Gauss congruences for rational functions in several variables

Frits Beukers[1], Marc Houben[1], and Armin Straub[2]

[1]Utrecht University
[2]University of South Alabama

October 1, 2017

Abstract

We investigate necessary as well as sufficient conditions under which the Laurent series coefficients $f_{\boldsymbol{n}}$ associated to a multivariate rational function satisfy Gauss congruences, that is $f_{\boldsymbol{m}p^r} \equiv f_{\boldsymbol{m}p^{r-1}}$ modulo p^r. For instance, we show that these congruences hold for certain determinants of logarithmic derivatives. As an application, we completely classify rational functions P/Q satisfying the Gauss congruences in the case that Q is linear in each variable.

1 Introduction

We say that a sequence $(a_k)_{k\geq 0}$ of rational numbers satisfies the *Gauss congruences* for the prime p, if $a_k \in \mathbb{Z}_p$ (that is, the a_k are p-adically integral) and

$$a_{mp^r} \equiv a_{mp^{r-1}} \pmod{p^r} \tag{1}$$

for all integers $m \geq 0$ and $r \geq 1$. These congruences hold for all primes if and only if

$$\sum_{d|m} \mu\left(\frac{m}{d}\right) a_d \equiv 0 \pmod{m},$$

where μ is the Möbius function, and they are named after the classical congruences that hold in the case $a_k = \alpha^k$, with $\alpha \in \mathbb{Z}$. We refer to [Zar08] and [Min14] for a survey of these and related congruences. Well-known examples of sequences satisfying the Gauss congruences for all primes include the Lucas numbers L_n defined by $L_{n+1} = L_n + L_{n-1}$, with $L_0 = 2$, $L_1 = 1$, and the Apéry numbers

$$A_n = \sum_{k=0}^{n} \binom{n}{k}^2 \binom{n+k}{k}^2, \tag{2}$$

which featured in Apéry's proof [Apé79] of the irrationality of $\zeta(3)$. In fact, as shown in [Beu85], [Cos88], the Apéry numbers have the remarkable (and rare) property of satisfying (1) modulo p^{3r} if $p \geq 5$ (often referred to as a supercongruence).

In this paper, we consider the case of multivariate sequences $(a_{\boldsymbol{k}})_{\boldsymbol{k}\in\mathbb{Z}^n}$. As in the univariate case, these are said to satisfy the *Gauss congruences* for the prime p, if $a_{\boldsymbol{k}} \in \mathbb{Z}_p$ and $a_{\boldsymbol{m}p^r} \equiv a_{\boldsymbol{m}p^{r-1}}$

(mod p^r) for all $\boldsymbol{m} \in \mathbb{Z}^n$ and all $r \geq 1$. Our particular focus is on the case when the $a_{\boldsymbol{k}}$ are the coefficients of a Laurent series of a rational function. As reviewed in Section 2, a rational function $f = P/Q$ has Laurent series associated with each vertex of the Newton polytope $N(Q)$ of Q. We show that Gauss congruences hold for one of these Laurent series (for all but finitely many primes) if and only if they hold for all Laurent series (Proposition 3.4), in which case we say that f has the *Gauss property*.

As observed in [Str14], the rational function

$$\frac{1}{(1-x_1-x_2)(1-x_3-x_4)-x_1x_2x_3x_4} = \sum_{\boldsymbol{k}\in\mathbb{Z}^4_{\geq 0}} A_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}, \tag{3}$$

where $\boldsymbol{x}^{\boldsymbol{k}}$ is short for $x_1^{k_1}x_2^{k_2}x_3^{k_3}x_4^{k_4}$, has the Apéry numbers (2) as its diagonal coefficients, that is, $A_{n,n,n,n} = A_n$. Moreover, it is proved in [Str14] that the supercongruences for the Apéry numbers hold for all coefficients $A_{\boldsymbol{n}}$, meaning that $A_{\boldsymbol{m}p^r} \equiv A_{\boldsymbol{m}p^{r-1}} \pmod{p^{3r}}$ for all primes $p \geq 5$. In particular, the rational function (3) has the Gauss property.

One of the goals of this paper is to address the question of which rational functions have the Gauss property. Towards that end, we provide several results that show that the Gauss property holds for large natural classes of rational functions in several variables $\boldsymbol{x} = (x_1, x_2, \ldots, x_n)$. For instance, in Section 4, we show that certain determinants of logarithmic derivatives have the Gauss property. The following is derived (as Theorem 4.5) from a similar result for Laurent series (Theorem 4.4). Because of its central character (indicated in Question 1.2 below) and for future applications, the results of Section 4 are proved over more general rings, namely domains with a Frobenius lift (Definition 4.1).

Theorem 1.1. *Let $m \leq n$ and let $f_1, \ldots, f_m \in \mathbb{Q}(\boldsymbol{x})$ be nonzero. Then the rational function*

$$\frac{x_1\cdots x_m}{f_1\cdots f_m}\det\left(\frac{\partial f_j}{\partial x_i}\right)_{i,j=1,\ldots,m} \tag{4}$$

has the Gauss property.

It would be of considerable interest to fully characterize multivariate rational functions with the Gauss property. Towards that end, one might be tempted to ask the following question.

Question 1.2. *Suppose that the rational function $f \in \mathbb{Q}(\boldsymbol{x})$ has the Gauss property. Can it be written as a $\mathbb{Q}$-linear combination of functions of the form (4)?*

A recent result of Minton [Min14] answers Question 1.2 affirmatively when $n = 1$, the case of a single variable. For the benefit of the reader and in order to be self-contained, we reprove this result, cast in our present language, in Section 8.

Theorem 1.3 (Minton, 2014)**.** *A rational function $f \in \mathbb{Q}(x)$ has the Gauss property if and only if f is a $\mathbb{Q}$-linear combination of functions of the form $xu'(x)/u(x)$, with $u \in \mathbb{Z}[x]$.*

Although characterizing multivariate rational functions with the Gauss property remains an open challenge, we obtain, in Section 5, the following concise classification in the case of rational functions P/Q, for which the Newton polytope $N(Q)$ of the denominator is contained in $\{0,1\}^n$. Note that, in that case, the vertices of $N(Q)$ equal the support of Q.

Theorem 1.4. *Let $P, Q \in \mathbb{Z}[\boldsymbol{x}]$ and suppose that Q is linear in each variable. Then P/Q has the Gauss property if and only if $N(P) \subseteq N(Q)$.*

As illustrated by (3), such results for (multivariate) rational functions allow us to establish congruences for numbers, such as the Apéry numbers, whose generating function is much more complicated than a rational function. Indeed, observe that Theorem 1.4 immediately implies that the rational function (3) has the Gauss property. In particular, it follows that the Apéry numbers satisfy the Gauss congruences. In a similar spirit, recent results of Rowland and Yassawi [RY15] show that the series coefficients of certain rational functions satisfy Lucas congruences. Their approach using Cartier operators can also be applied to provide an alternative proof (at least in parts) of the "if" portion of Theorem 1.4 (due to the technicalities involved, we do not pursue this path here).

We obtain Theorem 1.4 as an immediate consequence of the following more general result, which we prove in Section 5 as an application of Theorem 1.1.

Theorem 1.5. *Let $P, Q \in \mathbb{Z}[z, \boldsymbol{x}]$ such that Q is linear in the variables $x_1, \ldots, x_n$. Write $P = \sum_{\boldsymbol{k}} p_{\boldsymbol{k}}(z)\boldsymbol{x}^{\boldsymbol{k}}$ and $Q = \sum_{\boldsymbol{k}} q_{\boldsymbol{k}}(z)\boldsymbol{x}^{\boldsymbol{k}}$ with $p_{\boldsymbol{k}}, q_{\boldsymbol{k}} \in \mathbb{Z}[z]$. Then P/Q has the Gauss property if and only if $p_{\boldsymbol{k}} \neq 0$ implies $q_{\boldsymbol{k}} \neq 0$ and $p_{\boldsymbol{k}}/q_{\boldsymbol{k}}$ has the Gauss property for all $\boldsymbol{k}$ with $q_{\boldsymbol{k}} \neq 0$.*

Our proof of Theorem 1.5 answers Question 1.2 affirmatively for rational functions $f = P/Q$, in the case that Q is linear in all but one variable. We further show in Example 6.6, that the answer to Question 1.2 is affirmative in the case that Q is a function of two variables and total degree 2.

Although, in general, Question 1.2 remains far from being answered, we can give a number of necessary conditions for the Gauss property to hold. A simple such condition, proved in Proposition 3.5, is that the Newton polytope $N(P)$ of P must be contained in $N(Q)$. As another example, made precise in Proposition 3.8, consider a face F of $N(Q)$ and let P_F, Q_F be the restrictions of P, Q consisting of those monomials supported on F. If P/Q has the Gauss property, then the same holds for P_F/Q_F. In Proposition 6.1, we prove the straightforward observation that toroidal substitutions preserve the Gauss property. As a consequence, illustrated in Example 6.4, the rational function P_F/Q_F can be reduced to a rational function in essentially fewer than n variables.

Finally, let us indicate a useful consequence concerning arbitrary substitutions of an affirmative answer to Question 1.2. Suppose that $f \in \mathbb{Q}(\boldsymbol{x})$ is a $\mathbb{Q}$-linear combination of functions of the form (4), and let $g_1, \ldots, g_n \in \mathbb{Q}(\boldsymbol{x})$ be nonzero. Then, by the multivariate chain rule,

$$\frac{x_1 \cdots x_n}{g_1 \cdots g_n} \det\left(\frac{\partial g_j}{\partial x_i}\right)_{i,j=1,\ldots,n} f(g_1(\boldsymbol{x}), \ldots, g_n(\boldsymbol{x})) \tag{5}$$

also is a $\mathbb{Q}$-linear combination of functions of the form (4). In particular, by Theorem 1.1, the rational function (5) has the Gauss property. Hence, if Question 1.2 has an affirmative answer, then it follows that, for any rational function $f \in \mathbb{Q}(\boldsymbol{x})$ with the Gauss property, the rational function (5) has the Gauss property as well.

Since Question 1.2 remains open, we give a direct and independent proof of the following univariate version in Section 7.

Theorem 1.6. *Let $g_j \in \mathbb{Q}(x)$ be nonzero. If the rational function $f \in \mathbb{Q}(\boldsymbol{x})$ has the Gauss property, then so does the rational function*

$$\left(\prod_{j=1}^{n} \frac{x_j g_j'(x_j)}{g_j(x_j)}\right) f(g_1(x_1), \ldots, g_n(x_n)). \tag{6}$$

2 Preliminaries and Laurent series expansions

Throughout, p is a prime. The *p-adic valuation* $\nu_p(a)$ of a rational number $a \in \mathbb{Q}^\times$ is the largest $r \in \mathbb{Z}$ such that $a/p^r \in \mathbb{Z}_p$, with the understanding that $\nu_p(0) = \infty$. If $\boldsymbol{a} = (a_1, \ldots, a_n) \in \mathbb{Q}^n$ is a vector, then $\nu_p(\boldsymbol{a}) = \min\{\nu_p(a_1), \ldots, \nu_p(a_n)\}$. Similarly, we say that p divides a vector $\boldsymbol{a}$ if and only if $\nu_p(\boldsymbol{a}) \geq 1$, that is, p divides each component of $\boldsymbol{a}$.

When working with several variables, we typically use the vector notation $\boldsymbol{x} = (x_1, \ldots, x_n)$ and write, for instance, $\mathbb{Q}(\boldsymbol{x}) = \mathbb{Q}(x_1, \ldots, x_n)$ for the ring of rational functions, or $\mathbb{Q}[\boldsymbol{x}^{\pm 1}] = \mathbb{Q}[x_1^{\pm 1}, \ldots, x_n^{\pm 1}]$ for the ring of Laurent polynomials in several variables. Similarly, we write $\boldsymbol{x}^{\boldsymbol{k}} = x_1^{k_1} \cdots x_n^{k_n}$ for monomials and refer to $\boldsymbol{k} = (k_1, \ldots, k_n)$ as its exponent vector. The *support* of a Laurent polynomial $P \in \mathbb{Q}[\boldsymbol{x}^{\pm 1}]$, denoted $\operatorname{supp}(P) \subseteq \mathbb{Z}^n$, is the set of exponent vectors of the (non-zero) monomials of P. The *Newton polytope* $N(P)$ of P is the convex closure of $\operatorname{supp}(P)$. The *cone* generated by vectors $\boldsymbol{v}_1, \boldsymbol{v}_2, \ldots \in \mathbb{R}^n$ is the $\mathbb{R}_{\geq 0}$-span of these vectors. We say such a cone C is *proper* if there exists a linear form α such that $\alpha(\boldsymbol{w}) > 0$ for all nonzero $\boldsymbol{w} \in C$. The cones of importance to us are proper. For instance, suppose that $\boldsymbol{v}$ is a vertex of the Newton polytope $N(P)$ of a Laurent polynomial P. Then the cone generated by $N(P\boldsymbol{x}^{-\boldsymbol{v}})$ is a proper cone. Note that our cones are based on the vertex $\boldsymbol{0}$.

In this paper, we frequently discuss rational functions $F = P/Q \in \mathbb{Q}(\boldsymbol{x})$. In principle, we could choose P and Q to be polynomials. However, for certain purposes, it turns out to be natural to allow P and Q to be Laurent polynomials, that is, $P, Q \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$. We have a Laurent series expansion of F associated to each vertex $\boldsymbol{v}$ of $N(Q)$ as follows [GKZ94, p. 195]. Writing $Q = \sum_{\boldsymbol{k}} q_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}}$ with $q_{\boldsymbol{k}} \in \mathbb{Z}$, note that $\boldsymbol{x}^{\boldsymbol{v}}/Q$ can be expanded as

$$\frac{\boldsymbol{x}^{\boldsymbol{v}}}{Q} = \frac{1}{q_{\boldsymbol{v}} + \sum_{\boldsymbol{k} \neq \boldsymbol{v}} q_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}-\boldsymbol{v}}} = \frac{1}{q_{\boldsymbol{v}}} \sum_{m=0}^{\infty} \left(- \sum_{\boldsymbol{k} \neq \boldsymbol{v}} \frac{q_{\boldsymbol{k}}}{q_{\boldsymbol{v}}} \boldsymbol{x}^{\boldsymbol{k}-\boldsymbol{v}} \right)^m = \sum_{\boldsymbol{k} \in C} g_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}}, \tag{7}$$

where C is the proper cone generated by the vectors $N(Q/\boldsymbol{x}^{\boldsymbol{v}})$. To see that the $g_{\boldsymbol{k}}$ in (7) are finite, so that the series is well-defined, let α be a linear form such that $\alpha(\boldsymbol{w}) > 0$ for all nonzero $\boldsymbol{w} \in C$, and observe that $\alpha(\boldsymbol{k} - \boldsymbol{v}) > 0$ for all $\boldsymbol{k} \in \operatorname{supp}(Q)$ with $\boldsymbol{k} \neq \boldsymbol{v}$. Clearly, $g_{\boldsymbol{k}} \in \mathbb{Z}[q_{\boldsymbol{v}}^{-1}]$. Multiplying the series (7) with $P/\boldsymbol{x}^{\boldsymbol{v}}$, we obtain a Laurent series $f = \sum_{\boldsymbol{k}} f_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}}$ for $F = P/Q$. Its coefficients again satisfy $f_{\boldsymbol{k}} \in \mathbb{Z}[q_{\boldsymbol{v}}^{-1}]$. We refer to $f \in \mathbb{Q}[[\boldsymbol{x}^{\pm 1}]]$ as the *Laurent series expansion* of F with respect to $\boldsymbol{v}$. The support of f, denoted by $\operatorname{supp}(f)$, is the set of all $\boldsymbol{k} \in \mathbb{Z}^n$ such that $f_{\boldsymbol{k}} \neq 0$. Observe that, if p is a prime such that $q_{\boldsymbol{v}} \in \mathbb{Z}_p^\times$, then $f \in \mathbb{Z}_p[[\boldsymbol{x}^{\pm 1}]]$. In particular, for all but finitely many primes p, all Laurent series expansions of F have coefficients that are p-adic integers.

For any Laurent series $f = \sum_{\boldsymbol{k}} f_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}} \in \mathbb{Q}[[\boldsymbol{x}^{\pm 1}]]$, we refer to $f_{\boldsymbol{0}}$ as its constant term.

Finally, especially in Section 4, it will be convenient to use the Euler operator $\theta_y = y\frac{\partial}{\partial y}$. If there is no possibility for confusion, we simply write $\theta_i = \theta_{x_i}$.

3 Gauss congruences

Definition 3.1. We say that a Laurent series

$$f = \sum_{\boldsymbol{k} \in \mathbb{Z}^n} f_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}} \in \mathbb{Q}[[\boldsymbol{x}^{\pm 1}]]$$

satisfies the *Gauss congruences* for the prime p if $f \in \mathbb{Z}_p[[\boldsymbol{x}^{\pm 1}]]$ and

$$f_{\boldsymbol{m}p^r} \equiv f_{\boldsymbol{m}p^{r-1}} \pmod{p^r}$$

for all $\boldsymbol{m} \in \mathbb{Z}^n$ and all $r \geq 1$. We say that f has the *Gauss property* if it satisfies the Gauss congruences for all but finitely many primes.

Let U_p be the operator on Laurent series defined by

$$U_p\left(\sum_{\boldsymbol{k}\in\mathbb{Z}^n} c_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}\right) = \sum_{\boldsymbol{k}\in\mathbb{Z}^n} c_{p\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}. \tag{8}$$

Note that a Laurent series f has the Gauss property if and only if, for all $r \geq 1$ and all but finitely many primes p,

$$U_p^r(f) \equiv U_p^{r-1}(f) \pmod{p^r}.$$

The following observation is more or less straightforward.

Proposition 3.2. *Let $\zeta = e^{2\pi i/p}$. If f is the Laurent series of the rational function $F \in \mathbb{Q}(\boldsymbol{x})$ with respect to the vertex $\boldsymbol{v}$, then $U_p(f)$ is the Laurent series of the rational function*

$$F^{(p)} = \frac{1}{p^n}\sum_{r_1,\ldots,r_n=0}^{p-1} F(\zeta^{r_1}x_1^{1/p},\ldots,\zeta^{r_n}x_n^{1/p})$$

with respect to the vertex $p^{n-1}\boldsymbol{v}$.

In fact, let us note that, with $F = P/Q$ for $P, Q \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$, we can write $F^{(p)} = P^{(p)}/Q^{(p)}$ with denominator

$$Q^{(p)} = \prod_{r_1,\ldots,r_n=0}^{p-1} Q(\zeta^{r_1}x_1^{1/p},\ldots,\zeta^{r_n}x_n^{1/p}),$$

which is in $\mathbb{Z}[\boldsymbol{x}^{\pm 1}]$ with Newton polytope $N(Q^{(p)}) = p^{n-1}N(Q)$. If $\boldsymbol{v}$ is a vertex of $N(Q)$ with coefficient $q_{\boldsymbol{v}} \in \mathbb{Z}_p^\times$, then $p^{n-1}\boldsymbol{v}$ is a vertex of $N(Q^{(p)})$ with coefficient $q_{\boldsymbol{v}}^{p^n} \in \mathbb{Z}_p^\times$.

Definition 3.3. A rational function $F = P/Q \in \mathbb{Q}(\boldsymbol{x})$ has the *Gauss property* if, for every vertex $\boldsymbol{v}$ of $N(Q)$, the Laurent series expansion of F with respect to $\boldsymbol{v}$ has the Gauss property.

By the next result, it suffices to consider a single vertex $\boldsymbol{v}$ in that definition. The proof relies on the following simple but important observation. If $P, Q \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$ and $\boldsymbol{v}$ is a vertex of $N(Q)$, then, for all but finitely many primes p, the Laurent expansion f of P/Q with respect to $\boldsymbol{v}$ has p-adic integers as coefficients. In such a case, $f \equiv 0 \pmod{p^r}$ if and only if $P \equiv 0 \pmod{p^r}$.

Proposition 3.4. *Let $P, Q \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$. Let $\boldsymbol{v}, \boldsymbol{w}$ be vertices of $N(Q)$. Then the Laurent series expansion of $F = P/Q$ with respect to $\boldsymbol{v}$ has the Gauss property if and only if the Laurent series expansion of F with respect to $\boldsymbol{w}$ has the Gauss property.*

Proof. Suppose that $f = \sum_{\boldsymbol{k}\in\mathbb{Z}^n} f_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}$ is the Laurent series expansion of F with respect to $\boldsymbol{v}$. By Proposition 3.2, $U_p^r(f) \in \mathbb{Z}_p[[\boldsymbol{x}^{\pm 1}]]$ is the Laurent expansion of a rational function $P^{(p^r)}/Q^{(p^r)}$ with respect to $p^{r(n-1)}\boldsymbol{v}$. Consequently, $U_p^r(f) - U_p^{r-1}(f)$ is the Laurent expansion of a rational function $R_{p,r}$ with denominator $Q^{(p^r)}Q^{(p^{r-1})} \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$. This expansion is with respect to the vertex $p^{(2r-1)(n-1)}\boldsymbol{v}$. Note that the rational function $R_{p,r}$ is independent of the choice of $\boldsymbol{v}$.

Let p be a prime such that $f \in \mathbb{Z}_p[[\boldsymbol{x}^{\pm 1}]]$. Then, the corresponding Laurent expansion $U_p^r(f) - U_p^{r-1}(f)$ of $R_{p,r}$ has p-adic integers as coefficients as well. Consequently, the congruence $U_p^r(f) - U_p^{r-1}(f) \equiv 0 \pmod{p^r}$ holds if and only if the numerator of $R_{p,r}$ is divisible by p^r.

Hence, f has the Gauss property if and only if, for all but finitely many primes p, the numerator of $R_{p,r}$ is divisible, for all $r \geq 1$, by p^r. Since this latter statement is independent of the choice of vertex $\boldsymbol{v}$, the claim follows. $\square$

The proof of the next observation actually only makes use of the fact that P/Q satisfies the Gauss congruences for a single suitable prime p.

Proposition 3.5. *Let $P, Q \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$. If P/Q has the Gauss property, then $N(P) \subseteq N(Q)$.*

Proof. To prove this claim it is sufficient to show that, for every vertex $\boldsymbol{v} \in N(Q)$, the Newton polytope $N(P/\boldsymbol{x}^{\boldsymbol{v}})$ is contained in the cone C generated by the vectors $N(Q/\boldsymbol{x}^{\boldsymbol{v}})$. Let p be a prime such that the Gauss congruences for P/Q hold for p and such that the coefficients of P corresponding to vertices of $N(P)$ are p-adic units.

Let $\boldsymbol{v} \in N(Q)$, and let $\sum_{\boldsymbol{k}} f_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}}$ be the Laurent series for P/Q with respect to $\boldsymbol{v}$. For contradiction, suppose that there is a vertex $\boldsymbol{w}$ of $N(P/\boldsymbol{x}^{\boldsymbol{v}})$ such that $\boldsymbol{w} \notin C$. It follows from (7) that $\boldsymbol{w}$ is a vertex of the convex hull of the support of the Laurent series of P/Q with respect to $\boldsymbol{v}$. By our choice of p, $f_{\boldsymbol{w}}$ is a p-adic unit. On the other hand, the point $p\boldsymbol{w}$ is not in the support of the Laurent series, so that $f_{p\boldsymbol{w}} = 0$. This contradicts the congruence $f_{p\boldsymbol{w}} \equiv f_{\boldsymbol{w}} \pmod{p}$. $\square$

Example 3.6. The rational function

$$\frac{P}{Q} = \frac{1 + 2x - x^2}{1 - x^2} = \frac{1}{1-x} + \frac{x}{1+x}$$

obviously satisfies the Gauss congruences for all primes. As predicted by Proposition 3.5, $N(P) \subseteq N(Q)$. However, note that $\operatorname{supp}(P) \nsubseteq \operatorname{supp}(Q)$.

Corollary 3.7. *Suppose $F = P/Q$ with $P, Q \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$ has the Gauss property. Then the Laurent series expansion of F with respect to any vertex $\boldsymbol{v}$ of $N(Q)$ is supported on a proper cone, namely the cone generated by $N(Q/\boldsymbol{x}^{\boldsymbol{v}})$.*

Proof. Recall from (7) that $\boldsymbol{x}^{\boldsymbol{v}}/Q$ has a Laurent series supported on the proper cone C generated by the vectors $N(Q/\boldsymbol{x}^{\boldsymbol{v}})$. By Proposition 3.5, $N(P) \subseteq N(Q)$, so that the Laurent polynomial $P/\boldsymbol{x}^{\boldsymbol{v}}$ is supported on $N(P/\boldsymbol{x}^{\boldsymbol{v}}) \subset C$. Hence, multiplying the Laurent series for $\boldsymbol{x}^{\boldsymbol{v}}/Q$ with $P/\boldsymbol{x}^{\boldsymbol{v}}$, results in a Laurent series for P/Q supported on C. $\square$

A face of $N(Q)$ is a nonempty set $F \subseteq N(Q)$, which is the intersection of $N(Q)$ and $h(\boldsymbol{w}) = d$, where h is a linear form such that $N(Q)$ is contained in the half-space $h(\boldsymbol{w}) \geq d$. Let F be a face of $N(Q)$. We denote with Q_F the Laurent polynomial, which is the sum of monomials of Q with support in F. P_F is likewise obtained from P.

Proposition 3.8. *Let $P, Q \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$. If P/Q satisfies the Gauss congruences for the prime p, then so does P_F/Q_F for every face F of $N(Q)$.*

Proof. Choose a vertex $\boldsymbol{v}$ of $N(Q)$ contained in F. After multiplication of P, Q with $\boldsymbol{x}^{-\boldsymbol{v}}$, we may as well assume that $\boldsymbol{v} = \boldsymbol{0}$. Let h be the linear form such that F is given as the intersection of $h(\boldsymbol{w}) = 0$ and $N(Q)$. Let C be the cone spanned by the vectors of $N(Q)$.

Let $\sum_{\boldsymbol{k}} f_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}}$ be the Laurent series for P/Q with respect to $\mathbf{0}$. We observe from (7) that the Laurent expansion of $1/Q_F$ with respect to $\mathbf{0}$ is obtained from the corresponding expansion of $1/Q$ by selecting only those terms corresponding to $\boldsymbol{k}$ such that $h(\boldsymbol{k}) = 0$. Consequently, the Laurent expansion of P_F/Q_F with respect to $\mathbf{0}$ is similarly given by

$$\sum_{\boldsymbol{k} \in \mathbb{Z}^n} g_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}} = \sum_{\boldsymbol{k} \in \mathbb{Z}^n, h(\boldsymbol{k})=0} f_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}}.$$

Since h is linear, the Gauss congruences $g_{\boldsymbol{m}p^r} \equiv g_{\boldsymbol{m}p^{r-1}} \pmod{p^r}$, for $\boldsymbol{m}$ such that $h(\boldsymbol{m}) = 0$, translate into $f_{\boldsymbol{m}p^r} \equiv f_{\boldsymbol{m}p^{r-1}} \pmod{p^r}$ which holds by assumption. On the other hand, we trivially have $g_{\boldsymbol{m}p^r} \equiv g_{\boldsymbol{m}p^{r-1}} \pmod{p^r}$ if $h(\boldsymbol{m}) \neq 0$ because then both $g_{\boldsymbol{m}p^r}$ and $g_{\boldsymbol{m}p^{r-1}}$ are zero. □

4 Determinants of logarithmic derivatives

This section is concerned with a proof of Theorem 1.1. As indicated in Question 1.2 and the comments following it, Theorem 1.1 appears to play a central role in the quest of classifying rational functions with the Gauss property. In this section, we therefore work over more general rings before again specializing to $\mathbb{Z}$. Though possible, for other, less central, results in this paper we do not pursue this level of generality.

Definition 4.1. An integral domain R with characteristic 0 has a *p-Frobenius lift* ϕ if

(a) (p) is a prime ideal in R, and

(b) there is a ring homomorphism $\phi : R \to R$ such that $\phi(a) \equiv a^p \pmod{p}$ for every $a \in R$.

In the sequel, we often write a^ϕ instead of $\phi(a)$.

The most common example we shall look at is $\mathbb{Z}$, in which case the identity map ϕ is a p-Frobenius lift for all primes p. More generally, if $N \in \mathbb{Z}$, we can consider the ring $\mathbb{Z}[1/N]$, in which case the identity map ϕ is a p-Frobenius lift for all primes p not dividing N. A nontrivial example is the polynomial ring $R = \mathbb{Z}[x]$ with $\phi(Q(x)) = Q(x^p)$. The following lemma suggests a generalization of the Gauss congruences to R.

Lemma 4.2. *Let R be a domain with p-Frobenius lift ϕ. Then, for any $a \in R$ and any positive integer*

$$a^{mp^r} \equiv (a^\phi)^{mp^{r-1}} \pmod{p^r} \tag{9}$$

for all integers $m \geq 0$ and $r \geq 1$.

Proof. It suffices to prove the statement for $m = 1$. We use induction on r. For $r = 1$, the statement follows from the definition of ϕ. Suppose that (9) is true for some $r \geq 1$. That is, $a^{p^r} = (a^\phi)^{p^{r-1}} + p^r b$ for some $b \in R$. Raise this equality to the pth power and consider the result modulo p^{r+1}. Using $p^{kr} \equiv 0 \pmod{p^{r+1}}$ for all $k > 1$, we obtain

$$a^{p^{r+1}} \equiv (a^\phi)^{p^r} + p(a^\phi)^{p^{r-1}(p-1)} p^r b \equiv (a^\phi)^{p^r} \pmod{p^{r+1}}.$$

This completes the induction step. □

Extending Definition 3.1, we therefore say that a Laurent series $f = \sum_{\boldsymbol{k}\in\mathbb{Z}^n} f_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}} \in R[[\boldsymbol{x}^{\pm 1}]]$ satisfies the *Gauss congruences* for the prime p if R has a p-Frobenius lift ϕ and

$$f_{\boldsymbol{m}p^r} \equiv f^{\phi}_{\boldsymbol{m}p^{r-1}} \pmod{p^r}$$

for all $\boldsymbol{m} \in \mathbb{Z}^n$ and all $r \geq 1$.

Proposition 4.3. *Let R be an integral domain and let $f \in R[[\boldsymbol{x}^{\pm 1}]]$ with constant term 1. If $\operatorname{supp}(f) \subseteq C$ for a proper cone C, then there exist $a_{\boldsymbol{k}} \in R$ such that*

$$f = \prod_{\boldsymbol{k}\in C, \boldsymbol{k}\neq \boldsymbol{0}} (1 - a_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}). \tag{10}$$

Proof. Choose α to be a linear form such that $\alpha(\boldsymbol{w}) > 0$ for all nonzero $\boldsymbol{w} \in C$, with the additional property that $\alpha(\boldsymbol{w}) \in \mathbb{Z}$ for $\boldsymbol{w} \in \mathbb{Z}^n$. For $r \in \mathbb{Z}_{>0}$, let I_r be the ideal consisting of Laurent series

$$\sum_{\boldsymbol{k}\in C, \alpha(\boldsymbol{k})\geq r} g_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}.$$

We now construct the exponents $a_{\boldsymbol{k}}$ using induction on $\alpha(\boldsymbol{k})$. Initialization follows from the observation that $f \equiv 1 \pmod{I_1}$. Suppose we have constructed $a_{\boldsymbol{k}} \in R$, for all $\boldsymbol{k} \in C$ with $\alpha(\boldsymbol{k}) < r$, such that

$$f \equiv \prod_{\boldsymbol{k}\in C, \boldsymbol{k}\neq\boldsymbol{0}, \alpha(\boldsymbol{k})<r} (1 - a_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}) \pmod{I_r}. \tag{11}$$

Consider the Laurent series

$$g = f \prod_{\boldsymbol{k}\in C, \boldsymbol{k}\neq\boldsymbol{0}, \alpha(\boldsymbol{k})<r} (1 - a_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}})^{-1} = \sum_{\boldsymbol{k}\in C} g_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}},$$

and note that $g \equiv 1 \pmod{I_r}$. For $\boldsymbol{k} \in C$ with $\alpha(\boldsymbol{k}) = r$, we now simply choose $a_{\boldsymbol{k}} = g_{\boldsymbol{k}}$. By construction, (11) then holds with r replaced by $r + 1$. ☐

Recall that $\theta_i = x_i \frac{\partial}{\partial x_i}$ denotes the Euler operator. Suppose that $f \in R[[\boldsymbol{x}^{\pm 1}]]$ is a Laurent series satisfying the conditions of Proposition 4.3, so that (10) holds. Then,

$$\frac{\theta_i f}{f} = -\sum_{\boldsymbol{k}\in C, \boldsymbol{k}\neq\boldsymbol{0}} \frac{k_i a_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}}{1 - a_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}} \in R[[\boldsymbol{x}^{\pm 1}]].$$

If R is a domain with p-Frobenius lift ϕ, then a brief argument and Lemma 4.2 show that $k_i a_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}/(1 - a_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}})$ satisfies the Gauss congruences for p. We conclude that $\theta_i f/f$, as a sum of such terms, satisfies the Gauss congruences for p. This is the case $m = 1$ of the next result, which generalizes this observation.

Theorem 4.4. *Let R be a domain with p-Frobenius lift ϕ. Let $m \leq n$ and let $f_1, \ldots, f_m \in R[[\boldsymbol{x}^{\pm 1}]]$, each with constant term equal to 1 and $\operatorname{supp}(f_j) \subseteq C$ for a proper cone C. Then the Laurent series*

$$F = \det\left(\frac{\theta_i f_j}{f_j}\right)_{i,j=1,\ldots,m} \tag{12}$$

satisfies the Gauss congruences for p.

Proof. Suppose that $m < n$. If we define $f_i = x_i$ for $i = m+1, m+2, \ldots, n$, then the original $m \times m$ determinant (12) obtained from $f_1, \ldots, f_m$ is the same as the $n \times n$ determinant obtained from $f_1, \ldots, f_n$. In the sequel, we may therefore assume that $m = n$.

We start with the special case $f_j = 1 - a_j \boldsymbol{x}^{\boldsymbol{k}^{(j)}}$ with $\boldsymbol{k}^{(j)} = (k_1^{(j)}, \ldots, k_n^{(j)}) \in C$ and $a_j \in R$. Let K be the $n \times n$ matrix with entries $k_i^{(j)}$ with $i, j = 1, 2, \ldots, n$. Then,

$$F = \det \left(\frac{-k_i^{(j)} a_j \boldsymbol{x}^{\boldsymbol{k}^{(j)}}}{1 - a_j \boldsymbol{x}^{\boldsymbol{k}^{(j)}}} \right)_{i,j=1,\ldots,n} = (-1)^n \det(K) \prod_{j=1}^{n} \frac{a_j \boldsymbol{x}^{\boldsymbol{k}^{(j)}}}{1 - a_j \boldsymbol{x}^{\boldsymbol{k}^{(j)}}},$$

which can be expanded as

$$F = (-1)^n \det(K) \sum_{r_1, \ldots, r_n \geq 1}^{n} \left(\prod_{j=1}^{n} a_j^{r_j} \right) \boldsymbol{x}^{r_1 \boldsymbol{k}^{(1)} + \cdots + r_n \boldsymbol{k}^{(n)}} = \sum_{\boldsymbol{k} \in C} c_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}}.$$

If $\det(K) = 0$, then all terms are zero and the claim is trivially true. So, let us assume $\det(K) \neq 0$. Then the exponents $r_1 \boldsymbol{k}^{(1)} + \cdots + r_n \boldsymbol{k}^{(n)} = K\boldsymbol{r}$ are in one-to-one correspondence with the n-tuples $\boldsymbol{r} = (r_1, \ldots, r_n)$.

First, suppose that $\boldsymbol{r}$ is such that p divides $\boldsymbol{r}$. Then, by Lemma 4.2,

$$\boldsymbol{a}^{\boldsymbol{r}} = \prod_{j=1}^{n} a_j^{r_j} \equiv \prod_{j=1}^{n} (a_j^{\phi})^{r_j/p} = (\boldsymbol{a}^{\phi})^{\boldsymbol{r}/p} \pmod{p^{\nu_p(\boldsymbol{r})}},$$

so that

$$\begin{aligned} c_{K\boldsymbol{r}} &= (-1)^n \det(K) \boldsymbol{a}^{\boldsymbol{r}} \\ &\equiv (-1)^n \det(K) (\boldsymbol{a}^{\phi})^{\boldsymbol{r}/p} \\ &= ((-1)^n \det(K) \boldsymbol{a}^{\boldsymbol{r}/p})^{\phi} = c^{\phi}_{K\boldsymbol{r}/p} \pmod{p^{\nu_p(\boldsymbol{r}) + \nu_p(\det(K))}}. \end{aligned}$$

Some linear algebra shows that $\nu_p(K\boldsymbol{r}) \leq \nu_p(\det(K)) + \nu_p(\boldsymbol{r})$. Therefore, $c_{K\boldsymbol{r}} \equiv c^{\phi}_{K\boldsymbol{r}/p} \pmod{p^{\nu_p(K\boldsymbol{r})}}$. Next, suppose that p does not divide $\boldsymbol{r}$. Then $\nu_p(K\boldsymbol{r}) \leq \nu_p(\det(K))$ and, thus, $c_{K\boldsymbol{r}} = (-1)^n \det(K) \boldsymbol{a}^{\boldsymbol{r}}$ is divisible by $p^{\nu_p(K\boldsymbol{r})}$, whereas $c_{K\boldsymbol{r}/p} = 0$. Hence, the congruence $c_{K\boldsymbol{r}} \equiv c^{\phi}_{K\boldsymbol{r}/p} \pmod{p^{\nu_p(K\boldsymbol{r})}}$ holds again. We conclude that F satisfies the Gauss congruences for the prime p.

In the case of general Laurent series f_j, we consider the differential form

$$\Omega = \frac{\mathrm{d}f_1}{f_1} \wedge \cdots \wedge \frac{\mathrm{d}f_n}{f_n}$$

and observe that the coefficient of $\mathrm{d}x_1 \wedge \cdots \wedge \mathrm{d}x_n / (x_1 \cdots x_n)$ is given by F. On the other hand, it follows from Proposition 4.3 that

$$f_j = \prod_{\boldsymbol{k} \in C, \boldsymbol{k} \neq \boldsymbol{0}} (1 - a_{\boldsymbol{k}}^{(j)} \boldsymbol{x}^{\boldsymbol{k}}),$$

for $a_{\boldsymbol{k}}^{(j)} \in R$, so that

$$\Omega = (-1)^n \sum_{\substack{\boldsymbol{k}^{(1)}, \ldots, \boldsymbol{k}^{(n)} \in C \\ \boldsymbol{k}^{(1)}, \ldots, \boldsymbol{k}^{(n)} \neq \boldsymbol{0}}} \left(\prod_{j=1}^{n} a_{\boldsymbol{k}}^{(j)} \right) \frac{\mathrm{d}\boldsymbol{x}^{\boldsymbol{k}^{(1)}}}{1 - a_{\boldsymbol{k}}^{(1)} \boldsymbol{x}^{\boldsymbol{k}^{(1)}}} \wedge \cdots \wedge \frac{\mathrm{d}\boldsymbol{x}^{\boldsymbol{k}^{(n)}}}{1 - a_{\boldsymbol{k}}^{(n)} \boldsymbol{x}^{\boldsymbol{k}^{(n)}}}.$$

From our initial special case, we see that the coefficient of $\mathrm{d}x_1 \wedge \cdots \wedge \mathrm{d}x_n/(x_1 \cdots x_n)$ in each term satisfies the Gauss congruences for p. Hence, the same holds for their sum, which equals F. $\square$

Theorem 4.5. *Let $m \le n$ and let $f_1, \ldots, f_m \in \mathbb{Q}(\boldsymbol{x})$ be nonzero. Then the rational function*

$$\det\left(\frac{\theta_i f_j}{f_j}\right)_{i,j=1,\ldots,m} \tag{13}$$

has the Gauss property.

Proof. Let us write $D(f_1, \ldots, f_m)$ for (13). Observe that this quantity is logarithmic in each of its arguments f_j. That is, for instance,

$$D(gh, f_2, \ldots, f_m) = D(g, f_2, \ldots, f_m) + D(h, f_2, \ldots, f_m).$$

From this logarithmic property it follows that it suffices to restrict to Laurent polynomials $f_1, \ldots, f_m \in \mathbb{Z}[\boldsymbol{x}^{\pm 1}]$ (we could further restrict to polynomials but the argument to follow works with Laurent polynomials).

We next determine vertices $\boldsymbol{v}_i$ of $N(f_i)$ such that $f_i/\boldsymbol{x}^{\boldsymbol{v}_i}$ are Laurent polynomials with support in the same proper cone C. To that end, let α be a linear form on $\mathbb{R}^n$ whose coefficients are $\mathbb{Q}$-linearly independent. For each $i = 1, \ldots, m$, let c_i be the minimum of the set $\{\alpha(\boldsymbol{x}) : \boldsymbol{x} \in N(f_i)\}$. Then $N(f_i)$ is contained in the half-space $\alpha(\boldsymbol{x}) \ge c_i$. Moreover, because the coefficients of α are $\mathbb{Q}$-linearly independent, the hyperplane $\alpha(\boldsymbol{x}) = c_i$ intersects $N(f_i)$ in a unique vertex $\boldsymbol{v}_i$. Hence, $N(f_i/\boldsymbol{x}^{\boldsymbol{v}_i})$ is contained in the half-space $\alpha(\boldsymbol{x}) \ge 0$, and the intersection of $N(f_i/\boldsymbol{x}^{\boldsymbol{v}_i})$ and $\alpha(\boldsymbol{x}) = 0$ consists of only the point $\mathbf{0}$. Let C be the cone spanned by all the $N(f_i/\boldsymbol{x}^{\boldsymbol{v}_i})$. Note that C is proper because $\alpha(\boldsymbol{x}) > 0$ for all nonzero $\boldsymbol{x} \in C$.

By construction, the Laurent polynomials $g_i = f_i/\boldsymbol{x}^{\boldsymbol{v}_i}$ are supported on C and $\mathbf{0}$ is a vertex of $N(g_i)$. Using the logarithmic property of (13), and the fact that $\partial x_j/\partial x_i = 0$ if $i \ne j$, it follows that $D(f_1, \ldots, f_m)$ is a $\mathbb{Z}$-linear combination of terms of the form $D(g_{i_1}, \ldots, g_{i_s})$ with $1 \le i_1 < \ldots < i_s \le m$. On the other hand, it follows from Theorem 4.4 that $D(g_{i_1}, \ldots, g_{i_s})$ has the Gauss property, from which we conclude that $D(f_1, \ldots, f_m)$ has the Gauss property as well. $\square$

5 A classification result

We begin with a somewhat technical but general result. Observe that the case $r = 0$ implies that $q_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}/Q$ in (14) satisfies Gauss congruences. Likewise, the determinant in (14) satisfies Gauss congruences by Theorem 4.4. That is, both factors of (14) satisfy Gauss congruences. However, if two Laurent series satisfy Gauss congruences, then it is not the case, in general, that their product satisfies Gauss congruences as well.

Proposition 5.1. *Let $Q \in \mathbb{Z}_p[[\boldsymbol{x}, \boldsymbol{y}]]$ with constant term 1. Suppose that Q is linear in the variables $\boldsymbol{x} = x_1, \ldots, x_n$ (but not necessarily in $\boldsymbol{y} = y_1, \ldots, y_m$). Further, for $0 \le r \le m$, let $f_1, \ldots, f_r \in \mathbb{Z}_p[[\boldsymbol{y}]]$ with constant term 1. Write $Q = \sum_{\boldsymbol{k}} q_{\boldsymbol{k}}(\boldsymbol{y})\boldsymbol{x}^{\boldsymbol{k}}$. Then, for any $\boldsymbol{k}$,*

$$\frac{q_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}}{Q} \det\left(\frac{\theta_i f_j}{f_j}\right)_{i,j=1,\ldots,r} \tag{14}$$

satisfies Gauss congruences for the prime p.

Proof. Let $\boldsymbol{k} = (k_1, \ldots, k_n) \in \{0,1\}^n$. Notice that

$$\left[\prod_{j=1}^{n} \theta_j^{k_j} (1-\theta_j)^{1-k_j}\right] Q = q_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}}.$$

Hence, it suffices to show that (14) holds with $q_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}}$ replaced with any product of θ_j applied to Q. Without loss of generality, we consider the product $\theta_1 \cdots \theta_\ell Q$.

For $j = 1, \ldots, \ell$, define

$$g_j = \frac{\partial}{\partial x_{j-1}} \cdots \frac{\partial}{\partial x_2} \frac{\partial}{\partial x_1} Q,$$

so that $g_1 = Q$. Note that g_j does not depend on the variables $x_1, \ldots, x_{j-1}$ because Q is linear in the variables $x_1, \ldots, x_n$. Therefore, applying Theorem 4.4 to $g_1, \ldots, g_\ell, f_1, \ldots, f_r$, we find that

$$\frac{\theta_1 g_1}{g_1} \cdots \frac{\theta_\ell g_\ell}{g_\ell} \det \left(\frac{\theta_i f_j}{f_j}\right)_{i,j=1,\ldots,r}$$

satisfies the Gauss congruences for p. Observe that, since $\theta_j g_j = x_j g_{j+1}$,

$$\frac{\theta_1 g_1}{g_1} \cdots \frac{\theta_\ell g_\ell}{g_\ell} = \frac{\theta_1 \cdots \theta_\ell Q}{Q}.$$

We have therefore shown that (14) indeed holds with $q_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}}$ replaced with any product of θ_j applied to Q. $\square$

Example 5.2. Take $Q(x,y) = \frac{1}{f(y)} - x$ for some

$$f = \sum_{k=0}^{\infty} a_k y^k \in \mathbb{Z}[[y]]^\times.$$

Since $Q(x,y)$ is linear in x, Proposition 5.1 implies that

$$\frac{1/f(y)}{Q(x,y)} = \frac{1}{1 - f(y)x} = \sum_{k=0}^{\infty} f(y)^k x^k$$

satisfies the Gauss congruences for all primes. Equivalently, the coefficients $c_{k,\ell}$ of $x^k y^\ell$, that is

$$c_{k,\ell} = \sum_{\substack{j_1,\ldots,j_k \geq 0 \\ j_1+\ldots+j_k=\ell}} a_{j_1} \cdots a_{j_\ell},$$

satisfy the congruences $c_{kp^r,\ell p^r} \equiv c_{kp^{r-1},\ell p^{r-1}} \pmod{p^r}$ for all primes p and all $r \geq 1$. Establishing these congruences directly is less straightforward.

Example 5.3. Take $Q(x,y) = 1 - x - x^2 - y$. Since Q is linear in y, it follows from Proposition 5.1 with $\boldsymbol{k} = \boldsymbol{0}$ that, for any $f \in \mathbb{Z}_p[[x]]$ with $f(0) = 1$, the product

$$\frac{1 - x - x^2}{1 - x - x^2 - y} \frac{\theta_x f}{f}$$

satisfies the Gauss congruences for p. In fact, since $(\theta_x f)/f$ is logarithmic in f and since $(\theta_x x^k)/x^k = k$, the same is obviously true for any $f \in \mathbb{Z}_p[[x]]$. For instance, choosing $f = x^2/(1-x-x^2)$, we find that

$$\frac{2-x}{1-x-x^2-y}$$

satisfies the Gauss congruences for all primes. In this particular case, the same conclusion follows from Theorem 5.4.

Theorem 5.4. *Let $P, Q \in \mathbb{Z}[z, \boldsymbol{x}]$ such that Q is linear in the variables $\boldsymbol{x}$. Write $P = \sum_{\boldsymbol{k}} p_{\boldsymbol{k}}(z)\boldsymbol{x}^{\boldsymbol{k}}$ and $Q = \sum_{\boldsymbol{k}} q_{\boldsymbol{k}}(z)\boldsymbol{x}^{\boldsymbol{k}}$ with $p_{\boldsymbol{k}}, q_{\boldsymbol{k}} \in \mathbb{Z}[z]$. Then P/Q has the Gauss property if and only if $p_{\boldsymbol{k}} \neq 0$ implies $q_{\boldsymbol{k}} \neq 0$ and $p_{\boldsymbol{k}}/q_{\boldsymbol{k}}$ has the Gauss property for all $\boldsymbol{k}$ with $q_{\boldsymbol{k}} \neq 0$.*

Proof. Suppose P/Q has the Gauss property. Let $\boldsymbol{k}$ be such that $p_{\boldsymbol{k}} \neq 0$. Suppose $q_{\boldsymbol{k}} = 0$. Since the points $\boldsymbol{k}$ are vertices of the hypercube $[0,1]^n$, this means that the support of $p_{\boldsymbol{k}}\boldsymbol{x}^{\boldsymbol{k}}$ is outside $N(Q)$, contradicting Proposition 3.5. Hence, $q_{\boldsymbol{k}} \neq 0$. Further, notice that $p_{\boldsymbol{k}}/q_{\boldsymbol{k}}$ is P_F/Q_F, where F is the face of $N(Q)$ corresponding to $\boldsymbol{k}$. According to Proposition 3.8, $p_{\boldsymbol{k}}/q_{\boldsymbol{k}}$ has the Gauss property.

Now, fix $\boldsymbol{k}$ and suppose that $q_{\boldsymbol{k}} \neq 0$ and that $p_{\boldsymbol{k}}/q_{\boldsymbol{k}}$ has the Gauss property. We shall prove that $p_{\boldsymbol{k}}(z)\boldsymbol{x}^{\boldsymbol{k}}/Q$ has the Gauss property. The general theorem then follows by summing over all such $\boldsymbol{k}$. First, observe that Theorem 8.1 tells us that there are polynomials $u_j \in \mathbb{Z}[z]$ such that $p_{\boldsymbol{k}}/q_{\boldsymbol{k}} = \sum_j c_j z u_j'/u_j$ for some $c_j \in \mathbb{Q}$.

By Proposition 5.1,

$$\sum_j \frac{q_{\boldsymbol{k}}(z)\boldsymbol{x}^{\boldsymbol{k}}}{Q}\frac{zu_j'}{u_j} = \frac{q_{\boldsymbol{k}}(z)\boldsymbol{x}^{\boldsymbol{k}}}{Q}\frac{p_{\boldsymbol{k}}(z)}{q_{\boldsymbol{k}}(z)} = \frac{p_{\boldsymbol{k}}(z)\boldsymbol{x}^{\boldsymbol{k}}}{Q}$$

has the Gauss property. ☐

Example 5.5. Monthly problem #11757 [Ges14], proposed by Gessel, concerns the rational function

$$F(x,y) = \frac{1}{(1-3x)(1-y-3x+3x^2)} = \sum_{m,n=0}^{\infty} c_{m,n}x^m y^n.$$

The problem asks the reader to show that the diagonal Taylor coefficients $c_{n,n}$ equal 9^n. We will not spoil the fun of that challenge but only note that, as a consequence, the sequence of diagonal coefficients satisfies Gauss congruences for all primes. On the other hand, it is an immediate consequence of Theorem 5.4 and Theorem 8.1, applied to

$$\frac{1}{(1-3x)(1-3x+3x^2)} = \frac{\theta_x u}{u}, \quad u = \frac{x(1-3x+3x^2)}{(1-3x)^3},$$

that $F(x,y)$ has the Gauss property for all primes. In other words, all Taylor coefficients $c_{m,n}$ satisfy Gauss congruences for all primes.

A useful and immediate consequence of Theorem 5.4 is the following characterization of rational functions, whose denominator is linear in each variable (that is, the denominator $Q \in \mathbb{Z}[\boldsymbol{x}]$ has support $\mathrm{supp}(Q) \subseteq \{0,1\}^n$).

Theorem 5.6. *Let $P, Q \in \mathbb{Z}[\boldsymbol{x}]$ and suppose that Q is linear in each variable. Then P/Q has the Gauss property if and only if $N(P) \subseteq N(Q)$.*

Example 5.7. The *Delannoy numbers*

$$D_{n_1,n_2} = \sum_{k=0}^{\min(n_1,n_2)} \binom{n_1}{k}\binom{n_1+n_2-k}{n_1}$$

are the Laurent series coefficients of the rational function

$$\frac{1}{1-x-y-xy} = \sum_{k_1,k_2=0}^{\infty} D_{k_1,k_2} x^{k_1} y^{k_2}$$

with respect to the vertex $(0,0)$. By Theorem 5.6, each of the rational functions

$$\frac{1}{1-x-y-xy}, \quad \frac{x}{1-x-y-xy}, \quad \frac{y}{1-x-y-xy}, \quad \frac{xy}{1-x-y-xy}$$

has the Gauss property. In fact, they satisfy the Gauss congruences for all primes. Consequently, for any prime p and $\boldsymbol{\delta} \in \{0,1\}^2$, the Delannoy numbers $D_{\boldsymbol{n}}$ satisfy the (shifted) congruences

$$D_{\boldsymbol{m}p^r-\boldsymbol{\delta}} \equiv D_{\boldsymbol{m}p^{r-1}-\boldsymbol{\delta}} \pmod{p^r}$$

for all $\boldsymbol{m} \in \mathbb{Z}^2_{>0}$ and all $r \geq 1$.

6 Toroidal substitutions

A substitution of the form $x_i = \boldsymbol{y}^{\boldsymbol{a}_i}$, $i = 1,\dots,n$, with $\boldsymbol{a}_1,\dots,\boldsymbol{a}_n \in \mathbb{Q}^m$ linearly independent, is called a *toroidal substitution*. Let A be the $m \times n$ matrix with columns $\boldsymbol{a}_1,\dots,\boldsymbol{a}_n$. Note that, for any $\boldsymbol{k} \in \mathbb{Z}^n$, $\boldsymbol{x}^{\boldsymbol{k}} = \boldsymbol{y}^{A\boldsymbol{k}}$. We therefore write the toroidal substitution simply as $\boldsymbol{x} = \boldsymbol{y}^A$. The next result shows that toroidal substitutions preserve the Gauss property.

Proposition 6.1. *Let $f = \sum_{\boldsymbol{k}\in\mathbb{Z}^n} f_{\boldsymbol{k}} \boldsymbol{x}^{\boldsymbol{k}} \in \mathbb{Z}_p[[\boldsymbol{x}^{\pm 1}]]$. Let A be an $m \times n$ matrix with linearly independent columns $\boldsymbol{a}_1,\dots,\boldsymbol{a}_n \in \mathbb{Q}^m$, such that $A\boldsymbol{k} \in \mathbb{Z}^m$ for all $\boldsymbol{k} \in \operatorname{supp}(f)$. Define the Laurent series $g \in \mathbb{Z}_p[[\boldsymbol{y}^{\pm 1}]]$ by*

$$g(y_1,\dots,y_m) = f(\boldsymbol{y}^{\boldsymbol{a}_1},\dots,\boldsymbol{y}^{\boldsymbol{a}_n}) = \sum_{\boldsymbol{k}\in\mathbb{Z}^n} f_{\boldsymbol{k}} \boldsymbol{y}^{A\boldsymbol{k}}.$$

Suppose that the prime p is such that $A \in \mathbb{Z}_p^{m\times n}$ and $A \pmod p$ has rank n. Then, g satisfies the Gauss congruences for p if and only if f does.

Proof. Since $\operatorname{rank}(A) = n$, the map $\mathbb{Z}^n \to \mathbb{Q}^m$, $\boldsymbol{k} \mapsto A\boldsymbol{k}$, is injective. Let us write I for the image of this map restricted to $\mathbb{Z}^m$. That is, I is the set of $\boldsymbol{m} \in \mathbb{Z}^m$ such that $\boldsymbol{m} = A\boldsymbol{k}$ for some $\boldsymbol{k} \in \mathbb{Z}^n$. In the sequel, we write $A^{-1}\boldsymbol{m} = \boldsymbol{k}$ for that unique vector $\boldsymbol{k}$.

We claim that $\nu_p(A\boldsymbol{k}) = \nu_p(\boldsymbol{k})$ for all $\boldsymbol{k} \in \mathbb{Z}^n$. Since $A \in \mathbb{Z}_p^{m\times n}$, we obviously have $\nu_p(A\boldsymbol{k}) \geq \nu_p(\boldsymbol{k})$. On the other hand, $A \pmod p$ has rank n, that is, $A\boldsymbol{k} \equiv \boldsymbol{0} \pmod p$ implies $\boldsymbol{k} \equiv \boldsymbol{0} \pmod p$. It follows inductively (or from the fact that $A \pmod{p^r}$ has rank n) that $A\boldsymbol{k} \equiv \boldsymbol{0} \pmod{p^r}$ implies $\boldsymbol{k} \equiv \boldsymbol{0} \pmod{p^r}$. Hence, $\nu_p(A\boldsymbol{k}) \leq \nu_p(\boldsymbol{k})$. Observe that, as a consequence, $\boldsymbol{m}p^r \in I$ if and only if $\boldsymbol{m} \in I$.

By construction,

$$g = \sum_{\boldsymbol{m} \in \mathbb{Z}^m} g_{\boldsymbol{m}} \boldsymbol{y}^{\boldsymbol{m}} = \sum_{\boldsymbol{k} \in \mathbb{Z}^n} f_{\boldsymbol{k}} \boldsymbol{y}^{A\boldsymbol{k}} = \sum_{\boldsymbol{m} \in I} f_{A^{-1}\boldsymbol{m}} \boldsymbol{y}^{\boldsymbol{m}},$$

so that $g_{\boldsymbol{m}} = f_{A^{-1}\boldsymbol{m}}$ if $\boldsymbol{m} \in I$ and $g_{\boldsymbol{m}} = 0$ otherwise. On the other hand, $f_{\boldsymbol{k}} = g_{A\boldsymbol{k}}$ for all $\boldsymbol{k}$ such that $A\boldsymbol{k} \in \mathbb{Z}^m$.

Suppose that g satisfies the Gauss congruences for p. Let $\boldsymbol{k} \in \mathbb{Z}^n$. If $A\boldsymbol{k} \in \mathbb{Z}^m$, then

$$f_{\boldsymbol{k}p^r} \equiv g_{(A\boldsymbol{k})p^r} \equiv g_{(A\boldsymbol{k})p^{r-1}} \equiv f_{\boldsymbol{k}p^{r-1}} \pmod{p^r}.$$

If $A\boldsymbol{k} \notin \mathbb{Z}^m$, then it follows from $A \in \mathbb{Z}_p^{m \times n}$ that $A\boldsymbol{k}p^r \notin \mathbb{Z}^m$. Hence, $f_{\boldsymbol{k}p^r} = f_{\boldsymbol{k}p^{r-1}} = 0$. Thus, f satisfies the Gauss congruences for p.

Finally, suppose that f satisfies the Gauss congruences for p. Let $\boldsymbol{m} \in \mathbb{Z}^m$. If $\boldsymbol{m} \in I$, then $\boldsymbol{m} = A\boldsymbol{k}$ for some $\boldsymbol{k} \in \mathbb{Z}^n$, and

$$g_{\boldsymbol{m}p^r} = f_{\boldsymbol{k}p^r} \equiv f_{\boldsymbol{k}p^{r-1}} = g_{\boldsymbol{m}p^{r-1}} \pmod{p^r}.$$

If $\boldsymbol{m} \notin I$, then $\boldsymbol{m}p^r, \boldsymbol{m}p^{r-1} \notin I$, so that $g_{\boldsymbol{k}p^r} = g_{\boldsymbol{k}p^{r-1}} = 0$. Consequently, g satisfies the Gauss congruences for p. $\square$

Example 6.2. It follows from Proposition 6.1 that

$$\frac{2 - xy}{1 - xy - x^2y^2}$$

has the Gauss property if and only if $(2-x)/(1-x-x^2)$ does. The latter is the generating function for the Lucas numbers. That it has the Gauss property follows, for instance, from Theorem 4.5.

Example 6.3. As observed in Example 5.3, the rational function $F(x, y) = (2-x)/(1-x-x^2-y)$ has the Gauss property. However, $F(x, 1) = (x-2)/(x+x^2)$ does not have the Gauss property because it violates the necessary condition of Proposition 3.5. This illustrates that the condition in Proposition 6.1 on the rank of A cannot be dropped.

Example 6.4. Consider $Q = 1 + y_1^3y_2y_3 + y_1y_2y_3^3 + 3y_1^2y_2y_3^2$. In that case, $N(Q)$ lies in a two-dimensional subspace of $\mathbb{R}^3$. Note that $(3, 1, 1)$ and $(1, 1, 3)$ are vertices of $N(Q)$, while $(2, 1, 2)$ is not. We can obtain $Q(\boldsymbol{y})$ from $\tilde{Q}(\boldsymbol{x}) = 1 + x_1^2 + x_2^2 + 3x_1x_2$ via the toroidal substitution

$$x_1 = y_1^{3/2}y_2^{1/2}y_3^{1/2}, \quad x_2 = y_1^{1/2}y_2^{1/2}y_3^{3/2}.$$

Let $p > 2$ be a primes. It follows from Proposition 6.1 that $1/Q$ satisfies the Gauss congruences for p if and only if $1/\tilde{Q}$ satisfies the Gauss congruences for p.

Remark 6.5. Let $\boldsymbol{x} = \boldsymbol{y}^A$ be a toroidal substitution with invertible matrix $A \in \mathbb{Q}^{n \times n}$. Observe that, for any $f_1, \ldots, f_n$,

$$\det\left(\frac{\theta_{y_i} f_j}{f_j}\right)_{i,j=1,\ldots,n} = \det(A) \det\left(\frac{\theta_{x_i} f_j}{f_j}\right)_{i,j=1,\ldots,n}.$$

This can be seen, for instance, by recalling that the left-hand side is the coefficient of $\mathrm{d}y_1 \wedge \cdots \wedge \mathrm{d}y_n/(y_1 \cdots y_n)$ in $\mathrm{d}f_1 \wedge \cdots \wedge \mathrm{d}f_n/(f_1 \cdots f_n)$, and realizing that $\mathrm{d}x_1 \wedge \cdots \wedge \mathrm{d}x_n/(x_1 \cdots x_n)$ and $\mathrm{d}y_1 \wedge \cdots \wedge \mathrm{d}y_n/(y_1 \cdots y_n)$ only differ by a factor of $\det(A)$. We conclude that an invertible toroidal substitution does not affect the answer to Question 1.2.

Example 6.6. Suppose that $Q \in \mathbb{Z}[x, y]$ has total degree 2. We will show that, for any rational function P/Q with $P \in \mathbb{Z}[x, y]$, the answer to Question 1.2 is affirmative. That is, P/Q has the Gauss property if and only if P/Q can be written as a $\mathbb{Q}$-linear combination of functions of the form (4). By Theorem 4.5, we only need to prove the "only if" part of that statement.

First, observe that this is a consequence of our proof of Theorem 5.4 in the case that Q is linear in at least one of the variables x, y. We may therefore assume that $(2, 0)$ and $(0, 2)$ are vertices of $N(Q)$. Suppose that $(0, 0)$ is not a vertex of $N(Q)$. Then $Q = bx + cy + dx^2 + exy + fy^2$, so that $Q/x^2 = bu + cuv + d + ev + fv^2$ in terms of the toroidal substitution $u = 1/x$, $v = y/x$. Note that the latter is linear in u, so that, by Proposition 6.1, we are reduced to a known case. We may therefore assume in the sequel that $N(Q)$ is the triangle with vertices $(0, 0), (2, 0), (0, 2)$. The number of lattice points in $N(Q)$ is 6.

Consider the vector space V_Q of polynomials $P \in \mathbb{Z}[x, y]$ such that P/Q has the Gauss property. It follows from Proposition 3.5 that V_Q consists of polynomials of total degree at most 2. In particular, $\dim V_Q \leq 6$. On the other hand, by Theorem 4.5, 1 as well as $x\frac{\partial Q}{\partial x}/Q$ and $y\frac{\partial Q}{\partial y}/Q$ have the Gauss property. Hence, V_Q contains Q, $x\partial Q/\partial x$ and $y\partial Q/\partial y$, implying that $\dim V_Q \geq 3$. We will see below that $\dim V_Q$ can indeed take any value in $\{3, 4, 5, 6\}$. Let F be one of the three 1-dimensional faces of $N(Q)$. By Proposition 3.8, if $P \in V_Q$, then P_F/Q_F has the Gauss property.

Note that, possibly after a toroidal substitution, P_F/Q_F is a univariate rational function $p_F(x)/q_F(x)$ with $p_F, q_F \in \mathbb{Z}[x]$, $\deg q_F = 2$ and $q_F(0) \neq 0$. By the same arguments as above, the vector space V_{q_F} of polynomials $p \in \mathbb{Z}[x]$, such that p/q_F has the Gauss property, has dimension 2 or 3. Moreover, it follows from Theorem 8.1 that $\dim V_{q_F} = 3$ if and only if $q_F(x)$ has two distinct rational roots.

Let F_x be the face with vertices $(0, 0)$ and $(2, 0)$. Likewise, let F_y be the face with vertices $(0, 0)$, $(0, 2)$, and F_{xy} the face with vertices $(2, 0), (0, 2)$.

Suppose $q_{F_{xy}}(x)$ has two distinct rational roots. That is, $Q = a + bx + cy + dx^2 + exy + fy^2$ and $dx^2 + exy + fy^2 = d(x + \alpha y)(x + \beta y)$ for some $\alpha, \beta \in \mathbb{Q}$ with $\alpha \neq \beta$. Without loss, $d = 1$. Observe that $Q = \varepsilon + (x + \alpha y + \gamma)(x + \beta y + \delta)$, where $\gamma = (\alpha b - c)/(\alpha - \beta)$, $\delta = (c - \beta b)/(\alpha - \beta)$ and $\varepsilon = a - \gamma\delta$ are all rational. Theorem 4.5, applied to $f_1 = x + \alpha y + \gamma$ and $f_2 = Q$, shows that

$$\frac{\theta_x f_1}{f_1}\frac{\theta_y f_2}{f_2} - \frac{\theta_y f_1}{f_1}\frac{\theta_x f_2}{f_2} = \frac{(\beta - \alpha)xy}{Q}$$

has the Gauss property. In particular, xy/Q has the Gauss property. By using a toroidal substitution to translate to this case and applying Proposition 6.1, we conclude that, for $m \in \{x, y, xy\}$, if $q_{F_m}(x)$ has two distinct rational roots, then m/Q has the Gauss property and, by Remark 6.5, is a linear combination of functions of the form (4).

Let $M \subseteq \{x, y, xy\}$ consist of those m such that $q_{F_m}(x)$ has two distinct rational roots. For each $m \in \{x, y, xy\}$ with $m \notin M$, we obtain a linear constraint for V_Q coming from the condition that P_{F_m}/Q_{F_m} has the Gauss property. These $3 - |M|$ constraints are linearly independent, so that $\dim V_Q \leq 6 - (3 - |M|) = 3 + |M|$. On the other hand, V_Q contains Q, $x\partial Q/\partial x$, $y\partial Q/\partial y$ as well as m for $m \in M$. Since these are linearly independent, we conclude that $\dim V_Q = 3 + |M|$ and that all $P \in V_Q$ are a linear combination of functions of the form (4).

7 Univariate substitutions

In order to prove Theorem 1.6, we begin with the following corresponding result for Laurent series. The statement is necessarily more technical because conditions are needed to ensure that the composition of series is well-defined.

Theorem 7.1. *Let α be a linear form on $\mathbb{R}^{n+1}$ such that $\alpha(1,0,0,\dots,0) > 0$. Let $f(z,\boldsymbol{x}) \in \mathbb{Z}_p[[z^{\pm 1},\boldsymbol{x}^{\pm 1}]]$ such that $\alpha(\boldsymbol{w}) > 0$ for all $\boldsymbol{w} \in \operatorname{supp}(f)$. Let $g(z) \in z^r\mathbb{Z}_p[[z]]^\times$, for $r \in \mathbb{Z}_{>0}$. Suppose f satisfies the Gauss congruences for the prime p. Then so does*

$$F(z,\boldsymbol{x}) = \frac{zg'(z)}{g(z)} f(g(z),\boldsymbol{x}).$$

Proof. By assumption,

$$f(z,\boldsymbol{x}) = \sum_{\alpha(\ell,\boldsymbol{k})>0} f_{\ell,\boldsymbol{k}} z^\ell \boldsymbol{x}^{\boldsymbol{k}}, \tag{15}$$

where the sum is over all $\ell \in \mathbb{Z}$, $\boldsymbol{k} \in \mathbb{Z}^n$ such that $\alpha(\ell,\boldsymbol{k}) > 0$. First, let us note that

$$f(g(z),\boldsymbol{x}) = \sum_{\alpha(\ell,\boldsymbol{k})>0} f_{\ell,\boldsymbol{k}} g(z)^\ell \boldsymbol{x}^{\boldsymbol{k}}$$

is a well-defined Laurent series in $\mathbb{Z}_p[[z^{\pm 1},\boldsymbol{x}^{\pm 1}]]$, since contributions to the coefficient of $z^L\boldsymbol{x}^{\boldsymbol{k}}$ only come from the indices $(\ell,\boldsymbol{k})$ with $\ell \le L$. By the assumption that $\alpha(1,\boldsymbol{0}) > 0$, there are only finitely many such $(\ell,\boldsymbol{k})$ with $\alpha(\ell,\boldsymbol{k}) > 0$.

Write $f(z,\boldsymbol{x}) = f_0(\boldsymbol{x}) + zf_1(z,\boldsymbol{x})$. It follows from the case $m=1$ of Theorem 4.4 that $\frac{zg'(z)}{g(z)} f_0(\boldsymbol{x})$ satisfies the Gauss congruences. We may therefore replace $f(z,\boldsymbol{x})$ with $f(z,\boldsymbol{x}) - f_0(\boldsymbol{x})$. In other words, we may assume that the sum in (15) is over all $\ell \in \mathbb{Z}$, $\boldsymbol{k} \in \mathbb{Z}^n$ such that $\alpha(\ell,\boldsymbol{k}) > 0$ and $\ell \neq 0$. All subsequent sums are assumed to be of this form. Observe that

$$F(z,\boldsymbol{x}) = \frac{zg'(z)}{g(z)} f(g(z),\boldsymbol{x}) = \sum_{\ell\neq 0,\boldsymbol{k}} \frac{f_{\ell,\boldsymbol{k}}}{\ell} z\frac{\mathrm{d}}{\mathrm{d}z}[g(z)^\ell]\boldsymbol{x}^{\boldsymbol{k}}.$$

We rewrite this as $F = F_1 + F_2$ with

$$F_1(z,\boldsymbol{x}) = \sum_{\ell,\boldsymbol{k}} \frac{f_{\ell,\boldsymbol{k}} - f_{\ell/p,\boldsymbol{k}/p}}{\ell} z\frac{\mathrm{d}}{\mathrm{d}z}[g(z)^\ell]\boldsymbol{x}^{\boldsymbol{k}}$$

and

$$F_2(z,\boldsymbol{x}) = \sum_{\ell,\boldsymbol{k}} \frac{f_{\ell/p,\boldsymbol{k}/p}}{\ell} z\frac{\mathrm{d}}{\mathrm{d}z}[g(z)^\ell]\boldsymbol{x}^{\boldsymbol{k}},$$

where we use the convention that $f_{\ell/p,\boldsymbol{k}/p} = 0$ if ℓ or $\boldsymbol{k}$ is not divisible by p. The second sum equals

$$F_2(z,\boldsymbol{x}) = \sum_{\ell,\boldsymbol{k}} f_{\ell/p,\boldsymbol{k}/p} z\frac{\mathrm{d}}{\mathrm{d}z}\left[\frac{g(z)^\ell - g(z^p)^{\ell/p}}{\ell}\right]\boldsymbol{x}^{\boldsymbol{k}} + F(z^p,\boldsymbol{x}^p).$$

To prove our claim, we need to show that the coefficient of $z^L\boldsymbol{x}^{\boldsymbol{k}}$ in $F(z,\boldsymbol{x}) - F(z^p,\boldsymbol{x}^p)$ is divisible by p^r with $r = \min(\nu_p(L),\nu_p(\boldsymbol{k}))$.

Let $h(z) = (g(z)^\ell - g(z^p)^{\ell/p})/\ell$ for $\ell \in p\mathbb{Z}$. Since $g(z) \in \mathbb{Z}_p[[z]]$, we have $g(z)^p \equiv g(z^p)$, which implies that h has p-adically integer coefficients. Let $h_L \in \mathbb{Z}_p$ be the coefficient of z^L in $h(z)$. Then, the coefficient of z^L in $z\frac{\mathrm{d}}{\mathrm{d}z}h(z)$ is Lh_L, which is divisible by $p^{\nu_p(L)}$.

It therefore only remains to show that the coefficient of $z^L \boldsymbol{x}^{\boldsymbol{k}}$ in $F_1(z, \boldsymbol{x})$ is divisible by p^r with $r = \min(\nu_p(L), \nu_p(\boldsymbol{k}))$. Equivalently, if C_L is the coefficient of z^L in

$$\frac{f_{\ell,\boldsymbol{k}} - f_{\ell/p,\boldsymbol{k}/p}}{\ell} z \frac{\mathrm{d}}{\mathrm{d}z}[g(z)^\ell],$$

then we need to show that $\nu_p(C_L) \geq \min(\nu_p(L), \nu_p(\boldsymbol{k}))$. Observe that the p-adic valuation of the coefficient of z^L in $z\frac{\mathrm{d}}{\mathrm{d}z}g(z)^\ell$ is at least $\max(\nu_p(\ell), \nu_p(L))$. Then, because f satisfies the Gauss congruences for p,

$$\nu_p(C_L) \geq \min(\nu_p(\ell), \nu_p(\boldsymbol{k})) - \nu_p(\ell) + \max(\nu_p(\ell), \nu_p(L)) \geq \min(\nu_p(L), \nu_p(\boldsymbol{k})),$$

which completes the proof. ☐

Corollary 7.2. *Let $g_j \in \mathbb{Q}(x)$ be nonzero. If the rational function $f \in \mathbb{Q}(\boldsymbol{x})$ has the Gauss property, then so does the rational function*

$$\left(\prod_{j=1}^{n} \frac{x_j g_j'(x_j)}{g_j(x_j)}\right) f(g_1(x_1), \ldots, g_n(x_n)).$$

Proof. Clearly, it suffices to show that, if $f \in \mathbb{Q}(z, \boldsymbol{x})$ has the Gauss property, then, for any nonzero $g \in \mathbb{Q}(z)$, the rational function

$$F(z, \boldsymbol{x}) = \frac{zg'(z)}{g(z)} f(g(z), \boldsymbol{x})$$

has the Gauss property.

First, consider the case that $g(0) = 0$. Let $P, Q \in \mathbb{Z}[z, \boldsymbol{x}]$ and suppose that $f = P/Q$ has the Gauss property. Observe that there exists a vertex $\boldsymbol{v}$ of $N(Q)$ and a linear form α with $\alpha(1, 0, \ldots 0) > 0$, such that $\alpha(\boldsymbol{w}) > 0$ for all nonzero $\boldsymbol{w}$ in the proper cone C generated by $N(Q/(z, \boldsymbol{x})^{\boldsymbol{v}})$. It follows from Corollary 3.7 that the Laurent series expansion of f with respect to $\boldsymbol{v}$ is supported on C. Since adding a constant does not affect the Gauss property, we may assume that this series has constant term 0. Hence, the assumptions of Theorem 7.1 are satisfied for all but finitely many primes p. We conclude that $F(z, \boldsymbol{x})$ has the Gauss property.

Next, suppose that $g(z)$ has a pole at $z = 0$. By Proposition 6.1, $F(z, \boldsymbol{x})$ has the Gauss property if and only if $F(1/z, \boldsymbol{x})$ has the Gauss property. Let $h(z) = g(1/z)$, and note that

$$F(1/z, \boldsymbol{x}) = -\frac{zh'(z)}{h(z)} f(h(z), \boldsymbol{x}).$$

Since $h(0) = 0$, it follows from the previous case that $F(1/z, \boldsymbol{x})$ and, hence, $F(z, \boldsymbol{x})$ has the Gauss property.

It therefore remains to consider the case $g(0) = c \in \mathbb{Q}^\times$. In light of the first case, it suffices to consider $g(z) = z + c$. Observe that $g(z) = g_1(g_2(g_1(z)))$ with $g_1(z) = 1/z$ and $g_2(z) = z/(1 + cz)$. Since the result holds for g_1 and g_2, we conclude that it also holds for g. ☐

8 A proof of Minton's result

In this section, we reprove the following result of Minton [Min14].

Theorem 8.1 (Minton, 2014)**.** *Let $f \in \mathbb{Q}(x)$. Then the following are equivalent:*

(a) f has the Gauss property.

(b) The coefficients a_n of the Laurent series expansion $f = \sum a_n x^n$ satisfy

$$a_{np} \equiv a_n \pmod{p}$$

for almost all primes p.

(c) f is $f(0)$ plus a $\mathbb{Q}$-linear combination of functions of the form $xu'(x)/u(x)$, where $u \in \mathbb{Q}[x]$ is irreducible and $u(0) = 1$.

Note that statement (b) concerns only congruences modulo primes. By the theorem, this already implies the Gauss congruences modulo prime powers.

Proof. That (c) implies (a) is a consequence of the case $m = 1$ of Theorem 4.5. Since (a) obviously implies (b), it remains to show that (b) implies (c).

Write $f = P/Q$ with $P, Q \in \mathbb{Z}[x]$. Assume that the congruences (b) hold or, equivalently, that

$$U_p(P/Q) \equiv P/Q \pmod{p}, \tag{16}$$

where U is the operator introduced in (8). It follows as in the proof of Proposition 3.5 (which only relied on the Gauss congruences modulo primes, not prime powers) that $N(P) \subseteq N(Q)$. This implies that P/Q has no pole in $x = 0$ and that $\deg(P) \leq \deg(Q)$. Since adding a constant to f does not affect the result, we may assume that $Q(0) = 1$ and that $\deg(P) < \deg(Q)$. Then, P/Q has a partial fraction expansion of the form

$$\frac{P}{Q} = \sum_{i=1}^{r} \sum_{j=1}^{m_i} \frac{A_{ij}}{(1 - \alpha_i x)^j},$$

where the $\alpha_i \in \bar{\mathbb{Q}}$ are distinct algebraic numbers, $m_i \geq 1$ and $A_{ij} \in \bar{\mathbb{Q}}$. We first show that $m_i = 1$. To that end, note that, for all sufficiently large prime numbers p, we have that, for all i and j, the norms of α_i and A_{ij} are p-adic units, the α_i are distinct modulo p, and $p > m_i$. Let p be a prime number satisfying these conditions. Since $p > m_i$, we then have, for all $j = 1, 2, \ldots, m_i$,

$$\begin{aligned} U_p\left(\frac{1}{(1 - \alpha_i x)^j}\right) &= U_p\left(\sum_{k \geq 0} \binom{k + j - 1}{j - 1} \alpha_i^k x^k\right) \\ &= \sum_{k \geq 0} \binom{pk + j - 1}{j - 1} \alpha_i^{pk} x^k \\ &\equiv \sum_{k \geq 0} \alpha_i^{pk} x^k = \frac{1}{1 - \alpha_i^p x} \pmod{p}. \end{aligned}$$

As a consequence, we see that $U_p(P/Q)$, modulo p, is equal to a rational function with simple poles. From (16) we conclude that P/Q has only simple poles as well.

From now on, we may therefore write $A_i = A_{i1}$ and have

$$\frac{P}{Q} = \sum_{i=1}^{r} \frac{A_i}{1-\alpha_i x}, \quad U_p\left(\frac{P}{Q}\right) \equiv \sum_{i=1}^{r} \frac{A_i}{1-\alpha_i^p x}.$$

Moreover, the kth coefficient of $P/Q = \sum_{k\geq 0} f_k x^k$ is $f_k = \sum_{i=1}^r A_i \alpha_i^k$. Since $f_k \in \mathbb{Q}$ is a p-adic integer, we have

$$f_k \equiv f_k^p \equiv \sum_{i=1}^{r} A_i^p \alpha_i^{pk} \pmod p,$$

which implies that

$$\frac{P}{Q} \equiv \sum_{i=1}^{r} \frac{A_i^p}{1-\alpha_i^p x} \pmod p.$$

Since $P/Q \equiv U_p(P/Q) \pmod p$, we conclude that $A_i^p \equiv A_i \pmod p$, for all $i = 1, 2, \ldots, r$. From Frobenius's density theorem, see, for instance, [Jan73, p. 134], it follows that $A_i \in \mathbb{Q}$ for all i.

Finally, let us group the α_i in Galois orbits under $\mathrm{Gal}(\bar{\mathbb{Q}}/\mathbb{Q})$. Suppose, say, that $\alpha_1, \ldots, \alpha_s$ is such a Galois orbit. Since P/Q is Galois invariant, and the A_i are rational, we must have $A_1 = A_2 = \ldots = A_s$. Hence, we conclude that P/Q is a rational linear combination of functions of the form

$$\sum_{i=1}^{s} \frac{1}{1-\alpha_i x} = s - x\frac{v'(x)}{v(x)},$$

where $v(x) = \prod_{i=1}^s (1-\alpha_i x)$. Moreover, $v \in \mathbb{Q}[x]$ because $\alpha_1, \ldots, \alpha_s$ form a Galois orbit. $\square$

Acknowledgements. The first and third author would like to thank the Max-Planck-Institute for Mathematics in Bonn, where this work was initiated, for providing support and wonderful working conditions.

References

[Apé79] Roger Apéry. Irrationalité de $\zeta(2)$ et $\zeta(3)$. *Astérisque*, 61:11–13, 1979.

[Beu85] Frits Beukers. Some congruences for the Apéry numbers. *Journal of Number Theory*, 21(2):141–155, October 1985.

[Cos88] Matthijs J. Coster. *Supercongruences*. PhD thesis, Universiteit Leiden, 1988.

[Ges14] Ira Gessel. Problem 11757. *American Mathematical Monthly*, 121(2):170, February 2014.

[GKZ94] I. M. Gelfand, M. M. Kapranov, and A. V. Zelevinsky. *Discriminants, Resultants, and Multidimensional Determinants*. Birkhäuser, Boston, MA, 1994.

[Jan73] Gerald J. Janusz. *Algebraic Number Fields*. Academic Press, New York, 1973.

[Min14] Gregory T. Minton. Linear recurrence sequences satisfying congruence conditions. *Proceedings of the American Mathematical Society*, 142(7):2337–2352, April 2014.

[RY15] Eric Rowland and Reem Yassawi. Automatic congruences for diagonals of rational functions. *Journal de Théorie des Nombres de Bordeaux*, 27(1):245–288, 2015.

[Str14] Armin Straub. Multivariate Apéry numbers and supercongruences of rational functions. *Algebra & Number Theory*, 8(8):1985–2008, 2014.

[Zar08] A. V. Zarelua. On congruences for the traces of powers of some matrices. *Proceedings of the Steklov Institute of Mathematics*, 263(1):78–98, December 2008.