

LUCAS CONGRUENCES FOR THE APÉRY NUMBERS MODULO p^2

ERIC ROWLAND, REEM YASSAWI, AND CHRISTIAN KRATTENTHALER

ABSTRACT. The sequence $A(n)_{n \geq 0}$ of Apéry numbers can be interpolated to \mathbb{C} by an entire function. We give a formula for the Taylor coefficients of this function, centered at the origin, as a \mathbb{Z} -linear combination of multiple zeta values. We then show that for integers n whose base- p digits belong to a certain set, $A(n)$ satisfies a Lucas congruence modulo p^2 .

1. INTRODUCTION

For each integer $n \geq 0$, the n th Apéry number is defined by

$$A(n) := \sum_{k \geq 0} \binom{n}{k}^2 \binom{n+k}{k}^2.$$

These numbers arose in Apéry's proof of the irrationality of $\zeta(3)$. This sum is finite, since $\binom{n}{k} = 0$ when $k > n$. The sequence $A(n)_{n \geq 0}$ is

$$1, 5, 73, 1445, 33001, 819005, 21460825, 584307365, \dots$$

The Apéry numbers satisfy the recurrence

$$(1) \quad n^3 A(n) - (34n^3 - 51n^2 + 27n - 5)A(n-1) + (n-1)^3 A(n-2) = 0$$

for all integers $n \geq 2$.

Exceptional properties of the Apéry sequence have been observed in many settings [15]. Gessel [6] showed that the Apéry numbers satisfy the Lucas congruence

$$(2) \quad A(d+pn) \equiv A(d)A(n) \pmod{p}$$

for all $d \in \{0, 1, \dots, p-1\}$ and $n \geq 0$. Beukers [1] established the supercongruence $A(p^\alpha n - 1) \equiv A(p^{\alpha-1}n - 1) \pmod{p^{3\alpha}}$ for all primes $p \geq 5$, and Straub [13] showed that a related supercongruence holds more generally for a four-dimensional sequence containing $A(n)_{n \geq 0}$ as its diagonal.

Gessel also extended Congruence (2) to a congruence modulo p^2 as follows. Define the sequence $A'(n)_{n \geq 0}$ by

$$(3) \quad A'(n) := 2 \sum_{k=0}^n \binom{n}{k}^2 \binom{n+k}{k}^2 (H_{n+k} - H_{n-k}),$$

where $H_k = 1 + \frac{1}{2} + \dots + \frac{1}{k}$ is the k th harmonic number. The sequence $A'(n)_{n \geq 0}$ is

$$0, 12, 210, 4438, 104825, \frac{13276637}{5}, 70543291, \frac{67890874657}{35}, \dots$$

This paper was originally posted on the arXiv by the first two authors. Christian Krattenthaler became a coauthor after improving the proof of Theorem 1.

Then

$$(4) \quad A(d + pn) \equiv (A(d) + pnA'(d))A(n) \pmod{p^2}$$

for all $d \in \{0, 1, \dots, p-1\}$ and for all $n \geq 0$ [6, Theorem 4].

Gessel remarks that if $A(n)$ can be extended to a differentiable function $A(x)$ defined for $x \in \mathbb{R}_{\geq 0}$ such that $A(x)$ satisfies Recurrence (1), then $A'(n) = \left(\frac{d}{dx}A(x)\right)|_{x=n}$. As shown by Zagier [15, Proposition 1] and proved in an automated way by Osburn and Straub [10, Remark 2.5], $A(n)$ can be extended to an entire function $A(z)$ satisfying

$$(5) \quad \begin{aligned} z^3 A(z) - (34z^3 - 51z^2 + 27z - 5)A(z-1) + (z-1)^3 A(z-2) \\ = \frac{8}{\pi^2}(2z-1)(\sin(\pi z))^2 \end{aligned}$$

for all $z \in \mathbb{C}$. Since both $\frac{8}{\pi^2}(2z-1)(\sin(\pi z))^2$ and its derivative vanish at integer values of z , it follows that $A'(n) = \left(\frac{d}{dz}A(z)\right)|_{z=n}$, hence the notation $A'(n)$. Therefore the extension $A(z)$ confirms Gessel's intuition.

In this article we use an elementary approach to write the coefficients in the Taylor series of $A(z) = \sum_{m \geq 0} a_m z^m$ at $z = 0$ as an explicit \mathbb{Z} -linear combination of multiple zeta values. A striking fact is that the coefficient of each multiple zeta value is a signed power of 2. Let s_1, s_2, \dots, s_j be positive integers with $s_1 \geq 2$. The *multiple zeta value* $\zeta(s_1, s_2, \dots, s_j)$ is defined as

$$\zeta(s_1, s_2, \dots, s_j) := \sum_{n_1 > n_2 > \dots > n_j > 0} \frac{1}{n_1^{s_1} n_2^{s_2} \dots n_j^{s_j}}.$$

The *weight* of $\zeta(s_1, s_2, \dots, s_j)$ is $s_1 + s_2 + \dots + s_j$.

Let $\chi(m)$ be the characteristic function of the set of odd numbers. That is, $\chi(m) = 0$ if m is even and $\chi(m) = 1$ if m is odd. For a tuple $\mathbf{s} = (s_1, s_2, \dots, s_j)$, let $e(\mathbf{s}) = |\{i : 2 \leq i \leq j \text{ and } s_i = 2\}|$.

Theorem 1. *Let $A(z) = \sum_{m \geq 0} a_m z^m$ be the Taylor series of the Apéry function, centered at the origin. For each $m \geq 1$,*

$$a_m = \sum_{\mathbf{s}} (-1)^{\frac{m-s_1}{2}} 2^{e(\mathbf{s})+\chi(m)} \zeta(s_1, s_2, \dots, s_j),$$

where the sum is over all tuples $\mathbf{s} = (s_1, s_2, \dots, s_j)$, with $j \geq 1$, of non-negative integers satisfying

- $s_1 + s_2 + \dots + s_j = m$,
- $s_1 = 3$ if m is odd and $s_1 \in \{2, 4\}$ if m is even, and
- $s_i \in \{2, 4\}$ for all $i \in \{2, \dots, j\}$.

The first several coefficients are

$$\begin{aligned}
a_0 &= 1 \\
a_1 &= 0 \\
a_2 &= \zeta(2) \\
a_3 &= 2\zeta(3) \\
a_4 &= \zeta(4) - 2\zeta(2, 2) \\
a_5 &= -4\zeta(3, 2) \\
a_6 &= \zeta(2, 4) - 2\zeta(4, 2) + 4\zeta(2, 2, 2) \\
a_7 &= 2\zeta(3, 4) + 8\zeta(3, 2, 2) \\
a_8 &= \zeta(4, 4) - 2\zeta(2, 2, 4) - 2\zeta(2, 4, 2) + 4\zeta(4, 2, 2) - 8\zeta(2, 2, 2, 2) \\
a_9 &= -4\zeta(3, 2, 4) - 4\zeta(3, 4, 2) - 16\zeta(3, 2, 2, 2).
\end{aligned}$$

Let $F(m)$ be the m th Fibonacci number. Since the number of integer compositions of m using parts 1 and 2 is $F(m+1)$, Theorem 1 expresses a_m as a linear combination of $F(\frac{m}{2} + 1)$ multiple zeta values if m is even and $F(\frac{m-1}{2})$ multiple zeta values if m is odd.

Let $P(m)$ be the number of integer compositions of $m - 3$ using parts 2 and 3. Then $P(m)$ is the m th Padovan number and satisfies the recurrence $P(m) = P(m-2) + P(m-3)$ with initial conditions $P(3) = 1$, $P(4) = 0$, $P(5) = 1$. Let d_m be the dimension of the \mathbb{Q} -vector space spanned by the weight- m multiple zeta values. Recent progress by Brown [2] shows that $d_m \leq P(m+3)$. For $m \geq 13$, the representation of a_m in Theorem 1 uses fewer than $P(m+3)$ multiple zeta values. Since $F(\frac{m}{2} + 1) > P(m+3)$ for $m \in \{4, 6, 8, 10, 12\}$, this implies that $a_4, a_6, a_8, a_{10}, a_{12}$ can be written as \mathbb{Q} -linear combinations of fewer multiple zeta values than Theorem 1 provides. Namely,

$$\begin{aligned}
a_4 &= -\frac{1}{2}\zeta(4) \\
a_6 &= \frac{3}{2}\zeta(6) - 3\zeta(4, 2) \\
a_8 &= -\frac{13}{24}\zeta(8) + 6\zeta(4, 2, 2) \\
a_{10} &= \frac{7}{8}\zeta(10) + 3\zeta(2, 4, 4) - 12\zeta(4, 2, 2, 2) \\
a_{12} &= -\frac{915}{22112}\zeta(12) + 6\zeta(4, 2, 2, 4) + 6\zeta(4, 2, 4, 2) + 6\zeta(4, 4, 2, 2) + 24\zeta(4, 2, 2, 2, 2).
\end{aligned}$$

We prove Theorem 1 in Section 2. The proof technique can also be applied to compute the Taylor coefficients for a larger family of hypergeometric functions. We remark that there are some parallels between Theorem 1 and work of Cresson, Fischler, and Rivoal [4], who show that a class of hypergeometric series can be decomposed as \mathbb{Q} -linear combinations of multiple zeta values. Numerically, Golyshev and Zagier [7, Section 2.4] also obtained multiple zeta values in coefficients of a formal power series related to the Apéry numbers.

Returning to congruences for $A(n)$ in Section 3, we consider the following question. For which base- p digits d does Congruence (2) hold not just modulo p but modulo p^2 ? The following theorem characterizes such digits. Let

$$D(p) = \{d \in \{0, 1, \dots, p-1\} : A(d) \equiv A(p-1-d) \pmod{p^2}\}.$$

Theorem 2. *Let p be a prime, and let $d \in \{0, 1, \dots, p-1\}$. The congruence $A(d+pn) \equiv A(d)A(n) \pmod{p^2}$ holds for all $n \in \mathbb{Z}$ if and only if $d \in D(p)$.*

In particular, if n is a non-negative integer and all digits in its standard base- p representation $n_\ell \cdots n_1 n_0$ belong to $D(p)$, then

$$A(n) \equiv A(n_0)A(n_1) \cdots A(n_\ell) \pmod{p^2}.$$

Theorem 2 has an analogue for binomial coefficients, established by the first-named author [11].

2. TAYLOR COEFFICIENTS OF THE APÉRY FUNCTION

In this section we give a proof of Theorem 1. Let $\mathbb{N} = \{0, 1, 2, \dots\}$. The sequence $A(n)_{n \geq 0}$ can be interpolated to \mathbb{C} using the gamma function $\Gamma(z)$. Recall that $\Gamma(z)$ is a meromorphic function satisfying

$$\Gamma(1) = 1 \text{ and } \Gamma(z+1) = z\Gamma(z)$$

for $z \notin -\mathbb{N}$. The gamma function has simple poles at the non-positive integers.

For $n \geq 0$, we can write $A(n)$ as

$$\begin{aligned} A(n) &= \sum_{k \geq 0} \binom{n}{k}^2 \binom{n+k}{k}^2 \\ &= \sum_{k \geq 0} \frac{\Gamma(n+k+1)^2}{\Gamma(n-k+1)^2 \Gamma(k+1)^4}. \end{aligned}$$

We extend $A(n)$ to complex values by defining

$$A(z) = \sum_{k \geq 0} \frac{\Gamma(z+k+1)^2}{\Gamma(z-k+1)^2 \Gamma(k+1)^4}.$$

Note that for each $k \in \mathbb{N}$ the function $\frac{\Gamma(z+k+1)^2}{\Gamma(z-k+1)^2 \Gamma(k+1)^4}$ is a polynomial in z . Furthermore, for each $z \in \mathbb{C}$, the series $\sum_{k \geq 0} \frac{\Gamma(z+k+1)^2}{\Gamma(z-k+1)^2 \Gamma(k+1)^4}$ is locally uniformly convergent. Thus $A(z)$ is an entire function, which we call the *Apéry function*. We remark that $A(z)$ can be written using the hypergeometric function ${}_4F_3$. Let $(z)_k := z(z+1)(z+2) \cdots (z+k-1)$ be the Pochhammer symbol (rising factorial). By writing $\frac{\Gamma(z+k+1)^2}{\Gamma(z-k+1)^2} = (-z)_k^2 (z+1)_k^2$, we see that

$$\begin{aligned} (6) \quad A(z) &= \sum_{k \geq 0} \frac{(-z)_k (-z)_k (z+1)_k (z+1)_k}{k!^4} \\ &= {}_4F_3(-z, -z, z+1, z+1; 1, 1, 1; 1). \end{aligned}$$

Straub [13, Remark 1.3] proved the reflection formula $A(-1-n) = A(n)$ for all $n \in \mathbb{Z}$. Equation (6) shows that this formula also holds for non-integers, since the hypergeometric series is invariant under replacing z with $-1-z$.

Proposition 3. *For all $z \in \mathbb{C}$, we have $A(-1-z) = A(z)$.*

Figure 1 shows this symmetry on the real line. In light of Proposition 3, Theorem 1 also gives us the Taylor expansion of $A(z)$ at $z = -1$ for free. We note that, at the symmetry point $z = -\frac{1}{2}$, Zagier has shown that $A(-\frac{1}{2}) = \frac{16}{\pi^2} L(f, 2)$ where $L(f, 2)$ is the critical L -value of f , the unique normalized Hecke eigenform of weight 4 for $\Gamma_0(8)$; see [15] for an account and [16] for a generalization. There is no reason to expect that the Taylor coefficients of $A(z)$ centered at non-integer points are \mathbb{Q} -linear combinations of multiple zeta values.

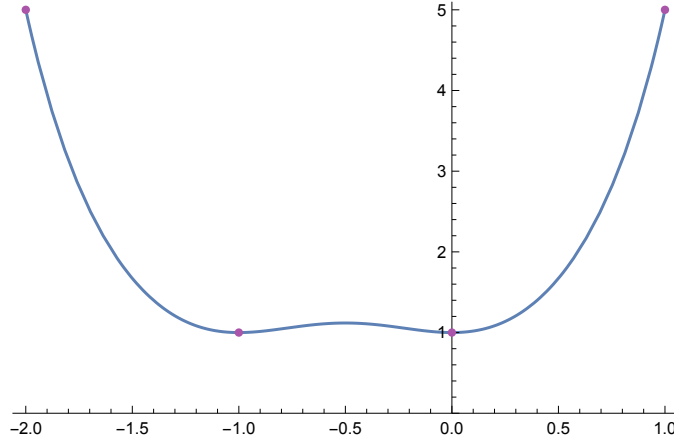


FIGURE 1. A plot of $A(z)$ for real z in the interval $-2 \leq z \leq 1$, showing the reflection symmetry $A(-1-z) = A(z)$.

Let

$$(7) \quad A(z) = \sum_{k \geq 0} \frac{\Gamma(z+k+1)^2}{\Gamma(z-k+1)^2 \Gamma(k+1)^4} = \sum_{m \geq 0} a_m z^m$$

be the Taylor series expansion of the Apéry function centered at the origin. It is possible to compute a_m by directly evaluating the m th derivative $A^{(m)}(z)$ at $z = 0$.

Example 4. The derivative of the summand is

$$\frac{1}{k!^4} \frac{d}{dz} \frac{\Gamma(z+k+1)^2}{\Gamma(z-k+1)^2} = \frac{1}{k!^4} \frac{\Gamma(z+k+1)^2}{\Gamma(z-k+1)^2} (2\psi(z+k+1) - 2\psi(z-k+1)),$$

where the digamma function $\psi(z) := \frac{\Gamma'(z)}{\Gamma(z)}$ is the logarithmic derivative of $\Gamma(z)$.

This agrees with the expression for $A'(n)$ in Equation (3). Since $\frac{\Gamma(z+k+1)^2}{\Gamma(z-k+1)^2} = O(z^2)$ as $z \rightarrow 0$ and $2\psi(z+k+1) - 2\psi(z-k+1)$ has a simple pole at 0 for each k , we have $a_1 = \frac{A'(0)}{1!} = 0$. Similarly, the second derivative is

$$\begin{aligned} \frac{1}{k!^4} \frac{d^2}{dz^2} \frac{\Gamma(z+k+1)^2}{\Gamma(z-k+1)^2} &= \frac{1}{k!^4} \frac{\Gamma(z+k+1)^2}{\Gamma(z-k+1)^2} (4\psi(z+k+1)^2 + 2\psi'(z+k+1) \\ &\quad - 8\psi(z+k+1)\psi(z-k+1) + 4\psi(z-k+1)^2 - 2\psi'(z-k+1)). \end{aligned}$$

The series expansions of $\psi(z+k+1)$ and $\psi(z-k+1)$ imply $A''(0) = \sum_{k \geq 1} \frac{2}{k^2} = 2\zeta(2)$, so $a_2 = \frac{A''(0)}{2!} = \zeta(2)$.

Theorem 1 can be proved by carrying out the same approach for general m . However, we give a shorter proof in the spirit of [5, Section 1.4].

Proof of Theorem 1. We consider the summand in Equation (7). For $k = 0$, we have $\frac{\Gamma^2(z+k+1)}{\Gamma^2(z-k+1)k!^4} = 1$. For $k \geq 1$, we have

$$\begin{aligned}
(8) \quad \frac{\Gamma^2(z+k+1)}{\Gamma^2(z-k+1)k!^4} &= \frac{(z-k+1)^2 \cdots (z-1)^2 z^2 (z+1)^2 \cdots (z+k)^2}{k!^4} \\
&= \left(1 - \frac{z}{k-1}\right)^2 \cdots \left(1 - \frac{z}{1}\right)^2 \left(1 + \frac{z}{1}\right)^2 \cdots \left(1 + \frac{z}{k-1}\right)^2 \frac{z^2}{k^2} \left(1 + \frac{z}{k}\right)^2 \\
&= \left(1 - \frac{z^2}{(k-1)^2}\right)^2 \cdots \left(1 - \frac{z^2}{1^2}\right)^2 \frac{z^2}{k^2} \left(1 + \frac{z}{k}\right)^2 \\
&= \left(1 - 2\frac{z^2}{1^2} + \frac{z^4}{1^4}\right) \cdots \left(1 - 2\frac{z^2}{(k-1)^2} + \frac{z^4}{(k-1)^4}\right) \left(\frac{z^2}{k^2} + 2\frac{z^3}{k^3} + \frac{z^4}{k^4}\right).
\end{aligned}$$

Recall that $\chi(m)$ is the characteristic function of the set of odd numbers, and $e(\mathbf{s}) = |\{i : 2 \leq i \leq j \text{ and } s_i = 2\}|$ for a tuple $\mathbf{s} = (s_1, s_2, \dots, s_j)$. By expanding the product (8) to extract the coefficient of z^m , one sees that this coefficient equals

$$\sum_{\substack{\mathbf{s}=(s_1, \dots, s_j) \\ s_1 + \dots + s_j = m}} \sum_{k=n_1 > n_2 > \dots > n_j > 0} (-1)^{\frac{m-s_1}{2}} 2^{e(\mathbf{s}) + \chi(m)} \frac{1}{n_1^{s_1} n_2^{s_2} \cdots n_j^{s_j}},$$

where the outer sum is over all \mathbf{s} described in the statement of Theorem 1. Now we sum over all k to obtain a_m , and the statement follows. \square

As discussed in Section 1, the coefficients $a_4, a_6, a_8, a_{10}, a_{12}$ can be written as \mathbb{Q} -linear combinations of fewer multiple zeta values than given by Theorem 1. The strategy given in the following example can be used to reduce a_m for all even $m \geq 4$.

Example 5. For $m = 10$, Theorem 1 gives

$$\begin{aligned}
a_{10} &= \zeta(2, 4, 4) - 2\zeta(4, 2, 4) - 2\zeta(4, 4, 2) \\
&\quad + 4\zeta(2, 2, 2, 4) + 4\zeta(2, 2, 4, 2) + 4\zeta(2, 4, 2, 2) - 8\zeta(4, 2, 2, 2) \\
&\quad + 16\zeta(2, 2, 2, 2, 2).
\end{aligned}$$

We will rewrite several products $\zeta(s_1, s_2, \dots, s_j)\zeta(i)$ as linear combinations of multiple zeta values. For example,

$$\begin{aligned}
&\left(\sum_{k_1 > k_2 > 0} \frac{1}{k_1^a k_2^b}\right) \left(\sum_{k_3 > 0} \frac{1}{k_3^c}\right) \\
&= \sum_{k_3 > k_1 > k_2 > 0} \frac{1}{k_1^a k_2^b k_3^c} + \sum_{k_1 > k_3 > k_2 > 0} \frac{1}{k_1^a k_2^b k_3^c} + \sum_{k_1 > k_2 > k_3 > 0} \frac{1}{k_1^a k_2^b k_3^c} \\
&\quad + \sum_{k_1 > k_2 > 0} \frac{1}{k_1^{a+c} k_2^b} + \sum_{k_1 > k_2 > 0} \frac{1}{k_1^a k_2^{b+c}},
\end{aligned}$$

so that

$$(9) \quad \zeta(a, b)\zeta(c) = \zeta(c, a, b) + \zeta(a, c, b) + \zeta(a, b, c) + \zeta(a+c, b) + \zeta(a, b+c).$$

As in the derivation of Equation (9), we have $\zeta(a)\zeta(b) = \zeta(a, b) + \zeta(b, a) + \zeta(a+b)$.

We first express $-2\zeta(4, 2, 4) - 2\zeta(4, 4, 2)$ in terms of $\zeta(2, 4, 4)$ and $\zeta(10)$. By (9) we have

$$\zeta(4, 4)\zeta(2) = \zeta(2, 4, 4) + \zeta(4, 2, 4) + \zeta(4, 4, 2) + \zeta(6, 4) + \zeta(4, 6).$$

The relations $\zeta(4)\zeta(4) = 2\zeta(4, 4) + \zeta(8)$ and $\zeta(4)\zeta(6) = \zeta(4, 6) + \zeta(6, 4) + \zeta(10)$ allow us to write

$$\begin{aligned} -2\zeta(4, 2, 4) - 2\zeta(4, 4, 2) &= 2\zeta(2, 4, 4) + 2\zeta(4)\zeta(6) - 2\zeta(10) - \zeta(4)^2\zeta(2) + \zeta(8)\zeta(2) \\ &= 2\zeta(2, 4, 4) - \frac{3}{40}\zeta(10) \end{aligned}$$

using $\zeta(2) = \frac{\pi^2}{6}$, $\zeta(4) = \frac{\pi^4}{90}$, $\zeta(6) = \frac{\pi^6}{945}$, $\zeta(8) = \frac{\pi^8}{9450}$, and $\zeta(10) = \frac{\pi^{10}}{93555}$. Next we rewrite

$$4\zeta(2, 2, 2, 4) + 4\zeta(2, 2, 4, 2) + 4\zeta(2, 4, 2, 2).$$

For this we use

$$\begin{aligned} \zeta(2, 2, 2)\zeta(4) - \zeta(2, 2, 2, 4) - \zeta(2, 2, 4, 2) - \zeta(2, 4, 2, 2) - \zeta(4, 2, 2, 2) \\ &= \zeta(2, 2, 6) + \zeta(2, 6, 2) + \zeta(6, 2, 2) \\ &= \zeta(2, 2)\zeta(6) - (\zeta(8, 2) + \zeta(2, 8)) \\ &= \zeta(2, 2)\zeta(6) - (\zeta(2)\zeta(8) - \zeta(10)). \end{aligned}$$

Therefore $4\zeta(2, 2, 2, 4) + 4\zeta(2, 2, 4, 2) + 4\zeta(2, 4, 2, 2)$ can be written using $\zeta(2, 2)\zeta(6)$, $\zeta(2, 2, 2)\zeta(4)$, $\zeta(4, 2, 2, 2)$, and $\zeta(10)$. Finally, we use

$$\zeta(\underbrace{2, \dots, 2}_j) = \frac{\pi^{2j}}{(2j+1)!}$$

(see for example [8]) to write $\zeta(2, 2)$, $\zeta(2, 2, 2)$, and $\zeta(2, 2, 2, 2, 2)$. Consolidating these results, we obtain

$$a_{10} = \frac{7}{8}\zeta(10) + 3\zeta(2, 4, 4) - 12\zeta(4, 2, 2, 2).$$

3. LUCAS CONGRUENCES MODULO p^2

Gessel [6] proved three theorems on congruences for $A(n)$ where $n \geq 0$. In this section we generalize these theorems to $n \in \mathbb{Z}$, making substantial use of the reflection formula $A(-1-z) = A(z)$ from Proposition 3. We simplify one of the arguments by using the fact that we can differentiate $A(z)$. We then use these congruences to prove Theorem 2.

First we generalize Gessel's result that the Apéry numbers satisfy a Lucas congruence modulo p [6, Theorem 1].

Theorem 6. *Let p be a prime. For all $d \in \{0, 1, \dots, p-1\}$ and for all $n \in \mathbb{Z}$, we have $A(d+pn) \equiv A(d)A(n) \pmod{p}$.*

Proof. Gessel proved the statement for $n \geq 0$. Let $n \leq -1$. By Proposition 3,

$$\begin{aligned} A(d+pn) &= A(-1-(d+pn)) \\ &= A((p-1-d)+p(-1-n)) \\ &\equiv A(p-1-d)A(-1-n) \pmod{p} \\ &= A(p-1-d)A(n). \end{aligned}$$

Malik and Straub [9, Lemma 6.2] proved that $A(p-1-d) \equiv A(d) \pmod{p}$, which completes the proof. \square

Next we generalize Gessel's congruence for $A(pn)$ modulo p^3 for $p \geq 5$ and variants for $p = 2$ and $p = 3$ [6, Theorem 3].

Theorem 7. *For all $n \in \mathbb{Z}$,*

- $A(n) \equiv 5^n \pmod{8}$ for all $n \geq 0$ and $A(n) \equiv 5^{n+1} \pmod{8}$ for all $n \leq -1$,
- $A(d+3n) \equiv A(d)A(n) \pmod{9}$ for all $d \in \{0, 1, 2\}$, and
- $A(pn) \equiv A(n) \equiv A(pn+p-1) \pmod{p^3}$ for all primes $p \geq 5$.

A special case of a theorem of Straub [13, Theorem 1.2] shows that $A(pn) \equiv A(n) \pmod{p^3}$ for all $n \in \mathbb{Z}$ and all primes $p \geq 5$. We prove this result another way, using an approach similar to Gessel's.

Proof of Theorem 7. Gessel proved $A(n) \equiv 5^n \pmod{8}$ for all $n \geq 0$. For $n \leq -1$, we use Proposition 3 to write

$$\begin{aligned} A(n) &= A(-1-n) \equiv 5^{-1-n} \pmod{8} \\ &\equiv 5^{1+n} \pmod{8} \end{aligned}$$

since $5^{-1} \equiv 5 \pmod{8}$.

For $p = 3$, the proof is similar to the proof of Theorem 6. Gessel proved the statement for $n \geq 0$, so for $n \leq -1$ we have

$$\begin{aligned} A(d+3n) &= A(-1-(d+3n)) \\ &= A((2-d)+3(-1-n)) \\ &\equiv A(2-d)A(-1-n) \pmod{9} \\ &\equiv A(d)A(n) \pmod{9} \end{aligned}$$

since one checks that $A(2-d) \equiv A(d) \pmod{9}$.

Let $p \geq 5$. Gessel proved $A(pn) \equiv A(n) \pmod{p^3}$ for all $n \geq 0$. We show $A(pn+p-1) \equiv A(n) \pmod{p^3}$ for all $n \geq 0$. We write

$$\begin{aligned} A(pn+p-1) &= \sum_{k=0}^{pn+p-1} \binom{pn+p-1}{k}^2 \binom{pn+p-1+k}{k}^2 \\ &= \sum_{d=0}^{p-1} \sum_{m=0}^n \binom{pn+p-1}{pm+d}^2 \binom{p(n+m+1)+d-1}{pm+d}^2 \\ &= \sum_{d=0}^{p-1} \sum_{m=0}^n \binom{pn+p-1}{pm+d}^2 \frac{p^2(n+1)^2}{(p(n+m+1)+d)^2} \binom{p(n+m+1)+d}{pm+d}^2 \\ &= S_0 + S_1 \end{aligned}$$

where

$$S_0 = \sum_{m=0}^n \binom{pn+p-1}{pm}^2 \frac{(n+1)^2}{(n+m+1)^2} \binom{p(n+m+1)}{pm}^2$$

is the summand for $d = 0$, and

$$S_1 = \sum_{d=1}^{p-1} \sum_{m=0}^n \binom{pn+p-1}{pm+d}^2 \frac{p^2(n+1)^2}{(p(n+m+1)+d)^2} \binom{p(n+m+1)+d}{pm+d}^2.$$

For S_0 , we have

$$\begin{aligned} S_0 &= \sum_{m=0}^n \frac{(pn + p - pm)^2}{(pn + p)^2} \binom{pn + p}{pm}^2 \frac{(n + 1)^2}{(n + m + 1)^2} \binom{p(n + m + 1)}{pm}^2 \\ &\equiv \sum_{m=0}^n \frac{(n - m + 1)^2}{(n + m + 1)^2} \binom{n + 1}{m}^2 \binom{n + m + 1}{m}^2 \pmod{p^3} \\ &= \sum_{m=0}^n \binom{n}{m}^2 \binom{n + m}{m}^2 \\ &= A(n) \end{aligned}$$

by Jacobsthal's congruence $\binom{pa}{pb} \equiv \binom{a}{b} \pmod{p^3}$, which holds for all primes $p \geq 5$ [3].

For S_1 , we have

$$\begin{aligned} S_1 &\equiv p^2 \sum_{d=1}^{p-1} \sum_{m=0}^n \binom{pn + p - 1}{pm + d}^2 \frac{(n + 1)^2}{d^2} \binom{p(n + m + 1) + d}{pm + d}^2 \pmod{p^3} \\ &\equiv p^2 \sum_{d=1}^{p-1} \sum_{m=0}^n \binom{p-1}{d}^2 \binom{n}{m}^2 \frac{(n + 1)^2}{d^2} \binom{d}{d}^2 \binom{n + m + 1}{m}^2 \pmod{p^3} \end{aligned}$$

by the Lucas congruence for binomial coefficients modulo p . Since

$$\binom{p-1}{d} = \frac{(p-1)(p-2)\cdots(p-d)}{1 \cdot 2 \cdots d} \equiv \frac{(-1)(-2)\cdots(-d)}{1 \cdot 2 \cdots d} \equiv (-1)^d \pmod{p},$$

we obtain

$$\begin{aligned} S_1 &\equiv p^2 \left(\sum_{d=1}^{p-1} \frac{1}{d^2} \right) \sum_{m=0}^n \binom{n}{m}^2 (n + 1)^2 \binom{n + m + 1}{m}^2 \pmod{p^3} \\ &\equiv 0 \pmod{p^3} \end{aligned}$$

since $\sum_{d=1}^{p-1} \frac{1}{d^2} \equiv 0 \pmod{p}$, as established by Wolstenholme [14]. Therefore $A(pn + p - 1) = S_0 + S_1 \equiv A(n) \pmod{p^3}$.

Now for $n \leq -1$ we have

$$\begin{aligned} A(pn) &= A(-1 - pn) \\ &= A((p-1) + p(-1 - n)) \\ &\equiv A(-1 - n) \pmod{p^3} \\ &= A(n) \end{aligned}$$

and

$$\begin{aligned} A(pn + p - 1) &= A(-1 - (pn + p - 1)) \\ &= A(p(-1 - n)) \\ &\equiv A(-1 - n) \pmod{p^3} \\ &= A(n). \end{aligned} \quad \square$$

Finally, we generalize Gessel's congruence for $A(d+pn)$ modulo p^2 [6, Theorem 4]. Recall that $A'(n)$ is given by Equation (3). Since $A'(n) \in \mathbb{Q}$ for every $n \geq 0$, it follows that if the denominator of $A'(n)$ is not divisible by p then we can interpret $A'(n)$ modulo p^2 .

Theorem 8. *Let p be a prime, and let $d \in \{0, 1, \dots, p-1\}$. The denominator of $A'(d)$ is not divisible by p . Moreover, for all $n \in \mathbb{Z}$,*

$$(10) \quad A(d+pn) \equiv (A(d) + pnA'(d))A(n) \pmod{p^2}.$$

Proof. Gessel proved the statement for $n \geq 0$. The same approach allows us to prove the general case.

Fix $n \in \mathbb{Z}$. For each $d \in \{0, 1, \dots, p-1\}$, define $c_d \in \{0, 1, \dots, p-1\}$ such that $A(d+pn) \equiv A(d)A(n) + pc_d \pmod{p^2}$; this can be done by Theorem 6. Let $c_{-1} = 0$. (The value of c_{-1} does not actually matter, since it will be multiplied by 0.) We show that $(c_d)_{0 \leq d \leq p-1}$ and $(nA'(d)A(n))_{0 \leq d \leq p-1}$ satisfy the same recurrence and initial conditions modulo p ; this will imply $c_d \equiv nA'(d)A(n) \pmod{p}$. Theorem 7 implies that $A(pn) \equiv A(n) \pmod{p^2}$, so $c_0 = 0$. Since $A'(0) = 0$, the initial conditions are equal.

Let $d \in \{1, 2, \dots, p-1\}$. Write Equation (1) as

$$(11) \quad \sum_{i=0}^2 r_i(n)A(n-i) = 0,$$

where each $r_i(n)$ is a polynomial in n with integer coefficients. Note that Equation (11) holds for all $n \in \mathbb{Z}$. Substituting $d+pn$ for n in Equation (11) gives

$$\sum_{i=0}^2 r_i(d+pn)A(d-i+pn) = 0.$$

If $d-i = -1$ then $r_i(d+pn) = r_2(1+pn) = (pn)^3 \equiv 0 \pmod{p^2}$, hence the arbitrary value of c_{-1} . Therefore, using the Taylor expansion of $r_i(n)$, we have

$$\sum_{i=0}^2 (r_i(d) + pnr'_i(d))(A(d-i)A(n) + pc_{d-i}) \equiv 0 \pmod{p^2}.$$

Since $\sum_{i=0}^2 r_i(d)A(d-i) = 0$, expanding and dividing by p gives

$$\sum_{i=0}^2 (r_i(d)c_{d-i} + nr'_i(d)A(d-i)A(n)) \equiv 0 \pmod{p}.$$

This gives a recurrence satisfied by $(c_d)_{0 \leq d \leq p-1}$ that can be used to compute c_1, c_2, \dots, c_{p-1} since $r_0(d) = d^3 \not\equiv 0 \pmod{p}$.

To obtain a recurrence for $(nA'(d)A(n))_{0 \leq d \leq p-1}$, we differentiate Equation (5) to obtain

$$\sum_{i=0}^2 (r_i(d)A'(d-i) + r'_i(d)A(d-i)) = 0.$$

Since $A'(0)$ and $A'(1)$ are integers and $r_0(d) \not\equiv 0 \pmod{p}$, the denominator of $A'(d)$ is not divisible by p . By multiplying by $nA(n)$, we obtain

$$\sum_{i=0}^2 (r_i(d)nA'(d-i)A(n) + nr'_i(d)A(d-i)A(n)) = 0.$$

By subtracting this from the recurrence for $(c_d)_{0 \leq d \leq p-1}$, we see that

$$\sum_{i=0}^2 r_i(d)(c_{d-i} - nA'(d-i)A(n)) \equiv 0 \pmod{p}.$$

Since $r_0(d) \not\equiv 0 \pmod{p}$, it follows that $c_d \equiv nA'(d)A(n) \pmod{p}$ for all $d \in \{0, 1, \dots, p-1\}$. \square

In the case $p = 3$, Theorem 8 gives a second proof of the congruence $A(d+3n) \equiv A(d)A(n) \pmod{9}$ from Theorem 7, since $A'(0) \equiv A'(1) \equiv A'(2) \equiv 0 \pmod{3}$. For larger primes, in general $A(d+pn) \not\equiv A(d)A(n) \pmod{p^2}$. However, if we restrict to certain sets of base- p digits, then we do obtain congruences that hold modulo p^2 . For example, if $d \in \{0, 2, 4\}$, then

$$A(d+5n) \equiv A(d)A(n) \pmod{25}.$$

This was proven by the authors [12] by computing an automaton for $A(n) \pmod{25}$. Since $A(0) \equiv 1 \equiv A(4) \pmod{25}$ and $A(2) \equiv 23 \pmod{25}$, this implies $A(n) \equiv 23^{e_2(n)} \pmod{25}$ for all $n \geq 0$ whose base-5 digits belong to $\{0, 2, 4\}$, where $e_2(n)$ is the number of 2s in the base-5 representation of n . Theorem 2, reformulated as the following theorem, generalizes this result to other primes.

We say that the set $D \subseteq \{0, 1, \dots, p-1\}$ supports a *Lucas congruence* for the sequence $s(n)_{n \in \mathbb{Z}}$ modulo p^α if $s(d+pn) \equiv s(d)s(n) \pmod{p^\alpha}$ for all $d \in D$ and for all $n \in \mathbb{Z}$. As mentioned in the proof of Theorem 6, Malik and Straub [9, Lemma 6.2] proved that $A(d) \equiv A(p-1-d) \pmod{p}$ for each $d \in \{0, 1, \dots, p-1\}$. Let $D(p)$ be the set of base- p digits for which this congruence holds modulo p^2 ; that is,

$$D(p) = \{d \in \{0, 1, \dots, p-1\} : A(d) \equiv A(p-1-d) \pmod{p^2}\}.$$

Theorem 9. *The set $D(p)$ is the maximum set of digits that supports a Lucas congruence for the Apéry numbers modulo p^2 .*

Proof. Let $d \in D(p)$, so that $A(d) \equiv A(p-1-d) \pmod{p^2}$. Letting $n = -1$ in Theorem 8 gives $A(d-p) \equiv A(d) - pA'(d) \pmod{p^2}$. Applying Proposition 3, we find

$$\begin{aligned} pA'(d) &\equiv A(d) - A(d-p) \pmod{p^2} \\ &= A(d) - A(p-1-d) \\ &\equiv 0 \pmod{p^2}. \end{aligned}$$

Therefore it follows from Theorem 8 that, for all $n \in \mathbb{Z}$,

$$\begin{aligned} A(d+pn) &\equiv (A(d) + pnA'(d))A(n) \pmod{p^2} \\ &\equiv A(d)A(n) \pmod{p^2}. \end{aligned}$$

Therefore $D(p)$ supports a Lucas congruence for the Apéry numbers modulo p^2 .

To see that $D(p)$ is the maximum such set, assume $A(d+pn) \equiv A(d)A(n) \pmod{p^2}$ for all $n \in \mathbb{Z}$. Then

$$\begin{aligned} (A(d) + pnA'(d))A(n) &\equiv A(d+pn) \pmod{p^2} \\ &\equiv A(d)A(n) \pmod{p^2}, \end{aligned}$$

and it follows that $pnA'(d)A(n) \equiv 0 \pmod{p^2}$ for all $n \in \mathbb{Z}$. Therefore $A(d) - A(p-1-d) = A(d) - A(d-p) \equiv pA'(d) \equiv 0 \pmod{p^2}$. \square

As a special case, we obtain the following congruence, since $\{0, p-1\} \subseteq D(p)$ by Theorem 7, and $A(0) = 1 \equiv A(p-1) \pmod{p^2}$.

Corollary 10. *Let $p \neq 2$ and $n \geq 0$. If the base- p digits of n all belong to $\{0, \frac{p-1}{2}, p-1\}$, then $A(n) \equiv A(\frac{p-1}{2})^{e(n)} \pmod{p^2}$ where $e(n)$ is the number of occurrences of the digit $\frac{p-1}{2}$.*

These are the first several primes with digit sets $D(p)$ containing at least 4 digits:

p	$D(p)$
7	$\{0, 2, 3, 4, 6\}$
23	$\{0, 7, 11, 15, 22\}$
43	$\{0, 5, 18, 21, 24, 37, 42\}$
59	$\{0, 6, 29, 52, 58\}$
79	$\{0, 18, 39, 60, 78\}$
103	$\{0, 17, 51, 85, 102\}$
107	$\{0, 14, 21, 47, 53, 59, 85, 92, 106\}$
127	$\{0, 17, 63, 109, 126\}$
131	$\{0, 62, 65, 68, 130\}$
139	$\{0, 68, 69, 70, 138\}$
151	$\{0, 19, 75, 131, 150\}$
167	$\{0, 35, 64, 83, 102, 131, 166\}$

A natural question, which we do not address here, is the following. How big can $|D(p)|$ be, as a function of p ?

Theorem 7 implies the following Lucas congruence modulo p^3 .

Theorem 11. *Let $p \geq 5$ and $n \geq 0$. If the base- p digits of n all belong to $\{0, p-1\}$, then $A(n) \equiv 1 \pmod{p^3}$.*

Experiments do not suggest the existence of any additional Lucas congruences for the Apéry numbers modulo p^3 . We leave this as open question.

ACKNOWLEDGEMENT

We thank Manon Stipulanti for productive discussions.

REFERENCES

- [1] Frits Beukers, Some congruences for the Apéry numbers, *Journal of Number Theory* **21** (1985) 141–155.
- [2] Francis Brown, Mixed Tate motives over \mathbb{Z} , *Annals of Mathematics* **175** (2012) 949–976.
- [3] V. Brun, J. O. Stubban, J. E. Fjeldstad, R. Tambs Lyche, K. E. Aubert, W. Ljunggren, and E. Jacobsthal, On the divisibility of the difference between two binomial coefficients, *Skandinaviske Matematikerkongress* **11** (1949) 42–54.
- [4] J. Cresson, J. S. Fischler, and T. Rivoal, Séries hypergéométriques multiples et polyzêtas, *Bulletin de la Société Mathématique de France* **136** (2008) 97–145.
- [5] Stéphane Fischler, Irrationalité de valeurs de zêta (d’après Apéry, Rivoal, ...), *Astérisque* **294** (2004) 27–62.
- [6] Ira Gessel, Some congruences for Apéry numbers, *Journal of Number Theory* **14** (1982) 362–368.
- [7] Vasily V. Golyshev and Don Zagier, Proof of the gamma conjecture for Fano 3-folds of Picard rank 1, *Izvestiya: Mathematics* **80** (2016) 24–49.
- [8] Michael E. Hoffman, Multiple harmonic series, *Pacific Journal of Mathematics* **152** (1992) 275–290.
- [9] Amita Malik and Armin Straub, Divisibility properties of sporadic Apéry-like numbers, *Research in Number Theory* **2** (2016) Article 5.
- [10] Robert Osburn and Armin Straub, Interpolated sequences and critical L -values of modular forms, Chapter 14 in *Elliptic Integrals, Elliptic Functions and Modular Forms in Quantum Field Theory* (2019), Texts & Monographs in Symbolic Computation, Springer.

- [11] Eric Rowland, Lucas' theorem modulo p^2 , to appear in *The American Mathematical Monthly*.
- [12] Eric Rowland and Reem Yassawi, Automatic congruences for diagonals of rational functions, *Journal de Théorie des Nombres de Bordeaux* **27** (2015) 245–288.
- [13] Armin Straub, Multivariate Apéry numbers and supercongruences of rational functions, *Algebra & Number Theory* **8** (2014) 1985–2008.
- [14] Joseph Wolstenholme, On certain properties of prime numbers, *The Quarterly Journal of Pure and Applied Mathematics* **5** (1862) 35–39.
- [15] Don Zagier, Arithmetic and topology of differential equations, *Proceedings of the 2016 ECM* (2017).
- [16] Wadim Zudilin, A hypergeometric version of the modularity of rigid Calabi–Yau manifolds, *Symmetry, Integrability and Geometry: Methods and Applications* **14** (2018) Article 086, 16 pages.

DEPARTMENT OF MATHEMATICS, HOFSTRA UNIVERSITY, HEMPSTEAD, NY, USA

SCHOOL OF MATHEMATICS AND STATISTICS, OPEN UNIVERSITY, MILTON KEYNES, UK

FAKULTÄT FÜR MATHEMATIK, UNIVERSITÄT WIEN, VIENNA, AUSTRIA