NEWTON ONLINE: MATHEMATICS COMES OUT OF THE CLOSET

Peter Borwein

Simon Fraser University Centre for Constructive and Experimental Mathematics

http://www.cecm.sfu.ca/~pborwein

Typeset by $\mathcal{AMS}$-TeX

Preamble

• We live, both philosophically and technologically, in a mathematical world. More so than most of us care to admit.

• Our faith in science is in large part based on the "unreasonable efficacy of mathematics" that has been apparent at least since the time of Newton.

• Mathematics has also been arcane and inaccessible.

• There is some hope that, with computers, this will change....

Predicting the Past

"It would appear that we have reached the limits of what it is possible to achieve with computer technology, although one should be careful with such statements, as they tend to sound pretty silly in 5 years."

John Von Neumann (ca. 1949)

★★★★★★

- Von Neumann was in good company....

"Fooling around with alternating current is just a waste of time. Nobody will use it, ever."

Thomas Edison

"I think there is a world market for about five computers."

T.J. Watson, CEO, IBM, 1947

"I have traveled the length and breadth of this country and talked with the best people, and I can assure you that data processing is a fad that won't last out the year."

Chief business ed., Prentice Hall , 1957

- Typical of the caution were quotes like

"In spite of its powers, the analyser cannot solve problems the mathematician cannot do himself"

despite the title of the 1949 Newsweek article "The Great Electro-Mechanical Brain"

- Aitken did speculate in Time (1950)

"it might be possible to "program" a machine to beat the stock market"

He should have added "into the ground."

- By and large predictions were mundane and extraordinarily cautious.

A Conjectures people should have made

★★★★★★

" Computers will solve the four colour conjecture"

• The **Riemann Hypothesis** is the great unsolved problem in pure mathematics.It was conjectured by Riemann in 1859.

• It conjectures (quite precisely) how many primes there are among the first n numbers.

• For example it predicts 50,847,641 primes up to a billion. The actual number is 50,847,562 (out by 79).

•Actually what the Riemann Hypothesis really says is that all the complex zeros of the function

$$\sum_{n=1}^{\infty} \frac{(-1)^n}{n^z}$$

have real part 1/2. Which is true for the first 1.5 billion.

Two Way Out Prediction For The Next Fifty Years

So far, on predictions, I am batting 1.000.

★★★★★★

“ Computers will solve the Riemann Hypothesis”

Extensive experimentation will uncover a family of positive definite operators whose eigenvalues are the (suitably normalized) zeros of the Zeta function.

★★★★★★

★★★★★★

“ Computers will not solve the Riemann Hypothesis”

★★★★★★

No one has ever batted .500. Too bad baseball isn’t this easy.

Compulsive Personality Disorder

According to DSM–III must meet 4 of the following:

- restricted ability to express warmth ... unduly conventional, serious and formal

- perfectionism (that misses the forest for the trees)

- insistence that others submit to his or her way of doing things

- excessive devotion to work and productivity

- indecisiveness: decision-making is either avoided, postponed or protracted

Alan Turing: 1912–1954

- One of the fathers of computer science

- A principal in breaking the U-boat Enigma cipher

- Known for Turing Machines and the Turing Test

- Committed suicide in 1954 after a protracted period of estrogen therapy (instead of jail for his homosexuality).

Theorem: There is no algorithm that can tell if an algorithm is an algorithm.

• Computers are the legitimate progeny of mathematicians. They were invented, analyzed and found wanting long before any were ever built.

• At least ten years before the construction of anything really resembling a digital computer, mathematicians had proved the limitations of computers.

• Mathematicians spawned computers but then largely ignore them. They rarely if ever helped - and if they did it was in an aesthetically unacceptable way.

"Beauty is the first test; there is no permanent place in the world for ugly mathematics." G.H. Hardy

"Computers are useless. They can only give you answers."

Pablo Picasso (1881-1973)

★★★★★★

• Picasso is wrong and this is the key to why the face of pure mathematics will change completely over the next 50 years.

• Consider $P \neq NP$

• Consider Factoring Integers.

• Consider Multiplication.

• Consider Fractals.

The $P \neq NP$ conjecture

•This is a problem that had no context 70 years ago.

•This conjectures that problems we believe to be computationally difficult really are. (Cook)

• For example, the Travelling Salesman Problem. (NP Hard).

Factoring large Integers

•This is a problem that was answered 70 years ago.

• RSA-155 was factored last year. It took 35.7 CPU years.

10941738641570527421809707322040357612003732945449205990913842131476349984288934784717997257891267332497625752899781833797076537244027146743531593354333897
=
102639592829741105772054196573991675900716567808038066803341933521790711307779
*
106603488380168454820927220360012878679207958575989291522270608237193062808643

• This is all intimately tied to the Riemann Hypothesis. And, surprisingly enough, there is a lot of money riding on it.

• The following 200 digit number is not a prime. The challenge is to find the two factors.

RSA-200 = 279978339112213278
7082946763872260162107044678
6955428537560009929326128400
1076093456710529553608560618
2235191095136578863710595448
2006576775098580557613579098
7349501441788631789462951872
37869221823983

Multiplication

- Another problem we thought was answered 70 years ago.

- Conventional multiplication of very large numbers is a disaster.

- Multiplying very large numbers correctly requires the same technology that allows CAT scanners to work.

Fractals and Chaos

- This was a problem that was too complicated to consider 70 years ago.

- No sane person would have constructed a single fractal image.

The Safest Prediction of All

★★★★★★

“ The undergraduate curriculum will be completely rewritten”

★★★★★★

- and it is about time!

- There will be no such thing as a non-computationally adept scientist or mathematician

- Maple already outperforms the average undergraduate in many courses.

More Predictions For The Next Fifty Years

★★★★★★

“ The process of doing mathematics will profoundly change”

★★★★★★

- Or perhaps more precisely change back.

★★★★★★

“ mathematics will emerge as a (partially) experimental endevour”

★★★★★★

“God does not care about our mathematical difficulties. He integrates empirically.”

Albert Einstein (1879-1955)

• In future God should use Maple (or Mathematica or ...)

"It still remains true that, with negative theorems such as this, transforming personal convictions into objective ones requires deterringly detailed work. To visualize the whole variety of cases, one would have to display a large number of equations by curves; each curve would have to be drawn by its points, and determining a single point alone requires lengthy computations.

You do not see from Fig. 4 in my first paper of 1799, how much work was required for a proper drawing of that curve."

K. F. Gauss (Letter to Schumacher 1836)

On The Experimental Nature of Math.

An Example:

$$\sum_{k=1}^{\infty}\left(1+\frac{1}{2}+\cdots+\frac{1}{k}\right)^{4}(k+1)^{-5}$$

$$= -\frac{29}{2}\zeta(9)+\frac{37}{2}\zeta(4)\zeta(5)$$

$$+\frac{33}{4}\zeta(3)\zeta(6)-\frac{8}{3}\zeta^{3}(3)-7\zeta(2)\zeta(7)$$

- It is true - it is not (yet) proven.

- The proof of the pudding is in the eating.

Reliability and Necessity

"Imagine if every Thursday your shoes exploded if you tied them the usual way. This happens to us all the time with computers, and nobody thinks of complaining."

Jeff Raskin, interviewed in Doctor Dobb's Journal

★★★★★★

"Computers make it easier to do a lot of things, but most of the things they make it easier to do don't need to be done."

Andy Rooney

Another Example:

$$\sqrt{\pi} \doteq \frac{1}{10^5} \sum_{n=-\infty}^{\infty} e^{-n^2/10^{10}}$$

This is correct to over 42 billion digits but not to 43 billion digits.

- Coincidence?

- “Messing” around only works if you know where to look.

Inverse Symbolic Calculation

- What is 1.1981402347355922075?

If $a_0 := 1, b_0 := \sqrt{2}$ and

$$a_{n+1} := \frac{a_n + b_n}{2}, \quad b_{n+1} := \sqrt{a_n b_n}$$

Then

$$\lim_{n\to\infty} a_n = \lim_{n\to\infty} b_n = \frac{\pi/2}{\int_0^1 \frac{dt}{\sqrt{1-t^4}}}$$
$$= 1.1981402347355922075...$$

In 1799, Gauss observed this purely numerically and wrote that this result

"will surely open a whole new field of analysis."

- What is 3.14159265358979323853?
- What is 2.71828182845904523536?
- What is 14.8613416176874701868?
- What is $(e^{\pi\sqrt{163}} - 744)^{\frac{1}{3}}$?

$(e^{\pi\sqrt{163}} - 744)^{\frac{1}{3}} = 640320$ to 30 digits

- However to thirty five places it equals

640319.99999999999999999999999939032

The 40 Trillionth Binary Digit of Pi is 0.

- 9C381872D27596F81D0E48B95A6C46 (actually 100 Billionth Hex)

- by Colin Percival as a distributed computation

- Amazing that it can be done

- Requires the following (experimentally uncovered) identity of Bailey, Plouffe and PB. This is really the interesting part of the story.

- Remember the Pentium (and Brun's constant)

Theorem.

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

Proof. This is equivalent to:

$$\pi = \int_0^{1/\sqrt{2}} \frac{4\sqrt{2} - 8x^3 - 4\sqrt{2}x^4 - 8x^5}{1 - x^8} dx.$$

which on substituting $y := \sqrt{2}x$ becomes

$$\pi = \int_0^1 \frac{16\,y - 16}{y^4 - 2\,y^3 + 4\,y - 4} dy\,.$$

The equivalence follows from the identity

$$\int_0^{1/\sqrt{2}} \frac{x^{k-1}}{1 - x^8}\, dx = \int_0^{1/\sqrt{2}} \sum_{i=0}^{\infty} x^{k-1+8i}\, dx$$

$$= \frac{1}{\sqrt{2}^k} \sum_{i=0}^{\infty} \frac{1}{16^i(8i+k)}$$

□

Littlewood's Other Conjecture.

Conjecture (1966). There is some

$$p(z) := \sum_{n=0}^{N} c_n z^n \qquad c_i \pm 1$$

so that for all z on the boundary of the unit disc

$$C_1 < \frac{|p(z)|}{\sqrt{n}} < C_2.$$

• Littlewood, in part, based his conjecture on computations of all such polynomials up to degree twenty.

• Odlyzko has now done 200 MIPS years of computing on this problem

- In Advice to a Young Scientist, P.B. Medawar defines four different kinds of experiment: the Kantian, Baconian, Aristotelian, and the Galilean. Mathematics has always participated deeply in the first three categories but has somehow managed to avoid employing the Galilean model.

“ (the Baconian experiment) is the consequence of ‘trying things out’ or even of merely messing about.”

“(the) Galilean Experiment is 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.”

★★★★★★

“Change is scientific, progress is ethical; change is indubitable, whereas progress is a matter of controversy.”

Bertrand Russell (1872-1970)

★★★★★★

“It seems to me that the mine is already almost too deep, and unless we discover new seams we shall sooner or later have to abandon it. ... It is not impossible that the mathematical positions in the Academies will one day become what the University chairs in Arabic are now.”

J. L. Lagrange (1736-1813)

★★★★★★

“Progress is measured funeral by funeral”