Diatonic Interval Cycles and Hierarchical Structure

John Clough

This paper extends and generalizes my work on diatonic circles published some years ago in this journal.[1] In the earlier work I showed that cycles of scale degrees based on a single generic interval (seconds up/sevenths down, or thirds up/sixths down, or fourths up/fifths down, and so on) may be linked in any order by means of an appropriate sequence of "rhythmic" operators. Here I study a particular class of linked cycles—those formed with a *single* operator—and generalize the results to scales of any odd prime cardinality. As I will try to show by means of a brief analysis, this approach highlights certain hierarchical features of Western tonal music. I will attempt to suggest, as well, some implications for the design of microtonal systems.

In the discussion of scales of more or less than seven notes, the reader may wonder how these scales are tuned, and in what larger chromatic scales they are embedded, if any. The scope here is very broad: if scales are conceived as collections of notes wherein intervals are classified on the basis of diatonic length—analogously to the usual case where, for example, minor and major thirds, though different, are members of the class "third"—then the results of this paper are valid for all scales of odd prime cardinality.

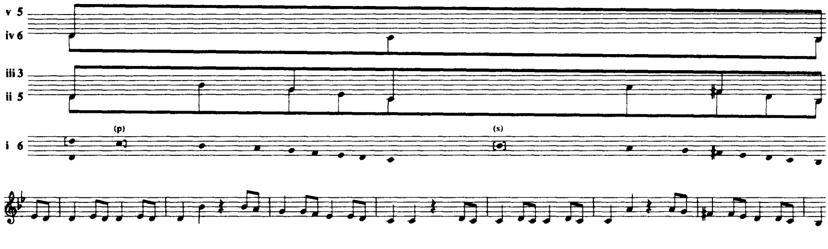
The immediate stimulus for resuming this investigation is Jay Rahn's recent discussion of interval "bisection" in certain scales.[2] In a later section of this paper I will comment on the relationship between Rahn's work and the present effort.

Scale-Degree Cycles and Transformations

I begin by reviewing and recasting my earlier work. Scale degrees are numbered consecutively upwards, using the integers 0, 1, 2, ... By ***interval*** I mean the distance from one scale degree to another, measured in upward scale steps: for a set of n scale degrees, the interval from scale degree a to scale degree b is defined as $b - a \pmod{n}$. For example, if the notes of the C-major set are numbered C = 0, D = 1, . . . , B = 6, then the interval from C to B is $6 - 0 \equiv 6 \pmod{7}$, and the interval from G to E is $2 - 4 \equiv -2 \equiv 5 \pmod{7}$.[3] Intervals are usually represented by nonnegative integers $0, 1, \ldots, n - 1 \pmod{n}$, but in some cases (e.g., inversion) negative integers are useful. As we shall not be concerned with concepts of tonic, dominant, and the like, the assignment of zero to a particular note of a scale has no special significance.

Example 1 shows a typical case of hierarchical structure in Western classical music. In the first few bars of the first theme of Mozart's Symphony no. 40 in G minor, level i, the surface, consists entirely of downward intervals of one step or upward intervals of six steps (in traditional terms, downward seconds/upward sevenths), except for two places where an implied passing note (P) or suspension (S) may be heard to maintain the stream of such intervals. Each of the higher structural levels, ii–v, arises from special attention to alternate notes of the next lower level, and consists entirely of a single interval, given as a positive integer at the left of each level.

Regarding Example 1, objections may be raised at once to (1) the imagined (P) and (S), (2) the special attention to alternate notes, especially at level iii, (3) the inclusion of the nondiatonic F♯, and (4) the fact that certain successions are not consistent with either voice-leading rules or arpeggiation (e.g., F♯–B♭ at level iii). I believe that these objections may be convincingly countered, but to do so would require a lengthy discussion not germane to the present purpose. So in order to get on with the project at hand, I ask the reader to accept my reading of the example as a hypothesis.



EXAMPLE 1

Note that exactly half of the six nonzero intervals (3, 5, and 6) are represented in the analysis of Example 1. As we move up from level i through levels ii and iii and go on to level iv, the hierarchy begins to repeat itself: if there were one more level higher than level v, based on the same process of alternate-note selection, that level would consist of interval 3, completing a repetition of the pattern of levels i–iii. Thus Example 1 exhibits three distinct interval-to-interval transitions: moving up from level i, we find 6 → 5, 5 → 3, and 3 → 6 before encountering the aforementioned repetition. We will see later what lies behind this particular pattern. For now, let us ask a more general question growing out of the example.

Since there are six distinct nonzero intervals (mod 7), it is reasonable to think there are thirty-six possible ordered pairs of intervals that may occur as representatives of two successive levels of a hierarchy (moving either up or down the hierarchy, and allowing the case where two successive levels are based on the same interval). The potential for any stated transition to be realized depends, of course, on the rules of construction. The hierarchy of Example 1 may be conceived in either direction. If we start at level i, next to the surface, each next-higher level is generated by a process which I call "extraction." If instead we start at level v and move down the hierarchy, each next-lower level is generated by what I call "interpolation" of "passing" notes such that the newly generated intervals are all identical. In Example 1, the "rhythm" of extraction is binary: in moving to the next-higher level, every second note is extracted, yielding half as many notes; in moving down, a "passing" note is inserted between the two notes of each adjacent pair, yielding twice as many notes (with allowances for terminating the process without "left-over" notes at the beginning and end).

Now the general question. Suppose the rules of construction allow extraction of every *g*th note from the next-lower level or interpolation of *g* notes between every adjacent pair of notes in the next-higher level, *g* being any positive integer. (The reason for using *g* as a variable name here will soon become clear.) May all thirty-six possible ordered pairs of intervals appear in hierarchies so fashioned? As I showed in my earlier work, the answer is yes. My method was to construct what amounts to a generalized interval system (GIS) as defined by David Lewin,[4] and I now recast the earlier work in his terms, which I trust will be familiar to many readers. As this is a very simple GIS, I believe that readers unfamiliar with Lewin's work will nevertheless be able to grasp the essential points.[5]

Let $S = \{s_1, s_2, s_3, s_4, s_5, s_6\}$ be the space of $\text{GIS}_7 = \{S, G, \text{int}\}$, where each member of S is an indefinitely extended sequence of scale degrees generated by repetition of a single nonzero interval:

$$
\begin{aligned}
s_1 &= \ldots 0, 1, 2, 3, 4, 5, 6, 0, 1, 2, 3, 4, 5, 6, 0, \ldots, \\
s_2 &= \ldots 0, 2, 4, 6, 1, 3, 5, 0, 2, 4, 6, 1, 3, 5, 0, \ldots, \\
&\;\cdot \\
&\;\cdot \\
&\;\cdot \\
s_6 &= \ldots 0, 6, 5, 4, 3, 2, 1, 0, 6, 5, 4, 3, 2, 1, 0, \ldots .
\end{aligned}
$$

The integers 0–6 in each s_i represent the seven scale degrees while the i of s_i represents the generating interval. Each s_i is thus a *circle* of i's (e.g., the traditional circle of descending diatonic fifths) that produces a *cycle* of seven scale degrees, indefinitely repeated.

Let the group of intervals for GIS_7 be $G = \{1, 2, 3, 4, 5, 6\}$ with multiplication modulo 7. (The fact that seven is a prime number is crucial here; this point will be taken up later.) The distance from one member of S to another, reckoned multiplicatively, is some member of G. For example, the distance from s_2 to s_1 is 4, by multiplication modulo 7 ($2 \cdot 4 \equiv 1 \pmod 7$): when we multiply each scale degree in s_2 by 4 (mod 7), we obtain s_1. Note that, although the set G contains the same numbers that appear as subscripts in s_1, s_2, and so on, the intervals of G—the multiplicative distances—are not the same as the intervals that occur between the scale degrees of s_1, s_2, and so on. To get from, say, scale degree 1 to scale degree 3 in s_2, we ***add*** 2; to get from s_1 to s_2, we ***multiply*** by 2. To keep this distinction clear, I shall refer to intervals from one scale degree to another as "intervals" and to the intervals of G as "group-intervals."

To complete the construction of GIS_7, it now remains to specify formally the function int, which assigns a member of G to each member of the Cartesian product of S. For any s_i, s_j ($i = j$ is permitted), we have

$$\mathrm{int}(s_i, s_j) \cdot i \equiv j \pmod{7}$$

and

$$\mathrm{int}(s_i, s_j) \equiv ji^{-1} \equiv i^{-1}j \pmod{7}$$

(since G is commutative). (In this context, the inverse of i, written i^{-1}, is that number which, when multiplied by i, yields 1, mod 7.) For example, we find the interval from s_4 to s_5 as follows:

$$\mathrm{int}(s_4, s_5) \equiv 5 \cdot 4^{-1} \equiv 5 \cdot 2 \equiv 3 \pmod{7}.$$

The result of this computation tells us that the group-interval from s_4 to s_5 is 3. Perhaps it is easier to see what this means if we think in terms of transformations instead of group-intervals.[6] The transformation which takes us from s_4 to s_5 is "extraction of every third note" (here is the "3" of the above result) from s_4:

$$\ldots \underline{0}, 4, 1, \underline{5}, 2, 6, \underline{3}, 0, 4, \underline{1}, 5, 2, \underline{6}, 3, 0, \underline{4}, 1, 5, \underline{2}, 6, 3, \underline{0}, \ldots.$$

The group-intervals of G correspond to transformational "rhythms" of extraction—each g in G represents the taking of every gth note from a member of S. These transformations compose according to multiplication modulo 7. Suppose, for example, we pass through s_5 on the way from s_4 to s_1. We already know that $\mathrm{int}(s_4, s_5) \equiv 3 \pmod{7}$. So

$$\mathrm{int}(s_4, s_1) \equiv \mathrm{int}(s_4, s_5) \cdot \mathrm{int}(s_5, s_1) \equiv 3 \cdot (5^{-1} \cdot 1) \equiv 3 \cdot 3 \equiv 2 \pmod{7}.$$

This tells us that if we take every third note of s_4, and then every third note of the resulting s_5, we get s_1, as shown by single and double underlining below:

$$\ldots \underline{\underline{\overline{0}}}, 4, \overline{1}, \underline{5}, \overline{2}, 6, \underline{\overline{3}}, 0, \overline{4}, \underline{\underline{1}}, \overline{5}, 2, \underline{\overline{6}}, 3, \overline{0}, \underline{4}, \overline{1}, 5, \underline{\underline{\overline{2}}}, 6, \overline{3}, \underline{0}, \ldots.$$

And since $\mathrm{int}(s_4, s_1) \equiv 2 \pmod{7}$, we can also get s_1 by extracting every other note, as shown by overlining above. These are just two of many paths from s_4 to s_1.

What about interpolation of "passing" notes? It is easy to see from the above that if we want to go from s_5 to s_4 by interpolation, we can do it by inserting 2 notes between each adjacent pair of s_5, such that the resulting note-to-note intervals are all equivalent (mod 7), thus tripling the number of notes. Clearly int(s_4, s_5) and int(s_5, s_4) are inverses in the sense that, speaking transformationally, $s_5 \rightarrow s_4$ "undoes" the operation $s_4 \rightarrow s_5$. They are inverses in the mathematical sense too. That is to say,

$$\text{int}(s_4, s_5) \equiv \text{int}(s_5, s_4)^{-1}$$
$$3 \equiv (5^{-1} \cdot 4)^{-1} \equiv (3 \cdot 4)^{-1} \equiv 5^{-1} \pmod 7.$$

Thus we can go from s_5 to s_4 either by extracting every fifth ($5^{-1} \cdot 4 \equiv 5$) note from s_5 or by adding passing notes to increase the number of notes by a factor of $5^{-1} \equiv 3$.

All of this may be nicely summarized by the table for multiplication modulo 7, with products reduced to smallest positive integers (mod 7):

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

From the table we read, for example, $4 \cdot 2 \equiv 1 \pmod 7$, indicating that we can go from s_4 to s_1 by taking every second note of s_4 or by interpolating notes in the ratio of 4 ($\equiv 2^{-1}$) : 1, that is, by adding three passing notes between each two adjacent notes:

$$\begin{array}{ll} s_1: & \ldots 012345601234560123456012345601234 \ldots \\ s_4: & \ldots 0 \quad 4 \quad 1 \quad 5 \quad 2 \quad 6 \quad 3 \quad 0 \quad 4 \ldots \\ s_1: & \ldots 0 \qquad\quad 1 \qquad\quad 2 \qquad\quad 3 \qquad\quad 4 \ldots \end{array}$$

The properties of G dictate that for any g, h in G, the congruence $g \cdot x \equiv h$ has a unique solution in G. It follows that we can go *from* any particular member of S *to* any particular member of S by means of a unique member of G, interpreted as either an extraction or an interpolation "rhythm." This answers the general question raised above and completes the review and recasting of my earlier work.

Exhaustive Cycles of Intervals

The mathematically knowledgeable reader will have noticed that the properties of GIS_7 rest on the fact that seven is a prime number, since, for any positive integer n, the set $\{1, 2, \ldots, n-1\}$ forms a mathematical group under multiplication (mod n) if and only if n is prime. (Here and elsewhere in this paper, the integer one is regarded as nonprime.) Also, each of the sequences $s_1, s_2, \ldots, s_{n-1}$, as defined above, contains all n scale degrees if and only if n is prime.

It will be useful to understand the last statement more formally. By way of the usual definition, a set of integers $R = \{a_1, a_2, \ldots, a_n\}$ is a *complete system of residues* (mod n) if every integer is congruent (mod n) to exactly one member of R. Thus the simplest example of a complete system of residues (mod n) is the set $\{0, 1, \ldots, n-1\}$. It is not difficult to see that if a is one of the numbers $1, 2, \ldots, n-1$, then for all a, the sequence $0a, 1a, 2a, \ldots, (n-1)a$ (mod n) forms a complete system of residues (mod n) if and only if n is prime. It is for this reason that each of the six s_n in GIS_7 contains all seven scale degrees. Thus scales of prime cardinality constitute a special class, and I restrict my attention to them in the present paper.

Let p be any prime. From the above it is clear that we can construct $\text{GIS}_p = \{S, G, \text{int}\}$, where S is the set of cycles generated by each one of the intervals $\{1, 2, \ldots, p-1\}$, G is the group consisting of the same set of integers under multiplication (mod p), and int is defined as above. All of the results in this paper may be cast in terms of such GISs, and readers are invited to rehearse the results in that framework.

In the above discussion, the members of S are conceived as different cyclic *orderings* of the pcs, and the members of the group G are intervals corresponding to the operations of extraction and interpolation, which take us from one cyclic ordering to another. There are other interpretations of S and G. Assuming that p is prime, they may be taken, respectively, as the complete set of p pcs and the group of $p-1$ multiplicative transformations performed on the pcs. Or S may be taken as the set of singular, abstract nonzero intervals $\{1, 2, \ldots, p-1\}$, with corresponding reinterpretation of G. As far as the central ideas of this paper are concerned, it makes no difference which of these interpretations we choose, but, in order to maintain a consistent discourse, I will speak of S and G as described at the beginning of this paragraph.

Returning to Example 1 for a moment, recall that the intervals in the hierarchy form a cycle with an almost complete repetition: $6 \rightarrow 5 \rightarrow 3 \rightarrow 6 \rightarrow 5$, reading from foreground to background. Each next-higher level is gained by means of the *same* transformation—extraction of every second note from the previous level (or multiplication by

2). It is cycles of this kind—formed by a *single* transformation—that we are concerned with in this paper. Note that these cycles of ***intervals*** are different from the cycles of ***scale degrees*** which are members of S.

A word on notation and terminology: In notations such as $6 \rightarrow 5 \rightarrow 3 \rightarrow 6 \rightarrow 5$, the numbers represent ***intervals*** (conceived as single intervals or note-to-note intervals of the corresponding s_n in S) and the arrows represent ***group-intervals*** or ***transformations.*** Unless otherwise noted, in any particular series of numbers connected by arrows, the arrows represent the ***same*** group-interval or transformation. Because of this constraint, the sequences of transformations studied in this paper have the potential to generate repeated cycles of intervals (in fact this property is at the heart of the investigation). Therefore I refer to any production based on a single group-interval or transformation, such as $6 \rightarrow 5 \rightarrow 3 \rightarrow 6 \rightarrow 5$, as *cyclic* whether or not a complete repetition is present.

We now lift the cyclic structure $6 \rightarrow 5 \rightarrow 3 \rightarrow 6 \rightarrow 5$ out of the context of the Mozart analysis and make an alternative interpretation of it, as suggested earlier. If each of the numbers 6, 5, and 3 is taken to represent a ***single*** abstract interval in the seven-note scale, instead of a sequence of scale degrees generated by that interval, we can read the information to indicate that any of the intervals 6, 5, and 3, is capable of being divided into two equal parts (remembering that the arrows here represent multiplication by 2). Thus, reading backwards, interval 5 ($\equiv$ 12) bisected becomes interval 6, 6 becomes 3, 3 becomes 5, and we have translated the statement about hierarchies in Mozart to say something about the seven-note diatonic scale in the abstract, to which we now turn our attention.

Adopting Jay Rahn's term, I will say that an interval $a \neq 0$ is ***bisected*** by an interval b (mod n) if and only if $a \equiv 2b$ (mod n). This avoids complications that arise in attempting to define division (mod n). Note that, for n odd, if $a \equiv 2b$ (mod n), then $b \equiv 2^{-1}a$ (mod n). If 6, 5, and 3 can be bisected, what about the other nonzero intervals in the seven-note scale? They too can be bisected: 4 bisected becomes 2, 2 becomes 1, and 1 ($\equiv$ 8) becomes 4. The two cycles

$$\ldots 6 \rightarrow 3 \rightarrow 5 \rightarrow 6 \ldots$$

$$\ldots 1 \rightarrow 4 \rightarrow 2 \rightarrow 1 \ldots$$

jointly exhaust the set of nonzero intervals $\{1, 2, \ldots, 6\}$. Rahn observes that if the nonzero intervals are paired as additive inverses (mod 7) to form the three interval classes (1, 6), (2, 5), (3, 4), then each of the two cycles $\ldots 6 \rightarrow 3 \rightarrow 5 \rightarrow 6 \ldots$ and $\ldots 1 \rightarrow 4 \rightarrow 2 \rightarrow 1 \ldots$ runs through all three interval classes, including one member from each class in a complete cycle. Calling this "cycling in precise halves" (with reference to the bisection of intervals), he goes on to address the question of which scalar cardinalities allow cycling in precise halves, where a complete cycle includes one or both members of each intervals class. I shall give his result below, but in order to develop the material of this paper in logical sequence, I first pose another question that is at the same time broader and narrower than Rahn's.

Which scalar cardinalities support a cycle comprising all nonzero *intervals* $1, 2, \ldots, n - 1$ (i. e., both members of each interval class) and based entirely on bisection? Mathematically, this amounts to asking the following question: for which odd primes p does the set $\{2, 2^2, 2^3, \ldots, 2^{p-1}\}$ form a reduced system of residues (mod p)? For any n, the members of a complete system of residues (mod n) that are relatively prime to n constitute a *reduced system of residues* (mod n); so for any prime p, the set $\{1, 2, \ldots, p - 1\}$ is a reduced system of residues (mod p). A partial answer to the above question is that $p = 3$ works, and so does $p = 5$:

$$2 \equiv 2, 2^2 \equiv 4, 2^3 \equiv 3, 2^4 \equiv 1 \pmod 5.$$

But, as the previous discussion of the seven-note scale suggests, $p = 7$ does not.

It is conceivable that powers of 2 might cycle through all the nonzero intervals in haphazard fashion with respect to the interval classes (e.g., hitting some interval classes twice before hitting all of them once). However, I will soon show that, for any odd prime cardinality, if a cycle includes all $n - 1$ nonzero intervals, it includes each of them once, cycling twice through the $(n - 1)/2$ interval classes and thus satisfying Jay Rahn's condition.

Having restricted Rahn's question, I now broaden it to include not only bisection, but division of intervals into any fixed number of equivalent parts. This amounts to asking: for which primes p and integers a does the set $\{a, a^2, a^3, \ldots, a^{p-1}\}$ form a reduced system of residues (mod p)? Mathematicians cannot answer this question generally, but they can tell us quite a lot about it, and we need only a modest amount of elementary number theory to understand it.

The number of distinct integers in a reduced residue system (mod n) is important here. This number is known as *Euler's Φ function*. For example, 1, 3, 7, and 9 are all the distinct residues (mod 10) relatively prime to 10, so $\Phi(10) = 4$. Obviously, for any prime p, $\Phi(p) = p - 1$, and for any composite n, $\Phi(n) < n - 1$.

A second necessary concept here has to do with the congruence $a^k \equiv 1$ (mod n). If $(a, n) \neq 1$, there is no k which satisfies $a^k \equiv 1$ (mod n).[7] But given $(a, n) = 1$, there is some k which satisfies this congruence, and we are interested in the smallest positive integer k which does so. This number goes by various names; I will call it the *period of a* (mod *n*), and write $\mathrm{per}_n(a) = k$. For example, given $a = 9$, $n = 10$, we find $9^2 = 81 \equiv 1$ (mod 10). As there is no exponent smaller than 2 which works, the period of 9 (mod 10) is 2, that is, $\mathrm{per}_{10}(9) = 2$. For our purposes, the main significance of this notion lies in the following well-known theorem.

THEOREM 1. *If* $\mathrm{per}_n(a) = k$, *the numbers* $a, a^2, a^3, \ldots, a^k$ *are all distinct* (mod *n*).

Proof. Suppose that for integers i and j, $1 \leq i < j \leq k$, $a^i \equiv a^j$ (mod n). Then $a^{j-i} \equiv 1$ (mod n). Since $j - i < k$, this contradicts the hypothesis $\mathrm{per}_n(a) = \mathrm{k}$.

If $\mathrm{per}_n(a) = \Phi(n)$, we say that a is a *primitive root* (mod n). For example, $3^4 = 81 \equiv 1$ (mod 10), and 4 is the smallest k for which $3^k \equiv 1$ (mod 10), so $\mathrm{per}_{10}(3) = 4 = \Phi(10)$, and therefore 3 is a primitive root (mod 10). Since for any prime p, $\Phi(p) = p - 1$, an integer a is a primitive root (mod p) if and only if $k = p - 1$ is the smallest integer satisfying $a^k \equiv 1$ (mod$p$), that is to say, if and only if $\mathrm{per}_p(a) = p - 1$. For example, the smallest integer satisfying $2^k \equiv 1$ (mod 5) is $4 = 5 - 1$, so 2 is a primitive root (mod 5). It is easy to see that for any composite n and any integer a, $(a, n) = 1$, $\mathrm{per}_n(a) < n - 1$; so if we are given $\mathrm{per}_p(a) = p - 1$, then p is prime and a is a primitive root mod p).[8]

We are now in a position to understand cycles which exhaust the nonzero intervals.

THEOREM 2. *The number p is a prime and g is a primitive root* (mod *p*) *if and only if the numbers* $g, g^2, \ldots, g^{p-1}$ *are all distinct* (mod *p*).

Proof. If the numbers $g, g^2, \ldots, g^{p-1}$ are all distinct (mod p), none of them can be congruent to zero (mod p) (via elementary number theory). Therefore one of them must be congruent to one (mod p). This number must be g^{p-1}, else the numbers would not all be distinct (mod p). Thus $\mathrm{per}_p(g) = p - 1$, implying p is prime and g is a primitive root (mod p).

Conversely, if p is a prime and g is a primitive root (mod p), then $\mathrm{per}_p(g) = p - 1$ and, by Theorem 1, the numbers $g, g^2, \ldots, g^{p-1}$ are all distinct (mod p).

The significance of Theorem 2 here is that for a scale of prime cardinality p, the group-intervals (transformations) of GIS_p that run through all the nonzero intervals in a complete cycle are precisely the primitive roots of p.[9] All prime numbers have primitive roots, but, as suggested above, there is no formula that generates the primes that have, say, 2 as a primitive root, although there are tests that rule out certain primitive roots for certain classes of primes. For example, if $p \equiv \pm 1 \pmod 8$, then 2 is not a primitive root (mod p). So in the familiar diatonic case ($p = 7$), 2 is not a primitive root (mod 7), as evidenced by the cycle $1 \rightarrow 2 \rightarrow 4 \rightarrow 1$ discussed above. The numbers $2, 2^2, 2^3, \ldots, 2^{p-1}$ include 1, 2, and 4 (twice each, mod 7), but not 3, 5, or 6. Since 2 is not a primitive root (mod 7), neither is 4, its multiplicative inverse (mod 7). (If $ab \equiv 1$ (mod n), a and b are said to be ***multiplicative inverses*** (mod n), and we write $a = b^{-1}$ (mod n); e. g., $2 = 4^{-1}$ (mod 7).) But 3 is a primitive root (mod 7):

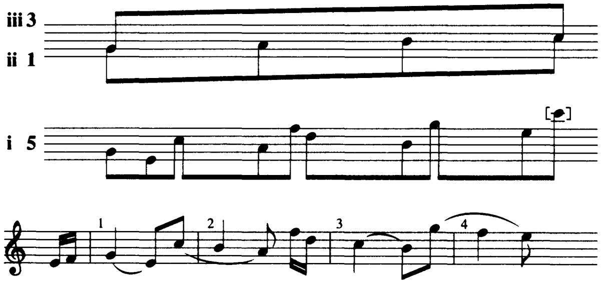
$$3 \equiv 3,\ 3^2 \equiv 2,\ 3^3 \equiv 6,\ 3^4 \equiv 4,\ 3^5 \equiv 5,\ 3^6 \equiv 1 \pmod 7,$$

or, in "arrow" notation:

$$3 \rightarrow 2 \rightarrow 6 \rightarrow 4 \rightarrow 5 \rightarrow 1,$$

where the arrows represent multiplication by 3 (mod 7). Therefore 5, the multiplicative inverse of 3 (mod 7), is also a primitive root (mod 7) and these are the only distinct residues which are primitive roots (mod 7).

This tells us that it is possible to generate the entire space of GIS_7 by means of a single transformation corresponding to multiplication by either 3 or 5 (mod 7). Curiously, this potential does not seem to be exploited in traditional Western music. Various explanations might be advanced to account for this omission (such a hierarchy would be beyond perception; many repetitions of the same group-interval would be boring; there are serious problems with registration.) The fact is that when group-interval 3 is applied more than once, consecutively, in a hierarchy, it is (so far as I have been able to discover) applied just twice, yielding a "hemisphere" of three intervals so connected. Example 2 shows such a reading of a phrase from the opening of the fourth movement of Haydn's Symphony no. 97 in C major. Omitting the anacrustic sixteenths and the appoggiaturas on the downbeats of bars 2–4, and adjoining the high "C" from the beginning of the next phrase, yields level i, where interval 5 (descending thirds/ascending sixths) is presented in the form of four successive melodic "chords of the sixth," the first and second related conjunctly, the second and third related disjunctly, the third and fourth related again conjunctly. Levels ii and iii are each based on extraction of every third note from the next lower level.[10]



EXAMPLE 2

It remains to show, as claimed above, that, for any odd prime cardinality, a cycle which exhausts the nonzero intervals comprises two cycles of interval classes. Theorems 3, 4, and 5 lead to this result and lay the groundwork for investigation of another kind of cycle in the next section. Theorem 3, given without proof, may be found in most textbooks on elementary number theory.

THEOREM 3. *If* $(a, n) = 1$ *and for some* $k > 0$, $a^k \equiv 1 \pmod{n}$, *then* $\mathrm{per}_n(a)$ *divides* k. *Conversely, if* $\mathrm{per}_n(a)$ *divides* k, *then* $a^k \equiv 1 \pmod{n}$.

THEOREM 4. *Let* p *be a prime and let* $k = \mathrm{per}_p(a)$. *If* k *is even, then* $a^{k/2} \equiv -1 \pmod{p}$ *and conversely. If* k *is odd, then for all integers* i, $1 \leq i \leq k-1$, $a^i \not\equiv -1 \pmod{p}$ *and conversely.*

Proof. Suppose k is even. Then $a^{k/2} \equiv \pm 1 \pmod{p}$ (for p prime, $n^2 \equiv 1 \pmod{p}$ implies $n \equiv \pm 1 \pmod{p}$, via elementary number theory). But $a^{k/2} \equiv +1 \pmod{p}$ contradicts the hypothesis $k = \mathrm{per}_p(a)$; therefore $a^{k/2} \equiv -1 \pmod{p}$. Conversely, if $a^{k/2} \equiv -1 \pmod{p}$, then there is an integer $i = k/2$, $1 \leq i \leq k-1$, such that $a^i \equiv -1 \pmod{p}$, and $k = 2i$ is even.

Now suppose k is odd and $a^i \equiv -1 \pmod{p}$. Then $a^{2i} \equiv 1$, implying $k \mid 2i$ (Theorem 3). Since $i < k$, $k \mid 2i$ implies $k = 2i$, $k/2$ is an integer, and k is even, contradicting the supposition k is odd. Conversely, if for all integers i, $1 \leq i \leq k-1$, $a^i \not\equiv -1 \pmod{p}$, then k must be odd, else $a^{k/2} \equiv -1 \pmod{p}$.

THEOREM 5. *Let p be a prime. If $k = \mathrm{per}_p(a)$ is even, then for all integers i,*

$$a^{k/2+i} \equiv -a^i \pmod{p}.$$

The converse is also true.

Proof. The theorem follows as a corollary of Theorem 4: Since k is even, $a^{k/2} \equiv -1 \pmod{p}$. Multiplying both sides by a^i yields $a^{k/2+i} \equiv -a^i \pmod{p}$. Conversely, multiplying both sides of this congruence by a^{-i} yields $a^{k/2} \equiv -1 \pmod{p}$, implying $k = \mathrm{per}_p(a)$ is even.

After one more definition, we are ready to apply the results of Theorems 2 and 5 so as to see the potential structure of hierarchical systems based on primitive roots. If S is a complete residue system (mod n), then we say that the set S', consisting of all elements of S except 0 (mod n), is *a complete system of nonzero residues* (mod n). Note that a reduced residue system (mod n) is a complete system of nonzero residues (mod n) if and only if n is prime.

THEOREM 6. *If p is an odd prime and a is a primitive root* (mod p), *then*

(1) *the numbers $a, a^2, \ldots, a^{p-1}$ form a complete system of nonzero residues* (mod p), *and*
(2) *$(p-1)/2$ is an integer and, for all integers i, $a^{(p-1)/2+i} \equiv -a^i$* (mod p).

The converse is also true: statements (1) and (2) together imply that p is an odd prime and a is a primitive root (mod p).

Proof. Statement (1) follows from the hypotheses via Theorem 2. The hypotheses also imply $\mathrm{per}_p(a) = \Phi(p) = p - 1$ is even, and statement (2) follows by Theorem 5.

Conversely, statement (1) implies p is prime and a is a primitive root (mod p), via Theorem 2, and statement (2) implies p is odd.

Note that statement (2) of Theorem 6, by itself, implies neither that p is prime nor that the numbers $a, a^2, \ldots, a^{p-1}$ are distinct (mod p). For example, statement (2) is satisfied by $p = 15$, $a = 14$.

Theorem 6 might be enlarged to accommodate the case $p = 2$. But this case is degenerate in that it contains just one interval class and hence no pairs of interval classes that are distinct (mod 2). It therefore seems reasonable to state Theorem 6 in the simpler version given here.

Theorem 6 allows us to see how a single cycle of all nonzero intervals comprises a double cycle of all interval classes. For any odd prime p, let us define the *set of interval classes* (mod p) ICSp = $\{(1, p-1), (2, p-2), \ldots, ((p-1)/2, p-(p-1)/2)\}$ to be the reduced system of residues (mod p) in pairs of additive inverses (mod p), or, in musical terms, the set of interval classes excluding interval 0. (We may think of an interval class as the distance between two distinct ***unordered*** scale degrees.) Now consider the sequence $g, g^2, \ldots, g^{p-1}$ based on the primitive root g. Halfway through it we reach $g^{(p-1)/2} \equiv -1$ (mod p), and each of the $(p-1)/2$ remaining terms $g^{(p-1)/2+i}$, including the final term $g^{p-1} \equiv 1$, will be the negative (i.e., the additive inverse (mod p)) of its counterpart g^i in the first half of the sequence. For example, let $p = 11$ and $g = 2$. Then

$$g, g^2, \ldots, g^{p-1} =$$

$$2, \quad 4, \quad 8, \quad 5, \quad 10\ (\equiv -1),$$

$$9\ (\equiv -2), 7\ (\equiv -4), 3\ (\equiv -8), 6\ (\equiv -5), 1\ (\equiv -10 \equiv -(-1))\ (\text{mod } 11),$$

and the first five terms and second five terms are related by inversion.

Cycles of Interval Hemispheres

In the preceding section we were concerned with situations where a particular transformation (bisection, trisection, and so forth) generates *all* the nonzero intervals in a single cycle. As noted, such transformations are based on primitive roots. In this section we look at cases where a repeated transformation generates only *some* of the nonzero intervals—in particular, exactly *half* of them—a *hemisphere* of intervals. As we will see, if per$_p(a) = (p-1)/2$, then p is a prime; therefore the inquiry is necessarily restricted to scales of prime cardinality.

Let p be a prime and g a primitive root (mod p). Then per$_p(g) = p - 1$. Now suppose $(a, p) = 1$, but a is not a primitive root (mod p). Then, by Theorem 3, we see that the largest value that per$_p(a)$ can have is $(p-1)/2$. That is to say, the smallest integer k satisfying $a^k \equiv 1$ (mod p) cannot be larger than $(p-1)/2$. More generally, since per$_p(a)$ always divides $\Phi(p) = p - 1$, the possible values for per$_p(a)$ are $(p-1)/2$, $(p-1)/3$, $(p-1)/4$, and so forth. It is easy to see that if p is a prime, $(a, p) = 1$, and k does not divide $p - 1$, then per$_p(a) \neq k$.

HORIZONTAL CYCLES

Let us study the case $\mathrm{per}_p(a) = (p-1)/2$. (I am tempted to say that a is a *semiprimitive* root in this case.) From Theorem 1, we know that the series a, a^2, . . . $a^{(p-1)/2}$ yields $(p-1)/2$ distinct numbers (mod p). From the discussion of the Mozart example above, we know that the powers of 2 are 2, 4, and 1 (mod 7): $2^1 \equiv 2$, $2^2 \equiv 4$, and $2^{3=(p-1)/2} \equiv 1$ (mod 7), after which the cycle repeats. So $\mathrm{per}_7(2) = 3 = (7-1)/2$. As noted, the other three nonzero intervals (mod 7), namely, 3, 5, and 6, can also be bisected to form a second sequence of three intervals. If we start with -2 instead of $+2$ and multiply repeatedly by 2 we have

$$5\ (\equiv -2),\ 3\ (\equiv 2 \cdot 5 \equiv -4),\ 6\ (\equiv 2 \cdot 3 \equiv -1)\ (\mathrm{mod}\ 7).$$

Multiplying each of the intervals 2, 4, 1, by -1 amounts to the same thing:

$$2 \cdot -1 \equiv 5\ (\equiv -2),\ 4 \cdot -1 \equiv 3\ (\equiv -4),\ 1 \cdot -1 \equiv 6\ (\equiv -1)\ (\mathrm{mod}\ 7),$$

so we have produced the "inversion" (i.e., the additive inverses, in corresponding order). Note the two interval hemispheres: the cycle $2 \rightarrow 4 \rightarrow 1$ includes one interval from each of the interval classes in $\mathrm{ICS}_7 = \{(1, 6), (2, 5), (3, 4)\}$, and the "inverse" cycle $5 \rightarrow 3 \rightarrow 6$ includes the remaining interval from each pair in ICS_7. Cycles such as these, which cut across ICS_p, I call *horizontal* cycles. They arise under particular conditions, as the following theorem shows.

THEOREM 7. *Let* $A = \{a, a^2, \ldots, a^{(p-1)/2}\}$ *and* $A' = \{-a, -a^2, \ldots, -a^{(p-1)/2}\}$. *If* $p \equiv 3$ (mod 4) *is prime and* $\mathrm{per}_p(a) = (p-1)/2$, *then*

(1) *A and A' are disjoint* (mod p), *and* $(A \cup A')$ *is a complete system of nonzero residues* (mod p); *and*

(2) *for all integers i,* $a^i \equiv a^{(p-1)/2+i}$ (mod p), *hence* $-a^i \equiv -a^{(p-1)/2+i}$ (mod p).

The converse is also true: (1) *and* (2) *together imply* $p \equiv 3$ (mod 4) *is prime and* $\mathrm{per}_p(a) = (p-1)/2$.

Proof. Since $p \equiv 3$ (mod 4), $(p-1)/2$ is odd; therefore -1 (mod p) $\notin A$, by Theorem 4. It follows that, for all integers i, $-a^i \notin A$, and $a^i \notin A'$; hence A and A' are disjoint (mod p). Thus A and A' each include

$(p-1)/2$ distinct elements (mod p), and $(A \cup A')$ includes $p-1$ distinct elements (mod p). Since $\mathrm{per}_p(a)$ exists, $(a, p) = 1$, and 0 (mod p) $\notin (A \cup A')$, and the second part of statement (1) follows. Statement (2) follows directly from $\mathrm{per}_p(a) = (p-1)/2$.

Conversely, statement (1) implies that A and A' each include $(p-1)/2$ distinct elements (mod p); thus $\mathrm{per}_p(a) \geq (p-1)/2$. And $\mathrm{per}_p(a)$ divides $p-1$; therefore either $\mathrm{per}_p(a) = (p-1)/2$ or $\mathrm{per}_p(a) = (p-1)$. But $\mathrm{per}_p(a) = (p-1)$ contradicts statement (2); so $\mathrm{per}_p(a) = (p-1)/2$. Statement (2) implies 1 (mod p) $\in A$ and -1 (mod p) $\notin A$. Then, by Theorem 4, $\mathrm{per}_p(a) = (p-1)/2$ is odd, and $p \equiv 3 \pmod 4$. Since $\mathrm{per}_p(a) = (p-1)/2$, each member of A is coprime with p; it follows that each member of A' (which contains the additive inverses (mod p) of all elements in A) is coprime with p. Thus there exist $p-1$ distinct numbers (mod p) all coprime with p—that is, a reduced residue system with $p-1$ distinct numbers (mod p)—hence p is prime.

By way of illustration, suppose $p = 11$, $a = 3$. Then

$$a, a^2, \ldots, a^{(p-1)/2} = 3, 9, 5, 4, 1 \pmod{11},$$

a horizontal cycle cutting across $\mathrm{ICS}_{11} = \{(1, 10), (2, 9), (3, 8), (4, 7), (5, 6)\}$. Multiplying each term of 3, 9, 5, 4, 1 by -1 (mod 11) produces the "inversion," another horizontal cycle disjoint from the first:

$$-a, -a^2, \ldots, -a^{(p-l)/2} = 8, 2, 6, 7, 10 \pmod{11}.$$

Multiplying the original horizontal cycle by *any* nonzero residue missing from that cycle produces the inversion of the original cycle, within rotation.[11] Suppose we choose 2 as a multiplier. Then

$$2 \cdot 3 \equiv 6, 2 \cdot 9 \equiv 7, 2 \cdot 5 \equiv 10, 2 \cdot 4 \equiv 8, 2 \cdot 1 \equiv 2 \pmod{11}.$$

VERTICAL CYCLES

We now consider the case $\mathrm{per}_p(a) = (p-1)/2$ with $p \equiv 1 \pmod 4$. It happens that $\mathrm{per}_{17}(2) = 8 = (p-1)/2$. If $p = 17$, $a = 2$, then

$$a, a^2, \ldots, a^{8=(p-1)/2} = 2, 4, 8, 16\ (\equiv -1),$$
$$15\ (\equiv -2), 13\ (\equiv -4), 9\ (\equiv -8), 1\ (\equiv -16 \equiv -(-1) \pmod{17}).$$

Continued multiplication by 2 leads to repetition of the same sequence. But the numbers a, a^2, . . . , $a^{(p-1)/2}$ do not cycle through ICS$_{17}$ = {(1, 16), (2, 15), (3, 14), (4, 13), (5, 12), (6, 11), (7, 10), (8, 9)}. Instead, beginning with $15 \equiv -2$, the "inversion" of 2, 4, 8, 16 unfolds, completing the hemisphere of eight intervals. This is because $a^4 \equiv 16 \equiv -1$, or $a^{(p-1)/4} \equiv -1$. In contrast to the case of horizontal inversion studied above, the numbers 2, 4, 8, 16, 15, 13, 9, 1, include *both* intervals of exactly *half* the pairs in ICS$_p$. Similarly to the case of horizontal inversion, if we choose any nonzero residue r (mod p) not in the original cycle and multiply each term of that cycle by r, we produce all the intervals of the second hemisphere. For example let $r = 3$. Then

$$2 \cdot 3 \equiv 6, 4 \cdot 3 \equiv 12, 8 \cdot 3 \equiv 7, 16 \cdot 3 \equiv 14,$$
$$15 \cdot 3 \equiv 11, 13 \cdot 3 \equiv 5, 9 \cdot 3 \equiv 10, 1 \cdot 3 \equiv 3 \pmod{17}.$$

Thus each of the two cycles of eight intervals exhausts the intervals of half the interval classes in ICS$_{17}$. As such cycles slice ICS$_p$ in half, partitioning it into two disjoint subsets of interval classes, I call them *vertical* cycles. The next theorem shows that this situation occurs under the conditions stated above.

THEOREM 8. *Let* $A = \{a, a^2, \ldots, a^{(p-1)/2}\}$ *and* $A' = \{r \cdot a, r \cdot a^2, \ldots, r \cdot a^{(p-1)/2}\}$, *where r is a nonzero integer not congruent to any member of A* (mod p). *If* $p \equiv 1$ (mod 4) *is prime, and* $\mathrm{per}_p(a) = (p-1)/2$, *then*

(1) *A and A' are disjoint* (mod p), *and* $(A \cup A')$ *is a complete system of nonzero residues* (mod p); *and*

(2) $(p-1)/4$ *is an integer and, for all integers i,* $a^i \equiv -a^{(p-1)/4+i}$ (mod p), *hence* $r \cdot a^i \equiv r \cdot -a^{(p-1)/4+i}$ (mod p).

The converse is also true: (1) *and* (2) *together imply* $p \equiv 1$ (mod 4) *is prime and* $\mathrm{per}_p(a) = (p-1)/2$.

Proof. By hypothesis, $a^{(p-1)/2} \equiv 1$ (mod p). Hence for any integer i, a^i is one of the numbers a, a^2, . . . , $a^{(p-1)/2}$ (mod p). Now let i, j be integers, $1 \le i$, $j \le (p-1)/2$, and suppose $r \cdot a^i \equiv a^j$. Then $r \cdot a^{-i}a^i \equiv a^{-i}a^j$; hence $r \equiv a^{-i}a^j \equiv a^{-i+j}$. But $-i + j$ is an integer, implying r is congruent (mod p) to one of the numbers in A, contradicting the restriction on r. Therefore A and A' are disjoint (mod p), and we have altogether $2 \cdot (p-1)/2 = p-1$ distinct numbers, excluding 0 (mod p) (since $(a, p) = 1$, and $r \neq 0$), which is to say, a complete system of nonzero residues (mod p). This proves statement (1).

Since $p \equiv 1 \pmod 4$, $(p-1)/2$ is even and $(p-1)/4$ is an integer. By Theorem 4 we get $a^{(p-1)/4} \equiv -1 \pmod p$ which yields statement (2) by Theorem 5.

Conversely, from the definition of A and statement (1) it is clear that $\text{per}_p(a) \geq (p-1)/2$. By reasoning as in the proof of Theorem 7 (converse), we see that $\text{per}_p(a) = (p-1)/2$. Further, since $(p-1)/4$ is an integer, $p \equiv 1 \pmod 4$. Since $\text{per}_p(a) = (p-1)/2$, each member of A is coprime with p. Similarly $\text{per}_p(r \cdot a) = (p-1)/2$, so each member of A' is coprime with p. Thus there exist $p-1$ distinct numbers (mod p) all coprime with p, that is, a reduced residue system with $p-1$ distinct numbers (mod p). Hence p is prime.

Theorems 7 and 8 are structured in parallel: in both theorems, (1) describes the partitioning of nonzero residues into two hemispheres and (2) specifies conditions on periodicity and inverses. The theorems reflect important similarities between the two cases. But there is one interesting shared feature not given in both theorems: if r is any residue not included in one hemisphere, then the other hemisphere consists of $r \cdot a$, $r \cdot a^2$, $\ldots$, $r \cdot a^{(p-1)/2} \pmod p$. This feature, given as the definition of A' in Theorem 8, is omitted from Theorem 7, as it seems more important to relate the two hemispheres of that case—where $p \equiv 3 \pmod 4$—on the basis of inversion. Interested readers may satisfy themselves that the proof of this feature given in Theorem 8, both direct and converse, holds for Theorem 7 as well.

To summarize the results thus far, we have distinguished three categories of interval cycles based on a scale of prime cardinality p, and an integer a, $(a, p) = 1$, under particular conditions:

i. Two connected inversionally related, complete cycles of ICS_p within one complete cycle of nonzero intervals. *Condition: a is a primitive root* (mod *p*) (Theorem 6).

ii. Two separate, disjoint inversionally related cycles, each comprised of $(p-1)/2$ intervals including one interval from each member of ICS_p, jointly exhausting the nonzero intervals. *Conditions:* $p \equiv 3$ (mod 4) *and* $\text{per}_p(a) = (p-1)/2$ (Theorem 7).

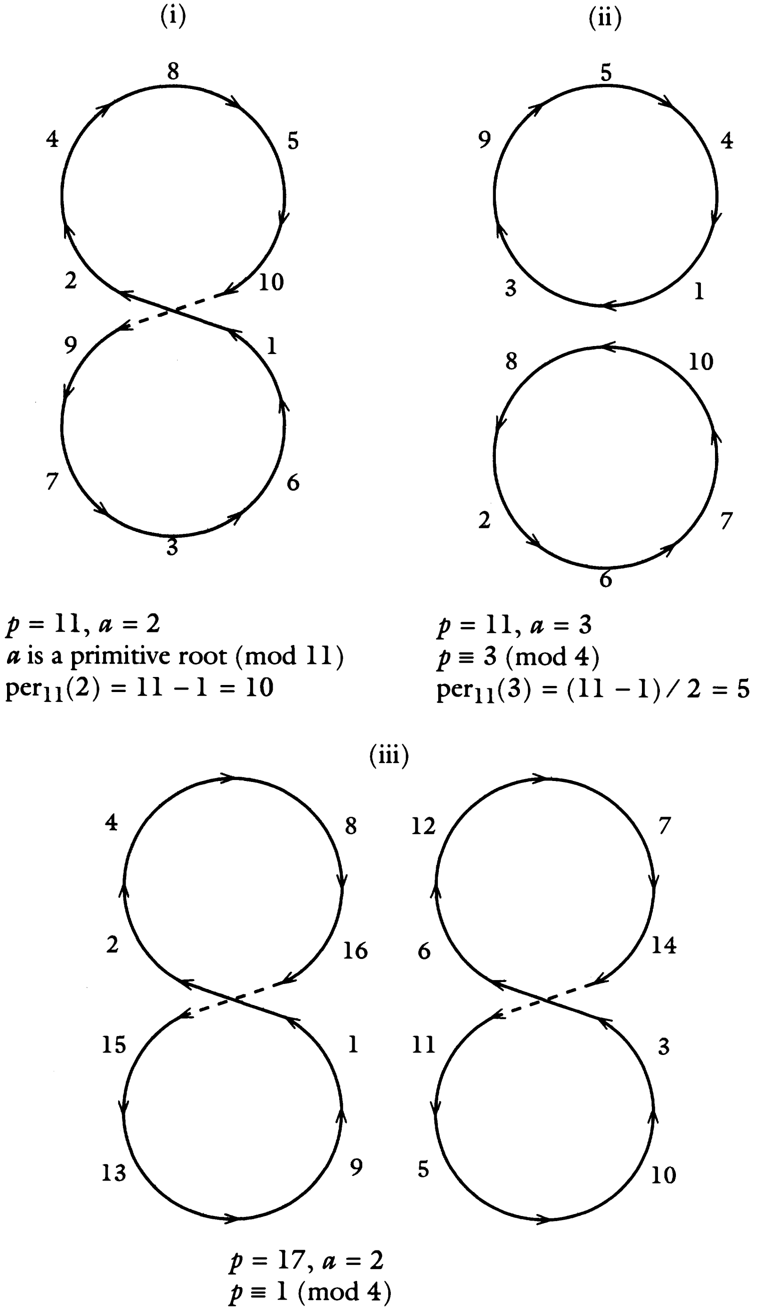
iii. Two separate, disjoint cycles, each cycle comprised of $(p-1)/2$ intervals in two inversionally related half-cycles of $(p-1)/4$ intervals, each cycle exhausting the intervals of $(p-1)/4$ interval classes of ICS_p, and the two cycles jointly exhausting the nonzero intervals. *Conditions:* $p \equiv 1$ (mod 4) *and* $\text{per}_p(a) = (\text{p} - 1)/2$ (Theorem 8).

Example 3 contrasts the three categories graphically. Each circle or figure-eight represents the generation of scale degrees by a single multiplier $a = 2$ or $a = 3$. The diagrams are arranged to exhibit inversional relationships: additive inverses (mod p) are placed in symmetrical positions on the two circles (Example 3 (i)) or upper and lower parts of the figure-eight (Example 3 (ii) and (iii)).

The three cases are pair-wise mutually exclusive; no choice of p and a can satisfy more than one of the three sets of conditions. Are there choices of p (prime) and a, $(a, p) = 1$ that fit *none* of the three cases? Yes. This will be the case whenever $\text{per}_p(a) = (p - 1) / n$, $n > 2$. For example, if we choose $a = 2$, the first few primes that do not work for any of the three cases are 31, 43, 73, and 89, and there are infinitely many such primes, as there are for any choice of a. If we choose one of the three cases, are there particular choices of a for which no choice of p will work? Yes. For example, if $a = 1, 4, 9, 16, \ldots$ is a perfect square, then a cannot be a primitive root for any prime; and there are similar restrictions for the other two cases. However, it is generally believed among number theorists that, for many (perhaps infinitely many) choices of a, there are infinitely many primes that fit *each* of the three cases, but no one can prove it, even for a particular choice of a.

Cycles of Interval Classes

The organization of the two preceding sections associates cases 2 and 3, as given in the preceding summary, on the basis of *intervals*: in each of these cases, a complete cycle comprises exactly half the nonzero intervals. It is also reasonable to associate cases 1 and 2 on the basis of *interval classes*: in each of these cases, a complete cycle touches all of the interval classes in ICS_p. This was in fact the approach of Jay Rahn, who searched for conditions which would guarantee cycling through the interval classes by means of bisection, and found that for a scale of cardinality p, the numbers $2, 2^2, 2^3, \ldots$ cycle through the interval classes if and only if p is an odd prime and $k = (p - 1) / 2$ is the smallest positive integer for which $2^{2k} \equiv 1 \pmod{p}$. This single condition suffices to merge the products of cases 1 and 2 for bisection. Rahn argues persuasively for the preeminence of bisection over other possible divisions, musically. Mathematically, however, there is nothing special about the number 2 in this context. I will show that Rahn's statement, given without proof (though with supporting mathematical information) in his paper, may be generalized. First it is necessary to establish some limits on the case $\text{per}_p(a) = (p - 1) / 2$ by means of the following two theorems. The first, stated without proof, may be found in many textbooks on number theory.



$p = 11$, $a = 2$
a is a primitive root (mod 11)
$\text{per}_{11}(2) = 11 - 1 = 10$

$p = 11$, $a = 3$
$p \equiv 3 \pmod 4$
$\text{per}_{11}(3) = (11 - 1)/2 = 5$

$p = 17$, $a = 2$
$p \equiv 1 \pmod 4$
$\text{per}_{17}(2) = (17 - 1)/2 = 8$

EXAMPLE 3

THEOREM 9. *Let $n > 1$. There exist primitive roots* (mod *n) if and only if*

$$n = 2, n = 4, n = q^x, n = 2q^x,$$

where q is an odd prime and x is a positive integer.

THEOREM 10. *If* $\mathrm{per}_p(a) = (p - 1)/2$, *then p is an odd prime.*

Proof. The number p must be odd, otherwise $(p - 1)/2$ is not an integer. It remains to show that p is prime. Suppose p is composite. Then $\Phi(p) < p - 1$. Since $\mathrm{per}_p(a)$ divides $\Phi(p)$, if $\mathrm{per}_p(a) = (p - 1)/2$, then $\Phi(p) = (p - 1)/2$, and a is a primitive root (mod p). By Theorem 9, if there exists a primitive root (mod p), then $p = 2, 4, q^x, 2q^x$, where q is an odd prime. We need consider only $p = q^x$, as p is even in the other three cases. If $p = q^x$, then (by the unique factorization theorem) $q, q^2, q^3, \ldots, q^{x-1}$ are the only integers greater than one and less than p that divide p. It follows that the only integers less than p and not coprime with p are $q, 2q, \ldots, (p/q - 1)q = p - q$. There are $p/q - 1$ of these integers; thus $\Phi(p) = (p - 1) - (p/q - 1) = p - p/q$. Since p is odd, composite, and a power of q, it is clear that $p/q < p/2$ and $p - p/q > p/2$ (the smallest p that fits this case is $p = 9 = 3^2$). Thus $\Phi(p) = p - p/q$ contradicts $\Phi(p) = (p - 1)/2$, implying p is prime.

We are now in a position to see how Rahn's statement may be generalized by connecting the results of Theorems 6, 7, and 10.

THEOREM 11. *The following three statements are all equivalent:*

(1) (i) *p is an odd prime, and either*

(ii) *a is a primitive root* (mod *p), or*

(ii') $p \equiv 3$ (mod 4) *and* $\mathrm{per}_p(a) = (p - 1)/2$.

(2) *The numbers $a, a^2, \ldots, a^{(p-1)/2}, -a, -a^2, \ldots, -a^{(p-1)/2}$ are all distinct* (mod *p) and they form a reduced system of residues* (mod *p).*

(3) *$k = (p - 1)/2$ is the smallest positive integer for which $a^{2k} \equiv 1$* (mod *p).*

Proof. ($1 \Rightarrow 2$) This is proved in Theorems 6 and 7.

(2 ⇒ 3) Since the numbers a, a^2, . . . , $a^{(p-1)/2}$ are all distinct (mod p), either $\text{per}_p(a) = p - 1$ or $\text{per}_p(a) = (p - 1)/2$. If $\text{per}_p(a) = p - 1$, then statement (3) holds, else $\text{per}_p(a) < p - 1$.

Now suppose $\text{per}_p(a) = (p - 1)/2$ and there exists a $j < (p - 1)/2$ such that $a^{2j} \equiv 1 \pmod{p}$. Then $a^j \equiv \pm 1 \pmod{p}$, but $\text{per}_p(a) = (p - 1)/2$ implies $a^j \equiv -1 \pmod{p}$. Since $j < (p - 1)/2$, a^{j+1} is one of the numbers a, a^2, . . . , $a^{(p-1)/2}$. But $a^{j+1} = a^j \cdot a \equiv -a \pmod{p}$, so $-a$ is not distinct from one of the numbers a, a^2, . . . , $a^{(p-1)/2}$, contradicting statement (2).

(3 ⇒ 1) Statement (3) implies $a^{p-1} \equiv 1 \pmod{p}$, so $\text{per}_p(a)$ must divide $p - 1$ (Theorem 3), and $\text{per}_p(a) \geq (p - 1)/2$, else $a^{2j} \equiv 1$ (mod p), where $j = \text{per}_p(a) < (p - 1)/2 = k$, contradicting statement (3). It follows that $\text{per}_p(a) = p - 1$ or $\text{per}_p(a) = (p - 1)/2$.

Suppose $\text{per}_p(a) = p - 1$. Then p is a prime and a is a primitive root (mod p). Further, p is odd, otherwise $p = 2$ and $(p - 1)/2$ is not an integer, contradicting (3).

Now suppose $\text{per}_p(a) = (p - 1)/2$. Then p is a prime (Theorem 10) and p must be odd, as shown above. So $p \equiv 1 \pmod{4}$ or $p \equiv 3 \pmod{4}$. But if $p \equiv 1 \pmod{4}$, then $j = (p - 1)/4$ is an integer and $a^{2j} \equiv 1$ (mod p), contradicting statement (3). It follows that $p \equiv 3 \pmod{4}$.

Topics for Future Research

There is much unexplored territory here. We have not studied cases where $\text{per}_p(a) = (p - 1)/n$, $n > 2$. Consider for example, $p = 13$, $a = 5$. Here $\text{per}_{13}(5) = (p - 1)/3 = 4$, and we can construct three separate cycles which jointly exhaust the intervals in "quadruple rhythm" (a little knowledge of subgroups and cosets will help to understand how this works):

Let $a = 5$: $a, a^2, a^3, a^4 = 5, 12, 8, 1$

Let $b = 2$: $ba, ba^2, ba^3, \text{ba}^4 = 10, 11, 3, 2$

Let $c = 4$: $ca, ca^2, ca^3, ca^4 = 7, 9, 6, 4 \pmod{13}$

(b and c may be any of the numbers 1, 2, . . . , $p - 1$, not previously generated.)

To glimpse another open area, reconsider the case $p = 17$, $a = 2$, an instance of category iii, as discussed above. This case does not satisfy Jay Rahn's criterion of producing a complete cycle of interval classes, but it does generate all the intervals by means of bisection. In fact, if it is universal bisection that we are after, it can be had for any *odd* cardinality, if we are willing to sacrifice touching all interval classes in a single cycle and partitioning the intervals into two precise hemispheres. With n odd, it is always possible to produce separate cyclic chains (possibly more than two of them) which jointly cycle through all the $n - 1$ nonzero intervals by means of bisection. For example, with $n = 9$, we have

$$2, 2^2 \equiv 4, 2^3 \equiv 8, 2^4 \equiv 7, 2^5 \equiv 5, 2^6 \equiv 1$$

and

$$3, 3 \cdot 2 \equiv 6 \pmod 9.$$

More generally, similar constructions exist for any cardinality n and all a, $(a, n) = 1$.

Finally, what happens if we "mix" generating intervals under particular constraints? For example, choose a prime $p > 3$, and write a series of terms of the form $2^i \cdot 3^j \pmod p$. Suppose we start the sequence with $2^0 \cdot 3^0 \equiv 1 \pmod p$ and generate each successive term by incrementing either i or j by one. If $p = 7$, then with the knowledge gained from our study of GIS$_7$, it is easy to construct a sequence that includes all of the nonzero intervals:

$$2^0 \cdot 3^0 \equiv 1; 2^1 \cdot 3^0 \equiv 2; 2^2 \cdot 3^0 \equiv 4;$$

$$2^2 \cdot 3^1 \equiv 5; 2^3 \cdot 3^1 \equiv 3; 2^4 \cdot 3^1 \equiv 6$$

Do such intervallically exhaustive sequences occur as hierarchies of scale-degree circles in traditional Western music? In sequences like the above, limitation of the operators to 2s and 3s models much of our intuition of metric hierarchy in Western music, suggesting that further investigation of this topic would likely be worthwhile. But we have now come full circle back to the freer approach taken in my earlier work and recapitulated in the first section of this paper. So, having established what I hope will be a more solid foundation for further research, I conclude with the speculation that such relatively "free" hierarchies, formed by partially constrained sequences of multiplicative operators, may play a role in microtonal music of the future, as may the "strict" hierarchies which are the principal topic of this paper.

Acknowledgment

I am grateful to Gerald Myerson, who showed me how primitive roots relate to the problems of this paper, to Jack Douthett, who provided patient mathematical guidance, and to David Clampitt, who offered useful suggestions. Any mathematical errors are, of course, entirely my responsibility. An earlier version of this paper was presented at the Eastman School of Music in May 1990.

Notes

1. John Clough, "Diatonic Interval Sets and Transformational Structures," *Perspectives of New Music* 18 (1979–80): 461–82.

2. Jay Rahn, "Coordination of Interval Sizes in Seven-Tone Collections," *Journal of Music Theory* 35 (1991): 33–60.

3. Inevitably, and especially for "diatonic" scales of n notes, $n \neq 7$, the question arises as to whether it is legitimate to reckon intervals in this way, since classes of "real" intervals (upward major and minor thirds, downward major and minor sixths, and so on) are made equivalent. I refer the concerned reader to my earlier arguments on this question in "Diatonic Interval Sets" (see note 1) and "Aspects of Diatonic Sets," *Journal of Music Theory* 23 (1979): 45–61.

4. David Lewin, *Generalized Musical Intervals and Transformations* (New Haven and London: Yale University Press, 1985).

5. In working out the mathematics of this paper, I have assumed some familiarity with elementary algebra, including the definition of a group, and with basic properties of congruences. The proofs of Theorems 7 and 8 may be slightly simplified by appealing to the concepts *subgroup* and *coset*, but the effect seems not worth the introduction of these additional tools in such a limited context.

6. In Lewin's terms, these transformations form a group of *operations*, since they are one-to-one and onto with respect to S.

7. The notation (a, n) denotes the greatest common divisor of a and n. Thus $(a, n) = 1$ means that a and n are *relatively prime* (no common divisor greater than 1).

8. For another application of primitive roots in music theory, see David Lewin, "Letter re Mallalieu Rows," *In Theory Only* 2, no. 7 (1976): 8. While he does not mention primitive roots explicitly, Lewin's exposition is based upon the fact that 2 is a primitive root (mod 13). For a broader treatment of the process of selecting every *n*th note of a twelve-tone row, see David Lewin, "On Certain Techniques of Reordering in Serial Music," *Journal of Music Theory* 10 (1966): 276–87. A recent, related investigation is Andrew Mead's "Some Implications of the Pitch-Class/Order-Number Isomorphism Inherent in the Twelve-Tone System: Part Two: The Mallalieu Complex: Its Extensions and Related Rows," *Perspectives of New Music* 27 (1989): 180–233.

9. It is not difficult to prove that for any scale of composite cardinality n, there is no generator g such that $g, g^2, \ldots$ produces the set $\{1, 2, \ldots, n-1\}$.

10. Richard Cohn called to my attention a similar example: the theme from the Presto of Haydn's Symphony no. 101.

11. The reader who desires a more general understanding of this process is advised to study subgroups and cosets in elementary group theory.