Acta Crystallographica Section A
Foundations of Crystallography
ISSN 0108-7673

Received 23 May 2009
Accepted 14 September 2009

Multiplicative congruential generators, their lattice structure, its relation to lattice–sublattice transformations and applications in crystallography

Wolfgang Hornfeck* and Bernd Harbrecht

Department of Chemistry and Center for Material Sciences, Philipps-University Marburg, Hans-Meerwein-Strasse, D-35032 Marburg, Germany. Correspondence e-mail: wolfgang.hornfeck@web.de

An analysis of certain types of multiplicative congruential generators – otherwise known for their application to the sequential generation of pseudo-random numbers – reveals their relation to the coordinate description of lattice points in two-dimensional primitive sublattices. Taking the index of the lattice–sublattice transformation as the modulus of the multiplicative congruential generator, there are special choices for its multiplier which induce a symmetry-preserving permutation of lattice-point coordinates. From an analysis of similar sublattices with hexagonal and square symmetry it is conjectured that the cycle structure of the permutation has its crystallographic counterpart in the description of crystallographic orbits. Some applications of multiplicative congruential generators in structural chemistry and biology are discussed.

1. Lattice–sublattice transformations

Given a two-dimensional lattice Λ of unit size, which shall be either the hexagonal (alias triangular) lattice A_2 or the square lattice $\mathbb{Z}^2$ (Conway & Sloane, 1999), we restrict our discussion to primitive sublattices $\Lambda' \subseteq \Lambda$ similar to their respective basic lattice Λ.

A sublattice $\Lambda' \subseteq \Lambda$ is called primitive if no integer $n \in \mathbb{N}$ with $n > 1$ exists, for which $(1/n)\mathbf{x} \in \Lambda$ holds true for all $\mathbf{x} \in \mathbf{\Lambda}'$, where $\mathbf{x}$ is a generic lattice vector of the sublattice. A sublattice $\Lambda' \subseteq \Lambda$ is called similar if the transformation from the lattice Λ to a sublattice Λ' with enlarged unit cell satisfies $\Lambda' = \sigma(\Lambda)$, where σ is called a similarity transformation (Conway *et al.*, 1999), such that all angles are preserved while all distances are changed in the same ratio. Requiring the sublattices to be similar and primitive enforces them to be scaled *and* rotated copies of themselves (*cf.* Fig. 1).

A more general approach to sublattices of the hexagonal lattice is given by Bernstein *et al.* (1997) and a great deal of crystallographic research concerning sublattices in general is due to Rutherford (1992, 1993, 1995, 2006, 2009). Lattices of arbitrary dimension and different symmetry are treated by Conway & Sloane (1999).

For a lattice Λ with basis $(\mathbf{a}, \mathbf{b})$ the transformation to the basis $(\mathbf{a}', \mathbf{b}')$ of the sublattice Λ' is described by the matrix equation

$$(\mathbf{a}', \mathbf{b}') = (\mathbf{a}, \mathbf{b})\boldsymbol{M}, \tag{1}$$

where $\boldsymbol{M}$ is a 2×2 transformation matrix (transformed quantities are labeled by a prime). The coordinates transform according to

$$(x', y')^{\mathrm{t}} = \boldsymbol{M}^{-1}(x, y)^{\mathrm{t}}, \tag{2}$$

where $\boldsymbol{M}^{-1}$ is the matrix inverse of $\boldsymbol{M}$ and t stands for transposition. For a hexagonal lattice–sublattice pair $\boldsymbol{M}$ corresponds to the generator matrix

$$\boldsymbol{T} = \begin{pmatrix} q & -r \\ r & q-r \end{pmatrix}, \text{ while } \boldsymbol{Q} = \begin{pmatrix} q & -s \\ s & q \end{pmatrix} \tag{3}$$

is the analogous matrix for a square lattice–sublattice pair (Müller & Brelle, 1995). Here, the matrices $\boldsymbol{T}$ and $\boldsymbol{Q}$ conform to the conventional choice of the basis, as preferred in crystallography, which may be transformed to any other basis by the action of an integer matrix $\boldsymbol{N}$ with determinant $|\boldsymbol{N}| = 1$. This has to be accounted for in the general case, where the lattice and the sublattice each may be defined by a nonconventional choice of their basis. The given generator matrix $\boldsymbol{M} = \{m_{ij}\}$ allows for another definition of a primitive sublattice – a lattice is primitive if the greatest common divisor (gcd) of the matrix entries is unity, $\gcd(m_{ij}) = 1$. The matrix inverses are given by

$$\boldsymbol{T}^{-1} = \frac{1}{T}\begin{pmatrix} q-r & r \\ -r & q \end{pmatrix} \text{ and } \boldsymbol{Q}^{-1} = \frac{1}{Q}\begin{pmatrix} q & s \\ -s & q \end{pmatrix}, \tag{4}$$

where T and Q are equal to the overall enlargement factor of the unit-cell transformation given by the index $M = [\Lambda : \Lambda']$ of the lattice–sublattice transformation. The index gives the number of lattice points within a unit mesh of the sublattice and equals its relative volume, which is calculated by evaluating the determinant $|\boldsymbol{M}| = M$. For a hexagonal sublattice $|\boldsymbol{T}|$ is given by the quadratic form $T(q, r) = q^2 - qr + r^2$, whereas $|\boldsymbol{Q}| = Q(q, s) = q^2 + s^2$ is the corresponding relation for a

square sublattice. Moreover, the values obtained for T or Q correspond to the number-theoretic norms $N(z)$ of the respective sublattices, which equal the squared distances between two lattice points (Conway & Sloane, 1999).

The possible values for T and Q form the sequences

$$\mathcal{T} = 0, 1, 3, 4, 7, 9, 12, 13, 16, 19, 21, 25, 27, 28, 31, 36, 37, \ldots$$

and

$$\mathcal{Q} = 0, 1, 2, 4, 5, 8, 9, 10, 13, 16, 17, 18, 20, 25, 26, 29, 32, \ldots$$

solely determined by the geometry of the basic lattice (Fig. 1; Sloane, 2008: sequences A003136 and A001481). The question whether a given number N is an element of the set $\mathcal{T}$ (or $\mathcal{Q}$) may be judged from its prime factorization [Hardy & Wright (2008); see also Ball (1971) and Conway *et al.* (1999)]: $N \in \mathcal{T}$ ($N \in \mathcal{Q}$) if primes p of the form $p \equiv 2 \pmod 3$ [$p \equiv 3 \pmod 4$] appear to even powers only.

2. Multiplicative congruential generators

A linear congruential generator (LCG) is defined by the recurrence relation

$$Z_{n+1} \equiv mZ_n + a \pmod M, \tag{5}$$

where m and a are multiplicative and additive constants and M is the modulus ($m, a, M \in \mathbb{Z}$). The Z_i are integer variables with Z_0 the starting value (seed) of the LCG. The special case where $a = 0$ is known as a multiplicative congruential generator (MCG; Downham & Roberts, 1967). MCGs are among the most used algorithms for the generation of pseudo-random number sequences and the first to introduce MCGs for this purpose was Lehmer in 1949 [see Knuth (1998) for a survey]. Given a reasonable choice of parameters, MCGs enable a simple, portable and efficient way of computing any required amount of pseudo-random numbers. In order to obtain pseudo-random numbers lying in the interval [0, 1) one introduces a normalization by dividing each number with the modulus: $z_i = Z_i/M$. It was only in 1968 that Marsaglia found an inherent defect of MCGs, namely that tuples of n successive numbers generated by an MCG and plotted in a Euclidean space of n dimensions, *e.g.* inside a unit hypercube [*i.e.* an n-dimensional measure polytope; see Coxeter (1973), p. 123], fall into at most $(n!\,M)^{1/n}$ parallel and equidistant $(n-1)$-dimensional hyperplanes (Marsaglia, 1968, 1970). Essentially, the lattice structure of an MCG guarantees a uniform distribution of pseudo-random numbers, although their randomness, which may be evaluated and expressed by different statistical methods and measures, depends crucially on the choice of the parameters. One way to decide on which choice of parameters is to be preferred in order to get a reasonably good MCG is to analyze the exact nature of the lattice structure of the MCG by means of determining the magnitude of the orthogonal interplanar distance between neighboring hyperplanes *via* the spectral test algorithm. The action of an MCG on a given set of numbers is illustrated in Fig. 2.

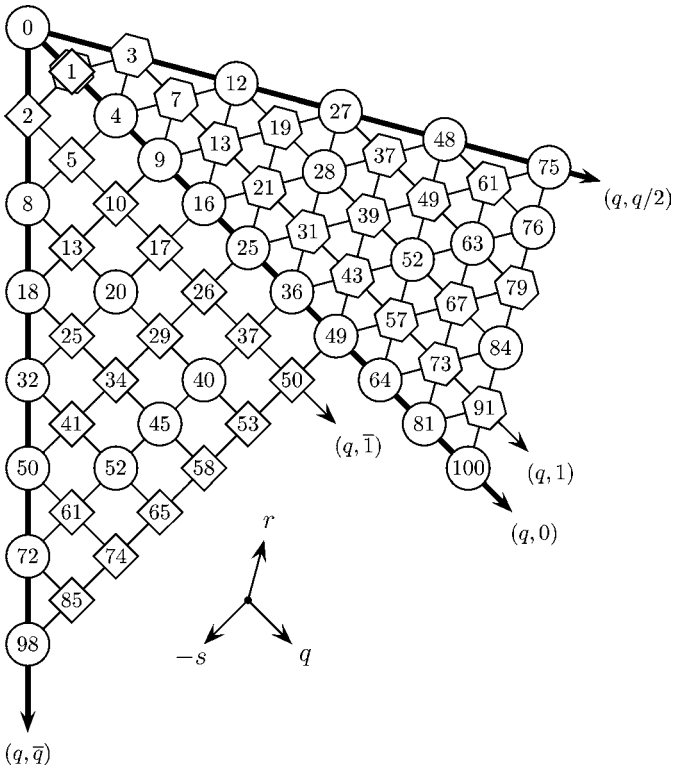

Figure 1
Possible indices ≤ 100 for similar hexagonal and square sublattices. For ease of depiction both types of sublattices share a common direction q, thus showing the $-s$ axis instead of the s axis for the square sublattices. Primitive sublattices, for which $\gcd(q, r) = \gcd(q, s) = 1$, are framed by polygons, nonprimitive ones by circles.

3. The use of MCGs in crystallography

To our knowledge, a first use of a modular algebra for the description of crystal structures, similar in its intention to our approach but differing in its details, traces back to the work of Loeb (1958, 1962, 1964; Morris & Loeb, 1960), which appears to be singular, however, and does not mention the concept of an MCG explicitly.

While MCGs and their lattice structure are extensively studied in discrete mathematics (*e.g.* Beyer *et al.*, 1971; Ripley, 1983; Afflerbach, 1986; L'Ecuyer, 1999), their relation to crystallography seems to be nearly unexplored.

An explanation for this and the rationale behind the suggested use of MCGs in crystallography is given by the fundamental differences in the points of view of a mathematician and a crystallographer regarding the lattice structure of MCGs:

(1) Regarding pseudo-random number generation, any repetition of the number sequence is considered prohibitive. Since each LCG inheres a fundamental periodicity, with the modulus acting as an upper bound, any MCG feasible for practical applications in pseudo-random number generation is in need of a high modulus, irrespective of the maximal period achievable, which depends on *both* the modulus and the multiplier. For instance, an MCG with modulus $M = 2^{31} - 1 = 2\,147\,483\,647$ (Mersenne prime M_{31}), a multiplier $m = 7^5 = 16\,807$ (a primitive root modulo M_{31}) and the

initial seed relatively prime to M_{31} was proposed by Park & Miller (1988) as a minimal standard MCG, representing a reasonably good method for pseudo-random number generation in terms of the statistical quality of the resulting sequences. Nevertheless, it is clear that $2^{31}-1$ is far too high to act as a physically reasonable index for a crystallographic lattice–sublattice transformation, although the sublattice index T, regarding the triangular surface lattice of the largest known virus, Mimivirus, is of the order 10^3 (Xiao *et al.*, 2009)!

(2) In a mathematical sense the lattice structure of MCGs proves to be of an ambivalent nature: given a good choice of parameters (m, M) the lattice structure of an MCG warrants a uniform distribution of the generated numbers, a necessary condition for achieving the desired degree of randomness. On the contrary, the lattice structure of an MCG is *not at all* a good instance for a truly random structure, leading to serious problems, especially if the parameters are poorly chosen (as was the case for the MCG known as RANDU; Knuth, 1998). From the viewpoint of a crystallographer, however, the lattice structure of an MCG is highly welcome and seems to be interesting in its own right.

(3) Finally, the recursive definition of an MCG gives rise to serial correlations between successive elements in the sequence of pseudo-random numbers, thus prohibiting the use of MCGs for certain applications, *e.g.* cryptographic purposes or special types of Monte Carlo simulations. From the viewpoint of a crystallographer, the serial correlations are inevitably linked to the symmetry of the underlying lattice, as will be exemplified in the following. Therefore the serial correlations will not be regarded as some kind of defect of an MCG, but as an essential feature, *i.e.* a certain type of structural invariant.

4. The lattice structure of MCGs

To illustrate the lattice structure of an MCG we chose the MCG with modulus $M = 21$ and the (special) multiplier $\mu = 17$.

The action of the MCG on each integer Z_n from the interval $[0, 21)$ is shown in equation (6). The Z_n are listed in the upper row and in ascending order, whereas the lower row contains the resulting integers Z_{n+1}:

$$\begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 & 14 & 15 & 16 & 17 & 18 & 19 & 20 \\ 0 & 17 & 13 & 9 & 5 & 1 & 18 & 14 & 10 & 6 & 2 & 19 & 15 & 11 & 7 & 3 & 20 & 16 & 12 & 8 & 4 \end{pmatrix}. \tag{6}$$

An inspection of this result shows that the action of an MCG is described as a mapping of a set of integers onto itself while maintaining a one-to-one correspondence between them. In the present case the set under consideration is given by $\mathbb{Z}/21\mathbb{Z} = \{Z_n \mid Z_n \in \mathbb{Z}, 0 \le Z_n < 21\}$, the residue class ring modulo 21. A bijective mapping of a set onto itself is a permutation and equation (6) is one notation for it. A more concise notation is given by the cycle representation

$$(0)(1\ 17\ 16\ 20\ 4\ 5)(2\ 13\ 11\ 19\ 8\ 10)(3\ 9\ 6\ 18\ 12\ 15)(7\ 14), \tag{7}$$

which shows the decomposition of a permutation into a product of disjoint cycles. A single cycle $(Z_1\ Z_2\ \ldots\ Z_{n+1}\ \ldots\ Z_{\ell-1}\ Z_\ell)$ is characterized by the number of its elements Z_i and its cycle length ℓ, and is itself a permutation. A cycle of length $\ell = 1$, *e.g.* (0) in equation (7), is a fixed point of the permutation and is usually skipped in its cycle representation, although listed throughout this work for reasons of completeness. Cycles of length $\ell = 2$, exchanging two elements, *e.g.* (7 14) in equation (7), are called transpositions. Calculating the $(n + 1)$th element of a cycle from the first one is carried out by using

$$Z_{n+1} \equiv \mu^n Z_1 \,(\mathrm{mod}\, M) \tag{8}$$

or

$$Z_{n+m} \equiv \mu^n Z_m \,(\mathrm{mod}\, M) \tag{9}$$

in the general case. Thus the cycle with the seed $Z_1 = 1$ is given by the multiplier μ raised to its powers, *i.e.* $(\mu^0\ \mu^1\ \ldots\ \mu^{\ell-1}) \,(\mathrm{mod}\, M)$.

In order to show the lattice structure of this MCG in two dimensions, the sequence of numbers in each cycle, represented by equation (7), is transformed into a set of 21 coordinate pairs (X_i, Y_i),

$$\begin{aligned} &(0, 0) \\ &(1, 17),\ (17, 16),\ (16, 20),\ (20, 4),\ (4, 5),\ (5, 1) \\ &(2, 13),\ (13, 11),\ (11, 19),\ (19, 8),\ (8, 10),\ (10, 2) \\ &(3, 9),\ (9, 6),\ (6, 18),\ (18, 12),\ (12, 15),\ (15, 3) \\ &(7, 14),\ (14, 7) \end{aligned} \tag{10}$$

with successive numbers in the sequence forming overlapping pairs. Crystallographic coordinates are obtained after the normalization $(x_i, y_i) = (X_i/M, Y_i/M)$ with $M = 21$. Now, the normalized coordinate set of equation (10), plotted in the reference frame of a hexagonal unit cell, clearly reveals the

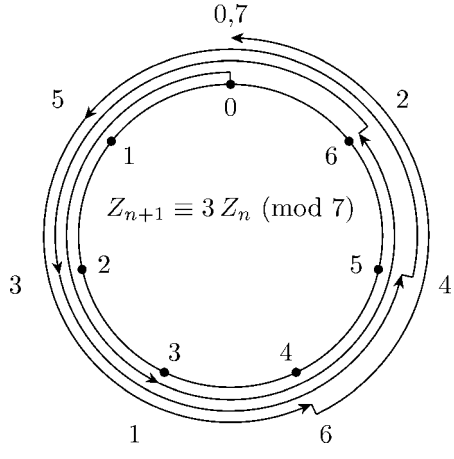

Figure 2
Action of the MCG with $M = 7$, $m = 3$ on the set $\mathbb{Z}/7\mathbb{Z} = \{0, \ldots, 6\}$, illustrating the cyclic nature – modular arithmetics is colloquially known as clock arithmetic – of the permutation (0)(1 3 2 6 4 5) resulting in the coordinates $(X_i, Y_i) = (0, 0), (1, 3), (2, 6), (3, 2), (4, 5), (5, 1), (6, 4)$. For a general introduction into permutations, modular arithmetics and other number-theoretic topics see Ash & Gross (2006).

hexagonal lattice structure of the MCG under consideration (Fig. 3); each cycle represents a set of lattice points equivalent by the symmetry of the lattice (plane group $p6$).

It should be pointed out again that a lattice structure is an intrinsic feature of any MCG, whatever the choice of multiplier m and modulus M (and reference frame) would be for a particular one. Lattice structures in accordance with hexagonal (or square) symmetry, however, are restricted to MCGs with a special choice of multiplier μ and modulus T (or Q) and their representation within an appropriate (*i.e.* symmetry-adapted) coordinate system.

Several questions about the nature of the MCG and its corresponding lattice structure immediately arise:

(1) Is there a relation between the values chosen for the modulus and the multiplier of an MCG and its lattice structure?

(2) What information, if any, can be retrieved from the knowledge of the cycle structure of an MCG-induced permutation in terms of lattice–sublattice transformations?

(3) If there is a one-to-one correspondence between an MCG's lattice structure and the crystallographic description thereof, what are the reasons for it?

(4) Are there generalizations?

In the following sections we will address each question, proposing answers for them.

5. Construction of an MCG for sublattices of given index

To explain the interrelation of the values chosen for the MCG and its lattice structure we refer to Fig. 3, essentially reversing the problem, *i.e.* we will show how to construct a certain MCG from a given lattice–sublattice pair. The first observation to make is that the coordinates of any lattice point are given as multiples of $1/M$, where M is the sublattice index. A second observation is that in a primitive sublattice each lattice point in the sublattice unit cell can be reached successively (and therefore sorted in ascending order), because all lattice points lie on a single line crossing the origin of the lattice and some translationally equivalent point (*e.g.* direction $[1\bar{4}]$ in Fig. 3 as well as $[1\bar{4}0]$ in Fig. 6). In order to construct the MCG and find the special value μ of the multiplier, one only has to search for the integer value of the shift in the y coordinate necessary to reach a lattice point while going $1/M$ in the x direction. This may be done graphically for low moduli/sublattice indices and algebraically for the higher ones. This is to find integral solutions u, v and μ to the equation

$$u\mathbf{a} + v\mathbf{b} = (1/M)\mathbf{a}' + (\mu/M)\mathbf{b}'. \tag{11}$$

In the present case, 17 steps, in units of $1/M$, are needed to reach the first lattice point while advancing one step in x (thus $\mu = 17$). The second lattice point is reached again after 17 steps, modulo the lattice translations (given by M, here $M = 21$), and so on, until each lattice point is crossed exactly once. Both the multiplier and the modulus, and therefore the MCG, are uniquely determined by this process:

$$Y_i \equiv 17X_i \,(\mathrm{mod}\, 21). \tag{12}$$

Alternatively, by advancing one step in the y direction first and asking for the number of steps needed in the x direction to reach a lattice point one defines another MCG (with the special multiplier $\overline{\mu}$):

$$X_i \equiv 5Y_i \,(\mathrm{mod}\, 21). \tag{13}$$

Equation (13) describes the inverse function to equation (12). Accordingly, μ and $\overline{\mu}$ are multiplicative inverse modulo 21, *i.e.* $1 \equiv \overline{\mu}\mu \,(\mathrm{mod}\, 21)$. Thus, the cycle structure associated with the MCG of equation (13) describes the inverse permutation,

$$(0)(1\ 5\ 4\ 20\ 16\ 17)(2\ 10\ 8\ 19\ 11\ 13)(3\ 15\ 12\ 18\ 6\ 9)(7\ 14), \tag{14}$$

to equation (7). The algebraic determination of $\overline{\mu}$ then consists of finding the integer solutions $\overline{u}$, $\overline{v}$, $\overline{\mu}$ for

$$\overline{u}\mathbf{a} + \overline{v}\mathbf{b} = (\overline{\mu}/M)\mathbf{a}' + (1/M)\mathbf{b}'. \tag{15}$$

The pairs (u, v) and $(\overline{u}, \overline{v})$ each describe the coordinates of a point in terms of the basic lattice Λ. For practical purposes equations (11) and (15) are rewritten using the matrix formalism of equation (3) yielding

$$(u, v)^{\mathrm{t}} = (1/|\mathbf{M}|)\mathbf{M}(1, \mu)^{\mathrm{t}} \tag{16}$$

$$(\overline{u}, \overline{v})^{\mathrm{t}} = (1/|\mathbf{M}|)\mathbf{M}(\overline{\mu}, 1)^{\mathrm{t}} \tag{17}$$

as the equivalent equations. In addition, exchanging the coordinates while retaining the multiplier, *e.g.*

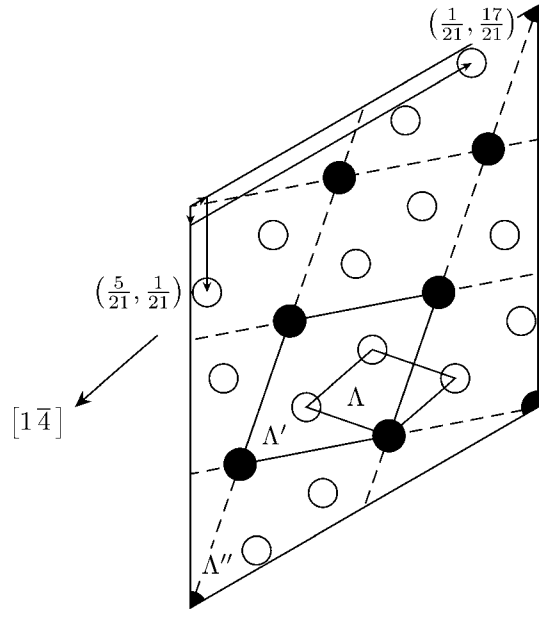

Figure 3
Hexagonal sublattice of index $T(5, 4) = 21$, $\Lambda \rightarrow \Lambda''$. With respect to the solid circles the sublattice is of index $T(3, 1) = 7$ only, $\Lambda' \rightarrow \Lambda''$. The corresponding MCGs are given by $Y_i \equiv 17X_i \,(\mathrm{mod}\, 21)$ and $Y_i \equiv 3X_i \,(\mathrm{mod}\, 7)$. See Fig. 4 for the enantiomorphous sublattice $T(5, 1) = 21$ and Fig. 6 for chemical realizations.

$$X_i \equiv 17Y_i \,(\mathrm{mod}\, 21), \tag{18}$$

$$Y_i \equiv 5X_i \,(\mathrm{mod}\, 21), \tag{19}$$

[*cf.* equations (12) and (13)] gives rise to a description of the enantiomorphic sublattice.

From Fig. 3 one sees some additional sublattice structure in a hexagonal sublattice of index 21. Starting from the basic lattice there are additional lattice–sublattice transformations of indices 3 and 7, respectively. In terms of group–subgroup relations this corresponds to *klassengleiche* transitions (isomorphic if the space-group type of the group and the subgroup are the same). In shorthand notation:

$$\Lambda \overset{k3}{\rightarrow} \Lambda' \overset{k7}{\rightarrow} \Lambda'' \cong \Lambda \overset{k21}{\rightarrow} \Lambda''. \tag{20}$$

This has an equivalent in number-theoretic terms,

$$\mathbb{Z}/21\mathbb{Z} = \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}, \tag{21}$$

and another one with respect to MCGs, where it can be shown that the weighted sum of two (or n) MCGs with coprime moduli $M_1, M_2, \ldots, M_n$ is equivalent to another combined MCG with modulus $M = \prod_{i=1}^{n} M_i$ [Wichmann-Hill MCGs; see L'Ecuyer & Tezuka (1991) and Sakamoto & Morita (1995) for details]. Take, in particular, two MCGs Ξ_1 and Ξ_2 with

$$\Xi_1: \quad Z_{n+1} \equiv 2Z_n \,(\mathrm{mod}\, 3), \tag{22}$$

and

$$\Xi_2: \quad Z_{n+1} \equiv 3Z_n \,(\mathrm{mod}\, 7). \tag{23}$$

A combined MCG Ξ_{1+2} may then be defined as

$$\Xi_{1+2}: \quad z_{n+1} \equiv n_1(\Xi_1/3) + n_2(\Xi_2/7) \,(\mathrm{mod}\, 1), \tag{24}$$

with integer weighting factors n_i and normalized output lying in the interval $[0, 1)$. The sequence of numbers resulting from the combined MCG with weights $n_1 = 1$ and $n_2 = -2$ proves to be identical to the one generated by the single MCG $z_{n+1} = (1/21)\{17Z_n \,(\mathrm{mod}\, 21)\}$.

A profound number-theoretic analysis may be given, making use of complex number fields [see Conway & Sloane (1999) and Hardy & Wright (2008)].

The points of the hexagonal lattice A_2 are then identified with the ring $\mathbb{Z}[\omega]$ of Eisenstein integers, which are complex numbers of the form $z = q + r\omega$ where $q, r \in \mathbb{Z}$, $\omega = (1/2)(-1 + 3^{1/2}i)$ and $i^2 = -1$. The unit ω is one of the sixth roots of unity, $z^6 = 1$, where $z \in \{\pm 1, \pm\omega, \pm\omega^2\}$ with ω^2 the complex conjugate of ω, *i.e.* $\omega^2 = (1/2)(-1 - 3^{1/2}i)$. The number-theoretic norm of an Eisenstein integer is given by $N(q + r\omega) = |q + r\omega|^2 = (q + r\omega)(q + r\omega^2) = q^2 - qr + r^2$, *i.e.* $N(q + r\omega) = T$. An application of Eisenstein integers in structural chemistry is given by Mitani & Niizeki (1987).

A similar approach is possible for the square lattice $\mathbb{Z}^2$, whose points are identified with the ring $\mathbb{Z}[i]$ of Gaussian integers $z = q + si$ with $q, s \in \mathbb{Z}$ and $i^2 = -1$. The unit i is one of the fourth roots of unity, $z^4 = 1$, where $z \in \{\pm 1, \pm i\}$. The number-theoretic norm of a Gaussian integer is given by $N(q + si) = |q + si|^2 = (q + si)(q - si) = q^2 + s^2$, *i.e.* $N(q + si) = Q$.

For a depiction of the lattice structure of the Eisenstein and Gaussian integers see Conway & Smith (2005).

In either case a single complex number is sufficient to describe a lattice–sublattice pair [a complex number $z = r\exp(i\varphi)$ elegantly describes a roto-dilation in two-dimensions, where the scaling factor r is given by the modulus of z, $r = |z|$, and the positive rotation angle φ is given by the argument of z, $\varphi = \arg(z)$].

Notably, both the Eisenstein and the Gaussian integers have a unique factorization, up to units, into the primes of their respective number field [see *e.g.* Baake & Grimm (2006) treating the case of the Eisenstein integers and Hardy & Wright (2008) for a general overview]. For a hexagonal lattice with $T(5, 1) = 21$ the corresponding Eisenstein number is $5 + \omega$ and

$$5 + \omega = (2 + \omega)(2 - \omega) \tag{25}$$

is its prime factorization, where

$$N(2 + \omega) = 3 \quad \text{and} \quad N(2 - \omega) = 7 \tag{26}$$

are the respective number-theoretic norms [*cf.* equations (20), (21) and (24)].

Referring to the cycle representation

$$(0)\underbrace{(1\ 17\ 16\ 20\ 4\ 5)}_{\gcd = 1}\underbrace{(2\ 13\ 11\ 19\ 8\ 10)}_{1}\underbrace{(3\ 9\ 6\ 18\ 12\ 15)}_{3}\underbrace{(7\ 14)}_{7}, \tag{27}$$

there seems to be a similar relation, expressing itself in the values of the greatest common divisor (gcd) of the different cycles. Actually, the cycles for which gcd = 3 and gcd = 7 each are associated to a set of points (X_i, Y_i) corresponding to sublattices of index 3 and 7, respectively, in reference to a common basic lattice Λ [*cf.* equation (10) and Fig. 3].

This correspondence of the coordinates is deeper, having some far-reaching crystallographic implications. Essentially there is not only a correspondence of the coordinate pairs derived from the action of an MCG with some points of the lattice, but a correspondence encompassing a set of symmetry-equivalent points (crystallographic orbit or point configuration, depending on whether the symmetry group is included or not). This can be rationalized by analyzing the action (symmetry operation $\boldsymbol{R}$) of the six- or fourfold rotation axis (with negative rotation sense, *i.e.* clockwise rotation) in the plane groups $p6$ or $p4$, respectively, expressed in matrix notation as

$$\boldsymbol{R}: \quad 6^-_{(00)} = \begin{pmatrix} 0 & 1 \\ \bar{1} & 1 \end{pmatrix} \quad \text{or} \quad 4^-_{(00)} = \begin{pmatrix} 0 & 1 \\ \bar{1} & 0 \end{pmatrix} \tag{28}$$

for transformations of the type

$$(x', y')^{\mathrm{t}} = \boldsymbol{R}(x, y)^{\mathrm{t}}. \tag{29}$$

The essential part of the transformation is given by the mapping $x' = y$. The MCG, in the first place, describes a one-to-one mapping of an x-coordinate value to a y-coordinate value, $x \rightarrow y$, whereas the symmetry operation represented by $\boldsymbol{R}$ gives a transformed x'-coordinate value from the y-coordinate value of the original point, $y \rightarrow x'$. One after

another this describes a mapping $x \rightarrow x'$ and consequently one of the type $x \rightarrow x' \rightarrow x'' \ldots$, until the original point is reached again, due to the cyclic nature of the symmetry operation of a rotation axis.

In some sense it is not surprising at all to find permutations on the very ground of the description of crystal structures. Treating atoms as point-like particles, characterized by their coordinates, the space-group symmetry will essentially map all of the atoms onto each other in some way, permutating their relative coordinates, because the set of crystallographically independent atoms is closed.

6. Cycle representations of MCGs

From the definition given in equation (5) it is clear that MCGs have an inherent fundamental periodicity, *i.e.* their modulus, fixing the maximal length of a single cycle in their cycle representation. For an MCG a maximal cycle length of $\ell = M - 1$ may be achieved obeying certain restrictions, namely if the modulus is prime and both the multiplier and the modulus are relatively prime, *i.e.* $\gcd(m, M) = 1$. The maximum achievable cycle length for composite moduli as well as powers of two or prime powers can be elucidated using a theorem of Carmichael (1910).

Altogether, given a fixed M, the choice of the multiplier m fully determines the behavior of the MCG, as is illustrated in the following for a hexagonal sublattice:

$$
\begin{aligned}
T(3,1) = 7 \quad m &= 1 \quad (0)(1)(2)(3)(4)(5)(6)\\
m &= 2 \quad (0)(1\ 2\ 4)(3\ 6\ 5)\\
\mu &= 3 \quad (0)(1\ 3\ 2\ 6\ 4\ 5) \cong 6^-\\
m &= 4 \quad (0)(1\ 4\ 2)(3\ 5\ 6)\\
\overline{\mu} &= 5 \quad (0)(1\ 5\ 4\ 6\ 2\ 3) \cong 6^+\\
m &= 6 \quad (0)(1\ 6)(2\ 5)(3\ 4).
\end{aligned}
$$

In the case $m = 1$ every point is mapped onto itself, corresponding to the identity operation. Every other multiplier leads to a distinct cycle decomposition, representing different types of permutations. For every permutation there is the inverse permutation described by an MCG with a different multiplier. In the case $m = 6$ the permutation consists of the fixpoint and transpositions only, therefore being self-inverse. In the special cases were $m = \mu$ or $m = \overline{\mu}$ the cycle representation consists of the fixpoint and a single cycle of length $\ell = 6$ each, which corresponds to a crystallographic orbit reflecting the symmetry of the sixfold rotation axis [μ ($\overline{\mu}$) for the 6^- (6^+) axis with negative (positive) rotation sense].

7. Cycle representations for special values of T and Q

The following cycle representations serve as examples to illustrate the use of MCGs in a crystallographic context. Besides this, they are interesting in their own right.

7.1. The first sublattices with equal index: $T = Q = 13$

There are a number of instances in which hexagonal and square sublattices share the same index. This is true for all indices given by a square number and for several other cases. Among these the indices associated with a primitive sublattice are again of interest here. These are 13, 37, 61, 73, 97 (below 100). The cycle representations for the simplest case $T = Q = 13$ are given by

$$
\begin{aligned}
&T(4,1) = 13\\
&\mu = \ \ 4 \quad (0)(1\ 4\ 3\ 12\ 9\ 10)(2\ 8\ 6\ 11\ 5\ 7)\\
&\bar{\mu} = 10 \quad (0)(1\ 10\ 9\ 12\ 3\ 4)(2\ 7\ 5\ 11\ 6\ 8)
\end{aligned}
$$

$$
\begin{aligned}
&Q(3,2) = 13\\
&\mu = 8 \quad (0)(1\ 8\ 12\ 5)(2\ 3\ 11\ 10)(4\ 6\ 9\ 7)\\
&\bar{\mu} = 5 \quad (0)(1\ 5\ 12\ 8)(2\ 10\ 11\ 3)(4\ 7\ 9\ 6)
\end{aligned}
$$

showing that which type of cycle decompositions is realized for a hexagonal–square sublattice pair of given index depends solely on the choice of the multiplier (*cf.* Fig. 4).

7.2. The first sublattices with fully structured cycle decompositions: $T = 21$, $Q = 10$

We call any cycle decomposition fully structured if its representation in symbolic notation is given by either $(0)(Z_{i1}\ \ldots\ Z_{i6})_{i=1}^{n}(\frac{1}{3}T\ \ \frac{2}{3}T)$ or $(0)(Z_{i1}\ \ldots\ Z_{i4})_{i=1}^{n}(\frac{1}{2}Q)$, depending on the symmetry (hexagonal or square) of the sublattice under consideration. Thus, a fully structured cycle decomposition contains the fixpoint (0), a variable number n of cycles of length 6 (or 4), and, *in addition*, a single cycle of length 2 (or 1), whose content is directly derived from the knowledge of the sublattice index T (or Q). The first such cycle decompositions are reached at the index values $T = 21$ and $Q = 10$ and are given below (*cf.* Fig. 4).

$$
\begin{aligned}
&T(5,1) = 21\\
&\mu = 5 \quad (0)(1\ 5\ 4\ 20\ 16\ 17)(2\ 10\ 8\ 19\ 11\ 13)(3\ 15\ 12\ 18\ 6\ 9)(7\ 14)\\
&\overline{\mu} = 17 \quad (0)(1\ 17\ 16\ 20\ 4\ 5)(2\ 13\ 11\ 19\ 8\ 10)(3\ 9\ 6\ 18\ 12\ 15)(7\ 14)
\end{aligned}
$$

$$
\begin{aligned}
&Q(3,1) = 10\\
&\mu = 3 \quad (0)(1\ 3\ 9\ 7)(2\ 6\ 8\ 4)(5)\\
&\bar{\mu} = 7 \quad (0)(1\ 7\ 9\ 3)(2\ 4\ 8\ 6)(5)
\end{aligned}
$$

The sublattices with fully structured cycle representations are the ones where the one-to-one correspondence between number-theoretic and crystallographic terms can be fully illustrated (*cf.* §8).

A survey of the cycle decompositions of primitive similar sublattices for reasonably small indices (≤ 61) is presented in tabular form, with Table 1 giving the hexagonal and Table 2 giving the square cases.

7.3. The first pair of distinct sublattices: $T = 91$, $Q = 65$

The number of representations of a given index increases with its value. The index $T = 49$ is the first one that can be constructed in two different ways, *i.e.* as $T(7, 0)$ and $T(8, 3)$.

The same holds true for $Q = 25$, where $Q(5, 0)$ and $Q(4, 3)$ yield the same index. In these cases one of the solutions is a nonprimitive sublattice, whereas the other one gives rise to two enantiomorphic sublattices (which is true in general for all sublattice indices not lying on any of the bold lines in Fig. 1). The first case, where two distinct pairs of primitive sublattices are encountered, is given by $T = 91 = 7 \cdot 13$ and $Q = 65 = 5 \cdot 13$, respectively. We restrict ourselves in giving not the full cycle representation here, but instead the special multipliers,

$$\begin{array}{lll} T(10, 1) = 91 & \mu = 10 & \overline{\mu} = 82, \\ T(11, 5) = 91 & \mu = 75 & \overline{\mu} = 17, \\ & & \\ Q(7, 4) = 65 & \mu = 18 & \overline{\mu} = 47, \\ Q(8, 1) = 65 & \mu = \ 8 & \overline{\mu} = 57, \end{array} \qquad (30)$$

from which the cycle representations can be easily constructed.

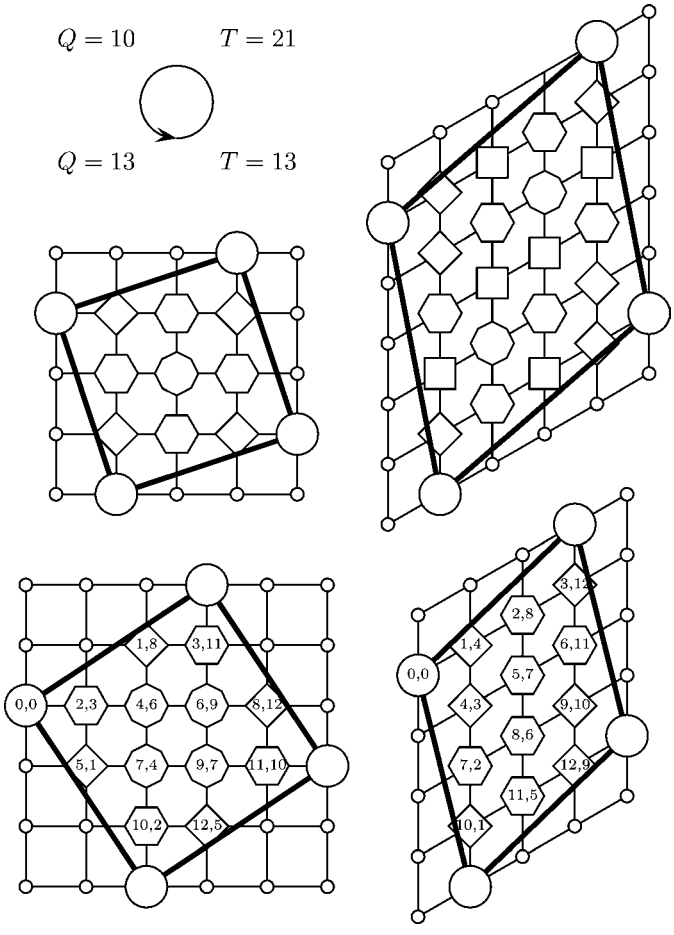

Figure 4
Anticlockwise from top left to top right: square sublattice with minimal index $Q(3, 1) = 10$ for a full cycle structure; square sublattice with $Q(3, 2) = 13$; hexagonal sublattice with $T(4, 1) = 13$; hexagonal sublattice with minimal index $T(5, 1) = 21$ for a full cycle structure. Points equivalent under the symmetry operation of a six- or fourfold rotation point are distinguished by a distinct polyhedral hull and given with their (X_i, Y_i) coordinates for the index 13 sublattices: $(x_i, y_i) = (1/13)(X_i, Y_i)$.

Table 1
Cycle decompositions of primitive hexagonal similar sublattices ($T \leq 61$).

T	(q, r)	μ	$\overline{\mu}$	Cycle representation
3	(2, 1)	2	2	(0)(1 2)
7	(3, 1)	3	5	(0)(1 3 2 6 4 5)
13	(4, 1)	4	10	(0)(1 4 3 12 9 10)(2 8 6 11 5 7)
19	(5, 2)	12	8	(0)(1 12 11 18 7 8)(2 5 3 17 14 16) (4 10 6 15 9 13)
21	(5, 1)	5	17	(0)(1 5 4 20 16 17)(2 10 8 19 11 13) (3 15 12 18 6 9)(7 14)
31	(6, 1)	6	26	(0)(1 6 5 30 25 26)(2 12 10 29 19 21) (3 18 15 28 13 16)(4 24 20 27 7 11) (8 17 9 23 14 22)
37	(7, 3)	27	11	(0)(1 27 26 36 10 11)(2 17 15 35 20 22) (3 7 4 34 30 33)(5 24 19 32 13 18) (6 14 8 31 23 29)(9 21 12 28 16 25)
39	(7, 2)	23	17	(0)(1 23 22 38 16 17)(2 7 5 37 32 34) (3 30 27 36 9 12)(4 14 10 35 25 29) (6 21 15 33 18 24)(8 28 20 31 11 19)(13 26)
43	(7, 1)	7	37	(0)(1 7 6 42 36 37)(2 14 12 41 29 31) (3 21 18 40 22 25)(4 28 24 39 15 19) (5 35 30 38 8 13)(9 20 11 34 23 32) (10 27 17 33 16 26)
49	(8, 3)	19	31	(0)(1 19 18 48 30 31)(2 38 36 47 11 13) (3 8 5 46 41 44)(4 27 23 45 22 26) (6 16 10 43 33 39)(7 35 28 42 14 21) (9 24 15 40 25 34)(12 32 20 37 17 29)
57	(8, 1)	8	50	(0)(1 8 7 56 49 50)(2 16 14 55 41 43) (3 24 21 54 33 36)(4 32 28 53 25 29) (5 40 35 52 17 22)(6 48 42 51 9 15) (10 23 13 47 34 44)(11 31 20 46 26 37) (12 39 27 45 18 30)(19 38)
61	(9, 4)	48	14	(0)(1 48 47 60 13 14)(2 35 33 59 26 28) (3 22 19 58 39 42)(4 9 5 57 52 56) (6 44 38 55 17 23)(7 31 24 54 30 37) (8 18 10 53 43 51)(11 40 29 50 21 32) (12 27 15 49 34 46)(16 36 20 45 25 41)

8. Translating the terms of MCGs into the language of lattice–sublattice transformations and the coordinate description of crystal structures

Following the discussions in the previous sections it becomes clear that there is indeed a one-to-one correspondence between the terms used for the description of MCGs and the ones used for the description of crystal structures. Table 3 lists the crystallographic counterparts to terms used throughout this report for the characterization of MCGs. Table 4 is an extension of Table 3 intended to illustrate the one-to-one correspondence between the cycle structure of an MCG and the Wyckoff sequence of a crystal structure based on a lattice–sublattice pair. It gives the coordinates (x, y) of the special positions for the plane groups $p6$ and $p4$, their corresponding Wyckoff symbols and the corresponding cycles in the cycle representation of a MCG-induced permutation. The holohedral groups $p6mm$ and $p4mm$ are not considered here because they are only valid for the simplest cases of primitive sublattices. The Wyckoff positions 1*a* correspond to the fixpoint of the permutation induced by an MCG which, identified as the origin of the unit cell, is also the fixpoint in the lattice–sublattice transformation. The *b*-lettered Wyckoff positions correspond to special positions at high-symmetry points inside the unit cells. The *c*-lettered Wyckoff positions instead have no counterpart in the cycle representations, because an occupa-

Table 2
Cycle decompositions of primitive square similar sublattices ($Q \leq 61$).

Q	(q, s)	μ	$\overline{\mu}$	Cycle representation
2	(1, 1)	1	1	(0)(1)
5	(2, 1)	2	3	(0)(1 2 4 3)
10	(3, 1)	3	7	(0)(1 3 9 7)(2 6 8 4)(5)
13	(3, 2)	8	5	(0)(1 8 12 5)(2 3 11 10)(4 6 9 7)
17	(4, 1)	4	13	(0)(1 4 16 13)(2 8 15 9)(3 12 14 5)(6 7 11 10)
25	(4, 3)	18	7	(0)(1 18 24 7)(2 11 23 14)(3 4 22 21)(5 15 20 10) (6 8 19 17)(9 12 16 13)
26	(5, 1)	5	21	(0)(1 5 25 21)(2 10 24 16)(3 15 23 11)(4 20 22 6) (7 9 19 17)(8 14 18 12)(13)
29	(5, 2)	17	12	(0)(1 17 28 12)(2 5 27 24)(3 22 26 7)(4 10 25 19) (6 15 23 14)(8 20 21 9)(11 13 18 16)
34	(5, 3)	13	21	(0)(1 13 33 21)(2 26 32 8)(3 5 31 29)(4 18 30 16) (6 10 28 24)(7 23 27 11)(9 15 25 19) (12 20 22 14)(17)
37	(6, 1)	6	31	(0)(1 6 36 31)(2 12 35 25)(3 18 34 19)(4 24 33 13) (5 30 32 7)(8 11 29 26)(9 17 28 20)(10 23 27 14) (15 16 22 21)
41	(5, 4)	32	9	(0)(1 32 40 9)(2 23 39 18)(3 14 38 27)(4 5 37 36) (6 28 35 13)(7 19 34 22)(8 10 33 31) (11 24 30 17)(12 15 29 26)(16 20 25 21)
61	(6, 5)	50	11	(0)(1 50 60 11)(2 39 59 22)(3 28 58 33)(4 17 57 44) (5 6 56 55)(7 45 54 16)(8 34 53 27)(9 23 52 38) (10 12 51 49)(13 40 48 21)(14 29 47 32) (15 18 46 43)(19 35 42 26)(20 24 41 37) (25 30 36 31)

tion of these sites would inevitably result in a nonprimitive sublattice. Finally, the d-lettered Wyckoff positions represent crystallographic orbits with a number of points equalling the order of the point group, and, correspondingly, a full-length cycle representation. Thus, the Wyckoff sequence is either

$$pN, d^n a \quad \text{or} \quad pN, d^n ba, \tag{31}$$

where N corresponds to the order of the rotation axis, *i.e.* $N = 6$ (or 4), and n is the number of cycles of length $\ell = 6$ (or 4).

9. Generalized cycle representations

From the aforementioned findings it is conjectured that

$$\begin{aligned} &(0)(Z_{i1} \ \ldots \ Z_{i6})_{i=1}^{n} && \forall\, T \mid 0 \not\equiv T \,(\mathrm{mod}\, 3) \\ &&& \rightarrow T = 6n + 1 \\ &(0)(Z_{i1} \ \ldots \ Z_{i6})_{i=1}^{n}(\tfrac{1}{3}T \ \tfrac{2}{3}T) && \forall\, T \mid 0 \equiv T \,(\mathrm{mod}\, 3) \\ &&& \rightarrow T = 6n + 3 \end{aligned}$$

and

$$\begin{aligned} &(0)(Z_{i1} \ \ldots \ Z_{i4})_{i=1}^{n} && \forall\, Q \mid 0 \not\equiv Q \,(\mathrm{mod}\, 2) \\ &&& \rightarrow Q = 4n + 1 \\ &(0)(Z_{i1} \ \ldots \ Z_{i4})_{i=1}^{n}(\tfrac{1}{2}Q) && \forall\, Q \mid 0 \equiv Q \,(\mathrm{mod}\, 2) \\ &&& \rightarrow T = 4n + 2 \end{aligned}$$

are the general forms for the cycle representations of primitive hexagonal and square sublattices of arbitrary index. The special multipliers μ (and $\overline{\mu}$) associated with these cycle representations share the property

$$1 \equiv \mu^6 \,(\mathrm{mod}\, T) \quad \text{and} \quad 1 \equiv \mu^4 \,(\mathrm{mod}\, Q). \tag{32}$$

Equation (32) gives a simple alternative for the determination of the special multipliers associated with certain lattice–sublattice transformations. From the definition of the multiplicative inverse it follows that

$$1 \equiv \mu^{\ell} \equiv \mu^{\ell-1}\mu \equiv \overline{\mu}\,\mu \,(\mathrm{mod}\, M) \tag{33}$$

$$\Rightarrow \quad \overline{\mu} \equiv \mu^{\ell-1} \,(\mathrm{mod}\, M). \tag{34}$$

Furthermore it is conjectured that

$$\mu + \overline{\mu} = T + 1 \quad \text{and} \quad \mu + \overline{\mu} = Q$$

holds true consistently.

Table 3
Crystallographic counterparts to terms used for the characterization of MCGs.

Multiple congruential generators	Lattice–sublattice transformations
Modulus M	Index T or Q
MCG-induced permutation	Symmetry group
Pairs of successive cycle elements	Lattice-point coordinates
Single cycle	Crystallographic orbit
No. of cycles	No. of Wyckoff positions
Cycle lengths ℓ	Wyckoff multiplicities
Cycle representation	Wyckoff sequence

Table 4
Scheme showing the one-to-one correspondence between the cycle structure of an MCG and the Wyckoff sequence of a crystal structure.

	Cycle	(0)	$(\frac{1}{3}T \ \frac{2}{3}T)$	–	$(Z_{i1} \ \ldots \ Z_{i6})_{i=1}^{n}$
$p6$	(x, y)	0 0	$\frac{1}{3}\ \frac{2}{3}$	$0\ \frac{1}{2}$	$x\ y$
	Wyckoff positions	1a	2b	3c	6d
$p4$	Wyckoff positions	1a	1b	2c	4d
	(x, y)	0 0	$\frac{1}{2}\ \frac{1}{2}$	$0\ \frac{1}{2}$	$x\ y$
	Cycle	(0)	$(\frac{1}{2}Q)$	–	$(Z_{i1} \ \ldots \ Z_{i4})_{i=1}^{n}$

10. MCGs with irrational parameters

An MCG is defined by two parameters, its modulus M and a general multiplier m. Essentially these numbers define *two* fundamental periodicities (length scales), with their ratio m/M being a rational number, causing the cyclic behavior of the MCG after M successive steps (*cf.* Fig. 3). To put it another way, one can say that m and M are commensurate. What happens if m and M are incommensurate? This requires the ratio m/M to be irrational, $\eta = m/M \notin \mathbb{Q}$, and the definition of a modulo operator in order to include real numbers. This is done according to

$$(x \bmod M) = x - M\lfloor x/M \rfloor, \tag{35}$$

where $\lfloor\cdot\rfloor$ denotes the floor function, which gives the largest integer less than or equal to its argument. As a consequence the sequence of numbers generated by the MCG will no longer be cyclic and will never reach the seed value again. That is,

$$1 \neq (\eta^n \bmod M) \tag{36}$$

for any $n \in \mathbb{N}$. In a way the exact value of the modulus becomes irrelevant, thus it would be justifiable to set it to unity, constructing another type of MCG. The action of a unit modulus may be conceived as a back-projection of values

exceeding unity into the interval $[0, 1)$. In the same way as before, a two-dimensional plot is generated by factoring out pairs of successive numbers,

$$p_n = (z_n, z_{n+1}) = \big((\eta^{n-1} z_1 \bmod 1), (\eta^n z_1 \bmod 1)\big). \quad (37)$$

In the limit where $n \to \infty$ the set of points $\{p_n\}_{n=1}^{n}$ will densely cover the unit mesh (except its origin).

Bowman (1995) introduced the LCG

$$Z_{n+1} \equiv 157 Z_n + 1 \,(\mathrm{mod}\, \pi) \quad (38)$$

with an irrational modulus, whereas the irrationality of the MCG

$$z_{n+1} = \big|(100 \ln z_n \bmod 1)\big| \quad (39)$$

proposed by Pickover (1995) for a seed $z_0 = 0.1$ and $n \in \mathbb{N} \cup \{0\}$ stems from taking the natural logarithm of the seed and the successive values. The first few points resulting from Pickover's LCG are $(0.1, 0.258\ldots)$, $(0.258\ldots, 0.282\ldots)$, $(0.282\ldots, 0.456\ldots)$, and a two-dimensional plot of the first 10 000 points is given by the (minimally functional) *Mathematica* code

```
X[x_] = Abs[FractionalPart[100 Log[x]]];
Show[Graphics[Table[
  Point[{Nest[X, 0.1, n], Nest[X, 0.1, n + 1]}],
                                {n, 0, 9999}]],
PlotRange -> {{0, 1}, {0, 1}},
AspectRatio -> 1, Frame -> True]
```

and depicted in Fig. 5.

Both LCGs yield pseudo-random number sequences which pass all the standard tests judging their randomness. Without knowing their generation method in advance, these sequences, despite being totally deterministic, are barely discernible from a true random sequence derived *via* a stochastic process like coin flipping! In fact, all MCGs exhibit properties similar to deterministic chaotic dynamical processes, namely Bernoulli shifts (Herring & Palmore, 1989).

In a way there is plenty of room to play with the parameters, taking either the modulus, the multiplier or the seed as irrational, or using combinations of parameters, or using MCGs that result in an irrational behavior. However, in nearly all cases where the parameters were chosen at random, there remains a remarkable tendency for lattice-like structures (for finite values of n, especially low ones), whereas in a strict mathematical sense, there is no lattice structure present anymore, but instead that of a $\mathbb{Z}$-module. This owes much similarity to aperiodic crystals, among them incommensurately modulated structures and quasicrystals.

In order to study approximations to incommensurate structures it would be nice to find such irrational multipliers that 'approximate' an integer multiplier in some predictable way. By the Lindemann–Weierstrass theorem any number e^{α} is transcendental, and thus irrational, for which α is a nonzero algebraic, *e.g.* rational, number (e is Euler's constant). Given an integer multiplier μ we may search for an irrational multiplier $\eta = e^{\alpha}$ for which η is arbitrarily close to μ. Setting $\alpha = \ln \mu$, however, results in a rational multiplier $\eta = e^{\ln \mu} = \mu$. The natural logarithm of any integer $n \geq 2$ is an irrational number, and so is $\ln \mu$. Any irrational number can be approximated to arbitrary precision by a sequence of rational numbers (convergents) r_i, with consecutive elements of the sequence given by a stepwise truncation of terms of the irrational numbers infinite continued fraction expansion. Thus, irrational numbers of the type e^r, $r \in \mathbb{Q}$, where the r's correspond to ever-improving rational approximations of $\ln \mu$, give an ever-improving 'approximate' of the integer multiplier μ. With respect to crystal structures this situation is quite contrary to the well known approach of approximating an incommensurate crystal structure by a series of commensurate structures. Here, instead, we define a series of irrational MCGs related to a single rational one.

11. MCGs in structural chemistry and biology

The use of MCGs in the aforementioned way is essentially restricted to two-dimensional cases, although there exists an intrinsic lattice structure for MCGs in Euclidean space of arbitrary dimension. Below we give some suggestions about chemical and biological systems in which the use of MCGs may prove beneficial.

11.1. Planar systems in two dimensions

Essentially, two-dimensional systems encountered in solid-state chemistry, where lattice–sublattice transformations of the aforementioned type are of significant importance, are self-assembling monolayers, intercalation compounds (*e.g.* of alkaline metals in graphite) and certain types of layered structures.

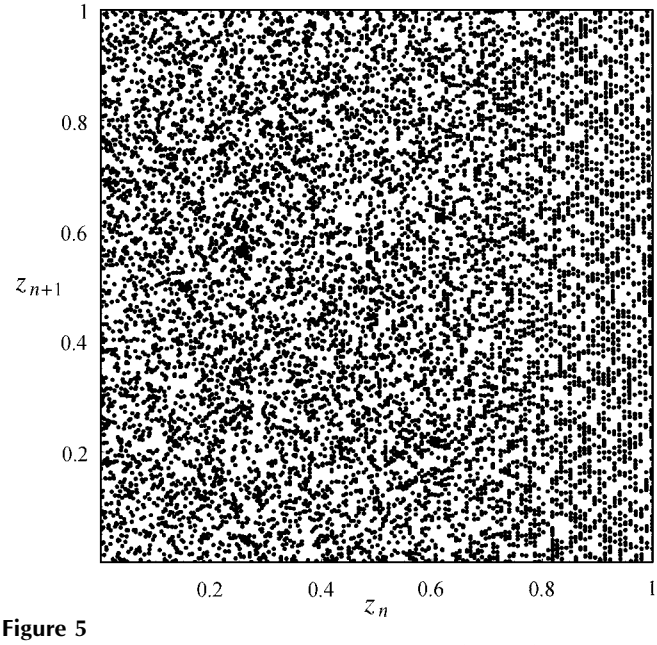

Figure 5
Two-dimensional plot for the first 10 000 points (z_n, z_{n+1}) generated by Pickover's MCG [equation (39)]. No perceivable sublattice structure is seen.

An example of the latter are transition-metal dichalcogenides MQ_2, which generally show strong bonding interactions inside the two-dimensional layers and weak ones perpendicular to them, *i.e.* between adjacent layers of Q atoms. Compounds of this type are often subject to an electronic distortion due to the presence of a charge-density wave, resulting in an incommensurate modulation of the structure with complex lock-in superstructures frequently observed. The disulfides, diselenides and ditellurides of the transition metals vanadium, titanium, niobium and tantalum, for instance, crystallize in two-dimensional superstructures with sublattice indices of $T = 3, 4, 7, 13, 16, 19, 31$ (van Landuyt *et al.*, 1978).

A second example is given by a description of the crystal structures of a number of structurally complex intermetallic compounds, among them the quasicrystal approximant structure of λ-Al_4Mn, in terms of stacked atom layers (Uchida & Matsui, 2000). Each of these layers is derived from the hexagonal closest packing of atoms in a plane containing a certain amount of vacant sites. The two-dimensional ordering of atoms and vacancies now defines a lattice–sublattice relation

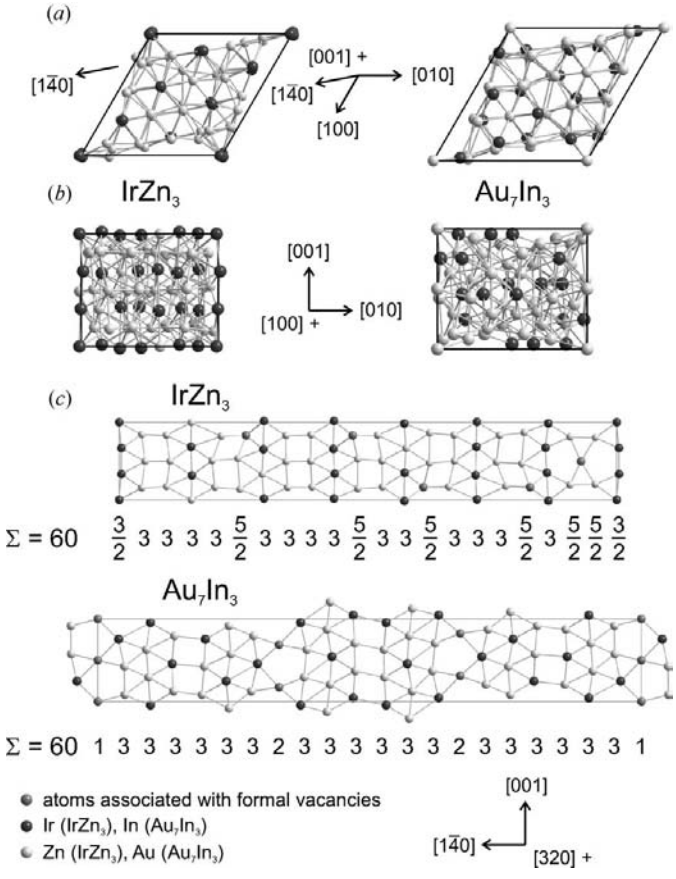

Figure 6
Comparison of the crystal structures of $IrZn_3$ and Au_7In_3 taking advantage of the fact that there exists a direction, here *e.g.* [1$\bar{4}$0], for which every lattice point in a primitive hexagonal sublattice is reached successively. Shown are projections of the crystal structures parallel (*a*) and perpendicular (*b*) to the trigonal axis, and sections taken along [1$\bar{4}$0] (*c*).

of the aforementioned kind. Hence, the ideal positions of atoms and vacancies are given by an MCG.

Another example is taken from the structural chemistry of intermetallic alloys. The crystal structures of Au_7In_3 (Pušelj & Schubert, 1975), Co_2Zn_{15} (Boström & Lidin, 2002) and $IrZn_3$ (Hornfeck *et al.*, 2004) are examples of complex metallic alloys, each encompassing 60 atoms in a hexagonal unit cell of similar metric. The analysis and description of such structures is usually complicated by the high degree of topological interconnection between the constituent atoms, giving rise to high coordination numbers and a pronounced interpenetration of coordination polyhedra. Whereas the crystal structures of Co_2Zn_{15} and $IrZn_3$ are easily described and compared after analyzing the flat and puckered layers of atoms perpendicular to the c direction, a similar approach fails for the Au_7In_3 structure, although the projection along **c** affirms the close structural relationship to $IrZn_3$. Dissecting the structures along the [1$\bar{4}$0] direction, however, resolves this problem. Including nearby atoms the section [1$\bar{4}$0] × [001] contains all the 60 atoms of both unit cells, facilitating a direct comparison and plotting of the structures without any interference due to overlapping atoms (see Fig. 6).

11.2. Generalization to non-Euclidean two-dimensional spaces

Since the seminal work of Caspar & Klug (1962) there is the notion in the structural biology of viruses that the capsid structure of a majority of icosahedral viruses – icosahedral in terms of symmetry rather than shape – can be described by means of triangular surface lattices, giving each capsomer a high-symmetry quasi-equivalent surrounding. Regarding its structure, an icosahedral virus is therefore classified by its triangulation number, being identical to the sublattice index T used throughout this report. From a chemist's point of view it is fascinating that viruses realize both forms of enantiomorphous surface lattices, *e.g.* a $T = 7d$ (*dextro*) surface lattice for the polyomavirus SV40 and a $T = 7l$ (*laevo*) surface lattice for the prohead of bacteriophage HK97 (Chiu *et al.*, 1997), whereas Nature prefers one sense of chirality elsewhere (amino acids, sugars).

Besides the generalization to spherical geometry, there is an ongoing interest in solid-state chemistry in two-dimensional hyperbolic tilings (see *e.g.* Nesper & Leoni, 2001; Hyde & Ramsden, 2003; Ramsden *et al.*, 2009).

According to Fig. 7 a generalization to non-Euclidean spaces seems straightforward, and even though some of the correspondences present in two-dimensional Euclidean space will get lost, some others may possibly emerge.

12. Conclusion

It is well known that MCGs offer an elegant and thus well established algorithmic method for the sequential generation of high-quality pseudo-random numbers.

Their inherent lattice structure, however, extensively researched by mathematicians for high moduli and multipliers,

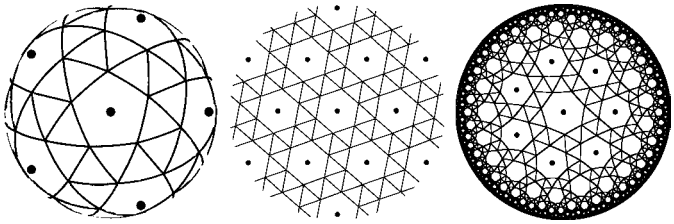

Figure 7
Hexagonal $T(3, 2) = 7$ sublattice embedded on two-dimensional surfaces with constant positive (spherical embedding, spherical polyhedron view), zero (planar embedding, Euclidean plane view) or negative (hyperbolical embedding, Poincaré disc model view; Brant, 2007) curvature. Note that in each case there is an enantiomorphic sublattice. The above illustrations are the special cases n = 5, 6, 7 of the so-called snub n-gonal tilings with Schläfli symbol $s\{3, n\}$ and vertex-configuration 3^4n [see Schläfli (1950) for a description of the symbols bearing his name]. The first members are the icosahedron (n = 3), one of the regular (Platonic) solids, and the snub cube (n = 4), one of the semi-regular (Archimedean) solids. The case n = 5 depicts a spherical polyhedral view of the snub dodecahedron, another semi-regular (Archimedean) solid. Members with $3 \leq n < 6$ are convex polyhedra, whereas the ones with $n > 6$ are concave ones, with a semi-regular (Archimedean) tiling representing the planar case, for which $n = 6$. The generalization to sublattices of higher index T is straightforward.

and for spaces of arbitrary dimensions, proves to be of its own interest in the crystallographic description of two-dimensional structures exhibiting a lattice–sublattice (group–subgroup) relationship with possible embeddings in spaces of positive, zero or negative curvature.

Of particular interest herein is the cycle structure of the permutations associated with an MCG of given modulus, which, for a special selection of multipliers, favors a one-to-one correspondence with crystallographic notions like crystallographic orbits, Wyckoff multiplicities or Wyckoff sequences. In this context the concept of an MCG seems to have some didactic value, too.

Additionally, the calculation of lattice-point coordinates employing an MCG need not make use of matrix inversion or multiplication operations, with the MCG containing all the information about the whole set of coordinates within a single, concise, size-independent (regarding the sublattice index) formula – which therefore is easier to implement, faster to evaluate, more elegant in notation, and, if nothing else, easy to remember.

The authors wish to thank Michael Baake and Peter Zeiner for their interest, a pleasant stay in Bielefeld (WH) and helpful discussions, and Ulrich Müller for his valuable comments.

References

Afflerbach, L. (1986). *Manuscr. Math.* **55**, 455–465.
Ash, A. & Gross, R. (2006). *Fearless Symmetry – Exposing the Hidden Patterns of Numbers.* 1st ed. Princeton, Woodstock: Princeton University Press.
Baake, M. & Grimm, U. (2006). *Z. Kristallogr.* **221**, 571–581.
Ball, D. G. (1971). *Math. Gaz.* **55**, 373–379.
Bernstein, M., Sloane, N. J. A. & Wright, P. E. (1997). *Discret. Math.* **170**, 29–39.
Beyer, W. A., Roof, R. B. & Williamson, D. (1971). *Math. Comput.* **25**, 345–363.
Boström, M. & Lidin, S. (2002). *J. Solid State Chem.* **166**, 53–57.
Bowman, R. L. (1995). *Comput. Graph.* **19**, 315–324.
Brant, D. (2007). *Hyperbolic Tessellations*, http://dmitrybrant.com/2007/01/24/hyperbolic-tessellations.
Carmichael, R. D. (1910). *Bull. Am. Math. Soc.* **16**, 232–238.
Caspar, D. L. D. & Klug, A. (1962). *Cold Spring Harbor Symp. Quant. Biol.* **27**, 1–24.
Chiu, W., Burnett, R. M. & Garcea, R. L. (1997). Editors. *Structural Biology of Viruses.* 1st ed. Oxford, New York: Oxford University Press.
Conway, J. H., Rains, E. M. & Sloane, N. J. A. (1999). *Can. J. Math.* **51**, 1300–1306.
Conway, J. H. & Sloane, N. J. A. (1999). *Sphere Packings, Lattices and Groups.* 3rd ed. New York: Springer.
Conway, J. H. & Smith, D. A. (2005). *On Quaternions and Octonions.* 3rd ed. Wellesley: A. K. Peters Ltd.
Coxeter, H. S. M. (1973). *Regular Polytopes.* 3rd ed. New York: Dover Publications.
Downham, D. Y. & Roberts, F. D. K. (1967). *Comput. J.* **10**, 74–77.
Hardy, G. H. & Wright, E. M. (2008). *An Introduction to the Theory of Numbers.* 6th ed. Oxford, New York: Oxford University Press.
Herring, C. & Palmore, J. I. (1989). *ACM SIGPLAN Not.* **24**, 76–79.
Hornfeck, W., Freistein, S. & Harbrecht, B. (2004). *Z. Anorg. Allg. Chem.* **630**, 1730.
Hyde, S. T. & Ramsden, S. J. (2003). *Eur. Phys. J. B*, **31**, 273–284.
Knuth, D. E. (1998). *The Art of Computer Programming.* 3rd ed., Vol. 2, ch. 3. Reading: Addison-Wesley.
Landuyt, J. van, Wiegers, G. A. & Amelinckx, S. (1978). *Phys. Status Solidi. A*, **46**, 479–492.
L'Ecuyer, P. (1999). *Math. Comput.* **68**, 249–260.
L'Ecuyer, P. & Tezuka, S. (1991). *Math. Comput.* **57**, 735–746.
Loeb, A. L. (1958). *Acta Cryst.* **11**, 469–476.
Loeb, A. L. (1962). *Acta Cryst.* **15**, 219–226.
Loeb, A. L. (1964). *Acta Cryst.* **17**, 179–182.
Marsaglia, G. (1968). *Proc. Natl Acad. Sci.* **61**, 25–28.
Marsaglia, G. (1970). *Numer. Math.* **16**, 8–10.
Mitani, H. & Niizeki, K. (1987). *J. Phys. C Solid State Phys.* **20**, 1017–1030.
Morris, I. L. & Loeb, A. L. (1960). *Acta Cryst.* **13**, 434–443.
Müller, U. & Brelle, A. (1995). *Acta Cryst.* A**51**, 300–304.
Nesper, R. & Leoni, S. (2001). *Chem. Phys. Chem.* **2**, 413–422.
Park, S. K. & Miller, K. W. (1988). *Commun. ACM*, **31**, 1192–1201.
Pickover, C. A. (1995). *Vis. Comput.* **11**, 369–377.
Pušelj, M. & Schubert, K. (1975). *J. Less-Common Met.* **41**, 33–44.
Ramsden, S. J., Robins, V. & Hyde, S. T. (2009). *Acta Cryst.* A**65**, 81–108.
Ripley, B. D. (1983). *Proc. R. Soc. London Ser. A*, **389**, 197–204.
Rutherford, J. S. (1992). *Acta Cryst.* A**48**, 500–508.
Rutherford, J. S. (1993). *Acta Cryst.* A**49**, 293–300.
Rutherford, J. S. (1995). *Acta Cryst.* A**51**, 672–679.
Rutherford, J. S. (2006). *Acta Cryst.* A**62**, 93–97.
Rutherford, J. S. (2009). *Acta Cryst.* A**65**, 156–163.
Sakamoto, M. & Morita, S. (1995). *WSC '95 Proc. 27th Conf. Winter Simul.* pp. 309–315. Washington: IEEE Computer Society.
Schläfli, L. (1950). *Theorie der vielfachen Kontinuität. Gesammelte Mathematische Abhandlungen.* 1st ed., Vol. 1, p. 215. Basel: Birkhäuser.
Sloane, N. J. A. (2008). *The On-Line Encyclopedia of Integer Sequences*, http://www.research.att.com/~njas/sequences/.
Uchida, M. & Matsui, Y. (2000). *Acta Cryst.* B**56**, 654–658.
Xiao, C., Kuznetsov, Y. G., Sun, S., Hafenstein, S. L., Kostyuchenko, V. A., Chipman, P. R., Suzan-Monti, M., Raoult, D., McPherson, A. & Rossmann, M. G. (2009). *PLoS Biol.* **7**, e1000092.