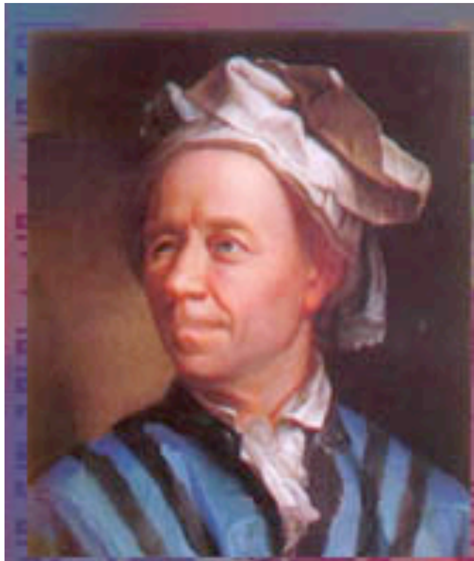
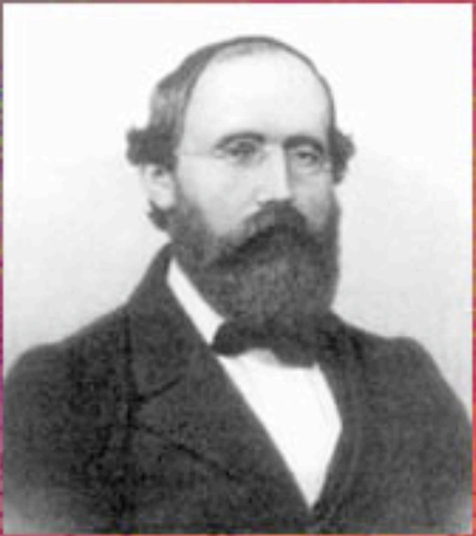
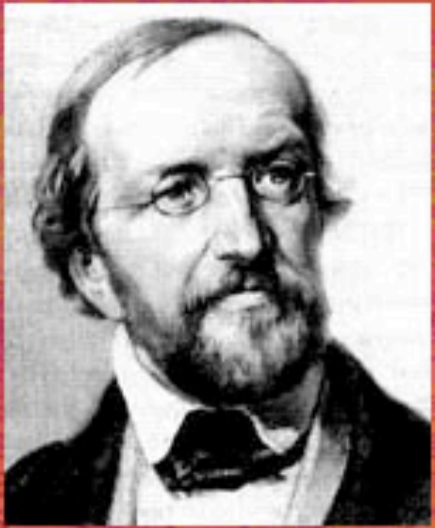
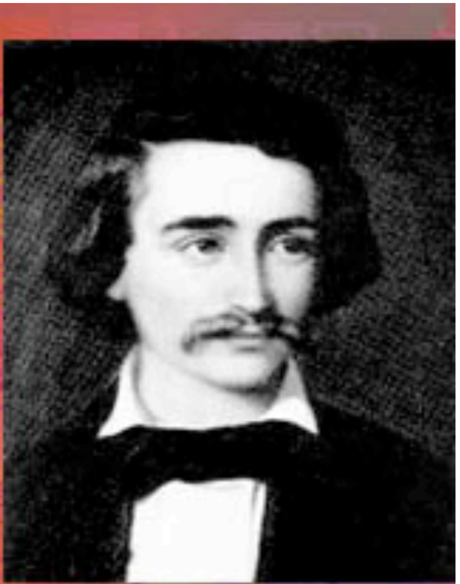
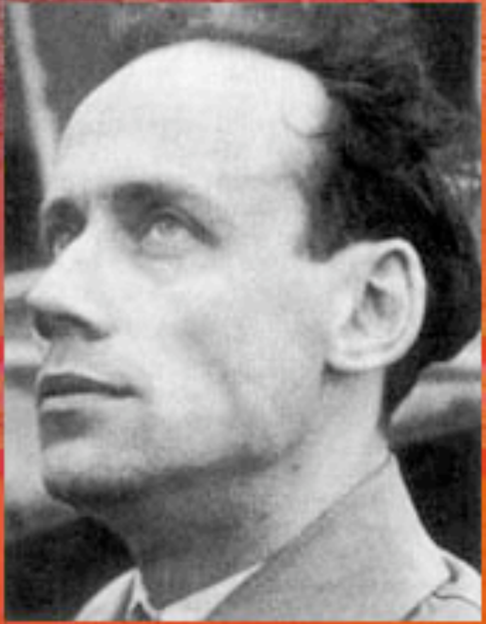


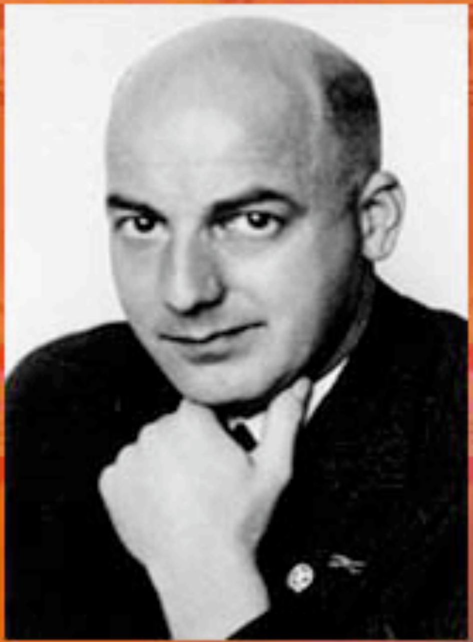


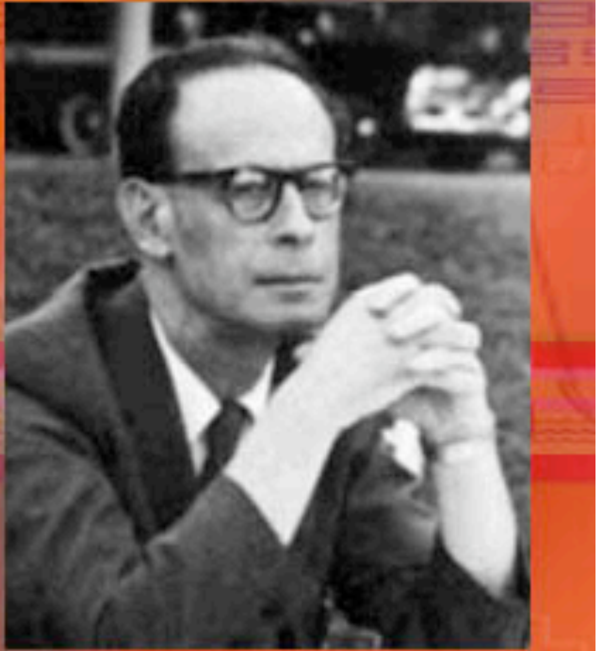




Name the mathematicians







Leonhard Euler 1707-1783

Johann

Jacob

Daniel

Nicolaus

The Bernoulli Family

Leonhard Euler 1707-1783

Johann

Jacob

Daniel

Nicolaus

The Bernoulli Family

Dear Leonhard,
Please bring: 15 pounds of coffee,
one pound of best green tea,
six bottles of brandy, 12 dozen fine tobacco pipes
and a few dozen packs of playing cards.

Leonhard Euler 1707-1783

$$1 + 1/4 + 1/9 + 1/16 + \cdots + 1/n^2 + \cdots$$

So much work has been done on the series that it seems hardly likely that anything new about them may still turn up...I, too in spite of repeated effort, could achieve nothing more than approximate values for their sums.

Now, however, quite unexpectedly, I have found an elegant formula depending on the quadrature of the circle.

Leonhard Euler 1707-1783

$$1+1/4+1/9+1/16+\cdots+1/n^2+\cdots=\pi^2/6$$

$$\zeta(s)=1+2^{-s}+3^{-s}+\cdots+n^{-s}+\cdots$$

$$\zeta(2n)=\frac{2^{2n-1}|B_{2n}|}{(2n)!}\pi^{2n}$$

Euler's Product

$$\zeta(s)=\prod_{p\ \text{prime}}\frac{1}{(1-p^{-s})}$$

Divergence at s=1 implies there are infinitely many primes

Leonhard Euler 1707-1783

Lejeune Dirichlet

1805-1859

“He is rather tall, lanky-looking man with moustache and beard about to turn grey…with a somewhat harsh voice and rather deaf: it was early, he was unwashed and unshaved and with his schlafrock, slippers, cup of coffee and cigar.”

Fermat conjectured that if r and N are prime then the sequence

$$r,\ r+N,\ r+2N,\ r+3N, \dots$$

contains infinitely many primes.

Dirichlet used a variant of the zeta function to prove Fermat correct.
For example, the analytic behaviour of the following function at $s=1$ proves there are infinitely many primes congruent to 1 modulo 4

$$\mathbf{L(s,\chi) = \sum_{n=1}^{\infty} \chi(n) n^{-s}}$$

where

$$\begin{aligned} \chi(n) &= 1 \text{ if } n = 1 \pmod 4 \\ \chi(n) &= -1 \text{ if } n = 3 \pmod 4 \\ \chi(n) &= 0 \text{ if } n \text{ is even} \end{aligned}$$

Dirichlet series $\mathbf{\sum_{n=1}^{\infty} a_n n^{-s}}$

Georg Friedrich Bernhard

Riemann

1826 - 1866

Richard Dedekind (1831-1916)

Dedekind zeta function

K algebraic number field extending $\mathbb{Q}$

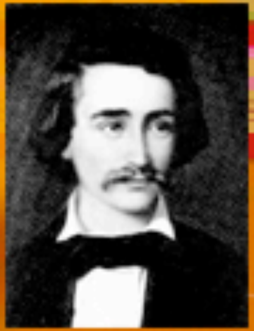
$$\begin{aligned}\zeta_K(s) &= \sum_{\mathfrak{a} \lhd \vartheta_K} N(\mathfrak{a})^{-s} \\ &= \sum_{\mathfrak{a} \lhd \vartheta_K} |\vartheta_K : \mathfrak{a}|^{-s}\end{aligned}$$

The residue of the pole at $s = 1$ contains information about how badly ϑ_K factorizes

Class number formula

$$\lim_{\mathbf{s}=\mathbf{1}} (\mathbf{s}-\mathbf{1})\zeta_{\mathbf{K}}(\mathbf{s}) = \frac{2^{r_1}(2\pi)^{r_2}}{w\sqrt{|d|}}\mathbf{R}\,h$$

h=class number



Emil Artin
(1898-1962)

Helmut Hasse
(1898-1979)

André Weil
(1906-1998)

The local zeta function of an elliptic curve at p

$\mathbf{K} = \mathbb{F}_{\mathbf{p}}(\mathbf{x})(\sqrt{x^3 - Ax - B})$ elliptic curve $\mathbf{E} : \mathbf{y}^2 = \mathbf{x}^3 - \mathbf{Ax} - \mathbf{B}$

D integral closure of $\mathbb{F}_{\mathbf{p}}(\mathbf{x})[\sqrt{x^3 - Ax - B}]$

Artin in his thesis considered

$$\zeta_D(s) = \sum_{I \lhd \vartheta_K} |D : I|^{-s} = (1 - p^{-s})\zeta(E_p, s)$$

where

$$\zeta(E_p, s) = \exp\left(\sum_{m=1}^{\infty} N_{p^m}\frac{p^{-ms}}{m}\right)$$

and

$$N_{p^m} = \left|E(\mathbb{F}_{p^m})\right| = \left|\left\{(a, b) \in \mathbb{F}_{p^m}^2 : b^2 = a^3 - Aa - B\right\}\right| + 1$$

Artin proved

$$\zeta(E_p, s) = \frac{\left(1 - (p + 1 - N_p)p^{-s} + p^{1-2s}\right)}{(1 - p^{-s})(1 - p^{1-s})} = \frac{(1 + \alpha_p p^{-s})(1 + \beta_p p^{-s})}{(1 - p^{-s})(1 - p^{1-s})}$$

a rational function

Artin conjectured the Riemann Hypothesis for elliptic curves

$$|\alpha_p| = |\beta_p| = p^{1/2}$$

The first person to prove a Riemann Hypothesis was

GAUSS

The last entry of Gauss's mathematical diary proves for the elliptic curve $E: y^2 = x^3 - x$

$$\begin{aligned} &\text{If } p = 3 \pmod 4 \text{ then } & N_p &= p+1 \\ &\text{If } p = 1 \pmod 4 \text{ then } & N_p &= p+1-2a \text{ where } p = a^2+b^2 \\ &&& \qquad\text{and } a+bi = 1 \pmod{2+2i} \\ &&&= p+1-\alpha_p-\beta_p \end{aligned}$$

Weil proved the Riemann Hypothesis for non-singular curves.

André Weil (1906-1998)

Weil proved the Riemann Hypothesis for non-singular curves.

"My mathematics work is proceeding beyond my wildest hopes, and I am even a bit worried - if it is only in prison that I work so well, will I have to arrange to spend two or three months locked up a year?"

"I am very pleased with it, especially because of where it was written (it must be the first in the history of mathematics) and because it is a fine way of letting all my friends around the world know that I exist. And I am thrilled by the beauty of my theorems."

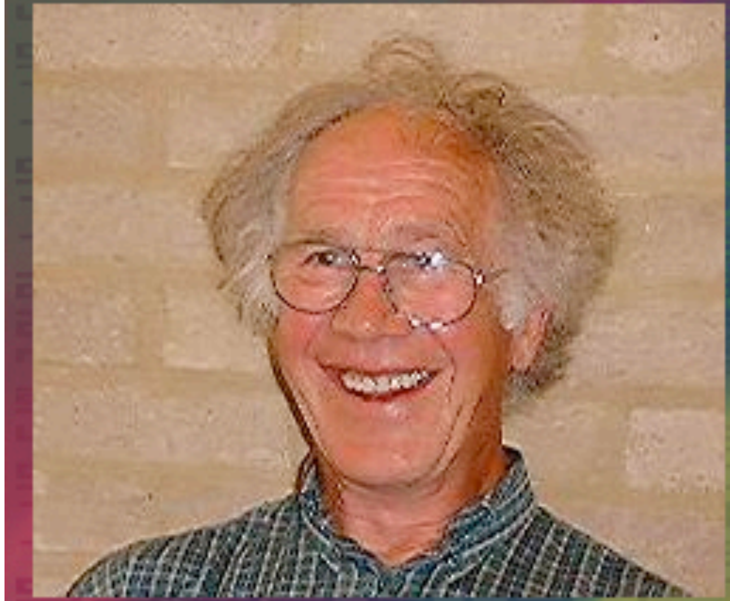
André Weil (1906-1998)

Hasse proposed that the zeta functions of an elliptic curve at each prime p should be regarded as part of a global zeta function

$$\zeta(E,s) \approx \prod_p \zeta(E_p, s)$$

Hasse conjectured that $\zeta(E,s)$ has analytic continuation to the whole complex plane. Now proved thanks to the Taniyama-Weil-Shimura Theorem.

Helmut Hasse (1898-1979)



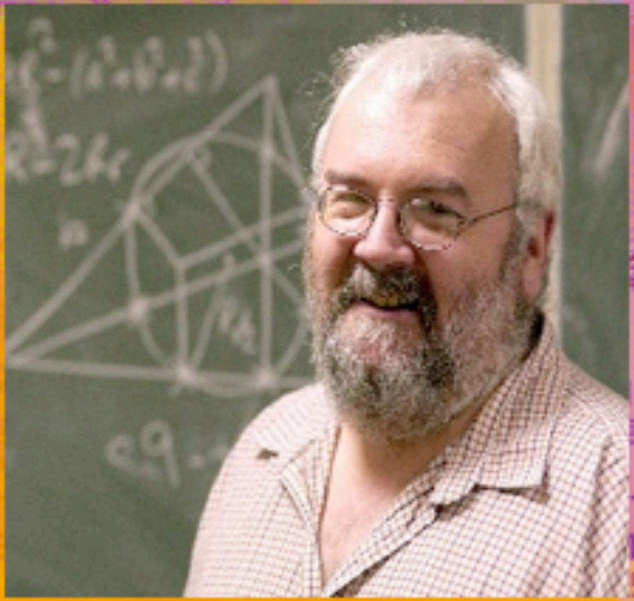
If $\zeta(E,s)$ has a zero of order r at $s=1$ then

$$E(\mathbb{Q}) \cong \mathbb{Z}^r \oplus T \qquad T \text{ finite.}$$

Birch Swinnerton-Dyer Conjecture

Fritz Grunewald

Dan Segal



Geoff Smith

In 1988 the concept of a zeta function of a group was introduced.

F.J. Grunewald, D. Segal and G.C. Smith, *Subgroups of finite index in nilpotent groups*, Invent. Math. **93** (1988), 185-223.

Let G be a finitely generated group.

Define

$$\begin{aligned} a_n(G) &= |\{H \leq G : |G:H| = n\}| \\ a_n^{\triangleleft}(G) &= |\{H \triangleleft G : |G:H| = n\}|. \end{aligned}$$

Define the zeta function and normal zeta function of G to be

$$\begin{aligned} \zeta_G(s) &= \sum a_n(G) n^{-s} = \sum_{H \leq G} |G:H|^{-s} \\ \zeta_G^{\triangleleft}(s) &= \sum a_n^{\triangleleft}(G) n^{-s} = \sum_{H \triangleleft G} |G:H|^{-s}. \end{aligned}$$

These Dirichlet series look like non-commutative generalizations of Dedekind's zeta function of a number field.

Examples

(1) $G = \mathbb{Z}$ then $\zeta_G(s) = \zeta(s) = \sum_{n=1}^{\infty} n^{-s}$ Riemann zeta function

(2) $G = \mathbb{Z}^d$ then $\zeta_G = \zeta(s) \cdots \zeta(s-d+1)$

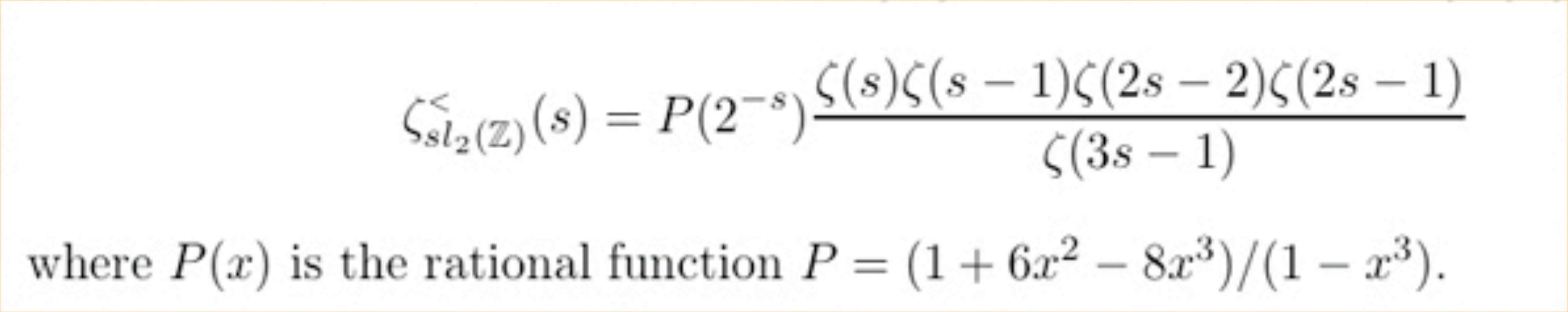
(3) $G = H_2 = \begin{pmatrix} 1 & \mathbb{Z} & \mathbb{Z} \\ 0 & 1 & \mathbb{Z} \\ 0 & 0 & 1 \end{pmatrix}$ Heisenberg group

$$\zeta_G(s) = \frac{\zeta(s)\zeta(s-1)\zeta(2s-2)\zeta(2s-3)}{\zeta(3s-3)}$$

Let L be a ring additively isomorphic to $\mathbb{Z}^d$. The zeta function of L is defined to be

$$\zeta_L(s) = \sum_{H \leq L} |L : H|^{-s}$$

where the sum is taken over all subalgebras H of finite index in L.



$$\zeta^{<}_{sl_2(\mathbb{Z})}(s) = P(2^{-s}) \frac{\zeta(s)\zeta(s-1)\zeta(2s-2)\zeta(2s-1)}{\zeta(3s-1)}$$

where $P(x)$ is the rational function $P = (1 + 6x^2 - 8x^3)/(1 - x^3)$.

Theorem (Grunewald, Segal, Smith 1988) If G is a nilpotent group then the zeta function of G has an Euler product:

$$\zeta_G(s) = \prod_{p \text{ prime}} \zeta_{G,p}(s)$$

where

$$\zeta_{G,p}(s) = \sum_{n=0}^{\infty} a_{p^n}(G)p^{-ns}$$

The local factors $\zeta_{G,p}(s)$ are all rational functions in p^{-s}

How do the zeta functions vary as you vary p?

Example *Let K be a quadratic extension of $\mathbb{Q}$.*

$$H(\vartheta_K) = \begin{pmatrix} 1 & \vartheta_K & \vartheta_K \\ 0 & 1 & \vartheta_K \\ 0 & 0 & 1 \end{pmatrix}.$$

(i) if p is inert then

$$\zeta^{\triangleleft}_{G,p}(s) = \frac{(1+p^{4-5s})}{\left(\prod_{i=0}^{3}(1-p^{i-s})\right)(1-p^{5-5s})(1-p^{8-6s})}$$

(ii) if p is ramified then

$$\zeta^{\triangleleft}_{G,p}(s) = \frac{1}{\left(\prod_{i=0}^{3}(1-p^{i-s})\right)(1-p^{5-5s})(1-p^{4-3s})}$$

(iii) if p is split then

$$\zeta^{\triangleleft}_{G,p}(s) = \frac{(1+p^{4-5s})}{\left(\prod_{i=0}^{3}(1-p^{i-s})\right)(1-p^{5-5s})(1-p^{4-3s})^{2}}.$$

Question *Let G be a finitely generated nilpotent group. Do there exist finitely many rational functions $W_1(X,Y),\dots,W_r(X,Y) \in \mathbb{Q}(X,Y)$ such that for each prime p there is an i for which*

$$\zeta^{\triangleleft}_{G,p}(s) = W_i(p,p^{-s})?$$

The answer is “yes” for

(1) class 2 free nilpotent groups

(2) Heisenberg group over an arbitrary number field.

If the answer is “yes” we say that G is finitely uniform.

Theorem (du S and Grunewald) *For each finitely generated nilpotent group G there exists an explicit system of subvarieties E_i ($i \in T$, T finite) of a variety Y defined over $\mathbb{Z}$ and, for each subset I of T, a rational function $W_I(X,Y) \in \mathbb{Q}(X,Y)$ such that for almost all primes p*

$$\zeta^{\triangleleft}_{G,p}(s) = \sum_{I\subset T} c_I(p) W_I(p,p^{-s})$$

where

$$c_I(p) = \text{card}\{a \in Y(\mathbb{F}_p) : a \in E_i(\mathbb{F}_p)$$

$$\text{if and only if } i \in I\}.$$

What varieties can we realise in the zeta function of a nilpotent group

Theorem (du S) *Let G be the Hirsch length 9, class two nilpotent group given by the following presentation:*

$$G = \left\langle a_1, a_2, a_3, b_1, b_2, b_3, X, Y, Z : \begin{array}{lll} [a_1,b_1] = Y & [a_1,b_2] = Z & [a_1,b_3] = X \\ [a_2,b_1] = X & [a_2,b_2] = Y & \\ & [a_3,b_2] = X & [a_3,b_3] = Z \end{array} \right\rangle$$

Let E be the elliptic curve $Y^2 = X^3 - X$. Then there exist two rational function $P_1(X,Y)$ and $P_2(X,Y) \in \mathbb{Q}(X,Y)$ such that for almost all primes p :

$$\zeta^{\triangleleft}_{G,p}(s) = P_1(p, p^{-s}) + |E(\mathbb{F}_p)| P_2(p, p^{-s}).$$

Where is the elliptic curve?

$$G = \left\langle a_1, a_2, a_3, b_1, b_2, b_3, X, Y, Z : \begin{array}{lll} [a_1, b_1] = Y & [a_1, b_2] = Z & [a_1, b_3] = X \\ [a_2, b_1] = X & [a_2, b_2] = Y & \\ & [a_3, b_2] = X & [a_3, b_3] = Z \end{array} \right\rangle$$

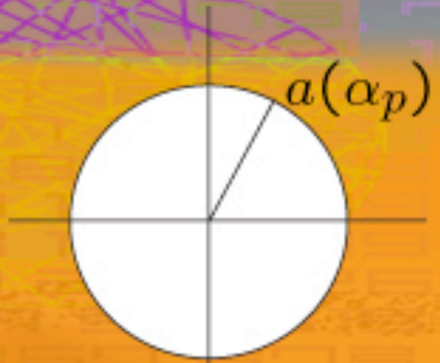
Where is the elliptic curve?

$$\det\begin{pmatrix} [a_1,b_1]=Y & [a_1,b_2]=Z & [a_1,b_3]=X \\ [a_2,b_1]=X & [a_2,b_2]=Y & 0 \\ 0 & [a_3,b_2]=X & [a_3,b_3]=Z \end{pmatrix}$$

$$= \quad Y^2Z + X^3 - XZ^2$$

$$|E(\mathbb{F}_p)| = N_p = p + 1 - \alpha_p - \beta_p$$

$$a(\alpha_p) = \frac{\alpha_p}{|\alpha_p|} \in S^1 \subset \mathbb{C}$$



Hecke: *If the elliptic curve E has complex multiplication then*

$$\{a(\alpha_p) : p \text{ prime}\}$$

is dense in S^1.

Sato-Tate conjectures imply that this is also true for elliptic curves without CM.

Theorem (du S) *There do NOT exist finitely many polynomials $f_1(X), \ldots, f_r(X)$ such that for each prime p there is a $j \in \{1, \ldots, r\}$ such that*

$$|E(\mathbb{F}_p)| = f_j(p).$$

Corollary (du S) *The nilpotent group*

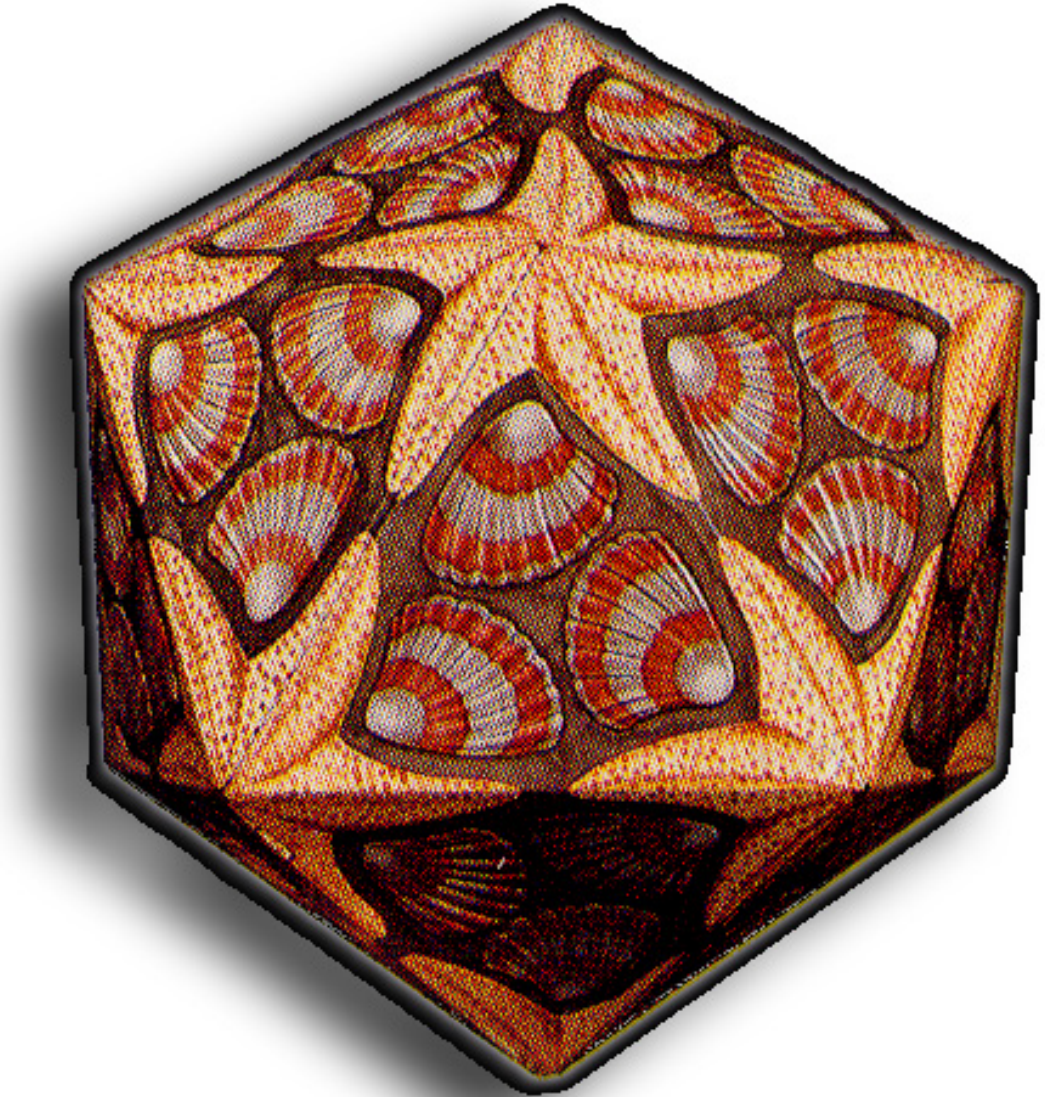
$$G = \langle a_1, a_2, a_3, b_1, b_2, b_3, X, Y, Z : \quad \begin{array}{lll} [a_1, b_1] = Y & [a_1, b_2] = Z & [a_1, b_3] = X \\ [a_2, b_1] = X & [a_2, b_2] = Y & \\ & [a_3, b_2] = X & [a_3, b_3] = Z \end{array} \rangle$$

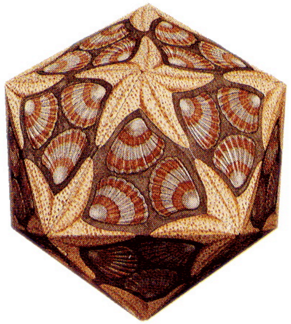
is NOT finitely uniform.

Animals are divided into:

A belonging to the Emperor
B embalmed
C tame
D sucking pigs
E sirens
F fabulous
G stray dogs
H included in the present classification
I frenzied
J innumerable
K drawn with a camel hair brush
L et cetera
M having just broken the water pitcher
N that from a long way off look like flies.

Borges quoting from
"a certain Chinese encyclopaedia".





Chocolate box designed by **Escher**

Its symmetries are one of the first building blocks in the periodic table of symmetry

Simple group of order 7

Animals are divided into:

A belonging to the Emperor

B embalmed

C tame

D sucking pigs

E sirens

F fabulous

G stray dogs

H included in the present classification

I frenzied

J innumerable

K drawn with a camel hair brush

L et cetera

M having just broken the water pitcher

N that from a long way off look like flies.

Borges quoting from
"a certain Chinese encyclopaedia".

Let $f(n,p)$= the number of p-groups of order p^n

	$p=2$	$p=3$	$p\geq 5$
p	1	1	1
p^2	2	2	2
p^3	5	5	5
p^4	14	15	15
p^5	51	67	$2p+61+2\gcd(p-1,3)+\gcd(p-1,4)$
p^6	267	504	$3p^2+39p+344+24\gcd(p-1,3)+11\gcd(p-1,4)+2\gcd(p-1,5)$

Higman's PORC Conjecture: *For fixed n there is an integer N and polynomials $P_{n,i}(X)$ for $0 \leq i \leq N-1$ so that if $p \equiv i \mod N$ then*

$$f(n,p) = P_{n,i}(p).$$

PORC = Polynomial On Residue Classes

Connecting finite p-groups and infinite nilpotent groups.

Definition Let

$f(n,p,c,d)$ = p-groups of order p^n of class c on d generators

Define

$$\zeta_{c,d,p}(s) = \sum_{n=0}^{\infty} f(n,p,c,d)p^{-ns}$$

Example

$$\zeta_{1,d,p}(s) \;=\; \zeta_p(s)...\zeta_p(ds) = \frac{1}{(1-p^{-s})...(1-p^{-ds})}$$

p-groups of order p^n of class c on d generators =

finite p-power quotients of the free nilpotent group of class c on d generators upto isomorphism.

Theorem *For a fixed prime p and integers c and d, the function $\zeta_{c,d,p}(s)$ is a rational function in p^{-s}.*

Corollary *For a fixed prime p and integers c and d the function $f(n) = f(n,p,c,d)$ satisfies a linear recurrence relation with constant coefficients.*

Let $f(n,p)$= the number of p-groups of order p^n

Higman's PORC Conjecture: *For fixed n there is an integer N and polynomials $P_{n,i}(X)$ for $0 \leq i \leq N-1$ so that if $p \equiv i \mod N$ then*

$$f(n,p) = P_{n,i}(p).$$

Theorem (du S) *For each n there exist finitely many subvarieties $E_{i,n}$ $(i \in T(n))$ of a variety Y_n defined over $\mathbb{Q}$ and for each $I \subset T(n)$ a polynomial $H_{n,I}(X) \in \mathbb{Q}[X]$ such that for almost all primes p*

$$f(n,p) = \sum_{I \subset T(n)} e_{n,p,I} H_{n,I}(p)$$

where

$$e_{n,p,I} = \text{card}\{a \in \overline{Y_n}(\mathbb{F}_p) : a \in \overline{E_{i,n}}(\mathbb{F}_p) \text{ if and only if } i \in I\}$$