Karlsruhe
March 03 2017

Table for the multiplicative non-cyclic groups of integers modulo A033949

Wolfdieter Lang [1]

The multiplicative group of integers modulo n is denoted by $(\mathbb{Z}\,/\,\mathbb{Z}_n)^\times$, the group with elements from a restricted residue system modulo n under multiplication modulo n. The smallest positive such system is chosen, and this set of relatively prime numbers is called $RRS(n)$ with its number of elements $\varphi(n)$ = A000010(n). This group is isomorphic to the *Galois* group $\mathcal{G}al(\mathbb{Q}(\zeta(n))/\mathbb{Q})$ with $\zeta(n) = exp(\frac{2\pi i}{n})$ (see, *e.g.*, [1], p. 235, Theorem 9.1.11). This is also called the cyclotomic group belonging to the cyclotomic polynomials, the minimal polynomials of the algebraic number $\zeta(n)$ with extension field $\mathbb{Q}(\zeta(n))$. These groups are abelian.

For n from A033948 this group is the cyclic group C_n, generated by a primitive root modulo n. See A279398 for the smallest prime primitive roots for these n. Here we are interested in the non-cyclic cases, *i.e.*, n is from A033949. These groups are direct products of cyclic groups.

For the *Table* the non-negative powers modulo n of each element of $RRS(n)$ are considered. Negative powers are then included because the inverse of each elements of $RRS(n)$ is again an element of $RRS(n)$. (See A038566 and A124224). The orders of these elements with n from A033949 are proper divisors of $\varphi(n)$ (no primitive root exist) and a set of independent cycles is given in the third column. Independent means that all other cycles generated by elements of $RRS(n)$ are subsets of the recorded ones, and no recorded cycle is a subset of another one. Here we follow the strategy to look first for prime elements from $RRS(n)$ ordered increasingly. See A279399 for these primes, and A279401 for their orders modulo n, *i.e.*, the primitive cycle lengths (in the following we just write cycle length). These orders appear as subscripts. In general it will, however, not be possible to use only primes for finding the independent cycles; also composite numbers with their cycles will be needed. This happens for the first time for $n = 32$ where also the cycle of length 2 (a 2-cycle in short) generated by 15, *i.e.*, [15, 1], is needed. Such composite numbers which be underlined.

The number of independent cycles has been given in [3] in *Table 7* in the fourth column, also given as A282623. In the third column of that table the structure of the independent cycles is given, where, *e.g.*, 4_2 means that two 4-cycles are present. Such independent cycles are important for drawing cycle graphs of the groups appearing in the last column of the present table (see the examples for cycle graphs in [3], Figure 4, where the vertices have to be labeled with the $RRS(n)$ numbers appearing in these cycles. The root has label 1).

In the fourth column of the present table the generators of the *Galois* group $\mathcal{G}al(\mathbb{Q}(\boldsymbol{\zeta}(n))/\mathbb{Q})$ or $(\mathbb{Z}\,/\,\mathbb{Z}_n)^\times$ are given. At least two elements of $RRS(n)$ will be needed in the considered non-cyclic case. For the largest proper factor f of $\varphi(n)$ we check if cycle lengths f and $\varphi(n)\,/\,f$ are present among the orders modulo n of the primes of $RRS(n)$ and test if their nonnegative powers generate all elements of $RRS(n)$. E.g. for $n = 20$ with $\varphi(20) = 8$ one tries $f = 4$ and finds a 4-cycle for 3 and a 2-cycle for 7, and these two elements provide indeed the generators. If, however, no prime element of $RRS(n)$ has the largest proper factor of $\varphi(n)$ as order modulo n then smaller factors are tested. *E.g.*, for $n = 24$ with $\varphi(24) = 8$ there are no 4-cycles for primes, but only 2−cycles. A possible generator set turns out to be 5, 7, 13, corresponding to the factorization $2 \cdot 2 \cdot 2$ of 8.

[1] wolfdieter.lang@partner.kit.edu, http://www.itp.kit.edu/~wl

Note that not only elements of the independent cycles appear as generators. *E.g.*, for $n = 21$ with $\varphi(21) = 12$ the $2-$cycle from 13 is used together with the $6-$cycle from 2. This is because 13 is the only prime element of $RRS(21)$ which generates a 2-cycle, and all the elements of the independent cycles have order $6 \pmod{21}$.

Amazingly, it will not always be possible to find a generator set with primes only. The first instance is $n = 51$ with $\varphi(51) = 32$. The primes have only cycle lengths 16, 8, 6, 4, but never 2, and no combination of an $8-$ with a $4-$cycle, like 2 with 13 or 2 with 47 provides a basis. Therefore one needs also a composite number from $RRS(n)$, e.g. the 2-cycle of 35 (the smallest number) or 50. Indeed, a generator set with smallest numbers is then $\{2, \underline{35}\}$. The only other case for n from A033949 between 8 and 130 is $n = 69$ with $\varphi(69) = 44$. Here the primes with cycle length 22 and 2, *e.g.*, 2 and 47 will not generate the group. There is no prime with cycle length 4. Then the smallest composite number with a 2-cycle is 22 but 2 and 22 do not generate the group, but 2 and 68 will do it. We call these n values whose generating set necessarily contains composite elements *exceptional cases*. Such composite elements will be underlined and colored in the table.

With this procedure to find a generating set, where always the smallest elements of $RRS(n)$ which do the job are chosen, scanning the orders modulo n for decreasing factors of $\varphi(n)$, the fourth column of the present table will result. The generators are also given in the irregular triangle A282624.

This table is not always in accordance with the one given in Wikipedia [6]. There the product of the orders of the elements of the generating set sometimes overshoots $\varphi(n)$, which is never the case in the present table. *E.g.*, Wikipedia has for $n = 72$ with $\varphi(72) = 24$ the generators 5_6, 7_6, 11_6 but $6^3 > 24$. We have 5_6, 17_2, 19_2 which is minimal in this sense. (The case $n = 70$ where this overshooting also appears is in fact wrong, because 3_{12}, 11_3 provides in fact no basis. This Wikipedia entry will have to be corrected.)

In the Wikipedia table there are also composite generators used when they are not necessary. *E.g.*, for $n = 15$ with $\varphi(15) = 8$ the generators are 2_4, 14_2 but in our table they are 2_4, 11_2. As mentioned above only $n = 51$ and 69 (in the table up to $n = 130$) do need composite generators.

The groups given in the present table in the last column are totally factorized. This means that the orders of the cyclic factors are always powers of primes (power 1 included). In the Wikipedia table factors like C_6, C_{10}, C_{12}, C_{18}, ... appear, but they can be factored further, whenever the factors of the order are relatively prime. So, $C_6 = C_3 \times C_2$, $C_{10} = C_5 \times C_2$, etc. For some more examples see the list of abelian groups in [5]. Therefore the number of factors of cyclic groups in the direct product for the group $(\mathbb{Z}\,/\,\mathbb{Z}_n)^{\times}$ depends on the definition of the factors. *E.g.*, A046072 uses as definition of the factors $C_{i_1} \times C_{i_2} \cdots \times C_{i_m}$ that i_j divides i_k for $i_j < i_k$. This means that, *e.g.*, for $n = 35$ with $\varphi(35) = 24$ the factorization is there, like in the Wikepedia table, $C_2 \times C_{12}$ with A046072(35) $= 2$, In the total factorization this is $C_4 \times C_3 \times C_2$ with 3 factors. (Note that the direct product is always associative, and in the abelian group case it is also commutative).

For the non-cyclic case the table of the orders of the cyclic factors in the total factorization are given also in A281854. The number of these factors is given in A281855, and the number of factors in this factorization for all groups, including the cyclic ones, is given in A282625.

One of the reasons for listing the generators for the non-cyclic multiplicative groups of integers modulo A033949 was to give a recipe to compute the *Dirichlet* character tables $\chi(n; r, m)$, $r = 1, 2, ..., \varphi(n)$, $m = 1, 2, ..., n$. *Davenport* [2] gives a prescription first for powers of primes (also for powers ≥ 3 of 2 which have no primitive root) and then employs the usual multiplicativity (not the strong one) of characters for general $n \geq 2$ (the case $n = 1$ is trivial).

Here we distinguish between the cyclic and non-cyclic case. The cyclic case is trivial due to the existence of a primitive root modulo n. For the non-cyclic case one considers first the columns m values given by the generators. If the order modulo n (with n from A033949) of a generator g is $L(g)$ (the cycle length generated by g) then one takes all the roots $\zeta(L(g); j) = exp(2\,\pi\,i\,j/L(g))$, $j = 0, 1, ..., (L(g)-1)$

as first entries of column $m = g$. Together with the roots belonging to the order of the other generators one can then fill the character table for all values m given by the generators. One has to obtain all direct products of these roots in the $\varphi(n)$ rows. For the other columns with m from the set $RRS(n)$ one determines the exponents of the generators which give $m \pmod{n}$, and uses strong multiplicity of the characters. All other columns are filled with zeros. This works also if some generators should be composite (for the exceptional n values, like 51 and 69).

E.g., $n = 20$ with $\varphi(20) = 8$. The generators with their orders modulo n as subscripts are 3_4 and 11_2. Column $m = 3$ is filled with the roots $\zeta(4;\, r-1), r = 1, 2, ..., 4$ (*i.e.*, $1, i, -1, -i$) and because the other generator has order 2 one needs the same roots again: $\zeta(4;\, r-5)$, for rows $r = 5, ..., 8$. The column $m = 11$ is filled with the roots $+1$ and -1; in the first four rows 1 and in the remaining four rows -1. Then the other values of the table follow as described above. *E.g.*, for column $m = 19$ one finds the values from $19 \equiv 3^2\, 11^1 \pmod{20}$ by strong multiplicity $\chi(3^2\, 11^1) = \chi(3)^2\, \chi(11)$ for each row r. Compare this with *Table 19* given by *R. J. Mathar* in a link to A093954 or [4] on p. 7: there rows $r = 2$ and 4 have to be exchanged, as well as rows $r = 5$ and 7, in order to obtain the proposed character table.

References

[1] David A. Cox, *Galois Theory*, John Wiley & Sons, Inc., Hoboken, New Jersey, 2004, p. 235, Theorem 9.1.11.

[2] Harold Davenport, Multiplicative Number Theory, Second ed., Springer, 1980, pp. 27-30.

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

[4] Richard J. Mathar, Table of Dirichlet L-Series and Prime Zeta Modulo Functions for Small Moduli, arXiv:1008.2547 [math.NT], https://arxiv.org/abs/1008.2547.

[5] Wikipedia, List of small groups, https://en.wikipedia.org/wiki/List_of_small_groups.

[6] Wikipedia, Multiplicative group of integers modulo n,

https://en.wikipedia.org/wiki/Multiplicative_group_of_integers_modulo_n.

OEIS A-numbers: A000010, A033948, A033949, A038566, A046072, A124224, A279398, A279399, A279401, A281854, A281855, A282623, A282624, A282625.

Table: Non-cyclic Galois groups $\mathcal{G}al(\mathbb{Q}(\boldsymbol{\zeta}(\mathbf{n}))/\mathbb{Q})$, $\mathbf{n} \leq \mathbf{130}$

n	φ**(n)**	**independent cycles**	**generators**	**group**
$\boxed{\mathbf{8}}$	4	$3_2,\ 5_2,\ 7_2$	$< 3_2,\ 5_2 >$	$C_2 \times C_2$
12	4	$5_2,\ 7_2,\ 11_2$	$< 5_2,\ 7_2 >$	$C_2 \times C_2$
$\boxed{\mathbf{15}}$	8	$2_4,\ 7_4,\ 11_2,\ \underline{14}_2$	$< 2_4,\ 11_2 >$	$C_4 \times C_2$
16	8	$3_4,\ 5_4,\ 7_2,\ \underline{15}_2$	$< 3_4,\ 7_2 >$	$C_4 \times C_2$
20	8	$3_4,\ 11_2,\ 13_4,\ 19_2$	$< 3_4,\ 11_2 >$	$C_4 \times C_2$
$\boxed{\mathbf{21}}$	12	$2_6,\ 5_6,\ 19_6$	$< 2_6,\ 13_2 >$	$C_3 \times C_2^2$
$\boxed{\mathbf{24}}$	8	$5_2,\ 7_2,\ 11_2,\ 13_2,\ 17_2,\ 19,\ 23_2$	$< 5_2,\ 7_2,\ 13_2 >$	C_2^3
28	12	$3_6,\ 5_6,\ 11_6$	$< 3_6,\ 13_2 >$	$C_3 \times C_2^2$
30	8	$7_4,\ 11_2,\ 17_4,\ 29_2$	$< 7_4,\ 11_2 >$	$C_4 \times C_2$
$\boxed{\mathbf{32}}$	16	$3_8,\ 5_8,\ 7_4,\ 31_2,\ \underline{15}_2$	$< 3_8,\ 31_2 >$	$C_8 \times C_2$
$\boxed{\mathbf{33}}$	20	$2_{10},\ 5_{10},\ 7_{10},$	$< 2_{10},\ 23_2 >$	$C_5 \times C_2^2$
$\boxed{\mathbf{35}}$	24	$2_{12},\ 3_{12},\ 19_6,\ 31_6$	$< 19_6,\ 13_4 >$	$C_4 \times C_3 \times C_2$
36	12	$5_6,\ 7_6,\ 11_6$	$< 5_6,\ 19_2 >$	$C_3 \times C_2^2$
39	24	$2_{12},\ 7_{12},\ 17_6,\ 19_6$	$< 17_6,\ 5_4 >$	$C_4 \times C_3 \times C_2$
$\boxed{\mathbf{40}}$	16	$3_4,\ 7_4,\ 11_2,\ 13_4,\ 17_4,\ 19_2,\ 29_2,\ 31_2,\ \underline{21}_2,\ \underline{39}_2$	$< 3_4,\ 11_2,\ 29_2 >$	$C_4 \times C_2^2$
42	12	$5_6,\ 11_6,\ 19_6$	$< 5_6,\ 13_2 >$	$C_3 \times C_2^2$
44	20	$3_{10},\ 7_{10},\ 13_{10},$	$< 3_{10},\ 43_2 >$	$C_5 \times C_2^2$
45	24	$2_{12},\ 7_{12},\ 11_6,\ 29_6,\ 6_2$	$< 11_6,\ 17_4 >$	$C_4 \times C_3 \times C_2$
48	16	$5_4,\ 7_2,\ 11_4,\ 13_4,\ 17_2,\ 19_4,\ 23_2,\ 31_2,\ 41_2,\ 47_2$	$< 5_4,\ 7_2,\ 17_2 >$	$C_4 \times C_2^2$
$\boxed{\mathbf{51}}$	32	$2_8,\ 5_{16},\ 7_{16},\ 47_4,\ \underline{35}_2,\ \underline{50}_2$	$< 5_{16}, \underline{35}_2 >$	$C_{16} \times C_2$
52	24	$3_6,\ 7_{12},\ 23_6,\ 37_{12}$	$< 3_6,\ 5_4 >$	$C_4 \times C_3 \times C_2$
$\boxed{\mathbf{55}}$	40	$2_{20},\ 3_{20},\ 19_{10},\ 41_{10}$	$< 19_{10},\ 23_4 >$	$C_5 \times C_4 \times C_2$
$\boxed{\mathbf{56}}$	24	$3_6,\ 5_6,\ 11_6,\ 17_6,\ 23_6,\ 31_6,\ 37_6$	$< 3_6,\ 13_2,\ 29_2 >$	$C_3 \times C_2^3$
$\boxed{\mathbf{57}}$	36	$2_{18},\ 5_{18},\ 13_{18}$	$< 2_{18},\ 37_2 >$	$C_9 \times C_2^2$
60	16	$7_4,\ 11_2,\ 13_4,\ 17_4,\ 19_2,\ 23_4,\ 29_2,\ 31_2,\ 41_2,\ 59_2$	$< 7_4,\ 11_2,\ 19_2 >$	$C_4 \times C_2^2$
$\boxed{\mathbf{63}}$	36	$2_6,\ 5_6,\ 11_6,\ 13_6,\ 17_6,\ 19_6,\ 29_6,\ 31_6,\ 41_6,\ 47_6,\ 53_6,\ \underline{40}_6$	$< 2_6,\ 5_5 >$	$C_3^2 \times C_2^2$
64	32	$3_{16},\ 5_{16},\ 7_8,\ 31_2,\ 47_4,\ \underline{63}_2$	$< 3_{16},\ 31_2 >$	$C_{16} \times C_2$
$\boxed{\mathbf{65}}$	48	$2_{12},\ 3_{12},\ 7_{12},\ 11_{12},\ 17_{12},\ 19_{12}$	$< 2_{12},\ 31_4 >$	$C_4^2 \times C_3$
66	20	$5_{10},\ 7_{10},\ 17_{10}$	$< 5_{10},\ 43_2 >$	$C_5 \times C_2^2$
68	32	$3_{16},\ 5_{16},\ 19_8,\ 47_4,\ 67_2,\ \underline{35}_2$	$< 3_{16},\ 67_2 >$	$C_{16} \times C_2$
$\boxed{\mathbf{69}}$	44	$2_{22},\ 5_{22},\ 7_{22}$	$< 2_{22}, \underline{68}_2>$	$C_{11} \times C_2^2$
70	24	$3_{12},\ 19_6,\ 23_{12},\ 31_6$	$< 19_6,\ 14_4 >$	$C_4 \times C_3 \times C_2$
72	24	$5_6,\ 7_6,\ 11_6,\ 13_6,\ 23_6,\ 41_6,\ 43_6$	$< 5_6,\ 17_2,\ 19_2 >$	$C_3 \times C_2^3$
75	40	$2_{20},\ 11_{10},\ 13_{20},\ 29_{10}$	$< 11_{10},\ 7_4 >$	$C_5 \times C_4 \times C_2$
76	36	$3_{18},\ 13_{18},\ 23_{18}$	$< 3_{18},\ 37_2 >$	$C_9 \times C_2^2$
$\boxed{\mathbf{77}}$	60	$2_{30},\ 3_{30},\ 17_{30}$	$< 3_{30},\ 43_2 >$	$C_5 \times C_3 \times C_2^2$
78	24	$7_{12},\ 11_{12},\ 17_6,\ 29_6$	$< 7_{12},\ 53_2 >$	$C_4 \times C_3 \times C_2$
$\boxed{\mathbf{80}}$	32	$3_4,\ 7_4,\ 11_4,\ 13_4,\ 17_4,\ 19_4,\ 29_4,\ 31_2,$ $43_4,\ 47_4,\ 53_4,\ 61_4,\ 71_2,\ 73_4,\ 79_2,\ \underline{39}_2$	$< 3_4,\ 7_4,\ 31_2 >$	$C_4^2 \times C_2$

Continued on the next page.

Table continued: Non-cyclic Galois groups $\mathcal{G}al(\mathbb{Q}(\boldsymbol{\zeta}(\mathbf{n}))/\mathbb{Q})$, n $\leq$ 130

n	φ(n)	independent cycles	generators	group
84	24	$5_6, 11_6\ , 19_6, 47_6, 53_6, 61_6, 67_6$	$< 5_6, 13_2, 71_2 >$	$C_3 \times C_2^3$
$\boxed{85}$	64	$3_{16}, 11_{16}, 13_4, 23_{16}, 29_{16}, 43_8, 47_4, 53_8, 67_4, \underline{18}_4$	$< 3_{16}, 13_4 >$	$C_{16} \times C_4$
$\boxed{87}$	56	$2_{28}, 5_{14}, 19_{28}, 23_{14}$	$< 2_{28}, 59_2 >$	$C_7 \times C_4 \times C_2$
$\boxed{88}$	40	$3_{10}, 5_{10}, 7_{10}, 13_{10}, 17_{10}, 19_{10}, 29_{10}, 31_{10}, 73_{10}, 83_{10}$	$< 3_{10}, 23_2, 43_2 >$	$C_5 \times C_2^3$
90	24	$7_{12}, 11_6, 23_{12}, 29_6$	$< 7_{12}, 71_2 >$	$C_4 \times C_3 \times C_2$
$\boxed{91}$	72	$2_{12}\, 3_6, 5_{12}, 11_{12}, 17_6, 19_{12}, 41_{12}, 59_{12}, 71_{12},$ $\underline{10}_6, \underline{12}_6, \underline{18}_{12}, \underline{40}_6, \underline{48}_6, \underline{62}_6, \underline{68}_6$	$< 2_{12}, 3_6 >$	$C_4 \times C_3^2 \times C_2$
$\boxed{92}$	44	$3_{22}, 5_{22}, 7_{22}$	$< 5_{22}, 47_2 >$	$C_{11} \times C_2^2$
93	60	$11_{30}, 13_{30}, 41_{30}$	$< 11_{30}, 61_2 >$	$C_5 \times C_3 \times C_2^2$
$\boxed{95}$	72	$2_{36}, 17_{36}, 29_{18}, 41_{18}$	$< 29_{18}, 37_4 >$	$C_9 \times C_4 \times C_2$
$\boxed{96}$	32	$5_8, 7_4, 11_8, 13_8, 17_2, 19_8, 23_4, 31_2, 41_4,$ $47_2, 79_2, \underline{65}_2, \underline{95}_2$	$< 5_8, 17_2, 31_2 >$	$C_8 \times C_2^2$
99	60	$2_{30}, 5_{30}, 7_{30}$	$< 2_{30}, 89_2 >$	$C_5 \times C_3 \times C_2^2$
100	40	$3_{20}, 11_{10}, 13_{20}, 19_{10}$	$< 11_{10}, 43_4 >$	$C_5 \times C_4 \times C_2$
102	32	$5_{16}, 7_{16}, 47_4, 53_8, 101_2, 35_2$	$< 5_{16}, 101_2 >$	$C_{16} \times C_2$
$\boxed{104}$	48	$3_6, 7_{12}, 11_{12}, 23_6, 29_6, 37_{12}, 41_{12}, 43_6, 101_6, \underline{55}_6$	$< 7_{12}, 53_2, 79_2 >$	$C_4 \times C_3 \times C_2^2$
105	48	$2_{12}, 11_6, 17_{12}, 19_6, 31_6, 37_{12}, 59_6, 73_{12}, 101_6, \underline{44}_6$	$< 2_{12}, 29_2, 41_2 >$	$C_4 \times C_3 \times C_2^2$
108	36	$5_{18}, 7_{18}, 11_{18}$	$< 5_{18}, 107_2 >$	$C_9 \times C_2^2$
110	40	$3_{20}, 7_{20}, 19_{10}, 41_{10}$	$< 3_{20}, 109_2 >$	$C_5 \times C_4 \times C_2$
111	72	$2_{36}\, 13_{36}, 41_{18}, 53_{18}$	$< 41_{18}, 43_4 >$	$C_9 \times C_4 \times C_2$
112	48	$3_{12}, 5_{12}, 11_{12}, 17_6, 23_6, 31_6, 37_{12}, 73_6, 79_6, 103_6$	$< 3_{12}, 41_2, 71_2 >$	$C_4 \times C_3 \times C_2^2$
114	36	$5_{18}, 13_{18}, 29_{18}$	$< 5_{18}, 37_2 >$	$C_9 \times C_2^2$
$\boxed{115}$	88	$2_{44}, 7_{44}, 11_{22}, 19_{22}$	$< 11_{22}, 47_4 >$	$C_{11} \times C_4 \times C_2$
116	56	$3_{28}, 37_{28}, 7_{14}, 67_{14}$	$< 3_{28}, 59_2 >$	$C_7 \times C_4 \times C_2$
117	72	$2_{12}, 5_{12}, 7_{12}, 19_{12}, 31_{12}, 41_{12}, 71_{12}, \underline{58}_{12},$ $17_6, 23_6, 29_6, 101_6, 107, \underline{14}_6, \underline{38}_6, \underline{68}_6$	$< 2_{12}, 17_6 >$	$C_4 \times C_3^2 \times C_2$
$\boxed{119}$	96	$3_{48}, 11_{48}, 19_{24}, 47_{12}, 101_6, 103_6$	$< 29_{16}, 101_6 >$	$C_{16} \times C_3 \times C_2$
$\boxed{120}$	32	$7_4, 11_2, 13_4, 17_4, 19_2, 23_4, 29_2, 31_2, 41_2,$ $43_4, 53_4, 59_2, 61_2, 71_2, 73_4, 79_2, 83_4, 89_2,$ $101_2, 109_2, \underline{91}_2, \underline{119}_2$	$< 7_4, 11_2, 19_2, 29_2 >$	$C_4 \times C_2^3$
$\boxed{123}$	80	$2_{20}, 7_{40}, 11_{40}, 23_{10}, 59_{10}$	$< 7_{40}, 83_2 >$	$C_8 \times C_5 \times C_2$
124	60	$3_{30}, 7_{30}, 13_{30}$	$< 3_{30}, 61_2 >$	$C_5 \times C_3 \times C_2^2$
126	36	$5_6, 11_6, 13_6, 17_6, 19_6, 29_6, 31_6,$ $41_6, 47_6, 53_6, 103_6, \underline{65}_6$	$< 5_6, 13_6 >$	$C_3^2 \times C_2^2$
$\boxed{128}$	64	$3_{32}, 5_{32}, 7_{16}, 31_4, 47_8, 127_2, \underline{63}_2$	$< 3_{32}, 127_2 >$	$C_{32} \times C_2$
$\boxed{129}$	84	$5_{42}, 17_{42}, 19_{42}$	$< 7_6, 11_{14} >$	$C_7 \times C_3 \times C_2^2$
130	48	$3_{12}, 7_{12}, 11_{12}, 17_{12}, 19_{12}, 67_{12}$	$< 3_{12}, 31_4 >$	$C_4^2 \times C_3$
$\vdots$				

The cyclic group of order m is denoted by $\mathbf{C_m}$. For all other values n $\leq$ 130 the Galois group is the cyclic group $\mathbf{C_{\varphi(n)}}$ which sometimes may be factorized further.

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

The notation, e.g., $\mathbf{7_{12}}$, $\mathbf{11_6}$, $\mathbf{23_{12}}$, $\mathbf{29_6}$, indicates that there are two 12-cycles starting with numbers 7 and 23, and two 6-cycles starting with numbers 11 and 29, ending always in 1.

Direct products of identical cyclic groups are sometimes written in exponent form, e.g., $\mathbf{C_2^2}$ stands for $\mathbf{C_2} \times \mathbf{C_2}$.

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 of [3].

Composite generators (for the exceptional cases n) are underlined and colored.