Karlsruhe
October 03 2012

The field $\mathbb{Q}(2\cos\left(\frac{\pi}{n}\right))$, its Galois group, and length ratios in the regular n-gon

Wolfdieter Lang[1]

Abstract

The normal field extension $\mathbb{Q}(\rho(n))$, with the algebraic number $\rho(n) \;:=\; 2\,\cos\left(\frac{\pi}{n}\right)$, for $n \in \mathbb{N}$, is related to ratios of the lengths between diagonals and the side of a regular $n-$gon. This has been considered in a paper by P. Steinbach. These ratios, numbered $k = 1, ..., n-1$, are given by *Chebyshev* polynomials $S(k-1, x = \rho(n))$. The product formula for these ratios was found by *Steinbach* and is re-derived here from a known formula for the product of *Chebyshev* $S-$polynomials. It is shown that it follows also from the $S-$polynomial recurrence and certain rules following from the trigonometric nature of the argument $x = \rho(n)$. The minimal integer polynomial $C(n, x)$ for $\rho(n)$ is presented, and its simple zeros are expressed in the power-basis of $\mathbb{Q}(\rho(n))$. Also the positive zeros of the *Chebyshev* polynomial $S(k-1, \rho(n))$ are rewritten in this basis. The number of positive and negative zeros of $C(n, x)$ is determined. The coefficient $C(n, 0)$ is computed for special classes of n values. Theorems on $C(n, x)$ in terms of monic integer *Chebyshev* polynomials of the first kind (called here $\hat{t}$) are given. These polynomials can be factorized in terms of the minimal C-polynomials. A conjecture on the discriminant of these polynomials is made. The *Galois* group is either $Z_{\delta(n)}$, the cyclic group of the order given by the degree $\delta(n)$ of $C(n, x)$, or it is a direct product of certain cyclic groups. In order to determine the cycle structure a novel modular multiplication, called *Modd* n is introduced. On the reduced odd residue system *Modd* n this furnishes a group which is isomorphic to this *Galois* group.

1 Introduction and Summary

Length ratios between diagonals and the side of a regular $n-$gon (called diagonal/side ratios, abbreviated DSRs) have been considered by Steinbach [29]. He gave a product formula for these ratios (called by him diagonal product formula (DPF)), and for the pentagon and heptagon details were given. In the pentagon case the quadratic number field $\mathbb{Q}(\sqrt{5})$ with the basis $< 1, \varphi >$ for integers of this field turns up. Here φ, the golden section, is identified with $\rho(5)$ which is the length ratio between any of the two diagonals and the pentagon side. For the heptagon there are two different diagonal length and the two ratios between them and the side length have been called $\rho := \rho(7)$ and σ. The DPF allowed to reduce all products and quotients of ρ and σ to $\mathbb{Q}$-vectors with the basis $< 1, \rho, \sigma >$. For example, $\rho^2 \;=\; 1 + \sigma$, and one can use instead the power basis $< 1, \rho, \rho^2 >$ of the algebraic number field $\mathbb{Q}(\rho(7))$ (the use of the same acute bracket notation for different bases should not lead to a confusion). The minimal polynomial of $\rho(7)$, in the present work called C(7,x), is $x^3 - x^2 - 2\,x + 1$, and this was also given in [29]. Therefore, $[\mathbb{Q}(\rho(7)) : \mathbb{Q}] \;=\; 3$, which is the degree of this field extension. For odd n, $n = 2\,k + 1$, Steinbach gave a polynomial with one of its roots $\rho(2\,k+1)$. In the present work the minimal polynomial for $\rho(n)$, called C(n,x), for every $n \in \mathbb{N}$, is given in terms of the known one for $\cos\left(\frac{2\,\pi}{N}\right)$, called $\Psi(N, x)$, with $N = 2\,n$. The connection between $\Psi(N, x)$ and divisor product representations of N, and to *Chebyshev* $T-$polynomials has been worked out earlier by the author. See the links under OEIS [27] A181875 and A007955 (in the sequel OEIS Anumbers will appear without repeating this reference). $C(n, x)$ turns out to be an integer polynomials of degree $\delta(n) \;=$A055034(n) . All its zeros are known, and they are simple.

[1] wolfdieter.lang@kit.edu, http://www-itp.particle.uni-karlsruhe.de/~wl

$\mathbb{Q}(\rho(n))$ is the splitting field for the minimal polynomial $C(n,x)$ of $\rho(n)$. It is a normal extension of the rational field. These C-polynomial zeros are written in the power basis of $\mathbb{Q}(\rho(n))$ with the help of certain scaled *Cheyshev* $T-$polynomials (called here $\hat{t}$ with their integer coefficient array A128672). This array can also be used to rewrite the positive zeros of the *Chebyshev* $S(n-1,x)$ polynomial, related to the DSRs, in this power basis. The use of $S-$polynomial technology allows also for a re-derivation of the product formulae (DPF) for the length ratios between the regular $n-$gon diagonals and side.

In section 2 $S(k-1,\rho(n))$ is shown to yield the DSRs of the regular n-gon. The DPF is also re-derived there, and the independent products are extracted. This is called reduced algebra over $\mathbb{Q}$. In section 3 the minimal polynomial $C(n,x)$ is presented, and its zeros are related to the power basis of the algebraic number field $\mathbb{Q}(\rho(n))$. In section 4 the $\mathbb{Q}$-automorphisms of this field, the *Galois* group $G(\mathbb{Q}(\rho(n))/\mathbb{Q})$, is treated. It is the cyclic group $Z_{\delta(n)}$, except for infinitely many n-values where it is the direct product of cyclic groups, hence non-cyclic. For n from 1..100 there are 30 non-cyclic groups. A novel modular multiplication on the odd numbers, called *Modd* n, is introduced which serves to determine the cycle graph structure of this *Galois* group. The multiplicative group *Modd* n is isomorphic to this *Galois* group.

2 Regular polygon diagonals/side ratios (DSRs)

Motivated by a paper of Steinbach [29] we consider the diagonals and the side in the regular $n-$gon (inscribed in the unit circle). The vertices on the unit circle are called $V_k^{(n)}$, $k=0,....,n-1,\ n\ =\ 2,3,...;$ $V_0^{(n)}$ has coordinates $(1,0)$; the side length (with the radius' length 1 unit) is $s(n)\ =\ 2\ \sin\left(\frac{\pi}{n}\right)$. The length of $\overline{V_0^{(n)}\,V_k^{(n)}}$ is $d_k^{(n)}\ =\ 2\ \sin\left(\frac{\pi\, k}{n}\right)$, for $k=1,...,n-1$, hence $d_1\ =\ s(n)$. We only need one side and the diagonals in the upper half plane, *i.e.* it suffices to consider $k\in\{1,...,\lfloor n/2\rfloor\}$. For even n, the largest diagonal ($k\ =\ \frac{n}{2}$), of length 2, lies on the negative real axis. See *Fig. 1*, and *Fig. 2*, for the case $n\ =\ 10$ (decagon), and for $n\ =\ 11$ (enneagon), respectively. The length ratios of interest, the DSRs, are $R_k^{(n)}\ =\ \frac{d_k^{(n)}}{d_1^{(n)}}$ for the given $k-$values. Here *Chebyshev* $S-$polynomials in their trigonometric form enter the stage (see A049310 for their coefficients):

$$R_k^{(n)}\ =\ S(k-1,\rho(n)), \tag{1}$$

where we use the second ratio (for the smallest diagonal) $\rho(n)\ :=\ R_2^{(n)}\ =\ 2\ \cos\left(\frac{\pi}{n}\right)$. Remember that $S(n,x)\ :=\ U(n,x/2)$ with *Cheyshev* $U-$polynomial (second kind). It is well known that the zeros of the polynomials $S(n-1,x)$ are $x_{k,\pm}^{(n-1)}\ =\ \pm 2\ \cos\left(\frac{k\,\pi}{n}\right)$, for $k\ =\ 1,\ ...,\ \lceil\frac{n-1}{2}\rceil$. Note that in the even n case the zero $x=0$ appears twice from ± 0. The $S-$polynomials are orthogonal polynomials defined on the real interval $[-2,+2]$. Hence their zeros are guaranteed to be simple. They belong to the *Jacobi* class. Due to (anti)symmetry it is sufficient to consider only the positive zeros (we disregard $x=0$ in the even n case). Now also *Chebyshev* $T-$polynomials (first kind; see the coefficient table A053120) enter, which are written in terms of $S-$polynomials. (The $T-$polynomials appear as trace polynomials in a 2×2 transfer matrix when one solves the three term recurrences of these classical orthogonal polynomials.)

$$\begin{aligned} x_k^{(n-1)}\ \equiv\ x_{k,+}^{(n-1)} &=\ 2\,T(k,\rho(n)/2)\ =:\ \hat{t}_k(\rho(n))\ \equiv\ \hat{t}(k,\rho(n)) && (2)\\ &=\ S(k,\rho(n))\ -\ S(k-2,\rho(n))\,,\ \ k=1,...,\left\lfloor\frac{n-1}{2}\right\rfloor\,. && (3)\end{aligned}$$

Note that these positive zeros decrease with k, and that $\hat{t}_k$ is an integer polynomial of degree k because the $S-$polynomials are integer. The coefficient array for these monic $\hat{t}$-polynomials is A127672. In [1] these polynomials are called *Chebyshev C*-polynomials, but we use the letter C for the minimal polynomials of $\rho(n)$. The zeros can be replaced by DSRs from the above given eq. (1).

Positive zeros of $\mathbf{S(n-1,x)}$ from DSRs: $$x_k^{(n-1)} \,=\, R_{k+1}^{(n)} \,-\, R_{k-1}^{(n)}\,. \tag{4}$$

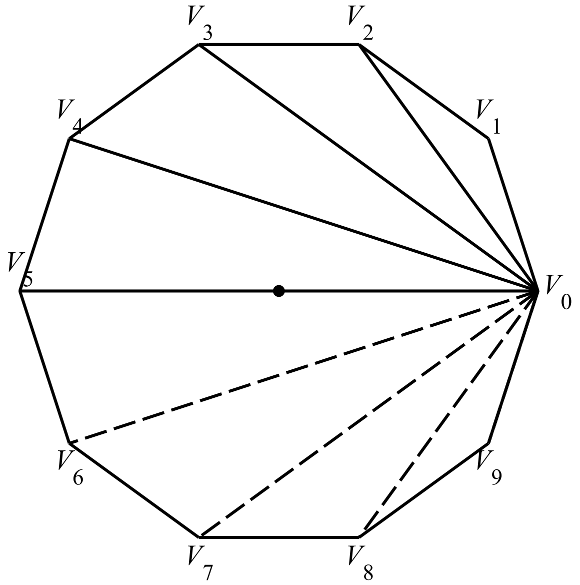


Figure 1: Dekagon $n \,=\, 10$

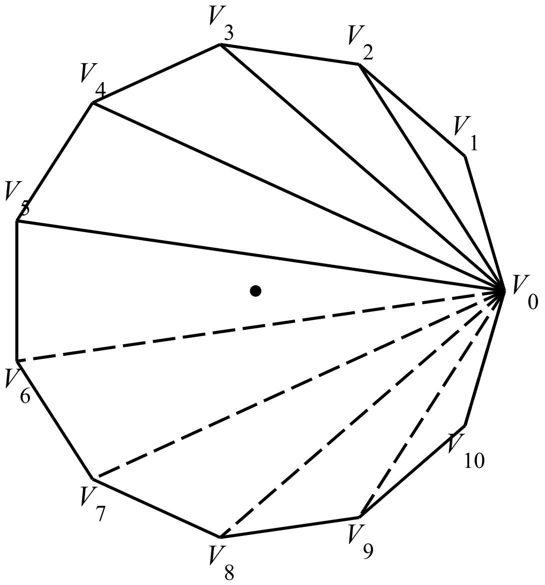


Figure 2: Enneagon (n=11)

As an aside we give the factorization of $S(n-1,x)$ in terms of the polynomial $P(k,x) \,:=\, \prod_{l=1}^{k}\left(x \,-\, 2\,\cos\left(\frac{l\,\pi}{2\,k+1}\right)\right)$ with positive zeros.

$$S(n-1,x) \,=\, x^{\Theta(n-1)}\,P\left(\left\lfloor\frac{n-1}{2}\right\rfloor, x\right)\,(-1)^{\left\lfloor\frac{n-1}{2}\right\rfloor}\,P\left(\left\lfloor\frac{n-1}{2}\right\rfloor, -x\right)\,, \tag{5}$$

where $\theta(n-1) \,:=\, 0$ if n is odd, and 1 if n is even. This factorization is also considered in [4] for the $U(n,x)$ polynomials for even and odd n separately. For example, for the heptagon $n \,=\, 7$ one finds the factorization of $S(6,x)$ with the following real polynomial $P(3,x)$.

$$P(3,x) \,=\, x^3 \,-\, (2\,\sigma(7)-1)\,x^2 \,+\, 2\,\rho(7)\,x \,-\, 1\,, \tag{6}$$

with $\rho(7) \,=\, R_2^{(7)}$ and $\sigma(7) \,:=\, R_3^{(7)}$ (see also the introduction). The three positive zeros are, written in terms of the DSRs, $\rho(7)$, $\sigma(7) \,-\, 1$ and $\sigma(7) \,-\, \rho(7)$. Here we used the general translation formulae eq. (4) to rewrite the positive zeros of $S(n-1,x)$ in terms of DSRs. One should also write this in terms of powers of $\rho(7)$ with the help of eq. (1) (see eq. (7) below).

Each $P\left(\left\lfloor\frac{n-1}{2}\right\rfloor, x\right)$ can be considered as characteristic polynomial for a $(\left\lfloor\frac{n-1}{2}\right\rfloor \,+\, 1)$-term recurrence sequence $\{f_k\}_{k=0}^{\infty}$ in the integral domain of $\mathbb{Q}(\rho(n))$ (represented by a $\delta(n)$-tuple of ordinary (rational) integers $(A_{1,k}, A_{2,k}, ..., A_{\delta(n),k})$. Here $\delta(n)$ is the degree of the minimal polynomial of $\rho(n)$ which will be discussed in sect. 3. In fact, one has $\left\lfloor\frac{n-1}{2}\right\rfloor$ such $\delta(n)$-tuple sequences corresponding to the independent inputs. As a simple example take the $n = 5$ pair $(\delta(5) \,=\, 2)$ of sequences corresponding to $P(2,x) \,=\, x^2-(2\,\varphi-1)\,x+1$, with the golden section $\varphi := \rho(5)$ and the simplest input. This is $S(k,\sqrt{5}) \,=\, A_{1,k}\,1 + A_{2,k}\,\varphi$ with input $S(-1,\sqrt{5}) \,=\, 0$, $S(0,\sqrt{5}) \,=\, 1$. See A005013$(k+1)\,(-1)^k$, and 2 A147600$(k-1)$, for $A_{1,k}$ and $A_{2,k}$, respectively.

For later purposes it is also useful to give a dictionary between the positive zeros of $S(n-1,x)$, *i.e.* those of $P(\left\lfloor\frac{n-1}{2}\right\rfloor, x)$, and powers of $\rho(n)$. One direction follows from the above given formula, eq. (2), for

$x_k^{(n-1)}$ in terms of the monic integer polynomials $\hat{t}(k,\rho) \,=\, 2\,T(k,\rho/2)$. The dependence on n has here been omitted.

Positive zeros of $\mathbf{S(n-1,x)}$ from $\boldsymbol{\rho}\mathbf{(n)}$-powers: $$x_k^{(n-1)} \,=\, \sum_{l=0}^{\lfloor \frac{k}{2} \rfloor} (-1)^l \binom{k-l}{l} \rho(n)^{k-2l}\ . \qquad (7)$$

The coefficients are given in the triangle A127672. *E.g.*, $x_5 \,=\, 5\,\rho \,-\, 5\,\rho^3 \,+\, \rho^5$ (omitting n). For the *heptagon* this shows that the three positive zeros of $S(6,x)$ are $\rho(7)$, $\sigma(7) - 1 \,=\, \rho^2(7) \,-\, 2$ and $\sigma(7) \,-\, \rho(7) \,=\, \rho(7)^2 \,-\, \rho(7) \,-\, 1$. In this case these three zeros could be used as a $\mathbb{Q}$-vector space basis. Note that the n dependence is *via* the $\hat{t}$-polynomial variable $\rho(n)$ (which satisfies $C(n,\rho(n)) = 0$ by definition of the minimal polynomial C). For example, it is true for all n that the second largest positive zero of $S(n-1,x)$, namely $x_2^{(n-1)}$, is always $\rho(n)^2 \,-\, 2$. Hence, from above, $R_3^{(n)} \,-\, 1 \,=\, \rho(n)^2 \,-\, 2$; or if one calls $R_3^{(n)} \;=:\; \sigma(n)$ then $\rho(n)^2 \,=\, \sigma(n) \,+\, 1$. This has been noted for $n = 7$ above but is holds in general, showing that $\sigma(n)$ is algebraically dependent on $\rho(n)$. This fact has been observed already in [29] where it appeared as a special product formula (see the later DPF eq. (13), $m \,=\, k \,=\, 2$, or eq. (11) with $k \,=\, 2$).

The inverse formulae (DSRs in terms of ρ-powers) have already been given above in eq. (1). Here one uses the S-triangle A049310 for the translation. *E.g.*, $R_4^{(n)} \,=\, -2\,\rho(n) \,+\, \rho^3(n) \,=\, \rho(n)\,(\rho(n)^2 \,-\, 2) \,=\, \rho(n)\,(\sigma(n) \,-\, 1)$. Of course, $R_4^{(n)}$ is interesting only for $n \geq 9$ because only then the corresponding diagonal lies in the upper half-plane (including the negative real axis).

Note that the number of positive zeros of $S(n-1,x)$, *i.e.*, $\lfloor \frac{n-1}{2} \rfloor$, is less or equal to $\lfloor \frac{n}{2} \rfloor$, the number of DSRs for diagonals in the upper half plane including the negative real axis. The zero $x \,=\, 1$ never appears. As can be seen in the $n = 7$ case these zeros can nevertheless be used as $\mathbb{Q}$-vector space basis (in sect. 3 it will become clear that the degree $\delta(7)$ is also 3). In the case $n \,=\, 9$ the two numbers are both 4, but the degree $\delta(9)$ is 3, hence only three of the zeros and three of the DSRs are rationally independent. To wit: $x^{(8)} \,=\, -5\,x_3^{(8)} \,+\, 3\,x_1^{(8)} \,-\, 4\,x_2^{(8)}$ and $R_4^{(9)} \,=\, R_1^{(9)} \,+\, R_2^{(9)} \,=\, 1 \,+\, \rho(9)$.

Because of symmetry only DSRs for diagonals of the upper half plane (including the negative real axis), *i.e.*, $k \,\in\, \{0, 1, ..., \left\lfloor \frac{n}{2} \right\rfloor\}$, are of interest. The reduction for other k values, also negative ones, is accomplished by the rules

$$\textbf{o)}\ R_{n+k}^{(n)} \,=\, -R_k^{(n)} \quad , \quad \textbf{i)}\ R_{-|k|}^{(n)} \,=\, -R_{|k|}^{(n)} \quad , \quad \textbf{ii)}\ \textbf{for}\ k \in \{\left\lfloor \frac{n}{2} \right\rfloor + 1, \,...,\, n\} \ :\ R_k^{(n)} \,=\, R_{n-k}^{(n)}\ . \qquad (8)$$

These rules follow from eq. (1) with the trigonometric definition (with the specific value of $\rho(n)$) of the S-polynomials, and therefore also negative values for the DSRs show up (the interesting DSRs are, of course, positive). **i)** follows also from $S(-|n|,x) \,=\, -S(|n|-2,x)$ which derives from a backward use of the recurrence (given later in eq. (12)). This rule does therefore not depend on the special choice of the variable x, in contrast to the rules **o)** and **ii)**. With negative k one counts the diagonals in the clockwise direction. **ii)** is used to translate from the lower to the upper half-plane.

The product formula for *Chebyshev* S-polynomials of different degree, but with the same argument, is well known. See *e.g.*, [1], p.782, 22.7.25, for the U-polynomials, and replace the T-polynomials by the S-polynomials *via* the trace formula given in eqs (2) and (3).

$$\begin{aligned} S(m-1,x)\,S(n-1,x) \,=\, \frac{1}{4\,((\frac{x}{2})^2 \,-\, 1)} \quad & [S(n+m,x) \,-\, S(n+m-2,x) - \\ & S(n-m,x) \,+\, S(n-m-2,x)\,] \quad n \geq m\ . \end{aligned} \qquad (9)$$

For our purpose $x \,=\, \rho(n) \,=\, R_2^{(n)} \,\neq\, \pm 2$ but its special form is for this formula not of interest . It is in fact symmetric under exchange of n with m if the rules for negative indices on the S-polynomials, stated above, are employed. Here we restrict to $n \geq m$ in order to have non-negative indices. Thus the product formula for the DSRs, now with $x = \rho(n)$, but without using its specific value, is

$$(4 - (R_2^{(n)})^2)\, R_m^{(n)}\, R_k^{(n)} = R_{k-m+1}^{(n)} - R_{k-m-1}^{(n)} - R_{k+m+1}^{(n)} + R_{k+m-1}^{(n)}\,,\ k \geq m > 0\,. \tag{10}$$

For $m = 0$ this becomes trivial. This is not yet the DPF given by *Steinbach* in [29] which linearizes the product of $R_m^{(n)}\, R_k^{(n)}$. In order to eliminate the pre-factor $(4 - \rho(n)^2)$ one can use the three term recurrence relation of the orthogonal S-polynomials, written for the DSRs by eq. (1) as a special product formula

$$[\mathbf{Rec}, \mathbf{k}]^{(\mathbf{n})}\ : \qquad R_2^{(n)}\, R_k^{(n)} = R_{k+1}^{(n)} + R_{k-1}^{(n)}\,,\quad k \geq 0\,. \tag{11}$$

From now on we also use the specific form of $\rho(n)$. Thus also rules **o**) and **ii**) of eq. (8) will be applicable. For $k = 0$ one uses (see **ii)**) $R_{-1}^{(n)} = -R_1^{(n)} = -1$, and it becomes trivial. For $k = 2$ it shows that $\rho(n)^2 = \sigma(n) + 1$ for all n, if one uses $\sigma(n) := R_3^{(n)}$. This recurrence can now be used twice as $R_2^{(n)}\,(R_2^{(n)}\, R_k^{(n)})$ in eq. (10) to produce the following recurrence for two step differences of $R_m^{(n)}\, R_k^{(n)} =: p_k^{(n,m)} \equiv p_k$

$$(p_{k+2} - p_k) - (p_k - p_{k-2}) = c_k - c_{k-2}\,, \tag{12}$$

where we used the abbreviation $c_k \equiv c_k^{(n,m)} := R_{k+m+1}^{(n)} - R_{k-m+1}^{(n)}$. This shows that $p_{k+2} - p_k - c_k$ is k independent. From the inputs $p_2 - p_0 - c_0 = 0$, due to the recurrence relation eq. (11), and $p_1 - p_{-1} - c_{-1} = 0$ with the help of the rule **i)** from eq. (8), this leads to the recurrence $p_{k+2} - p_k = c_k$, with the inputs $p_0 = 0$ and $p_1 = -p_1 = R_m^{(n)}$. The solution for p_k is found for even and odd k separately, where again the rules for negative indices are employed. Both solutions can then be combined as

$$\mathbf{DPF}\ \ [\mathbf{m}, \mathbf{k}]^{(\mathbf{n})}\,: \qquad R_m^{(n)}\, R_k^{(n)} = \sum_{j=0}^{k-1} R_{m+k-(2j+1)}^{(n)}\,,\ 1 \leq m \leq k\,. \tag{13}$$

This is finally the DPF found by *Steinbach* in [29] and gives a linearization of the DSR products. We need only to consider $m \geq 2$ ($m = 1$ becomes trivial), and due to the symmetry of this formula under the transformation $k \to n-k$ (using the rules of eq. (8)) is suffices to consider $k \in \{1, 2, \ldots \lfloor \frac{n}{2} \rfloor\}$. Hence one has only to consider the $\binom{\lfloor \frac{n}{2} \rfloor}{2}$ products for $2 \leq m \leq k \leq \lfloor \frac{n}{2} \rfloor$.

The DPF formula looks un-symmetric with respect to $m \leftrightarrow k$, but it is, in fact, symmetric because $\sum_{j=0}^{m-1} R_{k+m-(2j+1)}^{(n)}$ for $k < m$ reduces, due to cancellations after using the rule **i**) from eq (8), to the expected sum with only k terms. One can see this for even and odd $m > k$ separately, remembering that $R_0^{(n)} = 0$ in the former case.

The idea is to work out, for a given $n \geq 4$, all DPFs of interest, using the rules from eq. (8), especially **i**) and **ii**) in order to write all $\binom{\lfloor \frac{n}{2} \rfloor}{2}$ products as linear combinations of the DSRs.

Example 1: $n = 7$ **heptagon**, treated in detail in reference [29]. Here we recapitulate and link to OEIS [27] sequences (the analoga of *Fibonacci* numbers in the pentagon case). Superscripts and arguments 7 are suppressed. [2, 2]: $\rho^2 = \sigma + 1$. [2, 3]: $\rho\,\sigma = \sigma + \rho + 0$. [3, 3]: $\sigma^2 = \rho + \sigma + 1$. Here, $R_5 = R_2$ was used. This shows that the $\mathbb{Q}$-vector space basis is at most $< 1, \rho, \sigma >$. It will be shown to be indeed the heptagon basis in sect. 4, where the power basis will be used instead.

With these DPFs one can compute all powers of interest in the heptagon basis $< 1, \rho, \sigma >$ (this has already been done explicitely for σ in [29], p. 28).

$\rho^k = $ A052547$(k-2)\,1 +$ A052547$(k-1)\,\rho +$ A006053$(k)\,\sigma$, $k \geq 0$,

$\rho^{-k} \,=\,$ A077998$(k)\,1+$ A077998$(k-1)\,\rho-$ A006054$(k+1)\,\sigma,\ k\,\geq 0$,
$\sigma^k \,=\,$ A106803$(k-1)\,1+$ A006054$(k-1)\,\rho+$ A106803$(k)\,\sigma,\ k\,\geq 0,$
$\sigma^{-k} = (\sigma\,-\,\rho)^k \,=\,$ A052547$(k)\,1-$ A006053$(k+1)\,\rho-$ A052547$(k-1)\,\sigma,\ k\,\geq 0,$
$(\rho\,\sigma)^k \,=\, (\rho\,+\,\sigma)^k \,=\,$ A120757$(k)\,1+$ —A006054$(k-1)|\,\rho\,+\,$ 4 A181879$(k)\,\sigma,\ k\,\geq 0,$
$(\rho\,\sigma)^{-k} \,=\, (\rho\,+\,\sigma)^{-k} \,=\,$ A085810$(k)\,1\,+\,(-1)^k$ A181880$(k-2)\,\rho\,+\,(-1)^{k+1}$ A116423$(k+1)\,\sigma,\ k\,\geq 0.$

One can also compute $\dfrac{1}{a\,1\,+\,b\,\rho\,+\,c\,\rho} \,=\, A\,1\,+\,B\,\rho\,+\,\sigma$ and find with $N(a,b,c) \,=\, a^3\,-\,b^3\,-\,c^3\,-\,2\,a\,b^2\,-\,a\,b\,c\,+\,a^2\,b\,+\,b^2\,c\,+\,2\,a^2\,c\,-\,a\,c^2\,+\,2\,b\,c^2$

$$A \;=\; \frac{1}{N(a,b,c)}\,(a^2\,-\,b^2\,+\,a\,b\,+\,2\,a\,c\,-\,b\,c)\ \ ,\ \ B\,=\,\frac{1}{N(a,b,c)}\,(b^2\,-\,c^2\,+\,a\,b)\ \ , \tag{14}$$

$$C \;=\; \frac{1}{N(a,b,c)}\,(c^2\,-\,b^2\,+\,a\,c\,-\,b\,c). \tag{15}$$

Example 2: $n\,=\,9$ (**Enneagon**), where we use $\rho\,=\,R_2^{(9)},\ \sigma\,=\,R_3^{(9)}, \tau\,=\,R_4^{(9)}$. $[2,2]:\ \rho^2\,=\,1\,+\,\sigma$, $[2,3]:\ \rho\sigma\,=\,\rho\,+\,\tau$, $[2,4]:\ \rho\tau\,=\,\sigma\,+\,\tau$, $[3,3]:\ \sigma^2\,=\,1\,+\,\tau\,+\,\sigma$, $[3,4]:\ \sigma\,\tau\,=\,\rho\,+\,\sigma\,+\,\tau$, $[4,4]:\ \tau^2\,=\,1\,+\,\rho\,+\,\sigma\,+\,\tau$. This DSR-algebra (over $\mathbb{Q}$) shows that not all ratios (including $R_1^{(n)}\,=\,1$) are linear independent: $\tau\,(\rho\,-\,1)\,=\,\sigma\,=\,\rho^2\,-\,1\,=\,(\rho\,+\,1)\,(\rho\,-\,1)$, *i.e.*, $\tau\,=\,\rho\,+\,1$. Therefore, $\rho^3\,=\,\rho\,(\sigma\,+\,1)\,=\,2\,\rho\,+\,\tau\,+\,2\,=\,3\,\rho\,+\,1$. In sect. 3 we will see that the algebraic number $\rho(9)$ has degree 3, and its minimal polynomial is indeed $C(9,x)\,=\,x^3\,-\,3\,x\,-\,1$. The enneagon basis is thus $<1,\rho,\sigma>$ which can be related to the power basis $<1,\rho,\rho^2>$ (remember that we use the same notation for different bases). The reduced DSR-algebra (the algebra modulo $C(9,\rho)\,=\,0$) is $\rho^2\,=\,1+\sigma$, $\rho\,\sigma\,=\,1\,+\,2\,\rho$, and $\sigma^2\,=\,2\,+\,\rho\,+\,\sigma$.

Remark 1: $[2,2]$ in eq. (13) becomes $(R_2^{(n)})^2\,=\,R_3^{(n)}\,=\,1$, showing that for all interesting values $n\geq 4$ one has $\sigma(n)\,:=\,R_3^{(n)}\,=\,\rho(n)^2\,-\,1$. This is known already from eq (1) for $k=3$, and it will be used in sect. 3 as $R_3^{(n)}$ rewritten in terms of the power basis of $\mathbb{Q}(\rho(n))$.

Remark 2: For $n\,=\,4$ and $n\,=\,5$ the second diagonal (defining $R_3^{(n)}$) is not of interest because it is in the lower half plane. According to eq. (8), **ii)** $R_2^{(5)}\,=\,R_3^{(5)}$, hence $\sigma(5)\,=\,\rho(5)$ and the general relation $[2,2]$ from eq. (13) between $\sigma(n)$ and $\rho(n)$ leads to $\rho(5)\,=\,\rho(5)^2\,-\,1$, the golden section formula $\rho(5)\,=\,\varphi\,:=\,(1\,+\,\sqrt{5})/2$. In sect. 2 it will be seen that the minimal polynomial for $\rho(5)$ is indeed $C(5,x)\,=\,x^2\,-\,x\,-\,1$.

Instead of deriving the DPF from the product formula for S-polynomials and the rules of eq. (8) one can prove it directly by induction from the $S-$recurrence including negative indices in accordance with these rules.

Proposition 1:

The DPFs $[m,k]^{(n)}$, eq. (13) but now for all $2\,\leq\,m,\ 2\,\leq\,k$, follow from the recurrence, eq. (11), and the rules **i)** and **ii)** from eq. (8).

Proof: This is shown by double induction. First one shows this for given $m\,\geq\,2$ for all $k\,\geq\,2$ by induction over k. Then by induction over m for all $k\geq 2$.

The k-induction uses as starter $[2,2]^{(n)}$ which is the recurrence. Assume that $[2,k']^{(n)}$ is true for all $k'\,=\,2,3,...,k-1$. Now (we omit the superscripts) $R_2\,R_k\,=\,R_2\,(R_2\,R_{k-1}\,-\,R_{k-2})$ from the recurrence. Then use for both terms the induction hypothesis. Note that one obtains for the first term $k-1$, and for the second one $k-2$ terms. However, due to rule **ii)** only two terms survive in each case. (The same type of cancellation was at work when we remarked above on the symmetry of the DPF formula in m and k.) Therefore, one obtains $R_2\,(R_k\,-\,R_{k-2}\,+\,0)\,-\,(R_{k-1}\,-\,R_{k-3}\,+\,0)$ which becomes, after use of the recurrence applied twice, $R_{k+1}\,+\,R_{k-1}$. This is indeed the desired result for $[2,k]$ if one uses again rule **ii)** to get a truncation of the sum after two terms.

The m-induction uses as starter $[2,k]$ for all $k\,\geq 2$, which has just been established. Then assume that $[m',k]$ is true for all $m'\,=\,2,3,...,m\,-\,1$. $R_m\,R_k\,=\,R_2\,R_{m-1}\,R_k\,-\,R_{m-2}\,R_k$ from the recurrence.

Assume the induction hypothesis for each term, obtaining, after use of the recurrence for the first sum, $\sum_{j=0}^{k-1}(R_{m+k-(2j+1)} + R_{m+k-2-(2j+1)}) - \sum_{j=0}^{k-1}(R_{m-2+k-(2j+1)}$ which is indeed the assertion after cancellation of the last two sums. □

As mentioned in the *example 2* the DSR-algebra turns sometimes out to be reducible because some DSRs can be expressed as rational linear combinations of other ones. Later it will become clear that this happens precisely whenever $\lfloor \frac{n}{2} \rfloor - \delta(n) > 0$, and this is the number of linear dependent DSRs. See *Table 1* for details for $n = 3, ..., 12$.

We shall see in *sects. 3* and *4* that it is simpler to use the power basis of $\mathbb{Q}(\rho(n))$ and the minimal $C(n,x)$-polynomials of the algebraic number $\rho(n)$ instead of the DSR-algebra. Then one obtains automatically the reduced algebra.

3 Minimal polynomial of ρ(n), its zeros, absolute term and factorization

The minimal polynomial of an algebraic number α of degree d_α is the monic, minimal degree rational polynomial which has as root, or as one of its roots, α. This degree d_α is 1 iff α is rational, and the minimal polynomial in this case is $p(x) = x - \alpha$. For the notion 'minimal polynomial of an algebraic number' see, *e.g.*, [22], p. 28 or [25] p. 13.

For the algebraic number $\rho(n) := 2\cos\left(\frac{\pi}{n}\right)$, for $n \in \mathbb{N}$, the degree is $\delta(1) = 1$, and $\delta(n) = \frac{\varphi(2\,n)}{2}$ for $n \geq 2$, with *Euler*'s totient function $\varphi(n) =$ *A000010*(n). This is the sequence A055034(n). The sequence of allowed δ values is given in A207333. The array with the indices of the polynomials for given allowed δ values is shown in A207334. Of course, δ is not multiplicative, *e.g.*, $2 = \delta(6) \neq \delta(3)\,\delta(3) = 1 \cdot 1 = 1$. These polynomials can be obtained from the ones of $\cos\left(\frac{2\,\pi}{n}\right)$ which are found, *e.g.*, under A181875/ A181876, and they have been called there $\Psi(n,x)$. See also [17], and [22], Theorem 3.9, p. 37, for the degree $d(n)$ of these polynomials. From the trivial identity $\cos\left(\frac{\pi}{n}\right) = \cos\left(\frac{2\,\pi}{2\,n}\right)$ one finds the minimal polynomial of $2\cos\left(\frac{\pi}{n}\right)$, called here $C(n,x)$, from

$$C(n,x) = 2^{\delta(n)}\,\Psi\left(2\,n, \frac{x}{2}\right) . \tag{16}$$

Therefore the above formula for $\delta(n)$ derives from $d(2\,n)$. These polynomials are given for $n = 1$, ..., 30 in *Table 2*, and the first 15 rows of their coefficient array are shown in *Table 3*. Concerning the parity of the degree δ one has the following lemma.

Lemma 1: Parity of the degree δ

$\delta(n)$ is odd iff $n = 1,\, 2$, and p^e, with an odd prime p of the form $4\,k + 3$, $k \in \mathbb{N}_0$, and $e \geq 1$.

Proof: The case $n = 1$ is clear by definition. For $n = 2$ one uses the prime number factorization $n = 2^\beta \prod_{j=1}^{N} p_j^{e_j}$, with $\beta \geq 0$ and $e_j = 1$. It follows from the definition that $\delta(n) = 2^{\beta-1}\prod_{j=1}^{N}(p_j - 1)\,p_j^{e_j-1}$. For $\beta \geq 2$ this is always even. For $\beta = 0$ one needs $N = 1$, otherwise this will be even. For $N = 1$ one needs $\frac{p-1}{2}$ to be odd, *i.e.*, $p = 4\,k + 3$ with $k \in \mathbb{N}_0$. If $\beta = 1$ one needs $N = 0$ in order to have an odd value. Thus $n = 2$. □

In order to relate to sect. 2 we are interested here in $n \geq 4$. It turns out that these polynomials are in fact integer (not only rational) polynomials. The proof will use the following lemma based on our divisor product representation paper [14].

Lemma 2: Minimal polynomial $\mathbf{C(n,x)}$ written as a rational function.

$$C(n,x) \;=\; \frac{p(d_p(n),x)}{q(d_q(n),x)}\;, \tag{17}$$

with monic *integer* polynomials p and q with a certain degree $d_p(n)$ and $d_q(n) \,=\, \delta_p(n) \,-\, \delta(n)$, respectively.

Proof: $\Psi\left(2\,n,\frac{x}{2}\right)$ is obtained from the unique divisor product representation $dpr(2\,n)$ defined in [14] by replacing each $a(k)$ in the numerator, as well as in the denominator, by $t(k,\frac{x}{2})$ which is given as a difference of monic *integer* polynomials $\hat{t}$ which have been defined already in eq. (2), multiplied with a certain prefactor.

$$t(k,\frac{x}{2}) \;=\; \begin{cases} \frac{1}{2^{\frac{k}{2}+1}}\,\left(\hat{t}(\frac{k}{2}\,+\,1,x)\,-\,\hat{t}(\frac{k}{2}\,-\,1,x)\right) & \text{if } k \text{ is even }, \\ \\ \frac{1}{2^{\frac{k-1}{2}+1}}\,\left(\hat{t}(\frac{k+1}{2},x)\,-\,\hat{t}(\frac{k-1}{2},x)\right) & \text{if } k \text{ is odd}. \end{cases} \tag{18}$$

The monic $\Psi(2\,n,x)$ polynomials have degree $d(2\,n)$ (see *e.g.*, [13]) which implies that all the prefactors in this replacement of the $a(k)$s in $dpr(2\,n)$ have to become $1/2^{d(2\,n)}$. (This could be formulated as a separate lemma). *E.g.*, $n \,=\, 34$ with $dpr(34) \,=\, \frac{a(34)\,a(1)}{a(17)\,a(2)}$ has from the numerator the factor $1/2^{18+1}$ and from the denominator 2^{9+2}, fitting with $1/2^{d(34)}$ because $d(34) \,=\, 8$. Therefore, one may in the calculation of $C(n,x)$, found above from $\Psi(2\,n,\frac{x}{2})$, forget about these prefactors in the replacements altogether. Thus the numerator, *resp.* denominator, is a product of monic integer polynomials $\hat{t}$ leading to the monic integer polynomials p, *resp.* q, of a certain degree $d_p(n)$, *resp.* $d_q(n)$. (One could give more details on these degrees but this is not important here. Trivially, $d_p(n) \,-\, d_q(n) \,=\, d(2\,n)$. For the given example $n = 34$: $(18+1) \,-\, (9+2) \,=\, 8$ from the degrees of the $\hat{t}$ polynomials.) Because C(n,x) is a minimal *polynomial* this rational function allows polynomial division without remainder. □

Proposition 2: $\mathbf{C \in \mathbb{Z}[x]}$

$C(n,x)$, the minimal polynomial of $\rho(n) \,=\, 2\,\cos\left(\frac{\pi}{n}\right)$, is an *integer* monic polynomial.

Proof: From *lemma 2* we have $q(d_q(n),x)\,C(n,x) \,=\, p(d_p(n),x)$ which leads by induction to the result that the integer coefficients of the monic polynomials p and q imply integer coefficients for the monic polynomial C. Call these monic polynomials $q(N,x) := \sum_{l=0}^{N} q_l\,x^l$, $C(M,x) := \sum_{k=0}^{M} c_k\,x^k$ and $p(N+M,x) := \sum_{l=0}^{N+M} p_l\,x^l$ with $q_N = 1$, $c_M = 1$ and $p_{N+M} = 1$. Collecting terms for x^{N+M-j}, for $j = (0), 1,\, 2,\, ...,\, M$, one obtains the formula for the C-coefficient c_{M-j} in terms of lower indexed ones: $c_{M-j} \,=\, p_{N+M-j} - \sum\limits_{k=1}^{j} c_{M-j-k}\,q_{N-k}$. With this the inductive proof on j, using the integer coefficients of q, p and the integer higher C-coefficients due to the induction hypothesis becomes obvious. The starting point is the trivial $j = 0$ case. □

Next we give all the zeros of $C(n,x)$. This follows directly from the knowledge of all zeros of $\Psi(2\,n,\frac{x}{2})$ (see, *e.g.*, [13], from p. 473 of [30])

Proposition 3: All zeros of C

$$C(n,x) \;=\; \prod_{\substack{k=1\\ gcd(k,2\,n)=1}}^{n-1}\left(x \,-\, 2\,\cos\left(\frac{\pi\,k}{n}\right)\right)\;,\; n\in\mathbb{N}\,. \tag{19}$$

In the product the index k starts with 1 because $gcd(0,2\,n) \,=\, 2n$, and it stops at $n-1$ for all $n \geq 2$ because $gcd(n,2\,n) = n$. One has to omit the even k values $>\, 0$ which leads to (for $n \,=\, 1$ one takes only $l\, =\, 0$ in the following product)

$$C(n,x) \;=\; \prod_{\substack{l=0\\ gcd(2\,l+1,n)=1}}^{\lfloor\frac{n-2}{2}\rfloor} \left(x \;-\; 2\,\cos\left(\frac{\pi\,(2\,l+1)}{n}\right)\right)\;. \tag{20}$$

Proof: This is a simple consequence of the mentioned known results for $\Psi(2\,n, \frac{x}{2})$. It implies, *en passant*, a formula for the known degree $\delta(n)$ (see A055034) in terms of the number of factors of this product. □

The following proposition lists the nonnegative and negative zeros of C for prime n. A vanishing zero (which will be counted later as positive) appears only for $n = 2$.

Proposition 4: Non-negative and negative zeros of $\mathbf{C(p,x)}$

i) If $n = 2$ then $C(2,0)\, =\, 0$, and this is the only case with a vanishing zero.

ii) If n is an odd prime $1\,(mod\,4)$ then the number of positive and negative zeros coincides, and this number is $\frac{n-1}{4}$. These zeros are $(-1)^{k+1}\,2\,\cos\left(\frac{\pi\,k}{n}\right)$, with k values $1, 2, ..., \frac{n-1}{2}\, =\, \delta(n)$.

iii) If n is an odd prime $3\,(mod\,4)$ then the number of positive zeros exceeds the number of negative ones by one, and the number of negative ones is $\frac{n-3}{4}$. These zeros are $(-1)^{k+1}\,2\,\cos\left(\frac{\pi\,k}{n}\right)$ with k values $1, 2, ..., \frac{n-3}{2}$, and an extra positive zero appears for $k\, =\, \frac{n-1}{2}\, =\, \delta(n)$.

Proof:

i) Vanishing zeros require $n\, \equiv\, 2\,(mod\,4)$ from $\frac{k}{n}\, =\, \frac{1}{2}$ and k odd in eq. (20). A vanishing zero appears for $n = 2$. For other such n values, $n\, =\, 4\,K\, +\, 2,\ K\, \geq 1$, the odd $k\, =\, \frac{n}{2}\, >\, 1$ divides n, hence it does not appear in the product of eq. (20).

For odd primes $n\, =\, p\, =\, 2\,q + 1$ the product in eq. (20) is unrestricted, and there are $(q-1) + 1\, =\, \dfrac{p-1}{2}$ factors, in accordance with the degree $\delta(p)\, =\, \dfrac{\varphi(2\,p)}{2}$. The *cos* function will produce negative zeros for $\dfrac{2\,l\, +\, 1}{p}\, >\, \dfrac{1}{2}$, *i.e.*, for $2\,l\, \geq q$.

ii) $n\, =\, p\, =\, 4\,K\, +\, 1$ means that $l\, =\, 0,\, 1,\, ...,\, K-1$ lead to positive zeros, and $l\, =\, K,\, K+1,\, ...,\, 2K-1$ to negative ones. In both cases there are $K\, =\, \dfrac{n-1}{4}$ such zeros. For the l values leading to negative zeros one can use the formula $\cos\left(\dfrac{\pi}{p}\,(2\,l+1)\right)\, =\, -\cos\left(\dfrac{\pi}{p}\,(p\, -\, (2\,l+1))\right)$. In this way even multiples of $\dfrac{\pi}{p}$ appear, and one produces, counted backwards, beginning with the largest l value, the new values $2, 4, ..., 2\,K$. This proves **ii)**. As a test consider $n\, =\, 13,\ K\, =\, 3$: the $2\,l\, +\, 1$ values for the positive zeros are 1, 3, 5, and the ones for the negative ones are 7, 9, 11. The latter become (we use underlining to indicate that they come with a minus sign in the final formula) $\underline{6}$, $\underline{4}$, $\underline{2}$. Rearranged these values are 1, $\underline{2}$, 3, $\underline{4}$, 5, $\underline{6}$, as given in **ii)**.

iii) For $n\, =\, p\, =\, 4\,K\, +\, 3$ a similar analysis leads to $l\, =\, 0,\, 1,\, ...,\, K$, and $l\, =\, K+1,\, ...,\, 2\,K$ for positive, and negative zeros, respectively. This shows that the number of negative zeros is $K\, =\, \dfrac{p\, -\, 3}{4}$, and the number of positive ones exceeds the one for negative zeros by one. Again, the odd values leading to negative zeros are transformed to even ones $2,\, 4,\, ...,\, 2\,K$ with a minus sign in front of 2 cos. Take, *e.g.*, $n = 19$, $K\, =\, 4$, with the new k values of **iii)** $1, \underline{2},\ 3,\ \underline{4},\ 5, \underline{6}, 7, \underline{8},\ 9$. □

For general values n one can also find the number of positive and negative zeros of $C(n,x)$. In the non-prime or non-power-of-2 case the *gcd* restriction in the product excludes certain l values. Therefore one has to eliminate from the unrestricted $2\,l\, +\, 1$ values in the product of eq. (20) all odd multiples for each odd prime dividing n. Multiples of 2 are irrelevant for even n , therefore only the odd primes dividing n are of interest. This shows that the prime factors of the *squarefree kernel* of n, denoted here by

$sqfk(n)$, *i.e.*, the largest squarefree number dividing n (see A007947) will be of interest. This squarefree kernel is also known as radical of n, denoted by $rad(n)$. We will denote the set of primes of this kernel by $sqfkset(n)$, *E.g.*, $sqfkset(2^3 \cdot 3^2 \cdot 11) = \{2, 3, 11\}$, $sqfk(2^3 \cdot 3^2 \cdot 11) = 66$ (strip off all exponents in the prime number factorization of n). Because one may encounter multiple counting (*e.g.*, 15 is hit by the multiples of 3 as well as 5 for any n which has in its squarefree kernel set the primes 3 and 5, and which is larger than 16) one can employ *PIE*, the principle of inclusion-exclusion, *e.g.*, [5], p. 134, to get a correct counting.

Proposition 5: Number of positive and negative zeros of $\mathbf{C(n, x)}$

i) If $n = 2^m$, $m \geq 1$, one has for $m = 1$ a vanishing zero (see *proposition 4 i)*). For $m \geq 2$ the number of positive zeros, which is $\frac{n}{4}$, coincides with the one for negative ones. This is in accordance with the degree $\delta(2^m) = 2^{m-1} = \frac{n}{2}$. These zeros lie symmetric: $\pm 2\cos\left(\frac{\pi}{n}(2\,l+1)\right), l = 0, 1, ..., \frac{n}{4} - 1$.

ii) If $n = 1$ then there is only the negative zero -2. If $n \geq 3$ is not a power of 2 then the number of positive zeros, called $\delta_+(n)$, is

$$\delta_+(n) \;=\; K(n) \,+\, \sum_{r=1}^{M(n)} (-1)^r \sum_{<i_1,i_2,\ldots,i_r>} \left\lfloor \frac{1}{2}\left(\frac{L(n)}{p_{i_1}\cdots p_{i_r}} \,-\, 1\right)\right\rfloor \;, \tag{21}$$

where $M(n)$ (sometimes called $\omega(n)$) is in the odd n case the number of elements (cardinality) of the set $sqfkset(n)$, denoted by $|sqfkset(n)|$, (see A001221). $M(n)$ is for even n the number of odd primes in $sqfkset(n)$, *i.e.*, $|sqfkset(n)| - 1$. This is because multiples of 2 are irrelevant here. The sum $< i_1, i_2, ..., i_r >$ extends over the $\binom{M}{r}$ combinations $1 \leq i_1 < i_2 < \ldots < i_r \leq M$. Only the odd primes from the set $sqfkset(n)$ enter. The values $K(n)$ and $L(n)$ depend on the parity of n and they are given by

$$\alpha)\quad n\,\text{even}: \qquad K(n) \;=\; \left\lfloor \frac{n-2}{4} \right\rfloor \;,\quad L(n) \;=\; 2\,K(n) \,+\, 1 \;, \tag{22}$$

$$\beta 1)\; n \quad \text{odd},\; 1(mod\,4): \; K(n) \;=\; \frac{n-5}{4} \quad,\quad L(n) \;=\; 2\,K(n) \,+\, 1 \;=\; \frac{n-3}{2}, \tag{23}$$

$$\beta 2)\; n \quad \text{odd},\; 3(mod\,4): \; K(n) \;=\; \frac{n-3}{4} \quad,\quad L(n) \;=\; 2\,K(n) \,+\, 1 \;=\; \frac{n-1}{2}. \tag{24}$$

Note that also negative values for the floor function may appear. In this way the pure prime case from *proposition* 4 is also included.

iii) If $n \geq 3$ is not a power of 2 then the number of negative zeros, called $\delta_-(n)$, is

$$\delta_-(n) \;=\; N(n) \,+\, \sum_{r=1}^{M(n)} (-1)^r \sum_{<i_1,i_2,\ldots,i_r>} \left\{ \left\lfloor \frac{1}{2}\left(\frac{P(n)}{p_{i_1}\cdots p_{i_r}} \,-\, 1\right)\right\rfloor \,-\, \left\lfloor \frac{1}{2}\left(\frac{L(n)}{p_{i_1}\cdots p_{i_r}} \,-\, 1\right)\right\rfloor \right\} \;, \tag{25}$$

where $M(n)$ and $L(n)$ are as above, and

$$\alpha)\quad n \;\;\text{even}: \qquad N(n) \;=\; \frac{n-2}{2} \,-\, \left\lfloor \frac{n-2}{4} \right\rfloor \;,\quad P(n) \;=\; n \,-\, 1 \;, \tag{26}$$

$$\beta 1)\; n \quad \text{odd},\; 1(mod\,4): \; N(n) \;=\; \frac{n-1}{4} \quad,\quad P(n) \;=\; n \,-\, 2, \tag{27}$$

$$\beta 2)\; n \quad \text{odd},\; 3(mod\,4): \; N(n) \;=\; K(n) \;=\; \frac{n-3}{4} \quad,\quad P(n) \;=\; n \,-\, 2. \tag{28}$$

Proof:

i) All $l\,=\,0,\,..,\,\left\lfloor\frac{n-2}{2}\right\rfloor\,=\,2^{m-1}\,-\,1$ values contribute to the product of eq. (20), compatible with the degree $\delta(2^m)\,=\,\frac{\varphi(2^m)}{2}\,=\,2^{m-1}\,=\,\frac{n}{2}$. The negative zeros appear for $2\,l+1\,=\,2\,2^{m-2}+1,...,n-1$, hence there are $\frac{n}{4}$ of them. With the cos formula given in the proof of *proposition 4* **ii)** with $p\,\to\,n$, they can be rewritten in the notation, also used in the above context, when read backwards, as $\underline{1},\underline{3},...,\underline{2^{m-1}-1}$. Therefore one obtains the same cos arguments like for the $\frac{n}{4}$ positive zeros, only the overall sign is different.

ii) For $n\,\geq\,3$, not a power of 2, one uses PIE to count the positive zeros. For this consider the odd multiples of some odd number a, say $(2\,k\,+\,1)\,a$, (only such multiples come up as $2\,l\,+\,1$ values in the product (20)) up to k_{max} such that all positive zeros are reached. If the largest $2\,l+1$ value in the product which leads to a positive zero is $\bar n$, then $k_{max}\,=\,\left\lfloor\frac{1}{2}\left(\frac{\bar n}{a}\,-\,1\right)\right\rfloor$, and there are $k_{max}\,+\,1$ of these odd multiples of a. In the following application of PIE a will be taken as any odd prime or product of odd primes from the set $sqfkset(n)$.

α) Case even n, not a power of 2: The counting of the positive zeros starts at level $r\,=\,0$ with all positive ones in the unrestricted product eq. (20). There are $\left\lfloor\frac{n-2}{4}\right\rfloor\,+\,1$ of them (the l values are $0,\,1,\,...,\,\left\lfloor\frac{n-2}{4}\right\rfloor$). In the next step, $r\,=\,1$, all odd multiples of every odd prime p_{i_1} in $sqfkset(n)$ not exceeding $2\,\left\lfloor\frac{n-2}{4}\right\rfloor\,+\,1$ are discarded (there are $M(n)$ such primes, where $M(n)\,:=\,|sqfkset(n)|-1$). This leads to a subtraction of the form $-\sum_{i_1=1}^{M(n)}\left\lfloor\frac{1}{2}\left(\frac{L(n)}{p_{i_1}}\,-\,1\right)\right\rfloor\,+\,1$ with $L(n)$ given in the *proposition* **ii)** α). Now double subtractions may have appeared and one adds, at step $r\,=\,2$, all odd multiples of the product of two odd primes from $sqfkset(n)$, call them $p_{i_1}\,p_{i_2}$ with $i_1\,<\,i_2$ (because no problem of over-subtraction appeared for $i_1\,=\,i_2$). This leads to the term $+\sum_{1\,\leq\,i_1<i_2\,\leq\,M(n)}\left\lfloor\frac{1}{2}\left(\frac{L(n)}{p_{i_1}\,p_{i_2}}\,-\,1\right)\right\rfloor\,+\,1$. Now one has to correct for triple products in the step $r\,=\,3$, etc., up to level $r\,=\,M(n)$. This leads to the formula given in part **ii)** α) if one observes that the $+1$ term in each r-sum becomes a $\binom{M(n)}{r}$ term because of the number of terms of this sum. Then, because the alternating sum over row $M(n)$ in *Pascal*'s triangle (see A007318) vanishes ($(1-1)^{M(n)}\,=\,0$), all these terms add up to -1 (the missing $r=0$ term). Therefore the formula starts with $\left\lfloor\frac{n-2}{4}\right\rfloor$, the K(n) value given in **ii)** α), and only the floor term remains for each r-sum .

$\beta1$) The counting of the positive zeros in the odd n case distinguishes the two cases $1\,(mod\,4)$ and $3\,(mod\,4)$. Here we discuss the former one. The procedure is the same as the one given for case α). One has just to determine the boundary values for the l_{max} value leading still to a positive zero. This is $l_{max}\,=\,K-1$, if $n\,=\,4\,K+1$, *i.e.*, $\frac{n-5}{4}$. Hence there are $l_{max}\,+\,1$ such l values to start with at level $r\,=\,0$. Again the extra $+1$ can later be taken as $r\,=\,0$ term $\binom{M(n)}{0}$ for the vanishing alternating sum over row No. $M(n)$ in *Pascal*'s triangle. Here $M(n)\,:=\,|sqfkset(n)|$. Therefore the PIE formula starts with the $K(n)$ given in $\beta1$) of the *proposition*. The $L(n)$ of the PIE sum is now $2\,\frac{n-5}{4}\,+\,1\,=\,\frac{n-3}{2}$, the largest $2\,l\,+\,1$ value leading to a positive zero.

$\beta2$) In the case $M(n)\,:=\,|sqfkset(n)|$, $n\,=\,4\,K\,+\,3$ the maximal $2\,l\,+\,1$ value leading to a positive zero, the $L(n)$ in the formula, is $2\,K\,+\,1\,=\,\frac{n-1}{2}$, coming from the largest l value which is K. This K is the $K(n)$ in the formula claimed for this case $\beta2$).

iii) For the number of negative zeros the counting is done by finding all the odd multiples of odd primes, or products of them, which cover the $2\,l + 1$ range for the negative zeros. This is the difference of the number of such multiples for the whole range and the range for the positive zeros.

α) If n is even, not a power of 2, the whole range is determined by $l_{max} + 1 = n - 1$. From the above **ii)** α) case one knows the corresponding upper bound for the positive zeros, therefore the PIE formula has $N(n) = (\frac{n-2}{2} + 1) - (\left\lfloor \frac{n-2}{4} \right\rfloor + 1)$, the number of factors in the unrestricted product which lead to negative zeros, which is the value claimed in the *proposition* **iii)** α). Accordingly, $P(n) = n - 1$ and $L(n) = 2\left\lfloor \frac{n-2}{4} \right\rfloor + 1$ as given in eq. (26).

$\beta1$) In this $n \equiv 1\,(mod\,4)$ case the maximal number $2\,l + 1$ in the product is $n - 2$, determining $P(n)$. The corresponding number $L(n)$ for the positive zeros is taken from above as $\frac{n-3}{2}$. There are $N(n) = \left(\frac{n-3}{2} + 1\right) - \left(\frac{n-5}{4} + 1\right) = \frac{n-1}{4}$ unrestricted factors in the product with negative zeros.

$\beta2$) In this $n \equiv 3\,(mod\,4)$ case one has also $P(n) = n - 2$ like for any odd n. $L(n)$ is taken from the corresponding **ii)** case as $\frac{n-1}{2}$, and $N(n)$ is obtained from $\left(\frac{n-3}{2} + 1\right) - \left(\frac{n-3}{4} + 1\right) = \frac{n-3}{4}$.

□

We give the first entries of the $\delta_+(n)$ and $\delta_-(n)$ sequences. Remember that the vanishing zero for $n = 2$ is here counted as positive. The A-numbers given for $\delta_-(2\,k)$ and $\delta_-(2\,k)$ are conjectured.

n even:

$\delta_+(2\,k),\ k = 1, 2, ...;$ A055034 : $[1, 1, 1, 2, 2, 2, 3, 4, 3, 4, 5, 4, 6, 6, 4, 8, 8, 6, 9, 8, 6, 10, ...]$,

$\delta_-(2\,k),\ k = 1, 2, ...;$ A055034 with first entry 0 : $[0, 1, 1, 2, 2, 2, 3, 4, 3, 4, 5, 4, 6, 6, 4, 8, 8, 6, 9, 8, 6, 10, ...]$,

n odd, $1(mod\,4)$:

$\delta_+(4\,k + 1),\ k = 0, 1, ...;\ [1, 5, 9, 13, 17, 21, 25, 29, 33, 37, 41, 45, 49, 53, 57, 61, 65, 69, 73, ...]$,

$\delta_-(4\,k + 1),\ k = 0, 1, ...;\ [1, 1, 2, 3, 4, 4, 5, 7, 6, 9, 10, 6, 11, 13, 10, 15, 12, 12, 18, 16, 14, ...]$,

n odd, $3(mod\,4)$:

$\delta_+(4\,k + 3),\ k = 0, 1, ...;\ [1, 2, 3, 2, 5, 6, 5, 8, 6, 6, 11, 12, 8, 10, 15, 10, 17, 18, 10, 20, ...]$,

$\delta_-(4\,k + 3),\ k = 0, 1, ...;\ [0, 1, 2, 2, 4, 5, 4, 7, 6, 6, 10, 11, 8, 10, 14, 8, 16, 17, 10, 19, 20, ...]$.

The start of the sequences for odd n is therefore

$\delta_+(2\,k + 1),\ k = 0, 1, ...;\ [0, 1, 1, 2, 1, 3, 3, 2, 4, 5, 2, 6, 5, 5, 7, 8, 4, 6, 9, 6, 10, 11, ...]$,

$\delta_-(2\,k + 1),\ k = 0, 1, ...;\ [1, 0, 1, 1, 2, 2, 3, 2, 4, 4, 4, 5, 5, 4, 7, 7, 6, 6, 9, 6, 10, 10, 6, 11, ...]$.

Finally, combining for all n:

$\delta_+(n),\ n = 1, 2, ...;$ A193376 : $[0, 1, 1, 1, 1, 1, 2, 2, 1, 2, 3, 2, 3, 3, 2, 4, 4, 3, 5, 4, 2, 5, 6, 4, 5, ...]$,

$\delta_-(n),\ n = 1, 2, ...;$ A193377 : $[1, 0, 0, 1, 1, 1, 1, 2, 2, 2, 2, 2, 3, 3, 2, 4, 4, 3, 4, 4, 4, 5, 5, 4, 5, 6, ...]$.

On can check that $\delta(n) - (\delta_+(n) + \delta_-(n))$ vanishes in each case.

Observe that from these examples it seems that $\delta_+(2\,k) = \delta_-(2\,k) =$ A055034$(k) = \delta(k)$ for $k \geq 2$. This is compatible with $\delta(2\,k) = 2\,\delta(k)$, *i.e.*, $\frac{\varphi(4\,k)}{2} = 2\,\varphi(2\,k)$ for these k values. The latter eq., which holds also for $k = 1$, can be checked by considering the two cases $k = 2^{e(1)} \cdot$ (odd number) and k odd. Recall that $\delta(2) = \delta(1) = 1$, because $\delta(1)$ was special (it is not $\frac{\varphi(2)}{2}$).

Zeros of $\mathbf{C(n, x)}$ in the power basis $< \boldsymbol{\rho}(\mathbf{n})^{\mathbf{0}} = \mathbf{1}, \boldsymbol{\rho}(\mathbf{n})^{\mathbf{1}}, ..., \boldsymbol{\rho}(\mathbf{n})^{\boldsymbol{\delta}(\mathbf{n})-\mathbf{1}} >$

As will be explained in the next section, the minimal polynomial $C(n, x)$ with degree $\delta(n)$ leads to the splitting field $\mathbb{Q}(\rho(n))$ which is a simple field extension of the rational field $\mathbb{Q}$, and the degree of $\mathbb{Q}(\rho(n))$

over $\mathbb{Q}$, the dimension of $\mathbb{Q}(\rho(n))$, considered as a vector space over $\mathbb{Q}$, is just the degree of C. In standard notation $[\mathbb{Q}(\rho(n)) : \mathbb{Q}] = \delta(n)$. Therefore it is interesting to write the zeros of C in the power basis for this $\mathbb{Q}$-vector space. This task is accomplished by using for the zeros $\tilde{\xi}_l^{(n)} = \cos\left(\frac{\pi}{n}(2\,l + 1)\right)$, $l \in \{0, 1, ..., \left\lfloor \frac{n-2}{2} \right\rfloor\}$ with $gcd(2\,l + 1, n) = 1$ (see eq. (20)),the formula $\tilde{\xi}_l^{(n)} = \hat{t}(2\,l + 1, \rho(n)) = 2\,T(2\,l + 1, \frac{\rho(n)}{2})$ (compare with eq. (2)). Remember that the integer coefficient array for these $\hat{t}$-polynomials is shown in A127672. Of course, one has to reduce this integer polynomials using $C(n, \rho(n)) = 0$, *i.e.*, one has to replace $\rho(n)^{\delta(n)}$ (and higher powers) by an integer polynomial of lower degree. This can be done on a computer and *Table 4* has been found with the help of Maple13 [18]. For example, the zeros of $C(15, x)$ are $\tilde{\xi}_1^{(15)} = \rho(15)$, $\tilde{\xi}_2^{(15)} = -2 + 3\,\rho(15) + \rho(15)^2 - \rho(15)^3$, $\tilde{\xi}_3^{(15)} = -1 - 4\,\rho(15) + \rho(15)^3$, $\tilde{\xi}_4^{(15)} = 2 - \rho(15)^2$. Here the reduction has been performed with $\rho(15)^4 \to -\rho(15)^3 + 4\,\rho(15)^2 + 4\,\rho(15) - 1$. One can check these zeros which have approximate values 1.956295201, 0.209056928, −1.338261216 and −1.827090913, respectively. We will call the zeros with increasing value $\xi_1, \xi_2, ..., \xi_{\delta(n)}$.

Our next objective is to compute $C(n, 0)$ (the sign and the number multiplying x^0, also called the absolute term) and relate it first to the cyclotomic polynomial $cy(n, x)$ (the minimal polynomial of the complex algebraic number $e^{\frac{2\pi i}{n}}$, see *e.g.*, [30] or [9], p. 149, Exercise 50 a and b), evaluated at $x = -1$, which is

$$cy(n, -1) = (-1)^{\varphi(n)} \prod_{\substack{k=1 \\ gcd(k,n)=1}}^{n-1} (1 + e^{2\pi\, i \frac{k}{n}}) \ , \ n = 2, 3, ... \tag{29}$$

We used the fact that the product in the definition of $cy(n, x)$ has $\varphi(n)$ factors (the degree as minimal polynomial). For $n = 1$ one has $cy(1, -1) = -2$, which fits this formula if one defines $\varphi(1) := 1$ and takes the undefined product as 1. One may rewrite this for $n \geq 2$ by extracting $e^{\frac{\pi i}{n}}$, using for the sum of the $\varphi(n)$ terms the formula

$$\frac{2}{n^2} \sum_{\substack{k=1 \\ gcd(k,n)=1}}^{n-1} k = \frac{\varphi(n)}{n} \ , \ n = 2, 3, ... \tag{30}$$

This is a formula listed by *R. Zumkeller* under A023022 which is found in[2], p. 48, exercises 15 and 16, written such that both sides depend only on the distinct primes in the prime number factorization of n. For the *r.h.s.* there is the well known formula [2], p. 27, $\frac{\varphi(n)}{n} = \prod_{j=1}^{M(n)} \left(1 - \frac{1}{p_j}\right) = \sum_{d|n} \mu(d)\,\frac{n}{d}$, if n has the distinct prime factors p_j, $j = 1, 2, ..., M(n) =$ A001221(n) $= |sqfkset(n)|$ (see above for the notion ‘squarefree kernel’). The *Möbius* function μ entered here (see A008683). The PIE proof of eq. (30), given in the *appendix A*, uses this form of $\varphi(n)$. If one uses also $e^{i\,\pi} = -1$ the rewritten eq. (29) becomes

$$cy(n, -1) = (-1)^{\frac{\varphi(n)}{2}} \prod_{\substack{k=1 \\ gcd(k,n)=1}}^{n-1} 2\,\cos\left(\pi\,\frac{k}{n}\right) \ , \ n = 2, 3, ... \tag{31}$$

This can also be related to a special *Sylvester* sequence. In general the complex cyclotomic *Sylvester*-numbers $Sy(a, b; n)$ are related to the sequence with three term recurrence $f_n = a\,f_{n-1} + b\,f_{n-2}$, which has characteristic polynomial $x^2 - a\,x - b$ with zeros $\alpha \equiv \alpha(a, b) = (a + \sqrt{a^2 + 4\,b})/2$ and $\beta \equiv \beta(a, b) = (a - \sqrt{a^2 + 4\,b})/2$. The definition is (see *e.g.*, [19])

$$Sy(a, b; n) := \prod_{\substack{k=1 \\ gcd(k,n)=1}}^{n-1} (\alpha - \beta\, e^{2\pi\, i \frac{k}{n}}) \ , \ n = 2, 3, ... \tag{32}$$

For $n = 1$ one takes $Sy(a,b;1) = \alpha - \beta$. For our purpose the values are $(a,b) = (0,-1)$, *i.e.*, $(\alpha,\beta) = (i,-i)$, and

$$Sy(0,-1;n) := (-1)^{\frac{\varphi(n)}{2}} \prod_{\substack{k=1\\ gcd(k,n)=1}}^{n-1} (1 + e^{2\pi i \frac{k}{n}}) \ , \ n = 2, 3, ..., \tag{33}$$

with $Sy(0,-1;1) = 2i$. This can be rewritten, using again eq. (30) and $e^{i\pi} = -1$, as

$$Sy(0,-1;n) = (-1)^{\varphi(n)} \prod_{\substack{k=1\\ gcd(k,n)=1}}^{n-1} 2 \cos\left(\pi \frac{k}{n}\right) \ , \ n = 2, 3, ... \tag{34}$$

Therefore

$$Sy(0,-1;n) := (-1)^{\frac{\varphi(n)}{2}} cy(n,-1) \ , n = 2, 3, ... \tag{35}$$

One could also include the $n = 1$ case, with $\varphi(1) := 1$ if one takes $\frac{1}{i^{\varphi(n)}}$ instead of the prefactor.

After these preliminaries back to the number $C(n,0)$.

Proposition 6: $\mathbf{C(2\,m,0)}$, $\mathbf{m} \in \mathbb{N}$

$$C(2\,m,0) = (-1)^{\frac{\varphi(4\,m)}{2} + \varphi(2\,m)} Sy(0,-1;2\,m) = (-1)^{\frac{\varphi(4\,m)}{2} + \frac{\varphi(2\,m)}{2}} cy(2\,m,-1) \ , \ m \in \mathbb{N}\,. \tag{36}$$

Proof: Use eqs. (19) and (35). The number of factors in eq. (19) with $n = 2\,m$ is $\frac{\varphi(4\,m)}{2}$, the degree $\delta(2\,m)$. Note that the restriction in the $Sy(0,-1;2\,m)$ product is $gcd(k,2\,m) = 1$, while in the $C(2\,m,0)$ product it is $gcd(k,4\,m) = 1$, but this just says that only odd ks can contribute in both cases, and those odd numbers $\leq 2\,m - 1$ dividing $4\,m$ or $2\,m$ have to be omitted. Both restrictions exclude the same odd numbers. □

Corollary 1: $\mathbf{C(2\,p,0)}$, p a prime

$$\text{for prime } p: \quad C(2\,p,0) = (-1)^{\frac{p-1}{2}}\, p \ . \tag{37}$$

Proof:

This follows immediately from eqs. (19) and (31) if one uses the known formulae $cy(2\,p,x) = cy(p,-x)$, $cy(p,1) = p$, and evaluates the φ functions to obtain the sign. This formula follows from $cy(n,x) = \prod_{d|n} (x^d - 1)^{\mu(\frac{n}{d})}$ where the multiplicative *Möbius* function (with $\mu(p) = -1$) enters (see, *e.g.*, [9], exercise 50 b., solution p.506).

Proposition 7: $\mathbf{C(2^m,x)}$, $\mathbf{m} \in \mathbb{N}_0$

$$C(2^m,x) = \hat{t}(2^{m-1},x) \ , \ m \in \mathbb{N}, \tag{38}$$

with the integer polynomials $\hat{t}$ defined in eqs. (2) and (3) in terms of *Chebyshev* T- or $S-$polynomials.

Proof: Use eq. (16) and the *Note added* to the link [13], where it was shown in eq. (8) that $2^{2^{m-1}}\,\Psi\left(2^{m+1},\frac{x}{2}\right) = 2\,T\left(2^{m-1},\frac{x}{2}\right) =: \hat{t}(2^{m-1},x)$, for $m = 1,2,\ldots$. It is clear that $C(1,x) = x + 2$. This *proposition* will later be generalized in *theorem 1A*. □

Corollary 2: $\mathbf{C(2^m,0)}$, $\mathbf{m} \in \mathbb{N}_0$

From the *proposition 7* and the known fact that $T(2\,n,0) = (-1)^n$ follows that

$$C(1,0) = +2, \ \ C(2,0) = 0, \ \ C(2^2,0) = -2, \ \ C(2^m,0) = +2, \ m \geq 3\ . \tag{39}$$

Note that a standard formula for the cyclotomic polynomials $cy(2^m,x)$ which involves divisors (see *e.g.*, [9], p. 149, Exercise 50 b, with $\Psi_m(x) \equiv cy(m,x)$) leads to undetermined expressions for $cy(2^m,-1)$ if $m \geq 1$.

For the following *theorem 1A* on a formula for $C(n,x)$ for even n, based on the divisor product representation (*dpr*) of numbers [14], we need two *lemmata*.

Lemma 3: Pairing in dpr($\mathbf{2\,m}$)

In the divisor product representation of an even number $2\,m$, $m \in \mathbb{N}$, for each a-factor in the numerator (resp. denominator) one finds exactly one a-factor in the denominator (resp. numerator) with argument ratio either $1:2$ or $2:1$.

Proof:

Due to the $*$-multiplication property of *dprs* (see the *theorem* in [14]) it is sufficient to prove this *lemma* for $dpr(2\,p_1 \cdots p_N)$ with odd primes p_1, ..., p_N. Indeed, if the prime factorization of $2\,m$ is $2^{k+1}\,p_1^{e_1} \cdots p_N^{e_N}$, with $k \in \mathbb{N}_0$ and odd primes p_j and positive exponents e_j, for $j = 1, ..., N$, then $dpr(2\,m) = (2^k\,p_1^{e_1-1} \cdots p_N^{e_N-1}) * dpr(2\,p_1 \cdots p_N)$ and the pairing property of the latter *dpr* will be preserved after multiplication of each argument. Now the proof of the pairing property for $dpr(2\,p_1 \cdots p_N)$ becomes elementary, once one splits the products in eq. (7) of [14] (note that N in this reference is now $N+1$) into those a-factors which are even (*i.e.*, contain the even prime 2) and those which are odd (*i.e.*, those composed of only odd primes). Indicate a-factors with odd arguments, being the product of k odd primes, by $a_o(.(k).)$. Then any a-factor in the numerator (resp. denominator) with some even argument $2\,n$ is found in the denominator (resp. numerator) exactly once with the argument n. This is because for each factor in the numerator product $\Pi\, a(2\,.(N-2\,j).)$, with $j \in \{1, ..., \left\lfloor \frac{N}{2} \right\rfloor\}$, say, $a(2\,p_{i_1} \cdots p_{i_{N-2\,j}})$, there is exactly one factor in the denominator product $\Pi\, a_o(.(N-2\,j).)$, namely the one which uses the same $N-2\,j$ odd primes $a(p_{i_1} \cdots p_{i_{N-2\,j}})$. Similarly, for each a-factor in the denominator product $\Pi\, a(2\,.(N-(2\,j+1)).)$, with $j \in \{0, ..., \left\lfloor \frac{N-1}{2} \right\rfloor\}$, there is exactly one factor in the numerator product $\Pi\, a_o(.(N-(2\,j+1)).)$. The first factor in the numerator, $a(2\,p_1 \cdots p_N)$ $(j=0)$ is paired with the single odd argument a-factor of the first product in the denominator $\Pi\, a_o(.(N).) = a(p_1 \cdots p_N)$.
Note, that the example for the primorial A002110(5) = 2310, given in [14], *table* 2 shows that the pairing occurs in general not between numerator and denominator factors at the same position, given the ordering prescription indicated by $\mathcal{O}$ (falling arguments) in eq. (7) in [14]. See the fifth position in the $N = 5$ case there.

Recall also, for later purposes, that because $dpr(2\,m)$ has the same number of factors in the numerator and in the denominator, *viz* 2^N (this balance holds true for all $dpr(n)$, $n \geq 2$, due to *proposition 5* in [14]), after the split into even and odd arguments the number of pairs with even argument in the numerator matches the one with even argument in the denominator. This will later lead to a balanced formula for $C(2\,m, x)$ in terms of $\hat{t}$-polynomials (the same number of $\hat{t}$s in the numerator and in the denominator, *viz* 2^{N-1}) . □

Lemma 4:

$$\frac{\hat{t}(\frac{n}{2}+1,x) - \hat{t}(\frac{n}{2}-1,x)}{\hat{t}(\frac{n}{4}+1,x) - \hat{t}(\frac{n}{4}-1,x)} = \frac{S(\frac{n}{2}+1,x)}{S(\frac{n}{4}-1,x)} = 2\,T\left(\frac{n}{4},\frac{x}{2}\right) = \hat{t}\left(\frac{n}{4},x\right) \;, \text{ for } n \equiv 0\,(mod\,4)\;. \qquad (40)$$

This identity involves the integer polynomials $\hat{t}$ introduced earlier in eqs. (2) and (3).

Proof:

Use the known identity for *Chebyshev* polynomials, [20], p. 261, first line, specialized, $T(m+1,x) - T(m-1,x) = 2\,(x^2-1)\,U(m-1,x)$, written for x replaced by $\frac{x}{2}$, with $S(m-1,x) = U(m-1,\frac{x}{2})$ and the definition of the $\hat{t}$-polynomials from eq. (2). For $n \equiv 0\,(mod\,4)$ this identity can be used in the numerator as well as in the denominator. The $n-$independent factor $(\frac{x}{2})^2 - 1$ drops out if $x \neq \pm 2$. However, the lemma holds also for these $x-$values as can be seen after applying l'Hôpital's rule, using the well known identity $T'(x,n) = n\,U(n-1,x)$. In the second to last step the well known identity, [20] p. 260, last line, written as $2\,T\left(m,\frac{x}{2}\right)\,S(m-1,x) = S(2\,m - 1,x)$ has been employed. $\square$

Theorem 1A: $\mathbf{C(2\,m,x)}$, $\mathbf{m \geq 1}$, in terms of $\hat{\mathbf{t}}$-polynomials

With the prime number factorization of $2\,m = 2^k\,p_1^{e_1}\,\cdots p_N^{e_N}$ with $k \in \mathbb{N}$, odd primes p_j and positive exponents e_j, $j = 1, ..., N$, one has

$$C(2\,m,x) = \frac{\hat{t}(2^{k-1}\,p_1^{e_1}\cdots p_N^{e_N},x)\,\Pi\,\hat{t}(2^{k-1}\,{}_*(N-2).,x)\,\Pi\,\hat{t}(2^{k-1}\,{}_*(N-4).,x)\cdots}{\Pi\,\hat{t}(2^{k-1}\,{}_*(N-1).,x)\,\Pi\,\hat{t}(2^{k-1}\,{}_*(N-3).,x)\cdots}\,. \tag{41}$$

with $\hat{t}(2^{k-1}\,{}_*(0).,x) = \hat{t}(2^{k-1}\,p_1^{e_1-1}\,p_2^{e_2-1}\cdots p_N^{e_N-1},x)$, and the products $\Pi\,\hat{t}(2^{k-1}\,{}_*(K).,x)$ are over the $\binom{N}{K}$ factors with K primes from the set $\{p_1,p_2,...,p_N\}$ multiplied by $p_1^{e_1-1}\,p_2^{e_2-1}\cdots p_N^{e_N-1}$, *i.e.*, K-products of the form $\hat{t}(2^{k-1}\,p_1^{e_1-1}\,p_2^{e_2-1}\cdots p_N^{e_N-1}\,p_{i_1}\,p_{i_2}\cdots p_{i_K},x)$. We used ${}_*(k).$ instead of $.(k).$ for the indices of the $\hat{t}$ polynomials to remind one of the extra factor (without the powers of 2 because the even prime has been extracted everywhere) due to the $*$-multiplication.

Before we give the proof an example will illustrate this *theorem*.

Example 3: $\mathbf{k = 1}$, $\mathbf{N = 2}$

$$C(1350,x) = C(2\cdot 3^3\,5^2,x) = \frac{\hat{t}(3^3\,5^2,x)\,\hat{t}(3^2\,5,x)}{\hat{t}(3^3\,5,x)\,\hat{t}(3^2\,5^2,x)} = \frac{\hat{t}(675,x)\,\hat{t}(45,x)}{\hat{t}(135,x)\,\hat{t}(225,x)}\,. \tag{42}$$

Proof:

This is based on [14] applied for the minimal polynomials $\Psi\left(4\,m,\frac{x}{2}\right)$ (see the definition for $C(2\,m,x)$ given in eq. (16)). Let $2^{k+1}\,p_1^{e_1}\,\cdots p_N^{e_N}$ be the prime number factorization for $4\,m$. Only the squarefree kernel $2\,p_1\cdots p_N$ is important due to the *theorem* in [14] for the divisor product representations (*dpr*s) and the $*$-multiplication. This means that one has to multiply after the computation of $\Psi(2\,p_1\cdots p_N)$, using *proposition 1* of [14], the first argument, the index in conventional notation, of each factor $t(n_i,x)$ in the the numerator, and of each $t(m_i,x)$ in the denominator (see [14], eq. (1)) with the number $2^k\,p_1^{e_1-1}\,p_2^{e_2-1}\cdots p_N^{e_N-1}$. Here the pairing *lemma 3* is crucial which carries over to the indices of the t-factors in the numerator and denominator of [14], eq. (1). Because there is always at least one factor of 2 in the number which multiplies every t index after the $*$-multiplication, the pairing will occur always between indices which are $0\,(mod\,4)$ and $0\,(mod\,2)$. Then only the n even alternative in the definition of $t\left(n,\frac{x}{2}\right)$ from eq. (2) of [14], rewritten here as eq. (18), is relevant. Observe that the prefactors in this definition of $t\left(n,\frac{x}{2}\right)$ are not of interest, provided we take $2\left(T\left(\frac{n}{2}+1,\frac{x}{2}\right) - T\left(\frac{n}{2}-1,\frac{x}{2}\right)\right)$ which is the monic integer polynomial $\hat{t}\left(\frac{n}{2}+1,x\right) - \hat{t}\left(\frac{n}{2}-1,x\right)$. See eq. (18), and the discussion in connection with *lemma 2*. $C(2\,m,x)$ is written here as a rational function of monic integer polynomials. For each replaced $t\left(n,\frac{x}{2}\right)\Big/t\left(\frac{n}{2},\frac{x}{2}\right)$ (either in the numerator or denominator, depending on where the larger index appears), one can apply *lemma 4*. This is how for each such t-quotient one obtains $\hat{t}\left(\frac{n}{4},x\right)$. Here the fact that the larger index of a pair is always equivalent to $0\,(mod\,4)$ is important. From the structure of the numerator and denominator of the original $dpr(2\,m)$ with the separation of the even and odd a-arguments (which carries over to the t-indices), discussed in the proof of *lemma 3*, one now finds the numerators and denominators of the theorem. Just search the products for the even t-indices. *E.g.*, $\Pi\,\hat{t}(2^{k-1}\,{}_*(N-2).,x)$ in the numerator of the *theorem* originates from the quotient of products $\dfrac{\Pi\,t(2\,.(N-2).,\frac{x}{2})}{\Pi\,t_o(.(N-2).,\frac{x}{2})}$ before the $*$-multiplication has to be applied. This leads, with eq. (18) and *lemma 4*, to $\Pi\,\hat{t}\left(\frac{2^{k+1}}{4}\,{}_*(N-2).,x\right)$ after multiplying each $\hat{t}$ index in the product with $2^k\,p_1^{e_1-1}\,p_2^{e_2-1}\cdots p_N^{e_N-1}$, where the $*$ reminds one to multiply each index with this number divided by 2^k.

As announced at the end of the proof of *lemma 3* the number of $\hat{t}$ polynomials in the numerator is the same as the one for the denominator, *viz* 2^{N-1}, which is due to the sum in the *Pascal*-triangle A007318 row No. N over even, resp. odd numbered positions.

Note that this *theorem 1A*, evaluated for $x = 0$ leads in general to undetermined expressions, remembering that $\hat{t}(n,0) = 0$ if n is odd, and $2\,(-1)^{\frac{n}{2}}$ if n is even. However, a correct evaluation (using *l'Hôpital*'s rule) has to reproduce the result known from *corollary 2*.

The following factorization of the monic integer $\hat{t}$-polynomials is related to *theorem 1A*.

Theorem 1B: Factorization of $\hat{\mathbf{t}}$-polynomials in terms of the minimal C-polynomials

$$\hat{t}(n,x) \;=\; \prod_{d|op(n)} C(2\,n/d, x) \;=\; \prod_{d|op(n)} C(2^{k+1}\,d, x)\ , \tag{43}$$

with $op(n)$ =A000265(n), the odd part of n, and 2^k is the largest power of 2 dividing n. The exponents are $k = k(n)$ =A007814(n), $k \in \mathbb{N}_0$.

Before the proof we give an example.

Example 4: n = 10

$$\begin{aligned} &-2 \,+\, 25\,x^2 \,-\, 50\,x^4 \,+\, 35\,x^6 \,-\, 10\,x^8 \,+\, x^{10} \,=\, \hat{t}(10,x) \,=\, C(20,x)\,C(4,x) \,= \\ &(x^8 \,-\, 8\,x^6 \,+\, 19\,x^4 \,-\, 12\,x^2 \,+\, 1)\,(x^2 \,-\, 2)\ . \end{aligned} \tag{44}$$

Proof: This is modeled after a similar proof in [30].

It is clear that both sides are monic integer polynomials. See the definition of $\hat{t}$ in eqs. (2), (3) and *proposition 2*.

In order to check the degree we consider the even and odd n cases separately. If $n = 2^{k(n)}\,op(n)$ with $k(n)$ =A007814$(n) \geq 1$ then $\sum_{d|op(n)} \delta(2^{k+1}\,d) = \sum_{d|op(n)} \frac{\varphi(2^{k+2}\,d)}{2}$ from the known degree δ of the C-polynomials, here for index > 1. Due to well known properties of the *Euler* totient function (see *e.g.*, [2], *Theorem* 2.5, (a) and (c), p. 28 and *Theorem* 2.2., p. 26) this leads to $\frac{2^{k(n)+2} - 2^{k(n)+1}}{2}\,op(n) = n$, the degree of $\hat{t}(n,x)$. In the odd case, if $n = op(n)$ then $\sum_{d|n} \frac{\varphi(4\,d)}{2} = \sum_{d|n} d = n$, again the degree of $\hat{t}(n,x)$.

For the proof one compares the zeros of both sides. The zeros of $\hat{t}(n,x)$ are $\hat{x}_l^{(n)} = 2\,cos\left((2\,l+1)\,\frac{\pi}{2\,n}\right)$ for $l = 0,\,1,\,...,\,n-1$. This is known from the zeros of the *Chebyshev* T-polynomials. The zeros of the $C(2^{k+1}\,d,x)$-polynomials are used in the form given by eq. (20): $2\,cos\left((2\,l'+1)\,\frac{\pi}{2^{k+1}\,d}\right)$ for $l' = 0, 1, ..., 2^k\,d - 1$, where $gcd(2\,l'+1, 2^{k+1}\,d) = 1$, *i.e.*, $gcd(2\,l'+1, d) = 1$. Because the degrees match, it is sufficient to show that each zero of $\hat{t}(n,x)$ occurs on the *r.h.s.*. For $n = 2^k(n)\,op(n)$, with $k(n)$ =A007814(n), consider $gcd(2\,l+1, 2\,n) = gcd(2\,l+1, 2^{k+1}\,op(n)) = gcd(2\,l+1, op(n)) = g$ (some odd number). Hence $2\,l+1 = (2\,l'+1)\,g$, with some l' and $op(n) = d\,g$, *i.e.*, $d|op(n)$. Therefore $\frac{2\,l+1}{2\,n} = \frac{2\,l'+1}{2^{k+1}\,d}$. Thus the $\hat{t}(n,x)$ zero $2\,cos\left((2\,l+1)\,\frac{\pi}{2\,n}\right)$ appears on the *r.h.s.* as one of the $C(2^{k+1}\,d,x)$ zeros. $\square$.

Remark 3: Derivation of Theorem 1A from Theorem 1B

Theorem 1B can be used as recurrence for the C-polynomials in terms of the $\hat{t}$-polynomials. This is similar to the case treated in [30] for the minimal polynomials Ψ of $\frac{2\,\pi}{n}$ (see A181875/A181876 for their coefficients). The solution of this recurrence has been given in [14]. Indeed, *theorem 1A* has been derived above from this solution. Originally we found *theorem 1B* starting from *theorem 1A* building up iteratively a formula for $\hat{t}(2^{k-1}\, p_1^{e_1} \cdots p_N^{e_N}, x)$ in terms of the C-polynomials. We give this formula as a corollary.

Corollary 3: $\hat{\mathbf{t}}$-polynomials in terms of C-polynomials

$$\hat{t}(2^{k-1}\, p_1^{e_1} \cdots p_N^{e_N}, x) \,=\, \prod_{q_1=0}^{e_1} \prod_{q_2=0}^{e_2} \cdots \prod_{q_N=0}^{e_N} C(2^k\, p_1^{q_1}\, p_2^{q_2} \cdots p_n^{q_N}, x)\ , k \,=\, \mathbb{N},\ N \,\in\, \mathbb{N}_0\ . \tag{45}$$

In order to find a simplified expression for $C(2\,m+1, x), m \,\in\, \mathbb{N}_0$ we need the following *lemma* in order to rewrite the quotient $\dfrac{t(even, \frac{x}{2})}{t(odd, \frac{x}{2})}$, given the definition eq. (18).

Lemma 5:

for $n \,=\, 2\,M \,+\, 1, M \,\in\, \mathbb{N}_0$ one has

$$\frac{t\left(2\,n, \frac{x}{2}\right)}{t\left(n, \frac{x}{2}\right)} \;=\; 2^{M-n}\, \frac{\hat{t}(n+1, \frac{x}{2}) \,-\, \hat{t}(n-1, \frac{x}{2})}{\hat{t}(M+1, \frac{x}{2}) \,-\, \hat{t}(M, \frac{x}{2})} \,=\, \frac{1}{2^{M+1}}\, \frac{(x^2 \,-\, 4)\, S(n-1, x)}{(x \,-\, 2)\, S(2\,M, \sqrt{2 \,+\, x}\,)} \tag{46}$$

$$\;=\; \frac{x \,+\, 2}{2^{M+1}}\, \frac{S(n-1, x)}{S(n-1, \sqrt{2 \,+\, x}\,)}\ . \tag{47}$$

Here new important monic integer polynomials enter the stage:

Definition 1: q-polynomials

With $n \,\in\, \mathbb{N}_0$ define

$$q(n, x) \,:=\, \frac{S(2\,n, x)}{S(2\,n, \sqrt{2 \,+\, x}\,)}\ . \tag{48}$$

That this defines indeed monic integer polynomials of degree n is shown by the next *lemma*.

Lemma 6:

$$q(n, x) \,=\, (-1)^n\, S(2\,n\,, \sqrt{2 \,-\, x}\,) \,=\, S(n, x) \,-\, S(n-1, x)\ . \tag{49}$$

Proof:

It is known from the *o.g.f.* of the *Chebyshev* S-polynomials that the bisection yields $S(2\,n, y) \,=\, S(n, y^2 - 2) \,+\, S(n-1, y^2 \,-\, 2)$, or $S(2\,n\,, \sqrt{x \,+\, 2}\,) \,=\, S(n, x) \,+\, S(n-1, x)$. With x replaced by $-x$ one has $S(2\,n, \sqrt{2 \,-\, x}\,) \,=\, (-1)^n\,(S(n, x) \,-\, S(n-1, x))$ which explains the second equation of the *lemma*. Therefore one has to prove $S(2\,n, x) \,=\, S(n, x)^2 \,-\, S(n-1, x)^2$. This identity can, for example, be proved using the *o.g.f.* for the square of the S-polynomials (for their coefficient table see A181878, also for the paper [15] given there as a link). This computation was based on the *Binet-de Moivre* formula for the $S-$polynomials. This *o.g.f.* was found to be $\dfrac{1 \,+\, z}{1 \,-\, z}\, \dfrac{1}{1 \,+\, (2 \,-\, x^2)\, z \,+\, z^2}$. The *o.g.f.* for $\{S(2\,n, x)\}_{n=0}^{\infty}$ is $(1 \,+\, z)/(1 \,+\, (2 \,-\, x^2)\, z \,+\, z^2)$ (from the bisection). Because the *o.g.f.* for $S(n, x)^2 \,-\, S(n-1, x)^2$ is $(1+z)$ times the one for $S(n, x)^2$ the completion of the proof is then obvious. □

Remark 4 : O.g.f. and coefficient array for the q-polynomials

From *lemma 6* the *o.g.f.* $Q(z, x) := \sum_{n=0}^{\infty} q(n, x)\, z^n \,=\, (1 \,-\, z)/(1 - x\, z \,+\, z^2)$ from the known *o.g.f.* of the S-polynomials. This shows that the $q(n, x)$ coefficients constitute a *Riordan*-array (infinite lower triangular ordinary convolution matrix), which is in standard notation $\left(\dfrac{1 \,-\, x}{1 \,+\, x^2}, \dfrac{x}{1 \,+\, x^2}\right)$, meaning that the *o.g.f.* of the column No. m sequence is $\dfrac{1 \,-\, x}{1 \,+\, x^2}\left(\dfrac{x}{1 \,+\, x^2}\right)^m$. This is the triangle A130777 where more information can be found. For example, the explicit form for the coefficients is $Q(n,m) = (-1)^{\frac{n-m+1}{2}} \binom{\frac{n+m}{2}}{m}$ if $n \geq m \geq 0$ and 0 otherwise.

The pairing *lemma 3* will also be used in the proof of the following *theorem.*

Theorem 2A: $\mathbf{C(n,x)}$, $\mathbf{n \geq 3}$, odd, in terms of q-polynomials

With the prime number factorization of $n = p_1^{e_1} \cdots p_N^{e_N}$ with odd primes $p_1, ..., p_N$ and positive exponents e_j, $j = 1, ..., N$, one has

$$C(n,x) = \frac{q\left(\frac{n-1}{2}, x\right) \prod_{i_1<i_2} q\left(\frac{n/(p_{i_1}\,p_{i_2})-1}{2}, x\right) \prod_{i_1<i_2<i_3<i_4} q\left(\frac{n/(p_{i_1}\,p_{i_2}\,p_{i_3}\,p_{i_4})-1}{2}, x\right) \cdots}{\prod_{i_1} q\left(\frac{n/p_{i_1}-1}{2}, x\right) \prod_{i_1<i_2<i_3} q\left(\frac{n/(p_{i_1}\,p_{i_2}\,p_{i_3})-1}{2}, x\right) \cdots} . \tag{50}$$

Here each index i_j of the products runs from 1 to N.

Before we give the proof an examples will illustrates this *theorem.*

Example 5: $\mathbf{n = 3^2 \cdot 5 = 45}$

$$C(45) = C(3^2 \cdot 5) = \frac{q(22,x)\,q(1,x)}{q(7,x)\,q(4,x)} . \tag{51}$$

This checks.

Proof: This is analogous to the proof of *theorem 1A*. Again the $dpr(2\,n)$ representation, from which one derives $\Psi(2\,n,x)$, with the prime number factorization for the odd n, is considered. The $*$-multiplication property allows to consider $dpr(2\,p_1 \cdots p_N)$ with a subsequent multiplication of all arguments in the numerator and denominator by $p_1^{e_1-1} \cdots p_N^{e_N-1}$. Because of the paired numerator/denominator structure due to *lemma 3* one finds, either in the numerator or in the denominator quotients of the type $\frac{t(2\,k,\,\frac{x}{2})}{t(k,\,\frac{x}{2})}$ which are up to a factor $2^{\frac{k+1}{2}}\,(x\,+\,\;2)$ equal to $q\left(\frac{n-1}{2}, x\right)$. Factors of powers of 2 are irrelevant (they have to cancel) because on both sides of *theorem* monic polynomials appear. The factors of $x-2$ also cancel because the number of q-polynomials in the numerator and denominator have also to match (see the remark at the end of the proof of *lemma 3*). This number is 2^{N-1}. The structure of the numerator of the *theorem* originates from products with the even indexed $t\left(2k, \frac{x}{2}\right)$ polynomials in the numerator after $*$- multiplication. Before this multiplication on has in the numerator $t\left(2\,p_1 \cdots p_N, \frac{x}{2}\right)$ and $t-$products over all possibilities to leave out 2, 4, ... of the odd primes from the set $\{p_1,\, ...,\, p_N\}$. The $*$-multiplication then leads to $t\left(n, \frac{x}{2}\right)$ and $t-$products over all possibilities to divide n by these $2, 4, ...$ odd primes. Together with the pairing partners from the denominator this leads to the q-polynomials given in the numerator of the *theorem.* A similar argument produces the denominator q-polynomials. The number of these $q-$polynomials in the numerator, *viz* 2^{N-1} , matches the one for the denominator. □

Theorem 2B: Factorization of q-polynomials in terms of C-polynomials

$$q(n,x) = \prod_{1\,<\,d|(2\,n+1)} C(d,x) \;,\; n \in \mathbb{N} . \tag{52}$$

Example 6: $\mathbf{n = 17}$

$$q(17,x) = C(5,x)\,C(7,x)\,C(35,x) . \tag{53}$$

This checks.

Proof:

This is again modeled after a similar proof in [30]. Compare this with the proof of *theorem 1B*.

It is clear that both sides are monic integer polynomials, and the degree fits due to $n \,=\, \sum_{d|(2\,n+1)} \frac{\varphi(d)}{2} - \frac{1}{2}\,\varphi(1)$. See the properties of the *Euler* totient function mentioned above in the proof of *theorem 1B*. The zeros of $q(n,x)$ are $x_l^{(n)} \,=\, 2\,\cos\left(\pi\,\frac{2l+1}{2n+1}\right)$, for $l \,=\, 0,1,...,n-1$. This follows from *definition 1* and *lemma 6* with the zeros of $S(2\,n,\sqrt{2\,-\,x}\,)$ which are known from those of *Chebyshev* S-polynomials. To show that each of these zeros appears on the *r.h.s.* for $C(d,x)$ with some $d|(2\,n+1), d\,\neq\,1$, *i.e.*, as $2\,\cos\left(\pi\,\frac{2l'+1}{q}\right)$ for some $l' \,\in\, \{0,\,1,\,...,\,\frac{d-3}{2}\}$ and $gcd(2l'+1,d) \,=\, 1$ (see eq. 20), let $gcd(2l+1,2n+1) \,=\, g$, with some odd g with $2\,n+1 \,=\, d\,g$. Then $2\,l\,+\,1 \,=\, (2\,l'\,+\,1)\,g \,=\, (2\,l'\,+\,1)\frac{2n+1}{d}$, and for each $l \,\in\, \{0,\,1,\,...,\,n-1\}$ there is one $l' \,\in\, \{0,\,1,\,...\,,\,\frac{d-3}{2}\}$. □

Remark 5: Derivation of Theorem 2A from Theorem 2B

Theorem 2B can be used as recurrence for the C-polynomials in terms of the q-polynomials. See the *remark 3*. We give the solution in the following *corollary*.

Corollary 4: q-polynomials in terms of C-polynomials

With the prime number factorization of $2\,n+1 \,=\, p_1^{e_1}\cdots p_N^{e_N}$, with odd primes, $n \,\in\, \mathbb{N}$, one has

$$q(n,x) \,=\, \prod_{q_1=0}^{e_1} \cdots \prod_{q_N=0}^{e_N} C(p_1^{q_1}\cdots p_N^{q_N})/C(1,x)\;. \tag{54}$$

The division by $C(1,x) \,=\, x\,+\,2$ was necessary because not all q_j-indices were originally allowed to vanish.

These rational representations of $C(n,x)$ do not lend itself to extraction of the value $C(n,0)$ because undetermined $\frac{0}{0}$ quotients appear. In the following we give the absolute term of C for prime indices.

Proposition 8: $\mathbf{C(p,0)}$

For $n \,=\, p$, a prime, one has

$$C(p,0) \;=\; \begin{cases} 0 & \text{if p } = 2\;, \\ (-1)^{\frac{p-1}{4}} & \text{if p} \equiv 1\,(\text{mod}\,4)\;, \\ (-1)^{\frac{p+1}{4}} & \text{if p} \equiv 3\,(\text{mod}\,4)\;. \end{cases} \tag{55}$$

Proof: In eq. (31) with $n \,=\, p$ there is no *gcd*-restriction on the product. Therefore, one can use a known formula (see *appendix B* for a proof)

$$\prod_{k=1}^{n-1} 2\,\cos\left(\pi\,\frac{k}{n}\right) \;=\; \begin{cases} (-1)^{\frac{n-1}{2}} & \text{if n is odd,} \\ \\ 0 & \text{if n is even,} \end{cases} \tag{56}$$

to obtain $cy(2,-1) \,=\, 0$ (which is also clear from the definition: $cy(2,x) \,=\, x\,+\,1$), and for odd primes $cy(p,-1) \,=\, (-1)^{p-1} \,=\, +1$. Because all k contribute in the product, one can use for even k the formula $\cos\left(\pi\,\frac{2\,K}{p}\right) \;=\; -\cos\left(\pi\,\frac{p\,-\,2\,K}{p}\right)$ which shows that one generates again all odd k contributions, however each with a minus sign. This leads to $cy(p,-1) \,=\, (-1)^{p-1} \prod_{l=0}^{\frac{p-3}{2}} \left(2\,\cos\left(\pi\,\frac{2\,l\,+\,1}{p}\right)\right)^2 \;=\; C(p,0)^2$.

Thus $C(p,0) = \pm 1$. The sign of $C(p,0)$ is $(-1)^{\delta_+(p)}$ from eq. (19) for $n = p$. This number $\delta_+(p)$ of positive zeros has been found in *proposition 5* to be $\frac{p-1}{4}$ if $p \equiv 1\,(mod\,4)$, and $\frac{p+1}{4}$ if $p \equiv 3\,(mod\,4)$. For $C(2,0) = 0$, the sign is, of course, irrelevant. □

We close this section with a conjecture on the discriminant of the $C-$polynomials. The discriminant of a monic polynomial p of degree n can be written as the square of the determinant of an $n \times n$ *Vandermonde* matrix $V_n(x_1^{(n)}, ..., x_n^{(n)})$ with elements $(V_n)_{i,j} := (x_i^{(n)})^j, = 1, ..., n$ and $j = 0, ..., n-1$ with the zeros $x_i^{(n)}$ of p . Here the $\delta(n)$ zeros of C_n are given in eq. (20). Another formula for the discriminant (see *e.g.*, [26], Theorem 5.1, p. 218) is in terms of the derivative $C'(n,x)$ and the zeros of C: $(-1)^{\frac{\delta(n)\,(\delta(n)-1)}{2}} \prod_{i=1}^{\delta(n)} C'(n, x_i^{(n)})$. The result is the sequence $Discr(C(n,x)) =$ A193681$(n) =$ $[1, 1, 1, 8, 5, 12, 49, 2048, 81, 2000, 14641, 2304, 371293, ...]$ for $n \geq 1$. The following conjecture is on the sequence $q(n) = \dfrac{n^{\delta(n)}}{Discr(C(n,x))}$ which is A215041, $[1, 2, 3, 2, 5, 3, 7, 2, 9, 5, 11, 9, 13, 7, 45, 2, 17, 27, 19, 25, ...]$.

Conjecture: explicit form of the q-sequence

o) $q(1) = 1$ (clear).

i) If $n = 2^k$ for $k \in \mathbb{N}$ then $q(n) \overset{!}{=} 2$.

ii) If $n = p^k$ for odd prime p and $k \in \mathbb{N}$ then $q(n) \overset{!}{=} p^{(p^{k-1}+1)/2}$.

iii) if $n = 2^{k_2}\,p(i_1)^{k_{i_1}} \cdots p(i_N)^{k_{i_N}}$ with $k_2 \in \mathbb{N}_0$, the $i_j - th$ odd primes $p(i_j)$, where $2 \leq i_1 < i_2 < ... < i_N$, with $N \in \mathbb{N}$ if $k_2 \neq 0$ and $N \geq 2$ if $k_2 = 0$, then

$$\begin{aligned} q(n) \; &\overset{!}{=} \; \prod_{j=1}^{N} p(i_j)^{2^{k_2-1}\,p(i_1)^{k_{i_1}-1} \cdots p(i_N)^{k_{i_N}-1}\,P(N,j)} \quad \text{, with} \quad P(N,j) = \prod_{l=1, l\neq j}^{N} (p(i_l) - 1) \;, \\ &= \prod_{odd\;\, p|n} p^{\frac{\delta(n)}{p-1}} \;. \end{aligned} \tag{57}$$

The last eq. follows from the degree $\delta(n) = \dfrac{\varphi(2\,n)}{2}$. This last formula does, however, not work in the cases **i)** and **ii)**. One can compare this formula with the proven one for the discriminant of the cyclotomic polynomials (the minimal polynomials of $exp(2\,\pi\,\frac{1}{n})$ (or any of the primitive n-th root of 1), as given in [25], eq. (1) p. 297. For this (slightly rewritten) formula see also A004124 and A193679.

Example 7:

ii) $p = p(4) = 7$, $k = 3$: $q(7^3) = q(343) = 7^{(7^2+1)/2} = 1341068619663964900807$.

iii) $n = 2^3{\cdot}3^2{\cdot}7$, $q(n) = 3^{2^2\cdot 3\cdot 6}\,7^{2^2\cdot 3\cdot 2} = 431601852585283909095465817662614956498091534846320304 1$.

These values have been checked with the help of Maple13 [18].

4 Splitting field $\mathbb{Q}(\rho(\mathbf{n}))$ for $\mathbf{C(n,x)}$, field extension and Galois group

The algebraic number $\rho(n) = 2\,\cos\left(\frac{\pi}{n}\right)$, $n \in \mathbb{N}$, with minimal polynomial $C(n,x)$ over $\mathbb{Q}$ of degree $\delta(n)$, has been studied in sect. 3. Each of these polynomials, being minimal, is irreducible. All roots have been given in eq. (19) (or eq. (20)). $C(n,x)$ is also separable because all of its roots are distinct. Because $2\,\cos\left(\dfrac{\pi\,k}{n}\right) = \hat{t}(k, \rho(n))$ (see eq. (2), and the coefficient array A127672), with the monic integer $\hat{t}$-polynomials, each zero can be written as integer linear combination in the vector space basis $< 1, \rho(n), \rho(n)^2, ..., \rho(n)^{\delta(n)-1} >$, called the power basis. One has to reduce in $\hat{t}(k, \rho(n))$ all powers $\rho(n)^p$,

$p \geq \delta(n)$ with the help of the equation $C(n, \rho(n)) = 0$. See *Table 4* for the zeros of $C(n, x)$, $n = 1, ..., 30$ written in this power basis.

Example 8: n = 8 (octogon)

The $\delta(8) = 4$ zeros of $C(8, x) = x^4 - 4\,x^2 + 2$ are, with $\rho \equiv \rho(8) = \sqrt{2 + \sqrt{2}}$, $\pm\rho$ and $\pm(-3\,\rho + \rho^3) = \pm\sqrt{2 - \sqrt{2}}$. In this case the degree 4 coincides with the number of DSRs in the upper half plane and the negative real axis.

This shows that the extension of the rational field $\mathbb{Q}$, called $\mathbb{Q}(\rho(n))$, obtained by adjoining just one algebraic element (called a simple field extension) is the splitting field (Zerfällungskörper in German) for the polynomial $C(n, x)$. Note that even though the polynomial $C(n, x)$ is from the ring $\mathbb{Z}[x]$ one needs $\mathbb{Q}(\rho(n))$ with rational coefficients r_j for the general element $\alpha = \sum_{j=0}^{\delta(n)-1} r_j\,\rho(n)^j$. For example, $\rho(8)^{-1} = 2\rho(8) - \dfrac{1}{2}\rho(8)^3$. Some references for field extensions and *Galois* Theory are [6], [12], chpts. V and VI, [3], and the on-line lecture notes [16]. The dimension of of $\mathbb{Q}(\rho(n))$ as a vector space over $\mathbb{Q}$ is $\delta(n)$. This is the degree of the extension, denoted usually by $[\mathbb{Q}(\rho(n)) : \mathbb{Q}]$, and it coincides with the degree of the minimal polynomial for $\rho(n)$. Of course, it is a proper extension only if $\delta(n) \geq 2$, *i.e.*, for $n \geq 4$. This extension of $\mathbb{Q}$ is separable, *i.e.*, the minimal polynomial for the general algebraic number α given above is separable (has only distinct zeros). It is a normal field extension, meaning that every irreducible rational polynomial with one root in $\mathbb{Q}(\rho(n))$ splits completely over $\mathbb{Q}(\rho(n))$. See, e.g., [6], Theorem 5.24, p. 108.

We now consider a subgroup of the group of automorphisms of $\mathbb{Q}(\rho(n))$, called $\mathcal{A}ut(\mathbb{Q}(\rho(n)))$, which consists of those elements σ which leave the subfield $\mathbb{Q}$ pointwise invariant (fixed point field $\mathbb{Q}$):
$\sigma : \mathbb{Q}(\rho(n)) \to \mathbb{Q}(\rho(n))$, $\alpha \mapsto \sigma(\alpha)$, with $\sigma(\beta) = \beta$ for all $\beta \in \mathbb{Q}$. The subgroup of $\mathcal{A}ut(\mathbb{Q}(\rho(n))$ of these so-called $\mathbb{Q}$-automorphisms is called the *Galois* group of $\mathbb{Q}(\rho(n))$ over $\mathbb{Q}$, denoted by $\mathcal{G}al(\mathbb{Q}(\rho(n))/\mathbb{Q})$. Occasionally we abbreviate this with $\mathcal{G}_n$. In order to find the elements σ (we omit the label n) of this subgroup it is sufficient to know $\sigma(\rho(n))$, because of the usual rules for automorphisms: *(i)* $\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta)$, *(ii)* $\sigma(\alpha\,\beta) = \sigma(\alpha)\,\sigma(\beta)$, and *(iii)* $\alpha \neq 0 \Rightarrow \sigma(\alpha) \neq 0$. Indeed, because of $\sigma(1) = \sigma(1^2) = \sigma(1)\,\sigma(1)$, one has $\sigma(1) = 1$, and the images of products of $\rho(n)$ are obtained from products of $\sigma(\rho(n))$. Applying σ on the equation $C(n, \rho(n)) = 0$ (minimal polynomial), leads to $C(n, \sigma(\rho(n))) = 0$, because the integer (rational) coefficients and 0 are invariant under the $\mathbb{Q}$-automorphism σ we are looking for. Therefore we have exactly $\delta(n)$ distinct $\mathbb{Q}$-automorphisms σ_j, $j = 0, ..., \delta(n) - 1$, determined from the distinct roots of $C(n, \sigma(\rho(n)))$, *viz* $\sigma_j(\rho(n)) = \tilde{\xi}_{j+1}^{(n)}$ with the zeros of $C(n, x)$ ordered like in eq. (19) with increasing k values (see the *Table 4*). By the same token $C(n, \sigma(\tilde{\xi}_j^{(n)})) = 0$, for $j = 1, ..., \delta(n)$ for every σ. Because all roots are distinct (separable C) this leads to an isomorphism between $\mathcal{G}al(\mathbb{Q}(\rho(n))/\mathbb{Q})$ and a subgroup of the symmetric group $S_{\delta(n)}$. The $\mathbb{Q}$-automorphisms σ can therefore be identified with permutations of the roots of C (see *e.g.*, [6] ch. 6.3, pp. 132 ff. One identifies the roots $\tilde{\xi}_j^{(n)}$ with j, and σ_j with the permutation $\begin{pmatrix} 1 & 2 & \dots & \delta(n) \\ \sigma_j(1) & \sigma_j(2) & \dots & \sigma_j(\delta(n)) \end{pmatrix} \equiv [\sigma_j(1)\,\sigma_j(2)\,...\,\sigma_j(\delta(n))]$. This subgroup of $S_{\delta(n)}$ is Abelian because only products of powers of $\rho(n)$ appear and due to the automorphism property of σ this carries over to the *Galois* group.

Example 9: n = 5 (pentagon) $\mathbb{Q}$-automorphisms

$\alpha = r_0\,1 + r_1\,\rho(5)$ with $\rho(5) = \varphi$, the golden section. In this case $\mathbb{Q}(\varphi)$ is as quadratic number field usually called $\mathbb{Q}(\sqrt{5})$ with the basis $< 1, \varphi >$ for integers in $\mathbb{Q}(\sqrt{5})$ (see *e.g.*, [10], ch. 14.3, p. 207, where $\tau = (\varphi - 1)$). The two ($\delta(5) = 2$) $\mathbb{Q}$-automorphisms are obtained from the solutions $\sigma(\varphi) = \varphi$ or $-\dfrac{1}{\varphi} = 1 - \varphi$ of $C(5, n) = x^2 - x - 1$. Hence $\sigma_0 = id:\ \sigma_0(1) = 1,\ \sigma_0(\varphi) = \varphi$ and $\sigma_1:\ \sigma_1(1) = 1,\ \sigma_1(\varphi) = 1 - \varphi$. Because $\sigma_1^2 = \sigma_0$, $\mathcal{G}_5$ is generated by σ_1, hence the *Galois* group

$\mathcal{G}al(\mathbb{Q}(\varphi)/\mathbb{Q})$ is the cyclic group Z_2 (also known as additive group $\mathbb{Z}/2\,\mathbb{Z}$ or C_2, but we reserve C for the minimal polynomials). The fixed field for $\mathcal{G}_5$ is $\mathbb{Q}$; for the trivial subgroup with element σ_0 it is $\mathbb{Q}(\varphi)$.

Example 10: n = 7 (heptagon) $\mathbb{Q}$-automorphisms

The three zeros ($\delta(7) = 3$) of $C(7, n)$ are $\tilde{\xi}_1^{(7)} = \rho(7)$, $\tilde{\xi}_2^{(7)} = -1 - \rho(7) + \rho(7)^2$ and $\tilde{\xi}_3^{(7)} = 2 - \rho(7)^2$ (see *Table 4*). In the sequel we omit the argument 7. Computing powers of ρ modulo $C(7, \rho) = 0$ one finds the $\mathbb{Q}$-automorphisms $\sigma_0 = id$, $\sigma_1(\rho = \tilde{\xi}_1) = \tilde{\xi}_2$, $\sigma_1(\tilde{\xi}_2) = \tilde{\xi}_3$, $\sigma_1(\tilde{\xi}_3) = \tilde{\xi}_1$ and $\sigma_2(\rho = \tilde{\xi}_1) = \tilde{\xi}_3$, $\sigma_2(\tilde{\xi}_2) = \tilde{\xi}_1$, $\sigma_2(\tilde{\xi}_3) = \tilde{\xi}_2$. Therefore, the identification with S_3 permutations is $\sigma_0 \doteq [1\,2\,3] = e$, $\sigma_1 \doteq [2\,3\,1]$ and $\sigma_2 \doteq [3\,1\,2]$. Each σ_j permutation can be depicted in a circle diagram with vertices labeled $1, 2$ and 3 and directed edges, also allowing for loops. The only (Abelian) group of order three is the cyclic Z_3 subgroup of S_3.

We can also characterize these *Galois* groups $\mathcal{G}_n$ by giving their cycle structure and depict them as cycle graphs. For cycle graphs see, *e.g.*, [31] "Cycle graph" and "List of small groups" with all cycle graphs for groups (also non-Abelian ones) of order 1, ..., 16. In order to manage powers of *Galois* group elements we first need some fundamental identities of *Chebyshev* T-polynomials, whence $\hat{t}$-polynomials.

We will need iterations of $\hat{t}$ polynomials governed by the following well known identity.

Lemma 7: Iteration of $\hat{\mathbf{t}}$-polynomials

$$\hat{t}(n, \hat{t}(m, x)) = \hat{t}(n\,m, x),\ n, m \in \mathbb{N}_0\ . \tag{58}$$

Proof: See [26], Exercise 1.1.6, p. 5, first with the trigonometric definition of *Chebyshev* T-polynomials which then carries over to the general polynomials defined by their recurrence relation. This identity is then rewritten for $\hat{t}$-polynomials. □

Lemma 8: mod n reduction of $\hat{\mathbf{t}}$-polynomials in the variable $\boldsymbol{\rho}(\mathbf{n})$

$$\hat{t}(k, \rho(n)) = (-1)^{\left\lfloor \frac{k}{n} \right\rfloor}\, \hat{t}(k (mod\, n), \rho(n)),\ n \in \mathbb{N}, k \in \mathbb{Z}\ . \tag{59}$$

$(-1)^{\left\lfloor \frac{k}{n} \right\rfloor} =: p_n(k)$, the parity of $\left\lfloor \frac{k}{n} \right\rfloor$, will become important in the following. Sometimes $\left\lfloor \frac{k}{n} \right\rfloor$ is called quotient and denoted also by $k\backslash n$.

Proof: This follows, with $k = l\,n + r$, trivially from the trigonometric identity $\cos\left(\frac{\pi}{n}\,(l\,n + r)\right) = \cos\left(\pi\, l + \frac{\pi\, r}{n}\right) = (-1)^l \cos\left(\frac{\pi}{n}\, r\right)$, with $r \in \{0, 1, ..., n-1\}$. □

To simplify notation we will use also $\hat{t}_n(x)$ for $\hat{t}(n, x)$. From *lemmata* 7 and 8 we have *e.g.*, $\hat{t}_3(t_3(\rho(7)) = \hat{t}_9(\rho(7)) = -\hat{t}_2(\rho(7)) = -(\rho(7)^2 - 2)$. This is also $+\hat{t}_5(\rho(7))$ from the identity $\cos\left(\frac{\pi}{n}(n \pm l)\right) = -\cos\left(\frac{\pi}{n}\, l\right)$. This proves the following *lemma*.

Lemma 9: Symmetry relation of $\hat{\mathbf{t}}$ polynomials

$$\hat{t}(n - l, \rho(n)) = -\hat{t}(l, \rho(n))\,,\ n \in \mathbb{N},\ l \in \{0, 1, ..., n\}\ . \tag{60}$$

Lemma 7 which used the trigonometric $\rho(n)$ definition can be rewritten as a congruence for the $\hat{t}$-polynomials with indeterminate x. This is because all what is needed is that $\rho(n)$ is a zero of $C(n, x)$.

Corollary 5: Congruence for $\hat{\mathbf{t}}$ polynomials modulo C-polynomials

$$\hat{t}(k, x) \equiv (-1)^{\left\lfloor \frac{k}{n} \right\rfloor}\, \hat{t}(k (mod\, n), x)\, (mod\, C(n, x))\ ,\ n \in \mathbb{N}, k \in \mathbb{Z}\ . \tag{61}$$

An example will illustrate this before we give an another proof of this *corollary* based on known T-polynomial identities.

Example 11: Congruence for n = 7, k = 9

$\hat{t}(9, x) = x^9 - 9\,x^7 + 27\,x^5 - 30\,x^3 + 9\,x$ and $C(7, x) = x^3 - x^2 - 2\,x + 1$. Polynomial division shows that $\hat{t}(9, x) = (x^6 + x^5 - 6\,x^4 - 5\,x^3 + 9\,x^2 + 5\,x - 2)\,C(7, x) + (-x^2 + 2)$, hence $\hat{t}(9, x) \equiv -\hat{t}(2, x)\,(mod\, C(7, x))$.

The alternative proof of *corollary 5* is based on the following factorization of *Chebyshev* S-polynomials in terms of the minimal polynomials $\Psi(n,x)$ of $\cos\left(\frac{2\,\pi}{n}\right)$ over $\mathbb{Q}$ (for these polynomials see A049310 and A181875/A181876).

Proposition 9: Factorization of S-polynomials in terms of Ψ-polynomials

$$S(n-1,x) \,=\, 2^{n-1} \prod_{2<d\,|\,2n} \Psi\left(d,\frac{x}{2}\right)\,,\, n\,\in\,\mathbb{N}\,. \tag{62}$$

As usual, the undefined (empty) product is defined to be 1.

Proof: Start with the eq. (3) of [30], p. 471, written for $n\,\to\,2\,n$ and for the $\hat t$-polynomials instead of the T-polynomials. This is $\hat t(n+1,x)\,-\,\hat t(n-1,x)\,=\,2^{n+1}\prod_{d|2\,n}\Psi\left(d,\frac{x}{2}\right)$. Then use the identity [20], p. 261, first line, with $m\,\to\,n$, $n\,\to\,m$ and U-polynomials replaced by $S-$polynomials. This leads to the identity

$$\hat t(n+m,x)\,-\,\hat t(n-m,x)\,=\,(x^2\,-\,4)\,S(n-1,x)\,S(m-1,x)\,,\;m\,\leq\,n\,\in\,\mathbb{N}\,. \tag{63}$$

Here we only need the case $m\,=\,1$. Then dividing out $2\,\Psi(1,\frac{x}{2})\,=\,x\,-\,2$ and $2\,\Psi(2,\frac{x}{2})\,=\,x\,+\,2$ leads to the claimed identity. □

To end the preparation for an independent proof of *corollary 5* we state:

Corollary 6: C-polynomial divides some family of S-polynomials

$$C(n,x)\,|\,S(l\,n-1,x)\,,\,n\,\geq 2,\;l\,\in\,\mathbb{N}\,. \tag{64}$$

This is clear from the definition of C in eq. (16) and the fact that $2\,<\,2\,n\,|\,2\,l\,n$, for $l\,\geq\,1$. *E.g.*, $C(10,x)\,=\,x^4\,-\,5\,x^2\,+\,5$ divides the family $\{S(9,x),S(19,x),S(29,x),...\}$

Proof of corollary 5: From the *corollary 6* and the identity eq. (63) with $n\,\to\,l\,n$ and $m\,\to\,r$ one sees that $\hat t(k,x)\,=\,\hat t(l\,n\,+\,r,x)\,\equiv\,\hat t(l\,n\,-\,r,x)\,(mod\,C(n,x))$. Now $\hat t(l\,n\,-\,r,x)\,=\,\hat t((l-1)\,n\,+\,(n-r),x)$, and one can use $l_1\,:=\,l-1$ and $r_1\,:=\,n-r$ (remember that $r\,\in\,\{0,1,...,n-1\}$, hence r_1 has identical range) as new l and r variables in this congruence, to get $\hat t(l_1\,n+r_1,x)\,\equiv\,\hat t(l_1\,n\,-\,r_1,x)\,(mod\,C(n,x))\,=\,\hat t((l-2)\,n\,+\,r,x)\,(mod\,C(n,x))$. This can be continued until one ends up with
$\hat t(0\,n+k(mod\,n),x)\,(mod\,C(n,x))$. □

Now we are in a position to compute powers of elements of the *Galois* group $\mathcal{G}_n$. The subset of odd numbers $2\,l\,+\,1\,<\,n$ entering the product in eq. (20) will be denoted by $\mathcal{M}(n)$. There are $\delta(n)$ (degree of $C(n,x)$) such odd numbers.

Definition 2: The fundamental set $\mathcal{M}(n)$

$$\mathcal{M}(n)\,:=\,\left\{2\,l\,+\,1\middle|\,l\,\in\,\left\{0,....,\left\lfloor\frac{n-2}{2}\right\rfloor\right\}\text{and}\,gcd(2\,l+1,n)=1\right\}\,=\,\{m_1(n),...,m_{\delta(n)}(n)\}, \tag{65}$$

with $m_1(n)\,=\,1$ and we use the order $m_i(n)\,<\,m_j(n)$ if $i\,<\,j$. For $n\,=\,1$ one takes $\mathcal{M}(1)\,=\,\{1\}$.

Example 12: $|\mathcal{M}(2)|\,=\,\delta(2)\,=\,1$, $\mathcal{M}(2)\,=\,\{1\}$; $|\mathcal{M}(14)|\,=\,\delta(14)\,=\,6\,,\,\mathcal{M}(14)\,=\,\{1,3,5,9,11,13\}$.

For $\mathcal{M}(n)$ see the row No. n of the array A216319.

For later purpose we define here, for odd n, the extended fundamental set $\widehat{\mathcal{M}}(n)$ and its first difference set $\triangle\,\widehat{\mathcal{M}}(n)$

Definition 3: The fundamental extended set $\widehat{\mathcal{M}}(\mathbf{n})$ for odd n

For n odd, ≥ 1: $\widehat{\mathcal{M}}(n)\,:=\,\{0,m_1(n)=1,...,m_{\delta(n)}(n)\,=\,n-2,n+2\}$.

Thus $|\widehat{\mathcal{M}}(n)|\,=\,\delta(n)+2$. Note that $gcd(n\,\pm\,2,n)\,=\,1$ for odd n (proof by assuming the contrary: $gcd(n+2,n)\,=\,d>2$ because n and $n+2$ are odd. Then $d\,|\,(n+2)$ and $d\,|\,n$, hence $d\,|\,((n+2)-n)$, $d\,|\,2$, implying $d=2$ or $d=1$, but $d>2$.) The reason for defining this extended set is that for odd n the first difference set $\triangle\widehat{\mathcal{M}}(n) = \{1, \triangle m_2(n), ..., \triangle m_{\delta(n)}(n), 4\}$ with $\triangle m_j(n) := m_j(n) - m_{j-1}(n)$, will become important later on. $\triangle m_1(n) = 1$ and $\triangle m_{\delta(n)+1}(n) = 4$ for each odd n.

With *definition 2* eq. (20) implies,

$$\begin{aligned}\sigma_j(\rho(n)) &= \sigma_j(\tilde{\xi}_1^{(n)}) = \tilde{\xi}_{j+1}^{(n)} = 2\cos\Big(\frac{\pi}{n}\, m_{j+1}(n)\Big) = \\ &\hat{t}(m_{j+1}(n), \rho(n)) \text{ for } j \in \{0, 1, ..., \delta(n) - 1\}\ .\end{aligned} \tag{66}$$

E.g., $n = 7$: $\delta(7) = 3$, $\mathcal{M}(7) = \{1, 3, 5\}$, $\sigma_0(\rho(7)) = \rho(7)$, $\sigma_1(\rho(7)) = \hat{t}(3, \rho(7))$, and $\sigma_2(\rho(7)) = \hat{t}(5, \rho(7))$.

Because $\hat{t}$ is a rational integer polynomial

$$\sigma_j^2(\rho(n)) = \sigma_j(\sigma_j(\rho(n))) = \hat{t}(m_{j+1}(n), \sigma_j(\rho(n))) = \hat{t}(m_{j+1}(n), \hat{t}(m_{j+1}, \rho(n)))\ , \tag{67}$$

and with *lemma 6* this becomes $\sigma_j^2(\rho(n)) = \hat{t}((m_{j+1}(n))^2, \rho(n))$. In general we have

$$\sigma_j^k(\rho(n)) = \hat{t}((m_{j+1}(n))^k, \rho(n))\, , \text{for}\, j \in \{0, 1, ..., \delta(n) - 1\}\ , n, k \in \mathbb{N}\ . \tag{68}$$

Instead of powers of $\sigma_j(\rho(n))$ we can therefore consider powers of $m_{j+1}(n)$. *Lemmata* 8 and 9 are now employed to prove that a $\hat{t}$ polynomial with a product of elements from $\mathcal{M}(n)$ as its first argument (or index) is again a $\hat{t}$ polynomial with first argument from $\mathcal{M}(n)$. In this way one can build sequences of powers, starting from any element of $\mathcal{M}(n)$. Trivially, $1^k = 1$. Before proving this closure of $\mathcal{M}(n)$ under powers, provided the rules for $\hat{t}$ polynomials are taken into account, we give two examples, and then define a new equivalence relation on the integers, called (*Modd* n), denoted by $\overset{n}{\sim}$.

Example 13: Cycle structure for n = 12 (dodecagon)

$\delta(12) = 4$, $\mathcal{M}(12) = \{1, 5, 7, 11\}$. $5^2 = 25 \equiv 1\,(mod\ 12)$, reflecting *lemma 8*. The sign $p_n(25)$ in eq. (59) is here $+$. (If later the sign will be $-$, the *mod n* result will be underlined.) The first 2-cycle is therefore $[5, 1]$. Similarly, $7^2 = 49 \equiv 1\,(mod\ 12)$ (sign $+$), whence the second 2-cycle is $[7, 1]$, and finally, $11^2 = 121 \equiv 1\,(mod\ 12)$ (sign $+$), producing the third 2-cycle $[11, 1]$. This result appears as the $n = 12$ entry in *Table 6*. In this example the *Galois* group is not generated by one element. hence it is non-cyclic. In fact, $\mathcal{G}al(\mathbb{Q}(\rho(12))/\mathbb{Q}) = Z_2 \times Z_2 = Z_2^2$ (see second entry in *Table 7*). The corresponding cycle graph is shown in *Figure 4* as the first entry, where the shaded (colored) vertex stands for 1 and the open vertices should here be labeled with 5, 7 and 11. The cycle structure is 2_3 (three 2-cycles). In this example it was not necessary to employ *lemma 9* because the signs were always $+$.

Example 14: Cycle structure for n = 7 (heptagon)

$\delta(7) = 3$, $\mathcal{M}(7) = \{1, 3, 5\}$. $3^2 \equiv \underline{2}\,(mod\ 7)$, where now the sign $-$ in eq. (59) is remembered by the underlining. $2 \notin \mathcal{M}(7)$, and now *lemma 9* is used to rewrite this $\underline{2}$ as $7 - 2 = 5$. Therefore, $3^2 \overset{7}{\sim} 5 \in \mathcal{M}(7)$ (or $3^2 \equiv 5\,(Modd\,7)$). The symbol $\overset{7}{\sim}$ (or $Modd$ 7) is used for the congruence in the new sense, due to *lemmata* 8 and 9. Then $3 \cdot 5 = 15 \equiv 1\,(mod\ n)$ (sign $+$). The first 3-cycle is therefore $[3, 5, 1]$. Here 3 generates all the elements of $\mathcal{M}(7)$, and $\mathcal{G}al(\mathbb{Q}(\rho(7))/\mathbb{Q}) = Z_3$, the cyclic group of order $3 = \delta(7)$. The corresponding cycle graph is a circle with three vertices, one of them, labeled 1, is shaded (colored) and the other two open ones are labeled by 3 and 5.

This brings us to the definition of an equivalence relation $\overset{n}{\sim}$ (or *Modd* n) over the integers $\mathbb{Z}$. Remember that the floor function for negative arguments is defined as $\lfloor -x \rfloor = -\lfloor x \rfloor$ if $x \in \mathbb{N}_0$, and $\lfloor -x \rfloor = -(\lfloor x \rfloor + 1)$ if $0 < x \notin \mathbb{N}$.

Definition 4: Equivalence relation $\overset{n}{\sim}$ on $\mathbb{Z}$

For $k, l \in \mathbb{Z}, n \in \mathbb{N}$: $k \overset{n}{\sim} l \Leftrightarrow a_n(k) = a_n(l)$, with the map $a_n : \mathbb{Z} \to I_n := \{0, 1, ..., n - 1\}$, $k \mapsto a_n(k)$, where

$$a_n(k) = \begin{cases} r_n(k) & \text{if } p_n(k) = +1\ , \\ \\ r_n(-k) & \text{if } p_n(k) = -1\ , \end{cases} \tag{69}$$

where we used the division algorithm to write $k = q_n(k)\,n + r_n(k)$, with the quotient $q_n(k) \in \mathbb{Z}$ and the residue $r_n(k) \in I_n$. Note that $q_n(k) = \left\lfloor \frac{k}{n} \right\rfloor$. The sign $p_n(k) = (-1)^{\lfloor \frac{k}{n} \rfloor} = (-1)^{q_n(k)}$ corresponding to the parity of $q_n(k)$, appeared already in *lemma 8*. $a_n(1) = 0$ because $-1 \equiv 0\,(mod\,1)$.

Instead of $k \overset{n}{\sim} l$ we also write $k \equiv l\,(Modd\,\mathrm{n})$ (this should not to be confused with $mod\,n$). Therefore the sequence a_n could also be called *Modd* n. The first of these $2\,n$-periodic sequences a_n are found in A000007$(n+1), n \geq 0$, (the 0-sequence), A000035, A193680, A193682, A203571, A203572 and A204453, for $n = 1, ..., 7$, respectively.

The smallest non-negative residue system *mod* n, *viz* $0, 1, ..., n-1$ is used here. For the residue of k modulo n Maple [18] uses $r_n(k) = modp(k, n)$. We also use $k(mod\,n)$ for $r_n(k)$. The reader should verify that $\overset{n}{\sim}$ is indeed an equivalence relation satisfying reflexivity, symmetry and transitivity. The disjoint and exhaustive equivalence classes are given by $\{[0], [1], .., [n-1]\}$, called the smallest non-negative complete representative classes (or residue classes) $Modd\,n$ (we omit the index n at the classes: $[m] = {}_n[m]$, written this way in order to distinguish this class from the ordinary one $[m]_n$ used in the arithmetic $mod\,n$). These classes are defined by $[m] = \{l \in \mathbb{Z}\,|\,l \overset{n}{\sim} m\} = \{l \in \mathbb{Z}\,|\,a_n(l) = m\}$. Because $r_n(-k) = 0$ if $k \equiv 0\,(mod\ n)$ and $r_n(-k) = n - r_n(k)$ if $k \not\equiv 0\,(mod\ n)$ (later listed as *lemma 17*) one can characterize these residue classes also in the following way.

Lemma 10: Complete residue classes Modd n

$$\begin{aligned}
l &\in [0] \Leftrightarrow l \equiv 0\,(mod\,n).\ \text{Equivalently, } [0] = [0]_n\ , \\
l &\in [1] \Leftrightarrow l \equiv 1\,(mod\,2\,n) \text{ or } \equiv -1\,(mod\,2\,n).\ \text{Equivalently, } [1] = [1]_{2\,n} \cup [2\,n-1]_{2\,n}\ , \\
&\vdots \\
l &\in [n-1] \Leftrightarrow l \equiv n-1\,(mod\,2\,n) \text{ or } \equiv -(n-1)\,(mod\,2\,n). \\
&\quad \text{Equivalently, } [n-1] = [n-1]_{2\,n} \cup [n+1]_{2\,n}\ . \qquad (70)
\end{aligned}$$

For example, take $n = 7$, then $[3] = {}_7[3] = [3]_{14} \cup [14-3]_{14} = \{..., -25, -11, 3, 17, ...\} \cup \{... -17, -3, 11, 25, ...\} = \{..., -25, -17, -11, -3, 3, 11, 17, 25, ...\}$. If $n = 2$ one has ${}_2[0] = [0]_2$ and ${}_2[1] = [1]_2$. The first differences in the class $[0]$ are, of course, n, and in the class $[m]$, for $m = 1, 2, ..., n-1$, they alternate between $\triangle_1 = 2\,(n - m)$ and $\triangle_2 = 2\,m$, *e.g.*, $n = 7, m = 3$, $\triangle_1 = 8$, $\triangle_2 = 6$: 3, 11, 17, 25, 31, ... This difference alternation invalidates certain theorems known for $mod\,n$. *E.g.*, *Theorem* 53 of reference [10], p. 50, is no longer true: take $m = 5$, $n = 7$, $a = 3$, $b = 17$. a and b belong both to the class ${}_5[3]$ as well as ${}_7[3]$ but they do obviously not both belong to the class ${}_{35}[3]$. The following *lemma 11* shows that is is sufficient to know the positive values, and append the negative of these values for each class $[m]$, for $m \in \{0, 1, ..., n-1\}$.

Lemma 11: Antisymmetry of the classes $[\mathbf{m}]$, for $\mathbf{m} \in \{\mathbf{0}, ..., \mathbf{n-1}\}$

For $n \in \mathbb{N}$ and every $m \in \{0, ..., n-1\}$ the elements of the equivalence class [m] are antisymmetric around 0.

Proof: This is obvious for the class $[0] = \{...-2\,n, -n, 0, n, 2\,n, ...\}$. For $m > 0$ the negative of every positive numbers of $m\,(mod\,2\,n)$ appears as a negative number of $(2\,n - m)\,(mod\,2\,n)$, and *vice versa*: the negative of every positive numbers of $[2\,n - m]_{2\,n}$ appears as a negative one of $[m]_{2\,n}$. This is true because $-(m + l\,2\,n) = (2\,n - m) - (l+1)\,2\,n$, for every $l \in \mathbb{N}$, and similarly, $-((2\,n - m) + l\,2\,n) = m - (l+1)\,2\,n$, for every $l \in \mathbb{N}$. □

This leads immediately to the following *corollary*.

Corollary 7: Non-negative elements of the classes $[\mathbf{m}]$

For $n \in \mathbb{N}$ and every $m \in \{0, ..., n-1\}$ one has

$$[m]_{\geq} = [m]_{2\,n,\geq} \cup [2\,n - m]_{2\,n,>}\ , \text{ and } [m] = [m]_{\geq} \cup -([m]_{>})\ . \qquad (71)$$

Here we used the notations $[m]_{\geq}$ and $[\,\cdot\,]_{2\,n,\geq}$ or $[\,\cdot\,]_{2\,n,>}$ to denote the subset of non-negative numbers of [m] and the non-negative or positive numbers of the ordinary residue classes $mod\,2n$, respectively. Of course 0 appears only in the class [0]. $-([m]_{>})$ is obtained from the set $[m]_{>}$(excluding 0 in the case of class [0]) by taking all elements negative. Note that $[-m]$ is not used here.

With $g(n,m) := gcd(m, 2\,n{-}m)$ one has, for $m \in \{1, 2, ..., n{-}1\}$, $[m]_{2n,>} = g(n,m)\,[m/g(n,m)]_{2\,n/g(n,m),>}$ and $[2\,n - m]_{2n,>} = g(n,m)\,[(2\,n - m)/g(n,m)]_{2\,n/g(n,m),>}$. This is. of course, only of interest if $g(n,m) \neq 1$. *E.g.*, $n = 6$, $m = 3$, $g(n,m) = 3$: $[3]_{12,>} = 3 * [1]_{4,>}$ and $[9]_{12,>} = 3 * [3]_{4,>}$, where again $k * [p]_{q,>}$ is the set with all members of the set $[p]_{q,>}$ multiplied with k. This is obvious.

The trivial formula for the members of the residue classes $[m]_{\geq}$, considered as sequences of increasing numbers called $\{c(n,m;k)\}_{k=1}^{\infty}$, is

$$c(n,m;k) \;=\; \begin{cases} (k-1)\,n & \text{if } m \,=\, 0\ , \\[2ex] \left\lfloor \frac{k}{2} \right\rfloor\, 2\,n \,+\, (-1)^k\, m & \text{if } m \,\in\, \{1, 2, ..., n-1\}\ . \end{cases} \tag{72}$$

The nonnegative members of the complete residue classes (*Modd* n) for $n = 3, 4, 5, 6$, and 7 are found in A088520, A203575, A090298, A092260, and A113807. Sometimes 0 has to be added, in order to obtain the class [0]. Of course, these complete residue classes can be recorded as a permutation sequence of the non-negative integers.

We now list several *lemmata* (the trivial *lemma 17* has already been used) in order to prepare for the proof of the multiplicative structure of these equivalence classes.

Lemma 12: Parity of Modd n residue classes

For even n the parity of the members of the residue class ${}_{n}[m]$, $m \in \{0, 1, ..., n-1\}$ coincides with the one of m. If n is odd this is also true for the classes with $m \in \{1,\ 2,\ \ldots, n-1\}$, and for $m = 0$ the parity of the elements alternates, starting with + (for even).

Proof: The case of the residue class [0] is clear for even or odd n because of its members $0\,mod\,n$ (see *lemma 10*). Similarly, for the other m values, because then $mod\,2n$ applies.

Lemma 13: Periodicity of the parity sequence $\mathbf{p_n}$ with period length $\mathbf{2\,n}$

$$p_n(k) \;=\; p_n(k \,+\, 2\,n\,l) \text{ for } l \,\in\, \mathbb{Z},\ \ i.e.,\ \ p_n(k) \;=\; p_n(r_{2\,n}(k)) \;=\; p_n(k\,(mod\,2\,n)),\ \text{ for } k \,\in\, \mathbb{Z}, n \,\in\, \mathbb{N}. \tag{73}$$

Proof: This is obvious from the definition of $p_n(k)$ given in *lemma 8*, eq. (59), with *definition 4*, eq. (69). For the second part use $k \;=\; 2\,n\,q_{2\,n}(k) + r_{2\,n}(k)$.

Lemma 14: (A)symmetry of sequence $\mathbf{p_n}$ around $\mathbf{k \,=\, 0}$

$$\text{for } n \,\in\, \mathbb{N},\ \ k \,\in\, \mathbb{N}_0\ :\ \ p_n(-k) \;=\; \begin{cases} +p_n(k) & \text{if } k \,\equiv\, 0\,(mod\,n) \\[2ex] -p_n(k)\ , & \text{if } k \,\not\equiv\, 0\,(mod\,n)\ . \end{cases} \tag{74}$$

Proof: This follows immediately from the property of the $\lfloor -x \rfloor$ function mentioned above before *definition 4*. □

Lemma 15: Product formula for the residue $\mathbf{r_n}$

For $n \,\in\, \mathbb{N}$ and $k, l \,\in\, \mathbb{Z}$ one has: $r_n(k\,l) \;=\; r_n(k)\,r_n(l)\,(mod\,n)$.

Proof: Just multiply $k \;=\; q_n(k)\,n + r_n(k)$ with $l \;=\; q_n(l)\,n + r_n(l)$.

Lemma 16: Residue $\mathbf{r_{2\,n}}$ from $\mathbf{r_n}$

$$\text{For } n \,\in\, \mathbb{N} \text{ and } k \,\in\, \mathbb{Z} \text{ one has: } r_{2\,n}(k) \;=\; \begin{cases} r_n(k) & \text{iff } r_{2\,n}(k) \,\in\, \{0,\ 1,\ ...,\ n-1\}, \\[2ex] r_n(k) + n & \text{iff } r_{2\,n}(k) \,\in\, \{n,\ n+1,\ ...,\ 2\,n-1\}. \end{cases}$$

Proof: Obvious for $r_{2\,n}(k) \,\in\, \{0, ..., n{-}1\}$ as well as $\in\, \{n, ..., 2\,n{-}1\}$. □

Lemma 17: Residue for negative numbers

For $n \in \mathbb{N}$ and $k \in \mathbb{N}_0$ one has: $r_n(-k) = \begin{cases} 0 & \text{if } k \equiv 0\,(mod\,n)\ , \\ \\ n - r_n(k) & \text{if } k \not\equiv 0\,(mod\,n)\ . \end{cases}$

Proof: Obvious. □

Lemma 18: Symmetry of the $\mathbf{a_n}$ (or Modd n) sequence around $\mathbf{k = 0}$

For $n \in \mathbb{N}$ and $k \in \mathbb{N}_0$ one has: $a_n(-k) = a_n(k)$.

Proof: This is proved for the two cases $k \equiv 0\,(mod\,n)$ and $k \not\equiv 0\,(mod\,n)$ separately. In the first case $r_n(k) = 0$, as well as $r_n(-k) = 0$, hence $a_n(k \equiv 0\,(mod\,n)) = 0$, which is symmetric around $k = 0$. In the other case, we employ *lemma 13*, noting that $r_{2\,n}(k) \neq 0, n$ (otherwise $k \equiv 0\,(mod\,n)$). The two cases $r_{2\,n}(k) \in \{1,\, 2,\, ...,\, n-1\}$ and $r_{2\,n}(k) \in \{n+1,\, n+2,\, ...,\, 2n-1\}$ have $p_n(k) = p_n(r_{2\,n}(k))$ equal $+1$ or -1, respectively. Then with the second alternative of *lemma 14* one finds $a_n(-k) = r_n(-k)$ if $p_n(-k) = -p_n(k) = +1$ and $a_n(-k) = r_n(k)$ if $p_n(-k) = -p_n(k) = -1$ which coincides with the definition of $a_n(+k)$. □

Now we turn to the arithmetic structure of the *Modd n* residue classes. It is clear from the following counter-example that addition cannot be done class-wise. Consider $n = 6$, $k = 2$ and $l = 7$. Then $a_6(2 + 7) = 3$ but $a_6(a_6(2) + a_6(7)) = a_6(2 + 5) = a_6(7) = 5$. In other words, $2 \overset{6}{\sim} 2$ and $7 \overset{6}{\sim} 5$, but $2 + 7 = 9 \overset{6}{\sim} 3$ but $(2 + 5) = 7 \overset{6}{\sim} 5$, and 3 is not equivalent to $5\,(Modd\,6)$. Similarly, from $(a-1) \overset{n}{\sim} 0$ does in general not follow $a \overset{n}{\sim} 1$, because for $n > 2$ in the latter case a can also be of the form $-1 + k\,2\,n$ if it belongs to a class $[m]$ with positive m, whereas in the first case it has to be of the form $1 + k'\,n$, which can only match for $n = 1$ and 2. However, it turns out that multiplication can be done class-wise. This is the content of the following *proposition*.

Proposition 10: Modd n residue classes are multiplicative

For $n \in \mathbb{N}$ and $k, l \in \mathbb{Z}$ one has:

$$a_n(k\,l) = a_n(a_n(k)\,a_n(l)) \ \ \textit{i.e.,} \ \ \ k\,l \overset{n}{\sim} a_n(k)\,a_n(l)\,,\ \text{i.e.,}\, kl \equiv a_n(k)\,a_n(l)\,(Modd\,n)\ . \tag{75}$$

Before giving the proof, consider the example $n = 6$, $k = 2$ and $l = 7$. Now $a_6(2 \cdot 7) = 2$ and $a_6(a_6(2) \cdot a_6(7)) = a_6(2 \cdot 5) = a_6(10) = 2$. Or stated equivalently, $2 \cdot 7 = 14 \overset{6}{\sim} 2 \overset{6}{\sim} 2 \cdot 5 \overset{6}{\sim} a_6(2)\ a_6(7)$.

Proof:

i) Due to the symmetry of a_n (see *lemma 18*) it is clear that it is sufficient to consider only non-negative k and l.

ii) Consider first the cases $k \equiv 0\,(mod\,n)$ or $l \equiv 0\,(mod\,n)$. If $m \equiv 0\,(mod\,n)$ then $a_n(m) = 0$. This follows for both alternatives in eq. (69). Therefore, if $k \equiv 0\,(mod\,n)$, $a_n(k\,l) = 0$ because $k\,l \equiv 0\,(mod\,n)$ for every l, and $a_n(0 \cdot a_n(l)) = a_n(0) = 0$, proving the assertion. In the other case, $l \equiv 0\,(mod\,n)$, the proof is done analogously.

iii) Now $r_n(k)$ and $r_n(l)$ are non-vanishing, and k and l are positive. Four cases are distinguished according to the signs of $(p_n(k), p_n(l))$, *viz* $(+,+)$, $(-,-)$, $(+,-)$ and $(-,+)$.

(+,+): In this case, due to the $2\,n$-periodicity of p_n (see *lemma 13*), $r_{2\,n}(k)$ and $r_{2\,n}(l)$ are both from $\{1, 2, ..., n-1\}$, hence

$$(+,+): \qquad\qquad r_{2\,n}(k) = r_n(k) \ and\ r_{2\,n}(l) = r_n(l)\,. \tag{76}$$

Also, from eq. (69), one obtains in this case $a_n(k)\,a_n(l) = r_n(k)\,r_n(l)$. There is an alternative for $a_n(r_n(k)\,r_n(l))$, depending on $p_n(r_n(k)\,r_n(l))$ being $+1$ or -1. Both cases are possible as the following examples for $n = 6$ show: $p_6(3 \cdot 4) = p_6(12\,(mod\,12)) = p_6(0) = +1$ and $p_6(3 \cdot 7) = p_6(21\,(mod\,12)) = p_6(9) = -1$. First the argument of p_n is rewritten with the help of eq. (76). $p_n(r_n(k)\,r_n(l)) = p_n(r_{2\,n}(k)\,r_{2\,n}(l))$. Due to the $(2\,n)$-periodicity (*lemma 13*) this is $p_n(r_{2\,n}(k)\,r_{2\,n}(l)\,mod(2\,n)) = p_n(r_{2\,n}(k\,l)) =$

$p(k\,l)$, due to *lemma 15* with $n \to 2\,n$, and again the $(2\,n)$-periodicity. In the first alternative, the $+1$ case, $a_n(a_n(k)\,a_n(l)) = r_n(k)\,r_n(l)\,(mod\,n) = r_n(k\,l)$, again from *lemma 15*. This is just $a(k\,l)$ if $p_n(k\,l) = +1$, proving the assertion for this alternative. In the other case, $p_n(k\,l) = -1$, $a_n(r_n(k)\,r_n(l)) = -(r_n(k)\,r_n(l))(mod\,n)$ which is rewritten with $mod\,n$-arithmetic and *lemma 15* as $-r_n(k\,l)(mod\,n) = -(k\,l)(mod\,n) = r_n(-k\,l)$. This coincides with $a(k\,l)$ for this alternative, proving the assertion.

(-,-): Now we have from *lemma 16*

$$(-,-): \qquad r_{2\,n}(k) = n + r_n(k) \text{ and } r_{2\,n}(l) = n + r_n(l)\,. \tag{77}$$

Here $p_n((r_n(-k)\,r_n(-l))$ is rewritten with *lemma 17*, eq. (77), the $2\,n$ periodicity, and *lemma 15*, as follows. $p_n((n - r_n(k))\,(n - r_n(l))) = p_n((2\,n - r_{2\,n}(k))\,(2\,n - r_{2\,n}(l))) = p_n(r_{2\,n}(k)\,r_{2\,n}(l)) = p_n(r_{2\,n}(r_{2\,n}(k)\,r_{2\,n}(l))) = p_n(r_{2\,n}(k)\,r_{2\,n}(l)\,(mod\,2\,n))$. With *lemma 15* (with $n \to 2\,n$ this becomes $p_n(r_{2\,n}(k\,l)) = p_n(k\,l)$, again from the $(2\,n)$-periodicity. In the first alternative $p_n(k\,l) = +1$ and $a_n(r_n(-k)\,r_n(-l)) = r_n(r_n(-k)\,r_n(-l))$. With *lemma 17* and $mod\,n$-arithmetic this is $r_n((-r_n(k))\,(-r_n(l))) = r_n(r_n(k)\,r_n(l))$, and with *lemma 15* this becomes $r_n(k\,l)$, coinciding with $a_n(k\,l)$ for this alternative. For the other alternative, $p_n(k\,l) = -1$, $a_n(r_n(-k)\,r_n(-l)) = -(r_n(-k)\,r_n(-l))(mod\,n)$. This becomes, with *lemma 17*, $mod\,n$-arithmetic and *lemma 15*
$-(r_n(k)\,r_n(l))\,(mod\,n) = -r_n(k\,l)(mod\,n)$. This vanishes if $r_n(k\,l) = 0$ which means $k\,l \equiv 0\,(mod\,n)$ (which is possible, *e.g.*, $n = 6, k = 2, l = 3$), and then this coincides with the claim which is for this alternative $a(k\,l) = r_n(-(k\,l)) = 0$. If $r_n(k\,l) \neq 0$ then $-r_n(k\,l)\,(mod\,n) = n - r_n(k\,l)$ which also coincides with the claim $a(k\,l) = n - r_n(k\,l)$ if $k\,l \not\equiv 0\,(mod\,n)$.

We skip the proofs of the other two cases, $(+,-)$ and $(-,+)$, which run along the same line. Here one arrives first at $p_n(-(k\,l))$, and in order to compare it with $p(k\,l)$ both alternatives in *lemma 17* have to be considered like in the just considered second alternative. □

For the computation of the cycle structure of the *Galois* group $\mathcal{G}_n = \mathcal{G}al(\mathbb{Q}(\rho(n))/\mathbb{Q})$ we are only interested, due to eq. (20), in odd numbers relatively prime to n. Contrary to ordinary $mod\,n$-arithmetic where the set of odd numbers $\mathbb{O} := \{2l+1\,|\,l \in \mathbb{Z}\}$ is in general not closed under multiplication (*e.g.*, $5 \cdot 5 = 25 \equiv 4\,(mod\,7)$), it will be shown that $\mathbb{O}$ is closed under $Modd\,n$ multiplication. Of interest are the units, the elements which have inverses, in order to see the expected group structure. First consider the reduced set $\mathbb{O}_n^*$, given by the odd numbers relatively prime to n. The negative odd numbers in this set are just the negative of the positive odd numbers, therefore it will suffice to consider $\mathbb{O}_{n,>}^* := \{2l+1\,|\,l \in \mathbb{N}_0,\ gcd(2l+1,n) = 1\}$. If n is a power of 2 the set $\mathbb{O}_2^*$ will be $\mathbb{O}$, with the *o.g.f.* $G(x) = \dfrac{x}{(1-x)^2}\,(1 + x)$ for the sequence of positive odd numbers $\{o_{2,>}^*(k) := 2\,k+1\}_{k=0}^{\infty}$. For the other even numbers n only the odd numbers relatively prime to the squarefree kernel of n, called $sqfk(n)$, (see A007947, encountered already several times), will enter the discussion. Therefore, besides the just considered (trivial) case of the even prime 2, the set $\mathbb{O}_n^*$ is only relevant for squarefree odd moduli, either prime or composite. We consider first the case of odd primes $n = p$, and give the *o.g.f.* of the sequences of numbers from $\mathbb{O}_{p,>}^*$, called $o_{p,>}^*(k)$, as well as an explicit formula in terms of floor functions. These are the positive odd integers without odd multiples of the odd p.

Proposition 11: Odd prime moduli, o.g.f. and explicit formula for $\mathbb{O}_{\mathbf{p},>}^*$ elements

With $G_p(x) := \sum_{k=0}^{\infty} o_{p,>}^*(k)\,x^k$, for odd primes p, one has

$$G_p(x) = \frac{x}{(1-x^{p-1})\,(1-x)}\left\{1 + 2\sum_{k=1}^{\frac{p-3}{2}} x^k\,(1 + x^{\frac{p-1}{2}}) + 4^{\frac{p-1}{2}} + x^{p-1}\right\}, \tag{78}$$

and

$$o^*_{p,>}(k) \;=\; \begin{cases} 0 & \text{if } \; k = 0\;, \\[2ex] 2\,k \;-\; 1 \,+\, 2\, \left\lfloor \frac{k + \frac{p-3}{2}}{p-1} \right\rfloor & \text{if } \; k \,\in\, \mathbb{N}\;. \end{cases} \tag{79}$$

We have used the even number 0 for $k \,=\, 0$ such that the $G_p(x)$ sum can start with $k \,=\, 0$.

Proof: This *proposition* will become a corollary to the later treated general case of odd squarefree moduli n in *proposition 13*.

Example 15: O.g.f.s and formula for reduced odd numbers for modulus p = 7.

$$G_7(x) \;=\; \frac{x}{(1-x^6)\,(1-x)}\,\left\{1 + 2\,(x \,+\, x^2) \,+\, 4\,x^3 \,+\, 2\,(x^4 \,+\, x^5) \,+\, x^6\right\}\;, \tag{80}$$

$$o^*_{7,>}(n) \;=\; 2\,n \;-\; 1 \,+\, 2\,\left\lfloor\frac{n+2}{6}\right\rfloor,\; n \,\geq 1\,. \tag{81}$$

The instances for $p \,=\, 3, 5, 7, 11, 13$ and 17 are found under A007310, A045572, A162699, A204454, A204457, and A204458, respectively.

In order to prepare for the general case of odd squarefree modulus n, we state a *proposition* on the structure of the reduced odd numbers set $\mathbb{O}^*_{n,>}$.

Proposition 12: Mirror symmetry and modular periodicity of $\mathbb{O}^*_{\mathbf{n},>}$ for odd n

i) Mirror symmetry. For $k \,\in\, \{1, 2, ..., \delta(n)\}$ one has:

$$o^*_{n,>}(2\,\delta(n) - (k-1)) \;=\; 2\,n \;-\; o^*_{n,>}(k), \tag{82}$$

where $o^*_{n,>}(k) \;=\; m_k(n)$ from $\mathcal{M}(n)$, given in *definition 2*, eq. (65).

ii) *mod* $2\,n$ periodicity: For $k \in \mathbb{N}$ one has:

$$o^*_{n,>}(k) \;=\; o^*_{n,>}(k \,+\, 2\,\delta(n))\,(mod\,2\,n). \tag{83}$$

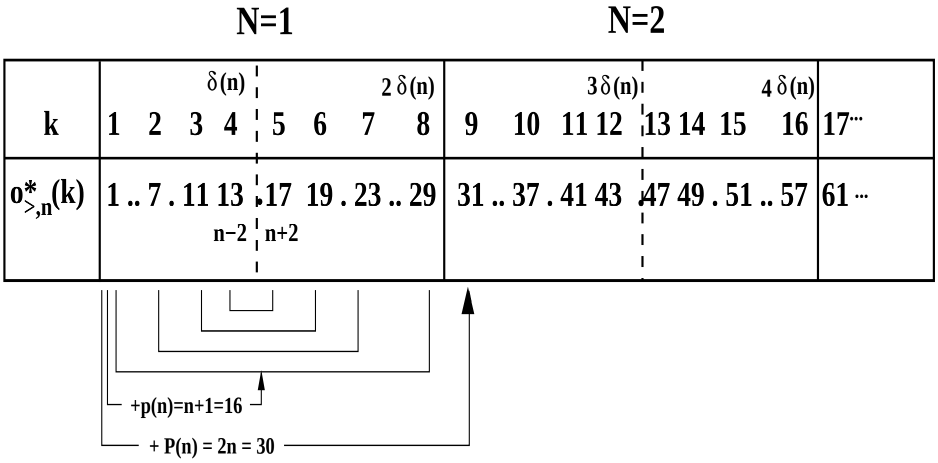
Written as a relation between neighboring fundamental units, numbered by $N \,\geq\, 1$, this becomes the following statement. For $k \,\in\, \{2\,(N-1)\,\delta(n)+1,\, ...,\, 2\,N\,\delta(n)\}$, with $N \,\in\, \{2,\, 3,\, 4,\, ...\}$, one has:

$$o^*_{n,>}(k) \;=\; (N-1)\,2\,n \,+\, o^*_{n,>}(k \,-\, (N-1)\,2\,\delta(n))\;. \tag{84}$$

$\delta(n)$ is the degree of the minimal polynomial $C(n, x)$ for the algebraic number $\rho(n)$ introduced in *section 2*. Note that if $n \;=\; \prod_{j=1}^{\omega(n)} p_j$ with distinct odd primes p, and $\omega(n)$ =A001221(n), then $2\,\delta(n) \;=\; \prod_{j=1}^{\omega(n)} (p_j - 1)$. $L(n) \;:=\; 2\,\delta(n)$ is the length of the fundamental N-units.

Before we give the proof consider *figure 3* for the case $n \;=\; 3\cdot 5 \;=\; 15$ with $\delta(n) \;=\; 4$. The second statement **ii)** concerns the relation of the numbers of the second fundamental unit ($N \;=\; 2$) to the one in the $N \;=\; 1$ unit. *E.g.*, the odd number 37 for $k \;=\; 2\cdot 4 + 2 \;=\; 10$ is equal to $30 \,+\, o^*_{15,>}(10 \,-\, 2\cdot 4) \;=\; 30 \,+\, o^*_{15,>}(2) \;=\; 30 \,+\, 7$, which checks. The statement **i)** shows the mirror symmetry within the first (and any other) unit of length $L(15) \;=\; 2\cdot 4 \;=\; 8$. In *figure 3* this symmetry is indicated by the brackets below the first unit, and it is a symmetry around the missing number $n \;=\; 15$. Missing numbers have been indicated by a dot. It is the pattern of missing odd numbers which is mirror symmetric, not the one of the actual values of the odd numbers. But the relation between the odd numbers in the second half of a unit and the first one then follows, and is given by the statement of the *proposition*. In *figure 3* $P(n) \;:=\; 2\,n \;=\; 30$ is the shift for the $o^*_{>,n}$ values from the $N \;=\; 1$ to the $N \;=\; 2$ unit (or any of the neighboring units), and $p(n) \;:=\; n \,+\, 1 \;=\; 16$ is the shift for these values from the first half of every unit to the second half.

Figure 3: Structure of the sequence of mod n reduced odd numbers, n=15



	N=1		N=2		
	$\delta(n)$	$2\,\delta(n)$	$3\,\delta(n)$	$4\,\delta(n)$	
k	1 2 3 4	5 6 7 8	9 10 11 12	13 14 15 16	17···
$o^*_{>,n}(k)$	1 .. 7 . 11 13 n−2	17 19 . 23 .. 29 n+2	31 .. 37 . 41 43	47 49 . 51 .. 57	61 ···

Proof: **i)** It is clear from the degree of the minimal polynomial and eq. (20) that the number of $mod\, n$ reduced positive odd numbers smaller than $2\,n$ is $\delta(2\,n) = 2\,\delta(n)$ (from the definition of $\delta(n)$ in terms of *Euler*'s φ function). We now determine $\delta(n)$ reduced odd numbers $mod\, n$ which lie between n and $2\,n$, by mirroring the $\delta(n)$ elements of $\mathcal{M}(n)$ around the position where the missing number n is situated, which is between the position $k = \delta(n)$ and the next one. The mirror symmetry refers to the gaps. The number $m_k(n)$ from $\mathcal{M}(n)$ will be mapped to $o^*_{n,>}(2\,\delta(n) - (k-1))$ at the mirrored position in the second half of the later defined first fundamental unit ($N = 1$). To find this odd number the first difference set $\triangle\,\widehat{\mathcal{M}}(n)$, introduced in connection with $\widehat{\mathcal{M}}(n)$ from the *definition 3*, becomes important in order to count the gaps in the sequence of odd numbers when they are reduced $mod\, n$. $o^*_{n,>}(2\,\delta(n) - (k-1))$ is found by adding to $m_k(n)$ twice the value of the sum of the gaps from the position k to the center, the mirror axis. This is $2\,(\triangle m_{k+1}(n) + \triangle m_{k+2}(n) + ... + \triangle\, m_{\delta(n)}(n) + 2)$. The 2 in this sum is half the gap-length from the value $n-2$ at the position $\delta(n)$ and $n+2$ at the next position, the mirror-position $\delta(n)+1$ of $\delta(n)$. This is a telescopic sum which becomes $2\,(-m_k(n) + m_{\delta(n)}(n) + 2)$. Therefore, the value of $o^*_{n,>}(2\,\delta(n) - (k-1))$ is $m_k + 2\,(-m_k(n) + m_{\delta(n)}(n) + 2) = 4 + 2\,m_{\delta(n)}(n) - m_k(n) = 2\,n - m_k(n)$, because always $m_{\delta(n)}(n) = n-2$ holds. See *figure 3*, $n = 15$ with the values $30 - 1 = 29$, $30 - 7 = 23$, $30 - 11 = 19$ and $30 - 13 = 17$ for $k = 1, 2, 3$ and 4, respectively. Now it is clear that this mirroring leads to the correct number of reduced odd numbers for the second half of the fundamental $N = 1$ unit, because $gcd(m_k(n), n) = 1$, as member of $\mathcal{M}(n)$, implies for the mirror image also $gcd(o^*_{n,>}(2\,\delta(n) - (k-1)), n) = 1$. All positive odd numbers relatively prime to n and not exceeding $2\,n - m_1(n) = 2\,n - 1$ have thus be found.

Proof of **ii)**: From above we know that the number at position $k = 2\,\delta(n) + 1$ is $2\,n + 1$ because the one for $k = 2\,\delta(n)$ has been shown to be $2\,n - 1$ and $gcd(2\,n+1, n) = 1$ (indirect proof by assuming the contrary, using odd n; this is similar to the proof given in connection with *definition 3* of $\widehat{\mathcal{M}}(n)$). Now it is clear that a shift in the $o^*_{n,>}$ numbers with $P(n) := 2\,n$ leads from the fundamental unit No. $N = 1$ to the second one, $N = 1$, by putting $o^*_{n,>}(2\,\delta(n) + k) = o^*_{n,>}(k) + P(n)$, for $k \in \{1, 2, ..., \delta(n)\}$. This is obvious because the gcd value 1 is not changed by adding $2\,n$. This process can be iterated to find the $mod\, 2\,n$ periodicity structure stated in **ii)**. See *figure 3*, $n = 15$ with $k = 14$, $N = 2$: $o^*_{15,>}(14) = 49 = 2 \cdot 15 + o^*_{15,>}(14 - 1 \cdot 2 \cdot 4) = 30 + o^*_{15,>}(6) = 30 + 19$. □

The sequences $\{o^*_{n,>}\}$ for $n = 15$ and $n = 21$ are found in A007775 and A206547, respectively.

The sequences of the $M odd\, n$ residues of the numbers $o^*_{n,>}(k)$, for $k = 1, 2, ...$, for prime moduli $n = p = 3, 5, 7, 11, 13, 17$, and for the first odd composed ones for $n = 15, 21$ are found in A000012, A084101, A110551, A206543, A206544, A206545, and A206546, A206548, respectively.

For the following formula for the nonnegative odd numbers reduced $mod\, n$ involving floor functions we need the following list (increasingly ordered set) $\mathcal{F}(n)$ of length $L(n) = 2\,\delta(n)$ derived from the list $\triangle\widehat{\mathcal{M}}$.

Definition 5: List $\mathcal{F}(\mathbf{n})$

$\mathcal{F}(n) = \{f(n,1), ..., f(n, 2\,\delta(n)\}$ with

$$\begin{aligned} f(n,j) &= \frac{\triangle m_{j+1}(n) - 2}{2}, \text{ for } j \in \{1,2,...,\delta(n)-1\} \\ f(n,\delta(n)) &= 1, \;\; f(n,\delta(n) + j) = f(n,\delta(n) - j), \text{ for } j \in \{1,2,...,\delta(n)-1\}, \text{ and} \\ f(n, 2\,\delta(n)) &= 0. \end{aligned} \tag{85}$$

Here $\triangle m_k(n) := m_k(n) - m_{k-1}(n)$, (the kth element of $\triangle\widehat{\mathcal{M}}(n)$). This list $\mathcal{F}(n)$ is obtained from first enlarging $\triangle\widehat{\mathcal{M}}$ by mirroring the first $\delta(n)$ entries at the last element 4, to obtain a list of order $2\,\delta(n)+1$. Then the first and last element of this new list is put to zero and all the other elements are diminished by 2, thus obtaining a set of only even numbers. Then one divides by 2, omits the final 0, and reverses the remaining list.

Example 16: $\mathcal{F}(15)$

$n = 15 = 3\cdot 5$, $2\,\delta(15) = 2\cdot 4 = 8$, $\mathcal{M}(15) = \{1,7,11,13\}$, $\widehat{\mathcal{M}}(15) = \{0,1,7,11,13,17\}$, $\triangle\widehat{\mathcal{M}}(15) = \{1,6,4,2,4\}$, the mirror extension is $\{1,6,4,2,4,2,4,6,1\}$, the reduction step leads to $\{0,4,2,0,2,0,2,4,0\}$, and finally, dividing by 2, omitting the last 0 and reverting, leads to $\mathcal{F}(15) = \{2,1,0,1,0,1,2,0\}$. Except for the last 0 there is a mirror-symmetry around the fourth entry 1. See the first row of *table 5*.

For the odd squarefree composite numbers $n =$ A024556(m), $m = 1, 2, \ldots, 17$, see *table 5* for $\widehat{\mathcal{M}}(n)$, $\triangle\,\widehat{\mathcal{M}}(n)$ and $\mathcal{F}(n)$.

Proposition 13: O.g.f. and formula for $\mathbb{O}^*_{\mathbf{n},>}$ elements.

With $G_n(x) := \sum_{k=1}^{\infty} o^*_{n,>}(k)\, x^k$, for odd n, one has

$$G_n(x) = \frac{x}{(1-x^{2\,\delta(n)})\,(1-x)} \left\{ 1 + \sum_{k=1}^{2\,\delta(n)-1} \triangle o^*_{n,>}(k+1)\, x^k + x^{2\,\delta(n)} \right\} \tag{86}$$

with the first differences $\triangle o^*_{n,>}(j) := o^*_{n,>}(j) - o^*_{n,>}(j-1)$.

This generates

$$o^*_{n,>}(k) = 2\,k - 1 + 2 \sum_{j=1}^{2\,\delta(n)} f(n,j) \left\lfloor \frac{k + (j-1)}{2\,\delta(n)} \right\rfloor . \tag{87}$$

Note that the numerator polynomial in $G_n(x)$ needs the first differences of the sequence members of the fundamental $N = 1$ unit, which due to the mirror symmetry of *proposition 12* can be reduced to the first differences of $\{m_2(n), m_3(n), .., m_{\delta(n)}, n+2\}$ with $m_{\delta(n)} = n - 2$.

One could use, like in *proposition 11*, $o_{n,>}(0) = 0$ and let the sum in $G_n(x)$ start with $k = 0$.

Proof: We start with the periodicity of the sequence due to *proposition 12 ii)*. Taking the difference $o^*_{n,>}(k) - o^*_{n,>}(k-1) = o^*_{n,>}(k - 2\,\delta(n)) - o^*_{n,>}(k - 1 - 2\,\delta(n))$ leads to the recurrence (we omit all unnecessary indices) $o(k) = o(k-1) + o(k - 2\,\delta(n)) - o(k - 1 - 2\,\delta(n))$, for $k \geq 2\,\delta(n) + 1$. Here one needs also $o^*_{n,>}(0) := -1$. For some of these recurrences the *o.g.f.*s were determined by *R. J. Mathar* in *e.g.*, A045572 and A162699. I general $G_n(x) = \sum_{k=1}^{2\,\delta(n)} o(k)\, x^k + x \sum_{k=2\,\delta(n)+1}^{\infty} o(k-1)\, x^{k-1} + x^{2\,\delta(n)} \sum_{k=2\,\delta(n)+1}^{\infty} o(n - 2\,\delta(n)) - x^{2\,\delta(n)+1} \sum_{k=2\,\delta(n)+1}^{\infty} o(n - 2\,\delta(n) - 1)\, x^{n-2\,\delta(n)-1}$, where the recurrence has been used (and the infinite sum has been reordered, not bothering about absolute convergence, in the sense of formal power series). Shifting the indices, one arrives at $G_n(x) \;=\; \sum_{k=1}^{2\,\delta(n)} o(k)\,x^k \,+$ $x\,\left\{G_n(x) \,-\, (o(1)\,x \,+\, ... \,+\, o(2\,\delta(n)-1)\,x^{2\,\delta(n)-1})\right\} + x^{2\,\delta(n)}\,G_n(x) - x^{2\,\delta(n)+1}\,(G_n(x) \,+\, (-1))$, where the -1 resulted from putting $o(0) \,=\, -1$ (see above). This rearranges into $(1 \,-\, x \,-\, x^{2\,\delta(n)} \,+\, x^{2\,\delta(n)+1})\,G_{\,n}(x) \,=\, x\,\left(1 \,+\, \triangle o(2)\,x \,+\, ... \,+\, \triangle o(2\,\delta(n))\,x^{2\,\delta(n)-1} \,+\, x^{2\,\delta(n)}\right)$. Factorizing the bracket on the *l.h.s.* and division leads to the claimed form for $G_n(x)$. Of course, the denominator factor $(1-x^{2\,\delta(n)})$ can be factorized into cyclotomic polynomials.

For the proof of the second part we use $L \,:=\, 2\,\delta(n)$. Given $G_n(x)$ with the $L\,+\,1$ input coefficients of the numerator polynomial one derives the claimed explicit form for $o^*_{n,>}(k)$, by defining first the sequence with entries $b_L(k) \,:=\, \left\lfloor\frac{k+L-1}{L}\right\rfloor$, generated by $\frac{x}{(1-x^L)\,(1-x)}$ (partial sums of the characteristic sequence for multiples of L, then shifted). The numerator polynomial leads for $o^*_{n,>}(k)$ to a sum of $L+1$ floor-functions with decreasing arguments, starting with $\left\lfloor\frac{k-0+L-1}{L}\right\rfloor$, ending with $\left\lfloor\frac{k-L+L-1}{L}\right\rfloor \,=$ $\left\lfloor\frac{k-1}{L}\right\rfloor$, and corresponding coefficients. In order to find a standard form for this sum we use the following floor-identity

$$\sum_{j=0}^{L-1}\left\lfloor\frac{k+j}{L}\right\rfloor \;=\; k,\ \text{for}\ L\,\in\,\mathbb{N},\ \text{and}\ k\,\in\,\mathbb{Z}\ , \tag{88}$$

which can be seen from $\sum_{j=0}^{L-1}(k+j)\,(mod\,L) \;=\; \frac{L\,(L-1)}{2}$, $k\,\in\,\mathbb{Z}$, which is trivial (just add the L terms which are $0,\,1,\,...\,,L-1$ in a certain cyclic order), and the relation between $mod\,L$ and the floor function $\left\lfloor\frac{k}{L}\right\rfloor \;=\; \frac{1}{L}\,(k \,-\, k\,(mod\,L))$. This identity allows us to lower L consecutive coefficients of this sum of $L\,+\,1$ terms by 1, producing a term k if one uses the identity for the first L terms because the second to last floor-argument is then $\lfloor\frac{k+0}{L}\rfloor$, and the identity is read backwards. If one uses the identity for the last L terms one produces a $k-1$, because the last term has $\lfloor\frac{k-1}{L}\rfloor$. When we apply this identity twice in the described way we pick up $n\,+\,(n-1) \,=\, 2\,n \,-\, 1$ and the first and last coefficient, which were originally 1, become 0, and all other coefficients are diminished by 2 because they participate in both applications of the identity. It is guaranteed that all coefficients are now even and ≥ 0, because the coefficients except the first and last one were even and ≥ 2, because these numerator polynomial coefficients resulted from first differences of the sequence of odd numbers. Therefore one can extract a factor 2 and if the floor-functions are written with increasing arguments, starting with $\left\lfloor\frac{k}{L}\right\rfloor$ (the second to last term in the original order), one has exactly the coefficients given by the list $\mathcal{F}(n)$ of length L of *definition 5*. This proves the explicit form for $o^*_{n,>}(k)$. □

Example 17: O.g.f. $\mathbf{G_8(x)}$

$$G_8(x) \;=\; x\,\frac{(1+2\,(x \,+\, x^2 \,+\, x^3 \,+\, x^4 \,+\, x^5 \,+\, x^6 \,+\, x^7) \,+\, x^8}{(1-x^8)\,(1-x)} \;=\; x\,\frac{1\,+\,x}{(1\,-\,x)^2} \tag{89}$$

generating, with offset 0, the odd numbers A004273.

Before coming to the multiplicative group *Modd* n we define reduced residue systems *Modd* n as well as reduced odd residue systems *Modd* n. See *e.g.*, [2], p. 113 for the *mod* n case.

Definition 6a: Reduced residue system Modd n

A reduced residue system *Modd* n (*RRSn*) is any set of $\varphi(n)$ pairwise incongruent *Modd* n numbers, each of which is relatively prime to n.

E.g., $n = 15$, $\varphi(15) = 8$, $\{1, 2, 4, 7, 8, 11, 13, 14\}$ or $\{29, 32, 26, 23, 22, 41, 17, 16\}$, *etc.* The first one is the smallest positive one. These systems will not play a rôle later on.

Definition 6b: Reduced odd residue system Modd n

A reduced odd residue system *Modd* n (*RoddRSn*) is any set of $\delta(n)$ odd pairwise incongruent *Modd* n numbers, each of which is relatively prime to n

E.g., $n = 15$, $\delta(15) = 4$, $\{1, 7, 11, 13\}$ or $\{29, 27, 19, 17\}$. The first one coincides with $\mathcal{M}(15)$ from eq. (65) and is the smallest positive reduced residue system *Modd* n. Remember that the parity of the members in each *Modd* n residue class, not in class $[0]$, is the same (see *lemma 12*). Later on we will restrict ourselves mostly to the system $\mathcal{M}(n)$.

We next study the multiplicative group *Modd* n. The elements are the residue classes $[m_j]$, for j = 1, 2, ..., $\delta(n)$, corresponding to the members of the reduced residue system $\mathcal{M}(n)$. In fact, we will take these representatives, multiplying *Modd* n, as we have done above.

In order to see the group structure one first convinces oneself that this set $\mathcal{M}(n)$ is closed under *Modd* n multiplication. This follows from *proposition 10* and *lemma 12* which showed that these classes have only odd numbers, and every odd numbers appear exactly once because of the definition of these classes. The associativity, commutativity and the identity element 1 are also clear. We do not have a formula how to find the inverse element m_j^{-1} of m_j but coming to this *Modd* n multiplication from the study of automorphisms of the splitting field for the minimal polynomial $C(n, x)$ for the algebraic number $\rho(n)$, it is clear that these inverses have to exist (the invariance property defines a group). We are dealing here with the *Galois* groups for these polynomials. The cycle structure for n = 1, 2, ..., 40 is given in *table 6*. Because each group is Abelian one has for every group of prime order a cyclic group, which can be checked for the examples given in *table 6*.

Remark 6: The multiplicative group *Modd* n is cyclic if $\delta(n)$ is prime.

This is a corollary on the fundamental theorem on finite Abelian groups (see *e.g.*, [28], p. 49, see also [6], p. 511, *Cauchy*'s Theorem A.1.5), or use *Lagrange*'s theorem on the order of subgroups, and the fact that the powers of an element, not the identity, generate a cyclic subgroup, to prove that in fact every group of prime order is cyclic. The values n for which the order $\delta(n)$ is prime are given in A215046. This is the sequence $[4, 5, 6, 7, 9, 11, 23, 47, 59, 83, 107, 167, 179, 227, 263, 347, 359, ...]$. Of course, there are other values n with cyclic *Modd* n group, like $n = 2, 3, 8, 10, ...$. For $n = 1$ one has the trivial case with cycle structure $[[0]]$, also a cyclic group, *viz* Z_1. One can give a more general sequence of n numbers with cyclic $\mathcal{G}_n \cong$ multiplicative *Modd* n group, namely A210845.

Remark 7: The multiplicative group *Modd* n is cyclic if $\delta(n)$ is squarefree.

The squarefree numbers are given in A005117, namely $[1, 2, 3, 4, 5, 6, 7, 9, 11, 13, 14, 18, 21, 22, 23, 25, 29, 31, ...]$. This *remark 7* results from the fact that A000688, giving the number of Abelian groups of order n, is 1 exactly for the squarefree numbers A005117. See the formula, based on the *H.-E. Richert* reference quoted there. Because for each order there is at least the cyclic group these values lead necessarily to a cyclic group. The above given A215046 values are a proper subset of those from A210845. There are. however, still more values n with a cyclic *Modd* n group. Missing are *e.g.*, $8, 10, 15, 16, 17, ...$. All the n values with cyclic *Modd* n group are in A206551. The complementary sequence is A206552, giving the n values with non-cyclic *Modd* n group. See *Table 8* for all values $n \leq 100$.

As an aside we remark that special squarefree numbers are the so called cyclic numbers A003277. It is known that if the order of a (finite) group is a cyclic number then there is only one group, the cyclic one. See a comment on A003277. Therefore A000001(n), the number of groups of order n is 1 if n is a cyclic number, in fact, the reverse also holds: if A000001$(n) = 1$ then n is a cyclic number. This can be taken as an alternative definition for cyclic numbers because then there is only one (non-isomorphic) group of this order which has to be the cyclic group. See also Yimin Ge's Math Blog [YiminGe], where the 'only if' statement in the proposition may be misleading but in the proof the given statement is correct. *E.g.*, for order 6 (not a cyclic number) there are groups other than Z_6. In fact A000001(6) $=$ 2, and there is the (non-Abelian) group D(3) (dihedral group). (It is clear that cyclic numbers are not the numbers n for which the multiplicative group $mod\, n$, which is Abelian of order $\varphi(n)$, is cyclic. These numbers are given in A033948). Because we are dealing with Abelian groups the squarefree numbers are more interesting here.

Recall the situation for the *Galois* group for the cyclotomic polynomials (the minimal polynomials for $\zeta(n)$, an n-th root of unity) which is isomorphic to the multiplicative (Abelian) group modulo n. See *Table 7* were we have listed these non-cyclic groups for $n \in \{1, \ldots, 100\}$. This $n-$value sequence is known as A033949. (The case $n = 15$ is an exercise in [7], p. 159, Ex. 9.6. 3)a)). The values n with a cyclic *Galois* group coincide with the moduli n which possess primitive roots $r = r(n)$, *i.e.*, the order of r modulo n is φ: $r^{\varphi(n)} \equiv 1\,(mod\, n)$, and no smaller positive exponent k satisfies this congruence. These moduli n are known to be exactly p^e, $2\,p^{e'}$, 1 and 2, with some positive powers e and e'. See *e.g.*, [23], *Theorem 2.41*, p. 104. All other n lead to non-cyclic multiplicative groups modulo n . See A033949. For the smallest primitive roots in this case see [1], pp. 864-869, the column called g. We do not know a similar characterization of the non-cyclic numbers n for the *Modd* n group which are shown in *Table 8*. However, these numbers have also to appear in A033949. It is clear that we should determine primitive roots $r \equiv r(n)$ for the *Modd* n multiplication, *i.e.*, find those r from $\mathcal{M}(n)$ which have order $\delta(n)$: the smallest positive k which satisfies $r^k \equiv +1\,(Modd\, n)$ is $k = \delta(n)$. See A206550 for these smallest positive primitive roots *Modd* n, where a 0 entry, except for $n = 1$, indicates that there exists no such primitive root. This sequence starts, with offset 1, as $[0, 1, 1, 3, 3, 5, 3, 3, 5, 3, 3, 0, 7, 5, 7, 3, 3, 5, 3, 0, 11, 3, 3, 0, 3, 7, ...]$. In general one does not expect a formula for these primitive roots $r = r(n)$, because also in the multiplication modulo n case there is no one available.

Proposition 14: Number of Modd n primitive roots

If a primitive root r for the multiplicative group *Modd* n exists there are $\varphi(\delta(n))$ of them.

This is the sequence A216322. For example, $n = 13$, $\delta(13) = 6$, $\varphi(6) = 2$ with $r_1 = 7$ and $r_2 = 11$; $n = 14$, $\delta(14) = 6$, $\varphi(6) = 2$ with $r_1 = 5$ and $r_2 = 11$.

Proof: If a *Modd* n primitive root exists then the multiplicative group *Modd* n is cyclic. The order of this group is $\delta(n)$, Then the number of pairwise incongruent primitive roots is obtained exactly like in the case of primitive m-roots of unity on the unit circle by the number of relatively prime numbers less than m which is *Euler*'s $\varphi(m)$. Here $m = \delta(n)$. □

Now the question whether the multiplicative group *Modd* p with p a prime is cyclic is answered. Up to now we know from *remark 7* the positive answer only for those primes with $\delta(p) = \frac{p-1}{2}$ squarefree. These are the primes given in A066651. The case $p = 2$ with $\delta(2) = 1$ is trivially cyclic. For general prime p one wants to show that there exists a primitive root in the multiplicative *Modd* p group. This is analog to the $mod\, p$ case, where a proof can be found in [23], Theorem 2.36, p. 99, or in [2], ch. 10.4, pp 206 ff. One has, however, to be careful to use only the multiplicative group structure in the proof. Already in connection with *lemma 10* we have given a warning to use theorems valid in the modular arithmetic $mod\, n$ in our case. Another failure occurs for the theorem [23], *Theorem 2.3(c)*, p. 49, *e.g.*, $x \equiv y\,(mod\, m_1), x \equiv y\,(mod\, m_2)$ if and only if $x = y\left(mod\,\frac{m_1\, m_2}{gcd(m_1, m_2)}\right)$. For the $Modd\, n$ case one has the counterexample $19 = 5\,(Modd\, 3)$ and $19 = 5\,(Modd\, 7))$ but 19 is obviously not congruent $5\,(Modd\, 21)$. Several *lemmata*, the analoga of *mod n* facts, are collected before stating *proposition 15.*

Lemma 19: Analogon of the Fermat-Euler Theorem

If a is odd and $gcd(a, n) = 1$ then $a^{\delta(n)} \equiv +1\,(Modd\, n)$, with $delta(n) =$A055034(n) (see the start of *section 3).*

Proof: Analog to *e.g.*, [2], *Theorem 5.17*, p. 113, with $m \to n$, $\varphi \to \delta$, the order of the set (reduced odd residue system) $\mathcal{M}(n)$ of eq. (65), and modulo $\to$ *Modd n* (we avoid the term Moddulo). Instead of $\mathcal{M}(n)$ one can use any other reduced odd residue system *Modd n* (see *definition 6b*), with $m_j(n)$, $j \in \{1,\, 2,\, \dots, \delta(n)\}$, replaced by any member of the residue class $[m_j(n)]$. The cancellation used at the end of the proof in [2] can be done here by multiplying with the existing inverses of the b_is there. We are dealing with the multiplicative group Modd n.

Next follows the definition of the order of an element from a reduced odd residue system *Modd n*.

Definition 7: Modd n order of a from a RoddRSn

The *Modd n* order of a positive (odd) integer a from a reduced odd residue system *Modd n* is the smallest positive integer h such that $a^h \equiv 1\,(Modd\, n)$.

E.g., $n = 10, a = 9, h = 2$ because $9^1 = 9\,(Modd\, 10)$, and $9^2 = 1\,(Modd\, 10)$. See the table A216320 corresponding to the *Modd n* orders h of the smallest positive *RoddRSn* members A216319.

Lemma 19 guarantees the existence of a *Modd n* order $h \le \delta(n)$ for each positive odd number a with $gcd(a,n) = 1$.

Example 18: $n = 12$, $\delta(12) = 4$, $\mathcal{M}(12) = \{1,5,7,11\}$, $1^4 \equiv 1\,(Modd\, 12)$, $5^2 \equiv 1\,(Modd\, 12) \Rightarrow 5^4 \equiv (Modd\, 12)$, similarly for 7 and 11. See the cycle structure for $n = 12$ in *table 6.*

Lemma 20: The Modd n order divides $\delta(\mathbf{n})$

If h is the *Modd n* order of a then $h|\delta(n)$. Moreover, $a^j \equiv a^k\ (Modd\, n)$, *w.l.o.g.* $j > k$, if and only if $h|(j-k)$.

Proof: The first part is analog to [23], *Corollary 2.32*, p. 98, with $\varphi \to \delta$. It uses lemma 19, the *Fermat-Euler* analogon. Remember that always $gcd(a,n) = 1$ from the order definition. The second part, for which one can use the group property, follows from the analog of [23], *Lemma 2.31*, p. 98. (In the older German version of this book, vol. I, the analog of this *lemma 20* appears as *Satz 22.3* on p. 63.) □

Lemma 21: On the Modd p order of a, p a prime

If h is the *Modd p* order of a, with p a prime, one has $(a^k)^h \equiv 1\,(\mathrm{Modd}\, p)$ for all k, and $1 = a^0,\, a^1,\, a^2,\, \dots, a^{h-1}$ are pairwise incongruent *Modd p.*

Proof: First part: $(a^k)^h = (a^h)^k$, $a^h \equiv 1\,(Modd\, p)$ and *Modd p* respects multiplication (see *proposition 10*). Second part: assume the contrary, *i.e.*, $a^i \equiv a^j\,(Modd\, p)$, $1 \le j < i \le h-1$. Apply *lemma 20* for $n = p$, showing that $h|(i-j)$, but $i-j \le i \le h-1$ leading to a contradiction. □

Lemma 22: $\mathbf{X^h} \equiv \mathbf{1\,(Modd\, p)}$ has at most h incongruent solutions

The congruence $X^h \equiv 1\ (Modd\, p)$, h a positive integer, has at most h pairwise incongruent solutions *Modd p.*

Proof: If $\left\lfloor \frac{X^h}{p} \right\rfloor$ is even then $X^h \equiv 1\,(mod\, p)$. and due to the *mod p* theorem, *e.g.*, [21], *Theorem 42*, p. 80, there are at most h incongruent solutions. If $\left\lfloor \frac{X^h}{p} \right\rfloor$ is odd then $-X^h \equiv 1\,(mod\, p)$, *i.e.*, $X^h \equiv (p-1)\,(mod\, p)$ which again has at most h incongruent solutions. □

This is a weak statement, but sufficient for the following. One could try to prove that the number of *Modd n* incongruent solutions of the congruence $X^h \equiv 1\ (Modd\, p)$ is $gcd(h, \frac{p-1}{2})$ if p is odd. This number is trivially 1 for $p = 2$.

Lemma 23: On the Modd n order of $\mathbf{a^k}$

If h is the *Modd n* order of a, then $\dfrac{h}{gcd(h,k)}$ is the *Modd n* order of a^k.

Proof: This is the analogon of [23] *lemma 2.33*, p. 98, using the present *lemma 20*, part 2. □

Now we are ready for the following *proposition.*

Proposition 15: Existence of Modd p primitive roots

For every prime p there exists a primitive root for the multiplicative group *Modd* p.

Proof: One shows that there are precisely $\varphi(\delta(p))$ primitive roots and because this number is always ≥ 1 the claim will then follow.

Following the proof of [23], *Theorem 2.36*, p. 99, we infer from the present *lemma 19* (with $n \to p$) that every positive odd integer a with $gcd(a,p) = 1$ has a *Modd* p order $h \equiv h_p(a)$, $1 \leq h \leq \delta(p) = \frac{p-1}{2}$, and from *lemma 20* $h|\delta(p)$. Moreover, $(a^h)^k \equiv 1 (Modd\ p)$ for all k, and 1, a^1, $a^2 \ldots a^{h-1}$ are h pairwise incongruent odd numbers *Modd* p. From *lemma 22* these are all the solutions of the congruence $X^h \equiv 1$ (*Modd* p). *Lemma 23* shows that there are $\varphi(h)$ numbers a^k, with $k \in \{1, \ldots h-1\}$ which have *Modd* p order $h \equiv h_p(a)$ because $\varphi(h)$ is the number of such k with $gcd(k,h) = 1$. The case $h = 1$ is covered with $\varphi(1) := 1$.

With [2], p. 207, we define for each $h|\delta(p)$ the set $A_p(h) := \left\{ a \;\middle|\; a \in \mathcal{M}(p) \text{ and } Modd\,p \text{ order of } a \text{ is } h \right\}$.

There are $\tau(\delta(p))$ ($\tau =$A000005, the number of divisors) such disjoint sets. This is the sequence [1, 1, 2, 2, 2, 4, 4, 3, 2, 4, 4, 6, ...] $=$A216326. *E.g.*, $p = 7$, $\mathcal{M}(7) = \{1, 3, 5\}$, $\tau(3) = 2$ (see also row No. n $=$p $=$7 of the *Modd* n order table A21630). Call $\psi_p(h) := |A_p(h)|$, the number of elements of this set. We have seen that $\psi_p(h)$ is 0 or $\varphi(h)$ because for each $h|\delta(p)$ the set $A_p(h)$ is either empty (no $a \in \mathcal{M}(p)$ has *Modd* p order h) or this set has $\varphi(h)$ elements. Thus $\psi_p(h) \leq \varphi(h)$. It is clear that $\sum_{h|\delta(h)} \psi_p(h) = \delta(p)$ because each $a \in \mathcal{M}(p)$ belongs to one of these sets $A_p(h)$. Now a standard result is $\sum_{h|\delta(h)} \varphi(h) = \delta(p)$ (see *e.g.*, [2], *Theorem 2.2*, p. 26, wit h$n \to \delta(p)$), therefore, $\sum_{h|\delta(h)} (\varphi(h) - \psi_p(h)) = 0$, but because $\varphi(h) - \psi_p(h) \geq 0$ it follows that $\psi_p(h) = \varphi(h) > 1$, not 0, for each $h|\delta(p)$. This holds especially for $h = \delta(p)$. Hence the number of primitive *Modd* p roots is $\psi_p(\delta(p)) = \varphi(\delta(p)) > 1$, and the proof is complete. □

For the sequence $\delta(p(n))\, n \geq 1$, see A130290. For the smallest positive primitive *Modd* n roots see the sequence A206550. Here for prime n.

Corollary 8: Cyclic Modd p group

The multiplicative (Abelian) *Modd* p group, for p a prime, is the cyclic group $Z_{\delta(p)}$.

We now concentrate on those groups *Modd* n which are cyclic and notice that whenever $\delta(n)$ is even there exists a unique smallest positive odd number > 1 which solves the congruence $x^2 \equiv 1$ (*Modd* n). This is the nontrivial solution of this congruence. The trivial one is $x = 1$ (standing for the class of solutions 1 (*Modd* n) which also includes -1). We prove this first for even n.

Proposition 16: Nontrivial square-root of 1 (Modd 2 k), k $\geq$ 2

If $n = 2\,k$, for $k \in \{2, 3, 4, \ldots\}$, and if the *Galois* group $\mathcal{G}al(\mathbb{Q}(\rho(n))/\mathbb{Q})$ is cyclic, a unique smallest positive solution $r > 1$ of the congruence $x^2 \equiv 1$ (*Modd* $2\,k$) exists, and it is $r = n - 1$.

Proof: For even $n = 2\,k$, $k \geq 2$, the cyclic group is then $Z_{\delta(2\,k)}$ and $\delta(2\,k)$ is even because with the standard prime factorization $\delta(2^e\, p_1^{e_1} \cdots p_N^{e_N}) = 2^{e-1} \prod_{j=1..N} p_j^{e_j - 1}\,(p_j - 1)$, and if $N = 0$ then $e \geq 2$, and if $N \geq 1$ then $e \geq 1$. In both cases δ is even, because in the second case there is at least one j and $p_j - 1$ is even. Even order $\delta(2\,k)$ of the cyclic group means that powers of the generator c of the δ-cycle, the smallest positive primitive root (of 1) (*Modd* 2 k), come in pairs which are mutually inverse, except for $1 = c^{\delta(2\,k)}$ and $s := c^{\frac{\delta(2\,k)}{2}}$. This $s > 1$ is unique and solves of the congruence $x^2 \equiv 1$ (*Modd* $2\,k$). Because $\left\lfloor \frac{(n-1)^2}{n} \right\rfloor = n - 2 + 0$ is, with even n, even, and in order to compute $(n-1)^2$ (*Modd* n)

one has to determine $(n-1)^2\,(mod\,n)$, which is 1. Therefore, the unique s for even n is $s = n-1$. $\square$

Example 19: Nontrivial square-root of 1 (Modd 8)

$s(8) = 7$: $7^2 = 49 \equiv 1\,(Modd\,8)$, because $\left\lfloor \frac{49}{8} \right\rfloor = 6$, hence $p_8(49) = +1$, and $49 \equiv +1\,(mod\,8)$, therefore $49 \equiv +1\,(Modd\,8)$.

Similarly, for $n = p$, p an odd prime, the cycle length is $\delta(p) = \frac{p-1}{2}$. In the event that $\frac{p-1}{2}$ is even, *i.e.*, if p is of the form $4\,k+1$, *i.e.*, $p \equiv 1\,(mod\,4)$, (see A002144) a smallest positive nontrivial solution of the quadratic congruence $x^2 \equiv 1\,(Modd\,n)$ exists. We will numerate the primes congruent $1\,(mod\,4)$ by defining $\hat{p}(n) :=$ A002144(n), $n \geq 1$. *E.g.*, for $n = \hat{p}(2) = 13$ one has, besides the trivial solution $x = 1\,(Modd\,13)$ (this residue class includes -1), $x \equiv 5\,(Modd\,13)$ as a solution. This means that in the group table the row for the element 5 has a 1 in the diagonal, like in the row for the identity element 1. These elements are self-inverse like the identity element 1. Note that in the ordinary reduced $mod\,n$ case there is always a 1 in the diagonal for row $p-1$, besides the 1 in the row for the identity element, but in that case $p-1 \equiv -1\,(mod\,n)$, and hence is a trivial solution. See A206549 for these non-trivial solutions in our case. The other inverses in these cyclic groups can be read off the cycle structure. One pairs the first entry, the generator c of the cycle, with the second to last (the one before the 1, the second with the third to last, etc. *E.g.*, for $n = 13$ one has the inverses $7^{-1} \equiv 11\,(Modd\,13)$, $11^{-1} \equiv 7\,(Modd\,13)$, and $3^{-1} \equiv 9\,(Modd\,13)$, $9^{-1} \equiv 3\,(Modd\,13)$, and the left over 5 is self-inverse, as mentioned above. This pairing of inverses is clear from the cyclic structure.

The next objective is to find some method to compute this uniquely existing smallest positive non-trivial solution $s(p)$ of the congruence $x^2 \equiv 1\,(Modd\,p)$ for given prime $p = \hat{p}(n) =$ A002144(n) for the $k(n) := \frac{\hat{p}(n)-1}{4}$ values given in A005098. This k-sequence starts with $[1, 3, 4, 7, 9, 10, 13, 15, 18, ...]$. The following l-algorithm will determine all these non-trivial solutions $s(\hat{p}(n))$ of the congruence $x^2 \equiv 1\,(M\,odd\,\hat{p}(n))$. We start with the *Ansatz* $s(p) = \sqrt{(o+1)\,p\,-\,1}$, with some odd number o. This means that we are looking for primes of the form $\frac{s^2\,+\,1}{o+1}$, and we are interested only in primes of the form $4\,k\,+\,1$, *i.e.*, $\hat{p}(n)$. Because $s(\hat{p})^2 = (o+1)\,\hat{p}\,-\,1$, $s(\hat{p})$ is odd, say $2\,K\,+\,1$. This implies $2\,K\,(K+1)\,+\,1 = \frac{o+1}{2}\,\hat{p}$, which shows that $\frac{o+1}{2}$ has to be odd, *i.e.*, $o = 4\,\hat{l}\,+\,1$. Now we compute the even number $2\,k = \frac{p-1}{2} = \frac{(2\,K+1)^2\,-\,(4\,\hat{l}+1)\,\hat{p}}{2} = 4\,T(K)\,-\,2\,\hat{l}\,-\,2\,k\,(4\,\hat{l}+1)$, where we have introduced the triangular numbers $T(K) := \frac{K\,(K+1)}{2}$, given in A000217. This implies that $2\,k\,(2\,\hat{l}\,+\,1) = 2\,T(K)\,-\,\hat{l}$. Therefore, $\hat{l}$ is even, say $2\,l$, and we have, with inputs k, l and K: $p = 4\,k\,+\,1$, $s^2(\hat{p}) = (o\,+\,1)\,p\,-\,1$, $o = 8\,l\,+\,1$ and $s(\hat{p}) = 2\,K(\hat{p})\,+\,1$. Because now $2\,T(K) = 2\,k\,+\,2l\,(4\,k\,+\,1) = 2\,l\,+\,2k\,(4\,l\,+\,1)$, we find the 'nice equation'

$$4\,T(K)\,+\,1 = (4\,k\,+\,1)\,(4\,l\,+\,1)\,. \tag{90}$$

For given prime $\hat{p}$ of the form $4\,k+1$, i.e. for $k = \frac{p-1}{4}$ (see A005098), we determine the minimal $l \in \mathbb{N}_0$, such that $k\,(1\,+\,4\,l)\,+\,l$ produces a triangular number, namely $T(K)$. The index of this triangular number is then $K = \frac{\sqrt{8\,T(K)+1}-1}{2}$. We have uses Maple [18] to compute these minimal l values. It will be seen from the later *proposition 15* that there is always such a minimal l, and not all non-negative values appear. Precisely the entries of A094178 and 0 occur as minimal l values. We will from now on denote this minimal l also by l (hoping to cause no confusion). If $l = 0$ then k is a triangular number, and conversely. The non-vanishing l values are characterized by having as elements of the squarefree kernel set of $4\,l+1$ only distinct primes congruent $1\,(mod\,4)$. *E.g.*, $l = 2$ will not appear because the squarefree kernel of 9 consists of the prime 3 which is not congruent $1\,(mod\,4)$. In order to proof that only numbers from A094178 can appear as positive l values, we use the 'nice equation' and observe that

$4\,T(K)\,+\,1\,=\,K^2\,+\,(K+1)^2$, *i.e.*, it is the sum to two neighboring squares with $gcd(K, K+1)\,=\,1$ (shown by indirect proof, see the remark following *definition 3*). Now a theorem ensures that all prime factors of $4\,T(K)\,+\,1$ are congruent $1\,(mod\,4)$. See the theorem 3.20 on p. 164 of the reference [23]. From the 'nice equation' we have either $4\,l\,+\,1\,=\,1$, *i.e.*, $l\,=\,0$, or, if l is non-vanishing, then the squarefree kernel set of $4\,l+1$ has only primes congruent $1\,(mod\ 4)$. Therefore l can be 0 or it is from A094178, *i.e.*, from $[0, 1, 3, 4, 6, 7, 9, 10, 13, 15, 16, 18, 21, 22, 24, 25, 27, 28, ...]$. The $l\,=\,0$ value appears for the primes $[5, 13, 41, 61, 113, 181, 313, 421, ...]$, which is the sequence A027862. In this case $k\,=\,\frac{\hat{p}-1}{4}$ is a triangular number. $l\,=\,1$ for the primes $[17, 29, 53, 73, 109, 137, 281, 397, 449, 593, 757, ...]$ This is the sequence A207337(n), $n\,\geq\,2$. These are the primes $\hat{p}$ such that $5\,\hat{p}\,=\,4\,T(K)\,+\,1$ for some $K\,=\,K(\hat{p})$. *E.g.*, $5\,17\,=\,85\,=\,4\,21\,=\,1$, thus $K(17)\,=\,6$. These are also the primes of the form $(m^2+1)/10$. Just use $m\,=\,m(K)\,=\,2\,K\,+\,1$. In general, $k\,=\,\dfrac{T(K)\,-\,l}{4\,l\,+\,1}$, (see eq. (90) and $K\,=\,\dfrac{\sqrt{2\,(4\,l\,+\,1)\,\hat{p}\,+\,1}\,-\,1}{2}$. *E.g.*, $\hat{p} = 53$ belongs to $l\,=\,1$ and $K\,=\,11$, and $T(K)\,=\,66$. This checks with the 'nice equation'. We do not give here the tables of the sequences $l(n)\,=\,l(\hat{p}(n))$ and $K(n)\,=\,K(l(n))$ (this incorrect renaming of arguments should not lead to confusion) for given $\hat{p}(n)$ because after the next *proposition 17* we will find another way to obtain the $K(n)$ numbers directly, hence the corresponding $l(n)$ numbers, and from these the desired $s(\hat{p}(n))$ solutions from $s(\hat{p}(n))\,=\,2\,K(n)\,+\,1$.

Proposition 17: Congruence $\mathbf{4\,T(X)\,+\,1\,=\,X^2\,+\,(X+1)^2\,\equiv\,0\,(mod\,p)}$

There are precisely two incongruent solutions of the congruence $f(X)\,:=\,2\,X^2\,+\,2\,X\,+\,1\,\equiv\,0\,(mod\,p)$, provided $p = \hat{p}(n)\,=$A002144(n), $n\,\geq\,1$. The smallest positive representative will be called $K(n)$, and the next larger incongruent one is then $K2(n)\,:=\,\hat{p}(n)\,-\,1\,-\,K(n)$.

Proof: Because of the degree 2 of f this congruence has at most two incongruent solutions. We shall see that in fact there are two. This congruence is reduced to a problem of quadratic residues, following a standard prescription (see, *e.g.*, [21], pp. 132-3). The discriminant of f is $D\,=\,2^2\,-\,4\,2\,1\,=\,-4$. Multiplying f by 8 yields $(4\,X+2)^2\,+\,4\,\equiv\,0\,(mod\,8\,p)$. With $Y\,=\,4\,X+2$ this is $Y^2\,=\,D\,(mod\,n)$, with a composite modulus $n\,=\,2^3\,p$. This is a quadratic residue problem, but $gcd(D, n)$ is not 1, but 4. Theorem 77 of [21] is applied with $d\,=\,4$, $e\,=\,2$, $f\,=\,1$, $a+1\,=\,-1$ and $n_1\,=\,2\,p$ Thus the problem is reduced to the quadratic residue problem $Z^2\,\equiv\,-1\,(mod\,2\,p)$. This is solved by studying the congruences for the powers of primes, here just 2 and p, separately (see *e.g.*, [21], sect. 26, pp. 83-5). The congruence modulo 2 has only the solution $+1$ (because $-1\,\equiv\,+1\,(mod\,2)$), and modulo p one can consult the *Legendre* symbol $\left(\dfrac{-1}{p}\right)$ which is $(-1)^{\frac{p-1}{2}}$ (see *e.g.*, [23], *Theorem* 3.2 (1), p. 132). Therefore -1 is a quadratic residue modulo p if and only if this symbol is $+1$, demanding that $p\,\equiv\,1\,(mod\,4)$, *i.e.*, $p\,=\,\hat{p}$ from A002144. Call the smallest positive solution x_0, then $\hat{p}\,-\,x_0$ is also an incongruent solution modulo $\hat{p}$, and two is the maximal number of solutions because of the degree 2 of this congruence. This implies that there are $1\cdot 2\,=\,2$ incongruent solutions of this congruence modulo $2\,p$ (see *e.g.*, [21], Theorem 46, p. 84). Returning to the original problem this proves that there are also two incongruent solutions. If the smallest positive solution for $\hat{p}(n)\,=$A207337(n) is called $K(n)$, then the next larger incongruent solution of $4\,T(X)\,+\,1\,=\,X^2\,+\,(X\,+\,1)^2)\,\equiv\,0\,(mod\,\hat{p}(n))$ is $K2(n)\,:=\,\hat{p}(n)\,-\,1\,-\,K(n)$, which is obvious. □

The pair of sequences of all positive solutions modulo 5, 13, and 17 are given in A047219, A212160 and A212161, respectively, where in each case the even indexed members are the positive solutions congruent to $K(n)$ and the odd indexed ones are the positive solutions congruent to $K2(n)$, *i.e.*, $a(2\,k)\,=\,k\,\hat{p}(n)\,+\,K(n)$ and $a(2\,k+1)\,=\,k\,\hat{p}(n)\,+\,K2(n)$, $k\,\geq\,0$. For the three given examples $n\,=\,1,\,2,\,3$ respectively. The companions $(K(n), K2(n))$ have been computed with Maple [18] and they can be found as A212353 and A212354. The first entries are for K: $[1, 2, 6, 8, 15, 4, 11, 5, 13, 27, 37, 45, 16, 7, 18, 52, 64, ...]$ and for K2: $[3, 10, 10, 20, 21, 36, 41, 55, 59, 61, 59, 55, 92, 105, 118, 96, 92, 126, ...]$ corresponding to the primes $\hat{p}$: $[5, 13, 17, 29, 37, 41, 53, 61, 73, 89, 97, 101, 109, 113, 137, 149, 157, 173, ...]$. Note that *proposition 17* yields directly the searched for nontrivial solution of $s(\hat{p}(n))^2\,\equiv\,+1\ (Modd\ \hat{p}(n))$ *via* $s(\hat{p}(n))\,=\,2\,K(n)\,+\,1$. Compare this with the s values given in A206549 with first entries $[3, 5, 13, 17, 31, 9, 23, 11, 27, 55, 75, 91, 33, 15, 37, 10$

Because $\hat{s}(n) := s(\hat{p}(n)) = 2\,K(n) + 1 \leq \hat{p}(n) - 2$, *i.e.*, $K(n) \leq \frac{\hat{p} - 3}{2}$ iff $\widehat{s2}(n) := K2(n) + 1 \geq \hat{p}(n)$ and $\hat{s}(n) \leq \widehat{s2}(n)$, $n \geq 1$. Thus only $\hat{s}(n) \in \mathcal{M}(\hat{p})$, the restricted odd residue class *Modd* $\hat{p}$, and the solution $\widehat{s2}(n)$ is discarded.

This *proposition* and the 'nice equation' eq. (90) show that the $l-$algorithm from above will indeed produce a solution l, related to the existing $K(n)$ for given $\hat{p}(n)$, *via* $l(n) = \left(\frac{4\,T(K(n)) \,+\, 1}{\hat{p}(n)} - 1\right)/4$. The smallest positive non-trivial solution $s(\hat{p}(n))$ of the congruence $x^2 \equiv +1\,(Modd\,\hat{p}(n))$ is then $2\,K(n) + 1$. See $K(n)$ =A212353(n), $n \geq 1$. *E.g.*, $n = 5$, $\hat{p}(5) = 37$, $K(5) = 15$, $l = \left\lfloor \frac{4\,120, \,+\, 1}{37} \right\rfloor - 1)/4 = 3$, $\hat{s}(n) = 31$, with $\left\lfloor \frac{31^2}{37} \right\rfloor = 25 = o$ and $31^2 = 961 = -1\,(mod\,37) = 36$.

As a application involving $s(\hat{p}(n))$ we derive the analog of *Wilson*'s theorem $\prod \mathcal{R}(p) = (p - 1)! \equiv (p-1)\,(mod\,p) \equiv -1\,(mod\,p)$, for each prime p (see *e.g.*, [2], Theorem 5.24, p. 116, or [10], Theorem 80, p. 68), where $\mathcal{R}(n)$is the set of the representatives of the smallest positive reduced residue system *mod* n for $n \geq 2$ which is of order $\varphi(n)$. In the *Modd* p case we have to replace the set $\mathcal{R}(n)$ by the set $\mathcal{M}(n)$ of eq. (65) with order $\delta(n)$.

Proposition 18: Analog of Wilson's theorem for Modd p

$$\prod \mathcal{M}(p) = (p-2)!! \equiv \begin{cases} 1 & \text{if } \frac{p-1}{2} \text{ is odd} \\ \\ \hat{s}(n) & \text{if } \frac{p-1}{2} \text{ is even, } p = \hat{p}(n),\ n \in \mathbb{N} \end{cases} \qquad (Modd\,p)\,, \tag{91}$$

where $\hat{s}(n) = s(\hat{p}(n))$, $\hat{p}(n)$ =A002144(n), stands for the above treated nontrivial root *Modd* n, *i.e.*, the solution of the congruence $x^2 \equiv 1\,(Modd\,n)$ which is not 1, if it exists. Note that $-1 \equiv +1\,(Modd\,n)$, $n \geq 2$ (see *lemma 10*). For the double factorials $(p-2)!!$ see A207332.

Proof: The multiplicative group group *Modd* p, p a prime, is the cyclic group $Z_{\delta(p)}$ from *proposition 14*. The order $\delta(p)$ of this group is even if and only if $p = \hat{p}$, *i.e.*, a prime $1\,(mod\,4)$. In this case we know from above that the non-trivial $\hat{s}(n) = s(\hat{p}(n))$ exists, and an algorithm for finding it has been given. Besides the unit element 1 and this $\hat{s}(n)$ all other factors in $\prod \mathcal{M}(\hat{p})$ can be paired such that their product is 1 (*Modd* $\hat{p}$) (see the discussion after *proposition 16*), leaving only $s(\hat{p})$. In the other case, when $p \equiv 3\,(mod\,p)$, the group order is odd. Then all numbers besides 1 can be paired in the product to produce $1\,(Modd\,p)$, and the result is therefore 1. □

For the cyclic *Galois* groups belonging to $C(n, x)$ the list of the smallest positive primitive roots $r(n)$ (*i.e.*, the smallest element from $\mathcal{M}(n)$ which generate these cyclic groups) are found under A206550. As mentioned above, we do not have a formula for those $n > 3$ values whose cycle does not start with 3 as smallest positive primitive root, like for $n = [6, 9, 13, 14, 15, 18, 21, 26, 27, 33, 37, 38, 39, ...]$.

Open problems:

- Proof of the *conjecture* on the $q-$sequence related to the discriminant of the minimal $C(n, x)$ polynomials; or find a counterexample.
- Characterization of the values n for which the *Galois* group $\mathcal{G}_n$ is non-cyclic.
- Characterization of the values n for which the cycle of the cyclic multiplicative group *Modd* $n \cong \mathcal{G}_n$ is generated by 3.
- More theorems on multiplicative *Modd* n arithmetic.

Appendix A

The proof of eq. (30), with $\frac{\varphi(n)}{n}$ replaced by the product-formula given there a bit later, is a (nice) application of *PIE* (the principle of inclusion and exclusion. See *e.g.*, [5], Theorem 4.2, pp. 134 ff). As mentioned above, this formula uses only the distinct prime factors of n, the elements of the set $sqfkset(n)$, the set of primes of the squarefree kernel of n. The product formula for $\frac{\varphi(n)}{n}$ can be read as the generating function for the *elementary symmetric functions* (here polynomials) in the variables $\frac{1}{p_j}, j = 1, 2, ..., M(n)$. $M(n)$, also called $\omega(n)$, is given in [27] as A001221(n).

$$\frac{\varphi(n)}{n} = \prod_{j=1}^{M(n)} \left(1 - \frac{1}{p_j}\right) = \sum_{r=0}^{M(n)} (-1)^r \, \sigma_r \left(\frac{1}{p_1}, ..., \frac{1}{p_{M(n)}}\right) , \tag{92}$$

with $\sigma_0 = 1$, and symbolically $\sigma_r = \sum\limits_r \frac{1}{p_. \cdots p_.}$, where the sum extends over the $\binom{M}{r}$ terms with r factors $\frac{1}{p_.}$ with increasing indices. *E.g.*, $M = 3$ with $\sigma_2 = \frac{1}{p_1\,p_2} + \frac{1}{p_1\,p_3} + \frac{1}{p_2\,p_3}$.

To calculate $\sum\limits_{\substack{k=1\\ gcd(k,n)=1}}^{n-1} k$ one starts, at the zeroth step ($r = 0$), with the unrestricted sum which is $\frac{n}{2}\,(n-1)$, and subtracts, in the next step (r $=1$), the sum of all multiples of each prime dividing n which are $\leq\, (n-1)$. For the p_j-multiples this sum is $p_j \sum\limits_{k=1}^{\frac{n}{p_j}-1} k = \frac{n}{2}\left(\frac{n}{p_j} - 1\right)$, for $j = 1, 2, ..., M(n)$. This leads, in step $r = 1$ to the subtraction of $\frac{n}{2} \sum\limits_j \left(\frac{n}{p_j} - 1\right)$. Now in this subtraction all multiples of the product of two different p_js appeared twice, therefore one has, in the next step ($r = 2$), to add them once. This is done by $+1 \sum\limits_{i<j} p_i\,p_j \sum\limits_{k=1}^{\frac{n}{p_i\,p_j}-1} k = \frac{n}{2} \sum\limits_{i<j} \left(\frac{n}{p_.\,p_.} - 1\right)$. In step $r = 3$ one concentrates on products of three different primes $p_{i_1}\,p_{i_2}\,p_{i_3}$ with $i_1 < i_2 < i_3$. Now such a 3$-$product appeared once in step $r = 0$ (in the unrestricted sum), -3 times in step $r = 1$, originating from the multiples $(p_{i_1}\,p_{i_2}) \cdot p_{i_3}$, $(p_{i_1}\,p_{i_3}) \cdot p_{i_2}$ and $(p_{i_2}\,p_{i_3}) \cdot p_{i_1}$, and $+3$ times in step $r = 2$, from the multiples $p_{i_1} \cdot (\,p_{i_2}\,p_{i_3})$, $p_{i_2} \cdot (\,p_{i_1}\,p_{i_3})$, and $p_{i_3} \cdot (\,p_{i_1}\,p_{i_2})$. Therefore, up to this stage, each such 3$-$product appeared once too much, and it is subtracted in this step $r = 3$ when all these 3$-$products terms are summed. Now the pattern starts to become clear. Up to, and including, step $r = 3$ one has for each 4$-$product the counting $1 - 4 + 6 - 4 = -1$. Hence in step $r = 4$ one adds once the sum over all multiples of each such 4$-$product. In general, in step r this counting will produce $(-1)^{r+1}$ (from the alternating row $r = 4$ in the *Pascal* triangle A007318), and one will therefore add $(-1)^r$ times the sum over all multiples of each such $r-$product. This yields

$$\begin{aligned}\sum_{\substack{k=1\\ gcd(k,n)=1}}^{n-1} k = \quad & \frac{n}{2}\left[(n-1) - \sum_{i_1}\left(\frac{n}{p_{i_1}} - 1\right) + \sum_{i_1<i_2}\left(\frac{n}{p_{i_1}\,p_{i_2}} - 1\right) ... - + \right. \\ & \left. ... \, (-1)^{M(n)} \sum_{i_1<...<i_{M(n)}} \left(\frac{n}{p_1\,p_2\,\cdots\,p_{M(n)}} - 1\right)\right] .\end{aligned} \tag{93}$$

Now the ± 1 terms all cancel if one takes into account the number of terms of each $r-$ sum, which is $\binom{M}{r}$. This is due to the vanishing alternating sum over *Pascal* triangle's row M. Thus the result becomes the alternating sum over the elementary symmetric polynomials with the reciprocal distinct prime factors of

n as variables.

$$\sum_{\substack{k=1\\ gcd(k,n)=1}}^{n-1} k \;=\; \frac{n^2}{2} \sum_{r=0}^{M(n)} (-1)^r\, \sigma_r \left(\frac{1}{p_1}, ..., \frac{1}{p_{M(n)}}\right) \;. \tag{94}$$

As mentioned above this is written as the generating function of these polynomials and the final result is with the second part of eq. (92)

$$\sum_{\substack{k=1\\ gcd(k,n)=1}}^{n-1} k \;=\; \frac{n^2}{2} \prod_{j=0}^{M(n)} \left(1 \,-\, \frac{1}{p_j}\right) \;. \tag{95}$$

This shows that $s(n) \;:=\; \frac{2}{n^2} \sum_{\substack{k=1\\ gcd(k,n)=1}}^{n-1} k$ is indeed $\frac{\varphi(n)}{n}$, which appears in [27] as A076512(n)/A109395(n). $s(n)$ is identical for all n with the same distinct prime factors, independent of their multiplicity, *i.e.*, it depends only on the elements of $sqfset(n)$. From the multiplicativity of φ one sees that this scaled sum $s(n)$ is also multiplicative. *E.g.*, $s(12) \;=\; s(6) \;=\; s(2)\, s(3)$.

Appendix B

For the proof of eq. (56) we follow [24], p.33, and consider the rewritten version

$$\prod_{k=1}^{n-1} \left(1 \,-\, e^{2\,\pi\,i\,\frac{k}{n}}\right) \;=\; \begin{cases} 1 & \text{if } n \text{ is odd}\,, \\ 0 & \text{if } n \text{ is even}\;. \end{cases} \tag{96}$$

In order to see that this is identical to eq. (56), just extract $e^{\pi\,i\,\frac{k}{n}}$, leading to the (2 cos) factors under the product, and in front summing in the exponent leads to the factor $e^{\frac{1}{2}\,\pi\,i\,(n-1)} \;=\; i^{n-1} \;=\; (-1)^{\frac{n-1}{2}}$. The *l.h.s.* of eq. (96) is then computed using (for the last step see *e.g.*, [9], Exercise 50, p. 149)

$$1 \,+\, z \,+\, z^2 \,+\, \;...\; +\, z^{n-1} \;=\; \frac{z^n \,-\, 1}{z \,-\, 1} \;=\; \prod_{k=1}^{n-1} (z \,-\, e^{2\,\pi\,i\,\frac{k}{n}})\;, \tag{97}$$

where one specializes to $z = -1$. (By putting $z \;=\; +1$ one finds the result $\prod_{k=1}^{n-1} 2\,\sin\left(\pi\,\frac{k}{n}\right) \;=\; n\,,\; n \,\geq\, 2$, with 1 for $n \;=\; 1$.)

References

[1] Abramowitz and I. A. Stegun, eds., *Handbook of Mathematical Functions*, National Bureau of Standards Applied Math. Series 55, Tenth Printing, reprinted as Dover publication, seventh printing 1968, New York, 1972

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

[3] E. Artin, with a section by N. A, Milgram, Galoissche Theorie, 3. Auflage, Harri Deutsch, 1988. English version: Galois theory. Lectures delivered at the University of Notre Dame, 1966

[4] Chan-Lye Lee and K. B. Wong, On Chebyshev's polynomials and certain combinatorial identities, 2009, Bull. Malaysian Sciences Soc.

http://www.emis.de/journals/BMMSS/accepted_papers.htm.

[5] Ch. A. Charalambides, *Enumerative Combinatorics*, Chapman &Hall/CRC, 2002

[6] D. A. Cox, *Galois Theory*, Wiley, 2004

[7] J.-P. Escofier, *Galois Theory*, Springer, 2001

[8] Yimin Ge's Math Blog, 2009,

http://yiminge.wordpress.com/2009/01/22/all-groups-of-order-n-are-cyclic-iff/

[9] R. L. Graham, D. E. Knuth and O. Patashnik, *Concrete Mathematics*, Addison-Weseley, Reading, Massachusetts, 1991

[10] G. H. Hardy and E. M. Wright, An Introduction to the Theory of Numbers, fifth ed,. Oxford Science publications, 2003

[11] The On-Line Encyclopedia of Integer Sequences^{TM} (OEIS), published electronically at http://oeis.org, 2011

[12] S. Lang, Algebra, revised third ed., Springer, 2002

[13] W. Lang, Minimal Polynomials for $\cos\left(\frac{2\,\pi}{n}\right)$, a link under [27] A181875.

[14] W. Lang, Divisor Product Representation for Natural Numbers, a link under [27] A007955.

[15] W. Lang, A181878, Coefficient array for square of Chebyshev S-polynomials, a link under [27] A181878.

[16] A. Lazarev, Galois Theory, lecture notes with problems and solutions, University of Leicester,

http://www2.le.ac.uk/departments/mathematics/extranet/staff-material/staff-profiles/al179

[17] D. H. Lehmer, A Note on Trigonometric Algebraic Numbers, Am. Math. Monthly 40,8 (1933) 165-6.

[18] Maple^{TM}, http://www.maplesoft.com/

[19] Wolfram Mathworld, http://mathworld.wolfram.com/SylvesterCyclotomicNumber.html, Sylvester Cyclotomic Number.

[20] W. Magnus, F. Oberhettinger, R. P. Soni, Formulas and theorems for the special functions of mathematical physics. 3$^{\text{rd}}$ enlarged ed., 1966, Springer, Berlin.

[21] T. Nagell, *Introduction to Number Theory*, Chelsea Pub. Comp., N.Y., 2nd ed., 1964.

[22] I. Niven, *Irrational Numbers*, The Math. Assoc, of America, second printing, distributed by John Wiley and Sons, 1963.

[23] I. Niven, H. S. Zuckerman and H. L. Montgomery, *An Introduction to the Theory Of Numbers*, Fifth Edition, John Wiley and Sons, Inc., NY, 1991.

[24] R. Remmert, *Funktionentheorie 2*, Springer, 1991

[25] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer, 2001.

[26] Th. J. Rivlin, *Chebyshev Polynomials. From Approximation Theory to Algebra and Number Theory*, second edition, Wiley-Interscience, 1990.

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

[28] A. Speiser, *Die Theorie der Gruppen endlicher Ordnung*, Vierte Auflage, 1956, Birkhäuser, Basel

[29] P. Steinbach, Golden Fields: A Case for the Heptagon, Mathematics Magazine, 70,1 (1997) 22-31, http://www.jstor.org/pss/2691048.

[30] W. Watkins and J. Zeitlin, The Minimal Polynomial of $\cos(2\pi/n)$, Am. Math. Monthly 100,5 (1993) 471-4, http://www.jstor.org/pss/2324301.

[31] Wikipedia, *Cycle graph (algebra)* http://en.wikipedia.org/wiki/Cycle_graph_(algebra) and *List of small groups* http://en.wikipedia.org/wiki/List_of_small_groups.

Keywords: regular n-gons, algebraic number, minimal polynomial, zeros, factorization, congruences, *Galois* theory, cycle graphs.

AMS MSC numbers: 11R04, 11R32 , 08B10, 13F20, 12D10, 13P05

OEIS A-numbers: A000001, A000005, A000007, A000010, A000012, A000035, A000265, A000668, A000688, A001221, A002110, A002144, A003277, A004124, A005013, A005098, A005117, A006053, A006054, A007310, A007318, A007775, A007814, A007947, A007955, A008683, A023022, A024556, A027862, A033949, A045572, A049310, A0503384, A052547, A047219, A053120, A055034, A066651, A076512, A077998, A084101, A085810, A088520, A090298, A092260, A094178, A106803, A109395, A110551, A113807, A116423, A120757, A127672, A128672, A130290, A130777, A147600, A162699, A181875, A181876, A181878, A181879, A181880, A193376, A193377, A193679, A193680, A193681, A193682, A203571, A203572, A203575, A204453, A204454, A204457, A204458, A206543, A206544, A206545, A206546, A206547, A206548, A206549, A206550, A206551, A206552, A207333, A207334, A207337, A210845, A212160, A212161, A212353, A212354, A215041, A215046, A216319, A216320, A216322, A216326.

Table 1: Reduced DSR-algebras (over $\mathbb{Q}$), $\mathbf{n = 3, ..., 12}$.

n	$\rho \equiv \rho(n)$	reduced DSR-algebra	δ(n)	DSR – basis
3	1	$\rho^2 = 1$	1	$< 1 >$
4	$\sqrt{2}$	$\rho^2 = 2$	2	$< 1, \rho >$
5	$\varphi = \frac{1}{2}(1 + \sqrt{5})$	$\rho^2 = \rho + 1$	2	$< 1, \rho >$
$\boxed{6}$	$\sqrt{3}$	$\rho^2 = 3, \; [\sigma = \rho^2 - 1 = 2]$	2	$< 1, \rho >$
7	$2 \cos\left(\frac{\pi}{7}\right)$	$\rho^2 = 1 + \sigma, \; \sigma^2 = 1 + \rho + \sigma, \; \rho\sigma = \rho + \sigma$	3	$< 1, \rho, \sigma >$
8	$\sqrt{2 + \sqrt{2}}$	$\rho^2 = 1 + \sigma, \; \sigma^2 = 2\sigma + 1, \; \tau^2 = 2(1 + \sigma),$ $\rho\sigma = \rho + \tau, \; \rho\tau = 2\sigma, \; \sigma\tau = 2\rho + \tau,$ $(\sigma = 1 + \sqrt{2}, \; \tau = \sqrt{2}\rho)$	4	$< 1, \rho, \sigma, \tau >$
$\boxed{9}$	$2 \cos\left(\frac{\pi}{9}\right)$	$\rho^2 = 1 + \sigma, \; \sigma^2 = 2 + \rho + \sigma, \; \rho\sigma = 2\rho + 1,$ $(\sigma = \rho^2 - 1), \; [\tau = \rho(\sigma - 1) = 1 + \rho]$	3	$< 1, \rho, \sigma >$
$\boxed{10}$	$\varphi\sqrt{3 - \varphi}$	$\rho^2 = 1 + \sigma, \; \sigma^2 = -1 + 3\sigma, \; \tau^2 = -1 + 4\sigma,$ $\rho\sigma = \rho + \tau, \; \rho\tau = 3\sigma - 2, \; \sigma\tau = \rho + 2\tau,$ $(\sigma = \rho^2 - 1 = 1 + \varphi, \; \tau = \rho(\sigma - 1),$ $\quad = (1 + \varphi)\sqrt{3 - \varphi})$ $[\omega = 2(-1 + \sigma) = 2\varphi]$	4	$< 1, \rho, \sigma, \tau >$
11	$2 \cos\left(\frac{\pi}{11}\right)$	$\rho^2 = 1 + \sigma, \; \sigma^2 = 1 + \sigma + \omega,$ $\tau^2 = 1 + \sigma + \tau + \omega, \; \omega^2 = 1 + \rho + \sigma + \tau + \omega,$ $\rho\sigma = \rho + \tau, \; \rho\tau = \sigma + \omega, \; \rho\omega = \tau + \omega,$ $\sigma\tau = \rho + \tau + \omega, \; \sigma\omega = \sigma + \tau + \omega,$ $\tau\omega = \rho + \sigma + \tau + \omega,$ $(\sigma = \rho^2 - 1, \; \tau = \rho(\sigma - 1), \; \omega = \sigma(\sigma - 1) - 1)$	5	$< 1, \rho, \sigma, \tau, \omega >$
$\boxed{12}$	$\sqrt{2 + \sqrt{3}}$	$\rho^2 = 1 + \sigma, \; \sigma^2 = 2(1 + \tau), \; \tau^2 = 3(1 + \sigma),$ $\rho\sigma = \rho + \tau, \; \rho\tau = 1 + 2\sigma, \; \sigma\tau = 3\rho + \tau,$ $[\omega = 1 + \sigma, \; \chi = 2\rho],$ $(\sigma = \rho^2 - 1 = 1 + \sqrt{3}, \; \tau = \frac{\sqrt{2}}{2}(3 + \sqrt{3}))$	4	$< 1, \rho, \sigma, \tau >$
$\vdots$				

$$\rho(n) := 2 \cos\left(\frac{\pi}{n}\right), \quad R_k^{(n)} = S(k-1, \rho(n)), \quad k = 1, ..., \left\lfloor \frac{n}{2} \right\rfloor,$$

$$R_1 = 1, \; R_2 \equiv \rho, \; R_3 \equiv \sigma, \; R_4 \equiv \tau, \; R_5 \equiv \omega, \; R_6 \equiv \chi \text{ (dependence on } n \text{ suppressed).}$$

In round brackets the values for the basis elements are given in terms of ρ. In square brackets the linear dependent DSRs are given. Boxed n-numbers indicate linear dependent DSRs.

Table 2: Minimal polynomials of $\mathbf{2\cos\left(\frac{\pi}{n}\right)}$ for $\mathbf{n = 1, 2, ..., 30}$.

n	$\mathbf{C(n, x)}$
1	$x+2$
2	x
3	$x-1$
4	x^2-2
5	x^2-x-1
6	x^2-3
7	$x^3-x^2-2\,x+1$
8	$x^4-4\,x^2+2$
9	x^3-3x-1
10	$x^4-5\,x^2+5$
11	$x^5-x^4-4\,x^3+3\,x^2+3\,x-1$
12	$x^4-4\,x^2+1$
13	$x^6-x^5-5\,x^4+4\,x^3+6\,x^2-3\,x-1$
14	$x^6-7\,x^4+14\,x^2-7$
15	$x^4+x^3-4\,x^2-4\,x+1$
16	$x^8-8\,x^6+20\,x^4-16\,x^2+2$
17	$x^8-x^7-7\,x^6+6\,x^5+15\,x^4-10\,x^3-10\,x^2+4\,x+1$
18	$x^6-6\,x^4+9\,x^2-3$
19	$x^9-x^8-8\,x^7+7\,x^6+21\,x^5-15\,x^4-20\,x^3+10\,x^2+5\,x-1$
20	$x^8-8\,x^6+19\,x^4-12\,x^2+1$
21	$x^6+x^5-6\,x^4-6\,x^3+8\,x^2+8\,x+1$
22	$x^{10}-11\,x^8+44\,x^6-77\,x^4+55\,x^2-11$
23	$x^{11}-x^{10}-10\,x^9+9\,x^8+36\,x^7-28\,x^6-56\,x^5+35\,x^4+$ $35\,x^3-15\,x^2-6\,x+1,$
24	$x^8-8\,x^6+20\,x^4-16\,x^2+1$
25	$x^{10}-10\,x^8+35\,x^6-x^5-50\,x^4+5\,x^3+25\,x^2-5\,x-1$
26	$x^{12}-13\,x^{10}+65\,x^8-156\,x^6+182\,x^4-91\,x^2+13$
27	$x^9-9\,x^7+27\,x^5-30\,x^3+9\,x-1$
28	$x^{12}-12\,x^{10}+53\,x^8-104\,x^6+86\,x^4-24\,x^2+1$
29	$x^{14}-x^{13}-13\,x^{12}+12\,x^{11}+66\,x^{10}-55\,x^9-165\,x^8+$ $120\,x^7+210\,x^6-126\,x^5-126\,x^4+56\,x^3+28\,x^2-7\,x-1$
30	$x^8-7\,x^6+14\,x^4-8\,x^2+1$
⋮	

Table 3: A187360(n, m) coefficient array of minimal polynomials of $2\cos\left(\frac{\pi}{n}\right)$, rising powers

n/m	**0**	**1**	**2**	**3**	**4**	**5**	**6**	...
1	2	1						
2	0	1						
3	-1	1						
4	-2	0	1					
5	-1	-1	1					
6	-3	0	1					
7	1	-2	-1	1				
8	2	0	-4	0	1			
9	-1	-3	0	1				
10	5	0	-5	0	1			
11	-1	3	3	-4	-1	1		
12	1	0	-4	0	1			
13	-1	-3	6	4	-5	-1	1	
14	-7	0	14	0	-7	0	1	
15	1	-4	-4	1	1			
⋮								

Table 4: Zeros of $\mathbf{C(n,x)}$ in power basis (rising powers of $\rho(\mathbf{n})$) for $\mathbf{n = 1, 2, ..., 30}$.

n	**coefficients of C-zeros in power basis $< \rho^{0}, ..., \rho^{\delta(n)-1} >$**
1	$[[-2]]$
2	$[[0]]$
3	$[[1]]$
4	$[[0,1],[0,-1]]$
5	$[[0,1],[1,-1]]$
6	$[[0,1],[0,-1]]$
7	$[[0,1],[-1,-1,1],[2,0,-1]]$
8	$[[0,1],[0,-3,0,1],[0,3,0,-1],[0,-1]]$
9	$[[0,1],[-2,-1,1],[2,0,-1]]$
10	$[[0,1],[0,-3,0,1],[0,3,0,-1],[0,-1]]$
11	$[[0,1],[0,-3,0,1],[1,2,-3,-1,1],[-2,0,4,0,-1],[2,0,-1]]$
12	$[[0,1],[0,4,0,-1],[0,-4,0,1],[0,-1]]$
13	$[[0,1],[0,-3,0,1],[0,5,0,-5,0,1],[1,-3,-3,4,1,-1],[-2,0,4,0,-1],[2,0,-1]]$
14	$[[0,1],[0,-3,0,1],[0,5,0,-5,0,1],[0,-5,0,5,0,-1],[0,3,0,-1],[0,-1]]$
15	$[[0,1],[-2,3,1,-1],[-1,-4,0,1],[2,0,-1]]$
16	$[[0,1],[0,-3,0,1],[0,5,0,-5,0,1],[0,-7,0,14,0,-7,0,1],[0,7,0,-14,0,7,0,-1],[0,-5,0,5,0,-1],$ $[0,3,0,-1],[0,-1]]$
17	$[[0,1],[0,-3,0,1],[0,5,0,-5,0,1],[0,-7,0,14,0,-7,0,1],[-1,4,6,-10,-5,6,1,-1],$ $[2,0,-9,0,6,0,-1],[-2,0,4,0,-1],[2,0,-1]]$
18	$[[0,1],[0,5,0,-5,0,1],[0,-4,0,5,0,-1],[0,4,0,-5,0,1],[0,-5,0,5,0,-1],[0,-1]]$
19	$[[0,1],[0,-3,0,1],[0,5,0,-5,0,1],[0,-7,0,14,0,-7,0,1],[1,4,-10,-10,15,6,-7,-1,1],$ $[-2,0,16,0,-20,0,8,0,-1],[2,0,-9,0,6,0,-1],[-2,0,4,0,-1],[2,0,-1]]$
20	$[[0,1],[0,-3,0,1],[0,-7,0,14,0,-7,0,1],[0,8,0,-18,0,8,0,-1],[0,-8,0,18,0,-8,0,1],$ $[0,7,0,-14,0,7,0,-1],[0,3,0,-1],[0,-1]]$
21	$[[0,1],[0,5,0,-5,0,1],[2,3,-4,-1,1],[-3,-9,1,6,0,-1],[-2,0,4,0,-1],[2,0,-1]]$
22	$[[0,1],[0,-3,0,1],[0,5,0,-5,0,1],[0,-7,0,14,0,-7,0,1],[0,9,0,-30,0,27,0,-9,0,1],$ $[0,-9,0,30,0,-27,0,9,0,-1],[0,7,0,-14,0,7,0,-1],[0,-5,0,5,0,-1],[0,3,0,-1],[0,-1]]$
23	$[[0,1],[0,-3,0,1],[0,5,0,-5,0,1],[0,-7,0,14,0,-7,0,1],[0,9,0,-30,0,27,0,-9,0,1],$ $[-1,-5,15,20,-35,-21,28,8,-9,-1,1],[2,0,-25,0,50,0,-35,0,10,0,-1],$ $[-2,0,16,0,-20,0,8,0,-1],[2,0,-9,0,6,0,-1],[-2,0,4,0,-1],[2,0,-1]]$
24	$[[0,1],[0,5,0,-5,0,1],[0,-7,0,14,0,-7,0,1],[0,-8,0,6,0,-1],[0,8,0,-6,0,1],$ $[0,7,0,-14,0,7,0,-1],[0,-5,0,5,0,-1],[0,-1]]$
25	$[[0,1],[0,-3,0,1],[0,-7,0,14,0,-7,0,1],[0,9,0,-30,0,27,0,-9,0,1],$ $[0,-10,5,30,-5,-27,1,9,0,-1],[0,10,-15,-15,20,7,-8,-1,1],[-2,0,16,0,-20,0,8,0,-1],$ $[2,0,-9,0,6,0,-1],[-2,0,4,0,-1],[2,0,-1]]$
26	$[[0,1],[0,-3,0,1],[0,5,0,-5,0,1],[0,-7,0,14,0,-7,0,1],[0,9,0,-30,0,27,0,-9,0,1],$ $[0,-11,0,55,0,-77,0,44,0,-11,0,1],[0,11,0,-55,0,77,0,-44,0,11,0,-1],$ $[0,-9,0,30,0,-27,0,9,0,-1],[0,7,0,-14,0,7,0,-1],[0,-5,0,5,0,-1],[0,3,0,-1],[0,-1]]$
27	$[[0,1],[0,5,0,-5,0,1],[0,-7,0,14,0,-7,0,1],[-2,7,1,-14,0,7,0,-1],[2,-5,-4,5,1,-1],$ $[2,-1,-16,0,20,0,-8,0,1],[-2,0,16,0,-20,0,8,0,-1],[-2,0,4,0,-1],[2,0,-1]]$
$\vdots$	**continued on next page**

Note: the higher power coefficients not shown are all zero.

Example: $\mathbf{n = 27}$: the first zero of $\mathbf{C(27,x)}$ is $\rho(27)$, the second zero is $\mathbf{5}\,\rho(\mathbf{27}) - \mathbf{5}\,\rho(\mathbf{27})^{\mathbf{3}} - \mathbf{1}\,\rho(\mathbf{27})^{\mathbf{5}}$, etc.

Table 4 continued: Zeros of $\mathbf{C(n,x)}$ in power basis (rising powers of $\boldsymbol{\rho}(\mathbf{n})$) for $\mathbf{n\,=\,28,...,30.}$

n	**power basis coefficients for** $< \boldsymbol{\rho}^{\mathbf{0}}, ..., \boldsymbol{\rho}^{\boldsymbol{\delta}(\mathbf{n})-\mathbf{1}} >$
28	$[[0,1],[0,-3,0,1],[0,5,0,-5,0,1],[0,9,0,-30,0,27,0,-9,0,1],[0,-11,0,55,0,-77,0,44,0,-11,0,1],$ $[0,12,0,-67,0,96,0,-52,0,12,0,-1],[0,-12,0,67,0,-96,0,52,0,-12,0,1],$ $[0,11,0,-55,0,77,0,-44,0,11,0,-1],[0,-9,0,30,0,-27,0,9,0,-1],[0,-5,0,5,0,-1],[0,3,0,-1],$ $[0,-1]]$
29	$[[0,1],[0,-3,0,1],[0,5,0,-5,0,1],[0,-7,0,14,0,-7,0,1],[0,9,0,-30,0,27,0,-9,0,1],$ $[0,-11,0,55,0,-77,0,44,0,-11,0,1],[0,13,0,-91,0,182,0,-156,0,65,0,-13,0,1],$ $[1,-7,-21,56,70,-126,-84,120,45,-55,-11,12,1,-1],[-2,0,36,0,-105,0,112,0,-54,0,12,0,-1],$ $[2,0,-25,0,50,0,-35,0,10,0,-1],[-2,0,16,0,-20,0,8,0,-1],[2,0,-9,0,6,0,-1],[-2,0,4,0,-1],$ $[2,0,-1]]$
30	$[[0,1],[0,-7,0,14,0,-7,0,1],[0,-7,0,22,0,-13,0,2],[0,4,0,-13,0,7,0,-1],[0,-4,0,13,0,-7,0,1],$ $[0,7,0,-22,0,13,0,-2],[0,7,0,-14,0,7,0,-1],[0,-1]]$
$\vdots$	

Table 5: Extended set $\widehat{\mathcal{M}}(\mathrm{n})$, first differences $\triangle\,\widehat{\mathcal{M}}(\mathrm{n})$, and floor-pattern $\mathcal{F}(\mathrm{n})$ for composed odd squarefree modulus n.

m	**n(m)**	$\mathbf{2}\,\boldsymbol{\delta}(\mathrm{n})$	$\widehat{\mathcal{M}}(\mathbf{n})$	$\triangle\,\widehat{\mathcal{M}}(\mathbf{n})$	$\mathcal{F}(\mathbf{n})$
1	**15**	8	$[0, 1, 7, 11, 13, 17]$	$[1, 6, 4, 2, 4]$	$[2, 1, 0, 1, 0, 1, 2, 0]$
2	**21**	12	$[0, 1, 5, 11, 13, 17, 19, 23]$	$[1, 4, 6, 2, 4, 2, 4]$	$[1, 2, 0, 1, 0, 1, 0, 1, 0, 2, 1, 0]$
3	**33**	20	$[0, 1, 5, 7, 13, 17, 19, 23, 25, 29, 31, 35]$	$[1, 4, 2, 6, 4, 2, 4, 2, 4, 2, 4]$	$[1, 0, 2, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 2, 0, 1, 0]$
4	**35** $5 \cdot 7$	24	$[0, 1, 3, 9, 11, 13, 17, 19, 23, 27, 29, 31, 33, 37]$	$[1, 2, 6, 2, 2, 4, 2, 4, 4, 2, 2, 2, 4]$	$[0, 2, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 2, 0, 0]$
5	**39** $3 \cdot 13$	24	$[0, 1, 5, 7, 11, 17, 19, 23, 25, 29, 31, 35, 37, 41]$	$[1, 4, 2, 4, 6, 2, 4, 2, 4, 2, 4, 2, 4]$	$[1, 0, 1, 2, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 2, 1, 0, 1, 0]$
6	**51** $3 \cdot 17$	32	$[0, 1, 5, 7, 11, 13, 19, 23, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53]$	$[1, 4, 2, 4, 2, 6, 4, 2, 4, 2, 4, 2, 4, 2, 4, 2, 4]$	$[1, 0, 1, 0, 2, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 2, 0, 1, 0, 1, 0]$
7	**55** $5 \cdot 11$	40	$[0, 1, 3, 7, 9, 13, 17, 19, 21, 23, 27, 29, 29, 31, 37, 39, 41, 43, 47, 49, 51, 53, 57]$	$[1, 2, 4, 2, 4, 4, 2, 2, 2, 4, 2, 2, 6, 2, 2, 2, 4, 2, 2, 2, 4]$	$[0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 2, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 2, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0]$
8	**57** $3 \cdot 19$	36	$[0, 1, 5, 7, 11, 13, 17, 23, 25, 29, 31, 31, 35, 37, 41, 43, 47, 49, 53, 55, 59]$	$[1, 4, 2, 4, 2, 4, 6, 2, 4, 2, 4, 2, 4, 2, 4, 2, 4, 2, 4]$	$[1, 0, 1, 0, 1, 2, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 2, 1, 0, 1, 0, 1, 0]$
9	**65** $5 \cdot 13$	48	$[0, 1, 3, 7, 9, 11, 17, 19, 21, 23, 27, 29, 31, 33, 33, 37, 41, 43, 47, 49, 51, 53, 57, 59, 61, 63, 67]$	$[1, 2, 4, 2, 2, 6, 2, 2, 2, 4, 2, 2, 2, 4, 4, 2, 4, 2, 2, 2, 4, 2, 2, 2, 4]$	$[0, 1, 0, 0, 2, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 2, 0, 0, 1, 0, 0]$
10	**69** $3 \cdot 23$	44	$[0, 1, 5, 7, 11, 13, 17, 19, 25, 29, 31, 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 65, 67, 71]$	$[1, 4, 2, 4, 2, 4, 2, 6, 4, 2, 4, 2, 4, 2, 4, 2, 4, 2, 4, 2, 4, 2, 4]$	$[1, 0, 1, 0, 1, 0, 2, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 2, 0, 1, 0, 1, 0, 1, 0]$
11	**77** $7 \cdot 11$	60	$[0, 1, 3, 5, 9, 13, 15, 17, 19, 23, 25, 27, 29, 31, 37, 39, 41, 43, 45, 47, 51, 53, 57, 59, 61, 65, 67, 69, 71, 73, 75, 79]$	$[1, 2, 2, 4, 4, 2, 2, 2, 4, 2, 2, 2, 2, 6, 2, 2, 2, 2, 2, 4, 2, 4, 2, 2, 4, 2, 2, 2, 2, 2, 4]$	$[0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 2, 0, 0, 0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 0, 0]$

continued

Table 5 ctnd.: Extended set $\widehat{\boldsymbol{\mathcal{M}}}(\mathrm{n})$, first differences $\triangle\,\widehat{\boldsymbol{\mathcal{M}}}(\mathrm{n})$, and floor-pattern $\boldsymbol{\mathcal{F}}(\mathrm{n})$ for composed odd squarefree modulus n.

m	**n(m)**	**2** $\boldsymbol{\delta}$(n)	$\widehat{\boldsymbol{\mathcal{M}}}(\mathbf{n})$	$\triangle\,\widehat{\boldsymbol{\mathcal{M}}}(\mathbf{n})$	$\boldsymbol{\mathcal{F}}(\mathbf{n})$
12	**85** 5 · 17	64	[0, 1, 3, 7, 9, 11, 13, 19, 21, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 49, 53, 57, 59, 61, 63, 67, 69, 71, 73, 77, 79, 81, 83, 87]	[1, 2, 4, 2, 2, 2, 6, 2, 2, 4, 2, 2, 2, 4, 2, 2, 2, 4, 2, 4, 4, 2, 2, 2, 4, 2, 2, 2, 4, 2, 2, 2, 4]	[0, 1, 0, 0, 0, 2, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 2, 0, 0, 0, 1, 0, 0]
13	**87** 3 · 29	56	[0, 1, 5, 7, 11, 13, 17, 19, 23, 25, 31 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 65, 67, 71, 73, 77, 79, 83, 85, 89]	[1, 4, 2, 4, 2, 4, 2, 4, 2, 6, 4, 2, 4, 2, 4, 2, 4, 2, 4, 2, 4, 2, 4, 2, 4, 2, 4, 2, 4]	[1, 0, 1, 0, 1, 0, 1, 0, 2, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 2, 0, 1, 0, 1, 0, 1, 0, 1, 0]
14	**91** 7 · 13	72	[0, 1, 3, 5, 9, 11, 15, 17, 19, 23, 25, 27, 29, 31, 33, 37, 41, 43, 45, 47, 51, 53, 55, 57, 59, 61, 67, 69, 71, 73, 75, 79, 81, 83, 85, 87, 89, 93]	[1, 2, 2, 4, 2, 4, 2, 2, 4, 2, 2, 2, 2, 2, 4, 4, 2, 2, 2, 4, 2, 2, 2, 2, 2, 6, 2, 2, 2, 2, 4, 2, 2, 2, 2, 2, 4]	[0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0, 0, 0, 0, 2, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 1, 0, 0, 0, 0, 0, 0, 1, 0, 0, 1, 0, 1, 0, 0, 0]
15	**93** 3 · 31	60	[0, 1, 5, 7, 11, 13, 17, 19, 23, 25, 29, 35, 37, 41, 43, 47, 49, 53, 55, 59, 61, 65, 67, 71, 73, 77, 79, 83, 85, 89, 91, 95]	[1, 4, 2, 4, 2, 4, 2, 4, 2, 4, 6, 2, 4, 2, 4, 2, 4, 2, 4, 2, 4, 2, 4, 2, 4, 2, 4, 2, 4, 2, 4]	[1, 0, 1, 0, 1, 0, 1, 0, 1, 2, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0, 2, 1, 0, 1, 0, 1, 0, 1, 0, 1, 0]
16	**95** 5 · 19	72	[0, 1, 3, 7, 9, 11, 13, 17, 21, 23, 27, 29, 31, 33, 37, 39, 41, 43, 47, 49, 51, 53, 59, 61, 63, 67, 69, 71, 73, 77, 79, 81, 83, 87, 89, 91, 93, 97]	[1, 2, 4, 2, 2, 2, 4, 4, 2, 4, 2, 2, 2, 4, 2, 2, 2, 4, 2, 2, 2, 6, 2, 2, 4, 2, 2, 2, 4, 2, 2, 2, 4, 2, 2, 2, 4]	[0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 2, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 2, 0, 0, 0, 1, 0, 0, 0, 1, 0, 0, 0, 1, 0, 1, 1, 0, 0, 0, 1, 0, 0]
17	**105** 3 · 5 · 7	48	[0, 1, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, 101, 103, 107]	[1, 10, 2, 4, 2, 4, 6, 2, 6, 4, 2, 4, 6, 6, 2, 6, 4, 2, 6, 4, 6, 8, 4, 2, 4]	[4, 0, 1, 0, 1, 2, 0, 2, 1, 0, 1, 2, 2, 0, 2, 1, 0, 2, 1, 2, 3, 1, 0, 1, 0, 1, 3, 2, 1, 2, 0, 1, 2, 0, 2, 2, 1, 0, 1, 2, 0, 2, 1, 0, 1, 0, 4, 0]
⋮					

Table 6: Cycle structure of $\mathcal{G}al(\mathbb{Q}(\boldsymbol{\rho}(\mathbf{n}))/\mathbb{Q})$ for $\mathbf{n} = \mathbf{1, 2, ..., 40}$.

n	cycles
1	$[[0]] = [[1]]$
2	$[[1]]$
3	$[[1]]$
4	$[[\mathbf{3}, 1]]$
5	$[[\mathbf{3}, 1]]$
6	$[[\mathbf{5}, 1]]$
7	$[[3, 5, 1]]$
8	$[[3, \mathbf{7}, 5, 1]]$
9	$[[5, 7, 1]]$
10	$[[3, \mathbf{9}, 7, 1]]$
11	$[[3, 9, 5, 7, 1]]$
$\boxed{12}$	$[[\mathbf{5}, 1], [\mathbf{7}, 1], [\mathbf{11}, 1]]$
13	$[[7, 3, \mathbf{5}, 9, 11, 1]]$
14	$[[5, 3, \mathbf{13}, 9, 11, 1]]$
15	$[[7, \mathbf{11}, 13, 1]]$
16	$[[3, 9, 5, \mathbf{15}, 13, 7, 11, 1]]$
17	$[[3, 9, 7, \mathbf{13}, 5, 15, 11, 1]]$
18	$[[5, 11, \mathbf{17}, 13, 7, 1]]$
19	$[[3, 9, 11, 5, 15, 7, 17, 13, 1]]$
$\boxed{20}$	$[[3, \mathbf{9}, 13, 1], [7, \mathbf{9}, 17, 1], [\mathbf{11}, 1], [\mathbf{19}, 1]]$
21	$[[11, 5, \mathbf{13}, 17, 19, 1]]$
22	$[[3, 9, 17, 7, \mathbf{21}, 19, 13, 5, 15, 1]]$
23	$[[3, 9, 19, 11, 13, 7, 21, 17, 5, 15, 1]]$
$\boxed{24}$	$[[5, \mathbf{23}, 19, 1], [\mathbf{7}, 1], [11, \mathbf{23}, 13, 1], [\mathbf{17}, 1]]$
25	$[[3, 9, 23, 19, \mathbf{7}, 21, 13, 11, 17, 1]]$
26	$[[7, 3, 21, 9, 11, \mathbf{25}, 19, 23, 5, 17, 15, 1]]$
27	$[[5, 25, 17, 23, 7, 19, 13, 11, 1]]$
$\boxed{28}$	$[[3, 9, \mathbf{27}, 25, 19, 1], [5, 25, \mathbf{13}, 9, 11, 1], [17, 9, \mathbf{15}, 25, 23, 1]]$
29	$[[3, 9, 27, 23, 11, 25, \mathbf{17}, 7, 21, 5, 15, 13, 19, 1]]$
$\boxed{30}$	$[[7, \mathbf{11}, 17, 1], [13, \mathbf{11}, 23, 1], [\mathbf{19}, 1], [\mathbf{29}, 1]]$
31	$[[3, 9, 27, 19, 5, 15, 17, 11, 29, 25, 13, 23, 7, 21, 1]]$
32	$[[3, 9, 27, 17, 13, 25, 11, \mathbf{31}, 29, 23, 5, 15, 19, 7, 21, 1]]$
33	$[[5, 25, 7, 31, \mathbf{23}, 17, 19, 29, 13, 1]]$
34	$[[3, 9, 27, 13, 29, 19, 11, \mathbf{33}, 31, 25, 7, 21, 5, 15, 23, 1]]$
35	$[[3, 9, 27, 11, 33, \mathbf{29}, 17, 19, 13, 31, 23, 1]]$
$\boxed{36}$	$[[5, 25, \mathbf{19}, 23, 29, 1], [7, 23, \mathbf{17}, 25, 31, 1], [11, 23, \mathbf{35}, 25, 13, 1]]$
37	$[[5, 25, 23, 33, 17, 11, 19, 21, \mathbf{31}, 7, 35, 27, 13, 9, 29, 3, 15, 1]]$
38	$[[13, 17, 7, 15, 33, 27, 29, 3, \mathbf{37}, 25, 21, 31, 23, 5, 11, 9, 35, 1]]$
39	$[[7, 29, 31, 17, 37, \mathbf{25}, 19, 23, 5, 35, 11, 1]]$
$\boxed{40}$	$[[3, \mathbf{9}, 27, 1], [7, \mathbf{31}, 23, 1], [11, \mathbf{39}, 29, 1], [13, \mathbf{9}, 37, 1], [17, \mathbf{31}, 33, 1], [19, \mathbf{39}, 21, 1]]$
$\vdots$	

Boxed and colored **n**-numbers indicate non-cyclic Galois groups. See Table 7.
Boldface numbers are nontrivial square roots Modd **n**, denoted by **s** in the text.

Table 7: Non-cyclic Galois groups $\mathcal{G}al(\mathbb{Q}(\boldsymbol{\zeta}(\mathbf{n}))/\mathbb{Q})$, n $\leq$ 100

n	φ(n)	cycle structure	no. of cycles	Galoisgroup
$\boxed{8}$	4	2_3	3	$Z_2 \times Z_2$
12	4	2_3	3	$Z_2 \times Z_2$
$\boxed{15}$	8	$4_2\,2_2$	4	$Z_4 \times Z_2$
16	8	$4_2\,2_2$	4	$Z_4 \times Z_2$
20	8	$4_2\,2_2$	4	$Z_4 \times Z_2$
$\boxed{21}$	12	6_3	3	$Z_3 \times Z_2^2$
$\boxed{24}$	8	2_7	7	Z_2^3
28	12	6_3	3	$Z_3 \times Z_2^2$
30	8	$4_2\,2_2$	4	$Z_4 \times Z_2$
$\boxed{32}$	16	$8_2\,4_1\,2_2$	5	$Z_8 \times Z_2$
$\boxed{33}$	20	10_3	3	$Z_5 \times Z_2^2$
$\boxed{35}$	24	$12_2\,6_2$	4	$Z_4 \times Z_3 \times Z_2$
36	12	6_3	3	$Z_3 \times Z_2^2$
39	24	$12_2\,6_2$	4	$Z_4 \times Z_3 \times Z_2$
$\boxed{40}$	16	$4_4\,2_6$	10	$Z_4 \times Z_2^2$
42	12	6_3	3	$Z_3 \times Z_2^2$
44	20	10_3	3	$Z_5 \times Z_2^2$
45	24	$12_2\,6_2$	4	$Z_4 \times Z_3 \times Z_2$
48	16	$4_4\,2_6$	10	$Z_4 \times Z_2^2$
$\boxed{51}$	32	$16_2\,8_1\,4_1\,2_2$	6	$Z_{16} \times Z_2$
52	24	$12_2\,6_2$	4	$Z_4 \times Z_3 \times Z_2$
$\boxed{55}$	40	$20_2\,10_2$	4	$Z_5 \times Z_4 \times Z_2$
$\boxed{56}$	24	6_7	7	$Z_3 \times Z_2^3$
$\boxed{57}$	36	18_3	3	$Z_9 \times Z_2^2$
60	16	$4_4\,2_6$	10	$Z_4 \times Z_2^2$
$\boxed{63}$	36	6_{12}	12	$Z_3^2 \times Z_2^2$
64	32	$16_2\,8_1\,4_1\,2_2$	6	$Z_{16} \times Z_2$
$\boxed{65}$	48	12_6	6	$Z_4^2 \times Z_3$
66	20	10_3	3	$Z_5 \times Z_2^2$
68	32	$16_2\,8_1\,4_1\,2_2$	6	$Z_{16} \times Z_2$
$\boxed{69}$	44	22_3	3	$Z_{11} \times Z_2^2$
70	24	$12_2\,6_2$	4	$Z_4 \times Z_3 \times Z_2$
72	24	6_7	7	$Z_3 \times Z_2^3$
75	40	$20_2\,10_2$	4	$Z_5 \times Z_4 \times Z_2$
76	36	18_3	3	$Z_9 \times Z_2^2$
$\boxed{77}$	60	30_3	3	$Z_5 \times Z_3 \times Z_2^2$
78	24	$12_2\,6_2$	4	$Z_4 \times Z_3 \times Z_2$
$\boxed{80}$	32	$4_{12}\,2_4$	16	$Z_4^2 \times Z_2^2$

Continued on the next page.

Table 7 continued: Non-cyclic Galois groups $\mathcal{G}al(\mathbb{Q}(\boldsymbol{\zeta}(\mathbf{n}))/\mathbb{Q})$, $\mathbf{n} \leq \mathbf{100}$

n	δ(n)	cycle structure	no. of cycles	Galoisgroup
84	24	6_7	7	$Z_3 \times Z_2^3$
$\boxed{\mathbf{85}}$	64	$16_4\, 8_2\, 4_4$	10	$Z_{16} \times Z_4$
$\boxed{\mathbf{87}}$	56	$28_2\, 14_2$	4	$Z_7 \times Z_4 \times Z_2$
$\boxed{\mathbf{88}}$	40	10_7	7	$Z_5 \times Z_2^3$
90	24	$12_2\, 6_2$	4	$Z_4 \times Z_3 \times Z_2$
$\boxed{\mathbf{91}}$	72	$12_8\, 6_8$	16	$Z_4 \times Z_3^2 \times Z_2$?
$\boxed{\mathbf{92}}$	44	22_3	3	$Z_{11} \times Z_2^2$
93	60	30_3	3	$Z_5 \times Z_3 \times Z_2^2$
$\boxed{\mathbf{95}}$	72	$36_2\, 18_2$	4	$Z_9 \times Z_4 \times Z_2$
$\boxed{\mathbf{96}}$	32	$8_4\, 4_3\, 2_6$	13	$Z_8 \times Z_2^2$
99	60	30_3	3	$Z_5 \times Z_3 \times Z_2^2$
100	40	$20_2\, 10_2$	4	$Z_5 \times Z_4 \times Z_2$
$\vdots$				

The cyclic group of order $\mathbf{m}$ is denoted by $\mathbf{Z_m}$. For all other values $\mathbf{n} \leq \mathbf{100}$ the Galois group is the cyclic group $\mathbf{Z_{\varphi(n)}}$.

Only independent cycles are counted, i.e., cycles which appear as sub-cycles of the given ones have been omitted.

The notation, e.g., $\mathbf{16_2\, 8_1\, 4_1\, 2_2}$, means that there are **2** cycles of order (length) **16**, one cycle of order **8**, one cycle of order **4** and two cycles of order **2**.

Direct products of identical cyclic groups are sometimes written in exponent form, e.g., $\mathbf{Z_2^2}$ stands for $\mathbf{Z_2} \times \mathbf{Z_2}$.

Boxed and colored **n**-numbers indicate where some non-cyclic Galois group appears for the first time. Some of the cycle graphs are shown in Fig. 4.

Table 8: Non-cyclic Galois groups $\mathcal{G}al(\mathbb{Q}(\boldsymbol{\rho}(\mathbf{n}))/\mathbb{Q})$, $\mathbf{n} \leq \mathbf{100}$

n	δ(n)	cycle structure	no. of cycles	Galoisgroup
$\boxed{\mathbf{12}}$	4	2_3	3	$Z_2 \times Z_2$
$\boxed{\mathbf{20}}$	8	$4_2\,2_2$	4	$Z_4 \times Z_2$
24	8	$4_2\,2_2$	4	$Z_4 \times Z_2$
$\boxed{\mathbf{28}}$	12	6_3	3	$Z_3 \times Z_2^2$
30	8	$4_2\,2_2$	4	$Z_4 \times Z_2$
36	12	6_3	3	$Z_3 \times Z_2^2$
$\boxed{\mathbf{40}}$	16	4_6	6	$Z_4 \times Z_4$
42	12	6_3	3	$Z_3 \times Z_2^2$
$\boxed{\mathbf{44}}$	20	10_3	3	$Z_5 \times Z_2^2$
$\boxed{\mathbf{48}}$	16	$8_2\,4_1\,2_2$	5	$Z_8 \times Z_2$
$\boxed{\mathbf{52}}$	24	$12_2\,6_2$	4	$Z_4 \times Z_3 \times Z_2$
56	24	$12_2\,6_2$	4	$Z_4 \times Z_3 \times Z_2$
$\boxed{\mathbf{60}}$	16	$4_4\,2_6$	10	$Z_4 \times Z_2^2$
$\boxed{\mathbf{63}}$	18	6_4	4	$Z_3^2 \times Z_2$
65	24	$12_2\,6_2$	4	$Z_4 \times Z_3 \times Z_2$
66	20	10_3	3	$Z_5 \times Z_2^2$
$\boxed{\mathbf{68}}$	32	$16_2\,8_1\,4_1\,2_2$	6	$Z_{16} \times Z_2$
70	24	$12_2\,6_2$	4	$Z_4 \times Z_3 \times Z_2$
72	24	$12_2\,6_2$	4	$Z_4 \times Z_3 \times Z_2$
$\boxed{\mathbf{76}}$	36	18_3	3	$Z_9 \times Z_2^2$
78	24	$12_2\,6_2$	4	$Z_4 \times Z_3 \times Z_2$
$\boxed{\mathbf{80}}$	32	$8_4\,4_4$	8	$Z_8 \times Z_4$
$\boxed{\mathbf{84}}$	24	6_7	7	$Z_3 \times Z_2^3$
85	32	$16_2\,8_1\,4_1\,2_2$	6	$Z_{16} \times Z_2$
$\boxed{\mathbf{88}}$	40	$20_2\,10_2$	4	$Z_5 \times Z_4 \times Z_2$
90	24	$12_2\,6_2$	4	$Z_4 \times Z_3 \times Z_2$
$\boxed{\mathbf{91}}$	36	12_4	4	$Z_4 \times Z_3^2$
92	44	22_3	3	$Z_{11} \times Z_2^2$
96	32	$16_2\,8_1\,4_1\,2_2$	6	$Z_{16} \times Z_2$
100	40	$20_2\,10_2$	4	$Z_5 \times Z_4 \times Z_2$
⋮				

The cyclic group of order **m** is denoted by $\mathbf{Z_m}$. For all other $\mathbf{n} \leq \mathbf{100}$ cases the Galois group is the cyclic group $\mathbf{Z_{\delta(n)}}$. The **n** values are given in A206552.

Only independent cycles are counted, i.e., cycles which appear as sub-cycles of the given ones have been omitted.

The notation, e.g., $\mathbf{16_2\,8_1\,4_1\,2_2}$, means that there are **2** cycles of order (length) **16**, one cycle of order **8**, one cycle of order **4** and two cycles of order **2**.

Direct products of identical cyclic groups are sometimes written in exponent form, e.g., $\mathbf{Z_2^2}$ stands for $\mathbf{Z_2} \times \mathbf{Z_2}$.

Boxed and colored **n**-numbers indicate where some non-cyclic Galois group appears for the first time. For the cycle graphs see Fig. 4.

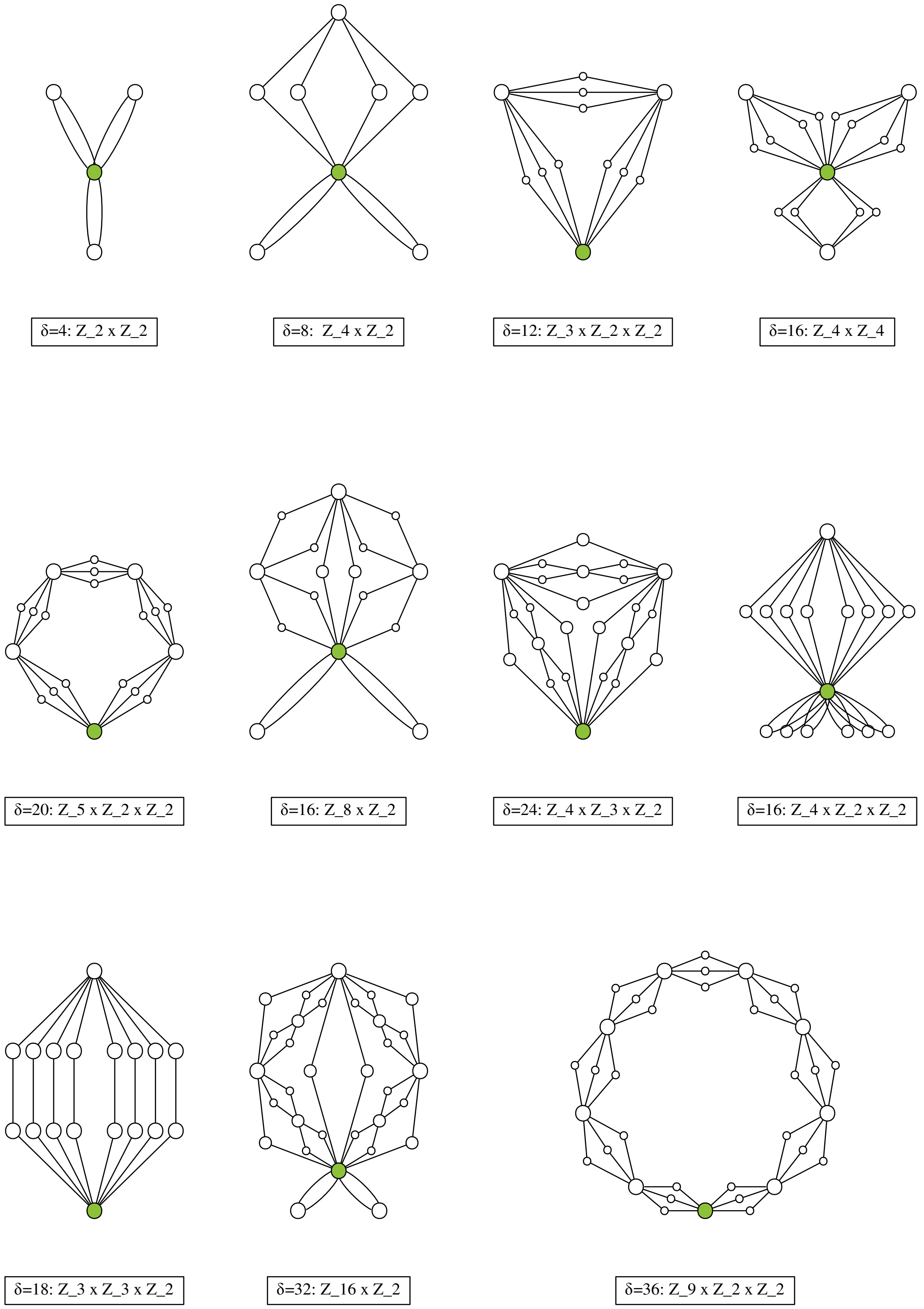
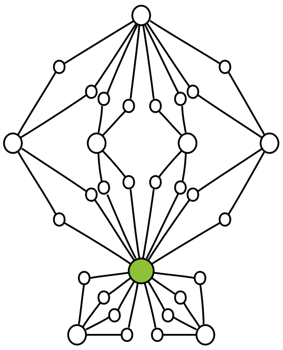
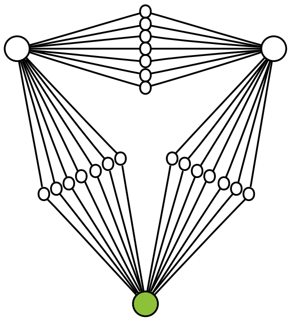


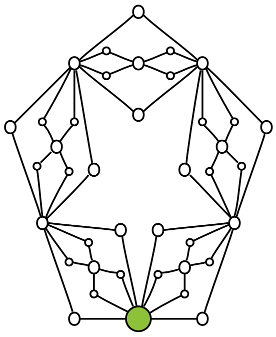
Figure 4: Cycle graphs for non-cyclic Galois groups $\mathcal{G}al(\mathbb{Q}(\boldsymbol{\rho}(\mathbf{n}))/\mathbb{Q})$ appearing for $\mathbf{n} = \mathbf{1..100}$. δ is the degree of $\mathbf{C}(\mathbf{n}, \mathbf{x})$, the maximal polynomial of $\boldsymbol{\rho}(n)$, hence the order of the Galois group. See Table 8. Continued on next page.



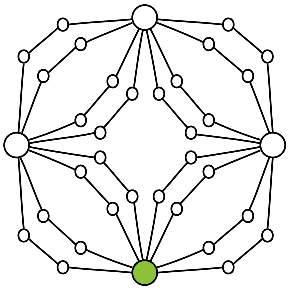
δ=32: Z_8 x Z_4



δ=24: Z_3 x Z_2 x Z_2 x Z_2



δ=40: Z_5 x Z_4 x Z_2



δ=36: Z_4 x Z_3 x Z_3

• • •

Figure 4 continued: Cycle graphs for non-cyclic Galois groups $\mathcal{G}al(\mathbb{Q}(\boldsymbol{\rho}(\mathbf{n}))/\mathbb{Q})$ appearing for $\mathbf{n} = \mathbf{1..100}$. See Table 8.