Matematisk Seminar
Universitetet i Oslo

Nr. 13
November 1963

UNSOLVABLE PROBLEMS IN THE THEORY OF COMPUTABLE NUMBERS

By

Brian Mayoh

Several equivalent definitions of the computable numbers are presented in part 1. Two theorems are then proved which show that most, if not all, the individual real numbers that have hitherto interested mathematicians are computable. In part 2 the decision problems for the usual properties of real numbers are shown to be unsolvable. An interesting analogy with the theory of the presentation of semigroups and Thue systems is also given. In part 3 an unavoidable non-effectiveness in the theory of computable numbers is discussed.

Many of the results given here are not new, though earlier proofs are much longer. This paper requires no previous knowledge of its subject, but in consequence is somewhat imprecise.

PART I. THE CLASS C OF COMPUTABLE NUMBERS

A real number α is said to be c o m p u t a b l e if it satisfies one of the following requirements:

A) There is an effective rule for writing down the decimal expansion of to arbitrarily many places;

B) There is an effective rule for writing down the regular continued fraction expansion of α to arbitrarily many places;

C) There is a sequence $\{r_n\}$ of rationals satisfying:

   1) One can effectively generate r_n,

   2) $\{r_n\}$ converges to α,

   3) For any positive integer n, one can effectively find an n^+ such that: $|r_l - r_m| < 10^{-n}$ for all $l,m > n^+$;

D) α is defined by an effective Dedekind "cut" i.e. by a partition of the rationals into two non-empty, mutually disjoint classes X, Y such that:

1) Every element of X is smaller than every element of Y,

2) One can effectively tell whether an arbitrary rational is in X or in Y;

E) There is a nested sequence $\{[l_i, r_i]\}$ of closed intervals in the rationals satisfying:

1) For every i, $l_i \leqslant \alpha \leqslant r_i$,

2) The length of the intervals tends to 0,

3) One can effectively generate the sequences $\{l_i\}$, $\{r_i\}$;

F) There is a sequence of positive natural numbers $\{m_i\}$ such that:

1) One can effectively generate $\{m_i\}$,

2) For every i, $\left|\alpha - \frac{m_i}{i}\right| < \frac{1}{i}$.

C) and D) respectively are the constructive equivalents of the Cantor and Dedekind definitions of the real numbers R. It is a remarkable fact that if a real number enjoys any one of the above properties, it enjoys them all.

The class C of computable numbers is denumerable, so almost all real numbers fail to be computable. Nevertheless it is difficult, if not impossible, to find a non-computable real number. Cantor's diagonalization procedure for example does not work as one cannot effectively list ALL computable numbers. The usual long division algorithm insures that C contains every rational number.

T h e o r e m 1. If function $f : R^K \longrightarrow R$ and open interval $\Omega \subset R^K$ satisfy:

a) f restricted to Ω is continuous and monotone in each argument,

b) for every K-tuple $< d_1 \ldots d_K >$ of finite decimals in Ω, one can effectively compute $f(d_1 \ldots d_K)$ then $f(\alpha_1 \ldots \alpha_K)$ is a computable number for every K-tuple $< \alpha_1 \ldots \alpha_K >$ of computable numbers in Ω.

P r o o f : For each positive integer n and for $i = 1, 2, \ldots, n$ we define d_{im} as the m-place decimal that agrees with α_i at the first m decimal places, and the "m-arguments" as the $\langle y_1 \ldots y_K \rangle$ such that y_i is either d_{im} or $d_{im} + 10^{-m}$ (+ if d_{im} positive, - otherwise) for each i. As Ω is open, the m-arguments all lie in Ω for sufficiently large m - say $m > 1$ - and one can effectively compute the corresponding values of f. Consider the following process ρ started on any integer n :

I) Set $n^* = \max\ n,1$ and $m = 1 + 1$;

II) Compute the value of f for each of the 2^K m-arguments;

III) If these values do not agree on the first n^* decimal places then increase n by 1 and return to step II; otherwise present the common n^{th} decimal and stop.

If $\alpha = f(\alpha_1, \ldots, \alpha_K)$ is not a finite decimal, continuity ensures that ρ stops for every n and monotony ensures that it presents the n^{th} decimal of α. If α is a finite decimal the theorem is obviously true; however ρ may not stop for sufficiently large n, so our proof is not constructive.

Now we can assert that:

C is closed under addition, subtraction, division, multiplication, exponentiation, root extraction and the taking of logarithms.

In particular $e = \exp 1$ is computable.

T h e o r e m 2 . If $f : R^K \longrightarrow R$ is a continuous function whose sign can be computed effectively at any finite decimal that is not a root, then all simple roots of f are computable.

P r o o f : It suffices to consider the case of a simple root α that is not a finite decimal. As $x \to -x$ satisfies the requirement of theorem

1, we can assume that α is positive. Since α is isolated there is an 1-place finite decimal d such that α is the only root of f in $< d, d + 10^{-1} >$. Consider the following process Q, started on any integer n :

a) Set $n^* = \max \{1, n\}$;

b) Compute the sign of $f(d')$ for $d' = d, d + 10^{-n^*}, d + 2.10^{-n^*}, d + 3.10^{-n^*}, \ldots, d + 10^{-k}$;

c) Present the n^{th} decimal of the d' just before the first (and only) sign change.

By Wierstrass' theorem, Q stops and presents the n^{th} decimal of α for every n. If α is a finite decimal and n is sufficiently large, this process may never stop so the proof is not constructive.

C o r o l l a r y 2 a . All the roots of a polynomial with computable coefficients are computable. In particular all algebraic numbers are computable.

C o r o l l a r y 2 b . $x \to \sin x$ satisfies the requirements so π is computable.

Combining theorems 1 and 2 we also have:

C is closed under the circular, hyperbolic, inverse circular and inverse hyperbolic functions.

PART II. PROPERTIES OF COMPUTABLE NUMBERS

There is a close analogy between the way in which a computable number is given by a rule for writing down its decimal expansion, and that in which a semigroup is presented by a Thue system. Just as finite semigroups

can be given by a multiplication table whilst infinite semigroups require a set of defining relations, so finite decimals can be written down directly whilst infinite decimals must be given by a rule. Just as not all semigroups can be presented by Thue systems, so not all real numbers are computable.

A. Markov ((1,3)) has shown that one cannot effectively tell whether or not a given pair of Thue systems present isomorphic semigroups. The analogue of this is:

T h e o r e m 3 . One cannot effectively tell whether or not two computable numbers are equal.

P r o o f : E.L. Post ((5)) has described an infinite set K of positive integers such that:

1) One can effectively generate K ,
2) K has an unsolvable decision problem, i.e. one cannot effectively tell whether or not a given integer is in K .

For any positive integer n let P_n denote the following process:

Suppose we start on j ;

a) Generate the first j elements of K ,
b) If n occurs amongst these elements, then present 1 and stop, else present 0 and stop.

This process enables one to write down the decimal expansion of a computable number α_n . But

$$\alpha_n = 0 \quad \text{if and only if} \quad n \in K$$

If we could effectively tell whether or not two processes compute the same number, then for any n we could effectively tell whether or not P_n

computed the same number as a process for writing 0.00000 ...., and so whether or not n is in K. But this is ruled out by the definition of K since then we could derive a version of the Liar Paradox.

Most interesting properties P of semigroups - for example "being Abelian" - are "Markov properties" in the following sense:

1) There is a Thue system $\mathcal{T}$, that presents a semigroup enjoying P;
2) There is a Thue system that presents an inhibiting semigroup S^*, i.e. if S^* can be embedded in a finitely presented semigroup S, then S does not enjoy P;
3) P is preserved under isomorphisms.

The natural analogue of this is:

A property P of real numbers is said to be p s e u d o - M a r k o v if

1) P is non-trivial, i.e. there is a computable number α_p that enjoys P;
2) There is an inhibiting computable number α_p^* such that no number, differing from α_p^* at only a finite number of decimal places, enjoys P.

For each Markov property P of semigroups, Markov ((2,4)) has proved that one cannot effectively tell whether or not the semigroup presented by a given Thue system enjoys P. Analogously we have:

T h e o r e m 4. For no pseudo-Markov property P of real numbers can one effectively tell whether or not a computable number enjoys P.

P r o o f : For any positive integer n, let Q_n be the following process:

a) Start on j;

b) Generate the first j element of K ;

c) If n occurs amongst these elements then present the digit in the j^{th} decimal place of α^{*}_{p} and stop; otherwise present the digit in the j^{th} decimal place of α_{p} .

Q_n enables us to write the decimal expansion of a number α_n such that: α_n enjoys P if and only if $n \in K$. As the decision problem of K is unsolvable, one cannot effectively tell whether or not Q_n computes a number enjoying P .

But how useful is this result? Clearly "being zero", "being an integer", and "being a prime" and the like are pseudo-Markov properties. We also have

T h e o r e m 5 . If P is a property of computable numbers satisfying:

a) One can effectively generate all computable numbers that enjoy P ,

b) If a enjoys P and d is a finite decimal then $a + d$ enjoys P ,

c) At least one computable number enjoys P ,

then P is pseudo-Markov.

P r o o f : It suffices to prove that there is a computable number that does not enjoy P . Such a number is computed by the following process:

Start on any j ,

a) Generate the digit in the $(j + 1)^{st}$ decimal place of the $(j + 1)^{st}$ computable number that enjoys P ,

b) If this digit is 5 then present 6 and stop; otherwise present 5 and stop.

So "being a finite decimal", "being rational" and "being algebraic" are pseudo-Markov properties of computable numbers. If one could solve the decision problem for any one of the properties satisfying theorem 5, one

could solve them all and also such problems as:

Are two given computable numbers equal?

Is a given computable number an integer?

Is a given computable number 0 ?

Is a given computable number positive?

If one could solve any of the problems just listed then one could solve them all, but still be unable to solve the decision problem for any property satisfying theorem 5. In other words the listed problems, though unsolvable, are of a lower degree of unsolvability than the theorem 5 decision problems.

It is not yet known whether Euler's constant $\gamma = \lim_{n\to\infty} (\sum_{v=1}^{n} \frac{1}{v} - \log n)$ is rational or irrational. According to theorem 4, one cannct hope to resolve this by finding a general method for deciding the rationality of every computable number (γ is computable). Naturally one can still hope to solve the problem using some method that does not apply to all computable numbers.

PART III. OPERATIONS ON COMPUTABLE NUMBERS

A function f can be computable in the sense that it has computable values for computable arguments and yet non-effective in the sense that one cannot give a general rule for computing its value. Furthermore the effectiveness or otherwise of a computable function depends on which of A, B, C, D, E or F we choose to be the "official" definition of a computable number.

T h e o r e m 6 . There is no effective way of finding a rule for writing down the decimal expansion of a real number that is computable under definition C .

P r o o f : For each positive integer n , we can effectively generate

the sequence $\{r_i^n\}$ of rationals defined by:

$$r_i^n = \begin{cases} 0 & \text{if } n \text{ is amongst the first } i \text{ elements of } K \\ 1 & \text{otherwise} \end{cases}$$

If $n \in K$ we can take 1 as n^* otherwise we can take "the number of elements of K that one has to generate before meeting n" as n^*, so the limit of r_i^n is computable under definition C.

If one could effectively find the integral part i of this limit, one could solve the decision problem of K since $i = 0$ iff $n \in K$.

For the next theorem we need to assign distinct numbers to every expression that can be formulated in a given language (possible in all languages with only denumerably many letters). For expressions that describe a function f from the natural numbers to the natural numbers, this number $\hat{f}$ is said to be the Gödel number of f.

T h e o r e m 7. If A is chosen as the official definition of a computable number then addition is not effective.

P r o o f : For each effective function f, we can give rules for writing down the decimal expansions of the numbers

$d_f = +d_o . d_1 d_2 \ldots$, $d_f^* = +d_o^* . d_1^* d_2^* \ldots$ defined by

$$d_i = \begin{cases} 0 & \text{if } f \text{ stops within } i \text{ steps when started on } \hat{f}, \\ & \quad f(\hat{f}) = 1 \quad \text{and} \quad i \geqslant 1 \\ 9 & \text{otherwise} \end{cases}$$

$$d_i^* = \begin{cases} 2 & \text{if } f \text{ stops within } i \text{ steps when started on } \hat{f}, \\ & \quad f(\hat{f}) = 0 \quad \text{and} \quad i \geqslant 1 \\ 0 & \text{otherwise} \end{cases}$$

If one could effectively find the integral part of $d_f + d_f^*$ then one could effectively describe the function ϕ satisfying:

a) ϕ is defined for every natural number,

b) ϕ takes on only the values 0 and 1 ,

c) If i is the Gödel number of a function ψ such that $\psi(i) = 1$, then $\phi(i) = 0$,

d) If i is the Gödel number of a function ψ such that $\psi(i) = 0$, then $\phi(i) = 1$.

But if ϕ were effective, we could take $\hat{\phi}$ for i and derive a contradiction.

Similar proofs show that subtraction, division, multiplication, exponentiation, extraction of roots and the taking of logarithms are also non effective. Moreover for any computable number α one can show that $x \to x + \alpha$, $x \to x - \alpha$, and $x \to x/\alpha$ (for $\alpha \neq 0$) are effective if and only if α is a finite decimal. Thus doubling but not trebling is effective. If we had chosen to work with ternary instead of decimal expansions, the opposite would have been true. Such dependence on the number base can occur, as conversion from base p to base q is only effective when q divides a power of p .

References

((1)) A. Markov: Impossibility of certain algorithms in the theory of associative systems. (In Russian) Dokl. Akad. Nauk SSSR, 77 (1951) 19-20.

((2)) A. Markov: Impossibility of algorithms for recognizing some properties of associative systems. (In Russian) Dokl. Akad. Nauk SSSR 77 (1951) 953-956.

((3)) A. Mostowski: Review of 1 . J. Symb. Logic 16 (1951) 245.

((4)) A. Mostowski: Review of 2 . J. Symb. Logic 17 (1952) 151.

((5)) E.L. Post: Recursively enumerable sets of positive integers and their decision problems. Bull. Amer. Math. Soc. 50 (1944) 284-316.