Experimental Mathematics: and Exact Computation

Jonathan M. Borwein

CECM

Centre for Experimental & Constructive Mathematics

Simon Fraser University, Burnaby, BC Canada

Revised September 2000

URL: www.cecm.sfu.ca/~jborwein/talks.html

ABSTRACT. Computation in Mathematics is fast becoming ubiquitous. My intention is to discuss "pure and applied experimental computation" from a mathematician's perspective. I shall try to illustrate what is currently easy and what is currently hard, what is possible and what we aspire to be be able to do. I shall discuss a few of the underlying philosophical issues and shall also summarize some of the very demanding *exact* (hybrid symbolic/ numeric) computations I have undertaken in the last few years with David Bailey, David Bradley, David Broadhurst, Petr Lisoněk, Peter Borwein and others.

⋄ *Maple Examples* are downloadable at

`www.cecm.sfu.ca/ jborwein/talks`

as Worksheets and may be tried in a *Java Maple Interface* at `www.cecm.sfu.ca/projects/JMI` (password protected) or at

`www.cecm.sfu.ca/projects/IntegerRelations`

And I will be rash enough – at any rate verbally – to give my own perspective on what needs to happen for experimental mathematics and symbolic computation to blossom in the 21st century: that is effectively using the pervasive (parallel) high performance systems of the next decade.

In that context, I may also discuss the recently funded *Canadian Computational Collaboratory* known as *C3.ca*. This an ambitious national Canadian high performance computing network dedicated to providing broad access to heterogeneous parallel computing resources from coast to coast (see `http://www.c3.ca`).

GAUSS and HADAMARD

Gauss once confessed,

"I have the result, but I do not yet know how to get it."

⋄ Issac Asimov and J. A. Shulman, ed., *Isaac Asimov's Book of Science and Nature Quotations*, Weidenfield and Nicolson, New York, 1988, pg. 115.

...

"The object of mathematical rigor is to sanction and legitimize the conquests of intuition, and there was never any other object for it."

⋄ J. Hadamard quoted at length in E. Borel, *Lecons sur la theorie des fonctions*, 1928.

MOTIVATION and GOAL

INSIGHT – demands speed ≡ parallelism

- For rapid verification.
- For validation; proofs *and* refutations.
- For "monster barring".

† What is "easy" changes while HPC and HPN blur; merging disciplines and collaborators.

- Parallelism ≡ more space, speed & stuff.
- Exact ≡ hybrid ≡ symbolic '+' numeric (MapleVI meets NAG).
- For analysis, algebra, geometry & topology.

COMMENTS

- Towards an Experimental Mathodology – philosophy and practice.
- Intuition is acquired – mesh computation and mathematics.
- Visualization – three is a lot of dimensions.
- "Caging" and "Monster-barring" (Lakatos).
  - graphic checks: compare $2\sqrt{y}-y$ and $\sqrt{y}\ln(y)$, $0<y<1$
  - randomized checks: equations, linear algebra, primality

PART of OUR 'METHODOLOGY'

1. (*High Precision*) computation of object(s).
2. *Pattern Recognition* of *Real Numbers* (Inverse Calculator and 'RevEng')*, or *Sequences* (Salvy & Zimmermann's 'gfun', Sloane and Plouffe's Encyclopedia).
3. Extensive use of 'Integer Relation Methods': *PSLQ* & *LLL* and FFT.†
   - Exclusion bounds are especially useful.
   - Great test bed for "Experimental Math".
4. Some automated theorem proving (Wilf-Zeilberger etc).

*ISC space limits: from 10Mb in 1985 to 10Gb today.

†Top Ten "Algorithm's for the Ages," Random Samples, Science, Feb. 4, 2000.

FOUR EXPERIMENTS

• 1. **Kantian** example: generating "the classical non-Euclidean geometries (hyperbolic, elliptic) by replacing Euclid's axiom of parallels (or something equivalent to it) with alternative forms."

• 2. The **Baconian** experiment is a contrived as opposed to a natural happening, it "is the consequence of 'trying things out' or even of merely messing about."

• 3. **Aristotelian** demonstrations: "apply electrodes to a frog's sciatic nerve, and lo, the leg kicks; always precede the presentation of the dog's dinner with the ringing of a bell, and lo, the bell alone will soon make the dog dribble."

• 4. The most important is **Galilean**: "a critical experiment – one that discriminates between possibilities and, in doing so, either gives us confidence in the view we are taking or makes us think it in need of correction."

◇ It is also the only one of the four forms which will make Experimental Mathematics a serious enterprise.

• From Peter Medawar's *Advice to a Young Scientist*, Harper (1979).

MILNOR

"If I can give an abstract proof of something, I'm reasonably happy. But if I can get a concrete, computational proof and actually produce numbers I'm much happier. I'm rather an addict of doing things on the computer, because that gives you an explicit criterion of what's going on. I have a visual way of thinking, and I'm happy if I can see a picture of what I'm working with."

...

• Consider the following images of zeroes of 0/1 polynomials
`www.cecm.sfu.ca/MRG/INTERFACES.html`

◇ But symbols are often more reliable than pictures.

On to the examples ...

I: GENERAL EXAMPLES

1. TWO INTEGRALS

• A. $\pi \neq \frac{22}{7}$.

$$\int_0^1 \frac{(1-x)^4 x^4}{1+x^2}\, dx = \frac{22}{7} - \pi.$$

...

• *B. The sophomore's dream.*

$$\int_0^1 \frac{1}{x^x}\, dx = \sum_{n=1}^{\infty} \frac{1}{n^n}.$$

2. TWO INFINITE PRODUCTS

• *A. a rational evaluation*:

$$\prod_{n=2}^{\infty} \frac{n^3-1}{n^3+1} = \frac{2}{3}$$

...

• *B. and a transcendent one*:

$$\prod_{n=2}^{\infty} \frac{n^2-1}{n^2+1} = \frac{\pi}{\sinh(\pi)}$$

3. HIGH PRECISION FRAUD

and CONTINUED FRACTIONS

$$\sum_{n=1}^{\infty} \frac{[n \tanh(\pi)]}{10^n} \stackrel{?}{=} \frac{1}{81}$$

is valid to 268 places; while

$$\sum_{n=1}^{\infty} \frac{[n \tanh(\frac{\pi}{2})]}{10^n} \stackrel{?}{=} \frac{1}{81}$$

is valid to just 12 places.

• Both are actually transcendental numbers.

⋄ Correspondingly the *simple continued fractions* for $\tanh(\pi)$ and $\tanh(\frac{\pi}{2})$ are respectively

$$[0, 1, \mathbf{267}, 4, 14, 1, 2, 1, 2, 2, 1, 2, 3, 8, 3, 1]$$

and

$$[0, 1, \mathbf{11}, 14, 4, 1, 1, 1, 3, 1, 295, 4, 4, 1, 5, 17, 7]$$

4. PARTIAL FRACTIONS & CONVEXITY

• We consider a network *objective function* p_N given by

$$p_N(\vec{q}) = \sum_{\sigma \in S_N} (\prod_{i=1}^{N} \frac{q_{\sigma(i)}}{\sum_{j=i}^{N} q_{\sigma(j)}})(\sum_{i=1}^{N} \frac{1}{\sum_{j=i}^{N} q_{\sigma(j)}})$$

summed over *all* $N!$ permutations; so a typical term is

$$(\prod_{i=1}^{N} \frac{q_i}{\sum_{j=i}^{N} q_j})(\sum_{i=1}^{N} \frac{1}{\sum_{j=i}^{n} q_j}) .$$

⋄ For $N = 3$ this is

$$q_1 q_2 q_3 (\frac{1}{q_1 + q_2 + q_3})(\frac{1}{q_2 + q_3})(\frac{1}{q_3})$$

$$\times(\frac{1}{q_1 + q_2 + q_3} + \frac{1}{q_2 + q_3} + \frac{1}{q_3}) .$$

• We wish to show p_N is *convex* on the positive orthant. First we try to simplify the expression for p_N.

• The *partial fraction decomposition* gives:

$$\begin{aligned}
p_1(x) &= \frac{1}{x}, \\
p_2(x_1, x_2) &= \frac{1}{x_1} + \frac{1}{x_2} - \frac{1}{x_1 + x_2}, \\
p_3(x_1, x_2, x_3) &= \frac{1}{x_1} + \frac{1}{x_2} + \frac{1}{x_3} \\
&- \frac{1}{x_1 + x_2} - \frac{1}{x_2 + x_3} - \frac{1}{x_1 + x_3} \\
&+ \frac{1}{x_1 + x_2 + x_3}.
\end{aligned}$$

So we predict the 'same' for $N = 4$ and **CONJECTURE.** For each $N \in \mathbb{N}$

$$p_N(x_1, \ldots, x_N) := \int_0^1 \left(1 - \prod_{i=1}^{N} (1 - t^{x_i})\right) \frac{dt}{t}$$

is convex, indeed 1/concave.

• Check $N < 5$ via large symbolic Hessian.

PROOF. A year later, *joint expectations* gave:

$$p_N(\vec{x}) = \int_{\mathbb{R}_+^n} e^{-(y_1 + \cdots + y_n)} \max\left(\frac{y_1}{x_1}, \ldots, \frac{y_n}{x_n}\right) dy$$

[See *SIAM Electronic Problems and Solutions.*]

5. CONVEX CONJUGATES and NMR

The *Hoch and Stern information measure*, or *neg-entropy*, is defined in complex $n-$space by

$$H(z) = \sum_{j=1}^{n} h(z_j/b),$$

where h is convex and given (for scaling b) by:

$$\boxed{h(z) \triangleq |z| \ln\left(|z| + \sqrt{1 + |z|^2}\right) - \sqrt{1 + |z|^2}}$$

for quantum theoretic (NMR) reasons.

• Recall the *Fenchel-Legendre conjugate*

$$f^*(y) := \sup_x \langle y, x \rangle - f(x).$$

• Our *symbolic convex analysis* package (stored at `www.cecm.sfu.ca/projects/CCA/`) produced:

$$h^*(z) = \cosh(|z|)$$

⋄ Compare the *Shannon entropy*:

$$(z \ln z - z)^* = \exp(z).$$

◇ I'd never have tried by hand!

• Efficient *dual algorithms* now may be constructed.

◇ Knowing 'closed forms' helps:

$$(\exp\exp)^*(y) = y\ln(y) - y\{W(y) + W(y)^{-1}\}$$

where Maple or Mathematica knows the complex *Lambert* W function

$$W(x)e^{W(x)} = x.$$

Thus, the conjugate's series is

$$-1+(\ln(y)-1)\,y-\frac{1}{2}y^2+\frac{1}{3}y^3-\frac{3}{8}y^4+\frac{8}{15}y^5+O\left(y^6\right).$$

Coworkers: Marechal, Naugler, $\cdots$, Bauschke, Fee, Lucet

6. SOME FOURIER INTEGRALS

Recall the *sinc* function

$$\mathrm{sinc}(x) := \frac{\sin(x)}{x}.$$

Consider, the seven highly oscillatory integrals below.*

$$I_1 := \int_0^\infty \mathrm{sinc}(x)\,dx = \frac{\pi}{2},$$

$$I_2 := \int_0^\infty \mathrm{sinc}(x)\mathrm{sinc}\left(\frac{x}{3}\right)\,dx = \frac{\pi}{2},$$

$$I_3 := \int_0^\infty \mathrm{sinc}(x)\mathrm{sinc}\left(\frac{x}{3}\right)\mathrm{sinc}\left(\frac{x}{5}\right)\,dx = \frac{\pi}{2},$$

$$\cdots$$

$$I_6 := \int_0^\infty \mathrm{sinc}(x)\mathrm{sinc}\left(\frac{x}{3}\right)\cdots\mathrm{sinc}\left(\frac{x}{11}\right)\,dx = \frac{\pi}{2},$$

$$I_7 := \int_0^\infty \mathrm{sinc}(x)\mathrm{sinc}\left(\frac{x}{3}\right)\cdots\mathrm{sinc}\left(\frac{x}{13}\right)\,dx = \frac{\pi}{2}.$$

*These are hard to compute accurately numerically.

However,

$$I_8 := \int_0^\infty \mathrm{sinc}(x)\mathrm{sinc}\left(\frac{x}{3}\right)\cdots\mathrm{sinc}\left(\frac{x}{15}\right)\,dx$$

$$= \frac{467807924713440738696537864469}{935615849440640907310521750000}\pi$$

$$\approx 0.499999999992646\pi.$$

• When a researcher, using a well-known computer algebra package, checked this he – and the makers – concluded there was a "bug" in the software. Not so!

◇ Our analysis, via Parseval's theorem, links the integral

$$I_n := \int_0^\infty \mathrm{sinc}(a_1x)\mathrm{sinc}(a_2x)\cdots\mathrm{sinc}(a_nx)\,dx$$

with the volume of the polyhedron P_N given by

$$\{(x_2,x_3,\cdots,x_N) : \sum_{k=2}^N a_kx_k \le a_1, |x_k| \le 1, 2 \le k \le N\}.$$

If we let

$$C_N := \{(x_2,x_3,\cdots,x_N) : -1 \le x_k \le 1, 2 \le k \le N\},$$

then

$$\boxed{I_N = \frac{\pi}{2a_1}\frac{Vol(P_N)}{Vol(C_N)}.}$$

• Thus, the value drops precisely when the constraint $\sum_{k=2}^N a_kx_k \le a_1$ becomes *active* and bites into the hypercube C_N. That occurs when

$$\sum_{k=2}^N a_k > a_1.$$

In the above example, $\frac{1}{3}+\frac{1}{5}+\cdots+\frac{1}{13} < 1$, but on the addition of the term $\frac{1}{15}$, the sum exceeds 1, the volume drops, and the identity $I_N = \frac{\pi}{2}$ no longer holds.

• A somewhat cautionary example for too enthusiastically inferring patterns from seemingly compelling symbolic or numerical computation.

Coworkers: D. Borwein, Mares

7. MINIMAL POLYNOMIALS

of COMBINATORIAL MATRICES

Consider matrices A, B, C, M:

$$A_{kj} := (-1)^{k+1}\binom{2n-j}{2n-k},$$

$$B_{kj} := (-1)^{k+1}\binom{2n-j}{k-1},$$

$$C_{kj} := (-1)^{k+1}\binom{j-1}{k-1}$$

$(k, j = 1, \ldots, n)$ and

$$\boxed{M := A + B - C.}$$

• In earlier work on *Euler Sums* we needed to prove M invertible: actually

$$\boxed{M^{-1} = \frac{M+I}{2}.}$$

• The key is discovering

$$\begin{aligned} A^2 &= C^2 = I \\ B^2 &= CA, AC = B. \end{aligned} \tag{1}$$

• It follows that $B^3 = BCA = AA = I$, and that the <u>*group generated by* A,B and C is S_3</u>.

⋄ Once discovered, the combinatorial proof of this is routine – either for a human or a computer ('$A = B$', Wilf-Zeilberger).

• One now easily shows using (**??**)

$$\boxed{M^2 + M = 2I}$$

as formal algebra since $M = A + B - C$.

• The truth is I started with instances of

$$'minpoly(M, x)'$$

and then emboldened I typed

$$'minpoly(B, x)'$$

in Maple . . . !

• Random matrices have full degree *minimal polynomials*.

† *Jordan Forms* uncover Spectral Abscissas.

8. PARTITIONS and PATTERNS

• The number of *additive partitions* of n, $p(n)$, is generated by

$$\prod_{n\geq 1}(1-q^n)^{-1}.$$

⋄ Thus $p(5) = 7$ since

$$5 = 4+1 = 3+2 = 3+1+1 = 2+2+1$$

$$= 2+1+1+1 = 1+1+1+1+1.$$

QUESTION. How hard is $p(n)$ to compute – in 1900 (for MacMahon), and 2000 (for Maple)?

. . .

• *Euler's pentagonal number theorem* is

$$\boxed{\prod_{n\geq 1}(1-q^n) = \sum_{n=-\infty}^{\infty}(-1)^n q^{(3n+1)n/2}.}$$

⋄ We can recognize the *triangular numbers* in *Sloane's* on-line 'Encyclopedia of Integer Sequences'. And much more.

9. ESTABLISHING INEQUALITIES

and the MAXIMUM PRINCIPLE

• Consider the two *means*

$$\mathcal{L}^{-1}(x, y) := \frac{x-y}{\ln(x) - \ln(y)}$$

and

$$\mathcal{M}(x, y) := \sqrt[3]{\frac{x^{\frac{2}{3}} + y^{\frac{2}{3}}}{2}}$$

• An *elliptic integral* estimate reduced to the elementary inequalities

$$\boxed{\mathcal{L}(\mathcal{M}(x,1), \sqrt{x}) < \mathcal{L}(x,1) < \mathcal{L}(\mathcal{M}(x,1),1)}$$

for $0 < x < 1$.

⋄ We first discuss a method of showing

$$\mathcal{E}(x) := \mathcal{L}(x,1) - \mathcal{L}(\mathcal{M}(x,1), \sqrt{x}) > 0$$

on $0 < x < 1$.

A. Numeric/symbolic methods

- $\lim_{x\to 0^+} \mathcal{E}(x) = \infty$.

- *Newton-like iteration* shows that $\mathcal{E}(x) > 0$ on $[0.0, 0.9]$.

- *Taylor series* shows $\mathcal{E}(x)$ has 4 zeroes at 1.

- *Maximum Principle* shows there are no more zeroes inside $C := \{z : |z-1| = \frac{1}{4}\}$:

$$\frac{1}{2\pi i}\int_C \frac{\mathcal{E}'}{\mathcal{E}} = \#(\mathcal{E}^{-1}(0); C)$$

- When we make each step *effective*.

B. Graphic/symbolic methods

Consider the 'opposite' (cruder) inequality

$$\mathcal{F}(x) := \mathcal{L}(\mathcal{M}(x,1),1) - \mathcal{L}(x,1) > 0$$

- Then we may observe that it holds since
  - $\mathcal{M}$ is a mean; and
  - $\mathcal{L}$ is decreasing.

BERLINSKI

"The computer has in turn changed the very nature of mathematical experience, suggesting for the first time that mathematics, like physics, may yet become an empirical discipline, a place where things are discovered because they are seen."

...

"The body of mathematics to which the calculus gives rise embodies a certain swashbuckling style of thinking, at once bold and dramatic, given over to large intellectual gestures and indifferent, in large measure, to any very detailed description of the world. It is a style that has shaped the physical but not the biological sciences, and its success in Newtonian mechanics, general relativity and quantum mechanics is among the miracles of mankind. *But the era in thought that the calculus made possible is coming to an end.* Everyone feels this is so and everyone is right."

II. π and FRIENDS

A: (*A quartic algorithm.*) Set $a_0 = 6 - 4\sqrt{2}$ and $y_0 = \sqrt{2} - 1$. Iterate

$$y_{k+1} = \frac{1 - (1 - y_k^4)^{1/4}}{1 + (1 - y_k^4)^{1/4}}$$

$$\begin{aligned} a_{k+1} &= a_k(1 + y_{k+1})^4 \\ &- 2^{2k+3} y_{k+1}(1 + y_{k+1} + y_{k+1}^2) \end{aligned}$$

Then a_k converges *quartically* to $1/\pi$.

• Used since 1986, with Salamin-Brent scheme, by Bailey, Kanada (Tokyo).

• In 1997, Kanada computed over 51 billion digits on a Hitachi supercomputer (18 iterations, 25 hrs on 2^{10} cpu's). His present world record is 2^{36} digits in April 1999.

◇ A billion (2^{30}) digit computation has been performed on a single Pentium II PC in under 9 days.

◇ 50 billionth decimal digit of π *or* $\frac{1}{\pi}$ is 04$\underline{2}$! And after 18 billion digits 0123456789 has finally appeared (Brouwer's famous intuitionist example *now* converges!).

Details at: www.cecm.sfu.ca/personal/jborwein/pi_cover.html.

B: (A *nonic (ninth-order) algorithm.*) In 1995 Garvan and I found genuine η-based m-th order approximations to π.

◇ Set

$$a_0 = 1/3,\ r_0 = (\sqrt{3}-1)/2,\ s_0 = \sqrt[3]{1-r_0^3}$$

and iterate

$$\begin{aligned} t &= 1+2r_k \\ u &= [9r_k(1+r_k+r_k^2)]^{1/3} \\ v &= t^2+tu+u^2 \\ m &= \frac{27(1+s_k+s_k^2)}{v} \\ a_{k+1} &= ma_k + 3^{2k-1}(1-m) \\ s_{k+1} &= \frac{(1-r_k)^3}{(t+2u)v} \\ r_{k+1} &= (1-s_k^3)^{1/3} \end{aligned}$$

Then $1/a_k$ converges *nonically* to π.

• Their discovery and proof both used enormous amounts of computer algebra (e.g., hunting for '$\sum \Rightarrow \prod$' and 'the modular machine')

† Higher order schemes are slower than quartic.

• Kanada's estimate of time to run the same FFT/Karatsuba-based π algorithm on a serial machine: *"infinite"*.

Coworkers: Bailey, P. Borwein, Garvan, Kanada, Lisoněk

C: (*'Pentium farming' for binary digits.*) Bailey, P. Borwein and Plouffe (1996) discovered a series for π (and some other *polylogarithmic constants*) which allows one to compute hex–digits of π *without* computing prior digits.

• The algorithm needs very little memory and does not need multiple precision. The running time grows only slightly faster than linearly in the order of the digit being computed.

• The key, found by 'PSLQ' (below) is:

$$\pi = \sum_{k=0}^{\infty} \left(\frac{1}{16}\right)^k \left(\frac{4}{8k+1} - \frac{2}{8k+4} - \frac{1}{8k+5} - \frac{1}{8k+6}\right)$$

• Knowing an algorithm would follow they spent several months hunting for such a formula.

◇ Once found, easy to prove in Mathematica, Maple or by hand.

⋄ A most successful case of

REVERSE MATHEMATICAL ENGINEERING

• (Sept 97) Fabrice Bellard (INRIA) used a variant formula to compute 152 binary digits of π, starting at the *trillionth position* (10^{12}). This took 12 days on 20 work-stations working in parallel over the Internet.

• (August 98) Colin Percival (SFU, age 17) finished a similar "embarassingly parallel" computation of *five trillionth bit* (using 25 machines at about 10 times the speed). In *Hex*:

$$\underline{0}7E45733CC790B5B5979$$

The binary digits of π starting at the 40 trillionth place are

$$\underline{0}0000111110011111.$$

• (September 00) The quadrillionth bit is '0' (using 250 cpu years on 1734 machines from 56 countries).

Starting at the $999,999,999,999,997$th bit of π one has:

$$111\mathbf{0}0011000100001011010110000011 0$$

D: (*Other polylogarithms.*) Catalan's constant

$$G := \sum_{k=0}^{\infty} \frac{(-1)^k}{(2k+1)^2}$$

is not proven irrational.

• In a series of inspired computations using *polylogarithmic ladders* Broadhurst has since found – and proved – similar identities for constants such as $\zeta(3)$, $\zeta(5)$ and G. Broadhurst's binary formula is

$$G = 3\sum_{k=0}^{\infty} \frac{1}{2\cdot 16^k}\left\{ \frac{1}{(8k+1)^2} - \frac{1}{(8k+2)^2} + \frac{1}{2(8k+3)^2} - \frac{1}{2^2(8k+5)^2} + \frac{1}{2^2(8k+6)^2} - \frac{1}{2^3(8k+7)^2}\right\}$$
$$+$$

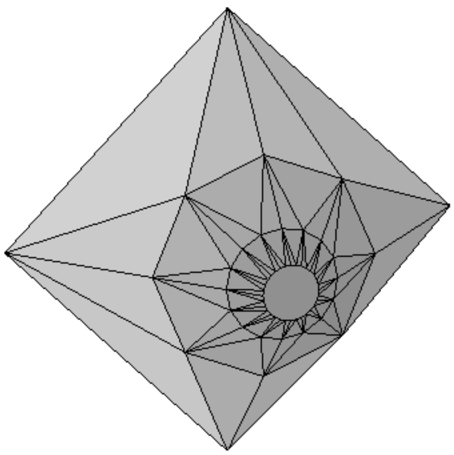
$$-2\sum_{k=0}^{\infty} \frac{1}{8\cdot 16^{3k}}\left\{ \frac{1}{(8k+1)^2} + \frac{1}{2(8k+2)^2} + \frac{1}{2^3(8k+3)^2} - \frac{1}{2^6(8k+5)^2} - \frac{1}{2^7(8k+6)^2} - \frac{1}{2^9(8k+7)^2}\right\}$$

• Why was G missed earlier?

• He also gives some constants with ternary expansions.

Coworkers: BBP, Bellard, Broadhurst, Percival, the Web, $\cdots$

A MISLEADING PICTURE



III. NUMBER THEORY

1. NORMAL FAMILIES

† High–level languages or computational speed?

• A family of primes $\mathcal{P}$ is *normal* if it contains no primes p, q such that p divides $q-1$.

A: *Three Conjectures*:

◇ *Giuga's conjecture* ('51) is that

$$\boxed{\sum_{k=1}^{n-1} k^{n-1} \equiv n-1 \ (\mathrm{mod}\ n)}$$

if and only if n is prime.

• *Agoh's Conjecture* ('95) is equivalent:

$$\boxed{nB_{n-1} \equiv -1 \ (\mathrm{mod}\ n)}$$

if and only if n is prime; here B_n is a *Bernoulli number*.

◇ *Lehmer's conjecture* ('32) is that

$$\boxed{\phi(n) \mid n-1}$$

if and only if n is prime.

> "A problem as hard as existence of odd perfect numbers."

...

• For these conjectures the set of prime factors of any counterexample n is a normal family.

◇ We exploited this property aggressively in our (Pari/Maple) computations

• Lehmer's conjecture had been variously verified for up to 13 prime factors of n. We extended and unified this for 14 or fewer prime factors.

◇ We also examined the related condition

$$\boxed{\phi(n) \mid n+1}$$

known to have 8 solutions with up to 6 prime factors (Lehmer) : $2, F_0, \cdots, F_4$ (the *Fermat primes* and a rogue pair: 4919055 and

6992962672132095.

• We extended this to 7 prime factors – by dint of a heap of factorizations!

• But the next Lehmer cases (15 and 8) were way too large. The *curse of exponentiality*!

B. *Counterexamples* to the Giuga conjecture must be *Carmichael numbers**

$$\boxed{(p-1) \mid (\frac{n}{p}-1)}$$

and **odd** *Giuga numbers*: n square-free and

$$\boxed{\sum_{p|n} \frac{1}{p} - \prod_{p|n} \frac{1}{p} \in Z}$$

when $p \mid n$ and p prime. An **even** example is

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{5}-\frac{1}{30}=1.$$

⋄ RHS must be '1' for $N < 30$. With 8 primes:

$$554079914617070801288578559178$$

$$= 2 \times 3 \times 11 \times 2331 \times 47059$$

$$\times 2259696349 \times 110725121051.$$

† The largest Giuga number we know has 97 digits with 10 primes (one has 35 digits).

*Only recently proven an infinite set!

† Guiga numbers were found by relaxing to a combinatorial problem. We recursively generated *relative primes* forming *Giuga sequences* such as

$$\frac{1}{2}+\frac{1}{3}+\frac{1}{7}+\frac{1}{83}+\frac{1}{5\times 17}-\frac{1}{296310}=1$$

• We tried to 'use up' the only known *branch and bound* algorithm for Giuga's Conjecture: 30 lines of Maple became 2 months in C++ which crashed in Tokyo; but confirmed our local computation that a counterexample n has more than 13,800 digits.

Coworkers: D. Borwein, P. Borwein, Girgensohn, Wong and Wayne State Undergraduates

2. DISJOINT GENERA

Theorem. There are at most 19 integers not of the form of $xy + yz + xz$ with $x, y, z \geq 1$.

The only non-square-free are 4 and 18. The first 16 square-free are

$$1, 2, 6, 10, 22, 30, 42, 58, 70, 78, 102$$

$$130, 190, \mathbf{210}, 330, 462.$$

which correspond to "discriminants with one quadratic form per genus".

• If the 19th exists, it is greater than 10^{11} which the *Generalized Riemann Hypothesis* (GRH) excludes.

• The Matlab road to proof & the hazards of *Sloane's Encyclopedia*.

Coworker: Choi

3. KHINTCHINE'S CONSTANT

† In different contexts different algorithms star.

A: The celebrated *Khintchine constants* K_0, (K_{-1}) – the limiting geometric (harmonic) mean of the elements of *almost all* simple continued fractions – have efficient reworkings as *Riemann zeta* series.

⋄ Standard definitions are cumbersome products.

• The rational ζ series we used was:

$$\ln K_0 \ln 2 = \sum_{n=1}^{\infty} \frac{\zeta(2n)-1}{n}\left(1-\frac{1}{2}+\frac{1}{3}-\ldots+\frac{1}{2n-1}\right).$$

Here

$$\zeta(s) := \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

• When accelerated and used with "recycling" evaluations of $\{\zeta(2s)\}$, this allowed us to compute K_0 to thousands of digits.

• Computation to 7,350 digits suggests that K_0's continued fraction obeys its own prediction.

⋄ A related challenge is to find natural constants that provably behave 'normally' – in analogy to the *Champernowne* number

$$.0123456789101112\cdots$$

which is provably normally distributed base ten.

B. *Computing* $\zeta(N)$

⋄ $\boxed{\zeta(2N) \cong B_{2N}}$ can be effectively computed in parallel by

- *multi-section* methods - these have space advantages even as serial algorithms and work for *poly-exp* functions (Kevin Hare);

- FFT–enhanced symbolic *Newton (recycling) methods* on the series $\frac{\sinh}{\cosh}$.

⋄ $\boxed{\zeta(2N+1).}$ The harmonic constant K_{-1} needs odd ζ-values.

• We chose to use identities of Ramanujan et al ...

A TASTE of RAMANUJAN

• For $M \equiv -1 \pmod 4$

$$\zeta(4N+3) = -2\sum_{k\geq 1}\frac{1}{k^{4N+3}\left(e^{2\pi k}-1\right)}$$

$$+\frac{2}{\pi}\left\{\frac{4N+7}{4}\zeta(4N+4)-\sum_{k=1}^{N}\zeta(4k)\zeta(4N+4-4k)\right\}$$

where the interesting term is the hyperbolic trig series.

• Correspondingly, for $M \equiv 1 \pmod 4$

$$\zeta(4N+1) = -\frac{2}{N}\sum_{k\geq 1}\frac{(\pi k+N)e^{2\pi k}-N}{k^{4N+1}(e^{2\pi k}-1)^2}$$

$$+\frac{1}{2N\pi}\left\{(2N+1)\zeta(4N+2)+\sum_{k=1}^{2N}(-1)^k 2k\zeta(2k)\zeta(4N+2-2k)\right\}.$$

• Only a finite set of $\zeta(2N)$ values is required and the full precision value e^{π} is reused throughout.

⋄ The number e^{π} is the easiest transcendental to fast compute (by elliptic methods). One "differentiates" $e^{-s\pi}$ to obtain π (the AGM).

• For $\zeta(4N+1)$ I've lately decoded "nicer" series from a few PSLQ cases of Plouffe. It is equivalent to:

$$\left\{2-(-4)^{-N}\right\}\sum_{k=1}^{\infty}\frac{\coth(k\pi)}{k^{4N+1}}$$

$$-(-4)^{-2N}\sum_{k=1}^{\infty}\frac{\tanh(k\pi)}{k^{4N+1}}$$

$$= Q_N \times \pi^{4N+1}. \quad (2)$$

⋄ The quantity Q_N in (**??**) is an explicit rational:

$$(3)\ Q_N := \sum_{k=0}^{2N+1} \frac{B_{4N+2-2k}B_{2k}}{(4N+2-2k)!(2k)!} \times \left\{(-1)^{\binom{k}{2}}(-4)^N 2^k + (-4)^k\right\}.$$

• On substituting

$$\tanh(x) = 1 - \frac{2}{\exp(2x)+1}$$

and

$$\coth(x) = 1 + \frac{2}{\exp(2x)-1}$$

one may solve for

$$\zeta(4N+1).$$

• Thus,

$$\zeta(5) = \frac{1}{294}\pi^5 + \frac{2}{35}\sum_{k=1}^{\infty}\frac{1}{(1+e^{2k\pi})k^5} + \frac{72}{35}\sum_{k=1}^{\infty}\frac{1}{(1-e^{2k\pi})k^5}.$$

⋄ Will we ever be able to identify universal formulae like (**??**) automatically? My solution was highly human assisted.

Coworkers: Bailey, Crandall, Hare, Plouffe.

IV: INTEGER RELATION EXAMPLES

1. The USES of LLL and PSLQ

• A vector $(x_1, x_2, \cdots, x_n)$ of reals *possesses an integer relation* if there are integers a_i not all zero with

$$0 = a_1x_1 + a_2x_2 + \cdots + a_nx_n.$$

PROBLEM: Find a_i if such exist. If not, obtain lower bounds on the size of possible a_i.

- ($n = 2$) *Euclid's algorithm* gives solution.
- ($n \geq 3$) Euler, Jacobi, Poincare, Minkowski, Perron, others sought method.
- *First general algorithm* in 1977 by Ferguson & Forcade. Since '77: **LLL** (in Maple), HJLS, PSOS, **PSLQ** ('91, *parallel* '99).

• Integer Relation Detection was recently ranked among "the 10 algorithms with the greatest influence on the development and practice of science and engineering in the 20th century." J. Dongarra, F. Sullivan, *Computing in Science & Engineering* **2** (2000), 22–23.

Also: Monte Carlo, Simplex, Krylov Subspace, QR Decomposition, Quicksort, ..., FFT, Fast Multipole Method.

ALGEBRAIC NUMBERS

Compute α to sufficiently high precision (O(n^2)) and apply LLL to the vector

$$(1, \alpha, \alpha^2, \cdots, \alpha^{n-1}).$$

- Solution integers a_i are coefficients of a polynomial likely satisfied by α.
- If no relation is found, exclusion bounds are obtained.

FINALIZING FORMULAE

⋄ If we know or suspect an identity exists integer relations are very powerful.

- (*Machin's Formula*) We try `lin_dep` on
  $$[\arctan(1), \arctan(1/5), \arctan(1/239)]$$
  and recover `[1, -4, 1]`. That is,
  $$\frac{\pi}{4} = 4\arctan(\frac{1}{5}) - \arctan(\frac{1}{239}).$$
  (Used on all serious computations of π from 1706 (100 digits) to 1973 (1 million).)

- (*Dase's Formula*). We try `lin_dep` on
  $$[\arctan(1), \arctan(1/2), \arctan(1/5), \arctan(1/8)]$$
  and recover `[-1, 1, 1, 1]`. That is,
  $$\frac{\pi}{4} = \arctan(\frac{1}{2}) + \arctan(\frac{1}{5}) + \arctan(\frac{1}{8}).$$
  (Used by Dase to compute 200 digits of π in his head.)

ZETA FUNCTIONS

- The *zeta function* is defined, for $s > 1$, by
$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

- Thanks to *Apéry* (1976) it is well known that
$$\begin{aligned} S_2 := \zeta(2) &= 3\sum_{k=1}^{\infty} \frac{1}{k^2\binom{2k}{k}} \\ A_3 := \zeta(3) &= \frac{5}{2}\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k^3\binom{2k}{k}} \\ S_4 := \zeta(4) &= \frac{36}{17}\sum_{k=1}^{\infty} \frac{1}{k^4\binom{2k}{k}} \end{aligned}$$

⋄ These results might suggest that
$$Z_5 \;:=\; \zeta(5)/\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k^5\binom{2k}{k}}$$
is a simple rational or algebraic number.

PSLQ RESULT: If Z_5 satisfies a polynomial of degree ≤ 25 the Euclidean norm of coefficients *exceeds* 2×10^{37}.

2. BINOMIAL SUMS and LIN_DEP

- Any relatively prime integers p and q such that
$$\zeta(5) \stackrel{?}{=} \frac{p}{q}\sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k^5\binom{2k}{k}}$$
have q astronomically large (as "lattice basis reduction" showed).

- But ⋯ PSLQ yields in *polylogarithms*:
$$\begin{aligned} \sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k^5\binom{2k}{k}} &= 2\zeta(5) \\ &- \tfrac{4}{3}L^5 + \tfrac{8}{3}L^3\zeta(2) + 4L^2\zeta(3) \\ &+ 80\sum_{n>0}\left(\frac{1}{(2n)^5} - \frac{L}{(2n)^4}\right)\rho^{2n} \end{aligned}$$
where $L := \log(\rho)$ and $\rho := (\sqrt{5}-1)/2$; with similar formulae for A_4, A_6, S_5, S_6 and S_7.

- A less known formula for $\zeta(5)$ due to Koecher suggested generalizations for $\zeta(7), \zeta(9), \zeta(11)\ldots.$

⋄ Again the coefficients were found by integer relation algorithms. *Bootstrapping* the earlier pattern kept the search space of manageable size.

- For example, and simpler than Koecher:
$$\begin{aligned} (4) \qquad \zeta(7) &= \frac{5}{2}\sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k^7\binom{2k}{k}} \\ &+ \frac{25}{2}\sum_{k=1}^{\infty} \frac{(-1)^{k+1}}{k^3\binom{2k}{k}}\sum_{j=1}^{k-1}\frac{1}{j^4} \end{aligned}$$

- We were able – by finding integer relations for $n = 1, 2, \ldots, 10$ – to encapsulate the formulae for $\zeta(4n+3)$ in a single conjectured generating function, (entirely *ex machina):*

THEOREM. For any complex z,

$$\sum_{n=1}^{\infty} \zeta(4n+3) z^{4n}$$

$$(5) \quad = \sum_{k=1}^{\infty} \frac{1}{k^3(1-z^4/k^4)}$$

$$= \quad \frac{5}{2}\sum_{k=1}^{\infty} \frac{(-1)^{k-1}}{k^3\binom{2k}{k}(1-z^4/k^4)} \prod_{m=1}^{k-1} \frac{1+4z^4/m^4}{1-z^4/m^4}.$$

⋄ The first '=' is easy. The second is quite unexpected in its form!

• $z=0$ yields Apéry's formula for $\zeta(3)$ and the coefficient of z^4 is (**??**).

HOW IT WAS FOUND

⋄ The first ten cases show (**??**) has the form

$$\frac{5}{2}\sum_{k\geq 1} \frac{(-1)^{k-1}}{k^3\binom{2k}{k}} \frac{P_k(z)}{(1-z^4/k^4)}$$

for undetermined P_k; with abundant data to compute

$$\boxed{P_k(z) = \prod_{m=1}^{k-1} \frac{1+4z^4/m^4}{1-z^4/m^4}.}$$

• We found many reformulations of (**??**), including a marvelous finite sum:

$$(6) \quad \boxed{\sum_{k=1}^{n} \frac{2n^2}{k^2} \frac{\prod_{i=1}^{n-1}(4k^4+i^4)}{\prod_{i=1,\, i\neq k}^{n}(k^4-i^4)} = \binom{2n}{n}.}$$

⋄ Obtained via Gosper's (Wilf-Zeilberger type) *telescoping algorithm* after a mistake in an electronic Petrie dish ('infty' $\neq$ 'infinity').

• This identity was recently proved by Almkvist and Granville (Experimental Math, 1999) thus finishing the proof of (**??**) and giving a rapidly converging series for any $\zeta(4N+3)$ where N is positive integer.

⋄ And perhaps shedding light on the irrationality of $\zeta(7)$? Recall that $\zeta(2N+1)$ is not proven irrational for $N>1$.

† Paul Erdos, when shown (**??**) shortly before his death, rushed off. Twenty minutes later he returned saying he did not know how to prove it but if proven it would have implications for Apéry's result ('$\zeta(3)$ is irrational').

3. MULTIPLE ZETA VALUES and LIN_DEP

• *Euler sums* or *MZVs* ("multiple zeta values") are a wonderful generalization of the classical ζ function.

• For natural numbers $i_1, i_2, \ldots, i_k$

$$(7) \quad \zeta(i_1, i_2, \ldots, i_k) := \sum_{n_1>n_2>n_k>0} \frac{1}{n_1^{i_1} n_2^{i_2} \cdots n_k^{i_k}}$$

⋄ Thus $\zeta(a) = \sum_{n\geq 1} n^{-a}$ is as before and

$$\zeta(a,b) = \sum_{n=1}^{\infty} \frac{1+\frac{1}{2^b}+\cdot+\frac{1}{(n-1)^b}}{n^a}$$

• The integer k is the sum's *depth* and $i_1 + i_2 + \cdots + i_k$ is its *weight*.

• Definition (**??**) clearly extends to alternating and character sums. MZVs have recently found interesting interpretations in high energy physics, knot theory, combinatorics ...

• MZVs satisfy many striking identities, of which

$$\zeta(2,1) = \zeta(3)$$

$$4\zeta(3,1) = \zeta(4)$$

are the simplest.

◇ Euler himself found and partially proved theorems on reducibility of depth 2 to depth 1 ζ's ($\zeta(6,2)$ is the lowest weight 'irreducible').

◇ A high precision *fast ζ-convolution* (EZFace/Java) allows use of integer relation algorithms leading to important dimensional (reducibility) conjectures and amazing identities.

• We illustrate with a conjecture of Zagier first proved by Broadhurst et al:

$$\zeta(\{3,1\}_n) = \frac{1}{2n+1}\zeta(\{2\}_{2n})$$

$$(8) \qquad \left(= \frac{2\pi^{4n}}{(4n+2)!}\right)$$

where $\{s\}_n$ is the string s repeated n times.

† The *unique* non-commutative analogue of Euler's evaluation of $\zeta(2n)$.

◇ My favourite conjecture (open for $n > 2$) is

$$\boxed{8^n\,\zeta(\{-2,1\}_n) \stackrel{?}{=} \zeta(\{2,1\}_n).}$$

Can just $n = 2$ be proven symbolically as is the case for $n = 1$?

• Our simplest conjectures (on the number of irreducibles) are beyond present proof techniques. Does $\zeta(5)$ or $G \in \mathbb{Q}$?

◇ Dimensional conjectures sometimes involve finding integer relations between hundreds of quantities and so demanding precision of thousands of digits – often of hard to compute objects.

• Bailey and Broadhurst have recently found a *polylogarithmic ladder* of length 17 (a record) with such "ultra-PSLQing".

Coworkers: B^4, Fee, Girgensohn, Lisoněk, others.

4. MULTIPLE CLAUSEN VALUES

• We are now studying *Deligne words* for multiple integrals generating *Multiple Clausen Values* at $\pi/3$ such as

$$\mu(a,b) := \sum_{n>m>0} \frac{\sin(n\frac{\pi}{3})}{n^a m^b},$$

and which seem quite fundamental.

◇ Thanks to a note from Flajolet which led to prove results like $S_3 = \frac{2\pi}{3}\mu(2) - \frac{4}{3}\zeta(3)$,

$$\sum_{k=1}^{\infty} \frac{1}{k^5\binom{2k}{k}} = 2\pi\mu(4) - \frac{19}{3}\zeta(5) + \frac{2}{3}\zeta(2)\zeta(3),$$

$$\sum_{k=1}^{\infty} \frac{1}{k^6\binom{2k}{k}} = -\frac{4\pi}{3}\mu(4,1) + \frac{3341}{1296}\zeta(6) - \frac{4}{3}\zeta(3)^2.$$

Coworkers: Broadhurst & Kamnitzer

KUHN

"The issue of paradigm choice can never be unequivocally settled by logic and experiment alone.

...

in these matters neither proof nor error is at issue. The transfer of allegiance from paradigm to paradigm is a conversion experience that cannot be forced."

HERSH

• Whatever the outcome of these developments, mathematics is and will remain a uniquely human undertaking. Indeed Reuben Hersh's arguments for a humanist philosophy of mathematics, as paraphrased below, become more convincing in our setting:

1. *Mathematics is human*. It is part of and fits into human culture. It does not match Frege's concept of an abstract, timeless, tenseless, objective reality.

2. *Mathematical knowledge is fallible*. As in science, mathematics can advance by making mistakes and then correcting or even re-correcting them. The "fallibilism" of mathematics is brilliantly argued in Lakatos' *Proofs and Refutations*.

3. *There are different versions of proof or rigor.* Standards of rigor can vary depending on time, place, and other things. The use of computers in formal proofs, exemplified by the computer-assisted proof of the four color theorem in 1977, is just one example of an emerging nontraditional standard of rigor.

4. *Empirical evidence, numerical experimentation and probabilistic proof all can help us decide what to believe in mathematics.* Aristotelian logic isn't necessarily always the best way of deciding.

5. *Mathematical objects are a special variety of a social-cultural-historical object*. Contrary to the assertions of certain post-modern detractors, mathematics cannot be dismissed as merely a new form of literature or religion. Nevertheless, many mathematical objects can be seen as shared ideas, like Moby Dick in literature, or the Immaculate Conception in religion.

◇ From "Fresh Breezes in the Philosophy of Mathematics", *American Mathematical Monthly*, August-Sept 1995, 589–594.

• The recognition that "quasi-intuitive" analogies may be used to gain insight in mathematics can assist in the learning of mathematics. And honest mathematicians will acknowledge their role in discovery as well.

We should look forward to what the future will bring.

A FEW CONCLUSIONS

- Draw your own! – perhaps ···
- Proofs are often out of reach – understanding, even certainty, is not.
- Packages can make concepts accessible (Groebner bases).
- Progress is made 'one funeral at a time' (Niels Bohr).
- 'You can't go home again' (Thomas Wolfe).

***

C3 Computational Inc

Nationally shared – Internationally competitive

The scope of the C3.ca is a seven year plan to build computational infrastructure on a scale that is globally competitive, and that supports globally competitive research and development. The plan will have a dramatic impact on Canada's ability to develop a knowledge based economy. It will attract highly skilled people to new jobs in key application areas in the business, research, health, education and telecommunications sectors. It will provide the tools and opportunity to enhance their knowledge and experience and retain this resource within the country.

◇ Canadian government has funded/matched $75 million worth of equipment in the last year.

- Eight installations in Five Provinces.
- More to come : long-term commitment.
- Good human support at a distance/web tools are key.
- A pretty large investment for a medium size country.
- A good model for other such countries?

• 25% of Memorial University of Newfoundland's large Dec Alpha was used for Euler sum research at a distance in 1997 – 98.

REFERENCES

- D. H. Bailey, J.M. Borwein and R.H. Crandall, "On the Khintchine constant," *Mathematics of Computation*, **66** (1997), 417-431. [CECM Research Report 95:036]
- J.M. Borwein, P.B. Borwein, R. Girgensohn and S. Parnes, "Making Sense of Experimental Mathematics," *Mathematical Intelligencer*, **18**, Number 4 (Fall 1996), 12–18. [CECM Research Report 95:032]
- J.M. Borwein, D.M. Bradley and D.J. Broadhurst, "Evaluations of k–fold Euler/Zagier sums: a compendium of results for arbitrary k," *Electronic Journal of Combinatorics*, **4** (1997), R5 (21 pages). (The Wilf Festschrift) [CECM Research Report 96:067]
- J.M. Borwein and D.M. Bradley, "Empirically determined Apéry–like formulae for zeta(4n+3)," *Experimental Mathematics*, **6** (1997), 181–194. [CECM Research Report 96:069]

- Jonathan M. Borwein and Robert Corless, "Emerging tools for experimental mathematics," *American Mathematical Monthly*, **106** (1999), 889–909. [CECM Preprint 98:110]

- J.M. Borwein and P. Lisoněk, "Applications of Integer Relation Algorithms," *Discrete Mathematics* (Special issue for FPSAC 1997), in press, 2000. [CECM Research Report 97:104]

- D.H. Bailey and J.M. Borwein, "Experimental Mathematics: Recent Developments and Future Outlook," *World Mathematical Year 2000 Book,* Springer–Verlag, in press. [CECM Preprint 99:143]

• These and other references are available at www.cecm.sfu.ca/preprints/

◇ Quotations at jborwein/quotations.html