Some Identities for Enumerators of Circulant Graphs

Valery Liskovets*

October 29, 2018

Abstract

We establish analytically several new identities connecting enumerators of different types of circulant graphs of prime, twice prime and prime-squared orders. In particular, it is shown that the semi-sum of the number of undirected circulants and the number of undirected self-complementary circulants of prime order is equal to the number of directed self-complementary circulants of the same order.

Keywords: circulant graph; cycle index; cyclic group; nearly doubled primes; Cunningham chain; self-complementary graph; tournament; mixed graph

Mathematics Subject Classifications (2000): 05C30, 05A19, 11A41

1 Introduction

Identities considered in this paper connect different enumerators of circulant graphs mainly of prime, twice prime and prime-squared orders. The idea of this paper goes back to the article [KLP96], where we counted uniformly circulants of five kinds and derived several identities. Here we consider six types of circulants: directed, undirected and oriented circulants (specified by valency or not), and self-complementary circulants of the same types. Most of the obtained identities may be called analytical (or formal) in the sense that they rest exclusively on the enumerative formulae and follow from special properties of the cycle indices of regular cyclic groups. As a rule, it is more difficult to discover such an identity than to prove it analytically. Almost all identities were first revealed and conjectured due to numerical observations and computational experiments.

From the combinatorial point of view, most of the identities look rather strange. They are very simple but no structural or algebraic properties of circulants are used to derive them (with few exceptions), nor establish we bijective proofs. The latter is challenging although in some cases it is doubtful that there exist natural bijections between participating circulants. Of course there may

---

*Institute of Mathematics, National Academy of Sciences, 220072, Minsk, Belarus, liskov@im.bas-net.by
exist other combinatorial or algebraic explanations or interpretations of the identities.

Several identities hold only for a special type of prime orders \( p \), namely, those for which \( \frac{p+1}{2} \) is also prime. Such primes are familiar in number theory. Probably this is the first combinatorial context where they play a substantial role.

We comprise here numerous identities that have been obtained previously and deduce about ten new ones. We deliberately represent new identities in different equivalent forms and formulate simple corollaries keeping in mind possible future generalizations and combinatorial proofs. Some derived identities look more elegant than the original ones.

The present paper is partially based upon the work [KILP0X] that contains most detailed formulae for circulants, vast tables and several identities. Here we reproduce all necessary results from it, and our exposition is basically self-contained.

1.1. Main definitions. Let \( n \) be a positive integer, \( Z_n := \{0, 1, 2, \ldots, n-1\} \). We denote by \( Z_n^* \) the set of numbers in \( Z_n \) relatively prime to \( n \) (that is invertible elements modulo \( n \)). So, \( |Z_n^*| = \phi(n) \), where \( \phi(n) \) is the Euler totient function. \( Z(n) \) denotes a regular cyclic permutation group of order and degree \( n \), i.e. the group generated by an \( n \)-cycle.

The cycle index of \( Z(n) \) is the polynomial

\[
I_n(x) = \frac{1}{n} \sum_{r|n} \phi(r)x^{n/r},
\]

where \( x \) stands for the sequence of variables \( x_1, x_2, x_3, \ldots \).

The term “graphs” means both undirected and directed graphs. We consider only simple graphs, that is graphs without loops and multiple edges or arcs. The order of a graph means the number of its vertices. We refer to Harary [Har69] for notions concerning graphs.

An (undirected) edge is identified with the pair of the corresponding oppositely directed arcs. Accordingly, an undirected graph is considered as a (symmetric) digraph. On the contrary, a digraph is oriented if it has no pair of oppositely directed arcs.

A circulant graph of order \( n \), or simply a circulant, means a graph \( \Gamma \) on the vertex set \( Z_n \) which is invariant with respect to the cyclic permutation \( (0, 1, 2, \ldots, n-1) \), i.e. if \((u,v)\) is an edge of \( \Gamma \) then such is \((u+1, v+1)\). In other terms, this is a Cayley graph with respect to the cyclic group \( Z_n \). Every circulant is a regular graph of some valency \( r \).

Graphs are considered here up to isomorphism. We deal with the enumerators of (non-isomorphic) circulants of several types. For convenience, the type is written as the subscript. Henceforth:

- \( C_d(n) \) denotes the number of directed circulant graphs;
- \( C_u(n) \) denotes the number of undirected circulant graphs;
- \( C_o(n) \) denotes the number of oriented circulant graphs;
There are several technical formulae connecting the cycle indices

- $C_{sd}(n)$ and $C_{su}(n)$ denote the numbers of self-complementary directed and undirected circulant graphs respectively;
- $C_t(n)$ denotes the number of circulant tournaments;
- $C_d(n, r)$, $C_u(n, r)$ and $C_o(n, r)$ denote the corresponding numbers of circulants of order $n$ and valency $r$ while $c_d(n, z)$, $c_u(n, z)$ and $c_o(n, r)$ are their generating functions by valency (polynomials in $z$):

\[
c_d(n, z) := \sum_{r \geq 0} C_d(n, r) z^r, \quad c_u(n, z) := \sum_{r \geq 0} C_u(n, r) z^r, \quad c_o(n, r) := \sum_{r \geq 0} C_o(n, r) z^r.
\]

Clearly $C_d(n) = c_d(n, z)|_{z = 1} = c_d(n, 1)$, $C_u(n) = c_u(n, 1)$ and $C_o(n) = c_o(n, 1)$.

In more detail these quantities and the corresponding circulants are considered in [KLP96, KLP03]. In particular, the following simple uniform enumerative formulae have been obtained there:

1.2. Theorem (counting circulants of prime and twice prime order). For any odd prime $p$,

\[
\begin{align*}
C_d(p, z) &= J_{p-1}(x)|_{\{x_r := 1 + z^r\} \text{ for } r = 1, 2, \ldots } \\
c_u(p, z) &= J_{p-1}(x)|_{\{x_r := 1 + 2z^r\} \text{ for } r = 1, 2, \ldots } \\
c_o(p, z) &= J_{p-1}(x)|_{\{x_r := 2, \text{ if } r \text{ even}, \{x_r := 0, \text{ if } r \text{ odd} \} \text{ for } r = 1, 2, \ldots } \\
C_{sd}(p) &= J_{p-1}(x)|_{\{x_r := 2, \text{ if } r \text{ even}, \{x_r := 0, \text{ if } r \text{ odd} \} \text{ for } r = 1, 2, \ldots } \\
C_{su}(p) &= J_{p-1}(x)|_{\{x_r := 2, \text{ if } r \text{ even}, \{x_r := 0, \text{ if } r \text{ odd} \} \text{ for } r = 1, 2, \ldots } \\
C_t(p) &= J_{p-1}(x)|_{\{x_r := 0, \text{ if } r \text{ even}, \{x_r := 2, \text{ if } r \text{ odd} \} \text{ for } r = 1, 2, \ldots } \\
c_d(2p, z) &= J_{p-1}(x)|_{\{x_r := 1 + z^r\} \text{ for } r = 1, 2, \ldots \cdot (1 + z)} \\
c_u(2p, z) &= J_{p-1}(x)|_{\{x_r := 1 + 2z^r\} \text{ for } r = 1, 2, \ldots \cdot (1 + z)} \\
c_o(2p, z) &= J_{p-1}(x)|_{\{x_r := 2, \text{ if } r \text{ even}, \{x_r := 0, \text{ if } r \text{ odd} \} \text{ for } r = 1, 2, \ldots }.
\end{align*}
\]

2 Cycle indices of cyclic groups

There are several technical formulae connecting the cycle indices $J_{p-1}$ and $J_{p-1}$. They are interesting per se and will be used in the proofs of subsequent identities.

For any natural $m$, we set

\[
m := 2^k m'
\]

where $m'$ is odd.

In the polynomial $J_{2m}$ we first distinguish the terms corresponding to the divisors $r$ with the highest possible power of 2, i.e. $k + 1$:

\[
J_{2m}(x) = \frac{1}{2m} \sum_{r | 2m} \phi(r) x_r^{2m/r} = \frac{1}{2m} \left( \sum_{r | m} \phi(r) x_r^{2m/r} + \sum_{r | m'} \phi(2^{k+1}r) x_r^{2k+1/r} \right).
\]

After easy transformations taking into account that $\phi(2^{k+1}r) = 2^k \phi(r)$ for odd $r$ and $k \geq 0$ we obtain
2.1. Lemma.

\[ 2J_{2m}(x) = J_m(x^2) + J_{m'}(x_{(k+1)}) \]  \hspace{1cm} (2.1)

where \( x^2 = x_1^2, x_2^2, x_3^2, \ldots \) and \( x_{(k+1)} := x_{2k+1}, x_{2k+1}, x_{3,2k+1} \ldots \)

Now in \( J_m(x) \) we partition the set of divisors with respect to powers of 2:

\[ J_m(x) = \frac{1}{m} \left( \sum_{r|m'} \phi(r)x_r^{2m'/r} + \sum_{i=1}^{k} \sum_{r|m'} 2^{i-1} \phi(r)x_r^{2k-i}m'/r \right) \]

and the same for \( J_{2m}(x) \). Comparing similar terms in both formulae, we easily arrive at the following:

\[ J_m(x) = J_{2m}(0, x_1, 0, x_2, 0, x_3, 0, \ldots) + \frac{1}{2m} \sum_{r|m'} \phi(r)x_r^{m/r}. \]  \hspace{1cm} (2.2)

The second summand on the right-hand side of formula (2.2) can be represented in different useful forms. First of all, this is evidently \( \frac{1}{2m} \sum_{r|m' \text{ odd}} \phi(r)x_r^{m/r} \).

And this is also \( \frac{1}{2}J_m(x_1, 0, x_3, 0, x_5, 0, \ldots) \). Hence

\[ J_m(x) = J_{2m}(0, x_1, 0, x_2, 0, x_3, 0, \ldots) + \frac{1}{2}J_m(x_1, 0, x_3, 0, x_5, 0, \ldots). \]  \hspace{1cm} (2.3)

Every term in \( J_m \) contains only one variable. Therefore

\[ J_m(x_1, 0, x_3, 0, x_5, 0, \ldots) = J_m(x) - J_m(0, x_2, 0, x_4, 0, x_6, 0, \ldots). \]

Hence by (2.3) we have

2.2. Lemma.

\[ 2J_{2m}(0, x_1, 0, x_2, 0, x_3, 0, \ldots) = J_m(x) + J_m(0, x_2, 0, x_4, 0, x_6, 0, \ldots), \]  \hspace{1cm} (2.4)

that is,

\[ 2J_{2m}(y) \mid \{y_r:0\}_{r \text{ odd}}, \{y_r:=x_r/2\}_{r \text{ even}} = J_m(x) + J_m(y) \mid \{y_r:0\}_{r \text{ odd}}, \{y_r:=x_r\}_{r \text{ even}}. \]

Now \( J_m(x_1, 0, x_3, 0, x_5, 0, \ldots) = 2J_{2m}(\sqrt{x_1}, 0, \sqrt{x_3}, 0, \sqrt{x_5}, 0, \ldots) \). Therefore by (2.3),

\[ J_m(x) = J_{2m}(0, x_1, 0, x_2, 0, x_3, 0, \ldots) + J_{2m}(\sqrt{x_1}, 0, \sqrt{x_3}, 0, \sqrt{x_5}, 0, \ldots). \]  \hspace{1cm} (2.5)

Since the non-zero variables in both right-hand side summands alternate, one may join them into a single cycle index. This gives rise to the following expression:

2.3. Lemma.

\[ J_m(x) = J_{2m}(\sqrt{x_1}, x_1, \sqrt{x_3}, x_2, \sqrt{x_5}, x_3, \ldots). \]  \hspace{1cm} (2.6)

In other words, \( J_m(x) = J_{2m}(y) \mid \{y_r:=x_r\}_{r \text{ odd}}, \{y_r:=x_r/2\}_{r \text{ even}}. \)
Finally we need one further formula. Substituting (2.5) into (2.4) we obtain

\[
I_m(0, x_1, 0, x_2, 0, x_3, \ldots) = I_m(\sqrt{x_1}, 0, \sqrt{x_3}, 0, \sqrt{x_5}, \ldots) + I_m(0, x_2, 0, x_4, 0, x_6, \ldots).
\]

(2.7)

3 Known identities

3.1. Let \( p \) be a prime such that \( q = \frac{p+1}{2} \) is also prime. Then by Klin – Liskovets – Pöschel [KILP96],

\[
c_u(p, z) = c_d(\frac{p+1}{2}, z^2),
\]

that is,

\[
C_u(p, 2r) = C_d(\frac{p+1}{2}, r), \quad r \geq 0,
\]

and

\[
C_{su}(p) = C_{sd}(\frac{p+1}{2}).
\]

(3.1)

These equalities follow directly from Theorem 1.2 and are in fact the first formal (i.e. analytically proved) identities for enumerators of circulants.

We note that

\[
p - 1 = 2(q - 1)
\]

what explains a specific role of such primes in our considerations.

It follows from (3.1) that

\[
C_u(p) = C_d(\frac{p+1}{2}).
\]

(3.1')

3.2. If \( p > 3 \) is a prime such that \( q = \frac{p+1}{2} \) is also prime, then

\[
2c_o(p, z) = c_o(p + 1, z) + 1.
\]

(3.3)

PROOF [KILP08]. Identity (3.3) follows directly from Theorem 1.2 (the third and ninth formulae) and the equality

\[
2J_{2m}(x) = J_m(x^2) + 1
\]

for an arbitrary \( m \) where \( J_m(x) := J_m(x)_{|x_r = 1, \text{ even}} \). This equality is a particular case of expression (2.1) since \( J_m(1, 1, 1, \ldots) = 1 \). Here we put \( 2m := p - 1 \) (hence \( m = q - 1 \)). Q. E. D.

Putting \( z := 1 \) we obtain

\[
2C_o(p) = C_o(p + 1) + 1.
\]

(3.3')

3.3. According to [KILP96],

\[
C_{su}(n) = 0
\]

(3.4)

and

\[
C_{sd}(n) = C_1(n)
\]

(3.5)
if $n = p$ or $p^2$ and $p \equiv 3 \pmod{4}$.

Next, combining (3.5) with (3.2) we obtain

$$C_{su}(p) = C_{t}(\frac{p+1}{2})$$

(3.6)

if both $p$ and $\frac{p+1}{2}$ are prime and $p \equiv 5 \pmod{8}$.

The least $p$ that meets the first two conditions and does not meet the third is 73.

3.4. For any prime $p$,

$$C_{sd}(p) = C_{t}(p) + C_{su}(p)$$

(3.7)

Since tournaments and undirected self-complementary circulants are particular cases of directed self-complementary circulants (hence in general $C_{sd}(n) \geq C_{t}(n) + C_{su}(n)$), equality (3.7) has a simple sense: any directed self-complementary circulant graph of prime order is either anti-symmetric (a tournament) or symmetric (an undirected graph). This beautiful claim has been first established by Chia – Lim [ChL86] by means of simple algebraic arguments. But in view of Theorem 1.2 (the fourth, fifth and sixth formulae), identity (3.7) is a direct consequence of formula (2.7): merely substitute 2 for all variables $x_1, x_2, x_3, \ldots$

3.5. According to Fronček – Rosa – Širáň [FRS99] (see also [AlMV99]), undirected self-complementary circulants of order $n$ exist if and only if all prime divisors $p$ of $n$ are congruent to 1 modulo 4. Hence (3.4) holds if there is a prime $p | n, p \equiv 3 \pmod{4}$.

3.6. For composite orders, directed self-complementary circulants that are neither tournaments nor undirected graphs do exist but are comparatively rare. We call them mixed. The least suitable order is 15: $C_{sd,min}(15) := C_{sd}(15) - C_{su}(15) - C_{t}(15) = 20 - 0 - 16 = 4$ (see Table 3 in the Appendix). The four circulants are constructed in [KILP0x]. We will return to mixed circulants in Sections 5 and 7.2.

3.7. The last known identity concerns undirected circulants of even order and odd valency:

$$C_u(2n, 2r + 1) = C_u(2n, 2r)$$

(3.8)

for any $n$ and $r$. This identity is known to hold for square-free $n$. Moreover it has been verified for all orders less 54 and is conjectured to be valid for all even orders (McKay [McK95]; see also [KILP0x], where a stronger conjecture concerning isomorphisms of circulants has been proposed).
4 New identities for circulants of prime order

4.1. Proposition. For prime \( p \),
\[ 2C_{sd}(p) = C_u(p) + C_{su}(p). \]  (4.1)
In particular,
\[ C_u(p) = 2C_{sd}(p) = 2C_t(p) \quad \text{if} \quad p \equiv 3 \mod 4. \]  (4.1')

Proof. Substitute 2 for all variables in formula (2.4) with \( p - 1 = 2m \). By Theorem 1.2 (the fourth, second and fifth formulae), we immediately obtain (4.1).

Clearly the second summand in (2.4) vanishes if \( m \) is odd (see (3.4)). Q.E.D.

In Section 6.2 we will obtain a generalization of (4.1') to \( p \equiv 1 \mod 4 \).

4.2. Remarks. 1. Despite that all participating quantities (and the corresponding numerical values for small \( p \)) have been known long ago, this striking identity has evidently escaped attention of the previous researchers including the present author.

2. In view of equation (3.7), identity (4.1) can be represented equivalently in the following form:
\[ C_u(p) = C_{sd}(p) + C_t(p) = C_{su}(p) + 2C_t(p). \]  (4.1'')

3. Is it possible to give a bijective proof of identity (4.1) or at least (4.1')? This question looks especially intriguing in view of the fact that circulant graphs are naturally partitioned by valency contrary to self-complementary circulants. Hence such a bijection would introduce a certain artificial graduation (“pseudo-valency”) into the class of self-complementary circulants of prime order. In particular, some self-complementary graphs would correspond to the empty and complete graphs. To this end we could put formally \( x_r := 1 + z^r, \ r = 1, 2, \ldots, \) in (2.4) instead of \( x_r := 2 \). But is there a natural combinatorial interpretation of the coefficients of the left hand-side polynomial thus obtained?

4. I do not know whether identity (4.1) can be generalized to non-prime orders.

4.3. We return to identity (3.3). There are subtler analogs of it for undirected and directed circulants. By straightforward observations of numerical data and subsequent numerical verifications with the help of the formulae for prime and twice prime orders (Theorem 1.2, the second, eighth, first and seventh formulae) we arrived at the following somewhat unusual formulae:

\[ 4C_u(p) = C_u(p+1) + 2C_{u}(2\tilde{p}+1), \]  (4.2)
\[ 2c_u(p, z) = \frac{c_u(p+1, z)}{1+z} + \bar{c}_u(2\tilde{p} + 1, z^{2^k}), \]  (4.3)
\[ 4C_d(p) = C_d(p+1) + 2C_{d}(2\tilde{p}+1) \]  (4.4)

and
\[ 2c_d(p, z) = \frac{c_d(p+1, z)}{1+z} + \bar{c}_u(2\tilde{p} + 1, z^{2^k}) \]  (4.5)
whenever \( p \) and \( q = (p + 1)/2 \) are both odd primes. Here \( \tilde{p} \) denotes the maximal odd divisor of \( p - 1 \) and \( p - 1 := 2^{k+1} \tilde{p} \). Now \( \bar{c}_u(2\tilde{p} + 1, z) := c_u(2\tilde{p} + 1, z) \) if \( 2\tilde{p} + 1 \) is prime, otherwise \( \bar{c}_u \) is calculated by the same formula (the second formula in Theorem 1.2) despite that this time it does not represent the number of non-isomorphic undirected circulants of order \( 2\tilde{p} + 1 \).

**Proof.** It is clear that formulae (4.2) and (4.4) follow directly from (4.3) and (4.5) respectively. The latter formulae are immediate consequences of equation (2.1) with \( q - 1 = 2m \) and the corresponding formulae of Theorem 1.2 for the orders \( p \) and \( p + 1 = 2^2m+1 \). Q. E. D.

For instance, by data in Table 2 one can verify that \( 2c_d(37, z) = 4c_d(38, z)/(1 + z) + c_u(19, z^2) \). Hence for the valency \( r = 4 \) we have numerically \( 2(1641 + 199) = 3679 + 1, \) etc.

In particular, by (4.3),
\[
2C_u(p, 4r + 2) = C_u(p + 1, 4r + 2) \tag{4.3'}
\]
since other terms correspond to undirected circulants of odd orders and odd valency and, thus, vanish.

From (4.2) and (4.4) we obtain the following identity not depending on \( \tilde{p} \):
\[
4C_d(p) - C_d(p + 1) = 4C_u(p) - C_u(p + 1), \quad \frac{p + 1}{2} \text{ prime.} \tag{4.6}
\]

For example, for \( p = 13, 4 \cdot 352 - 1400 = 4 \cdot 14 - 48 = 8 \) (= \( 2C_u(7) \)). For \( p = 73 \) we obtain rather spectacularly \( 4 \cdot 65588423374144427520 - 2623569349657709960 = 4 \cdot 1908881900 - 7635527480 = 120 \) (= \( 2C_u(19) \)).

Identity (4.6) can also be written as
\[
4(C_d(p) - C_u(p)) = C_d(p + 1) - C_u(p + 1)
\]
or
\[
4C_{d\setminus u}(p) = C_{d\setminus u}(p + 1), \quad \frac{p + 1}{2} \text{ prime,} \tag{4.6'}
\]
where \( C_{d\setminus u}(n) \) denotes the number of directed circulant graphs that are not undirected graphs.

Similarly from (4.3) and (4.5) we obtain
\[
2(1 + z)c_{d\setminus u}(p, z) = c_{d\setminus u}(p + 1, z), \quad \frac{p + 1}{2} \text{ prime,} \tag{4.7}
\]
or, equivalently,
\[
2(C_{d\setminus u}(p, r) + C_{d\setminus u}(p, r - 1)) = C_{d\setminus u}(p + 1, r). \tag{4.7'}
\]

Thus, for example, for \( p = 13 \) and \( r = 5 \) we have \( C_{d\setminus u}(13, 5) = 66 - 0 = 66, \ C_{d\setminus u}(13, 4) = 43 - 3 = 40, \ 66 + 40 = 106 \) and \( C_{d\setminus u}(14, 5) = 217 - 5 = 2 \cdot 106. \)

4.4. Remark. Can identities (4.2) – (4.7) (as well as (4.1) – (4.3)) be treated bijectively? What then is a sense of the sum or the corresponding difference? This is particularly curious for (4.2) and (4.4) in the case of small \( \tilde{p} \). The

---

1. In the designations of Section 2, \( \tilde{p} = m' \) where \( p - 1 = 2(q - 1) := 4m. \)

2. Moreover, \( 120 = 4 \cdot 14602 - 58288 = 4C_u(37) - C_u(38). \)
existence of such a treatment seems doubtful at least for composite \(2p + 1\). In this respect, identities (4.6') and (4.7') appear to be more promising.

4.5. Number theoretic digression. Some number theoretic aspects of identities (4.2) – (4.7) together with (3.1) – (3.3) are worth considering.

There are 21 such pairs of primes \(p = 2q - 1\) less 1000. The first six are 3, 5, 13, 37, 61 and 73 with their corresponding \(q = 2, 3, 7, 19, 31\) and 37. These are the sequences M2492 and M0849 in Sloane’s Encyclopedia [SIP93] (resp., A005383 and A005382 in its extended on-line version [SloEIS]). In number theory these numbers are called nearly doubled primes, and the pairs \(q, p\) are also known as Cunningham chains of the second kind of length 2 (see, e.g., [Loh89, For99]).

By definition, such primes \(q\) resemble the familiar Sophie Germain primes, that is, the primes \(q\) such that \(p = 2q + 1\) is also prime. The latter primes play a different role in our formulae: the polynomial \(I_p - 1 = I_2 q\) contains the minimal possible (for \(p > 3\)) number of terms, four.

It is commonly believed that the set of nearly doubled primes is infinite. Moreover, there is a conjecture that the number of such primes \(p < N\) grows asymptotically as \(C N^{2 \log N - 1}\) where \(C = 1.320\) (for \(N = 10^m\), this function is very close to \(10^{m+4} m^2\)). Recall that the number of all primes \(p < N\) grows approximately as \(N \log N - 1\).

At present a lot of efforts in computational number theory are devoted to the search for Cunningham chains of huge numbers, especially long chains (see, e.g., [For99]). In particular, the familiar program proth.exe by Y. Gallot allows to effectively verify the primality of numbers \(\tilde{p} \cdot 2^k + 1\) with a fixed \(\tilde{p}\). Keeping in mind (4.2) – (4.5) we are especially interested in nearly doubled primes with small \(\tilde{p}\). In general it is easy to see that such a pair \(q, p\) can exist only if \(3|\tilde{p}\).

Here are the current numerical results for \(\tilde{p} \leq 27\).

Pairs of primes \(q, p\) of the form \(3 \cdot 2^k + 1\) occur twice for \(k \leq 303000\): only with \(k = 1, 2\) and \(k = 5, 6\) \((\tilde{p} = 193)\); see the sequence M1318 in [SIP93] (or A002253 [SloEIS]).

Pairs of primes \(q, p\) of the form \(9 \cdot 2^k + 1\) occur four times for \(k \leq 145000\): with \(k = 1, 2, k = 2, 3, k = 6, 7\) and \(k = 42, 43\); see M0751 (A002256).

Pairs of primes \(q, p\) of the form \(15 \cdot 2^k + 1\) occur three times for \(k \leq 184000\): with \(k = 1, 2, k = 9, 10\) and \(k = 37, 38\); see M1165 (A002258).

Pairs of primes \(q, p\) of the form \(21 \cdot 2^k + 1\) occurs three times for \(k \leq 164000\): with \(k = 4, 5, k = 16, 17\) and \(k = 128, 129\) (see A032360 [SloEIS]).

Pairs of primes \(q, p\) of the form \(27 \cdot 2^k + 1\) occurs twice for \(k \leq 117000\): with \(k = 19, 20\) and \(k = 46, 47\) (see A032363 [SloEIS]). This gives rise to the least possible composite value of \(2\tilde{p} + 1, 55\). So, for the first time it arises for \(p = 2q - 1 = 27 \cdot 2^{20} + 1 = 28311553\).

Clearly \(2\tilde{p} + 1 = q\) if 8 does not divide \(p - 1\). For \(p < 2000\), \(2\tilde{p} + 1\) turns out to be composite only in three cases. \(q = 229, p = 457\) is the least one; here \(\tilde{p} = 57\) and \(2\tilde{p} + 1 = 115\).

By numerical data we also found out that no Cunningham chain exists for \(\tilde{p} = 51\) at least for \(k < 140000\). And the same for the numbers \(\tilde{p} = 87\) and \(\tilde{p} = 93\).
5 Circulants of prime-squared order

5.1. Theorem [KLP96, KLP0x].

\[
c_d(p^2, z) = \mathcal{E}(p^2; x, y)|\{x_r = 1+z^{r}, \quad y_r = 1+z^{pr}\}_{r=1,2,\ldots}
\]

\[
c_u(p^2, z) = \mathcal{E}^*(p^2; x, y)|\{x_r = 1+z^{2r}, \quad y_r = 1+z^{2pr}\}_{r=1,2,\ldots}
\]

\[
c_0(p^2, z) = \mathcal{E}(p^2; x, y)|\{x_r = 1, \quad y_r = 1\}_{r \text{ even}}, \quad \{x_r = 1+2z^r, \quad y_r = 1+2z^{pr}\}_{r \text{ odd}}
\]

\[
C_{sd}(p^2) = \mathcal{E}(p^2; x, y)|\{x_r = 2, \quad y_r = 2\}_{r \text{ even}}, \quad \{x_r = 0, \quad y_r = 0\}_{r \text{ odd}}
\]

\[
C_{su}(p^2) = \mathcal{E}^*(p^2; x, y)|\{x_r = 2, \quad y_r = 2\}_{r \text{ even}}, \quad \{x_r = 0, \quad y_r = 0\}_{r \text{ odd}}
\]

\[
C_i(p^2) = \mathcal{E}(p^2; x, y)|\{x_r = 0, \quad y_r = 0\}_{r \text{ even}}, \quad \{x_r = 2, \quad y_r = 2\}_{r \text{ odd}}
\]

where

\[
\mathcal{E}(p^2; x, y) := \frac{1}{p}J_{p-1}(x^{p+1}) - \frac{1}{p}J_{p-1}(xy) + \frac{1}{p}J_{p-1}(x)J_{p-1}(y)
\]

and

\[
\mathcal{E}^*(p^2; x, y) := \frac{1}{p}J_{\frac{p-1}{2}}(x^{p+1}) - \frac{1}{p}J_{\frac{p-1}{2}}(xy) + \frac{1}{p}J_{\frac{p-1}{2}}(x)J_{\frac{p-1}{2}}(y)
\]

with \(x^{p+1} = x_1^{p+1}, x_2^{p+1}, x_3^{p+1}, \ldots\) and \(xy := x_1y_1, x_2y_2, x_3y_3, \ldots\)

5.2. Mixed self-complementary circulant graphs. By definition (see Section 3.6),

\[
C_{sd}^{\text{mixed}}(p^2) := C_{sd}(p^2) - C_{su}(p^2) - C_i(p^2).
\]

According to [LisP00, KLP0x], the number of non-CI (non-Cayley isomorphic) circulants of order \(p^2\) is

\[
D_i(p^2) = C_i(p^2),
\]

where \(i \in \{sd, su, t\}\). We recall that a circulant is said to be non-CI if there exists a circulant isomorphic but not Cayley isomorphic to it. A Cayley isomorphism means an isomorphism that is induced by an automorphism of the underlying group \(\mathbb{Z}_n\).

5.3. Proposition.

\[
C_{sd}^{\text{mixed}}(p^2) = 2C_{su}(p)C_i(p)
\]

and

\[
C_{sd}^{\text{mixed}}(p^2) = D_{sd}(p^2) - D_{su}(p^2) - D_i(p^2),
\]

They are taken from the corresponding tables maintained in the WWW by W. Keller and N. S. A. Melo, see [http://www.prothsearch.net/riesel.html] (cf. also [3m179]).
that is, the mixed self-complementary circulants of order $p^2$ are exactly the non-CI mixed self-complementary circulants.

**Proof.** We make use of an algebraic property of self-complementary circulants of prime-power order. According to a result announced by Li [Li98] (Theorem 3.3), if $\Gamma$ is a self-complementary circulant of order $p^2$ then one of the following holds.

- $\Gamma$ can be obtained by means of the well-known (alternating cycle) construction discovered by Sachs and Ringel.
- $\Gamma = \Gamma_1[\Gamma_2]$ where $\Gamma_1$ and $\Gamma_1$ are self-complementary circulants of order $p$. Here $\Gamma_1[\Gamma_2]$ is the composition (called also the wreath or lexicographic product) defined as follows: in $\Gamma_1$ we replace each vertex by a copy of $\Gamma_2$; each edge of $\Gamma_1$ gives rise to the edges connecting all pairs of vertices from the two corresponding copies of $\Gamma_2$.

The first construction generates only undirected circulants or tournaments (cf. [LisP00]); moreover, all of them are CI. Now, there is no mixed self-complementary circulant of order $p$ (this is identity (3.7)). Therefore the second construction gives rise to a mixed graph if and only if one of the factors is an undirected self-complementary circulant and the other factor is a tournament. This proves (5.3). Further, all self-complementary circulants $\Gamma = \Gamma_1[\Gamma_2]$ are non-CI [LisP00]. This, together with (5.2), proves (5.4) (moreover, this proves (5.2) since the composition of two undirected circulants is undirected and the composition of two tournaments is a tournament). Q.E.D.

It would be interesting to find an analytical derivation of these equations with the help of Theorem 5.1.

By (5.1) we have

**5.4. Corollary.**

$$C_{sd}(p^2) - C_{su}(p^2) - C_t(p^2) = C_{sd}(p)^2 - C_{su}(p)^2 - C_t(p)^2. \quad (5.5)$$

**5.5. Example.** $p = 13$. By Theorem 5.1,

- $C_{sd}(13^2) = 123992391755402970674764$,
- $C_{su}(13^2) = 56385212104$ and
- $C_t(13^2) = 123992391755346585462636$. It follows that $C_{sd}(13^2) = 24$. Now $C_{sd}(13^2) = 8^2 = 64$, $C_{su}(13^2) = 2^2 = 4$, $C_t(13^2) = 6^2 = 36$ and $64 - 4 - 36 = 24 = 2 \cdot 2 \cdot 6$.

By (3.7) (or, instead, by (3.1) and (3.3)), identity (5.5) can be represented as follows:

$$C_{sd}(p^2) = C_{su}(p^2) + C_t(p^2) + 2C_{su}(p)C_t(p). \quad (5.6)$$

We note also that if $p \equiv 3 \pmod 4$, then $C_{su}(p)$ and $C_{su}(p^2)$ vanish by (3.4), and identity (5.6) turns into (3.5) for $n = p^2$. 

11
6 Alternating sums

Alternating sums serve as one further source of formal identities. First consider
directed circulants of prime order. Take the generating function \( c_d(p, t) \) and
put \( t := -1 \). By Theorem 1.2 we see that the result is equal to \( C_{sd}(p) \). By
Theorem 5.1, the same result is valid for the orders \( n = p^2 \). Moreover, by
formulae given in [KLP03] this is valid for arbitrary odd square-free orders.
Therefore we have

\[ c_d(n, -1) = C_{sd}(n). \] (6.1)

The corresponding result holds for undirected circulants with respect to the
substitution \( t^2 := -1 \), or \( t := \sqrt{-1} \):

\[ c_u(n, t)|_{t^2 := -1} = C_{su}(n). \] (6.2)

Both formulae have been proved for square-free and prime-squared \( n \) and it is
natural to suggest that they are valid in general:

6.1. Conjecture. Identities (6.1) and (6.2) hold for any odd order \( n \).

Trivially (by complementarity), identity (6.1) holds also for even \( n \), and (6.2)
holds for \( n \equiv 3 \pmod{4} \). Identity (6.2) is also valid for \( n = 45 \) as numerical
data [McK95] show.

The behaviour of oriented circulant graphs is different. Numerical observa-
tions show that

\[ c_o(n, -1) = 0 \] (6.3a)

if \( n \) has at least one prime divisor \( p \equiv 3 \pmod{4} \), otherwise

\[ c_o(n, -1) = 1. \] (6.3b)

These identities hold for prime \( n = p \) by Theorem 1.2, for odd square-free \( n \)
by [KLP03] and for \( n = p^2 \) by Theorem 5.1. Again we conjecture they to be
valid for all odd \( n \).

For even square-free \( n \) we found that identity (6.3b) holds if \( n = 2n', \ n' \)
odd, and (6.3a) holds if \( n = 4n', \ n' \) square-free. The behaviour of \( c_o(n, -1) \) for
\( n = 8n', \ n' > 1 \), remains unknown.

Identities (6.1) and (6.2) for prime \( n = p \) transform (4.1) into the following
equality:

\[ 2c_d(p, -1) = c_u(p, 1) + c_u(p, \sqrt{-1}). \] (6.4)

6.2. Even- and odd-valent circulants. Due to (6.1) and (6.2) we can find
simple expressions for the numbers of circulants of (non-specified) even (and,
resp., odd) valency; for undirected circulants we consider only odd orders and
mean even and odd semi-valencies, that is, valencies congruent, respectively, to
0 and 2 modulo 4. We use the superscript \( e \) and \( o \) to denote these numbers. Now,
formula (6.1) is nothing than \( C_e(n) = C_o(n) = C_{sd}(n) \). Since \( C_e(n) + C_o(n) =
C_{d}(n) \), we obtain

\[ C_e(n) = \frac{C_{d}(n) + C_{sd}(n)}{2} \] (6.5e)
and
\[ C^o_d(n) = \frac{C_d(n) - C_{sd}(n)}{2}. \]  
(6.5o)

So, these expressions hold for square-free, prime-squared and even \( n \) and are assumed to hold for all orders.

Similarly, (6.2) gives rise to
\[ C^e_v(n) = \frac{C_u(n) + C_{su}(n)}{2}, \]
and
\[ C^o_u(n) = \frac{C_u(n) - C_{su}(n)}{2}. \]  
(6.6o)

for undirected circulants of odd orders and even and, resp., odd semi-valency. Equations (6.6e) and (6.6o) remain unproven unless \( n \) is square-free or prime-squared or congruent to 3 modulo 4.

Clearly the respective expressions can be extracted from (6.3a) and (6.3b) for oriented circulants.

Comparing formula (6.6e) for prime \( n = p \) with (4.1) we obtain the following curious identity:
\[ C^e_v(p) = C_{sd}(p). \]  
(6.7)

This equation directly generalizes identity (4.1') to \( p \equiv 1 \pmod{4} \) because
\[ C^e_v(p) = C_u(p)/2 \]  
for \( p \equiv 3 \pmod{4} \).

7 Conclusion

We conclude that the enumerative theory of circulants is full of hidden interdependencies, part of which are presented in this paper. Table 3 in the Appendix contains a summary of previous and new identities.

We expect that there should exist further generalizations of the obtained identities for other classes of circulant graphs, first of all, for multigraphs and graphs with coloured or marked edges.

7.1. In general, analytical identities are characteristic for the enumerators of self-complementary graphs of diverse classes and can be found in numerous publications. These results are collected in the surveys by Robinson [Rob81] and Farrugia [Far99] (mainly in Ch. 7). In the latter paper, several open questions are also posed. In particular, the problem K in Sect. 7.64 is just the problem of finding a natural bijection for identity (3.2).

7.2. Open question. Is identity (3.5) valid for the orders all whose prime divisors are congruent to 3 modulo 4? In other words (since (3.4) holds according to Section 3.3), are there mixed self-complementary circulants of such orders? As conjectured in [KLP0x], mixed self-complementary circulants of order \( n \) exist if and only if \( n \) is odd composite and has a prime divisor \( p \equiv 1 \pmod{4} \). If so, then identity (3.7) holds exactly for the other orders. This claim is valid for square-free orders, and it can also be proved for the prime-power orders \( n = p^k \).
7.3. Identities (6.1), (6.2), (6.5) and (6.6) are rather typical; cf., e.g., my paper [Lis00], where other examples of even- and odd-specified quantities and the corresponding semi-sum expressions for them are given.

7.4. Finally, instead of equalities, we touch one important type of inequalities which are usually proved analytically. I suppose that the sequence of the numbers $C_u(p, 2r), 1 < r < (p - 1)/2$, is *logarithmically concave*, that is

$$C_u(n, 2r)^2 \geq C_u(n, 2r - 2)C_u(n, 2r + 2)$$

for any prime order $n = p$ and $1 < r < (n - 1)/2$. In other words, the sequence of ratios $C_u(p, 2r)/C_u(p, 2r + 2)$ is increasing except for the first and the last member. For composite orders this does not necessarily hold. In particular, the opposite inequality holds for $r = 2$ when $n = 27, 121$ and 169. However I do not know counterexamples for square-free orders.

References

[AlMV99] B. Alspach, J. Morris and V. Vilfred, Self-complementary circulant graphs, *Ars Combinatoria*, 53 (1999), 187–191.

[Bai79] R. Baillie, New primes of the form $k \cdot 2^n + 1$, *Math. Comput.*, 33 (1979), No 148, 1333–1336.

[ChL86] G. L. Chia and C. K. Lim, A class of self-complementary vertex-transitive digraphs, *J. Graph Th.*, 10 (1986), No 2, 241–249.

[Far99] A. Farrugia, *Self-Complementary Graphs and Generalisations: a Comprehensive Reference Manual*, Master’s Thesis, Univ. of Malta (1999), 257 p. (available at http://www.math.uwaterloo.ca/~afarrugia/sc-graph.html).

[For99] T. Forbes, Prime clusters and Cunningham chains, *Math. Comput.*, 68 (1999), No 228, 1739–1747.

[FrRŠ96] D. Fronček, A. Rosa and J. Širáň, The existence of selfcomplementary circulant graphs, *Europ. J. Combin.*, 17 (1996), No 7, 625–628.

[Har69] F. Harary, *Graph Theory*, Addison-Wesley, Reading, MA (1969).

[KILP96] M. Klin, V. Liskovets and R. Pöschel, Analytical enumeration of circulant graphs with prime-squared number of vertices, *Sém. Lotharing*. *Combin.*, 36 (1996), B36d, 36 p. (available at http://cartan.u-strasbg.fr80/~slc/).

[KILP0x] M. Klin, V. Liskovets and R. Pöschel, On the analytical enumeration of circulant graphs (submitted).

[Li98] C. H. Li, On finite graphs that are self-complementary and vertex-transitive, *Australas. J. Combin.*, 18 (1998), 147–155.

[Lis00] V. A. Liskovets, Some easily derivable integer sequences, *J. Integer Seq.*, 3 (2000), Article 00.2.2, 15 p. (available at http://www.research.att.com/~njas/sequences/JIS).
[LisP00] V. Liskovets and R. Pöschel, Non-Cayley-isomorphic self-complementary circulant graphs, *J. Graph Th.*, 34 (2000), No 2, 128–141.

[Loëh89] G. Löh, Long chains of nearly doubled primes, *Math. Comput.*, 53 (1989), No 188, 751–759.

[McK95] B. D. McKay, Personal communication (1995).

[Rob81] R. W. Robinson, Counting graphs with a duality property, *Combinatorics*, Proc. 8th Brit. Comb. Conf., Swansea 1981, *Lond. Math. Soc. Lect. Notes Ser.*, 52 (1981), 156–186.

[SloEIS] N. J. A. Sloane, *The On-Line Encyclopedia of Integer Sequences*, published electronically (the state on 3.2001) at [http://www.research.att.com/~njas/sequences/](http://www.research.att.com/~njas/sequences/)

[SIP95] N. J. A. Sloane and S. Plouffe, *The Encyclopedia of Integer Sequences*, Academic Press, San Diego (1995).
Appendix: numerical results and summary

Tables 1 and 2 contain relevant numerical data obtained by Theorems 1.2 and 5.1 (they partially reproduce data from KLP0x).

Table 1: Non-isomorphic circulant graphs

| n  | $C_d(n)$ | $C_u(n)$ | $C_o(n)$ | $C_{sd}(n)$ | $C_{su}(n)$ | $C_t(n)$ |
|----|----------|----------|----------|-------------|-------------|----------|
| 2  | 2        | 2        | 1        | 0           | 0           | 0        |
| 3  | 3        | 2        | 2        | 1           | 0           | 1        |
| 4  | 6        | 4        | 2        | 0           | 0           | 0        |
| 5  | 6        | 3        | 3        | 2           | 1           | 1        |
| 6  | 20       | 8        | 5        | 0           | 0           | 0        |
| 7  | 14       | 4        | 6        | 2           | 0           | 2        |
| 8  | 46       | 12       | 7        | 0           | 0           | 0        |
| 9  | 51       | 8        | 16       | 3           | 0           | 3        |
| 10 | 140      | 20       | 21       | 0           | 0           | 0        |
| 11 | 108      | 8        | 26       | 4           | 0           | 4        |
| 12 | 624      | 48       | 64       | 0           | 0           | 0        |
| 13 | 352      | 14       | 63       | 8           | 2           | 6        |
| 14 | 1400     | 48       | 125      | 0           | 0           | 0        |
| 15 | 2172     | 44       | 276      | 20          | 0           | 16       |
| 16 | 4116     | 36       | 411      | 20          | 4           | 16       |
| 17 | 22040    | 192      | 1105     | 0           | 0           | 0        |
| 18 | 14602    | 60       | 1098     | 30          | 0           | 30       |
| 19 | 68016    | 336      | 2472     | 0           | 0           | 0        |
| 20 | 88376    | 200      | 4938     | 88          | 0           | 88       |
| 21 | 209936   | 416      | 5909     | 0           | 0           | 0        |
| 22 | 190746   | 188      | 8054     | 94          | 0           | 94       |
| 23 | 839094   | 423      | 26577    | 214         | 7           | 205      |
| 24 | 2797000  | 1400     | 44301    | 0           | 0           | 0        |
| 25 | 11276704 | 3104     | 132964   | 0           | 0           | 0        |
| 26 | 9587580  | 1182     | 170823   | 596         | 10          | 586      |
| 27 | 67195520 | 8768     | 597885   | 0           | 0           | 0        |
| 28 | 35792568 | 2192     | 478318   | 1096        | 0           | 1096     |
| 29 | 214863120| 6768     | 2152366  | 3280        | 0           | 3280     |
| 30 | 536879180| 16460    | 2690421  | 0           | 0           | 0        |
| 31 | 715901096| 11144    | 5381028  | 5560        | 0           | 5472     |
| 32 | 1908881900| 14602    | 10761723 | 7316        | 30          | 7286     |
| 33 | 7635527480| 58288   | 21523445 | 0           | 0           | 0        |
| 34 | 11454711464| 44424  | 48427776 | 21944       | 0           | 21856    |
| 35 | 27487816992| 52488  | 87169619 | 26272       | 56          | 26216    |
| 36 | 183264019200| 355200 | 290566525| 0          | 0           | 0        |
| 37 | 104715443852| 99880  | 249056138| 49940       | 0           | 49940    |
| 38 | 440020029120| 432576 | 523020664| 0          | 0           | 0        |
| 39 | 1599290021720| 762608 | 1426411805| 0         | 0           | 0        |
| 40 | 1529755490574| 364724 | 204650846| 182362     | 0           | 182362   |
| 41 | 6701785562464| 798952 | 6724513104| 399472    | 0           | 399472   |
| 42 | 28147499352824| 3356408| 14121476937| 0        | 0           | 0        |
Table 2: Enumeration of circulant graphs by valency (for selective orders)

\[ c_u(n, r), \ r \text{ even} \]

| \( n \) | 7 | 13 | 14 | 19 | 37 | 38 | 61 | 62 | 73 | 74 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 2 | 1 | 2 | 1 | 2 | 1 | 2 | 1 | 2 | |
| 4 | 1 | 3 | 5 | 4 | 9 | 17 | 15 | 29 | 18 | 36 |
| 6 | 1 | 4 | 8 | 10 | 46 | 92 | 136 | 272 | 199 | 398 |
| 8 | 3 | 5 | 14 | 172 | 340 | 917 | 1827 | 1641 | 3281 |
| 10 | 1 | 2 | 14 | 476 | 952 | 4751 | 10472 | 20944 |
| 12 | 1 | 1 | 10 | 1038 | 2066 | 19811 | 390195 | 840652 |
| 14 | 4 | 1768 | 3536 | 67860 | 135720 | 231880 | 463760 |
| 16 | 1 | 2438 | 4862 | 195143 | 390195 | 840652 | 1681300 |
| 18 | 1 | 2704 | 5408 | 476913 | 953826 | 2615104 | 5230208 |
| 20 | 2438 | 4862 | 1001603 | 2003005 | 7060984 | 14121968 |
| 22 | 1768 | 3536 | 1820910 | 3641820 | 6486060 | 12837720 |
| 24 | 1038 | 2066 | 2883289 | 5766243 | 13769374 | 27538748 |
| 26 | 476 | 952 | 195143 | 390195 | 840652 | 1681300 |
| 28 | 172 | 340 | 4847637 | 9694845 | 105453584 | 210907168 |
| 30 | 46 | 92 | 5170604 | 10341208 | 4769374 | 953826 |
| 32 | 9 | 17 | 4847637 | 9694845 | 105453584 | 210907168 |
| 34 | 1 | 2 | 3991995 | 7983990 | 238819350 | 477638700 |
| 36 | 1 | 1 | 2883289 | 5766243 | 105453584 | 210907168 |
| 38 | 1820910 | 3641820 | 238819350 | 477638700 |
| 40 | 1001603 | 2003005 | 202997670 | 405995326 |

| \( n \) | 7 | 13 | 14 | 19 | 37 | 38 | 61 | 62 | 73 | 74 |
|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 | 1 |
| 1 | 1 | 3 | 1 | 1 | 1 | 3 | 1 | 2 | 1 | 2 |
| 2 | 6 | 14 | 9 | 15 | 18 | 38 | 5 | 10 | 17 | 34 |
| 3 | 4 | 50 | 46 | 136 | 199 | 434 | 14 | 28 | 182 | 364 |
| 4 | 3 | 123 | 172 | 917 | 1641 | 3679 | 20 | 40 | 1360 | 2720 |
| 5 | 1 | 66 | 476 | 4751 | 10472 | 24225 | 16 | 32 | 7616 | 15232 |
| 6 | 1 | 80 | 292 | 1038 | 19811 | 54132 | 129208 | 6 | 12 | 33006 | 66012 |
| 7 | 66 | 292 | 1768 | 67860 | 231880 | 572024 | 113152 | 226304 |
| 8 | 43 | 217 | 2438 | 195143 | 840652 | 2145060 | 311168 | 622336 |
| 9 | 19 | 123 | 2704 | 476913 | 2615104 | 6911508 | 691494 | 1382988 |
| 10 | 6 | 50 | 2438 | 1001603 | 7060984 | 19352176 | 2144672 | 4289344 |
| 11 | 1 | 14 | 1768 | 1820910 | 16689036 | 47500040 | 1810432 | 3620864 |
| 12 | 1 | 3 | 1038 | 2883289 | 34769374 | 102916810 | 2112184 | 4224368 |
| 13 | 1 | 476 | 3991995 | 64188600 | 197915938 | 1949696 | 3899392 |
| 14 | 172 | 4847637 | 105453584 | 339284368 | 1392640 | 2785280 |
| 15 | 46 | 5170604 | 154646044 | 520235176 | 742752 | 1485504 |
| 16 | 9 | 4847637 | 202997670 | 715323534 | 278528 | 557056 |
| 17 | 1 | 3991995 | 238819350 | 883634026 | 65536 | 131072 |
| 18 | 1 | 2883289 | 252088496 | 981815692 | 7286 | 14572 |
| 19 | 1820910 | 238819350 | 981815692 |
| 20 | 1001603 | 202997670 | 883634026 |
Table 3: Systematized list of identities

| No | Formula | Orders | Restrictions | Types | Proof | Refer. |
|----|---------|--------|--------------|-------|-------|--------|
| 1  | (3.4)   | n      | \( \exists p \mid n, p \equiv 3 \pmod{4} \) | su    | Combin. | FrRS90 |
|    | p or \( p^2 \) | \( p \equiv 3 \pmod{4} \) | Analytr. | AIMV99 |
| 2  | (3.5)   | p or \( p^2 \) | \( p \equiv 3 \pmod{4} \) | t, sd | Analytr. | KILP96 |
|    |         |         | \Leftarrow (3.4), (5.3) |       | (New)  |        |
| 3  | (3.7)   | p      | n = \( p \ldots b \) | su, t, sd | Algebr. | ChL86 |
| 4  | (4.1)   | p      | -                | u, su, sd | Analytr. | New    |
| 5  | (4.1')  | p      | \( p \equiv 3 \pmod{4} \) | u, sd | \Leftarrow (4.1), (3.4) | (New) |
| 6  | (4.1'') | p      | -                | u, su, t | \Leftarrow (4.1), (3.7) | (New) |
| 7  | (5.5)   | p, p^2 | -                | su, t, sd | \Leftarrow (5.2), (5.4) | (New) |
| 8  | (5.6)   | p, p^2 | -                | su, t, sd | \Leftarrow (3.7), (5.5) | (New) |
| 9  | (3.6)   | p, q   | \( p + 1 = 2q \equiv 6 \pmod{8} \) | su, t | \Leftarrow (3.2), (3.7) | (New) |
| 10 | (3.2)   | p, q   | \( p + 1 = 2q \) | su, sd | Analytr. | KILP96 |
|    |         |        |                |       |        |        |
| 11 | (3.1')  | p, q   | \( p + 1 = 2q \) | u, d | \Leftarrow (3.1) | KILP96 |
| 12 | (3.3')  | p, p + 1 | \( p + 1 = 2q \) | o     | \Leftarrow (3.3) | (New) |
| 13 | (4.2)   | p, p + 1 | \( p + 1 = 2q \) | u     | \Leftarrow (4.3) | (New) |
| 14 | (4.4)   | p, p + 1 | \( p + 1 = 2q \) | u, d  | \Leftarrow (4.5) | (New) |
| 15 | (4.6)   | p, p + 1 | \( p + 1 = 2q \) | u, d  | \Leftarrow (4.2), (4.4) | (New) |
| 16 | (4.6')  | p, p + 1 | \( p + 1 = 2q \) | d \( \setminus u \) | \Leftarrow (4.6) | (New) |
| 17 | (3.1)   | p, q   | \( p + 1 = 2q \) | u, d  | Analytr. | KILP96 |
| 18 | (3.3)   | p, p + 1 | \( p + 1 = 2q \) | o     | Analytr. | New    |
| 19 | (4.3)   | p, p + 1 | \( p + 1 = 2q \) | u     | Analytr. | New    |
| 20 | (4.3')  | p, p + 1 | \( p + 1 = 2q \) | u     | \Leftarrow (4.3) | (New) |
| 21 | (4.5)   | p, p + 1 | \( p + 1 = 2q \) | u     | Analytr. | New    |
| 22 | (4.7)   | p, p + 1 | \( p + 1 = 2q \) | d \( \setminus u \) | \Leftarrow (4.3), (4.5) | (New) |
| 23 | (3.8)   | 2n     | \( n \not\equiv 27 \) | u     | Exh. search | McK97/ |
|    |         |        | square-free \( ^c \) |       |        |        |
|    |         |        | Analytr. |       |       |        |
| 24 | (6.1)   | n      | \( p^2 \) or sq. free \( ^d \) | d, sd | Analytr. | New    |
| 25 | (6.2)   | n      | \( p^2 \) or sq. free \( ^d \) | u, su | Analytr. | New    |
| 26 | (6.3)   | n      | \( p^2 \) or sq. free \( ^d \) | o     | Analytr. | New    |
| 27 | (6.4)   | p      | -                | u, d  | \Leftarrow (6.1), (4.1) | (New) |
| 28 | (5.2)   | p, p^2 | -                | su    | Algebr. | LisP00 |
|    |         |        | t                |       |        |        |
| 29 | (5.3)   | p, p^2 | -                | su, t, sd | Algebr. | New    |
| 30 | (5.4)   | p^2    | -                | su, t, sd | Algebr. | New    |
| 31 | (6.7)   | p      | -                | u, sd | \Leftarrow (6.1), (4.1) | (New) |

\( ^a \) p and q are prime.

\( ^b \) Holds also for \( n = p^k \) and square-free \( n \) with all prime divisors \( p \equiv 3 \pmod{4} \).

Is conjectured to hold for arbitrary \( n \) with all such prime divisors.

\( ^c \) Is conjectured to hold for arbitrary even orders.

\( ^d \) Is conjectured to hold for arbitrary odd orders.

\( ^e \) There is a corresponding conjecture for arbitrary even orders \( n, 8 \nmid n \).