# Ten Problems I Can't Solve

Jeffrey Shallit
Department of Computer Science
University of Waterloo
shallit@uwaterloo.ca
http://www.math.uwaterloo.ca/~shallit

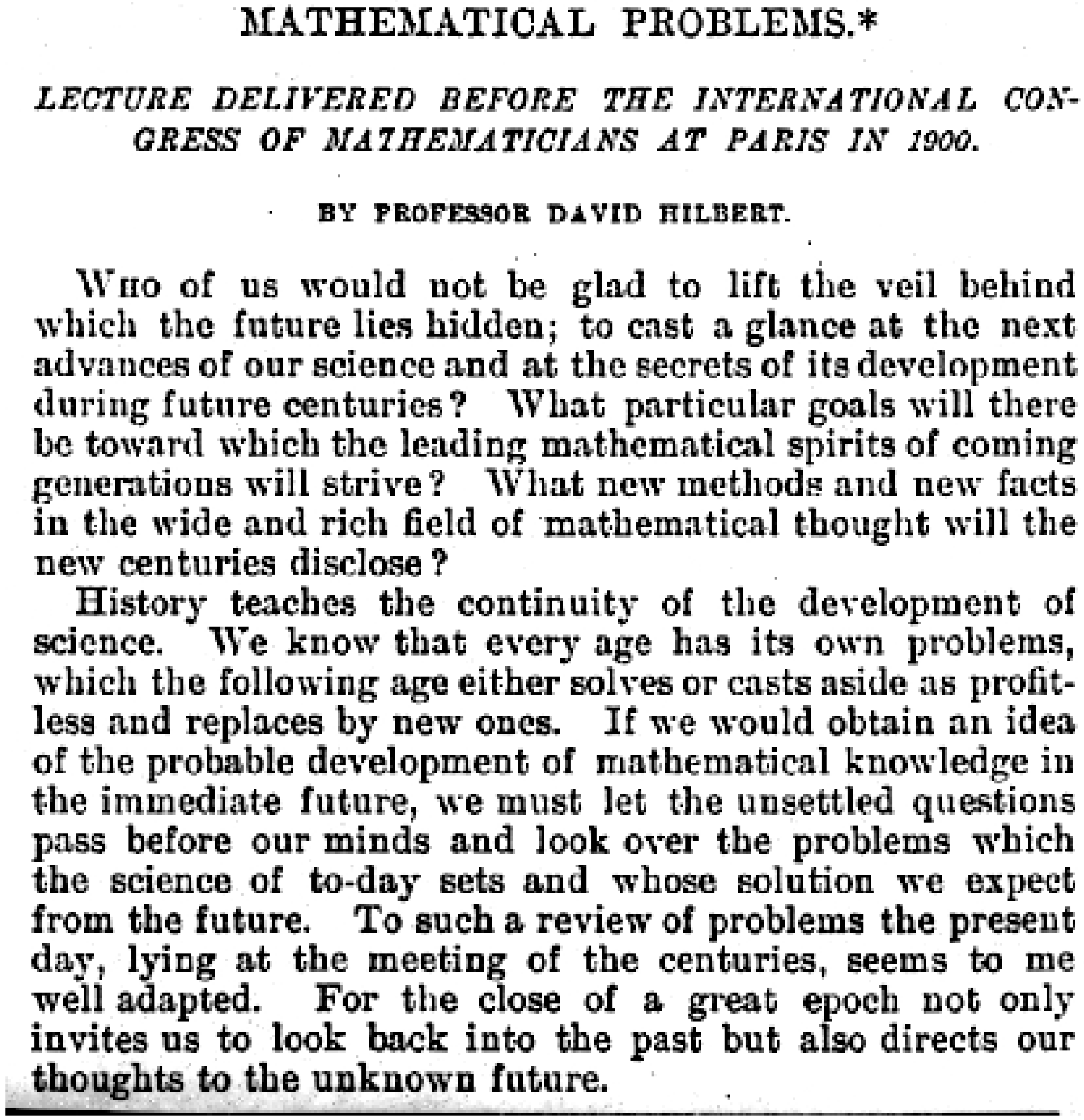
# Hilbert's Problems

In 1900, David Hilbert gave an address to the International Congress of Mathematician entitled "Mathematical Problems". In this talk he discussed 23 problems for which he felt a solution would have a significant impact on mathematics.

Figure 1: David Hilbert (1862–1943)

# Hilbert's Problems

Here is a photocopy of the first part of a translation of Hilbert's address:



## MATHEMATICAL PROBLEMS.*

*LECTURE DELIVERED BEFORE THE INTERNATIONAL CONGRESS OF MATHEMATICIANS AT PARIS IN 1900.*

BY PROFESSOR DAVID HILBERT.

WHO of us would not be glad to lift the veil behind which the future lies hidden; to cast a glance at the next advances of our science and at the secrets of its development during future centuries? What particular goals will there be toward which the leading mathematical spirits of coming generations will strive? What new methods and new facts in the wide and rich field of mathematical thought will the new centuries disclose?

History teaches the continuity of the development of science. We know that every age has its own problems, which the following age either solves or casts aside as profitless and replaces by new ones. If we would obtain an idea of the probable development of mathematical knowledge in the immediate future, we must let the unsettled questions pass before our minds and look over the problems which the science of to-day sets and whose solution we expect from the future. To such a review of problems the present day, lying at the meeting of the centuries, seems to me well adapted. For the close of a great epoch not only invites us to look back into the past but also directs our thoughts to the unknown future.

Figure 2: Translation of David Hilbert's 1900 Address

# Shallit's Problems

In this talk I will present ten problems that I am unable to solve. The order of presentation is random. Some are my own invention, others not. Some of them are probably easy, but others may be quite hard. I offer a cash reward for a solution to these problems.

# Problem 1: Pierce Expansions

Let $a, b$ be integers with $0 < a < b$. Define $a_0 = a$ and $a_{n+1} = b \bmod a_n$ for $n \geq 0$. Now $a_{n+1} < a_n$, so eventually we must have $a_r = 0$. Define $P(a, b) = r$.

The question is, how big can $P(a, b)$ be as a function of $a$ and $b$?

For example, if $a = 12$, $b = 19$, we have

$$\begin{aligned} a_0 &= 12 \\ a_1 &= 7 \\ a_2 &= 5 \\ a_3 &= 4 \\ a_4 &= 3 \\ a_5 &= 1 \\ a_6 &= 0 \end{aligned}$$

so $P(12, 19) = 6$.

# Problem 1: Pierce Expansions

This question is related to the expression of $a/b$ as a series of the form

$$\frac{1}{c_1} - \frac{1}{c_1 c_2} + \frac{1}{c_1 c_2 c_3} - \cdots \pm \frac{1}{c_1 c_2 \cdots c_r}$$

Provided $0 < c_1 < c_2 < \cdots$ and $c_r > c_{r-1} + 1$, this expansion is unique.

For example,

$$\frac{12}{19} = \frac{1}{1} - \frac{1}{1 \cdot 2} + \frac{1}{1 \cdot 2 \cdot 3} - \frac{1}{1 \cdot 2 \cdot 3 \cdot 4} + \frac{1}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 6} - \frac{1}{1 \cdot 2 \cdot 3 \cdot 4 \cdot 6 \cdot 19}.$$

Erdös and Shallit proved $P(a,b) = O(b^{1/3+\epsilon})$ [*Séminaire de Théorie des Nombres de Bordeaux* **3** (1991), 43–53]. Vlado Keselj improved this to $P(a,b) = O(b^{1/3})$. But probably $P(a,b) = O((\log b)^2)$.

I offer \$ 50 for a proof that $P(a,b) = O((\log b)^c)$ for some constant $c$, and another \$ 50 for the determination of the optimal $c$.

# Problem 2: An Infinite Product

Consider the sequence

$$\frac{1}{2}, \quad \frac{1/2}{3/4}, \quad \frac{\frac{1/2}{3/4}}{\frac{5/6}{7/8}}, \ldots$$

What does this converge to?

Here is a proof that this sequence converges to $\frac{\sqrt{2}}{2}$.

First, we observe that the limit is

$$\prod_{n \geq 0} \left( \frac{2n+1}{2n+2} \right)^{(-1)^{t_n}} \tag{1}$$

where $t_n$ is the sum of the bits (mod $2$) in the binary expansion of $n$.

# Problem 2: An Infinite Product

We now use a trick of Allouche: let $P = \prod_{n \geq 0} \left(\frac{2n+1}{2n+2}\right)^{(-1)^{t_n}}$ and let $Q = \prod_{n \geq 1} \left(\frac{2n}{2n+1}\right)^{(-1)^{t_n}}$.

Clearly

$$PQ = \frac{1}{2} \prod_{n \geq 1} \left(\frac{n}{n+1}\right)^{(-1)^{t_n}}.$$

Now break this infinite product into separate products over odd and even indices; we find

$$\begin{aligned} PQ &= \frac{1}{2} \prod_{n \geq 0} \left(\frac{2n+1}{2n+2}\right)^{(-1)^{t_{2n+1}}} \prod_{n \geq 1} \left(\frac{2n}{2n+1}\right)^{(-1)^{t_n}} \\ &= \frac{1}{2} P^{-1} Q. \end{aligned}$$

It follows that $P^2 = \frac{1}{2}$.

But how about $Q$? Is it irrational? Transcendental?

I offer \$ 25 for the solution to this problem.

## Problem 3: A Matrix Problem

Suppose $M$ is an $n \times n$ matrix with non-negative integer entries.

**Conjecture.** Suppose there exist non-negative integer vectors $u$ and $v$ of the appropriate dimensions such that

$$uv > uMv > uM^2v > \cdots > uM^kv.$$

Then $k \leq n$.

Note that we can achieve $k = n$. For example, let

$$u = \begin{bmatrix} 1 \\ 1 \\ 1 \\ 1 \end{bmatrix}; \quad M = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 \end{bmatrix}; \quad v = \begin{bmatrix} 1 & 1 & 1 & 1 \end{bmatrix} \tag{2}$$

Then

$$\begin{aligned} uv &= 4 \\ uMv &= 3 \\ uM^2v &= 2 \\ uM^3v &= 1 \\ uM^4v &= 0 \end{aligned}$$

Ming-wei Wang and I have proved that $k \leq 2^n$ [*Linear Algebra and Its Applications* **290** (1999), 135-144].

## Problem 3: A Matrix Problem

This problem can be rephrased in terms of formal languages. Let $\Sigma$ be a finite alphabet, and let $\varphi : \Sigma^* \to \Sigma^*$ be a homomorphism, i.e., a map such that $\varphi(xy) = \varphi(x)\varphi(y)$ for all $x, y \in \Sigma^*$.

**Conjecture.** Let $|\Sigma| = n$. Suppose $w \in \Sigma^*$ is such that

$$|w| > |\varphi(w)| > |\varphi^2(w)| > \cdots > |\varphi^k(w)|.$$

Then $k \leq n$.

I offer $ 25 for the solution to this problem.

## Problem 4: Lexicographically Least Squarefree Word

A *square* is a word of the form $ww$. An *overlap* is a word of the form $awawa$, where $a$ is a single letter.

For example, *murmur* is an example of a square in English and *alfalfa* is an example of an overlap.

A word is *squarefree* if it contains no square subword. A word is *overlap-free* if it contains no overlap as a subword.

Thue proved that the infinite word

$$\mathbf{t} = t_0 t_1 t_2 \cdots = 0110100110010110 \cdots$$

is overlap-free. From this, it is easy to construct a squarefree infinite word on a three-letter alphabet.

It can be proved that the *lexicographically least* infinite overlap-free word over $\{0, 1\}$ is

$$001001\overline{\mathbf{t}} = 001001100101100110100 1 \cdots .$$

See *Electronic J. Combinatorics* **5** (1) (1998), #R27.

But can you characterize the *lexicographically least* infinite square-free word over $\{0, 1, 2\}$ ?

The first few terms are known to be

$$010201202101201020 12.$$

I offer $ 25 for the solution to this problem. (I get to decide what is a solution!)

# Problem 5: Linear Recurrences

Suppose $(a_n)_{n\geq 0}$ and $(b_n)_{n\geq 0}$ are integer sequences satisfying a linear recurrence with constant coefficients.

Suppose $A = \lim_{n\to\infty} \frac{a_n}{b_n}$ exists.

Prove or disprove: $A$ is algebraic.

I offer \$ 20 for the solution to this problem.

# Problem 6: An Unusual Sequence

Consider the sequence of 1's and 2's which is the fixed point $\mathbf{f}$ of the map which sends

$$1 \to 121$$

$$2 \to 12221$$

We have

$$\mathbf{f} = f(0)f(1)f(2)\cdots = 121122211211212221\cdots$$

Then $f(16n+1) = f(64n+1)$ for $n = 0, 1, \ldots, 1864134$, but not for $n = 1864135$. Explain this.

It is known that $\mathbf{f}$ is the run lengths of the Thue-Morse sequence

$$0110100110010110\cdots$$

See *Discrete Mathematics* **139** (1995), 455–461.

I offer \$ 20 for the solution to this problem.

# Problem 7: Separating Automata

Suppose you are given two distinct words $u, v$ with $|u|, |v| \leq n$.

What is the size of the smallest deterministic finite automaton (DFA) which accepts $u$ but rejects $v$, or vice versa?

If $u$ and $v$ are of different lengths then a simple argument gives a $O(\log n)$ upper bound.

How about if $u$ and $v$ are of the same length?

Robson [*Info. Proc. Letters* **30** (1989), 209–214] showed that in this case a separating DFA of size $O(n^{2/5}(\log n)^{3/5})$ exists. Can this be improved?

I offer \$ 25 for the solution to this problem.

# Problem 8: Rauzy's Sequence

G. Rauzy has proposed the following problem:

Define $u(1) = a$, $u(2) = b$, and

$$u(n) = u(\lfloor n/3 \rfloor) + u(n - \lfloor n/3 \rfloor)$$

for integers $n \geq 3$.

Prove or disprove:

$$\lim_{n \to \infty} u(n)/n$$

exists. If it exists compute this limit in terms of $a$ and $b$.

I offer $ 10 for the solution to this problem.

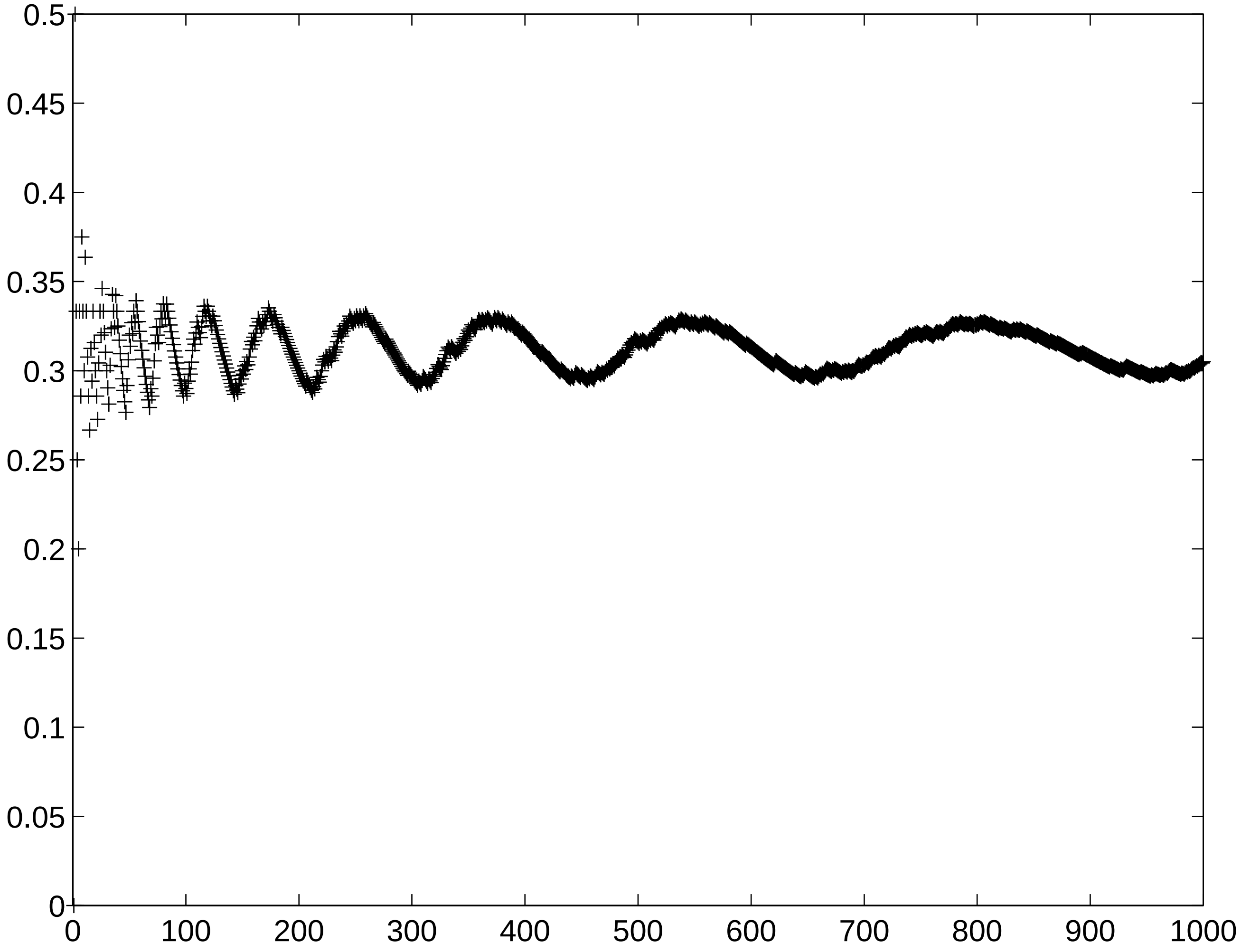


Figure 3: First thousand values of $u(n)/n$ with $a = 0$, $b = 1$

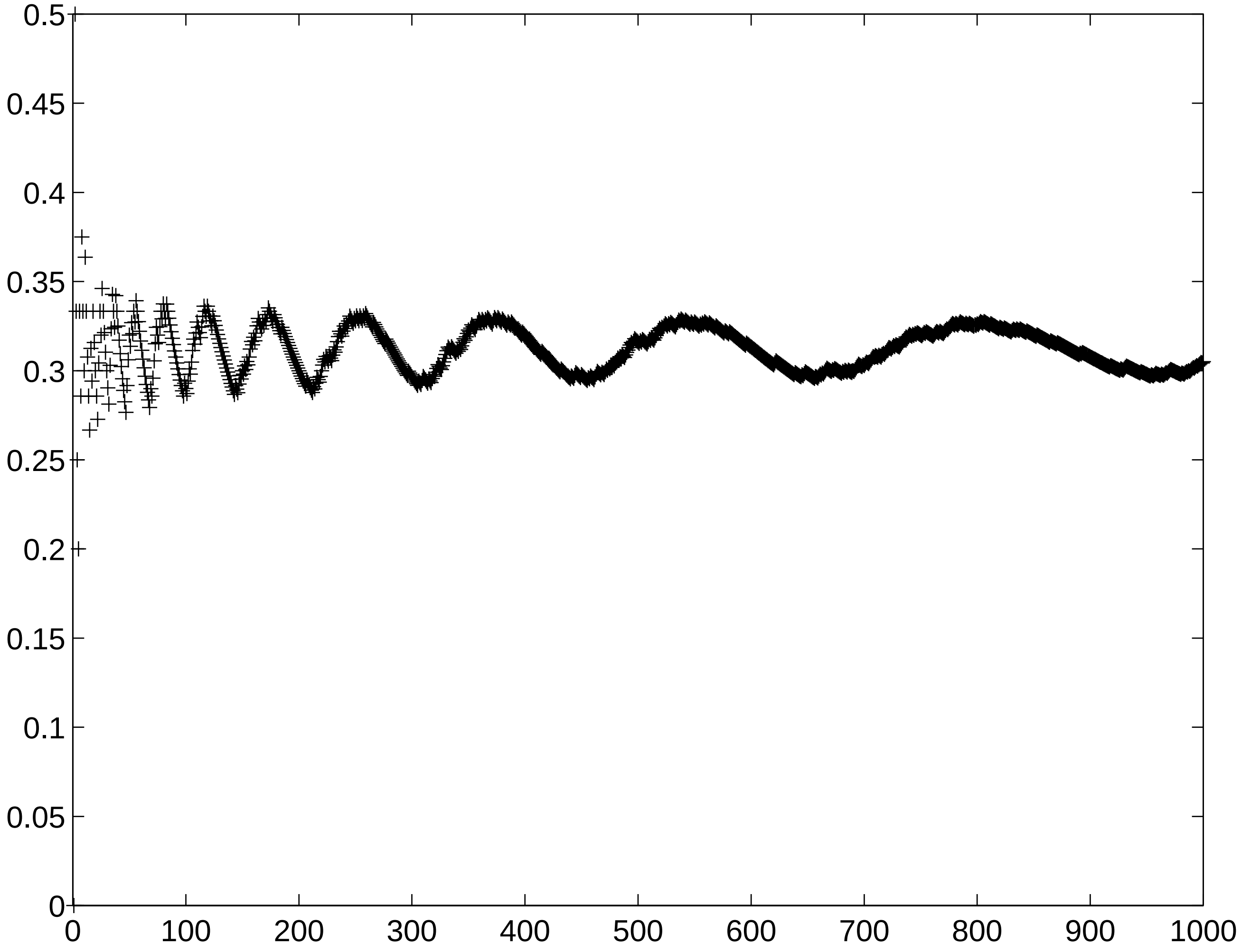


Figure 4: First thousand values of $u(n)/n$ with $a = 1$, $b = 0$

# Problem 9: Diversity of Sequences

We say a sequence $\mathbf{s} = (s(i))_{i \geq 0}$ is *diverse* if for all integers $r, a, b$ with $r \geq 2$ and $0 \leq a < b < r$, there exists $n$ such that $s(rn + a) \neq s(rn + b)$.

It is easy to prove that almost all sequences over $\{0, 1\}$ are diverse.

If $\mathbf{s}$ is diverse, and there exists a function $f$ such that $n = O(f(r))$, then we call $f$ a *diversity measure* for $\mathbf{s}$.

It can be proved that almost all sequences over $\{0, 1\}$ have diversity measure $O(\log r)$. See, for example, *Journal de Théorie des Nombres de Bordeaux* **8** (1996), 347–367.

Problem: construct an explicit example of a sequence with diversity measure $O((\log r)^c)$.

I offer \$ 10 for the solution to this problem.

## Problem 10: Exponentiation

Can you compute the $i$'th digit of the base-$k$ representation of $a^n$ using $O(\log n)$ space?

It is known that it can be computed in $O((\log n)^2)$ space.

I offer \$ 15 for the solution to this problem.

# Additional Open Problems

For additional sources of open problems, see

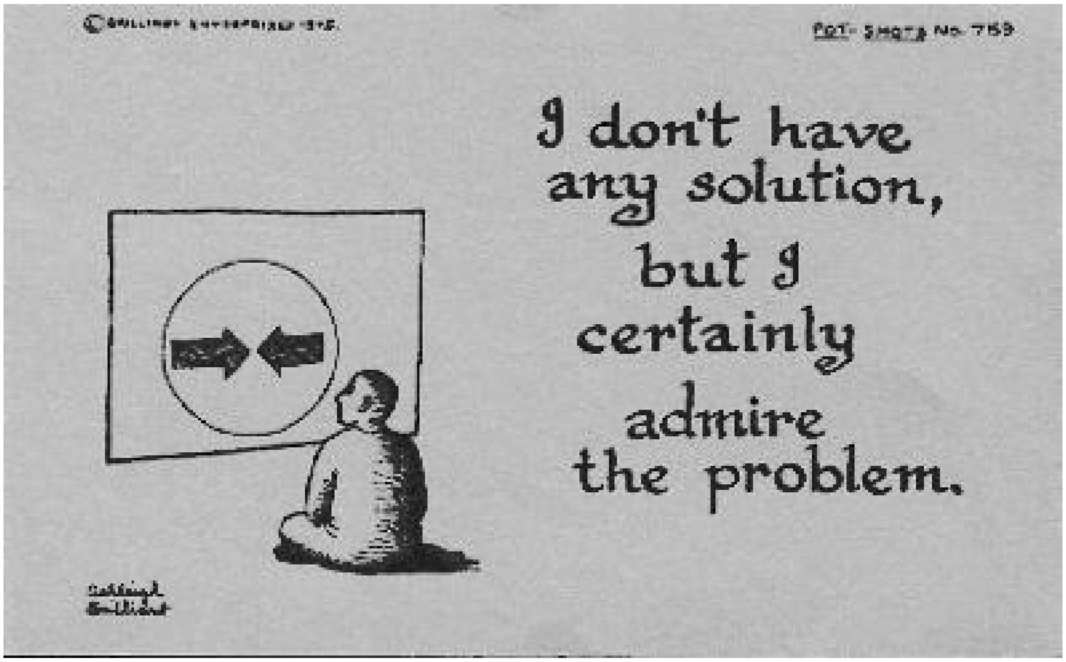
R. K. Guy, Unsolved Problems in Number Theory, Springer-Verlag, 1994, 2nd edition.

or visit

`http://www.mathsoft.com/asolve`

and

`http://www.claymath.org/prize_problems/index.htm`


POT-SHOTS No. 759
I don't have any solution, but I certainly admire the problem.