INTEGRAL BINOMIAL COEFFICIENTS

ANTHONY G. O'FARRELL

ABSTRACT. We give a very short proof, using analysis, of a fact about the denominators of certain binomial coefficients.

1. INTRODUCTION

The binomial coefficients are defined by

$$\binom{\alpha}{k} = \frac{\alpha(\alpha-1)\cdots(\alpha-k+1)}{k!},$$

for nonnegative integral k and any α. Usually, α is a real or complex number, but the definition makes sense if α belongs to any field of characteristic zero. The following is well-known:

Theorem 1. *The binomial coefficients $\binom{n}{k}$ are positive integers, for integers n, k with $0 \leq k \leq n$.* □

The usual proof uses the Law of Pascal's Triangle, and induction.

The binomial coefficients $\binom{r}{k}$, with rational r, occur in the Maclaurin series expansion of $(1+x)^r$ (convergent for real or complex x with $|x| < 1$). For instance,

$$\sqrt{1+x} = \sum_{k=0}^{\infty} \binom{\frac{1}{2}}{k} x^k.$$

Calculating a few terms, one finds that the series begins

$$1 + \frac{1}{2}x - \frac{1}{8}x^2 + \frac{1}{16}x^3 - \frac{5}{64}x^4 \cdots .$$

The coefficients are not integral (or nonnegative), but when common factors are cancelled (i.e. they are expressed in *reduced form* m/n, with $m \in \mathbb{Z}$, $n \in \mathbb{N}$, and $\gcd(m,n) = 1$), it is remarkable that only powers of 2 occur in the denominators. This is not an accident: the

---

Date: June 29, 2017.

This article is based on a lecture given at the Irish Mathematics Students' Conference at UCD in March 2012. The author is grateful for the hospitality of the organisers and the enthusiasm of the audience.

pattern continues forever. We have the following, slightly less well-known result:

Theorem 2. *Let $r \in \mathbb{Q}$ and $0 \le k \in \mathbb{Z}$. Suppose that $r = m/n$ in reduced form. Then the binomial coefficient $\binom{r}{k}$ has reduced form s/t, where t is a product of powers of primes that divide n.*

For instance, in the expansion of $(1+x)^{\frac{5}{6}}$, the coefficients all take the form $s/(2^a 3^b)$, for some $s \in \mathbb{Z}$.

The theorem may be proved using elementary number theory, for instance by reducing it to the statement that if $d, k \in \mathbb{N}$ and r is the largest factor of $k!$ prime to d, then r divides the product of the terms of each k-term arithmetic progression of integers having step d.

The purpose of this note is to give a very short soft proof of Theorem 2, by using a little analysis. Specifically, the proof uses the field $\mathbb{Q}_p$ of p-adic numbers. For the benefit of readers who have not met these numbers, we give a short introduction in the next section, and then give the proof in the final section.

2. The p-adic Numbers

For a prime p, the *p-adic valuation* of a rational number is defined by setting $\|0\|_p = 0$ and

$$\left\| \frac{\pm r p^n}{s} \right\|_p = p^{-n}$$

whenever $r \in \mathbb{N}$, $s \in \mathbb{N}$, and $n \in \mathbb{Z}$ with $\gcd(r,p) = \gcd(s,p) = 1$. For instance,

$$\|300\|_2 = \frac{1}{4},\ \|301\|_2 = 1,\ \text{and}\ \|\frac{1}{300}\|_2 = 4.$$

Thus some numbers that have large absolute value have small valuations, and vice-versa. Also, numbers that have small valuations with respect to one prime may have large valuations with respect to another.

The *p-adic metric* on the set $\mathbb{Q}$ is defined by setting the distance between two rationals a and b equal to $\|a-b\|_p$. You can verify easily that this does, indeed, define a metric. In particular, the triangle inequality follows from a stronger form known as the *ultrametric* inequality:

$$\|a-b\|_p \le \max\{\|a-c\|_p, \|c-b\|_p\}.$$

The space $\mathbb{Q}_p$ of *p-adic numbers* is the completion of $\mathbb{Q}$ with respect to the p-adic metric. It is a complete metric field, i.e. the field operations are continuous. One can show (although we do not need this for the proof below) that $\mathbb{Q}_p$ has the same cardinality as $\mathbb{R}$, and that it is locally-compact and totally-disconnected.

The closure of $\mathbb{Z}$ in $\mathbb{Q}_p$ is denoted $\mathbb{Z}_p$, and called the set of *p-adic integers*. It is a compact, totally-disconnected metric space, and an integral domain, and $\mathbb{Q}_p$ is its quotient field.

From the point of view of number theorists, there is little to choose between $\mathbb{R}$ and any of the $\mathbb{Q}_p$. They are all more-or-less equally-interesting ways to complete the set of rationals. For instance, if one is interested in solving a Diophantine equation such as $x^3 + y^3 = z^3$ for integers, then it is necessary that the equation have a solution in each $\mathbb{Z}_p$ and in $\mathbb{R}$. For some equations, the converse holds — such a result is called a "Hasse Principle".

Each infinite series of the form

$$\sum_{n=0i}^{\infty} a_n p^n$$

with $a_n \in \mathbb{Z}$ is convergent in p-adic metric, and so represents some p-adic integer. For instance, in 2-adic metric we have the formula

$$1 + 2 + 4 + \cdots + 2^n + \cdots = -1,$$

which may be found in Euler's work. More generally, for any prime p,

$$(p-1) + (p-1)p + (p-1)^2 p + \cdots = -1$$

in p-adic metric. From this we deduce that every p-adic integer is the limit of a sequence of *positive* integers.

A non-integral rational number may be a p-adic integer. For instance,

$$1 + 3 + 3^2 + 3^3 + \cdots = -\frac{1}{2}$$

in 3-adic metric. More generally, it is not hard to see that a rational number r with reduced form m/n belongs to $\mathbb{Z}_p$ if and only if p does not divide n.

3. The Proof

Theorem 3. *If $p \in \mathbb{N}$ is prime, $a \in \mathbb{Z}_p$ and $0 < k \in \mathbb{Z}$, then $\binom{a}{k} \in \mathbb{Z}_p$.*

Proof. Fix $k \in \mathbb{Z}$, $k \geq 0$. The function

$$f : x \mapsto \binom{x}{k}$$

is a polynomial with coefficients in $\mathbb{Q}$, and hence it is continuous, as a function from $\mathbb{Q}_p$ into $\mathbb{Q}_p$. (This just depends on the fact that $\mathbb{Q}_p$ is a metric field.) Choose a sequence $(a_n) \subset \mathbb{N}$ with $a_n \to a$ in p-adic metric. Then $f(a_n) \in \mathbb{N} \subset \mathbb{Z}_p$, and hence $f(a) = \lim_n f(a_n) \in \mathbb{Z}_p$, since $\mathbb{Z}_p$ is closed. $\square$

We remark that a rational number r is an integer if and only if $r \in \mathbb{Z}_p$ for each prime p, and so this theorem may be regarded as a 'local version' of Theorem 1. The proof shows that the local version follows at once from Theorem 1, and a simple bit of topology.

Proof of Theorem 2. Let $r = m/n$, k, and $\binom{r}{k} = s/t$ be as in the statement. Suppose a prime p divides t. If p does not divide n, then $r \in \mathbb{Z}_p$, so $s/t \in \mathbb{Z}_p$, which is false. Thus each prime that divides t divides n. $\square$

References

[1] J.-P. Serre, A Course of Arithmetic. Springer. New York. 1996.

Mathematics Department, NUI, Maynooth, Co. Kildare, Ireland