A (semi-) automatic method for the determination of differentially algebraic integer sequences modulo powers of 2 and 3

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?

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?

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?

What can we say about the value of a_n modulo 3^k?

Congruences modulo powers of 2

Congruences modulo powers of 2

Example: Catalan numbers

The *Catalan numbers* are the numbers

$$\mathrm{Cat}_n = \frac{1}{n+1}\binom{2n}{n}, \qquad n = 1, 2, 3, \dots .$$

Congruences modulo powers of 2

Example: Catalan numbers

The *Catalan numbers* are the numbers

$$\operatorname{Cat}_n = \frac{1}{n+1}\binom{2n}{n}, \qquad n = 1, 2, 3, \dots .$$

The first few numbers are

$$1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786, 208012,$$
$$742900, 2674440, 9694845, 35357670, 129644790, 477638700,$$
$$1767263190, 6564120420, \dots .$$

Congruences modulo powers of 2

Example: Catalan numbers

The *Catalan numbers* are the numbers

$$\mathrm{Cat}_n = \frac{1}{n+1}\binom{2n}{n}, \qquad n = 1, 2, 3, \dots .$$

The first few numbers are

$$1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786, 208012,\\ 742900, 2674440, 9694845, 35357670, 129644790, 477638700,\\ 1767263190, 6564120420, \dots .$$

What can we say modulo 2?

Congruences modulo powers of 2

Example: Catalan numbers

The *Catalan numbers* are the numbers

$$\mathrm{Cat}_n = \frac{1}{n+1}\binom{2n}{n}, \qquad n = 1, 2, 3, \dots .$$

The first few numbers are

$$1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786, 208012, \\ 742900, 2674440, 9694845, 35357670, 129644790, 477638700, \\ 1767263190, 6564120420, \dots .$$

What can we say modulo 2?
The Catalan numbers are odd for $n = 1, 3, 7, 15, \dots$.

Congruences modulo powers of 2

Example: Catalan numbers

The *Catalan numbers* are the numbers

$$\mathrm{Cat}_n = \frac{1}{n+1}\binom{2n}{n}, \qquad n = 1, 2, 3, \dots .$$

The first few numbers are

$$1, 2, 5, 14, 42, 132, 429, 1430, 4862, 16796, 58786, 208012,$$
$$742900, 2674440, 9694845, 35357670, 129644790, 477638700,$$
$$1767263190, 6564120420, \dots .$$

What can we say modulo 2?
The Catalan numbers are odd for $n = 1, 3, 7, 15, \dots$.
Guess: The Catalan number Cat_n is odd if and only if $n = 2^s - 1$, for some non-negative integer s.

Guess: The Catalan number Cat_n is odd if and only if $n = 2^s - 1$, for some non-negative integer s.

Guess: The Catalan number Cat_n is odd if and only if $n = 2^s - 1$, for some non-negative integer s.

A trivial[©] proof. Everybody knows that the generating function $C(z) = \sum_{n \geq 0} \mathrm{Cat}_n z^n$ for the Catalan numbers satisfies

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

In terms of generating functions, our guess is equivalent to

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

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

[©] Doron Zeilberger: A computer can do this!

Guess: The Catalan number Cat_n is odd if and only if $n = 2^s - 1$, for some non-negative integer s.

A trivial[©] **proof.** Everybody knows that the generating function $C(z) = \sum_{n \ge 0} \mathrm{Cat}_n \, z^n$ for the Catalan numbers satisfies

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

In terms of generating functions, our guess is equivalent to

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

where $\Phi(z) = \sum_{s \ge 0} z^{2^s} = z + z^2 + z^4 + z^8 + z^{16} + \cdots$.
To prove the guess, we substitute in the equation and reduce:

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

[©] Doron Zeilberger: A computer can do this!

What about Catalan numbers modulo $4, 8, 16, \ldots$?

What about Catalan numbers modulo $4, 8, 16, \ldots$?

Maybe, after reduction modulo 2^k, the generating function $C(z) = \sum_{n \geq 0} \mathrm{Cat}_n \, z^n$ is expressible as a polynomial in $\Phi(z)$,

$$C(z) = \sum_{i=0}^{d} a_i(z) \Phi^i(z),$$

where the $a_i(z)$ are suitable Laurent polynomials in z, and d is a suitable degree bound.

What about Catalan numbers modulo $4, 8, 16, \ldots$?

Maybe, after reduction modulo 2^k, the generating function $C(z) = \sum_{n \geq 0} \mathrm{Cat}_n \, z^n$ is expressible as a polynomial in $\Phi(z)$,

$$C(z) = \sum_{i=0}^{d} a_i(z) \Phi^i(z),$$

where the $a_i(z)$ are suitable Laurent polynomials in z, and d is a suitable degree bound.

Recall that

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

Hence,

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

So, we may choose $d = 2k - 1$.

What about Catalan numbers modulo $4, 8, 16, \dots$?

Maybe, after reduction modulo 2^k, the generating function $C(z) = \sum_{n\ge 0} \mathrm{Cat}_n\, z^n$ is expressible as a polynomial in $\Phi(z)$,

$$C(z) = \sum_{i=0}^{2k-1} a_i(z)\Phi^i(z),$$

where the $a_i(z)$ are suitable Laurent polynomials in z,

What about Catalan numbers modulo $4, 8, 16, \ldots$?

Maybe, after reduction modulo 2^k, the generating function $C(z) = \sum_{n \geq 0} \mathrm{Cat}_n \, z^n$ is expressible as a polynomial in $\Phi(z)$,

$$C(z) = \sum_{i=0}^{2k-1} a_i(z) \Phi^i(z),$$

where the $a_i(z)$ are suitable Laurent polynomials in z,

This Ansatz is then substituted for $C(z)$ in the equation

$$zC^2(z) - C(z) + 1 = 0 \quad \text{modulo } 2.$$

One reduces “high” powers of $\Phi(z)$ by the relation

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

compares coefficients of powers $\Phi^j(z)$, $j = 0, 1, ;2k - 1$, obtains a system of (algebraic) equations for the unknowns $a_i(z)$ over $\mathbb{Z}/2^k\mathbb{Z}$, and ....

What about congruences modulo higher powers of 2?

Well . . .

What about congruences modulo higher powers of 2?

Well . . .

The proposed approach has two problems:

1. The relation
$$(\Phi^2(z) - \Phi(z) - z)^k = 0 \quad \text{modulo } 2^k.$$
may not be the "minimal" one. In fact, we have
$$\Phi^4(z)+6\Phi^3(z)+(2z+3)\Phi^2(z)+(2z+6)\Phi(z)+2z+5z^2 = 0 \quad \text{modulo } 8.$$

What about congruences modulo higher powers of 2?

Well . . .

The proposed approach has two problems:

1. The relation
$$(\Phi^2(z) - \Phi(z) - z)^k = 0 \quad \text{modulo } 2^k.$$
may not be the "minimal" one. In fact, we have
$$\Phi^4(z)+6\Phi^3(z)+(2z+3)\Phi^2(z)+(2z+6)\Phi(z)+2z+5z^2 = 0 \quad \text{modulo } 8.$$
2. Solving a system of (algebraic-differential) equations over $\mathbb{Z}/2^k\mathbb{Z}$ is not a piece of a cake . . . .

What about congruences modulo higher powers of 2?

Re 1). In general, we are not able to provide a formula for a monic polynomial of minimal degree satisfied by $\Phi(z)$ modulo 2^k. (More on this later.)

So, as a "best" compromise, we base our considerations on the congruence

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

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

The "method" for proving congruences modulo 2^k

Re 2). The general problem. Suppose we have a sequence $(f_n)_{n\ge0}$ which we want to determine modulo a power of 2. We form the generating function $F(z)=\sum_{n\ge0} f_n z^n$, 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.

The "method" for proving congruences modulo 2^k

Re 2). The general problem. Suppose we have a sequence $(f_n)_{n\geq 0}$ which we want to determine modulo a power of 2. We form the generating function $F(z)=\sum_{n\geq 0} f_n z^n$, 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.

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

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

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.

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:

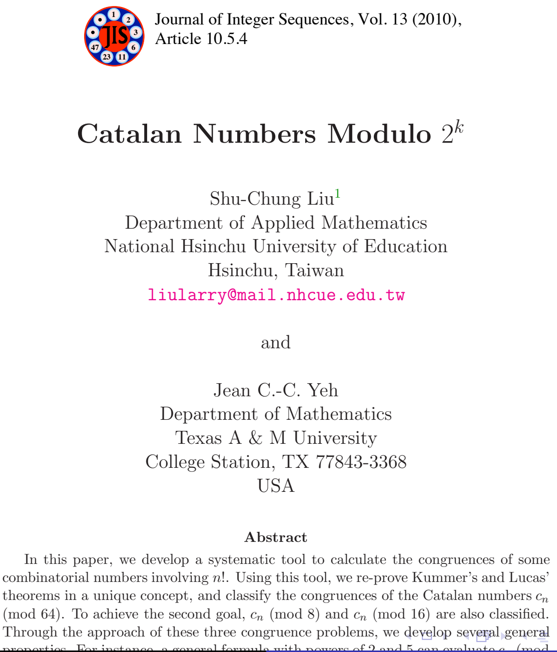
We have

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

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

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

Theorem

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

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

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

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

modulo 4096.

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

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

modulo 4096.

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

Subgroup numbers modulo powers of 2

Subgroup numbers modulo powers of 2

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 $k \geq 2$.

Subgroup numbers modulo powers of 2

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 $k \geq 2$.

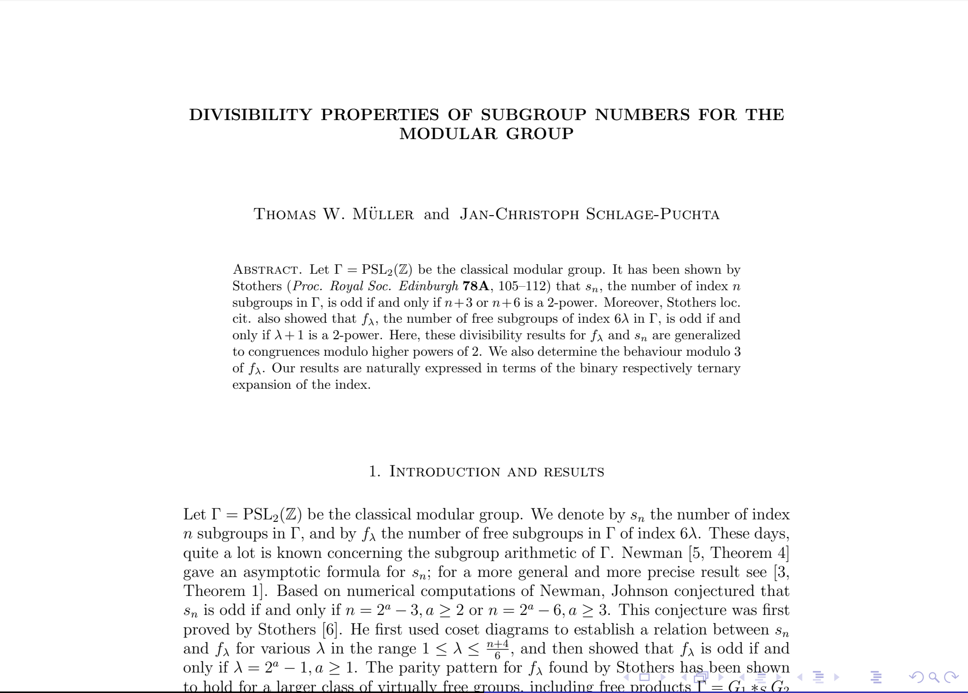
Subgroup numbers modulo powers of 2

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 terms of $\Phi(z)$:

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



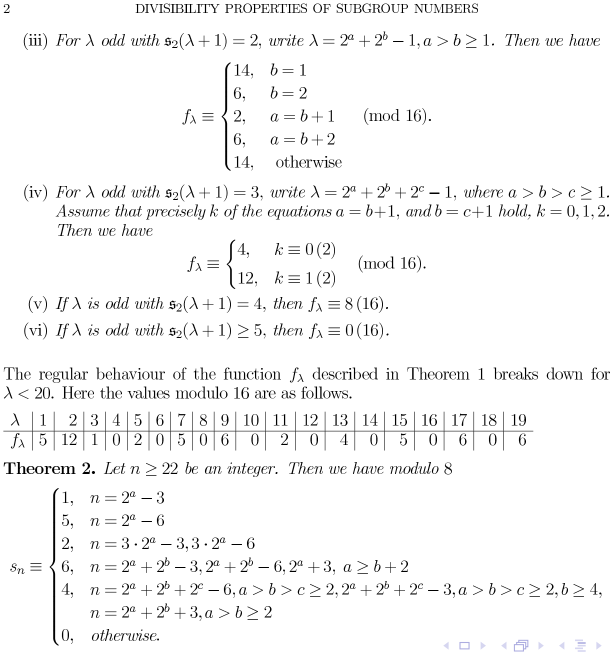
DIVISIBILITY PROPERTIES OF SUBGROUP NUMBERS FOR THE MODULAR GROUP

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 $\lambda=2^a+2^b-1, a>b\geq 1$. 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*

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

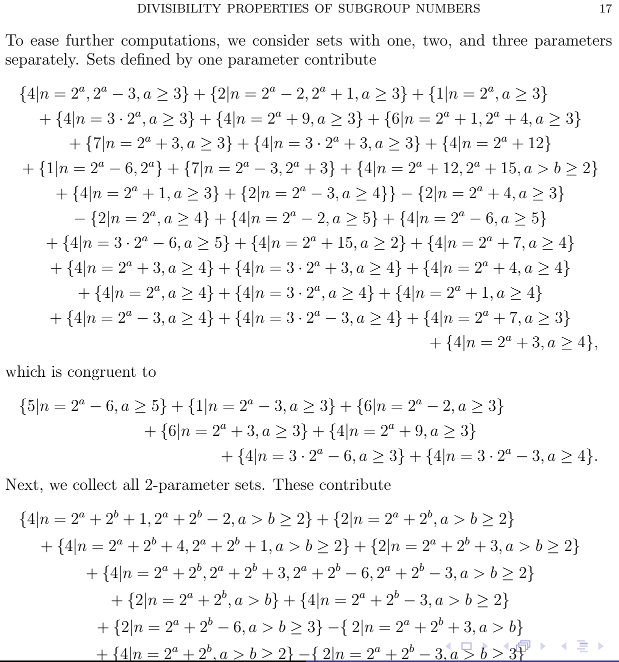
In this way we may simplify the last displayed expression as follows.

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

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

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

Finally, consider the quantity $\#\{n=2^a+2^b+2^c, b>c\ge 2, a\ge 2\}$. 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

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

which is congruent to

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

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

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

In terms of the series $\Phi(z)$, the result of Müller and Schlage–Puchta can be compactly expressed in the form

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

Subgroup numbers modulo powers of 2

Let $S(z)=\sum_{n\ge 0} s_{n+1}z^n$ be the generating function for the subgroups numbers of $PSL_2(\mathbb{Z})$. Then Godsil, Imrich and Razen found the differential equation

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

Subgroup numbers modulo powers of 2

Let $S(z) = \sum_{n\ge0} s_{n+1} z^n$ be the generating function for the subgroups numbers of $PSL_2(\mathbb{Z})$. Then Godsil, Imrich and Razen found the differential equation

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

Theorem

Let $\Phi(z) = \sum_{n\ge0} z^{2^n}$, and let α be some positive integer. Then the generating function $S(z) = S_{PSL_2(\mathbb{Z})}(z)$, when reduced modulo $2^{3\cdot2^\alpha}$, 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.

Theorem

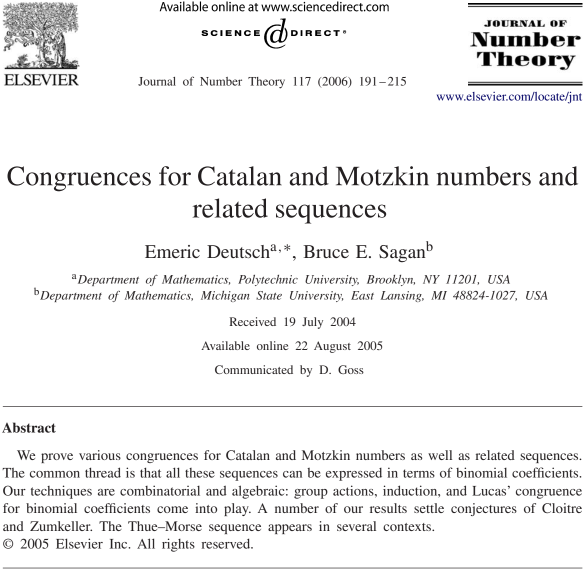
Let $\Phi(z) = \sum_{n\geq 0} z^{2^n}$*. Then, modulo* 64*, we have*

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

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

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

Congruences modulo powers of 3



Available online at www.sciencedirect.com

SCIENCE DIRECT®

Journal of Number Theory 117 (2006) 191–215

JOURNAL OF Number Theory

www.elsevier.com/locate/jnt

Congruences for Catalan and Motzkin numbers and related sequences

Emeric Deutsch[a,*], Bruce E. Sagan[b]

[a] *Department of Mathematics, Polytechnic University, Brooklyn, NY 11201, USA*
[b] *Department of Mathematics, Michigan State University, East Lansing, MI 48824-1027, USA*

Received 19 July 2004

Available online 22 August 2005

Communicated by D. Goss

Abstract

We prove various congruences for Catalan and Motzkin numbers as well as related sequences. The common thread is that all these sequences can be expressed in terms of binomial coefficients. Our techniques are combinatorial and algebraic: group actions, induction, and Lucas' congruence for binomial coefficients come into play. A number of our results settle conjectures of Cloitre and Zumkeller. The Thue–Morse sequence appears in several contexts.

Central trinomial coefficients modulo 3

Theorem (Deutsch and Sagan)

Let T_n denote the n-th central trinomial coefficient, that is, the coefficient of z^n in $(1+z+z^2)^n$. Then

$$T_n \equiv \begin{cases} 1 \pmod 3, & \text{if } n \in T(01), \\ 0 \pmod 3, & \text{otherwise}. \end{cases}$$

Here, $T(01)$ denotes the set of all positive integers n, which have only digits 0 and 1 in their ternary expansion.

Motzkin numbers modulo 3

Theorem (Deutsch and Sagan)

The Motzkin numbers M_n satisfy

$$M_n \equiv \begin{cases} 1 \pmod 3, & \text{if } n \in 3T(01) \text{ or } n \in 3T(01)-2, \\ -1 \pmod 3, & \text{if } n \in 3T(01)-1, \\ 0 \pmod 3, & \text{otherwise}. \end{cases}$$

Here, $T(01)$ denotes the set of all positive integers n, which have only digits 0 and 1 in their ternary expansion.

Central binomial coefficients modulo 3

Theorem (Deutsch and Sagan)

The central binomial coefficients satisfy

$$\binom{2n}{n} \equiv \begin{cases} (-1)^{\delta_3(n)} \pmod 3, & \textit{if } n \in T(01), \\ 0 \pmod 3, & \textit{otherwise}. \end{cases}$$

Here, $T(01)$ denotes the set of all positive integers n, which have only digits 0 and 1 in their ternary expansion, and $\delta_3(n)$ denotes the number of 1s in the ternary expansion of n.

Catalan numbers modulo 3

Theorem (Deutsch and Sagan)

The Catalan numbers C_n satisfy

$$C_n \equiv \begin{cases} (-1)^{\delta_3^*(n+1)} \pmod 3, & \text{if } n \in T^*(01)-1, \\ 0 \pmod 3, & \text{otherwise.} \end{cases}$$

Here, $T^*(01)$ denotes the set of all positive integers n, where all digits in their ternary expansion are 0 or 1 except for the right-most digit, and $\delta_3^*(n)$ denotes the number of 1s in the ternary expansion of n ignoring the right-most digit.

Central Eulerian numbers modulo 3

Let $A(n,k)$ denote the number of permutations of $\{1,2,\ldots,n\}$ with exactly $k-1$ descents.

Theorem (Deutsch and Sagan)

The central Eulerian numbers $A(2n-1,n)$ and $A(2n,n)$ satisfy

$$A(2n-1,n) \equiv \begin{cases} 1 \pmod 3, & \text{if } n \in T(01)+1, \\ 0 \pmod 3, & \text{otherwise.} \end{cases}$$

and

$$A(2n,n) \equiv \begin{cases} 1 \pmod 3, & \text{if } n \in T(01)+1, \\ -1 \pmod 3, & \text{if } n \in T(01) \text{ or } n \in T(01)+2, \\ 0 \pmod 3, & \text{otherwise.} \end{cases}$$

Here, $T(01)$ denotes the set of all positive integers n, which have only digits 0 and 1 in their ternary expansion.

The paper by Deutsch and Sagan contains results of similar nature for *Motzkin prefix numbers*, *Riordan numbers*, *sums of central binomial coefficients*, *central Delannoy numbers*, *Schröder numbers*, and *hex tree numbers*.

Let us have another look at the central trinomial numbers theorem:

Theorem (Deutsch and Sagan)

Let T_n denote the n-th central trinomial coefficient, that is, the coefficient of z^n in $(1+z+z^2)^n$. Then

$$T_n \equiv \begin{cases} 1 \pmod 3, & \text{if } n \in T(01), \\ 0 \pmod 3, & \text{otherwise}, \end{cases}$$

where $T(01)$ denotes the set of all positive integers n, which have only digits 0 and 1 in their ternary expansion.

Let us have another look at the central trinomial numbers theorem:

Theorem (Deutsch and Sagan)

Let T_n denote the n-th central trinomial coefficient, that is, the coefficient of z^n in $(1+z+z^2)^n$. Then

$$T_n \equiv \begin{cases} 1 \pmod 3, & \textit{if } n \in T(01), \\ 0 \pmod 3, & \textit{otherwise}, \end{cases}$$

where $T(01)$ denotes the set of all positive integers n, which have only digits 0 and 1 in their ternary expansion.

Let us have another look at the central trinomial numbers theorem:

Theorem (Deutsch and Sagan)

Let T_n denote the n-th central trinomial coefficient, that is, the coefficient of z^n in $(1+z+z^2)^n$. Then

$$T_n \equiv \begin{cases} 1 \pmod 3, & \text{if } n \in T(01), \\ 0 \pmod 3, & \text{otherwise}, \end{cases}$$

where $T(01)$ denotes the set of all positive integers n, which have only digits 0 and 1 in their ternary expansion.

In other words: Let

$$\Psi(z) = \sum_{k \geq 0} \sum_{n_1 > \cdots > n_k \geq 0} z^{3^{n_1}+3^{n_2}+\cdots+3^{n_k}} = \prod_{j=0}^{\infty} (1 + z^{3^j})$$
$$= 1 + z + z^3 + z^4 + z^9 + z^{10} + z^{12} + z^{13} + \cdots .$$

Then: $\sum_{n \geq 0} T_n z^n = \Psi(z)$ modulo 3.

A functional equation modulo 3 satisfied by $\Psi(z)$

A functional equation modulo 3 satisfied by $\Psi(z)$

Lemma

The series $\Psi(z)=\prod_{j=0}^{\infty}(1+z^{3^j})$ *satisfies*

$$\Psi^2(z)=\frac{1}{1+z}\quad\text{modulo }3.$$

A functional equation modulo 3 satisfied by $\Psi(z)$

Lemma

The series $\Psi(z) = \prod_{j=0}^{\infty}(1+z^{3^j})$ *satisfies*

$$\Psi^2(z) = \frac{1}{1+z} \quad \text{modulo } 3.$$

Proof.

We have

$$\begin{aligned}
\Psi^2(z) &= \prod_{j=0}^{\infty}(1+z^{3^j})^2 = \frac{1}{1+z}(1+z)\prod_{j=0}^{\infty}(1+z^{3^j})^2 \\
&= \frac{1}{1+z}(1+z)^3\prod_{j=1}^{\infty}(1+z^{3^j})^2 = \frac{1}{1+z}(1+z^3)\Psi^2(z^3) \quad \text{modulo } 3 \\
&= \frac{1}{1+z}(1+z^9)\Psi^2(z^9) \quad \text{modulo } 3 \\
&= \cdots \\
&= \frac{1}{1+z} \quad \text{modulo } 3.
\end{aligned}$$

A functional equation modulo 3 satisfied by $\Psi(z)$

Lemma

The series $\Psi(z) = \prod_{j=0}^{\infty}(1 + z^{3^j})$ *satisfies*

$$\Psi^2(z) = \frac{1}{1+z} \quad \text{modulo } 3.$$

A functional equation modulo 3 satisfied by $\Psi(z)$

Lemma

The series $\Psi(z) = \prod_{j=0}^{\infty}(1 + z^{3^j})$ *satisfies*

$$\Psi^2(z) = \frac{1}{1+z} \quad \text{modulo } 3.$$

A functional equation modulo 3 satisfied by $\Psi(z)$

Lemma

The series $\Psi(z) = \prod_{j=0}^{\infty}(1 + z^{3^j})$ *satisfies*

$$\Psi^2(z) = \frac{1}{1+z} \quad \text{modulo } 3.$$

It is well-known that the generating function $T(z) \sum_{n\geq 0} T_n z^n$ is given by $T(z) = 1/\sqrt{1-2z-3z^2}$, or, phrased differently,

$$(1-2z-3z^2)T^2(z) - 1 = 0.$$

Morover, this functional equation determines $T(z)$ uniquely.

A functional equation modulo 3 satisfied by $\Psi(z)$

Lemma

The series $\Psi(z)=\prod_{j=0}^{\infty}(1+z^{3^j})$ *satisfies*

$$\Psi^2(z)=\frac{1}{1+z}\quad\text{modulo 3.}$$

It is well-known that the generating function $T(z)\sum_{n\ge0}T_nz^n$ is given by $T(z)=1/\sqrt{1-2z-3z^2}$, or, phrased differently,

$$(1-2z-3z^2)T^2(z)-1=0.$$

Morover, this functional equation determines $T(z)$ uniquely. Taken modulo 3, the above functional equation becomes:

$$(1+z)T^2(z)-1=0\quad\text{modulo 3.}$$

Consequently:

$$\sum_{n\ge0}T_nz^n=\Psi(z)\quad\text{modulo 3.}$$

What are the common features?

What are the common features?

- In each case, the generating function satisfied a quadratic equation (and, as a matter of fact, this applies as well for Motzkin prefix numbers, Riordan numbers, sums of central binomial coefficients, central Delannoy numbers, Schröder numbers, and hex tree numbers).

What are the common features?

- In each case, the generating function satisfied a quadratic equation (and, as a matter of fact, this applies as well for Motzkin prefix numbers, Riordan numbers, sums of central binomial coefficients, central Delannoy numbers, Schröder numbers, and hex tree numbers).
- In each case, one could express the generating function, after reduction of its coefficients modulo 3, as a linear expression in $\Psi(\pm z)$.

What are the common features?

- In each case, the generating function satisfied a quadratic equation (and, as a matter of fact, this applies as well for Motzkin prefix numbers, Riordan numbers, sums of central binomial coefficients, central Delannoy numbers, Schröder numbers, and hex tree numbers).
- In each case, one could express the generating function, after reduction of its coefficients modulo 3, as a linear expression in $\Psi(\pm z)$.

Can this be so many accidents?

A meta-theorem

Theorem

Let $F(z)$ be a formal power series with integer coefficients which satisfies a quadratic equation

$$c_2(z)F^2(z)+c_1(z)F(z)+c_0(z)=0 \quad \text{modulo } 3,$$

where

Then

$$F(z)=\frac{c_1(z)}{c_2(z)}\pm\frac{z^{f_1}(1+\varepsilon z^{\gamma})^{f_2+1}}{c_2(z)}\Psi(\varepsilon z^{\gamma}) \quad \text{modulo } 3.$$

A meta-theorem

Theorem

Let $F(z)$ be a formal power series with integer coefficients which satisfies a quadratic equation

$$c_2(z)F^2(z) + c_1(z)F(z) + c_0(z) = 0 \quad \text{modulo } 3,$$

where

1. $c_2(z) = z^{e_1}(1+\varepsilon z^{\gamma})^{e_2}$ modulo 3, *with non-negative integers* e_1, e_2 *and* $\varepsilon \in \{1, -1\}$*;*

Then

$$F(z) = \frac{c_1(z)}{c_2(z)} \pm \frac{z^{f_1}(1+\varepsilon z^{\gamma})^{f_2+1}}{c_2(z)}\Psi(\varepsilon z^{\gamma}) \quad \text{modulo } 3.$$

A meta-theorem

Theorem

Let $F(z)$ be a formal power series with integer coefficients which satisfies a quadratic equation

$$c_2(z)F^2(z) + c_1(z)F(z) + c_0(z) = 0 \quad \text{modulo } 3,$$

where

1. $c_2(z) = z^{e_1}(1+\varepsilon z^{\gamma})^{e_2}$ modulo 3, *with non-negative integers* e_1, e_2 *and* $\varepsilon \in \{1,-1\}$*;*
2. $c_1^2(z) - c_0(z)c_2(z) = z^{2f_1}(1+\varepsilon z^{\gamma})^{2f_2+1}$ modulo 3, *with non-negative integers* f_1, f_2*.*

Then

$$F(z) = \frac{c_1(z)}{c_2(z)} \pm \frac{z^{f_1}(1+\varepsilon z^{\gamma})^{f_2+1}}{c_2(z)}\Psi(\varepsilon z^{\gamma}) \quad \text{modulo } 3.$$

Proof.

Proof.

Proof.

. . . . □

Proof.

. . . . □

The corresponding choices of $c_2(z), c_1(z), c_0(z)$ are:

	$c_2(z)$	$c_1(z)$	$c_0(z)$	$c_1^2(z) - c_0(z)c_2(z)$ mod 3
trinomial	$1-2z-3z^2$	0	-1	$1+z$
Motzkin	z^2	$z-1$	1	$1+z$
cent.bin.	$1-4z$	0	-1	$1-z$
Catalan	z	-1	1	$1-z$
Motz.pref.	$z-3z^2$	$1-3z$	-1	$1+z$
Riordan	$z+z^2$	$1+z$	1	$1+z$
Delannoy	$1-6z+z^2$	0	-1	$1+z^2$
Schröder	z	$z-1$	1	$1+z^2$
hex tree	z^2	$3z-1$	1	$1-z^2$
...	...	...	...	...

Can we also do congruences modulo powers of 3?

Can we also do congruences modulo powers of 3?

Yes!

One follows the recipe that we developed for the series $\Phi(z)$ in order to find congruences modulo powers of 2:

One expresses the generating function now as polynomial in $\Psi(z)$ (or $\Psi(-z)$, or $\Psi(z^2)$, or $\dots$), with undetermined coefficients, which may be Laurent polynomials in z and $1+z$ (respectively $1-z$, $1+z^2$, $\dots$). Again, "high" powers of $\Psi(z)$ can be reduced, here by means of the relation

$$\left(\Psi^2(z)-\frac{1}{1+z}\right)^{3^\alpha}=0 \quad \text{modulo } 3^{3^\alpha}.$$

Can we also do congruences modulo powers of 3?

Yes!

One follows the recipe that we developed for the series $\Phi(z)$ in order to find congruences modulo powers of 2:

One expresses the generating function now as polynomial in $\Psi(z)$ (or $\Psi(-z)$, or $\Psi(z^2)$, or $\dots$), with undetermined coefficients, which may be Laurent polynomials in z and $1+z$ (respectively $1-z$, $1+z^2$, $\dots$). Again, "high" powers of $\Psi(z)$ can be reduced, here by means of the relation

$$\left(\Psi^2(z) - \frac{1}{1+z}\right)^{3^\alpha} = 0 \quad \text{modulo } 3^{3^\alpha}.$$

It is also possible to extract coefficients from powers of $\Psi(z)$.

As it turns out, there is even a meta-theorem which refines all the modulo 3-results of Deutsch and Sagan to any power of 3. The corresponding results can be found automatically. Moreover, this meta-theorem produces as well several new congruence results.

Theorem

Let α be some positive integer. Furthermore, suppose that the formal power series $F(z)$ with integer coefficients satisfies the functional-differential equation

$$c_2(z)F^2(z) + c_1(z)F(z) + c_0(z)$$

where $$+ 3\mathcal{Q}(z; F(z), F'(z), F''(z), \dots, F^{(s)}(z)) = 0,$$

Then $F(z)$, when coefficients are reduced modulo 3^{3^α}, can be expressed as a polynomial in $\Psi(\varepsilon z^\gamma)$ of the form

$$F(z) = a_0(z) + \sum_{i=0}^{2\cdot 3^\alpha - 1} a_i(z)\Psi^i(\varepsilon z^\gamma) \quad \text{modulo } 3^{3^\alpha},$$

where the coefficients $a_i(z)$, $i = 0, 1, \dots, 2 \cdot 3^\alpha - 1$, are Laurent polynomials in z and $1 + \varepsilon z^\gamma$.

Theorem

Let α be some positive integer. Furthermore, suppose that the formal power series $F(z)$ with integer coefficients satisfies the functional-differential equation

$$c_2(z)F^2(z) + c_1(z)F(z) + c_0(z) + 3\mathcal{Q}(z; F(z), F'(z), F''(z), \dots, F^{(s)}(z)) = 0,$$

where

1. $c_2(z) = z^{e_1}(1 + \varepsilon z^{\gamma})^{e_2}$ modulo 3, *with non-negative integers* e_1, e_2 *and* $\varepsilon \in \{1, -1\}$*;*

Then $F(z)$, when coefficients are reduced modulo $3^{3^{\alpha}}$, can be expressed as a polynomial in $\Psi(\varepsilon z^{\gamma})$ of the form

$$F(z) = a_0(z) + \sum_{i=0}^{2\cdot 3^{\alpha}-1} a_i(z)\Psi^i(\varepsilon z^{\gamma}) \quad \text{modulo } 3^{3^{\alpha}},$$

where the coefficients $a_i(z)$, $i = 0, 1, \dots, 2 \cdot 3^{\alpha} - 1$, are Laurent polynomials in z and $1 + \varepsilon z^{\gamma}$.

Theorem

Let α be some positive integer. Furthermore, suppose that the formal power series $F(z)$ with integer coefficients satisfies the functional-differential equation

$$c_2(z)F^2(z)+c_1(z)F(z)+c_0(z) \\ +3\mathcal{Q}(z;F(z),F'(z),F''(z),\dots,F^{(s)}(z))=0,$$

where

1. $c_2(z)=z^{e_1}(1+\varepsilon z^{\gamma})^{e_2}$ modulo 3, *with non-negative integers* e_1,e_2 *and* $\varepsilon\in\{1,-1\}$*;*
2. $c_1^2(z)-c_0(z)c_2(z)=z^{2f_1}(1+\varepsilon z^{\gamma})^{2f_2+1}$ modulo 3, *with non-negative integers* f_1,f_2*;*

Then $F(z)$, when coefficients are reduced modulo 3^{3^α}, can be expressed as a polynomial in $\Psi(\varepsilon z^{\gamma})$ of the form

$$F(z)=a_0(z)+\sum_{i=0}^{2\cdot 3^\alpha-1}a_i(z)\Psi^i(\varepsilon z^{\gamma})\quad\text{modulo } 3^{3^\alpha},$$

where the coefficients $a_i(z)$, $i=0,1,\dots,2\cdot 3^\alpha-1$, are Laurent polynomials in z and $1+\varepsilon z^{\gamma}$.

Theorem

Let α be some positive integer. Furthermore, suppose that the formal power series $F(z)$ with integer coefficients satisfies the functional-differential equation

$$c_2(z)F^2(z)+c_1(z)F(z)+c_0(z)$$

where $$+\,3\mathcal{Q}(z;F(z),F'(z),F''(z),\dots,F^{(s)}(z))=0,$$

1. $c_2(z)=z^{e_1}(1+\varepsilon z^{\gamma})^{e_2}$ modulo 3, *with non-negative integers* e_1, e_2 *and* $\varepsilon\in\{1,-1\}$*;*
2. $c_1^2(z)-c_0(z)c_2(z)=z^{2f_1}(1+\varepsilon z^{\gamma})^{2f_2+1}$ modulo 3, *with non-negative integers* f_1, f_2*;*
3. $\mathcal{Q}$ *is a polynomial with integer coefficients.*

Then $F(z)$, when coefficients are reduced modulo 3^{3^α}*, can be expressed as a polynomial in* $\Psi(\varepsilon z^{\gamma})$ *of the form*

$$F(z)=a_0(z)+\sum_{i=0}^{2\cdot 3^\alpha-1}a_i(z)\Psi^i(\varepsilon z^{\gamma})\quad\text{modulo } 3^{3^\alpha},$$

where the coefficients $a_i(z)$, $i=0,1,\dots,2\cdot 3^\alpha-1$, *are Laurent polynomials in* z *and* $1+\varepsilon z^{\gamma}$*.*

Central trinomial numbers modulo 27

Theorem

We have

$$\sum_{n\geq 0} T_n\, z^n = -\left(9z^2+24z+15\right)\Psi(z^3) + \left(15z^5+25z^4+4z^3+12z^2+10z+19\right)\Psi^3(z^3) + \left(9z^8+6z^7+6z^6+9z^5+21z^4+3z^3+15z+24\right)\Psi^5(z^3)$$

modulo 27.

Minimal polynomials for $\Phi(z)$ and $\Psi(z)$

It would be desirable to know “minimal” relations for the series $\Phi(z)$ and $\Psi(z)$.

Minimal polynomials for $\Phi(z)$ and $\Psi(z)$

It would be desirable to know “minimal” relations for the series $\Phi(z)$ and $\Psi(z)$.

Definition

A polynomial $A(z,t)$ in z and t is *minimal for the modulus* 2^γ, if it is monic (as a polynomial in t), has coefficients which are Laurent polynomials in z, satisfies $A(z,\Phi(z)) = 0$ modulo 2^γ, and there is no monic polynomial $B(z,t)$ whose coefficients are Laurent polynomials in z, whose t-degree is less than that of $A(z,t)$, and which satisfies $B(z,\Phi(z)) = 0$ modulo 3^γ.

Minimal polynomials for $\Phi(z)$ and $\Psi(z)$

It would be desirable to know "minimal" relations for the series $\Phi(z)$ and $\Psi(z)$.

Definition

A polynomial $A(z,t)$ in z and t is *minimal for the modulus* 2^γ, if it is monic (as a polynomial in t), has coefficients which are Laurent polynomials in z, satisfies $A(z,\Phi(z))=0$ modulo 2^γ, and there is no monic polynomial $B(z,t)$ whose coefficients are Laurent polynomials in z, whose t-degree is less than that of $A(z,t)$, and which satisfies $B(z,\Phi(z))=0$ modulo 3^γ.

Minimal polynomials for $\Phi(z)$ and $\Psi(z)$

It would be desirable to know "minimal" relations for the series $\Phi(z)$ and $\Psi(z)$.

Definition

A polynomial $A(z,t)$ in z and t is *minimal for the modulus* 2^{γ}, if it is monic (as a polynomial in t), has coefficients which are Laurent polynomials in z, satisfies $A(z,\Phi(z)) = 0$ modulo 2^{γ}, and there is no monic polynomial $B(z,t)$ whose coefficients are Laurent polynomials in z, whose t-degree is less than that of $A(z,t)$, and which satisfies $B(z,\Phi(z)) = 0$ modulo 3^{γ}.

Definition

A polynomial $A(z,t)$ in z and t is *minimal for the modulus* 3^{γ}, if it is monic (as a polynomial in t), has coefficients which are Laurent polynomials in z and $1+z$, satisfies $A(z,\Psi(z)) = 0$ modulo 3^{γ}, and there is no monic polynomial $B(z,t)$ whose coefficients are Laurent polynomials in z and $1+z$, whose t-degree is less than that of $A(z,t)$, and which satisfies $B(z,\Psi(z)) = 0$ modulo 3^{γ}.

Conjecture

The degree of a minimal polynomial for the modulus 2^γ, $\gamma \geq 1$, *is the least* d *such that* $2^\gamma \mid d!$.

Conjecture

The degree of a minimal polynomial for the modulus 2^γ, $\gamma \geq 1$, is the least d such that $2^\gamma \mid d!$.

Proposition

Minimal polynomials for the moduli $2, 4, 8, 16, 32, 64, 128$ are

$$\begin{aligned}
&A_1(z,t) := t^2 + t + z && \text{modulo } 2,\\
&A_1(z,t)^2 && \text{modulo } 4,\\
&A_2(z,t) := A_1(z,t)^2 + 4t^3 + 2t^2 + 6t + 2z + 4z^2 && \text{modulo } 8,\\
&A_1(z,t)A_2(z,t) && \text{modulo } 16,\\
&A_2(z,t)^2 && \text{modulo } 32,\\
&A_2(z,t)^2 && \text{modulo } 64,\\
&t^8 + 124t^7 + t^6(68z + 18) + t^5(124z + 24) + t^4\left(62z^2 + 64z + 81\right)\\
&\quad + t^3\left(20z^2 + 76z + 28\right) + t^2\left(116z^3 + 114z^2 + 12z + 92\right)\\
&\quad + t\left(116z^3 + 28z^2 + 8z + 16\right) + 9z^4 + 124z^3 + 12z^2 + 112z && \text{modulo } 128.
\end{aligned}$$

Conjecture

The degree of a minimal polynomial for the modulus 3^γ, $\gamma \geq 1$, *is* $2d$, *where* d *is the least positive integer such that* $3^\gamma \mid 3^d d!$.

Conjecture

The degree of a minimal polynomial for the modulus 3^γ, $\gamma \geq 1$, is $2d$, where d is the least positive integer such that $3^\gamma \mid 3^d d!$.

Proposition

Minimal polynomials for the moduli $3, 9, 27, 81, 243, 729, 2187, \dots, 3^{13}$ *are*

$$\begin{array}{ll}
A_0(z,t) := t^2 - \frac{1}{1+z} & \text{modulo } 3, \\
A_0^2(z,t) & \text{modulo } 9, \\
A_0^3(z,t) & \text{modulo } 27, \\
A_1(z,t) := \left(t^2 - \frac{1}{1+z}\right)^3 - \frac{9}{(1+z)^2}\left(t^2 - \frac{1}{1+z}\right) + \frac{27z}{(1+z)^5} & \text{modulo } 81, \\
A_0(z,t)A_1(z,t) & \text{modulo } 243, \\
A_0^2(z,t)A_1(z,t) & \text{modulo } 729, \\
A_1^2(z,t) & \text{modulo } 2189, \\
A_1^2(z,t) & \text{modulo } 3^8, \\
A_0(z,t)A_1^2(z,t) & \text{modulo } 3^9, \\
A_0^2(z,t)A_1^2(z,t) & \text{modulo } 3^{10}, \\
A_1^3(z,t) & \text{modulo } 3^{11},
\end{array}$$