Computer proofs of some combinatorial congruences

Narad Rampersad

Department of Mathematics and Statistics
University of Winnipeg

(This is joint work with Jeffrey Shallit.)

We look at some computational methods for obtaining congruences for combinatorial sequences like

- the Catalan numbers

$$1, 1, 2, 5, 14, 42, 132, 429, 1430, \dots$$

  which count, among other things, the number of strings of properly nested parentheses of length $2n$, or the number of binary trees on n vertices;

- the Motzkin numbers

$$1, 1, 2, 4, 9, 21, 51, 127, 323, 835, \ldots$$

  which count the number of lattice paths from $(0,0)$ to $(n,0)$ with steps $\nearrow$, $\searrow$, $\rightarrow$ and that don't dip below the x-axis;
- etc.

Let p be prime. Our main tool is the Freshman's Dream:

$$(1+x)^p \equiv_p 1 + x^p.$$

We also will work with base-p expansions. If

$$n = n_0 + n_1 p + n_2 p^2 + \cdots + n_r p^r$$

we write

$$(n)_p = n_0 n_1 n_2 \cdots n_r$$

for the the base-p expansion of n written least-significant-digit first.

- Let's start with the central binomial coefficients:
- $\binom{2n}{n}$ is the coefficient of x^n in $(1+x)^{2n}$
- Suppose I would prefer $\binom{2n}{n}$ to be the constant term; i.e., the coefficient of x^0.
- Divide by x^n: $\binom{2n}{n}$ is the constant term of

$$\frac{(1+x)^{2n}}{x^n} = \left(\frac{(1+x)^2}{x}\right)^n = \left(\frac{1+2x+x^2}{x}\right)^n = \left(\frac{1}{x}+2+x\right)^n.$$

We can do the same for the Catalan numbers:

$$\begin{aligned} C_n &= \frac{1}{n+1}\binom{2n}{n} \\ &= \binom{2n}{n} - \binom{2n}{n-1} \\ &= \mathrm{ct}\left(\frac{1}{x}+2+x\right)^n - \mathrm{ct}\left(x\left(\frac{1}{x}+2+x\right)^n\right) \\ &= \mathrm{ct}\left(\left(\frac{1}{x}+2+x\right)^n(1-x)\right). \end{aligned}$$

The Motzkin numbers satisfy:

$$M_n = \sum_{k \geq 0} \binom{n}{2k} C_k = \mathrm{ct}\left(\left(\frac{1}{x} + 1 + x \right)^n (1 - x^2) \right).$$

Many similar combinatorial sequences involving sums of binomial coefficients can be written as the constant term of a Laurent polynomial with integer coefficients of the form $[P(x)]^n Q(x)$.

Let's evaluate the Catalan numbers modulo 2. Define

$$\begin{aligned} C_n &= \mathrm{ct}\left(\left(\frac{1}{x} + 2 + x\right)^n (1-x)\right) \\ &\equiv_2 \mathrm{ct}\left(\left(\frac{1}{x} + x\right)^n (1+x)\right) =: A_1(n). \end{aligned}$$

We compute $A_1(2n)$ and $A_1(2n+1)$.

$$\begin{aligned} A_1(2n) &= \mathrm{ct}\left((1/x + x)^{2n}(1+x)\right) \\ &\equiv_2 \mathrm{ct}\left((1/x^2 + x^2)^n(1+x)\right) \quad \text{(by Freshman's Dream)} \\ &= \mathrm{ct}\left((1/x^2 + x^2)^n\right) \\ &= \mathrm{ct}\left((1/x + x)^n\right) \\ &=: A_2(n) \end{aligned}$$

$$
\begin{aligned}
A_1(2n+1) &= \mathrm{ct}\left((1/x+x)^{2n+1}(1+x)\right) \\
&= \mathrm{ct}\left(((1/x+x)^2)^n(1/x+x)(1+x)\right) \\
&\equiv_2 \mathrm{ct}\left((1/x^2+x^2)^n(1/x+1+x+x^2)\right) \\
&= \mathrm{ct}\left((1/x^2+x^2)^n(1+x^2)\right) \\
&= \mathrm{ct}\left((1/x+x)^n(1+x)\right) \\
&= A_1(n)
\end{aligned}
$$

Now we compute $A_2(2n)$ and $A_2(2n+1)$.

$$\begin{aligned} A_2(2n) &= \mathrm{ct}\left((1/x + x)^{2n}\right) \\ &\equiv_2 \mathrm{ct}\left((1/x^2 + x^2)^n\right) \\ &= \mathrm{ct}\left((1/x + x)^n\right) \\ &= A_2(n) \end{aligned}$$

$$\begin{aligned} A_2(2n+1) &= \mathrm{ct}\left((1/x + x)^{2n+1}\right) \\ &\equiv_2 \mathrm{ct}\left((1/x^2 + x^2)^n (1/x + x)\right) \\ &= 0 \end{aligned}$$

So we get the recurrences

$$\begin{aligned} A_1(2n) &\equiv_2 A_2(n) \\ A_1(2n+1) &\equiv_2 A_1(n) \\ A_2(2n) &\equiv_2 A_2(n) \\ A_2(2n+1) &\equiv_2 0, \end{aligned}$$

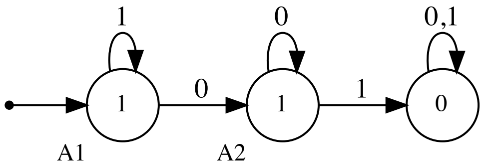
with initial conditions $A_1(0) = 1$, $A_2(0) = 1$.

Let $w = (n)_2$; i.e., w is the binary representation of n, written left-to-right. The previous recurrences can be written (with an abuse of notation) as

$$A_1(0w) \equiv_2 A_2(w)$$
$$A_1(1w) \equiv_2 A_1(w)$$
$$A_2(0w) \equiv_2 A_2(w)$$
$$A_2(1w) \equiv_2 0,$$

with initial conditions $A_1(0) = A_2(0) = 1$.

This can be represented graphically by the finite automaton



This is a machine that reads input $w = (n)_2$, digit-by-digit, and follows the arcs labeled by each digit read. If the machine ends in states labeled 1 (i.e., A_1 or A_2), then $C_n \equiv_2 1$ and if it ends in the 0 state, we have $C_n \equiv_2 0$.

We have thus proved the following folklore theorem:

Theorem

C_n is odd iff $(n)_2 = 1^k 0^j$; i.e., iff $n = 2^k - 1$.

(Here 1^k means a string of k 1's and 0^j means a string of j 0's.)

- This illustrates a general method due to Rowland and Zeilberger.
- We are given a sequence defined as $\mathrm{ct}([P(x)]^n Q(x))$, for some Laurent polynomials P and Q.
- Modulo any prime power, if we compute recurrence relations as we did above, this process will eventually terminate, giving a finite set of recurrence relations.
- We can then translate these recurrence relations into a finite automaton.

They implemented this in Maple, and were thus able to prove many hundreds of congruence results for the Catalan numbers and other sequences.

https://sites.math.rutgers.edu/~zeilberg/mamarim/mamarimhtml/meta.html

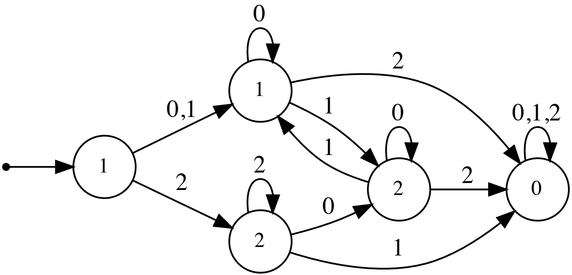
Rowland and Yassawi (2015) have also given a completely different method for computing finite automata for these kinds of combinatorial sequences.

Now let's look at the Catalan numbers C_n modulo 3. (Alter and Kubota (1973) studied the general case $C_n \bmod p$.)

Let

$$\mathbf{c}_3 = (C_n \bmod 3)_{n\geq 0}$$
$$= (1, 1, 2, 2, 2, 0, 0, 0, 2, 2, 2, 1, 1, 1, 0, 0, 0, 0,$$
$$0, 0, 0, 0, 0, 0, 0, 0, 2, 2, 2, 1, 1, 1, 0, 0, 0, 1,$$
$$1, 1, 2, 2, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,$$
$$0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0,$$
$$0, 0, 0, 0, 0, 0, 2, 2, 2, 1, 1, 1, 0, 0, 0, 1, 1, 1, 2,$$
$$2, 2, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 1, 1, 1, 2, 2,$$
$$2, 0, 0, 0, 2, 2, 2, 1, 1, 1, \ldots)$$

Applying the Rowland–Zeilberger method gives the automaton



which is rather more complicated than the modulo 2 automaton.

Theorem (Deutsch and Sagan 2006)

The runs of 0's in $\mathbf{c}_3$ begin at positions n where either

$$(n)_3 = 21^i \text{ or } (n)_3 = 21^i 0\{0,1\}^j,\ i \geq 1,\ j \geq 0,$$

and have length $(3^{i+2} - 3)/2$.

Theorem cont'd. (Deutsch and Sagan 2006)

The blocks of non-zero values in $\mathbf{c}_3$ are given by the following:

- The block 11222 occurs at position 0.
- The block 111222 occurs at all positions n where $(n)_3 = 2^i 0w$ for some $i \geq 2$ and some $w \in \{0,1\}^*$ that contains an odd number of 1's.
- The block 222111 occurs at all positions n where $(n)_3 = 2^i 0w$ for some $i \geq 2$ and some $w \in \{0,1\}^*$ that contains an even number of 1's.

We can obtain this result purely by computer using a program called Walnut (developed by Jeffrey Shallit's student Hamoon Mousavi). Suppose we are given

- A finite automaton reading input n in base-k and outputing the n-th term of a sequence $\mathbf{s}$; and,
- A formula φ in first-order-logic involving variables (over $\mathbb{N}$), constants, quantifiers, logical operations, ordering, addition and subtraction of natural numbers, and indexing into $\mathbf{s}$.
- We can also multiply by a constant (this is just repeated addition), but we can't multiply two variables.

- If φ has no free variables, Walnut will output either that φ is TRUE or φ is FALSE.
- If φ has free variables, Walnut will produce an automaton that accepts the base-k representations of the values of the free variables that satisfy φ.
- We won't get into the theory of how it evaluates these logical formulas.

e.g., the formula

$$\varphi := \exists i \, \forall j \, ((j \geq 0 \land j < 4) \Rightarrow \mathbf{c}_3(i+j) = 1)$$

asserts that there is a "run" of at least four 1's in $\mathbf{c}_3$.

In Walnut's language, this is

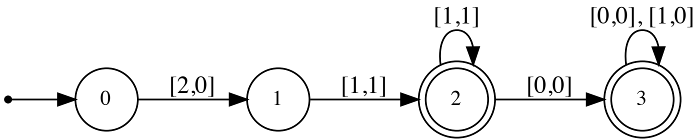
```
eval run4ones "?lsd_3 Ei Aj ((j>=0 & j<4) =>
    CAT3[i+j]=@1)":
```

and evaluates to "FALSE".

The Walnut command

```
eval cat3max0 "?lsd_3 n>=1 &
    (At t<n => CAT3[i+t]=@0) &
    CAT3[i+n]!=@0 & (i=0|CAT3[i-1]!=@0)":
```

produces the automaton



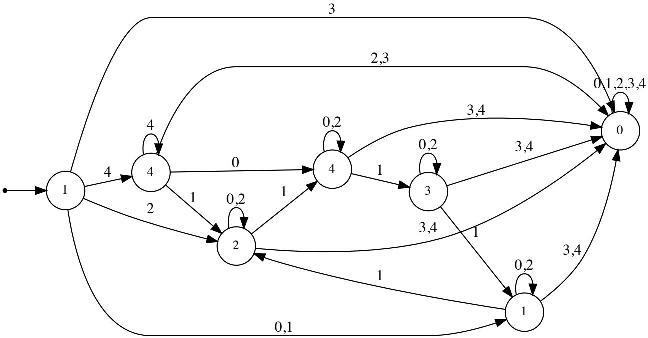
Examining the transition labels of the first component of the input gives the claimed representation for the starting positions of the runs of 0's

$$(i)_3 = 21^k \text{ or } (i)_3 = 21^k0\{0,1\}^j$$

and examining the transition labels of the second component gives the claimed length

$$(n)_3 = 01^k; \text{ i.e., } n = (3^{k+2} - 3)/2.$$

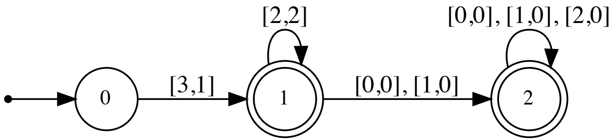
For $p = 5$, the Rowland–Zeilberger method gives the automaton



for

$\mathbf{c}_5 := (C_n \bmod 5)_{n \geq 0}$.

Using Walnut, one can obtain the following automaton for the runs of 0's in $\mathbf{c}_5$:



From this automaton we derive:

Theorem (R. and Shallit)

The runs of 0's in $\mathbf{c}_5$ begin at positions n where either

$$(n)_5 = 32^i \text{ or } (n)_5 = 32^i\{0,1\}\{0,1,2\}^j,\ i \geq 0,\ j \geq 0,$$

and have length $(5^{i+2} - 3)/2$.

We can easily characterize the non-zero blocks in $\mathbf{c}_5$ as well.

Let's examine the Motzkin numbers next. These are closely related to the central trinomial coefficients:

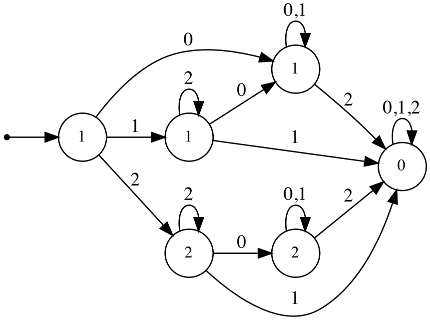
$$\begin{aligned}\sum_{k\geq 0}\binom{n}{2k}\binom{2k}{k} &= \sum_{k\geq 0}\binom{n}{2k}\,\mathrm{ct}\left(\frac{(1+x^2)^{2k}}{x^{2k}}\right)\\ &= \mathrm{ct}\left(\sum_{k\geq 0}\binom{n}{2k}\left(\frac{1+x^2}{x}\right)^{2k}\right)\\ &= \mathrm{ct}\left(1+\frac{1+x^2}{x}\right)^n\\ &= \mathrm{ct}\left(1+\frac{1}{x}+x\right)^n\end{aligned}$$

Hence

$$
\begin{aligned}
M_n &= \sum_{k\geq 0} \binom{n}{2k} C_k \\
&= \sum_{k\geq 0} \binom{n}{2k} \left[\binom{2k}{k} - \binom{2k}{k-1} \right] \\
&= \sum_{k\geq 0} \binom{n}{2k}\binom{2k}{k} - \sum_{k\geq 0} \binom{n}{2k}\binom{2k}{k-1} \\
&= \mathrm{ct}\left(1 + \frac{1}{x} + x\right)^n - \mathrm{ct}\left(x^2 \left(1 + \frac{1}{x} + x\right)^n\right) \\
&= \mathrm{ct}\left(\left(1 + \frac{1}{x} + x\right)^n (1 - x^2)\right)
\end{aligned}
$$

Now we can compute automata for $M_n \bmod p$ using the Rowland–Zeilberger algorithm.

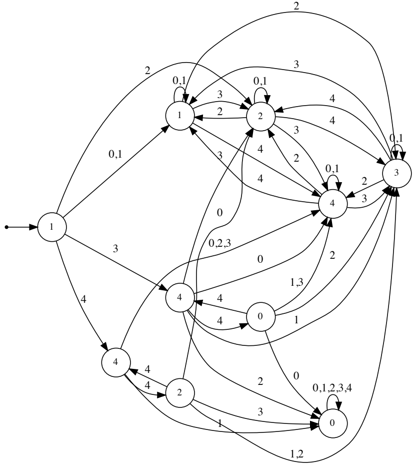
The automaton for $M_n \bmod 3$ is



- Let $\mathbf{m}_3 := (M_n \bmod 3)_{n\geq 0}$.
- Note that no matter where you are in the automaton, the input 02 takes you to the 0 state.
- So for any w, the input $w02$ results in output 0.
- Letting w run through all ternary strings of any fixed length, we find that $\mathbf{m}_3$ contains arbitrarily large runs of 0's.

$$
\begin{aligned}
\mathbf{m}_3 &= (M_n \bmod 3)_{n\geq 0} \\
&= (1, 1, 2, 1, 0, 0, 0, 1, 2, 1, 1, 2, 1, 0, 0, 0, 0, 0, 0, 0, \\
&0, 0, 0, 0, 0, 1, 2, 1, 1, 2, 1, 0, 0, 0, 1, 2, 1, 1, 2, \\
&1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, \\
&0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, \\
&1, 2, 1, 1, 2, 1, 0, 0, 0, 1, 2, 1, 1, 2, 1, 0, 0, 0, 0, 0, 0, \\
&0, 0, 0, 0, 0, 0, 1, 2, 1, 1, 2, 1, 0, 0, 0, 1, 2, 1, 1, 2, \\
&1, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, 0, \ldots)
\end{aligned}
$$

The automaton for $M_n \bmod 5$ is



$$\mathbf{m}_5 = (M_n \bmod 5)_{n\geq 0}$$

$$= (1, 1, 2, 4, 4, 1, 1, 2, 3, 0, 3, 3, 1, 0, 4, 2, 2, 4, 2, 4,$$

$$4, 4, 3, 0, 2, 1, 1, 2, 4, 4, 1, 1, 2, 3, 0, 3, 3, 1, 0, 4,$$

$$2, 2, 4, 2, 4, 4, 4, 3, 4, 3, 3, 3, 1, 2, 2, 3, 3, 1, 4, 0,$$

$$4, 4, 3, 0, 2, 1, 1, 2, 1, 2, 2, 2, 4, 3, 3, 2, 2, 4, 3, 3,$$

$$2, 2, 4, 1, 0, 1, 1, 2, \ldots)$$

- Unlike $\mathbf{m}_3$, the sequence does not contain arbitrarily long runs of 0's.
- With Walnut we can easily prove that the longest runs in $\mathbf{m}_5$ are $(1,1,1)$, $(2,2,2)$, $(3,3,3)$, and $(4,4,4)$.

- We have seen that $\mathbf{m}_3$ and $\mathbf{m}_5$ have very different behaviour.
- Burns (arxiv preprints) studied $\mathbf{m}_p$ for primes p between 7 and 29 using automata computed using the Rowland–Yassawi algorithm.
- His work suggests that depending on the value of p, the sequence $\mathbf{m}_p$:
- either behaves like $\mathbf{m}_3$, where 0 has density 1 (i.e., $p = 7, 17, 19$),
- or $\mathbf{m}_p$ behaves like $\mathbf{m}_5$, where 0 has density < 1 (i.e., $p = 11, 13, 23, 29$).

- $\mathbf{m}_5$ has another nice property: if a length-n pattern of residues occurs in $\mathbf{m}_5$, it is guaranteed to re-occur within the next $200n$ terms (in combinatorics on words, we call this phenomenon uniform recurrence).

The Walnut commands to prove this recurrence property are:

```
def mot5faceq "?lsd_5 At (t<n) =>
    (MOT5[i+t]=MOT5[j+t])":
eval tmp "?lsd_5 An (n>=1) => Ai Ej (j>i) &
    (j<i+200*n+1) & $mot5faceq(i,j,n)":
```

Problem

Characterize the primes p for which $\mathbf{m}_p$ is uniformly recurrent.

We guess that the answer to this problem is given by the sequence

$$2, 5, 11, 13, 23, 29, 31, 37, 53, \ldots$$

of primes that do not divide any central trinomial number.

This is sequence **A113305** of the OIES.

Theorem (Deutsch and Sagan)

The central trinomial coefficient T_n satisfies

$$T_n \equiv_3 \begin{cases} 1, & \text{if } (n)_3 \text{ does not contain a } 2; \\ 0, & \text{otherwise.} \end{cases}$$

Deutsch and Sagan proved this by an application of Lucas' Theorem; it is also immediate from the automaton produced by the Rowland–Zeilberger algorithm.

As with the Motzkin numbers, the behaviour of T_n modulo 5 is rather different from that modulo 3.

Theorem (R. and Shallit)

Let $\mathbf{t}_5 := (T_n \bmod 5)_{n\geq 0}$. Then

1. $\mathbf{t}_5$ does not contain 0 (i.e., T_n is never divisible by 5);
2. the only patterns that repeat three times in $\mathbf{t}_5$ are 111, 222, 333, and 444;

Theorem (cont'd.)

3. $\mathbf{t}_5$ is uniformly recurrent; Furthermore, if a length-n pattern w occurs at position i in $\mathbf{t}_5$, then there is another occurrence of w at some position j, where $i < j \leq i + 200n - 192$.
4. If w is a length-n pattern appearing in $\mathbf{t}_5$, then w appears at some position $i < 121n$.

Theorem (Deutsch and Sagan)

Let $(n)_p = n_0 n_1 \cdots n_r$. Then

$$T_n \equiv_p \prod_{i=0}^{r} T_{n_i}.$$

- An immediate consequence is that T_n is divisible by p if and only if one of the T_{n_i} is divisible by p.
- This criterion allows one to determine the primes p that do not divide any central trinomial coefficient; i.e., those in **A113305** of OEIS, which we conjectured in the previous section to be the ones for which $\mathbf{m}_p$ is uniformly recurrent.

Using the previous result of Deutsch and Sagan we can prove the following:

Theorem (R. and Shallit)

Let $\mathbf{t}_p$ be the sequence of central trinomial numbers modulo p. If the first p terms of $\mathbf{t}_p$ do not contain 0, but do contain a primitive root modulo p, then $\mathbf{t}_p$ is uniformly recurrent.

For $p = 5$, we have $(T_0, T_1, T_2, T_3, T_4) = (1, 1, 3, 7, 19)$, so $(\tau_0, \tau_1, \tau_2, \tau_3, \tau_4) = (1, 1, 3, 2, 4)$ contains the primitive root 2. The word

$$\mathbf{t}_5 = 1132411324334122214344231113 24 \cdots$$

is therefore uniformly recurrent.

- A computer calculation shows that for each prime p appearing in the list of initial values $2, 5, 11, 13, \ldots, 479$ of **A113305**, the first p terms of $\mathbf{t}_p$ always contain a primitive root modulo p.
- Hence, each of these $\mathbf{t}_p$'s are uniformly recurrent.

Problem

Prove this in general.

References

- Walnut can be downloaded here:

  https://cs.uwaterloo.ca/~shallit/walnut.html

- Rowland and Zeilberger's paper and accompanying material can be downloaded here:

  https://sites.math.rutgers.edu/~zeilberg/mamarim/mamarimhtml/meta.html

- Deutsch and Sagan's paper is: Congruences for Catalan and Motzkin numbers and related sequences, J. Number Theory 117 (2006), 191–215.

The End