ON AN INTERESTING PROPERTY OF 112359550561797752809

J. L. HUNSUCKER and CARL POMERANCE
University of Georgia, Athens, Georgia 30602

In solving Problem 301 by J. A. Hunter in [1] an interesting Fibonacci property arose. The problem was to find the smallest positive integer with the property that when the digit 1 was appended to both ends, the new number was 99 times the old. If x is the original number then the problem can be restated by solutions x, k to

$$\frac{10^{k+2}+1}{89} = x \qquad \text{and} \qquad [\log_{10} x] = k,$$

where $[\cdots]$ is the greatest integer function. The problem can of course be generalized to other bases. In particular in the base g, $g-1$ plays the role of 9 in the base 10, so the original problem becomes

Generalized Problem: Find x, k if

$$g^{k+2} + gx + 1 = (g^2-1)x\ ,$$

or equivalently

$$x = \frac{g^{k+2}+1}{g^2-g-1}\ , \qquad \text{and} \qquad k = [\log_g x]\ .$$

It is an easy inequality argument to show for a positive integer $g \geqslant 3$ that

$$g^k < \frac{g^{k+2}+1}{g^2-g-1} < g^{k+1}\ .$$

Thus the condition $[\log_g x] = k$ can be dropped for $g \geqslant 3$ and we will do so for the remainder.

By long division,

$$x = \frac{g^{k+2}+1}{g^2-g-1} = \left(\sum_{i=1}^{k+1} g^{k+i-1}F_i\right) + \frac{gF_{k+2}+F_{k+1}+1}{g^2-g-1}\ ,$$

where F_i is the i^{th} Fibonacci number ($F_1 = F_2 = 1$, etc.). So all the solutions for a given g are found by finding the k's for which

$$\frac{gF_{k+2}+F_{k+1}+1}{g^2-g-1}$$

is an integer.

Solving the equation

$$\frac{g^{k+2}+1}{g^2-g-1} = x$$

for x and k is equivalent to solving the congruence $g^t \equiv -1 \pmod{g^2-g-1}$ for $t \geqslant 2$. As a matter of fact, since $10^{22} \equiv -1 \pmod{89}$ we see that for $g = 10$, all solutions x are given by

$$x = \frac{10^{22+44j}+1}{89}\ .$$

The first such x is 112359550561797752809.

In the remainder of this paper we will always use p to denote an odd prime. It is easy to show that $g^t \equiv -1 \pmod{p^a}$ has a solution t if and only if $\mathrm{ord}_p g$ is even, where $\mathrm{ord}_p g$ means the order of g in the multiplicative group of integers modulo p. In this case t is an odd number times ½ $\mathrm{ord}_p g$. Then using the Chinese Remainder Theorem, the fact that $\mathrm{ord}_m g = \text{l.c.m.}\left\{\mathrm{ord}_{p^a} g ; p^a \| m\right\}$, and the fact that $\mathrm{ord}_{p^a} g$ is a power of p times $\mathrm{ord}_p g$, it is an elementary argument to show for m odd and $(g,m) = 1$ that $g^t \equiv -1 \pmod m$ has a solution t if and only if there is an $x \geqslant 1$ such that $2^x \| \mathrm{ord}_p g$ for each $p|m$, in which case t is an odd number times ½ $\mathrm{ord}_m g$. Compiling this result with our earlier discussion and the fact that $g^2 - g - 1$ is always odd leads to the following theorem.

Theorem 1. Let $g \geqslant 3$ be an integer. Then the following statements are equivalent.

(a) The Generalized Problem has a solution x, k.

(b) There is an integer k such that

$$\frac{gF_{k+2} + F_{k+1} + 1}{g^2 - g - 1}$$

is an integer.

(c) There is an integer $x \geqslant 1$ such that $2^x \| \mathrm{ord}_p g$ for every prime $p | g^2 - g - 1$.

If these statements hold, then $k + 2$ is any odd number times ½ $\mathrm{ord}_{g^2-g-1} g$.

The question naturally arises as to how many bases g are there for which the Generalized Problem has a solution. Towards this end let A denote the set of those $g \geqslant 3$ for which the Generalized Problem has a solution and let

$$B = \left\{ g \geqslant 3 : g \notin A \right\}.$$

Let p be a prime of the form 3 (mod 4) which divides $h^2 - h - 1$ some h. Then p also divides $(-h+1)^2 - (-h+1) - 1$. Furthermore

$$\left(\frac{h}{p}\right)\left(\frac{-h+1}{p}\right) = \left(\frac{-1}{p}\right) = -1,$$

where $(\cdots/p)$ is the Legendre symbol. So either

$$\left(\frac{h}{p}\right) = 1 \qquad \text{or} \qquad \left(\frac{-h+1}{p}\right) = 1.$$

Let a_p stand for h or $-h + 1$ according as to which Legendre symbol is 1. Then if $g \equiv a_p \pmod p$ we have that $p | g^2 - g - 1$ and that $\mathrm{ord}_p g$ is odd (since

$$g^{(p-1)/2} \equiv a_p^{(p-1)/2} \equiv \left(\frac{a_p}{p}\right) \equiv 1 \pmod p \quad \text{and} \quad \frac{p-1}{2}$$

is odd). On the other hand if p is any prime of the form 1 or 4 (mod 5) then $p | h^2 - h - 1$ for

$$h = \frac{1}{2}(1+b)(1+p),$$

where $b^2 \equiv 5 \pmod p$. (Note that

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right) = 1,$$

so b exists.) Therefore if $p \equiv 1$ or $4 \pmod 5$ and in addition $p \equiv 3 \pmod 4$, i.e., $p \equiv 11$ or $19 \pmod{20}$, then there is an a_p such that for every $g \equiv a_p \pmod p$ we have $\mathrm{ord}_p g$ is odd and $p | g^2 - g - 1$. Let $P = \left\{ p : p \text{ is a prime of the form } 11 \text{ or } 19 \pmod{20} \right\}$ and let $C = \left\{ g \geqslant 3 : g \equiv a_p \pmod p \text{ for some } p \in P \right\}$. Then Theorem 1 implies $C \subset B$. Furthermore, Dirichlet's theorem on primes in arithmetical progressions implies

$$\sum_{p \in P} \frac{1}{p} = \infty .$$

It then follows that the asymptotic density of C, and hence B, is 1. We have thus proved the following theorem.

Theorem 2. The probability of a random choice of a base $g \geq 3$ not yielding a solution to the Generalized Problem is 1.

In light of this theorem it seems that the choice of the base 10 in the problem as originally stated was a wise choice! We leave as an entertaining problem for the reader the question of the identity of the bases g less than 100 for which there is a solution.

We have shown that in some sense A has far fewer elements than B. But is A finite or infinite? If $g \equiv 3 \pmod 4$ is a prime and $p = g^2 - g - 1$ is also a prime, then $p \equiv 1 \pmod 4$ and

$$\left(\frac{g}{p}\right) = \left(\frac{p}{g}\right) = \left(\frac{-1}{g}\right) = -1.$$

Hence $g^t \equiv -1 \pmod p$ has a solution and $g \in A$. We note that Schinzel's Conjecture H [2] implies there are infinitely many primes $g \equiv 3 \pmod 4$ for which $g^2 - g - 1$ is also prime. Hence if this famous conjecture is true it follows that our set A is infinite.

REFERENCES

1. J. A. Hunter, Problem 301, *J. Recreational Math.*, 6 (4), Fall 1973, p. 308.
2. A. Schinzel and W. Sierpiński, "Sur certaines hypothèses concernant les nombres premiers," *Acta Arith.* 4 (1958), pp. 185–208.

****

[Continued from P. 330.]

$$\left(\frac{(-1/a)}{(-1/b)}\right) = (-1)^{(a-1)(b-1)/4} = 1$$

if and only if $a \equiv 1 \pmod 4$ and/or $b \equiv 1 \pmod 4$.

If $A = \pm 1$ and $B = \pm 1$ are logical variables, then the sixteen functions of those variables are given by ± 1, $\pm A$, $\pm B$, $\pm AB$ and $\pm(\pm A/\pm B)$. This is a result that cannot be obtained with the definition $(-1/-1) = 1$. If $A = (-1/b)$ and $B = (-2/b)$, then the logical functions of A and B give the congruence of b modulo 8. For example,

$$(A/B) = (-1)^{(b^3-b^2+7b-7)/16} = 1$$

if and only if $b \equiv 1$, 3 or 5 (mod 8). The function -1 is a null function which cannot occur.

If $b = \pm p_1 p_2 \cdots p_k$ with p_i not necessarily distinct, and n is the number of p_i for which $(a/p) = -1$, then

$$(ab) = \left(\frac{(a/-1)}{(b/-1)}\right)(-1)^n .$$

Theorem. If $ab \equiv 1 \pmod 2$ and $(a,b) = 1$, then

$$(a/b)(b/a) = \left(\frac{(a/-1)}{(b/-1)}\right)\left(\frac{(-1/a)}{(-1/b)}\right) .$$

In other words,

$$(a/b)(b/a) = 1$$

if and only if ((a is positive and/or b is positive) and ($a \equiv 1 \pmod 4$ and/or $b \equiv 1 \pmod 4$)) or (a is negative and b is negative and $a \equiv -1 \pmod 4$ and $b \equiv -1 \pmod 4$)).

Proof.

$$((-1/a)/(-1/b)) = -1$$

if and only if

$$(-1/a) = (-1/b) = -1;$$

$$((-1/-a)/(-1/b)) = -1$$

[Continued on P. 336.]