AN INTERESTING SEQUENCE OF FIBONACCI SEQUENCE GENERATORS

JOSEPH J. HEED
Norwich University, Northfield, Vermont 05663
and
LUCILLE KELLY
Vermont College, Montpelier, Vermont 05666

An observation that certain sequences of power residues modulo some primes were generalized Fibonacci sequences led to the investigation of the positive sequence with general term $n^2 - n - 1$. This sequence was found to have some interesting properties.

For example,

$$3^k \equiv 3^{k-1} + 3^{k-2} \pmod 5, \qquad 4^k \equiv 4^{k-1} + 4^{k-2} \pmod{11},$$

$\{5^k\}$ is similarly defined mod 19, etc. If we take as initial values $1, n,$ and define a Fibonacci sequence based on these values, the r^{th} term is given by $nf_{r-1} + f_{r-2}$, where f_r is the r^{th} Fibonacci number. It is then a simple matter to show that $n^2 - n - 1$ divides $n^r - nf_{r-1} - f_{r-2}$. Thus,

$$n^k \equiv n^{k-1} + n^{k-2} \pmod{n^2 - n - 1}.$$

THE SEQUENCE $\{n^2 - n - 1\}$

1. Let $m(n) = n^2 - n - 1$. Let p be prime, and let $p|m(N)$. Then there is a unique partition of p, $p = a + b$, such that $p|m(N + kp)$ and $p|m(N + kp + a)$.

i. That $p|m(N + kp)$ is easily verified

ii. $p|m(N + kp + a)$

$$m(N + kp + a) = N^2 + 2Nkp + 2Na + k^2p^2 + 2kpa + a^2 - N - kp - a - 1 .$$

This is divisible by p if $p|2N + a - 1$.

There is some smallest value of a for which this is true, and this value of a is independent of N. For let $p|m(n)$ $n \neq N$. Then $p|m(N + kp + a')$ for a' such that $p|2n + a' - 1$.

Thus,

$$pk' = a - 1 + 2N, \qquad pk''' = a' = 1 + 2n.$$

Subtracting and adding:

$$pk'' = (a' - a) + 2(n - N) \qquad \text{and} \qquad pk^* = a + a' + 2(N + n - 1).$$

Since

$$p|N^2 - N - 1 \qquad \text{and} \qquad p|n^2 - n - 1,$$

then

$$p|(N^2 - N - 1) - (n^2 - n - 1),$$

that is, $p|(N - n)(N + n - 1)$.

Either $p|N - n$ or $p|N + n - 1$.

In the former instance it follows that $p|a' - a$, and since both are less than p, $a = a'$. In the latter case $p|a + a'$, and $a + a' = p$, that is, $a' = b$.

2. If $p|m(N)$, then $p|m(N - b)$.

$$m(N - b) = m(N) + b(b - 2N + 1).$$

But

$$b - 2N + 1 = p - a - 2N + 1 = p - (a - 1 + 2N), \qquad \text{and} \qquad p|(a - 1 + 2N).$$

3. If a prime p appears as a factor in the sequence it does appear at these regular intervals of a and b, and only then. For let

$$p\,|\,m(N),\quad p\,|\,m(N+a)\quad\text{and}\quad p\,|\,m(N+a+x),\quad a+x \leqslant p.$$

$$m(N+a+x) = m(N+a)+x(2N+a-1)+(a+x).$$

Since $p\,|\,m(N+a)$ and $p\,|\,2N+a-1$, p must divide $a+x$. But this is possible only if $p = a+x$, and $x = b$.

4. Let

$$m(N) = p_1^{r_1}p_2^{r_2}\cdots p_t^{r_t},$$

p_i prime, $t > 1$. We have $N^2 > m(N) > (N-1)^2$. No $p = N$, for if $m(N) = p\cdot Q$ with $p = N$, we have

$$Q = N - 1 - \frac{1}{N},$$

which is impossible. Thus some $p < N$. But in that event $N - p > 0$ and $p\,|\,m(N-p)$, yielding: if $p\,|\,m(N)$, then

$$p = m(N) \text{ or } p\,|\,m(n)$$

for some $n < N$.

5. All factors of $m(N)$ terminate in $1, 5$ or 9. The period for $m(N)$ *modulo* 10 is $1, 5, 1, 9, 9$. The product of such elements terminates in $1, 5$ or 9. Since $N^2 > m(N)$, at most one p can exceed N, and by (4) at most one prime factor new to the sequence can be introduced per term. If we assume for $n < k$ all factors terminate in $1, 5$ or 9, and if $m(N) = p\cdot Q$ for $N \geqslant k$, with p a new factor, then since Q terminates in $1, 5$ or 9 so must p.

6. Further, it is true that every prime of the form $10n \pm 1$ is a member of the sequence.

i. First we establish that 5 is a quadratic residue of every prime of the form $10n \pm 1$. If p is an odd prime $(p \neq 5)$, then by the Law of Quadratic Reciprocity,

$$\left(\frac{5}{p}\right)\left(\frac{p}{5}\right) = (-1)^{\frac{5-1}{2}\cdot\frac{p-1}{2}} = +1.$$

Thus $(p/5) = (5/p)$, and if 5 is a quadratic residue of p, p is also a quadratic residue of 5, that is, $5\,|\,x^2 - p$ for some x. It is easily verified that $p \equiv \pm 1 \mod 10$.

ii. There are two incongruent solutions to $x^2 - 5 \equiv 0 \mod p$, z and $p - z$. One is odd, the other even. Let z be odd, and let $N = (z+1)/2$.

$$N^2 - N - 1 = \tfrac{1}{4}(z^2 - 5).\quad p\,|\,z^2 - 5\quad \therefore\ p\,|\,N^2 - N - 1.$$

7. An examination of the sequence reveals an unexpected number of terms which are prime. However, this situation cannot be expected to continue. It is known that primes of the form $10n \pm 1$ and $10n \pm 3$ are equinumerous [1], and that $\sum 1/p$, p prime, diverges.

$$\sum_{n=2}^{\infty} 1/n^2 - n - 1$$

converges, as must the subseries consisting of terms which are prime. The implication being, terms, $n^2 - n - 1$, which are prime must become rarer as n increases.

SOME TERMS OF $m(n) = n^2 - n - 1$

n	$m(n)$	n	$m(n)$	n	$m(n)$	n	$m(n)$	n	$m(n)$	n	$m(n)$	n	$m(n)$	n	$m(n)$	n	$m(n)$	n	$m(n)$
2	1	12	131	22	461	32	991	42	1721	52	11·241	62	19·199	72	19·269	82	29·229	92	11·761
3	5	13	5·31	23	5·101	33	5·211	43	$5\cdot 19^2$	53	5·19·29	63	5·11·71	73	5·1051	83	5·1361	93	5·29·59
4	11	14	181	24	19·29	34	19·59	44	31·61	54	2861	64	29·139	74	11·491	84	6971	94	8741
5	19	15	11·19	25	599	35	29·41	45	1979	55	2969	65	4159	75	31·179	85	$11^2\cdot 59$	95	8929
6	29	16	239	26	11·59	36	1259	46	2069	56	3079	66	4289	76	41·139	86	7309	96	11·829
7	41	17	271	27	701	37	11^3	47	2161	57	3191	67	4421	77	5851	87	7481	97	9311
8	5·11	18	5·61	28	5·151	38	5·281	48	5·11·41	58	5·661	68	5·911	78	5·1201	88	5·1531	98	5·1901
9	71	19	11·31	29	811	39	1481	49	2351	59	11·311	69	4691	79	61·101	89	41·191	99	89·109
10	89	20	379	30	11·79	40	1559	50	31·79	60	3539	70	11·439	80	71·89	90	8009	100	19·521
11	109	21	419	31	929	41	11·149	51	2549	61	3659	71	4969	81	11·19·31	91	19·431		

REFERENCE

1. Daniel Shanks, *Solved and Unsolved Problems in Number Theory*, Vol. 1, p. 22.

****