Will Society benefit most by finding the solutions to The Millennium Prize Problems or Hilbert's Problems?

The Millennium Prize Problems and Hilbert's Problems are sets of partially unsolved problems in the field of Mathematics selected and stated by the Clay Mathematics Institute and Mathematician David Hilbert respectively. The former are noted for their million-dollar prize for the first verified solution to any of the seven problems, six of which remain unsolved at the time of writing.

While some high profile fields are largely saturated in terms of research progress, Computer Science has taken an opposite path and the field is increasingly gaining momentum, with discoveries emerging due to breakthroughs in logic and theoretical computational systems and Mathematics.

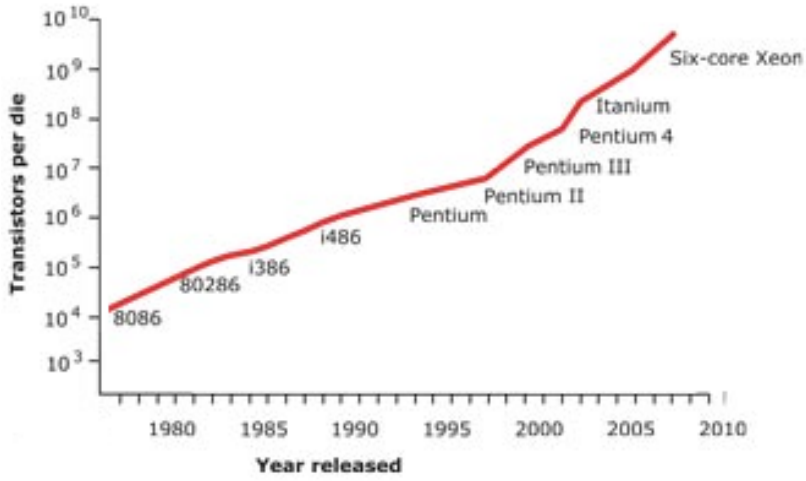

Figure 1 (left)
Number of transistors per die within processors over time.
Source: Intel

Figure 1 shows the number of transistors within computer processor chips increasing over time. This roughly follows Moore's Law, which states the number of transistors will double every 18 months and eventually reach a limit. This limit is frequently extended and consumers continue to see improvements yearly.

Figure 2 (above)
Spheres accurate to one part in a million are possible.
Source: The Australian Centre for Precision Optics

If Physics is the application of Mathematics to the Universe, then Computing is the application of Mathematics to the virtual Universe. Creating a perfect sphere is impossible in the physical realm, though such perfect elements are digitally representable. This opened the door to new methods of analysis.

The Riemann Hypothesis, considered one of the most important problems in pure maths (*Borwein et al. 2008*), involves the distribution of the prime numbers. The hypothesis states that the solutions to the Riemann-Zeta function (**figure 3**) lie on a critical line. The first ten trillion values have been computationally verified.

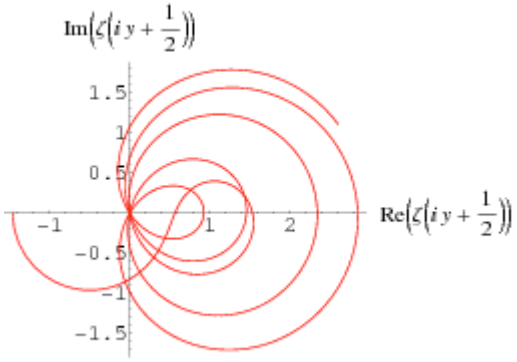

Figure 3 (left)
A plot of values 0 to 35.
Source: Wolfram MathWorld, Derbyshire (2004)

While an underlying pattern is suggested, this Hilbert Problem remains unproven. The unpredictable nature of the prime numbers has been put to use in RSA (*Rivest, Shamir and Adleman, MIT, 1978*). This system, considered unbreakable, provides digital security with primes. Banks, websites and governments worldwide have adopted RSA. A brute force search would need to test possible primes to break this, but since there is no reliable way of determining the next prime, computers may take years to perform this, rendering this method impractical. A proof of the Riemann Hypothesis, however, may provide a means of determining a pattern and breaking RSA.

Brute force guessing of standard passwords is also impractical. Computer users currently create case-sensitive alphanumeric passwords as in **figure 4**. The problem with checking every possibility lies not with verification; a computer can easily identify whether two pieces of text are equal. It lies with first obtaining the solution to compare. Some techniques search through dictionary entries, allowing quicker identification of common passwords.

Th3!Wh1rld1zN0tEnuf

Figure 4 (above)
A case sensitive password consisting of alphanumeric characters.

Another Millennium Prize Problem, touted the most important unsolved problem in Computer Science, P vs NP (*Cook, 1971*) revolves around this concept. It asks the question of whether a problem having quick machine verifiable solutions means those solutions can also be found quickly. Problems of the latter are classified P, while those that are hard to compute are NP. In the case of guessing passwords, it becomes apparent that verification is a P problem (easy) while searching for the correct password is NP (hard).

The world currently assumes P≠NP along with most Computer Scientists (*Gasarch, 2002*), while majority of security systems rely on this assumption. A claimed proof of P=NP (*Deolalikar, 2010*) was later shown to be incorrect, though the possibility raised many concerns for security. The implications would be far-reaching for society. A correct proof either way will have great impact, since the solution to P vs NP intrinsically links to solutions of the other Problems. If P=NP, not only will a new era of cryptography need to be abruptly ushered in, but NP-hard problems within countless other fields such as Biology (genome sequencing, protein structure prediction) and Physics (simulations) would become easier.

The effects of solutions on society's widely used systems cannot be ignored. They would pave the way to a once-distant future, with consequences such as the rise of new, future-proof technologies resistant to P=NP attacks and Riemann-Hypothesis friendly, leading to better consumer systems. A hail of advancements in knowledge would be made, with improvements to society's quality of life due to significant improvements to Biology, Medicine and other fields. Perelman, responsible for solving the Poincaré Conjecture (involving the characteristics of spheres in higher dimensions) remarked:

"Where technology creates new machines and devices, Mathematics creates their analogues – logical methods for analysis in any field of science. Every Mathematical theory, if it's strong, will sooner or later find an application." (*Perelman, 2003*)

As researchers move on to proving the next unsolved theorem, the laypeople of society would truly revel in the consequences of such discoveries, and would therefore benefit the most overall.