How large can a finite group of matrices be?

Blundon Lecture
UNB Fredericton 10/13/2007

Martin Lorenz
Temple University, Philadelphia

Overview

- Groups . . . and some of their uses

Overview

- Groups . . . and some of their uses
- The size of finite matrix groups

Overview

- Groups . . . and some of their uses
- The size of finite matrix groups
- The Minkowski sequence: two mysteries

Reference

R. M. Guralnick & L.: *Orders of finite groups of matrices*, Contemp. Math. **420**, 141–162 (2006), arXiv:math.GR/0511191.

Reference

R. M. Guralnick & L.: *Orders of finite groups of matrices*, Contemp. Math. **420**, 141–162 (2006), arXiv:math.GR/0511191.

☞ pdf file of **this talk** on my web page

Part I: Groups

The definition of a “group”

. . . here it is (from **Bourbaki**):

DÉFINITION 1. — *On appelle* groupe *un ensemble muni d'une loi de composition associative, possédant un élément neutre et pour laquelle tout élément est inversible.*

The definition of a “group”

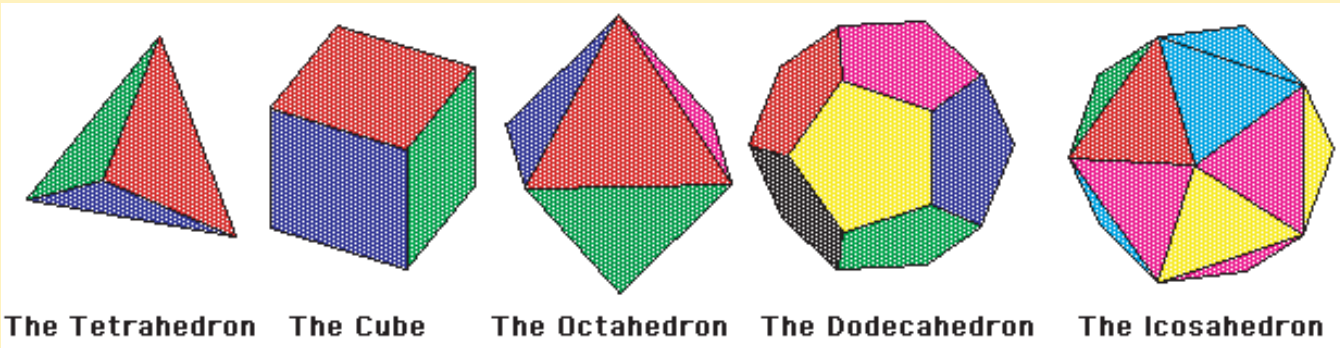
. . . here it is (from **Bourbaki**):

DÉFINITION 1. — *On appelle* groupe *un ensemble muni d'une loi de composition associative, possédant un élément neutre et pour laquelle tout élément est inversible.*

Groups have been around long before they were defined in the above terms . . .

Geometry: symmetry groups

Given $X \subset \mathbb{R}^n$ (e.g., a Platonic solid in $\mathbb{R}^3$), any distance preserving transformation of $\mathbb{R}^n$ that maps X to itself is called a symmetry of X.



(from MacTutor History of Mathematics archive)

Example: the dodecahedron

$\rightsquigarrow$ symmetry group

A_5

It has **60** symmetries which form the so-called alternating group of degree 5.

Physics: gauge groups

Theories in physics are often described by "Lagrangians" which are invariant under certain symmetry transformation groups, called gauge groups.

These are infinite groups such as the orthogonal group

$$\begin{aligned}\mathbf{O}_n(\mathbb{R}) &= \{A \in \mathrm{M}_n(\mathbb{R}) \mid \|Ax\| = \|x\| \quad \forall x \in \mathbb{R}^n\} \\ &= \{A \in \mathrm{M}_n(\mathbb{R}) \mid A \cdot A^{\mathrm{tr}} = \mathbf{1}_{n\times n}\}\end{aligned}$$

$n \times n$-matrices

transpose matrix

Algebra: Galois groups

Recall: the **quadratic polynomial** equation

$$ax^2 + bx + c = 0$$

has solutions

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}$$

Algebra: Galois groups

Similar formulas (more complicated and requiring higher roots) are known for **cubic** and **quartic** polynomials.

Tartaglia, Ferrari, Cardano; 16^{th} century

Algebra: Galois groups

Similar formulas (more complicated and requiring higher roots) are known for **cubic** and **quartic** polynomials.

Tartaglia, Ferrari, Cardano; 16^{th} century

For **degree 5**, however, this is no longer possible!

Niels Henrik Abel, 1824

Algebra: Galois groups

The ultimate reason for the "non-solvability of the quintic equation by radicals" is **group theoretical**:

A_5 is non-abelian simple

FINAL WORD: associated to a polynomial eq^n of **any degree**, there is a finite group, the Galois group of the eq^n.

Evariste Galois
1811 – 1832

The eq^n is solvable by radicals

$\Updownarrow$

its Galois group has no non-abelian simple "pieces"

The Enormous Theorem

Finite simple groups are the “elementary particles” of finite group theory.

Finite simple groups are the "elementary particles" of finite group theory.

They are now all known; the Enormous Theorem (about 1983) gives a complete classification:

There are several series of finite simple groups (e.g. A_5, A_6, A_7, ...) and **26** isolated ones, known as the sporadic groups.

Size of the Classification Project

- The original “proof” of the Enormous Theorem was spread over a vast number journal articles and various unpublished manuscripts, some of which are incomplete.

Size of the Classification Project

- The original “proof” of the Enormous Theorem was spread over a vast number journal articles and various unpublished manuscripts, some of which are incomplete.

- Some skepticism on the proof remains; it is currently being completely reworked. The “2^{nd}-generation” proof will run to approximately 5,000 pages when finished.

Size of the Classification Project

- The original "proof" of the Enormous Theorem was spread over a vast number journal articles and various unpublished manuscripts, some of which are incomplete.

- Some skepticism on the proof remains; it is currently being completely reworked. The "2^{nd}-generation" proof will run to approximately 5,000 pages when finished.

- The largest sporadic group is known as the Monster; it has size

$$808017424794512875886459904961710757005754368000000000$$

Part II: Matrix Groups

We will be looking at matrices in

$$\mathrm{GL}_n(\mathbb{C}) = \{\text{all invertible } n \times n\text{-matrices over } \mathbb{C}\}$$

We will be looking at matrices in

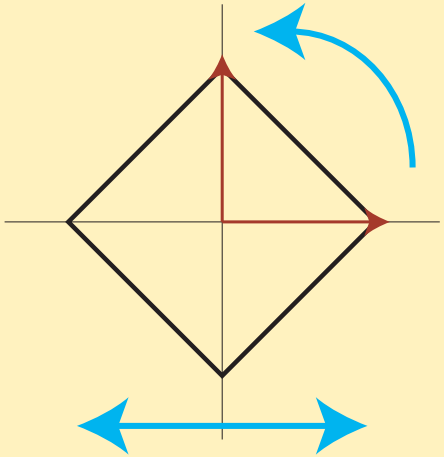
$$\mathrm{GL}_n(\mathbb{C}) = \{\text{all invertible } n \times n\text{-matrices over } \mathbb{C}\}$$

Def$^{\mathbf{n}}$: A finite subgroup of $\mathrm{GL}_n(\mathbb{C})$ is a finite (non-empty) collection of matrices $\mathcal{G} \subseteq \mathrm{GL}_n(\mathbb{C})$ satisfying

$$A, B \in \mathcal{G} \qquad \Rightarrow \qquad A \cdot B \in \mathcal{G}$$

The number of matrices in $\mathcal{G}$ is called the order of $\mathcal{G}$.

Example: symmetries of the square ($n = 2$)

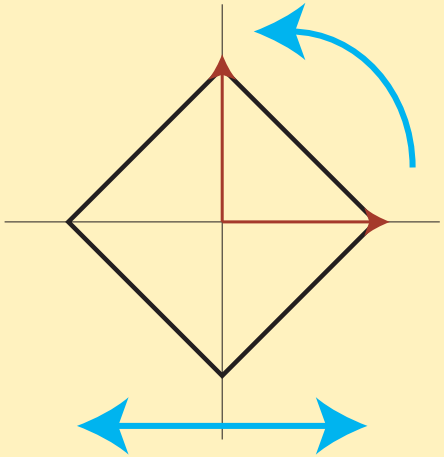


$\rightsquigarrow$ **matrices**:

$90°$ rotation: $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

reflection across y-axis: $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$

Example: symmetries of the square ($n = 2$)



$\rightsquigarrow$ **matrices**:

90° rotation: $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$

reflection across y-axis: $\begin{pmatrix} -1 & 0 \\ 0 & 1 \end{pmatrix}$

The group $\mathcal{G} = \{$ all symmetries of the square $\} \subseteq \mathrm{GL}_2(\mathbb{C})$ has order

$$|\mathcal{G}| = 4 \cdot 2 = 2^n \, n! \; .$$

Basic Q$^{\mathbf{n}}$: Given n, what are the possible orders of finite subgroups of $\mathrm{GL}_n(\mathbb{C})$?

Basic Q$^{\mathbf{n}}$: Given n, what are the possible orders of finite subgroups of $\mathrm{GL}_n(\mathbb{C})$?

Answer: They can be anything you want! Indeed, pick s and form the scalar matrix

$$A = \begin{pmatrix} e^{2\pi i/s} & & \\ & \ddots & \\ & & e^{2\pi i/s} \end{pmatrix}_{n\times n}$$

Then $\mathcal{G} = \{\mathbf{1}_{n\times n}, A, A^2, \ldots A^{s-1}\}$ is a subgroup of $\mathrm{GL}_n(\mathbb{C})$ of order s.

Modified Q$^{\mathbf{n}}$: What about $\mathrm{GL}_n(\mathbb{Q})$ instead?

Minkowski's Theorem

Hermann Minkowski
1864 – 1909

- "geometry of numbers"
- relativity: "space-time"
- quadratic forms

Minkowski's Theorem

Minkowski (1887): *The least common multiple of the orders of all finite subgroups of* $\mathrm{GL}_n(\mathbb{Q})$ *is given by*

$$M(n) = \prod_{\ell \text{ prime}} \ell^{\left\lfloor \frac{n}{\ell-1} \right\rfloor + \left\lfloor \frac{n}{\ell(\ell-1)} \right\rfloor + \left\lfloor \frac{n}{\ell^2(\ell-1)} \right\rfloor + \cdots}$$

Here $\lfloor \quad \rfloor$ is the greatest integer ("floor") function

Minkowski's Theorem

Minkowski (1887): *The least common multiple of the orders of all finite subgroups of* $\mathrm{GL}_n(\mathbb{Q})$ *is given by*

$$M(n) = \prod_{\ell \text{ prime}} \ell^{\left\lfloor \frac{n}{\ell-1} \right\rfloor + \left\lfloor \frac{n}{\ell(\ell-1)} \right\rfloor + \left\lfloor \frac{n}{\ell^2(\ell-1)} \right\rfloor + \cdots}$$

The ℓ-factor for $\ell > n+1$ equals 1; so the product is finite.
E.g.,

$$M(1) = 2^1 = 2 \qquad M(2) = 2^{2+1}\,3^1 = 24$$
$$M(3) = 2^{3+1}\,3^1 = 48 \qquad M(4) = 2^{4+2+1}\,3^2\,5^1 = 5760$$

Minkowski's Theorem

Minkowski (1887): *The least common multiple of the orders of all finite subgroups of* $\mathrm{GL}_n(\mathbb{Q})$ *is given by*

$$M(n) = \prod_{\ell \text{ prime}} \ell^{\left\lfloor \frac{n}{\ell-1} \right\rfloor + \left\lfloor \frac{n}{\ell(\ell-1)} \right\rfloor + \left\lfloor \frac{n}{\ell^2(\ell-1)} \right\rfloor + \cdots}$$

Recursion: $M(2n+1) = 2\,M(2n)$

$$M(2n) = 2\,M(2n-1) \prod_{\ell \text{ prime},\ \ell-1 \mid 2n} \ell n_\ell$$

Minkowski's Theorem

Minkowski (1887): *The least common multiple of the orders of all finite subgroups of* $\mathrm{GL}_n(\mathbb{Q})$ *is given by*

$$M(n) = \prod_{\ell \text{ prime}} \ell^{\left\lfloor \frac{n}{\ell-1} \right\rfloor + \left\lfloor \frac{n}{\ell(\ell-1)} \right\rfloor + \left\lfloor \frac{n}{\ell^2(\ell-1)} \right\rfloor + \cdots}$$

Recursion: $M(2n+1) = 2\,M(2n)$

$M(2n) = 2\,M(2n-1)$ $\underbrace{\prod_{\ell \text{ prime},\ \ell-1 \mid 2n} \ell^{n_\ell}}_{= \text{denominator of } \frac{B_{2n}}{n}}$

Bernoulli numbers: $\frac{x}{e^x-1} = \sum_{n \geq 0} \frac{B_n x^n}{n!}$

Minkowski's Theorem

Minkowski (1887): *The least common multiple of the orders of all finite subgroups of* $\mathrm{GL}_n(\mathbb{Q})$ *is given by*

$$M(n) = \prod_{\ell \text{ prime}} \ell^{\left\lfloor \frac{n}{\ell-1} \right\rfloor + \left\lfloor \frac{n}{\ell(\ell-1)} \right\rfloor + \left\lfloor \frac{n}{\ell^2(\ell-1)} \right\rfloor + \cdots}$$

Using the identity $(m!)_\ell = \ell^{\left\lfloor \frac{m}{\ell} \right\rfloor + \left\lfloor \frac{m}{\ell^2} \right\rfloor + \cdots}$, one can rewrite the ℓ-factor:

ℓ-part

$$M(n)_\ell = \ell^{\left\lfloor \frac{n}{\ell-1} \right\rfloor} \left(\left\lfloor \frac{n}{\ell-1} \right\rfloor ! \right)_\ell$$

Minkowski (1887): *The least common multiple of the orders of all finite subgroups of* $\mathrm{GL}_n(\mathbb{Q})$ *is given by*

$$M(n) = \prod_{\ell \text{ prime}} \ell^{\left\lfloor \frac{n}{\ell-1} \right\rfloor + \left\lfloor \frac{n}{\ell(\ell-1)} \right\rfloor + \left\lfloor \frac{n}{\ell^2(\ell-1)} \right\rfloor + \cdots}$$

More on the Minkowski numbers $M(n)$ later ...

Example: $\mathrm{GL}_n(\mathbb{Q})$ contains the subgroup of "monomial matrices": exactly one entry ± 1 in each row and column, all other entries are 0

$$\mathbf{O}_n(\mathbb{Z}) = \begin{pmatrix} \pm 1 & & \\ & \ddots & \\ & & \pm 1 \end{pmatrix} \rtimes S_n$$

Example: $\mathrm{GL}_n(\mathbb{Q})$ contains the subgroup of "monomial matrices": exactly one entry ± 1 in each row and column, all other entries are 0

$$\mathbf{O}_n(\mathbb{Z}) = \begin{pmatrix} \pm 1 & & \\ & \ddots & \\ & & \pm 1 \end{pmatrix} \rtimes S_n$$

This group has order $|\mathbf{O}_n(\mathbb{Z})| = 2^n\, n!$ $\quad\rightsquigarrow\quad$ $|\mathbf{O}_n(\mathbb{Z})|_2 = M(n)_2$

($n = 2$: symmetries of the square)

Example: $\mathrm{GL}_n(\mathbb{Q})$ contains the subgroup of "monomial matrices": exactly one entry ± 1 in each row and column, all other entries are 0

$$\mathbf{O}_n(\mathbb{Z}) = \begin{pmatrix} \pm 1 & & \\ & \ddots & \\ & & \pm 1 \end{pmatrix} \rtimes S_n$$

This group has order $|\mathbf{O}_n(\mathbb{Z})| = 2^n\, n!$ $\rightsquigarrow$ $|\mathbf{O}_n(\mathbb{Z})|_2 = M(n)_2$

($n = 2$: symmetries of the square)

Similarly: for each prime ℓ, there is a subgroup $\mathcal{G} \subseteq \mathrm{GL}_n(\mathbb{Q})$ such that $|\mathcal{G}|_\ell = M(n)_\ell$.

Hence, the main content of Minkowski's Theorem is:

> *The order of any finite subgroup of* $\mathrm{GL}_n(\mathbb{Q})$ *divides* $M(n)$

Hence, the main content of Minkowski's Theorem is:

The order of any finite subgroup of $\mathrm{GL}_n(\mathbb{Q})$ *divides* $M(n)$

How does one go about proving this?

Idea of proof

Given: $\mathcal{G}$ a finite subgp. of $\mathrm{GL}_n(\mathbb{Q})$
ℓ a prime

Want: $|\mathcal{G}|_\ell$ divides $M(n)_\ell$

Idea of proof

Given: $\mathcal{G}$ a finite subgp. of $\mathrm{GL}_n(\mathbb{Q})$
ℓ a prime

Want: $|\mathcal{G}|_\ell$ divides $M(n)_\ell$

Step 1 (group theory & linear algebra): After a base change, $\mathcal{G} \subseteq \mathrm{GL}_n(\mathbb{Z})$ (!)

Idea of proof

Given: $\mathcal{G}$ a finite subgp. of $\mathrm{GL}_n(\mathbb{Q})$ **Want**: $|\mathcal{G}|_\ell$ divides $M(n)_\ell$
ℓ a prime

Step 1 (group theory & linear algebra): After a base change, $\mathcal{G} \subseteq \mathrm{GL}_n(\mathbb{Z})$ (!) So we can reduce entries modulo another prime p :

$$\begin{array}{ccc} \mathrm{GL}_n(\mathbb{Z}) & \longrightarrow & \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z}) \\ \cup & & \cup \\ A = (a_{ij}) & \mapsto & \overline{A} = (a_{ij} \bmod p) \end{array}$$

Idea of proof

Given: $\mathcal{G}$ a finite subgp. of $\mathrm{GL}_n(\mathbb{Q})$ **Want**: $|\mathcal{G}|_\ell$ divides $M(n)_\ell$
ℓ a prime

Step 1 (group theory & linear algebra): After a base change, $\mathcal{G} \subseteq \mathrm{GL}_n(\mathbb{Z})$ (!) So we can reduce entries modulo another prime p :

$$\begin{array}{ccc} \mathrm{GL}_n(\mathbb{Z}) & \longrightarrow & \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z}) \\ \cup & & \cup \\ A = (a_{ij}) & \mapsto & \overline{A} = (a_{ij} \bmod p) \end{array}$$

As long as $p \neq 2$, this map is **1-to-1** on $\mathcal{G}$ (!) Hence $|\mathcal{G}| \leq |\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})|$.

Idea of proof

Given: $\mathcal{G}$ a finite subgp. of $\mathrm{GL}_n(\mathbb{Q})$ **Want**: $|\mathcal{G}|_\ell$ divides $M(n)_\ell$
ℓ a prime

Step 1 (group theory & linear algebra): After a base change, $\mathcal{G} \subseteq \mathrm{GL}_n(\mathbb{Z})$ (!) So we can reduce entries modulo another prime p :

$$\begin{array}{ccc} \mathrm{GL}_n(\mathbb{Z}) & \longrightarrow & \mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z}) \\ \cup & & \cup \\ A = (a_{ij}) & \mapsto & \overline{A} = (a_{ij} \bmod p) \end{array}$$

As long as $p \neq 2$, this map is **1-to-1** on $\mathcal{G}$ (!) Hence $|\mathcal{G}| \leq |\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})|$. In fact, by Lagrange's Theorem (!)

$$|\mathcal{G}| \textbf{ divides } |\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})|$$

Idea of proof

Given: $\mathcal{G}$ a finite subgp. of $\mathrm{GL}_n(\mathbb{Q})$ **Want**: $|\mathcal{G}|_\ell$ divides $M(n)_\ell$

ℓ a prime

Counting bases of n-space over $\mathbb{Z}/p\mathbb{Z}$ one obtains

$$|\,\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})| = (p^n-1)(p^n-p)(p^n-p^2)\ldots(p^n-p^{n-1})$$
$$= p^{n(n-1)/2}\prod_{i=1}^{n}(p^i-1)$$

Idea of proof

Given: $\mathcal{G}$ a finite subgp. of $\mathrm{GL}_n(\mathbb{Q})$ **Want**: $|\mathcal{G}|_\ell$ divides $M(n)_\ell$
ℓ a prime

Counting bases of n-space over $\mathbb{Z}/p\mathbb{Z}$ one obtains

$$|\,\mathrm{GL}_n(\mathbb{Z}/p\mathbb{Z})| = (p^n-1)(p^n-p)(p^n-p^2)\ldots(p^n-p^{n-1})$$
$$= p^{n(n-1)/2}\prod_{i=1}^{n}(p^i-1)$$

To summarize: if $p \neq 2$ then the order $|\mathcal{G}|$ divides this number; so

$$p \neq 2, p \neq \ell \quad \Rightarrow \quad |\mathcal{G}|_\ell \;\Big|\; \textstyle\prod_{i-1}^{n}(p^i-1)_\ell$$

Idea of proof

Given: $\mathcal{G}$ a finite subgp. of $\mathrm{GL}_n(\mathbb{Q})$
ℓ a prime

Want: $|\mathcal{G}|_\ell$ divides $M(n)_\ell$

Step 2 (number theory): $\ell \neq 2 \quad \Rightarrow \quad \prod_{i-1}^{n}(p^i - 1)_\ell = M(n)_\ell$
for infinitely many primes p

Idea of proof

Given: $\mathcal{G}$ a finite subgp. of $\mathrm{GL}_n(\mathbb{Q})$
ℓ a prime

Want: $|\mathcal{G}|_\ell$ divides $M(n)_\ell$

Step 2 (number theory): $\ell \neq 2 \quad \Rightarrow \quad \prod_{i-1}^{n}(p^i - 1)_\ell = M(n)_\ell$
for infinitely many primes p

$$\therefore \qquad |\mathcal{G}|_\ell \;\Big|\; M(n)_\ell \qquad \text{at least for } \ell \neq 2$$

The prime $\ell = 2$ requires more work, as usual ...

Part III: Two Mysteries

Entering the first six terms of $M(n)$,

$$2, 24, 48, 5760, 11520, 2903040$$

into the *On-Line Encyclopedia of Integer Sequences* by Neil Sloane (AT&T) brings up sequence **A053657**.

A053657 has two alternative descriptions . . .

Sequence $M(n)$ – First Alternative

- **Integer-valued polynomials on primes:** Consider all polynomials $f(x) \in \mathbb{Q}[x]$ of degree $\leq n$ such that $f(p) \in \mathbb{Z}$ for all primes p.

Sequence $M(n)$ – First Alternative

- **Integer-valued polynomials on primes:** Consider all polynomials $f(x) \in \mathbb{Q}[x]$ of degree $\leq n$ such that $f(p) \in \mathbb{Z}$ for all primes p.

The **smallest positive** leading coefficient of any such polynomial is a fraction of the form $\frac{1}{a(n)}$ for some positive integer $a(n)$.

Sequence $M(n)$ – First Alternative

- **Integer-valued polynomials on primes:** Consider all polynomials $f(x) \in \mathbb{Q}[x]$ of degree $\leq n$ such that $f(p) \in \mathbb{Z}$ for all primes p.

The **smallest positive** leading coefficient of any such polynomial is a fraction of the form $\frac{1}{a(n)}$ for some positive integer $a(n)$.

Minkowski's formula is identical with the one proved independently for $a(n+1)$ by Chabert et. al.; so

$$a(n+1) = M(n)$$

Reference: Jean-Luc Chabert, Scott T. Chapman, and William W. Smith, *A basis for the ring of polynomials integer-valued on prime numbers,* Factorization in integral domains (Iowa City, IA, 1996), Lecture Notes in Pure and Appl. Math., vol. 189, Dekker, New York, 1997, pp. 271–284.

Sequence $M(n)$ – Second Alternative

- **Logarithm power expansion**: Let $P(n, z) \in \mathbb{Q}[z]$ be the coefficient of x^n in the Taylor series for $\left(\frac{-\ln(1-x)}{x}\right)^z$.

  — Paul Hanna: OEIS

Sequence $M(n)$ – Second Alternative

- **Logarithm power expansion**: Let $P(n,z) \in \mathbb{Q}[z]$ be the coefficient of x^n in the Taylor series for $(\frac{-\ln(1-x)}{x})^z$.

  — Paul Hanna: OEIS

In detail: put $\xi = \frac{-\ln(1-x)}{x} - 1 = \sum_{k=1}^{\infty} \frac{x^k}{k+1}$ to get

$$\left(\frac{-\ln(1-x)}{x}\right)^z = (1+\xi)^z = \sum_{m\geq 0} \binom{z}{m} \xi^m = 1 + \sum_{n\geq 1} P(n,z)x^n$$

- **Logarithm power expansion**: Let $P(n,z) \in \mathbb{Q}[z]$ be the coefficient of x^n in the Taylor series for $\left(\frac{-\ln(1-x)}{x}\right)^z$.

  — Paul Hanna: OEIS

In detail: put $\xi = \frac{-\ln(1-x)}{x} - 1 = \sum_{k=1}^{\infty} \frac{x^k}{k+1}$ to get

$$\left(\frac{-\ln(1-x)}{x}\right)^z = (1+\xi)^z = \sum_{m\geq 0} \binom{z}{m} \xi^m = 1 + \sum_{n\geq 1} P(n,z)x^n$$

Examples:

$$P(1,z) = \frac{z}{2} \qquad P(2,z) = \frac{5z+3z^2}{24}$$

$$P(3,z) = \frac{6z+5z^2+z^3}{48} \qquad P(4,z) = \frac{502z+485z^2+150z^3+15z^4}{5760}$$

Sequence $M(n)$ – Second Alternative

- **Logarithm power expansion**: Let $P(n, z) \in \mathbb{Q}[z]$ be the coefficient of x^n in the Taylor series for $\left(\frac{-\ln(1-x)}{x}\right)^z$.

  — Paul Hanna: OEIS

Putting $b(n) =$ denominator of $P(n, z)$, it has recently been proved that

$$b(n) = a(n+1)$$

So $b(n) = M(n)$.

Reference: Jean-Luc Chabert, *Integer-valued polynomials on prime numbers and logarithm power expansion*, European Journal of Combinatorics **28** (2007), 754–761.

Coincidence ?

. . . if time

Large matrix groups (again)

Recall: $\mathrm{GL}_n(\mathbb{Q})$ contains the group of monomial matrices $\mathbf{O}_n(\mathbb{Z})$ of order $|\mathbf{O}_n(\mathbb{Z})| = 2^n\, n!$

Large matrix groups (again)

Recall: $\mathrm{GL}_n(\mathbb{Q})$ contains the group of monomial matrices $\mathbf{O}_n(\mathbb{Z})$ of order $|\mathbf{O}_n(\mathbb{Z})| = 2^n\, n!$

Feit (unpubl., $\approx$ 1998):

Walter Feit
1930 – 2004

$|\mathbf{O}_n(\mathbb{Z})| = 2^n n!$ is the largest order of any finite subgroup of $\mathrm{GL}_n(\mathbb{Q})$ for $n > 10$ and $n = 1, 3, 5$. Moreover, $\mathbf{O}_n(\mathbb{Z})$ is the unique subgroup of that order, up to conjugacy.

Large matrix groups (again)

Feit relies on an unfinished manuscript of **Weisfeiler** on the "Jordan bound" (based on the Enormous Theorem).

Boris Weisfeiler has been missing in Chile since January 4, 1985 (`http://boris.weisfeiler.com`)

Large matrix groups (again)

Feit relies on an unfinished manuscript of **Weisfeiler** on the "Jordan bound" (based on the Enormous Theorem).

Weisfeiler's work has now been completed (and improved) by **Michael Collins** (preprints, Oxford University, 2005)