Designs of Uniform and Independent Random Numbers with Long Period and High Precision

Control of the Sequential Geometry through Product Group Structures and Lattice Configurations

Hiroshi Nakazawa[1] **and Naoya Nakazawa**[2]

(March 9-July 8, 2008)

Abstract Any sequence $\{x_1, x_2, \cdots, x_T\}$ of integers fulfilling $0 \leq x_j < z$ for all j and for an integer $z \geq 2$ may be identified with a period of the base-z numeral representation of an irreducible fraction $n/d = 0.\dot{x}_1 x_2 \cdots \dot{x}_T$ with $0 < n < d$. The division process for n/d implies that the quotient x_j is large or small in accordance with the preceding remainder r_j, as the estimate $0 < r_j/d - x_j/z < 1/z$ shows precisely. This plain fact is notable in two respects for large d and z. The one is that noted remainders

$$\{r_1 = n, r_2, r_3, \cdots\} \equiv \{n, nz, nz^2, \cdots\} \equiv n\{1, z, z^2, \cdots\} \equiv: n <z> \mod (d)$$

are integers in $(0, d)$ produced by the multiplicative congruential random number generator with modulus d and multiplier z. The other is that $\{x_j/z| \ \ j = 1, 2, \cdots\}$ may be any sample of uniform and independent random numbers, truncated to a suitable precision so as to give an integer x_j. Thus, the multiplicative congruential method is the central existence among uniform random number generators, as a representative of all others to within a prescribed precision $1/z$. We thus examined anew the reduced residue class group Z_d^* formed by integers coprime to a *composite* modulus d, and found a vein of ingenious, non-linear shuffling associated with Chinese remainder theorem that composes the cyclic subgroup $<z>= \{1, z, z^2, \cdots\}$ or any of its coset $n<z>$ in Z_d^* from component cyclic (sub)groups or their respective cosets. The full comprehension of the mechanism reveals novel prescriptions that will furnish computers feasibly with simple, fast and *spectrally tested* generators of uniform and independent random numbers which will have amply long periods and high precision, together with the freedom from improbable symmetry restrictions on the geometry of points they generate.

1. Introduction and summary

Random number generators on computers are restricted by the requirement that they should be reproducible and transportable; they should generate identical sequences any number of times on demands of users performing simulations, and should also do so on different computers as well.

[1]Mail address: h-nkzw@lapis.plala.or.jp.
[2]Mail address: nao-nkzw@cpost.plala.or.jp.

Random number generators on computers should thus deal exclusively with sequences of integers whose arithmetic is free from truncation or round off error. This report aims to show the existence of a novel way in the line to equip computers with fast generators for uniform and independent random numbers, with amply long period and high numerical precision, together with statistical properties ensured by spectral tests. Even the geometry of points, formed by consecutive numbers they generate, will be controllable so as to be freed of improbable symmetry restrictions.

Noted generators belong to the class of multiplicative congruential method of Lehmer.[3] This is a choice motivated by simple facts of arithmetic.[4] Take an arbitrary sequence $\{x_1, x_2, \cdots, x_T\}$ of positive or zero integers which are smaller than a prescribed integer $z \geq 2$. This finite sequence admits an obvious identification with a period of a base-z numeral representation of an irreducible fraction $n/d = 0.\dot{x}_1 x_2 \cdots \dot{x}_T$ with $0 < n < d$. As detailed in Sec. 2, procedures of division n/d stipulate that every term of the sequence $\{x_j/z |\ j = 1, 2, \cdots\}$ is approximated, to within a uniform error bound $1/z$, by the corresponding term in the sequence $\{r_j/d |\ j = 1, 2, \cdots\}$ constructed on remainders $\{r_j |\ 0 < r_j < d,\ j = 1, 2, \cdots\}$. Since the integer sequence $\{x_1, x_2, \cdots\}$ is arbitrary, it may be any sample of uniform and independent random number sequences of physical origin, with its numbers multiplied by a large integer z and truncated to form the noted sequence of integers. Or, it may well be a sequence of pseudo-random numbers generated by any numerical procedures on computers.

The sequence of remainders

$$\{r_1 = n, r_2, \cdots\} \equiv \{n, nz, nz^2, \cdots\} \equiv n\{1, z, z^2, \cdots\} \equiv n <z> \bmod(d),$$

is the n-coset of the cyclic subgroup $<z>:\equiv \{1, z, z^2, \cdots\} \bmod (d)$ generated by z in the reduced residue class group Z_d^*, which is formed by integers coprime to the modulus d. Multiplicative congruential generators thus rule all of uniform random number sequences, as they approximate ably any members of the latter, if only the modulus d is allowed to be an arbitrary composite integer formed by distinct primes. All new features of our analysis stem from this seemingly minute change of the modulus d to be a general composite integer with the factorization

$$d = {p_1}^{i_1} {p_2}^{i_2} \cdots {p_s}^{i_s},$$

where $p_1, p_2, \cdots, p_s$ are distinct primes and $i_1, i_2, \cdots, i_s$ are their respective positive exponents. It calls naturally for Chinese remainder theorem (or Sun Tsu's theorem) that establishes the group isomorphism $\approx$ between Z_d^* and the direct product group,

$$Z_d^* \approx Z_{{p_1}^{i_1}}^* \times Z_{{p_2}^{i_2}}^* \times \cdots \times Z_{{p_s}^{i_s}}^*.$$

The aim of the report is to answer the question: How should we design a good random number generator on this perspective of generalized structures? Happy to say, mathematical notions for the analysis, noted Chinese remainder theorem and direct product group structures, are all ripe for us to use, and the analysis reveals that Chinese remainder theorem, besides nice conservation of group structures, is even furnishing us with ingenious methods of shuffling, so to say, in the sense of random number generation problems. We are further equipped with the established technological weapon, the spectral test based on lattice structures inherent in multiplicative (and linear) congru-

[3] D. H. Lehmer: "Mathematical methods in large scale computing units," Annals Comp. Lab. Harvard Vol. **26** (1951) pp. 141-146.

[4] H. Nakazawa: "Coset representation of uniform and independent random number sequences I. Cosets associated with periodic sequences," http://www10.plala.or.jp/h-nkzw/ (August, 2004).

ential random number sequences.[5] The test enables us to select outstanding multipliers by specific examinations of z, even in the present setting with generalizations. Last but not least, notions of groups, in particular Lagrange's theorem to denote only one, help us to select desirable structures generically for the composite modulus d itself.

We shall have better prospects by summarizing conclusions and prescriptions for the generator design beforehand, putting some details off to Sections 7 and 8. They run as (I)-(IV) below.

(I) Choose two odd, distinct primes p_1, p_2 satisfying requirements that

$$q_1 := (p_1 - 1)/2, \quad q_2 := (p_2 - 1)/2$$

are coprime and different in their parity.

(II) For respective $j = 1, 2$ perform spectral tests on all primitive roots of $Z^*_{p_j}$ examining l-tuples[6] of consecutive numbers in $<z_j>$ up to $l = 6$, and take several multipliers $\{z_j, z'_j, \cdots\}$ that show the best performance.

(III) Use Chinese remainder theorem to determine the multiplier z for the modulus $d = p_1 p_2$ by

$$z \approx (z_1, z_2) \bmod (p_1, p_2),$$

which implies congruential equations $z \equiv z_1 \bmod (p_1)$ and $z \equiv z_2 \bmod (p_2)$.

(IV) Perform the second-stage spectral test[7] on the cyclic sequence $<z>$ and its coset sequence $n<z>$ in $Z^*_{p_1 p_2}$ up to a selected degree l. Admit z if the result is passable to within the prescribed range from the theoretical optimum. If not, discard z, and try different choices of z_1 and z_2 (and of primes p_1, p_2 if necessary) until satisfactory combinations are found.

In principle, the number s of odd primes in (I) may be chosen for any $s \geq 3$. However, there are theoretical and practical reasons to regard the case $s = 2$ to be optimal. So we speak of $s = 2$ cases exclusively. Taking results of Sec. 3 beforehand, we may say that $<z> \bmod (d = p_1 p_2)$ constructed by z of (III) has the period $T = \mathrm{LCM}(p_1 - 1, p_2 - 1)$, which is the period of two-component vector sequence whose components are taken by congruences in respective moduluses,

$$<z> \approx <(z_1, z_2)> \equiv \{(1,1),\ (z_1, z_2),\ ({z_1}^2, {z_2}^2),\ \cdots,\ ({z_1}^j, {z_2}^j),\ \cdots\} \bmod (p_1, p_2).$$

Thus, (I) and (II) ensure the largest period $T = 2q_1 q_2$ for the cyclic sequence $<z>$, which will be seen to have a decisive meaning for the uniform distribution of numbers in $<z>$ and its coset $n<z>$.

In 1986 Fishman and Moore[8] gave monumental 6-th degree spectral tests exhausting all primitive roots for the prime modulus $p = 2^{31} - 1$. The total number of primitive roots amounts to 24.89% of this p. Fishman[9] then gave in 1990 spectral tests for the modulus d up to 2^{48}. The number of relevant multipliers for $d = 2^{48}$ amounts to 2^{45}, and their $2 \times 10^{-3}\% = 1/(5 \times 10^4)$ portion underwent 6-th

[5] D. E. Knuth: *The Art of Computer Programming* Vol. 2 *Semi-numerical Algorithms*, Third Ed. (Addison-Wesley 1998), Sec. 3.3.4.

[6] We call a spectral test as *l-th degree*, if it examines the distribution of 2 to l consecutive numbers in the cyclic sequence $<z>$ (and in coset sequences $n<z>$ for composite moduluses, as we shall see) generated by z in Z^*_d.

[7] The spectral test used here for composite moduluses have meanings slightly different from the existing usage for, in particular, $d = 2^r$. See Sections 5 and 6.

[8] G. S. Fishman and L. R. Moore: "An exhaustive analysis of multiplicative congruential random number generators with modulus $2^{31} - 1$," SIAM Journal on Scientific and Statistical Computing Vol. **7** (1986), pp. 24-45. After Fishman and Moore we call the spectral test *exhaustive* if it examines all relevant multipliers, primitive roots for a prime modulus or generators of a (sub)group for modulus $d = 2^i$.

[9] G. S. Fishman: "Multiplicative congruential random number generators with modulus 2^β: An exhaustive analysis for $\beta = 32$ and a partial analysis for $\beta = 48$," Mathematics of Computation **54** (1990), pp. 331-344.

degree spectral tests. Estimated from these data, we should have had a report of exhaustive tests for the modulus $d = 2^{48}$ if the computer was faster by 5×10^4 times in 1990. We dearly remember that CRAY-2 in 1989 had the performance of 2 giga flops $= 2 \times 10^9$ flops, while a supercomputer of 10^{16} flops is said to be a real existence in few years. It might well be guessed that at present we are able to extend herculean works[10] of Fishman and Moore, and of Fishman, to exhaustive 6-th degree tests for $d \simeq \mathrm{O}(2^{48})$.

Let us consider implications of recipes (I)-(IV) by the case of $d = 2^{48}$. Assume that primes p_1 and p_2 of (I) are similar in magnitude and estimated as $\mathrm{O}(p)$. The period $T \simeq p_1 p_2/2 \simeq p^2/2 = 2^{48}$ will be realized by $p \simeq 2^{24.5}$. For primes $p_1, p_2 \simeq 2^{24.5}$ exhaustive spectral tests of 6-th degree to select best of multipliers $z_j \in Z^*_{p_j}$ $(j = 1, 2)$ were certainly computable as early as 1986. Chinese remainder theorem will be seen in Sec. 3 as realizing an ingenious way to shuffle and unite two processes $<z_1> \subset Z^*_{p_1}$ and $<z_2> \subset Z^*_{p_2}$ into the cyclic sequence $<z>$ or its coset sequence $n<z>$ in $Z^*_{p_1 p_2}$. Chances for two processes with good distribution to be shuffled into another good process will naturally be higher than the magical realization of a good process out of two not-so-good ones. Thus, we had better discard cases of little prospects, and concentrate on combinations of excellent multipliers. Taking the composite modulus $d = p_1 p_2 \simeq \mathrm{O}(2^{49})$, we obtain the convenience afforded by (I)-(IV) to replace the problem with far smaller number of combinations of far easier exhaustive 6-th degree spectral tests. The change of tactics will also be seen to give us the freedom to choose the geometry of points generated by consecutive numbers of $<z>$.

Suppose we are a little more ambitious, and aim to realize a longer period $T = \mathrm{O}(2^{64}) \simeq p^2/2$. We have, of course, real single precision random numbers from Mersenne Twister[11] with its gigantic period $\mathrm{O}(2^{19937 \pm 32})$ and 623-dimensional equidistribution property over this whole period. Yet, the process seems to defy all efforts to perform reliable tests on the distribution of numbers generated, not only for the whole period but also for *shorter* practical portions of the length $T = \mathrm{O}(2^{64})$, say. All of 19937-th degree primitive polynomials[12] over the finite field $\boldsymbol{F}_2$ yield linear recurrence equations that give the same period and the same equidistribution property to generated single precision real number sequences. Since Mersenne Twister uses one of these primitive polynomials, some principle or test for the choice will be necessary.[13] But this test seems to pose an extremely difficult problem, even for any portion of the sequence of length $T = 2^{64}$.

It seems more productive to convert the problem, and try to find good multiplicative congruential generators of period $T = 2^{64}$ by spectral tests, as an approximant of all conceivable such random number sequences with any distribution properties. In fact, exhaustive spectral tests of 6-th degree for $p_j \simeq \mathrm{O}(2^{32.5})$ is certainly possible for $j = 1, 2$. If we require in (IV) only $l = 3$ for the degree of the second stage spectral test of $z \in Z^*_{p_1 p_2}$ with $d = p_1 p_2 \simeq \mathrm{O}(2^{65})$, the amount of computations needed is estimated smaller than that of preceding two spectral tests of 6-th degree for $p = \mathrm{O}(2^{32.5})$; see Sec. 8. We have now the possibility of a multiplicative congruential generator for $d = p_1 p_2 = \mathrm{O}(2^{65})$ and the period $T = 2^{64}$, with its distribution properties ensured by the 3rd degree spectral test. Since we have reasons to believe that exhaustive 6-th degree tests are possible for $p = \mathrm{O}(2^{48})$ at present, we might even think of multiplicative congruential generators with the period $T \simeq 2^{95} = 10^{28.60}$ with

[10] S. K. Park and K. W. Miller: "Good random number generators are hard to find," Communications of the ACM Vol. 31 (1988),1192.

[11] M. Matsumoto and T. Nishimura: "Mersenne Twister; A 623-dimensionally equidistributed uniform pseudorandom number generator," ACM Transactions on Modeling and Computer Simulation Vol. 4 (1994), 254-266.

[12] The total number of such primitive polynomials is given by Euler's function as $\varphi(2^{19937} - 2)/19937$.

[13] See Sec. 6 for the order of the probability to obtain a good primitive root out of generators of Z^*_p for $p = 2^{31} - 1$, which is the multiplicative group over the finite field $\boldsymbol{F}_p$. The problem to choose a primitive polynomial of 19937-th degree over the finite field $\boldsymbol{F}_2$ is the same as choosing a set of 19937 generators of the multiplicative group of the extension field $\boldsymbol{F}_{2^{19937}}$.

3rd degree spectral tests as a realizable object.

The idea of spectral tests for composite moduluses is not new. The use of the modulus $d = 2^i$ with spectral tests has been a popular choice including linear congruential generators.[14] The way of our use in Sec. 6, however, has different aspects from the existing usage which invariably assumes that the lattice points are occupied (almost) fully by points generated by the cyclic sequence $<z>$. In contrast, we are forced to use $<z>$ and $n <z>$ that occupy only a portion of the group to realize the uniformity of generated numbers. Differences necessitates us to give arguments in as self-contained a manner as possible, which will call for the patience of readers and efforts of the authors. All these difficulties are rather gifts, however, and we shall have new, significant insights on the structure of the problem. Thus, spectral tests will be recognized of their validity on geometrical grounds in far broader circumstances, and the symmetry of point sets generated by consecutive numbers of $<z>$ and $n <z>$ will be found even controllable with the aid of group structures conserved by Chinese remainder theorem. In short, we shall recognize Chinese remainder theorem not only as an able shuffler of component sequences, but also as the constructor that is standing at every stage of the direct product formation and building a graded world of reduced residue class groups.

The report is constructed as follows. Section 2 recapitulates the fact that any sequence of integers of finite length is approximated by a cyclic or coset sequence in a reduced residue class group. We refer in Sec. 3 to the isomorphism between reduced residue class groups with composite moduluses and direct product groups on the basis of Chinese remainder theorem. Section 4 pursues possible devices that will ensure the uniform distribution to the generated sequences. Though a multitude of complicated mechanisms may be conceived of, the best way for our skill will be to resort to cyclicity of component groups, utilizing the specific convenience that arises with cases of composite modulus d consisting of *two* primes. Section 5 on lattice structures is for the mathematical confirmation of the applicability of spectral tests, in the mentioned generalized setting, as the measure of statistical independence of sequential numbers. Efforts will be rewarded in Sec. 6 for spectral tests by some generic comprehension of the geometry of points generated by $<z>$, which will clarify how the prime moduluses constituting d should be chosen. The aimed design for uniform and independent random number generators will be understood precisely in Sec. 7. In the final Sec. 8 we discuss the aspects of computability of spectral tests and will have the above noted prescriptions with their full details, together with short comments on other possible choices.

2. Finite sequences of integers and cyclic sequences in reduced residue class groups

Consider a finite sequence $\{x_1, x_2, \cdots, x_T\}$ of positive integers or 0 with length $T \geq 1$. Assume for later convenience that the sequence is not a zero sequence $\{0, 0, \cdots, 0\}$. Take an arbitrary integer $z \geq 2$ bounding the sequence as $0 \leq x_j < z, \quad 1 \leq j \leq T$. We concatenate the sequence indefinitely to form a periodic sequence in base-z numerals that admits an interpretation as a rational number x,

$$x := 0.x_1x_2\cdots x_Tx_1x_2\cdots x_T\cdots = 0.\dot{x}_1x_2\cdots\dot{x}_T = \frac{x_1}{z} + \frac{x_2}{z^2} + \frac{x_3}{z^3} + \cdots .$$

In order to make notions clear, we shall call a rational number x with a periodic base-z numeral sequence as *proper* or *in proper form* if the following conditions (i)-(iii) are satisfied:

(i) The base-z $(z \geq 2)$ numeral sequence for x has the vanishing whole number part.

(ii) The sequence has a period $T \geq 1$ that begins from the first numeral to the right of 0.

[14] There is even an indication of spectral tests with the modulus $d = (2^{31} - 1)(2^{31} - 249)$; see pp. 106-107 of D. E. Knuth in footnote,[5] in particular Line 22 of Table 1. However, we would like to avoid the use of this modulus. See Sec. 7A.

(iii) The sequence includes at least one positive numeral in its period.

Thus, the sequence x, as introduced above by concatenation, has a proper form in base-z numerals. It is well-known that this x has the following fractional expressions :[15]

$$x = \frac{x_1 x_2 \cdots x_T}{z^T - 1} = \frac{n}{d}, \quad 0 < x \leq 1, \quad 0 < n \leq d,$$

where and hereafter the fraction n/d is restricted to be irreducible. Note that d and z are coprime, because d is a factor of $z^T - 1$.[16] Note also that the following sequence with $\overline{z} := z - 1$,

$$x = 0.\overline{z}\,\overline{z}\,\overline{z}\cdots = \frac{x_1 x_2 \cdots x_T}{z^T - 1} = \frac{(z-1)(z^{T-1} + z^{T-2} + \cdots + z + 1)}{z^T - 1} = \frac{z^T - 1}{z^T - 1} = 1 = \frac{1}{1},$$

conforms to the definition of a proper sequence in base-z numerals with period $T = 1$. We thus include $x = n/d = 1/1 = 1$ in our *irreducible fraction*, obeying the definition that $n = 1$ and $d = 1$ are coprime by $\mathrm{GCD}(n, d) = 1$.

Proper periodic sequences and the corresponding irreducible fractions may be characterized as follows, as regards their mutual relation.

Corollary 1 (I) Let an integer $z \geq 2$ and a base-z numeral sequence x $(0 < x \leq 1)$ be given in proper form with period $T \geq 1$. Then, there exist integers n, d fulfilling

$$\mathrm{GCD}(n, d) = 1, \quad 0 < n \leq d, \quad d | z^T - 1, \quad \mathrm{GCD}(z, d) = 1,$$

and x has the representation $x = n/d$ as an irreducible fraction with $0 < x = n/d \leq 1$.
(II) Let conversely positive integers n, d, z be given fulfilling

$$0 < n \leq d, \quad \mathrm{GCD}(n, d) = 1, \quad z \geq 2, \quad \mathrm{GCD}(z, d) = 1.$$

The irreducible fraction $x = n/d$ then has a unique expansion in base-z numeral sequence in proper form. Its period T is any multiple of the order $t = \mathrm{ord}(z)$ of z in the reduced residue class group Z_d^* modulo d, and is independent of the numerator n of the irreducible fraction.

(Proof) (I) The statement has been shown in the above.
(II) Consider the arithmetic process of division for n/d. Putting the case of $x = 1$ or $n = d = 1$ aside for the moment, we assume $0 < n < d$ which means $d \geq 2$. Denote $r_1 := n$. The whole number part of $x = n/d$ is 0 by $0 < n < d$. The first base-z numeral x_1 is determined uniquely by the equation

$$zn = zr_1 = dx_1 + r_2, \quad 0 \leq x_1 \leq \overline{z},$$

as the quotient of the division of $zn = zr_1$ by d with the remainder r_2. This remainder is written compactly in terms of the congruence relation as

$$r_2 \equiv nz \bmod (d), \quad 0 < r_2 < d.$$

In the next step we multiply the remainder r_2 by z, and divide it with d to obtain uniquely the quotient x_2 satisfying $0 \leq x_2 \leq \overline{z}$ and the remainder $0 < r_3 < d$. The procedure is summarized as:

$$zr_2 = dx_2 + r_3, \quad 0 \leq x_2 \leq \overline{z}, \quad r_3 = zr_2 - dx_2 \equiv nz^2 \bmod (d), \quad 0 < r_3 < d.$$

[15] In below the numerator $x_1 x_2 \cdots x_T$ stands for $x_1 z^{T-1} + x_2 z^{T-2} + \cdots + x_{T-1} z + x_T$.
[16] We might add: $g = \mathrm{GCD}(z, d)$ should then divide also $z^T - 1$, implying $g = 1$ as g is a divisor of 1.

Likewise, the sequence of quotients $\{x_1, x_2, \cdots, x_j, \cdots\}$ formed by zero or positive integers, and the sequence of remainders $\{r_1, r_2, \cdots, r_j, \cdots\}$ consisting of positive integers, are constructed uniquely; as remainders of the division of irreducible fraction n/d to the base z coprime with d, there never arises 0 in $\{r_j\}$. They satisfy:

$$zr_j = dx_j + r_{j+1}, \quad 0 \le x_j \le \overline{z}, \quad r_j \equiv nz^{j-1} \bmod (d), \quad 0 < r_j < d, \quad j = 1, 2, 3, \cdots. \qquad (1)$$

The whole setting may be abstracted as follows. Integers n, z are elements of the reduced residue class group Z_d^* with modulus d and with the order[17] $\sharp Z_d^* = \varphi(d)$, where $\varphi(d)$ is Euler's function. In Z_d^* the base z has its own order t, with the property $t|\varphi(d)$ (Lagrange's theorem), z^j for $1 \le j \le t$ are all different, and z^j becomes congruent to 1 for the first time at $j = t$. The sequence of remainders is the coset sequence $n<z>$ of the cyclic sequence $<z>$ generated by z in Z_d^*,

$$\begin{aligned} <z>:\equiv \quad & \{1, z^1, z^2, \cdots, z^j, \cdots\} \equiv \{1, z^1, z^2, \cdots, z^t \equiv 1, z^1, z^2, \cdots\} \bmod (d), \\ n\,<z>:\equiv \quad & \{n, nz^1, nz^2, \cdots, nz^t \equiv n, nz^1, nz^2, \cdots\} \bmod (d). \end{aligned}$$

These two sequences have the same period; note that $nz^j \equiv nz^k \bmod (d)$ gives $z^j \equiv z^k \bmod (d)$ upon multiplication by $n^{-1} \in Z_d^*$, together with the obvious converse. So, the sequence $\{x_1, x_2, \cdots\}$ of quotients that shares its period with remainders $n<z>$ also has the period $t = \mathrm{ord}(z)$ independent of n, with any other period T being a multiple of t. Thus, $x = n/d$ has the unique, proper form in base-z numeral sequence $x = 0.x_1x_2\cdots$; the whole number part is 0 by $n/d < 1$, the period starts from the first base-z numeral to the right of 0 because $<z>$ or $n<z>$ starts their period from the first term, and the sequence of quotients includes at least one positive element by $n > 0$.

As regards the remaining case $n = d = 1$ or $x = 1$, the process of division in base-z numerals of *irreducible fraction* $1/1$ may be performed as follows. Define $r_1 := n = 1$. Take artificially the whole number part 0, multiply $r_1 = n = 1$ by z, and divide $zr_1 = z$ by $d = 1$. Take the first quotient $x_1 = \overline{z}$ again artificially (but with no other choice in order to make the whole number part 0) to obtain the remainder 1. Manifestly, the procedure may be repeated indefinitely. We obtain the same relation (1), except for the change of $0 < r_j < d$ to $0 < r_j \le d$, together with the unique proper form

$$1 = 0.x_1x_2x_3\cdots = 0.\overline{z}\,\overline{z}\,\overline{z}\cdots, \quad \{r_1, r_2, r_3, \cdots\} = \{1, 1, 1, \cdots\},$$

of base-z sequence with period $T = 1$. Since all integers are congruent mutually modulo $d = 1$, we take $Z_1^* = \{1\}$ in order to make group multiplications intuitive. This gives $n \equiv z \equiv 1 \bmod (1)$, with $t = \mathrm{ord}(z) = 1$ and the sequence of remainders with period 1 independent of the choice of n,

$$\{r_1, r_2, \cdots\} \equiv n\,<z> \equiv <1> \equiv \{1, 1, 1, \cdots\} \bmod (1),$$

as the sole cyclic sequence and its coset in Z_1^*. This sequence of remainders conforms to the results of cases with $0 < n < d$.

We summarize this long, constructive proof of (II) adopted for the proof of Theorem 2 below. For any integers n, d, z satisfying $\mathrm{GCD}(n, d) = 1$, $0 < n \le d$, $\mathrm{GCD}(z, d) = 1$, $z \ge 2$, the irreducible fraction n/d is expressed in unique, base-z numeral sequence in proper form, with $\{x_1, x_2, x_3, \cdots\}$ for quotients and the associated sequence of remainders $\{r_1, r_2, \cdots\} \equiv n\{1, z^1, z^2, \cdots\} \bmod (d)$ satisfying the relations extending (1):

$$zr_j = dx_j + r_{j+1}, \quad 0 \le x_j \le \overline{z}, \quad r_j \equiv nz^{j-1} \pmod d, \quad 0 < r_j \le d, \quad j = 1, 2, 3, \cdots. \qquad (2)$$

We have also proved that the period of x in its base-z proper form is given by an arbitrary multiple of $t = \mathrm{ord}(z)$. ■

[17] The symbol $\sharp S$ expresses, as usual, the number of elements of the set S.

The above result (2), as well as the common sense that if the remainder is large then the next quotient will be large, are all well-known. Yet, we obtain a significant estimate by dividing the above with zd,

$$\frac{r_j}{d} = \frac{x_j}{z} + \varepsilon_j, \quad 0 < \frac{r_j}{d} - \frac{x_j}{z} = \varepsilon_j = \frac{r_{j+1}}{zd} \leq \left(\frac{1}{z}\right). \tag{3}$$

Consider the case that the sequence $\{x_j|\ j = 1, 2, \cdots\}$ is used for the uniformly distributed random number. Assuming that $\{x_1, x_2, \cdots\}$ are not all 0. Then $0 \leq x_j/z < 1$ is the appropriate candidate for the real random variable in the interval $[0, 1)$. Therefore we have[18] by Corollary 1:

Theorem 2 Let there be given integers $T \geq 1$ and $z \geq 2$, as well as a sequence $\{x_1, x_2, \cdots, x_T\}$ of positive or 0 integers in the range $0 \leq x_j < z$ for $1 \leq j \leq T$. Assume that $\{x_1, x_2, \cdots, x_T\}$ are not all 0. Let $x \in [0, 1)$ be the rational number represented by the base-z numeral sequence $x = 0.\dot{x}_1 x_2 \cdots \dot{x}_T$ in proper form, and denote its irreducible fraction representation as $x = n/d$. There hold

$$0 < n \leq d, \quad \mathrm{GCD}(n, d) = 1, \quad d|z^T - 1, \quad \mathrm{GCD}(z, d) = 1.$$

Correspondingly, the sequence $\{u_j := x_j/z|\ j = 1, 2, \cdots\}$ in $[0, 1)$ is approximated by the sequence $\{v_j := r_j/d|\ 0 < r_j \leq d,\ j = 1, 2, \cdots\}$ in $(0, 1]$ uniformly within the error $1/z$ as

$$0 < v_j - u_j \leq 1/z, \quad j = 1, 2, \cdots .$$

Here, $\{r_j\}$ is the sequence of remainders in the division process of $x = n/d$, and is identical with the coset sequence $n<z>\equiv \{n, nz^1, nz^2, \cdots\} \bmod (d)$ taken in the interval $(0, d]$, of the cyclic sequence $<z>$ generated by z in the reduced residue class group Z_d^*. Conversely, the sequence of quotients $\{x_1, x_2. \cdots\}$ is re-constructed as

$$x_j = (zr_j - r_{j+1})/d, \quad j = 1, 2, \cdots ,$$

if the cyclic sequence $<z>$ is known. **(End of Theorem 2)**

With a large odd prime modulus $d = p$ or with $d = 2^i$ for $i \gg 4$, the sequence of remainders

$$\{r_j|\ 0 < r_j < d,\ j = 1, 2, \cdots\} \equiv n <z> \bmod(d)$$

has been used as the multiplicative congruential generator for uniform and independent random numbers in the form $\{r_j/d|\ j = 1, 2, \cdots\}$. The use has been experienced vast applications, and the method to choose good multiplier z is well-established as spectral tests. Theorem 2 casts a new light on this setting, as discussed in Sec. 1.

We started with a base-z numeral sequence of length T given, and found Theorem 2 for large z. The case of $z = 2$, which is realized typically in coin tosses, is a significant problem with the smallest z, and inferences of Theorem 2 lose their power. However, practical applications as uniform and independent random numbers take 32 or 64 base-2 consecutive numerals for single or double precision real variables. The circumstance allows the reformulation of the problem to cases with $z = 2^{32}$ or $z = 2^{64}$ together with the corresponding modulus $d|z^T - 1$, and Theorem 2 would then work well. In general, if the problem starts with numerals for a small base z, we may take some large s of such numerals as a unit, and consider the sequence $\{y_j|\ j = 1, 2, \cdots\}$ defined by

$$y_j := x_{sj}x_{sj+1} \cdots x_{sj+s-1} = x_{sj}z^{j-1} + x_{sj+1}z^{j-2} + \cdots + x_{sj+(s-2)}z^{s-(s-1)} + x_{sj+(s-1)}.$$

[18] See H. Nakazawa, in footnote.[4]

This reformulates the problem to the one with the multiplier $z^s \gg 1$, and Theorem 2 recovers its power. If the length T of the original sequence is fixed but has the factorization $T = ts$ with large s, the same transformations $z \to z^s$ with $T \to t$ may be applied. Observations remind us of singular natures of the case with prime T, which will have occasions to be touched on later; at this place we note that, if the given value of T is not convenient, we may add arbitrary numbers, say 0's, to the end of the sequence at our will, transform $z \to z^s$, and discard the added tail in the result. A prime length T is not a truly impeding factor for the validity of Theorem 2.

3. Composite moduluses: Chinese remainder theorem and direct product decomposition

We turn to multiplicative, congruential generators and the corresponding reduced residue class groups with composite moduluses. The key is Chinese remainder theorem that leads us to the notion of product groups. We start from a preparatory corollary for this far-reaching theorem.

Corollary 3 Let $m := \mathrm{LCM}(d_1, d_2, \cdots, d_l)$ be the least common multiple of $d_1, d_2, \cdots, d_l$ which are positive integers. A necessary and sufficient condition for the congruence $a \equiv b \bmod (m)$ of any pair of integers a, b is that $a \equiv b \bmod (d_j)$ holds for every j in $1 \le j \le l$.

(Proof) If $a \equiv b \bmod (d_j)$ holds for all j satisfying $1 \le j \le l$, $a - b$ is surely a common multiple of $d_1, d_2, \cdots, d_l$. Thus $a - b$ is divisible by the least common multiple m, implying $a \equiv b \bmod (m)$. Conversely, $a \equiv b \bmod (m)$ implies that m divides $a - b$, so that all of d_j divide $a - b$, implying that $a \equiv b \bmod (d_j)$ holds for any j in $1 \le j \le l$. ■

Chinese remainder theorem 4 Let the modulus $d \ge 2$ be factorized into pairwise coprime integers as

$$d = d_1 d_2 \cdots d_l \quad (d_j \ge 2, \quad 1 \le j \le l), \quad l \ge 2.$$

Let $\{a_j |\ 1 \le j \le l\}$ be arbitrary integers given. Then, there exists an integer a satisfying

$$a \equiv a_1 \pmod{d_1}, \ \ a \equiv a_2 \pmod{d_2}, \ \ \cdots, \ \ a \equiv a_l \pmod{d_l}, \tag{4}$$

and a is unique modulo d. The form of a may be expressed as[19]

$$a \equiv a_1 U_1 + a_2 U_2 + \cdots + a_l U_l \pmod{d}, \quad U_j \equiv \delta_{jk} \pmod{d_k}, \quad (1 \le j, k \le l), \tag{5}$$

where $U_1, U_2, \cdots, U_l$ are determined by $d_1, d_2, \cdots, d_l$, and not dependent on $a_1, a_2, \cdots, a_l$.

(Proof) First, the uniqueness. Assume that a and a' fulfill (4). Since $d_1, d_2, \cdots, d_l$ are all pairwise coprime, d is their least common multiple. Therefore, (4) and Corollary 3 assure $a \equiv a' \bmod (d)$, the uniqueness modulo d. Next, the existence of a satisfying (4). We start by constructing $U_1, U_2, \cdots, U_l$ that fulfill the second half of (5). After Allenby and Redfern,[20] we put $e_j := d/d_j$. Since $d_1, d_2, \cdots, d_l$ are pairwise coprime, so are d_j and e_j. This ensures $\mathrm{GCD}(d_j, e_j) = 1$ for all $1 \le j \le l$. Thus, by Euclidean algorithm there exist integers D_j, E_j that give $1 = d_j D_j + e_j E_j$ for every j in $1 \le j \le l$. Note also that $\{e_j, D_j, E_j\}$ are determined by $\{d_k |\ 1 \le k \le l\}$ and do not depend on $\{a_k |\ 1 \le k \le l\}$. Put $U_j := e_j E_j$, and we have $1 = d_j D_j + U_j$. This equation taken modulo d_j gives $1 \equiv U_j \bmod (d_j)$. Since $U_j = e_j E_j$ contains all d_k with $k \ne j$, $U_j \equiv 0 \bmod (d_k)$ holds for any $k \ne j$. These prove the existence of $\{U_j\}$ fulfilling the second half of (5). Defining a by its first half, we have

$$a = a_1 U_1 + a_2 U_2 + \cdots + a_l U_l \equiv \textstyle\sum_k a_k \delta_{kj} = a_j \bmod (d_j), \quad 1 \le j \le l.$$ ■

[19] In below δ_{jk} is Kronecker's delta.

[20] R. B. J. T. Allenby and E. J. Redfern: *Introduction to Number Theory with Computing* (Arnold 1989) p. 105. See also D. E. Knuth in footnote[5], p.270 for another suggestive expression $U_j = (d/d_j)^{\varphi(d_j)}$.

Let there be given arbitrary groups G, G'. Denote their elements as $\{a, b, \cdots\}$ and $\{a', b', \cdots\}$, respectively. The pairs, $(a, a'), (b, b'), \cdots$, which are elements of the product set $G \times G'$, may be defined of their product by

$$(a, a')(b, b') := (aa', bb').$$

This definition makes the product set $G \times G'$ a group, called the direct product group of G and G'. In fact, the following relations are readily seen to prove this statement:

(I) The unit element of $G \times G'$ is (e, e'), in the obvious notation.

(II) $(a, a') \in G \times G'$ has the inverse $(a^{-1}, (a')^{-1})$.

(III) If G, G' are finite groups, then $\sharp(G \times G') = (\sharp G)(\sharp G')$.

The notion may be extended to the direct product of three or more groups. We discard generality, and summarize the relevant fact with reduced residue class groups. We shall denote $\approx$ for the group isomorphism.

Theorem 5 (I) Let $d = d_1 d_2 \cdots d_l$ be a factorization of d into pairwise coprime integers. An arbitrary element $z \in Z_d^*$ belongs to $Z_{d_j}^*$ for any j in the range $1 \leq j \leq l$. Let f denote the mapping of z in Z_d^* to the element $(z, z, \cdots, z)$ in the direct product group $Z_{d_1}^* \times Z_{d_2}^* \times \cdots \times Z_{d_l}^*$

$$f(z) := (z, z, \cdots, z) \in Z_{d_1}^* \times Z_{d_2}^* \times \cdots \times Z_{d_l}^*.$$

Taken in the congruence of respective moduluses, f is a bijection forming group isomorphism:

$$Z_d^* \approx Z_{d_1}^* \times Z_{d_2}^* \times \cdots \times Z_{d_l}^*, \qquad \sharp Z_d^* = (\sharp Z_{d_1}^*)(\sharp Z_{d_2}^*) \cdots (\sharp Z_{d_l}^*).$$

(II) For the prime factorization $d = {p_1}^{i_1} {p_2}^{i_2} \cdots {p_l}^{i_l}$ this isomorphism takes the form:

$$Z_d^* \approx Z_{{p_1}^{i_1}}^* \times Z_{{p_2}^{i_2}}^* \times \cdots \times Z_{{p_l}^{i_l}}^*, \qquad \sharp Z_d^* = \prod_{j=1}^{l} (\sharp Z_{{p_j}^{i_j}}^*).$$

(Proof) (I) Any $z \in Z_d^*$ is coprime to $d = d_1 d_2 \cdots d_l$, so that z is coprime to d_j and $z \in Z_{d_j}^*$ holds for all j in $1 \leq j \leq l$. Thus, f is a mapping from Z_d^* into the direct product group on the right hand side. Conversely, any element $(z_1, z_2, \cdots, z_l) \in Z_{d_1}^* \times Z_{d_2}^* \times \cdots \times Z_{d_l}^*$ determines, by Chinese remainder theorem 4 applicable by the assumption that $d_1, d_2, \cdots, d_l$ are pairwise coprime, an integer z that is unique modulo d with $z \equiv z_j \bmod (d_j)$ for all j in $1 \leq j \leq l$. This integer z is coprime to d_j for any j in $1 \leq j \leq l$; note that $z \equiv z_j \bmod (d_j)$ gives $\mathrm{GCD}(z, d_j) = \mathrm{GCD}(z_j, d_j) = 1$. Hence z is in $Z_{d_1 d_2 \cdots d_l}^*$ with

$$f(z) = (z, z, \cdots, z) \equiv (z_1, z_2, \cdots, z_l) \bmod (d_1, d_2, \cdots, d_l).$$

Thus, f is a bijection between Z_d^* and $Z_{d_1}^* \times Z_{d_2}^* \times \cdots \times Z_{d_l}^*$. Since any elements z, z' in Z_d^* give

$$f(zz') := (zz', zz', \cdots, zz') = (z, z, \cdots, z)(z', z', \cdots, z') = f(z) f(z'),$$

f is a group isomorphism. Counting the number of elements on both sides of the isomorphism $z \approx (z_1, z_2, \cdots, z_l)$, we obtain the equation for orders.

(II) This is the main theorem of the direct product decomposition of reduced residue class groups with composite moduluses, which is now obvious as a specific case of (I). ■

Admitting some redundancy of statements, we also note the following for later convenience.

Corollary 6 Let $d = d_1 d_2 \cdots d_l$ be a factorization of d into pairwise coprime integers. Elements z, n in Z_d^* are determined uniquely by their corresponding elements in component groups,

$$z \equiv z_1 \bmod (d_1),\ \ z \equiv z_2 \bmod (d_2),\ \ \cdots,\ \ z \equiv z_l \bmod (d_l),$$
$$n \equiv n_1 \bmod (d_1),\ \ n \equiv n_2 \bmod (d_2),\ \ \cdots,\ \ n \equiv n_l \bmod (d_l),$$

or by the isomorphism,

$$z \approx (z_1, z_2, \cdots, z_l) \bmod (d_1, d_2, \cdots, d_l), \quad n \approx (n_1, n_2, \cdots, n_l) \bmod (d_1, d_2, \cdots, d_l).$$

Elements in the cyclic sequence $<z>$ or in the coset sequence $n<z>$ for indices $s = 0, 1, 2, \cdots$ have following expressions:

$$\left.\begin{aligned} &z^s \equiv {z_1}^s U_1 + {z_2}^s U_2 + \cdots + {z_l}^s U_l \bmod (d), \\ &nz^s \equiv n_1 {z_1}^s U_1 + n_2 {z_2}^s U_2 + \cdots + n_l {z_l}^s U_l \bmod (d), \\ &U_j \equiv \delta_{jk} \bmod (d_k)\ \ (j, k = 1, 2, \cdots). \end{aligned}\right\} \tag{6}$$

Here, integers $U_1, U_2, \cdots, U_l$ are determined by $d_1, d_2, \cdots, d_l$, and do not depend on $z_1, z_2, \cdots, z_l$, $n_1, n_2, \cdots, n_l$ or s.

(Proof) We need only to discuss (6). Since $n = 1$ gives $nz^s = z^s$, we take nz^s exclusively in the proof. Resorting to Theorem 5 (I) we have the isomorphism

$$nz^s \approx (n_1, n_2, \cdots, n_l)(z_1, z_2, \cdots, z_l)^s = (n_1 {z_1}^s, n_2 {z_2}^s, \cdots, n_l {z_l}^s).$$

Thus, Chinese remainder theorem 4 proves all of (6). It is also suggestive to consider expressions

$$z \equiv z_1 U_1 + z_2 U_2 + \cdots + z_l U_l \bmod (d), \quad n \equiv n_1 U_1 + n_2 U_2 + \cdots + n_l U_l \bmod (d),$$

as well as the relation

$$U_j U_k \equiv U_j \delta_{jk} \bmod (d_i), \quad 1 \le \forall i \le l$$

obtained from (5) which gives $U_j U_k \equiv U_j \delta_{jk} \bmod (d)$ by Corollary 3. A few steps of calculation of products will readily convince us of (6). ■

The relations in (6) afforded by Chinese remainder theorem 4 reveal how the cyclic sequence $<z>$ and the coset sequence $n<z>$ in Z_d^* are constructed by the corresponding sequences in component groups. In words of random number generation problems, composite moduluses realize ways of shuffling of $<z_1>$, $<z_2>$, $\cdots$ as well as of $n_1 <z_1>$, $n_2 <z_2>$, $\cdots$. Any natural random number sequences are exploiting this mechanism tacitly. The linear disguise of (5) and (6), however, should be taken with care. Thus, small changes of $a_1, a_2, \cdots, a_l$ on the right hand side of (5) can give linear changes in a. However, nonlinear jumps of a may occur as the right hand side crosses integral multiples of d. It might be of some help to consider that the right hand sides of (5) and (6) represent some (nonlinear) sawtooth type function.

In passing we note a fact on the order of elements in direct product groups.

Corollary 7 Let $d = d_1 d_2 \cdots d_l$ be the factorization into relatively prime integers. Take an arbitrary integer $z \in Z_d^*$ characterized by

$$z \approx (z_1, z_2, \cdots, z_l) \bmod (d_1, d_2, \cdots, d_l).$$

The order t of z, the smallest positive t that gives $z^t \equiv 1 \bmod (d)$, is given by

$$t := \mathrm{ord}(z) = \mathrm{LCM}(t_1, t_2, \cdots, t_l),$$

where t_j is the order of z_j in $Z^*_{d_j}$ $(1 \le j \le l)$. The periods of the cyclic sequence $<z>$ and of a coset sequence for any $n \in Z^*_d$ are all the same as t.

(Proof) Since $d = d_1 d_2 \cdots d_l = \mathrm{LCM}(d_1, d_2, \cdots, d_l)$ holds by assumption, Corollary 3 ensures that $\mathrm{ord}(z)$ is the smallest positive of t satisfying:

$$z_j{}^t \equiv 1 \bmod (d_j), \quad 1 \le j \le l.$$

Thus $t = \mathrm{ord}(z) = \mathrm{LCM}(t_1, t_2, \cdots, t_l)$ holds true. Since $<z>$ is the special case $n = 1$ of $n<z>$, we consider only the period of $n<z>$. This is the smallest positive of t' that gives $nz^{j+t'} \equiv nz^j \bmod (d)$ for any $j = 0, 1, 2, \cdots$. Multiplication by $n^{-1}(z^j)^{-1} \in Z^*_d$ gives $z^{t'} \equiv 1 \bmod (d)$. Thus, a period t' is any multiple of the order t of z, implying $<z>$ and $n<z>$ have the period t. ■

4. Uniform distribution on composite modulus reduced residue class groups

If an element z in a group G generates a cyclic sequence $<z>$ that exhausts all elements of G, then G is qualified as cyclic, or a cyclic group, and z is called a generator of the group. So far, random number generators of multiplicative congruential type have taken, in essence, generators of cyclic reduced residue class groups as their multipliers and ascertained the uniformity of their output; see Theorem 8 below. We propose a different strategy, which comprises to take reduced residue class groups with composite moduluses formed by two distinct primes. Such groups cannot be cyclic. But there can be found a narrow path to the same uniformity as in the conventional generators. The use of such moduluses will be rewarded by longer periods and higher precision and, notably, with the freedom to control the geometry of points formed by the sequence of generated numbers.

In order to proceed we need to discern cases of cyclicity. The Existence or absence of cyclicity of a reduced residue class group Z^*_d is seen with the direct product decomposition corresponding to the factorization of the modulus d into prime powers. The following is known for cases of moduluses formed by a power of a single prime:

Theorem 8 Reduced residue class groups with powers of a prime for its modulus, $d = p^i$, are classified as follows.

(I) With any power $d = p^i$ $(i \ge 1)$ of an odd prime $p > 2$ for the modulus, $Z^*_{p^i}$ is cyclic. Its order, the number $\sharp Z^*_{p^i}$ of group elements, is given by Euler's function as $\varphi(d) = \varphi(p^i) = p^i - p^{i-1}$, an even number, which is also enumerated directly from the list of its elements:

$$Z^*_{p^i} = \{1, 2, \cdots, p-1, p+1, p+2, \cdots, 2p-1, 2p+1, \cdots, p^i - 1.\}$$

A generator z of a single prime modulus group Z^*_p is called a primitive root modulo p.[21]

(II) For $d = 2^i$ $(i \ge 4)$, $Z^*_{2^i}$ is not cyclic.[22] However, its subgroup $H_{1,5}$ with the order $\sharp H_{1,5} = 2^{i-2}$,

$$H_{1,5} := A_1^{(2^i)} \cup A_3^{(2^i)}, \quad A_k^{(2^i)} := \{8j + k |\ j = 0, 1, 2, \cdots, 2^{i-3} - 1\}, \quad k = 1, 3, 5, 7,$$

[21] Generators of $Z^*_{p^i}$ for $i \ge 2$ are also called primitive roots at times. A simple fact is that a generator for $d = p^i$ $(i \ge 2)$ is necessarily a primitive root for $d = p$. Note $a, z \in Z^*_p$ implies $a, z \in Z^*_{p^i}$ and vice versa. Note also the following: If $a, z \in Z^*_p$ fulfill $a \not\equiv z^j \bmod (p)$ for any integers $j = 0, 1, 2, \cdots$ (with $z^{p-1} \equiv 1 \bmod (p)$ by Fermat's little theorem), or if $a - z^j$ is not divisible by p for any $j = 0, 1, 2, \cdots$, then $a - z^j$ is never divisible by p^i for any j. Thus if z is not a primitive root of Z^*_p, z cannot be a generator of $Z^*_{p^i}$.

[22] Cases of $d = 2 = 2^1, 4 = 2^2$ give cyclic Z^*_d, but they are not practicable. For $d = 8 = 2^3$ it is easy to confirm

$$Z^*_8 = \{1, 3, 5, 7\}, \quad 1^2 = 1, \quad 3^2 \equiv 1, \quad 5^2 \equiv 1, \quad 7^2 \equiv 1 \bmod (8),$$

showing the absence of cyclic sequences that reproduce the whole group. This lack of cyclicity is inherited by $Z^*_{2^i}$ for all $i \ge 4$.

is cyclic, and its generators are all integers in $A_5^{(2^i)}$. **(End of Theorem 8)**

The reader is referred to Allenby and Redfern for the proof.[23]

The sequential distribution of numbers in $<z>$ is understood readily by visual information. We show below figures on which consecutive 2-tuples of numbers are plotted as points; the left shows points from the sequence of quotients $\{q_1, q_2, \cdots\}$, and the right is for the sequence of remainders $\{r_1, r_2, \cdots\}$, both for the irreducible fraction $1/d$. In more precise terms they represent points

$$\mathrm{P}_j := (q_j/z, q_{j+1}/z), \quad \text{and} \quad \mathrm{Q}_j := (r_j/d, r_{j+1}/d)$$

on the left and the right, respectively, for $j = 1, 2, \cdots, t$, where t is the order (or the period) of $<z>$. The outer frame shows the range $-0.05 \le x, y \le 1.05$.

Suppose that we take a point x on the horizontal axis of these figures, and draw a vertical band of width $1/\sqrt{\varphi(d)}$, say. If the band contains nearly $\sqrt{\varphi(d)}$ points irrespective of the position x, we may say that we have a uniform distribution in one period of the sequence. With this simple criterion in mind, we are suggested by these figures that uniform distributions will be realized most feasibly by

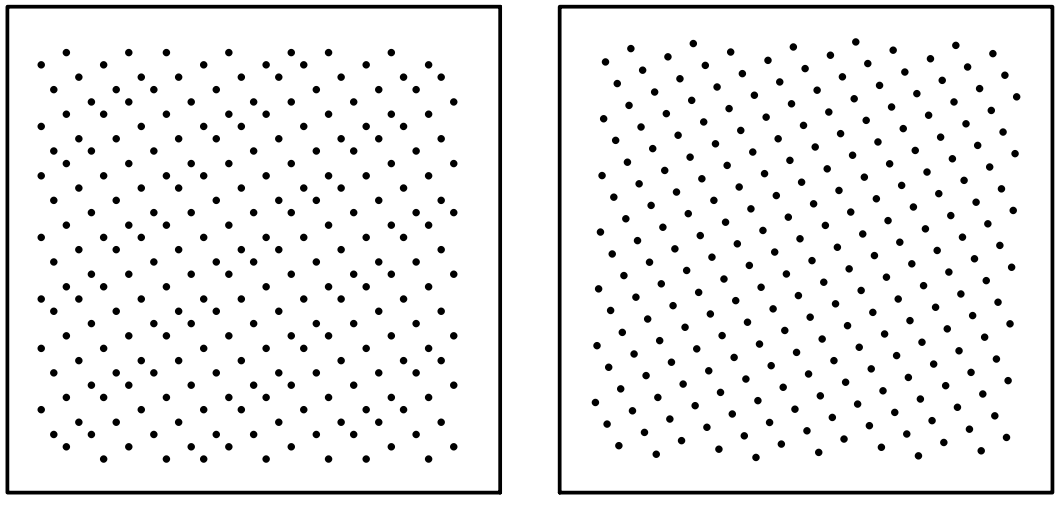

Fig. 1: Prime modulus $d = p = 251$, Z_d^* cyclic; $z = 34$ is a primitive root.

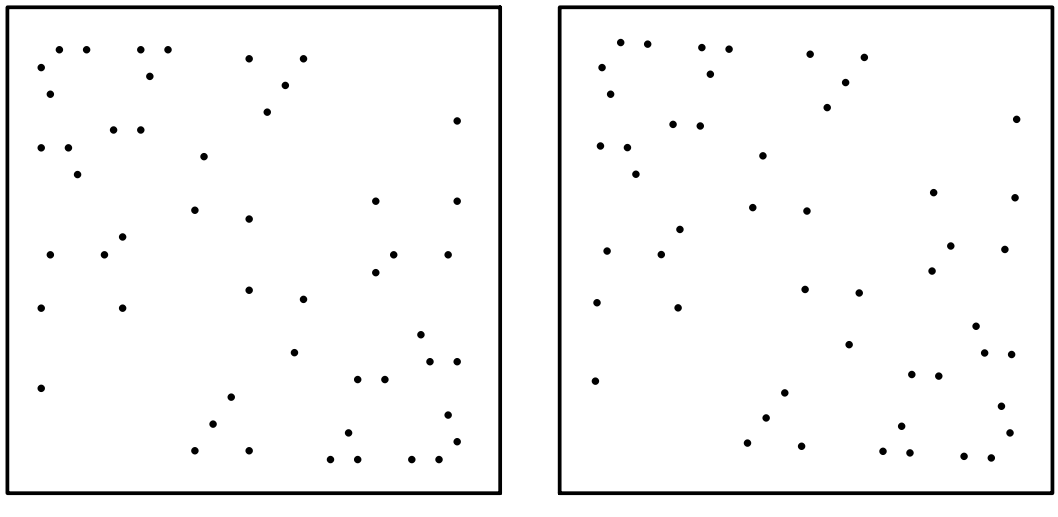

Fig. 2: Prime modulus $d = 251$, Z_d^* cyclic; $z = 47$ is not a primitive root.

[23] See pp. 125-135 of R. J. B. T. Allenby and E. J. Redfern in footnote.[18]

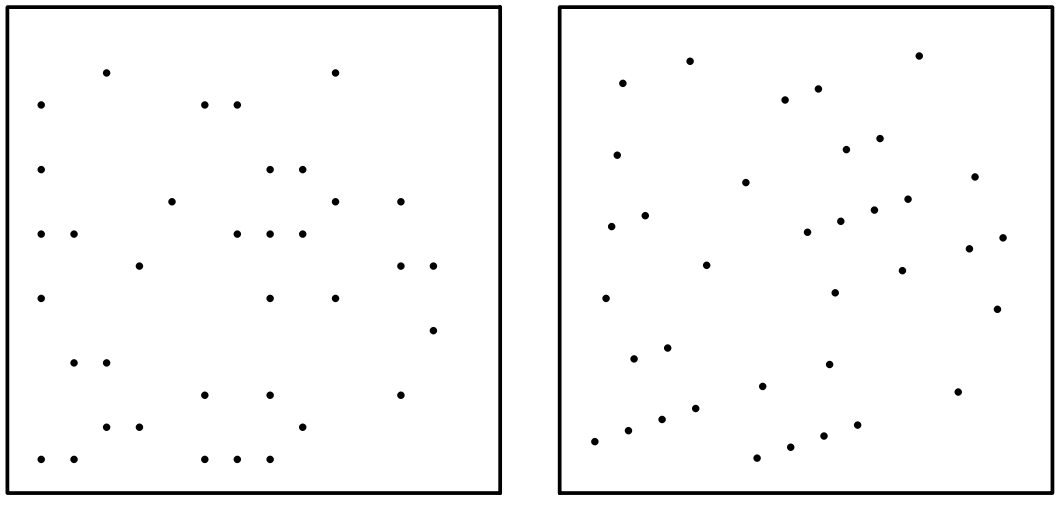

Fig. 3: Composite modulus $d = 304$, Z_d^* non-cyclic; $z = 13$.

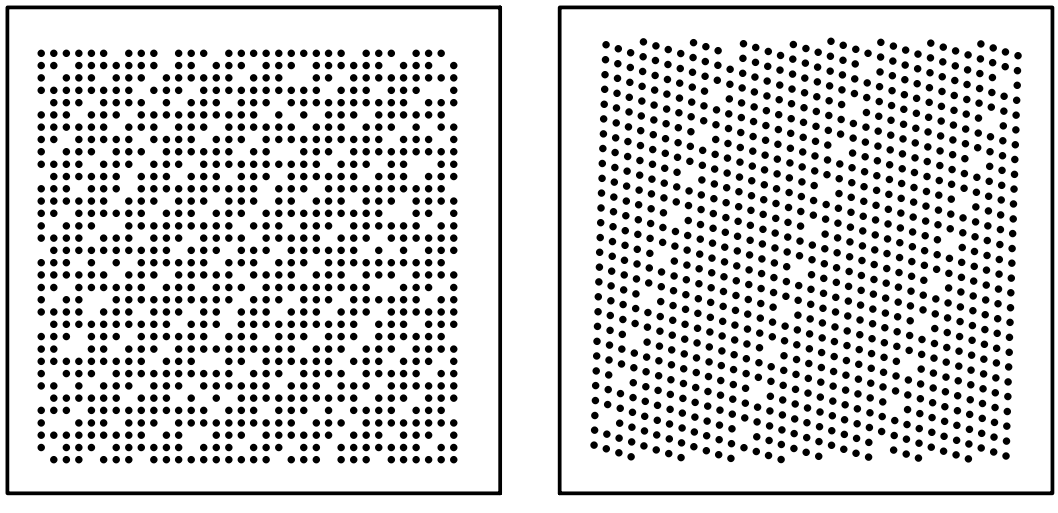

Fig. 4: Modulus $d = 31^2$, Z_d^* cyclic, generator $z = 34$, with $31^1 - 31^0 = 30$ vacancies.

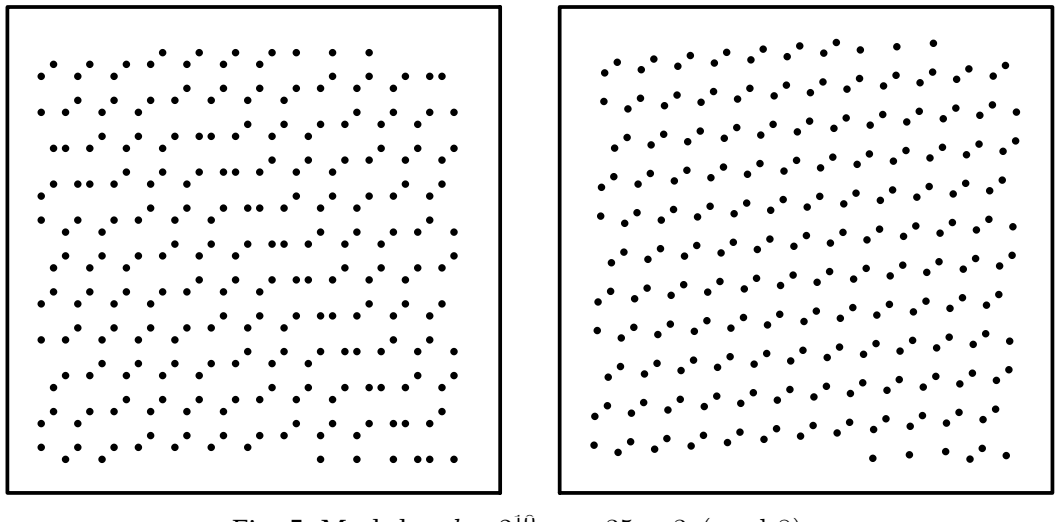

Fig. 5: Modulus $d = 2^{10}$, $z = 35 \equiv 3 \pmod 8$.

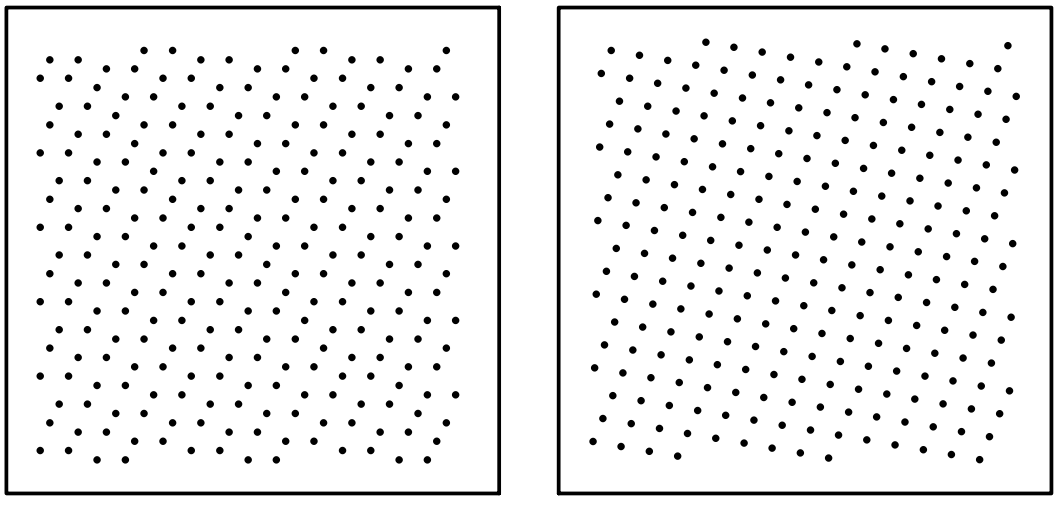

Fig. 6: Modulus $d = 2^{10}$, $z = 45 \equiv 5 \pmod 8$.

choosing Z_d^* and z to be a cyclic group and its generator, respectively. The choice has in fact been the setting for multiplicative congruential generators of random numbers. In more detail, odd primes for moduluses $d = p$ and corresponding primitive roots for z have been a leading configuration suggested by Theorem 8 (I). This choice makes $<z>$ itinerate every element of $Z_p^* = \{1, 2, \cdots, p-1\}$ once in the period $t = \varphi(p) = p - 1$. Though Z_p^* lacks 0 and $<z>$ leaves it unoccupied in the interval $[0, p)$, the fault is admitted as negligible for large p. The other leading choice has been $d = 2^i$ $(i \geq 4)$ and $z \equiv 5 \bmod (8)$ recommended by Theorem 8 (II). In this case $<z>$ with the period 2^{i-2} itinerates all elements of the subgroup $H_{1,5}$, which has the neat, equidistant distribution of its elements shown in Fig. 6.[24]

In contrast, cases of powers of an odd prime p, $Z_{p^i}^*$ for $i \geq 2$, seems to have been unpopular, and the present authors do not know their application. The group $Z_{p^i}^*$ is devoid of multiples of p in the interval $(0, p^i)$, which form the set V of numbers,

$$V := \{p, 2p, \cdots, (p^{i-1} - 1)p\}, \quad \sharp V = p^{i-1} - 1.$$

These give a regular array of vacancies in the plot of 2-tuples from the sequence $<z>$ in the right of Fig. 4. Its left figure of $\{q_1, q_2, \cdots\}$ of quotients is complicated by errors of $\mathrm{O}(1/z) = \mathrm{O}(1/\sqrt{d})$, but a view of the figure slanted will reveal the persistence of vacancies. Since we shall have a better prospect of the setting after observations of more general composite moduluses of our concern, we postpone the discussion of $d = p^i$ $(i \geq 2)$ cases to Sec. 8.

We now pass from visual information to considerations on the structure of composite modulus groups. For simplicity of arguments we leave generality, and start with the specific case of our interest. Take two distinct odd primes p_1, p_2, and form $d = p_1 p_2$ as the modulus. The orders of relevant groups are:

$$\sharp Z_{p_1}^* = p_1 - 1, \quad \sharp Z_{p_2}^* = p_2 - 1, \quad \sharp Z_{p_1 p_2}^* = (p_1 - 1)(p_2 - 1).$$

[24] As a preparation for Sec. 7 we note here a singularity of the prime 2 among primes, as frequently stated. Assume $d = 2^i$, $i \geq 4$. Integers that are coprime with 2^i are the totality of odd integers. Thus $Z_{2^r}^*$ is the set of odd integers modulo 2^r. They are classified into $1, 3, 5, 7$ modulo 8, as noted already. Though Theorem 8 (II) lacks descriptions, the integers in $H_{1,3} := A_1^{(2^i)} \cup A_3^{(2^i)}$, $\sharp H_{1,3} = 2^{i-2}$, also form a cyclic subgroup with generators in $A_3^{(2^i)}$. We may further add $A_1^{(2^i)}$ alone is cyclic, but with the order $\sharp A_1^{(2^i)} = 2^{i-3}$ smaller than that of $H_{1,5}$. The problem with $H_{1,3}$ is well-known; any integer $z \equiv 3 \bmod (8)$ has its powers with non-equidistant motion $3, 1, 3, 1, 3, 1, \cdots$ in their least significant 3 bits. Compare Figures 5 and 6. This subgroup $H_{1,3}$, though cyclic, should be regarded inadequate for uniform distribution.

It is important to see the elements of $Z^*_{p_1p_2}$, which are integers in the interval $[1, 2, \cdots, p_1p_2 - 1]$ excluding multiples of p_1 and p_2. Namely, $p_1 + p_2 - 2$ integers

$$p_1, 2p_1, \cdots, (p_2 - 1)p_1; \quad p_2, 2p_2, \cdots, (p_1 - 1)p_2$$

are absent in $Z^*_{p_1p_2}$. This fact gives another proof of the relation

$$\varphi(p_1p_2) = p_1p_2(1 - 1/p_1)(1 - 1/p_2) = (p_1 - 1)(p_2 - 1) = (p_1p_2 - 1) - (p_1 + p_2 - 2).$$

Let primitive roots modulo p_1 and modulo p_2 be z_1 and z_2, respectively. Apply Chinese remainder theorem 4 to obtain $z \in Z^*_{p_1p_2}$ fulfilling

$$z \equiv (z_1, z_2) \bmod (p_1, p_2), \quad z \equiv z_1U_1 + z_2U_2 \bmod (p_1p_2).$$

The order t of z is given by

$$t := \mathrm{ord}(z) = \mathrm{LCM}(\mathrm{ord}(z_1), \mathrm{ord}(z_2)) = 2\mathrm{LCM}(q_1, q_2), \quad q_1 := (p_1 - 1)/2, \;\; q_2 := (p_2 - 1)/2.$$

We take hereafter that q_1 and q_2 are coprime. This gives the largest order $t = 2q_1q_1$, but t is then only the half of $\sharp Z^*_{p_1p_2} = 4q_1q_2$. Thus, $Z^*_{p_1p_2}$ is not cyclic, and Lagrange's theorem dictates that the cyclic sequence $<z>$ and its coset $n<z>$, $n \notin <z>$, divide the group $Z^*_{p_1p_2}$ precisely into two parts.

This is the setting that we are going to exploit. We shall take $<z>$ or $n<z>$ for the candidate of integers distributed uniformly in the range $(0, p_1p_2)$. Note that our experiences on multiplicative congruential generators suggest that, even if a cyclic sequence $<z>$ generates all elements of the group as in Figures 1 and 6, the use of the whole sequence $<z>$ is inadequate. This is because the last half of the sequence just puts numbers into vacancies left by the first half, which should be taken as a strong correlation between two halves. Thus, the use in the present case of either one of $<z>$ or its coset $n<z>$ is the same as the use of half of $<z>$ in the case of cyclic z. The fact that the construction (6) for $z^j = {z_1}^j U_1 + {z_2}^j U_2$ or $nz^j = n_1{z_1}^j U_1 + n_2{z_2}^j U_2$ gives shuffling of two, uniformly distributed sequences lends further support to this viewpoint on the behavior of the sequence $<z>$ in smaller scales of $\mathrm{O}(p_1)$ or $\mathrm{O}(p_2)$.

Thoughts may be extended to cases with s distinct odd primes $p_1, p_2, \cdots, p_s$ forming a modulus $d = p_1p_2 \cdots p_s$. Assume that

$$q_i := (p_i - 1)/2, \quad i = 1, 2, \cdots, s, \quad q_1, q_2, \cdots, q_s \text{ are mutually coprime,}$$

are fulfilled as before. Take primitive roots z_i modulo p_i for respective $i = 1, 2, \cdots, s$, and determine $z \in Z^*_{p_1p_2\cdots p_s}$ by $z \equiv z_i \bmod (p_i)$ for $i = 1, 2, \cdots, s$ with the help of Chinese remainder theorem 4. The multiplier z then has the order

$$2\mathrm{LCM}(q_1, q_2, \cdots, q_s) = 2q_1q_2 \cdots q_s.$$

Thus, $<z>$ occupies $1/2^{s-1}$ $(s \geq 2)$ of the group elements that total to $\sharp Z^*_{p_1p_2\cdots p_s} = 2^s q_1q_2 \cdots q_s$. For s larger, this portion of the cyclic subgroup $<z>$ or its cosets $n<z>$ is smaller. Ambiguities will grow regarding the validity of the spectral test for sequential independence, as well as difficulties to have spectral tests for the enhanced period of $\mathrm{O}(2q_1q_2 \cdots q_s)$. We see here reasons to take the case $s = 2$ as optimal.

The remaining possibility of the factor 2^i in the modulus d will later be found to have a decisive reason that it should be avoided.

The merit of the modulus consisting of two distinct odd primes will now be manifest. The choice realizes the same type of uniformity as the existing multiplicative congruential methods, enhances

the period nearly to the square and nearly doubles the precision of emitted numbers. We see below that they may be tested spectrally. Last but not least, the progress of computers reinforces, but never diminishes, these merits of the specified way of design as random number generators.

5. Vector space and its points generated by cyclic sequences: Lattice structures

We turn to the independence of distribution of consecutive integers in sequences. Take a reduced residue class group Z_d^* with generally composite modulus d. We start here with fixing the notion, and discuss the fact that, irrespective of whether $z \in Z_d^*$ is a generator of Z_d^* or not, z generates a cyclic sequence $<z>$ or its coset sequence $n<z>$ whose consecutive l-tuples give points in a lattice determined by d, z. The fact that approximating cyclic sequences necessarily have lattice structures is our luck by which we are afforded chances and tools to translate the independence of distribution into a geometrical comprehension that may be estimated quantitatively by spectral tests.[25]

Let us consider for the moment without congruence relation modulo d. We identify points in E_l with their coordinates, and introduce specific notations below for a set of points:

$$\{\mathrm{P}_j := (z^j, z^{j+1}, z^{j+2}, \cdots, z^{j+l-1}) = z^j(1, z^1, z^2, \cdots, z^{l-1}) =: z^j\mathrm{P}_0 |\ j = 1, 2, \cdots\}.$$

A lattice is defined as follows for our later convenience:

Definition 9 Let $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l\}$ be a set of linearly independent[26] vectors[27] in l dimensional Euclidean space E_l. The set of their linear combinations with arbitrary integer coefficients is defined to be a lattice in E_l spanned by the bases (or basis vectors) $\{\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l\}$, with the notation

$$(\!(\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l)\!) := \{c_1\boldsymbol{e}_1 + c_2\boldsymbol{e}_2 + \cdots + c_l\boldsymbol{e}_l |\ c_1, c_2, \cdots, c_l \in \boldsymbol{Z}\},$$

where $\boldsymbol{Z}$ is the set of integers as usual. **(End of Definition 9)**

In the sense of solid state physics Definition 9 gives simple lattices. We deal exclusively with simple lattices. Points in the right of Figures 4,5 (and, in fact, those of Figures 2, 3, 6) are occupying *a portion* of simple lattices, as will be clarified below in Therem 11. The linear independence of vectors is well-known to be equivalent for the determinant formed by them to be non-zero, or for the hyper cube spanned by them to have non-vanishing volume. The same condition may be stated that their linear combination with real coefficients can be a zero vector if and only if coefficients are all zero. The lattice $(\!(\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l)\!)$ as a set of vectors is closed by multiplication of elements by integers and by additions of constituent vectors.

Given a point P in E_l, we often need to consider the set of all points with coordinates congruent to those of P modulo d. This is accomplished feasibly in terms of lattices.

Corollary 10 Introduce vectors that represent d-translation parallel to respective axes in E_l by

$$\boldsymbol{e}_1^{(d)} := {}^\tau(d, 0, 0, \cdots, 0, 0), \quad \boldsymbol{e}_2^{(d)} := {}^\tau(0, d, 0, \cdots, 0, 0), \quad \cdots, \quad \boldsymbol{e}_l^{(d)} := {}^\tau(0, 0, 0, \cdots, 0, d).$$

[25] We ask the reader to abandon the rootless feeling that lattice structure is contradicting randomness. Any sequence of integers with large upper bound z is approximated by the corresponding numbers in $n<z> \subset Z_d^*$ by Theorem 2, and the consecutive l-tuple of numbers of $n<z>$ forms a point belonging to a lattice in the l-dimensional space E_l. If we find difficulties in the recognition of lattice structures in plots of realistic integer sequences with large base z, say that of π in numerals of base $z = 10^3$, it is because the points occupy only a very small portion of lattice points, and our vision fails to grasp the underling lattice structures with too many vacancies. Or, if we had accustomed to use large base numerals in our arithmetic, say $z = 10^3$, and to plot the results in $[0, 1]$, we might have experienced lattice structures as common sense in any division processes for n/d.

[26] We define linear independence with real coefficients.

[27] All vectors are defined here to be column vectors. By reasons of the space on the paper they will be denoted typically as ${}^\tau\boldsymbol{e} = (a_1, a_2, \cdots, a_l)$ or $\boldsymbol{e} = {}^\tau(a_1, a_2, \cdots, a_l)$ by their transposed forms.

(I) Let a point P in E_l is given, together with a point Q chosen arbitrarily for the basis point. Denote $\mathrm{X} \equiv \mathrm{P} \bmod (d)$ if the point X has coordinates congruent to those of P modulo d. The set of position vectors $\overrightarrow{\mathrm{QX}}$ with components congruent to those of $\overrightarrow{\mathrm{QP}}$ modulo d is expressed as follows:[28]

$$\{\overrightarrow{\mathrm{QX}}|\ \mathrm{X} \equiv \mathrm{P} \bmod (d)\} = \overrightarrow{\mathrm{QP}} + (\!(\boldsymbol{e}_1^{(d)}, \boldsymbol{e}_2^{(d)}, \cdots, \boldsymbol{e}_l^{(d)})\!).$$

(II) The set of points in E_l congruent to points in $\{\mathrm{P}_1, \mathrm{P}_2, \cdots, \mathrm{P}_k\}$ modulo d may be denoted as:

$$\{\overrightarrow{\mathrm{QX}}|\ \mathrm{X} \text{ is congruent to one of } \mathrm{P}_1, \mathrm{P}_2, \cdots, \mathrm{P}_k \text{ modulo } d\}$$
$$= \{\overrightarrow{\mathrm{QP}_1}, \overrightarrow{\mathrm{QP}_2}, \cdots, \overrightarrow{\mathrm{QP}_k}\} + (\!(\boldsymbol{e}_1^{(d)}, \boldsymbol{e}_2^{(d)}, \cdots, \boldsymbol{e}_l^{(d)})\!).$$

(Proof) (I) Let the points P, X be $\mathrm{P} = (\pi_1, \pi_2, \cdots, \pi_l)$, $\mathrm{X} = (\xi_1, \xi_2, \cdots, \xi_l)$ in coordinates. The relation $\mathrm{X} \equiv \mathrm{P} \bmod (d)$ is equivalent to the existence of a set of integers $c_1, c_2, \cdots, c_l$ that give, for any point Q,

$$\overrightarrow{\mathrm{QX}} = \overrightarrow{\mathrm{QP}} + \overrightarrow{\mathrm{PX}} = \overrightarrow{\mathrm{QP}} + {}^{\tau}(\xi_1 - \pi_1, \xi_2 - \pi_2, \cdots, \xi_l - \pi_l) = \overrightarrow{\mathrm{QP}} + c_1\boldsymbol{e}_1^{(d)} + c_2\boldsymbol{e}_2^{(d)} + \cdots + c_l\boldsymbol{e}_l^{(d)}.$$

Forming sets of all possibilities on left hand side, we have

$$\{\overrightarrow{\mathrm{QX}}|\ \mathrm{X} \equiv \mathrm{P} \bmod (d)\} \subset \overrightarrow{\mathrm{QP}} + (\!(\boldsymbol{e}_1^{(d)}, \boldsymbol{e}_2^{(d)}, \cdots, \boldsymbol{e}_l^{(d)})\!).$$

Taking the all possibilities of the right hand side, we have the converse inclusion relation, and the conclusion of (I) holds true.
(II) It is obvious that the sum of sets obtained in (I) is the answer, as given. ■

We have now the lattice that nests points formed by consecutive numbers of the cyclic sequence $<z>$ and the coset sequence $n<z>$ of Z_d^*.

Theorem 11 Let the modulus $d \geq 1$ may be composite, z, n be any elements of Z_d^*, and $l \geq 1$ be any integer. Denote

$$\mathrm{P}_j := (nz^j, nz^{j+1}, nz^{j+2}, \cdots, nz^{j+l-1}) = nz^j(1, z^1, ^2, \cdots, z^{l-1}), \quad j = 0, 1, 2, \cdots$$

for points formed by l consecutive numbers of the coset sequence $n<z>$, or by those of the cyclic sequence $<z>$ in the case $n = 1$. The sequence of position vectors $\{\overrightarrow{\mathrm{OP}_j}|\ j = 0, 1, 2, \cdots\}$ in E_l, together with all position vectors of points that are congruent to $\{\mathrm{P}_j|\ j = 0, 1, 2, \cdots\}$ modulo d, are in the lattice $G_1 := (\!(\boldsymbol{e}_1')\!)$ for $l = 1$ and in $G_l := (\!(\boldsymbol{e}_1', \boldsymbol{e}_2^{(d)}, \cdots, \boldsymbol{e}_l^{(d)})\!)$ for $l \geq 2$ with[29]

$$\boldsymbol{e}_1' = {}^{\tau}(1, z, z^2, \cdots, z^{l-2}, z^{l-1}), \ \ \boldsymbol{e}_2^{(d)} = {}^{\tau}(0, d, 0, \cdots, 0, 0), \ \ \cdots, \ \ \boldsymbol{e}_l^{(d)} = {}^{\tau}(0, 0, 0, \cdots, 0, d). \quad (7)$$

In the l-dimensional hypercube C_l formed by intervals $[0, d)$ on respective coordinate axes, the lattice G_l has exactly d lattice points.

(Proof) In the case $l \geq 2$, the basis vectors $\boldsymbol{e}_2^{(d)}, \boldsymbol{e}_3^{(d)}, \cdots, \boldsymbol{e}_l^{(d)}$ realize d-shift of coordinates along the second, the third, $\cdots$, and the l-th axes upon addition to any position vectors. The d-shift along the first axis is realized by the vector $\boldsymbol{e}_1^{(d)}$ in G_l,

$$\boldsymbol{e}_1^{(d)} := d\boldsymbol{e}_1' \quad (l = 1); \qquad \boldsymbol{e}_1^{(d)} := d\boldsymbol{e}_1' - z\boldsymbol{e}_2^{(d)} - z^2\boldsymbol{e}_3^{(d)} - \cdots - z^{l-1}\boldsymbol{e}_l^{(d)} \quad (l \geq 2). \qquad (8)$$

Therefore, including the case $l = 1$, any element of the lattice $(\!(\boldsymbol{e}_1^{(d)}, \boldsymbol{e}_2^{(d)}, \cdots, \boldsymbol{e}_l^{(d)})\!)$ belongs to the lattice $(\!(\boldsymbol{e}_1', \boldsymbol{e}_2^{(d)}, \cdots, \boldsymbol{e}_l^{(d)})\!)$, and the following inclusion relation holds true:

[28] For sets A, B of vectors we denote $A + B := \{\boldsymbol{u} + \boldsymbol{v}|\ \boldsymbol{u} \in A, \ \boldsymbol{v} \in B\}$. Then $\{\overrightarrow{\mathrm{QP}}\} + (\!(\boldsymbol{e}_1, \boldsymbol{e}_2, \cdots, \boldsymbol{e}_l)\!)$ is the notation for the right hand side below, but we admit the omission of the symbol $\{\cdots\}$ if the set consists of a single element.

[29] In the case of $l = 1$, $\boldsymbol{e}_1'$ is a 1-component vector (1), or a scalar 1.

$$(\!(\boldsymbol{e}_1^{(d)}, \boldsymbol{e}_2^{(d)}, \cdots, \boldsymbol{e}_l^{(d)})\!) \subset G_l = (\!(\boldsymbol{e}'_1, \boldsymbol{e}_2^{(d)}, \cdots, \boldsymbol{e}_l^{(d)})\!).$$

Position vectors of points generated by l-tuples of numbers from $n<z>$ have thus expressions

$$\overrightarrow{\mathrm{OP}_0} = n\boldsymbol{e}'_1, \quad \overrightarrow{\mathrm{OP}_1} = nz\boldsymbol{e}'_1, \quad \overrightarrow{\mathrm{OP}_2} = nz^2\boldsymbol{e}'_1, \quad \cdots, \quad \overrightarrow{\mathrm{OP}_j} = z^j\boldsymbol{e}'_1, \quad \cdots.$$

These are all vectors in $G_l = (\!(\boldsymbol{e}'_1, \boldsymbol{e}_2^{(d)}, \cdots, \boldsymbol{e}_l^{(d)})\!)$. Therefore, the totality of position vectors for points congruent to $\{\mathrm{P}_0, \mathrm{P}_1, \cdots, \mathrm{P}_j, \cdots\}$ modulo d is $\{\overrightarrow{\mathrm{OP}_0}, \overrightarrow{\mathrm{OP}_1}, \cdots, \overrightarrow{\mathrm{OP}_j}, \cdots\} + (\!(\boldsymbol{e}_1^{(d)}, \boldsymbol{e}_2^{(d)}, \cdots, \boldsymbol{e}_l^{(d)})\!)$ by Lemma 10. We thus have:

$$\{\overrightarrow{\mathrm{OP}_0}, \overrightarrow{\mathrm{OP}_1}, \cdots, \overrightarrow{\mathrm{OP}_j}, \cdots\} + (\!(\boldsymbol{e}_1^{(d)}, \boldsymbol{e}_2^{(d)}, \cdots, \boldsymbol{e}_l^{(d)})\!) \subset G_l = (\!(\boldsymbol{e}'_1, \boldsymbol{e}_2^{(d)}, \cdots, \boldsymbol{e}_l^{(d)})\!),$$

which proves the first half of Theorem 11. As to the total number of lattice points in C_l, we need to consider only the number of ways to choose integer coefficients of vectors $\boldsymbol{e}'_1, \boldsymbol{e}_2^{(d)}, \cdots, \boldsymbol{e}_l^{(d)}$ so that

$$\boldsymbol{e} := c_1\boldsymbol{e}'_1 + c_2\boldsymbol{e}_2^{(d)} + \cdots + c_l\boldsymbol{e}_l^{(d)}$$

is in C_l. The first component of $\boldsymbol{e}$ is c_1 by (7), so that there are d ways to choose $c_1 = 0, 1, \cdots, d-1$. If $l = 1$, these are all of choices to be considered. In cases $l \geq 2$, the second component of $\boldsymbol{e}$ is pulled back to $[0, d)$ by the unique choice of c_2. Similarly, $c_3, \cdots, c_l$ are determined uniquely. We thus obtain exactly d ways to choose the set $c_1, c_2, \cdots, c_l$ of integers irrespective of l, which give d lattice points in C_l. ■

We stress that the theorem above applies to any reduced residue class group Z_d^* with modulus $d \geq 1$ that may be composite, and with its arbitrary elements z, n. Namely, Figures 1-6 shown, as well as all figures to be shown below, conform to this theorem.[30] The total d lattice points in the cube C_l is never occupied fully by the points in C_l generated by $<z>$ and $n<z>$ which can amount only to $\sharp Z_d^* = \varphi(d) < d$ in number. Figuratively speaking, the lattice in Theorem 11 provides abundant seats, but they are never occupied fully by points from $<z>$ and $n<z>$.

The case nearest to the full occupation arises with odd prime modulus $d = p > 2$, $\varphi(d) = d - 1$. The sole vacant seat is the origin of C_l, because 0 is absent in Z_p^*. This observation completes the usual proof of the lattice structure of $<z>$, which as a set is the same as $n<z>$ for a primitive root z in Z_p^*; we share the identical lattice with the spectral test for this case $d = p$ and its primitive root z. For $d = 2^i$ $(i \geq 4)$ the generator $z \equiv 5 \bmod (8)$ in subgroup $H_{1,5}$ has the order 2^{i-2}, while the seats provided by Theorem 11 is $d = 2^i$. Thus, occupied seats are only $1/4$ of the whole. The lattice in Theorem 11 for $d = 2^i$ is different from those used in the spectral test for this modulus. Since a detailed proof is not needed below, we note only the following.

Lemma Denote $\{\mathrm{P}_j | \ 1 \leq j \leq 2^{i-2}\}$ for the points[31] of l-tuples from $<z>$ generated by $z \equiv 5 \bmod (8)$ in $Z_{2^i}^*$. Define a vector $\boldsymbol{e} = {}^{\tau}(1, z, z^2, \cdots, z^{l-1})$. Taking the basis point Q defined by $\overrightarrow{\mathrm{OQ}} = -3\boldsymbol{e}$, the position vectors $\{\overrightarrow{\mathrm{QP}_j} | \ 1 \leq j \leq 2^{i-2}\}$ occupy *the whole* of the lattice $(\!(4\boldsymbol{e}, \boldsymbol{e}_2^{(d)}, \boldsymbol{e}_3^{(d)}, \cdots, \boldsymbol{e}_l^{(d)})\!)$ in C_l.

6. Spectral test and the geometrical distribution of points from cyclic sequences

Lattice structures of points generated by l-tuples from cyclic and coset sequences $<z>$ and $n<z>$ are the source of the power of spectral tests that furnish us with measures of statistical properties of

[30] As a minute point consider the case $l > t$, with t for the order of $z \in Z_d^*$. Then the sequence $<z>$ may give the identical z^{j+k-1} and $z^{j+k+t-1}$ to the point P_j as its k-th and $k+t$-th coordinates. Then d-shifts along these axes should be restricted to be identical. Restricted d-shifts, however, are included in d-shifts without restriction. Therefore, the statement that vectors are in the lattice, needs no alteration.

[31] Such points are plotted typically in Fig. 6 for $d = 2^{10}$.

numbers arising in these sequences. We refer the reader to penetrating descriptions on the theory, on the practice and on significant results of spectral tests given in Knuth.[32]; we shall also have a feature of the computational structure of spectral tests in Addendum at the end of the report. In this section we observe briefly some examples for $l = 2$, in order to obtain intuitional understanding of contents and terminologies of spectral tests.

Figures 7-10 below show typical cases with primitive root z in the prime modulus $d = 251$, which is the same as Figures 1 and 2. As before, the left shows points $\mathrm{P}_j = (x_j/z, x_{j+1}/z)$ of quotients in $n/d = 1/251$, and the right is for $\mathrm{Q}_j = (r_j/d, r_{j+1}/d)$, the points of remainders, both in the frame $-0.05 \leq x, y \leq 1.05$. Compared to Figures 1 and 2 primitive roots are taken larger, so that these 2-dimensional plots on the left and the right are closer to each other than in Figures 1 and 2.

Distributions of points take diverse forms in these figures, and various interpretations may be given. Take Fig. 7, and suppose intervals $[0, 1]$ on horizontal and vertical axes are divided by the width $1/\sqrt[3]{d}$, for example. Then the square is divided into small squares of area $\sqrt[3]{d^2}$. If each of these small squares contains approximately $\sqrt[3]{d}$ points, in particular irrespective of moderate change of its shape, we may interpret the figure to represent that consecutive numbers in $<z>$ are appearing

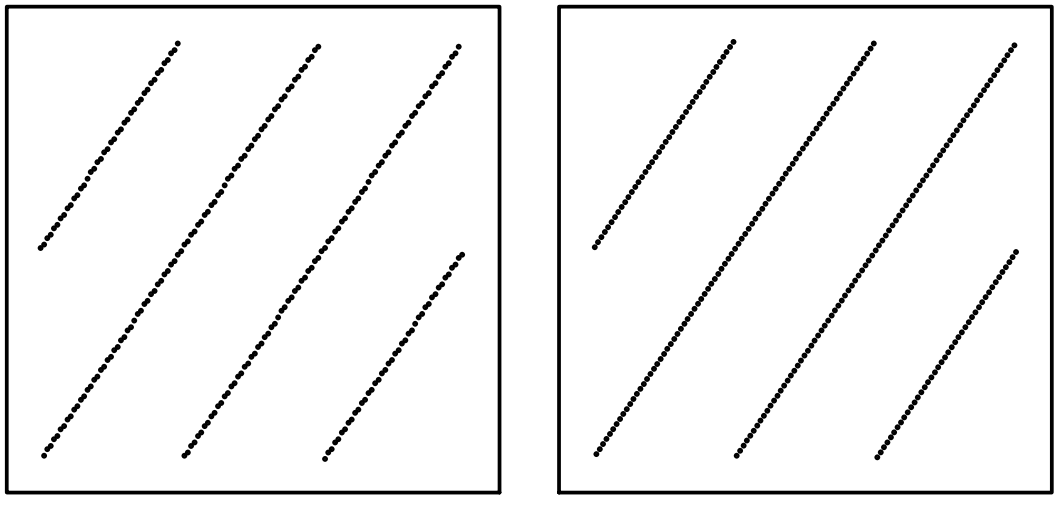

Fig. 7: $z = 127$, $d = p = 251$

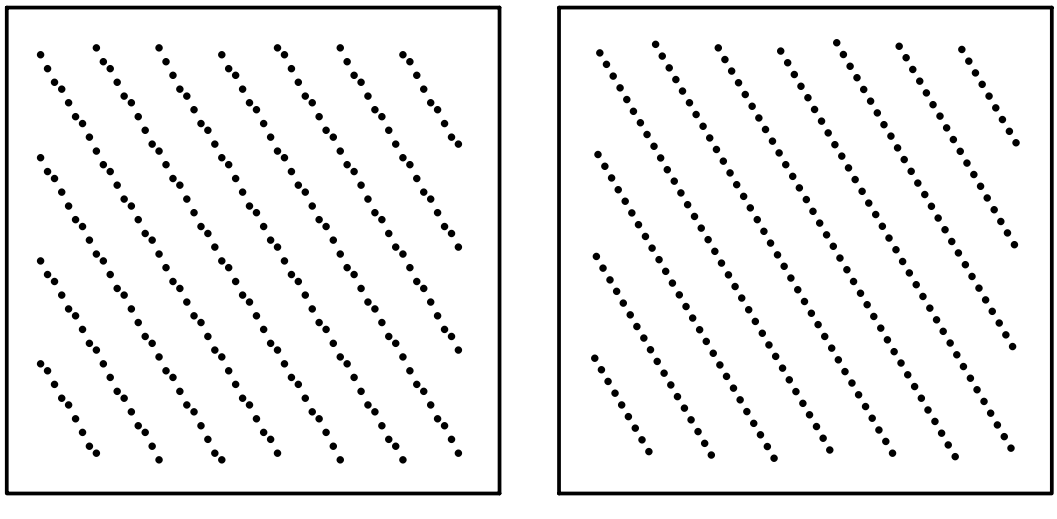

Fig. 8: $z = 61$, $d = p = 251$

[32] D. E. Knuth, in footnote[5], pp. 96-115.

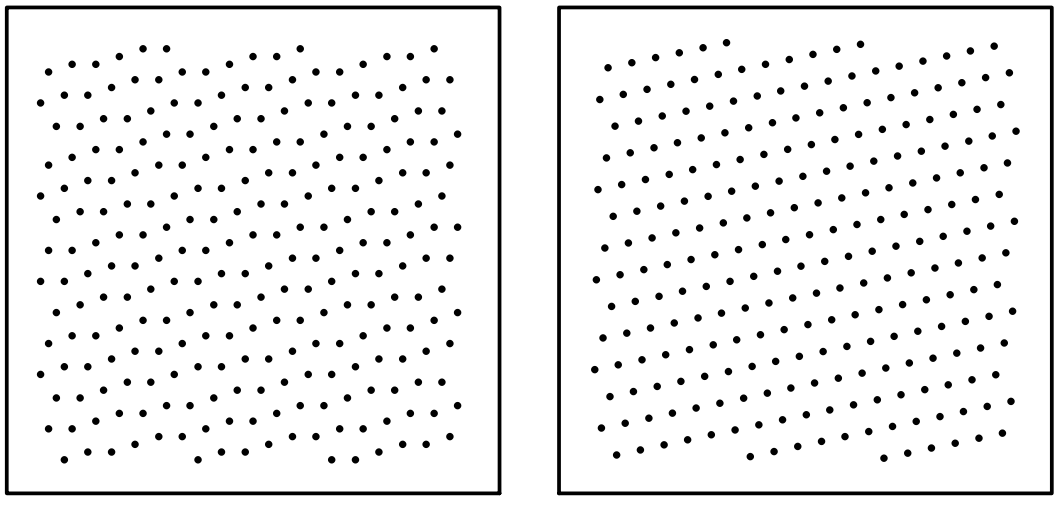

Fig. 9: $z = 54$, $d = p = 251$

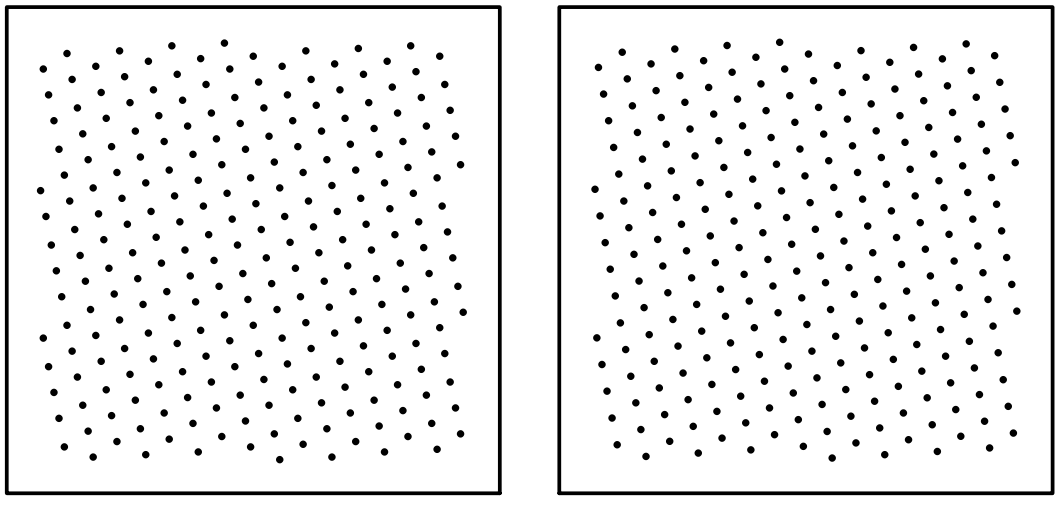

Fig. 10: $z = 162,\ d = p = 251$

independently. In this sense Fig. 7 shows poor distribution, Fig. 8 is a little better but unsatisfactory, while Figures 9 and 10 might be felt passable. Spectral tests express these feelings quantitatively. Namely, the test computes the largest distance $\lambda_{\max}$ between neighboring two lattice lines[33] for respective generator z, and evaluates z higher for smaller $\lambda_{\max}$.

Let us compute $\lambda_{\max}$ by our hand, magnifying the side of the square to 251. In Fig. 9 for $z = 54$ we find that $\lambda_{\max}$ is given by the distance from the origin to the line threading points $(5, 19)$ and $(19, 22)$. This gives

$$(z = 54): \quad \lambda_{\max} = 251/\sqrt{205}.$$

In Fig. 10 it is given by the distance from the origin to the line connecting $(14, 9), (11, 25)$. The computation results in

$$(z = 162): \quad \lambda_{\max} = 251/\sqrt{265}.$$

Thus the generator $z = 162$ is estimated to be the better, justifying the intuition.

[33] These are straight lines connecting two lattice points. In $l \geq 3$ the corresponding notion is (hyper)planes that contain l lattice points.

From a purely geometrical point of view in two dimension, the triangle lattice, the case that two basis vectors form a regular triangle, gives the shortest $\lambda_{\max}$, upon normalization of the area of the parallelopiped spanned by base vectors to 1. In other words, the spectral test for $l = 2$ seeks the lattice configuration that is nearest to the triangle lattice; this fact will be utilized below for visual judgments. This ideal lattice cannot be realized by vectors with integer components, so that the computed $\lambda_{\max}$ is always larger. In the case of Fig. 10 $\lambda_{\max}$ is 104.58% of the theoretical optimum.

Distances of lattice lines, or more generally those of lattice hyperplanes in higher dimensions, are related to the length of vectors in the so-called dual lattice, and $\lambda_{\max}$ is obtained by calculating the smallest magnitude of non-zero dual lattice vectors. As noted already,[34] G. S. Fishman and L. R. Moore (1986) performed epoch making spectral tests that exhaust all primitive roots for the prime modulus $d = p = 2^{31} - 1$, for dimensions $1 \leq l \leq 6$; in the terminology used already in Sec. 1, they gave exhaustive 6-th degree tests. Their criterion was that $\lambda_{\max}$ is within 125% of the theoretical optimum for respective $l = 2, 3, \cdots, 6$, and only $7.5 \times 10^{-5}\%$ of primitive roots are reported to have passed the test. This would indicate our general fate that we shall have too little chance to obtain a good generator without the exhaustive tests on possibilities.

Computational procedures of spectral tests, including cases for composite moduluses, will be sketched in Addendum at the end of this report, in the way to derive simple estimates of the amount of computations involved. We leave inferences and quotations to Sec. 8, and note here only the following prospect. For a prime $p \geq 3$ any primitive root z modulo p has the order $p - 1$, and z^j for j coprime to $p - 1$ are all of primitive roots modulo p. Thus, $\varphi(p-1) \leq (p-1)/2 = \mathrm{O}(p/2)$ is the total number of primitive roots modulo p. This factor enhances the amount of computation of exhaustive spectral tests, and computational amounts may be diminished if we could concentrate only on several hopeful candidates for good generators. Thinking of the shuffling nature of the construction of z out of z_1, z_2 by Chinese remainder theorem, we might expect fair chances to obtain good or passable generator z out of a few sets of good primitive roots z_1, z_2.

We examine this idea in the next section for its structural details, how the composite moduluses should be chosen, what are the attainable results and so forth. We also discuss in Sec. 8 necessary amounts of computation, or the complexity of the problem expressed by the total number of cases to be tested. Before setting out, we note an important motivation for the use of composite moduluses by considering the geometry of point sets generated. In Figures 1-10, the plot of remainders on the right may be classified into two cases. In one of them, constituted by Figures 1,4,7-10, plotted point sets are symmetric with respect to the center $\mathrm{M} = (1/2, 1/2, \cdots, 1/2)$ of the (hyper)cube C_l. In the remaining Figures 2,3,5 and 6 the point sets are asymmetrical with respect to M. These cases may be discerned in a simple and generic way described in Theorem 15 below, to which we prepare the following.

Corollary 14 Let integers $d, l \geq 1$ be given. Identify the point P in E_l with its coordinates as

$$\mathrm{P} := (\xi_1, \xi_2, \cdots, \xi_l).$$

Introduce the point $\mathrm{M}_d := (d/2, d/2, \cdots, d/2)$. Let A_l be any set of points in E_l, which is invariant under d translations along coordinate axes.
(I) Let N_l be an arbitrary point in E_l and denote A_l'' for the point set that is symmetric to A_l with respect to N_l. Then A_l'' is invariant in d-translations along any coordinate axes of E_l.
(II) Let A_l' and $\overline{A_l}$ be point sets in E_l symmetric to A_l about M_d and the origin O, respectively. Then $A_l' = \overline{A_l}$ holds true.

[34] See footnote[8].

(Proof) (I) Consider a set of points A on a line that is invariant under d translations. It is obvious that the point set A'' symmetric to A about any point N on the line is invariant under d translations. As regards the set A_l'' in E_l symmetric to A_l with respect to N_l, the transformation may be realized by consecutive reflections orthogonal to coordinate axes in each of which d-translation invariance is conserved. Therefore, A_l'' is d-translation invariant with A_l along any coordinate axes.
(II) By (I) A_l', and $\overline{A_l}$ also, are invariant in d translations along coordinate axes of E_l. This gives

$$\begin{aligned} A_l' &= \{\mathrm{P}' := (-\xi_1 + d, -\xi_2 + d, \cdots, -\xi_l + d) |\ P = (\xi_1, \xi_2, \cdots, \xi_l) \in A_l\} \\ &= \{\mathrm{P}' = (-\xi_1, -\xi_2, \cdots, -\xi_l) |\ (\xi_1, \xi_2, \cdots, \xi_l) \in A_l\}, \end{aligned}$$

which proves $A_l' = \overline{A_l}$. ■

Theorem 15 Let there be given a modulus $d \geq 1$ which may be composite. Take any $z, n \in Z_d^*$ and any integer $l \geq 1$. Denote S_l for the point set generated by consecutive l-tuples of integers in the coset sequence $n{<}z{>}$ in Z_d^*,

$$S_l := \{P_j \equiv (nz^j, nz^{j+1}, \cdots, nz^{j+l-1}) \bmod (d) |\ j = 0, 1, 2, \cdots\}.$$

Let S_l' and $\overline{S_l}$ be point sets symmetric to S_l with respect to the point $\mathrm{M}_d = (d/2, d/2, \cdots, d/2)$ and to the origin O, respectively.
(I) If $-1 \in {<}z{>} \bmod(d)$ is true, there holds $S_l = S_l'$. Namely, the point set formed by l consecutive numbers of $n{<}z{>}$ defined modulo d is symmetric about the point M_d, irrespective of the choice of $n \in Z_d^*$ including the case $n = 1$.
(II) If $-1 \notin {<}z{>} \bmod(d)$ is the case, then $S_l \cap S_l' = \phi$ holds true. Namely, the point set formed by l consecutive numbers of $n{<}z{>}$ defined modulo d is asymmetrical about the point M_d, irrespective of the choice of $n \in Z_d^*$ including the case $n = 1$.

(Proof) Since the points of S_l in E_l are defined by coordinates with congruence modulo d, S_l is invariant under d translations along coordinate axes. The same invariance is thus assured for $\overline{S_l}$ and S_l' by Corollary 14 (I).
(I) Assume $-1 \in {<}z{>} \bmod(d)$. Then, taken as numbers in the congruence modulo d, the periodic sequence $-\,{<}z{>}$ is a shift of another periodic sequence ${<}z{>}$; they are identical except for the choice of the starting point.[35] Thus $\overline{S_l} = S_l$ holds as sets, and Corollary 14 proves $S_l = \overline{S_l} = S_l'$.
(II) Suppose $-1 \notin {<}z{>} \bmod(d)$. Then ${<}z{>}$ is a proper subgoup of Z_d^* and has no number in common with the coset $-\,{<}z{>}$, with numbers taken in the sense of modulo d. Therefore, $n{<}z{>}$ and $-n\,{<}z{>}$ are also disjoint as sets of numbers modulo d, which implies S_l and $\overline{S_l}$ defined respectively on them cannot have a common point in E_l. Hence $S_l \cap \overline{S_l} = \phi$ holds. Since the relation $\overline{S_l} = S_l'$ still holds true by Corollary 14, we have $S_l \cap S_l' = \phi$, irrespective of the choice of $n \in Z_d^*$ including the case $n = 1$. ■

We have now plain but important prospects.

Corollary 16 Let there be given a modulus $d \geq 1$ and arbitrary elements $z, n \in Z_d^*$, together with an integer $l \geq 1$. Denote S_l and nS_l again for point sets generated in E_l by l-tuples of integers from the cyclic sequence ${<}z{>}$ and its coset sequence $n{<}z{>}$, respectively, with the inclusion of all points having congruent coordinates modulo d.
(I) If Z_d^* is cyclic and z is its generator, then $S_l = nS_l$ is symmetric about $\mathrm{M}_d = (d/2, d/2, \cdots, d/2)$, the center of the (hyper)cube C_d.
(II) In order for S_l and nS_l to be not symmetric with respect to M_d, it is necessary that z is not a generator of Z_d^*.

[35] Putting $-1 \equiv z^k$, we have $-\,{<}z{>} \equiv \{z^k, z^{k+1}, \cdots, z^{k+j-1}, \cdots\} \bmod (d)$.

(III) In particular, any generator $z \equiv 5 \bmod (2^i)$ in the subgroup $H_{1,5}$ of $Z^*_{2^i}$ generates S_l and nS_l that get rid of the symmetry with respect to M_d for any $n \in Z^*_{2^i} = A_1^{(2^i)} \cup A_3^{(2^i)} \cup A_5^{(2^i)} \cup A_7^{(2^i)}$.

(Proof) (I) If Z^*_d is cyclic and z is its generator, $<z>$ necessarily contains $n \in Z^*_d$ as well as $-1 \equiv d-1 \in Z^*_d$. Hence $S_l = nS_l$ holds, and the conclusion follows by (I) of Theorem 15.
(II) For the asymmetry of S_l and nS_l with respect to M_d, it is necessary (and sufficient) that $-1 \notin <z>$ holds by Theorem 15 (II). This certainly necessiates that z is not a generator of Z^*_d.
(III) Assumption $z \equiv 5 \bmod (8)$ gives $z^j \in H_{1,5}$, while -1 is in $A_7^{(2^i)}$. Because of $H_{1,5} \cap A_7^{(2^i)} = \phi$ we have $-1 \notin <z>$, and Theorem 15 (II) proves the statement. ■

7. Designs of uniform and independent random number sequences

With the obtained perspective we now turn to realistic aspects of composite modulus generators for uniform and independent random numbers. We start with cases of two odd primes forming the modulus, and gradually generalize the setting.

7A. Moduluses formed by the product of two odd primes

Let us reconfirm procedures and settings. We choose two distinct odd primes p_1, p_2 such that

$$q_1 := (p_1 - 1)/2, \quad q_2 := (p_2 - 1)/2$$

are co-prime. We next select *good* multipliers, z_1's and z_2's for moduluses p_1 and p_2, respectively, by 6-th degree exhaustive spectral tests. Then we choose another suitable element $n \in Z^*_{p_1 p_2}$ with properties[36]

$$n \approx (n_1, n_2) \bmod (p_1, p_2).$$

Chinese remainder theorem will finally provide us with the multiplier $z \in Z^*_{p_1 p_2}$ and the coset sequence $n<z>$ by

$$z \equiv z_1 \bmod (p_1), \quad z \equiv z_2 \bmod (p_2), \quad nz^j \equiv n_1 {z_1}^j U_1 + n_2 {z_2}^j U_2 \bmod (d = p_1 p_2), \quad j = 1, 2, \cdots .$$

The multiplier z has necessarily an even order $t = \mathrm{LCM}(p_1 - 1, p_2 - 1) = 2q_1 q_2$. The cyclic sequence $<z>$ and the coset sequence $n<z>$ for $n \notin <z>$, then form an exact division of the group $Z^*_{p_1 p_2}$ into two halves. The final spectral test on z in $Z^*_{p_1 p_2}$ examines the distribution of $d = p_1 p_2$ seats of a lattice characterized by z, d in the (hyper)cube C_d with sides of length d in the l-dimensional space E_l, $l \geq 2$. The seats are occupied by points generated by consecutive l-tuples of numbers from $<z>$ and $n<z>$, but leave vacancies (including the origin) totaling to $p_1 + p_2 - 1$. This the plot of the show to be presented.

Let us see what happens in reality with miniature cases for $l = 2$, the 2nd degree spectral tests. The point of significance is whether 2-dimensional configuration of seats realizes patterns close to a triangular lattice. The following Figures 11a-13c show plots of 2-tuples from $<z>$ in the same setting as Figures 1-10.

Figures 11a,b use twin primes $p_1 = 59,\ p_2 = 61$ to ensure co-prime $q_1 = 29$ and $q_2 = 30$. Primitive roots, $(z_1, z_2) = (13, 44) \bmod (59, 61)$ for Fig. 11a, and $(50 \equiv 13^{-1}, 44) \bmod (59, 61)$ for Fig. 11b, are chosen by their excellent performance in respective prime moduluses. The composite performance shown in Fig. 11a is poor as a 2-dimensional spectral test. In view of the individual excellence of z_1

[36]The choice may well be started from n_1, n_2 and then n may be obtained as below by Chinese remainder theorem.

and z_2, this is a problem arising from the combination, and may be ascribed to the closeness of periods, , similar to beats of sound waves or Moire fringes in optics. A moral will be that we should avoid twin primes as constituents of composite moduluses. Another point to be noted is that Fig. 11b shows some improvements, by the replacement of z_1 in Fig. 11a with its inverse that makes the sequence $<z_1> \bmod(p_1 = 59)$ move backward. This simple modification deserves trial in every case. Thus, all figures below are associated with b-named ones testing the possibility.

Figures 12a,b take odd primes $(p_1, p_2) = (43, 59)$ with a larger separation. Results are better; the difference between a and b is somewhat subtle. Figures 13a,b are still better; in particular Fig.13b is one of the best results obtained. Figure 13c shows the same plot as Fig. 13b for $<z>$, with the plot of points from the coset $n<z>$ added.

Figure 13c is attractive, and we are tempted to use its $<z>$ and $n<z>$ consecutively. This usage would realize, however, a statistically highly improbable integer sequence, viz. the sequence for $1/d$ first and then the sequence for n/d. Or, we may say that $<z>$ and its coset are strongly correlated. Though (almost) complete filling of seats, arising in single odd prime modulus cases with primitive root z or with $z \equiv 5 \bmod (8)$ in $d = 2^i$ moduluses, is similarly attractive, we should refrain from the

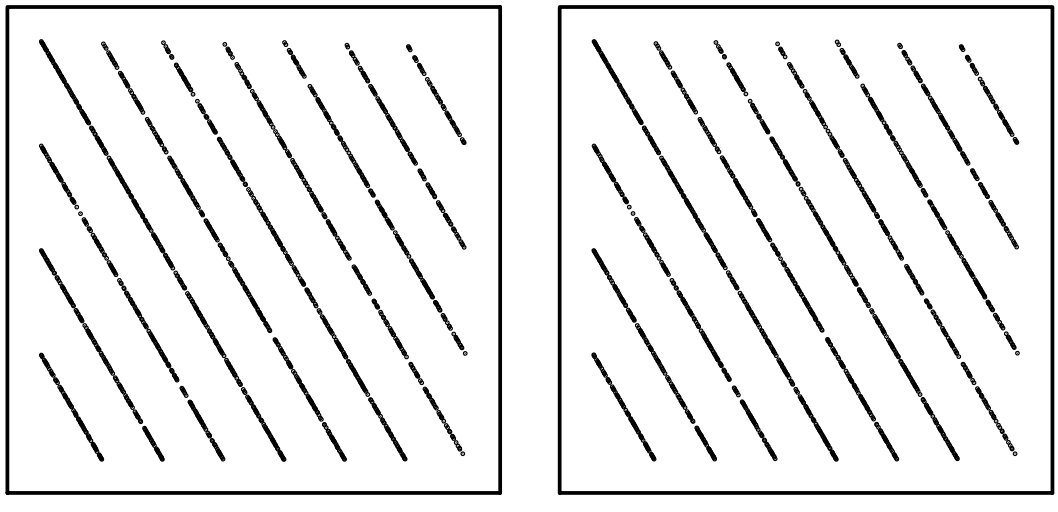

Fig. 11a: Modulus $d = 3599 = 59 \times 61$, $z = 898 \approx (13, 44) \bmod (59, 61)$.

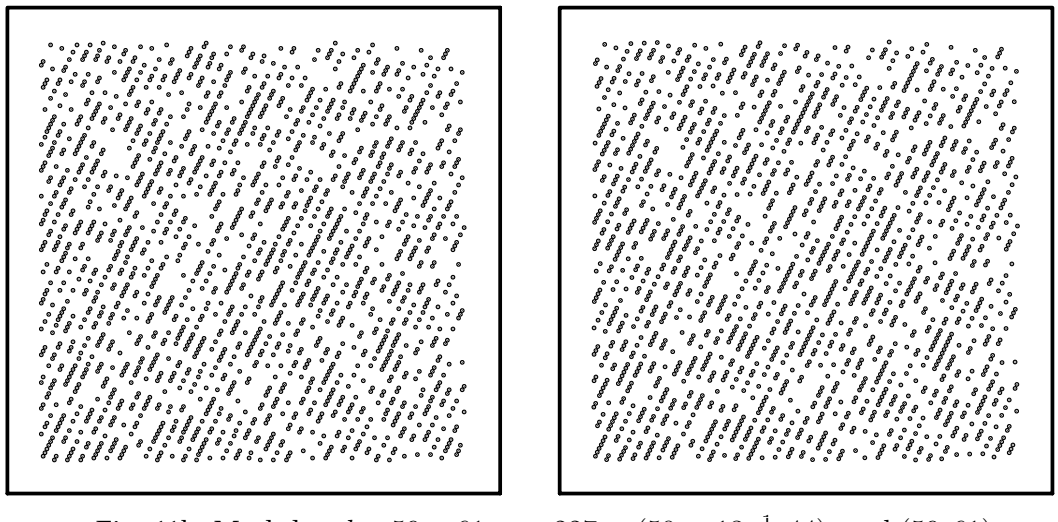

Fig. 11b: Modulus $d = 59 \times 61$, $z = 227 \approx (50 \equiv 13^{-1}, 44) \bmod (59, 61)$.

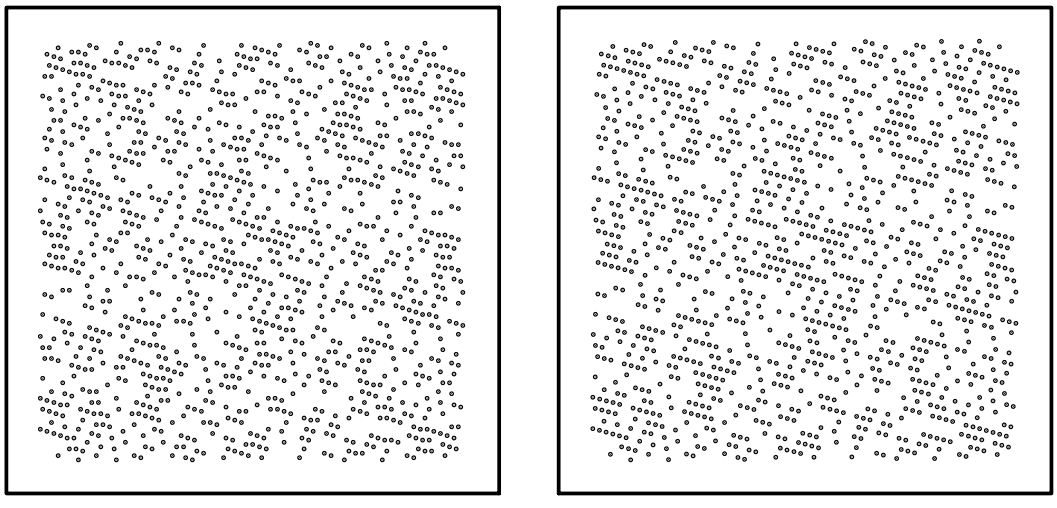

Fig. 12a: Modulus $d = 2537 = 43 \times 59$, $z = 190 \approx (18, 13) \bmod (43, 59)$.

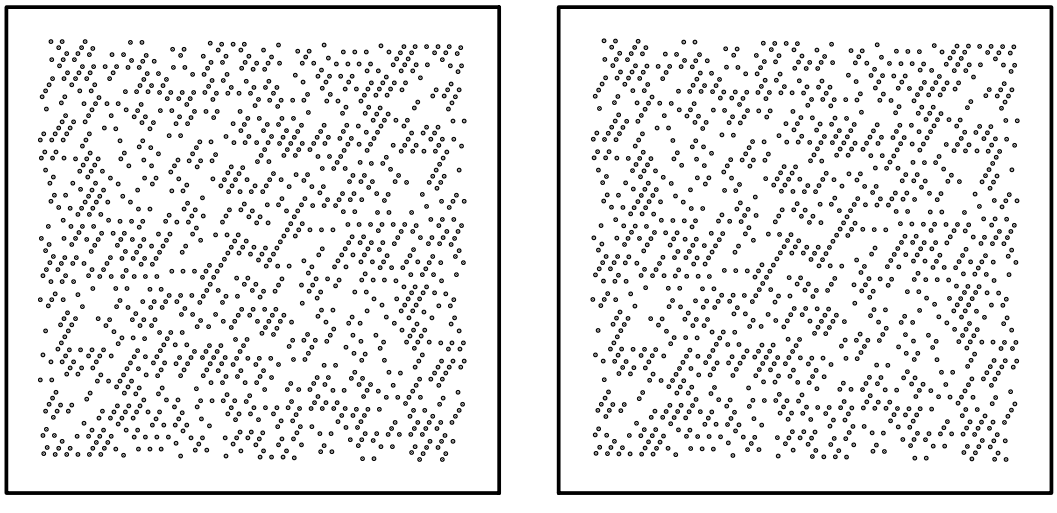

Fig 12b: Modulus $d = 2537$, $z = 485 \approx (12 \equiv 18^{-\hat{1}}, 13) \bmod (43, 59)$.

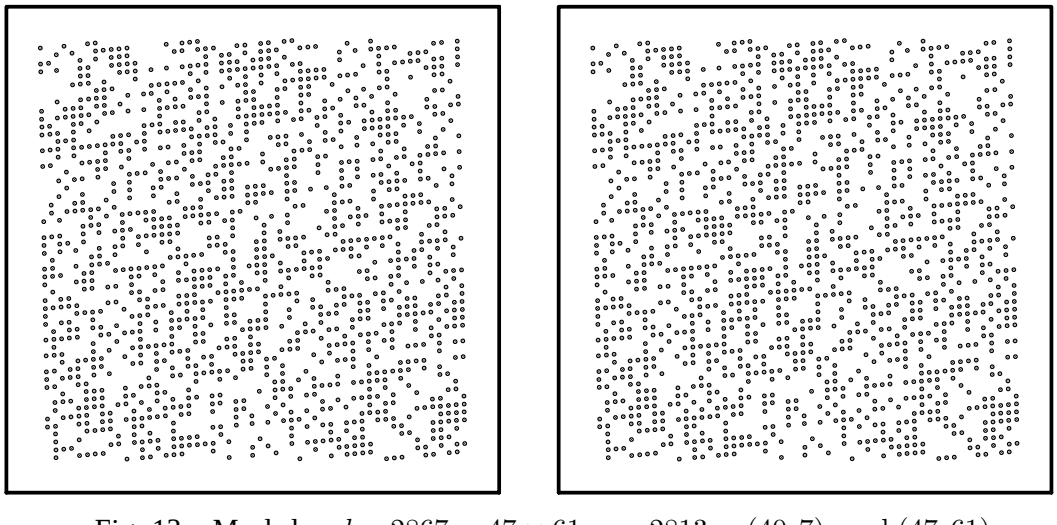

Fig. 13a: Modulus $d = 2867 = 47 \times 61$, $z = 2813 \approx (40, 7) \bmod (47, 61)$.

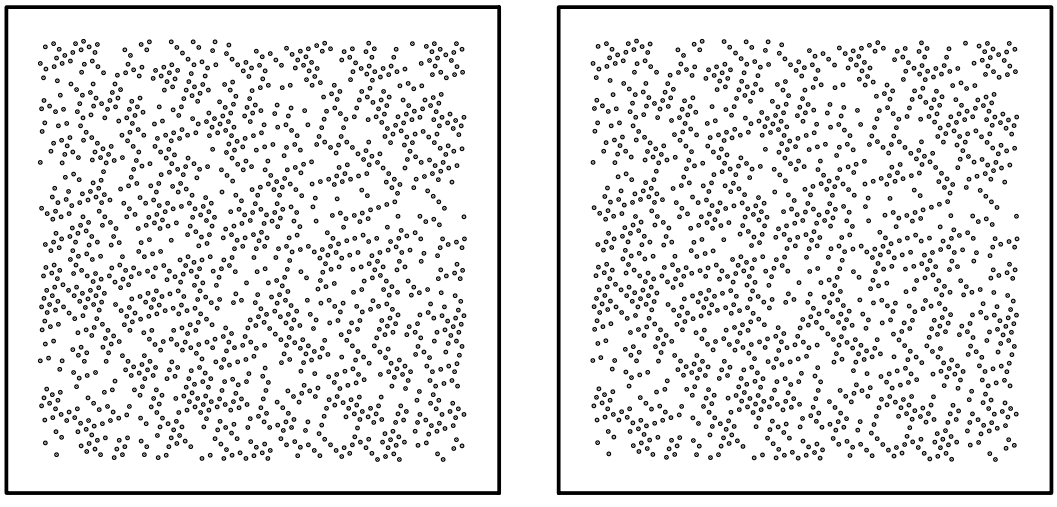

Fig. 13b: Modulus $d = 2867 = 47 \times 61$, $z = 678 \approx (20 \equiv 40^{-1}, 7) \bmod (47, 61)$.

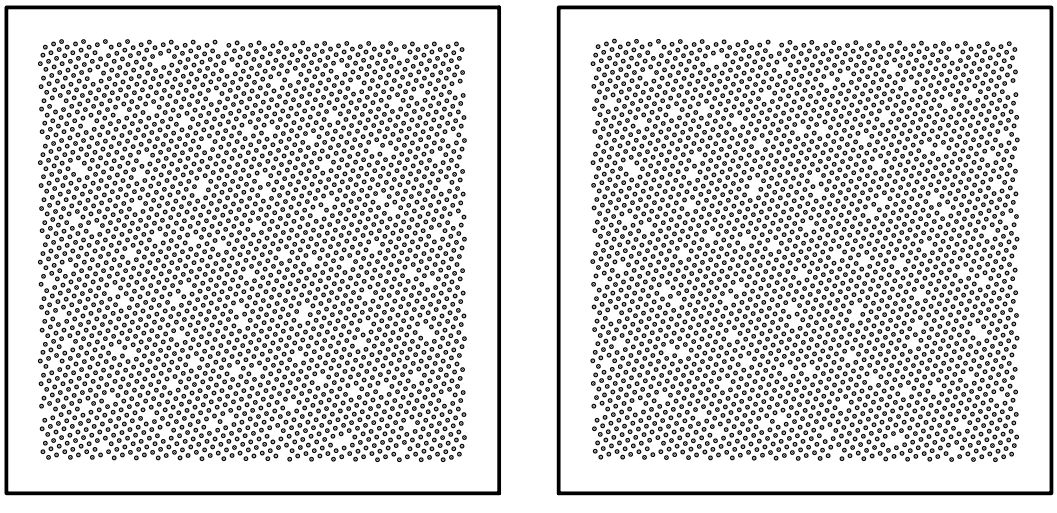

Fig. 13c: Modulus $d = 47 \times 61$, $z = 678 \approx (20, 7) \bmod (47, 61)$, initial values $(1, 1)$ and $(1, 7)$.

use of the whole of $<z>$ by the same reason.

It will be in order to note that Figures 11a,b and 13a,b have no symmetry with respect to the center of the square, while Figures 12a,b do have the symmetry. We now show that the use of two or more odd primes for the composite modulus furnishes us rooms to control this symmetry at our will.

Theorem 17 Let p_1, p_2 be distinct odd primes. Assume $q_1 := (p_1 - 1)/2$ and $q_2 := (p_2 - 1)/2$ are coprime, GCD$(q_1, q_2) = 1$. Take arbitrary primitive roots z_1, z_2 of primes p_1, p_2, respectively, and form $z \in Z_d^*$ $(d = p_1 p_2)$ by Chinese Remainder Theorem 4 as

$$z :\equiv z_1 U_1 + z_2 U_2 \bmod (d), \quad z \equiv z_1 \bmod (p_1), \quad z \equiv z_2 \bmod (p_2).$$

(I) If q_1, q_2 are both odd, the set S_l of points generated by l-tuples of numbers from the cyclic sequence $<z>$ or nS_l from its coset $n<z>$ are both symmetric about $\mathrm{M}_d = (d/2, d/2, \cdots, d/2)$ for all dimensions $l \geq 1$.
(II) If q_1, q_2 consist of even and odd coprime integers, both sets S_l and nS_l are asymmetrical with respect to M_d for any $l \geq 1$.

(Proof) By Theorem 15 we need only to see whether -1 is included in $<z>$ or not. In other words,

we inquire the existence of an integer $j \geq 1$ that gives $z^j \equiv -1 \bmod (d)$. Since z_1 is a primitive root modulo p_1, $(z_1)^j \equiv 1 \bmod (p_1)$ occurs for the first time at $j = p_1 - 1 = 2q_1$, and $(z_1)^j$ sweeps all of $Z^*_{p_1}$ including $-1 \equiv p_1 - 1 \bmod (p_1)$. These imply $(z_1)^{q_1} \equiv -1 \bmod (p_1)$. Likewise, there holds $(z_2)^{q_2} \equiv -1 \bmod (p_2)$. As regards z, its order (or the LCM period) in $Z^*_{p_1p_2}$ is $2q_1q_2$, as discussed before. Therefore, the sole possibility of $z^j \equiv -1 \bmod (d)$ arises with $j = q_1q_2$. Now we have

$$z^{q_1q_2} \approx ((z_1)^{q_1q_2}, (z_2)^{q_1q_2}) \equiv ((-1)^{q_2}, (-1)^{q_1}) \pmod{(p_1, p_2)}.$$

If q_1, q_2 are both odd, this gives $z^{q_1q_2} \approx ((-1)^{q_2}, (-1)^{q_1}) = (-1, -1)$. Therefore, Corollary 3 assures $z^{q_1q_2} \equiv -1 \bmod (p_1p_2)$, and S_l and nS_l are both symmetric with respect to M_d, proving (I). If q_1 and q_2 differ in their parity, the above congruence relation on the r.h.s. reduces to $\pm(1, -1)$. Thus Corollary 3 again works to prove $z \not\equiv -1 \bmod (p_1p_2)$,[37] and the conclusion (II) follows. ■

The statements may be generalized to the case with s odd primes.

Corollary 18 Let integer $s \geq 2$ be arbitrary, and take s odd primes $p_1, p_2, \cdots, p_s$ with mutually coprime $\{q_j := (p_j - 1)/2 \ (1 \leq j \leq s)\}$. Put $d := p_1p_2 \cdots p_s$ and choose a primitive root z_j modulo p_j for respective j $(1 \leq j \leq s)$. Define z by Chinese remainder theorem 4 as:

$$z :\equiv z_1U_1 + z_2U_2 + \cdots + z_sU_s \bmod (d), \quad z \approx (z_1, z_2, \cdots, z_s) \bmod (p_1, p_2, \cdots, p_s).$$

For any $l \geq 1$ denote S_l and nS_l for sets of points of l-tuples generated, respectively, from the cyclic sequence $<z>$ and from the coset sequence $n<z>$ in Z^*_d with an arbitrary $n \in Z^*_d$. The necessary and sufficient condition that the sets S_l and nS_l are asymmetrical about $\mathrm{M}_d := (d/2, d/2, \cdots, d/2)$ is that $q_1, q_2, \cdots, q_s$ consist of one even integer and all others that are odd.

(Proof) By the conditions given, z has the order t in the form of

$$t = \mathrm{LCM}(2q_1, 2q_2, \cdots, 2q_s) = 2q_1q_2 \cdots q_s.$$

Therefore, we need to examine, once and for all for $j = q_1q_2 \cdots q_s$, whether $z^j \equiv -1 \bmod (d)$ holds or not. Since $q_1, q_2, \cdots, q_s$ are mutually coprime, the dichotomy is that, none or the only one, of them is even, others being all odd. In the former case, it is now obvious that $z^{q_1q_2\cdots q_s} \equiv -1 \bmod (d)$ holds true, and S_l, nS_l are symmetric about M_d. As for the latter, let q_i be the sole even integer. There hold

$$z^{q_1q_2\cdots q_s} \equiv (z_j)^{q_1q_2\cdots q_s} \equiv (-1)^{q_i} = 1 \bmod (q_j), \quad j \neq i.$$

Thus, Corollary 3 stipulates $z^{q_1q_2\cdots q_s} \not\equiv -1 \bmod (d)$ and $-1 \notin <z>$, implying the asymmetry of S_l and nS_l with respect to M_d. ■

Conclusions of Theorem 17 will be readily confirmed on Figures 11a-13b.

7B. Modulus 2^i for the component of direct product groups

The subgroup $H_{1,5}$ of the reduced residue class group $Z^*_{2^i}$ $(i \geq 4)$ has been of frequent use as uniform and independent random numbers. Since its generator $z \equiv 5 \bmod (8)$ has the period 2^{i-2}, it can be used as a component of a direct product group only in combination with odd prime modulus groups in order to prevent further loss in the LCM period. Even with this restriction, however, the

[37] Since $Z^*_{p_1p_2}$ is not cyclic, the algebraic equation $z^2 - 1 \equiv 0 \bmod (p_1p_2)$ in $Z^*_{p_1p_2}$ can have more than two solutions besides ± 1. An example is seen in Z^*_8; the equation $z^2 \equiv 1 \bmod (8)$ has 4 solutions $z = 1, 3, 5, 7$. Also the case of twin primes $p_1, p_2 = a \pm 1$ has an extra answer $z \equiv a \pmod{p_1p_2}$. In this case of twin primes S_l is invariably asymmetric with respect to M_d. Yet the setting is not adequate for random number generators as we have seen.

situation does not improve for $H_{1,5}$. The complicated circumstances will be seen most feasibly again by figures. Below we show some two-dimensional plots of cases with $d = d_1 d_2 = p_1 \times 256$ together with a few odd prime $d_1 = p_1$, as examples for the relevant composite moduluses.

Figures 14a,b show the multiplier z isomorphic to $(z_1 = 12, z_2 = 37) \bmod (67, 256)$, both of z_1 and z_2 showing high performances in moduluses $d_1 = 67$ and $d_2 = 256$, respectively. The component multipliers in respective groups have orders 66 and $2^6 = 64$ which are situated, so to say, closest possible to each other. Chinese remainder theorem 4 gives

$$z \equiv 12U_1 + 37U_2 \equiv 7717 \bmod (67 \times 256 = 17152),$$

and the order or the period of $<z>$ is $(67 - 1) \times 2^6/2 = 2112$. Figure 14a plots 2-tuples from $<z>$ on the right, and the 2-tuples of the quotient sequence on the left, all as before. Figure 14b inverts z_1 to $28 \equiv 12^{-1} \bmod (67)$ with

$$z = 28U_1 + 37U_2 \equiv 1309 \bmod (17152),$$

as the multiplier in Z^*_{17152}. Since all these details will be calculable out from figure captions, we shall give only relevant expositions on respective figures hereafter.

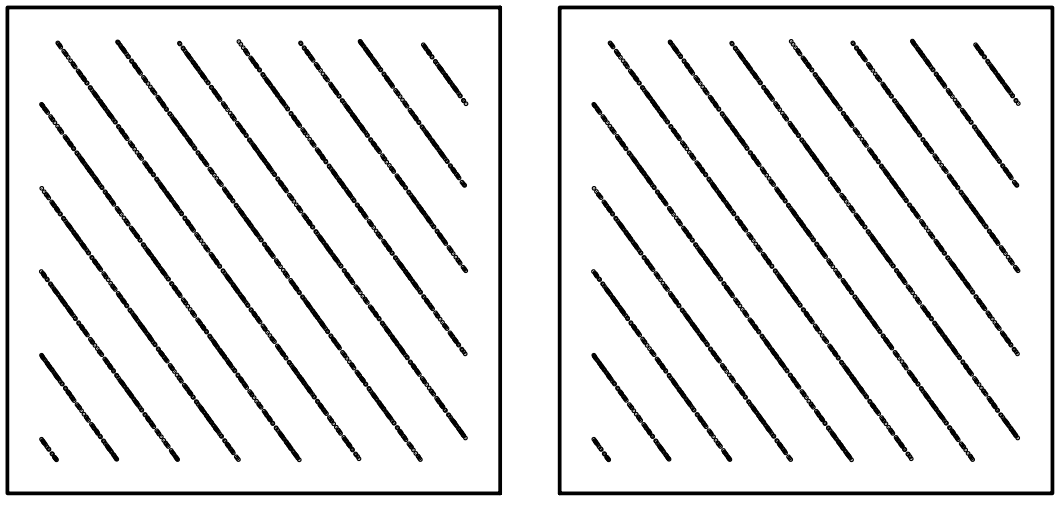

Fig.14a: modulus $d = 17152 = 67 \times 256$, $z = 7717 \equiv (12, 37) \bmod (67, 256)$.

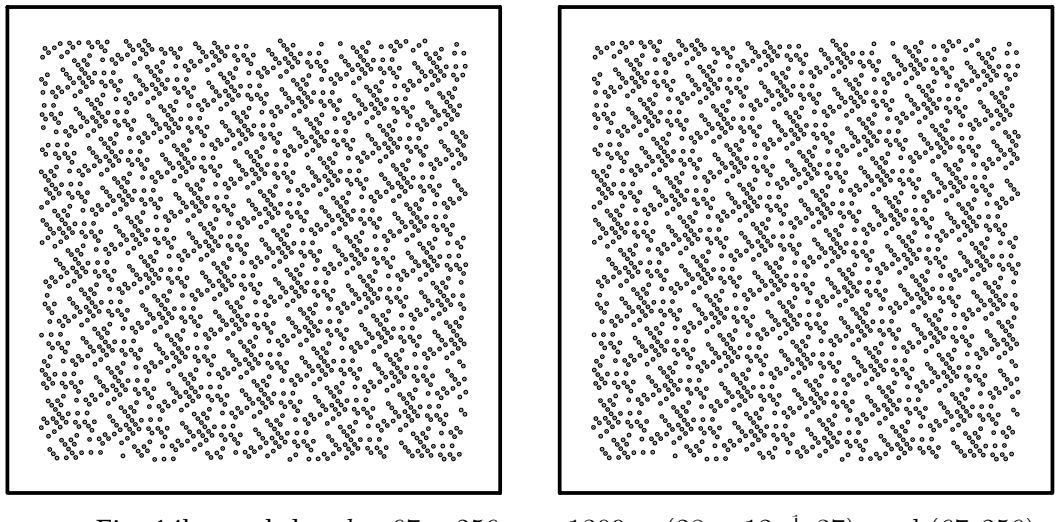

Fig. 14b: modulus $d = 67 \times 256$, $z = 1309 \equiv (28 \equiv 12^{-1}, 37) \bmod (67, 256)$.

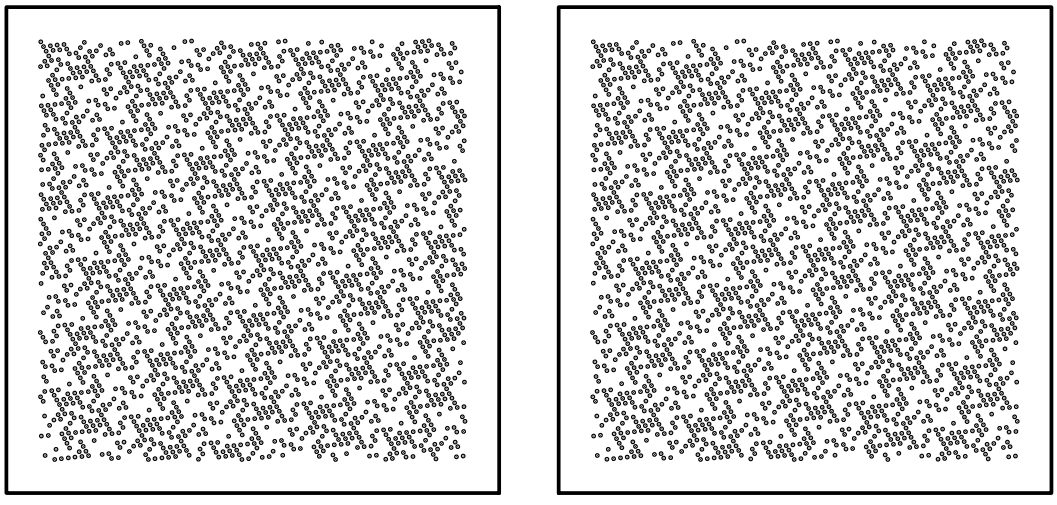

Fig. 15a: $d = 21248 = 83 \times 256$, $z = 6437 \equiv (46, 37) \bmod (83, 256)$.

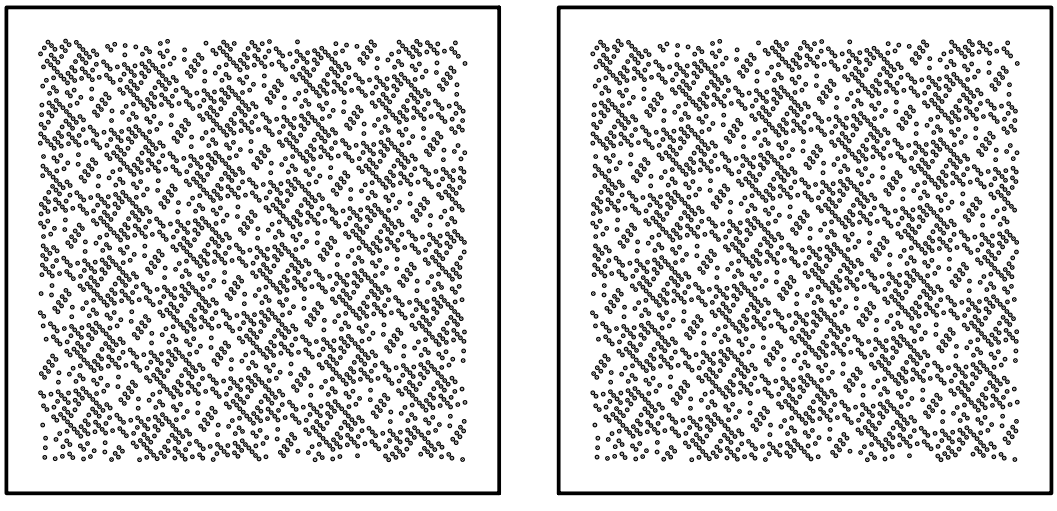

Fig. 15b: 法 $d = 83 \times 256$, $z = 7461 \equiv (74 \equiv 46^{-1}, 37) \bmod (83, 256)$.

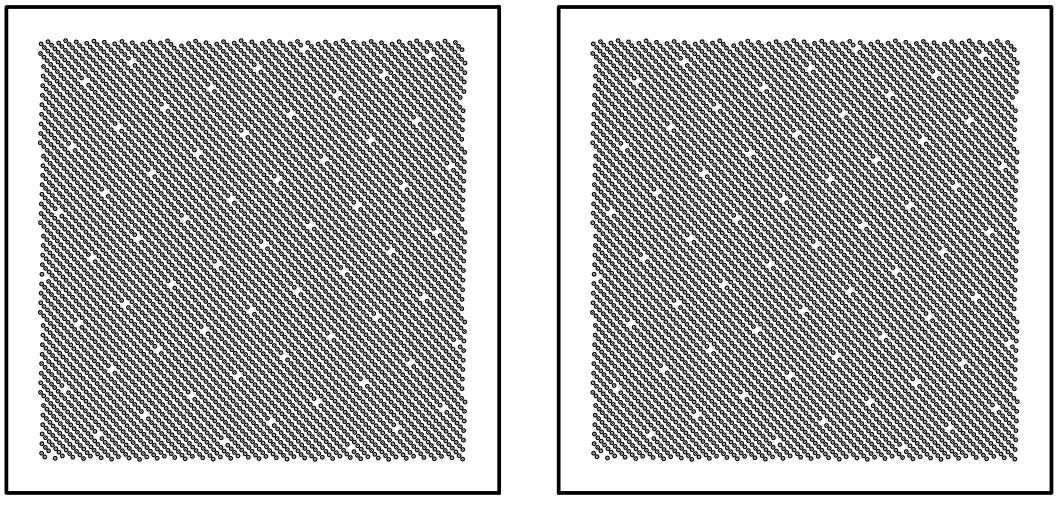

Fig. 15c: $d = 21248$, $z = 7461$, initial values $(1, 1), (46, 1) \bmod (83, 256)$.

The performance is poor in Fig. 14a, as expected by the closeness of component periods. We

should admit improvements in Fig. 14b, but conspicuous patterns are now surprising. It should be noted that, as we observe the development of the plot from the start, we recognize patterns only after a considerable portion, say $3/4$, of the period is used up. This is not that the initial, small portion of Fig. 14b may be used as random numbers; the patterns are always ruling the way of number generation, so that strong correlations are inherent in every portion of the sequence.

Figures 15a,b stand for more separated component periods, but improvements are unsatisfactory. Figure 15c shows Fig. 15b with added points taken from a coset $n<z>$; participating integers form a subgroup isomorphic to $Z_{83}^* \times H_{1,5}$, that occupies the half of $Z_{21248}^* \approx Z_{83}^* \times Z_{256}^*$. The patterns of Fig. 15b are erased out, and vacancies corresponding isomorphically to,

$$(83,1),(83,5),(83,9),(83,13),\cdots,(83,249),(83,253),$$

show up totaling to $(253-1)/4+1=64$ in number. Be that as it may, we can never use any portion of Figures 14a-15b as uniform and independent random number sequences, because correlations leading to Figures 15a,b in these sequences rule the generation at any stage of their periods.

In fact, the correlation originates from a flaw residing in any cyclic sequence in $H_{1,5} \subset Z_{2^i}^*$. The points will become clear by plotting the cyclic sequence in the isomorphic, direct product group. Figure 16 below shows the best combination for the modulus $d=47\times 256=12032$, as found by authors. The left shows the points $(z^j/d, z^{j+1}/d)$ formed by 2-tuples from the cyclic sequence $<z>$ which are pulled back to the unit square by the congruence modulo d. The multiplier is $z=349\approx (20,93) \bmod (47,256)$. The right plot gives points $(20^j/47, 93^j/256)$ from the direct product group, with the coordinates normalized by the congruence modulo $(47,256)$. The multiplier $93\equiv 5 \bmod (8)$ gives $93^j \equiv 5 \bmod (8)$ for odd j, while even j gives $1 \bmod (8)$. This regularity of the least significant 3 bits in multiplicative congruential generators modulo 2^i has long been known. The small flaw is magnified here, so to say, by the paired $z_1^j \equiv 20^j \bmod (47)$; integers z^j for odd j become correlated as they are forced to correspond to $5 \bmod (8)$, while those for even j are tied together to $1 \bmod (8)$; see the plot on the right.

For comparison, we show in Fig. 17 the case of two odd primes forming a composite modulus. This is another one of the best results in such composite moduluses. The reader is asked to consult figure captions for details. The differences in the product group plots on the right of Figures 16 and 17 will be impressive.

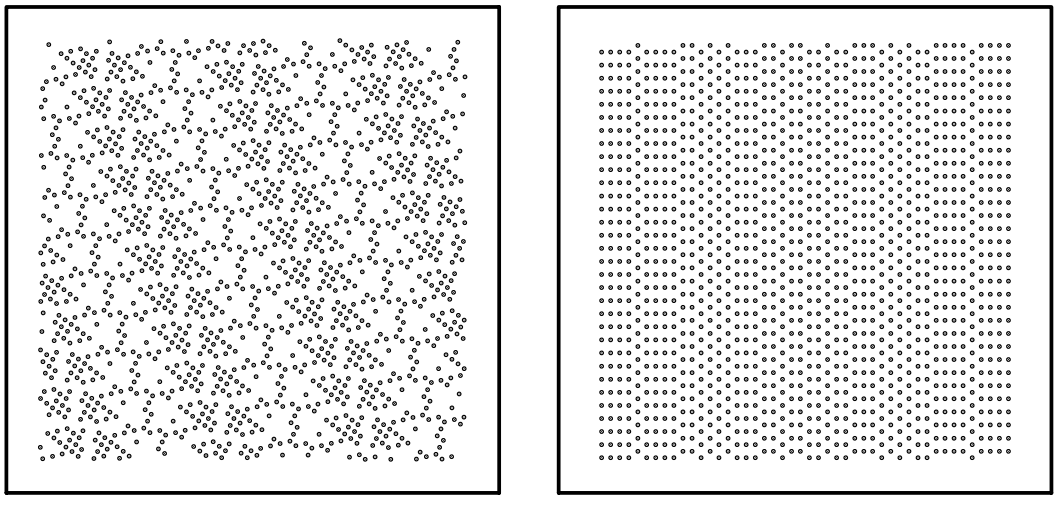

Fig. 16: Modulus $d=47\times 256=12032$, $z=349\approx (20,93) \bmod (47,256)$.

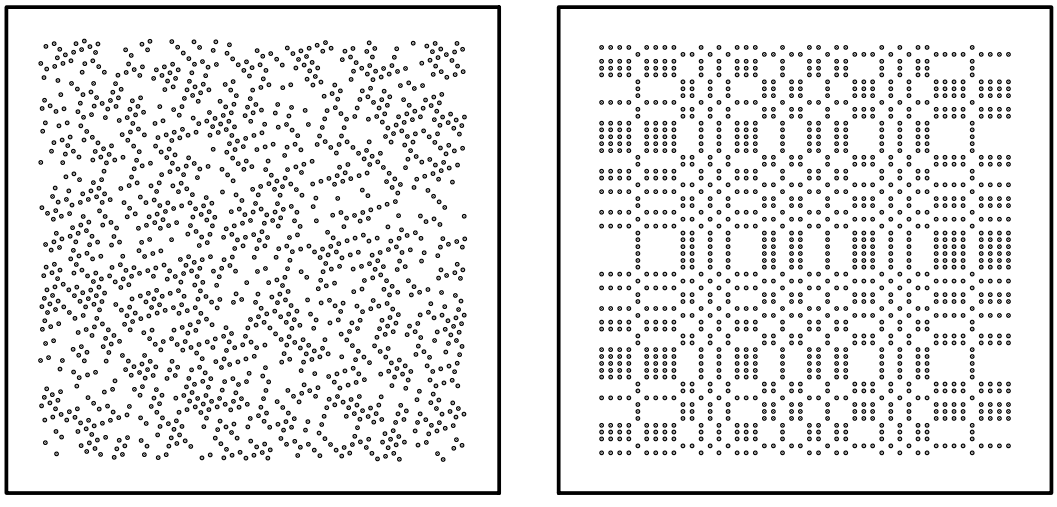

Fig 17: Modulus $d = 47 \times 61 = 2867$, $z = 678 \approx (20, 7) \bmod (47, 61)$.

The significant moral here is that powers of 2 should be excluded in composite moduluses. This stipulates also that moduluses such as 10^i should be avoided. At the same time we should note that spectral tests cannot detect the cases with pattern formation, as shown by Fig.15c. Thus, generic consideration on the configuration will be decisive in taking full advantage of the power of spectral tests on composite modulus groups. The choice of two odd primes for the modulus will be the best for our human skill, as well as from various points of view including problems of computability noted in the next section.

8. Complexity of spectral tests, conclusions and comments

Our endeavor might well be classified as belonging to pursuits of the possibility of shuffling in random number problems. Including similar composite modulus problems, there would have been many such efforts. Our luck among those was that, starting from simple arithmetic structures inherent in any integer sequences, we were lead to the ingenious mechanism of Chinese remainder theorem that conserves group structures of multiplicative congruential generators. The prospects obtained enable us now to restate prescriptions noted in Sec. 1 fully, but for the ambiguity about l left in (IV). They run as follows with due supplements.

(I) Choose two odd, distinct primes p_1, p_2, which should not be too close and should fulfill the condition that $q_1 = (p_1 - 1)/2,\ q_2 = (p_2 - 1)/2$ are coprime with different in parity.

(II) Choose sets of best of multipliers $\{z_1, z_1', \cdots\},\ \{z_2, z_2, \cdots\}$ for moduluses p_1, p_2, respectively, by exhaustive spectral tests of 6-th degree.

(III) Find the multiplier $z \approx (z_1, z_2) \bmod (p_1, p_2)$ with Chinese remainder theorem.

(IV) Perform the spectral test on z in $Z^*_{p_1 p_2}$ up to the *appropriate* degree l.

If the performance found in (IV) is not satisfactory in the closeness to the theoretical optimum, we need to try different choices of component multipliers and repeat the test. If the result is passable, we have the design of the uniform and independent random number generator with the period $T = 2q_1q_2$ and the precision of $\mathrm{O}(1/T)$.

Once the set of parameters d, z, n are given, there is no problem in the installation of the generator on computers and in letting it run fast in programs. However, the multiplier z should be prepared by computation, or should be tested within a reasonable time on computers. We have repeatedly

noted that procedures of exhaustive tests of (II) for primes $p_1, p_2 = \mathrm{O}(2^{32})$ were realized as early as 1986 by Fishman and Moore. The problem is to estimate the amount of computations needed in (IV), which will determine the degree l of possible spectral test for the multiplier $z \in Z^*_{p_1p_2}$. We leave the detailed algebra of estimates to Addendum at the end of this report.[38] Here we simply quote the result and discuss their implications.

If the spectral test is up to the 6-th degree and on the modulus d, the complexity $A(d)$, the amount of cases to be examined, is given as follows:

$$A(d) \simeq 2d^2 + 2^2d^3 + 2^3d^4 + 2^4d^5 + 2^5d^6.$$

In the particular case that odd primes p_1, p_2 have the magnitude $\mathrm{O}(p)$, this gives

$$A(d = p^2) \simeq 2p^4 + 2^2p^6 + 2^3p^8 + 2^4p^{10} + 2^5p^{12}.$$

If a single multiplier $z \in Z^*_{p_1p_2}$ is to be tested spectrally up to l-th degree, the term of p^{2l} in the above gives the relevant complexity.

As regards two sets of exhaustive spectral test for p_1 and p_2, respectively, the complexity may be estimated to the following $B(p)$. First, the number of primitive roots of a prime p is $\varphi(p-1) \le p/2$. Second, spectral test starts from the case of $l = 2$ and gradually proceeds to a larger l. Therefore, if the multiplier turn out to be not passable at l', then it does not survive in the next step $l' + 1$. Thus, the number of primitive roots to be examined diminishes as l increases. We might well assume that the rate of survival is a constant $0 < \kappa < 1$. We further assume that the exhaustive tests extend to $l = 6$-th degree always. These give the following:

$$\begin{aligned} B(p) &\simeq 2\{(p/2)\cdot(2p^2) + \kappa(p/2)\cdot(2^2p^3) + \kappa^2(p/2)\cdot(2^3p^4) + \kappa^3(p/2)\cdot(2^4p^5) + \kappa^4(p/2)\cdot(2^5p^6)\} \\ &= 2p^3 + 2^2\kappa p^4 + 2^3\kappa^2p^5 + 2^4\kappa^3p^6 + 2^5\kappa^4p^7. \end{aligned}$$

To have the rate κ, we quote again the result of Fishman and Moore who reported that $7.5 \times 10^{-5}\%$ of primitive roots passed the test to survive. If this is to have been realized by a constant κ, then we have $\kappa^4 \simeq 7.5 \times 10^{-7}$, implying $\kappa = 0.0294283\cdots$. Thus, the exhaustive spectral tests in two sets give the complexity

$$B(p) \simeq 2\kappa^4p^7 \quad (\kappa \simeq 0.029,\ p \ge 2^{20}).$$

As described in Sec. 1, if we choose $l = 6$ as the desirable degree for the test in (IV), and if it is computable at $d = p^2$, then

$$(\text{The term of } p^{12} \text{ in } A(d = p^2)) \simeq 2^5p^{12} \ge B(p) \simeq 2^5\kappa^4p^7 \quad (\kappa = 0.029,\ p \ge 2^{20})$$

should hold. It is certainly the case, and the exhaustive tests in two sets would always be possible.

If the choice of l in (IV) are $l = 4, 5$, the comparison of complexities of the 2nd stage spectral test and the exhaustive tests do not change the direction of the inequality noted above. Thus, choices $l = 4, 5, 6$ in (IV) imply that we should take first the modulus $d = p^2$ so that the second stage test is

[38] A brief conceptual descriptions will be in order. As partially noted, spectral tests form a class of problems that search the smallest positive length of vectors in a lattice determined by d, z. The greatest engineering problem has been to find the art to diminish the range of integers to be swept before starting the search; see pp. 96-115 of the penetrating textbook of D. E. Knuth in footnote[5]. Authors could not give neat estimates in taking the effect of reduction processes into account. Therefore, we describe in Addendum the bare amount of computation, the total number without reduction, of cases to be searched. This would certainly give a measure for the volume of the problem, though the value will not be realistic for the practical use.

possible, and then start the exhaustive tests for $p = \sqrt{d}$ which is assured to be computable. All is determined by the computer speed that rules the possible magnitude of p of the second stage spectral test, for choices of $l = 4, 5, 6$.

If we require $l = 3$ as the degree of spectral test in the second degree, the matter changes. The comparison of complexities of the second, single test and the first, exhaustive tests takes the form

$$\text{(The term of } p^6 \text{ in } A(p^2)) = 2^2 p^6 < 2^5 \kappa^4 p^7 = 2.40 \times 10^{-5} p^7 \quad (p \geq 2^{20}).$$

Therefore, the single spectral test for the modulus $d = p^2$ would always be computable. Recipes (I)-(IV) give now the generator with the period $T = p^2$ which is undergone third degree spectral tests, and the results stated in Sec. 1 are concluded.

Let us reflect on existing multiplicative congruential generators with the attained insights. If we would use a single, odd prime modulus p with a primitive root generator z, length of the sequence $<z>$ should be limited to $\mathrm{O}(p/2)$ to avoid the correlation induced by the symmetry of S_l which is the same as any coset nS_l. If we prefer the modulus $d = 2^i$ and the generator $z \equiv 5 \bmod (8)$, the lack of the symmetry around the center of the hypercube is gratifying. Yet, $<z>$ generates points that occupy all of their seats furnished by the lattice noted in Lemma at the end of Sec. 5. This completeness is suggestive that we had better not use the whole of $<z>$ in this case also, because the last half of the period is felt to be correlated to the first half in that points are destined to fill the vacancies left by the former. Far longer periods and the assurance of the performance with composite modulus generators will ease simulations in many respects.

Consider the direct product group consisting of $s \geq 3$ component groups. The composite modulus d should not contain powers of 2, by the same reason found in Sec. 7B. Thus, for the modulus d we assume s distinct odd primes $p_1, p_2, \cdots, p_s$ with mutually coprime

$$q_j := (p_j - 1)/2, \quad 1 \leq j \leq s.$$

We also take primitive roots $z_1, z_2, \cdots, z_s$ for respective primes, and use $z \approx (z_1, z_2, \cdots, z_s)$ as the multiplier. The order of Z_d^* $(d = p_1 p_2 \cdots p_s)$ is

$$\sharp Z_d^* = (p_1 - 1)(p_2 - 1) \cdots (p_s - 1) = 2^s q_1 q_2 \cdots q_s,$$

while the period T of $<z>$ is

$$T = \mathrm{LCM}(p_1 - 1, p_2 - 1. \cdots, p_s - 1) = 2 q_1 q_2 \cdots q_s = (\sharp Z_d^*)/2^{s-1}.$$

As s increases from 2, the cyclic sequence occupies smaller and smaller portion of the group Z_d^*. This might reduce the power of the spectral test that is measuring only seats for the whole group. Also, magnitude of $p_1, p_2, \cdots$ will need to be reduced so that the test on the composite modulus $d = p_1 p_2 \cdots$ should be computable. Thinking over these we feel at present that the choice of $s = 2$ will be the optimum.

We have left the case of moduluses of powers of odd primes. Though the modulus $d = p^i$ for an odd prime p does not relate $Z_{p^i}^*$ to a product group, it enjoys a large order $\sharp Z_{p^i}^* = \varphi(p^i) = p^i - p^{i-1}$. However, comparisons with the composite modulus group $Z_{p_1 p_2}^*$ remind us of the lack of freedom in choosing not only the combined modulus $d = p_1 p_2$, but also the geometry of S_l and nS_l.[39] Also,

[39]There is, of course, ways to realize $-1 \notin <z>$ artificially. Let z be a generator of $Z_{p^i}^*$. By $T = \sharp Z_{p^i}^* = p^{i-1}(p-1)$ we may choose $q := (p-1)/2$ to be odd, and take choose an arbitrary odd integer j that is coprime to p, q. Then $z' := z^{2j}$ has the order $T/2$ with $-1 \notin <z'>$. But the utility of such a choice is not clear.

generators of $Z^*_{p^i}$ is restricted to the primitive roots of Z^*_p but for the addition of some powers of p, which further restrains the design in choosing the generator. In view of the long period tenable with two-odd-prime moduluses, there will be little interest in the modulus $d = p^i$ cases.

We believe that insights obtained are large in amount. Yet, we do not know what an odd prime length T portion of a good, uniform and independent random sequence is doing, except for the puzzling fact that they are *not* using cyclic groups nor any generators of cyclic groups. The circumstance, however, may be regarded as suggesting that many interesting, unknown structures are waiting. Contributions from people in various engineering and scientific fields are waited for.

Addendum: Complexity of Spectral Tests for Multiplicative Congruential Method

As before we take vectors to be in column forms. We have seen in Sec. 5 that these position vectors (or points) are in a lattice spanned by bases or vectors of the basis:

$$\boldsymbol{f}_1 := \boldsymbol{e}_1' = \begin{pmatrix} 1 \\ z \\ z^2 \\ \cdot \\ \cdot \\ \cdot \\ z^{l-1} \end{pmatrix}, \quad \boldsymbol{f}_2 := \boldsymbol{e}_2^{(d)} = \begin{pmatrix} 0 \\ d \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{pmatrix}, \quad \boldsymbol{f}_3 := \boldsymbol{e}_3^{(d)} = \begin{pmatrix} 0 \\ 0 \\ d \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{pmatrix}, \quad \cdots, \quad \boldsymbol{f}_l := \boldsymbol{e}_l^{(d)} = \begin{pmatrix} 0 \\ 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ d \end{pmatrix}.$$

Linear independence of these vectors are obvious by inspection or by the determinant d^{l-1} they form. Correspondingly, basis vectors of the dual lattice are determined uniquely by the relation of their inner products with those of the original lattice:

$$(\boldsymbol{f}_j^*, \boldsymbol{f}_k) = d\delta_{jk}, \quad 1 \le j, k \le l. \tag{E1}$$

Their explicit forms are readily seen as follows:[40]

$$\boldsymbol{f}_1^* = \begin{pmatrix} d \\ 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{pmatrix}, \quad \boldsymbol{f}_2^* = \begin{pmatrix} -z \\ 1 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{pmatrix}, \quad \boldsymbol{f}_3^* = \begin{pmatrix} -z^2 \\ 0 \\ 1 \\ \cdot \\ \cdot \\ \cdot \\ 0 \end{pmatrix}, \quad \cdots, \quad \boldsymbol{f}_l^* = \begin{pmatrix} -z^{l-1} \\ 0 \\ 0 \\ \cdot \\ \cdot \\ \cdot \\ 1 \end{pmatrix}. \tag{E2}$$

Irrespective of whether a vector $\boldsymbol{a} = {}^{\tau}(a_1, a_2, \cdots, a_l)$ is in the lattice or in the dual, we define the length $\| \boldsymbol{a} \|$ by the Euclidean norm as

$$\| \boldsymbol{a} \| := \sqrt{{a_1}^2 + {a_2}^2 + \cdots + {a_l}^2}.$$

The lattice spanned by a linearly independent set $\{\boldsymbol{g}_1, \boldsymbol{g}_2, \cdots, \boldsymbol{g}_l\}$ of vectors in E_l was denoted by

$$(\!(\boldsymbol{g}_1, \boldsymbol{g}_2, \cdots, \boldsymbol{g}_l)\!) := \{c_1\boldsymbol{g}_1 + c_2\boldsymbol{g}_2 + \cdots + c_l\boldsymbol{g}_l | \ \ c_1, c_2 \cdots, c_l \in \boldsymbol{Z}\},$$

where $\boldsymbol{Z}$ denotes the set of intergers. Points in E_l are called lattice points if their position vectors are in the lattice. The spectral test relies on the following fact:

Lemma E1 Denote $\lambda_{\max}^{(l)}$ for the largest distance in E_l between parallel, neighboring hyperplanes, each of which contains at least $l-1$ lattice points of $G_l := (\!(\boldsymbol{f}_1, \boldsymbol{f}_2, \cdots, \boldsymbol{f}_l)\!)$. Let also denote $\mu_{\min}^{(l)}$ for the shortest, positive length of vectors in the dual lattice $G_l^* := (\!(\boldsymbol{f}_1^*, \boldsymbol{f}_2^*, \cdots, \boldsymbol{f}_l^*)\!)$. There holds the relation $\lambda_{\max}^{(l)} = d/\mu_{\min}^{(l)}$. **(End of Lemma A1)**

[40] In order to apply linear algebra efficiently, vectors in the dual lattice might better be defined as row vectors. For example, defining bases of the lattice as column vectors that form a square matrix $F := (\boldsymbol{f}_1, \boldsymbol{f}_2, \cdots, \boldsymbol{f}_l)$, and taking bases of the dual lattice as row vectors forming another square matrix F^* defined by ${}^tF^* := (\boldsymbol{f}_1^*, \boldsymbol{f}_2^*, \cdots, \boldsymbol{f}_l^*)$, we have for (E1) simple expressions

$$F^*F = dI \quad (I \text{ is the } l \times l \text{ unit matrix}), \quad F^* = dF^{-1}.$$

The clarity of this compact expression will be obvious in showing the structures associated with lattice bases and their duals. At this place we hasten, however, to the content of spectral tests, and will not use this convention only later, stressing our rule that bold face vectors represent column vectors.

This is well-known; we refer the reader to the penetrating textbook of Knuth.[41]

The spectral test of multiplicative congruential random numbers generated by z in Z_d^* looks for $\lambda_{\max}^{(l)}$ defined above, and Lemma E1 converts the problem to the search of shortest vectors in $G_l^* := (\!(\boldsymbol{f}_1^*, \boldsymbol{f}_2^*, \cdots, \boldsymbol{f}_l^*)\!)$ formed by (E2). Despite the frightening name of the shortest vector problem, the test presents a very mild type of the problem that admits polynomial complexity, thanks to the simplifying structure of (E2). We recapitulate that a vector $\boldsymbol{v}$ in G_l^* are defined by

$$\boldsymbol{v} = c_1^* \boldsymbol{f}_1^* + c_2^* \boldsymbol{f}_2^* + \cdots + c_l^* \boldsymbol{f}_l^*$$

with integer coefficients $(c_1^*, c_2^*, \cdots, c_l^*)$, and conversely, any integer set $c_1, c_2, \cdots, c_l$ gives a dual lattice vector $\boldsymbol{v}$ by this form. As a vector in E_l, $\boldsymbol{v} \in G_l^*$ also has the representation

$$\boldsymbol{v} = {}^t(\xi_1^*, \xi_2^*, \cdots, \xi_l^*),$$

in cartesian coordinates. A set of integer cartesian coordinates $(\xi_1^*, \xi_2^*, \cdots, \xi_l^*)$ cannot always give a vector in G_l^*. However, a simple criterion exists discerning cases.

Lemma E2 A necessary and sufficient condition for a vector $\boldsymbol{v}$ in E_l with integer cartesian coordinates $\boldsymbol{v} = {}^t(\xi_1^*, \xi_2^*, \cdots, \xi_l^*)$ to be in the dual lattice $G_l^* = (\!(\boldsymbol{f}_1^*, \boldsymbol{f}_2^*, \cdots, \boldsymbol{f}_l^*)\!)$ is given by the following:

$$\xi_1^* + z\xi_2^* + z^2\xi_3^* + \cdots + z^{l-1}\xi_l^* \equiv 0 \bmod (d). \tag{E3}$$

(Proof) A necessary and sufficient condition for $\boldsymbol{v}$ to be in the dual lattice is the existence of a set of integers $\{c_1, c_2, \cdots, c_l\}$ giving

$$\begin{aligned} \boldsymbol{v} &= c_1^* \boldsymbol{f}_1^* + c_2^* \boldsymbol{f}_2^* + c_3^* \boldsymbol{f}_3^* + \cdots + c_l^* \boldsymbol{f}_l^* \\ &= {}^t(c_1^* d - z c_2^* - z^2 c_3^* - \cdots - z^{l-1} c_l^*, c_2^*, c_3^*, \cdots, c_l^*). \end{aligned}$$

This relation may be rewritten for respective integer coordinates of $\boldsymbol{v}$ as

$$\xi_2^* = c_2^*, \quad \xi_3^* = c_3^*, \quad \cdots, \quad \xi_l^* = c_l^*; \qquad \xi_1^* = c_1^* d - z\xi_2^* - z^2\xi_3^* - \cdots - z^{l-1}\xi_l^*.$$

They are manifestly equivalent to the following to hold true,

$$\xi_1^* + z\xi_2^* + z^2\xi_3^* + \cdots + z^{l-1}\xi_l^* = c_1^* d,$$

which is the same as (E3). ■

The conclusion solves the problem with spectral tests. Given a modulus d (which may be a composite integer) and an element $z \in Z_d^*$, we need to find the set $\{\xi_1^*, \xi_2^*, \cdots, \xi_l^*\}$ of cartesian coordinates satisfying (E3) that give the smallest positive value $\mu_{\min}^{(l)}$ to

$$\sqrt{(\xi_1^*)^2 + (\xi_2^*)^2 + \cdots + (\xi_l^*)^2} = \| \boldsymbol{v} \| .$$

The larger the value of $\mu_{\min}^{(l)}$, the better is the multiplier z. Since the set (E2) is given as dual basis vectors, upper bounds of the length of $\boldsymbol{v}$ are known to start with. We need only to pick out cartesian coordinates within this bound that satisfy (3), compute $\| \boldsymbol{v} \|$ as above, and compare results to find the smallest. The problem is a search in a finite range. Though d and z in practice might horrify us with their magnitude of $O(2^{32})$ or larger, structures of (E2) give us further simplifications.

[41] D. E. Knuth, in footnote[5], Sec. 3.3.4.

We notice that forms of dual basis vectors in (E2) imply that bases for the dimension $l+1$ contains those for the dimension l by obvious identifications. Therefore, $\mu_{\min}^{(l)}$ is not increasing as l increases, and $\mu_{\min}^{(l)}$ provides an upper bound for $\mu_{\min}^{(l+1)}$. The spectral test should thus be started with the case $l=2$ and carried out by increasing l step by step. This fact enables us to consider the upper bound for the overall amount of computation (or complexity) in a very simple way.

Lemma E3 Let a modulus d and a multiplier $z \in Z_d^*$ be given. The complexity of the spectral test, the number of cases to be examined, for a single multiplier z up to the 6-th degree is given by

$$A(d) \simeq 2d^2 + 2^2\rho^3 d^3 + 2^3\rho^8 d^4 + 2^4\rho^{15} d^5 + 2^5\rho^{24} d^6. \qquad \text{(E4)}$$

Here $0<\rho<1$is the assumed constant rate of that gives $\mu_{\min}^{(l)} = \rho\mu_{\min}^{l-1)}$ $(2 \le l \le 6)$ with $\mu_{\min}^{(1)} := d$.

(Proof) In the case $l=2$, cartesian coordinates ξ_1^*, ξ_2^* of integers exhaust possibilities in the range $(-d, d)$. Hence the complexity, the total number of cases to be examined, is $\{2(d-1)+1\}^2$. Sicne $\pm\boldsymbol{v}$ give the same length $\| \boldsymbol{v} \|$ and do or do not fulfill (E3) simultaneously, we need to take only one of them to estimate the complexity as $2d^2$ for d large. In the case $l=3$, we need to consider integers ξ_j^* $(j=1,2,3)$ respectively in the range $-\mu_{\min}^{(2)} \le \xi_j^* \le \mu_{\min}^{(2)}$. By assumption $\mu_{\min}^{(2)} = \rho\mu_{\min}^{(1)} = \rho d$ hold the total number of cases to be searched is $(2\rho d)^3/2 = 2^2\rho^3 d^3$. Proceeding similarly, we have for $l=4$ the estimate $(2\rho^2 d)^4/2 = 2^3\rho^8 d^4$, and so forth, and we have (E4). The construction reveals that the single spectral test up to the l-th degree is given by the term of d^l in (E4). ■

A natural idea to estimate the constant ρ is to consider ideal cases. In Sec. 6 for cases of $l=2$ we took the triangle and derived the distance of opposite sides $\sqrt[4]{3}/\sqrt{2}$ of rhombus as ideal. The idea may be brought to higher dimension l by considering regular tetrahedron and so forth. A slightly different but more feasible way will be to think of diameters of spheres of volume 1 in l-dimensional spaces. They are given by

$$(l=2)\quad \pi r^2 \qquad (l=3)\quad 4\pi r^3/3 \qquad (l=4)\quad \pi^2 r^4$$
$$(l=5)\quad 8\pi^2 r^5/15 \qquad (l=6)\quad \pi^3 r^6/6.$$

Thus the diameter a_l of the sphere in the l-dimensional space E_l with volume 1 gives their inverses

$$1/a_2 = 0.88623, \qquad 1/a_3 = 0.80600, \qquad 1/a_4 = 0.74523,$$
$$1/a_5 = 0.69700, \qquad 1/a_6 = 0.65744,$$

together with their ratios

$$a_3/a_2 = 0.90947, \quad a_4/a_3 = 0.92460, \quad a_5/a_4 = 0.93528, \quad a_6/a_5 = 0.94324.$$

These may be averaged to give $\rho \simeq 0.92815$. However, this gives $\rho^{24} = 0.167\cdots$, and (E4) is little affected by putting all of this ρ as 1. Thus we used in Sec. 8 a simplification of (E4),

$$A(d) \simeq 2d^2 + 2^2 d^3 + 2^3 d^4 + 2^4 d^5 + 2^5 d^6. \qquad \text{(E5)}$$