NOTES

Edited by **William Adkins**

A Modified Problem of Pillai and Some Related Questions

G. E. Hardy and M. V. Subbarao

In memoriam: S. S. Pillai (1901–1950) on the occasion of his birth centenary.

1. INTRODUCTION. The famous number theorist of India S. S. Pillai (whose name Paul Erdős always delighted in saying in full: Subbayya Pillai Sivasankaranarayana Pillai) posed the following problem more than seven decades ago [2].

1.1. Problem. Is it true that every prime divisor of $n! + 1$ is of the form $1 (\mathrm{mod}\, n)$?

S. Chowla [2] remarked that there are at least two exceptions provided by

$$14! + 1 \equiv 0(\mathrm{mod}\, 23); \quad 18! + 1 \equiv 0(\mathrm{mod}\, 23),$$

in view of $23 \not\equiv 1(\mathrm{mod}\, 14)$ and $23 \not\equiv 1(\mathrm{mod}\, 18)$, and suggested further investigation.

Actually, the smallest n for which we have a counterexample is provided by

$$8! + 1 \equiv 0(\mathrm{mod}\, 61), \quad \equiv 0(\mathrm{mod}\, 661),$$

in view of 61 and 661 being primes $\not\equiv 1(\mathrm{mod}\, 8)$. On the other hand, if we confine ourselves to those integers n for which $n! + 1$ is a prime (such primes are sometimes called factorial primes), then the answer to the question raised in Problem 1.1 is, trivially, affirmative. We do not know if there are infinitely many factorial primes. The largest known factorial prime is, to our knowledge, $32659! + 1$ (44416 digits). This was found in the year 2000 by Steven L. Harvey, Prime Form (visit http://www.utm.edu/research/primes/largest.html).

Pillai's question did not attract any further attention until 1993 when, in correspondence with P. Erdős, we formulated the following problems.

1.2. Problem. Are there infinitely many primes p for which there is an integer n such that

$$n! + 1 \equiv 0(\mathrm{mod}\, p), \quad p \not\equiv 1(\mathrm{mod}\, n)? \tag{1.3}$$

1.4. Problem. Are there infinitely many integers n for which there is a prime p satisfying (1.3)?

Astonishingly simple, but rather tricky solutions were found in 1993 by Paul Erdős and independently by the second author. We recently found another simple proof, which we give in the next section. Section 3 lists several unsolved problems and the final section is an appendix with extracts from two of Erdős's letters to the second author. It also gives a table of values pertinent to Problem A in Section 3.

2. THE THEOREMS.

We first prove:

2.1. Theorem. *There are infinitely many primes p such that there is an integer n for which*

$$n! + 1 \equiv 0 (\bmod p), \quad p \not\equiv 1 (\bmod n). \tag{2.2}$$

A detailed proof. For each integer $K = 1, 2, 3, \ldots,$ consider the largest prime p for which the following congruence holds:

$$(10K + 7)! + 1 \equiv 0 (\bmod p). \tag{2.3}$$

Clearly, for each value of K, there is a larger value of K for which the corresponding primes p are different.

If $p \not\equiv 1 (\bmod 10K + 7)$ for infinitely many K, we are done. But if $p \equiv 1 (\bmod 10K + 7)$ for a particular value of K, then we can write, for some even integer $A > 0$,

$$p = 1 + A(10K + 7). \tag{2.4}$$

Wilson's theorem on primes says that

$$(p - 1)! + 1 \equiv 0 (\bmod p). \tag{2.5}$$

We now split $(p - 1)!$ into two factors, the first of which is $(p - 10K - 8)!$, so that the second factor is the product

$$(p - (10K + 8) + 1)\,(p - (10K + 8) + 2) \cdots (p - (10K + 8) + 10K + 7)\,.$$

This product is clearly congruent modulo p to $(-10K - 7) \cdots (-10K + (10K - 1))$, that is, to $(-1)^{10K+7}(10K + 7)!$.

Hence using (2.5), we have

$$(p - 10K - 8)!\,(10K + 7)! \equiv 1 (\bmod p),$$

which, on using (2.3), gives

$$(p - 10K - 8)! + 1 \equiv 0 (\bmod p). \tag{2.6}$$

Note that

$$p \not\equiv 1 (\bmod p - 10K - 8), \tag{2.7}$$

for, if $p \equiv 1 (\bmod p - 10K - 8)$, then

$$p = 1 + B(p - 10K - 8)$$

for some integer $B > 1$, and using the value of K given by (2.4) would lead to

$$1 + A(10K + 7) = 1 + B\,(1 + A(10K + 7) - 10K - 8)\,.$$

This would imply that $A = (A - 1)B$, so $A + B = AB$. Since A and B are positive integers, $A = B = 2$. But if $A = B = 2$, (2.4) gives $p = 1 + 2(10K + 7)$, or

$p = (20K + 15)$, contradicting the fact that p is a prime. In view of (2.6) and (2.7), Theorem 2.1 follows. ■

2.8. Remarks. In the proof of Theorem 2.1, instead of $10K + 7$, we can use any number $aK + b$, where a is even and b odd with the restriction that $\gcd(a, 2b + 1) > 1$. But other choices violating this restriction are possible, such as $6K + 5$; see Section 4.

In response to the second author's letter of April 1993, Paul Erdős replied on June 14, 1993, starting the letter with "the problems you wrote are probably very difficult...", but toward the end of the letter he mentioned a possible solution. He later gave a very concise proof of a few lines. His second proof is similar to our proof of Theorem 2.1.

2.9. Definition. A prime p satisfying the property described in Theorem 2.1 is called a *Pillai prime*. Thus, p is a Pillai prime if there is an n so that $n! + 1 \equiv 0(\bmod p)$, but $p \not\equiv 1(\bmod n)$. The symbol $\mathcal{P}$ denotes the set of all Pillai primes.

The first ten members of $\mathcal{P}$ are 23, 29, 59, 61, 67, 71, 79, 83, 109, and 137.

2.10. Remark. The sequence of Pillai primes is now entered in the Encyclopedia of Integer Sequences; see http://www.research.att.com/~njas/sequences.

2.11. Definition. $\mathcal{S}$ is the set of all those natural numbers m with the property that there is a corresponding prime p satisfying

$$m! + 1 \equiv 0(\bmod p), \quad p \not\equiv 1(\bmod m).$$

The first ten members of $\mathcal{S}$ are:

$$8, 9, 13, 14, 15, 16, 17, 18, 19, 22.$$

We call the members of S *EHS numbers*.

2.12. Theorem. *The set $\mathcal{S}$ is infinite.*

Proof. Suppose $\mathcal{S}$ is a finite set. Let its members be $m_1, \dots, m_r$. Consider the set Q of all primes q satisfying the relation

$$m_i! + 1 \equiv 0(\bmod q), \quad q \not\equiv 1(\bmod m_i)$$

for $i = 1, 2, \dots, r$.

Since the set $\mathcal{P}$ of Pillai primes is infinite by Theorem 2.1, the following is possible. Choose a prime $p \in \mathcal{P}$ such that $p \notin Q$. Since $p \in \mathcal{P}$, there is an integer m such that

$$m! + 1 \equiv 0(\bmod p), \quad p \not\equiv 1(\bmod m).$$

The definition of $\mathcal{S}$ ensures that $m \in \mathcal{S}$. But $m \notin \mathcal{S}$, for if $m \in \mathcal{S}$, p must belong to Q, contradicting the definition of p. Hence Theorem 2.12 follows. ■

2.13. Remark. One can show that Theorem 2.12 directly implies Theorem 2.1.

3. SOME OPEN PROBLEMS. Of the following problems, those marked with an asterisk are original to Erdős. Others, except Problem H, were raised in discussions with him.

A. Let $\pi(x)$ (respectively $\pi(\mathcal{P}, x)$) denote the number of primes (number of Pillai primes) less than or equal to x. Does the ratio $\pi(\mathcal{P}, x)/\pi(x)$ have a limit as $x \to \infty$? From the table in the Appendix, it would appear that if the limit exists, it is perhaps between 0.5 and 0.6. But then there seems to be no reason why the ratio should not tend to 1, even though very slowly and certainly not monotonically.

B. If $f(x)$ denotes the number of *EHS* numbers not exceeding x does $\lim_{x\to\infty} f(x)/x$ exist, and if so, what is it? We have a list of all *EHS* numbers up to 2^{10}, from which we obtained the following:

For $x = 100, 200, 300, 400$, and 500, the corresponding values of $f(x)/x$ are, correct to two decimals, 5.5, 5.25, 5.7, 5.45, and 4.98. If this trend continues, we expect $\lim_{x\to\infty} f(x)/x$ to be around 0.5, if it exists. The frequency with which the *EHS* numbers occur—most often in long sequences of consecutive integers—makes us believe that their asymptotic density exists and is unity. Erdős, though initially hesitant, later agreed with this view. See Section 4, Appendix 4(i).

C. If $g(p)$ denotes the number of integers $n < p$ (p prime) for which $n! + 1 \equiv 0 \bmod p$, is $\overline{\lim}\, g(p) = \infty$? Perhaps $g(p) \to \infty$ for almost all p.

D. For $g(p)$ as in (C), the density of primes p for which $g(p) = k$ probably exists for every k, and denoting this by e_k, $\sum_{k=1}^{\infty} e_k = 1$.

E*. Are there many primes p for which $n! \pmod p$ has $p - 2$ nonzero values? One example is $p = 5$.

The referee remarks: I hazard a guess that $p = 5$ is the only one with residues $1, 2, 1, 4$ ($5 - 2$ different values). $p = 3$ is just an example of the Law of Small Numbers. Theorem 114 of Hardy and Wright shows that any other example must be $\equiv 1 \pmod 4$, and I make a wild surmise that it could be proved that there are not many (more). If that is Erdős phraseology, then he may well have thought the same. The use of "many" (if that is what he used) seems to imply that he thought "a finite number" and a pretty small one at that.

F*. Let $A(x)$ denote the number of composite numbers $u < x$ for which $n! + 1 \equiv 0 \bmod u$. Examples of such numbers are 25, 121, 721. Is $A(x) = o(x^{\varepsilon})$?

G. Given a prime p, let $f(p)$ denote the smallest integer for which $f(p)! + 1 \equiv 0 \pmod p$. We believe that there are infinitely many p for which $f(p) = p - 1$, but probably the number of such $p \le x$ is $o(x/\log x)$.

Erdős believed that $f(p)/p \to 0$ for almost all p.

H. For any given prime $p > 5$, $(p-1)! + 1$ is not of the form p^r, $r > 1$ [**3**]. Thus for all such p, $(p-1)! + 1 \equiv 0 \pmod q$ for some prime or primes $q = q(p) > p$. Are there infinitely many primes p for which there is a corresponding q satisfying $q \not\equiv 1 \pmod{p-1}$? The first four examples of such p, with the corresponding primes q written in parenthesis, are 17(61, 137, 139), 19(23, 29, 61, 67), 37(83, 739, 1483), 41(59, 277). Equivalently, are there infinitely many *EHS* numbers of the form $p - 1$, p being a prime?

We believe that this is so and that the number of such primes $\le x$ is $O(x/\log x)$.

4. APPENDIX.

(i) For those readers who are curious to know Paul Erdős's first and second proofs of Theorem 2.1, we quote part of his letter dated June 14, 1993 and the full text of his letter dated July 2, 1993—both addressed to the second author.

(a) "Perhaps I can prove that there are infinitely many primes p for which

$$k! + 1 \equiv 0 \,(\mathrm{mod}\, p), \;\; p \not\equiv 1 (\mathrm{mod}\, k).$$

(Perhaps you know that already.)

$$(p-1)! + 1 \equiv 0 \,\mathrm{mod}\, q \quad \text{for some} \quad q > p;$$

if $q \not\equiv 1(\mathrm{mod}\, p)$, we have won, if not, then consider $(q-p-1)! + 1$. This is a multiple of q, but $q \equiv 1 \,\mathrm{mod}(q-p-1)$ unless $q = 2p+1$ and this can be excluded if we start with a p for which $2p+1$ is not a prime. I hope this is correct."

(b) "Dear Subbarao,

I write again about $n! + 1 \equiv 0(\mathrm{mod}\, p)$, $p \not\equiv 1(\mathrm{mod}\, n)$. When I told the proof to Suranyi, a slip was discovered, but we easily corrected the

Proof: $(6k+1)! + 1 \equiv 0(\mathrm{mod}\, p)$ if $p \not\equiv 1(\mathrm{mod}\, 6k+1)$ for inf many k we are finished—if not then $(p-6k-2)! + 1 \equiv 0(\mathrm{mod}\, p)$ and $p \not\equiv 1 \,\mathrm{mod}(p-6k-2)$, which proves that there are inf p for which $n! + 1 \equiv 0(\mathrm{mod}\, p)$, $p \not\equiv 1(\mathrm{mod}\, n)$. We do not see whether this holds for almost all p or whether for almost all n there is a p for which $n! + 1 \equiv 0(\mathrm{mod}\, p)$, $p \not\equiv 1(\mathrm{mod}\, n)$.

Kind regards and apologies for my carelessness.

Au revoir Paul Erdős"

Regarding Problem B, in a later letter dated July 29, 1993, he wrote: "I think that for almost all n there is a p, $p \not\equiv 1(\mathrm{mod}\, n)$, for which $n! + 1 \equiv 0(\mathrm{mod}\, p)$, but I do not see how to prove it; but perhaps this is not hopeless."

(ii) The first entry gives a select Pillai prime p and the second gives the ratio of the number of Pillai primes up to p over the number of all primes $\leq p$.

23	0.111111
193	0.295455
499	0.410526
1999	0.49505
3559	0.50501
5003	0.495522
10009	0.498781
20011	0.520548
36007	0.526275
44987	0.530053

ACKNOWLEDGMENT. The second author is partly supported by an NSERC grant.

REFERENCES

1. G. Hardy and M. V. Subbarao, *On a problem of Pillai and some related questions*, Leaflets in Mathematics, Proc. Number, Functions, Equations, International Conference dedicated to the 60th birthdays of Professors Zoltan Zaróczy and Imre Katai held at Noszväz, Hungary, Zsolt P'ales, ed., May 31–June 6, 1998, pp. 142–143.
2. S. S. Pillai, Question 1490, *J. Indian Math. Soc.* **18** (1930) 230.
3. J. V. Uspensky and M. S. Heaslet, Problem 1 in *Elementary Number Theory*, McGraw Hill, New York, 1930, p. 157.

University of Alberta, Edmonton, Alberta T6G 2G1, Canada
m.v.subbarao@ualberta.ca

Northern Alberta Institute of Technology, Edmonton, Alberta, Canada
georgeh@nait.ab.ca

Some Curious Sequences Involving Floor and Ceiling Functions

M. A. Nyblom

1. INTRODUCTION. Of all the well-known arithmetic functions in number theory, the integer part or *floor function* of a real number x, denoted by $\lfloor x \rfloor = \max\{n \in \mathbb{Z} : n \leq x\}$, is perhaps the simplest. This function has a companion function known as the *ceiling function* of x, denoted by $\lceil x \rceil = \min\{n \in \mathbb{Z} : x \leq n\}$. Both the floor and ceiling functions exhibit many varied and curious properties, some of which have been extensively studied in [**2**, chap. 3]. In this note we illustrate how these functions, individually and in combination, can be used to determine closed form expressions for the nth term of some unusual sequences. In the first half, the sequences considered are formed from either the addition or deletion of terms from a given sequence. As a consequence of the latter case, we derive a surprising formula for the nth positive integer that is not a perfect mth power. Finally, in the second half we solve a recurrence relation involving a floor function. We denote the set of strictly positive integers by $\mathbb{N}$.

2. ADDITION AND DELETION OF TERMS. Consider an arbitrary sequence of real numbers $\langle a_n \rangle$, from which we construct another sequence $\langle b_m \rangle$ in the following manner. Let $d \in \mathbb{N}$ be fixed, and for each $m \in \mathbb{N}$ define b_m to be the mth term of the sequence consisting of nd occurrences in succession of the term a_n, as follows:

$$\underbrace{a_1, \dots, a_1}_{d,\ a_1 \text{ terms}}, \underbrace{a_2, \dots, a_2}_{2d,\ a_2 \text{ terms}}, \underbrace{a_3, \dots, a_3}_{3d,\ a_3 \text{ terms}}, \dots. \tag{1}$$

For example, if $a_n = n$ and $d = 1$, then the resulting sequence $\langle b_m \rangle$ would be

$$1, 2, 2, 3, 3, 3, 4, 4, 4, 4, \dots.$$

Can we usefully describe a function $f : \mathbb{N} \to \mathbb{N}$ such that $b_m = a_{f(m)}$? For our first result, we show that such a function can be constructed in terms of a ceiling and square