DENSITIES OF BOUNDED PRIMES FOR HYPERGEOMETRIC SERIES WITH RATIONAL PARAMETERS

CAMERON FRANC, BRANDON GILL, JASON GOERTZEN, JARROD PAS, AND FRANKIE TU

ABSTRACT. The set of primes where a hypergeomeric series with rational parameters is p-adically bounded is known by [10] to have a Dirichlet density. We establish a formula for this Dirichlet density and conjecture that it is rare for the density to be large. We prove this conjecture for hypergeometric series whose parameters have denominators equal to a prime of the form $p = 2q^r + 1$, where q is an odd prime. The general case remains open. This paper is the output of an undergraduate research course taught by the first listed author in the winter semester of 2018.

CONTENTS

1. INTRODUCTION

The study of the coefficients of hypergeometric series has a long history. A basic question is to determine when a given series ${}_2F_1(a, b; c)$ with rational parameters a, b and c has integer coefficients, or perhaps more naturally, at most finitely many primes appearing in the denominators of its coefficients. This question was settled long ago by Schwarz when he classified in his famous list the series satisfying a hypergeometric differential equation with finite monodromy group. More recently, Beukers-Heckman generalized this result to series ${}_nF_{n-1}$ in [2]. In the intervening time, deep connections have been made between the arithmetic of the coefficients of ${}_nF_{n-1}$, quotient singularities, and the Riemann hypothesis — see [4], [3], [12] for an introduction to this subject.

Dwork intitiated a deep study of the p-adic properties of hypergeometric series (see for example his books [9] and [8]). One question that he addressed was the p-adic boundedness of hypergeometric series. In [6], Christol gave a necessary and sufficient condition for a given hypergeometric series ${}_nF_{n-1}$ to be p-adically bounded. Recently, these studies of the congruence and integrality properties of hypergeometric series have found applications in [7] in the study of integrality properties of hypergeometric mirror maps. Thus, in spite of its long history, the subject of the arithmetic of hypergeometric series remains of interest.

In [10] a new necessary and sufficient condition for the p-adic boundedness of a series ${}_2F_1$ with rational parameters was introduced, and it was used to show that the set of bounded primes for a given series is (with finitely many exceptions) a union of primes

Corresponding author: franc@math.usask.ca. Cameron Franc was partially supported by NSERC Discovery grant RGPIN-2017-06156.

in certain arithmetic progressions. These results have been generalized to ${}_nF_{n-1}$ in Tobias Bernstein's Master's thesis at the University of Alberta. The present paper continues the line of investigation opened in [10] toward a more global understanding of the arithmetic of hypergeometric series. Our first main result is Theorem 4, which reformulates the p-adic necessary and sufficient condition for boundedness from [10] into a global condition that more closely resembles the classification of hypergeometric equations with finite monodromy from [2] (and which goes back to work of Landau [11] in the case of ${}_2F_1$). Theorem 4 states that for all but finitely many primes, ${}_2F_1(a,b;c)$ is p-adically bounded if and only if p is congruent to an element of

$$B(a,b;c) = \{u \in (\mathbf{Z}/m\mathbf{Z})^\times \mid \text{ for all } j \in \mathbf{Z},\ \{-u^j c\} \leq \max(\{-u^j a\}, \{-u^j b\})\}$$

where m is the least common multiple of the denominators of a, b and c.

In Section 3 we turn to the question of how the density of bounded primes behaves on average. The expectation is that it should be rare for this density to be large. For example, the Schwarz list is quite sparse among all hypergeometric series, and it is the list of series such that the density of bounded primes is equal to one. At the other end of the spectrum, [10] showed that ${}_2F_1(a,b;c)$ has a zero density of bounded primes one-third of the time. More precisely, if a, b and c are normalized to lie in the interval $(0,1)$, then the density is zero precisely when c is smaller than a and b. Conjecture 6 is a precise formulation of the expectation that the density of bounded primes should usually be small, and we end Section 3 with computational evidence tabulating densities of hypergeometric series with parameters of height at most 64.

The final Section 4 provides evidence that Conjecture 6 is true in the form of an upper bound on the densities of bounded primes of certain hypergeometric series with restricted parameters. Theorem 17 proves the following: if p is a large prime of the form $p = 2q^r + 1$, where q is another odd prime and $r \geq 1$, then the density D of bounded primes for a series

$${}_2F_1\left(\frac{x}{p}, \frac{y}{p}; \frac{z}{p}\right)$$

satisfies

$$D \leq \frac{1}{q}.$$

In particular, the density of bounded primes goes to zero if q grows.

Computations suggest that $D \leq 1/q$ whenever $p \geq 59$, although we do not prove this slightly stronger result unless $p \equiv 3 \pmod 8$. Our proof of Theorem 17 relies crucially on previously known bounds on the smallest positive nonquadratic residue mod p. Effective versions of our results would follow from effective versions of such upper bounds, but we do not pursue this in the present paper.

Acknowledgements. This paper is the output of an undergraduate research course taught by Cameron Franc at the University of Saskatchewan in the winter semester of 2018. The other authors of the paper are the undergraduate students that took the course. We thank Chris Soteros and Jacek Szmigielski for helping us create this course.

2. A FORMULA FOR THE DENSITY OF BOUNDED PRIMES

Recall that hypergeometric series ${}_2F_1$ are defined as power series

$${}_2F_1(a,b;c) = \sum_{n \geq 0} \frac{(a)_n (b)_n}{(c)_n} \frac{X^n}{n!}$$

where $(a)_n = a(a+1)\cdots(a+n-1)$ is the rising factorial. When the hypergeometric parameters $(a, b; c)$ are rational, then ${}_2F_1(a, b; c)$ has rational coefficients that have been the subject of considerable investigation.

Definition 1. If p is a prime and if $F = \sum_{n\geq 0} a_n X^n$ is a power series with $a_n \in \mathbf{Q}$, then F is said to be *p-adically bounded* provided that its coefficients a_n are bounded in the p-adic topology. Equivalently, the power of p dividing the denominator of any coefficient a_n is bounded from above independently of n. A prime p is said to be *bounded* for F if F is p-adically bounded.

In [10] it was shown that the set of bounded primes for a given ${}_2F_1(a, b; c)$ with rational parameters always has a Dirichlet density. Our first goal is to describe a formula for the density of bounded primes for a given hypergeometric series with rational parameters. This is achieved in Theorem 4 below. As in [10], there is little harm in assuming that the parameters a, b and c satisfy $0 < a, b, c < 1$ and $c \neq a, b$, and so we do so throughout the paper. Recall that thanks to our normalization, if p is a prime such that $a - 1$ is a p-adic unit, then $a - 1$ has a perfectly periodic p-adic expansion of period M equal to the order of p in $(\mathbf{Z}/d\mathbf{Z})^\times$, where d is the denominator of $a - 1$ (Lemma 2.1 of [10]). Let $a_j(p)$ denote the jth p-adic digit of $a-1$, and define $b_j(p)$ and $c_j(p)$ similarly. Lemma 2.3 of [10] showed that

$$a_j(p) = \left\lfloor \left\{-p^{M-1-j}a\right\} p \right\rfloor. \tag{1}$$

where $\lfloor x \rfloor$ denotes the floor function and $\{x\} = x - \lfloor x \rfloor$. In particular,

$$\lim_{p\equiv u \pmod d} \frac{a_j(p)}{p} = \{-u^{d-1-j}a\} \tag{2}$$

where the limit varies over primes p within a fixed congruence class $u \pmod d$. Similar formulas hold for the digits of $b - 1$ and $c - 1$.

Example 2. Below we plot the p-adic digits of $-3/11$ for primes p satisfying $p \equiv 2 \pmod{11}$, which corresponds to $a = 8/11$ above. Since the order of 2 in $(\mathbf{Z}/11\mathbf{Z})^\times$ is 5, the digits are periodic of period 5. In the last column we print the digits divided by p as real numbers, up to four decimal places of accuracy, to demonstrate the convergence in Equation (2). In the last row we print the limit of the normalized digits.

$p \equiv 2 \pmod{11}$	Digits of $-3/11$	Normalized digits
13	$(8, 10, 11, 5, 9)$	$(0.6154, 0.7692, 0.8462, 0.3846, 0.6923)$
79	$(50, 64, 71, 35, 57)$	$(0.6329, 0.8101, 0.8987, 0.4430, 0.7215)$
101	$(64, 82, 91, 45, 73)$	$(0.6337, 0.8119, 0.9010, 0.4455, 0.7228)$
167	$(106, 136, 151, 75, 121)$	$(0.6347, 0.8144, 0.9042, 0.4491, 0.7245)$
211	$(134, 172, 191, 95, 153)$	$(0.6351, 0.8152, 0.9052, 0.4502, 0.7251)$
233	$(148, 190, 211, 105, 169)$	$(0.6352, 0.8155, 0.9056, 0.4506, 0.7253)$
277	$(176, 226, 251, 125, 201)$	$(0.6354, 0.8159, 0.9061, 0.4513, 0.7256)$
409	$(260, 334, 371, 185, 297)$	$(0.6357, 0.8166, 0.9071, 0.4523, 0.7262)$
$p \to \infty$		$(7/11, 9/11, 10/11, 5/11, 8/11)$

Recall the following result from [10]:

Theorem 3. *Let a, b and c denote rational numbers satisfying $0 < a, b, c < 1$ and $c \neq a, b$. Let p be a prime greater than the least common multiple of the denominators of $a - 1$, $b - 1$ and $c - 1$. Then the hypergeometric series ${}_2F_1(a, b; c; z)$ has p-adically bounded coefficients if and only if for every index j we have*

$$c_j(p) \leq \max(a_j(p), b_j(p)).$$

Proof. See Theorem 3.4 of [10]. □

Note that since the p-adic expansions of $a - 1$, $b - 1$ and $c - 1$ are all periodic, the condition in Theorem 3 only needs to be checked for a finite number of indices j.

Theorem 4. *Let a, b and c denote three rational numbers satisfying $0 < a, b, c < 1$ and $c \neq a, b$. Let m denote the least common multiple of the denominators of $a - 1$, $b - 1$ and $c - 1$ when written in lowest terms, and define*

$$B(a, b; c) = \{u \in (\mathbf{Z}/m\mathbf{Z})^\times \mid \textit{for all } j \in \mathbf{Z},\ \{-u^j c\} \leq \max(\{-u^j a\}, \{-u^j b\})\}.$$

Then for all primes $p > m$, the series ${}_2F_1(a, b; c; z)$ is p-adically bounded if and only if p is congruent to an element of $B(a, b; c)$ mod m. Thus, the density of the set of bounded primes for ${}_2F_1(a, b; c; z)$ is

$$D(a, b; c) = \frac{|B(a, b; c)|}{\phi(m)}.$$

Proof. Morally, this follows immediately from Theorem 3 by applying the limit formula of Equation (2). However, we want to ensure that Theorem 4 is true exactly for the primes p satisfying $p > m$, so a little more work is necessary.

Fix an index j. We can write $\{-p^j c\} = C/m$, $\{-p^j a\} = A/m$ and $\{-p^j b\} = B/m$ for integers A, B, C strictly betwen 0 and m, where $C \neq A, B$. By Equation (1), we must show that when $p > m$, then

$$\lfloor Cp/m \rfloor \leq \max\left(\lfloor Ap/m \rfloor, \lfloor Bp/m \rfloor\right)$$

if and only if

$$C/m \leq \max(A/m, B/m).$$

That the latter implies the former is obvious (multiply by p and take the floor). Conversely, suppose without loss of generality that $A/m \geq B/m$ and $\lfloor Cp/m \rfloor \leq \lfloor Ap/m \rfloor$. If $\lfloor Cp/m \rfloor < \lfloor Ap/m \rfloor$ then obviously $C/m < A/m$ and we're done. Hence assume that $\lfloor Cp/m \rfloor = \lfloor Ap/m \rfloor = N$, so that

$$\frac{Nm}{p} \leq A, C < \frac{Nm}{p} + \frac{m}{p}.$$

Since $p > m$ and A and C are integers, it follows from this that $A = C$, a contradiction. □

Theorem 4 has several useful consequences. For example, observe that $B(a, b; c)$ is a union of cyclic subgroups of $(\mathbf{Z}/m\mathbf{Z})^\times$. In particular, $B(a, b; c) = \emptyset$ if and only if $1 \notin B(a, b; c)$. From this one deduces that $D(a, b; c) = 0$ if and only if $c < a$ and $c < b$. This characterization of when the density of bounded primes satisfies $D(a, b; c) = 0$ was first established in Theorem 4.14 of [10] without the use of Theorem 4 above.

3. A CONJECTURE ON THE DENSITIES OF BOUNDED PRIMES

In this section we consider the general behaviour of the density $D(a,b;c)$ of bounded primes for a hypergeometric series. The expectation is that it should be rare for this density to be large. For example, in [10] it was shown that $D(a,b;c)=1$ if and only if the corresponding monodromy representation is finite[1]. In order to study this question we introduce a notion of complexity for the parameters of a hypergeomteric series. Recall that if $a \in \mathbf{Q}$, then the *height* $h(a)$ of a is the maximum size of the numerator or denominator of $|a|$ when $|a|$ is written in lowest terms.

Definition 5. The *parameter height* of a hypergeometric series ${}_2F_1(a,b;c)$ is the quantity

$$h(a,b;c) := \max\{h(a),h(b),h(c)\}.$$

The parameter height of ${}_2F_1(a,b;c)$ has nothing to do with the usual height of the rational coefficients of ${}_2F_1(a,b;c)$. Since we're normalizing our parameters to lie in the interval $(0,1)$, the parameter height is determined by the denominators of the parameters a, b and c.

Note that if a, b and c are any rational numbers such that a, b, c, $a-c$ and $b-c$ are not integers, then

$$D(a,b;c) = D(\{a\},\{b\};\{c\}),$$

although a finite number of bounded primes for one of the sets of parameters above could be unbounded for the other (see [10]). We thus let P denote the parameter set of hypergeometric triples $(a,b;c)$ where $a,b,c \in (0,1)\cap\mathbf{Q}$ and $c \neq a,b$.

For $r \in [0,1]$ define

$$\beta(r,N) = \frac{|\{(a,b;c)\in P \mid h(a,b;c)\le N \text{ and } D(a,b;c)\le r\}|}{|\{(a,b;c)\in X \mid h(a,b;c)\le N\}|}.$$

Then $\beta(r,N)$ measures what proportion of hypergeometric series have a density of bounded primes that is at most r. For example, [10] showed that, under our hypotheses on a, b and c, one has $D(a,b;c)=0$ exactly when c is the smallest parameter. Since $h(a,b;c)$ is invariant under permuting a, b and c, it follows that

$$\beta(0,N) = \frac{1}{3}.$$

Computations suggest that if $\varepsilon > 0$, then for large enough N, the proportion $\beta(\varepsilon,N)$ of hypergeometric series with a density of bounded primes that is at most ε should be quite large. In fact, the following conjecture is supported by computational evidence:

Conjecture 6. *For all $\varepsilon > 0$,*

$$\lim_{N\to\infty} \beta(\varepsilon,N) = 1.$$

We have performed extensive computations of densities of bounded primes for all hypergeometric series with parameters normalized as above, and satisfying $h(a,b;c)\le 64$. First we plot the frequency of each density count up to height 16 in Figure 1. Observe that the frequency of density zero in Figure 1 accounts for one-third of the data, and it dominates the figure. Thus, in Figure 2 we include similar plots up to heights 16, 32, 48 and 64, but we omit the data for density zero.

These plots contain spikes at certain densities, such as those of the form $1/2^n$, but the trend appears to be that the densities concentrate towards zero as the height grows. This is consistent with Conjecture 6. In the next section we prove Theorem 17 which bounds

[1]That finite monodromy implies $D(a,b;c)=1$ is a result that goes back to Eisenstein

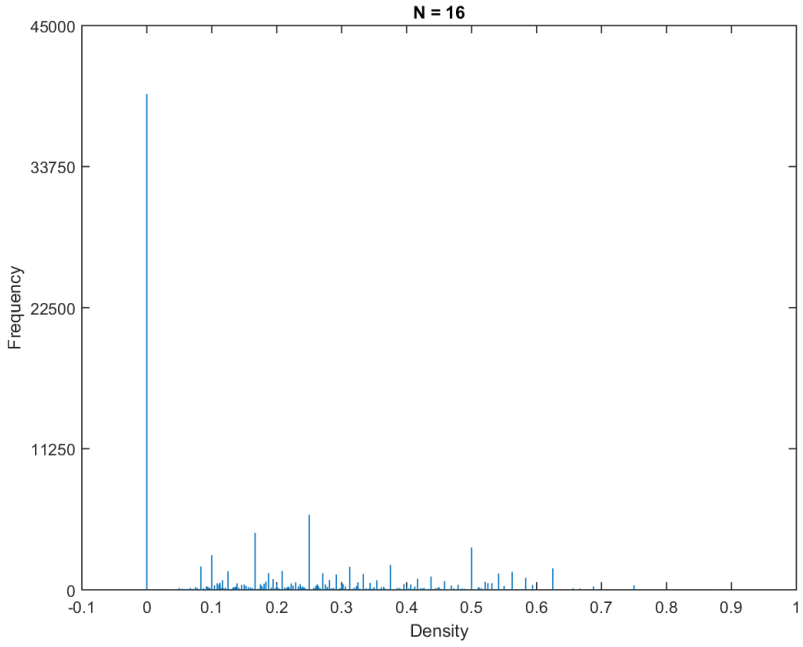

FIGURE 1. Densities of bounded primes for hypergeometric series up to parameter height 16.

certain densities of bounded primes from above, and which provides more evidence that supports the truth of Conjecture 6.

Remark 7. The classical Schwarz list classifies those hypergeometric parameters for which $D(a,b;c) = 1$. Given $\delta > 0$, one might similarly try to classify all those parameters such that $D(a,b;c) \geq \delta$ in some kind of δ-Schwarz list. If Conjecture 6 is true, then such a classification might not be unreasonable for certain values of δ, such as $\delta = 1/2^n$.

4. AN UPPER BOUND FOR DENSITIES OF BOUNDED PRIMES

Let m denote the least common multiple of the denominators of rational hypergeometric parameters a, b and c, and assume that U_m is cyclic. Let $u \in U_m$ be a generator. Then for every divisor $d \mid \phi(m)$, the element $u_d = u^{(p-1)/d}$ has order d. The possibilities for $B(a,b;c)$ are the sets generated by the various u_d:

$$\langle u_d \rangle = \{u_d, u_d^2, \ldots, u_d^d\}.$$

If x is a positive integer then let $d(x)$ denote the set of positive divisors of x. Let $I_x = \{J \subseteq d(x) \mid d \nmid e \text{ for all } d, e \in J\}$. Then the possibilities for $B = B(a,b;c)$ are the sets

$$B_J = \bigcup_{d \in J} \langle u_d \rangle$$

for all $J \in I_{\phi(m)}$. Note that the unions are definitely not disjoint. By the inclusion-exclusion principle,

$$|B_J| = \sum_{\substack{K \subseteq J \\ K \neq \emptyset}} (-1)^{|K|-1} \gcd(K)$$

where $\gcd(K)$ denotes the greatest common divisor of the elements of K.

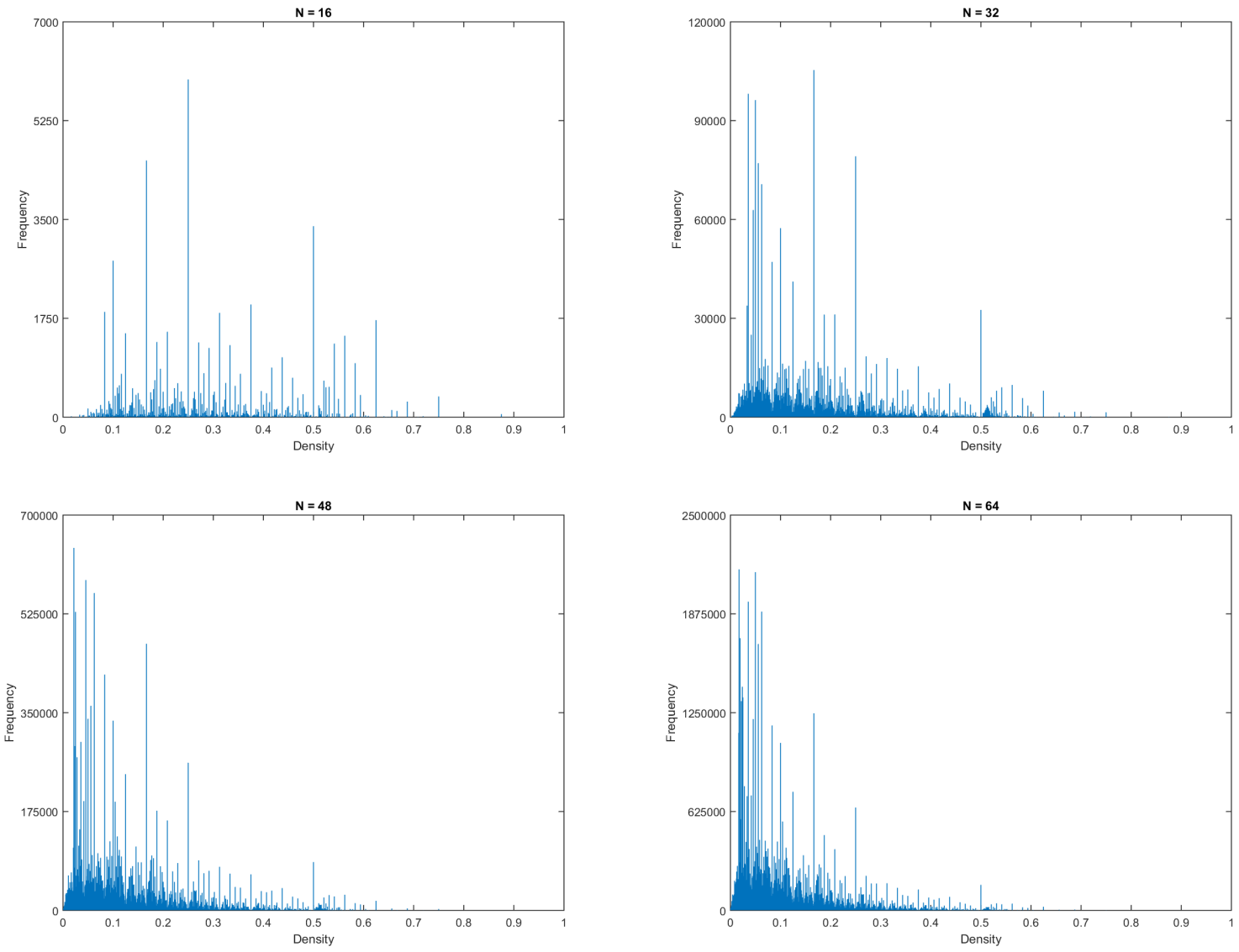

FIGURE 2. All densities of bounded primes up to parameter height $N = 16$, 32, 48 and 64, with the zero density counts removed.

We will work with a choice of m so that the subgroup structure of U_m is very simple: let m be a prime of the form $p = 2q^r + 1$ where q is also an odd prime, and $r \geq 1$. Note that then $p \equiv 3 \pmod 4$ and $p > 3$. If u is a generator for U_p then the discussion above specializes to the following possibilities for the subsets $B(a, b; c)$ and the corresponding densities of bounded primes:

$B(a,b;c)$	Density
$\emptyset$	0
$\langle u^{q^j} \rangle$	$1/(2q^j)$
$\langle -u^{q^k} \rangle$	$1/q^k$
$\langle u^{q^j} \rangle \cup \langle -u^{q^k} \rangle$ $(j < k)$	$(q^{k-j}+1)/(2q^k)$

Note that most of these densities are quite small. In Theorem 17 below we will show that if p is very large, then the large densities never occur.

For the moment let $p > 3$ be any odd prime such that $p \equiv 3 \pmod 4$, so that -1 is not a quadratic residue mod p. Let Q denote the set of quadratic residues in $(\mathbf{Z}/p\mathbf{Z})^\times$. Let h_p denote the class number of $\mathbf{Q}(\sqrt{-p})$. Since $p \equiv 3 \pmod 4$ and $p > 3$, Dirichlet's analytic class number formula implies that

$$-ph_p = \sum_{0<y<p} \chi(y)y \tag{3}$$

where $\chi(y) = \left(\frac{y}{p}\right)$ is the Legendre symbol.

If x is an integer or an element of $\mathbf{Z}/p\mathbf{Z}$, then let $[x]_p$ denote the unique integer congruent to x mod p such that $0 \le [x]_p < p$. Define

$$U_p(x) = \{y \in (\mathbf{Z}/p\mathbf{Z})^\times \mid [xy]_p < [y]_p\},$$
$$W_p(x) = U_p(x) \cap Q,$$

and let $w_p(x) = |W_p(x)|$.

Below we will see that the proof of Theorem 17, which gives an upper bound on the densities of bounded primes considered here, follows from the fact that the intersection $W_p(a/c) \cap W_p(b/c)$ is nonempty whenever p is large enough. In Proposition 9 below we show that the sets $W_p(x)$ are relatively large and often must intersect for trivial reasons. However, this simple proof does not work in all cases, and so more work is required. Proposition 14 establishes what we need on the nonemptiness of these intersections, but it will require a sequence of preliminary results.

Lemma 8. *Let p be an odd prime. If $x \not\equiv 0, 1 \pmod p$, the sets $U_p(x)$ satisfy the following:*

1. *$U_p(1)$ is empty;*
2. *$U_p(x)$ contains one element of each pair $\{y, -y\}$ and thus $|U_p(x)| = \frac{p-1}{2}$;*
3. *$U_p(x) = U_p(1-x)$;*
4. *$(x-1)U_p(x) = U_p(x/(x-1))$.*

Finally, if $1 \le x \le p-2$ then the set $U_p(-x)$ breaks up into disjoint intervals as follows:

$$U_p(-x) = \bigcup_{a=1}^{x} \left\{ \frac{ap}{x+1} < y < \frac{ap}{x} \right\}.$$

Proof. Part (1) is clear, and (2) follows since $[-y]_p = p - [y]_p$.

For (3) observe that $[xy]_p < [y]_p$ implies that we can write $xy = ap + r$ for $0 \le r < y < p$. But then $(1-x)y = -ap + (y - r)$ shows that $[(1-x)y] = y - r < [y]$. Hence $U(x) \subseteq U(1-x)$, and the reverse inclusion follows by replacing x with $1 - x$.

For part (4), define

$$V_p(x) = \{y \in (\mathbf{Z}/p\mathbf{Z})^\times \mid [y]_p < [xy]_p\}.$$

Observe that as above, $V_p(x) = V_p(1-x)$ for $x \not\equiv 0, 1 \pmod p$. Since $xU_p(x) = V_p(x^{-1})$ we find that

$$xU_p(x) = V_p(x^{-1}) = V_p(1 - x^{-1}) = V_p((x-1)/x) = (x/(x-1))U_p(x/(x-1)).$$

This establishes (4).

Finally, for the last statement, observe that if $\frac{ap}{x+1} < y < \frac{ap}{x}$, this is equivalent with $0 < ap - xy < y$. It follows that $[-xy]_P < y = [y]_p$, and hence $y \in U_p(-x)$.

Conversely, if $[-xy]_p < [y]_p$ we may write $ap - xy = [-xy]_p$. We are free to assume $0 \le y < p$, so that $[y]_p = y$ and $a > 0$. Similarly $ap - xy < y$ so that $ap < (x+1)y < (x+1)p$. Hence $1 \le a \le x + 1$ and we find that $\frac{ap}{x+1} < y < \frac{ap}{x}$. This implies that $U_p(-x)$ is as described. □

The following Proposition is not strictly necessary for the proof of Theorem 17, but we include it out of interest. It demonstrates that the while the sets $W_p(u)$ and $W_p(v)$ sometimes must intersect for trivial reasons (say if u, $1-u$, v and $1-v$ are all quadratic residues), such a simple-minded argument does not work in all cases.

Proposition 9. *Let p be a prime satisfying $p > 3$ and $p \equiv 3 \pmod 4$, and write $p = 2n+1$. Let $\chi(x) = \left(\frac{x}{p}\right)$ denote the Legendre symbol. If $x \not\equiv 0, 1 \pmod p$ then*

$$w_p(x) = \frac{1}{2}\left(n + (\chi(x) + \chi(1-x) - 1)h_p\right) = \begin{cases} \frac{n+h_p}{2} & \chi(x) = \chi(1-x) = 1, \\ \frac{n-h_p}{2} & \chi(x) \neq \chi(1-x), \\ \frac{n-3h_p}{2} & \chi(x) = \chi(1-x) = -1. \end{cases}$$

Proof. Begin by writing

$$w(x) = \sum_{y \in W_p(x)} 1 = \frac{1}{2} \sum_{y \in U_p(x)} (1 + \chi(y)) = \frac{n}{2} + \frac{1}{2} \sum_{y \in U_p(x)} \chi(y).$$

Therefore we define $u(x) = \sum_{y \in U_p(x)} \chi(y)$. We must show that

$$u(x) = (\chi(x) + \chi(1-x) - 1)h_p.$$

Since $U_p(x)$ contains one of each pair $\{y, -y\}$ of elements,

$$\sum_{0<y<p} \chi(y)y = \sum_{y \in U_p(x)} (\chi(y)y + \chi(-y)(p-y)) = 2 \sum_{y \in U_p(x)} \chi(y)y - pu(x).$$

By part (4) of Lemma 8, we know that $(x-1)U_p(x) = U_p(x/(x-1))$. Therefore,

$$\begin{aligned} \sum_{0<y<p} \chi(y)y &= \sum_{y \in U_p(x/(x-1))} (\chi(y)y + \chi(-y)(p-y)) \\ &= \sum_{y \in (x-1)U_p(x)} (\chi(y)y + \chi(-y)(p-y)) \\ &= \sum_{w \in U_p(x)} (\chi((x-1)w)[(x-1)w]_p + \chi(-(x-1)w)[-(x-1)w])_p \\ &= \chi(x-1) \sum_{w \in U_p(x)} \chi(w)([(x-1)w]_p - [-(x-1)w]_p) \end{aligned}$$

Note that $[-(x-1)w]_p = p - [(x-1)w]_p$. Hence,

$$\sum_{0<y<p} \chi(y)y = 2\chi(x-1) \sum_{y \in U_p(x)} \chi(w)[(x-1)w]_p - p\chi(x-1)u(x).$$

Using that $U_p(x) = U_p(1-x)$ by Lemma 8, we can replace x by $1-x$ above to deduce that

$$\sum_{0<y<p} \chi(y)y = 2\chi(-x) \sum_{y \in U_p(x)} \chi(w)[-xw]_p - p\chi(-x)u(x).$$

If we now apply Dirichlet's analytic class number formula (3) to these three identities, we've shown that

$$-ph_p = -pu(x) + 2\sum_{w\in U_p(x)} \chi(w)w$$
$$\chi(1-x)ph_p = -pu(x) + 2\sum_{w\in U_p(x)} \chi(w)[(x-1)w]_p$$
$$\chi(x)ph_p = -pu(x) + 2\sum_{w\in U_p(x)} \chi(w)[-xw]$$

Therefore,

$$(\chi(x)+\chi(1-x)-1)ph_p = -3pu(x) + 2\sum_{w\in U_p(x)} \chi(w)(w+[(x-1)w]_p+[-xw]_p)$$

Hence what we're trying to prove is equivalent to showing that

$$u(x) = \frac{1}{2p}\sum_{w\in U_(x)} \chi(w)(w+[(x-1)w]_p+[-xw]_p)$$

Observe that

$$w+[(x-1)w]_p+[-xw]_p = 2p+w-[(1-x)w]_p-[xw]_p.$$

Since $w\in U_p(x)$, we have $[xw]_p < [w]_p = w$. Write $xw = ap+r$ where $0\le r<w$. Then $(1-x)w = w-ap-r = -ap+(w-r)$ shows that $[(1-x)w]_p = w-r$. Therefore

$$\frac{1}{2p}\sum_{w\in U(x)} \chi(w)(w+[(x-1)w]_p+[-xw]_p) = \frac{1}{2p}\sum_{w\in U(x)} \chi(w)(2p) = u(x),$$

as desired. □

Remark 10. Part (5) of Lemma 8 shows that Proposition 9 is equivalent to the following formula: if $1\le x\le p-2$ and p is a prime satisfying $p\equiv 3 \pmod 4$, then

$$\sum_{a=1}^{x}\sum_{\frac{ap}{x+1}<y<\frac{ap}{x}} \left(\frac{y}{p}\right) = (\chi(x+1)-\chi(x)-1)h_p.$$

There is a long history concerning formulas for sums of Legendre symbols over restricted intervals in terms of class numbers (see for example the paper [1] or the more recent text [13]), although we were not able to find this particular result in the literature.

Let p denote an odd prime, and let $n_p > 1$ denote the smallest integer that is not a quadratic residue mod p. The Riemann hypothesis for Dirichlet L-series implies that

$$n_p < \frac{3}{2}(\log p)^2.$$

The following weaker but unconditional result is the best known bound to date.

Theorem 11. *For all odd primes p one has*

$$n_p = O_\varepsilon(p^{\frac{1}{4\sqrt{e}}+\varepsilon}).$$

Proof. See [5]. □

Lemma 12. *Let p be an odd prime. The following statements hold.*

(1) *If $y\in U_p(x)$ and $0<y<p$, then $yj\in U_p(x)$ for all j in the range $1\le j\le \lfloor p/y\rfloor$.*

(2) *Let* $0 < r < p$ *and* $n = p - r$*, and suppose* $r \notin U_p(x)$*. If* $N = \lfloor p/n \rfloor$*, and if*

$$Y = \{nj \mid 1 \leq j \leq N\},$$

then $Y \subseteq U_p(x)$*.*

Proof. For the first claim, since $y \in U_p(x)$, we can write $xy = ap + r$ for $0 \leq r < y < p$. Hence $x(yj) = ajp + rj$ where $0 \leq rj < yj < p$. Then

$$[x(yj)]_p = rj < yj = [yj]_p$$

shows that $yj \in U_p(x)$.

For the second claim observe that if $r \notin U_p(x)$ then $n \in U_p(x)$ by part (2) of Lemma 8. Thus (2) follows from (1). □

Example 13. If $p \equiv 3 \pmod 8$ then $n_p = 2$ is the smallest positive nonquadratic residue mod p and $r_p = p - 2$ is the largest quadratic residue between 0 and p. It's not hard to show that $r_p \notin U_p(x)$ if and only if $x \equiv (p+1)/2 \pmod p$. In this case Lemma 12 gives a complete description of $U_p((p+1)/2)$ as

$$U_p((p+1)/2) = \{2j \mid 1 \leq j \leq (p-1)/2\}.$$

Hence $W_p((p+1)/2)$ is the set of quadratic residues y whose least positive residue $[y]_p$ is even. By Proposition 9, there are $\frac{1}{2}(\frac{p-1}{2} - 3h_p)$ such quadratic residues. This classical result is well-known.

More generally, Theorem 11 and Lemma 12 together imply that if $p \equiv 3 \pmod 4$ and $U_p(x)$ does not contain the largest quadratic residue r_p in the range $0 < r_p < p$, then there is a large subset Y of $U_p(x)$ that we understand well. We will use this subset Y to prove that the various sets $W_p(x)$ must intersect if p is large enough.

Proposition 14. *Let* $p \equiv 3 \pmod 4$ *be prime. Then there exists an integer* N *such that if* $p > N$*, then for all* u, v *coprime to* p *and satisfying* $u \not\equiv 1 \pmod p$*,* $v \not\equiv 1 \pmod p$*, we have*

$$W_p(u) \cap W_p(v) \neq \emptyset.$$

Proof. Let n_p denote the smallest positive nonquadratic residue, and let $r_p = p - n_p$ denote the largest quadratic residue in the range $0 < r_p < p$. There is nothing to prove if $r_p \in W_p(u) \cap W_p(v)$. Suppose instead that $r_p \notin W_p(u)$ and $r_p \notin W_p(v)$. In this case Lemma 12 yields that

$$\{n_p j \mid 1 \leq j \leq \lfloor p/n_p \rfloor\} \subseteq U_p(u) \cap U_p(v).$$

Hence, we must show that the interval $1 \leq j \leq \lfloor p/n_p \rfloor$ contains n_p. This follows by Theorem 11 for large enough primes p, although weaker bounds would work for this case.

Finally suppose that $r_p \in W_p(u)$ but $r_p \notin W_p(v)$. Since $r_p = p - n_p$ satisfies $r_p \notin U_p(v)$, Lemma 12 tells us that with $N = \lfloor p/n_p \rfloor$, we have the containment

$$\{n_p j \mid 1 \leq j \leq N\} \subseteq U_p(v).$$

If $U_p(u)$ contains a nonquadratic residue j in the range $1 \leq j \leq N$, then it also contains the quadratic residue $n_p j$ by Lemma 12. Then $n_p j \in W_p(u) \cap W_p(v)$. So we may assume that $U_p(u)$ does not contain any nonquadratic residue in the range $1 \leq j \leq N$. Equivalently, by part (2) of Lemma 8, $U_p(u)$ contains every quadratic residue in the range $p - N \leq y \leq p - 1$.

Suppose that $n_p j \geq p - N$ for some $1 \leq j \leq N$. This means that

$$\frac{n_p - 1}{n_p^2} p < j < \frac{p}{n_p}. \tag{4}$$

Observe that $W_p(u) \cap W_p(v)$ contains all the elements $n_p j$ for nonquadratic residues j satisfying the inequality (4). If there are no nonquadratic residues j in this range, then the Polya-Vinogradov inequality

$$\left| \sum_{a=b}^{N} \left(\frac{a}{p} \right) \right| < \sqrt{p} \log(p)$$

with $b = \lceil (n_p - 1)p/n_p^2 \rceil$ gives

$$(p/n_p^2) - 1 < \sqrt{p} \log p.$$

But then Theorem 11 implies that

$$p^{1 - \frac{1}{2\sqrt{e}} - 2\varepsilon} = O_\varepsilon(\sqrt{p} \log(p)).$$

This is a contradiction for small enough ε, since $\frac{1}{2} - \frac{1}{2\sqrt{e}} > 0$. Therefore, for large enough primes, there is a nonquadratic residue j in the range (4), and then $n_p j \in W_p(u) \cap W_p(v)$. This concludes the proof. □

If $p \equiv 3 \pmod 8$ then we can use the fact that 2 is the smallest positive nonquadratic residue mod p to get an effective version of Proposition 14.

Proposition 15. *Let $p \equiv 3 \pmod 8$ be prime. If $p > 11$, then for all u, v coprime to p and satisfying $u \not\equiv 1 \pmod p$, $v \not\equiv 1 \pmod p$, we have*

$$W_p(u) \cap W_p(v) \neq \emptyset.$$

Proof. In this case $n_p = 2$ and $r_p = p - 2$. Again, there is nothing to show if $r_p \in W_p(u) \cap W_p(v)$. Suppose that $r_p \notin W_p(u)$ and $r_p \notin W_p(v)$. As in the proof of Proposition 14, we must prove that the interval $1 \leq j \leq \lfloor p/2 \rfloor$ contains n_p. This is obvious if $p > 3$.

Finally assume that $r_p \in W_p(u)$ but $r_p \notin W_p(v)$. Set $p = 2q + 1$, so that by Example 13,

$$W_p(q+1) = \{2, 4, \ldots, p-1\} \cap Q.$$

We must show that every set $W_p(u)$ contains a quadratic residue y such that $[y]_p$ is an even integer.

If $U_p(u)$ contains a nonquadratic residue in the range $0 < y < p/4$ then by part (1) of Lemma 12, $U_p(u)$ also contains the quadratic residue $2y = [2y]_p$, and hence $2y \in W_p(u)$ is an even element. Similarly, if $U_p(u)$ contains a quadratic residue in this range, then it also contains $4y = [4y]_p$ and $W_p(u)$ contains the even element $4y$. Therefore we can assume that $U_p(u)$ does not contain any element in the range $0 < y < p/4$. This means that $U_p(u)$ contains every element in the range $3p/4 < y < p$, by part (2) of Lemma 8.

Conisder the elements $3p/8 < y < p/2$. If there is a nonquadratic residue in this range then $3p/4 < 2y < p$ and $2y$ is an even quadratic residue, and it will thus be contained in $W_p(u)$. So we are reduced to proving that if p is large enough, then there is always a nonquadratic residue in the range $3p/8 < y < p/2$. If we write $p = 8k + 3$ then $\lceil 3p/8 \rceil = 3k + 1$ and $\lfloor p/2 \rfloor = 4k$, and if no nonquadratic residue is in this range, then the Polya-Vinogradov inequality gives

$$k = \left| \sum_{a=3k+1}^{4k} \left(\frac{a}{p} \right) \right| < \sqrt{p} \log p.$$

That is, we obtain $\frac{p-3}{8} < \sqrt{p} \log p$, which is a contradiction if $p > 568$. The remaining cases for primes $p > 11$ can be checked easily on a computer. □

Example 16. The bound of $p > 11$ in Proposition 15 cannot be improved. For example,

$$W_{11}(2) = \{9\}, \qquad W_{11}(6) = \{4\},$$

and $W_{11}(2) \cap W_{11}(6) = \emptyset$.

Theorem 17. *There exists a number N such that the following holds: for all primes $p > N$ of the form $p = 2q^r + 1$, with q an odd prime and $r \geq 1$, and for all rational parameters x/p, y/p and z/p where $1 \leq x, y, z \leq p-1$ and $x \neq z$, $y \neq z$, the density of bounded primes for*

$${}_2F_1\left(\frac{x}{p}, \frac{y}{p}; \frac{z}{p}\right)$$

is bounded above as follows:

$$D\left(\frac{x}{p}, \frac{y}{p}; \frac{z}{p}\right) \leq \frac{1}{q}.$$

In particular, if q grows, then the density of bounded primes goes to zero.

Proof. Observe that if $p = 2q^r + 1$ is prime for an odd prime q, then $p \equiv 3 \pmod 4$ and so -1 is not a quadratic residue mod p. Let $u \in (\mathbf{Z}/p\mathbf{Z})^\times$ have order q^r, so that u generates the group Q of quadratic residues mod p. Let $B = B(x/p, y/p; z/p)$ denote the set of congruence classes mod p representing bounded primes for our parameters, as in Theorem 4. Since B is a union of cyclic subgroups, there are a limited number of possibilities for the form it can take, and for the corresponding densities of bounded primes. The cyclic subgroups of $(\mathbf{Z}/p\mathbf{Z})^\times$ have the form $\langle u^{q^j}\rangle$ for $0 \leq j \leq r$ or $\langle -u^{q^j}\rangle$ for $0 \leq j \leq r$. Besides the obvious containments, we have $\langle u^{q^j}\rangle \subseteq \langle -u^{q^k}\rangle$ if and only if $k \leq j$. If $j < k$ then $\langle u^{q^j}\rangle \cap \langle -u^{q^k}\rangle = \langle u^{q^k}\rangle$ and

$$\left|\langle u^{q^j}\rangle \cup \langle -u^{q^k}\rangle\right| = \left|\langle u^{q^j}\rangle\right| + \left|\langle -u^{q^k}\rangle\right| - \left|\langle u^{q^k}\rangle\right| = q^{r-j} + 2q^{r-k} - q^{r-k} = q^{r-j} + q^{r-k}.$$

Therefore, we have the following possibilities for B and the corresponding density of bounded primes:

$B(a, b; c)$	Density
$\emptyset$	0
$\langle u^{q^j}\rangle$	$1/2q^j$
$\langle -u^{q^k}\rangle$	$1/q^k$
$\langle u^{q^j}\rangle \cup \langle -u^{q^k}\rangle$ ($j < k$)	$(q^{k-j}+1)/(2q^k)$

The problematically large densities satisfying

$$D(a, b; c) > \frac{1}{q}$$

are the cases when $j = 0$ and $k = 0$ in the second and third rows, and the cases when $j = 0$ in the last row. That is, the problematic cases are:

$B(a, b; c)$	Density
$\langle u\rangle$	$1/2$
$\langle -u\rangle$	1
$\langle u\rangle \cup \langle -u^{q^k}\rangle$ ($k > 0$)	$(q^k+1)/(2q^k)$

Observe that the problematic cases are exactly those for which $u \in B$. Thus, we must produce a value of N such that if $p > N$ then $u \notin B$.

Theorem 4 shows that $u \in B$ if and only if

$$\{-u^j z/p\} \leq \max(\{-u^j x/p\}, \{-u^j y/p\})$$

for all integers j. Notice that $\{-u^j z/p\}p = [-u^j z]_p$, and likewise for the other terms appearing above. As j varies, the term u^j varies over the set Q of quadratic residues mod p. Therefore, we find that $u \in B$ if and only if

$$[-vz]_p \leq \max([-vx]_p, [-vy]_p)$$

for all $v \in Q$. Thus, we must show that if p is big enough, then we can find a quadratic residue $v \in Q$ such that $[-vz]_p > [-vx]_p$ and $[-vz]_p > [-vy]_p$.

The simplest case is if $-z$ is not a quadratic residue, for then we can choose v such that $[-vz]_p = p - 1$, since $p \equiv 3 \pmod 4$ implies that -1 is not a quadratic residue mod p. Since $z \neq x, y$ then this implies that necessarily $p - 1 > [-vx]_p$ and $p - 1 > [-vy]_p$, as required. Observe that this does not require p to be large.

It remains to consider the case when $-z \in Q$. After replacing $-vz$ by v, we see that we are reduced to finding $v \in Q$ such that $[v]_p > [vx/z]_p$ and $[v]_p > [vy/z]_p$. That is, we must find $v \in W_p(x/z) \cap W_p(y/z)$. Proposition 14 supplies a value of N which ensures that this is possible whenever $p > N$. This concludes the proof. □

Remark 18. Let notation be as in Theorem 17 and write $D = D(x/p, y/p; z/p)$. If $p = 2q + 1$ is prime with q an odd prime then it's not hard to show that

(1) $D = 0$ if and only if $c < a$ and $c < b$;
(2) $D = 1/2q$ or $D = 1/2$ if and only if $a < c$ and $b < c$;
(3) $D = 1/q$ or $D = (q + 1)/(2q)$ if and only if $a < c < b$;
(4) $D = 1$ never occurs.

For such primes, computations suggest that $D \leq 1/q$ whenever $p \geq 59$. The bound of $p = 59$ above cannot be improved upon. For example,

$$W_{47}(29) = \{18, 25, 28, 36\}, \qquad W_{47}(43) = \{21, 32, 34, 42\},$$

and hence $W_{47}(29) \cap W_{47}(43) = \emptyset$. This can be used to produce examples of hypergeometric series with lots of bounded primes: unravelling the proof of Theorem 17 produces corresponding examples such as

$$D\left(\frac{4}{47}, \frac{18}{47}; \frac{46}{47}\right) = \frac{1}{2}.$$

Note that this density is indeed larger than the bound $1/q = 1/23$ from Theorem 17. An effective version of Theorem 17 follows for primes $p \equiv 3 \pmod 8$ by Proposition 15, but an effective version for primes $p \equiv 7 \pmod 8$ remains an open problem.

REFERENCES

[1] Bruce C. Berndt. Classical theorems on quadratic residues. *Enseignement Math. (2)*, 22(3–4):261–304, 1976.

[2] F. Beukers and G. Heckman. Monodromy for the hypergeometric function ${}_nF_{n-1}$. *Invent. Math.*, 95(2):325–354, 1989.

[3] Jonathan W. Bober. Factorial ratios, hypergeometric series, and a family of step functions. *J. Lond. Math. Soc. (2)*, 79(2):422–444, 2009.

[4] Alexander Borisov. Quotient singularities, integer ratios of factorials, and the Riemann hypothesis. *Int. Math. Res. Not. IMRN*, (15):Art. ID rnn052, 19, 2008.

[5] D. A. Burgess. The distribution of quadratic residues and non-residues. *Mathematika*, 4:106–112, 1957.

[6] Gilles Christol. Fonctions hypergéométriques bornées. *Groupe de travail d'analyse ultramétrique*, 14:1–16, 1986-1987.

[7] E. Delaygue, T. Rivoal, and J. Roques. On Dwork's p-adic formal congruences theorem and hypergeometric mirror maps. *Mem. Amer. Math. Soc.*, 246(1163):v+94, 2017.
[8] Bernard Dwork. *Generalized hypergeometric functions*. Oxford Mathematical Monographs. The Clarendon Press, Oxford University Press, New York, 1990. Oxford Science Publications.
[9] Bernard M. Dwork. *Lectures on p-adic differential equations*, volume 253 of *Grundlehren der Mathematischen Wissenschaften [Fundamental Principles of Mathematical Science]*. Springer-Verlag, New York-Berlin, 1982. With an appendix by Alan Adolphson.
[10] Cameron Franc, Terry Gannon, and Geoffrey Mason. On unbounded denominators and hypergeometric series. *arxiv*, 2017 (submitted).
[11] Edmund Landau. Eine Anwendung des Eisensteinschen Satzes auf die Theorie der Gaussschen Differentialgleichung. *J. Reine Angew. Math.*, 127:92–102, 1904.
[12] F. Rodriguez-Villegas. Integral ratios of factorials and algebraic hypergeometric functions. *Oberwolfach Rep.*, (8):1814–1816, 2005.
[13] Steve Wright. *Quadratic residues and non-residues*, volume 2171 of *Lecture Notes in Mathematics*. Springer, Cham, 2016. Selected topics.