A supercongruence for A002003

Peter Bala, March 2020

We prove the supercongruence A002003$(p) \equiv$ A002003$(1) \pmod{p^3}$ holds for prime $p \geq 5$.

- -

The terms of A002003 are defined by means of the binomial sum

$$a(n) = 2\sum_{k=0}^{n-1}\binom{n-1}{k}\binom{n+k}{k}. \tag{1}$$

Seiichi Manyama contributed the alternative representation

$$a(n) = [x^n]\left(\frac{1+x}{1-x}\right)^n. \tag{2}$$

Expanding the binomials in (2) and extracting the coefficient of x^n leads to a second representation for $a(n)$ as a binomial sum:

$$a(n) \quad = \quad \sum_{k=0}^{n}\binom{n}{k}\binom{2n-k-1}{n-1}. \tag{3}$$

We can verify (3) (and hence also (2)) by using Zeilberger's algorithm to show that the defining sum (1) and the sum (3) satisfy the same linear recurrence, namely,

$$4(3n^2-6n+2)a(n-1)-(n-2)(2n-1)a(n-2)-n(2n-3)a(n)=0.$$

Both sums have the same initial values, thus confirming Manyama's observation (2).

Supercongruences Given an integer sequence $s(n)$, there exists a formal power series $G(x) = 1 + g_1x + g_2x^2 + \cdots$, with rational coefficients, such that

$$s(n) = [x^n]\,G(x)^n \quad \text{for } n \geq 1. \tag{4}$$

$G(x)$ is given by

$$G(x) = \frac{x}{\text{Rev }(xE(x))}, \tag{5}$$

where Rev denotes the series reversion (inversion) operator and the power series $E(x) = \exp\left(\sum_{n\geq 1} s(n)\frac{x^n}{n}\right)$. See [Stan'99, Exercise 5.56 (a), p. 98, and its solution on p. 146] or [Bal'15].

We can invert (5) to express $E(x)$ in terms of $G(x)$:

$$E(x) = \frac{1}{x}\text{Rev}\left(\frac{x}{G(x)}\right). \tag{6}$$

A simple consequence of (5) and (6) is the following:

the power series $G(x)$ is integral $\iff$ the power series $E(x)$ is integral

Given a sequence $s(n)$, the condition that the power series $E(x) = \exp\left(\sum_{n\geq 1} s(n)\frac{x^n}{n}\right)$ is integral is known to be equivalent to the statement that the Gauss congruences

$$s\left(mp^k\right) \equiv s\left(mp^{k-1}\right) \pmod{p^k}$$

hold for all prime p and positive integers m, k [Stan'99, Ex. 5.2 (a), p. 72, and its solution on p. 104]. It therefore follows from Manyama's observation (2) that the sequence $a(n) = \text{A002003}(n)$ satisfies the Gauss congruences. In fact, calculation suggests that A002003 satisfies stronger supercongruences. Here is a particular case.

Proposition 1. *The supercongruence $a(p) \equiv a(1) \pmod{p^3}$ holds for prime $p \geq 5$.*

Proof. We rewrite the binomial sum representation (3) for $a(p)$ by separating out the first ($k = 0$) summand and last ($k = p$) summand and adding together the k-th and $(p-k)$-th summands for $1 \leq k \leq \frac{p-1}{2}$ to obtain

$$a(p) = \binom{2p-1}{p-1} + 1 + \sum_{k=1}^{\frac{p-1}{2}} \binom{p}{k}\left(\binom{2p-k-1}{p-1} + \binom{p+k-1}{p-1}\right).$$

Now by Wolstenholme's theorem [Mes'11, p. 3]

$$\binom{2p-1}{p-1} + 1 \equiv 2 \pmod{p^3}.$$

Hence

$$a(p) \equiv 2 + \sum_{k=1}^{\frac{p-1}{2}} \binom{p}{k}\left(\binom{2p-k-1}{p-1} + \binom{p+k-1}{p-1}\right) \pmod{p^3}. \tag{7}$$

To establish the Proposition we will show that each summand on the right side of (7) is divisible by p^3. Clearly, the first factor $\binom{p}{k}$ in each summand is divisible by p for k in the range of summation. Therefore, to prove the Proposition, it is enough to show that the second factor $\binom{2p-k-1}{p-1} + \binom{p+k-1}{p-1}$ is always divisible by p^2. To show this, we write the second factor as a product of two terms each of which is divisible by p.

One easily checks that

$$\binom{2p-k-1}{p-1}+\binom{p+k-1}{p-1} = \left\{\frac{(p+k-1)!}{k!(p-1)!(p-k)!}\right\}\left\{\frac{k!(2p-k-1)!}{(p+k-1)!}+(p-k)!\right\}. \tag{8}$$

The first factor on the right side of (8) is a rational number whose numerator is divisible by p since $k \geq 1$. Clearly, for k in the range $1 ... \frac{p-1}{2}$, the prime p cannot be a factor of the denominator. To show that the second factor on the right side of (8) is also divisible by p we first set $r = p - 2k \geq 1$. Then we have

$$\begin{aligned}\frac{k!(2p-k-1)!}{(p+k-1)!}+(p-k)! &= k!(2p-k-1)(2p-k-2)\cdots(2p-k-r)+(p-k)! \\ &\equiv (-1)^r k!(k+1)(k+2)\cdots(k+r)+(p-k)! \pmod p \\ &\equiv -(k+r)!+(p-k)! \pmod p \\ &\equiv -(p-k)!+(p-k)! \pmod p \\ &\equiv 0 \pmod p.\end{aligned}$$

We have shown that $\binom{2p-k-1}{p-1}+\binom{p+k-1}{p-1}$ is divisible by p^2 for $1 \leq k \leq \frac{p-1}{2}$, thus completing the proof of the Proposition. □

Conjecture. We conjecture that the more general supercongruences

$$a\left(mp^k\right) \equiv a\left(mp^{k-1}\right) \pmod{p^{3k}} \tag{9}$$

hold for prime $p \geq 5$ and all positive integers m and k.

Calculation suggests that the above approach of adding pairs of terms to get divisibility by powers of the prime p might extend to proving the general case.

A generalisation. We define a two parameter family of sequences $a_{(r,s)}(n)$ by

$$a_{(r,s)}(n) = [x^{rn}]\left(\frac{1+x}{1-x}\right)^{sn} \qquad r \in \mathbb{N}, s \in \mathbb{Z}. \tag{10}$$

In particular, $a_{(1,1)}(n) = \text{A002003}(n)$. Expanding the binomials in (10) and extracting the coefficient of x^n leads to the formula

$$a_{(r,s)}(n) = \sum_{k=0}^{sn}\binom{sn}{k}\binom{(r+s)n-k-1}{sn-1} \qquad n \geq 1. \tag{11}$$

We conjecture that the supercongruences

$$a_{(r,s)}\left(mp^k\right) \equiv a_{(r,s)}\left(mp^{k-1}\right) \pmod{p^{3k}} \tag{12}$$

hold for all prime $p \geq 5$ and $r \in \mathbb{N}$ and $s \in \mathbb{Z}$.

Another member of the family of sequences $a_{(r,s)}(n)$, already in the database, is $a_{(2,1)}(n) = \frac{1}{2}a_{(1,2)}(n) = \text{A103885}(n)$. Using the same method as in Proposition 1, one can show that $\text{A103885}(p) \equiv \text{A103885}(1) \pmod{p^3}$ holds for prime $p \geq 5$. We remark that $\text{A103885}(n) = [x^n]\, S(x)^n$ where $S(x) = \frac{1}{x}\text{Rev}\left(\frac{x(1+x)}{1-x}\right)$ is the o.g.f. of the sequence of large Schröder numbers A006318.

Table of values $a_{(r,s)}(n)$

r = 1

	$n=1$	2	3	4	5	6	7
$s=1$	2	8	38	192	1002	5336	28814
$s=2$	4	32	292	2816	28004	284000	2919620
$s=3$	6	72	978	14016	207006	3116952	47568618
$s=4$	8	128	2312	44032	864008	17282432	350353928
$s=5$	10	200	4510	107200	2625010	65520920	1657410310

r = 2

	$n=1$	2	3	4	5	6	7
$s=1$	2	16	146	1408	14002	142000	1459810
$s=2$	8	192	5336	157184	4780008	148321344	4666890936
$s=3$	18	912	53154	3281280	209070018	13591279920	895903147122
$s=4$	32	2816	284000	30316544	3339504032	375282559232	42760427177696
$s=5$	50	6800	1057730	174074240	29557550050	5119703270960	899105953178770

References

[Bal'15] Representing a sequence as [x{̂}n] G(x){̂}n, uploaded to A066398

[Mes'11] R. Mestrovic, Wolstenholme's theorem: Its Generalizations and Extensions in the last hundred and fifty years (1862-2011), arXiv:1111.3057 [math.NT], 2011.

[Stan'99] R. P. Stanley, Enumerative Combinatorics, Volume 2, Cambridge University Press, 1999