A method for determining the mod-2^k behaviour of (certain) recursive sequences

Manuel Kauers, Christian Krattenthaler and Thomas W. Müller

Universität Linz; Universität Wien; Queen Mary, University of London

Let $(a_n)_{n\geq 0}$ be a sequence of integers, where a_n is the number of ... of "size" n.

Let $(a_n)_{n\geq 0}$ be a sequence of integers, where a_n is the number of ... of "size" n.

What can we say about modular properties of these numbers?

Combinatorial sequences modulo powers of 2

Let $(a_n)_{n\geq 0}$ be a sequence of integers, where a_n is the number of ... of "size" n.

What can we say about modular properties of these numbers?

In this talk:

What can we say about the value of a_n modulo 2^k?

Combinatorial sequences modulo powers of 2

Let $(a_n)_{n\geq 0}$ be a sequence of integers, where a_n is the number of ... of "size" n.

What can we say about modular properties of these numbers?

In this talk:

What can we say about the value of a_n modulo 2^k?

Theorem (Stothers 1977)

The number s_n of index-n-subgroups in the inhomogeneous modular group $PSL_2(\mathbb{Z})$ is odd if, and only if, n is of the form $2^k - 3$ or $2^{k+1} - 6$, for some positive integer $k \geq 2$.

The first few numbers s_n, $n \geq 1$, are

$$1, 1, 4, 8, 5, 22, 42, 40, 120, 265, 286, 764, 1729, \ldots$$

Combinatorial sequences modulo powers of 2

Let $(a_n)_{n\geq 0}$ be a sequence of integers, where a_n is the number of ... of "size" n.

What can we say about modular properties of these numbers?

In this talk:

What can we say about the value of a_n modulo 2^k?

Theorem (Stothers 1977)

The number s_n of index-n-subgroups in the inhomogeneous modular group $PSL_2(\mathbb{Z})$ is odd if, and only if, n is of the form $2^k - 3$ or $2^{k+1} - 6$, for some positive integer $k \geq 2$.

The first few numbers s_n, $n \geq 1$, are

$$1, 1, 4, 8, 5, 22, 42, 40, 120, 265, 286, 764, 1729, \ldots$$

Combinatorial sequences modulo powers of 2

Let $(a_n)_{n\geq 0}$ be a sequence of integers, where a_n is the number of ... of "size" n.

What can we say about modular properties of these numbers?

In this talk:

What can we say about the value of a_n modulo 2^k?

Theorem (Stothers 1977)

The number s_n of index-n-subgroups in the inhomogeneous modular group $PSL_2(\mathbb{Z})$ is odd if, and only if, n is of the form $2^k - 3$ or $2^{k+1} - 6$, for some positive integer $k \geq 2$.

The first few numbers s_n, $n \geq 1$, are

$$1, 1, 4, 8, 5, 22, 42, 40, 120, 265, 286, 764, 1729, \ldots$$

Stothers proved his result by clever counting of coset diagrams. A different proof of this result was given by Godsil, Imrich, and Razen.

DIVISIBILITY PROPERTIES OF SUBGROUP NUMBERS FOR THE MODULAR GROUP

THOMAS W. MÜLLER and JAN-CHRISTOPH SCHLAGE-PUCHTA

ABSTRACT. Let $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$ be the classical modular group. It has been shown by Stothers (*Proc. Royal Soc. Edinburgh* **78A**, 105–112) that s_n, the number of index n subgroups in Γ, is odd if and only if $n+3$ or $n+6$ is a 2-power. Moreover, Stothers loc. cit. also showed that f_λ, the number of free subgroups of index 6λ in Γ, is odd if and only if $\lambda+1$ is a 2-power. Here, these divisibility results for f_λ and s_n are generalized to congruences modulo higher powers of 2. We also determine the behaviour modulo 3 of f_λ. Our results are naturally expressed in terms of the binary respectively ternary expansion of the index.

1. INTRODUCTION AND RESULTS

Let $\Gamma = \mathrm{PSL}_2(\mathbb{Z})$ be the classical modular group. We denote by s_n the number of index n subgroups in Γ, and by f_λ the number of free subgroups in Γ of index 6λ. These days, quite a lot is known concerning the subgroup arithmetic of Γ. Newman [5, Theorem 4] gave an asymptotic formula for s_n; for a more general and more precise result see [3, Theorem 1]. Based on numerical computations of Newman, Johnson conjectured that s_n is odd if and only if $n = 2^a - 3, a \geq 2$ or $n = 2^a - 6, a \geq 3$. This conjecture was first proved by Stothers [6]. He first used coset diagrams to establish a relation between s_n and f_λ for various λ in the range $1 \leq \lambda \leq \frac{n+4}{6}$, and then showed that f_λ is odd if and only if $\lambda = 2^a - 1, a \geq 1$. The parity pattern for f_λ found by Stothers has been shown to hold for a larger class of virtually free groups, including free products $\Gamma = G_1 *_S G_2$

(iii) *For* λ *odd with* $\mathfrak{s}_2(\lambda+1)=2$, *write* $\lambda = 2^a+2^b-1, a>b\ge 1$. *Then we have*

$$f_\lambda \equiv \begin{cases} 14, & b=1 \\ 6, & b=2 \\ 2, & a=b+1 \\ 6, & a=b+2 \\ 14, & \text{otherwise} \end{cases} \pmod{16}.$$

(iv) *For* λ *odd with* $\mathfrak{s}_2(\lambda+1)=3$, *write* $\lambda=2^a+2^b+2^c-1$, *where* $a>b>c\ge 1$. *Assume that precisely* k *of the equations* $a=b+1$, *and* $b=c+1$ *hold,* $k=0,1,2$. *Then we have*

$$f_\lambda \equiv \begin{cases} 4, & k\equiv 0\,(2) \\ 12, & k \equiv 1\,(2) \end{cases} \pmod{16}.$$

(v) *If* λ *is odd with* $\mathfrak{s}_2(\lambda+1)=4$, *then* $f_\lambda \equiv 8\,(16)$.

(vi) *If* λ *is odd with* $\mathfrak{s}_2(\lambda+1)\ge 5$, *then* $f_\lambda\equiv 0\,(16)$.

The regular behaviour of the function f_λ described in Theorem 1 breaks down for $\lambda<20$. Here the values modulo 16 are as follows.

λ	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
f_λ	5	12	1	0	2	0	5	0	6	0	2	0	4	0	5	0	6	0	6

Theorem 2. *Let* $n\ge 22$ *be an integer. Then we have modulo* 8

$$s_n \equiv \begin{cases} 1, & n=2^a-3 \\ 5, & n=2^a-6 \\ 2, & n=3\cdot 2^a-3, 3\cdot 2^a-6 \\ 6, & n=2^a+2^b-3, 2^a+2^b-6, 2^a+3,\ a\ge b+2 \\ 4, & n=2^a+2^b+2^c-6, a>b>c\ge 2, 2^a+2^b+2^c-3, a>b>c\ge 2, b\ge 4, \\ & n=2^a+2^b+3, a>b\ge 2 \\ 0, & \textit{otherwise.} \end{cases}$$

In this way we may simplify the last displayed expression as follows.

$$\begin{gathered}
2\#\{n=2^a+2^b, a>b\geq 2\}+2\#\{n=2^a+2^b-3, a\geq 3, b\geq 2\}\\
+2\#\{n=2^a+2^b-6, a>b\geq 3\}-2\#\{n=2^a+2^b+3, a>b\}\\
-2\#\{n=2^a+2^b, a\geq 3, b\geq 2\}-2\#\{n=2^a+2^b-3, a>b\geq 3\}\\
+4\#\{n=2^b+2^c+4, b>c\geq 2, b\geq 4\}+4\#\{n=2^a+9, a\geq 3\}\\
+4\#\{n=2^b+2^c+1, b>c\geq 2\}+4\#\{n=2^a+2^b+2^c-6, b>c\geq 2, a\geq 3\}\\
+4\#\{n=2^a+2^b+2^c+3, b>c\geq 2, a\geq 2, b\geq 4\}\\
+4\#\{n=2^a+2^b+2^c, b>c\geq 2, a\geq 2\}+4\#\{n=2^a+2^b+2^c-3, b>c\geq 2, a\geq 3\}\\
+4\#\{n=2^a+2^b+3, a\geq 3, b\geq 2\}+4\#\{n=2^a+2^b+9, a, b\geq 2\}
\end{gathered}$$

Next consider for example the quantity $4\#\{n=2^a+2^b+6, a\geq 3, b\geq 2\}$. If (a,b) is a solution with $a>b\geq 3$, then (b,a) is also a solution, that is, the number of solutions is even, unless n is of the form $n=2^a+10, a\geq 3$, or n is of the form 2^a+6 with $a\geq 4$. The same argument may be applied to several other terms as well, which allows us to simplify the expression further to obtain the following.

$$\begin{gathered}
2\#\{n=2^a+2^b, a>b\}+4\#\{n=2^a+1, a\geq 3\}+2\#\{n=2^a-3, a\geq 4\}\}\\
+4\#\{n=2^a+2^b-3, a>b\geq 2\}+2\#\{n=2^a+2^b-6, a>b\geq 3\}-2\#\{n=2^a+2^b+3, a>b\}\\
-2\#\{n=2^a+4, a\geq 3\}-2\#\{n=2^a, a\geq 4\}+4\#\{n=2^a+2^b, a>b\geq 2\}\\
-2\#\{n=2^a+2^b-3, a>b\geq 3\}+4\#\{n=2^b+2^c+4, b>c\geq 2, b\geq 4\}\\
+4\#\{n=2^b+2^c+1, b>c\geq 2\}+4\#\{n=2^a+2^b+2^c-6, b>c\geq 2, a\geq 3\}\\
+4\#\{n=2^a+2^b+2^c+3, b>c\geq 2, a\geq 2, b\geq 4\}\\
+4\#\{n=2^a+2^b+2^c, b>c\geq 2, a\geq 2\}+4\#\{n=2^a+2^b+2^c-3, b>c\geq 2, a\geq 3\}\\
+4\#\{n=2^a+7, a\geq 3\}+4\#\{n=2^a+3, a\geq 4\}
\end{gathered}$$

Finally, consider the quantity $\#\{n=2^a+2^b+2^c, b>c\geq 2, a\geq 2\}$. Let (a,b,c) be a solution counted. If all three components are distinct, there are no solutions with two

To ease further computations, we consider sets with one, two, and three parameters separately. Sets defined by one parameter contribute

$$\begin{aligned}
&\{4|n = 2^a, 2^a - 3, a \ge 3\} + \{2|n = 2^a - 2, 2^a + 1, a \ge 3\} + \{1|n = 2^a, a \ge 3\}\\
&\quad + \{4|n = 3 \cdot 2^a, a \ge 3\} + \{4|n = 2^a + 9, a \ge 3\} + \{6|n = 2^a + 1, 2^a + 4, a \ge 3\}\\
&\quad + \{7|n = 2^a + 3, a \ge 3\} + \{4|n = 3 \cdot 2^a + 3, a \ge 3\} + \{4|n = 2^a + 12\}\\
&\quad + \{1|n = 2^a - 6, 2^a\} + \{7|n = 2^a - 3, 2^a + 3\} + \{4|n = 2^a + 12, 2^a + 15, a > b \ge 2\}\\
&\quad + \{4|n = 2^a + 1, a \ge 3\} + \{2|n = 2^a - 3, a \ge 4\}\} - \{2|n = 2^a + 4, a \ge 3\}\\
&\quad - \{2|n = 2^a, a \ge 4\} + \{4|n = 2^a - 2, a \ge 5\} + \{4|n = 2^a - 6, a \ge 5\}\\
&\quad + \{4|n = 3 \cdot 2^a - 6, a \ge 5\} + \{4|n = 2^a + 15, a \ge 2\} + \{4|n = 2^a + 7, a \ge 4\}\\
&\quad + \{4|n = 2^a + 3, a \ge 4\} + \{4|n = 3 \cdot 2^a + 3, a \ge 4\} + \{4|n = 2^a + 4, a \ge 4\}\\
&\quad + \{4|n = 2^a, a \ge 4\} + \{4|n = 3 \cdot 2^a, a \ge 4\} + \{4|n = 2^a + 1, a \ge 4\}\\
&\quad + \{4|n = 2^a - 3, a \ge 4\} + \{4|n = 3 \cdot 2^a - 3, a \ge 4\} + \{4|n = 2^a + 7, a \ge 3\}\\
&\quad + \{4|n = 2^a + 3, a \ge 4\},
\end{aligned}$$

which is congruent to

$$\begin{aligned}
&\{5|n = 2^a - 6, a \ge 5\} + \{1|n = 2^a - 3, a \ge 3\} + \{6|n = 2^a - 2, a \ge 3\}\\
&\quad + \{6|n = 2^a + 3, a \ge 3\} + \{4|n = 2^a + 9, a \ge 3\}\\
&\quad + \{4|n = 3 \cdot 2^a - 6, a \ge 3\} + \{4|n = 3 \cdot 2^a - 3, a \ge 4\}.
\end{aligned}$$

Next, we collect all 2-parameter sets. These contribute

$$\begin{aligned}
&\{4|n = 2^a + 2^b + 1, 2^a + 2^b - 2, a > b \ge 2\} + \{2|n = 2^a + 2^b, a > b \ge 2\}\\
&\quad + \{4|n = 2^a + 2^b + 4, 2^a + 2^b + 1, a > b \ge 2\} + \{2|n = 2^a + 2^b + 3, a > b \ge 2\}\\
&\quad + \{4|n = 2^a + 2^b, 2^a + 2^b + 3, 2^a + 2^b - 6, 2^a + 2^b - 3, a > b \ge 2\}\\
&\quad + \{2|n = 2^a + 2^b, a > b\} + \{4|n = 2^a + 2^b - 3, a > b \ge 2\}\\
&\quad + \{2|n = 2^a + 2^b - 6, a > b \ge 3\} - \{2|n = 2^a + 2^b + 3, a > b\}\\
&\quad + \{4|n = 2^a + 2^b, a > b \ge 2\} - \{2|n = 2^a + 2^b - 3, a > b \ge 3\}
\end{aligned}$$

Generating Functions!!

Generating Functions!!

Let us have another look at Stothers' theorem:

Theorem (Stothers 1977)

The number s_n of index-n-subgroups in the inhomogeneous modular group $PSL_2(\mathbb{Z})$ is odd if, and only if, n is of the form $2^k - 3$ or $2^{k+1} - 6$, for some positive integer $k \geq 2$.

Generating Functions!!

Let us have another look at Stothers' theorem:

Theorem (Stothers 1977)

The number s_n of index-n-subgroups in the inhomogeneous modular group $PSL_2(\mathbb{Z})$ is odd if, and only if, n is of the form $2^k - 3$ or $2^{k+1} - 6$, for some positive integer $k \geq 2$.

Generating Functions!!

Let us have another look at Stothers' theorem:

Theorem (Stothers 1977)

The number s_n of index-n-subgroups in the inhomogeneous modular group $PSL_2(\mathbb{Z})$ is odd if, and only if, n is of the form $2^k - 3$ or $2^{k+1} - 6$, for some positive integer $k \geq 2$.

In other words: Let

$$\Phi(z) = \sum_{n \geq 0} z^{2^n} = z + z^2 + z^4 + z^8 + z^{16} + \cdots .$$

Then

$$\sum_{n \geq 0} s_{n+1} z^n = (z^{-7} + z^{-4})\Phi(z) + z^{-6} + z^{-5} + z^{-2} \quad \text{modulo } 2.$$

(iii) *For λ odd with $\mathfrak{s}_2(\lambda+1)=2$, write $\lambda = 2^a + 2^b - 1, a > b \geq 1$. Then we have*

$$f_\lambda \equiv \begin{cases} 14, & b=1 \\ 6, & b=2 \\ 2, & a=b+1 \\ 6, & a=b+2 \\ 14, & \text{otherwise} \end{cases} \pmod{16}.$$

(iv) *For λ odd with $\mathfrak{s}_2(\lambda+1)=3$, write $\lambda = 2^a + 2^b + 2^c - 1$, where $a > b > c \geq 1$. Assume that precisely k of the equations $a = b+1$, and $b = c+1$ hold, $k = 0, 1, 2$. Then we have*

$$f_\lambda \equiv \begin{cases} 4, & k \equiv 0\,(2) \\ 12, & k \equiv 1\,(2) \end{cases} \pmod{16}.$$

(v) *If λ is odd with $\mathfrak{s}_2(\lambda+1)=4$, then $f_\lambda \equiv 8\,(16)$.*

(vi) *If λ is odd with $\mathfrak{s}_2(\lambda+1)\geq 5$, then $f_\lambda \equiv 0\,(16)$.*

The regular behaviour of the function f_λ described in Theorem 1 breaks down for $\lambda < 20$. Here the values modulo 16 are as follows.

λ	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
f_λ	5	12	1	0	2	0	5	0	6	0	2	0	4	0	5	0	6	0	6

Theorem 2. *Let $n \geq 22$ be an integer. Then we have modulo 8*

$$s_n \equiv \begin{cases} 1, & n = 2^a - 3 \\ 5, & n = 2^a - 6 \\ 2, & n = 3\cdot 2^a - 3, 3\cdot 2^a - 6 \\ 6, & n = 2^a + 2^b - 3, 2^a + 2^b - 6, 2^a + 3,\ a \geq b+2 \\ 4, & n = 2^a + 2^b + 2^c - 6, a > b > c \geq 2, 2^a + 2^b + 2^c - 3, a > b > c \geq 2, b \geq 4, \\ & n = 2^a + 2^b + 3, a > b \geq 2 \\ 0, & \textit{otherwise.} \end{cases}$$

Let

$$\Phi(z) = \sum_{n\ge 0} z^{2^n} = z + z^2 + z^4 + z^8 + z^{16} + \cdots .$$

Then the result of Müller and Schlage–Puchta can be compactly expressed in the form

$$\sum_{n\ge 0} s_{n+1} z^n = z^{57}+4z^{20}+4z^{17}+4z^{14}+4z^{12}+4z^{11}+4z^{10}+4z^9+2z^8+4z^5+2z^4+4z^3+2z^2$$
$$+4z+2+\frac{1}{z^2}+\frac{7}{z^3}+\frac{5}{z^4}+\frac{5}{z^5}+\frac{2}{z^6}+\left(\frac{6}{z^7}+\frac{2}{z^6}+\frac{2}{z^4}+4z^3+\frac{2}{z^3}+4z^2+\frac{4}{z}\right)\Phi(z)$$
$$+\left(4z^8+\frac{3}{z^7}+\frac{2}{z^6}+\frac{2}{z^5}+4z^4+\frac{3}{z^4}+4z^3+\frac{6}{z^3}+2z^2+\frac{2}{z^2}+\frac{4}{z}+4\right)\Phi^2(z)$$
$$+\left(\frac{6}{z^7}+\frac{4}{z^6}+\frac{4}{z^5}+\frac{6}{z^4}+\frac{4}{z^3}+4z^2+\frac{4}{z^2}\right)\Phi^3(z) \quad \text{modulo } 8.$$

A proof "method" for congruences modulo 2

A proof "method" for congruences modulo 2

It is a simple observation that $\Phi(z) = \sum_{n \ge 0} z^{2^n}$ satisfies

$$\Phi^2(z) - \Phi(z) - z = 0 \quad \text{modulo } 2.$$

A proof "method" for congruences modulo 2

It is a simple observation that $\Phi(z) = \sum_{n\ge 0} z^{2^n}$ satisfies

$$\Phi^2(z) - \Phi(z) - z = 0 \quad \text{modulo } 2.$$

Suppose that we want to determine the behaviour of the sequence $(f_n)_{n\ge 0}$ modulo 2. We form the generating function $F(z) = \sum_{n\ge 0} f_n z^n$, and suppose that we know that it satisfies a differential equation of the form

$$\mathcal{P}(z; F(z), F'(z), F''(z), \dots, F^{(s)}(z)) = 0,$$

where $\mathcal{P}$ is a polynomial with integer coefficients, which has a unique formal power series solution.

A proof “method” for congruences modulo 2

We know

$$\Phi^2(z) - \Phi(z) - z = 0 \quad \text{modulo } 2. \tag{1}$$

and

$$\mathcal{P}(z; F(z), F'(z), F''(z), \dots, F^{(s)}(z)) = 0.$$

A proof "method" for congruences modulo 2

We know

$$\Phi^2(z) - \Phi(z) - z = 0 \quad \text{modulo } 2. \tag{1}$$

and

$$\mathcal{P}(z; F(z), F'(z), F''(z), \dots, F^{(s)}(z)) = 0.$$

Then, to prove a guessed congruence of the form

$$F(z) = a_0(z) + a_1(z)\Phi(z) \quad \text{modulo } 2,$$

where $a_0(z), a_1(z)$ are Laurent polynomials, is trivial:
one substitutes the guess into the differential equation, one reduces higher powers of $\Phi(z)$ by means of (1), one reduces the result modulo 2, using the trivial fact that

$$\Phi'(z) = 1 \quad \text{modulo } 2,$$

and one verifies that everything vanishes.

A proof "method" for congruences modulo 2

We know

$$\Phi^2(z) - \Phi(z) - z = 0 \quad \text{modulo } 2. \tag{1}$$

and

$$\mathcal{P}(z; F(z), F'(z), F''(z), \dots, F^{(s)}(z)) = 0.$$

Then, to prove a guessed congruence of the form

$$F(z) = a_0(z) + a_1(z)\Phi(z) \quad \text{modulo } 2,$$

where $a_0(z), a_1(z)$ are Laurent polynomials, is trivial:
one substitutes the guess into the differential equation, one reduces higher powers of $\Phi(z)$ by means of (1), one reduces the result modulo 2, using the trivial fact that

$$\Phi'(z) = 1 \quad \text{modulo } 2,$$

and one verifies that everything vanishes.
A computer can do this!

Example: Catalan numbers

Example: Catalan numbers

Everybody knows that the generating function $C(z) = \sum_{n \geq 0} \mathrm{Cat}_n z^n$ for the Catalan numbers $\mathrm{Cat}_n = \frac{1}{n+1}\binom{2n}{n}$ satisfies the equation

$$zC^2(z) - C(z) + 1 = 0.$$

Example: Catalan numbers

Everybody knows that the generating function $C(z) = \sum_{n \geq 0} \mathrm{Cat}_n \, z^n$ for the Catalan numbers $\mathrm{Cat}_n = \frac{1}{n+1}\binom{2n}{n}$ satisfies the equation

$$zC^2(z) - C(z) + 1 = 0.$$

It is easy to guess that

$$C(z) = z^{-1}\Phi(z) \quad \text{modulo } 2.$$

It is even easier to prove that: we substitute in the equation,

$$\begin{aligned} z(z^{-1}\Phi(z))^2 - z^{-1}\Phi(z) + 1 &= z^{-1}\Phi^2(z) - z^{-1}\Phi(z) + 1 \\ &= z^{-1}(\Phi(z) + z) - z^{-1}\Phi(z) + 1 = 0 \quad \text{modulo } 2, \end{aligned}$$

and do the reduction!

What about congruences modulo higher powers of 2?

First we need a polynomial equation satisfied by $\Phi(z)$. Recalling the congruence

$$\Phi^2(z) - \Phi(z) - z = 0 \quad \text{modulo } 2,$$

we might take

$$(\Phi^2(z) - \Phi(z) - z)^k = 0 \quad \text{modulo } 2^k.$$

What about congruences modulo higher powers of 2?

First we need a polynomial equation satisfied by $\Phi(z)$. Recalling the congruence

$$\Phi^2(z) - \Phi(z) - z = 0 \quad \text{modulo } 2,$$

we might take

$$(\Phi^2(z) - \Phi(z) - z)^k = 0 \quad \text{modulo } 2^k.$$

As it turns out, this is not "optimal." For example, we have actually

$$\Phi^4(z) + 6\Phi^3(z) + (2z+3)\Phi^2(z) + (2z+6)\Phi(z) + 2z + 5z^2 = 0 \quad \text{modulo } 8.$$

What about congruences modulo higher powers of 2?

In general, we are not able to provide a formula for a monic polynomial of minimal degree satisfied by $\Phi(z)$ modulo 2^k.
We do have a precise conjecture for the minimal degree, though, and a procedure for computing such a polynomial of minimal degree for every specific k.
So, in lack of a precise formula, we base our considerations on the congruence

$$(\Phi^4(z)+6\Phi^3(z)+(2z+3)\Phi^2(z)+(2z+6)\Phi(z)+2z+5z^2)^{2^\alpha} = 0 \quad \text{modulo } 8^{2^\alpha} = 2^{3\cdot 2^\alpha}.$$

What about congruences modulo higher powers of 2?

In general, we are not able to provide a formula for a monic polynomial of minimal degree satisfied by $\Phi(z)$ modulo 2^k.
We do have a precise conjecture for the minimal degree, though, and a procedure for computing such a polynomial of minimal degree for every specific k.
So, in lack of a precise formula, we base our considerations on the congruence

$$(\Phi^4(z)+6\Phi^3(z)+(2z+3)\Phi^2(z)+(2z+6)\Phi(z)+2z+5z^2)^{2^\alpha}=0 \quad \text{modulo } 8^{2^\alpha}=2^{3\cdot 2^\alpha}.$$

This is a polynomial relation of degree $2^{\alpha+2}$.

The “method” for proving congruences modulo 2^k

The “method” for proving congruences modulo 2^k

Idea:

Make the Ansatz

$$F(z) = \sum_{i=0}^{2^{\alpha+2}-1} a_i(z)\Phi^i(z) \quad \text{modulo } 2^{3\cdot 2^\alpha},$$

where the $a_i(z)$'s are (at this point) undetermined Laurent polynomials in z.

Then, gradually determine approximations $a_{i,\beta}(z)$ to $a_i(z)$ such that our differential equation

$$\mathcal{P}(z; F(z), F'(z), F''(z), \dots, F^{(s)}(z)) = 0$$

holds modulo 2^β, for $\beta = 1, 2, \dots, 3 \cdot 2^\alpha$.

The "method" for proving congruences modulo 2^k

The base step:

Substitute

$$F(z) = \sum_{i=0}^{2^{\alpha+2}-1} a_{i,1}(z)\Phi^i(z) \quad \text{modulo } 2$$

into the differential equation, considered modulo 2,

$$\mathcal{P}(z; F(z), F'(z), F''(z), \dots, F^{(s)}(z)) = 0 \quad \text{modulo } 2,$$

use $\Phi'(z) = 1$ modulo 2, reduce high powers of $\Phi(z)$ modulo the polynomial relation of degree $2^{\alpha+2}$ satisfied by $\Phi(z)$, and compare coefficients of powers $\Phi^k(z)$, $k = 0, 1, \dots, 2^{\alpha+2} - 1$. This yields a system of $2^{\alpha+2}$ (algebraic differential) equations (modulo 2) for the unknown Laurent polynomials $a_{i,1}(z)$, $i = 0, 1, \dots, 2^{\alpha+2} - 1$, which may or may not have a solution.

The "method" for proving congruences modulo 2^k

The iteration:

Provided we have already found $a_{i,\beta}(z)$, $i = 0, 1, \ldots, 2^{\alpha+2} - 1$, such that

$$F(z) = \sum_{i=0}^{2^{\alpha+2}-1} a_{i,\beta}(z)\Phi^i(z)$$

solves our differential equation modulo 2^β, we put

$$a_{i,\beta+1}(z) := a_{i,\beta}(z) + 2^\beta b_{i,\beta+1}(z), \quad i = 0, 1, \ldots, 2^{\alpha+2} - 1,$$

where the $b_{i,\beta+1}(z)$'s are (at this point) undetermined Laurent polynomials in z. Next we substitute

$$F(z) = \sum_{i=0}^{2^{\alpha+2}-1} a_{i,\beta+1}(z)\Phi^i(z)$$

in the differential equation.

The "method" for proving congruences modulo 2^k

The iteration:

One uses
$$\Phi'(z) = \sum_{n=0}^{\beta} 2^n z^{2^n-1} \quad \text{modulo } 2^{\beta+1},$$
one reduces high powers of $\Phi(z)$ using the polynomial relation satisfied by $\Phi(z)$, and one compares coefficients of powers $\Phi^j(z)$, $j = 0, 1, \ldots, 2^{\alpha+2} - 1$. After simplification, this yields a system of $2^{\alpha+2}$ (linear differential) equations (modulo 2) for the unknown Laurent polynomials $b_{i,\beta+1}(z)$, $i = 0, 1, \ldots, 2^{\alpha+2} - 1$, which may or may not have a solution.

The "method" for proving congruences modulo 2^k

The iteration:

One uses

$$\Phi'(z) = \sum_{n=0}^{\beta} 2^n z^{2^n - 1} \quad \text{modulo } 2^{\beta+1},$$

one reduces high powers of $\Phi(z)$ using the polynomial relation satisfied by $\Phi(z)$, and one compares coefficients of powers $\Phi^j(z)$, $j = 0, 1, \dots, 2^{\alpha+2} - 1$. After simplification, this yields a system of $2^{\alpha+2}$ (linear differential) equations (modulo 2) for the unknown Laurent polynomials $b_{i,\beta+1}(z)$, $i = 0, 1, \dots, 2^{\alpha+2} - 1$, which may or may not have a solution.

(More precisely, in general this will be a system of linear equations in the $b_{i,\beta+1}(z)$'s and $b'_{i,\beta+1}(z)$'s, $i = 0, 1, \dots, 2^{\alpha+2} - 1$. By separating each unknown polynomial $b(z)$ into "even part" and "odd part," $b(z) = b^{(e)}(z) + b^{(o)}(z)$, and by using the observation

$$b'(z) = z^{-1} b^{(o)}(z) \quad \text{modulo } 2,$$

this system can be converted into a system of linear equations in the even and odd parts of the $b_{i,\beta+1}(z)$'s.)

Catalan numbers again

Catalan numbers again

The Ansatz:

$$C(z) = \sum_{i=0}^{2^{\alpha+2}-1} a_i(z)\Phi^i(z) \quad \text{modulo } 2^{3\cdot 2^{\alpha}}.$$

Catalan numbers again

The Ansatz:

$$C(z) = \sum_{i=0}^{2^{\alpha+2}-1} a_i(z)\Phi^i(z) \quad \text{modulo } 2^{3\cdot 2^\alpha}.$$

The base step:

We have

$$C(z) = \sum_{k=0}^{\alpha} z^{2^k-1} + z^{-1}\Phi^{2^{\alpha+1}}(z) \quad \text{modulo } 2.$$

Catalan numbers again

The Ansatz:

$$C(z) = \sum_{i=0}^{2^{\alpha+2}-1} a_i(z)\Phi^i(z) \quad \text{modulo } 2^{3\cdot 2^\alpha}.$$

The base step:

We have

$$C(z) = \sum_{k=0}^{\alpha} z^{2^k-1} + z^{-1}\Phi^{2^{\alpha+1}}(z) \quad \text{modulo } 2.$$

The iteration: works automatically without problems.

Theorem

Let $\Phi(z) = \sum_{n\geq 0} z^{2^n}$, *and let* α *be some positive integer. Then the generating function* $C(z)$ *for Catalan numbers, reduced modulo* $2^{3\cdot 2^\alpha}$, *can be expressed as a polynomial in* $\Phi(z)$ *of degree at most* $2^{\alpha+2}-1$ *with coefficients that are Laurent polynomials in* z. *Moreover, for any given* α, *this polynomial can be found automatically.*

Journal of Integer Sequences, Vol. 13 (2010),
Article 10.5.4

Catalan Numbers Modulo 2^k

Shu-Chung Liu[1]
Department of Applied Mathematics
National Hsinchu University of Education
Hsinchu, Taiwan
liularry@mail.nhcue.edu.tw

and

Jean C.-C. Yeh
Department of Mathematics
Texas A & M University
College Station, TX 77843-3368
USA

Abstract

In this paper, we develop a systematic tool to calculate the congruences of some combinatorial numbers involving $n!$. Using this tool, we re-prove Kummer's and Lucas' theorems in a unique concept, and classify the congruences of the Catalan numbers c_n (mod 64). To achieve the second goal, c_n (mod 8) and c_n (mod 16) are also classified. Through the approach of these three congruence problems, we develop several general properties. For instance, a general formula with powers of 2 and 5 can evaluate c_n (mod

For those c_n (mod 64) with $\omega_2(c_n) = 2$, we can simply plug $u_{16}(c_n)$ given in (47) into (32). Here we also show a precise classification by tables.

Theorem 6.3. *Let $n \in \mathbb{N}$ with $d(\alpha) = 2$. Then we have*

$$c_n \equiv_{64} (-1)^{zr(\alpha)} 4 \times 5^{u_{16}(CF_2(c_n))},$$

where $u_{16}(CF_2(c_n))$ is given in (47). Precisely, let $[\alpha]_2 = \langle 10^a 10^b \rangle_2$, i.e., $[n]_2 = \langle 10^a 10^{b+1} 1^\beta \rangle_2$, and then we have c_n (mod 64) shown in the following four tables.

	$a=0$	$a=1$	$a=2$	$a\geq 3$
$b=0$	4	28	44	12
$b=1$	12	36	52	20
$b=2$	60	20	36	4
$b\geq 3$	28	52	4	36

when $\beta = 0$

	$a=0$	$a=1$	$a=2$	$a\geq 3$
$b=0$	52	12	28	60
$b=1$	44	4	20	52
$b=2$	60	20	36	4
$b\geq 3$	28	52	4	36

when $\beta = 1$

	$a=0$	$a=1$	$a=2$	$a\geq 3$
$b=0$	36	28	44	12
$b=1$	28	20	36	4
$b=2$	44	36	52	20
$b\geq 3$	12	4	20	52

when $\beta = 2$

	$a=0$	$a=1$	$a=2$	$a\geq 3$
$b=0$	4	60	12	44
$b=1$	60	52	4	36
$b=2$	12	4	20	52
$b\geq 3$	44	36	52	20

when $\beta \geq 3$

Proof. Notice that there are difference between $a \geq 3$ and $a = 3$, and similarly for b and β. We split (47) into two parts as follows:

$$\begin{aligned} A &:= \chi(\beta'=0)(2\ddot{\alpha}_1 - \ddot{\alpha}_0 - 1) - \chi(\beta'=1) + 2\chi(\beta'=2)\ddot{\alpha}_0 + 2\chi(\beta'=3)(1-\ddot{\alpha}_0), \\ B &:= 2\big[c_2(\ddot{\alpha}) + \ddot{\alpha}_0(1-\ddot{\alpha}_2) + \#(\mathcal{S}_4(\ddot{\alpha}), \{\langle 0011\rangle_2, \langle 1\text{x}00\rangle_2\})\big] - r_1(\ddot{\alpha}) - zr_1(\ddot{\alpha}) \\ &\quad + \ddot{\alpha}_0\ddot{\alpha}_1 + 1. \end{aligned}$$

Clearly, B is independent on β'. We will only prove the first table of this theorem. The other three tables can be checked in the same way. With simple calculation we obtain the values of A as $\beta = 0$ and B as follows:

	$a=0$	$a=1$	$a=2$	$a=3$
$b=0$	0	2	2	2

	$a=0$	$a=1$	$a=2$	$a=3$
$b=0$	0	2	1	3

Theorem (Liu and Yeh, compactly)

Let $\Phi(z) = \sum_{n\geq 0} z^{2^n}$. *Then, modulo* 64, *we have*

$$\begin{aligned}\sum_{n=0}^{\infty} \mathrm{Cat}_n\, z^n &= 32z^5+16z^4+6z^2+13z+1+\left(32z^4+32z^3+20z^2+44z+40\right)\Phi(z)\\ &+\left(16z^3+56z^2+30z+52+\frac{12}{z}\right)\Phi^2(z)+\left(32z^3+60z+60+\frac{28}{z}\right)\Phi^3(z)\\ &+\left(32z^3+16z^2+48z+18+\frac{35}{z}\right)\Phi^4(z)+\left(32z^2+44\right)\Phi^5(z)\\ &+\left(48z+8+\frac{50}{z}\right)\Phi^6(z)+\left(32z+32+\frac{4}{z}\right)\Phi^7(z) \qquad \text{modulo } 64.\end{aligned}$$

Theorem

Let $\Phi(z) = \sum_{n\geq 0} z^{2^n}$*. Then, modulo* 4096*, we have*

$$\begin{aligned}\sum_{n=0}^{\infty} \mathrm{Cat}_n\, z^n &= 2048z^{14} + 3072z^{13} + 2048z^{12} + 3584z^{11} + 640z^{10} + 2240z^9 + 32z^8 \\ &\quad + 832z^7 + 2412z^6 + 1042z^5 + 2702z^4 + 53z^3 + 2z^2 + z + 1 \\ &\quad + \big(2048z^{12} + 3840z^{10} + 2112z^8 + 2112z^7 + 552z^6 \\ &\qquad + 3128z^5 + 2512z^4 + 4000z^3 + 3904z^2\big)\,\Phi(z) \\ &\quad + \big(2048z^{13} + 3072z^{11} + 1536z^{10} + 1152z^9 + 1024z^8 + 4000z^7 + 3440z^6 \\ &\qquad + 3788z^5 + 3096z^4 + 3416z^3 + 2368z^2 + 288z\big)\,\Phi^2(z) \\ &\quad + \big(2048z^{11} + 2048z^{10} + 2304z^9 + 512z^8 + 2752z^7 + 3072z^6 + 728z^5 \\ &\qquad + 3528z^4 + 1032z^3 + 3168z^2 + 3456z + 3904\big)\,\Phi^3(z) \\ &\quad + \Big(2048z^{12} + 3072z^{11} + 1024z^{10} + 2048z^9 + 1152z^8 + 1728z^7 + 2272z^6 + 2464z^5 \\ &\qquad + 3452z^4 + 3154z^3 + 2136z^2 + 3896z + 1600 + \frac{48}{z}\Big)\,\Phi^4(z) \\ &\quad + \Big(2048z^{10} + 2048z^9 + 1792z^8 + 1792z^7 + 1088z^6 + 1536z^5 \\ &\qquad + 1704z^4 + 3648z^3 + 3288z^2 + 200z + 3728 + \frac{2272}{z}\Big)\,\Phi^5(z)\end{aligned}$$

$$
\begin{aligned}
&+ \big(2048z^{11}1024z^9 + 1536z^8 + 3200z^7 + 2816z^6 + 1312z^5 + 3824z^4 \\
&\qquad +140z^3 + 592z^2 + 3692z + 488 + \frac{2760}{z}\Big)\,\Phi^6(z) \\
&+ \big(2048z^9 + 2304z^7 + 2304z^6 + 3520z^5 + 960z^4 + 2456z^3 \\
&\qquad +2128z^2 + 2936z + 1784 + \frac{4024}{z}\Big)\,\Phi^7(z) \\
&+ \big(2048z^{10} + 1024z^9 + 2048z^8 + 512z^7 + 3968z^6 + 1088z^5 + 1888z^4 \\
&\qquad +832z^3 + 1444z^2 + 2646z + 3258 + \frac{339}{z}\Big)\,\Phi^8(z) \\
&+ \big(2048z^8 + 3328z^6 + 1536z^5 + 3008z^4 \\
&\qquad +320z^3 + 2168z^2 + 1144z + 3992 + \frac{3152}{z}\Big)\,\Phi^9(z) \\
&+ \big(2048z^9 + 3072z^7 + 512z^6 + 1408z^5 + 2560z^4 \\
&\qquad +3424z^3 + 3408z^2 + 1316z + 3608 + \frac{2380}{z}\Big)\,\Phi^{10}(z) \\
&+ \big(2048z^7 + 2048z^6 + 2816z^5 + 3072z^4 + 1856z^3 \\
&\qquad +2688z^2 + 1288z + 3880 + \frac{3904}{z}\Big)\,\Phi^{11}(z)
\end{aligned}
$$

$$
\begin{aligned}
&+ \big(2048z^8 + 1024z^7 + 3072z^6 + 2048z^5 + 1408z^4 \\
&\qquad + 2624z^3 + 1440z^2 + 224z + 948 + \frac{358}{z}\Big)\,\Phi^{12}(z) \\
&+ \left(2048z^6 + 2048z^5 + 3328z^4 + 2816z^3 + 1984z^2 + 384z + 2488 + \frac{2384}{z}\right)\Phi^{13}(z) \\
&+ \left(2048z^7 + 1024z^5 + 512z^4 + 2432z^3 + 1792z^2 + 3040z + 336 + \frac{260}{z}\right)\Phi^{14}(z) \\
&+ \left(2048z^5 + 768z^3 + 256z^2 + 64z + 2752 + \frac{2696}{z}\right)\Phi^{15}(z)
\end{aligned}
$$

modulo 4096.

$$
\begin{aligned}
&+ \big(2048z^8 + 1024z^7 + 3072z^6 + 2048z^5 + 1408z^4 \\
&\qquad + 2624z^3 + 1440z^2 + 224z + 948 + \frac{358}{z}\bigg) \Phi^{12}(z) \\
&+ \left(2048z^6 + 2048z^5 + 3328z^4 + 2816z^3 + 1984z^2 + 384z + 2488 + \frac{2384}{z}\right) \Phi^{13}(z) \\
&+ \left(2048z^7 + 1024z^5 + 512z^4 + 2432z^3 + 1792z^2 + 3040z + 336 + \frac{260}{z}\right) \Phi^{14}(z) \\
&+ \left(2048z^5 + 768z^3 + 256z^2 + 64z + 2752 + \frac{2696}{z}\right) \Phi^{15}(z)
\end{aligned}
$$

modulo 4096.

$$
\begin{aligned}
&+ \left(2048z^8 + 1024z^7 + 3072z^6 + 2048z^5 + 1408z^4\right.\\
&\qquad \left.+2624z^3 + 1440z^2 + 224z + 948 + \frac{358}{z}\right) \Phi^{12}(z)\\
&+ \left(2048z^6 + 2048z^5 + 3328z^4 + 2816z^3 + 1984z^2 + 384z + 2488 + \frac{2384}{z}\right) \Phi^{13}(z)\\
&+ \left(2048z^7 + 1024z^5 + 512z^4 + 2432z^3 + 1792z^2 + 3040z + 336 + \frac{260}{z}\right) \Phi^{14}(z)\\
&+ \left(2048z^5 + 768z^3 + 256z^2 + 64z + 2752 + \frac{2696}{z}\right) \Phi^{15}(z)\\
&\qquad \text{modulo } 4096.
\end{aligned}
$$

We have also a procedure for extracting coefficients of powers of $\Phi(z)$.

Subgroup numbers and homomorphism numbers

Subgroup numbers and homomorphism numbers

Given a group G, let $s_n(G)$ denote the number of subgroups of index n in G.

Subgroup numbers and homomorphism numbers

Given a group G, let $s_n(G)$ denote the number of subgroups of index n in G.

How to get a differential equation for $\sum_{n\geq 0} s_{n+1}(G)z^n$*?*

Subgroup numbers and homomorphism numbers

Given a group G, let $s_n(G)$ denote the number of subgroups of index n in G.

How to get a differential equation for $\sum_{n\geq 0} s_{n+1}(G)z^n$?

Theorem (Dey 1965)

We have

$$\sum_{n=0}^{\infty} |\operatorname{Hom}(G, S_n)| \frac{z^n}{n!} = \exp\left(\sum_{n=1}^{\infty} s_n(G)\frac{z^n}{n}\right).$$

$$\sum_{n=0}^{\infty} |\operatorname{Hom}(G, S_n)| \frac{z^n}{n!} = \exp\left(\sum_{n=1}^{\infty} s_n(G) \frac{z^n}{n}\right).$$

$$\sum_{n=0}^{\infty} |\operatorname{Hom}(G, S_n)| \frac{z^n}{n!} = \exp\left(\sum_{n=1}^{\infty} s_n(G) \frac{z^n}{n}\right).$$

Let

$$H(z) := \sum_{n=0}^{\infty} |\operatorname{Hom}(G, S_n)| \frac{z^n}{n!} \quad \text{and} \quad S(z) := \sum_{n=1}^{\infty} s_{n+1}(G) z^n.$$

$$\sum_{n=0}^{\infty} |\operatorname{Hom}(G, S_n)| \frac{z^n}{n!} = \exp\left(\sum_{n=1}^{\infty} s_n(G) \frac{z^n}{n}\right).$$

Let

$$H(z) := \sum_{n=0}^{\infty} |\operatorname{Hom}(G, S_n)| \frac{z^n}{n!} \quad \text{and} \quad S(z) := \sum_{n=1}^{\infty} s_{n+1}(G) z^n.$$

Then

$$\frac{H^{(k)}(z)}{H(z)} = P_k(S(z), S'(z), \dots), \qquad k = 1, 2, \dots,$$

where $P_k(S(z), S'(z), \dots)$ is a polynomial in $S(z)$ and its derivatives.

Hence:
If we have a *linear* differential equation for $H(z)$, via

$$\frac{H^{(k)}(z)}{H(z)} = P_k(S(z), S'(z), \dots), \qquad k = 1, 2, \dots,$$

it translates into a differential equation for $S(z)$.

We may then apply our method to this differential equation for $S(z)$.

Subgroup numbers of $PSL_2(\mathbb{Z})$

Subgroup numbers of $PSL_2(\mathbb{Z})$

The group $PSL_2(\mathbb{Z})$ is freely generated by

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

Hence

$$PSL_2(\mathbb{Z}) = C_2 * C_3 = \left\langle x, y : x^2 = y^3 = 1 \right\rangle.$$

Subgroup numbers of $PSL_2(\mathbb{Z})$

The group $PSL_2(\mathbb{Z})$ is freely generated by

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}.$$

Hence

$$PSL_2(\mathbb{Z}) = C_2 * C_3 = \left\langle x, y : x^2 = y^3 = 1 \right\rangle.$$

Hence:

$$\text{Hom}(PSL_2(\mathbb{Z}), S_n) = h_2(n) \cdot h_3(n),$$

where $h_2(n)$ is the number of involutions in S_n and $h_3(n)$ is the number of permutations of order 3 in S_n.

Subgroup numbers of $PSL_2(\mathbb{Z})$

We have

$$\mathrm{Hom}(PSL_2(\mathbb{Z}), S_n) = h_2(n) \cdot h_3(n).$$

Subgroup numbers of $PSL_2(\mathbb{Z})$

We have

$$\mathrm{Hom}(PSL_2(\mathbb{Z}), S_n) = h_2(n) \cdot h_3(n).$$

It is easy to see (and well-known) that

$$h_2(n) = h_2(n-1) + (n-1)h_2(n-2),$$
$$h_3(n) = h_3(n-1) + (n-1)(n-2)h_3(n-3).$$

These are recurrences with polynomial coefficients.
It is then routine (`gfun`!!) to find a recurrence with polynomial coefficients for the Hadamard product $h_2(n) \cdot h_3(n)$.
It is equally routine (`gfun`!!) to convert this recurrence into a (linear) differential equation with polynomial coefficients for the generating function $\sum_{n\geq 0} \mathrm{Hom}(PSL_2(\mathbb{Z}), S_n)\frac{z^n}{n!}$.

Subgroup numbers of $PSL_2(\mathbb{Z})$

Godsil, Imrich and Razen found

$$(z^7 - z^{10})H''(z) + (-1 + 4z^3 + 2z^4 + 4z^6 - 2z^7 - 4z^9)H'(z) \\ + (1 + z + 4z^2 + 4z^3 - z^4 + 4z^5 - 2z^6 - 2z^8)H(z) = 0.$$

Finally, this is converted into a differential equation for $S(z)$:

$$(-1+4z^3+2z^4+4z^6-2z^7-4z^9)S(z)+(z^7-z^{10})(S'(z)+S^2(z)) \\ + 1 + z + 4z^2 + 4z^3 - z^4 + 4z^5 - 2z^6 - 2z^8 = 0.$$

Theorem

Let $\Phi(z) = \sum_{n\ge 0} z^{2^n}$, *and let* α *be some positive integer. Then the generating function* $S(z) = S_{PSL_2(\mathbb{Z})}(z)$, *when reduced modulo* $2^{3\cdot 2^\alpha}$, *can be expressed as a polynomial in* $\Phi(z)$ *of degree at most* $2^{\alpha+2} - 1$ *with coefficients that are Laurent polynomials in* z*. Moreover, for any given* α, *this polynomial can be found* *automatically*.

(iii) *For λ odd with $\mathfrak{s}_2(\lambda+1)=2$, write $\lambda=2^a+2^b-1, a>b\geq 1$. Then we have*

$$f_\lambda \equiv \begin{cases} 14, & b=1 \\ 6, & b=2 \\ 2, & a=b+1 \\ 6, & a=b+2 \\ 14, & \text{otherwise} \end{cases} \pmod{16}.$$

(iv) *For λ odd with $\mathfrak{s}_2(\lambda+1)=3$, write $\lambda=2^a+2^b+2^c-1$, where $a>b>c\geq 1$. Assume that precisely k of the equations $a=b+1$, and $b=c+1$ hold, $k=0,1,2$. Then we have*

$$f_\lambda \equiv \begin{cases} 4, & k\equiv 0\,(2) \\ 12, & k\equiv 1\,(2) \end{cases} \pmod{16}.$$

(v) *If λ is odd with $\mathfrak{s}_2(\lambda+1)=4$, then $f_\lambda\equiv 8\,(16)$.*

(vi) *If λ is odd with $\mathfrak{s}_2(\lambda+1)\geq 5$, then $f_\lambda\equiv 0\,(16)$.*

The regular behaviour of the function f_λ described in Theorem 1 breaks down for $\lambda<20$. Here the values modulo 16 are as follows.

λ	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
f_λ	5	12	1	0	2	0	5	0	6	0	2	0	4	0	5	0	6	0	6

Theorem 2. *Let $n\geq 22$ be an integer. Then we have modulo 8*

$$s_n \equiv \begin{cases} 1, & n=2^a-3 \\ 5, & n=2^a-6 \\ 2, & n=3\cdot 2^a-3, 3\cdot 2^a-6 \\ 6, & n=2^a+2^b-3, 2^a+2^b-6, 2^a+3,\ a\geq b+2 \\ 4, & n=2^a+2^b+2^c-6, a>b>c\geq 2, 2^a+2^b+2^c-3, a>b>c\geq 2, b\geq 4, \\ & n=2^a+2^b+3, a>b\geq 2 \\ 0, & \textit{otherwise.} \end{cases}$$

Theorem

Let $\Phi(z) = \sum_{n\ge 0} z^{2^n}$. *Then, modulo* 64, *we have*

$$\begin{aligned}
&\sum_{n\ge 0} s_{n+1}(PSL_2(\mathbb{Z}))\, z^n \\
&= z^{57} + 32z^{50} + 48z^{44} + 48z^{41} + 32z^{36} + 32z^{35} + 32z^{33} + 48z^{32} + 16z^{28} + 40z^{26} \\
&\quad + 16z^{25} + 32z^{24} + 32z^{23} + 16z^{22} + 16z^{21} + 52z^{20} + 32z^{19} + 40z^{18} \\
&\quad + 60z^{17} + 48z^{16} + 4z^{14} + 32z^{13} + 4z^{12} + 36z^{11} + 16z^{10} + 60z^{9} + 2z^{8} + 16z^{7} \\
&\quad + 4z^{6} + 60z^{5} + 44z^{4} + 16z^{3} + 54z^{2} + 60z + 32 + \frac{56}{z} + \frac{36}{z^2} + \frac{51}{z^3} + \frac{33}{z^4} + \frac{52}{z^5} \\
&\quad + \Big(32z^{34} + 32z^{26} + 32z^{25} + 32z^{24} + 16z^{22} + 32z^{21} + 32z^{20} + 32z^{17} + 32z^{16} \\
&\quad + 48z^{14} + 16z^{13} + 16z^{12} + 16z^{11} + 32z^{10} + 32z^{8} + 48z^{7} + 8z^{5} + 8z^{4} + 48z^{3} + 24z + 32 \\
&\quad + \frac{20}{z} + \frac{12}{z^2} + \frac{8}{z^3} + \frac{36}{z^4} + \frac{4}{z^5} + \frac{24}{z^6}\Big)\Phi(z) \\
&\quad + \Big(32z^{34} + 32z^{29} + 32z^{28} + 32z^{26} + 32z^{24} + 32z^{21} + 48z^{19} + 32z^{18} + 48z^{17} + 32z^{14} \\
&\quad + 48z^{13} + 32z^{12} + 56z^{10} + 8z^{9} + 16z^{8} + 48z^{7} + 24z^{6} + 56z^{5} + 44z^{4} + 16z^{3} \\
&\quad + 48z^{2} + 40z + 44 + \frac{60}{z} + \frac{50}{z^2} + \frac{48}{z^3} + \frac{8}{z^4} + \frac{50}{z^5} + \frac{52}{z^6} + \frac{52}{z^7}\Big)\Phi^2(z)
\end{aligned}$$

$$
\begin{aligned}
&+\Big(32z^{28}+32z^{24}+32z^{21}+32z^{20}+32z^{19}+48z^{16}+32z^{14}+32z^{13}+32z^{12}\\
&+32z^{11}+16z^{10}+48z^{9}+8z^{8}+48z^{6}+56z^{4}+8z^{3}+16z^{2}+48z+56+\frac{32}{z}+\frac{20}{z^2}\\
&+\frac{52}{z^3}+\frac{4}{z^4}+\frac{36}{z^5}+\frac{12}{z^6}+\frac{36}{z^7}\Big)\Phi^3(z)\\
&+\Big(32z^{44}+32z^{41}+32z^{33}+32z^{32}+32z^{31}+32z^{30}+32z^{28}+32z^{27}+16z^{26}+32z^{24}\\
&+32z^{23}+48z^{22}+16z^{21}+40z^{20}+32z^{19}+32z^{18}+24z^{17}+16z^{16}+48z^{15}+32z^{14}\\
&+16z^{13}+8z^{12}+32z^{11}+56z^{10}+56z^{9}+44z^{8}+40z^{7}+48z^{6}+16z^{5}+20z^{4}+56z^{3}+30z^{2}\\
&+32z+28+\frac{40}{z}+\frac{34}{z^2}+\frac{52}{z^3}+\frac{17}{z^4}+\frac{26}{z^5}+\frac{40}{z^6}+\frac{29}{z^7}\Big)\Phi^4(z)\\
&+\Big(32z^{32}+32z^{30}+32z^{26}+32z^{24}+32z^{23}+32z^{22}+32z^{21}+48z^{20}+48z^{18}+32z^{16}+48z^{14}\\
&+32z^{13}+48z^{12}+48z^{11}+32z^{8}+16z^{7}+56z^{6}+48z^{5}+48z^{4}+40z^{3}+16z^{2}\\
&+32z+56+\frac{24}{z}+\frac{24}{z^2}+\frac{20}{z^3}+\frac{24}{z^4}+\frac{40}{z^5}+\frac{20}{z^6}\Big)\Phi^5(z)
\end{aligned}
$$

$$
\begin{aligned}
&+\Big(32z^{32}+32z^{31}+32z^{30}+32z^{27}+32z^{24}+32z^{23}+48z^{19}+16z^{18}+48z^{17}\\
&\quad+16z^{15}+48z^{14}+32z^{12}+32z^{11}+56z^{8}+40z^{7}+56z^{6}+16z^{5}\\
&\quad+8z^{4}+56z^{3}+4z^{2}+56z+32+\frac{8}{z}+\frac{52}{z^2}+\frac{60}{z^3}+\frac{30}{z^4}+\frac{20}{z^5}+\frac{20}{z^6}+\frac{14}{z^7}\Big)\Phi^6(z)\\
&+\Big(32z^{30}+32z^{26}+32z^{21}+32z^{20}+48z^{18}+32z^{16}+48z^{14}+32z^{13}+48z^{10}+16z^{9}+8z^{6}\\
&\quad+32z^{5}+16z^{4}+16z^{3}+8z^{2}+48z+40+\frac{48}{z}+\frac{8}{z^2}+\frac{40}{z^3}+\frac{60}{z^4}+\frac{8}{z^5}+\frac{24}{z^6}+\frac{60}{z^7}\Big)\Phi^7(z)\\
&\qquad\text{modulo } 64.
\end{aligned}
$$

What about the homogeneous modular group $SL_2(\mathbb{Z})$?

What about the homogeneous modular group $SL_2(\mathbb{Z})$?

Here, we have

$$SL_2(\mathbb{Z}) = \left\langle x, y : x^4 = y^6 = 1 \text{ and } x^2 = y^3 \right\rangle .$$

What about the homogeneous modular group $SL_2(\mathbb{Z})$?

Here, we have

$$SL_2(\mathbb{Z}) = \left\langle x, y : x^4 = y^6 = 1 \text{ and } x^2 = y^3 \right\rangle .$$

One can show that

$$\operatorname{Hom}(SL_2(\mathbb{Z}), S_n) = n! \sum_{r=0}^{\lfloor n/4 \rfloor} \sum_{s=0}^{\lfloor 2r/3 \rfloor} \frac{(2r)!\, h_2(n-4r) h_3(n-4r)}{2^{2(r-s)} 3^s r!\, s!\, (n-4r)!\, (2r-3s)!}.$$

We found and used a recurrence of order 50 and polynomial coefficients of degree 5 for $\operatorname{Hom}(SL_2(\mathbb{Z}), S_n)$. This translates into a differential equation for the generating function $S(z) := \sum_{n\ge0} s_{n+1}(SL_2)(\mathbb{Z})$, with $S(z), S'(z), S''(z), S'''(z), S''''(z)$ appearing.

What about the homogeneous modular group $SL_2(\mathbb{Z})$?

Here, we have

$$SL_2(\mathbb{Z}) = \left\langle x, y : x^4 = y^6 = 1 \text{ and } x^2 = y^3 \right\rangle .$$

One can show that

$$\mathrm{Hom}(SL_2(\mathbb{Z}), S_n) = n! \sum_{r=0}^{\lfloor n/4 \rfloor} \sum_{s=0}^{\lfloor 2r/3 \rfloor} \frac{(2r)!\, h_2(n-4r) h_3(n-4r)}{2^{2(r-s)} 3^s r!\, s!\, (n-4r)!\, (2r-3s)!} .$$

We found and used a recurrence of order 50 and polynomial coefficients of degree 5 for $\mathrm{Hom}(SL_2(\mathbb{Z}), S_n)$. This translates into a differential equation for the generating function $S(z) := \sum_{n \geq 0} s_{n+1}(SL_2)(\mathbb{Z})$, with $S(z), S'(z), S''(z), S'''(z), S''''(z)$ appearing.
The method works for this differential equation up to modulus 8.
It does not work for modulus 16!

Theorem

Let $\Phi(z) = \sum_{n\ge 0} z^{2^n}$. Then we have

$$
\begin{aligned}
\sum_{n\ge 0} s_{n+1}(SL_2(\mathbb{Z}))\, z^n
&= 4z^{20} + 4z^{17} + 4z^{14} + 4z^{12} + 4z^{10} + 4z^9 + 6z^8 + 4z^5 + 6z^4 + 4z^2 + 4z + 6 \\
&\quad + \frac{7}{z^2} + \frac{3}{z^3} + \frac{6}{z^6} + \frac{6}{z^7} + \frac{4}{z^8} + \frac{1}{z^9} + \frac{3}{z^{11}} + \frac{6}{z^{12}} \\
&\quad + \left(\frac{2}{z^{13}} + \frac{6}{z^{12}} + \frac{4}{z^{10}} + \frac{4}{z^9} + \frac{4}{z^8} + \frac{2}{z^7} + \frac{6}{z^6} + \frac{6}{z^4} + 4z^3 + \frac{6}{z^3} + 4z^2 + \frac{4}{z}\right)\Phi(z) \\
&\quad + \Bigg(4z^8 + 4z^4 + 4z^3 + 6z^2 + 4 + \frac{4}{z} + \frac{6}{z^2} + \frac{2}{z^3} + \frac{5}{z^4} + \frac{2}{z^5} \\
&\qquad + \frac{6}{z^6} + \frac{1}{z^7} + \frac{4}{z^8} + \frac{6}{z^9} + \frac{4}{z^{10}} + \frac{6}{z^{11}} + \frac{6}{z^{12}} + \frac{5}{z^{13}}\Bigg)\Phi^2(z) \\
&\quad + \left(4z^2 + \frac{4}{z^2} + \frac{4}{z^3} + \frac{2}{z^4} + \frac{4}{z^5} + \frac{4}{z^6} + \frac{2}{z^7} + \frac{4}{z^9} + \frac{4}{z^{11}} + \frac{4}{z^{12}} + \frac{2}{z^{13}}\right)\Phi^3(z) \\
&\qquad \text{modulo } 8.
\end{aligned}
$$

Theorem

The subgroup numbers $s_n(SL_2(\mathbb{Z}))$ *obey the following congruences modulo* 8 :

Theorem

The subgroup numbers $s_n(SL_2(\mathbb{Z}))$ *obey the following congruences modulo* 8 :

(i) $s_n(SL_2(\mathbb{Z})) \equiv 1 \pmod 8$ *if, and only if,* $n = 1, 2, 4, 10$, *or if* n *is of the form* $2^\sigma - 3$ *for some* $\sigma \geq 4$;

Theorem

The subgroup numbers $s_n(SL_2(\mathbb{Z}))$ *obey the following congruences modulo* 8 :

(i) $s_n(SL_2(\mathbb{Z})) \equiv 1 \pmod 8$ *if, and only if,* $n = 1, 2, 4, 10$, *or if* n *is of the form* $2^\sigma - 3$ *for some* $\sigma \geq 4$;

(ii) $s_n(SL_2(\mathbb{Z})) \equiv 2 \pmod 8$ *if, and only if,* $n = 7, 12, 17$, *or if* n *is of one of the forms*

$$3 \cdot 2^\sigma - 3,\ 3 \cdot 2^\sigma - 6,\ 3 \cdot 2^\sigma - 12, \quad \textit{for some } \sigma \geq 4;$$

Theorem

The subgroup numbers $s_n(SL_2(\mathbb{Z}))$ obey the following congruences modulo 8 :

(i) $s_n(SL_2(\mathbb{Z})) \equiv 1 \pmod 8$ *if, and only if,* $n = 1, 2, 4, 10$, *or if n is of the form* $2^\sigma - 3$ *for some* $\sigma \geq 4$;

(ii) $s_n(SL_2(\mathbb{Z})) \equiv 2 \pmod 8$ *if, and only if,* $n = 7, 12, 17$, *or if n is of one of the forms*

$$3 \cdot 2^\sigma - 3,\ 3 \cdot 2^\sigma - 6,\ 3 \cdot 2^\sigma - 12, \quad \text{for some } \sigma \geq 4;$$

(iii) $s_n(SL_2(\mathbb{Z})) \equiv 4 \pmod 8$ *if, and only if,* $n = 3, 22, 23, 27, 46, 47, 51$, *or if n is of one of the forms*

$$\begin{gathered}
2^\sigma + 6,\ 2^\sigma + 7,\ 2^\sigma + 11,\ 2^\sigma + 12,\ 2^\sigma + 18, \\
2^\sigma + 21, \quad \text{for some } \sigma \geq 5, \\
2^\sigma + 2^\tau - 2,\ 2^\sigma + 2^\tau + 1,\ 2^\sigma + 2^\tau + 3, \\
\text{for some } \sigma, \tau \text{ with } \sigma \geq 6 \text{ and } 4 \leq \tau \leq \sigma - 1, \\
2^\sigma + 2^\tau + 2^\nu - 12,\ 2^\sigma + 2^\tau + 2^\nu - 6,\ 2^\sigma + 2^\tau + 2^\nu - 3, \\
\text{for some } \sigma, \tau, \nu \text{ with } \sigma \geq 6,\ 5 \leq \nu \leq \sigma - 1, \text{ and } 3 \leq \tau \leq \nu - 1;
\end{gathered}$$

(iv) $s_n(SL_2(\mathbb{Z})) \equiv 5 \pmod 8$ *if, and only if,* $n = 5$, *or if* n *is of one of the forms*

$$2^\sigma - 6,\ 2^\sigma - 12, \quad \textit{for some } \sigma \geq 5;$$

(iv) $s_n(SL_2(\mathbb{Z})) \equiv 5 \pmod 8$ *if, and only if,* $n = 5$, *or if* n *is of one of the forms*

$$2^\sigma - 6,\ 2^\sigma - 12, \quad \textit{for some } \sigma \geq 5;$$

(v) $s_n(SL_2(\mathbb{Z})) \equiv 6 \pmod 8$ *if, and only if,* $n = 6, 11, 14, 18, 19, 21, 33, 34, 35, 37$, *or if* n *is of one of the forms*

$$\begin{aligned}
&2^\sigma - 2,\ 2^\sigma - 4, \quad \textit{for some } \sigma \geq 5,\\
&2^\sigma + 1,\ 2^\sigma + 2,\ 2^\sigma + 3,\ 2^\sigma + 4,\ 2^\sigma + 5,\ 2^\sigma + 10,\ 2^\sigma + 13,\\
&\qquad\qquad\qquad \textit{for some } \sigma \geq 6,\\
&2^\sigma + 2^\tau - 3,\ 2^\sigma + 2^\tau - 6,\ 2^\sigma + 2^\tau - 12,\\
&\qquad\qquad\qquad \textit{for some } \sigma, \tau \textit{ with } \sigma \geq 7 \textit{ and } 5 \leq \tau \leq \sigma - 2;
\end{aligned}$$

(iv) $s_n(SL_2(\mathbb{Z})) \equiv 5 \pmod 8$ *if, and only if,* $n = 5$, *or if* n *is of one of the forms*

$$2^\sigma - 6,\ 2^\sigma - 12, \quad \text{for some } \sigma \geq 5;$$

(v) $s_n(SL_2(\mathbb{Z})) \equiv 6 \pmod 8$ *if, and only if,* $n = 6, 11, 14, 18, 19, 21, 33, 34, 35, 37$, *or if* n *is of one of the forms*

$$\begin{aligned}
&2^\sigma - 2,\ 2^\sigma - 4, \quad \text{for some } \sigma \geq 5,\\
&2^\sigma + 1,\ 2^\sigma + 2,\ 2^\sigma + 3,\ 2^\sigma + 4,\ 2^\sigma + 5,\ 2^\sigma + 10,\ 2^\sigma + 13,\\
&\qquad\qquad\qquad\qquad \text{for some } \sigma \geq 6,\\
&2^\sigma + 2^\tau - 3,\ 2^\sigma + 2^\tau - 6,\ 2^\sigma + 2^\tau - 12,\\
&\qquad\qquad\qquad\qquad \text{for some } \sigma, \tau \text{ with } \sigma \geq 7 \text{ and } 5 \leq \tau \leq \sigma - 2;
\end{aligned}$$

(vi) *in the cases not covered by items* (i)–(v), $s_n(SL_2(\mathbb{Z}))$ *is divisible by* 8; *in particular,* $s_n(SL_2(\mathbb{Z})) \not\equiv 3, 7 \pmod 8$ *for all* n.

Epilogue

Epilogue

- What about other primes?

Epilogue

- What about other primes?
  The whole theory can also be developed for other primes. It works without any problem for *Fuß–Catalan numbers*. However, otherwise we are aware of just one (moderately) interesting example (for the prime 3).

Epilogue

- What about other primes?
  The whole theory can also be developed for other primes. It works without any problem for *Fuß–Catalan numbers*.
  However, otherwise we are aware of just one (moderately) interesting example (for the prime 3).
- Then how do the subgroup numbers of $PSL_2(\mathbb{Z})$ or of $SL_2(\mathbb{Z})$ behave modulo 3 or larger prime numbers?

Epilogue

- What about other primes?
  The whole theory can also be developed for other primes. It works without any problem for *Fuß–Catalan numbers*.
  However, otherwise we are aware of just one (moderately) interesting example (for the prime 3).
- Then how do the subgroup numbers of $PSL_2(\mathbb{Z})$ or of $SL_2(\mathbb{Z})$ behave modulo 3 or larger prime numbers?
  We do not know ...

Epilogue

- What about other primes?
  The whole theory can also be developed for other primes. It works without any problem for *Fuß–Catalan numbers*. However, otherwise we are aware of just one (moderately) interesting example (for the prime 3).
- Then how do the subgroup numbers of $PSL_2(\mathbb{Z})$ or of $SL_2(\mathbb{Z})$ behave modulo 3 or larger prime numbers?
  We do not know ...
- There are situations where the modular behaviour can be described using other "basic series," for example (this applies to *Motzkin numbers* modulo 3) by the series

$$\Psi(z) = \sum_{k \geq 0} \sum_{n_1 > \cdots > n_k > 0} z^{\sum_{i=1}^{k} 3^{n_i}} = \prod_{j=1}^{\infty} (1 + z^{3^j}).$$

  We are currently developing a theory for this series.