On the Equivalence of Three Complete Cyclic Systems of Integers

Wolfdieter Lang [1]

Karlsruhe

Germany

wolfdieter.lang@partner.kit.edu

Abstract

The system of coaches by *Hilton* and *Pedersen*, the system of cyclic sequences of *Schick*, and *Brändli-Beyne*, related to diagonals in regular $(2\,n)$-gons, and the system of modified modular doubling sequences elaborated in this paper are proved to be equivalent. The latter system employs the modified modular equivalence used by *Brändli-Beyne*. A sequence of *Euler* tours related on *Schick*'s cycles of diagonals is also presented.

1 Introduction

A) Complete coach system $\Sigma(\mathbf{b})$

Hilton and *Pedersen* [6] found in the context of paper-folding the quasi-order theorem and introduced a complete system of coaches $\Sigma(b)$, for $b = 2\,n + 1$, $n \in \mathbb{N}$. Each coach $\Sigma(b,\,i)$, for $i \in \{1, 2, ..., c(b)\}$ consists of two rows of length $r(b,\,i)$. There is the upper row $A(b,\,i)$ with odd positive integers $a(b,\,i)_j$, for $j = 1, 2, ..., r(b,\,i)$, that are relatively prime to b, and the lower row $K(b,\,i)$ with positive integers $k(b,\,i)_j$, that are certain maximal exponents of 2. All odd numbers from the upper rows of $\Sigma(b)$ constitute the smallest positive reduced residue system modulo b for odd numbers (here called $RRSodd(b)$, given in A216319). The recurrence for the a_j-numbers, defining also the k_j numbers, are (the arguments $(b,\,i)$ are suppressed)

$$a_{j+1} = \frac{b - a_j}{2^{k_j}}, \quad \text{for } j \geq 1, \text{ and odd input } a_1 < \frac{b}{2}, \text{ with } \gcd(a_j, b) = 1, \qquad (1)$$

where 2^{k_j} is the maximal power of 2 dividing $b - a_j$, *i.e.*, k_j is the 2-adic valuation of $b - a_j$. The length of a coach is determined by the cyclic condition $a(b,\,i)_{r(b,\,i)\,+\,1} = a(b,\,i)_1$ for the first time (the primitive period length is $r(b,\,i)$). The sum of the k values of the lower row is identical for all coaches of $\Sigma(b)$: $k(b) := \sum_{j=1}^{r(b,\,i)} k(b,\,i)_j$, for each $i \in \{1, 2, ..., c(b)\}$. The number of coaches $c(2\,n + 1)$ is given in OEIS[13] A135303(n), for $n \geq 1$, and $k(2\,n + 1)$, called the quasi-order of $2\,(\mathrm{mod}\,(2\,n + 1))$, is given in A003558$(n)$.

---

[1] http://www.itp.kit.edu/~wl

Example 1. *([6], p. 262)*

$$\Sigma(65) \;=\; \left|\begin{array}{c|ccc|ccc|ccccc} 1 & 3 & 31 & 17 & 7 & 29 & 9 & 11 & 27 & 19 & 23 & 21 \\ 6 & 1 & 1 & 4 & 1 & 2 & 3 & 1 & 1 & 1 & 1 & 2 \end{array}\right|. \tag{2}$$

In the following a coach is written like $\Sigma(65, 2) \;=\; [A(65, 2), K(65, 2)] \;=\; [[3, 31, 17], [1, 1, 4]]$. Here $c(65) = 4$, $k(65) = 6$, and the $r-$tuple is $\{r(65, 1), ..., r(65, 4)\} = \{1, 3, 3, 5\}$. $k(b)$ satisfies the quasi-order theorem ([6], p. 102 and p. 261)

$$2^{k(b)} \;\equiv\; (-1)^{r(b,\,i)} \,(\mathrm{mod}\,b), \quad \text{for each} \ \ i \in \{1, 2, ..., c(b)\}\,. \tag{3}$$

The $r-$tuples for $b \;=\; \{3, 5, ..., 41\}$ are shown in A332434, with $(-1)^{r(2\,n+1)}$ given in A332433(n), for $n \geq 1$. The coach theorem is ([6], p. 262)

$$c(b)\,k(b) \;=\; \frac{\varphi(b)}{2}, \quad \text{for} \ \ b = 2\,n + 1,\, n \in \mathbb{N}\,, \tag{4}$$

where *Euler*'s totient is $\varphi \;=\;$ A000010. In the example $4 \cdot 6 = 24 = \dfrac{\varphi(65)}{2}$.

B) Complete cycle system SBB(b)

i) In *Schick*'s book [16] a geometric algorithm in a unit circle is proposed which leads to periodic integer sequences with the recurrence relation for $\{q_j(b) \;=\; q_j(b;\, q_0)\}$ (in [16] p is used instead of the present odd b)

$$q_j(b) \;=\; b - 2\,|\,q_{j-1}(b)\,|, \quad \text{for} \ \ j \in \mathbb{N}\,, \tag{5}$$

with a certain odd input q_0, with $\gcd(q_0, b) \;=\; 1$, starting with $q_0(1) \;=\; (-1)^{\frac{b+1}{2}}$. This sequence of distinct odd numbers is periodic with length of the (principal) period $pes(b)$ (*pes* stands in [16] for *periode spéctrale*, because the construction is called *Spektalalgorithmus*). The recurrence leads to identical period length for each input q_0. If not yet all odd members from $RRSodd(b)$, with $\#RRSodd(b) \;=\; \delta(b) \;=\;$ A055034$(b) \;=\; \varphi(b)/2$, are present then a new periodic sequence with the smallest missing member of $RRSodd(b)$ as input $q_0(2)$ is considered (where the sign is $(-1)^{\frac{b+1}{2}} (-1)^{2\,q_0(2)-1}$), *etc.*, until all elements of $RRSodd(b)$ appear. The number of such disjoint periodic sequences with odd members coprime to b is in [16], Korollar, p. 14, called B. The recurrence shows that the primitive period length $pes(b)$ satisfies the same formula like $k(b)$ from the coach system, and it divides $\varphi(b)/2$. This leads to *Schick*'s theorem, and $B(b) \;=\; c(b)$, the number of coaches, in accordance with the coach theorem 4.

$$B(b)\,pes(b) \;=\; \frac{\varphi(b)}{2}\,. \tag{6}$$

See the tables 3.1 to 3.10 in [16], pp. 158 - 166 for these signed periodic sequences. These cycles will be called here $SBB(b, i)$ for $i \in 1, 2, ..., B(b)$ for the different inputs $q_0(b, i)$. The BB in the SBB notation comes from the following part **ii)** on the *Brändli-Beyne* paper using unsigned sequences. The complete cycle system is then $SBB(b)$.

2

Example 2. *([16], p. 161)*

$$SBB(65) = \{(-1,\ 63,\ -61,\ -57,\ -49,\ -33),\ (3,\ 59 - 53,\ -41,\ -17,\ 31),$$
$$(7,\ 51,\ -37,\ -9,\ 47,\ -29),\ (11,\ 43 - 21,\ 23,\ 19,\ 27)\}. \tag{7}$$

Here $B(65) = 4$, $pes(65) = 6$, and $4 \cdot 6 = \dfrac{\varphi(65)}{2} = 24$. Note that $\delta(b) = \dfrac{\varphi(2\,b)}{2} = \dfrac{\varphi(b)}{2}$.

ii) In the paper by *Brändli-Beyne* [3] unsigned *Schick* sequences are considered (we use the same symbols $q_j = q_j(b,\ i)$ but henceforth as positive integers)

$$q_j(b,\ i) = |\,b - 2\,q_{j-1}(b,\ i)\,|, \quad \text{for} \quad j \in \mathbb{N}, \tag{8}$$

with certain positive odd inputs $q_0(b,\ i)$, for $i \in \{1,\ 2,\ ...,\ B(b)\}$, and $\gcd(q_0(b,\ i),\ b) = 1$, as explained above. The complete system of (sign-less) cycles is also named $SBB(b)$ (without risk of confusion).

The numbers in these cycles correspond to certain length ratios diagonal/radius in a regular $(2\,b)$-gon, *viz* $d_j^{(2\,b)} = 2\sin\left(\dfrac{\pi}{2\,b}\,j\right)$, for $j \in \{1,\ 2,\ ...,\ 2\,b - 1\}$. The diagonals connect the vertices $V_j^{(2\,b)}$, for $j \in \{0,\ 1,\ ...,\ 2\,b\}$, with $V_0^{(2\,b)}$ (Cartesian coordinates $(0,\ r)$, with radius r of the circumscribing circle). The vertices are taken in the positive (counter-clockwise) sense, starting with the length ratio for the side $s(2\,b)/r = d_1^{(2\,n)}$.

The diagonals in the upper half plane (including the real axis) are labeled with $j \in \{1,\ 2,\ ...,\ b\}$. The (odd) numbers k of each cycle stand for the labels of the diagonals $d_k^{(2\,b)}$.

Example 3. *For $b = 17$ the two cycles are ($B(17) = 2$, $pes(17) = 4$)*

$$SBB(17,\ 1) = (1,\ 15,\ 13,\ 9), \quad and \quad SBB(17,\ 2) = (3,\ 11,\ 5,\ 7). \tag{9}$$

The elements of $RRSodd(17)$ are all odd numbers from 1 to 15.
The length ratios from the first cycle are (Maple [10] 10 digits): $d_1^{(34)} \approx .1845367190$, $d_{15}^{(34)} \approx 1.965946199$, $d_{13}^{(34)} \approx 1.864944459$, and $d_9^{(34)} \approx 1.478017835$. See Figure 1.
For $b = 11$, with $B(11) = 1$ and $pes(11) = 5$ see [3], Figure 1, with the diagonals called $\sigma_{2\,n+1}$, for $n \in \{1,\ 2,\ ...,\ 5\}$.

Each of the $B(b)$ cycles, for each odd $b \geq 3$, interpreted as length ratios for diagonals, suggests to consider a trail in the $(2\,b)$-gon by following the $pes(b)$ diagonals in the order of the cycle repeatedly, starting from node (vertex) $V_0^{(2\,b)}$ in the positive sense until a periodic sequence, an oriented *Euler* tour, is completed. That this is always possible will be proved in the next section. Periodicity will be reached after $L(b,\ i)$ steps. For $b = 7$ see *Figure 2*. Because of periodicity one can start at any vertex which is reached in the tour starting with vertex $V_0^{(2\,b)}$. In this example all 14 vertices are visited.
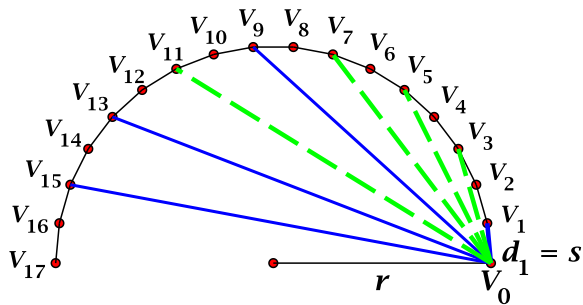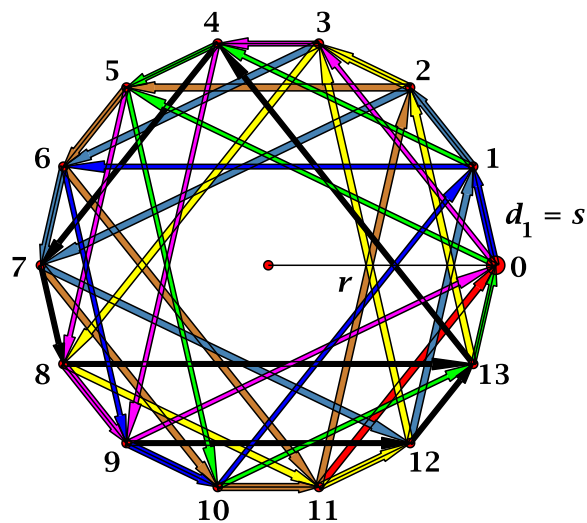
Figure 1   Figure 2

Figure 1: The diagonals in the 34-gon for $b = 17$ for cycle $(1, 15, 13, 9)$ (solid blue), and $(3, 11, 5, 7)$ (dashed green).

Figure 2: The counter-clockwise *Euler* tour for $b = 7$, with $14 \cdot 3 = 42$ arrows in the 14-gon. Start at the vertex with label 0. The color sequence for the arrows is blue, green, magenta, black, yellow, steel blue, and a final red arrow pointing back to label 0. The colors are given in order to follow the trail without looking at the sequence of the 42 vertex labels given later in section 2. For an enlarged version see a link in A332439.

Just for illustration, not for following the 68 arrows in both cases in detail, see the *Figures 3* and *4* for the two *Euler* tours for $b = 17$. All 34 vertices are visited, in fact twice.
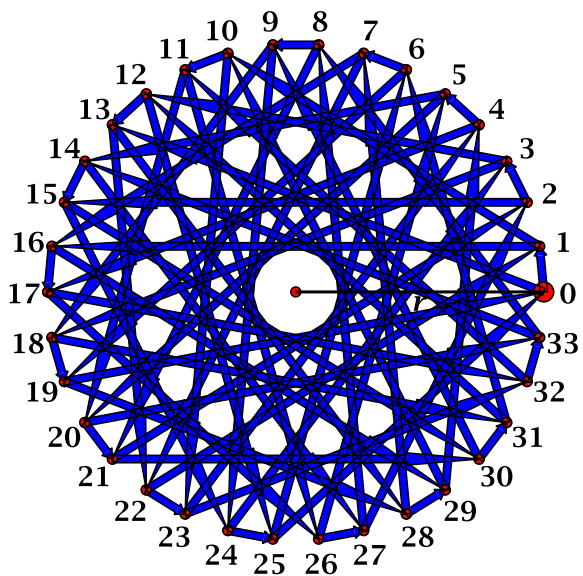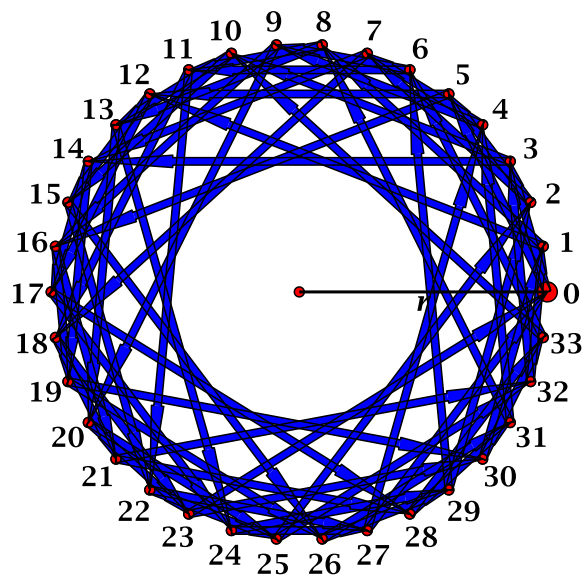

Figure 3   Figure 4

4

Figure 3: 68 arrows in the 34-gon for the directed *Euler* tour for $b = 17$ generated from the first cycle (1, 15, 13, 9) of diagonals.

Figure 4: 68 arrows in the 34-gon for the *Euler* tour for $b = 17$ generated from the second cycle (3, 11, 5, 7) of diagonals.

The underlying digraph with $2\,b$ nodes (vertices) and $L(b, i)$ directed edges (arrows) which are trailed only once in the tour from, say, node V_0^{2b}, is simple (neither parallel arrows nor loops), but may not be regular (nodes may be of different order). Also, not all of the $2\,b$ nodes may be involved in the tour. If one keeps the remaining nodes one will have an unconnected digraph of connectivity number $\mathcal{N}(b) - 1$. where the number of nodes of the *Euler* tour is $\mathcal{N}(b)$, Alternatively, one can discard the remaining nodes in order to have a connected digraph. For example, for $b = 21$ with $B(21) = 1$ only 21 nodes, not 42, are involved in the tour, $\mathcal{N}(21) = 21$, and it is also an irregular graph. See *Figure 5*.
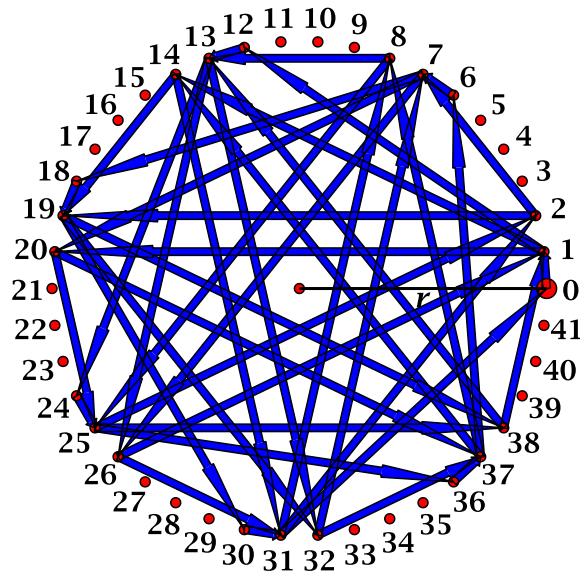

Figure 5

Figure 5: 42 arrows in the 42-gon for the directed *Euler* tour for $b = 21$ generated from the cycle (1, 19, 17, 13, 5, 11). Only 21 nodes are visited. The order of these nodes is 2, 6, 4 for the labels 0, 1, 2 (mod 6), respectively.

In the next section a theorem on the length of the primitive periods of these *Euler* tours will be given. Then, in *Section 3*, the third complete system of cyclic sequences, the $MDS(b)$ system (for **M**odified **D**iagonal **S**equences), for odd $b \geq 3$, will be treated. This system is simpler than the mentioned ones, and will be proved to be equivalent to each of the other two systems in *Section 4*. A modified multiplicative modular relation will be employed, which has already been introduced in the *Brändli* and *Beyne* paper [3]. This modification of the doubling sequence with powers of 2 has already been used in the proof of the quasi-order theorem in [6], p. 103, equation (7.12), and has also been proposed by *Gary W. Adamson* in a comment, Aug 20 2019, to A003558.

2 Schick sequences and Euler tours

The cycles $SBB(b, i)$ for the $B(b)$ = [A135303]$((b-1)/2)$ different input values $q_0(i)$ (B is identical with the coach number c), with period length $pes(b)$ = [A003558]$((b-1)/2)$ (identical with the quasi-order of 2 modulo b of the coach system, called $k(b)$), define by their odd elements length ratios diagonal/radius in a regular $(2\,b)$-gon, as explained above. Following a trail from, say, vertex $V_0^{(2\,b)}$ in the positive (counter-clockwise) sense, defined by a repetition of the diagonals according to the cycle numbers, leads, as will be proved in the theorem, to a positively oriented *Euler* tour, named $ET(b, i)$, of length $L(b, i)$, with the given formula 10.

Theorem 4.

1. *The trail on a regular $(2\,b)$-gon, with odd $b \geq 3$, starting at node (vertex) $V_0^{(2\,b)}$, with label 0 and arrows (directed diagonals) following repeatedly the cycle $SBB(b, i)$ of length $pes(b)$, for any $i \in \{1, 2, ..., B(b)\}$, in the positive sense, will lead to a periodic sequence of node labels with primitive length of the period $L(b, i)$. Therefore, this trail will be a counterclockwise oriented Euler tour $ET(b, i)$.*

2. *The formula for the length of $ET(b, i)$ is*

$$L(b,\, i) \; = \; \frac{2\,b\,pes(b)}{\gcd(SUM(SBB(b,\, i)),\, 2\,b)} \;, \tag{10}$$

where $SUM(SBB(b, i))$ is the sum of the elements of the (unsigned) cycle $SBB(b, i)$.

Proof.

1. Starting from the node (vertex) with label 0 the trail visits, in order, the nodes with labels given by the partial sums of the infinite periodic sequence $SBB(b, i)_\infty$ = repeat$(SBB(b, i))$, evaluated modulo $2\,b$. After the first block of length $pes(b)$, starting with 0, the second block of this length starts with $SUM(SBB(b, i))$. Each new block starts then with a multiple of $SUM(SBB(b, i))$. Therefore the trail will become a periodic Euler tour if after some $m = m(b, i)$ blocks the next block would begin again with 0 modulo $2\,b$. This means that $SUM(SBB(b, i))\, m \equiv 0 \pmod{2\,b}$. Because this linear congruence has always at least one solution periodicity is guaranteed.

2. The length $L(b, i)$ of the *Euler* tour is then $m(b, i)\, pes(b)$. The solution of a linear congruence is known (see *e.g.*, [2], Ch. 5.3, pp. 110 - 113), and in the present case it is the trivial solution $m = 0$ if $g := \gcd(SUM(SBB(b, i)), 2\,b) = 1$, and if $g \geq 2$ there is besides the trivial solution at least one other solution in $\{1, 2, ..., 2\,b - 1\}$. If $g = 1$ the second appearance of the 0 at the beginning of a block will be after $2\,b$ blocks, and $L(b, i) = 2\,b\,pes(b, i)$. If $g \geq 2$ the smallest non-trivial solution is $(2\,b)/g$, and for this m value periodicity appears for the first time.

$\square$

The sum of numbers of the unsigned *Schick* cycles $SBB(2n + 1, q_0 = 1)$ in the case of $B(2n+1) = $ A135303$(n) = 1$ are given in A333848(n), for $n \geq 1$. The corresponding numbers $\gcd(SUM(SBB(b, 1)), 2b)$ are given in A333849.

The b numbers with $B(b) \geq 2$ are listed increasingly in A333855, and their B numbers are in A333853. For these numbers $b = 2n + 1$ the sums of the cycles $SBB(b, i)$, for $i \in \{1, 2, ..., B(b)\}$, are given in the table A333850 (where k is used instead of i). The corresponding $\gcd(SUM(SBB(b, i)), 2(2n + 1))$ values are given in table A333851.

Note that the $\gcd(SUM(SBB(b, i)), 2b)$ values are not independent of i. See A333851 for the first cases with $b = 65, 133, ...$.

Example 5. Euler tour ET(7, 1)

$b = 7$, $B = 1$, $pes(7) = 3$, $SBB(7, 1) = [1, 5, 3]$. $SUM(SBB(7, 1)) = 9$, $\gcd(9, 2 \cdot 7) = 1$, *length* $L(7, 1) = \dfrac{2 \cdot 7 \cdot 3}{1} = 42$

$ET(7, 1) = [0, 1, 6, 9, 10, 1, 4, 5, 10, 13, 0, 5, 8, 9, 0, 3, 4, 9, 12, 13, 4,$
$\qquad\qquad\quad 7, 8, 13, 2, 3, 8, 11, 12, 3, 6, 7, 12, 1, 2, 7, 10, 11, 2, 5, 6, 11]$.

The corresponding digraph is shown in Figure 2, and enlarged as a link in A332439. There are 42 arrows, and all 14 nodes are visited thrice (a regular graph of order 6).

3   Interludium on Schick's cycles for primes

Special attention is paid in *Schick*'s book to prime b (remember that he uses p for odd numbers ≥ 3). The following theorem will show that A268923 gives in fact the odd prime numbers with $B \geq 2$. This will be done by proving that the complement relative to the set of odd primes is A216371 (the odd primes with $B = 1$). In this proof the identity, equation 6 is used, and $2\,pes(prime(n)) = order(2, 3\,prime(n))$, for $n \geq 2$, is derived.

Theorem 6.

1. $2 \cdot order(4, prime(n)) = order(2, 3\,prime(n))$, *for* $n \geq 2$.

2. $pes(prime(n)) = order(4, prime(n))$, *for* $n \geq 2$.

3. *The set of all odd primes p such that all odd primes q, with $q < p$, satisfy*
$\dfrac{\varphi(p\,q)}{2} \Big/ order(2, p\,q) > 1$ *is equal to the set of odd primes satisfying $B(prime) \geq 2$.*

Proof.

1. It will be proved for odd primes p that $2^{2 \cdot order(4, p)} - 1 = 3\,k\,p$, with integer k, and that this exponent is the least one ≥ 1. Clearly $4^{order(4, p)} - 1 = k'\,p$ with some integer k' by definition of $order(4, p)$, and this exponent is the least one ≥ 1. Also, $2^{2n} - 1 = (1 + 3)^n - 1 \equiv 0 \pmod 3$, certainly for any positive n, by the binomial theorem. Hence $k' = 3\,k$. See A082654$(n) = order(4, prime(n))$, for $n \geq 2$.

7

2. The *Jonathan Skowera* formula, Jun 29 2013, in [A003558](#) shows that $\underline{A003558}(\hat{n}) = pes(2\,\hat{n}+1)$, for $\hat{n} \geq 1$. Hence for $prime(n) = 2\,\hat{n}+1$, with $\hat{n} = \hat{n}(n)$, one has $pes(prime(n)) = \underline{A003558}(\hat{n}(n))$, for $n \geq 2$.

   The direction $\Rightarrow$ is then trivial from the definition of $\underline{A003558}(\hat{n}(n))$ by just squaring.

   The direction $\Leftarrow$ with $\underline{A082654}(n)$, for $n \geq 2$, means that $(2^{k(n)} + 1)\,(2^{k(n)} - 1)) \equiv 0 \pmod{prime(n)}$. But this implies $prime(n)$ divides one of the factors, hence $2^{k(n)} \equiv \pm 1 \pmod{prime(n)}$, for $n \geq 2$, with minimal $k(n) > 1$; this is the definition from [A003558](#).

3. It is proved that the complement of [A268923](#) relative to the set of odd primes is [A216371](#). For the complement one tries to find all odd primes p such that an odd prime $q < p$ exists with $\dfrac{\varphi(p\,q)/2}{order(2,\,p\,q)} = 1$.

   As such a prime $q = 3$ is chosen. From the *Schick*'s theorem eq. 6 one knows that $B(p) = \dfrac{p-1}{2\,pes(p)}$, for $p \geq 3$. With parts *1* and *2*, just proved, this becomes $B(p) = \dfrac{p-1}{order(2,\,3\,p)}$.

   In addition a corollary of *Theorem* 64, p. 106, by *Nagell* [11] (or the Theorem 10.8, p. 211, of *Apostol* [2]) is needed, namely the improvement of the *Euler-Fermat* theorem for certain non-exceptional numbers (here $p\,q$, with $q < p$): $2^{\varphi(p\,q)/2} \equiv 1 \pmod{p\,q}$, where $\varphi = \underline{A000010}$, *Euler*'s totient function. It is then clear that $order(2,\,p\,q)$ has to divide $\varphi(p\,q)/2$. For $q = 3$ this becomes $\dfrac{p-1}{order(2,\,3\,p)} \geq 1$ for all $p \geq 5$.

   From application of *Schick*'s theorem equation (6) it is clear for which odd primes ≥ 5 equality holds, namely for those with $B(p) = 1$. Hence the complement of [A216371](#) is 3, and the primes p with $B(p) = 1$, which is [A216371](#). Therefore [A268923](#) gives the odd primes p with $B(p) \geq 2$.

   $\square$

4 Complete cycle system of modified modular doubling sequences MDS(b)

A) Modified modular congruence (mod* n)

This modified modular congruence considered by *Brändli* and *Beyne* can be formulated based on ordinary reduced residue systems modulo n, whose smallest non-negative version is given by the set named RRS(n) shown in [A038566](#) (but with 0 for $n = 1$). $RRS(n) = \{r_1, r_2, \ldots r_{\varphi(n)}\}$, with r_j representing the residue class $_n\overline{r_j}$, and $\varphi(n) = \#RRS(n) = \underline{A000010}(n)$, for $n \in \mathbb{N}$. *E.g.*, $RRS(4) = \{1, 3\}$, with representative $_4\overline{1}$ consisting of all integers $a = 1 + k\,4$, with $k \in \mathbb{Z}$, *i.e.*, $a \equiv 1 \pmod 4$, and similarly for $_4\overline{3}$. Thus $RRS(4)$ represents all odd integers (the union of the sets congruent to 1 and 3 modulo 4).

Definition 7. *The smallest non-negative reduced residue system* $\text{mod}^* n$ *is denoted by* $RRS^*(n)$, *and this is* $RRS^*(1) = \{0\}$, $RRS^*(2) = \{1\}$, *and* $RRS^*(n)$ *consists of the elements of the first half of* $RRS(n)$, *for* $n \geq 3$.
Each element $r_j^* \in RRS^*(n)$ *represents the reduced residue class denoted by* $_n\overline{r_j}^*$, *and these classes are given in terms of ordinary ones by*

$$_1\overline{0}^* = {}_1\overline{0} \qquad _2\overline{1}^* = {}_2\overline{1},$$

$$_n\overline{r_j}^* := \{_n\overline{r_j}\} \cup \{_n\overline{(-r_j)}\}, \quad for \;\; j = 1, 2, ..., \frac{\varphi(n)}{2}, \;\; and \;\; n \geq 3. \qquad (11)$$

The number of elements of $RRS^*(n)$ is $\#RRS^*(n) =: \sigma(n) = \underline{\text{A023022}}(n)$, but with extra $\underline{\text{A023022}}(1) = 1$. Note that the mod^* residue classes represent together the same set of integers as the ones of $RRS(n)$, but $RRS^*(n) = RRS(n)$ only for $n = 1$ and $n = 2$.

E.g.,, $n = 4$: $RRS^*(4) = \{1\}$, and the reduced residue class $_4\overline{1}^*$ consists of the union of the ordinary reduced residue classes $_4\overline{1}$ and $_4\overline{3}$, hence $RRS^*(4) \neq RRS(4)$, but represents the same integers as $RRS(4)$, namely the odd ones (see above).

It is elementary that the elements of $RRS^*(2\,m)$ are only odd (and reduced) integers, and $RRS^*(2^m)$ represents all odd numbers, for each $m \in \mathbb{N}$.

If in $RRS^*(2\,m - 1)$, with $m \in \mathbb{N}$, all even integers are discarded, the remaining subsets of the residue classes could be called $RRS^* odd(2\,m - 1)$. But it is clear that $RRS^* odd(2\,m - 1)$ represents the same odd integers as $RRS^*(2\,(2\,m - 1))$.

The equivalence relation $a \overset{*n}{\sim} b$ for integer numbers a and b, coprime to $n \in \mathbb{N}$, is defined by $a \in {}_n\overline{r_j}^*$ and $b \in {}_n\overline{r_j}^*$, with $r_j^* \in RRS^*(n)$, for some $j \in \{1, 2, ..., \sigma(n)\}$. This is based on the fact that the restricted residue classes $\text{mod}^* n$ are pairwise disjoint and cover the integers coprime to n.

The notation $\text{mod}^*(a, n)$ gives $r_j^* \in RRS^*(n)$, if $a \in {}_n\overline{r_j}^*$.
It is defined by

$$\text{mod}^*(a, n) := \begin{cases} \text{mod}(a, n) & if \; \text{mod}(a, n) \leq \frac{n}{2}, \\[2mm] \text{mod}(-a, n) & if \; \text{mod}(a, n) > \frac{n}{2}, \end{cases} \qquad (12)$$

where $\text{mod}(a, n) \in \{0, 1, ..., n-1\}$ (0 can appear only for $n = 1$ because a is reduced).

Example 8.

1. $\text{mod}^*(17, 9) = 1$ *because* $\text{mod}(17, 9) = 8$ *and* $\text{mod}(-8, 9) = 1$.

2. $\text{mod}^*(4, 9) = 4$ *because* $\text{mod}(4, 9) = 4 < 4.5$.

3. $\text{mod}^*(5, 9) = 4$ *because* $\text{mod}(5, 9) = 5 > 4.5$.

Because $\text{mod}^* n$ uses numbers coprime to n it is not additive for $n \geq 2$, contrary to $\text{mod}\, n$. If $\gcd(a, n) = 1 = \gcd(b, n)$ then $\gcd(a + b, n) \neq 1$ in general if $n \geq 2$. Because $\text{mod}^*(a, n) = \text{mod}^*(-a + n, n)$, even if $\gcd(a + b, n) = 1$ (*e.g.*, $n = 9$, $a = 1$, $b = 4$) mod^* cannot be well defined (*e.g.*, $4 \overset{*9}{\sim} 5$, and $\gcd(1 + 5, 9) = 3$).

However, mod*, like mod, is multiplicative. This is based on the lemma that if $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$ then $\gcd(a\,b, n) = 1$ (see, *e.g.*, the simple proofs in [4], p. 30, Exercise 16 (a), or [12], p. 8, Satz 1.8). Also, $\gcd(a\,(-a + n), n) = 1$ provided $\gcd(a, n) = 1$.

That each reduced residue system mod$^*n$, with $\sigma(n) \geq 2$, forms an *Abelian* multiplicative group of degree $\sigma(n)$ follows from mod n properties. The identity element is the class congruent to $_n\overline{1}^*$. If the system $RRS^*(n)$ is used this is the element 1. That a unique inverse element exists is based on a theorem on the unique solution of the linear congruence $a\,x \equiv b\,(\mathrm{mod}\,n)$ if $\gcd(a, n) = 1$ (see, *e.g.*, [12], p. 41, Satz 2.13, [2], p. 114, Theorem 5.20), which generalizes to the mod* case. The cases with $\sigma(n) = 1$ are trivial one element groups.

In [3] this multiplicative group of representatives of $RRS^*(n)$ has been considered and named G_n^*. For $\sigma(n) \geq 2$ this is a direct product of cyclic groups C_k of order k, because it is a finite Abelian group (see *e.g.*, [15], Satz 43 and Satz 42 p. 49 and 47).

If n is a product of two odd primes the smallest noncyclic group appears for $n = 65 = 5 \cdot 13$ with the cycle structure $12_2\,6_2$ (meaning 2 cycles of length 12 and also of length 6, not regarding subcycles), namely (3, 9, 27, 16, 17, 14, 23, 4, 12, 29, 22, 1), (11, 9, 31, 16, 19, 14, 24, 4, 21, 29, 6, 1), (2, 4, 8, 16, 32, 1) and (7, 16, 18, 4, 28, 1). See [3], Theorem 3, p. 10, for the criterion on cyclic mod* groups for odd n. G_{65}^* is the group $C_4 \times C_3 \times C_2$. For the cycle graph see [8], Figure 4, the 7th plot, where cycle groups are called Z_k (as a side remark note that the modified modular congruence Modd used there in the context of regular n-gons and diagonal/side ratios is related to a set of representatives, called there $\mathcal{M}(n)$ (equation (65)) that is different from $RSS^*(n)$ considered here).

In a further paper *Brändli* and *Beyne*, with two collaborators [9], studied polynomials which have as *Galois* group G_n^*, now called $\mathbb{Z}_n^{*/2} = \mathbb{Z}_n^*/\langle n - 1\rangle$. They call these polynomials $\Psi_n^{re}(x)$ (*re* stands for reduced), and give the zeros in terms of $s_k(n) := 2\cos\left(\dfrac{2\,\pi\,k}{n}\right)$, for k values from $RRS^*(n)$, and $n \geq 1$. This can be rewritten in terms of the algebraic number $\rho(n) := 2\cos(\pi/n)$ of degree $\delta(n) = $ A055034(n), which is fundamental for regular $n-$gons (see [8]), as $s_k(n) = R(2\,k, \rho(n))$, with the monic *Chebyshev* polynomials R shown in A127672. The minimal polynomials of $\rho(n)$, called $C(n, x)$ in [8] (see also Table 2 there) are used in order calculate the *Galois* polynomials $\Psi_n^{re}(x)$ modulo $C(n)$ (in order to reduce powers of $\rho(n)$ with exponents larger than $\delta(n) - 1$).

These polynomials are then (the use of $C(n, x = \rho(n))$ is indicated by the vertical bar)

$$\Psi_n^{re}(x) = \prod_{j=1}^{\sigma(n)} (x - R(2\,RRS^*(n)_j, \rho(n)))\Big|_{C(n, \rho(n)) = 0}, \quad \text{for } n \in \mathbb{N}. \qquad (13)$$

It is not surprising that these are the minimal polynomials of the algebraic number $2\cos\left(\dfrac{2\,\pi}{n}\right) = R(2, \rho(n)) = \rho(n)^2 - 2$ of degree $\sigma(n)$, and they are given in A232624, where they are named $MPR2(n, x)$.

Example 9.

$$\Psi_{65}^{re}(x) = MPR2(65,\, x) = 1 - 12\,x - 180\,x^2 - 101\,x^3 + 2085\,x^4 + 1802\,x^5 - 9126\,x^6$$
$$- 7168\,x^7 + 20886\,x^8 + 13653\,x^9 - 28667\,x^{10} - 1\,5001\,x^{11} + 25284\,x^{12} + 10282\,x^{13}$$
$$- 14822\,x^{14} - 4540\,x^{15} + 5832\,x^{16} + 1292\,x^{17} - 1521\,x^{18} - 229\,x^{19} + 252\,x^{20} + 23\,x^{21}$$
$$- 24\,x^{22} - x^{23} + x^{24}\,. \tag{14}$$

B) Complete MDS(b) system

Instead of the two lines $A(b, i)$ and $K(b, i)$, with $b = 2\,n + 1$, $n \in \mathbb{N}$, $i \in \{1,\, 2,\, ...,\, c(b)\}$ and length $r(b.\,i)$ in the complete coach system $\Sigma(b)$ of *Hilton* and *Pedersen* [6] from section **A)** of the *Introduction*, and the periodic positive integer sequence $\{q(b,\, i)_j\}$ with $i \in \{1,\, 2,\, ...,\, B(b)\}$ and $j \in \{1,\, 2,\, ...,\, pes(b\}$ in the complete system $SBB(b)$ by *Schick* [16] and *Brändli-Beyne* [3] from section **B) i)** and *ii)* of the *Introduction*, periodic doubling sequences are used, namely $\{mod^*(a(b,\, i)\,2^j,\, b)\}$, with certain odd numbers $a(b,\, i)$ coprime to b, where $i \in \{1,\, 2,\, ...,\, c^*(b)\}$ and $j \in \{1,\, 2,\, ...,\, P(b)\}$.
It will turn out that $c^*(b) = c(b) = B(b)$, and the length of the period $P(b)$, independent of i, is identical with $k(b) = pes(b)$.
The short abbreviation MDS is used instead of $MMDS$, for Modified Modular Doubling Sequence.

Definition 10.

1. *A doubling sequence $DSseq(b,\, i)$, for $i \in \{1,\, 2,\, ...,\, c^*(b)\}$, is defined by*

   $\{mod(a(b,\, i)\,2^j,\, b)\}_{j \geq 1}$, *for $b = 2\,n + 1$, with $n \in \mathbb{N}$, and some odd element $a(b,\, i) \in RRS^*(b)$.*

2. *A modified modular doubling sequence $MDSseq(b,\, i)$, for $i \in \{1,\, 2,\, ...,\, c^*(b)\}$, is defined by $\{mod^*(a(b,\, i)\,2^j,\, b)\}_{j \geq 1}$, for $b = 2\,n + 1$, with $n \in \mathbb{N}$, and some odd element $a(b,\, i) \in RRS^*(b)$.*

Note that the input $a(b, i)$ appears not as first number (for $j = 1$) of these sequences. In the $MDSseq(b,\, i)$ case it will be shown to appear at the end of the first period (as it would also in the other sequence with a doubled length of the period).

The odd members of $RRS^*(b)$ are denoted by $RRS^*odd(b)$. $\#RRS^*odd(b) = $ A332435$((b - 1)/2)$, and $\#RRS^*even(b) = $ A332436$((b - 1)/2)$.

Example 11. $RRS^*odd(33) = \{1, 5, 7, 13\}$, $MDSseq(33,\, 1) = \{repeat(2,\, 4,\, 8,\, 16,\, 1)\}$, $MDSseq(33,\, 2) = \{repeat(10,\, 13,\, 7,\, 14,\, 5)\}$.

The two sequences of the example are periodic with the same length of period, *i.e.*, $P(33,\, 1) = P(33,\, 2) = 5$.
In general one starts with input $a(b,\, 1) = 1$, then if not all odd numbers from $RRS^*odd(b)$ are present in the period of the sequence one takes as next input, $a(b, 2)$, the smallest missing number in $RRS^*odd(b)$, in this example 5, *etc.*, until all odd numbers from $RRS^*odd(b)$

are present, and then the system $MDS(b)$ of $c^*(b)$ sequences is complete. In the example only two sequences are needed ($c^*(33) = 2$). This procedure is similar to the one of $SBB(b)$ systems with the different initial values for $q_0(b, i)$.

After it has been proved that $MDSseq(b, i)$ is always periodic with the same period length for different i, hence called $P(b)$, the primitive period will be denoted by $MDS(b, i)$.

Proposition 12. Complete MDS(b) system

1. *Each sequence $MDSseq(b, i)$ is periodic, and the length of the primitive period $MDS(b, i)$ is independent of any input $a(b, i) \in RRS^*odd(b)$, for $b \geq 3$. This length of the period will be called $P(b)$.*

2. *$P(b) = k(b) = pes(b) = \underline{A003558}(b)$.*

3. *$MDS(b, i)_{P(b)} = a(b, i)$.*

4. *$\bigcup\limits_{i=1}^{c^*(b)} MDS(b, i) = RRS^*(b)$.*

5. *$c^*(b) \, P(b) = \frac{\varphi(b)}{2}$. Hence $c^*(b) = c(b) = B(b) = \underline{A135303}(b)$, for $b \geq 3$.*

Proof.

1. The condition for the primitive length of the period $P(b, i)$ of $MDSseq(b, i)$, if existing, is $\mod^*(a(b, i)\,2^{P(b, i)+1}, b) = \mod^*(a(b, i)\,2^1, b)$ for the smallest $P(b, i) > 0$. Because $0 < a(b, i) \leq \lfloor \frac{b-1}{2} \rfloor$, hence $\mod(a(b, i), b) = a(b\ i)$, it follows that $\mod^*(a(b, i), b) = a(b, i)$. Multiplicativity of $\mod^*$ tells that the condition is $\mod^*(2^{P(b, i)}, b) = 1$, with $1 \in RRS^*(b)$, representing the unique identity element of $\mod^*$. Hence a solution exists, because there is always a solution for $\mod(2^{P(b, i)}, b) = +1$, namely the $order(2, b)$. But this $P(b, i)$ may not give the primitive length of the period (see the next part). Therefore $MDSseq(b, i)$ is certainly periodic for each i, independently of $a(b, i)$.

2. $\mod^*(2^{P(b)}, b) = 1$ means that $2^{P(b)} \equiv +1 \,(\mod b)$ or $2^{P(b)} \equiv -1 \,(\mod b)$. For the primitive length of the period the least $P(b) > 0$ has to be chosen. This is the same congruence problem as the one for $k(b)$ of the coach system $\Sigma(b)$, and also for $pes(b)$ of the $SBB(b)$ system.

3. $MDS(b, i)_{P(b)} = \mod^*(a(b, i)\,2^{P(b)}, b)$. Because $0 < a(b, i) \leq \frac{b-1}{2}$, and if $\mod(2^{P(b)}, b) = +1$ then $\mod^*$ becomes $\mod$, and the result is obviously $a(b, i)$. If $\mod(2^{P(b)}, b) = -1$ then $\mod(-a(b, i), b) \geq \frac{b-1}{2}$ and the result is $\mod(+a(i, b), b) = a(i, b)$.

4. By construction of $MDS(b)$ all odd numbers of RRS^* appear once in the union of $MDS(b, i)$, for $i = 1, 2, ..., c^*(b)$. Each even number $2\,k$ of the complete set $MDS(b)$ has a smaller odd ancestor $\underline{A000265}(2\,k)$ (its odd part) in some cycle $MDS(b, i)$ with a certain odd initial value. Every even element of RRS^*, always $\leq \frac{b-1}{2}$, is in one of the $c^*(b)$ cycles of $MDS(b)$ because its odd ancestor, always $< \frac{b-1}{2}$, has to be in precisely one cycle $MDS(b, i)$, with a certain odd initial value.

12

5. A corollary of *1.*, *4.* and *2.* because $\#RRS^*(b) = \sigma(b) = \dfrac{\varphi(b)}{2}$.

$\sum_{i=1}^{c^*(b)} P(b, i) = c^*(b) P(b) = \#RRS^*(b)$. Then *2.* together with eqs. 4 and 6 are used.

$\square$

For the cycle system $MDS(b)$ for $b = 2\,n + 1$, with $n = 1, 2, ..., 35$, see *Table 2*, and also A334430.

$MDS(b, i)_j$, for $j = 1, 2, ..., P(b)$, are the elements of the cycle $MDS(b, i)$. For simplicity the argument (b, i) will by suppressed, and instead of MDS_j just c_j (c for cycle) is used in the following *Proposition*.

Proposition 13. *For each cycle $MDS(b, i)$ the members $c_j = c(b, i)_j$ satisfy the recurrence*

$$c_j = \begin{cases} 2\,c_{j-1} & \text{if } c_{j-1} \le \left\lfloor \frac{b-1}{4} \right\rfloor, \\[2mm] b - 2\,c_{j-1} & \text{if } c_{j-1} > \left\lfloor \frac{b-1}{4} \right\rfloor, \end{cases} \tag{15}$$

for $j \ge 2$, and the input is $c_1 = mod^*(2\,a(b, i), b)$.

Proof. This uses the mod^* definition of c_j, and multiplicativity of mod to extract a factor 2. The second line follows from the c_j definition in the case when $(b-1)/2 < \text{mod}(2\,a\,2^{j-1}, b) \le (b-1)$, *i.e.*, $(b-1)/4 < \text{mod}(a\,2^{j-1}, b) \le \frac{b-1}{2}$. In this case the mod^* definition of c_{j-1} tells that $c_{j-1} = \text{mod}(a\,2^{j-1}, b)$. Because in this case $c_j = \text{mod}(-2\,a\,2^{j-1}, b) = -2\,c_{j-1}$, that is $b - 2\,c_{j-1}$ because the numbers c are always from $RRS^*(b)$, hence $\le \frac{b-1}{2}$. The simpler first line is proved in a similar manner. $\square$

This can be written as one line formulae.

Corollary 14.

$$\begin{aligned} c_j &= \frac{1}{2}\left(b - |b - 4\,c_{j-1}|\right). \\ c_j &= mod^*(2\,c_{j-1}, b). \\ c_j &= mod((-1)^{p_j}\,2\,c_{j-1}, b), \quad \text{where } p_j = parity(c_j). \end{aligned} \tag{16}$$

for $j = 2, 3, ..., P(b)$, and the initial value is $c_1 = c(b, i)_1$, that is $2\,a(b, i)$ if $a(b, i) \le \left\lfloor \frac{b-1}{4} \right\rfloor$, and $b - 2\,a(b, i)$ if $a(b, i) > \left\lfloor \frac{b-1}{4} \right\rfloor$. In the second equation $c(b, i)_{j-1} \in RRS^*(b, i)$ from *Proposition* 12 *4.* has been used, hence $\text{mod}(2\,c(b, i)_{j-1}, b) = 2\,c(b, i)_{j-1}$. In the last equation the recurrence is considered mod b. In the upper alternative c_j is even, and the lower one odd.

Example 15. $b = 63$, $c^*(63) = 3$, $P(63) = 6$, $\left\lfloor \frac{63-1}{4} \right\rfloor = 15$.
$MDS(63, 3) = [22, 19, 25, 13, 26, 11]$. $c_2(63, 3) = 19 > 15$, $c_3(63, 3) = 63 - 2 \cdot 19 = \frac{1}{2}(63 - (4 \cdot 19 - 63)) = 25$.

13

Like in the complete system $SBB(b)$ the elements (numbers) of the cycles of $MDS(b)$ are interpreted as length ratios diagonal/radius in regular $(2\,b)$-gons as follows. A number k (even or odd) from a cycle $MDS(b, i)$, hence $k \in [1, (b-1)/2]$, for $i \in \{1, 2, ..., c^*(b)\}$, is mapped to $2\cos\left(\dfrac{\pi\,k}{b}\right) = R(k, \rho(b)) > 0$, where R are monic *Chebyshev* polynomials shown in [A127672](#), and $\rho(b) = 2\cos\left(\dfrac{\pi}{b}\right)$, the length ratio diagonal/side of the diagonal $d_2^{(b)} = \overline{V_0^{(b)} V_2^{(b)}}$ in the regular b-gon. [The R polynomials are in [1], Table 22.7, p. 797, called C. In [7], Table 2, p. 72, they are called *Lucas* polynomials.]

The connection to length ratios diagonal/radius in the regular $(2\,b)$-gon comes from the trigonometric identity

$$2\cos\left(\frac{\pi\,k}{b}\right) = 2\sin\left(\frac{\pi\,(b\pm 2\,k)}{2\,b}\right). \tag{17}$$

For the positive sign see also the table and a comment in [A082375](#). But here the negative sign will be chosen. As mentioned above all values are positive. This is an advantage over considering cosine arguments $a(b, i)\,2^k$ like in the later discussed complete iteration system $IcoS(b)$.

E.g., $b = 5$, $MDS(5, 1) = (2, 1)$: $k = 1$ corresponds to the two diagonal/radius ratios $d_7^{(10)}$ and $d_3^{(10)}$ both of length φ, with the golden ratio $\varphi = 1.61803398... = $[A001622](#) (in the lower and upper half-plane, respectively). For $k = 2$ these are $d_9^{(10)}$ and $d_1^{(10)}$, the side/radius ratios of length $\varphi - 1$.

The numbers $2\cos\left(\dfrac{\pi\,k}{b}\right) = R(k, \rho(b))$, with $k \in RRS^*(b)$, can be taken as zeros of a monic polynomial $P^*(b, x)$ of degree $\sigma(b) = $[A023022](#)$(b) = $[A055034](#)$(b) = \delta(b)$. It follows that this is a polynomial with coefficients from the ring of integers of the simple algebraic field extension $\mathbb{Q}(\rho(b))$, denoted by $\mathcal{O}_{\mathbb{Q}(\rho(b))} =: \mathbb{Z}[\rho(b)]$. The following proposition gives the formula. See *Table 1* for $b = 2\,n + 1$. for $n = 1, 2, ..., 10$.

Proposition 16. P*(b, x) polynomials
The monic polynomials

$$P^*(b, x) := \prod_{j=1}^{\sigma(b)} \left(x - 2\cos\left(\frac{\pi\,RRS^*(b)_j}{b}\right)\right) = \prod_{j=1}^{\sigma(b)} (x - R(RRS^*(b)_j, \rho(b)))\Big|_{C(b, \rho(b)) = 0}. \tag{18}$$

with $b = 2\,n + 1$, $n \in \mathbb{N}$, *have coefficients which are integers in the simple field extension* $\mathbb{Q}(\rho(b))$, *where* $\rho(b) = 2\cos\left(\dfrac{\pi}{b}\right)$,

In the evaluation the minimal polynomial $C(b, x)$ of $\rho(b)$, given in [A187360](#), is used to eliminate powers of $\rho(b)$ with exponents larger than $\delta(b) - 1 = \sigma(b) - 1$.

Proof. The first equation gives the definition. The last equation follows from the definition of the R polynomials in terms of *Chebyshev* T polynomials, and their trigonometric definition. Then the coefficients will be expressed in the power basis of $\mathbb{Q}(\rho(b))$ of degree $[\mathbb{Q}(\rho(b)) : \mathbb{Q}] = \delta(b)$ with rational integer coefficients, because $R \in \mathbb{Z}[x]$. $\qquad\square$

Example 17.

$$RRS^*(9) = [1, 2, 4], \ \sigma(9) = 3,$$
$$P^*(9, x) = (x - 2\cos(\pi/9))(x - 2\cos(\pi\,2/9))(x - 2\,\cos(\pi\,4/9)),$$
$$= x^3 - 2\,\rho(9)\,x^2 + (-3 + 2\,\rho(9)^2)\,x - 1,$$
$$\text{with } \rho(9) = 2\cos(\pi/9) = \underline{A332437} = 1.87938524....\qquad(19)$$

C) Complete IcoS-system

An alternative approach to the modified modular doubling sequence has been considered by *Gary W. Adamson* and J. Kappraff [7] by studying iteration of the quadratic polynomial $R(2, x) = x^2 - 2$ with certain seeds (see above for *Chebyshev R* polynomials, and the name *Lucas* polynomial in [7]). It has also been used as *r-t* table (*r-t* for root trajectory) by *Gary W. Adamson* in his Aug 25 2019 comment in $\underline{A065941}$. As will be shown this is very similar to the *MDS*-system. The iteration of $x^2 - 2$ is proposed in a procedure 1. by *Devaney* [5], on p. 25, for investigation, and in chapter 7.1, pp. 69 - 71, this function is called $Q_{-2}(x)$. It is shown in chapter 10.2, pp. 121 - 126 to be semiconjugate to the function $V(x) = 2|x| - 2$, and also to the angle doubling function $D(\theta) = 2\theta$ on the unit circle.

If one starts the iteration of $R(2, x)$ with a seed $2\cos(\pi\,1/b)$, for $b = 2n + 1$, with $n \in \mathbb{N}$, one does not obtain a purely periodic sequence if signs are respected. In order to obtain purely periodic sequences one starts the iteration with $R^{[1]}(2, x)$, not with the identity map $R^{[0]}(2, x) = x$. The later given theorem shows periodicity with primitive period length $P(b)$ like for $MDS(b)$, and also the number of seeds $c^*(b)$ necessary to obtain finally all $2\cos(\pi\,j/b)$, values with $j \in RRS^*(b)$. Note that not all iterations will be positive. Hence for the interpretation as length ratios diagonal/radius in $(2\,b)$-gons the signs will have to be ignored.

This complete system of periodic signed cosine sequences obtained by iteration will be called $IcoS(b)$, and its elements are denoted by sets $IcoS(b, i)$, for $i = 1, 2, ..., c^*(b)$.

Lemma 18. *The iteration with the Chebyshev polynomial $R(2, x) = x^2 - 2$ is periodic for any seed $x = 2\cos(\pi\,j/b) = R(j, \rho(b))$, where $\rho(b) = 2\cos(\pi/b)$, and odd $j \in RRS^*(b)$, and the primitive length of the period is $P(b) = \underline{A003558}((b-1)/2)$.*

Proof. The standard formula for the *Chebyshev T*$-$polynomials (see $\underline{A053120}$, and [14], p. 5, Exercise 1.1.6) $T(n, T(m, x)) = T(n\,m, x)$ translates for $R(n, x) = 2\,T(n, x/2)$ to $R(n, R(m, x)) = R(n\,m, x)$. The T and R polynomials with negative index are identical with the ones for positive index: $R(-n, x) = R(n, x)$, for $n \in \mathbb{N}_0$.

From the periodicity of the cosine function, and $R(j, \rho(n)) = 2\cos(\pi\,j/n)$, follows that $R(k, R(j, \rho(n))) = R(k\,j, \rho(n)) = R(k\,j - q\,2\,n, \rho(n))$, for $n \in \mathbb{N}$ and $q \in \mathbb{Z}$. Together with the symmetry under sign flip of the index, periodicity requires that

$$R(k\,j, \rho(n)) = R(\pm(k\,j - q\,2\,n), \rho(n)), \text{ for } n \in \mathbb{N}, \text{ and } q \in \mathbb{Z}.\qquad(20)$$

For the iteration of $R^{[k]}(2, x) = R(2^k, x)$, for $k \in \mathbb{N}$, periodicity therefore means in the present context, that, with any seed $x = 2\cos(\pi\,j/b)$, and positive odd j with $\gcd(j, b) = 1$

15

and $j \leq \frac{b-1}{2}$, i.e., $j \in RRS^* odd(b)$,

$$R(2^k\, j,\, \rho(b)) \;=\; R(\pm(2^k\, j - q\, 2\, b),\, \rho(b)) \;\overset{!}{=}\; R(j\, 2^1,\, \rho(b)), \qquad (21)$$

For the smallest $k > 1$, and then the primitive length of the period is $P(b) = k - 1$. This leads to $q\, b = j\, (2^{k-1} \mp 1) > 0$, i.e., $q = q'\, j$, with positive integer q' because $j \nmid b$. Therefore, j drops out and $2^{k-1} \equiv \pm 1 \,(\mathrm{mod}\, b)$. Thus, $P(b) = pes(b) = \underline{A003558}((b-1)/2)$. $\qquad\square$

In order to see the close relationship to the *MDS*-system the following *lemma* will establish the connection to the mod* congruence.

Lemma 19.

$$R(a(b,\, i)\, 2^k,\, \rho(b)) \;=\; 2\cos\left(\frac{\pi\, a(b,\, i)\, 2^k}{b}\right) \;=\; \pm 2\cos\left(\frac{\pi\, \widehat{j}}{b}\right) \quad \text{with}\;\; \widehat{j} = mod^*(a(b,\, i)\, 2^k,\, b)\,,$$

$$(22)$$

and the sign is $+$ for $x := mod(a(b,\, i)\, 2^k,\, 2\, b) \in I := (0,\, \frac{b}{2})$ or $x \in IV := [\frac{b}{2},\, b)$, and the sign is $-$ if $x \in II := [b,\, \frac{3b}{2})$ or $x \in III := [\frac{3b}{2},\, 2b-1)$.

The identification of the unsigned $2\cos(\frac{\pi\,\widehat{j}}{b})$ values with length ratios diagonal/radius in a regular $(2\, b)$-gon are then obtained with the help of equation (15).

Proof. First note that the first term ($k = 1$) is only positive if $0 < a(b,\, i) \leq \frac{b-1}{4}$. The only negative case for $a(b,\, 1) = 1$ is $IcoS(3,\, 1) = \{-1\}$. Larger seeds are only needed for $b = 17, 31, 33, \ldots$ (\underline{A333855}), and seem to lead always to positive values of the first term. *E.g.*, even for $b = 127$ with $P(127) = 7$ and $c^*(127) = 9$ the largest seed is $21 < 31 = \lfloor\frac{b-1}{4}\rfloor$.

It is always possible to simplify to $\pm 2\cos(\frac{\pi\,\widehat{j}}{b})$ based on the periodicity of cosine, which implies that only $mod(a(b,\, i)\, 2^k,\, 2\, b)$ enters. Consider the four intervals I to IV, given in the *lemma*, with signs $+,\, -,\, -,\, +$ of $2\cos(\pi\, x/b)$, respectively. Here $x = mod(a(b,\, i)\, 2^k,\, 2\, b)$ is a positive integer $\in [1,\, 2\,(b-1)]$. If $x_1 \in I$ then $x_1 = mod(x_1,\, b) = mod^*(x_1,\, b)$ because $x_1 \leq \lfloor\frac{b}{2}\rfloor < \frac{b}{2}$, and its cosine value is positive. If $x_4 \in IV$ one has $mod(x_4,\, b) = x_4 - b \in II$. Hence $mod^*(x_4,\, b) = mod(-x_4,\, b) = -x_4 + 2\, b \in I$. Similarly for $x_2 \in II$ and for $x_3 \in III$, both with negative cosine values, leading to $mod^*(x_2,\, b) = -x_2 + b \in I$, and $mod^*(x_3,\, b) = -x_3 + b \in I$, respectively. $\qquad\square$

Definition 20. Complete system IcoS
The iteration procedure $\{R^{[k]}(2,\, x)\}_{k \geq 1}$ uses first the seed $x = 2\cos(\frac{\pi}{b}) = \rho(b)$. If in the period $IcoS(b,\, 1) = \{R(1 \cdot 2^k,\, \rho(b))\}_{k \geq 1}^{P(b)}$, consisting after trigonometric simplifications of terms $\pm 2\cos\left(\frac{\pi\,\widehat{j}}{b}\right)$ (shown in the preceding lemma), all odd and even numbers $\widehat{j} \in RRS^*(b)$ appear then only this seed $a(b,\, 1)$ is needed, and $IcoS(b) = IcoS(b,\, 1)$ is complete. Otherwise

another iteration is started using a seed $2 \cos(\pi\, a(b,\, 2)/b)$ *with the smallest odd member* $a(b,\, 2) \in RRS^*(b)$ *that did not appear in* $IcoS(b,\, 1)$. *This gives the period* $IcoS(b,\, 2) = \{R(a(b,\, 2) \cdot 2^k,\, \rho(b))\}_{k \geq 1}^{P(b)}$, *etc., and the* $IcoS(b)$ *system is complete after all numbers of* $RRS^*(b)$ *have been reached.*

Example 21.

$$
\begin{aligned}
b = 17, \; P(b) \;&=\; 4, \; c^*(b) = 2: \\
IcoS(17,\, 1) \;&=\; \{2 \cos(\pi\,(2/17)),\, 2 \cos(\pi\,(4/17)),\, 2 \cos(\pi\,(8/17)),\, -2 \cos(\pi\,(1/17))\} \\
&=\; \{1.8649...,\, 1.4780...,\, .1845...,\, -1.9659...\}. \\
IcoS(17,\, 2) \;&=\; \{2 \cos(\pi\,(6/17)),\, -2 \cos(\pi\,(5/17)),\, -2 \cos(\pi\,(7/17)),\, -2 \cos(\pi\,(3/17))\} \\
&=\; \{.8914...,\, -1.2052...,\, -.5473... -1.7004...\}. \qquad\qquad (23)
\end{aligned}
$$

Theorem 22. *The complete system* $IcoS(b)$*, with* $b = 2\,n + 1$*, consist of* $c(b) = \dfrac{\varphi(b)}{2\,P(b)} =$ [A135303](#)(n) *disjoint periods* $IcoS(b,\, i)$ *of length* $P(b) =$ [A003558](#)(n)*, and each number* $\widehat{j} \in RRS^*(b)$ *appears once in the elements* $\pm 2 \cos\left(\dfrac{\pi\,\widehat{j}}{b}\right)$ *of this set of complete periods.*

Proof. By construction of $IcoS(b)$ (definition 20) every odd number $\widehat{j}$ of $RRS^*(b)$ is in one of the periods $IcoS(B,\, i)$. The proof for the even numbers $\widehat{j}$ can be taken over, *mutatis mutandis*, from *Theorem* 12, *4* and *5*. $\qquad\qquad\square$

This shows that $IcoS(b)$ is very similar to the $MDS(b)$ (see the recurrence 14), but works with signed cosine values. The signs have to be ignored for the interpretation as diagonal/radius lengths ratios in the regular $(2\,b)$-gon. Therefore, the $MDS(b)$ system is preferred because it works with positive integers and maps to positive cosine and sine values.

5 Equivalence of the three complete systems

A1) MDS(b) $\Longrightarrow \Sigma$(b)

The proof will be given element-wise: $MDS(b,\, i) \Longrightarrow \Sigma(b,\, i)$, for odd $b \geq 3$ and $i = 1,\, 2,\, ...,\, c^*(b)$. The elements of $MDS(b,\, i)$ are $c(b,\, i)_j$, abbreviated as c_j, for $j = 1,\, 2,\, ...,\, P(b)$. It has been shown in *Theorem* 12 *5.* that $c^*(b) = c(b)$, and in 12 *2.* that $P(b) = k(b)$.

For the proof the recurrence relation of the odd members of $MDS(b,\, i)$ will be needed. For this one considers the cycle $MDS'(b,\, i)$ with the input $a(b,\, i)$ as first element c'_0, and $c'_j = c_j$, for $j = 1,\, 2,\, ...,\, P(b) - 1$. This MDS' appears (in a different notation) in [6], at the top of p. 103, in the proof of the quasi-order theorem.

Lemma 23. Recurrence for odd elements of MDS′(b, i)

The odd elements of $MDS'(b,\, i)$*, collected in the list* $Co'(b,\, i)$ *with elements* $co'(b,\, i)_j = co'_j$*, for* $j = 0,\, 1,\, ...,\, r^*(b,\, i) - 1$*, satisfy the recurrence relation (with* $l'_j = l'(b,\, i)_j$*)*

$$
co'_j \;=\; b - 2^{l'_j}\, co'_{j-1}, \quad \text{for} \;\; j = 1,\, 2,\, ...,\, r^*(b,\, i) - 1, \qquad\qquad (24)
$$

with input $co'_0 = a(b, i)$, and $i \in \{1, 2, ..., c^*(b)\}$. The l'-tuple of length $r^*(b, i)$ gives the differences of the indices ind of consecutive odd numbers in $MDS'(b, i)$. Its elements are

$$l'_j = ind(co'_j) - ind(co'_{j-1}), \quad for \ j = 1, 2, ..., r^*(b, i), \tag{25}$$

with $ind(co'_{r^*(b, i)}) = P(b)$.

Proof. Between the two consecutive odd numbers $co'_{j-1} = c'_{\sum_{i=1}^{j-1} l'_i}$ and $co'_j = c'_{\sum_{i=1}^{j-1} l'_i + l'_j}$ (empty sums vanish) there are $l'_j - 1$ doublings in MDS', and for the next odd number the second version of the recurrence of the $c' = c$ elements given in equation (15) of *Proposition 13*, applies. This means that $co'_j = b - 2(2^{l'_j - 1}) co'_{j-1} = b - 2^{l'_j} co'_{j-1}$. $\square$

For the odd elements of of $MDS(b, i)$, given by $Co(b, i) = [co(b, i)_1, ..., co(b, i)_{r^*(b, i)}]$, this translates to

Corollary 24. Recurrence for odd elements of MDS(b, i)

$$\begin{aligned} co(b, i)_j &= b - 2^{l'(b, i)_j} co(b. i)_{j-1}, \quad for \ j = 2, 3, ..., r^*(b, i), \\ and \ co(b, i)_1 &= b - 2^{l'(b, i)_1} a(b, i). \end{aligned} \tag{26}$$

Example 25. $b = 63$, $i = 2$: $P(63) = 6$, $r^* = 4$, $MDS = [10, 20, 23, 17, 29, 5]$, $MDS' = [5, 10, 20, 23, 17, 29]$, $Co' = [5, 23, 17, 29]$, $l' = [3, 1, 1, 1]$, *because e.g.,, $l'_1 = ind(23) - ind(5) = 3 - 0 = 3$, and $l'_4 = P(63) - ind(29) = 6 - 5 = 1$.*
Recurrences: $17 = co'_2 = 63 - 2^1 co'_1 = 63 - 2 \cdot 23 = 17$.
$29 = co_3 = 63 - 2^1 co_2 = 63 - 2 \cdot 17 = 29$.

Definition 26. two lists U(b, i) and L(b, i)
Let $MBS(b, i)$, for odd integer $b \geq 3$, and $i \in \{1, 2, ..., c^*(b) = c(b)\}$, be the period of length $P(b) = k(b)$. The elements of the list $MBS(b, i)$ are denoted by $c(b, i)_j$ (abbreviated as c_j). Let the sub-list of odd numbers of $MBS(b, i)$ be denoted by $Co(b, i)$ of length $r^*(b, i)$ with elements co_j (no interchange of the odd elements is allowed). The position (index) of co_j in the list $MBS(b, i)$ is denoted by $ind(co_j)$.

1. *The list $U(b, i)$ has elements u_j, for $j = \{1, 2, ..., r^*(b, i)\}$, given by*

$$u_j = co_{r^*(b, i) - j + 1}, \tag{27}$$

   i.e., the odd numbers of $MBS(b, i)$ are read backwards.

2. *The list $L(b, i)$ has elements l_j, for $j = \{1, 2, ..., r^*(b, i)\}$, given by*

$$l_j = ind(u_j) - ind(u_{j+1}), \quad with \ ind(u_{r^*(b, i)+1}) := 0, \tag{28}$$

   i.e., the number of steps to go in $MDS(b, i)$ backwards from one odd number to the next is counted (in a cyclic manner) .

Example 27. $b = 63$, $c^*(63) = 3$, $P(63) = 6$.
$MDS(63, 3) = [22, 19, 25, 13, 26, 11]$, $Co(63, 3) = [19, 25, 13, 11]$, $r^*(63, 3) = 4$,
$ind(19) = 2$, $ind(25) = 3$, $ind(13) = 4$, $ind(11) = P(63) = 6$.
$U(63, 3) = [11, 13, 25, 19]$, $length(U(63, 3)) = r(63, 3) = 4$.
$L(63, 3) = [2, 1, 1, 2]$, $length(L(63, 3)) = length(U(63, 3))$.

Proposition 28. *Let $MBS(b, i)$, $U(b, i)$ and $L(b, i)$ be as in the definition above, then*

$$U(b, i) = A(b, i), \quad and \ \ U(b, i) = K(b, i), \tag{29}$$

with the upper and lower lines $A(b, i)$ and $K(b, i)$ of the coach $\Sigma(b, i)$, respectively.

Proof. By definition of $U(b, i)$ the length $r^*(b, i)$ has been identified with $r(b, i)$, the length of coach $\Sigma(b, i)$. This is possible because the recurrence of the $MDS(b, i)$ elements c_j, when considered modulo b, satisfy the third equation of the *Corollary* 14. This implies, with *Proposition* 12, *3*, that $a(b, i) = c_{P(b)} = \mod(a(b, i) (-1)^{r^*(b, i)} 2^{P(b)}, b)$ because the number of sign flips starting with c_1, ending with $c_{P(b)}$ is the number $r^*(b, i)$ of odd numbers of $MDS(b, i)$. The input $a(b, i) < (b-1)/2$ and coprime to b drops out, and from $P(b) = k(b)$ and the quasi-order theorem 3 one can identify $r^*(b, i)$ with $r(b, i)$.

From $U(b, i)$ and $L(b, i)$ the recurrence for coaches, equation (1), can be proved by identifying $l(b, i)_j$ with $k(b, i)_j$. The reversed $l-$tuple is l', with $l'(b, i)_j = l(b, i)_{r^*(b, i)-j+1}$. The input of $MDS(b, i)$ is $A(b, i)_1 = a(b, i) = u(b, i)_1 = co(b, i)_{r^*(b, i)}$. With equation (25) one has to prove

$$b - co(b, i)_{r^*(b, i)-j+1} = 2^{l(b, i)_j} co(b, i)_{r^*(b, i)-j}, \quad for \ \ j = 1, 2, ..., r^*(b, i) - 1. \tag{30}$$

The input is now $co(b, i)_{r^*(b, i)} = a(b, i)$. An index change $\bar{j} = r^*(b, i) - j + 1$, and the relation between l and l' gives

$$co(b, i)_{\bar{j}} = b - 2^{l'(b, i)_{\bar{j}}} co(b, i)_{\bar{j}-1}, \quad for \ \ \bar{j} = 2, 3, ..., r^*(b, i), \tag{31}$$

and the input is now $co(b, i)_1 = b - 2^{l'(b, i)_1} a(b, i)$. But this is the proved recurrence from *Corollary* 24 equation (26). $\square$

A2) $\Sigma(\mathbf{b}) \Longrightarrow \mathbf{MDS(b)}$

The proof for this direction has essentially been given by *Hilton* and *Pedersen* [6], pp. 102 - 103, in their proof of the quasi-order theorem. It will be recapitulated here in a different notation.

Definition 29. [6] **Modified Coach Symbol MCSy(b, i)**
For fixed odd $b \geq 3$ and $i \in \{1, 2, ..., c(b)\}$ the modified coach symbol $MCSy(b, i)$ has upper line $Cy(b, i)$ with odd numbers (in the following the argument (b, i) will be mostly suppressed)

$$cy_j = a_{r+2-j}, \ for \ j = 1, 2, ..., r+1, \tag{32}$$

with the upper line coach numbers a_j from $A(b, i)$, of length $r = r(b, i)$, and $a_{r+1} = a_1$, hence $cy_1 = a_1 = cy_{r+1}$.

The lower line $Ly(b, i)$ of length r has elements

$$ly_j = k_{r+1-j}, \quad for \ j = 1, 2, ..., r, \tag{33}$$

with the lower line coach numbers $k_j = k(b, i)_j$ from $K(b, i)$.

$$\sum_{j=1}^{r} ly_j = \sum_{j=1}^{r} k_j = k(b), \quad \text{for each } i. \tag{34}$$

Definition 30. [6] **Extended Modified Coach Symbol EMCSy(b, i)**

Between each cy_j and cy_{j+1} of the upper line $Cy(b, i)$ of $MCSy(b, i)$ $ly_j - 1$ consecutive doublings of cy_j are inserted. This results in a one line list $EMCSy(b, i)$ of length $k(b) + 1$ but now with offset index 0.
With $s_j := \sum_{q=1}^{j} ly_q$ (where $s_0 = 0$), the elements n_q of $EMCSy(b, i)$, for $q = 0, 1, ..., k(b) - 1$, are formally

$$n_{s_j + p(j)} = 2^{p(j)} cy_{j+1}, \quad for \ p(j) = 0, 1, ..., ly_{j+1} - 1, \quad and \quad n_{k(b)+1} = cy_1, \tag{35}$$

for $j \in \{0, 1, ..., r(b, i) - 1\}$.

Example 31. $b = 63$, $i = 2$, $k(63) = 6$, $r(63, 2) = 4$.
$A = [5, 29, 17, 23]$, $K = [1, 1, 1, 3]$; $Cy = [5, 23, 17, 29, 5]$, $Ly = [3, 1, 1, 1]$.
$EMCSy(63, 2) = [5, 2^1 \cdot 5, 2^2 \cdot 5, 23, 17, 29, 5] = [5, 10, 20, 23, 17, 29, 5]$.

This shows, with the *Example* 25, that $EMCSy(63, 2)$ without its last entry coincides with $MDS'(63, 2)$, and without its first entry it becomes $MDS(63, 2)$.

Proposition 32. MDS(b, i) from EMCSy(b, i)

For odd $b \geq 3$, and $i \in \{1, 2, ..., c(b)\}$, the extended modified list $EMCSy(b, i)$, derived from the coach symbol $\Sigma(b, i)$, gives without its first term $n_0 = a(b, i)$ the modified modular doubling sequence $MDS(b, i)$.

Proof. The recurrence relation with input $a(b, i)$ for $EMCSy(b, i)$ given in [6]. p. 103, equation (7.13), for the entries n_q (here with offset $q = 0$), coincides with the one given in *Corollary* 14, equation (16) for the $MDS(b, i)$ entries c_j. ☐

B1) MDS(b) $\Longrightarrow$ SBB(b)

The proof will be given element-wise: $MDS(b, i) \Longrightarrow SBB(b, i)$, for odd $b \geq 3$ and $i \in \{1, 2, ..., c^*(b)\}$. It has been shown in *Proposition* 12 5. that $c^*(b) = B(b)$, and in 12 2. that $P(b) = pes(b)$. The fixed arguments (b, i) will be mostly suppressed.

The $SBB(b, i)$ recurrence for elements q_j from equation (8) with input $q_0 = a(b, i)$, an odd integer from $RRS^*(b)$, will be proved to follow from the recurrence *Proposition* 13, equation (15), for the $MDS(b, i)$ cycle elements c_j with input $a(b, i) = c_{P(b)}$ from *Proposition* 12 3..

Proposition 33. SBB(b, i) from MDS(b, i)

The elements of the (positive) $SBB(b, 1)$ cycle are given by

$$q_j = b - 2\,c_{P(b)-1+j}, \quad for \ \ j = 0, 1, ..., pes(b), \tag{36}$$

where c_j are the elements of the cycle $MDS(b, i)$ of length $P(b) = pes(b)$. $c_{P(b)+l} = c_l$, for $l \in \mathbb{N}$ (cyclicity). Hence the input is $q_0(b, i) = c(b, i)_{P(b)} = a(b, i)$.

Example 34. $b = 63$, $i = 2$, $P = 6 = pes$, $MDS(63, 2) = [10, 20, 23, 17, 29, 5]$:
$q_0 = = 63 - 2\,c_5 = c_6 = 5$, $q_1 = 63 - 2\,c_6 = 53$, $q_2 = 63 - 2\,c_7 = 63 - 2\,c_1 = 43$, $q_3 = 63 - 2\,c_2 = 23$, $q_4 = 63 - 2\,c_3 = 17$, $q_5 = 63 - 2\,c_4 = 29$, *hence* $SBB(63, 2) = (5, 53, 43, 23, 17, 29)$.

Proof. The recurrences fit because $2\,c_j = b - |\,b - 4\,c_{j-1}\,|$ from *Corollary* 14. Thus

$$
\begin{aligned}
q_j &= b - (b - |\,b - 4\,c_{P(b)-2+j}\,|) = |\,b - 4\,c_{P(b)-2+j}\,| \\
&= |\,b - 2\,(b - 2\,c_{P(b)-2+j})\,| = |\,b - 2\,q_{j-1}\,|.
\end{aligned}
\tag{37}
$$

The input $a(b, i)$ relation holds because of the recurrence equation (15), the lower line, because $c_{P(b)} = a(b, i)$ is odd, hence $q_0 = b - 2\,c_{P(b)-1} = c_{P(b)} = a(b, i)$. $\square$

B2) SBB(b) $\Longrightarrow$ MDS(b)

This direction is clear from reading **B1)** backwards. One can use cyclicity of $SBB(b, i)$ and replace $q_{j+1-pes(b)}$ by q_{j+1}, and use $q_{pes(b)} = q_0$ and $q_{pes(b)+1} = q_1$.

Proposition 35. MDS(b, i) from SBB(b, i)

The elements of the cycle $MDS(b, i)$ are given by

$$c_j = \frac{1}{2}\,(b - q_{j+1}), \quad for \ \ j = 1, 2, ..., P(b), \tag{38}$$

where q_j are the elements of the cycle $SBB(b, i)$ of length $pes(b) = P(b)$. $q_{pes(b)+l} = q_l$, for $l \in \mathbb{N}_0$ (cyclicity). Hence the input is $a(b, i) = c(b, i)_{P(b)} = q_0(b, i)$.

Proof. Use in **B1)** the index change $j' = P(b) - 1 + j$, cyclicity of $SBB(b, i)$, and the recurrence for q_j. For example, the equation for the input $a(b, i)$ is now $c_{P(b)} = \frac{1}{2}\,(b - q_{P(b)+1}) = \frac{1}{2}\,(b - q_1) = q_0 = a(b, i)$ from the recurrence $q_1 = |\,b - 2\,q_0\,| = b - 2\,a(b, i)$, because $RRS^*(b) \ni a(b, i) \leq \frac{b-1}{2}$. $\square$

Example 36. $b = 63$, $i = 3$, $P = 6 = pes$, $SBB(63, 3) = (11, 41, 19, 25, 13, 37)$:
$c_1 = \frac{1}{2}\,(63 - q_2) = \frac{1}{2}\,(63 - 19) = 22$, ..., $c_5 = \frac{1}{2}\,(63 - q_6) = \frac{1}{2}\,(63 - q_0) = 26$, $c_6 = \frac{1}{2}\,(63 - q_1) = 11$, *hence* $MDS(63, 3) = [22, 19, 25, 13, 26, 11]$.

6   Acknowledgments

References

[1] H M. Abramowitz and I. A. Stegun, eds.,*Handbook of Mathematical Functions*, National Bureau of Standards Applied Math.Series 55, Tenth Printing, 1972.

   http://www.convertit.com/Go/ConvertIt/Reference/AMS55.ASP?Res=150&Page=797&Submit=G

[2] Tom M. Apostol, *Introduction to Analytic Number Theory*, Springer, 1986

[3] Gerold Brändli and Tim Beyne, Modified Congruence Modulo n with Half the Amount of Residues, https://arxiv.org/abs/1504.02757, arXiv:1504.02757 [math.NT], 2016.

[4] David M. Burton, *Elementary Number Theory*, Revised Printing, 1980, Allyn and Bacon, Inc. .

[5] Robert P. Devaney, *A First Course in Chaotic Dynamical Systems*, Addison-Wesley Publishing Company, Inc., 1992, p. 25.

[6] Peter Hilton and Jean Pedersen, *A Mathematical Tapestry*, Cambridge University Press, 2010, 3rd printing 2012.

[7] Jay Kappraff and Gary W. Adamson, Polygons and Chaos, Journal of Dynamical Systems and Geometric Theories, Vol 2 (2004), pp. 67 - 80.

   http://archive.bridgesmathart.org/2001/bridges2001-67.pdf.

[8] Wolfdieter Lang, The field $\mathbb{Q}(2 \cos(\pi/n))$, its Galois group and length ratios in the regular n-gon, https://arxiv.org/abs/1210.1018, arXiv:1210.1018v2 [math.GR], 2012 (2017).

[9] Ki-Suk Lee, Ji-Eun Lee, Gerold Brändli, and Tim Beyne, Galois Polynomials from Quotient Groups, J. Chuncheong Math. Soc., 31,3 (2018), http://koreascience.or.kr/article/JAKO201825677732892.page.

[10] Maple, https://maplesoft.com/products/Maple/.

[11] Trygve Nagell, *Introduction to Number Theory*, Chelsea publishing company, New York, 1964.

[12] Ivan Niven and Herbert S. Zuckerman, *Einführung in die Zahlentheorie I*, BI Hochschultaschenbücher, Band 46, Bibliographisches Institut Mannheim/Wien/Zürich, 1985.

[13] The On-Line Encyclopedia of Integer Sequences (2010), published electronically at http://oeis.org.

[14] Theodore J. Rivlin, *Chebyshsev polynomials*, second ed,.1990, John Wiley & Sons.

[15] Andreas Speiser, *Die Theorie der Gruppen von endlicher Ordnung.* Birkhäuser Verlag, Basel and Stuttgart, 1956.

[16] Carl Schick, *Trigonometrie und unterhaltsame Zahlentheorie*, Bokos Druck, Zürich, 2003, ISBN 3-9522917-0-6.

Concerned with OEIS sequences:
A000010, A000265, A001622, A003558, A023022, A038566, A053120, A055034, A065942, A082375, A082654, A127672, A135303, A187360, A216319, A216371, A232624, A268923, A332433, A332434, A332435, A332436, A332437, A332439, A333848, A333849, A333850, A333851, A333853, A333855, A334430.

Table 1: $\mathbf{P}^*(\mathbf{b}, \mathbf{x})$ for $\mathbf{b} = \mathbf{2\,n} + \mathbf{1}$, $\mathbf{n} = 1, 2, ..., 10$, with $\boldsymbol{\rho} = \boldsymbol{\rho}(\mathbf{b})$

n	b	$\mathbf{P}^*(\mathbf{b}, \mathbf{x})$
1	3	$x - 1$
2	5	$x^2 + (1 - 2\,\rho)\,x + 1$
3	7	$x^3 + (3 - 2\,\rho^2)\,x^2 + 2\,\rho\,x - 1$
4	9	$x^3 - 2\,\rho\,x^2 + (-3 + 2\,\rho^2)\,x - 1$
5	11	$x^5 + (-1 + 6\,\rho^2 - 2\,\rho^4)\,x^4 + (-4 - 2\,\rho + 2\,\rho^2 + 2\,\rho^3)\,x^3$ $+(1 + 8\,\rho - 8\,\rho^2 - 4\,\rho^3 + 2\,\rho^4)\,x^2 + (3 + 4\,\rho - 12\,\rho^2 - 2\,\rho^3 + 4\,\rho^4)\,x - 1$
6	13	$x^6 + (1 - 6\rho + 8\rho^3 - 2\rho^5)x^5 + (-3 - 2\rho - 4\rho^2 + 2\rho^3 + 2\rho^4)x^4$ $+(-6 + 14\,\rho + 10\,\rho^2 - 12\,\rho^3 - 4\,\rho^4 + 2\,\rho^5)\,x^3 + (2 + 16\,\rho - 24\,\rho^3 + 6\,\rho^5)\,x^2 + (1 - 14\,\rho + 10\,\rho^3 - 2\,\rho^5)\,x + 1$
7	15	$x^4 + (3 - 8\,\rho - 2\,\rho^2 + 2\,\rho^3)\,x^3 + (-18\,\rho + 6\,\rho^3)\,x^2 + (-2 - 10\,\rho + 2\,\rho^3)\,x + 1$
8	17	$x^8 + (1 + 8\,\rho - 20\,\rho^3 + 12\,\rho^5 - 2\,\rho^7)\,x^7 + (-7 + 4\,\rho + 8\,\rho^2 - 6\,\rho^3 - 8\,\rho^4 + 2\,\rho^5 + 2\,\rho^6)\,x^6$ $+(-26\rho - 38\rho^2 + 60\rho^3 + 36\rho^4 - 30\rho^5 - 8\rho^6 + 4\rho^7)x^5 + (9 - 46\rho + 124\rho^3 - 6\rho^4 - 80\rho^5 + 2\rho^6 + 14\rho^7)x^4$ $+(52\rho + 32\rho^2 - 142\rho^3 - 24\rho^4 + 84\rho^5 + 4\rho^6 - 14\rho^7)x^3 + (-12 + 8\rho + 68\rho^2 - 52\rho^3 - 52\rho^4 + 36\rho^5 + 10\rho^6 - 6\rho^7)x^2$ $+(-20\rho + 6\rho^2 + 20\rho^3 - 2\rho^4 - 4\rho^5)x + 1$
9	19	$x^9 + (-1 + 20\rho^2 - 30\rho^4 + 14\rho^6 - 2\rho^8)x^8 + (-8 - 4\rho + 8\rho^2 + 14\rho^3 - 8\rho^4 - 10\rho^5 + 2\rho^6 + 2\rho^7)x^7$ $+(3 + 22\rho - 78\rho^2 - 60\rho^3 + 96\rho^4 + 42\rho^5 - 36\rho^6 - 8\rho^7 + 4\rho^8)x^6$ $+(29 - 14\rho - 156\rho^2 + 38\rho^3 + 244\rho^4 - 30\rho^5 - 120\rho^6 + 6\rho^7 + 18\rho^8)x^5$ $+(-17 - 8\rho + 254\rho^2 - 8\rho^3 - 350\rho^4 + 8\rho^5 + 156\rho^6 - 2\rho^7 - 22\rho^8)x^4$ $+(-20 - 30\rho + 112\rho^2 + 90\rho^3 - 136\rho^4 - 56\rho^5 + 52\rho^6 + 10\rho^7 - 6\rho^8)x^3$ $+(8 + 22\rho - 90\rho^2 - 28\rho^3 + 84\rho^4 + 20\rho^5 - 24\rho^6 - 4\rho^7 + 2\rho^8)x^2$ $+(5 + 10\rho - 54\rho^2 - 10\rho^3 + 54\rho^4 + 2\rho^5 - 18\rho^6 + 2\rho^8)x - 1$
10	21	$x^6 + (-1 - 12\rho + 10\rho^3 - 2\rho^5)x^5 + (-10 - 26\rho - 2\rho^2 + 16\rho^3 + 2\rho^4 - 2\rho^5)x^4$ $+(36\rho + 16\rho^2 - 26\rho^3 - 6\rho^4 + 4\rho^5)x^3 + (18 + 60\rho - 10\rho^2 - 44\rho^3 + 2\rho^4 + 8\rho^5)x^2 + (10 + 10\rho - 18\rho^2 - 4\rho^3 + 4\rho^4)x + 1$
⋮		

Table 2: MDS(b) for b = 2 n + 1, n = 1, 2, ..., 35.

n	b	MDS(b, i), i = 1, 2, ..., c*(b)
1	3	[1]
2	5	[2, 1]
3	7	[2, 3, 1]
4	9	[2, 4, 1]
5	11	[2, 4, 3, 5, 1]
6	13	[2, 4, 5, 3, 6, 1]
7	15	[2, 4, 7, 1]
8	17	[2, 4, 8, 1], [6, 5, 7, 3]
9	19	[2, 4, 8, 3, 6, 7, 5, 9, 1]
10	21	[2, 4, 8, 5, 10, 1]
11	23	[2, 4, 8, 7, 9, 5, 10, 3, 6, 11, 1]
12	25	[2, 4, 8, 9, 7, 11, 3, 6, 12, 1]
13	27	[2, 4, 8, 11, 5, 10, 7, 13, 1]
14	29	[2, 4, 8, 13, 3, 6, 12, 5, 10, 9, 11, 7, 14, 1]
15	31	[2, 4, 8, 15, 1], [6, 12, 7, 14, 3], [10, 11, 9, 13, 5]
16	33	[2, 4, 8, 16, 1], [10, 13, 7, 14, 5]
17	35	[2, 4, 8, 16, 3, 6, 12, 11, 13, 9, 17, 1]
18	37	[2, 4, 8, 16, 5, 10, 17, 3, 6, 12, 13, 11, 15, 7, 14, 9, 18, 1]
19	39	[2, 4, 8, 16, 7, 14, 11, 17, 5, 10, 19, 1]
20	41	[2, 4, 8, 16, 9, 18, 5, 10, 20, 1], [6, 12, 17, 7, 14, 13, 15, 11, 19, 3]
21	43	[2, 4, 8, 16, 11, 21, 1], [6, 12, 19, 5, 10, 20, 3], [14, 15, 13, 17, 9, 18, 7]
22	45	[2, 4, 8, 16, 13, 19, 7, 14, 17, 11, 22, 1]
23	47	[2, 4, 8, 16, 15, 17, 13, 21, 5, 10, 20, 7, 14, 19, 9, 18, 11, 22, 3, 6, 12, 23, 1]
24	49	[2, 4, 8, 16, 17, 15, 19, 11, 22, 5, 10, 20, 9, 18, 13, 23, 3, 6, 12, 24, 1]
25	51	[2, 4, 8, 16, 19, 13, 25, 1], [10, 20, 11, 22, 7, 14, 23, 5]
26	53	[2, 4, 8, 16, 21, 11, 22, 9, 18, 17, 19, 15, 23, 7, 14, 25, 3, 6, 12, 24, 5, 10, 20, 13, 26, 1]
27	55	[2, 4, 8, 16, 23, 9, 18, 19, 17, 21, 13, 26, 3, 6, 12, 24, 7, 14, 27, 1]
28	57	[2, 4, 8, 16, 25, 7, 14, 28, 1], [10, 20, 17, 23, 11, 22, 13, 26, 5]
29	59	[2, 4, 8, 16, 27, 5, 10, 20, 19, 21, 17, 25, 9, 18, 23, 13, 26, 7, 14, 28, 3, 6, 12, 24, 11, 22, 15, 29, 1]
30	61	[2, 4, 8, 16, 29, 3, 6, 12, 24, 13, 26, 9, 18, 25, 11, 22, 17, 27, 7, 14, 28, 5, 10, 20, 21, 19, 23, 15, 30, 1]
31	63	[2, 4, 8, 16, 31, 1], [10, 20, 23, 17, 29, 5], [22, 19, 25, 13, 26, 11]
32	65	[2, 4, 8, 16, 32, 1], [6, 12, 24, 17, 31, 3], [14, 28, 9, 18, 29, 7], [22, 21, 23, 19, 27, 11]
33	67	[2, 4, 8, 16, 32, 3, 6, 12, 24, 19, 29, 9, 18, 31, 5, 10, 20, 27, 13, 26, 15, 30, 7, 14, 28, 11, 22, 23, 21, 25, 17, 33, 1]
34	69	[2, 4, 8, 16, 32, 5, 10, 20, 29, 11, 22, 25, 19, 31, 7, 14, 28, 13, 26, 17, 34, 1]
35	71	[2, 4, 8, 16, 32, 7, 14, 28, 15, 30, 11, 22, 27, 17, 34, 3, 6, 12, 24, 23, 25, 21, 29, 13, 26, 19, 33, 5, 10, 20, 31, 9, 18, 35, 1]
⋮		