LARGE NUMBERS AND UNPROVABLE THEOREMS

JOEL SPENCER
Department of Mathematics, State University of New York, Stony Brook, NY 11794

"Yes, please," said Milo. "Can you show me the biggest number there is?"

"I'd be delighted," [the Mathemagician] replied, opening one of the closet doors. "We keep it right here. It took four miners just to dig it out."

Inside was the biggest

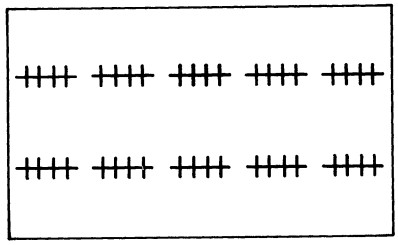
3

Milo had ever seen. It was fully twice as high as the Mathemagician.

—*The Phantom Tollbooth*
Norton Juster

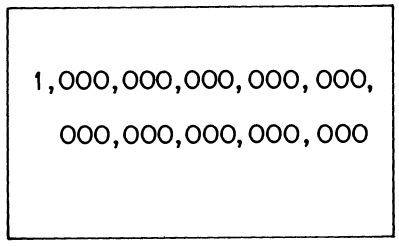
1. Large Numbers. "Describe, on a 3 × 5 card, as large a positive integer as you can."

Many mathematicians have at some time played the game above, either solitaire or in competition. My solutions in the second, sixth, and twelfth grades, respectively, are shown in Figs. 1, 2, 3.



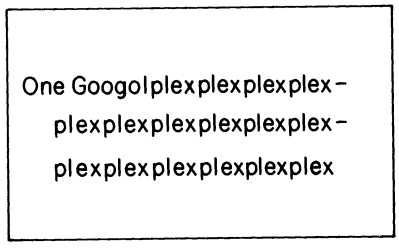
WARP 0

FIG. 1.



WARP 1

FIG. 2.



WARP 2

FIG. 3.

See this MONTHLY, 90 (1983)365, for the author's biography.

The last needs a word of explanation. Since googol is 10^{100} and googolplex is 10^{googol} let us define Nplex as 10^N. Actually, by twelfth grade I could write "One googolplexplexplex... with a googol plexes" and even some more elaborate variants. These were at best WARP 2.2. The next level is shown in Fig. 4.

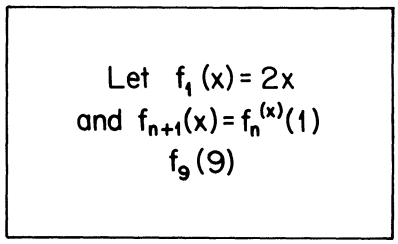


FIG. 4.

Here $f^{(x)}$ represents the xth iterate of f. Iterated doubling is exponentiation, $f_2(x) = 2^x$. Iterated exponentiation is the tower function,

$$f_3(x) = 2^{2^{\cdot^{\cdot^{\cdot^{2}}}}} \quad \text{with } x \quad 2\text{'s.}$$

My WARP 2 solution is approximately $f_3(21)$, one for each plex and five to get to a googol. There is no word for f_4. $f_4(4) = f_3(f_3(f_3(f_3(1)))) = f_3(f_3(4)) = f_3(65536)$ is already WARP 2.1.

Three ideas help us create large numbers. First, we concentrate on constructing rapidly growing functions. The numbers will then be the value of the function $f(x)$ for some reasonably small x. Second, we use iteration to build a larger function from a given one. Third, we introduce diagonalization. Having defined the functions f_n above, we define a diagonal function, called f_ω, by

$$f_\omega(n) = f_n(n).$$

This is called the Ackermann function. (There are several similar formulations.) The Ackermann function does occasionally appear in "real" mathematics. For example, van der Waerden proved in 1927 that to all n there exists $W(n)$ such that if the integers from 1 to $W(n)$ are divided into two classes, then there exists an arithmetic progression of length n in one of the classes. His proof gave a $W(n)$ roughly equal to $f_\omega(n)$. (It is possible that far smaller $W(n)$, even of exponential order, will suffice and this remains an open problem.)

Once $f_\omega(n)$ is defined, there is no reason to stop. We define a new function, let's call it $f_{\omega+1}$, by $f_{\omega+1}(n) = f_\omega^{(n)}(1)$. Having defined $f_{\omega+1}$, we may define $f_{\omega+2}, f_{\omega+3}, \ldots$. When faced with ellipses we resort to diagonalization. We define a new function, called $f_{2\omega}$, by $f_{2\omega}(n) = f_{\omega+n}(n)$. (See Fig. 5.)

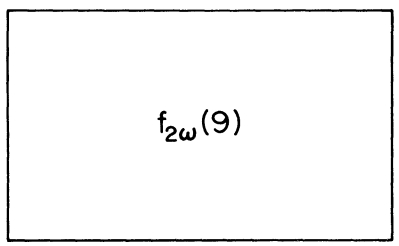


FIG. 5.

We are defining here a hierarchy of functions in which each function has an immediate successor and where limit functions are defined by diagonalization of an appropriate subsequence. The usual representation for ordinal numbers provides a perfect framework in which to do this. The ordinals $\alpha < \omega^\omega$ have a simple representation. Each such α may be uniquely written

$$\alpha = a_1\omega^{s_1} + a_2\omega^{s_2} + \cdots + a_r\omega^{s_r} \qquad (\omega > s_1 > s_2 > \cdots > s_r \geqslant 0)$$

where the a_i are positive integers. (We write $a\omega^s$ instead of the more customary $\omega^s a$ for convenience of expression.) The limit ordinals are those α with $s_r > 0$. For these we define a specific "natural" sequence $\alpha(n)$ of ordinals approaching ω^ω by

$$\alpha(n) = a_1\omega^{s_1} + \cdots + a_{r-1}\omega^{s_{r-1}} + (a_r - 1)\omega^{s_r} + n\omega^{s_r - 1}.$$

For example, if $\alpha = 2\omega^4 + 3\omega^3$, then $\alpha(n) = 2\omega^4 + 2\omega^3 + n\omega^2$. We define the natural sequence approaching ω^ω by

$$\omega^\omega(n) = \omega^n.$$

Now we define $f_\alpha(n)$ for each $\alpha \leqslant \omega^\omega$ using transfinite induction by

$$(+) \qquad f_{\alpha+1}(n) = f_\alpha^{(n)}(1),$$

$$(++) \qquad f_\alpha(n) = f_{\alpha(n)}(n),$$

where α is a limit ordinal and the initial value $f_1(n) = 2n$. (See Fig. 6.)

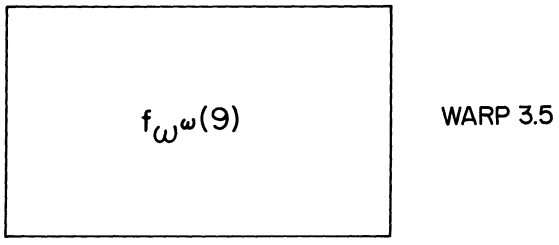


FIG. 6.

Let us emphasize that though we are using the language of infinite ordinals the functions f_α are recursive functions and the values $f_\alpha(t)$ are well-defined integers. The infinite ordinals are, in one sense, merely finite sequences of positive integers being manipulated in particular ways. A recursive program for computing $f_\alpha^{(t)}(n)$ could take the following form.

```
FUNCTION F(α, N, T)
BEGIN
IF T > 1,
        SET X = F(α, N, T − 1)
        RETURN F(α, X, 1)
IF T = 1 AND α = 1
        RETURN 2*N
IF T = 1 AND LIMITORDINAL (α)
        RETURN F(α(N), N, 1)
IF T = 1 AND NOT LIMITORDINAL (α)
        RETURN F(α − 1, 1, N)
END
```

The representation of α, the predicate LIMITORDINAL (α), and the functions $\alpha - 1$ and $\alpha(N)$ need to be defined explicitly, though we do not do so here.

We continue the ordinals a half-WARP further. Set

$$\omega_1 = \omega, \omega_2 = \omega^\omega, \ldots, \omega_{s+1} = \omega^{\omega_s}, \ldots$$

and set ε_0 equal the limit of the ω_s. (We emphasize that ω_1 is *not* the first uncountable ordinal. All ordinals in this paper are countable.) Each ordinal $\alpha < \omega_{s+1}$ is uniquely represented as

$$\alpha = a_1\omega^{\beta_1} + \cdots + a_r\omega^{\beta_r} \qquad (\omega_s > \beta_1 > \beta_2 > \cdots > \beta_r \geqslant 0)$$

with the a_i positive integers. A "typical" ordinal is

$$7\omega^{\omega^{2\omega+1}} + 14\omega^{3\omega^{\omega+8}+5\omega^\omega}$$

Now for limits. We say $n\omega^\beta$ is the natural sequence approaching $\omega^{\beta+1}$. If β itself is a limit ordinal, then its limit sequence $\beta(n)$ has already been defined and we call $\omega^{\beta(n)}$ the natural sequence approaching ω^β. For sums we keep all but the smallest term fixed and take a limit sequence approaching that smallest term. Thus

$$7\omega^{\omega^{2\omega+1}} + 13\omega^{3\omega^{\omega+8}+5\omega^\omega} + \omega^{3\omega^{\omega+8}+4\omega^\omega+\omega^n}$$

is the natural sequence for the ordinal above. Finally, ε_0 has the natural sequence $\varepsilon_0(n) = \omega_n$. Now the hierarchy f_α defined by $(+)$, $(++)$ may be extended to all $\alpha < \varepsilon_0 + \omega$. We have a big number. (See Fig. 7.)

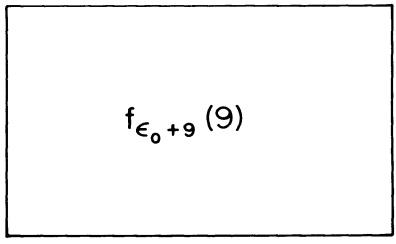


FIG. 7.

This should win the game against any nonlogician!

2. The Connection. Let PA stand for Peano Arithmetic, that first order theory of numbers which includes the basically finitistic methods of number theory. The surprising truth is that WARP 4 lies beyond the scope of PA. The sense in which we use this was shown by G. Kreisel [4] in 1952.

A statement $P(x_1,\ldots,x_r)$ is called provably recursive if there is an algorithm for deciding if $P(x_1,\ldots,x_r)$ is true and a proof, in PA, that the algorithm always terminates. Thus $P(x, y, z, t)$: $x^t + y^t = z^t$ is provably recursive (simply make the calculation) but

$$P(t)\colon (Ex)(Ey)(Ez)x^t + y^t = z^t$$

is not known to be provably recursive.

We say a function f dominates a function g if there exists n such that $f(x) > g(x)$ for all $x > n$.

Let $P(x, y)$ be a provably recursive statement in PA and suppose $(x)(Ey)P(x, y)$ is provable in PA. Set $f_P(x)$ equal the least y such that $P(x, y)$ is true. Then, Kreisel showed, the function f_P is dominated by f_α for some $\alpha < \varepsilon_0$. As f_{ε_0} dominates all previous f_α we draw the following conclusion.

> Let $(x)(Ey)P(x, y)$ be a statement of PA which is true for the natural numbers and let $f_P(x)$ be the least y for which $P(x, y)$ is true. Suppose $P(x, y)$ is provably recursive. If f_P dominates f_{ε_0}, then the statement $(x)(Ey)P(x, y)$ is unprovable in PA.

3. An Unprovable Theorem.* The epochal work of Kurt Gödel gave the existence of statements in PA which are true for the natural numbers but unprovable in PA. The statements constructed by Gödel suffered the defect of being unnatural and for the past half century a somewhat raggedy debate ensued concerning whether or not Gödel's result applied to statements of real mathematical interest. In 1977 Jeff Paris and Leo Harrington [2] gave the first natural example of a statement that was true for the integers and unprovable in PA. (The term "natural" is here a matter of subjective opinion.) Their statement comes from Ramsey Theory, a subdisci-

*The term "unprovable theorem" is abhorred by logicians. Theorems have proofs by definition. For our informal discussion, however, it seems appropriate to the subject matter to use this delightful oxymoron.

pline of Combinatorial Analysis, and to give it one needs a moment's introduction to that subject. (A detailed treatment is given in [1].)

By "an r-coloring of the k-sets of S" we mean a function χ with domain the family of k-element subsets of S and range $[r]$. (Notation: $[a, b] = \{a, a+1, \ldots, b\}, [r] = [1, r], [a, b) = [a, b-1]$.) Given such a coloring χ a set $B \subset S$ is called monochromatic if all of the k-element subsets of B have the same color.

We may state Ramsey's Theorem in either a finite or an infinite form.

RAMSEY'S THEOREM (*Infinite Form*). *For all k, r given any r-coloring of the k-sets of N, there exists a monochromatic infinite set B.*

RAMSEY'S THEOREM (*Finite Form*). *For all k, r, t there exists n so that given any r-coloring of the k-sets of $[n]$, there exists a monochromatic t-set B.*

From the infinite form of Ramsey's Theorem we deduce the finite form as follows. Suppose the finite form false and fix k, r, t so that for all n there exists an r-coloring of the k-sets of $[n]$ with no monochromatic t-set B. Any coloring for a larger n also works for a smaller one. Hence, for any given n, there is some coloring which can be extended to arbitrarily large n. Construct colorings for successively larger values of n in turn, each of which extends to arbitrarily large n. The union is an r-coloring of the k-sets of N with no monochromatic t-set B. Thus the infinite form of Ramsey's Theorem would be false. The reasoning above, often called a Compactness Argument, can be applied in many situations to reduce an "infinite form" to a "finite form," see, e.g., [1].

Define a set S of positive integers to be large if $|S| > \min(S)$. For example, $\{3,4,7,9\}$ is large but $\{4,63,1281,4504655\}$ is not. The statement of Paris and Harrington (in one version) requires a seemingly minor modification of Ramsey's Theorem.

(PH) *For all k, r there exists n so that given any r-coloring of the k-sets of $[k+1, n]$ there exists a large monochromatic $B \subset [k+1, n]$.* (The exclusion of $1, \ldots, k$ is purely technical, avoiding such trivial large sets as $\{2,3,4\}$.)

If we allow infinitistic techniques, (PH) is relatively simple to prove. Suppose (PH) is false for a particular k, r. By the Compactness Argument there would exist an r-coloring χ of the k-sets of $[k+1, \infty)$ with no large monochromatic finite B. However, given any such χ the infinite form of Ramsey's Theorem guarantees the existence of an infinite monochromatic set C. The first $\min(C)+1$ elements of C then give a large monochromatic finite B.

We have deduced both Ramsey's Theorem (finite form) and (PH) from Ramsey's Theorem (infinite form). Neither of these arguments is formalizable in PA since neither Ramsey's Theorem (infinite form) nor the Compactness Argument can even be stated in PA. This, by itself, does not show that Ramsey's Theorem (finite form) or (PH) are unprovable in PA, only that we have not proven them. In fact, Ramsey's Theorem (finite form) can be proven in PA (though we do not prove it here) but (PH) cannot.

Paris and Harrington, in their original work, showed by model-theoretic arguments that (PH) was unprovable in PA. Robert Solovay, hearing of their result but not of their proof, discovered a more combinatorial argument. Let $\mathrm{PH}(k, r)$ be the least n such that for every r-coloring of the k-element subsets of $[k+1, n]$ there exists a monochromatic large B. Solovay showed that PH grows too fast for PA.

A full discussion of Solovay's argument is somewhat beyond the bounds of this expository discussion (though not by too much, see [1] or the original [3]), but we can quite easily demonstrate that $\mathrm{PH}(2, r)$ grows quite rapidly. (A similar exposition was given by Smoryński [5].) To find a lower bound for $\mathrm{PH}(2, r)$ we give explicit r-colorings of the 2-sets of $[3, n]$.

Split $[3, \infty)$ into consecutive intervals of the form $[x, 2x)$—i.e., $[3,6), [6,12) [12,24), [24,48), \ldots$. We give the pair $\{i, j\}$ color 1 if i and j lie in a common interval. If all pairs in a set

$A = \{a_1,\ldots,a_s\}$ have color 1, then $A \subset [x,2x)$, so $|A| \leqslant x$ and $\min(A) \geqslant x$, hence A is not large. Set $g_1(x) = 2x$. Now we define $g_2(x) = g_1^{(x)}(x) = x2^x$ and split $[3,\infty)$ into consecutive intervals of the form $[x, g_2(x))$—that is,

$$[3,24), [24,24\cdot 2^{24}), [24\cdot 2^{24}, 24\cdot 2^{24}\cdot 2^{24\cdot 2^{24}}),\ldots.$$

We give a pair $\{i, j\}$ color 2 if i and j lie in a common interval and the pair does not have color 1. If all pairs in a set $A = \{a_1,\ldots,a_s\}$ have color 2, then $A \subset [x, g_2(x))$, which is split into x subintervals. Each element of A lies in a separate subinterval (since no pair has color 1) so $|A| \leqslant x$ and A is not large. On $[3, g_2(3))$ all 2-sets have either color 1 or 2 and there are no monochromatic large sets. Thus

$$\mathrm{PH}(2,2) \geqslant g_2(3) = 24.$$

We continue in this manner, defining $g_{s+1}(x) = g_s^{(x)}(x)$, partitioning $[3,\infty)$ into consecutive intervals of the form $[x, g_{s+1}(x))$, and giving a pair $\{i, j\}$ color $s+1$ if i and j lie in a common interval and the pair has not been given a smaller color. Then, quite explicitly, we have shown

$$\mathrm{PH}(2,3) \geqslant g_3(3) = 24\cdot 2^{24}\cdot 2^{24\cdot 2^{24}}$$

and, in general, $\mathrm{PH}(2, r) \geqslant g_r(3)$. The function $g_r(3)$ has order roughly $f_\omega(r)$.

The colorings of k-sets are equally explicit but require a greater technical effort. Solovay showed that $\mathrm{PH}(3, r)$ is bounded from below by $f_\alpha(r)$ where $\alpha = \omega^\omega$, $\mathrm{PH}(4, r)$ by $f_\alpha(r)$ where $\alpha = \omega^{\omega^\omega}$, etc., and that $\mathrm{PH}(r, r)$ was bounded from below by $f_{\varepsilon_0}(r)$. (Though we do not require it here, Ketonen found upper bounds on these functions of roughly the same order.)

Let $P(k, n)$ be the statement "Given any k-coloring of the k-sets of $[k+1, n]$ there exists a large monochromatic B." $P(k, n)$ is surely provably recursive as one may check all k-colorings of the k-sets of $[k+1, n]$. Applying Kreisel's fundamental result the statement

$$(k)(En)P(k,n)$$

is unprovable in PA.

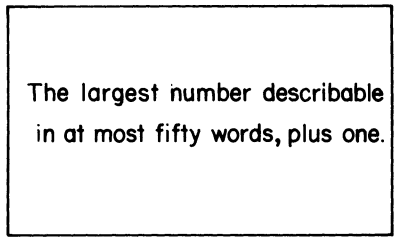
4. Reflections. WARP 4 takes us to the tradeoff between largeness and definiteness. We have described an algorithm for computing $f_\alpha(t)$—but how do we know that the algorithm will work (i.e., terminate)? One way is by transfinite induction, the determination of $f_\alpha(t)$ requires t calls of the algorithm to calculate $f_{\alpha-1}$ or, if α is a limit ordinal, the algorithm for $f_{\alpha(t)}$. In either case these are smaller ordinals, by induction the algorithm works for them, hence the f_α algorithm works. However, transfinite induction is a basically infinitistic tool and we can ask for a proof in PA that the algorithm for f_α will work. Here there is a very nice result. For $\alpha < \varepsilon_0$ there is such a proof in PA. However, for $\alpha = \varepsilon_0$ there is no proof in PA that the algorithm will always work. (This gives another statement which is true but unprovable, but one that would hardly be termed natural.)

We would agree that the number described in Fig. 8 is not legitimate as it stands. It gives, in fact, Berry's paradox, one of the classic Russell-type paradoxes. Since this number has been described in less than 50 words, it must be greater than itself. The problem lies in the notion of describable. Let us say that a number m is describable (modulo PA) in length n if there is a statement $A(x)$ in PA such that

(i) $(E_1x)A(x)$ has a proof in PA of length at most n. (E_1 = "there exists a unique.")
(ii) There is an algorithm for deciding $A(x)$ and a proof in PA of length at most n that the algorithm always terminates.
(iii) $A(m)$.

We construct a legitimate alternative (see Fig. 9). This number cannot be described by a book the size of the known universe, with electrons for characters, in the language of PA. The function g lies beyond PA—but just barely. It is of order f_{ε_0} and the above card is still WARP 4.

To go beyond WARP 4 we strengthen PA. Let GAM be a formalization of Generally Accepted Mathematics. (See Fig. 10.)



WARPED

FIG. 8.

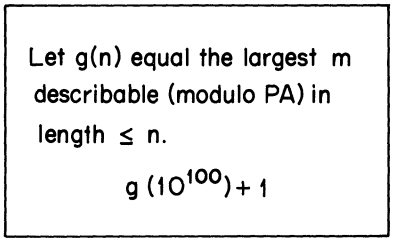
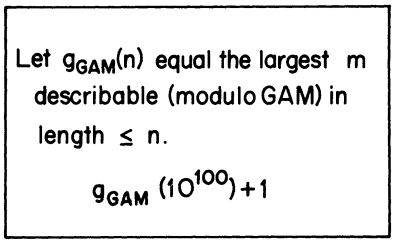


FIG. 9.



WARP 5 (?)

FIG. 10.

Travel beyond WARP 4 now depends on what one allows in GAM. There is always the danger that if too much is allowed, the system will become inconsistent and the 3 × 5 card will no longer define an integer. The game of describing the largest integer, when played by experts, lapses into hopeless argument over legitimacy.

References

1. R. L. Graham, B. L. Rothschild, and J. H. Spencer, Ramsey Theory, Wiley, New York, 1980.
2. J. Paris and L. Harrington, A Mathematical Incompleteness in Peano Arithmetic, in Handbook of Mathematical Logic (J. Barwise, Editor), North-Holland, 1977, 1133–1142.
3. J. Ketonen and R. Solovay, Rapidly growing Ramsey functions, Ann. of Math., 113 (1981)267–314.
4. G. Kreisel, On the interpretation of nonfinitistic proofs, II, J. Symbolic Logic, 17 (1952)43–58.
5. C. Smoryński, Some rapidly growing functions, Math. Intelligencer, 2 (1980)149–154.

MISCELLANEA

116.

The condensation of metaphor involves no denial of logic: it is simply an extension of the implications of grammar, the development of a notation which, being less cumbersome, enables us to think more easily. It may be compared to the invention of a new notation, say that of Leibniz or Hamilton, in mathematics: the new is defined in terms of the old, it is a shorthand which must be learned by patient effort, but, once learnt, it makes possible the solution of problems which were too complicated to attack before. The human head can only carry a certain amount of notation at any one moment and poetry takes up less space than prose.

–Michael Roberts, *The Faber Book of Modern Verse*, London, Faber and Faber, 1937, p. 20.