Prime divisibility of binomial coefficients

Russ Woodroofe
Univerza na Primorskem
russ.woodroofe@famnit.upr.si

Binomial coefficients

We write

$$\binom{n}{k} \text{ to mean } \frac{n!}{k! \cdot (n-k)!}. \qquad \text{Say as "}n \text{ choose } k\text{".}$$

That is,

$$\binom{n}{k} = \frac{n \cdot (n-1) \cdot (n-2) \cdots 4 \cdot 3 \cdot 2 \cdot 1}{k \cdot (k-1) \cdot (k-2) \cdots 4 \cdot 3 \cdot 2 \cdot 1 \cdot (n-k)!}.$$

Example:

$$\binom{5}{2} = \frac{5!}{2! \cdot 3!} = \frac{120}{2 \cdot 6} = 10.$$

The numbers $\binom{n}{k}$ are called *binomial coefficients*.

We'll explain why soon.

Why care about $\binom{n}{k}$? At least 3 reasons.

Why care about $\binom{n}{k}$? At least 3 reasons.

Reason 1: $\binom{n}{k}$ is the number of ways to choose
a set of k elements out of
a set of n elements.

Example: Forming a team of 3 people from 6 people, you could:

Choose a 1st person (in 6 ways)
Choose a 2nd person (in 5 ways)
Choose a 3rd person (in 4 ways)

Then notice the order of choosing didn't matter.

Since there are $3! = 6$ ways of ordering 1st, 2nd, 3rd,

$$\text{total \# of possible teams } = \binom{6}{3} = \frac{6 \cdot 5 \cdot 4}{3!} = 20.$$

Why care about $\binom{n}{k}$? Choosing sets!

Example: Possible teams of 3 from 6 mathematicians
Alice, **B**ob, **C**vetko, **D**aša, **E**rika, and **F**ranci.

ABC			
ABD			
ABE			
ABF			
ACD	BCD		
ACE	BCE		
ACF	BCF		
ADE	BDE	CDE	
ADF	BDF	CDF	
AEF	BEF	CEF	DEF

(You might notice that $\binom{6}{3} = \binom{5}{2} + \binom{4}{2} + \binom{3}{2} + \binom{2}{2}$.)

Why care about $\binom{n}{k}$? Powers of $(1+x)$ coefficients!

Why care about $\binom{n}{k}$? Powers of $(1+x)$ coefficients!

Reason 2: $\binom{n}{k}$ is the coefficient of x^k in $(1+x)^n$.

Example: To find $(1+x)^6$, expand it out:

$$(1+x)\cdot(1+x)\cdot(1+x)\cdot(1+x)\cdot(1+x)\cdot(1+x)$$

To get an x^k choose a set of k of the factors A, B, C, D, E, F to provide an x in the multiplication algorithm.

$$\begin{aligned}\text{So } (1+x)^6 &= 1+\binom{6}{1}\cdot x+\binom{6}{2}\cdot x^2+\binom{6}{3}\cdot x^3+\binom{6}{4}\cdot x^4+\ldots\\ &= 1+6x+15x^2+20x^3+15x^4+6x^5+x^6.\end{aligned}$$

Why care about $\binom{n}{k}$? Powers of $(1+x)$ coefficients!

Reason 2: $\binom{n}{k}$ is the coefficient of x^k in $(1+x)^n$.

Example: To find $(1+x)^6$, expand it out:

$$\underbrace{(1+x)}_{A} \cdot \underbrace{(1+x)}_{B} \cdot \underbrace{(1+x)}_{C} \cdot \underbrace{(1+x)}_{D} \cdot \underbrace{(1+x)}_{E} \cdot \underbrace{(1+x)}_{F}$$

To get an x^k choose a set of k of the factors A, B, C, D, E, F to provide an x in the multiplication algorithm.

$$\begin{aligned} \text{So } (1+x)^6 &= 1 + \binom{6}{1} \cdot x + \binom{6}{2} \cdot x^2 + \binom{6}{3} \cdot x^3 + \binom{6}{4} \cdot x^4 + \dots \\ &= 1 + 6x + 15x^2 + 20x^3 + 15x^4 + 6x^5 + x^6. \end{aligned}$$

Why care about $\binom{n}{k}$? Powers of $(1+x)$ coefficients!

Reason 2: $\binom{n}{k}$ is the coefficient of x^k in $(1+x)^n$. **(Binomial!)**

Example: To find $(1+x)^6$, expand it out:

$$\underbrace{(1+x)}_{A} \cdot \underbrace{(1+x)}_{B} \cdot \underbrace{(1+x)}_{C} \cdot \underbrace{(1+x)}_{D} \cdot \underbrace{(1+x)}_{E} \cdot \underbrace{(1+x)}_{F}$$

To get an x^k choose a set of k of the factors A, B, C, D, E, F to provide an x in the multiplication algorithm.

$$\begin{aligned} \text{So } (1+x)^6 &= 1 + \binom{6}{1} \cdot x + \binom{6}{2} \cdot x^2 + \binom{6}{3} \cdot x^3 + \binom{6}{4} \cdot x^4 + \ldots \\ &= 1 + 6x + 15x^2 + 20x^3 + 15x^4 + 6x^5 + x^6. \end{aligned}$$

Why care about $\binom{n}{k}$? Powers of $(1+x)$ coefficients!

You might have seen the coefficients of $(1+x)^n$ before through *Pascal's triangle* (another approach to binomial coefficients).

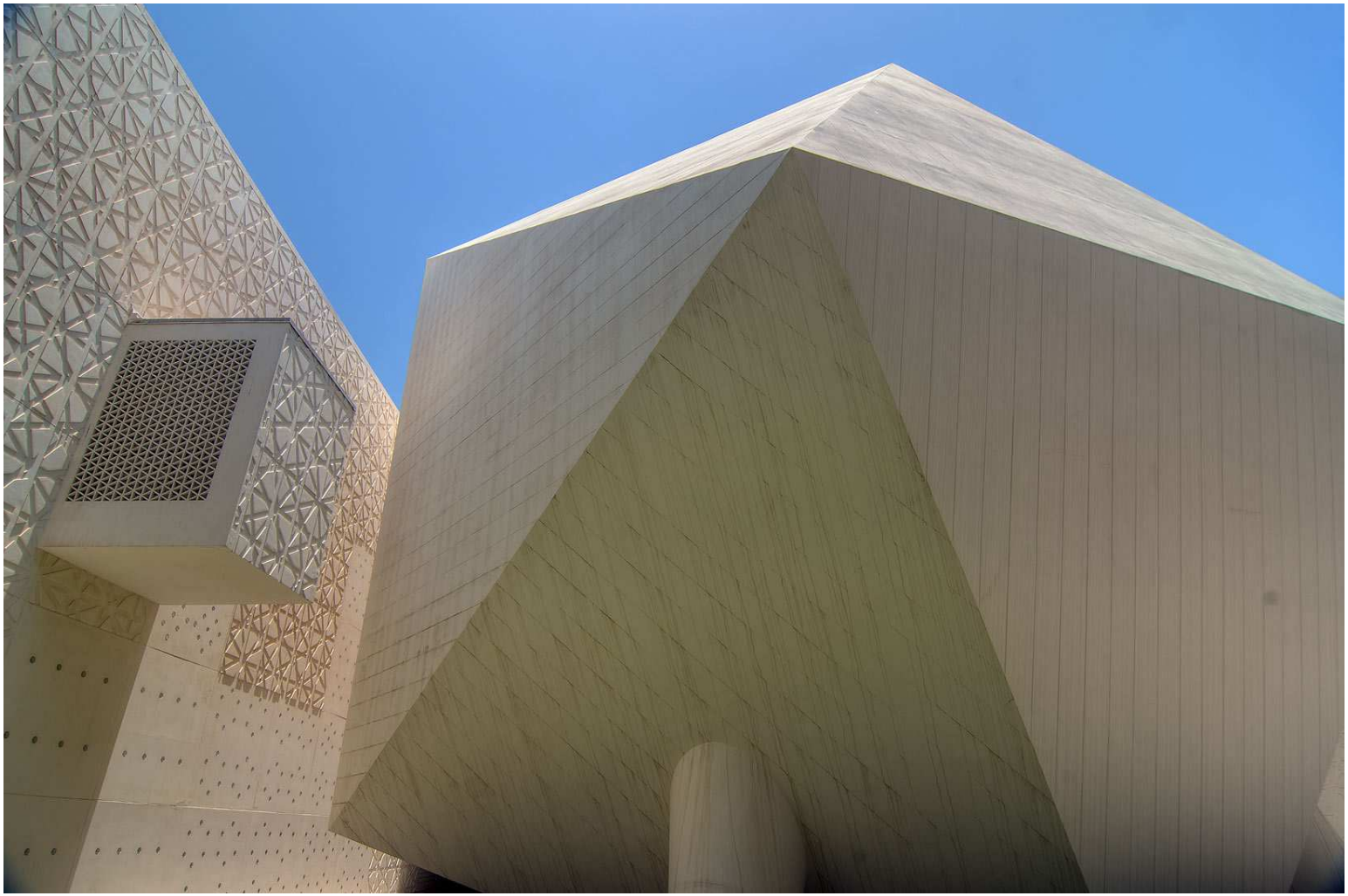
Here's a picture of Pascal:

(scan of a c.1690 painting, from Wikipedia)

Why care about $\binom{n}{k}$? Symmetry!

Reason 3: Symmetry!

Weill Cornell Medical College, Doha Qatar.
The icosohedral lecture hall and lattice work are both highly symmetric.



Why care about $\binom{n}{k}$? Symmetry!

Reason 3: Symmetry!

One kind of symmetry: rearranging (reordering) elements in a set.

Example: Rearrange ABCDEF to ACBDEF or to FEDCBA.

Question: How many rearrangements are there?

\# ways to rearrange a set with n elements?

Why care about $\binom{n}{k}$? Symmetry!

Reason 3: Symmetry!

One kind of symmetry: rearranging (reordering) elements in a set.

Example: Rearrange ABCDEF to ACBDEF or to FEDCBA.

Question: How many rearrangements are there?

\# ways to rearrange a set with n elements? $n!$

Why care about $\binom{n}{k}$? Symmetry!

Reason 3: Symmetry!

One kind of symmetry: rearranging (reordering) elements in a set.

Example: Rearrange ABCDEF to ACBDEF or to FEDCBA.

Question: How many rearrangements are there?

ways to rearrange a set with n elements? $n!$

ways to rearrange a set with n elements, so that the first k elements come before the last $n-k$?

Why care about $\binom{n}{k}$? Symmetry!

Reason 3: Symmetry!

One kind of symmetry: rearranging (reordering) elements in a set.

Example: Rearrange ABCDEF to ACBDEF or to FEDCBA.

Question: How many rearrangements are there?

ways to rearrange a set with n elements? $n!$

ways to rearrange a set with n elements, so that the first k elements come before the last $n-k$? $k! \cdot (n-k)!$

Why care about $\binom{n}{k}$? Symmetry!

Reason 3: Symmetry!

One kind of symmetry: rearranging (reordering) elements in a set.

Example: Rearrange ABCDEF to ACBDEF or to FEDCBA.

Question: How many rearrangements are there?

ways to rearrange a set with n elements? $n!$

ways to rearrange a set with n elements, so that the first k elements come before the last $n-k$? $k! \cdot (n-k)!$

So $\binom{n}{k}$ is the ratio of the above two!

Why care about $\binom{n}{k}$? Symmetry!

Reason 3: Symmetry!

One kind of symmetry: rearranging (reordering) elements in a set.

Example: Rearrange ABCDEF to ACBDEF or to FEDCBA.

Question: How many rearrangements are there?

ways to rearrange a set with n elements? $n!$

ways to rearrange a set with n elements, so that the first k elements come before the last $n-k$? $k! \cdot (n-k)!$

So $\binom{n}{k}$ is the ratio of the above two! **(Group Theory.)**

A problem of John Shareshian and myself

Our problem:
For a number n, must there be primes p, r so that

$$\binom{n}{1}, \binom{n}{2}, \binom{n}{3}, \binom{n}{4}, \ldots, \binom{n}{n-2}, \binom{n}{n-1}$$

are all divisible by at least one of the two primes?

Motivation: Problems on symmetry.

A problem of John Shareshian and myself

Our problem:
For a number n, must there be primes p, r so that

$$\binom{n}{1}, \binom{n}{2}, \binom{n}{3}, \binom{n}{4}, \ldots, \binom{n}{n-2}, \binom{n}{n-1}$$

are all divisible by at least one of the two primes?

Example:

$n = 6$: $\binom{6}{1} = 6, \binom{6}{2} = 15, \binom{6}{3} = 20, \ldots$

primes pairs $2, 3$ or $2, 5$ or $3, 5$ "work".

A problem of John Shareshian and myself

Our problem:
For a number n, must there be primes p, r so that

$$\binom{n}{1}, \binom{n}{2}, \binom{n}{3}, \binom{n}{4}, \ldots, \binom{n}{n-2}, \binom{n}{n-1}$$

are all divisible by at least one of the two primes?

Example:

$n = 6$: $\binom{6}{1} = 6, \binom{6}{2} = 15, \binom{6}{3} = 20, \ldots$

primes pairs $2, 3$ or $2, 5$ or $3, 5$ "work".

$n = 15$: $\binom{15}{1} = 15, \binom{15}{2} = 105, \binom{15}{3} = 455, \binom{15}{4} = 1365,$

A problem of John Shareshian and myself

Our problem:
For a number n, must there be primes p, r so that

$$\binom{n}{1}, \binom{n}{2}, \binom{n}{3}, \binom{n}{4}, \ldots, \binom{n}{n-2}, \binom{n}{n-1}$$

are all divisible by at least one of the two primes?

Example:

$n = 6$: $\binom{6}{1} = 6, \binom{6}{2} = 15, \binom{6}{3} = 20, \ldots$

primes pairs $2, 3$ or $2, 5$ or $3, 5$ "work".

$n = 15$: $15, 105, 455, 1365, 3003, 5005, 6435, 5005, \ldots$

A problem of John Shareshian and myself

Our problem:
For a number n, must there be primes p, r so that

$$\binom{n}{1}, \binom{n}{2}, \binom{n}{3}, \binom{n}{4}, \ldots, \binom{n}{n-2}, \binom{n}{n-1}$$

are all divisible by at least one of the two primes?

Example:

$n = 6$: $\binom{6}{1} = 6, \binom{6}{2} = 15, \binom{6}{3} = 20, \ldots$

primes pairs $2, 3$ or $2, 5$ or $3, 5$ "work".

$n = 15$: $15, 105, 455, 1365, 3003, 5005, 6435, 5005, \ldots$

primes pairs $3, 5$ or $3, 13$ or $5, 13$ "work".

Our problem:
For a number n, must there be primes p, r so that

$$\binom{n}{1}, \binom{n}{2}, \binom{n}{3}, \binom{n}{4}, \ldots, \binom{n}{n-2}, \binom{n}{n-1}$$

are all divisible by at least one of the two primes?

Notation: Let p divide $n = \dfrac{n!}{(n-1)!} = \binom{n}{1}$.

What we know

Our problem:
For a number n, must there be primes p, r so that

$$\binom{n}{1}, \binom{n}{2}, \binom{n}{3}, \binom{n}{4}, \ldots, \binom{n}{n-2}, \binom{n}{n-1}$$

are all divisible by at least one of the two primes?

Notation: Let p divide $n = \dfrac{n!}{(n-1)!} = \binom{n}{1}$.

Let r be the other prime. (Usually "pretty big".)

Bob Guralnick, Shareshian, and I showed:
The answer is "yes" for all $n \leq 10^{15} = 1{,}000{,}000{,}000{,}000{,}0000$.

Arithmetic modulo p

To organize our algebra, we use *arithmetic modulo* p. Write $\equiv_p$.

In this arithmetic we work as if the number p is 0.
Thus, also $2p \equiv_p 3p \equiv_p \cdots \equiv_p 0$, while

$$p + 1 \equiv_p 2p + 1 \equiv_p 1.$$

In particular, a number m is divisible by p exactly if $m \equiv_p 0$.

Arithmetic modulo p

To organize our algebra, we use *arithmetic modulo* p. Write $\equiv_p$.

In this arithmetic we work as if the number p is 0.
Thus, also $2p \equiv_p 3p \equiv_p \cdots \equiv_p 0$, while

$$p + 1 \equiv_p 2p + 1 \equiv_p 1.$$

(Like the arithmetic you do with clock times.)

In particular, a number m is divisible by p exactly if $m \equiv_p 0$.

Arithmetic modulo p

To organize our algebra, we use *arithmetic modulo* p. Write $\equiv_p$.

In this arithmetic we work as if the number p is 0.
Thus, also $2p \equiv_p 3p \equiv_p \cdots \equiv_p 0$, while

$$p + 1 \equiv_p 2p + 1 \equiv_p 1.$$

(Like the arithmetic you do with clock times.)

In particular, a number m is divisible by p exactly if $m \equiv_p 0$.

The coefficients of $(1 + x)^n$ can simplify nicely modulo p:

Freshman's Dream Identity:
If p is a prime, then

$$(1 + x)^p \equiv_p 1 + x^p.$$

Arithmetic modulo p

To organize our algebra, we use *arithmetic modulo* p. Write $\equiv_p$.

In this arithmetic we work as if the number p is 0.
Thus, also $2p \equiv_p 3p \equiv_p \cdots \equiv_p 0$, while

$$p + 1 \equiv_p 2p + 1 \equiv_p 1.$$

(Like the arithmetic you do with clock times.)

In particular, a number m is divisible by p exactly if $m \equiv_p 0$.

The coefficients of $(1 + x)^n$ can simplify nicely modulo p:

Freshman's Dream Identity:
If p is a prime, then

$$(1 + x)^p \equiv_p 1 + x^p.$$

More generally, for any power p^a, it holds that

$$(1 + x)^{p^a} \equiv_p 1 + x^{p^a}.$$

Main lemma

Applying the same idea as for 15 with $r = 13$ and $p = 3$ or 5, Shareshian and I proved:

Lemma: If n is a positive integer and p, r are primes so that
p^a divides n, and also
$r < n < r + p^a$,
then at least one of p, r divide each binomial coefficient of n.

Example: $n = 15, r = 13,$ or $n = 300, r = 293.$

Main lemma

Applying the same idea as for 15 with $r = 13$ and $p = 3$ or 5, Shareshian and I proved:

Lemma: If n is a positive integer and p, r are primes so that
p^a divides n, and also
$r < n < r + p^a$,
then at least one of p, r divide each binomial coefficient of n.

Example: $n = 15, r = 13$, or $n = 300, r = 293$.

The condition of the lemma is frequently met (but not always).

Antiexample: the prime preceding $n = 210 = 2 \cdot 3 \cdot 5 \cdot 7$ is $r = 199$.

Main lemma

Applying the same idea as for 15 with $r = 13$ and $p = 3$ or 5, Shareshian and I proved:

Lemma: If n is a positive integer and p, r are primes so that
p^a divides n, and also
$r < n < r + p^a$,
then at least one of p, r divide each binomial coefficient of n.

Example: $n = 15, r = 13$, or $n = 300, r = 293$.

The condition of the lemma is frequently met (but not always).

Antiexample: the prime preceding $n = 210 = 2 \cdot 3 \cdot 5 \cdot 7$ is $r = 199$.

Fails for n in large "prime gap" with small prime-power divisors.

Out to 10^{15}, the condition of the lemma is met for all about about 26 million numbers.

Main lemma

Applying the same idea as for 15 with $r = 13$ and $p = 3$ or 5, Shareshian and I proved:

Lemma: If n is a positive integer and p, r are primes so that
p^a divides n, and also
$r < n < r + p^a$,
then at least one of p, r divide each binomial coefficient of n.

Example: $n = 15, r = 13$, or $n = 300, r = 293$.

The condition of the lemma is frequently met (but not always).

Antiexample: the prime preceding $n = 210 = 2 \cdot 3 \cdot 5 \cdot 7$ is $r = 199$.

Fails for n in large "prime gap" with small prime-power divisors.

Out to 10^{15}, the condition of the lemma is met for all about about 26 million numbers. *(Checked in 10 days with 15 parallel threads.)*

Asymptotic density of lemma

The same lemma is also useful for non-computational work.

Lemma: If n is a positive integer and p, r are primes so that
p^a divides n, and also
$r < n < r + p^a$,
then at least one of p, r divide each binomial coefficient of n.

Shareshian and I showed that the conditions of the lemma are met with *asymptotic density* 1, assuming the "Riemann hypothesis".

Asymptotic density 1 means that large numbers where the condition is not met become vanishingly rare.

Asymptotic density of lemma

The same lemma is also useful for non-computational work.

Lemma: If n is a positive integer and p, r are primes so that
p^a divides n, and also
$r < n < r + p^a$,
then at least one of p, r divide each binomial coefficient of n.

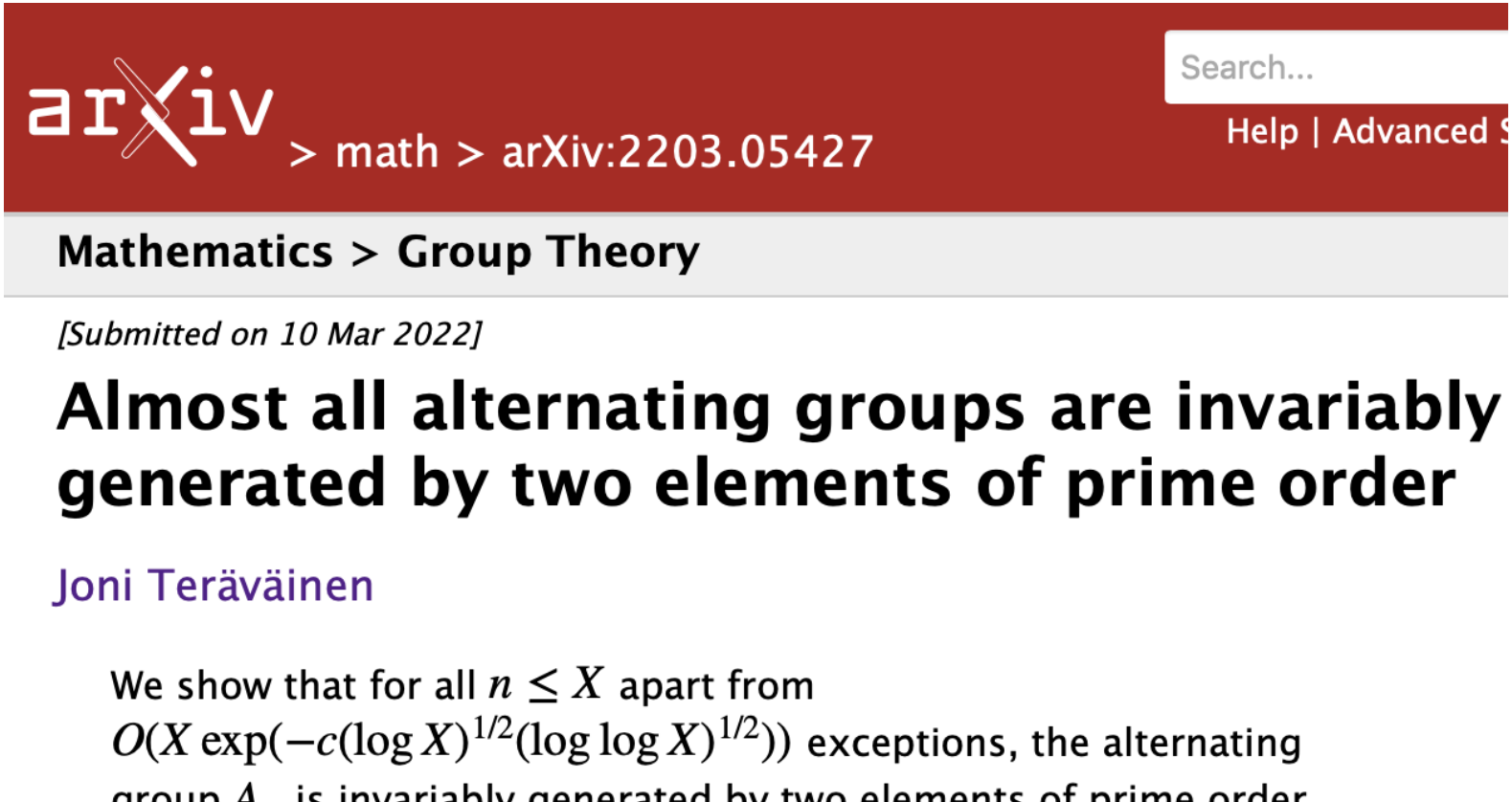
Shareshian and I showed that the conditions of the lemma are met with *asymptotic density* 1, assuming the "Riemann hypothesis".

Asymptotic density 1 means that large numbers where the condition is not met become vanishingly rare. The Riemann hypothesis is a famous conjecture about the distribution of primes.

This helps to predict why there are only a few failures out to 10^{15}. (Well, 26 million.)

Asymptotic density of binomial divisibility

Joni Teräväinen improved on these ideas to show (without RH) that the binomial divisibility question has a "yes" answer with asymptotic density 1.



26 million hard cases

For the remaining 26 million numbers,
we try replacing the condition

$$r < n < r + p^a \qquad \text{(from the lemma)}$$

26 million hard cases

For the remaining 26 million numbers,
we try replacing the condition

$$r < n < r + p^a \qquad \text{(from the lemma)}$$

with

$$2r < n < 2r + p^a$$

26 million hard cases

For the remaining 26 million numbers,
we try replacing the condition

$$r < n < r + p^a \qquad \text{(from the lemma)}$$

with

$$2r < n < 2r + p^a \qquad \text{or}$$
$$3r < n < 3r + p^a \qquad \text{or}$$
$$\ldots$$

26 million hard cases

For the remaining 26 million numbers,
we try replacing the condition

$$r < n < r + p^a \qquad \text{(from the lemma)}$$

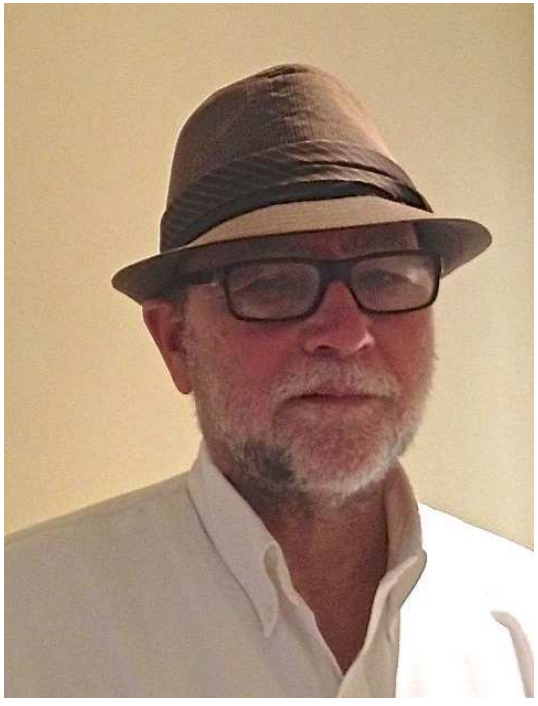
with

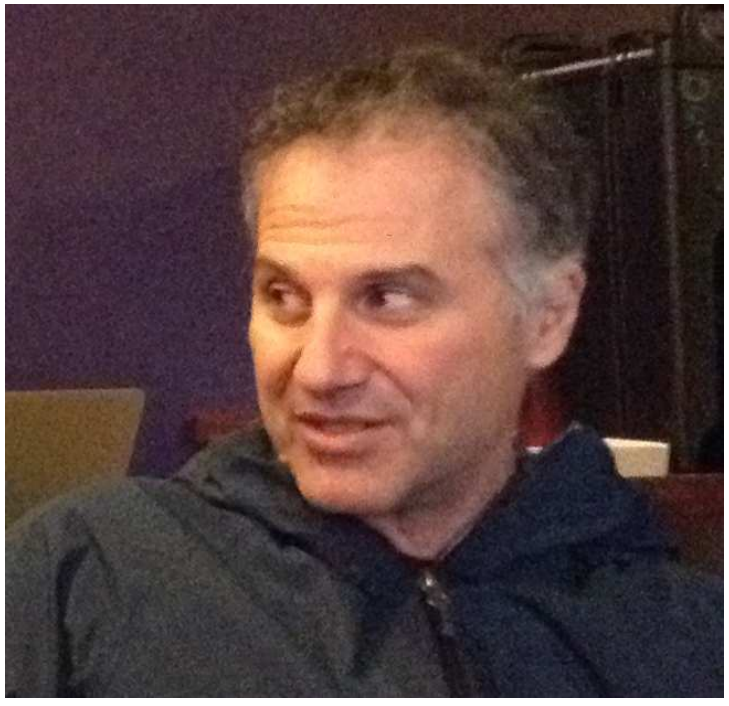
$$2r < n < 2r + p^a \qquad \text{or}$$
$$3r < n < 3r + p^a \qquad \text{or}$$
$$\ldots$$

Challenge problem:
Find p, r for $n = 31416$ so that every binomial coefficient of n is divisible by p or r.

Hint: Try $r = 7853 \approx n/4$.

Coauthors






Thank you!

Related book:

Concrete Mathematics, by R. Graham, D. Knuth, and O. Patashnik.

A readable introduction to mathematics around binomial coefficients and other nice topics. (Advanced high school level.)

Papers are linked from my webpage.

Russ Woodroofe / russ.woodroofe@famnit.upr.si