M \quad \text{for} \quad n \geq 0.$$

We obtain uniform PRN in $[0,1]$ by an appropriate scaling, i.e. by setting $x_n = y_n/M$ for $n \geq 0$. The following terminology is standard: M is called the modulus and λ the multiplier. In practice, one chooses M in such a way that the residue arithmetic is simplified, namely M prime (e.g. $M = 2^{31} - 1$) or M a power of 2 (e.g. $M = 2^{35}$).

Our first observation is that the sequence (y_n), and thus (x_n), is periodic. If τ is the length of the least period, then we always have $\tau \leq M$. Of course, periodicity is not a property of "true" random numbers. However, this drawback does not play a role if τ is larger than the number of PRN to be used. Therefore, one is only interested in the case where τ is large. Since we have chosen M large, it is possible to obtain large values of τ. It is customary to consider the following three cases in which we achieve $\tau \approx M$:

1) M prime, λ primitive root mod M, $r = 0$, $y_0 \neq 0$ (then $\tau = M - 1$);
2) $M = 2^{\alpha}$, $\lambda \equiv 5 \bmod 8$, $r \equiv 1 \bmod 2$ (then $\tau = M$);
3) $M = 2^{\alpha}$, $\lambda \equiv 5 \bmod 8$, $r = 0$, $y_0 \equiv 1 \bmod 2$ (then $\tau = M/4$).

For a more detailed account of the elementary properties of linear congruential PRN we refer to [6, Ch. 3], [16].

For the applications it is important to study the behavior of these PRN under statistical tests, especially tests for the quality of distribution and for statistical independence. Let $x_0,x_1,\ldots$ be a sequence of linear congruential PRN and let $s \in \mathbb{N}$. We consider the points

$$\underline{x}_n = (x_n,x_{n+1},\ldots,x_{n+s-1}) \in [0,1]^s, \quad n \geq 0. \tag{1}$$

In the ideal case where the x_n are uniformly distributed and independent random variables, the random vector $\underline{x}_n$ would be uniformly distributed over $[0,1]^s$. Therefore, we can measure the quality of the first N points in (1) by considering the maximal deviation between their empirical distribution and the uniform distribution on $[0,1]^s$. This leads to the so-called discrepancy

$$D_N^{(s)} = \sup_J \left| F_N(J) - |J| \right|,$$

where the supremum is extended over all subintervals J of $[0,1]^s$ with one vertex at the origin, $F_N(J) = N^{-1}\,\mathrm{card}\{n < N : \underline{x}_n \in J\}$ is the empirical distribution, and $|J|$ denotes the s-dimensional Lebesgue measure of J. For $s = 1$ a small value of $D_N^{(s)}$ means a good distribution behavior of the x_n, and for $s \geq 2$ a small value of $D_N^{(s)}$ means that s consecutive x_n are nearly statistically independent. General information on the discrepancy can be found in [8, Ch. 2], [16].

The statistical test based on the discrepancy (usually called the serial test) is also of interest because it leads to effective error bounds in a standard application of PRN, namely multidimensional numerical integration. This is discussed in detail in [20]. Here we mention only the following fact: if the integrand f has bounded variation $V(f)$ on $[0,1]^s$ in the sense of Hardy and Krause and if the points $\underline{x}_n$ are as in (1), then

$$(2) \qquad \left| \frac{1}{N} \sum_{n=0}^{N-1} f(\underline{x}_n) - \int_{[0,1]^s} f(\underline{x})\, d\underline{x} \right| \leq V(f) D_N^{(s)}.$$

For a later application we note that in the case $s = 2$ the variation $V(f)$ of a function $f = f(x,y)$ on $[0,1]^2$ is given by

$$(3) \qquad V(f) = \int_0^1 \int_0^1 \left| \frac{\partial^2 f(x,y)}{\partial x\, \partial y} \right| dx\, dy + \int_0^1 \left| \frac{df(x,1)}{dx} \right| dx + \int_0^1 \left| \frac{df(1,y)}{dy} \right| dy,$$

provided that all the indicated (partial) derivatives are continuous; compare with [16, Sec. 2].

The serial test for dimension s is at least as powerful as any other statistical test using s or fewer consecutive x_n. For $s = 2$ a widely used test for the pair correlation of consecutive x_n is based on the calculation of the serial correlation coefficient

$$\sigma_N = \frac{M[(x_n - M(x_n))(x_{n+1} - M(x_{n+1}))]}{M[(x_n - M(x_n))^2]^{1/2}\, M[(x_{n+1} - M(x_{n+1}))^2]^{1/2}},$$

where for given numbers $t_0, t_1, \ldots, t_{N-1}$ we define

$$M(t_n) = \frac{1}{N} \sum_{n=0}^{N-1} t_n.$$

The PRN pass the test if $|\sigma_N|$ is small. The following result shows that

$|\sigma_N|$ is small whenever $D_N^{(2)}$ is small. We note that this result does not depend on special properties of linear congruential PRN, but holds for any numbers $x_0, x_1, \ldots, x_N \in [0,1]$ for which the denominator of σ_N does not vanish.

Theorem 1. $|\sigma_N| < 73\, D_N^{(2)}$.

Proof. Put $D = D_N^{(2)}$ and note that if $D > \frac{1}{73}$, then $|\sigma_N| < 73\, D$ since we always have $|\sigma_N| \leq 1$ by the Cauchy-Schwarz inequality. Now assume $D \leq \frac{1}{73}$. For the numerator $\mathrm{Num}(\sigma_N)$ of σ_N a simple calculation shows that

$$\mathrm{Num}(\sigma_N) = M(x_n x_{n+1}) - M(x_n)\, M(x_{n+1}) \tag{4}$$

$$= [M(x_n x_{n+1}) - \tfrac{1}{4}] - [M(x_n)\, M(x_{n+1}) - \tfrac{1}{4}].$$

We apply (2) with the points $\underline{x}_n = (x_n, x_{n+1})$, $0 \leq n \leq N-1$, and $f(x,y) = xy$. Then together with (3) we obtain

$$\left| M(x_n x_{n+1}) - \tfrac{1}{4} \right| = \left| \frac{1}{N} \sum_{n=0}^{N-1} x_n x_{n+1} - \int_0^1 \int_0^1 xy\, dx\, dy \right| \leq 3D.$$

Similarly, using $f(x,y) = x$ and $f(x,y) = y$, respectively, we get

$$\left| M(x_n)\, M(x_{n+1}) - \tfrac{1}{4} \right| =$$

$$= \left| [M(x_n) - \tfrac{1}{2}][M(x_{n+1}) - \tfrac{1}{2}] + \tfrac{1}{2}[M(x_n) - \tfrac{1}{2}] + \tfrac{1}{2}[M(x_{n+1}) - \tfrac{1}{2}] \right| \leq D^2 + D.$$

It follows from (4) that

$$\left| \mathrm{Num}(\sigma_N) \right| \leq 4D + D^2 \leq \frac{293}{73}\, D. \tag{5}$$

For the denominator $\mathrm{Den}(\sigma_N)$ we have

$$\mathrm{Den}(\sigma_N)^2 = M[(x_n - M(x_n))^2]\, M[(x_{n+1} - M(x_{n+1}))^2] \tag{6}$$

$$= [M(x_n^2) - M(x_n)^2][M(x_{n+1}^2) - M(x_{n+1})^2].$$

Now

$$M(x_n^2) - M(x_n)^2 = \frac{1}{N}\sum_{n=0}^{N-1} x_n^2 - \left(\frac{1}{N}\sum_{n=0}^{N-1} x_n\right)^2$$

$$= \frac{1}{12} + \left(\frac{1}{N}\sum_{n=0}^{N-1} x_n^2 - \frac{1}{3}\right) - \left(\frac{1}{N}\sum_{n=0}^{N-1} x_n - \frac{1}{2}\right) - \left(\frac{1}{N}\sum_{n=0}^{N-1} x_n - \frac{1}{2}\right)^2$$

$$\geqq \frac{1}{12} - 2D - D^2$$

by (2) with $f(x,y) = x^2$ and $f(x,y) = x$, respectively. The same lower bound holds for the second factor in (6), hence

$$\mathrm{Den}(\sigma_N) \geqq \frac{1}{12} - 2D - D^2 \geqq \frac{1}{12} - \frac{2}{73} - \frac{1}{73^2} = \frac{3565}{12\cdot 73^2}.$$

Together with (5) we obtain

$$|\sigma_N| \leqq \frac{293\cdot 12\cdot 73}{3565} D < 73D. \quad \square$$

In the case of linear congruential PRN, effective bounds for $D_N^{(s)}$ are available. Because of earlier remarks it suffices to consider $D_N^{(s)}$ only for $1 \leqq N \leqq \tau$. The case $s = 1$ and general N was treated by the author [13], the case $s = 2$ and $N = \tau$ by Dieter [4], and the case of a general $s \geqq 2$ and general N by the author [14], [15], [19]. The results can be described as follows. For a lattice point $\underline{h} = (h_1,\ldots,h_s) \in \mathbb{Z}^s$ define

$$R(\underline{h}) = \prod_{i=1}^{s} \max(1, 2|h_i|).$$

For $m \in \mathbb{N}$ let

$$\rho^{(s)}(\lambda,m) = \min_{\underline{h}} R(\underline{h}),$$

where the minimum is extended over all $\underline{h} \neq \underline{0}$ with

$$\sum_{i=1}^{s} h_i \lambda^{i-1} \equiv 0 \mod m.$$

Theorem 2. In the cases 1), 2), 3) we have

$$\frac{c_1(s)}{\rho^{(s)}(\lambda,m)} \leqq D_\tau^{(s)} \leqq \frac{c_2(s)(\log M)^s}{\rho^{(s)}(\lambda,m)},$$

$$\frac{c_1(s)}{\rho^{(s)}(\lambda,m)} \leqq D_N^{(s)} \leqq \frac{c_3(s)\, M^{1/2}\, (\log M)^{s+1}}{N} + \frac{c_4(s)(\log M)^s}{\rho^{(s)}(\lambda,m)} \quad \text{for } 1 \leqq N < \tau,$$

where the $c_j(s)$, $1 \leq j \leq 4$, are effective positive constants only depending on s, and where $m = M$ in the cases 1) and 2) and $m = M/4$ in case 3).

The quality of the linear congruential PRN can thus be measured by the so-called figure of merit $\varrho^{(s)}(\lambda,m)$, which should be as large as possible. Although Theorem 2 is quite satisfactory, there are still various open problems connected with it. We will discuss several of these problems, which are all of number-theoretic character.

For $s = 1$ it is immediate that always $\varrho^{(1)}(\lambda,m) = 2m$. For $s \geq 2$ we can choose $h = (h_1, 1, 0,\ldots,0)$ with $h_1 \equiv -\lambda \bmod m$, $|h_1| \leq m/2$, so that always $\varrho^{(s)}(\lambda,m) \leq 2m$. In the case $s = 2$ there is an interesting connection with continued fractions. For our purposes it suffices to consider the case $g c d(\lambda,m) = 1$. Let

$$\frac{\lambda}{m} = [a_0;a_1,\ldots,a_k]$$

be the continued fraction expansion of λ/m in the standard notation, where we assume $a_k = 1$ for the sake of uniqueness. Let

$$\frac{p_j}{q_j} = [a_0;a_1,\ldots,a_j], \quad 0 \leq j \leq k,$$

be the convergents of λ/m. Then we have the formula

$$\varrho^{(2)}(\lambda,m) = 4 \min_{0 \leq j < k} q_j |p_j m - q_j \lambda| \tag{7}$$

obtained by Borosh and the author [2]. This formula allows the calculation of $\varrho^{(2)}(\lambda,m)$ in $O(\log m)$ steps, whereas a calculation by the definition would require $O(m)$ steps. If

$$K = K(\frac{\lambda}{m}) = \max_{1 \leq j \leq k} a_j,$$

then we have the bounds

$$\frac{4m}{K+2} \leq \varrho^{(2)}(\lambda,m) \leq \frac{4m}{K}.$$

The good parameters λ are therefore those with a small value of $K(\lambda/m)$. This leads already to the first open problem.

Problem 1 (Conjecture of Zaremba [22]). Prove that for every $m \geq 2$ there exists a λ with $g c d(\lambda,m) = 1$ and $K(\lambda/m) \leq 5$, or just $K(\lambda/m) \leq C$ with an absolute constant C.

This has been checked numerically for $m \leq (3.2)\cdot 10^6$ by Knuth [7] and for $m = 2^\alpha$, $\alpha \leq 35$, by Borosh and the author [2], yielding $C = 5$ in this range and even $C = 3$ for sufficiently large m. The best theoretical result says that we can always obtain $K(\lambda/m) \leq C_1 \log m$ with an absolute constant C_1; see [16, Sec. 4]. For the applications to PRN generation we also want λ to be a primitive root mod m if m is prime and $\lambda \equiv 5 \mod 8$ if $m = 2^\alpha$; see [2], [16, Sec. 11].

An algorithm for the determination of optimal λ, i.e. of those λ yielding the maximal value of $\rho^{(s)}(\lambda,m)$ for given s and m, was developed by Borosh and the author [2] for the case $s = 2$ on the basis of formula (7). This leads to two related problems.

Problem 2. Generalize (7) to a formula for $\rho^{(s)}(\lambda,m)$, $s \geq 3$, possibly using a suitable $(s-1)$-dimensional continued fraction algorithm.

Problem 3. Develop an efficient search algorithm for optimal λ in the case $s \geq 3$. This algorithm should be substantially faster than the trial-and-error search of all possible values of λ.

We turn now to results about the order of magnitude of $\rho^{(s)}(\lambda,m)$. In case 1) we have to consider $\rho^{(s)}(\lambda,m)$ with a prime m and a primitive root λ mod m. It was shown by the author [14] that for any $s \geq 2$ and any prime m there exists a primitive root λ mod m with

$$\rho^{(s)}(\lambda,m) > \frac{c(s)m}{(\log m)^{s-1} \log\log m}.$$

In the cases 2) and 3) we have to consider $\rho^{(s)}(\lambda,m)$ with m a power of 2 and $\lambda \equiv 5 \mod 8$. It was shown in [14] that for $s = 2$ and any $m = 2^\alpha$ there exists λ in a prescribed odd residue class mod 8 with

$$\rho^{(2)}(\lambda,m) > \frac{c(2)m}{\log m}.$$

In the above and in the sequel, $c(s)$ denotes an effective positive constant only depending on s.

Problem 4. Prove that for any $s \geq 3$ and any $m = 2^\alpha$ there exists λ in a prescribed odd residue class mod 8 with

$$\varrho^{(s)}(\lambda,m) > \frac{c(s)m}{(\log m)^{s-1}} .$$

We note that a noneffective version of the result desired in Problem 4 can be obtained from a method of Zaremba [23]. There are also results that contain stronger information on the order of magnitude of $D_\tau^{(s)}$ itself. In case 1) it was shown by the author [14] that for any $s \geqq 2$ and any prime modulus M there exists a multiplier λ which is a primitive root mod M and for which

$$D_\tau^{(s)} \leqq \frac{c(s)(\log M)^s \log\log M}{M} .$$

In the cases 2) and 3) an analogous result was shown in [14] for $s = 2$: for any modulus $M = 2^\alpha$ there exists a multiplier $\lambda \equiv 5 \bmod 8$ with

$$D_\tau^{(2)} \leqq \frac{c(2)(\log M)^2}{M} .$$

Problem 5. Prove that for any $s \geqq 3$ and any modulus $M = 2^\alpha$ there exists a multiplier $\lambda \equiv 5 \bmod 8$ with

$$D_\tau^{(s)} \leqq \frac{c(s)(\log M)^s}{M} .$$

Recently the case $s = 3$ of this problem was solved by the Austrian mathematician Larcher [9]. Since for any τ points in $[0,1]^s$ the smallest known value of the discrepancy is $D_\tau^{(s)} = O(\tau^{-1}(\log\tau)^{s-1})$, and since $\tau \approx M$ in our cases, we may pose the following (rather difficult) problem.

Problem 6. In the cases 1), 2), 3) prove that for any $s \geqq 2$ and any modulus M there exists a multiplier λ such that

$$D_\tau^{(s)} \leqq \frac{c(s)(\log M)^{s-1}}{M} .$$

It follows from [16, Theorem 11.11] that if Problem 1 can be solved for m prime and λ a primitive root mod m, or for $m = 2^\alpha$ and $\lambda \equiv 5 \bmod 8$, then the statement in Problem 6 holds for $s = 2$. The existence theorems mentioned above are all nonconstructive, so an even

more challenging problem would ask for general explicit contructions of parameters λ meeting the various bounds above.

Quite a different test for the performance of linear congruential PRN is based on ideas from the geometry of numbers. For a given dimension $s \geq 2$ we consider again the points

$$\underline{x}_n = (x_n, x_{n+1}, \ldots, x_{n+s-1}) \in [0,1]^s, \quad 0 \leq n < \tau,$$

from the full period, and in case 1) we add the point $\underline{0}$. Then we extend this point set periodically over $\mathbb{R}^s$ with period 1 in each coordinate. It turns out that this extended set E is either a lattice or a shifted lattice. In detail, let L be the lattice

$$L = \{ k_1\underline{b}_1 + \ldots + k_s\underline{b}_s : k_i \in \mathbb{Z} \text{ for } 1 \leq i \leq s\},$$

where

$$\underline{b}_1 = \frac{1}{m}(1, \lambda, \lambda^2, \ldots, \lambda^{s-1}),$$

$$\underline{b}_i = \text{ith unit vector for } 2 \leq i \leq s,$$

with m being defined as in Theorem 2. Then $E = L$ in case 1) and $E = \underline{x}_0 + L$ in the cases 2) and 3); see Beyer [1], Marsaglia [12], and Ripley [21]. For good PRN the lattice L should fill $\mathbb{R}^s$ in a "dense" manner. We measure the "denseness" of L as follows. Let S be the maximal distance between parallel hyperplanes in any family of parallel hyperplanes covering L, and put $\nu = S^{-1}$. The quantity ν should be large for good PRN. In fact, ν is connected with the successive minima $m_1, m_2, \ldots, m_s$ of the lattice L. We have $1 \leq \nu m_s \leq c(s)$, i.e. the order of magnitude of ν is essentially given by m_s^{-1}, and furthermore $\nu = mm_1$ for $s = 2$ with m as in Theorem 2; see Ripley [21].

The quantity ν can also be described in terms of the dual lattice

$$L^* = \{ k_1\underline{b}_1^* + \ldots + k_s\underline{b}_s^* : k_i \in \mathbb{Z} \text{ for } 1 \leq i \leq s\},$$

where $\underline{b}_1^*, \ldots, \underline{b}_s^*$ is the dual basis of $\underline{b}_1, \ldots, \underline{b}_s$, that is $\underline{b}_i \cdot \underline{b}_j^* = \delta_{ij}$. Then we have $\nu = m_1^*$, i.e. ν is equal to the length of the shortest nonzero vector in L^*. Various algorithms are known for finding or approximating the length of the shortest nonzero vector in a lattice. The algorithm of Dieter [5] gives ν exactly, and the algorithm of Lenstra, Lenstra, and Lovász [11] gives ν up to a factor at most $2^{(s-1)/2}$. It would be of interest to compare the running times of these algorithms.

We note that for another important class of uniform PRN, namely that of Tausworthe PRN, the behavior under the serial test was recently studied by the author, but we will not dwell on this subject here and refer the interested reader to the papers [17], [18].

References

1. W. A. Beyer, Lattice structure and reduced bases of random vectors generated by linear recurrences, Applications of Number Theory to Numerical Analysis (S. K. Zaremba, ed.), pp. 361-370, Academic Press, New York, 1972.
2. I. Borosh and H. Niederreiter, Optimal multipliers for pseudo-random number generation by the linear congruential method, BIT 23, 65-74 (1983).
3. P. Bratley, B. L. Fox, and L. E. Schrage, A Guide to Simulation, Springer-Verlag, New York, 1983.
4. U. Dieter, Pseudo-random numbers: The exact distribution of pairs, Math. Comp. 25, 855-883 (1971).
5. U. Dieter, How to calculate shortest vectors in a lattice, Math. Comp. 29, 827-833 (1975).
6. D. E. Knuth, The Art of Computer Programming, Vol. 2: Semi-numerical Algorithms, 2nd ed., Addison-Wesley, Reading, Mass., 1981.
7. D. E. Knuth, personal communication.
8. L. Kuipers and H. Niederreiter, Uniform Distribution of Sequences, Wiley-Interscience, New York, 1974.
9. G. Larcher, personal communication.
10. D. H. Lehmer, Mathematical methods in large-scale computing units, Proc. 2nd Symp. on Large-Scale Digital Calculating Machinery (Cambridge, Mass., 1949), pp. 141-146, Harvard Univ. Press, Cambridge, Mass., 1951.
11. A. K. Lenstra, H. W. Lenstra, Jr., and L. Lovász, Factoring polynomials with rational coefficients, Math. Ann. 261, 515-534 (1982).
12. G. Marsaglia, The structure of linear congruential sequences, Applications of Number Theory to Numerical Analysis (S. K. Zaremba, ed.), pp. 249-285, Academic Press, New York, 1972.

13. H. Niederreiter, On the distribution of pseudo-random numbers generated by the linear congruential method. I, II, III, Math. Comp. 26, 793-795 (1972); 28, 1117-1132 (1974); 30, 571-597 (1976).

14. H. Niederreiter, Pseudo-random numbers and optimal coefficients, Advances in Math. 26, 99-181 (1977).

15. H. Niederreiter, The serial test for linear congruential pseudo-random numbers, Bull. Amer. Math. Soc. 84, 273-274 (1978).

16. H. Niederreiter, Quasi-Monte Carlo methods and pseudo-random numbers, Bull. Amer. Math. Soc. 84, 957-1041 (1978).

17. H. Niederreiter, Applications des corps finis aux nombres pseudo-aléatoires, Sém. Théorie des Nombres 1982-1983, Exp. 38, Univ. de Bordeaux I, Talence, 1983.

18. H. Niederreiter, The performance of k-step pseudorandom number generators under the uniformity test, SIAM J. Sci. Statist. Computing, to appear.

19. H. Niederreiter, The serial test for pseudo-random numbers generated by the linear congruential method, preprint, 1983.

20. H. Niederreiter, Multidimensional numerical integration using pseudo-random numbers, preprint, 1984.

21. B. D. Ripley, The lattice structure of pseudo-random number generators, Proc. Roy. Soc. London Ser. A 389, 197-204 (1983).

22. S. K. Zaremba, La méthode des "bons treillis" pour le calcul des intégrales multiples, Applications of Number Theory to Numerical Analysis (S. K. Zaremba, ed.), pp. 39-119, Academic Press, New York, 1972.

23. S. K. Zaremba, Good lattice points modulo composite numbers, Monatsh. Math. 78, 446-460 (1974).

Mathematical Institute
Austrian Academy of Sciences
Dr. Ignaz-Seipel-Platz 2
A-1010 Vienna
Austria