Experimental Methods in Number Theory and Combinatorics

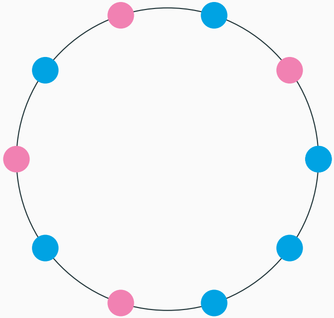
Robert Dougherty-Bliss
Rutgers University

March 4, 2024

Origami

Definition

A circular binary array is *valid* if it contains exactly two more 0's than 1's, or vice versa.

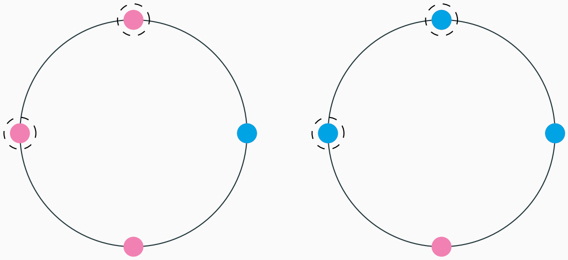


Left: A valid array of size 10. Right: An invalid array of size 10.

The all equal angles graph

The graph A_{2n} has one vertex for every valid array of length $2n$.

Edges are formed by flipping adjacent bits (if possible).



Two adjacent vertices in A_4 and their flipped bits.

Question

How many edges are there in A_{2n}?

Sequence begins:

$$2, 16, 84, 400, 1820, 8064, 35112, 151008,$$
$$643500, 2722720, 11454872, 47969376, 200107544, \ldots$$

Question

How many edges are there in A_{2n}?

Sequence begins:

$$2, 16, 84, 400, 1820, 8064, 35112, 151008,$$
$$643500, 2722720, 11454872, 47969376, 200107544, \ldots$$

Conjecture (Me)

$$\frac{(n+1)(3n-2)}{2n-1}\binom{2n}{n-1}.$$

Formula is extremely easy to find!

Many programs can guess recurrences given data.

Here, the resulting recurrence

$$a(n+1) = \frac{2(3n+1)(2n-1)}{n(3n-2)} a(n)$$

is easy to solve.

Rest of the talk

1. Primality tests and pseudoprimes
2. Hardinian arrays

Primality tests

(with Doron Zeilberger)

Perrin numbers

$$P(0) = 3 \quad P(1) = 0 \quad P(2) = 2$$
$$P(n) = P(n-2) + P(n-3)$$

Counts arrangements of people into n chairs at a circular table where:

Perrin numbers

$$P(0) = 3 \quad P(1) = 0 \quad P(2) = 2$$
$$P(n) = P(n-2) + P(n-3)$$

Counts arrangements of people into n chairs at a circular table where:

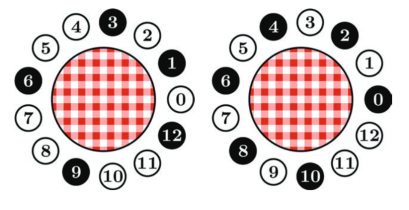
- No one is sitting next to another person (social distancing)

Perrin numbers

$$P(0) = 3 \quad P(1) = 0 \quad P(2) = 2$$
$$P(n) = P(n-2) + P(n-3)$$

Counts arrangements of people into n chairs at a circular table where:

- No one is sitting next to another person (social distancing)
- No one else could be sat down (maximal arrangement)



Two full tables with 13 chairs. From Vince Vatter.

Theorem

If p is prime, then $p \mid P(p)$.

“Proof”.

Easy to show that $P(n) = \alpha^n + \beta^n + \gamma^n$, where α, β, and γ are roots of $x^3 - x - 1$.

Theorem

If p is prime, then $p \mid P(p)$.

"Proof".

Easy to show that $P(n) = \alpha^n + \beta^n + \gamma^n$, where α, β, and γ are roots of $x^3 - x - 1$.

$$\begin{aligned} P(p) &= \alpha^p + \beta^p + \gamma^p \\ &\equiv (\alpha + \beta + \gamma)^p \pmod{p} \\ &= 0 \end{aligned}$$

□

This gives a primality test.

To check if n is prime, check whether n divides $P(n)$.

Psuedoprimes

Composites that pass the test are called *pseudoprimes*.

Perrin couldn't find any pseudoprimes in 1899.

Psuedoprimes

Composites that pass the test are called *pseudoprimes*.

Perrin couldn't find any pseudoprimes in 1899.

Adams and Shanks found the first one in 1982:

$$(521)^2 = 271441.$$

(My laptop finds this in 0.2 seconds.)

Psuedoprimes

Composites that pass the test are called *pseudoprimes*.

Perrin couldn't find any pseudoprimes in 1899.

Adams and Shanks found the first one in 1982:

$$(521)^2 = 271441.$$

(My laptop finds this in 0.2 seconds.)

Grantham proved that there are infinitely many in 2006:

$$271441, 904631, 16532714, 24658561, 27422714, 27664033, \ldots$$

Linear tests

This idea works in a more general setting.

Linear tests

This idea works in a more general setting.

1. Fix an integer coefficient polynomial

$$p(x) = x^d - ex^{d-1} - \cdots + a_1 x - a_0$$

   with roots $\alpha_1, \ldots, \alpha_d$.

Linear tests

This idea works in a more general setting.

1. Fix an integer coefficient polynomial

$$p(x) = x^d - ex^{d-1} - \cdots + a_1 x - a_0$$

   with roots $\alpha_1, \ldots, \alpha_d$.

2. Define the integer sequence

$$b(n) = \alpha_1^n + \alpha_2^n + \cdots + \alpha_d^n.$$

   (You can compute $b(n)$ without knowing the roots.)

Linear tests

This idea works in a more general setting.

1. Fix an integer coefficient polynomial

$$p(x) = x^d - {\color{red}e}x^{d-1} - \cdots + a_1 x - a_0$$

   with roots $\alpha_1, \ldots, \alpha_d$.

2. Define the integer sequence

$$b(n) = \alpha_1^n + \alpha_2^n + \cdots + \alpha_d^n.$$

   (You can compute $b(n)$ without knowing the roots.)

3. Then

$$b(p) \equiv {\color{red}e} \pmod{p}$$

   for any prime p.

We searched for polynomials that gave big pseudoprimes.

The sequence $b(n)$ with generating function

$$\frac{3x^4 + 5x^2 + 6x - 7}{4x^7 + x^4 + x^2 + x - 1}.$$

satisfies $b(p) \equiv 1 \pmod{p}$ for all primes p.

Couldn't find any pseudoprimes up to 1.5×10^6...

We searched for polynomials that gave big pseudoprimes.

The sequence $b(n)$ with generating function

$$\frac{3x^4 + 5x^2 + 6x - 7}{4x^7 + x^4 + x^2 + x - 1}.$$

satisfies $b(p) \equiv 1 \pmod{p}$ for all primes p.

Couldn't find any pseudoprimes up to 1.5×10^6...

...because the first one is 1,531,398.

Our stupidity

$$b(n) \sim (1.823)^n$$
$$b(1,531,398) \sim 10^{399287}$$

Arithmetic with 400,000 digits is very slow.

Computing $b(1), b(2), \ldots, b(n)$ directly takes $O(n^3)$ time.

- Bit size at step k: $O(k)$
- Multiplications at that step: $O(k^2)$
- Total runtime for $b(n)$: $\sum_k O(k^2) = O(n^3)$

Manuel Kauers suggested some improvements.

- Compute *only* $b(n) \bmod n$ (bit size restricted to $O(\log n)$)

Manuel Kauers suggested some improvements.

- Compute *only* $b(n) \bmod n$ (bit size restricted to $O(\log n)$)
- Iterated squaring (only $O(\log n)$ steps)

Manuel Kauers suggested some improvements.

- Compute *only* $b(n) \bmod n$ (bit size restricted to $O(\log n)$)
- Iterated squaring (only $O(\log n)$ steps)
- Write in C (10x-20x constant improvements)

Manuel Kauers suggested some improvements.

- Compute *only* $b(n) \bmod n$ (bit size restricted to $O(\log n)$)
- Iterated squaring (only $O(\log n)$ steps)
- Write in C (10x-20x constant improvements)
- Parallelize search (more constant reductions)

New runtime: $O((\log n)^3 n)$, with a much smaller constant.

All pseudoprimes up to $10^{12} \approx 1.82 \times 2^{39}$:

$$\begin{aligned} 1,531,398 \\ 114,009,582 \\ 940,084,647 \\ 4,206,644,978 \\ 7,962,908,038 \\ 20,293,639,091 \\ 41,947,594,698 \end{aligned}$$

(It took around 2.5 years of computer time to find these.)

We found much better tests.

Here are two examples.

$$\frac{8x^4 + 10x^3 + 21x^2 - 5}{6x^5 + 8x^4 + 5x^3 + 7x^2 - 1}$$

$$\frac{5x^4 + 8x^3 + 3x^2 + 4x - 5}{2x^5 + 5x^4 + 4x^3 + x^2 + x - 1}$$

Test	First pseudoprime

We found much better tests.

Here are two examples.

$$\frac{8x^4 + 10x^3 + 21x^2 - 5}{6x^5 + 8x^4 + 5x^3 + 7x^2 - 1}$$

$$\frac{5x^4 + 8x^3 + 3x^2 + 4x - 5}{2x^5 + 5x^4 + 4x^3 + x^2 + x - 1}$$

Test	First pseudoprime
Fermat	561
Perrin	$(521)^2$ = 271,441
Our test	1,531,398

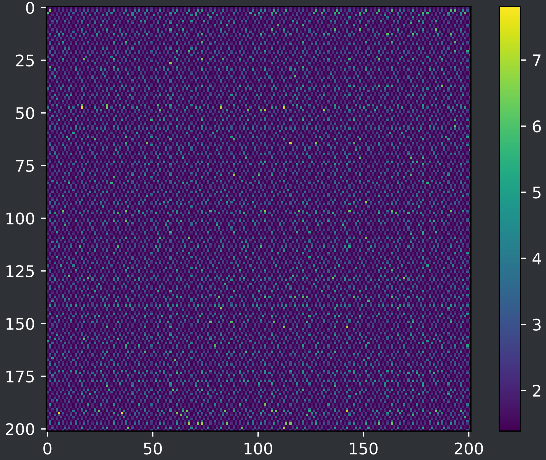
We found much better tests.

Here are two examples.

$$\frac{8x^4 + 10x^3 + 21x^2 - 5}{6x^5 + 8x^4 + 5x^3 + 7x^2 - 1}$$

$$\frac{5x^4 + 8x^3 + 3x^2 + 4x - 5}{2x^5 + 5x^4 + 4x^3 + x^2 + x - 1}$$

Test	First pseudoprime
Fermat	561
Perrin	$(521)^2 = 271{,}441$
Our test	1,531,398
Our test′	24,830,047
Our test″	50,768,194



Log-heatmap of the first pseudoprime of $x^2 - ax - b$.

Hardinian arrays

(with Manuel Kauers)

More guessing

Kauers and Koutschan searched the OEIS for recurrences using a novel lattice reduction technique.

This produced:

- Some junk.
- Some known or easy recurrences.
- About 20 *interesting* recurrences that no one knew.

More guessing

Kauers and Koutschan searched the OEIS for recurrences using a novel lattice reduction technique.

This produced:

- Some junk.
- Some known or easy recurrences.
- About 20 *interesting* recurrences that no one knew.

D-finite

$a(n)$ is D-finite if

$$p_d(n)a(n+d) + p_{d-1}(n)a(n+d-1) + \cdots + p_0(n)a(n) = 0$$

for some polynomials $p_i(n)$ and all $n \geq 0$.

Hardinian arrays

Definition (R.H. Hardin)

Let $H_1(n, k)$ be the number of $n \times k$ arrays which obey the following rules:

Hardinian arrays

Definition (R.H. Hardin)

Let $H_1(n, k)$ be the number of $n \times k$ arrays which obey the following rules:

- The top-left entry entry is 0.

Hardinian arrays

Definition (R.H. Hardin)

Let $H_1(n, k)$ be the number of $n \times k$ arrays which obey the following rules:

- The top-left entry entry is 0.
- Every king-step right, down, or south-east must increase values by 0 or 1.

Hardinian arrays

Definition (R.H. Hardin)

Let $H_1(n, k)$ be the number of $n \times k$ arrays which obey the following rules:

- The top-left entry entry is 0.
- Every king-step right, down, or south-east must increase values by 0 or 1.
- Every value must be within 1 of its king-distance from the top-left corner.

Definition (R.H. Hardin)

Let $H_1(n, k)$ be the number of $n \times k$ arrays which obey the following rules:

- The top-left entry entry is 0.
- Every king-step right, down, or south-east must increase values by 0 or 1.
- Every value must be within 1 of its king-distance from the top-left corner.
- The bottom-right entry equals its king-distance minus 1.

Example for $H_1(6, 5)$

$$\begin{bmatrix} 0 & 1 & 2 & 2 & 3 \\ 1 & 1 & 2 & 2 & 3 \\ 2 & 2 & 2 & 3 & 3 \\ 3 & 3 & 3 & 3 & 4 \\ 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 \end{bmatrix}$$

Example for $H_1(6, 5)$

$$\begin{bmatrix} \color{red}{0} & 1 & 2 & 2 & 3 \\ 1 & 1 & 2 & 2 & 3 \\ 2 & 2 & 2 & 3 & 3 \\ 3 & 3 & 3 & 3 & 4 \\ 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & 4 \end{bmatrix}$$

Example for $H_1(6, 5)$

$$\begin{bmatrix} \color{red}{0} & 1 & 2 & 2 & 3 \\ 1 & 1 & 2 & 2 & 3 \\ 2 & 2 & 2 & 3 & 3 \\ 3 & 3 & 3 & 3 & 4 \\ 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & \color{red}{4} \end{bmatrix}$$

Example for $H_1(6,5)$

$$\begin{bmatrix} \color{red}{0} & 1 & 2 & 2 & 3 \\ 1 & \color{red}{1} & 2 & 2 & 3 \\ 2 & 2 & 2 & 3 & 3 \\ 3 & 3 & 3 & 3 & 4 \\ 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & \color{red}{4} \end{bmatrix}$$

Example for $H_1(6, 5)$

$$\begin{bmatrix} \color{red}{0} & 1 & 2 & 2 & 3 \\ 1 & \color{red}{1} & \color{red}{2} & 2 & 3 \\ 2 & 2 & 2 & 3 & 3 \\ 3 & 3 & 3 & 3 & 4 \\ 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & \color{red}{4} \end{bmatrix}$$

Example for $H_1(6,5)$

$$\begin{bmatrix} \color{red}{0} & 1 & 2 & 2 & 3 \\ 1 & \color{red}{1} & \color{red}{2} & 2 & 3 \\ 2 & 2 & \color{red}{2} & 3 & 3 \\ 3 & 3 & 3 & 3 & 4 \\ 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & \color{red}{4} \end{bmatrix}$$

Example for $H_1(6, 5)$

$$\begin{bmatrix} \color{red}{0} & 1 & 2 & 2 & 3 \\ 1 & \color{red}{1} & \color{red}{2} & 2 & 3 \\ 2 & 2 & \color{red}{2} & 3 & 3 \\ 3 & 3 & 3 & \color{red}{3} & 4 \\ 4 & 4 & 4 & 4 & 4 \\ 4 & 4 & 4 & 4 & \color{red}{4} \end{bmatrix}$$

Example for $H_1(6, 5)$

$$\begin{bmatrix} \color{red}{0} & 1 & 2 & 2 & 3 \\ 1 & \color{red}{1} & \color{red}{2} & 2 & 3 \\ 2 & 2 & \color{red}{2} & 3 & 3 \\ 3 & 3 & 3 & \color{red}{3} & 4 \\ 4 & 4 & 4 & 4 & \color{red}{4} \\ 4 & 4 & 4 & 4 & \color{red}{4} \end{bmatrix}$$

Results

Hardin conjectured

$$H_1(n, n) = \frac{1}{3}(4^{n-1} - 1),$$

and also that $H_1(n, k)$ is a linear polynomial in n for $n \geq k$.

Results

Hardin conjectured

$$H_1(n,n) = \frac{1}{3}(4^{n-1} - 1),$$

and also that $H_1(n,k)$ is a linear polynomial in n for $n \geq k$.

Theorem (RDB, Kauers)

For $n \geq k \geq 1$,

$$H_1(n,k) = 4^{k-1}(n-k) + \frac{1}{3}(4^{k-1} - 1).$$

The diagonal case

$$\begin{bmatrix} 0 & 1 & 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 2 & 2 & 3 & 4 & 5 \\ 2 & 2 & 2 & 2 & 3 & 4 & 5 \\ 2 & 2 & 3 & 3 & 3 & 4 & 5 \\ 3 & 3 & 3 & 3 & 3 & 4 & 5 \\ 4 & 4 & 4 & 4 & 4 & 4 & 5 \\ 5 & 5 & 5 & 5 & 5 & 5 & 5 \end{bmatrix}$$

The diagonal case

$$\begin{bmatrix} 0 & 1 & 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 2 & 2 & 3 & 4 & 5 \\ 2 & 2 & 2 & 2 & 3 & 4 & 5 \\ 2 & 2 & 3 & 3 & 3 & 4 & 5 \\ 3 & 3 & 3 & 3 & 3 & 4 & 5 \\ 4 & 4 & 4 & 4 & 4 & 4 & 5 \\ 5 & 5 & 5 & 5 & 5 & 5 & 5 \end{bmatrix}$$

Every valid array can be partitioned into “regions” for each value.

The diagonal case

$$\begin{bmatrix} 0 & 1 & 1 & 2 & 3 & 4 & 5 \\ 1 & 1 & 2 & 2 & 3 & 4 & 5 \\ 2 & 2 & 2 & 2 & 3 & 4 & 5 \\ 2 & 2 & 3 & 3 & 3 & 4 & 5 \\ 3 & 3 & 3 & 3 & 3 & 4 & 5 \\ 4 & 4 & 4 & 4 & 4 & 4 & 5 \\ 5 & 5 & 5 & 5 & 5 & 5 & 5 \end{bmatrix}$$

Every valid array can be partitioned into “regions” for each value.

$H_1(n, n)$ is the number of tuples of nonintersecting paths from the first column to the first row.

Path counting

There is a well-known theorem to turn problems about nonintersecting paths into problems about determinants.

Path counting

There is a well-known theorem to turn problems about nonintersecting paths into problems about determinants.

Theorem (Gessel–Viennot)

Fix n distinct start points x_k and n distinct end points y_k.

Path counting

There is a well-known theorem to turn problems about nonintersecting paths into problems about determinants.

Theorem (Gessel–Viennot)

Fix n distinct start points x_k and n distinct end points y_k.

Let A be the $n \times n$ matrix where A_{ij} is the number of lattice paths from x_i to y_j.

Path counting

There is a well-known theorem to turn problems about nonintersecting paths into problems about determinants.

Theorem (Gessel–Viennot)

Fix n distinct start points x_k and n distinct end points y_k.

Let A be the $n \times n$ matrix where A_{ij} is the number of lattice paths from x_i to y_j.

The determinant of A gives the number of tuples of n non-intersecting paths which take x_i to y_i.

Plan of attack: Find *A* and compute its determinant.

$$\begin{bmatrix} 0 & \color{red}{1} & \color{red}{1} & 2 & 3 & 4 & 5 \\ 1 & 1 & 2 & 2 & 3 & 4 & 5 \\ \color{red}{2} & 2 & 2 & 2 & 3 & 4 & 5 \\ \color{red}{2} & 2 & 3 & 3 & 3 & 4 & 5 \\ 3 & 3 & 3 & 3 & 3 & 4 & 5 \\ 4 & 4 & 4 & 4 & 4 & 4 & 5 \\ 5 & 5 & 5 & 5 & 5 & 5 & 5 \end{bmatrix}$$

There are actually several matrices, because start and stop points are not fixed.

The first row and column each have exactly one “unused” position, so there is a matrix for each pair of position choices.

Sketch of computational proof for the diagonal case

$$H_1(n,n) = \sum_{i=0}^{n-2} \sum_{j=0}^{n-2} \det A_i^j$$

Sketch of computational proof for the diagonal case

$$H_1(n,n) = \sum_{i=0}^{n-2} \sum_{j=0}^{n-2} \det A_i^j$$

Possible to evaluate $\det A_i^j$ explicitly:

$$H_1(n,n) = \sum_{i=0}^{n-2} \sum_{j=0}^{n-2} \sum_{k=0}^{n-1} \binom{i}{k} \binom{j}{k}.$$

Sketch of computational proof for the diagonal case

$$s(n) := H_1(n, n) = \sum_{i=0}^{n-2} \sum_{j=0}^{n-2} \sum_{k=0}^{n-1} \binom{i}{k} \binom{j}{k}.$$

Could *probably* do this by hand, but we didn't try.

Sketch of computational proof for the diagonal case

$$s(n) := H_1(n,n) = \sum_{i=0}^{n-2}\sum_{j=0}^{n-2}\sum_{k=0}^{n-1}\binom{i}{k}\binom{j}{k}.$$

Could *probably* do this by hand, but we didn't try.

D-finite algorithms *provably* compute a recurrence.

$$s(n+2) = 5s(n+1) - 4s(n).$$

The closed form is easy from here.

Infinite families

Hardin submitted a *family* of sequences $H_r(n, k)$.

Definition (R.H. Hardin)

Let $H_r(n, k)$ be the number of $n \times k$ arrays which obey the following rules:

Hardin submitted a *family* of sequences $H_r(n,k)$.

Definition (R.H. Hardin)

Let $H_r(n,k)$ be the number of $n \times k$ arrays which obey the following rules:

- The top-left entry entry is 0.
- Every king-step right, down, or south-east must increase values by 0 or 1.
- Every value must be within r of its king-distance from the top-left corner.
- The bottom-right entry equals its king-distance minus r.

Theorem (RDB, Kauers)

$H_r(n, n)$ is D-finite for all $r \geq 1$.

Proof is non-constructive application of an identity due to Jacobi.

Constructive proof exists *in principle*, but too expensive beyond $r = 2$.

Theorem (RDB, Kauers)

$H_r(n,n)$ is D-finite for all $r \geq 1$.

Proof is non-constructive application of an identity due to Jacobi.

Constructive proof exists *in principle*, but too expensive beyond $r = 2$.

The $r = 2$ case requires computing recurrences satisfied by

$$S(n) := \sum_{i_1 \geq 0} \sum_{i_2 > i_1} \sum_{j_1 \geq 0} \sum_{j_2 > j_1} \sum_{u=0}^{n} \sum_{v=0}^{n} \binom{u}{i_1} \binom{u}{j_1} \binom{v}{i_2} \binom{v}{j_2},$$

and it gets worse from there.

Conjectures

For sufficiently large n:

$$H_2(n,1) = \frac{1}{2}n^2 - \frac{3}{2}n + 1$$
$$H_2(n,2) = 4n^2 - 20n + 25$$
$$H_2(n,3) = 40n^2 - 279n + 497$$
$$H_2(n,3) = 480n^2 - 4354n + 10098$$
$$H_2(n,4) = 6400n^2 - 71990n + 206573$$
$$H_2(n,5) = 90112n^2 - 1212288n + 4150790$$
$$H_2(n,6) = 1306624n^2 - 20460244n + 81385043$$

Similar conjectures for all $H_r(n,k)$, but no proofs!

Summary

Many more projects, not enough time.

- Irrationality proofs
- Summation, integration
- Lattice path enumeration
- Continued fractions

Committee collaboration distances

```
RDB:
  ⋆ Manuel Kauers
  ⋆ Doron Zeilberger:
      ⋆ Vladimir Retakh
        Christian Krattenthaler:
            Henk Hollmann:
              ⋆ Swee Hong Chan
```