Galois Groups of Apéry-like Series Modulo Primes

Xavier Caruso, Florian Fürnsinn, Daniel Vargas-Montoya and Wadim Zudilin

October 28, 2025

Abstract

We compute the Galois groups of the reductions modulo the prime numbers p of the generating series of Apéry numbers, Domb numbers and Almkvist–Zudilin numbers. We observe in particular that their behavior is governed by congruence conditions on p.

1 Introduction

The *Apéry numbers*

$$\alpha_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{n}^2 \quad \text{for } n = 0, 1, 2, \ldots$$

are a famous sequence of integer numbers, mostly known for playing a prominent role in Apéry's proof [Apé79] of the irrationality of $\zeta(3)$. Their generating series $f_\alpha \coloneqq \sum_{n=0}^{\infty} \alpha_n t^n$ enjoys many interesting properties. It is *D-finite*, i.e., it satisfies a linear differential equation with polynomial coefficients. Starting from the differential equation, integrality of the coefficients of its solutions is highly remarkable. Further, the Apéry numbers grow in a controlled manner, making their generating series a *G-function*. Moreover, letting p be an odd prime number, it is known [Ges82, Theorem 1] that the Apéry numbers have the *p-Lucas property* for all prime numbers p (see also the general result for Apéry-like numbers in [MS16]). That is, we have $\alpha_{np+\ell} \equiv \alpha_n \alpha_\ell \pmod{p}$ whenever $0 \le \ell < p$. On the level of generating functions this property translates to the congruence $f_\alpha \equiv A_p \cdot f_\alpha^p \pmod{p}$, where $A_p \coloneqq \sum_{n=0}^{p-1} \alpha_n t^n$ denotes the truncation of f_α at order p. This relation also shows that the reduction of the generating function $f_\alpha \bmod p$ is algebraic over the field of rational functions $\mathbb{F}_p(t)$ and that the extension it generates is Kummer.

Algebraicity modulo (almost) all primes p is a phenomenon observed for many classes of D-finite series. More precisely, for *diagonals* of multivariate rational, or, equivalently, algebraic functions this is a consequence of a theorem of Furstenberg [Fur67]. For *hypergeometric functions* this can be deduced from work by Christol [Chr86a] and was made explicit by Vargas-Montoya [Var21]. Further, if Christol's Conjecture [Chr86b] proves to be true, the result of Furstenberg would apply to all *globally bounded* D-finite series.

Having algebraic equations for the generating function modulo prime numbers, it is natural to consider their Galois groups for each prime number p. For D-finite series whose reductions modulo infinitely many prime numbers p are algebraic, in [CFV25] it was (conjecturally) observed that these Galois groups show some uniformity properties across different primes, and seem to be related to the *differential Galois group* of the minimal differential equation satisfied by the series. As an example in [CFV25, § 2.1.5], the Galois groups of the reductions of the Apéry series were computed for many prime numbers using a computer algebra system. However, the pattern that unfolded was stated without a proof, and the aim of this text is to provide one.

Fixing a prime number p and starting from the algebraic relation given by the p-Lucas property, the Galois group of $f_\alpha \bmod p$ can canonically be seen as a subgroup of $\mathbb{F}_p^\times$ *via* the embedding

$$\begin{array}{rcl} \mathrm{Gal}\left(\mathbb{F}_p(t, f_\alpha)/\mathbb{F}_p(t)\right) & \longrightarrow & \mathbb{F}_p^\times \\ \sigma & \mapsto & \sigma(f_\alpha)/f_\alpha. \end{array}$$

We aim to determine the image of the above map. Throughout the article, we denote by S the unique subgroup of $\mathbb{F}_p^\times$ of index 2; it is its subgroup of squares, hence the notation.

Theorem 1.

- *If* $p \equiv 1, 5, 7, 11 \pmod{24}$, *then* $\operatorname{Gal}\left(\mathbb{F}_p(t, f_\alpha)/\mathbb{F}_p(t)\right) = S$.
- *If* $p \equiv 13, 17, 19, 23 \pmod{24}$, *then* $\operatorname{Gal}\left(\mathbb{F}_p(t, f_\alpha)/\mathbb{F}_p(t)\right) = \mathbb{F}_p^\times$.

This result is the Galois theoretic shadow of the following factorization property of A_p.

Theorem 2. *There exists a polynomial* $B_p \in \mathbb{F}_p[t]$ *such that*

- *if* $p \equiv 1, 5, 7, 11 \pmod{24}$, *then* $A_p = B_p^2$,
- *if* $p \equiv 13, 17, 19, 23 \pmod{24}$, *then* $A_p = (t^2 - 34t + 1) \cdot B_p^2$.

The main ingredient in our proof is the fact that the Apéry series f_α is related to the generating function of the *Franel numbers*

$$h := \sum_{n=0}^{\infty} \sum_{k=0}^{n} \binom{n}{k}^3 x^n$$

by a simple rational substitution, namely $f_\alpha = (1+x) \cdot h^2$ where the variables t and x are linked by the relation $t = \frac{x(1-8x)}{1+x}$.

The sequence of Apéry numbers has two companions: the (alternating version of the) Domb numbers

$$\delta_n = (-1)^n \sum_{k=0}^{n} \binom{2k}{k} \binom{2n-2k}{n-k} \binom{n}{k}^2 \quad \text{for } n = 0, 1, 2, \dots$$

and the Almkvist–Zudilin numbers

$$\xi_n = \sum_{k=0}^{n} (-1)^{n-k} 3^{n-3k} \frac{(3k)!}{k!^3} \binom{n}{3k} \binom{n+k}{n} \quad \text{for } n = 0, 1, 2, \dots,$$

in the following sense: These three sequences satisfy similar difference equations of order 2 and degree 3, and their generating series

$$f_\alpha = \sum_{n=0}^{\infty} \alpha_n t^n, \quad f_\delta = \sum_{n=0}^{\infty} \delta_n t^n \quad \text{and} \quad f_\xi = \sum_{n=0}^{\infty} \xi_n t^n$$

admit modular parameterizations via the Hauptmoduln of the three subgroups of index 2 lying between $\Gamma_0(6)$ and its normalizer in $\mathrm{SL}_2(\mathbb{R})$ (see [CV09] and [CZ10]).

Thanks to [CZ10, Theorem 2.2], the argument for f_α extends to the series f_δ and f_ξ with the new relations:

$$f_\delta = (1-8x) \cdot h^2 \quad \text{with} \quad t = \frac{x(1+x)}{1-8x},$$
$$f_\xi = (1+x)(1-8x) \cdot h^2 \quad \text{with} \quad t = \frac{x}{(1+x)(1-8x)}$$

respectively.

Theorem 3. *Set*

$$A_{\delta,p} = \sum_{n=0}^{p-1} \delta_n t^n \in \mathbb{F}_p[t].$$

Then there exists a polynomial $B_{\delta,p} \in \mathbb{F}_p[t]$ *such that:*

- *if* $p \equiv 1 \pmod 6$, *then* $A_{\delta,p} = B_{\delta,p}^2$ *and* $\mathrm{Gal}\left(\mathbb{F}_p(t, f_\delta)/\mathbb{F}_p(t)\right) = S$,
- *if* $p \equiv 5 \pmod 6$, *then* $A_{\delta,p} = (64t^2 - 20t + 1)B_{\delta,p}^2$ *and* $\mathrm{Gal}\left(\mathbb{F}_p(t, f_\delta)/\mathbb{F}_p(t)\right) = \mathbb{F}_p^\times$.

Theorem 4. *Set*

$$A_{\xi,p} = \sum_{n=0}^{p-1} \xi_n t^n \in \mathbb{F}_p[t].$$

Then there exists a polynomial $B_{\xi,p} \in \mathbb{F}_p[t]$ *such that:*

- *if* $p \equiv 1, 3 \pmod 8$, *then* $A_{\xi,p} = B_{\xi,p}^2$ *and* $\mathrm{Gal}\left(\mathbb{F}_p(t, f_\xi)/\mathbb{F}_p(t)\right) = S$,
- *if* $p \equiv 5, 7 \pmod 8$, *then* $A_{\xi,p} = (81t^2 + 14t + 1)B_{\xi,p}^2$ *and* $\mathrm{Gal}\left(\mathbb{F}_p(t, f_\xi)/\mathbb{F}_p(t)\right) = \mathbb{F}_p^\times$.

In Section 3.3 we collect more examples of series, where we computationally observed similar patterns.

Acknowledgments We thank Alin Bostan for pointing out the observation that the Domb numbers and the AZ-numbers share the same behaviour as the Apéry numbers.

F.F. was funded by a DOC Fellowship (27150) of the Austrian Academy of Sciences at the University of Vienna. Further he thanks the French–Austrian project EAGLES (ANR-22-CE91-0007 & FWF grant 10.55776/I6130) for financial support.

X.C., F.F. and D.V.-M. thank Austria's Agency for Education and Internationalisation (OeAD) and Campus France for providing funding for research stays via WTZ collaboration project/Amadeus project FR02/2024. F.F. and W.Z. thank the Max Planck Institute for Mathematics (Bonn, Germany) for their hospitality and financial support in May 2025, where the initial discussion on the project commenced. The work of W.Z. was supported in part by the NWO grant OCENW.M.24.112.

2 The Apéry Numbers

Throughout this section, we fix an odd prime number p and we set $t := \frac{x(1-8x)}{1+x}$.

Lemma 5. *The extension* $\mathbb{F}_p(x)/\mathbb{F}_p(t)$ *is a quadratic extension, generated by* $(t^2 - 34t + 1)^{1/2}$, *with nontrivial element* $\sigma : x \mapsto \frac{1-8x}{8+8x}$ *of the Galois group.*

Proof. We note that x is a solution of the quadratic equation $8x^2 + (t-1)x + t = 0$ over $\mathbb{F}_p(t)$ with discriminant $\Delta = t^2 - 34t + 1$. An easy calculation shows that $\frac{1-8x}{8+8x}$ also solves this equation. $\square$

Let

$$h := \sum_{n=0}^{\infty} \sum_{k=0}^{n} \binom{n}{k}^3 x^n \in \mathbb{F}_p[\![x]\!] \qquad \text{and} \qquad H := \sum_{n=0}^{p-1} \sum_{k=0}^{n} \binom{n}{k}^3 x^n \in \mathbb{F}_p[x].$$

By Lucas' Theorem (on evaluating binomial coefficients modulo p) one easily checks that the coefficients of h satisfy Lucas' congruences and we deduce that $h = Hh^p$. Thus $h^2 = H^{-1/e}$ with $e := (p-1)/2$.

Lemma 6. *The polynomial* H *is not an* n*-th power in* $\mathbb{F}_p[x]$ *for* $n \geq 2$.

Proof. The series h satisfies the second order differential equation

$$x(x+1)(8x-1)\frac{d^2h}{dx^2} + (24x^2 + 14x - 1)\frac{dh}{dx} + (8x+2)h = 0. \tag{1}$$

By [CFV25, Lemma 2.1.3], H is not an e-th power of a polynomial for any e, as soon as H has a root different from $0, -1, 1/8$. One checks that H has degree $p-1$ and using that $\binom{p-1}{n} \equiv (-1)^n$

(mod p) that it has leading coefficient 1. Also, it is clear that its constant coefficient is 1, so it does not have 0 as a root. Assuming that

$$H = \left(x - \tfrac{1}{8}\right)^m (x+1)^{p-1-m}$$

for some m, we deduce by comparing the constant coefficients that $(-1/8)^m \equiv 1 \pmod p$. Comparing the coefficient of x one obtains that

$$m\left(-\frac{1}{8}\right)^{m-1} + (p-1-m) \equiv 2 \pmod p,$$

so we deduce $m = (p-1)/3$ if $p \equiv 1 \pmod 3$ and $m = (2p-1)/3$ otherwise. If $p \equiv 1 \pmod 3$, we can then compare coefficients of x^2 and find the contradiction $13 \equiv 10 \pmod p$. If $p \equiv 2 \pmod 3$, the contradiction already arises at the constant coefficient. Thus H has a root different from -1 and $1/8$, and the claim follows. $\square$

Since $\mathbb{F}_p(x)$ contains all e-roots of unity (as they are already in $\mathbb{F}_p$), Kummer theory implies that the extension $\mathbb{F}_p(x, h^2)/\mathbb{F}_p(x)$ is an abelian extension of degree e whose Galois group is canonically isomorphic to S.

We now consider the tower of extensions:

$$\begin{array}{c}
\mathbb{F}_p(x,h^2) = \mathbb{F}_p\left(x, \sqrt[e]{H}\right) \\
\Big| \ \mathrm{Gal} = S \\
\mathbb{F}_p(x) \\
\Big| \ \mathrm{Gal} = \langle \sigma \rangle \\
\mathbb{F}_p(t)
\end{array}$$

and aim at studying the Galois properties of the total extension $\mathbb{F}_p(x, h^2)/\mathbb{F}_p(t)$. In order to do this, we first determine the action of σ on H.

Lemma 7. *We have*

$$H = \begin{cases} \sigma(H) \cdot (x+1)^{p-1} & \text{if } p \equiv 1 \pmod 6 \\ -\sigma(H) \cdot (x+1)^{p-1} & \text{if } p \equiv 5 \pmod 6. \end{cases}$$

Proof. We first notice that σ is an involution and that $G = \sigma(H) \cdot (x+1)^{p-1}$ is a polynomial of degree $p-1$. Besides, one checks that H is a solution of the differential equation (1). Expressing now G, $\frac{dG}{dx}$ and $\frac{d^2G}{dx^2}$ as $\mathbb{F}_p(x)$-linear combinations of $\sigma(H)$ and its successives derivatives (just by applying the chain and product rules), we find that G is also a solution of the same differential equation. Therefore, we must have

$$H = aG = a \cdot \sigma(H) \cdot (x+1)^{p-1} \tag{2}$$

with $a \in \mathbb{F}_p$. Recalling that

$$\sigma(H) = \sum_{n=0}^{p-1} \sum_{k=0}^{n} \binom{n}{k}^3 \left(\frac{1-8x}{8+8x}\right)^n$$

we evaluate Equation (2) at $x = -1$ to obtain $H_{|x=-1} = a$. We set $y \coloneqq \frac{27x^2}{(1-2x)^3}$ and introduce the hypergeometric series

$$g \coloneqq {}_2F_1\left([1/3, 2/3], [1]; y\right) = \sum_{k=0}^{+\infty} \frac{(1/3)_k (2/3)_k}{k!^2} y^k \in \mathbb{F}_p[\![y]\!] \subset \mathbb{F}_p[\![x]\!]$$

where $(\alpha)_k \coloneqq \alpha(\alpha+1)\cdots(\alpha+k-1)$ denotes the *Pochhammer symbol*. We let also G denote the truncation at y^p of g. We know that $h = \frac{g}{1-2x}$, see for example [SZ15, Ex. 3.4]. Moreover g is p-Lucas as a series in y and thus $G = g^{1-p}$. From the fact that h is also p-Lucas, we get

$$H = h^{1-p} = \frac{(1-2x)^{p-1}}{g^{p-1}} = (1-2x)^{p-1}G.$$

Evaluating this expression at $x=-1$ gives $a = G_{|x=-1} = G_{|y=1}$.

Thus, if $p \equiv 1 \pmod 3$, *i.e.*, $p \equiv 1 \pmod 6$ we have

$$a \equiv \sum_{k=0}^{p-1} \binom{-1/3}{k}\binom{-2/3}{k} \equiv \sum_{k=0}^{p-1} \binom{(p-1)/3}{k}\binom{(2p-2)/3}{k} \equiv \binom{p-1}{(p-1)/3} \equiv 1 \pmod p.$$

If $p \equiv 2 \pmod 3$, *i.e.*, $p \equiv 5 \pmod 6$ we then obtain similarly

$$a \equiv \sum_{k=0}^{p-1} \binom{-1/3}{k}\binom{-2/3}{k} \equiv \sum_{k=0}^{p-1} \binom{(2p-1)/3}{k}\binom{(p-2)/3}{k} \equiv \binom{p-1}{(p-1)/3} \equiv -1 \pmod p.$$

We have used the Chu-Vandermonde identity $\sum_{k=0}^{r}\binom{r}{k}\binom{s}{k} = \binom{r+s}{r}$ and the classical congruence $\binom{p-1}{k} \equiv (-1)^k \pmod p$. □

Proposition 8. *The field extension $\mathbb{F}_p(x,h^2)/\mathbb{F}_p(t)$ is an abelian Galois extension.*

Proof. We first determine all the prolongations of $\sigma : \mathbb{F}_p(x) \to \mathbb{F}_p(x)$ to an automorphism of $\mathbb{F}_p(x,h^2)$. Such a prolongation is uniquely determined by the value of $\sigma(h^2)$, which needs to satisfy $\sigma(h^2)^e = \sigma(H)^{-1}$. Thus,

$$\sigma(h^2) = u \cdot h^2 \cdot (x+1)^2, \tag{3}$$

for some $u \in \mathbb{F}_p$. Besides, according to Lemma 7, u has to be a square if $p \equiv 1 \pmod 6$ and not a square otherwise. Consequently, there are precisely e prolongations of the automorphism σ. There are clearly also e prolongations of the identity (given by the group S of squares in $\mathbb{F}_p$ acting by multiplication on h^2). Hence, the extension $\mathbb{F}_p(x,h^2)/\mathbb{F}_p(t)$ is Galois. Moreover, any prolongation of σ clearly commutes with any element of S, making the Galois group abelian. □

Lemma 9. *There exists a prolongation of σ to $\mathbb{F}_p(x,h^2)$ that is an involution, if and only if one can take $u = \pm\frac{8}{9}$ in Equation (3).*

Proof. We have

$$\sigma^2(h^2) = \sigma(uh^2(x+1)^2) = u^2h^2(x+1)^2(\sigma(x)+1)^2 = u^2\left(\frac{9}{8}\right)^2 h^2.$$

The claim follows. □

Proposition 10. *The Galois group of $\mathbb{F}_p(x,h^2)/\mathbb{F}_p(t)$ is*

$$\mathrm{Gal}(\mathbb{F}_p(x,h^2)/\mathbb{F}_p(t)) = \begin{cases} \mathbb{Z}/(p-1)\mathbb{Z} \simeq \mathbb{Z}/e\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } p \equiv 3 \pmod 4 \\ \mathbb{Z}/(p-1)\mathbb{Z} & \text{if } p \equiv 13, 17 \pmod{24} \\ \mathbb{Z}/e\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } p \equiv 1, 5 \pmod{24}. \end{cases}$$

This corresponds to the cases where precisely one of the two numbers $u = \pm\frac{8}{9}$ corresponds to an involution $\sigma : h^2 \mapsto uh^2(1+x)^2$ in $\mathrm{Gal}(\mathbb{F}_p(x,h^2)/\mathbb{F}_p(t))$, none of them do, respectively both of them do.

Proof. Note that $\frac{8}{9} = 2 \cdot \left(\frac{2}{3}\right)^2$. Moreover, 2 is a square modulo p if and only if $p \equiv \pm 1 \pmod 8$ and -1 is a square modulo p if and only if $p \equiv 1 \pmod 4$.

If $p \equiv 1 \pmod 6$ then, for any prolongation of σ, as in Equation (3), u must be a square; if $p \equiv 5 \pmod 6$ the opposite must hold. As for $p \equiv 3 \pmod 4$, precisely one of the two values of $\pm\frac{8}{9}$ is a square, we always have precisely one adequate choice for u. If $p \equiv 1 \pmod 4$, either both of them are a square, or none of them are.

- If $p \equiv 1 \pmod{24}$, then u has to be a square, and $\pm\frac{8}{9}$ both are squares.
- If $p \equiv 5 \pmod{24}$, then u has to be a non-square, and $\pm\frac{8}{9}$ both are non-squares.
- If $p \equiv 13 \pmod{24}$, then u has to be a square, but $\pm\frac{8}{9}$ both are non-squares.
- If $p \equiv 17 \pmod{24}$, then u has to be a non-square, but $\pm\frac{8}{9}$ both are squares.

This concludes the proof of the second statement.

For the first statement, we note that $\mathrm{Gal}(\mathbb{F}_p(x,h^2)/\mathbb{F}_p(t))$ always contains a cyclic group of order e, corresponding to $\mathrm{Gal}(\mathbb{F}_p(x,h^2)/\mathbb{F}_p(x)) \simeq S$. This thus leaves us only with two possible choices, either $\mathbb{Z}/(p-1)\mathbb{Z}$ or $\mathbb{Z}/e\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ (which actually collapse in the case where $p \equiv 3 \pmod 4$). The direct factor $\mathbb{Z}/2\mathbb{Z}$ occurs if and only if there exists an element of the Galois group of order 2, which does not belong to S, *i.e.*, a prolongation of σ which is an involution. We conclude using Lemma 9. $\square$

We recall that $f = h^2 \cdot (x+1)$. This shows that $\mathbb{F}_p(t,f) \subseteq \mathbb{F}_p(x,h^2)$. Moreover $\mathbb{F}_p(t,f)$ is a cyclic extension of $\mathbb{F}_p(t)$, of degree $p-1$ or e, as explained in [CFV25, Subsection 2.1.5].

Proof of Theorem 1. We distinguish cases according to the congruence class of p modulo 24:

- If $p \equiv 1 \pmod{24}$, the Galois group of $\mathbb{F}_p(x,h^2)/\mathbb{F}_p(t)$ is not cyclic, according to Proposition 10. Thus, $\mathbb{F}_p(t,f)$ is a proper subfield of $\mathbb{F}_p(x,h^2)$, necessarily of degree e over $\mathbb{F}_p(t)$.
- If $p \equiv 5 \pmod{24}$ the Galois group of $\mathbb{F}_p(x,h^2)/\mathbb{F}_p(t)$ is not cyclic either, according to Proposition 10. We conclude again that $\mathbb{F}_p(f,t)$ has degree e over $\mathbb{F}_p(t)$.
- If $p \equiv 7 \pmod{24}$, the Galois group of $\mathbb{F}_p(x,h^2)/\mathbb{F}_p(t)$ is cyclic, because e is odd. Then, we need to check whether f is in the unique subfield of $\mathbb{F}_p(x,h^2)$ of index 2. This is equivalent to checking whether it is invariant under the unique element of the Galois group of order 2. According to Proposition 10, this element σ is uniquely given as the prolongation of $x \mapsto \frac{1-8x}{8+8x}$ with $\sigma(h^2) = u \cdot h^2 \cdot (x+1)^2$, where the prefactor u has to be $\frac{8}{9}$. We have

  $$\sigma(f) = \sigma(h^2)(\sigma(x)+1) = \tfrac{8}{9}h^2(x+1)^2(\sigma(x)+1) = h^2 \cdot (x+1) = f.$$

  So indeed, f is fixed by σ, and the extension has degree e.
- If $p \equiv 11 \pmod{24}$ one proceeds as for 7, as $u = \frac{8}{9}$ in the definition of the involution σ.
- If $p \equiv 13 \pmod{24}$, the group $\mathrm{Gal}(\mathbb{F}_p(x,h^2)/\mathbb{F}_p(t))$ is cyclic, and the unique element of order 2 in the Galois group is an element of S, sending h^2 to $-h^2$. Thus f is not fixed and $\mathbb{F}_p(t,f) \simeq \mathbb{F}_p(x,h^2)$, having degree $p-1$ over $\mathbb{F}_p(t)$.
- The case $p \equiv 17 \pmod{24}$ works as $p \equiv 13 \pmod{24}$, with the same conclusion.
- If $p \equiv 19 \pmod{24}$, we proceed as in the case $p \equiv 7 \pmod{24}$, with the exception that $u = -\frac{8}{9}$. Thus $\sigma(f) = -f$, and f is not in the unique subfield of index 2 of $\mathbb{F}_p(x,h^2)$. Thus $\mathbb{F}_p(t,f)$ has degree $p-1$.
- If $p \equiv 23 \pmod{24}$ we proceed as for $p \equiv 19 \pmod{24}$, as $u = -\frac{8}{9}$ again.

This concludes the proof. ☐

Proof of Theorem 2. We recall that we have the relation $f = (1+x)h^2$ in $\mathbb{F}_p(t,f)$. Therefore $f^e = (1+x)^e H \in \mathbb{F}_p(x)$, from which we deduce that $A_p = (1+x)^{p-1}H^2$. In particular, A_p is a square in $\mathbb{F}_p(x)$. Since moreover $\mathbb{F}_p(x) = \mathbb{F}_p(t, \sqrt{\Delta})$ with $\Delta = t^2 - 34t + 1$, we can write $A_p = (u + v\sqrt{\Delta})^2$ for $u, v \in \mathbb{F}_p(t)$. As $A_p \in \mathbb{F}_p(t)$, we must necessarily have that $2uv = 0$. Hence either $u = 0$, in which case $A_p = (t^2 - 34t + 1)v^2$, or $v = 0$, in which case $A_p = u^2$. Given that A_p is a square if $\mathbb{F}_p(t)$ if and only if the extension $\mathbb{F}_p(t,f)/\mathbb{F}_p(t)$ has degree e, we conclude using Theorem 1. ☐

3 Adaptation to Apéry-like Sequences

The *generalized* Apéry numbers $a_n(r,s) = \sum_{k=0}^{n} \binom{n}{k}^r \binom{n+k}{n}^s$ are p-Lucas for all primes p [DS06]. So we have $f_{r,s} = A_{r,s} f_{r,s}^p(x)$ for the generating series $f_{r,s}$ of $a_n(r,s)$ and its truncation $A_{r,s}$ at order p. For $(r,s) \in \{(0,0),(1,0),(0,1),(1,1),(2,0)\}$ the generating function $f_{r,s}$ is algebraic (for $(r,s) = (1,1)$ it is given by $(2x(\sqrt{1-4x}-1))^{-1}$, for $(r,s) = (1,1)$ it is given by $\sqrt{1-6t+t^2}^{-1}$ and for $(r,s) = (1,1)$ it is given by $\sqrt{1-4x}^{-1}$). Only for the case $(r,s) \in \{(2,2),(4,0)\}$ we (computationally) observed that $A_{r,s}$ is a square for a class of prime numbers depending on some congruence conditions: the case $(r,s) = (2,2)$ are the regular Apéry numbers, and $(4,0)$ is studied in Section 3.3, see level 10 in Table 2. So generalizing the investigation in this direction does not show many new interesting patterns.

As explained in the introduction, the Domb numbers and the AZ numbers are closely related to Apéry numbers. The proofs of very similar patterns, as stated in Theorems 3 and 4, proceed analogously to the Apéry case. We report in Sections 3.1 and 3.2 on the changes that need to be made.

In the last section, Section 3.3, more sequences of similar flavor are analyzed.

3.1 The Domb Numbers

We set $t_\delta := \frac{x(x+1)}{1-8x}$. Then the relation to $h(x)$ is given by $\frac{1}{1-8x} f_\delta(t_\delta) = h(x)^2$. In Lemma 5 we replace the involution σ by $\sigma_\delta : x \mapsto \frac{1+x}{8x-1}$, and the generator of the field extension $\mathbb{F}_p(x)/\mathbb{F}_p(t_\delta)$ is $(64t_\delta^2 - 20t_\delta + 1)^{1/2}$.

As in Lemma 7 we obtain

$$H = \begin{cases} \sigma_\delta(H) \cdot (8x-1)^{p-1} & \text{if } p \equiv 1 \pmod 6 \\ -\sigma_\delta(H) \cdot (8x-1)^{p-1} & \text{if } p \equiv 5 \pmod 6). \end{cases}$$

In Lemma 9, the automorphism σ_δ can be extended as $\sigma(h^2) = u \cdot h^2 \cdot (8x-1)^2$ for u being either a square or a non-square, depending on the congruence class of $p \bmod 6$. Such a prolongation is an involution on $\mathbb{F}_p(x,h^2)$ if and only if one can take $u = \pm\frac{1}{9}$. One of these values always is a square, while the other one is a square if and only if $p \equiv 1 \pmod 4$. Thus,

$$\mathrm{Gal}(\mathbb{F}_p(x,h^2)/\mathbb{F}_p(t_\delta)) = \begin{cases} \mathbb{Z}/(p-1)\mathbb{Z} \simeq \mathbb{Z}/e\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } p \equiv 7, 11 \pmod{12} \\ \mathbb{Z}/(p-1)\mathbb{Z} & \text{if } p \equiv 5 \pmod{12} \\ \mathbb{Z}/e\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} & \text{if } p \equiv 1 \pmod{12}, \end{cases}$$

again corresponding to the case of one, zero, respectively two extensions of σ_δ to an involution on $\mathbb{F}_p(x,h^2)$.

Finally, $f_\delta \in \mathbb{F}_p(x,h^2)$ because of the relations stated above and:

- If $p \equiv 1 \pmod{12}$ then the Galois group of $\mathbb{F}_p(x,h^2)/\mathbb{F}_p(t_\delta)$ is not cyclic and $\mathbb{F}_p(t_\delta, f_\delta)$ is a subfield of $\mathbb{F}_p(x,h^2)$ of order e.

- If $p \equiv 5 \pmod{12}$ then the Galois group $\mathbb{F}_p(x,h^2)/\mathbb{F}_p(t_\delta)$ is cyclic. The question then becomes to determine whether f_δ is fixed by σ_δ. However, the unique element of order 2 in the group in this case belongs to the group S sending h^2 to $-h^2$ and thus f_δ is not fixed.
- If $p \equiv 7 \pmod{12}$ then the Galois group of $\mathbb{F}_p(x,h^2)/\mathbb{F}_p(t_\delta)$ is cyclic. There is one involution extending σ, corresponding to $u = \frac{1}{9}$. We compute

  $$\sigma_\delta(f_\delta) = \sigma_\delta(h^2)(1-8\sigma_\delta(x)) = \tfrac{1}{9}h^2(1-8x)^2(1-8\sigma_\delta(x)) = h^2\cdot(1-8x) = f_\delta,$$

  so f_δ is fixed and thus contained in a proper subfield of $\mathbb{F}_p(x,h^2)$ of order e.
- If $p \equiv 11 \pmod{12}$ the prolongation of σ_δ corresponds to $u = -\frac{1}{9}$, and this time f_δ changes sign under σ_δ.

3.2 The Almkvist–Zudilin Numbers

For the AZ-numbers we set $t_\xi := \frac{x}{(1+x)(1-8x)}$ and find the involution $\sigma_\xi := x \mapsto -\frac{1}{8x}$ of $\mathbb{F}_p(x)$ fixing $\mathbb{F}_p(t_\xi)$. This time we obtain the simple relation $H = \sigma(H)\cdot x^{p-1}$ for all prime numbers p. The involution σ_ξ can be extended to $\mathbb{F}_p(x,h^2)$ by $\sigma(h)^2 = uh^2x^2$ with $u \in S$; it is an involution if and only if we can take $u = \pm 8$. Now 8 is a square if and only if $p \equiv \pm 1 \pmod 8$ and -1 is a square if and only if $p \equiv 1, 3 \pmod 5$. Thus

$$\mathrm{Gal}(\mathbb{F}_p(x,h^2)/\mathbb{F}_p(t_\xi)) = \begin{cases} \mathbb{Z}/(p-1)\mathbb{Z} \simeq \mathbb{Z}/e\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} & \text{if } p \equiv 3,7 \pmod 8 \\ \mathbb{Z}/(p-1)\mathbb{Z} & \text{if } p \equiv 5 \pmod 8 \\ \mathbb{Z}/e\mathbb{Z}\times\mathbb{Z}/2\mathbb{Z} & \text{if } p \equiv 1 \pmod 8. \end{cases}$$

Finally, $f_\xi \in \mathbb{F}_p(x,h^2)$ and investigations depending on the congruence class of $p \pmod 8$ yield the following:

- If $p \equiv 1 \pmod 8$ the Galois group $\mathrm{Gal}(\mathbb{F}_p(x,h^2)/\mathbb{F}_p(t_\xi))$ is not cyclic, and thus f_ξ is in a proper subfield of degree e.
- If $p \equiv 3 \pmod 8$ the unique prolongation of σ_ξ as an involution corresponds to $u = -8$ and because of

  $$\sigma_\xi(f_\xi) = \sigma(h^2)(1+\sigma_\xi(x))(1-8\sigma_\xi(x)) = h^2(1-8x)(1+x) = f_\xi,$$

  we conclude that f_ξ lies in a proper subfield of $\mathbb{F}_p(x,h^2)$ of degree e.
- If $p \equiv 5 \pmod 8$ the unique element of order 2 in $\mathrm{Gal}(\mathbb{F}_p(x,h^2)/\mathbb{F}_p(t_\xi)$ belongs to the subgroup of squares of $\mathbb{F}_p^\times$ and sends h so $-h$ and thus does not fix f_ξ. So $\mathbb{F}_p(t_\xi, f_\xi) = \mathbb{F}_p(x,h)$.
- If $p \equiv 7 \pmod 8$ the prolongation of σ_ξ as an involution corresponds to $u = +8$, and this time f_ξ changes sign under it and thus is not fixed by it. Again, $\mathbb{F}_p(t_\xi, f_\xi) = \mathbb{F}_p(x,h)$.

3.3 A Zoo of Further Examples

First, we consider the three other sequences of Zagier's sporadic examples of integral sequences satisfying a three-term recurrence relation [Zag09]. It is known that these sequences are p-Lucas for all primes p [MS16]; therefore, their generating series $f(t)$ satisfies the relation $f(t) \equiv A_p(t)f(t)^p \pmod p$, where $A_p(t) \in \mathbb{F}_p[t]$ is the truncation at t^p of $f(t) \bmod p$. As before, we are interested in the factorization of $A_p(t)$ of the form $A_p(t) = P(t)B_p(t)^2$. Table 1 shows how $P(t)$ varies with respect to p.

We pursue our investigations with other sequences associated to modular functions (of a given level), see Table 2. Thanks to [ABD19; BTY25], we know that all the series appearing in this

Sequence	Conditions	Coefficient $P(t)$
OEIS A229111 $2\cdot(-1)^n\cdot\sum_{k=0}^{n}\binom{n}{k}^3\left(\binom{4n-5k-1}{3n}+\binom{4n-5k}{3n}\right)$	$\left(\frac{-1}{p}\right)=1$ $\left(\frac{-1}{p}\right)=-1$	1 $1-22t+125t^2$
OEIS A290575 $\sum_{k=0}^{n}\binom{n}{k}^2\binom{2k}{n}^2$	$\left(\frac{-2}{p}\right)=1$ $\left(\frac{-2}{p}\right)=-1$	1 $1-24t+16t^2$
OEIS A290576 $\sum_{k=0}^{n}\sum_{\ell=0}^{n}\binom{n}{k}^2\binom{n}{\ell}\binom{k}{\ell}\binom{k+\ell}{n}$	$\left(\frac{-1}{p}\right)=1$ $\left(\frac{-1}{p}\right)=-1$	1 $1-18t+27t^2$

TABLE 1: Zagier's sporaric examples [Zag09; ASZ11]

table are p-Lucas except for levels 17, 20 and 23. However, in the former cases, they continue to satisfy a relation of the form $f(t) \equiv A_p(t)f(t)^p \pmod p$, where now $A_p(t) \in \mathbb{F}_p(t)$ is now a rational function; this follows from the main theorem of [Var23]. As a conclusion, in all cases, $A_p(t)$ is well defined and it makes sense to study its factorization as $A_p(t) = P(t)B_p(t)^2$ as before.

In all the examples of Tables 1 and 2, we computationally observed that the patterns for the polynomials $P(t)$ depend on explicit quadratic residues conditions for the prime p. These patterns are very much in line with those recorded in Theorems 1, 2, 3 and 4, and one can apply, case by case, a similar strategy to establishing the claims in the tables rigorously. The principal feature of the underlying series $f(t)$ is the presence of suitable rational parameterizations $t = t(x)$ such that $f(t(x)) = \rho(x)h(x)^2$ for a function $h(x)$ solving a second order linear differential equation and in turn related to an arithmetic ${}_2F_1$ hypergeometric function $g(y)$ via another parameterization $y = y(x)$; namely, $h(x) = \lambda(x)g(y(x))$. In Apéry's case (but also for the Domb and Almkvist–Zudilin sequences), all the intermediate functions are rational in x:

$$t(x) = \frac{x(1-8x)}{1+x}, \quad \rho(x) = 1 + x, \quad y(x) = \frac{27x^2}{(1-2x)^3}, \quad \lambda(x) = \frac{1}{1-2x}.$$

However, in general $\rho(x)$, $y(x)$ and $\lambda(x)$ are algebraic, which can make the structure of the corresponding Galois group more involved. The existence of such x-parameterizations is a consequence of modular parameterizations of all such Apéry-like sequences; the details of the latter can be found in the corresponding references where our examples originate from. We leave the details to an interested reader as exercises.

Going further, the observations on the splitting pattern of $A_p(t)$ as $P(t)B_p(t)^2$ suggest that the conditions of p depends only on the quadratic residues of the divisors of the squarefree part of the corresponding level. We also leave it to the interested reader to formulate and prove a precise statement about the pattern that unfolds here. We conclude by remarking that these observations provide more computational evidence for the conjectures on uniformity properties of Galois groups of reductions of D-finite series, that were formulated in [CFV25].

Sequence	Level	Conditions	Coefficient $P(t)$
OEIS A274786 [Coo12], [Bos+15], [Coo17], [HSY23] $\binom{2n}{n}\sum_{k=0}^{n}\binom{n}{k}^2\binom{n+k}{k}$	5	$\left(\frac{-5}{p}\right)=1$ $\left(\frac{-5}{p}\right)=-1$	1 $1-44t-16t^2$
OEIS A181418 [Coo12], [Coo17], [HSY23] $\binom{2n}{n}\sum_{k=0}^{n}\binom{n}{k}^3$	6	$\left(\frac{-3}{p}\right)=\left(\frac{-6}{p}\right)=1$ $\left(\frac{-3}{p}\right)=-1,\left(\frac{-6}{p}\right)=1$ $\left(\frac{-3}{p}\right)=1,\left(\frac{-6}{p}\right)=-1$ $\left(\frac{-3}{p}\right)=\left(\frac{-6}{p}\right)=-1$	1 $1+4t$ $1-32t$ $(1+4t)(1-32t)$
OEIS A183204 [Coo12], [Coo17], [HSY23] $\sum_{k=0}^{n}\binom{n}{k}^2\binom{2k}{n}\binom{k+n}{n}$	7	$\left(\frac{-7}{p}\right)=1$ $\left(\frac{-7}{p}\right)=-1$	1 $(1+t)(1-27t)$
OEIS A005260 [Coo12], [Coo17], [HSY23] $\sum_{k=0}^{n}\binom{n}{k}^4$	10	$\left(\frac{-5}{p}\right)=\left(\frac{-10}{p}\right)=1$ $\left(\frac{-5}{p}\right)=-1,\left(\frac{-10}{p}\right)=1$ $\left(\frac{-5}{p}\right)=1,\left(\frac{-10}{p}\right)=-1$ $\left(\frac{-5}{p}\right)=\left(\frac{-10}{p}\right)=-1$	1 $1+4t$ $1-16t$ $(1+4t)(1-16t)$
OEIS A284756 [CGY15, c_{11} Thm. 4.7] [Coo17], [HSY23]	11	$\left(\frac{-11}{p}\right)=1$ $\left(\frac{-11}{p}\right)=-1$	1 $1-20t+56t^2-44t^3$
[HSY20, Cor 3.6]	17	$\left(\frac{-17}{p}\right)=1$ $\left(\frac{-17}{p}\right)=-1$	1 $1-16t-66t^2-48t^3-127t^4$
OEIS A219692 [Coo12, s_{18} on p.171]	18	$\left(\frac{-1}{p}\right)=\left(\frac{-2}{p}\right)=1$ $\left(\frac{-1}{p}\right)=-1,\left(\frac{-2}{p}\right)=1$ $\left(\frac{-1}{p}\right)=1,\left(\frac{-2}{p}\right)=-1$ $\left(\frac{-1}{p}\right)=\left(\frac{-2}{p}\right)=-1$	1 $1-12t$ $1-16t$ $(1-12t)(1-16t)$
[HSY18, Cor 3.7]	20	$\left(\frac{-1}{p}\right)=\left(\frac{-5}{p}\right)=1$ $\left(\frac{-1}{p}\right)-1,=\left(\frac{-5}{p}\right)=1$ $\left(\frac{-1}{p}\right)=1,\left(\frac{-5}{p}\right)=-1$ $\left(\frac{-1}{p}\right)=\left(\frac{-5}{p}\right)=-1$	1 $1-4t$ $1-12t+16t^2$ $(1-4t)(1-12t+16t^2)$
[CGY15, c_{23} Thm. 4.7], [Coo17]	23	$\left(\frac{-23}{p}\right)=1$ $\left(\frac{-23}{p}\right)=-1$	1 $(1-3t+2t^2+t^3)(1-11t+22t^2-19t^3)$

TABLE 2: Examples of sequences connected to modular forms

References

[ABD19] B. Adamczewski, J. Bell, and É. Delaygue. “Algebraic independence of G-functions and congruences “à la Lucas””. *Ann. Sci. Éc. Norm. Supér.* (2019). DOI: 10.24033/asens.2392.

[Apé79] R. Apéry. “Irrationalité de $\zeta(2)$ et $\zeta(3)$”. *Astérisque* 61 (1979), pp. 11–13. URL: https://www.numdam.org/book-part/AST_1979__61__11_0/.

[ASZ11] G. Almkvist, D. van Straten, and W. Zudilin. “Generalizations of Clausen’s Formula and Algebraic Transformations of Calabi–Yau Differential Equations”. *Proceedings of the Edinburgh Mathematical Society* 54.2 (2011), pp. 273–295. DOI: 10.1017/S0013091509000959.

[Bos+15] A. Bostan, S. Boukraa, J.-M. Maillard, and J.-A. Weil. “Diagonals of Rational Functions and Selected Differential Galois Groups”. *Journal of Physics A: Mathematical and Theoretical* 48.50 (2015), p. 504001. DOI: 10.1088/1751-8113/48/50/504001.

[BTY25] F. Beukers, W.-L. Tsai, and D. Ye. “Lucas Congruences Using Modular Forms”. *Bulletin of the London Mathematical Society* 57.1 (2025), pp. 69–78. DOI: 10.1112/blms.13182.

[CFV25] X. Caruso, F. Fürnsinn, and D. Vargas-Montoya. *Galois groups of reductions modulo p of D-finite series*. 2025. arXiv: 2504.09429 [math.NT].

[CGY15] S. Cooper, J. Ge, and D. Ye. “Hypergeometric Transformation Formulas of Degrees 3, 7, 11 and 23”. *Journal of Mathematical Analysis and Applications* 421.2 (2015), pp. 1358–1376. DOI: 10.1016/j.jmaa.2014.07.061.

[Chr86a] G. Christol. “Fonctions et éléments algébriques”. *Pacific Journal of Mathematics* 125.1 (1986), pp. 1–37. DOI: 10.2140/pjm.1986.125.1.

[Chr86b] G. Christol. “Fonctions hypergéométriques bornées”. *Groupe de travail d’analyse ultramétrique*. exp. no 8 14 (1986–1987), pp. 1–16. URL: https://www.numdam.org/item/GAU_1986-1987__14__A4_0/.

[Coo12] S. Cooper. “Sporadic Sequences, Modular Forms and New Series for $1/\pi$”. *The Ramanujan Journal* 29.1–3 (2012), pp. 163–183. DOI: 10.1007/s11139-011-9357-3.

[Coo17] S. Cooper. *Ramanujan’s Theta Functions*. Cham: Springer International Publishing, 2017. DOI: 10.1007/978-3-319-56172-1.

[CV09] H. H. Chan and H. Verrill. “The Apéry numbers, the Almkvist–Zudilin numbers and new series for $1/\pi$”. *Math. Res. Lett.* 16.3 (2009), pp. 405–420. DOI: 10.4310/MRL.2009.v16.n3.a3.

[CZ10] H. H. Chan and W. Zudilin. “New representations for Apéry-like sequences”. *Mathematika* 56.1 (2010), pp. 107–117. DOI: 10.1112/S0025579309000436.

[DS06] E. Deutsch and B. E. Sagan. “Congruences for Catalan and Motzkin Numbers and Related Sequences”. *Journal of Number Theory* 117.1 (2006), pp. 191–215. DOI: 10.1016/j.jnt.2005.06.005.

[Fur67] H. Furstenberg. “Algebraic functions over finite fields”. *J. Algebra* 7 (1967), pp. 271–277. DOI: 10.1016/0021-8693(67)90061-0.

[Ges82] I. Gessel. “Some congruences for Apéry numbers”. *J. Number Theory* 14.3 (1982), pp. 362–368. DOI: 10.1016/0022-314X(82)90071-3.

[HSY18] T. Huber, D. Schultz, and D. Ye. “Series for $1/\pi$ of Level 20”. *Journal of Number Theory* 188 (2018), pp. 121–136. DOI: 10.1016/j.jnt.2017.12.010.

[HSY20] T. Huber, D. Schultz, and D. Ye. “Level 17 Ramanujan–Sato Series”. *The Ramanujan Journal* 52.2 (2020), pp. 303–322. DOI: 10.1007/s11139-018-0097-5.

[HSY23] T. Huber, D. Schultz, and D. Ye. “Ramanujan–Sato Series for $1/\pi$”. *Acta Arithmetica* 207.2 (2023), pp. 121–160. DOI: 10.4064/aa220621-19-12.

[MS16] A. Malik and A. Straub. “Divisibility properties of sporadic Apéry-like numbers”. *Res. Number Theory* 2 (2016), Paper No. 5, 26. DOI: 10.1007/s40993-016-0036-8.

[SZ15] A. Straub and W. Zudilin. “Positivity of Rational Functions and Their Diagonals”. *Journal of Approximation Theory* 195 (2015), pp. 57–69. DOI: 10.1016/j.jat.2014.05.012.

[Var21] D. Vargas-Montoya. “Algébricité modulo p, séries hypergéométriques et structures de Frobenius fortes”. *Bulletin de la Société mathématique de France* (2021). DOI: 10.24033/bsmf.2834.

[Var23] D. Vargas-Montoya. “Monodromie unipotente maximale, congruences “à la Lucas” et indépendance algébrique”. *Transactions of the American Mathematical Society* (2023). DOI: https://doi.org/10.1090/tran/8913.

[Zag09] D. Zagier. “Integral Solutions of Apéry-like Recurrence Equations”. *Groups and Symmetries*. Ed. by J. Harnad and P. Winternitz. Vol. 47. CRM Proceedings and Lecture Notes. Providence, Rhode Island: American Mathematical Society, 2009, pp. 349–366. DOI: 10.1090/crmp/047.

CNRS; IMB, Université de Bordeaux, 351 Cours de la Libération, 33405 Talence, France
Email: xavier@caruso.ovh

Faculty of Mathematics, University of Vienna, Oskar-Morgenstern-Platz 1, 1090 Vienna, Austria
Email: florian.fuernsinn@univie.ac.at

Institut de Mathématiques de Toulouse, Université Paul Sabatier, 118 route de Narbonne, 31062 Toulouse Cedex 9, France
Email: daniel.vargas-montoya@math.univ-toulouse.fr

IMAPP, Radboud University Nijmegen, PO Box 9010, 6500 GL Nijmegen, The Netherlands
Email: w.zudilin@math.ru.nl