Mathematics

Open Problems with Factorials

Hermite

supervised by
Advisor

April 22, 2018

Preamble

This essay contains the results of a research project on number theory focusing on two open problems that involve the factorial function. This project originated in a mathematics class at school in September 2016 where Stirling's formula was discussed. I was intrigued by the fact that the square root of the quotient $n^n/n!$ happened to be very close to the n^{th} Fibonacci number, at least for not too large values of n. This observation triggered my interest for the factorial function.

At the same time I had started reading about the ring of p-adic integers (which is an extension of the ordinary integers by allowing base p expansions to become infinite), and learned that many features of ordinary calculus have analogues in the p-adic numbers, for instance the convergence of sequences and infinite series. Then I wondered if there was also a p-adic version of Stirling's formula, providing a non-recursive way of approximating factorials. While pursuing this idea I discovered that p-adic analysis is a rich discipline, relatively recent in the body of mathematics.

Although most topics in p-adic analysis are too advanced, I discovered a surprisingly unsolved problem by browsing the Internet, namely the series $\sum n!$ converges in the p-adic metric for all primes p and it is not known whether its sum is rational (i.e., the quotient of two ordinary integers) or irrational. The fact that $\sum n!$ converges can easily be seen in base 10 by observing that when n grows large enough the lowest digits of the partial sums become unchanged since the subsequent terms being added are divisible by increasingly high powers of 10.

After several months of effort I could not find a proof of the fact (conjectured since 1984) that $\sum n!$ is a p-adic irrational for all primes p, yet I obtained several partial results which contribute to this open problem. I could prove, among other facts, that $\sum p^{v_p(n!)}$ converges to an irrational number for every p, where $v_p(n!)$ denotes the highest power of p dividing $n!$. This result is the subject of a short article [3] which has been posted in the arXiv database —the reference is not given since this is an anonymous version of the essay.

Meanwhile, my interest for the factorial function led me to work in another so far unsolved problem, proposed in an article that appeared in the arXiv in 2017. It was an apparently simple conjecture about binomial coefficients, with relevant implications in group theory. Specifically, it was conjectured that for every positive integer n there exist two primes p and r such that all binomial coefficients $\binom{n}{k}$ are divisible by either p or r if $1 \leq k \leq n-1$.

I became very much engaged with this problem and succeeded in proving the truth of the conjecture in many cases. It is easy to see, using Lucas' Theorem, that the conjecture holds when n is a prime power or a product of two prime powers. I proved that the conjecture also holds when the difference between n and the greatest prime smaller than n is smaller than some prime power dividing n, and refined this result in various ways. Two sequences of numbers for which our remarks do not suffice to prove the conjecture were accepted for publication in the On-Line Encyclopedia of Integer Sequences [4, 5].

We also found other assumptions under which the conjecture is true. For example, every n has infinitely many multiples for which the conjecture holds, assuming the truth of Cramér's Conjecture.

Interestingly, some results in this part of our work are based on the same approximation of $n!$ by powers of a prime p dividing $n!$ (Legendre's formula) that were used in the part concerned with p-adic analysis.

The two open problems that I have studied are the subject of Part I and Part II of this essay. The first part corresponds to the problem on divisibility of binomial coefficients, and the second part is devoted to convergence of p-adic series containing the factorial function. We present them in two separate parts because the first part, entitled *On the divisibility of binomial coefficients*, is what is going to be presented as an extended essay for the International Baccalaureate. More precisely, due to the word limit, we are going to present this first part with sections 8, 9 and 10 shifted to the Appendix, since, although these sections contain interesting results, they are not completely focused on the main objective of our project.

I should also mention that I have created a website in which all the C++ programs that were used to obtain numerical evidence in this work are made available to other people who could perhaps continue this research or go towards other goals. This website also contains explanations of the mathematical concepts involved in the problems that we have studied. The address is

`https://numbertheoryandgrouptheory.yolasite.com/`

Acknowledgements

I am very grateful to my tutor for his guidance, help and corrections throughout this work. I would also like to thank Oscar Mickelin for his suggestions and very useful comments. I am also thankful to Dr. Artur Travesa for making me realize that p-adic numbers can be a high-school research topic, and to Óscar Rivero for his great remarks. Finally, I am indebted to my family for supporting me so much at all times.

Contents

Part I

On the Divisibility of Binomial Coefficients

Is it true that for every positive integer n there are two primes p and r such that if $1 \leq k \leq n-1$ then $\binom{n}{k}$ is divisible by at least one of p or r?

1 Introduction

Apart from their many uses in various fields of mathematics, binomial coefficients display interesting divisibility properties. Kummer's [18] and Lucas' [20] Theorems are two remarkable results relating binomial coefficients and prime numbers. Kummer's Theorem provides an easy way to determine the highest power of a prime that divides a binomial coefficient, and Lucas' Theorem yields the remainder of the division of a binomial coefficient by a prime number. Davis and Webb [7] found a generalization of Lucas' Theorem for prime powers. Legendre [19] found two expressions for the largest power of a prime p that divides the factorial $n!$ of a given integer n.

However, some conjectures about binomial coefficients still remain unproven. We focus on the following condition considered by Shareshian and Woodroofe in a recent paper [29]:

Condition 1. *For a positive integer n, there exist primes p and r such that, for all integers k with $1 \leq k \leq n-1$, the binomial coefficient $\binom{n}{k}$ is divisible by at least one of p or r.*

This condition leads to the following question:

Question 1.1. *Does Condition 1 hold for every positive integer n?*

In [29] it is conjectured that Condition 1 is true for all positive integers, yet there is no known proof. Our main purpose in this work is to try to prove this conjecture, which is relevant because it is an open problem with implications in number theory and group theory. Therefore, it is very thrilling to obtain research results that might lead to a complete proof.

We also introduce the following variation of Condition 1, which we study later in this work:

Definition 1.2. A positive integer n satisfies the *N-variation* of Condition 1 if there exists a set consisting of N different primes such that if $1 \leq k \leq n-1$ then the binomial coefficient $\binom{n}{k}$ is divisible by at least one of the N primes.

This essay is organized as follows. After providing background information in Section 2, we prove that n satisfies Condition 1 if it is a product of two prime powers and also if it satisfies a certain inequality regarding the largest prime smaller than n. Next we provide bounds related to the prime power divisors of n and discuss several cases in which n satisfies Condition 1 depending on the largest prime smaller than $n/2$. In Section 6 and Section 7 we use prime gap conjectures in order to settle some cases in which a sufficiently large integer n satisfies Condition 1, and discuss cases in which n satisfies the 3-variation of Condition 1. Finally, in Section 8 we provide upper bounds for a number N so that all integers n satisfy the N-variation of Condition 1, followed by computational results and a generalization of Condition 1 to multinomials.

We have created a website that includes explanations and C++ codes of most concepts contained in this work. The address is

`https://numbertheoryandgrouptheory.yolasite.com/`

Screenshots of this website are included in the Appendix.

2 Background

Three theorems about divisibility of binomial coefficients and factorials are relevant for the proofs given in this work.

Theorem 2.1. (Kummer [18]) *Let k and n be integers with $0 \leq k \leq n$. If α is a positive integer and p a prime, then p^α divides $\binom{n}{k}$ if and only if α carries are needed when adding k and $n-k$ in base p.*

Theorem 2.2. (Lucas [20]) *Let m and n be positive integers, let p be a prime, and let $m = m_k p^k + m_{k-1}p^{k-1} + \cdots + m_1 p + m_0$ and $n = n_k p^k + n_{k-1}p^{k-1} + \cdots + n_1 p + n_0$ be the base p expansions of m and n respectively. Then $\binom{m}{n} \equiv \prod_{i=0}^{k} \binom{m_i}{n_i} \pmod{p}$.*

It is important to notice that by convention $\binom{m}{n} = 0$ if $m < n$. Hence, if any of the digits of the base p representation of m is 0 whereas the corresponding digit of the base p representation of k is not 0, then $\binom{m}{k}$ is divisible by p because everything is multiplied by zero and by Lucas' Theorem we have that $\binom{m}{k} \equiv 0 \pmod{p}$. This is usually the way in which we use Lucas' Theorem throughout this work.

The following diagram displays an example of this property. In order to know if $\binom{21}{12}$ is divisible by 2, we represent both numbers in base 2 and compare the digits. The key is the pair of numbers marked with red. Because the digit below (which corresponds to 12) is larger than the number above (which corresponds to 21), from Lucas' Theorem we infer that $\binom{21}{12}$ is divisible by 2.

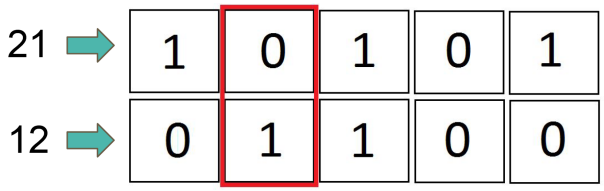


Figure 1: Example of an application of Lucas' Theorem.

Theorem 2.3. (Legendre [19]) *If $v_p(n)$ denotes the maximum power α of p such that p^α divides n, then $v_p(n!) = \sum_{k=1}^{\infty} \left\lfloor \frac{n}{p^k} \right\rfloor$.*

Here $\lfloor x \rfloor$ denotes the integer part of x. Moreover, Legendre also showed that

$$v_p(n!) = \frac{n - S_p(n)}{p-1},$$

where $S_p(n)$ denotes the sum of all the digits in the base p expansion of n.

3 Some cases of n satisfying Condition 1

3.1 When n is a prime power

Proposition 3.1. *A positive integer n satisfies the 1-variation of Condition 1 with p if and only if $n = p^\alpha$ for some $\alpha > 0$, for $\alpha \in \mathbb{N}$.*

Proof. If $n = p^\alpha$, then the base p representation of n is equal to $1\overbrace{0\ldots0}^{\alpha \text{ zeroes}}$. Any k such that $1 \leq k \leq n-1$ has at most $\alpha - 1$ zeroes in base p. Therefore, at least one of the digits of the base p representation of k is bigger than the corresponding digit of n in base p (at least the leading one). It then follows from Lucas' Theorem that $\binom{n}{k}$ is divisible by p. Otherwise, if n is not a prime power, then the i^{th} digit of n in base p is not 0 for some value of i. Thus, we can find at least one k such that the i^{th} digit of k in base p is larger than 0. Hence, by Lucas' Theorem $\binom{n}{k}$ is not divisible by p. □

Corollary 3.2. *If $n = p^\alpha + 1$, then n satisfies Condition 1 with p and any prime factor of n.*

Proof. The proof relies on the fact that $\binom{m}{k} + \binom{m}{k+1} = \binom{m+1}{k+1}$ for all positive integers m and k. If m is a power of a prime p, then it follows from Proposition 3.1 that $\binom{m}{k}$ and $\binom{m}{k+1}$ are divisible by p if $1 \leq k \leq m-1$. In these cases, because $\binom{m+1}{k+1}$ is the result of the sum of two multiples of p, it also is a multiple of p. When $k = 1$ or $k = m$, we have that $\binom{m+1}{k} = m + 1$, so any prime factor of $m + 1$ divides it. □

3.2 When n is a product of two prime powers

Proposition 3.3. *If a positive integer n is equal to the product of two prime powers p_1^α and p_2^β, then n satisfies Condition 1 with p_1 and p_2.*

Proof. Observe that $\text{lcm}(p_1^\alpha, p_2^\beta) = n$. The base p_1 representation of n ends in α zeroes and the base p_2 representation of n ends in β zeroes. Because any positive k smaller than n cannot be divisible by both p_1^α and p_2^β, it is not possible that k finishes with α zeroes in base p_1 and β zeroes in base p_2. Thus, we can apply Lucas' Theorem modulo the prime p_1 if $p_1^\alpha \nmid k$ or modulo the prime p_2 if $p_2^\beta \nmid k$. □

3.3 Considering the closest prime to n

After analyzing many cases in which n satisfies Condition 1, we observed that the largest prime smaller than n was almost always one of the two primes with which n fulfilled Condition 1. This finding led to the following statement and proof:

Theorem 3.4. *Let q be the largest prime smaller than n and let $p_i^{a_i}$ be any prime factor divisor of n. If $n - q < p_i^{a_i}$, then n satisfies Condition 1 with p_i and q.*

For the proofs of Theorem 3.4 and Corollary 3.6 we use the Bertrand-Chebyshev Theorem:

Theorem 3.5. (Bertrand-Chebyshev [2]) *For every integer $n > 3$ there exists a prime p such that $n/2 < p < n$.*

Proof of Theorem 3.4. We distinguish between two intervals: the interval $(1, n-q]$ and the interval $(n-q, n]$. Due to the symmetry of binomial coefficients, we only consider $k \leq n/2$. By the Bertrand-Chebyshev Theorem, we know that there is at least one prime between $n/2$ and n, hence $n/2 < q < n$. Then, for all k, $k < n/2 < q$. The base q representation of n is $1 \cdot q + (n-q)$. Therefore, we do not need to consider the interval $(n-q, n)$ because the last digit of the base q representation of any $k > n-q$ is larger than the last digit of the base q representation of n. Thus, by Lucas' Theorem, the binomial coefficient $\binom{n}{k}$ is divisible by q. If there is no multiple of $p_i^{a_i}$ in the interval $(1, n-q)$, then by Lucas' Theorem all the binomial coefficients $\binom{n}{k}$ with $1 \leq k \leq n/2$ are divisible by at least p_i or q. Moreover, equality in Theorem 3.4 cannot hold because $p_i^{a_i}$ divides both $p_i^{a_i}$ and n, and hence q would not be a prime. □

Corollary 3.6. *Let $p_j^{a_j}$ denote the largest prime power divisor of an integer n and q the closest prime to n. If $n - q < p_j^{a_j}$, then n satisfies Condition* 1 *with p_j and q.*

We show a diagram which illustrates the proof of Theorem 3.4. The key is to split the range of k into two intervals.

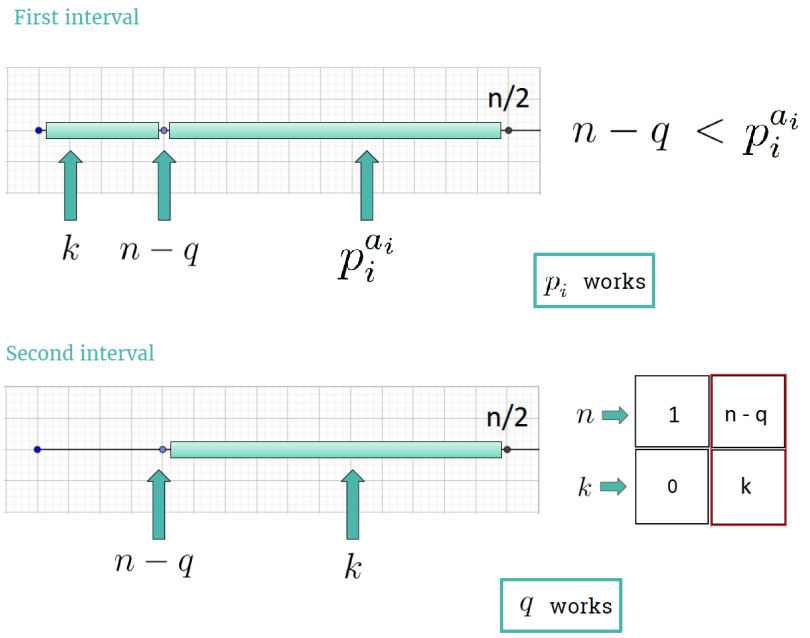


Figure 2: Illustration of the proof of Theorem 3.4.

Note that if n satisfies Condition 1 then at least one of these two primes has to be a prime factor of n, because otherwise $\binom{n}{1} = n$ is not divisible by either one of the two primes.

The only remaining cases are those in which $n - q > p_i^{a_i}$ and n is neither a prime nor a prime power. Let q_2 denote the largest prime smaller than $n/2$. By analyzing

the integers that are part of these remaining cases, we notice that n usually satisfies Condition 1 with the pair formed by a prime factor of n and q_2. If we analyze the six numbers smaller than 2,000 such that $n - q > p_i^{a_i}$, we see that the inequality $p_i^{a_i} > n - 2q_2$ holds and q_2 and p_i satisfy Condition 1. Table 1 provides evidence with the only four numbers until 1,000 that do not satisfy Condition 1 with q and p_i. However, the sequence of all such integers is infinite. The On-Line Encyclopedia of Integer Sequences (OEIS) has accepted our submission of this sequence [4]. These observations led my investigations towards q_2, which are described in the following sections.

Number	126	210	330	630
Prime factorization	$2 \cdot 3^2 \cdot 7$	$2 \cdot 3 \cdot 5 \cdot 7$	$2 \cdot 3 \cdot 5 \cdot 11$	$2 \cdot 3^2 \cdot 5 \cdot 7$
q	113	199	317	619
q_2	61	103	163	313
$n - q$	13	11	13	11
$n - 2q_2$	4	4	4	4
$(1, n - q]$	2, 3, 4	2, 3, 4	2, 3, 4	2, 3, 4
$(n - q, n]$	62, 63	104, 105	164, 165	314, 315
Pairs that satisfy 1	3-61	5-103	5-163	3-313, 5-313, 7-313

Table 1: Information about the four numbers below 1,000 that do not satisfy Condition 1 with q and p_i.

4 Bounds for $p_i^{a_i}$

Before analyzing q and q_2 further, we establish some bounds for $p_i^{a_i}$ assuming that $n - q > p_i^{a_i}$.

Lemma 4.1. *If n is not a prime and $n - q > p_i^{a_i}$, then $p_i^{a_i} < n/2$.*

Proof. Using the Bertrand-Chebyshev Theorem we see that $n/2 > n - q > 0$. Also, $n - q > p_i^{a_i}$. Therefore, $n/2 > p_i^{a_i}$. □

We can find an even lower bound for $p_i^{a_i}$. In 1952, Nagura [22] showed that if $n \geq 25$ then there is always a prime between n and $(1 + 1/5)n$. Therefore, we find that $5n/6 < q < n$ when $n \geq 30$.

Lemma 4.2. *If $n \geq 30$ is not a prime and $n - q > p_i^{a_i}$, then $p_i^{a_i} < n/6$.*

The proof is the same as the one for Lemma 4.1. In 1976 Schoenfeld [30] showed that for $n \geq$ 2,010,760 there is always a prime between n and $(1 + 1/16{,}597)n$. Therefore, we know that if $n >$ 2,010,882 then

$$\frac{16{,}597n}{16{,}598} < q_2 < n.$$

Shareshian and Woodroofe [29] checked computationally that all integers smaller than 10 million satisfy Condition 1, which means that we can apply Schoenfeld's bound.

Lemma 4.3. *If n is not a prime, $n > 2{,}010{,}882$ and $n-q > p_i^{a_i}$, then $p_i^{a_i} < n/16{,}598$.*

The proof follows the same steps as the previous two lemmas.

Proposition 4.4. *Let $n = p_i^{a_i}m$. If $n \geq 2{,}010{,}882$ and $m < 16{,}598$, then n satisfies Condition 1 with p_i and q.*

Proof. By Schoenfeld's bound we know that $n - q < n/16{,}598$. If $m < 16{,}598$, it means that $p_i^{a_i} > n/16{,}598$. Thus, $p_i^{a_i} > n - q$ and, by Theorem 3.4, q and p_i satisfy Condition 1. □

5 When $n - q > p_i^{a_i} > n - 2q_2$

In this section we analyze the integers n that satisfy the inequalities

$$n - q > p_i^{a_i} > n - 2q_2,$$

and we prove some cases in which n satisfies Condition 1 with p_i and q_2. The fact that we are considering $n - 2q_2$ comes from the base q_2 representation of n. We distinguish between two cases: when $k < q_2$ and when $k > q_2$. The base q_2 representation of n is $2 \cdot q_2 + (n - 2q_2)$. The base q_2 representation of k is $0 \cdot q_2 + k$ if $k < q_2$ and $1 \cdot q_2 + (k - q_2)$ if $k > q_2$. Hence, there is no need to analyze the interval $(n-2q_2, q_2]$ because for all k such that $n-2q_2 < k \leq q_2$, we can use Lucas' Theorem to see that the binomial coefficient $\binom{n}{k}$ is congruent to 0 modulo q_2. Therefore, we only need to consider the interval $(q_2, n/2]$.

5.1 If n is odd

It is important to remark that if k is not a multiple of $p_i^{a_i}$ then by Lucas' Theorem $\binom{n}{k}$ is divisible by p_i. Therefore, we only have to analyze the integers in $(q_2, n/2]$ that are multiples of $p_i^{a_i}$. We then claim the following:

Theorem 5.1. *If n is odd and $n - q > p_i^{a_i} > n - 2q_2$, then n satisfies Condition 1 with p_i and q_2.*

Proof. Since n is odd, $n/2$ is not an integer. Hence it is enough to prove that there is no multiple of $p_q^{a_q}$ in the interval $(q_r, n/2)$. We will prove this by contradiction. Thus assume that $q_r < \lambda p_q^{a_q} < n/2$ for some integer λ. Then $\lambda \geq (m-1)/2$ if $n = mp_q^{a_q}$, since $((m-1)/2)p_q^{a_q}$ is the largest multiple of $p_q^{a_q}$ that is smaller than $n/2$ (note that m is odd because n is odd). Now from the inequality $((m-1)/2)p_q^{a_q} > q_r$ it follows that $n - p_q^{a_q} > 2q_r$ and this contradicts the assumption that $n - 2q_r < p_q^{a_q}$. □

5.2 If n is even and p_i is not 2

Lemma 5.2. *If n is even and $p_q \neq 2$, then the only multiple of $p_q^{a_q}$ in the interval $(q_r, n/2]$ is $n/2$.*

Proof. Since $p_q \neq 2$, the integer $n/2$ is still a multiple of $p_q^{a_q}$. Hence we may write $n/2 = \lambda p_q^{a_q}$ for some integer λ. If there is another multiple of $p_q^{a_q}$ between q_r and $n/2$, then we have $q_r < (\lambda - 1)p_q^{a_q} < n/2$, and this implies that $n/2 - p_q^{a_q} > q_r$. Hence $n - 2q_r > 2p_q^{a_q} > p_q^{a_q}$, which is incompatible with our assumption which states that $n - 2q_r < p_q^{a_q}$. □

Theorem 5.3. *If 2^α is a prime power divisor of n and 2^α satisfies*

$$n - q > 2^\alpha > n - 2q_2,$$

then n satisfies Condition 1 with 2 and q_2.

Proof. The integer n has the factor 2^α in its prime factorization, which means that $n/2$ has the factor $2^{\alpha-1}$. The base 2 representation of n has one more zero than the base 2 representation of $n/2$, which means that by Lucas' Theorem $\binom{n}{n/2}$ is congruent to 0 modulo 2^α. By Lemma 5.2, $n/2$ is the only multiple of 2^α in the interval $(q_2, n/2]$; hence the proof is complete. □

5.3 If n is even and p_i is not 2

By Lemma 5.2 we only need to consider the central binomial coefficient $\binom{n}{n/2}$, because the only multiple of $p_i^{a_i}$ in the interval $(q_2, n/2]$ is $n/2$. We claim the following proposition, using Legendre's Theorem for its proof.

Proposition 5.4. *The prime factor p_i divides $\binom{n}{n/2}$ if and only if at least one of the fractions $\lfloor n/p^\alpha \rfloor$ with $\alpha \geq 1$ is odd.*

Proof. When we compare $v_{p_i}(n!)$ and $v_{p_i}((n/2)!)$ we see that, for each α,

$$\left\lfloor \frac{n}{p^\alpha} \right\rfloor = 2 \left\lfloor \frac{n/2}{p^\alpha} \right\rfloor$$

if $\lfloor n/p^\alpha \rfloor$ is even. If $\lfloor n/p^\alpha \rfloor$ is even for all α, we conclude that $v_{p_i}(n!) = 2v_{p_i}((n/2)!)$, and hence p_i does not divide $\binom{n}{n/2}$. However, if $\lfloor n/p^\alpha \rfloor$ is odd, then

$$\left\lfloor \frac{n}{p^\alpha} \right\rfloor = 2 \left\lfloor \frac{n/2}{p^\alpha} \right\rfloor + 1.$$

Therefore, $v_{p_i}(n!)$ is greater than $2v_{p_i}((n/2)!)$. □

Corollary 5.5. *Let $S_{p_i}(n)$ be the base p_i representation of n. If $\frac{n - S_p(n)}{p-1}$ is odd then p_i divides $\binom{n}{n/2}$.*

Corollary 5.5 is shown using Legendre's formula.

Corollary 5.6. *If any of the digits in the base p_i representation of $n/2$ is larger than $\lfloor p_i/2 \rfloor$, then the binomial coefficient $\binom{n}{n/2}$ is divisible by p_i.*

Corollary 5.7. *If one of the digits in the base p_i representation of n is odd, then the prime p_i divides $\binom{n}{n/2}$.*

Proof. The proofs of Corollaries 5.6 and 5.7 are similar. If a digit of $n/2$ is larger than $\lfloor p_i/2 \rfloor$, when we add $n/2$ to itself in base p_i to obtain n there at least one carry. Similarly, if n has an odd digit in base p_i, it means that there has been a carry when adding $n/2$ and $n/2$ in base p_i. By Kummer's Theorem with $k = n/2$, if there is at least one carry when adding $n/2$ to itself in base p_i, then p_i divides the binomial coefficient $\binom{n}{n/2}$. □

Corollary 5.8. *If* $p_i^{\left\lfloor \frac{\log(n)}{\log(p_i)} \right\rfloor} > n/2$ *and* $n - q > p_i^{a_i} > n - 2q_2$*, then* p_i *divides* $\binom{n}{n/2}$ *and therefore* n *satisfies Condition* 1 *with* p_i *and* q_2*.*

Proof. The largest α such that $p_i^{\alpha} < n < p_i^{\alpha+1}$ is $\left\lfloor \frac{\log(n)}{\log(p_i)} \right\rfloor$. Therefore, in Proposition 5.4, α is bounded by $1 \leq \alpha \leq \left\lfloor \frac{\log(n)}{\log(p_i)} \right\rfloor$. Also note that $\alpha \geq a_i$, where a_i is the exponent of p_i. If $p_i^{\left\lfloor \frac{\log(n)}{\log(p_i)} \right\rfloor} > n/2$ then $\lfloor n/p_i^{\alpha} \rfloor = 1$. Because this is odd, p_i divides $\binom{n}{n/2}$ by Proposition 5.4. □

5.4 Some cases in which $2n$ implies n

In this section we denote by $p_{i_k}^{a_i}$ and q_k any prime power factor of k and the largest prime smaller than k respectively. For integers that satisfy the inequality $n - q > p_i^{a_i} > n - 2q_2$, we observe three cases in which if $2n$ satisfies Condition 1 and $p_{i_{2n}} \neq 2$, then n also satisfies Condition 1. Note that since p_i is not 2, then $p_{i_{2n}} = p_{i_n}$. Also, $q_{2_{2n}} = q_n$. Therefore we claim:

Claim 5.9. *If* $2n$ *satisfies the inequality* $2n - 2q_{2_{2n}} < 2n - q_{2n} < p_{i_{2n}}^{a_{i_{2n}}}$*, then* n *satisfies Condition* 1 *with* p_i *and* q*.*

Proof. We rewrite the inequality above as $n - q_n < 2(n - q_n) < 2n - q_{2n} < p_{i_n}^{a_{i_n}}$. Therefore, $n - q_n < p_{i_n}^{a_{i_n}}$, and, by Theorem 4.2, n satisfies Condition 1 with the primes p_i and q. □

Claim 5.10. *If* $2n$ *satisfies the inequality* $2n - q_{2n} < 2n - q_{2_{2n}} < p_{i_{2n}}^{a_{i_{2n}}}$*, then* n *satisfies Condition* 1 *with* p_i *and* q*.*

Claim 5.11. *If* $2n$ *satisfies the inequality* $2n - 2q_{2_{2n}} < p_{i_{2n}}^{a_{i_{2n}}} < 2n - q_{2n}$*, then* n *satisfies Condition* 1 *with* p_i *and* q*.*

The proofs of Claims 5.10 and 5.11 follow the same steps as the one of Claim 5.9.

6 Large multiples of n satisfying Condition 1 with prime gap conjectures

After studying these inequalities, I considered using prime gap conjectures to study Condition 1 for large integers. In this section we always denote the t^{th} prime as $\hat{p}_t$.

6.1 Cramér's Conjecture

Conjecture 6.1. (Cramér [13]) *There exist constants M and N such that if $\hat{p}_t \geq N$ then $\hat{p}_{t+1} - \hat{p}_t \leq M(\log \hat{p}_t)^2$.*

We claim the following:

Proposition 6.2. *If Cramér's conjecture is true, then for every positive integer n and every prime p dividing n, the number np^k satisfies Condition 1 for all sufficiently large values of k.*

Proof. Let M and N be the constants given by Cramér's conjecture. Given a positive integer n which is not a prime power and a prime divisor p of n, we write $n = mp^a$ where p does not divide m, and compare $M(\log nx)^2$ with $p^a x$ as x goes to infinity. Using L'Hôpital's rule, we find that

$$\lim_{x\to\infty} \frac{p^a x}{M(\log nx)^2} = (\text{Hôp.}) \lim_{x\to\infty} \frac{p^a nx}{2Mn \log nx} = \lim_{x\to\infty} \frac{p^a x}{2M \log nx}$$

$$= (\text{Hôp.}) \lim_{x\to\infty} \frac{p^a nx}{2Mn} = \lim_{x\to\infty} \frac{p^a x}{2M} = \infty.$$

Therefore, $p^a x$ is bigger than $M(\log nx)^2$ when x is sufficiently large. Hence we can choose any k large enough so that $p^{a+k} > M(\log np^k)^2$ and furthermore, if q denotes the largest prime smaller than np^k, then $q \geq N$. Now, if r denotes the smallest prime larger than np^k, we infer that, if Cramér's conjecture holds, then, since $q \geq N$,

$$np^k - q \leq r - q \leq M(\log q)^2.$$

Moreover

$$M(\log q)^2 < M(\log np^k)^2 < p^{a+k}.$$

Hence $np^k - q < p^{a+k}$ and, since p^{a+k} is the highest power of p dividing np^k, Theorem 3.4 implies that np^k satisfies Condition 1. □

Cramér's conjecture also proves the following proposition:

Proposition 6.3. *Let m denote the number of distinct prime factors of n. If Cramér's conjecture is true and n grows sufficiently large keeping m fixed, then n satisfies Condition 1.*

Proof. If n has m distinct prime factors, we define the *average prime factor* of n as $\sqrt[m]{n}$ because if n were formed by m equal prime factors each one would equal $\sqrt[m]{n}$. It is true that $\sqrt[m]{n} \leq p_j^{a_j}$, where $p_j^{a_j}$ denotes the largest prime power divisor of n. Hence we must see if $M(\log n)^2 < \sqrt[m]{n}$ for large values of n. We apply again L'Hôpital's rule to compute the limit

$$\lim_{x\to\infty} \frac{\sqrt[m]{n}x}{M(\log nx)^2}$$

and we obtain that $M(\log n)^2 < \sqrt[m]{n}$ holds when n is sufficiently large. □

6.2 Oppermann's Conjecture

A weaker conjecture on prime gaps by Oppermann states the following:

Conjecture 6.4. (Oppermann [25]) For some constant M, $\hat{p}_{t+1} - \hat{p}_t \leq M\sqrt{\hat{p}_t}$.

Proposition 6.5. *If Oppermann's conjecture is true, then for every positive integer n and every prime p dividing n, the number np^k satisfies Condition 1 for all sufficiently large values of k.*

Proof. The proof is similar to the proof of Proposition 6.2. We apply L'Hôpital's rule once to solve the indetermination in

$$\lim_{x\to\infty} \frac{p^a x}{M\sqrt{nx}},$$

where p^a is the highest power of p dividing n. Since the ratio goes to infinity our inequality is satisfied, and by choosing $x = p^k$ with k large enough the proof is complete. □

6.3 Riemann's Hypothesis

The following conjecture is a consequence of Riemann's Hypothesis.

Conjecture 6.6. (Riemann [14]) *For some constant M, $\hat{p}_{t+1} - \hat{p}_t \leq M(\log \hat{p}_t)\sqrt{\hat{p}_t}$.*

This bound can be used to prove the following:

Proposition 6.7. *If Riemann's conjecture is true, then for every positive integer n and every prime p dividing n, the number np^k satisfies Condition 1 for all sufficiently large values of k.*

Proof. We apply again L'Hôpital's rule to solve the indetermination in

$$\lim_{x\to\infty} \frac{p^a x}{M(\log nx)\sqrt{nx}}$$

The limit goes to infinity and hence, by choosing $x = p^k$ with k large enough, the proof is complete. □

Due to the similarities of the inequalities, we skip the calculations of Propositions 6.5 and 6.7.

7 Using other primes to satisfy Condition 1

In Sections 3 and 5 we analyzed inequalities involving $n - q$ and $n - 2q_2$. This made us realize in general, for any positive integer d, we can study the function $n - dq_d$, where q_d refers to the largest prime smaller than n/d (when writing q_1 we omitted the subindex 1).

We consider the integers n that do not satisfy the inequality $p_i^{a_i} > n - 2p_2$. Up to 1,000,000 there are only 88 integers that do not satisfy $p_i^{a_i} > n - 2p_2$. The

On-Line Encyclopedia of Integer Sequences (OEIS) has accepted our submission of these numbers [5]. Up to 1,000,000, there are 25 integers that do not satisfy the inequality $p_i^{a_i} > n - 3p_3$; 7 integers that do not satisfy the inequality $p_i^{a_i} > n - 4p_4$; 5 integers that do not satisfy the inequality $p_i^{a_i} > n - 5p_5$, and only 1 integer that does not satisfy the inequality $p_i^{a_i} > n - 6p_6$. Figure 3 shows the number of integers up to 1,000,000 that do not satisfy the inequality $p_i^{a_i} > n - dp_d$ depending on d.

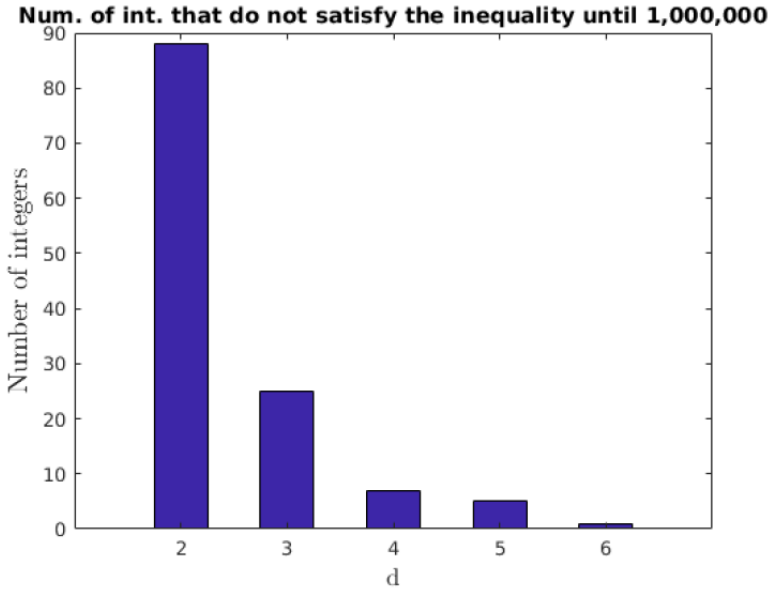


Figure 3: Number of integers up to 1,000,000 that do not satisfy the inequality $p_i^{a_i} > n - dp_d$ as a function of d.

We also observe that the function $n - dq_d$ tends to 0 as d increases, which means that it is likely that at some point the inequality is achieved. This is explained with the properties of the function n/d, which behaves in the same way as the function $1/x$ except for the constant n. As d grows large, the difference between n/d and $n/(d+1)$ grows smaller. Hence, the closest prime to n/d is the same one for all the n/d that are close. Then, when d increases, p_d decreases much more slowly, and because it is multiplied by d, which grows linearly, dp_d tends to n. Figure 4 shows how $n - dp_d$ tends to 0 as d increases taking 330 as an example. All the points correspond to values of d such that p_d satisfies Condition 1 with another prime. Note that if $n - dp_d$ is exactly zero then d is a divisor of n such that n/d is a prime.

Then there are two conditions that we use for p_i and q_d to satisfy Condition 1.

Condition 2. *For any integer n to satisfy Condition 1 with p_i and q_d we require that $p_i^{a_i} > n - dq_d$ and $n - dq_d < q_d$.*

When k is larger than $p_i^{a_i}$, we rely on the fact that k is larger than $n - dq_d$ to justify that the binomial coefficient $\binom{n}{k}$ is divisible by q_d using Lucas' Theorem unless if k is a multiple of q_d. However, if $n - dq_d$ were larger than q_d, when writing n in base q_d the inequality $p_i^{a_i} > n - dq_d$ would not hold.

Lemma 7.1. *If $n \geq 30$ and $d < 5$, then $n - dq_d < q_d$.*

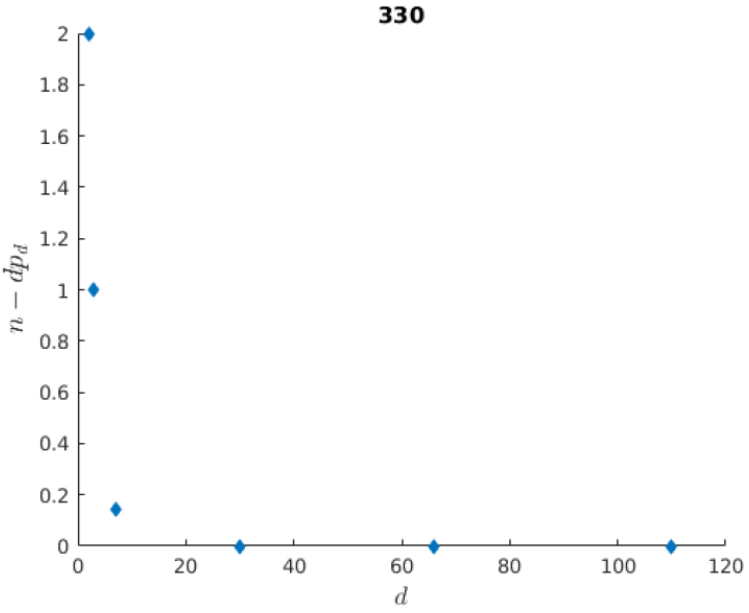


Figure 4: Decrease of $n - dp_d$ for $n = 330$.

Proof. By Lemma 4.2, if $n \geq 25$, $5n/6d < q_d < n/d$. Therefore, $n/6 > n - dq_d$. Now we need to show that $q_d > n - dq_d$. It follows that $n < q_d + dq_d$ and thus $n < q_d(1 + d)$. Using Lemma 4.2,

$$n < \frac{5n(d+1)}{6d} < q_d(1+d).$$

Therefore, $6d < 5d + 5$ and we get that $d < 5$. □

Lemma 7.2. *If $n \geq$ 2,010,882 and $d <$ 16,597, then $n - dq_d < q_d$.*

The proof is the same one as the one for Lemma 7.1, except that by Lemma 4.3, the initial inequality is $16{,}597n/16{,}598d < q_d < n/d$.

Corollary 7.3. *The integer $\lfloor d/2 \rfloor q_d$ is the largest multiple of q_d smaller than or equal to $n/2$.*

Proof. We apply the definition of q_d to obtain that $n \geq dq_d$. Assume, towards a contradiction, that $n > q_d(d+1)$. By Lemmas 7.1 and 7.2, $n - dq_d < q_d$ and therefore $n < q_d(d + 1)$. This contradicts the inequality $n > q_d(d + 1)$. □

7.1 The 3-variation of Condition 1

In Section 5 we proved that many integers that satisfy the inequalities

$$n - q > p_i^{a_i} > n - 2q_2$$

also satisfy Condition 1 with p_i and q_2. Although this does not fully answer the main question of this essay, the proofs explained in Section 5 lead to the results

of this section, which we consider to be relevant. Thus, in this section we prove some cases in which an integer n satisfies the 3-variation of Condition 1 (as stated in Definition 1.2 in the Introduction).

Theorem 7.4. *If an even integer n satisfies the inequality $n - q > p_i^{a_i} > n - 2q_2$ and $p_i \neq 2$, then n satisfies the 3-variation of Condition 1 with p_i, q_2 and any prime that divides $\binom{n}{n/2}$.*

Proof. In Section 5.2 we show that if n satisfies the inequality $n - q > p_i^{a_i} > n - 2q_2$ and p_i is not 2, the only binomial coefficient we could not prove that was divisible by either p_i or q_2 is the central binomial coefficient. Thus, for such n to satisfy the 3-variation of Condition 1 it suffices to add an extra prime that divides the central binomial coefficient. □

Regarding the two highest prime powers of n

For any n, let q be the largest prime smaller than n, let p_j be the prime factor of n such that $p_j^{a_j}$ is the largest prime power of n, and let p_r be the prime factor of n such that $p_r^{a_r}$ is the second largest prime power divisor of n. We then claim the following:

Proposition 7.5. *If $p_j^{a_j} p_r^{a_r} > n/6$, then n satisfies the 3-variation of Condition 1 with p_j, p_r and q.*

Proof. By Lucas' Theorem, for any k such that $1 \leq k \leq p_j^{a_j}$, the binomial coefficient $\binom{n}{k}$ is divisible by p_j. For the same reason, by Lucas' Theorem, for any k such that $n-q < k \leq n/2$ the binomial coefficient $\binom{n}{k}$ is divisible by p_j. Then we need a prime that divides at least the binomial coefficients $\binom{n}{k}$ with $p_j^{a_j} \leq k \leq n - q$ such that k is a multiple of $p_j^{a_j}$. Now take p_r as the third prime such that n might satisfy the 3-variation of Condition 1 with p_j, q and p_r. For the same reasoning, in this interval we only consider the k that are multiples of $p_r^{a_r}$. The only k such that the binomial coefficient $\binom{n}{k}$ is not divisible by either p_j of p_r are those k that are multiples of both $p_j^{a_j}$ and $p_r^{a_r}$. The least k that is multiple of both prime powers is $p_j^{a_j} p_r^{a_r}$. By Lemma 4.2 we know that $n - q < n/6$. Therefore, if $p_j^{a_j} p_r^{a_r} > n/6$, this integer is larger than $n - q$ and hence it is not part of the interval that we are considering. Thus, all the k lying in the interval $p_j^{a_j} \leq k \leq n - q$ are such that the binomial coefficient $\binom{n}{k}$ is divisible by either p_j or p_r. □

Moreover, using the bounds described in Lemma 4.2, we use the primes p_j, q and q_d for n to satisfy the 3-variation of Condition 1.

Proposition 7.6. *Let q_d be the largest prime smaller than n/d. If $q_d > n/6$, then n satisfies Condition 1 with p_j, q and q_d.*

Proof. The prime q fails to divide $\binom{n}{k}$ only if $1 \leq k \leq n - q$. Similarly, by Lucas' Theorem, the prime q_d fails to divide $\binom{n}{k}$ only if $cq_d \leq k \leq cq_d + (n - dq_d)$, where cq_d refers to any positive multiple of q_d. This is because $n - dq_d$ is the last digit of the base q_d representation of n. But because by assumption $q_d > n - p_j$, the intervals $[1, n - q]$ and $[cq_d, cq_d + (n - dq_d)]$ are disjoint. □

8 Bounds on the number of primes needed to satisfy the N-variation of Condition 1

The proofs obtained for the 3-variation of Condition 1 and the inequalities for $n-dq_d$ in Section 7 led us to consider the N-variation of Condition 1, because this is also relevant to the main question of the essay. For each positive integer n, we are interested in the minimum number N of primes such that n satisfies the N-variation of Condition 1. In this section we provide four upper bounds for N. Because in all four bounds N is a function of n, the suitability of each bound depends on n; some bounds may be better for certain values of n.

The proofs of the 3-variation of Condition 1 led my investigations towards finding upper bounds on the minimum number N of primes needed so that we can prove that all positive integers satisfy the N-variation of Condition 1.

8.1 First upper bound with prime factors of n

Claim 8.1. *If n has m different prime factors, then these prime factors satisfy the m-variation of Condition 1.*

Proof. The proof is similar to the one described when n is a product of two prime powers. The smallest integer divisible by all the m prime powers of n is n. The base p representation of all $k < n$ has less zeroes than the base p representation of n for at least one prime factor p of n. Using Lucas' Theorem, Claim 8.1 is proven. □

8.2 Second upper bound with d

Proposition 8.2. *Let q_d be the largest prime smaller than n/d and let $p_i^{a_i}$ be any prime power divisor of n such that $p_i^{a_i} > n - dq_d$. If $p_i^{a_i} > q_d + n - dq_d$, then n satisfies the N-variation of Condition 1 with $N = 2 + \lfloor d/2 \rfloor$.*

For the subsequent proofs we use the following definition:

Definition 8.3. Let cq_d be any multiple of q_d and let β be $n - dq_d$. We call the interval $[cq_d, cq_d + \beta]$ a *dangerous interval*.

Note that for every time that $p_i^{a_i}$ falls into a dangerous interval we need to add an extra prime.

Proof. By Lucas' Theorem all the binomial coefficients $\binom{n}{k}$ are divisible by q_d except if k lies in a dangerous interval. In these dangerous intervals we only consider the integers that are multiples of $p_i^{a_i}$ because if k is not a multiple of $p_i^{a_i}$, then by Lucas' Theorem the binomial coefficient $\binom{n}{k}$ is divisible by p_i. Because $p_i^{a_i} > \beta$ we know that in any dangerous interval there is at most one multiple of $p_i^{a_i}$. This means that the worst case is the one in which there is a multiple of $p_i^{a_i}$ in every dangerous interval until $c \leq \lfloor d/2 \rfloor$. Thus we need at most one extra prime each time that there is a multiple of $p_i^{a_i}$ in a dangerous interval. □

Claim 8.4. *If $d < 5$ and $p_i^{a_i} > q_d + \beta$, then n satisfies Condition 1 with q_d and p_i.*

Proof. If $d < 5$, then $\lfloor d/2 \rfloor$ equals either 1 or 2. If it equals one, then by assumption $p_i^{a_i} > q_d + \beta$, which means that no multiple of $p_i^{a_i}$ falls in any dangerous interval until $n/2$. If d equals 2, then we need to check that $2p_i^{a_i} > 2q_d + \beta$. This means that we want to see that the next multiple of $p_i^{a_i}$ does not fall into the second dangerous interval. The minimum value of $p_i^{a_i}$ such that our assumption $p_i^{a_i} > q_d + \beta$ holds is $q_d + \beta + 1$. The next multiple of $q_d + \beta + 1$ is $2q_d + 2\beta + 2$. This last expression is greater than $2q_d + \beta$, which means that $2p_i^{a_i}$ does not fall into the second dangerous interval. □

8.3 Third upper bound

In this subsection we consider the generalization of the cases that have been discussed so far. Let d be a natural number and let q_d be the largest prime number smaller or equal to n/d. Let β denote $n - dq_d$, let $p_i^{a_i}$ be any prime power divisor of n, and let $\gamma = p_i^{a_i} - cq_d$. In Sections 8.3 and 8.4 we do not consider the cases in which $q_d = p_i$ because the proofs hold by taking any other prime factor of n that is not p_i.

Theorem 8.5. *For all $c \geq 0$, n satisfies the N-variation of Condition 1 with*

$$N = 2 + \left\lfloor \frac{k\gamma q_d - (c-1)}{\gamma q_d} \right\rfloor \beta,$$

where $k = \left\lfloor \dfrac{d}{2q_d\gamma} \right\rfloor$.

Proof. We first consider the case in which $p_i^{a_i} = q_d + \gamma$ and $\gamma \leq \beta$. This means that $p_i^{a_i}$ falls in the first dangerous interval. Any subsequent multiple of $p_i^{a_i}$ is of the form $rp_i^{a_i} = rq_d + r\gamma$. Note that we only need to analyze $r\gamma$ because this is what determines if $p_i^{a_i}$ falls in a dangerous interval.

Lemma 8.6. *The prime power divisor $p_i^{a_i}$ falls into a dangerous interval if and only if $r\gamma \pmod{q_d} \leq \beta$.*

The proof of Lemma 8.6 comes from the definition of a dangerous interval (see Definition 8.3). Now consider all the possible values of $r\gamma$ modulo q_d from γ until γq_d. Note the following:

Remark 8.7. *The numbers γ and q_d are always coprime.*

For the proof of the remark it suffices to see that q_d is a prime number. This means that all the numbers from 1 to $q_d - 1$ appear exactly once in the interval $[\gamma, \gamma q_d)$. Therefore, by Lemma 8.6 the number of integers that fall into a dangerous interval are those such that $r\gamma \pmod{q_d} \leq \beta$. By Remark 8.7 we know there are only β such integers in the interval $[\gamma, \gamma q_d)$. Thus, if $\gamma q_d > d/2$, we only need $2 + \beta$ primes. We add 2 to β because we also need to count q_d and p_i. Note that this is an upper bound and therefore in some cases several of the primes that we use for the dangerous intervals are repeated.

Now we consider the general case in which $p_i^{a_i} = cq_d + \gamma$. We need to count the multiples of γq_d from cq_d until $k\gamma q_d$ (k has the same definition as in Theorem 7.1). This gives us the bound stated in Theorem 8.5. □

Note that, in Theorem 8.5, γ cannot be 0 because otherwise by definition p_i would be equal to q_d. This is a case that we are not considering (see the beginning of Section 8.3).

8.4 Fourth upper bound with Diophantine equations

We consider the Diophantine equation $p_i^{a_i}k_1 - q_d\alpha = \delta$, where $0 \leq \delta \leq \beta$. Let $x = k_1$ and let $y = \alpha$. The general solutions of these Diophantine equation depending on the particular solutions x_1 and y_1 are well-known:

$$x = x_1 - rq_d$$
$$y = y_1 + rp_i^{a_i}$$

Let $\hat{y}(\delta)$ denote the largest $y \leq \lfloor d/2 \rfloor$ depending on δ. Note that for all $y_1(\delta)$ we can add or subtract a certain number of $p_i^{a_i}$ until we reach $\hat{y}(\delta)$.

Theorem 8.8. *All integers n satisfy the N-variation of Condition 1 with*

$$N = 2 + \sum_{\delta=0}^{\beta} \left\lfloor \frac{\hat{y}(\delta)}{p_i^{a_i}} \right\rfloor \leq 2 + (\beta + 1) \left\lfloor \frac{d}{2p_i^{a_i}} \right\rfloor.$$

Proof. Note that the solutions of the Diophantine equation correspond to all the cases in which a multiple of $p_i^{a_i}$ falls in some dangerous interval. It is known that a Diophantine equation $ax + by = c$ has infinitely many solutions if $\gcd(a, b)$ divides c. Therefore, for all δ such that $0 \leq \delta \leq \beta$ there exists a particular solution $y_1(\delta)$ for y in Equation 6 because $\gcd(p_i^{a_i}, q_d) = 1$ (recall that we do not consider the case in which $p_i = q_d$). Thus, for each $\hat{y}(\delta)$ we count the number of multiples of $p_i^{a_i}$ in the interval $[1, \hat{y}(\delta)]$. This is the number of times that $p_i^{a_i}$ falls into a dangerous interval and hence we need to add an extra prime. We also add 2 to count p_d and p_i. Moreover, note that by definition $\hat{y}(\delta) \leq \lfloor d/2 \rfloor$. This gives us the expression stated in Theorem 8.8. □

9 Computational results

In order to obtain more information about which primes make n satisfy Condition 1 we wrote some C++ programs. The results are presented in this section.

9.1 When we fix a prime

In the original article of Shareshian and Woodroofe [29], the authors computed the percentage of integers below 1,000,000 that satisfy Condition 1 if p_1 is fixed to be 2, and they found a percentage of 86.7%. We compute the percentage of integers until 10,000 that satisfy Condition 1 fixing one prime to be not only 2 but also 3, 5, 7 and 11. Table 2 shows the number of integers below 10,000 that do not satisfy Condition 1 fixing one prime to be 2, 3, 5, 7 and 11 respectively. It also shows the percentage of integers satisfying Condition 1 fixing each prime. Figure 5 shows the percentage of integers until 10,000 that satisfy Condition 1 depending on the fixed prime.

Fixed prime	2	3	5	7	11
Number of integers not satisfying 1	1144	1633	2626	3259	4180
Percentage of integers satisfying 1	88.56%	83.67%	73.74%	67.41%	58.20%

Table 2: Number of integers that do not satisfy Condition 1 and percentage of integers that do satisfy Condition 1 fixing one prime until 10,000.

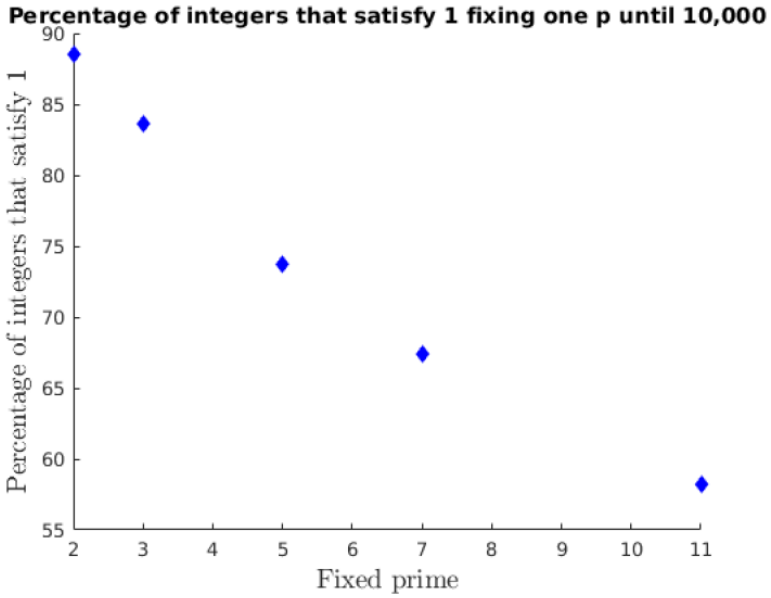


Figure 5: Percentage of integers until 10,000 that satisfy Condition 1 fixing one prime to be 2, 3, 5, 7 and 11 respectively.

9.2 How many pairs of primes satisfy Condition 1

Given a positive integer n, multiple pairs of primes p_1 and p_2 can satisfy Condition 1. We have found computationally all the possible pairs of primes that satisfy Condition 1 with a given $n \leq 3{,}000$. This findings helped us conjecture and then prove Theorem 3.4. Figure 6 shows the data for n up to 3,000. We note four main tendencies. The one with the greatest slope corresponds to the one formed with prime numbers and prime powers. This is explained by Proposition 3.1. Because only one prime is needed to satisfy the 1-variation of Condition 1 if n is a prime power, the other prime can be any prime smaller than n. Therefore, this first tendency follows the function $f(n) = n/\log n$ disregarding the prime powers [16]. The second greatest slope is formed with even numbers that satisfy Condition 1 with one prime being 2. The third one is formed by numbers satisfying Condition 1 with one of the primes being 3 and the following one with numbers that satisfy Condition 1 with one prime being 5.

In order to fit a function for each curve, we approximated the function $n/\log n$ for each branch using Matlab, and we obtained the following functions:

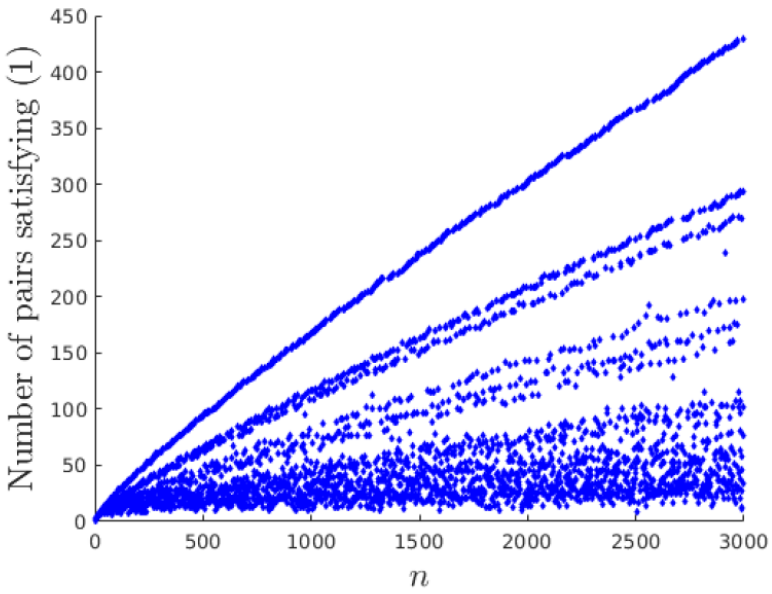


Figure 6: Number of pairs of primes that satisfy Condition 1 depending on the integer n until 3,000.

$$\text{First branch: } \frac{0.97n^{0.96}}{(\log n)^{0.75}} \qquad \text{Second branch: } \frac{0.80n^{0.96}}{(\log n)^{0.84}}$$

$$\text{Third branch: } \frac{3.30n^{1.14}}{(\log n)^{2.27}} \qquad \text{Fourth branch: } \frac{35.48n^{1.47}}{(\log n)^{4.81}}$$

Figure 7 shows a plot of each separate branch with its corresponding curve.

10 Multinomials

We also consider a generalization of Condition 1 to multinomials. We investigate the following condition that some integer n might satisfy:

Condition 3. *For a given fixed integer m there exist primes p_1 and p_2 such that whenever $k_1 + \cdots + k_m = n$ for $1 \leq k_i \leq n-1$, $\binom{n}{k_1,k_2,\ldots,k_m}$ is divisible by either p_1 or p_2.*

A very natural question follows:

Question 10.1. *Does Condition 3 hold for all positive integers n?*

Here we show that Condition 1 implies Condition 3. We claim the following:

Proposition 10.2. *If n satisfies Condition 1 with p_1 and p_2, then n also satisfies Condition 3 with these two primes and any $m \leq n$.*

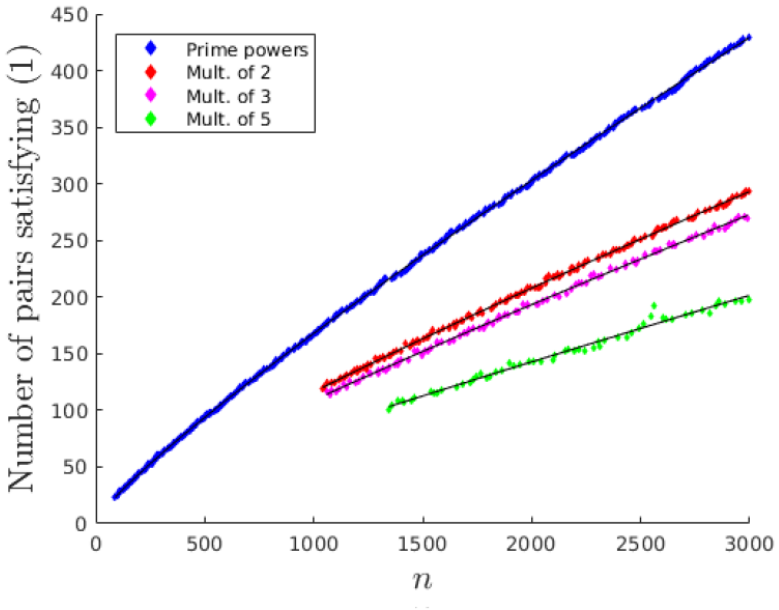


Figure 7: The four branches of Figure 6 separated and fitted with a curve.

Proof. We assume that p_1 and p_2 satisfy Condition 1 for a given n. We then take the multinomial

$$\binom{n}{k_1, k_2, \ldots, k_m} = \frac{n!}{k_1! k_2! \cdots k_m!}$$

with the same n and any $m \leq n$. We see that we can decompose the multinomial into a product of m binomials:

$$\frac{n!}{k_1! k_2! \cdots k_m!} = \frac{n(n-1)\cdots(n-k_1+1)}{k_1!}\cdot$$

$$\frac{(n-k_1)(n-k_1-1)\cdots(n-k_1-k_2+1)}{k_2!} \cdots \frac{(k_{m-1}+k_m)(k_{m-1}+k_m-1)\cdots 1}{(k_{m-1}! k_m!}$$

$$= \binom{n}{k_1}\binom{n-k_1-1}{k_2}\cdots\binom{k_{m-1}+k_m}{k_m}.$$

Because by assumption $\binom{m}{k_1}$ is divisible by either p_1 or p_2, the previous multinomial coefficient is also divisible by at least one of them. This decomposition can be used for any m and the first binomial coefficient can be $\binom{n}{k_i}$, k_i being any of the k in the denominator. □

Therefore, if Condition 1 is proven for binomial coefficients, then it automatically holds for multinomial coefficients.

11 Conclusions

In this work we have obtained results that significantly contribute to the unsolved conjecture that motivated our research (see Condition 1 in the Introduction), which was proposed in a recent article by Shareshian and Woodroofe [29]. We have found many instances in which the conjecture holds, namely a positive integer n satisfies Condition 1 at least in the following cases:

- When n is a prime power.
- When n is a prime power plus one.
- When n is a product of two prime powers.
- When n satisfies the inequality $n - q < p_i^{a_i}$, where q denotes the largest prime smaller than n and $p_i^{a_i}$ is any prime power factor of n.
- When n satisfies a similar inequality regarding the largest prime q_2 smaller than $n/2$.

Using these ideas, we have also found some cases in which if $2n$ satisfies Condition 1 then so does n, and we have used prime gap conjectures by Cramér, Oppermann and Riemann to prove that every integer n has infinitely many multiples that satisfy Condition 1. Moreover, we have considered variations of Condition 1 involving more than two primes and we have provided four different upper bounds on the minimum number of primes N needed in order to prove that all positive integers satisfy our N-variation.

We have written several C++ programs which have allowed us to observe what percentage of integers satisfy Condition 1 if we fix one prime, and also to obtain all pairs of primes that make a given n satisfy Condition 1. Finally, we have generalized Condition 1 to multinomials and have proven that if Condition 1 holds for binomials, then it also holds for multinomials.

After having obtained all these research results, we have analyzed how much we have contributed to the open problem addressed in this work. Up to 1,000,000, there are less than 50 numbers that do not fit into any of the cases that we have solved. We consider this to be a very substantial outcome. Moreover, our proofs concerning prime gap conjectures potentially have stronger implications, as we believe that we are very close to proving that all integers larger than a fixed constant satisfy Condition 1.

Also, our inequalities $n - dq_d < p_i^{a_i}$ for various values of d, where q_d denotes the largest prime smaller than n/d and $p_i^{a_i}$ is the largest prime power divisor of n, can also lead to better results, and we are convinced that further research in this direction would solve even more cases.

In conclusion, our proofs substantially contribute to a possible solution to the open problem proposed in [29], which has been the main objective of this essay, and we believe that we found ideas that could be studied in greater detail and lead to sharper results.

12 Appendix

12.1 Sequences of integers that do not satisfy the inequality for $n - dp_d$

In Section 7 we mentioned that the set of integers that do not satisfy the inequality for $n - dp_d$ becomes smaller when d increases. In this appendix we display the first terms of the sequence of integers that do not satisfy the inequality $n - dp_d < p_i^{a_i}$ when d equals 1, 2, 3, 4 and 5. The On-Line Encyclopedia of Integer Sequences has published our sequence in the cases when d equals 1 and when d equals 2. References are omitted in this anonymous versions of the essay.

When $d = 1$: 126, 210, 330, 630, 1144, 1360, 2520, 2574, 2992, 3432, 3960, 4199, 4620, 5544, 5610, 5775, 5980, 6006, 6930, 7280, 8008, 8415, 9576, 10005, 10032, 12870, 12880, 13090, 14280, 14586, 15708, 15725, 16182, 17290, 18480, 18837, 19635, 19656, 20475, 20592, 22610, 24310, 25296, 25300, 25520, 25840, 27170, 27720, 27846, 28272, 28275, 29716, 30628, 31416, 31450, 31464, 31465, 32292, 34086, 34100, 34580, 35568, 35650, 35670, 35728, 36036, 36432, 37944, 37950.

When $d = 2$: 3432, 5980, 12870, 12880, 13090, 14280, 14586, 20475, 28272, 28275, 31416, 31450, 34580, 35650, 39270, 45045, 45220, 72072, 76076, 96135, 97812, 106080, 106590, 120120, 121992, 125580, 132804, 139230, 173420, 181350, 185640, 191400, 195624, 202275, 203112, 215050, 216315, 222768, 232254, 240240, 266475, 271320, 291720, 293930, 336490, 338086, 350064, 351120, 358150, 371280, 388455, 408595, 421600, 430236, 447051, 447304, 471240, 480624.

When $d = 3$: 3432, 31416, 34580, 35650, 39270, 96135, 121992, 125580, 139230, 215050, 222768, 291720, 358150, 388455, 471240, 513590, 516120, 542640, 569296, 638001, 720720, 813960, 875160, 891480, 969969, 1046175, 1113840, 1153680, 1227600, 1343160, 1448655, 1557192, 1575860, 1745424, 1908816.

12.2 C++ code for finding all the possible pairs

Here we provide the C++ code that we used to find all the possible pairs of primes that satisfy Condition 1 for each integer. This code has been used to plot Figure 6.

```cpp
#include<iostream>
#include<vector>
#include<cmath>
#include<set>
#include<string>
#include<sstream>
#include <bits/stdc++.h>
#include "BigIntegerLibrary.hh"

using namespace std;

vector <bool> v;
vector <unsigned long long int> primers;
vector <vector <unsigned long long int> > factors;
vector <vector <unsigned long long int> > factorsrepet;
vector <vector <BigInteger> > bino;

string int2string(int n){
    stringstream s;
    s << n;
    return(s.str());
}

void garbell(){
    v[0]=false;
    v[1]=false;
    factors[0].push_back(0);
    factors[1].push_back(1);
    for(unsigned long long int i=2; i<v.size(); i++){
        if(v[i]){
            primers.push_back(i);
            factors[i].push_back(i);
            for(unsigned long long int h=2; h*i<v.size(); h++){
                v[i*h] = 0;
                factors[i*h].push_back(i);
            }
        }
    }
```

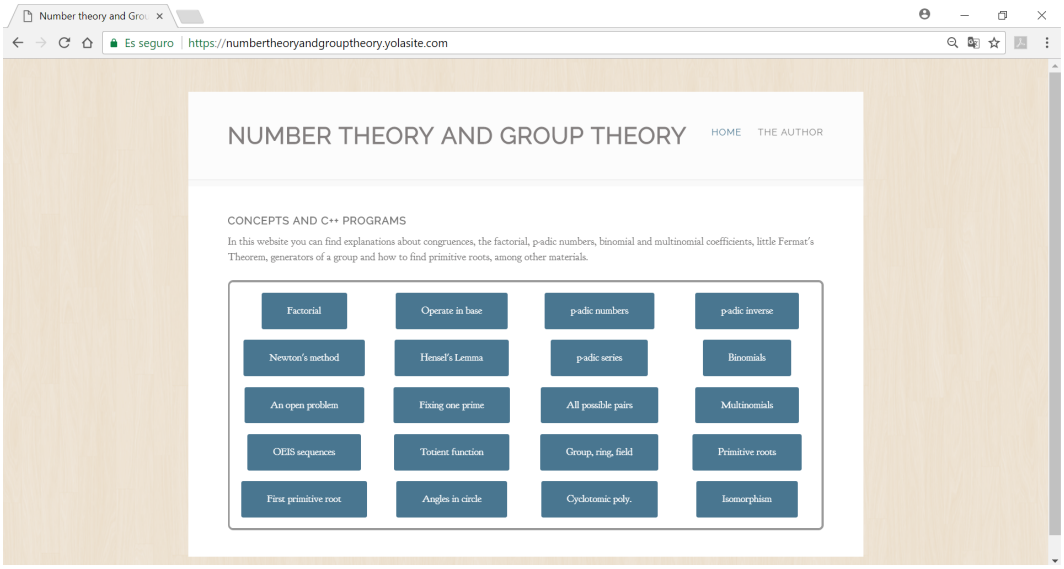
```cpp
int main(){
    ofstream cout("HowManyPrimes.txt");
    int n;
    cin >> n;
    v = vector <bool> (n, true);
    primers = vector <unsigned long long int> ();
    factors = vector <vector <unsigned long long int>> (n);
    factorsrepet = vector <vector <unsigned long long int>> (n);
    garbell();
    bino = vector <vector <BigInteger> > (n);
    bino[0].push_back(1);
    bino[1].push_back(1);
    bino[1].push_back(1);
    for(unsigned long long int i=2; i<n; i++) {
        //cout<<endl<<endl<<i<<" ";
        bino[i].push_back(1);
        for(unsigned long long int j=1; j<i; j++){
            bino[i].push_back(bino[i-1][j-1]+bino[i-1][j]);
            //cout<<bino[i][j]<<" ";
        }
        bino[i].push_back(1);
    }
    for(unsigned long long int i=2; i<n; i++) {
        cout<<"n =      "<<i;
        unsigned long long int aa = 0;
        unsigned long long int bb = 1;
        unsigned long long int p1 = primers[aa];
        unsigned long long int p2 = primers[bb];
        unsigned long long int res = 0;
        int howmany = 0;
        while(res==0){
                string pp1 = int2string(p1);
                BigInteger ppp1 =stringToBigInteger(pp1);
                string pp2= int2string(p2);
                BigInteger ppp2 =stringToBigInteger(pp2);
                for(unsigned long long int q=1; q<=i/2; q++){
```

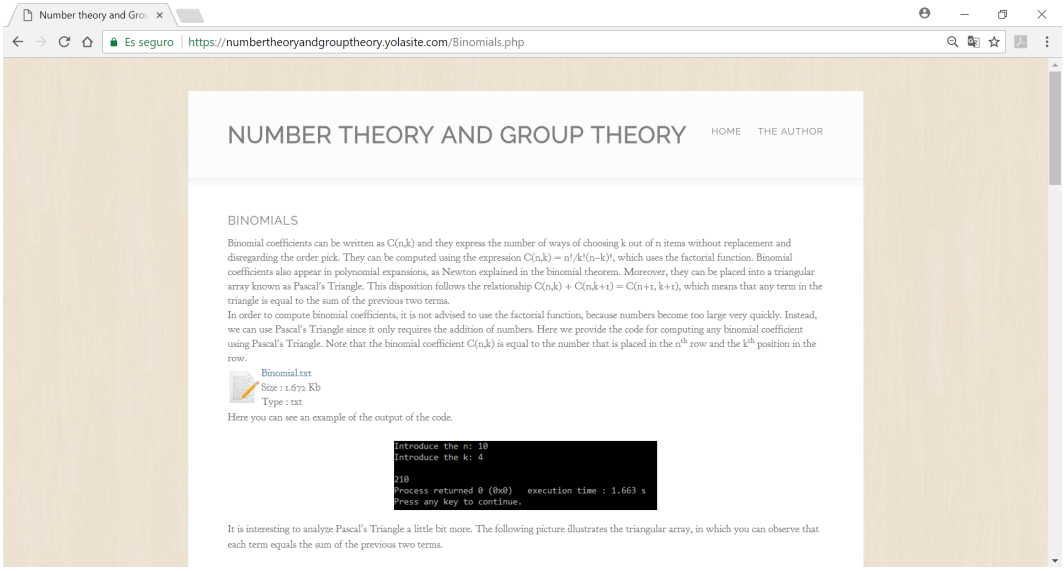
```cpp
                    if((bino[i][q]%ppp1!=0)and(bino[i][q]%ppp2!=0)){
                        res = 1;
                        break;
                    }
                }
            if(res==0){
                cout<<"PRIMES: "<<ppp1<<"       "<<ppp2<<endl;
                howmany++;
            }
            if(((bb+1==primers.size())and(aa+1==primers.size()-1))or(primers[aa+1]==i)){
                res=1;
            }
            else{
            if((bb+1==primers.size())or(primers[bb+1]>i)){
                aa++;
                p1 = primers[aa];
                bb = aa+1;
                p2 = primers[bb];
                res = 0;
            }
            else{
                bb++;
                p2 = primers[bb];
                res = 0;
            }
            }
    }
    cout<<"             "<<howmany<<endl;
    }
}
```

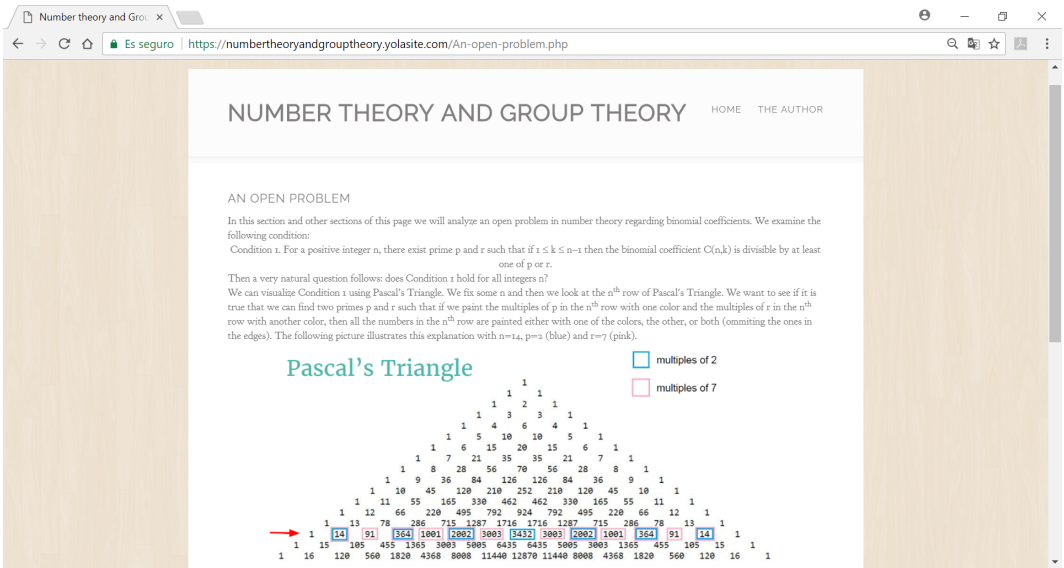
The code for the data on how many integers satisfy Condition 1 if we fix one prime is quite similar and is therefore not included.

12.3 Webpage about this problem

As explained in the Introduction, we have created a webpage in which all the concepts and results of this work are explained. From this website it is possible to download the C++ codes that we have used. The website, entitled *Number Theory and Group Theory*, also includes other concepts and programs regarding number theory and group theory. We wanted all these C++ codes to stay available to everyone interested, because they are potentially useful mathematical tools for anyone who wishes to continue investigating this problem or any related problems. The URL of the website is `https://numbertheoryandgrouptheory.yolasite.com/`.


Number theory and Grou
Es seguro | https://numbertheoryandgrouptheory.yolasite.com
NUMBER THEORY AND GROUP THEORY
HOME
THE AUTHOR
CONCEPTS AND C++ PROGRAMS
In this website you can find explanations about congruences, the factorial, p-adic numbers, binomial and multinomial coefficients, little Fermat's Theorem, generators of a group and how to find primitive roots, among other materials.
Factorial
Operate in base
p-adic numbers
p-adic inverse
Newton's method
Hensel's Lemma
p-adic series
Binomials
An open problem
Fixing one prime
All possible pairs
Multinomials
OEIS sequences
Totient function
Group, ring, field
Primitive roots
First primitive root
Angles in circle
Cyclotomic poly.
Isomorphism


Number theory and Grou
Es seguro | https://numbertheoryandgrouptheory.yolasite.com/Binomials.php
NUMBER THEORY AND GROUP THEORY
HOME
THE AUTHOR
BINOMIALS
Binomial coefficients can be written as C(n,k) and they express the number of ways of choosing k out of n items without replacement and disregarding the order pick. They can be computed using the expression C(n,k) = n!/k!(n−k)!, which uses the factorial function. Binomial coefficients also appear in polynomial expansions, as Newton explained in the binomial theorem. Moreover, they can be placed into a triangular array known as Pascal's Triangle. This disposition follows the relationship C(n,k) + C(n,k+1) = C(n+1, k+1), which means that any term in the triangle is equal to the sum of the previous two terms.
In order to compute binomial coefficients, it is not advised to use the factorial function, because numbers become too large very quickly. Instead, we can use Pascal's Triangle since it only requires the addition of numbers. Here we provide the code for computing any binomial coefficient using Pascal's Triangle. Note that the binomial coefficient C(n,k) is equal to the number that is placed in the n^th row and the k^th position in the row.
Binomial.txt
Size : 1.672 Kb
Type : txt
Here you can see an example of the output of the code.
Introduce the n: 10
Introduce the k: 4
210
Process returned 0 (0x0) execution time : 1.663 s
Press any key to continue.
It is interesting to analyze Pascal's Triangle a little bit more. The following picture illustrates the triangular array, in which you can observe that each term equals the sum of the previous two terms.


Number theory and Grou
Es seguro | https://numbertheoryandgrouptheory.yolasite.com/An-open-problem.php
NUMBER THEORY AND GROUP THEORY
HOME
THE AUTHOR
AN OPEN PROBLEM
In this section and other sections of this page we will analyze an open problem in number theory regarding binomial coefficients. We examine the following condition:
Condition 1. For a positive integer n, there exist prime p and r such that if 1 ≤ k ≤ n−1 then the binomial coefficient C(n,k) is divisible by at least one of p or r.
Then a very natural question follows: does Condition 1 hold for all integers n?
We can visualize Condition 1 using Pascal's Triangle. We fix some n and then we look at the n^th row of Pascal's Triangle. We want to see if it is true that we can find two primes p and r such that if we paint the multiples of p in the n^th row with one color and the multiples of r in the n^th row with another color, then all the numbers in the n^th row are painted either with one of the colors, the other, or both (ommiting the ones in the edges). The following picture illustrates this explanation with n=14, p=2 (blue) and r=7 (pink).
Pascal's Triangle
multiples of 2
multiples of 7

Number theory and Grou ×

Es seguro | https://numbertheoryandgrouptheory.yolasite.com/Fixing-one-prime.php

NUMBER THEORY AND GROUP THEORY

HOME THE AUTHOR

FIXING ONE PRIME

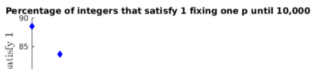
Regarding the problem explained in the section "An open problem", we compute the percentage of integers until 10,000 that satisfy Condition 1 fixing one prime to be 2, 3, 5, 7 and 11. Here we provide the code that returns how many integers smaller than n do not satisfy Condition 1 if we fix one prime. It is possible to change the fixed prime, named aa in the code, by just changing it in the code (note that if we want one prime to be 2, then aa has to be 0 because it is the 0^{th} prime. 3 is the 1^{th} prime, and so on. Also, we use the BigInt library for large numbers that can be downloaded in the following page: https://mattmccutchen.net/bigint/.

fixingp.txt
Size : 2.98 Kb
Type : txt

The following table shows the number of integers below 10,000 that do not satisfy Condition 1 fixing one prime to be 2, 3, 5, 7 and 11 respectively. It also shows the percentage of integers satisfying Condition 1 fixing each prime.

Prime	2	3	5	7	11
Number of integers not satisfying 1	1144	1633	2626	3259	4180
Percentage of integers satisfying 1	88.56%	83.67%	73.74%	67.41%	58.20%

The following figure shows the percentage of integers until 10,000 that satisfy Condition 1 depending on the fixed prime.



Number theory and Grou ×

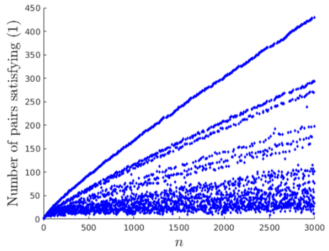
Es seguro | https://numbertheoryandgrouptheory.yolasite.com/All-possible-pairs.php

NUMBER THEORY AND GROUP THEORY

HOME THE AUTHOR

ALL POSSIBLE PAIRS

In this section we study given n how many pairs of primes make n satisfy Condition 1. We have found computationally all the possible pairs of primes that satisfy Condition 1 with a given $n \leq 3000$. The following figure shows the data for n up to 3,000.



We note four main tendencies. The one with the greatest slope corresponds to the one formed with prime numbers and prime powers. This is explained with the first proposition explained in the section "An open problem". Because only one prime is needed to satisfy Condition 1, the

Number theory and Grou ×

Es seguro | https://numbertheoryandgrouptheory.yolasite.com/Multinomials.php

NUMBER THEORY AND GROUP THEORY

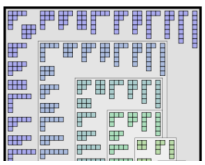
HOME THE AUTHOR

MULTINOMIALS

In this section we generalize the Condition 1 explained in the section "An open problem" to the multinomials. The multinomial $(k_1, k_2, \ldots k_m)$ is defined to be equal to $(k_1+k_2+\ldots+k_m)/(k_1!k_2!\ldots k_m!)$. Therefore, given n, if we want to compute all the possible multinomial coefficients with n in the numerator we need to introduce the concept of partitions. Imagine we want n to be 5. In how many ways can we add 1?

1+1+1+1+1 (m=5)
1+1+1+2 (m=4)
1+2+2 (m=3)
; 1+1+3 (m=3)
2+3 (m=2)
1+4 (m=2)
5 (m=1)

The following picture illustrates the number of partitions of n for n=1, 2, 3, 4, 5, 6, 7, 8.



Part II

p-Adic Series Containing the Factorial Function

Is it true that the sum of the factorial series $\sum n!$ is a p-adic irrational?

1 Introduction

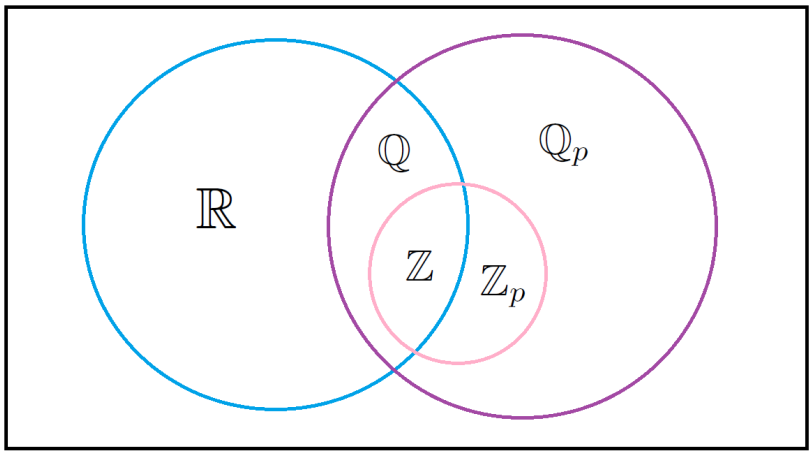
The p-adic numbers (where p denotes a prime) were introduced by Kurt Hensel in 1897 and they are a fundamental part of number theory [26]. For instance, the famous proof of Fermat's Last Theorem used p-adic numbers. Apart from number theory, p-adic numbers also appear in algebraic geometry, representation theory, algebraic dynamics, cryptography, and many other fields of mathematics. They have also found applications in physics (including p-adic quantum mechanics [9]), and researchers believe that in the future many other disciplines will benefit from the properties of p-adic numbers. This work focuses on p-adic analysis, which is a quite recent technique in mathematics. The applications of p-adic analysis are wide and have turned out to be a very powerful tool.

The p-adic number system for a given prime p extends the integer numbers [12]. Given a natural number n, if we choose a fixed prime p then we can express n in the form

$$n = \sum_{i=0}^{k} a_i p^i, \tag{1}$$

where each a_i is a natural number between 0 and $p-1$. Then we say that $\sum_{i=0}^{k} a_i p^i$ is the *p-adic expansion* of n. In traditional arithmetic, if n is an integer then this can be understood as the expression of n in base p. The system of p-adic numbers is constructed by allowing expressions such as (1) to be infinite sums, that is, formal series on powers of p. Infinite p-adic expansions play a role similar to infinite decimal expansions of real numbers. Furthermore, we can also talk about rationality of p-adic expansions: as in the case of real numbers, a p-adic expansion represents a rational number if and only if it is periodic, as explained in Section 4.2.

It is important to distinguish between the set $\mathbb{Z}_p$ of p-adic integers and the set $\mathbb{Q}_p$ of p-adic numbers because they are defined differently: $\mathbb{Z}_p$ is a ring whereas $\mathbb{Q}_p$ is a field and contains the field $\mathbb{Q}$ of rational numbers. Both rings and fields are algebraic structures which extend the concept of a group [27]. The following diagram relates the sets of numbers $\mathbb{Z}$, $\mathbb{Z}_p$, $\mathbb{Q}$, $\mathbb{Q}_p$ and $\mathbb{R}$:



The difference between a ring and a group is that a ring is defined as a set of elements with two operations (addition and multiplication) instead of just one. In the case of p-adic integers, we can add, subtract or multiply. Moreover, the difference between a field and a ring is that a field contains inverses with respect to the second operation of all non-zero elements. Therefore, in $\mathbb{Q}_p$ we can add, subtract, multiply or divide. In the ring $\mathbb{Z}_p$ it is also possible to divide by non-zero integers, except for powers of p.

A feature of p-adic integers is a concept of distance, which is formally similar but very different from the distance between real numbers. In the real numbers, we say that 2 and 3 are closer to each other than 2 and 10 because $|3-2| < |10-2|$. However, this is not how metric is defined in p-adic analysis. In $\mathbb{Z}_p$ we say that two numbers x and y are close if $x-y$ is divisible by a high power of p. The precise definition, which involves the concept of p-adic absolute value, is detailed in Section 3.2. This metric extends to $\mathbb{Q}_p$ and has unique characteristics when it comes to convergence of p-adic series.

In this work we focus on the series $\sum_{n=0}^{\infty} n!$. This series converges in $\mathbb{Z}_p$ for all p, but the question whether its value is rational or irrational is an open problem. It is believed to be irrational for all p, yet there is no known proof [28].

One of our main results is that, if we replace $n!$ by a suitable p-adic approximation (namely, the highest power of p dividing $n!$) then the resulting series converges to an irrational number for all p. The idea of replacing $n!$ by a p-adic approximation which is computable in a non-recursive way is reminiscent to Stirling's formula [23]:

$$n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}.$$

The difficulty about computing $n!$ for large values of n is that it has to be done recursively, and this makes it a very slow process. However, Stirling's formula provides a direct way to estimate $n!$.

In this work we also study the convergence of series of the form $\sum_{n=0}^{\infty} n^k(n+m)!$ for arbitrary values of k and m. We conjecture that such a series only converges to an integer for $k=2$, $m=1$, and for $k=5$, $m=1$. These two cases are mentioned without further comments in [28], were the following values are given:

$$\sum_{n=0}^{\infty} n^2(n+1)! = 2; \qquad \sum_{n=0}^{\infty} n^5(n+1)! = 26.$$

We describe a method to compute the value of each series $\sum_{n=0}^{\infty} n^k(n+m)!$ in terms of $\alpha = \sum_{n=1}^{\infty} n!$, extending results from [9], and obtain that

$$\sum_{n=0}^{\infty} n^k(n+m)! = x\alpha + y$$

where x and y are integers depending on k and m. We study the coefficient x and observe that, for $m=1$ and $m=-1$, the values of x are cyclic for consecutive values of k if they are reduced modulo a power of 2, or a power of 3, or a power of 6, and only in these cases. We then use this pattern to infer some cases in which the series $\sum_{n=0}^{\infty} n^k(n+m)!$ cannot converge to an integer since $x \neq 0$.

In Section 2 we collect some properties of p-adic integers and explain how to compute p-adic expansions manually. We then explain a recursive way to do so,

using Hensel's Lemma, which is introduced with Newton's Method due to their similarities. In Section 3 we define the p-adic valuation and relate it to convergence of series of p-adic numbers. In Section 4 we study the rationality of p-adic series, provide a p-adic approximation of $\sum n!$ and prove its irrationality. In Section 5 we discuss the irrationality of $\sum n!$ and then in Section 6 we explain how to compute the convergence of the series of the form $\sum n^k(n+m)!$ and prove a main result in which $\sum n^k(n+1)!$ cannot converge to an integer. Finally, in Section 7 we analyze these convergences modulo powers of primes.

2 Calculating with p-adic numbers

2.1 p-Adic expansions of roots of polynomials

In this section we explain how to compute p-adic expansions of roots of polynomials by hand. The first step in computing a p-adic expansion, which is of the form $a_0 + a_1p + a_2p^2 + \cdots$ with $0 \leq a_i < p$ for all i, is to find a_0. In order to do so for a root of a polynomial $P(x)$, it is necessary to find a value of x for which $P(x)$ is congruent to 0 modulo p. The claim that a number a is congruent to b modulo n means that a and b yield the same remainder when we divide them by n. This is denoted by $a \equiv b \pmod{n}$.

Therefore, in order to start a p-adic expansion of a root of a polynomial $P(x)$, we need to assure that there exists at least one x such that $P(x) \equiv 0 \pmod{p}$. We first observe the following fact about linear equations:

Claim 2.1. *For all a and b with $a \not\equiv 0 \pmod{p}$ there exists a unique x such that $ax + b \equiv 0 \pmod{p}$.*

Proof. Take the equation

$$ax + b \equiv 0 \pmod{p},$$

which can be rewritten as

$$ax - py = b.$$

This last expression is indeed a Diophantine equation since it is linear and there are two variables [11]. By assumption, $\gcd(a, p) = 1$. The necessary condition for a linear Diophantine equation to have infinite solutions is that b be a multiple of $\gcd(a, p)$. Clearly, b is a multiple of 1, and hence this equation has infinite solutions. Once we find a base solution x_0 and y_0 (both smaller than p), we can express the general solution [11] as

$$x = x_0 + \frac{kp}{\gcd(a,p)}; \qquad y = y_0 - \frac{ka}{\gcd(a,p)}.$$

If we add kp to the base solution x_0, then x becomes larger than p except when $k = 0$. Since x has to be smaller than p, it follows that the solution is x_0 and it is unique. □

We now explain a method to compute p-adic expansions of roots of any polynomial $P(x)$, but we are going to give first an example using the quadratic equation $x^2 = 5$. Note that in this case it is not true that we can find x_0 for every p. In the example $x^2 = 5$, we cannot find any root in $\mathbb{Z}_p$ for $p = 7$, because by inspection there is no x_0 such that $x_0^2 \equiv 5 \pmod 7$. However, x_0 does exist if $p = 11$, and the two solutions are $x_0 = 4$ and $x_0 = 7$. Note that 7 is the opposite of 4 modulo 11 with respect to the sum, since $7 + 4 = 11$. Then we start working in $\mathbb{Z}_{11}$ and take x_0 to be 4. We denote a solution of $x^2 = 5$ by α. Thus α is of the following form with $p = 11$:

$$\alpha = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots .$$

We want α^2 to be 5 and hence

$$5 = \alpha^2 = (a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots)(a_0 + a_1 p + a_2 p^2 + a_3 p^3 + \cdots).$$

If we multiply we obtain the following expression:

$$\alpha^2 = a_0^2 + (2a_0 a_1)p + (2a_0 a_2 + a_1^2)p^2 + (2a_0 a_3)p^3 + (2a_0 a_4 + 2a_1 a_3 + a_2^2)p^4 + \cdots .$$

All parentheses need to be congruent to 0 modulo 11. Also, for each occurrence of 11 in one parenthesis there is one carry (similarly as when we add in base 10). We already know that a_0 equals 4 and therefore

$$a_0^2 = 16 = 5 + 11.$$

We carry one to the next parenthesis, which needs to be congruent to 0 modulo 11:

$$2a_0 a_1 + 1 \equiv 0 \pmod{11}.$$

By substituting a_0 we find a_1:

$$8a_1 + 1 \equiv 0 \pmod{11}; \qquad 8a_1 \equiv -1 \equiv 10 \pmod{11}.$$

By inspection we see that a_1 equals 4. If we keep repeating this process we find the first terms of the 11-adic expansion of α, which is

$$\alpha = 4 + 4 \cdot 11 + 10 \cdot 11^2 + 4 \cdot 11^3 + 0 \cdot 11^4 + \cdots .$$

With this method the p-adic expansion of a root of any polynomial can be found, provided that the first digit a_0 exists.

2.2 *p*-Adic inverses

We proceed to explain how a p-adic inverse with respect to multiplication can be found. This is a number of the form $1/n$ evaluated in $\mathbb{Z}_p$, assuming that p does not divide n. Take the example of $1/7$ evaluated in $\mathbb{Z}_{11}$. This can be rewritten as

$$7x \equiv 1 \pmod{11}.$$

Here we substitute x with the 11-adic expansion

$$7(a_0 + a_1 11 + a_2 11^2 + a_3 11^3 + \cdots) = 1.$$

Therefore

$$7a_0 + 7a_1 11 + 7a_2 11^2 + 7a_3 11^3 + \cdots = 1,$$

where $7a_0 \equiv 1 \pmod{11}$. We see by inspection that a_0 equals 8. Hence

$$7a_0 = 7 \cdot 8 = 56 = 1 + 5 \cdot 11.$$

If we put this back into the 11-adic expansion we obtain

$$(1 + 5 \cdot 11) + 7a_1 11 + 7a_2 11^2 + \cdots = 1.$$

As explained in the previous section, 5 is carried to the next parenthesis:

$$1 + (5 + 7a_1)11 + \cdots = 1.$$

Now we need to solve

$$5 + 7a_1 \equiv 0 \pmod{11}.$$

This last expression is equivalent to

$$7a_1 \equiv -5 \equiv 6 \pmod{11}.$$

Since we know that the solution of $7a \equiv 1$ modulo 11 is $a = 8$, we can substitute

$$a_1 = 8 \cdot 6 = 48 \equiv 4 \pmod{11}.$$

If we keep using this method we obtain that

$$x = 8 + 4 \cdot 11 + 9 \cdot 11^2 + \cdots .$$

2.3 Newton's Method

In the previous two sections we described how to find p-adic expansions of roots of polynomials and inverses of nonzero integers. However, the process may take a long time, especially if the degree of the polynomial is high. There is a much more effective method to find p-adic expansions of roots of polynomials, namely Hensel's Lemma. The procedure is very similar to Newton's Method. Therefore in this section we first introduce Newton's Method [24], which is used to find the roots of a given polynomial $f(x)$ over $\mathbb{R}$ or $\mathbb{C}$. That is, we want to find x so that $f(x) = 0$. We first need to determine an x_0 which is close to the actual root x. The main idea behind the method is that if we take the tangent line at x_0 and we determine when it crosses the x-axis we obtain a value x_1 which should be much closer to the root that we are trying to find [32]. The following picture illustrates the method:

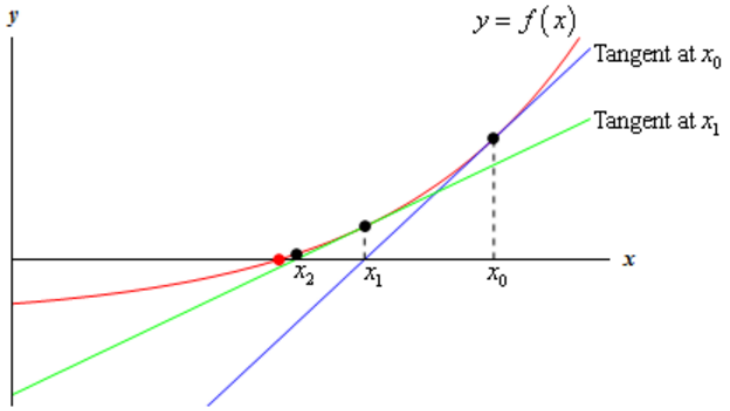


Figure 1: Illustration of Newton's Method using tangent lines.

In summary, Newton's Method to find a root of a polynomial $f(x)$ uses the recursion

$$x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}.$$

2.4 Hensel's Lemma

Similarly to Newton's Method, in p-adic analysis the way to find the roots of a polynomial is using Hensel's Lemma [6]. Let $f(x)$ be any polynomial and suppose that we want to find its roots in $\mathbb{Z}_p$ for some prime p. Hensel's Lemma states the following [6]:

Lemma 2.2. (Hensel) *If $f(x) \in \mathbb{Z}_p[x]$ and $a \in \mathbb{Z}_p$ satisfies $f(a) \equiv 0 \pmod{p}$ and $f'(a) \not\equiv 0 \pmod{p}$, then there is a unique $\alpha \in \mathbb{Z}_p$ such that $f(\alpha) = 0$ and $\alpha = a \pmod{p}$.*

The main idea behind Hensel's Lemma is to find a solution modulo p and then *lift* it modulo higher powers of p. Hensel's Lemma assures that if there exists a solution modulo p then there exists a p-adic expansion for the root of the polynomial and it is unique. The method is the following. First we find x_1 such that $f(x_1) \equiv 0 \pmod{p}$. Then we look for x_2; we know that it is of the form

$$x_2 = x_1 + pt,$$

where we need to determine t. We want that $x_2 \equiv x_1$ modulo p. By the Taylor polynomial expansion [12] we know that

$$f(x_2) = f(x_1 + pt) \approx f(x_1) + ptf'(x_1) + \cdots .$$

We do not need to write the whole expansion because

$$f(x_1) + ptf'(x_1) + \cdots \equiv f(x_1) + ptf'(x_1) \pmod{p^2}.$$

Since we know that $f(x_1) \equiv 0 \pmod{p}$, we can divide the previous expression by p:

$$\frac{f(x_1)}{p} + tf'(x_1) \equiv 0 \pmod{p}.$$

We can find t from this expression and then we can find x_2 since it is defined as $x_1 + pt$. These steps can be done recursively similarly as in Newton's Method. In general, we use these two expressions [12]:

$$\frac{f(x_{n-1})}{p^{n-1}} + tf'(x_{n-1}) \equiv 0 \pmod{p}; \qquad x_n = x_{n-1} + tp^{n-1} \pmod{p^n}.$$

Note that, similarly to Newton's Method, the necessary condition for Hensel's Lemma to work is that $f'(x) \neq 0 \pmod{p}$. Also, the coefficients of the polynomials need to be reduced modulo p. We can take as an example the polynomial $x^2 = 5$ in $\mathbb{Z}_{11}$ studied in Section 2.1. We know that x_1 equals 4 and hence

$$x_2 = x_1 + pt = 4 + 11t \pmod{11^2}.$$

We find t by using the previous recursive expression

$$\frac{11}{11} + 8t \equiv 0 \pmod{11}.$$

We see that t equals 4. Thus we know that

$$x_2 = 4 + 11t = 4 + 11 \cdot 4 = 48.$$

Using this method we obtain the successive a_i, which are $4, 4, 10, 4, 0, \ldots$. Note that these a_i that we obtained using Hensel's Lemma for the polynomial $x^2 = 5$ are the same values that we obtained in Section 2.1 by computing them manually for the same polynomial.

3 *p*-Adic convergence

3.1 *p*-Adic norm

In this section we provide necessary definitions for understanding convergence [10] of sequences and series in $\mathbb{Z}_p$.

Definition 3.1. Given a prime number p and a positive integer n, the *p-adic order* or *p-adic valuation* of n is the highest exponent $\alpha \in \mathbb{N}$ such that p^α divides n.

The p-adic valuation of α is denoted by $\alpha = v_p(n)$. For instance, $v_2(24) = 3$ since $2^3 = 8 \mid 24$ and $2^4 = 16 \nmid 24$. The p-adic valuation satisfies the following properties [10]:

1. $v_p(a \cdot b) = v_p(a) + v_p(b)$.
2. $v_p(a/b) = v_p(a) - v_p(b)$.

With the concept of p-adic valuation we can then define the p-adic absolute value, also called *p-adic norm* [17].

Definition 3.2. $|x|_p = p^{-v_p(x)}$ if $x \neq 0$. If $x = 0$, then $|x|_p = 0$.

The p-adic absolute value satisfies the following properties:

1. $|a|_p \geq 0$.
2. $|ab|_p = |a|_p|b|_p$.
3. $|-a|_p = |a|_p$.
4. $|a+b|_p \leq |a|_p + |b|_p$.
5. $|a+b|_p \leq \max(|a|_p, |b|_p)$.

This last property is a quite famous one because it means that the p-adic absolute value is *non-Archimedean* [17]. Therefore, using the previous example we can see that $|24|_2 = 2^{-3} = 1/2^3$.

Norm of a factorial

Because this work examines the p-adic factorial function, it is natural to ask which is the p-adic norm of $n!$. That is, given p, we want to find the largest α such that $p^\alpha \mid n!$. This problem was solved by Legendre:

Theorem 3.3. (Legendre) *If $v_p(n)$ denotes the largest power α of p such that p^α divides n, then*

$$v_p(n!) = \sum_{j \geq 1} \left\lfloor \frac{n}{p^j} \right\rfloor.$$

Moreover, Legendre showed that $v_p(n!)$ also equals $\frac{n - S_p(n)}{p-1}$, where S_p denotes the sum of the digits of n in base p. Therefore,

$$|n!|_p = 1/p^{\frac{n-S_p(n)}{p-1}}.$$

We also claim the following:

Claim 3.4. $\prod_p |n!|_p = 1/n!$.

Proof. The factorial $n!$ can be written as

$$n! = 2^{\alpha_1} \cdot 3^{\alpha_2} \cdot \cdots \cdot p^{\alpha_k}.$$

Hence the highest power of p that divides $n!$ is α_k; that is, $|n!|_p = p^{-\alpha_k}$. It follows that

$$\prod_p |n!|_p = \prod_p p^{-\alpha_k} = \frac{1}{\prod_p p^{\alpha_k}} = \frac{1}{n!},$$

as claimed. □

3.2 p-Adic series

As explained in the Introduction of this second part of the work, due to the properties of p-adic numbers the convergence of infinite series in $\mathbb{Q}_p$ is different than the converge of infinite series in $\mathbb{R}$. This is due to the following definitions and remarks from [15]:

Definition 3.5. A *Cauchy sequence* is a sequence such that its elements become arbitrarily close to each other as the sequence progresses. That is, for every given $\epsilon > 0$ there exists an N such that for all $m, n > N$ we have $|a_m - a_n| < \epsilon$.

Definition 3.6. A metric space is *complete* if every Cauchy sequence converges.

Theorem 3.7. *$\mathbb{Q}_p$ is complete.*

Then we can prove the following very important theorem in p-adic analysis [15]:

Theorem 3.8. *A series $\sum_{n=1}^{\infty} x_n$ converges in $\mathbb{Q}_p$ if and only if $\lim_{n\to\infty} x_n = 0$.*

Proof. We define $S_n = x_1 + x_2 + \cdots + x_n$, so $S_n - S_{n-1} = x_n$. By definition [10], $\sum_{n=1}^{\infty} x_n = \lim_{n\to\infty} S_n$. We first prove the first part of the implication. If $\sum x_n$ converges to $l \in \mathbb{Q}_p$, then $\lim_{n\to\infty} S_n = l$. Hence,

$$\lim_{n\to\infty} x_n = \lim_{n\to\infty} S_n - \lim_{n\to\infty} S_{n-1} = l - l = 0,$$

and the first part of the implication is proven. Now we prove that the converse is also true. If $\lim_{n\to\infty} x_n = 0$, then for all pairs of positive integers $m > n$ we have

$$S_m - S_n = S_m - S_{m-1} + S_{m-1} - S_{m-2} + \cdots + S_{n+1} - S_n = x_m + x_{m-1} + \cdots + x_{n+1}.$$

Consequently,

$$|S_m - S_n|_p \leq \max(|x_m|_p, \ldots, |x_{n+1}|_p).$$

Given $\epsilon > 0$, there exists a sufficiently large N such that $|x_m|_p < \epsilon, \ldots, |x_{n+1}|_p < \epsilon$ if $m, n > N$, because $|x_n|_p$ goes to 0. Therefore, according to Definition 3.5, S_n is a Cauchy sequence and hence converges because $\mathbb{Q}_p$ is a complete metric space. □

Theorem 3.9 is clearly not true in $\mathbb{R}$. The fact that the general term goes to 0 does not imply that the sequence converges. For instance, the general term of the well-known harmonic series $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \cdots$ tends to 0, but the series does not converge. Therefore, in p-adic analysis it is easier to decide whether a series converges or not.

4 The series $\sum n!$

4.1 Convergence in $\mathbb{Z}_p$

After having discussed convergence in general of series in p-adic analysis, we now turn to the factorial series $\sum n!$. We first observe the following:

Claim 4.1. *The series $\sum n!$ converges in $\mathbb{Z}_p$ for all primes p.*

Proof. Since $|n!|_p = 1/p^{\frac{n-s_p(n)}{p-1}}$, we have that $|n!|_p \to 0$ when $n \to \infty$. □

To compute the sum of $\sum n!$ in $\mathbb{Z}_p$ we can calculate the partial sums of the series $\sum n!$ in $\mathbb{Z}$ and then represent the result in base p. Since $n!$ is an integer, computing its p-adic expansion means representing $n!$ in base p. For instance, imagine we want to represent $1! + 2! + 3! + 4!$ in $\mathbb{Z}_3$. In $\mathbb{R}$ this sum equals 33. This is 1020 in $\mathbb{Z}_3$, because $33 = 1 \cdot 3^3 + 0 \cdot 3^2 + 2 \cdot 3 + 0$, which is the 3-adic expansion of 33. The first digits that become permanent are the ones corresponding to the lower powers of p. Therefore, we are interested in the last digits of the base p representation of $\sum n!$. Figure 2 illustrates the convergence of $\sum n!$ in $\mathbb{Z}_5$. Table 1 provides some digits of the sum of $\sum n!$ in $\mathbb{Z}_p$ with $p = 3, 5, 7, 11$. Also $\mathbb{Z}_{10}$ is included in the table because although it is technically not correct to talk about $\mathbb{Z}_{10}$ since 10 is not a prime, we usually operate in base 10 and hence the process is easier to visualize.

It is important to remark that the question whether $\sum n!$ is rational or irrational remains unanswered since this question was posed in [28]. In the following section we explore the p-adic meaning of rationality.

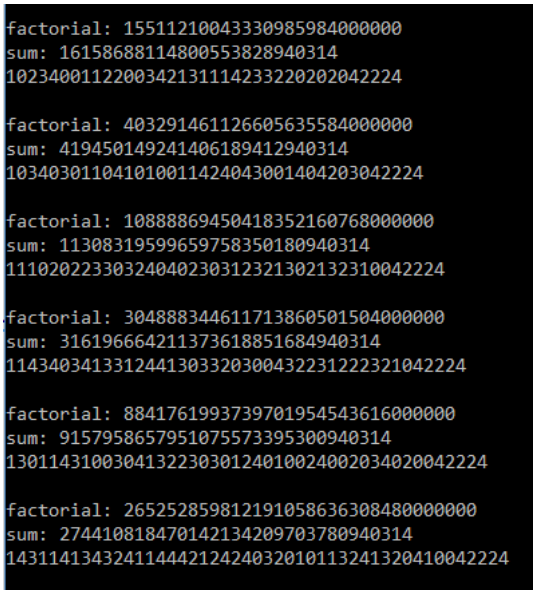


Figure 2: Example in our C++ code of how the sum of $n!$ converges in $\mathbb{Z}_5$.

p	Converges to
3	...2011012101
5	...1034004224
7	...3020161166
10	...0420940314
11	...61104109941 1

Table 1: Example of the convergence of $\sum n!$ in $\mathbb{Z}_p$ depending on p.

4.2 Rationality of p-adic expansions

In $\mathbb{R}$ we widely use the concepts of rationality and irrationality. It is clear that all integers are rational, and we say that a real number x is rational if it can be expressed in the form a/b where a and $b \neq 0$ are integers. When we write the decimal expansion of a given number x, we observe that if x is rational then its decimal expansion is periodic and viceversa. Therefore, periodicity is is a necessary and sufficient condition for rationality. We claim that the same property holds with p-adic numbers:

Theorem 4.2. *The p-adic expansion of any $x \in \mathbb{Z}_p$ is periodic if and only if x is rational.*

Proof. First we prove one part of the implication: if the p-adic expansion of x is periodic, then x is a rational number. Suppose that we have a p-adic expansion $a_1p + a_2p^2 + a_3p^3 + \cdots$. First we consider the expansion to be purely periodic without a_0, and we denote the length of the period by j. Therefore, we can rewrite the expansion as

$$p(a_1 + a_2p + a_3p^2 + \cdots + a_jp^{j-1}) + p^{j+1}(a_{j+1} + a_{j+2}p + a_{j+3}p^2 + \cdots + a_{2j}p^{j-1}) + \cdots .$$

Because the expansion is purely periodic and of length j it means that $a_1 = a_{j+1} = a_{2j+1} = \cdots = a_{kj+1}$, $a_2 = a_{j+2} = a_{2j+2} = \cdots = a_{kj+2}$, etc. Therefore, all the parentheses of length j are equal. We say that $a_{kj+1} + a_{kj+2}p + \cdots + a_{(k+1)j}p^{j-1}$ equals γ for all values of k. Then we can rewrite the previous expression as

$$\gamma p + \gamma p^{j+1} + \gamma p^{2j+1} + \cdots + \gamma p^{kj+1} + \cdots = \gamma(p + p^{j+1} + p^{2j+1} + \cdots p^{kj+1} + \cdots).$$

The parenthesis $(p + p^{j+1} + p^{2j+1} + \cdots + p^{kj+1} + \cdots)$ is a geometric series, which means that (applying the formula for the infinite sum of a geometric series) it is equal to $p/(1 - p^j)$. This is clearly rational, and therefore this part of the proof is complete. If the expansion is not purely periodic, then the proof still holds because we just subtract the non-periodic part from both sides of the equation: if we subtract a rational number from $p/(1 - p^j)$ the result is still rational.

Now we prove that rationality implies periodicity. If a p-adic number is rational, then it can be written as a/b for some integer a and b. Recall the method for finding the p-adic inverse of any number of the form $1/b$ for any non-zero value of b explained in Section 2.2. Each time we compute a new a_i for the p-adic expansion of the inverse $a_0 + a_1p + a_2p^2 + \cdots$ we multiply some number smaller than p by a fixed integer d such that $bd \equiv 1$ modulo p. Because this method finds the value of a_i regardless of i and only depends on the value of a_{i-1}, when the value of a_j for some j equals the value of any previous a_i the digits start to repeat and thus the expansion is periodic. This explains the periodicity of the p-adic expansion of $1/b$. In order to generalize this proof, we need to consider any fraction a/b. First $1/b = m + \gamma(p^r + p^{r+j+1} + p^{r+2j+1} + \cdots + p^{r+kj+1} + \cdots)$ because it is a periodic expansion, where $m \in \mathbb{Z}$ denotes the possible non-periodic part of $1/b$ and r is the exponent of p from which the expansion becomes purely periodic. When we multiply by a we obtain that $a/b = am + a\gamma(p^r + p^{r+j+1} + p^{r+2j+1} + \cdots + p^{r+kj+1} + \cdots)$, which is also periodic. □

4.3 A p-adic approximation of $n!$

The motivation for finding a p-adic approximation of $n!$ comes from Stirling's formula. As explained in the Introduction, it is not fast to compute large factorials because it has to be done recursively. However, Stirling's formula uses the function n^n in order the compute the factorial directly. Stirling's formula tells us that

$$n! \approx \left(\frac{n}{e}\right)^n \sqrt{2\pi n}.$$

Note that if we rearrange the expression as

$$\frac{n!}{n^n} \approx \left(\frac{1}{e}\right)^n \sqrt{2\pi n}$$

we observe that the quotient between $\sqrt[n]{n!}$ and n tends to a constant as n grows large. Therefore, we can say that although both $\sqrt[n]{n!}$ and n tend to infinity, they do so at the *same speed*.

Now we want to find a p-adic approximation of $n!$. Instead of going to infinity, as explained in Section 4.1, $n!$ goes p-adically to 0 when n grows large. Therefore, we want to find a function that goes p-adically to 0 with the same speed as $n!$. We have the following answer:

Claim 4.3. *The function $p^{\frac{n-S_p(n)}{p-1}}$ converges to 0 at the same speed as $n!$ in $\mathbb{Z}_p$.*

Proof. The function in Claim 4.3 comes from Legendre's Theorem (see Section 3.1). Since $\frac{n-S_p(n)}{p-1}$ returns the highest power of p that divides $n!$, when we represent $n!$ in $\mathbb{Z}_p$ it ends with $\frac{n-S_p(n)}{p-1}$ zeroes. Also, $p^{\frac{n-S_p(n)}{p-1}}$ in $\mathbb{Z}_p$ consists of 1 followed by $\frac{n-S_p(n)}{p-1}$ zeroes. Therefore, the two functions have the same number of ending zeroes for any value of n and thus their rates of convergence are the same. □

4.4 Irrationality of $\sum p^{\frac{n-S_p(n)}{p-1}}$

In this section we consider the series $\sum p^{\frac{n-S_p(n)}{p-1}}$ and we prove that it converges to an irrational number in $\mathbb{Z}_p$. We discuss this series because, as explained in the previous section, $p^{\frac{n-S_p(n)}{p-1}}$ is p-adically close to $n!$. We claim the following:

Theorem 4.4. *The sum of the series $\sum p^{\frac{n-S_p(n)}{p-1}}$ is irrational in $\mathbb{Z}_p$ for all p.*

Before we go to the proof, it is useful to study the evolution of $S_p(n)$ as n increases. Figure 3 illustrates the evolution of $S_p(n)$ for $p = 3$.

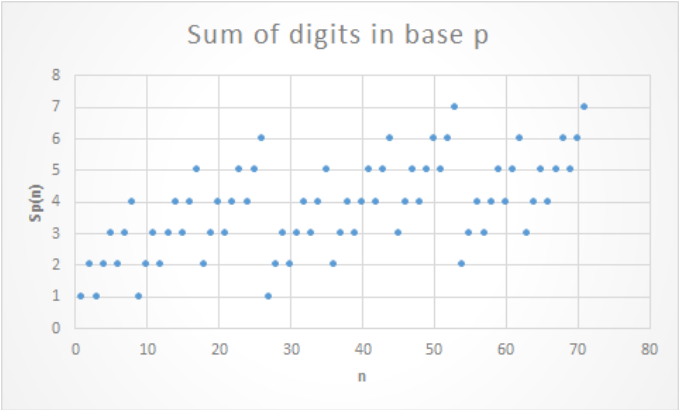


Figure 3: Evolution of the sum of the digits of n in base 3 until $n = 71$.

With this data we can construct the following table.

n	n in base p	$S_p(n)$	$p^{(n-Sp(n))/(p-1)}$
0	0	0	3^0
1	1	1	3^0
2	2	2	3^0
3	10	1	3^1
4	11	2	3^1
5	12	3	3^1
6	20	2	3^2
7	21	3	3^2
8	22	4	3^2
9	100	1	3^4
10	101	2	3^4
11	102	3	3^4
12	110	2	3^5
13	111	3	3^5
14	112	4	3^5
15	120	3	3^6
16	121	4	3^6
17	122	5	3^6
18	200	2	3^8
19	201	3	3^8
20	202	4	3^8

Table 2: Evolution of $p^{\frac{n-S_p(n)}{p-1}}$.

For the following claims we need to define a new term:

Definition 4.5. The k^{th} *package* of n in base p is the set formed by the numbers $S_p(n)$ with n from kp to $(k+1)p-1$.

Therefore, the cardinality of every package is p. First we note the following:

Claim 4.6. *The elements in any package are consecutive.*

Proof. Let $S_p(n)$ be the first element of any package. By definition n is a multiple of p, which means that the representation of n in base p ends with at least one zero. Let $S_p(m)$ denote any other element in the same package. The last digit of the base p representation of m cannot be zero, because by definition the next multiple of p lies in the next package. Therefore, the only difference between the base p representation of $n+i$ and the base p representation of $n+(i+1)$, where

$0 \leq i < p-1$, is that the last digit increases by one, starting with 0 for n and finishing with $p-1$ for $n+(i+1)$. Because $S_p(n+i)$ denotes the sum of the digits of the base p representation of $n+i$, it is clear that the elements in any package are consecutive. □

Corollary 4.7. *The number* $\frac{n-S_p(n)}{p-1}$ *is constant for all elements in the same package.*

Proof. From Claim 4.6 it is clear that in any package $S_p(n)$ increases by one when n increases by one. Therefore, $n - S_p(n)$ is constant for all elements in the same package. The number $p-1$ is also constant, which means that $\frac{n-S_p(n)}{p-1}$ remains the same for all elements in the same package. □

Corollary 4.8. *The number* $p^{\frac{n-S_p(n)}{p-1}}$ *finishes with the same number of zeroes for all the elements in the same package.*

Claim 4.9. *The number of zeroes of* $p^{\frac{n-S_p(n)}{p-1}}$ *in base* p *is increasing.*

Proof. As explained in Section 4.3, $p^{\frac{n-S_p(n)}{p-1}}$ finishes with the same number of zeroes as $n!$ in base p. Because $n! = 1 \cdot 2 \cdot \cdots \cdot (n-1) \cdot n$, the number of multiples of p in $n!$ can only be increasing. □

All these claims can be observed in Table 2. For the proof of Theorem 4.4 it is important to take into account the disposition shown in Figure 4. This diagram represents the addition by hand of $p^{\frac{n-S_p(n)}{p-1}}$ for $p = 3$ and until $n = 20$. In Figure 4 it can be observed how the number $p^{\frac{n-S_p(n)}{p-1}}$ finishes with the same number of zeroes for all the elements in the same package, as stated in Corollary 4.8.

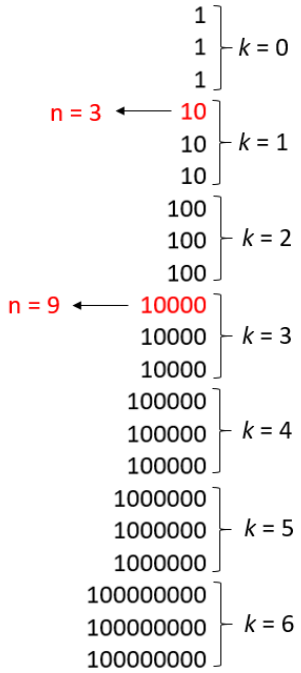


Figure 4: Values of $p^{\frac{n-S_p(n)}{p-1}}$ for $p = 3$ until $n = 20$. Powers of 3 are marked in red.

Having made all these observations we can now prove Theorem 4.4.

Proof of Theorem 4.4. We focus on what happens when n is a power of p. That is, $n = p^\alpha$ for some value of $\alpha \in \mathbb{N}$. We now compare the number of zeroes of $p^{\frac{(n-1)-S_p(n-1)}{p-1}}$ with the number of zeroes of $p^{\frac{n-S_p(n)}{p-1}}$. Because $n = p^\alpha$, the base p representation of n consists of 1 and α zeroes. Therefore, it is easy to compute the number of zeroes of $p^{\frac{n-S_p(n)}{p-1}}$ because $S_p(n) = 1$. Also, because $n - 1 = p^\alpha - 1$, the base p representation of $n-1$ consists only of $p-1$ digits, and there are α of them. Therefore, $S_p(n-1) = \alpha(p-1)$. Hence, the number of zeroes of $p^{\frac{n-S_p(n)}{p-1}}$ is $\frac{n-1}{p-1}$, whereas the number of zeroes of $p^{\frac{(n-1)-S_p(n-1)}{p-1}}$ is $\frac{n-1-\alpha(p-1)}{p-1} = \frac{n-1}{p-1} - \alpha$. So this means that $p^{\frac{n-S_p(n)}{p-1}}$ has α more zeroes than $p^{\frac{(n-1)-S_p(n-1)}{p-1}}$.

Then when we add $p^{\frac{n-S_p(n)}{p-1}}$ to $\sum_{i=0}^{n-1} p^{\frac{i-S_p(i)}{p-1}}$, between the first digit of $p^{\frac{(n-1)-S_p(n-1)}{p-1}}$ and the first digit of $p^{\frac{n-S_p(n)}{p-1}}$ there are $\alpha - 1$ zeroes. When we add $p^{\frac{n-S_p(n)}{p-1}}$ to $\sum_{i=0}^{n-1} p^{\frac{i-S_p(i)}{p-1}}$, we see that after the first digit of the result (which is a 1 that comes from $p^{\frac{n-S_p(n)}{p-1}}$) and the following 1 there are $\alpha - 2$ zeroes. It is $\alpha - 2$ and not $\alpha - 1$ because when adding the packages for each package there are p ones that we have to add together, which means that there is exactly one carry for each package. Then, the important observation is that when we add $p^{\frac{n-S_p(n)}{p-1}}$ to $\sum_{i=0}^{n-1} p^{\frac{i-S_p(i)}{p-1}}$, we fix all the digits that come before because by Claim 4.8 the number of zeroes of $p^{\frac{n-S_p(n)}{p-1}}$ is increasing (also see Figure 4). Therefore there are $\frac{n-1}{p-1}$ digits that are forever fixed in the expansion of $\sum p^{\frac{n-S_p(n)}{p-1}}$, which implies that there are $\alpha - 2$ zeroes that are forever fixed in the expansion of $\sum p^{\frac{n-S_p(n)}{p-1}}$. However, α increases by one for each power of p, which means that the number of zeroes fixed in $\sum p^{\frac{n-S_p(n)}{p-1}}$ increases by one each time we encounter a power of p. Therefore, this expansion cannot be periodic, and by Theorem 4.2 the p-adic expansion of $\sum p^{\frac{n-S_p(n)}{p-1}}$ is irrational, as we wanted to see. □

In order to make this proof more visual, the following diagram represents the addition for $3^3 - 1 = 26$ and $3^3 = 27$ in $\mathbb{Z}_3$. It can be observed that there is one zero forever fixed in the sum of $\sum 3^{\frac{n-S_3(n)}{3-1}}$, and when we add the term corresponding to $3^4 = 81$ there will be two zeroes forever fixed, and so on.

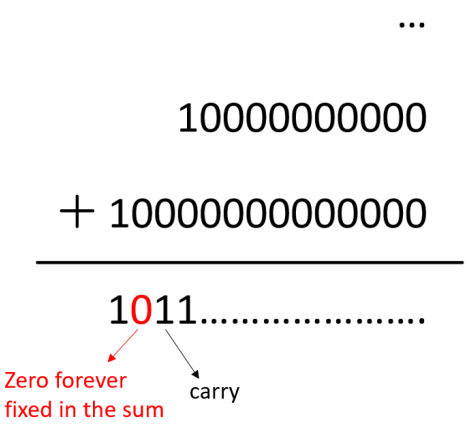


Figure 5: Visualization of an example: addition for $n = 26$ and $n = 27$ in $\mathbb{Z}_3$.

We have written a short article containing the proof of Theorem 4.4 and have posted it in the arXiv [3].

5 Regarding the irrationality of $\sum n!$

The main motivation of this work has been the series $\sum n!$, because it is not known if its sum is rational or not. After proving the irrationality of the p-adic analogous that we found, we tried to prove the p-adic irrationality of $\sum n!$ using the same ideas. However, we did not manage to prove it. Nevertheless, we found two arguments that could be useful towards a proof. The first one is the following:

Claim 5.1. *For any positive value of n,*

$$n! \geq \sum_{k=0}^{n-1} k!$$

Proof. We proceed to prove Claim 5.1 by induction. We assume that $k! \geq \sum_{i=0}^{k-1} i!$ is true and we want to see if it is also true for $k+1$. Our base case holds, since

$$\sum_{i=0}^{0} i! = 0! = 1 = 1!$$

Now we apply the induction hypothesis to see that our assumption is true for $n+1$:

$$\begin{aligned}(k+1)! = (k+1)k! \geq (k+1) > \sum_{i=0}^{k-1} i! = k\sum_{i=0}^{k-1} i! + \sum_{i=0}^{k-1} i! \\ = k(0! + 1! + \cdots + (k-1)!) + \sum_{i=0}^{k-1} i! \geq k(k-1)! + \sum_{i=0}^{k-1} i! \\ = k! + \sum_{i=0}^{k-1} i! = \sum_{i=0}^{k} i!\end{aligned}$$

Since the base case holds and we saw that if Claim 5.1 is true for k it is also true for $k+1$, the proof is complete. □

We also make a second observation:

Claim 5.2. *The number of ending zeros of $n!$ cannot be larger than the number of digits of $\sum_{k=0}^{n-1} k!$.*

Proof. We first observe the following: due to the rapid growth of $n!$, when we add $n!$ to $\sum_{k=0}^{n-1} k!$, the number of digits of $\sum_{k=0}^{n} k!$ is approximately the same as $n!$. This is supported by Claim 5.1. Therefore,

$$\log\left(\sum_{k=0}^{n} k!\right) \approx \log(n!).$$

We take the logarithm because it is well-known that the number of digits of x is roughly $\log(x)$. Now we can get an approximation of $\log(n!)$ applying Stirling's Formula. Recall from the explanation of Section 4.3 that, due to Stirling's Formula, $n! \approx n^n$, although it is clear that $n^n \geq n!$. Hence, $\log(n!) \approx n\log(n)$ and we have that

$$\log\left(\sum_{k=0}^{n} k!\right) \approx n\log(n).$$

Now we evaluate the number of zeroes of $(n+1)!$ compared to the number of zeroes of $\sum_{k=0}^{n} k!$. It suffices to analyze the case in which $(n+1)!$ has the maximum number of zeroes, and because we are working in $\mathbb{Z}_p$ this happens when $(n+1)!$ is a power of p. Then we can apply Legendre's Formula to obtain that $S_p(n+1) = 1$. Therefore, the number of ending zeroes of $(n+1)!$ is $\frac{(n+1)-1}{p-1} = \frac{n}{p-1}$. It is then clear that $n\log(n) > \frac{n}{p-1}$, and hence the proof is complete. □

6 Convergence of other p-adic series with $n!$

6.1 First type of series

After having analyzed the series $\sum n!$, we saw in [28] the following claim, which is stated but not proven there:

Claim 6.1. $\sum_{n=0}^{\infty} nn! = -1$.

Proof. We do not know if $\sum n!$ is rational or not, but we can compute the following:

$$\sum_{n=0}^{\infty}[(n+1)! - n!] = 1! - 0! + 2! - 1! + 3! - 2! + \cdots = -1.$$

Because of the alternating sign, all the terms cancel except for $-0!$, which is equal to -1. Moreover,

$$(n+1)! - n! = n!(n+1-1) = nn!$$

and therefore

$$\boxed{\sum_{n=0}^{\infty} nn! = -1}$$

as claimed. □

For the subsequent proofs we use the following notation:

Definition 6.2. We denote $\sum_{n=1}^{\infty} n!$ by α.

The following output of our C++ code illustrates the meaning of p-adic convergence to -1 in $\mathbb{Z}_5$. Note that the digit $p-1$ (in this case 4 because $-1 \equiv 4$ modulo 5), keeps appearing in the end more and more as n increases.

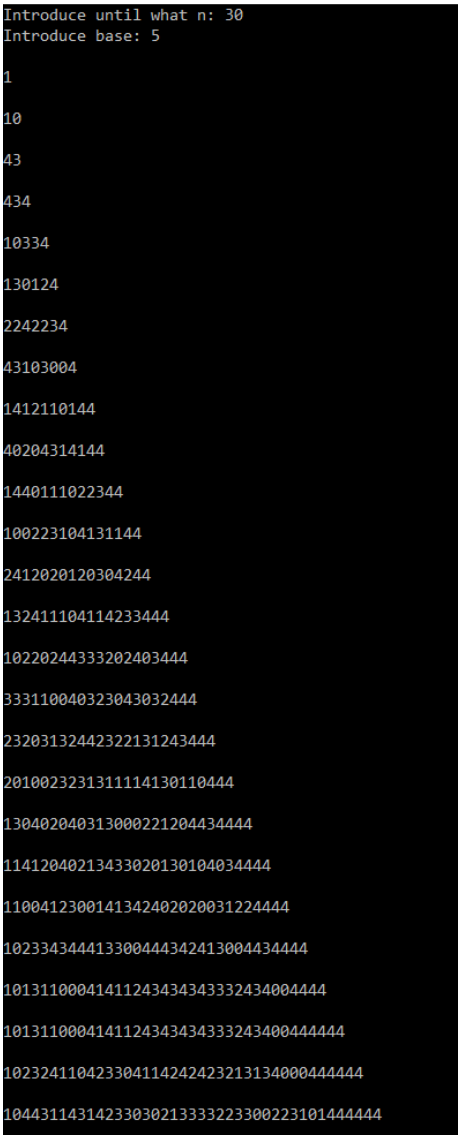


Figure 6: Convergence of the series $\sum nn!$ to -1 in $\mathbb{Z}_5$.

We then asked ourselves, given that this is a recursive method, if there is also a method to compute $\sum_{n=0}^{\infty} n^k n!$ for higher values of k. The answer is yes, and here we provide the method. We can compute $\sum_{n=0}^{\infty} n^2 n!$ using the following trick:

$$\sum_{n=0}^{\infty}(n+2)(n+1)n! = \sum_{n=0}^{\infty}(n+2)! = \sum_{n=2}^{\infty} n! = \alpha - 1. \tag{2}$$

However, we also have that

$$\sum_{n=0}^{\infty}(n+2)(n+1)n! = \sum_{n=0}^{\infty}(n^2+3n+2)n! = \sum_{n=0}^{\infty} n^2n! + 3\sum_{n=0}^{\infty} nn! + 2\sum_{n=0}^{\infty} n! \quad (3)$$

Then substituting with (2):

$$\sum_{n=0}^{\infty} n^2n! + 3\sum_{n=0}^{\infty} nn! + 2\sum_{n=0}^{\infty} n! = \sum_{n=0}^{\infty} n^2n! - 3 + 2(\alpha+1). \quad (4)$$

Equating (2) and (3) we obtain

$$\alpha - 1 = \sum_{n=0}^{\infty} n^2n! - 1 + 2\alpha$$

and therefore

$$\boxed{\sum_{n=0}^{\infty} n^2n! = -\alpha.}$$

The same method works when $k = 3$:

$$\sum_{n=0}^{\infty}(n+3)(n+2)(n+1)n! = \sum_{n=0}^{\infty}(n+3)! = \sum_{n=3}^{\infty} n! = \alpha - (1! + 2!) = \alpha - 3; \quad (5)$$

$$\sum_{n=0}^{\infty}(n+3)(n+2)(n+1)n! = \sum_{n=0}^{\infty}(n^3+6n^2+11n+6)n! \quad (6)$$

The last equation is equal to:

$$\sum_{n=0}^{\infty} n^3n! + 6\sum_{n=0}^{\infty} n^2n! + 11\sum_{n=0}^{\infty} nn! + 6\sum_{n=0}^{\infty} n! = \sum_{n=0}^{\infty} n^3n! + 6(-\alpha) + 11\cdot(-1) + 6\alpha \quad (7)$$

Therefore, from (5) and (7):

$$\boxed{\sum_{n=0}^{\infty} n^3n! = \alpha + 2.}$$

This is a recursive process and by obtaining all the values of $\sum_{n=0}^{\infty} n^in!$ for $i \leq k-1$ we can obtain the value of $\sum_{n=0}^{\infty} n^kn!$. Hence we infer the following:

Claim 6.3. *If $\alpha = \sum_{n=1}^{\infty} n!$ is rational, then $\sum_{n=0}^{\infty} n^kn!$ is also rational for all k.*

Proof. As seen from the recursion, $\sum_{n=0}^{\infty} n^kn! = s_k\alpha + y_k$, where the integers s_k and y_k depend on k. If α is rational then so is $s_k\alpha + y_k$. □

Note 6.4. From now on, we shall denote the value of the coefficient of α when we compute the sum of $\sum_{n=0}^{\infty} n^k n!$ by s_k.

Following the recursivity, we can display as many values of $\sum_{n=0}^{\infty} n^k n!$ as desired:

$$\sum_{n=0}^{\infty} nn! = -1 \tag{8}$$

$$\sum_{n=0}^{\infty} n^2 n! = -\alpha \tag{9}$$

$$\sum_{n=0}^{\infty} n^3 n! = \alpha + 2 \tag{10}$$

$$\sum_{n=0}^{\infty} n^4 n! = 2\alpha - 3 \tag{11}$$

$$\sum_{n=0}^{\infty} n^5 n! = -9\alpha - 4. \tag{12}$$

What is very interesting to observe about these series is the following: if the coefficient of α is 0, then $\sum_{n=0}^{\infty} n^k n!$ converges to an integer. We have computed using C++ the values of s_k (the coefficients of α) until very large numbers, and we have encountered that it only seems to be 0 when $k = 1$. Table 3 shows the values of the coefficient of α until $k = 15$. We observe that the value of the coefficient of α bounces between positive and negative values, but the absolute value seems to keep increasing. This provides evidence to conjecture the following:

Conjecture 6.5. *The series $\sum_{n=0}^{\infty} n^k n!$ converges to an integer only when $k = 1$.*

k	Coeficient of α
1	0
2	-1
3	1
4	2
5	-9
6	9
7	50
8	-267
9	413
10	2180
11	-17731
12	50533
13	110176
14	-1966797
15	9938669

Table 3: Coefficients s_k of α until $k = 15$.

When we checked if this sequence of integers existed in the On-line Encyclopedia of Integer Sequences (OEIS) we found out that it exists indeed, and the values of s_k are called *complementary Bell numbers* or *Uppuluri-Carpenter numbers*. They are related to combinatorics and to the function e^{1-e^t}. In several recent papers [1, 8, 21] and these numbers are also linked to other features in p-adic analysis.

In the next section we relate the numbers s_k with other p-adic series and provide C++ code to compute values of s_k

6.2 A variation of the previous series

Once we have discussed the series $\sum_{n=0}^{\infty} n^k n!$ we wondered what happened if we analyzed the series

$$\sum_{n=0}^{\infty} n^k (n+1)!.$$

We found a recursive method to compute the sums of these series based on α and on the values obtained in the previous section (the values of s_k). For this method to work we first need to compute $\sum_{n=0}^{\infty} n^k n!$ before computing $\sum_{n=0}^{\infty} n^k (n+1)!$. We start by showing an example:

$$\sum_{n=0}^{\infty} n^2 (n+1)! = \sum_{n=1}^{\infty} (n-1)^2 n! \tag{13}$$

and we also have that

$$\sum_{n=1}^{\infty} (n-1)^2 n! = \sum_{n=1}^{\infty} (n^2 - 2n + 1) n! = \sum_{n=1}^{\infty} n^2 n! - 2\sum_{n=1}^{\infty} n n! + \sum_{n=1}^{\infty} n!. \tag{14}$$

Substituting with the values obtained in the previous section we find that

$$\sum_{n=1}^{\infty} n^2 n! - 2\sum_{n=1}^{\infty} n n! + \sum_{n=1}^{\infty} n! = -\alpha + 2 + \alpha = 2. \tag{15}$$

The following output of our C++ code illustrates the meaning of the convergence of $\sum_{n=0}^{\infty} n^2 (n+1)!$ to 2 in $\mathbb{Z}_5$. Note that the digit 2 is always at the end of the expression. Before the 2 there is an increasing number of zeroes, which means that the series converges to 2.

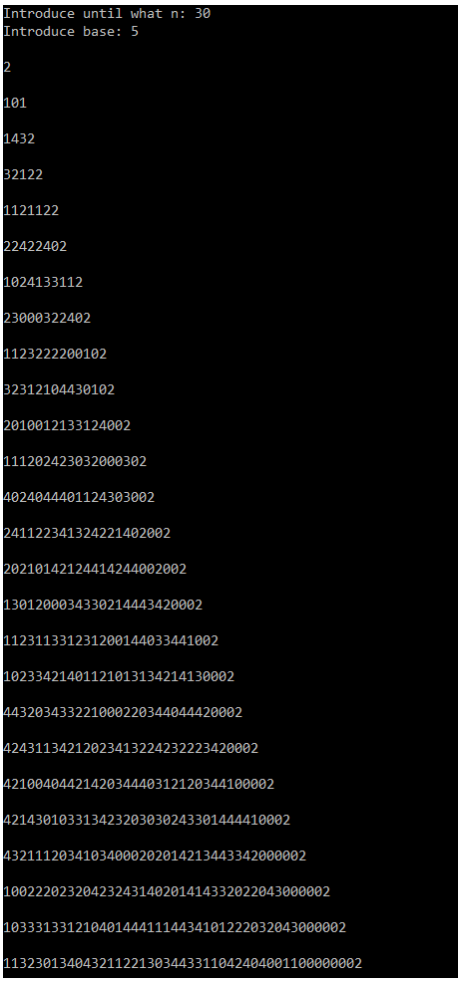


Figure 7: Convergence of the series $\sum n^2(n+1)!$ to 2 in $\mathbb{Z}_5$.

Using this trick and this method of recursion we can compute the following values of $\sum_{n=0}^{\infty} n^k(n+1)!$ until $k=5$:

$$\sum_{n=1}^{\infty} n^3(n+1)! = 3\alpha - 1 \tag{16}$$

$$\sum_{n=1}^{\infty} n^4(n+1)! = -7\alpha - 7 \tag{17}$$

$$\sum_{n=1}^{\infty} n^5(n+1)! = 26. \tag{18}$$

We observe that, in this case, $\sum_{n=0}^{\infty} n^k(n+1)!$ converges to an integer (which means that the coefficient of α is 0) for $k=2$ and $k=5$, regardless of the prime p with respect to which the convergence is taken. The question is: Will $\sum_{n=1}^{\infty} n^k(n+1)!$ converge to an integer for any other value of k? Again we have computed the coefficients of α until very large k and we conjecture that the answer is no. Table 4 provides the first 15 values of the coefficients of α.

k	Coeficient of α
2	0
3	3
4	-7
5	0
6	59
7	-217
8	146
9	2593
10	-15551
11	32802
12	160709
13	-1856621
14	7971872
15	1299951

Table 4: Coefficients of α in the sum of $\sum_{n=1}^{\infty} n^k(n+1)!$ until $k = 15$.

Similarly as in Table 3, the coefficients of α bounce between positive and negative values, yet the absolute value seems to be increasing. Therefore we conjecture the following:

Conjecture 6.6. *The series $\sum_{n=1}^{\infty} n^k(n+1)!$ only converges to an integer for $k = 2$ and $k = 5$.*

We have not found this conjecture in any of the papers related to this topic.

6.3 Generalizing further

In Section 6.1 we studied the series $\sum_{n=1}^{\infty} n^k n!$, and in Section 6.2 we considered the series $\sum_{n=1}^{\infty} n^k(n+1)!$. Now we analyze a broader generalization of those series, namely

$$\sum_{n=1}^{\infty} n^k(n+m)!$$

We ask again: when does this series converge to an integer in $\mathbb{Z}_p$? We have computed using our C++ program all the combinations of very large numbers of k and m and have encountered that $\sum_{n=1}^{\infty} n^k(n+m)!$ only converges to an integer when $k = 1$ and $m = 0$; $k = 2$ and $m = 1$; $k = 5$ and $m = 1$. Therefore we conjecture the following, which is the main conjecture of this work:

Conjecture 6.7. *The series $\sum_{n=1}^{\infty} n^k(n+m)!$ only converges to an integer when $k = 1$ and $m = 0$; $k = 2$ and $m = 1$; $k = 5$ and $m = 1$.*

As with Conjecture 6.6, we have not found Conjecture 6.7 in any article. If we analyze how to compute the sum of $\sum_{n=1}^{\infty} n^k(n+m)!$ when k is fixed, we can prove some results. We provide the following recursive method that also uses the coefficients of α described in Section 6.1 (the values of s_k). We start with $k = 1$:

$$\sum_{n=1}^{\infty} n(n+m)! = \sum_{n=1}^{\infty} nn! - m\sum_{n=1}^{\infty} n! \tag{19}$$

If we only take into account the coefficient of α we have that

$$\sum_{n=1}^{\infty} nn! - m\sum_{n=1}^{\infty} n! = -m\alpha. \tag{20}$$

It is clear that $-m$ is zero only if $m = 0$. We already knew that $\sum_{n=1}^{\infty} nn!$ converges to an integer (see Claim 6.1). Now we repeat the process for $k = 2$:

$$\begin{aligned}\sum_{n=1}^{\infty} n^2(n+m)! + t = \sum_{n=1}^{\infty}(n-m)^2 n! + t = \sum_{n=1}^{\infty}(n^2 - 2nm + m^2)n! + t \\ = \sum_{n=1}^{\infty} n^2 n! - 2m\sum_{n=1}^{\infty} nn! + m^2\sum_{n=1}^{\infty} n! + t.\end{aligned} \tag{21}$$

Then, substituting for the values of s_k and ignoring the independent value t found in Section 6.1 because is not related to the coefficient of α, we obtain the following:

$$\sum_{n=1}^{\infty} n^2 n! - 2m\sum_{n=1}^{\infty} nn! + m^2\sum_{n=1}^{\infty} n! = -\alpha + m^2\alpha = (-1 + m^2)\alpha. \tag{22}$$

It is clear that $(-1 + m^2)$ is 0 only when $m = 1$. As it is observed, this process is recursive and can be employed for any k and m. However, we have to clarify two steps:

1. When we go from $\sum_{n=1}^{\infty} n^k(n+m)!$ to $\sum_{n=1}^{\infty}(n-m)^k n!$ in the first step, the subindex of the second series should not be $n = 1$ but rather $n = k$. However, this does not affect the final coefficient of α, because to bring back the $n = 1$ in the subindex we would have to add some independent terms, which have nothing to do with the coefficients of α.

2. When we put the values of s_k in the sum we ignore the independent terms explained in Section 6.1, or t as written in (19). This is because we are only interested in seeing when the coefficient of α is 0, and thus we only take into account the coefficient of α and ignore the independent values.

As it is observed in the previous two examples, for each series we obtain that the coefficient of α is a polynomial that depends on m. Because when we evaluate a polynomial with any of its roots the result is zero, the coefficient of α equals zero if and only if the polynomial that depends on m has some positive integer root. Here we provide the polynomials that depend on m (which are the coefficients of α) for $k = 3, 4, 5, 6$:

$$\sum_{n=1}^{\infty} n^3(n+m)! = (1 + 3m - m^3)\alpha \tag{23}$$

$$\sum_{n=1}^{\infty} n^4(n+m)! = (2 - 4m - 6m^2 + m^4)\alpha \tag{24}$$

$$\sum_{n=1}^{\infty} n^5(n+m)! = (-9 - 10m + 10m^2 + 10m^3 - m^5)\alpha \tag{25}$$

$$\sum_{n=1}^{\infty} n^6(n+m)! = (9 + 54m + 30m^2 - 20m^3 - 15m^4 + m^6)\alpha. \tag{26}$$

If we analyze these polynomials, the only one which has one positive integer root is when $k = 5$ with $m = 2$. This series is part of our conjecture (see Conjecture 6.3). However, we can claim the following:

Proposition 6.8. *The series* $\sum_{n=1}^{\infty} n^k(n+m)!$ *does not converge to an integer for* $k = 3, 4, 6$.

Proof. For the proof it suffices to see that the polynomials given by (22), (23) and (24) have no positive integer roots. □

When we checked in the literature if these series had been computed, we found them in [31], where the same coefficients had been obtained. This seems to be the only paper in which these polynomials are mentioned.

Nevertheless, it is not feasible to keep computing these polynomials to prove Conjecture 6.7. Instead we need to find a general formula. Let $P_k(m)$ denote the polynomial that has been analyzed in this section that depends on m and corresponds to the coefficient of α in the sum of the series $\sum n^k(n+m)!$. We analyze what happens when we evaluate $P_k(0)$ for each k. Clearly, we get rid of all the terms except for the s_k term in the beginning. Observe, in the previous examples, that the only cas which there is no m in the coefficient is the one that corresponds to $\sum n^k n!$. As defined in Section 6.1, $\sum n^k n! = s_k$. Therefore we claim the following:

Claim 6.9. $P_k(0) = s_k$.

Now we make another observation: what if we evaluate $P_k(-1)$? We obtained the following results in our C++ code:

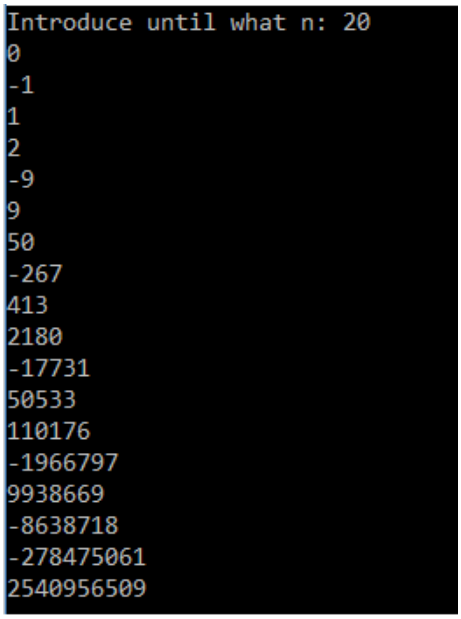


Figure 8: Result of $P_k(-1)$ for the first values of k.

Amazingly, these numbers are exactly the same as the ones found in Section 6.1:

Claim 6.10. $P_{k+1}(-1) = P_k(0) = s_k$.

We found that this property had been proven in [31].

7 Properties and cycles of $P_k(-1)$ and $P_k(1)$

Because with Claim 6.10 we know the result of $P_k(-1)$, we can now relate it to $P_k(1)$. Recall our conjecture stated in Section 6.1:

The series $\sum_{n=1}^{\infty} n^k(n+1)!$ *only converges to an integer value for* $k = 2$ *and* $k = 5$.

We again focus on $(n+1)!$ because these are the resulting series using $P_k(m)$ when $m = 1$. Observe the values of $P_k(1)$ and $P_k(-1)$ for $k = 2, 3, 4$ (recall that the definition of s_k is given in Section 6.1):

$$a_2(1) = s_2 - 2s_1 + 1$$

$$a_2(-1) = s_2 + 2s_1 + 1$$

$$a_3(1) = s_3 - 3s_2 + 3s_1 - 1$$

$$a_3(-1) = s_3 + 3s_2 + 3s_1 + 1$$

$$a_4(1) = s_4 - 4s_3 + 6s_2 - 4s_1 + 1$$

$$a_4(-1) = s_4 + 4s_3 + 6s_2 + 4s_1 + 1$$

From these observations (note that the coefficients of s_k are the binomial coefficients), and from the fact that we are developing the polynomials $(m-1)^k$ and $(m+1)^k$ for $P_k(1)$ and $P_k(-1)$ respectively, we can derive the following two formulae:

$$P_k(1) = \sum_{n=0}^{k} (-1)^{k-n} \binom{k}{n} s_n \tag{27}$$

$$P_k(-1) = \sum_{n=0}^{k} \binom{k}{n} s_n \tag{28}$$

where $u_0 = 0$. It is interesting to compute the difference between $P_k(1)$ and $P_k(-1)$. We define the following:

Definition 7.1. We denote $r_k = P_k(-1) - P_k(1)$.

Defining these numbers r_k is an idea that we have not found in any of the papers related to this topic, and it has turned out to be very useful for the subsequent proofs in this section. Therefore, using r_k is one of the main contributions in this part of our work.

The following equations show the results of $P_k(-1) - P_k(1)$ for $k = 2, 3, 4$:

$$r_2 = 2 \cdot \binom{2}{1} s_1$$

$$r_3 = 2 \cdot \binom{3}{1} s_2 + 2$$

$$r_4 = 2 \cdot \binom{4}{1} s_3 + 2 \cdot \binom{4}{3} s_1.$$

From these observations we can also find a formula for r_k:

$$r_{2k+1} = 2 \sum_{i=1}^{k} \binom{2k+1}{2i-1} s_{2k-2i+2} + 2 \tag{29}$$

$$r_{2k} = 2 \sum_{i=1}^{k} \binom{2k}{2i-1} s_{2k-2i+1}. \tag{30}$$

Therefore we claim the following:

Proposition 7.2. *The number r_k is even for all values of k.*

Proof. Due to the fact that $P_k(1)$ has alternate signs whereas $P_k(-1)$ only has positive signs, when we subtract $P_k(1)$ from $P_k(-1)$ we eliminate the terms s_k whose coefficient is $\binom{k}{2\gamma}$ (and thus have negative sign in $P_k(-1)$), for any positive value of $\gamma < k$. However, the other terms (the ones that are positive in both $P_k(1)$ and $P_k(-1)$) are added together and the result is therefore even. Because r_k is then formed with only even coefficients, r_k is even. □

Corollary 7.3. *$P_k(1)$ and $P_k(-1)$ have the same parity modulo 2.*

Proof. The difference between $P_k(1)$ and $P_k(-1)$ is r_k. If $P_k(1)$ and $P_k(-1)$ had a different parity modulo 2, then the difference between them would be an odd number. But this is a contradiction because, by Proposition 7.3, r_k is always even. □

Recall that we are interested in studying when is $P_k(1) = 0$. Observe the following:

Observation 7.4. *$P_k(1) = 0$ if and only if $P_k(-1) = r_k$.*

Proof. This is clear by the definition of r_k. □

We make the following remark: If $P_k(-1)$ and r_k are equal when $P_k(1) = 0$, then they are also equal modulo any prime. Therefore we claim the following, which is one of the main results of this work because we have not found it in any paper and it partially solves Conjecture 6.2:

Theorem 7.5. *If $P_k(-1) \equiv 1 \pmod 2$, then $\sum_{n=0}^{\infty} n^k(n+1)!$ does not converge to an integer.*

Proof. As stated in Proposition 7.3, $rk \equiv 0 \pmod 2$ for any value of k. Therefore, if $P_k(-1) \equiv 1 \pmod 2$ then the equality $P_k(-1) = r_k$ cannot occur. Thus, by Observation 7.5, $P_k(1)$ cannot be equal to 0. This means that because $P_k(1) = x$ in the sum of $\sum_{n=0}^{\infty} n^k(n+1)! = x\alpha + y$, the number x is not 0 and hence $\sum_{n=0}^{\infty} n^k(n+1)!$ does not converge to an integer. □

7.1 Cycles of $P_k(1)$ and $P_k(-1)$ modulo p

Because of Theorem 7.6 we want to analyze when is $P_k(-1) \equiv 1 \pmod 2$. The results and ideas found in this section are also new to this topic, because only in [21] the values of $P_k(-1)$ are evaluated modulo 2. In our work we find interesting results when evaluating not only $P_k(-1)$, but also $P_k(1)$ and r_k modulo n for different values of n. Our motivation for computing $P_k(-1)$ modulo 2 comes from Theorem 7.6. If we represent $P_k(-1)$ modulo 2 for some values of k we obtain the following plot:

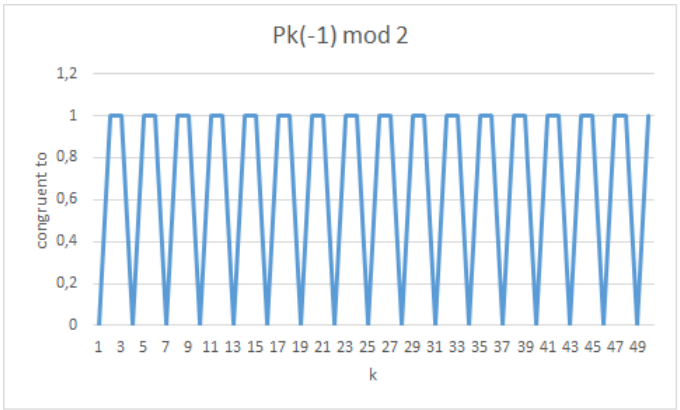


Figure 9: Result of $P_k(-1)$ modulo 2 for the first values of k.

In fact, as can be seen in Figure 9, if we compute the remainders of $P_k(-1)$ when we divide the polynomial by 2 we observe a period of length 3 which consists of the remainders $1, 1, 0$. This is proven in [21]. All these results lead to our main result in this part of our work:

Theorem 7.6. *The series* $\sum_{n=0}^{\infty} n^k(n+1)!$ *does not converge to an integer when* $k \equiv 0 \pmod 3$ *or* $k \equiv 1 \pmod 3$.

Proof. By Theorem 7.6, if $P_k(-1) \equiv 1 \pmod 2$ then $\sum_{n=0}^{\infty} n^k(n+1)!$ does not converge to an integer. Using that $s_k = P_k(0)$ and that $P_k(0) \equiv 1 \pmod 2$ when $k \equiv 0 \pmod 3$ or $k \equiv 1 \pmod 3$, since $P_{k+1}(-1) = P_k(0)$ Theorem 7.6 is proven. □

It is then natural to ask the following question: what if we evaluate $P_k(1)$, $P_k(-1)$ and r_k modulo other numbers? We did not observe any other patterns in any of the three sequences. However, we did observe cycles in the three sequences if we applied one little change: whenever we were evaluating $P_k(1)$, $P_k(-1)$ or r_k modulo n, if the resulting number was negative then we took the opposite of this number modulo n. So for example, imagine that $P_k(1) = -6$ for some value of k. Say that in our C++ program we are computing the results of $P_k(1)$ modulo 8. Then, because we are working modulo 8, we take the value of -6 to be 2, because $-6 \equiv 2 \pmod 8$. Therefore, our C++ program would return that $P_k(1) = -6$ is congruent to 2 modulo 8. By analyzing the three sequences with our little variation we obtained very interesting cycles:

Observation 7.7. *The representation of* $P_k(-1)$, $P_k(1)$ *and* r_k *modulo* n *for consecutive values of* k *is cyclic if and only if* n *is a power of* 2, 3 *or* 6.

The following figures illustrate the representation of $P_k(-1)$ modulo 3, 4 and 6 for some consecutive values of k. The periodicity of the remainders is clearly observable.

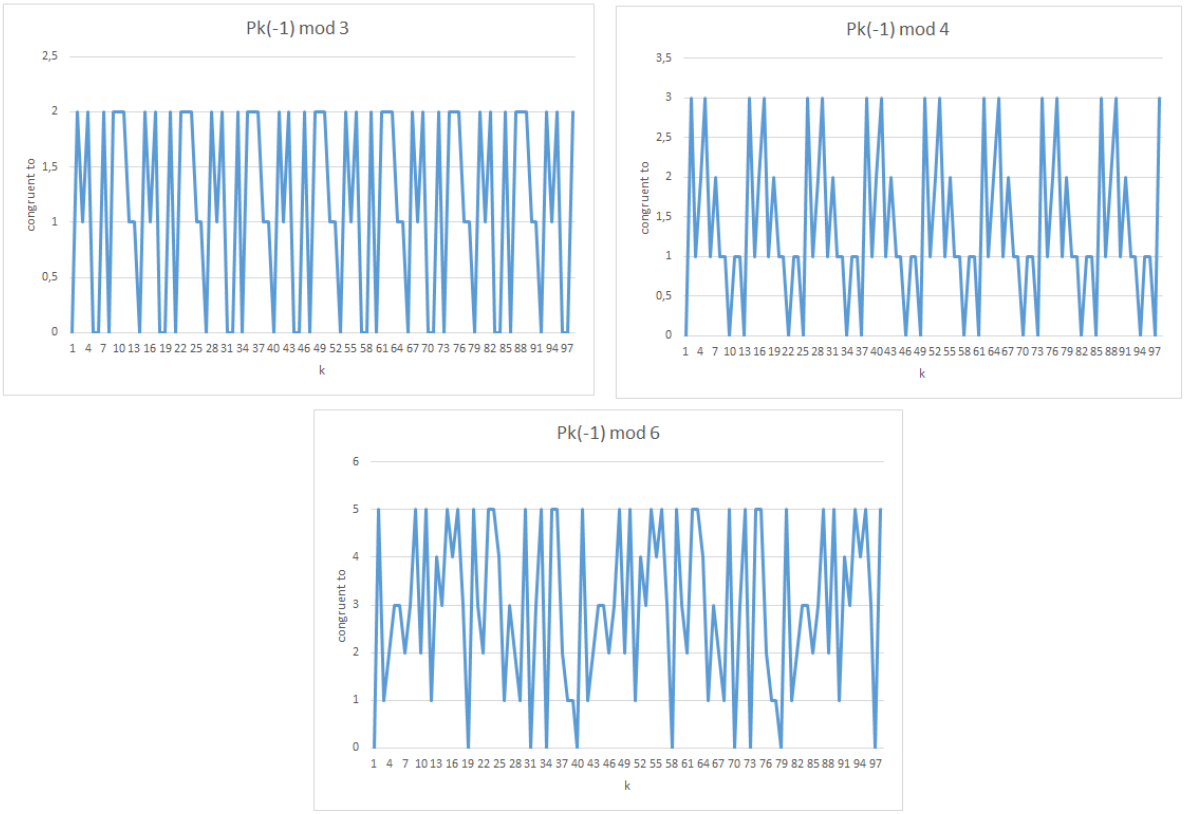


Figure 10: Result of $P_k(-1)$ modulo 3, 4 and 6 (in this order) for k until 100.

The same results occur with $P_k(1)$ and r_k. The following figures illustrate the representation of $P_k(1)$ and r_k modulo 3, 4 and 6 for some consecutive values of k.

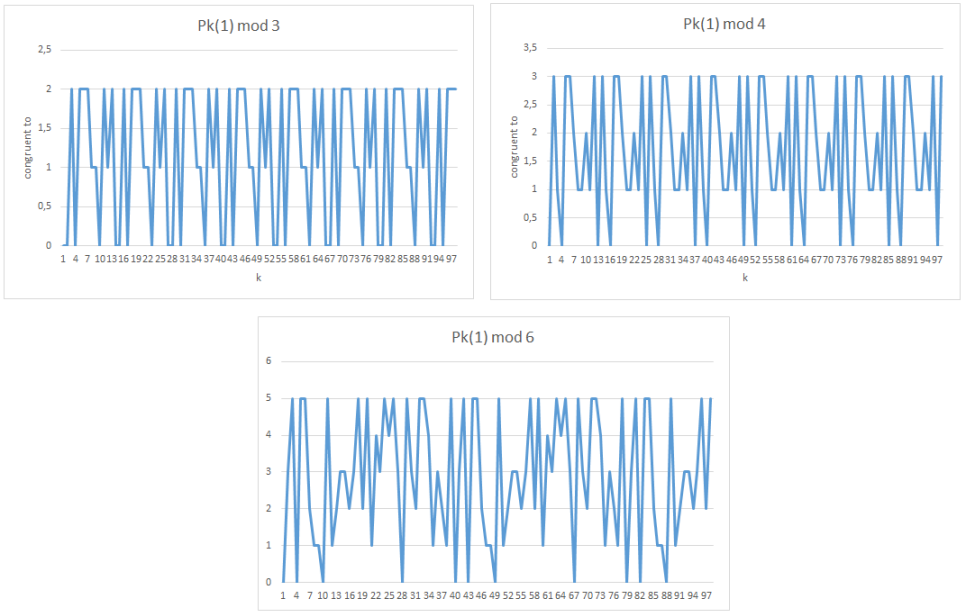


Figure 11: Result of $P_k(1)$ modulo 3, 4 and 6 (in this order) for k until 100.

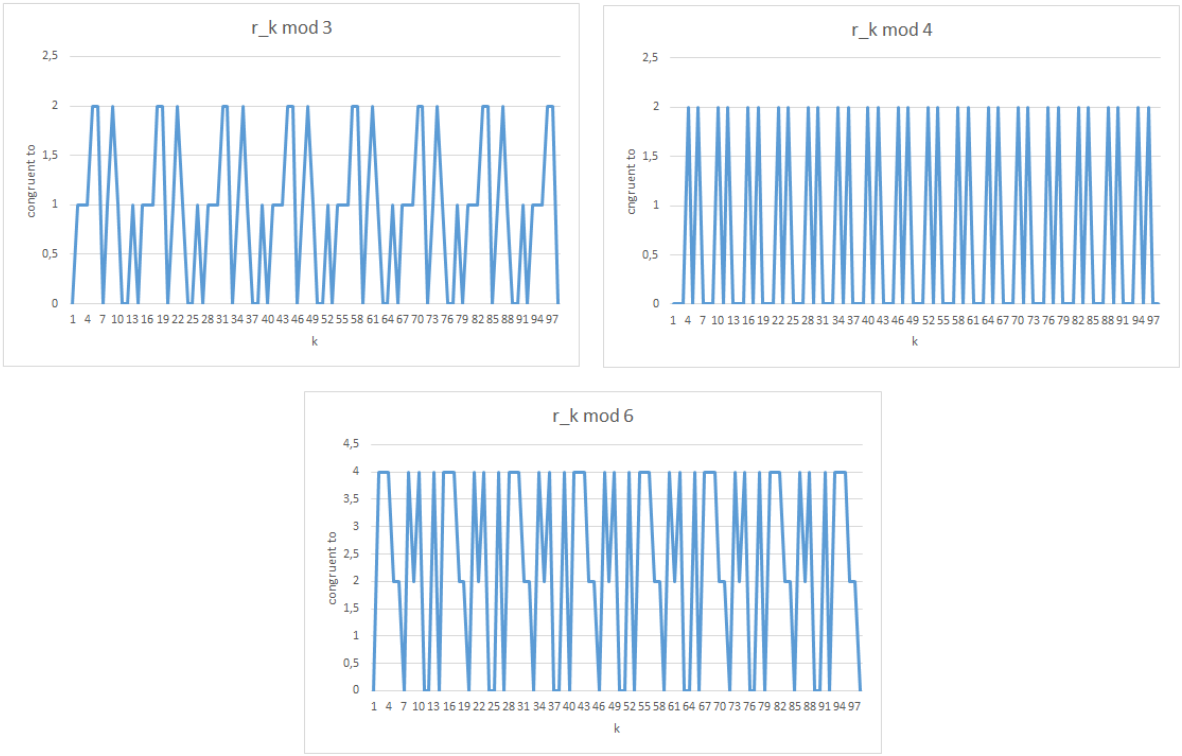


Figure 12: Result of r_k modulo 3, 4 and 6 (in this order) for k until 100.

Although the patterns are different in these other examples, the cycles are also very clear. On the other hand, if we try to find a cycle in any other prime, power of prime, or any composite number in general, we do not spot any patterns. Figure 13 shows an example of $P_k(-1)$ evaluated modulo 5.

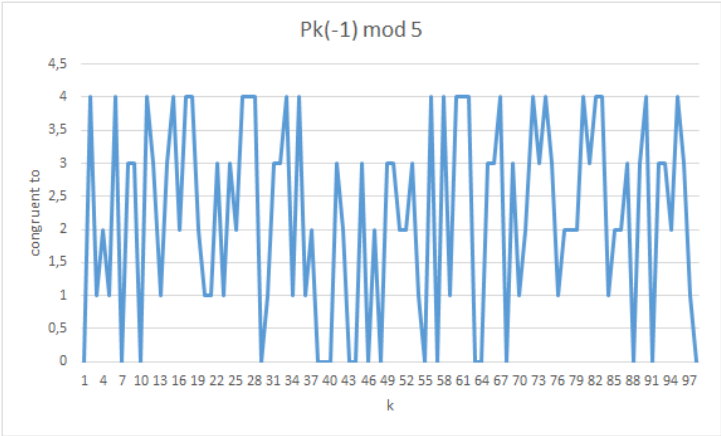


Figure 13: Result of $P_k(-1)$ modulo 5 for k until 100. No cycles are spotted.

We next study the relationship between the length of the different cycles. For instance, the length of the cycle of $P_k(-1)$ modulo 3 is 13, whereas the length of the cycle is 39 modulo 3 and 117 modulo 27. Observe that $39 = 13 \cdot 3$ and $117 = 39 \cdot 3$.

The same relationship occurs with the powers of 2. The length of the cycle of $P_k(-1)$ is 12 modulo 4; 24 modulo 8, 48 modulo 16 and 96 modulo 32. Observe that $24 = 12 \cdot 2$, $48 = 24 \cdot 2$ and $96 = 48 \cdot 2$. This also happens for powers of 6. Let L_{p^x} denote the length of the cycle of any of the three sequences $P_k(1)$, $P_k(-1)$, r_k) modulo p^x. Then we observe that the lengths of the cycles of $P_k(-1)$ are the following:

$$L_{2^x} = 3 \cdot 2^x \qquad L_{3^x} = 13 \cdot 3^{x-1} \qquad L_{6^x} = 39 \cdot 4^{x-1}$$

Moreover, the lengths of the cycles of $P_k(1)$ are:

$$L_{2^x} = 3 \cdot 2^x \qquad L_{3^x} = 13 \cdot 3^{x-1} \qquad L_{6^x} = 39 \cdot 2^{x-1}$$

Finally, the lengths of the cycles of r_k are:

$$L_{2^x} = 3 \cdot 2^{x-1} \qquad L_{3^x} = 13 \cdot 3^{x-1} \qquad L_{6^x} = 13 \cdot 6^{x-1}$$

The following three tables summarize the length of the cycles modulo powers of 2, 3 and 6 for $P_k(-1)$, $P_k(1)$ and r_k respectively. The powers of 2 are marked with blue, the powers of 3 are marked with red and the powers of 6 are marked with green.

mod	3	4	6	8	9	16	27	32	36
length	13	12	39	24	39	48	117	96	156

Table 5: Relationship between the modulo and the length of the cycle for $P_k(-1)$.

mod	3	4	6	8	9	16	27	32	36
length	13	12	39	24	39	48	117	96	78

Table 6: Relationship between the modulo and the length of the cycle for $P_k(1)$.

mod	3	4	6	8	9	16	27	32	36
length	13	6	13	12	39	24	117	48	78

Table 7: Relationship between the modulo and the length of the cycle for r_k.

Now we recall the conjecture stated in Section 6.1:

The series $\sum_{n=1}^{\infty} n^k n!$ *only converges to an integer for* $k = 1$.

Because, by Observation 6.1, $P_{k+1}(-1) = P_k(0) = s_k$, this conjecture is equivalent to the following:

Conjecture 7.8. *The number* $P_k(-1)$ *is* 0 *only for* $k = 2$.

Even though cycles only occur under the conditions stated in this section (using the opposite modulo n whenever $P_k(-1)$ is negative), this is not relevant whenever $P_k(-1)$ is zero modulo n. Therefore, with our variation of computing these congruences, we obtain cycles if n is a power of 2, 3 or 6, which are very useful when we consider the case in which $P_k(-1)$ is zero modulo n. For the values of n such that there exist these cycles we mark whenever $P_k(-1)$ is zero modulo n. Our main idea is the following: If $P_k(-1)$ is not 0 modulo n for any value of n, then $P_k(-1)$ cannot be zero, which means that the series does not converge to an integer. So for instance, in the cycle of length 12 generated by $n = 4$ there are two zeroes: in the first place of the cycle and in the 10^{th} place of the cycle. Because it is a cycle, it means that $P_k(-1)$ can be zero only if $k \equiv 2$ or $k \equiv 11$ modulo 12 (because we start the cycle at $k = 2$).

We can improve these results by combining different cycles. Combining the cycles for $n = 3, 4, 27, 81$ and using the Chinese Remainder Theorem [32] we obtain the following:

Observation 7.9. *$P_k(-1)$ can be zero only if $k \equiv 2$ or $k \equiv 1010$ modulo 1404.*

Because we use $n = 3, 4, 27, 81$, we combined the length of each cycle and computed the least common multiple, which is 1404. We checked all zeroes of each cycles until 1404 and found out that $P_k(-1)$ is zero modulo 3, 4, 27 and 81 only when $k = 2$ and $k = 1010$. Therefore, because this is cyclic, we can generalize this result modulo 1404. Clearly, by combining even more cycles we could obtain better results. However, we would never eliminate one zero: $P_1(-1) \equiv 0$ modulo n for any value of n, because $\sum n^k n!$ converges to an integer when $k = 1$. The following picture shows how we investigated the different cycles using their zeroes modulo powers of 2 and powers of 3.

MOD 2	MOD 3	MOD 4	MOD 6	MOD 8	MOD 9	MOD 16	MOD 32	MOD 27	MOD 81
0	0	0	0	0	0	0	0	0	0
1	2	3	5	7	8	15	31	26	80
1	1	1	1	1	1	1	1	1	1
0	2	2	2	2	2	2	2	2	2
1	0	3	3	7	0	7	23	18	72
1	0	1	3	1	0	9	9	9	9
0	2	2	2	2	5	2	18	23	50
1	0	1	3	5	3	5	21	3	57
1	2	1	5	5	8	13	29	8	8
0	2	0	2	4	2	4	4	20	74
1	2	1	5	5	8	13	29	8	8
1	1	1	1	5	7	5	5	16	70
0	1	0	4	0	7	0	0	16	16
1	0	3	3	3	0	3	19	18	45
1	2	1	5	5	5	13	13	23	50
0	1	2	4	2	4	2	2	13	13
1	2	3	5	3	5	11	11	23	23
1	0	1	3	5	0	13	29	9	36
0	0	2	0	2	0	10	26	9	9
1	2	1	5	1	5	1	17	5	32
1	0	1	3	1	6	9	25	15	69
0	2	0	2	4	8	12	12	26	53
1	2	1	5	1	5	9	9	5	5
1	2	1	5	1	5	9	25	23	23
0	1	0	4	0	1	0	0	10	37
1	1	3	1	7	1	7	23	1	55
1	0	1	3	1	3	9	9	3	30
0	2	2	2	2	5	2	2	5	5
1	1	3	1	7	7	15	15	7	61
1	2	1	5	1	5	1	1	23	77
0	0	2	0	2	3	2	2	21	48
1	0	1	3	5	6	13	29	15	15
1	2	1	5	5	5	5	5	14	41
0	0	0	0	4	0	4	20	18	45
1	2	1	5	5	5	5	5	14	41
1	2	1	5	5	8	13	29	26	53
0	2	0	2	0	8	0	0	8	8
1	1	3	1	3	1	11	11	19	73
1	1	1	1	5	1	5	21	19	46

Figure 14: Data collected and analyzed to obtain the results on the number of zeroes in the combined cycles. In different colors we mark the zeroes.

8 Conclusions

In this part of the work we have investigated a recent topic in mathematics: p-adic analysis. It has been a very challenging experience to learn a whole theory about a new branch of mathematics. Our work focused on some uses of the factorial function, mainly p-adic series in which the factorial function is involved.

After studying background of p-adic numbers, including Newton's Method and Hensel's Lemma, the main goal of this work has been the conjectural p-adic irrationality of $\sum n!$. It is believed to be irrational for all primes p, but there is no known proof. In this work we considered a p-adic analogue of the factorial function inspired by Stirling's formula and based on Legendre's formula. One of our main results is that the series whose general term is this p-adic analogue converges to an irrational p-adic integer for all p. This result has been included into an article that was posted in the arXiv database [3].

We also considered the series $\sum_{n=0}^{\infty} n^k(n+m)!$ and one of our conjectures is that $\sum_{n=0}^{\infty} n^k(n+m)!$ only converges to an integer for $k = 1$ and $m = 0$; $k = 2$ and $m = 1$; $k = 5$ and $m = 1$. We provided a recursive method to compute the sum of these series in terms of polynomials $P_k(m)$. Moreover, we described a recursive formula for computing $P_k(-1)$, $P_k(1)$ and $r_k = P_k(-1) - P_k(1)$. Using arguments from modular arithmetic, another relevant result is that the series $\sum_{n=0}^{\infty} n^k(n+1)!$ does not converge to an integer if $k \equiv 0 \pmod 3$ or $k \equiv 1 \pmod 3$.

Although we consider that we have obtained significant results about p-adic series containing factorials, we have encountered conjectures that still need to be proven. We believe that the sequence r_k introduced in the last section of this work can lead to stronger results because of our observation that $P_k(-1)$ and $P_k(1)$ are cyclic modulo n when n is a power of 2, 3 or 6. Further results might be obtained by inspecting for which values of m we have that $P_k(m)$ is cyclic modulo n for a fixed value of n.

Most of our conclusions and proofs were obtained after running C++ programs that we wrote for this purpose. Outputs of those programs provided large amounts of numerical evidence supporting the conjectures that we formulated and guiding our way to the new results contained in this work.

9 Appendix

9.1 Code

In this section we provide the code of the programs used for this work. For all the programs in this section we include the code and an example of the output.

Newton's Method

```
#include<iostream>
#include<cmath>
#include<vector>
using namespace std;


double der(double f, double fn, double n, double r, double s, double v, vector <int> coef, vector <int> deri, int p, int q){
if (p<5){
    double fd=0;
    fn=0;
    for (int i=0; i<n; i++){
        fd = fd + deri[i]*pow(v,(deri.size()-1-i));
    }
    for (int i=0; i<n+1; i++){
        fn = fn + coef[i]*pow(v,(coef.size()-1-i));
    }
    v = v - (fn/fd);
    p++;
    return der(f, fn, n, r, s, v, coef, deri, p, q);
}
else{
    return v;
}
}

double bolz(double f, double fn, double n, double r, double s, double v, vector <int> coef, vector <int> deri, int p, int q){
s=0.01;
    if (f<0){
        while(fn<0){
            fn=0;
```

```
            for (int i=0; i<n+1; i++){
                fn = fn + coef[i]*pow(r+s,(coef.size()-1-i));
        }
        s = s+0.01;
        }
    v = r+s-0.01;
    fn = 0;
        for (int i=0; i<n+1; i++){
                fn = fn + coef[i]*pow(v,(coef.size()-1-i));
        }
    return der(f, fn, n, r, s, v, coef, deri, p, q);
}
    if (f>0){
        while(fn>0){
            fn=0;
            for (int i=0; i<n+1; i++){
                fn = fn + coef[i]*pow(r+s,(coef.size()-1-i));
        }
        s = s+0.01;
        }
    v = r+s-0.01;
    fn = 0;
        for (int i=0; i<n+1; i++){
                fn = fn + coef[i]*pow(v,(coef.size()-1-i));
        }
    return der(f, fn, n, r, s, v, coef, deri, p, q);
}
}

float sii(double f, double fn, double n, double r, double s, double v, vector <int> coef, vector <int> deri, int p, int q){
```

```
f=0;
fn=0;
v = v+0.1;
    for (int i=0; i<n+1; i++){
        f = f + coef[i]*pow(v,(coef.size()-1-i));
    }
    for (int i=0; i<n+1; i++){
        fn = fn + coef[i]*pow(v+0.01,(coef.size()-1-i));
        }
    r = v;
    return bolz(f, fn, n, r, s, v, coef, deri, p, q);
    }


int main(){
double n, a, r=0, f=0, fn=0, s=0.01, p=0, v=0, q=0, t=0; //n el grau,
vector <int> coef;
vector <int> deri;
cout<<"Introdueix el grau del polinomi: ";
cin>>n;
q=n;
cout<<"Introdueix els coeficients en ordre: "<<endl;
for (int i=0; i<n+1; i++){
    cin>>a;
    coef.push_back(a);
}
cout<<"---"<<endl;
for (int i=0; i<n+1; i++){
    deri.push_back((coef.size()-1-i)*coef[i]);
    r = r + abs(coef[i]);
```

```
    coef.push_back(a);
}
cout<<"---"<<endl;
for (int i=0; i<n+1; i++){
    deri.push_back((coef.size()-1-i)*coef[i]);
    r = r + abs(coef[i]);
}
deri.pop_back();

for (int i=0; i<n+1; i++){
    f = f + coef[i]*pow(-r,(coef.size()-1-i));
}
for (int i=0; i<n+1; i++){
    fn = fn + coef[i]*pow(-r+s,(coef.size()-1-i));
}

v = bolz(f, fn, n, -r, s, v, coef, deri, p, q);
cout<<v<<endl;
q = q-1;

while(q!=0){
    if(v<r){
        v = sii(f, fn, n, r, s, v, coef, deri, p, q);
        cout<<v<<endl;
        q=q-1;
}

}
}
```

```
Introduce the degree of the polynomial: 2
Introduce the coefficients in order:
1
0
-2
---
-1.41421
1.41421

Process returned 0 (0x0)   execution time : 4.280 s
Press any key to continue.
```

Hensel's Lemma

```
#include<iostream>
#include<vector>
#include<cmath>
using namespace std;

int hensel(int p, int j, vector<int> deri, vector<int> red, int exp, int n, int er){
int t=0, fpri=0, ll=0, zz=0;
long double yy=0;
double qw, pff, ptt, fprit;
if (exp<10){
     er=0;
     for (int q=0; q<n; q++){
        fprit = deri[q]*pow(j, (n-q));
}
    fpri = fprit;
    if (fpri%p==0){
        cout<<"ERROR"<<endl;
        er = 1;
    }
    for (int q=0; q<n+1; q++){
        yy = yy + red[q]*pow(j, (n-q));
    }
    for (int kk=0; kk<exp; kk++){
        yy = yy/p;
    }
    for (int t=0; t<p; t++){
        ptt = yy + t*fprit;
        zz = ptt;
    if (zz%p==0){
        cout<<t<<"*"<<p<<"^"<<exp<<" + ";
        qw = t;
        break;
    }
```

```
    }
    pff = j + qw*(pow(p,exp));
    j = pff;
    exp++;
    ll = pow(p,exp);
    j = j%ll;
    if(er==1){
        return 0;
    }
    else{
        return hensel(p, j, deri, red, exp, n, er);
    }
}
else{
    return p;
}
}


int main(){
int n, y, p, zz, exp=1, i=0, er;
long double xx, yy, ee;
vector <int> coef;
vector <int> red;
vector <int> deri;
cout<<"Introdueix el grau del polinomi: ";
cin>>n;
cout<<"Introdueix els coeficients en ordre: "<<endl;
for (int e=0; e<n+1; e++){
    cin>>y;
    coef.push_back(y);
}
int a=2, b=3, z=0;
```

```
vector <int> pr;
pr.push_back(2);
while (b<30){
    for (a=2; a*a<=b; a++){
        if (b%a==0){
        z=1;
        break;
}
}
    if (z==0){
        pr.push_back(b);

}
   z=0;
   b = b+2;
}
for (int i=0; i<12; i++){
    for (int j=0; j<pr[i]; j++){
        red.clear();
        for (int w=0; w<n+1; w++){
            red.push_back(coef[w]%pr[i]);
        }
        ee=0;
        yy=0;
        int ss=0;
        for (int q=0; q<n+1; q++){
            ee = ee + red[q]*pow(j, (n-q));
        }
        ss = ee;
        if (ss%pr[i]==0){
            p = pr[i];
            for (int ii=0; ii<n+1; ii++){
            deri.push_back((coef.size()-1-i)*coef[i]);
}
deri.pop_back();
cout<<j<<" + ";
cout<<hensel(p, j, deri, red, exp, n, er)<<endl;
cout<<"MOD "<<pr[i]<<" x1 = "<<j<<endl;
        }
    }
}
}
```

```
Introduce the degree of the polynomial: 2
Introduce the coefficients in order:
1
0
-5
1 + ERROR
0*2^1 + 0
MOD 2 x1 = 1

0 + ERROR
0*5^1 + 0
MOD 5 x1 = 0

4 + 4*11^1 + 10*11^2 + 4*11^3 + 0*11^4 + 9*11^5 + 5*11^6 + 8*11^7 + 1*11^9 + 11
MOD 11 x1 = 4

7 + 6*11^1 + 0*11^2 + 6*11^3 + 10*11^4 + 1*11^5 + 5*11^6 + 2*11^7 + 3*11^8 + 11
MOD 11 x1 = 7

9 + 4*19^1 + 1*19^2 + 10*19^3 + 15*19^4 + 7*19^5 + 11*19^6 + 19
MOD 19 x1 = 9

10 + 14*19^1 + 17*19^2 + 8*19^3 + 3*19^4 + 11*19^5 + 7*19^6 + 19
MOD 19 x1 = 10

11 + 13*29^1 + 9*29^2 + 27*29^3 + 0*29^4 + 3*29^5 + 11*29^8 + ERROR
0*29^9 + 0
MOD 29 x1 = 11

18 + 15*29^1 + 19*29^2 + 1*29^3 + 28*29^4 + 25*29^5 + 1*29^6 + 0*29^7 + 29
MOD 29 x1 = 18
```

p-Adic inverses

```
#include<iostream>
#include<cmath>
#include<vector>
using namespace std;

int recur(int r, int p, int j, int passau, int passados, int c, int exp){
if (c==15){
    return 0;
}
else {
    passados = p-passau;
    j = (r*passados)%p;
    cout<<j<<"*"<<p<<"^"<<exp<<" + ";
    passau = (passau+r*j)/p;
    c++;
    exp++;
    return recur(r, p, j, passau, passados, c, exp);
}
}

int main(){
int n, d, r, passau, passados, p, c=0, exp=1;
cout<<"Introdueix el numerador: "<<endl;
cin>>n;
cout<<"Introdueix el denominador: "<<endl;
cin>>d;
int a=2, b=3, z=0;
vector <int> pr;
pr.push_back(2);
while (b<30){
    for (a=2; a*a<=b; a++){
        if (b%a==0){
```

```
int a=2, b=3, z=0;
vector <int> pr;
pr.push_back(2);
while (b<30){
    for (a=2; a*a<=b; a++){
        if (b%a==0){
        z=1;
        break;
}
}
    if (z==0){
        pr.push_back(b);

}
    z=0;
    b = b+2;
}
for (int i=0; i<5; i++){
    for (int j=0; j<pr[i]; j++){
        if((d*j)%pr[i]==n){
            r = j;
            cout<<"MOD"<<pr[i]<<": ";
            cout<<r<<" + ";
            passau = (d*j)/pr[i];
            p = pr[i];
            cout<<recur(r, p, j, passau, passados, c, exp)<<endl;
    }
    }
}
}
```

We can use our program to find the p-adic expansion described in Section 2.5.

```
Introduce the numerator:
1
Introduce the denominator:
7

MOD 2: 1 + -1*2^1 + 1*2^2 + 1*2^3 + 1*2^4 + 1*2^5 + 1*2^6 + 1*2^7 + 1*2^8 + 1*2^9 + 1*2^10 + 1*2^11 + 1*2^12 + 1*2^13 + 1*2^14 + 1*2^15 + 0
MOD 3: 1 + 1*3^1 + 2*3^2 + 2*3^3 + 2*3^4 + 2*3^5 + 2*3^6 + 2*3^7 + 2*3^8 + 2*3^9 + 2*3^10 + 2*3^11 + 2*3^12 + 2*3^13 + 2*3^14 + 2*3^15 + 0
MOD 5: 3 + 3*5^1 + 4*5^2 + 4*5^3 + 4*5^4 + 4*5^5 + 4*5^6 + 4*5^7 + 4*5^8 + 4*5^9 + 4*5^10 + 4*5^11 + 4*5^12 + 4*5^13 + 4*5^14 + 4*5^15 + 0
MOD 11: 8 + 4*11^1 + 9*11^2 + 7*11^3 + 4*11^4 + 9*11^5 + 7*11^6 + 4*11^7 + 9*11^8 + 7*11^9 + 4*11^10 + 9*11^11 + 7*11^12 + 4*11^13 + 9*11^14 + 7*11^15 + 0
MOD 13: 2 + 11*13^1 + 11*13^2 + 11*13^3 + 11*13^4 + 11*13^5 + 11*13^6 + 11*13^7 + 11*13^8 + 11*13^9 + 11*13^10 + 11*13^11 + 11*13^12 + 11*13^13 + 11*13^14 + 11*13^15 + 0
MOD 17: 5 + 7*17^1 + 7*17^2 + 7*17^3 + 7*17^4 + 7*17^5 + 7*17^6 + 7*17^7 + 7*17^8 + 7*17^9 + 7*17^10 + 7*17^11 + 7*17^12 + 7*17^13 + 7*17^14 + 7*17^15 + 0
MOD 19: 11 + 13*19^1 + 18*19^2 + 4*19^3 + 16*19^4 + 15*19^5 + 15*19^6 + 15*19^7 + 15*19^8 + 15*19^9 + 15*19^10 + 15*19^11 + 15*19^12 + 15*19^13 + 15*19^14 + 15*19^15 + 0

Process returned 0 (0x0)   execution time : 3.261 s
Press any key to continue.
```

Convergence of $\sum n!$

```
#include<iostream>
#include<vector>
#include<cmath>
#include<set>
#include<string>
#include<sstream>
#include "BigIntegerLibrary.hh"


using namespace std;

string int2string(int n){
    stringstream s;
    s << n; //el numero n passa a ser s
    return(s.str());
}

BigInteger base(BigInteger n, BigInteger b, BigInteger res, int cops, BigInteger help, vector<BigInteger> v){
    if(n>=b){
        help = n - (n/b)*b;
        v.push_back(help);
        n = n/b;
        cops++;
        base(n, b, res, cops, help, v);
    }
    else{
        v.push_back(n);
        for(int i=0; i<v.size(); i++){
            string aa;
            BigInteger a = stringToBigInteger(aa);
            a = v[v.size()-1-i];
            //cout<<"vector: "<<a<<endl;
            for(int j=1; j<v.size()-i; j++){
                a = a*10;
            }
            //cout<<"suit: "<<a<<endl;
            res = res+a;
        }
        cout<<res<<endl<<endl;
```

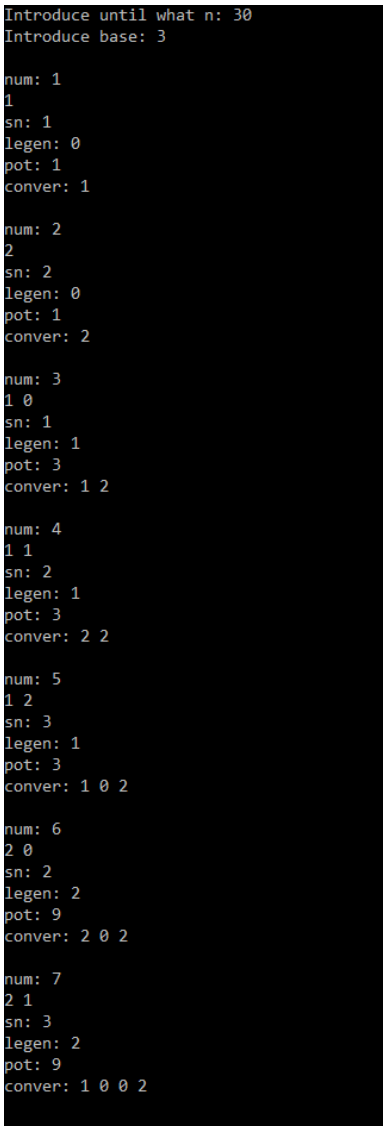
```
    }
}

int main(){
    //string nn;
    //BigInteger n = stringToBigInteger(nn);
    cout<<"Introduce until what n: ";
    int finsn;
    cin>>finsn;
    cout<<"Introduce base: ";
    string bb;
    cin>>bb;
    BigInteger b = stringToBigInteger(bb);
    //BigInteger m = n;
    string ress;
    BigInteger res = stringToBigInteger(ress);
    res = 0;
    string helpp;
    BigInteger help = stringToBigInteger(helpp);
    help = 0;
    vector<BigInteger> v;
    string unnn;
    BigInteger unn = stringToBigInteger(unnn);
    unn = 1;
    string dosnn;
    BigInteger dosn = stringToBigInteger(dosnn);
    dosn = 2;
    string totall;
    BigInteger total = stringToBigInteger(totall);
    total = 1;
    for(int i=1; i<=finsn; i++){
        string iii = int2string(i);
        BigInteger ii = stringToBigInteger(iii);
        unn = unn*ii;
        cout<<"factorial: "<<unn<<endl;
        total = total + unn;
        cout<<"convergence: "<<total<<endl;
        base(total, b, 0, 0, 0, v);
    }
```

```
Introduce until what n: 30
Introduce base: 5
factorial: 1
convergence: 2
2

factorial: 2
convergence: 4
4

factorial: 6
convergence: 10
20

factorial: 24
convergence: 34
114

factorial: 120
convergence: 154
1104

factorial: 720
convergence: 874
11444

factorial: 5040
convergence: 5914
142124

factorial: 40320
convergence: 46234
2434414

factorial: 362880
convergence: 409114
101042424

factorial: 3628800
convergence: 4037914
2013203124
```

p-Adic approximation of $\sum n!$: Legendre's formula

This code computes the number of ending zeroes of $n!$ using Legendre's formula for a given base. Then it computes the convergence of the series $\sum p^{\frac{n-S_p(n)}{p-1}}$ in $\mathbb{Z}_p$.

```
int main(){
    //string nn;
    //BigInteger n = stringToBigInteger(nn);
    cout<<"Introduce until what n: ";
    int finsn;
    cin>>finsn;
    cout<<"Introduce base: ";
    string bb;
    cin>>bb;
    cout<<endl;
    BigInteger b = stringToBigInteger(bb);
    //BigInteger m = n;
    vector<BigInteger> resultat;
    string converr;
    BigInteger conver = stringToBigInteger(converr);
    conver = 0;
    for(int i=1; i<=finsn; i++){
        cout<<"num: "<<i<<endl;
        vector<BigInteger> v;
        string iii = int2string(i);
        BigInteger ii = stringToBigInteger(iii);
        string copss;
        BigInteger cops = stringToBigInteger(copss);
        cops = 0;
        string nn;
        BigInteger n = stringToBigInteger(nn);
        n = ii;
        string helpp;
        BigInteger help = stringToBigInteger(helpp);
        while(n>=b){
            help = n - (n/b)*b;
            v.push_back(help);
            n = n/b;
            cops++;
        }
            string snn;
            BigInteger sn = stringToBigInteger(snn);
            sn = 0;
            v.push_back(n);
            for(int k=0; k<v.size(); k++){
                string aa;
                BigInteger a = stringToBigInteger(aa);
                a = v[v.size()-1-k];
                cout<<a<<" ";
                sn = sn+a;
            }
            //cout<<endl<<"nn: "<<nn<<endl<<"n: "<<ressu<<endl;
            string ressu;
            BigInteger ress = stringToBigInteger(ressu);
            ress = (ii-sn)/(b-1);
            cout<<endl<<"sn: "<<sn<<endl<<"legen: "<<ress<<endl;
            string pp;
            BigInteger p = stringToBigInteger(pp);
            p = b;
            string jj;
            BigInteger j = stringToBigInteger(jj);
            j = ress;
            if(ress==0){
                p = 1;
            }
            else{
                while(j>1){
                p = p*b;
                j--;
                }
            }
            cout<<"pot: "<<p<<endl<<"conver: ";
            conver = conver + p;
            v.clear();
            base(conver, 0, b, 0, 0, 0, v, conver, resultat);
            cout<<endl<<endl;
        }
    }
```



Values of s_k

This code computes the coefficient of α in the sum of the series $\sum n^k n!$ (the value of s_k) and the coefficient of α in the sum of the series $\sum n^k (n+1)!$ for each k.

```cpp
#include<iostream>
#include<vector>
#include<cmath>
#include<set>
#include<string>
#include<sstream>
#include "BigIntegerLibrary.hh"


using namespace std;

string int2string(int n){
    stringstream s;
    s << n; //el numero n pasaa a ser s
    return(s.str());
}

int main(){
    cout<<"Introduce until what n: ";
    int nnn;
    cin>>nnn;
    string nn = int2string(nnn);
    BigInteger n = stringToBigInteger(nn);
    vector<BigInteger> vres;
    vector<vector<BigInteger> > vpol1 (nnn+1);
    vector<vector<BigInteger> > vpol2 (nnn+1);
    vres.push_back(-1);
    string unn;
    BigInteger un = stringToBigInteger(unn);
    un = 1;
    vector<BigInteger> alpha;
    vector<BigInteger> indep;
    string alphanumm;
    BigInteger alphanum = stringToBigInteger(alphanumm);
    string indepnumm;
    BigInteger indepnum = stringToBigInteger(indepnumm);
    string sumafactt;
    BigInteger sumafact = stringToBigInteger(sumafactt);
```

```cpp
    sumafact = 0;
    alpha.push_back(1);
    alpha.push_back(0);
    indep.push_back(1);
    indep.push_back(-1);
    vpol1[1].push_back(1);
    vpol1[1].push_back(1);
    vector <vector <BigInteger> > bino (nnn);
    bino[0].push_back(1);
    bino[1].push_back(1);
    bino[1].push_back(1);
    for(unsigned long long int i=2; i<nnn; i++) {
        //cout<<endl<<endl<<1<<"  ";
        bino[i].push_back(1);
        for(unsigned long long int j=1; j<i; j++){
            bino[i].push_back(bino[i-1][j-1]+bino[i-1][j]);
            //cout<<bino[i][j]<<"  ";
        }
        bino[i].push_back(1);
    }
    for(int i=2; i<nnn; i++){
        alphanum = 0;
        indepnum = 0;
        string ii = int2string(i);
        BigInteger iii = stringToBigInteger(ii);
        vpol1[i].push_back(1);
        //cout<<1<<"  ";
        for(int j=1; j<i; j++){
            string jj = int2string(j);
            BigInteger jjj = stringToBigInteger(jj);
            vpol1[i].push_back(vpol1[i-1][j]+iii*vpol1[i-1][j-1]);
            //cout<<vpol1[i][j]<<"  ";
            alphanum = alphanum + vpol1[i][j]*alpha[i-j];
            indepnum = indepnum + vpol1[i][j]*indep[i-j];
        }
        vpol1[i].push_back(vpol1[i-1][i-1]*i);
        //cout<<vpol1[i-1][i-1]*i<<endl;
        alphanum = alphanum + vpol1[i][i];
        indepnum = indepnum + vpol1[i][i];
```

```
78          un = un*(iii-1);
79          sumafact = sumafact + un;
80          cout<<"alpha1: "<<(alpha[0]-alphanum)<<endl;
81          alpha.push_back(alpha[0]-alphanum);
82          cout<<"indep1: "<<(-indepnum-sumafact)<<endl;
83          indep.push_back(-indepnum-sumafact);
84          string alphaconverr;
85          BigInteger alphaconver = stringToBigInteger(alphaconverr);
86          alphaconver = 0;
87          string indepconverr;
88          BigInteger indepconver = stringToBigInteger(indepconverr);
89          indepconver = 0;
90          indep[0]=0;
91          for(int k=0; k<=i; k++){
92              if(k%2==0){
93                  alphaconver = alphaconver + (bino[i][k]*alpha[i-k]);
94                  indepconver = indepconver + (bino[i][k]*indep[i-k]);
95              }
96              else{
97                  alphaconver = alphaconver + (bino[i][k]*alpha[i-k])*(-1);
98                  indepconver = indepconver + (bino[i][k]*indep[i-k])*(-1);
99              }
100         }
101         indep[0]=1;
102         cout<<"alpha2: "<<alphaconver<<endl;
103         cout<<"indep2: "<<indepconver<<endl;
104         cout<<endl;
105     }
106 }
```

```
Introduce until what n: 20
alpha1: -1
indep1: 0
alpha2: 0
indep2: 2

alpha1: 1
indep1: 2
alpha2: 3
indep2: -1

alpha1: 2
indep1: -3
alpha2: -7
indep2: -7

alpha1: -9
indep1: -4
alpha2: 0
indep2: 26

alpha1: 9
indep1: 30
alpha2: 59
indep2: -25

alpha1: 50
indep1: -55
alpha2: -217
indep2: -181

alpha1: -267
indep1: -126
alpha2: 146
indep2: 1064

alpha1: 413
indep1: 1190
alpha2: 2593
indep2: -2143

alpha1: 2180
indep1: -3333
alpha2: -15551
indep2: -7855

alpha1: -17731
indep1: -4522
alpha2: 32802
indep2: 85832
```

Sum of the series $\sum n^k(n+m)!$

This code computes the coefficient of α for the sum of the series $\sum n^k(n+m)!$, for all possible combinations of k and m. This is the main program of the whole work, because it computes the generalization of the series that helped come up with Conjecture 6.2.

```
#include<iostream>
#include<vector>
#include<cmath>
#include<set>
#include<string>
#include<sstream>
#include <bits/stdc++.h>
#include "BigIntegerLibrary.hh"


using namespace std;

string int2string(int n){
    stringstream s;
    s << n; //el número n pasado a str s
    return(s.str());
}

int main(){
    cout<<"Introduce until which k, n^k: ";
    int mmm;
    cin>>mmm;
    string mm = int2string(mmm);
    BigInteger m = stringToBigInteger(mm);
    cout<<"Introduce until what r, n^k(n+r)!: ";
    int nnn;
    cin>>nnn;
    string nn = int2string(nnn);
    BigInteger n = stringToBigInteger(nn);
    vector<BigInteger> vres;
    vector<vector<BigInteger> > vpol1 (nnn+1);
    vres.push_back(-1);
    string unn;
    BigInteger un = stringToBigInteger(unn);
    un = 1;
    vector<BigInteger> alpha;
    vector<BigInteger> indep;
    string alphanumm;
    BigInteger alphanum = stringToBigInteger(alphanumm);
```

```
    string indepnumm;
    BigInteger indepnum = stringToBigInteger(indepnumm);
    string sumafactt;
    BigInteger sumafact = stringToBigInteger(sumafactt);
    sumafact = 0;
    alpha.push_back(1);
    alpha.push_back(0);
    indep.push_back(1);
    indep.push_back(-1);
    vpol1[1].push_back(1);
    vpol1[1].push_back(1);
    vector <vector <BigInteger> > bino (nnn);
    bino[0].push_back(1);
    bino[1].push_back(1);
    bino[1].push_back(1);
    for(unsigned long long int i=2; i<nnn; i++) {
        //cout<<endl<<endl<<1<<"  ";
        bino[i].push_back(1);
        for(unsigned long long int j=1; j<i; j++){
            bino[i].push_back(bino[i-1][j-1]+bino[i-1][j]);
            //cout<<bino[i][j]<<"  ";
        }
        bino[i].push_back(1);
    }
    for(int i=2; i<=mmm; i++){
        alphanum = 0;
        indepnum = 0;
        string ii = int2string(i);
        BigInteger iii = stringToBigInteger(ii);
        vpol1[i].push_back(1);
        //cout<<1<<"  ";
        for(int j=1; j<i; j++){
            string jj = int2string(j);
            BigInteger jjj = stringToBigInteger(jj);
            vpol1[i].push_back(vpol1[i-1][j]+iii*vpol1[i-1][j-1]);
            //cout<<vpol1[i][j]<<"  ";
            alphanum = alphanum + vpol1[i][j]*alpha[i-j];
            indepnum = indepnum + vpol1[i][j]*indep[i-j];
```

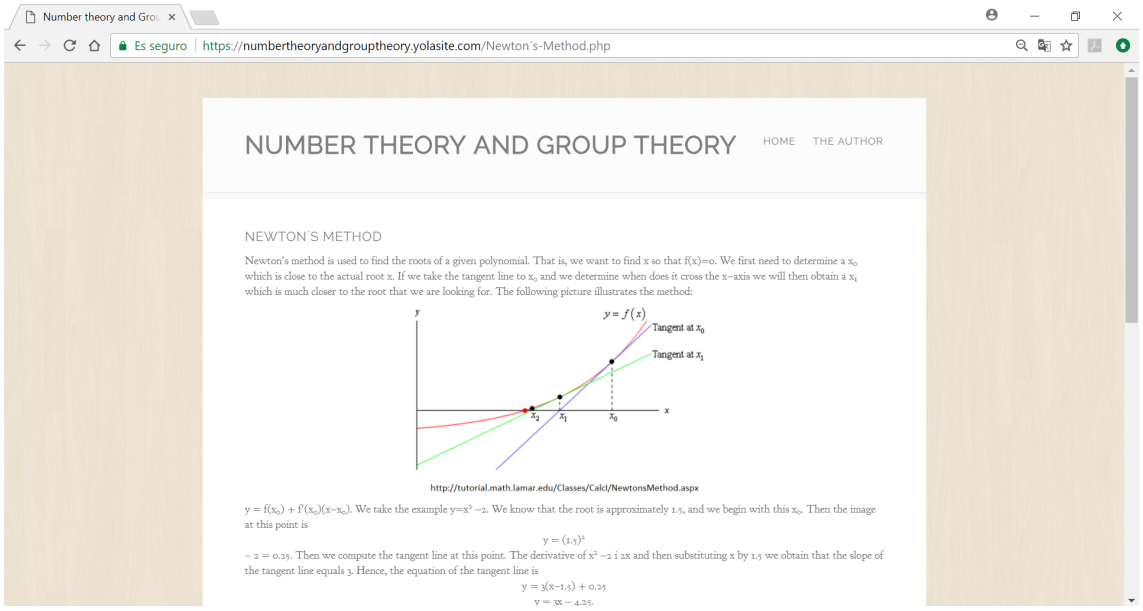
```
        }
        vpol1[i].push_back(vpol1[i-1][i-1]*i);
        //cout<<vpol1[i-1][i-1]*i<<endl;
        alphanum = alphanum + vpol1[i][i];
        indepnum = indepnum + vpol1[i][i];
        un = un*(iii-1);
        sumafact = sumafact + un;
        //cout<<"alpha: "<<(alpha[0]-alphanum)<<endl;
        alpha.push_back(alpha[0]-alphanum);
        //cout<<"indep: "<<(-indepnum-sumafact)<<endl;
        indep.push_back(-indepnum-sumafact);
    }

    for(int i=2; i<mmm; i++){  //L'EXPONENT
        cout<<endl<<"EXPONENT: "<<i<<endl;
        string ii = int2string(i);
        BigInteger iii = stringToBigInteger(ii);
        for(int k=1; k<nnn; k++){  //LO QUE SE SUMA EN EL FACTORIAL
            //cout<<"es suma al fact: "<<k<<endl;
            vector<vector<BigInteger> > vpol2 (nnn+1);
            vpol2[1].push_back(1);
            vpol2[1].push_back(k);
            for(int w=2; w<=i; w++){  //LES ITERACIONS NECESSÀRIES PER CALCULAR UN POLINOMI DE TAL GRAU FINS i
                vpol2[w].push_back(1);
                //cout<<"1 ";  //ja vols ometre el polinomi
                for(int q=1; q<w; q++){
                    vpol2[w].push_back(vpol2[w-1][q]+vpol2[w-1][q-1]*k);
                    //cout<<vpol2[w-1][q]<<"+"<<vpol2[w-1][q-1]<<"*k+"  ";
                }
                vpol2[w].push_back(vpol2[w-1][w-1]*k);
                //cout<<vpol2[w-1][w-1]*k<<endl;
            }
            //cout<<endl;
            alphanum = 0;
            for(int r=0; r<vpol2[i].size(); r++){
                if(r%2==0){
                    //cout<<"pol: "<<vpol2[i][r]<<endl;
                    //cout<<"alpha "<<(i-r)<<": "<<alpha[i-r]<<endl;
                    alphanum = alphanum + vpol2[i][r]*alpha[i-r];
                }
                if(r%2==1){
                    //cout<<"pol: "<<(vpol2[i][r])*(-1)<<endl;
                    //cout<<"alpha "<<(i-r)<<": "<<alpha[i-r]<<endl;
                    alphanum = alphanum - (vpol2[i][r])*alpha[i-r];
                }
            }
            cout<<alphanum;
            //cout<<"INDEP: "<<indepnum<<endl;
            cout<<endl;
        }
    }
}
```

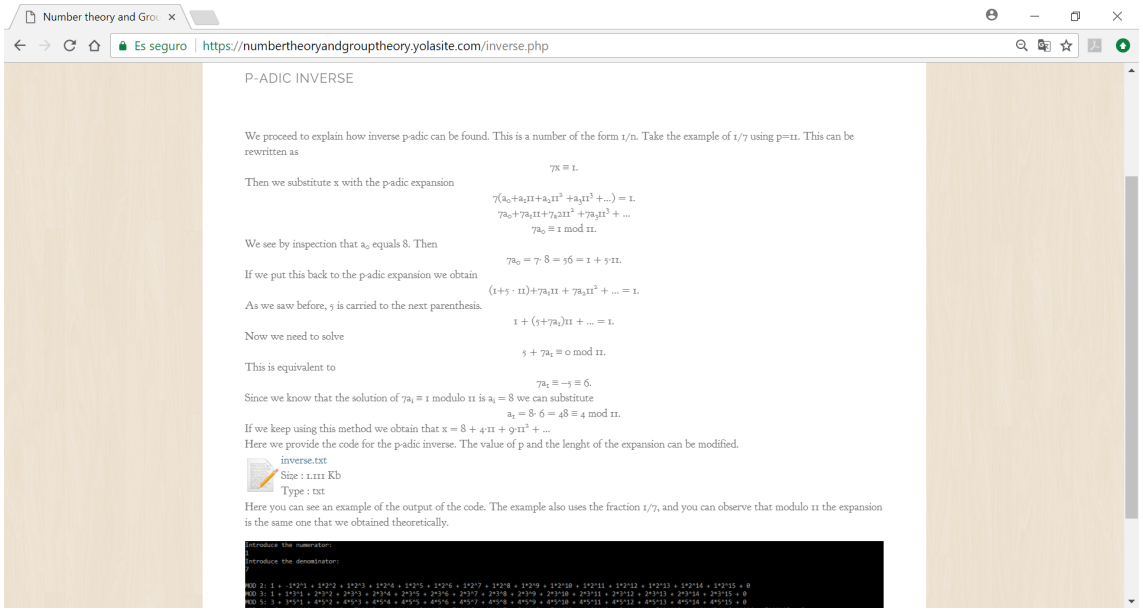
```
Introduce until which k, n^k: 10
Introduce until what r, n^k(n+r)!: 10

EXPONENT: 2
0
3
8
15
24
35
48
63
80

EXPONENT: 3
3
-1
-17
-51
-109
-197
-321
-487
-701

EXPONENT: 4
-7
-14
17
146
457
1058
2081
3682
6041

EXPONENT: 5
0
59
78
-273
-1684
-5325
-12966
-27097
-51048
```

9.2 Webpage

We also include screenshots of the webpage we created with all the concepts and C++ programs that are found in this work. The webpage is called *Number Theory and Group Theory*. The URL is

`https://numbertheoryandgrouptheory.yolasite.com/`





Bibliography

[1] N. C. Alexander, *Non-vanishing of Uppuluri-Carpenter numbers*, preprint, http://tinyurl.com/oo36das.

[2] J. Bertrand, Mémoire sur le nombre de valeurs que peut prendre une fonction quand on y permute les lettres qu'elle renferme, *Journal de l'École Royale Polytechnique*, 30:123–140, 1845.

[3] Hermite, *Irrationality of the sum of a p-adic series*, arXiv: Reference is omitted in this anonymous version.

[4] Hermite, The On-Line Encyclopedia of Integer Sequences: Reference is omitted in this anonymous version.

[5] Hermite, The On-Line Encyclopedia of Integer Sequences: Reference is omitted in this anonymous version.

[6] K. Conrad, *Hensel's Lemma*, University of Connecticut.

[7] K. S. Davis and W. A. Webb, Lucas' theorem for prime powers, *European Journal of Combinatorics*, 11:229–233, 1990.

[8] B. Dragovich, *On summation of p-adic series*, arXiv:1702.02569, 2017.

[9] B. Dragovich, A. Yu. Khrennikov, S. V. Kozyrev, I. V. Volovich. *On p-adic mathematical physics*, p-Adic Numbers, Ultrametric Analysis, and Applications, vol. 1, no. 1, March 2009.

[10] J. Evertse, *p-Adic Numbers*, March 2011.

[11] P. Fannon, V. Kadelburg, B. Woolley and S. Ward, *Discrete Mathematics for the IB Diploma*, Pearson, 2013.

[12] P. Garrett, *Classical definitions of $\mathbb{Z}_p$ and $\mathbb{A}$*, University of Minnessota, 2010.

[13] A. Granville, Harald Cramér and the distribution of prime numbers, *Scandinavian Actuarial Journal*, 1995:337–360, 1995.

[14] D. Heath-Brown, Gaps between primes, and the pair correlation of zeros of the zeta-function, *Acta Arithmetica*, 41:85–99, 1982.

[15] H. Hutter, M. Szedlák, P. Wirth, *Elementary Analysis in $\mathbb{Q}_p$*, November 2011.

[16] A. E. Ingham, *The Distribution of Prime Numbers*, Cambridge University Press, 1932.

[17] N. Koblitz, *p-Adic Numbers, p-Adic Analysis, and Zeta-Functions*, Springer, Berlin, 1948.

[18] E. Kummer, Über die Ergänzungssätze zu den allgemeinen Reziprozitätsgesetzen, *Journal für die reine und angewandte Mathematik*, 44:93–146, 1852.

[19] A. M. Legendre, *Théorie des Nombres*, Paris: Firmin Didot Frères, 1932.

[20] E. Lucas, Théorie des fonctions numériques simplement périodiques, *American Journal of Mathematics*, 44:184–196, 1878.

[21] M. R. Murty and S. Sumner, *On the p-adic series* $\sum_{n=1}^{\infty} n^k(n+m)!$, CRM Proc. Lecture Notes vol. 36, pp. 219–227, Amer. Math. Soc., Providence, RI, 2004.

[22] J. Nagura, *On the interval containing at least one prime number*, Proceedings of the Japan Academy, 1952.

[23] S. Niizeki and M. Araki, *Simple and clear proofs of Stirling's formula*, International Journal of Mathematical Education in Science and Technology, vol. 41, no. 4, 2010.

[24] A. Y. Osban, *Some new variants of Newton's Method*, Applied Mathematics Letters, 2004.

[25] G. Paz, *On Legendre's, Bocard's, Andrica's and Oppermann's conjectures*, arXiv:1310.1323, 2014.

[26] A. Robert, *A Course in p-Adic Analysis*, Graduate Texts in Mathematics, Springer, New York, 2000.

[27] J. S. Rose, *A Course on Group Theory*, Dover Books on Mathematics, 2003.

[28] W. H. Schikhof, *Ultrametric Calculus: An Introduction to p-Adic Analysis*, Cambridge University Press, Cambridge, 1984.

[29] J. Shareshian and R. Woodroofe, Divisibility of binomial coefficients and generation of alternating groups, *Pacific Journal of Mathematics*, 292:223–238, 2018.

[30] L. Shoenfeld, *Sharper bounds for Chebyshev functions* $\psi(x)$ *and* $\theta(x)$, ii, Mathematics of Computation, 1976.

[31] D. Subedi, Complementary Bell numbers and p-adic series, *Journal of Integer Sequences*, 17 (2014), article 14.3.1.

[32] I. Wazir and T. Garry, *Mathematics Higher Level for the IB Diploma*, Pearson, 2012.