A LETTER TO THE EDITOR

Enrico T. Federighi and Ronald G. Roll
The Johns Hopkins University
Silver Spring, Maryland

A careful study of the Tables of Fibonacci Entry Points has led us to make some observations regarding the factors of Fibonacci numbers.

It is readily seen that $Z(p)$ divides $p-1$ whenever $p \equiv \pm 1 \pmod{10}$ and divides $p+1$ whenever $p \equiv \pm 3 \pmod{10}$.

Our problem is to determine, if possible, the primes p for which $Z(p)$ divides $p(k) = (p \pm 1)/k$ for $k > 1$. We conjecture the following solutions.

$k=2$: $Z(p)$ divides $p(2)$ if and only if $p=4n+1$.

$k=3$: $Z(p)$ divides $p(3)$ if and only if $p=x^2 + 135y^2$ or $p = 5x^2 + 27y^2$.

$k=4$: $Z(p)$ divides $p(4)$ if and only if $p=x^2 + 80y^2$ or $p = 5x^2 + 16y^2$.

The rule is more complicated but is still reasonable if k is a small prime. Let k be such a prime and define $\beta = (k-1)/2$.

Let $p(k,\ell) = 2 \cos (2\pi\ell/k)$ and $\gamma_{ij} = g^{i+j-2}$, where g is a primitive root of k. Also let $\epsilon_{kj} = 2 - p(k, g^{j-1})$. Define

$$C(k, x, y) = \prod_{j=1}^{\beta} \left\{ \left[\sum_{i=1}^{\beta} a_i p(k, \gamma_{ij}) \right]^2 x^2 + \epsilon_{kj} \left[\sum_{i=1}^{\beta} b_i p(k, \gamma_{ij}) \right]^2 y^2 \right\}$$

$$= \sum_{r=0}^{\beta} c_{2r} x^{2\beta-2r} y^{2r} .$$

$k > 4$: $Z(p)$ divides $p(k)$ if and only if $mp = C(k, \sqrt{5}, 1)$ or $mp = C(k, 1, \sqrt{5})$ where $c_{2\beta} \equiv 0 \pmod{k^3}$. The nature of m is uncertain but it will usually be unity or a power of 2^β. If $5^n \equiv 1 \pmod{k}$ for $n < \beta$, m may also contain an even power of 5.

To illustrate how the formulations look in practice, a table of all primes under 1000 with $k \geq 3$ is listed. It is assumed that $x=y=1$. Type 1 means that

$$mp = \sum_{r=0}^{\beta} c_{2r} 5^{r}$$

and type 2 means that

$$mp = \sum_{r=0}^{\beta} c_{2r} 5^{\beta - r} .$$

p	k	type	m	c_0	c_2	c_4	c_6
47	3	1	1	4	27		
61	4	1	1	9	16		
89	4	2	1	9	16		
	8	2	1	1	12	4	
107	3	1	1	16	27		
109	4	1	1	9	64		
113	3	1	1	1	108		
139	3	2	1	4	27		
149	4	1	1	1	144		
151	3	2	1	16	27		
199	3	2	1	64	27		
	9	2	64	361	585	243	27
211	5	2	16	1	50	125	
233	3	1	1	25	108		
	9	1	64	1	153	2187	27
263	3	1	1	4	243		
269	4	1	1	25	144		
281	5	2	16	121	250	125	
307	7	1	64	1	581	931	343
331	3	2	1	196	27		
347	3	1	1	64	27		
353	3	1	1	49	108		
389	4	1	1	49	144		
401	4	2	1	81	64		
421	4	1	1	81	16		
	5	2	16	361	650	125	

p	k	type	m	c_0	c_2	c_4	c_6	c_8	c_{10}	c_{12}
461	5	2	16	1	850	125				
521	4	2	1	441	16					
	5	2	16	961	850	125				
541	3	2	1	1	108					
557	3	1	1	25	432					
	9	1	64	1	153	4779	7803			
563	3	1	1	64	243					
619	3	2	1	484	27					
661	3	2	1	121	108					
	4	1	1	81	256					
677	3	1	1	49	432					
691	5	2	16	1681	1250	125				
701	4	1	1	25	576					
709	3	2	1	169	108					
743	3	1	1	100	243					
761	4	2	1	441	64					
	8	2	1	1	96	256				
769	4	2	1	49	144					
	8	1	1	289	76	4				
797	7	1	64	169	917	1323	343			
809	4	2	1	729	16					
811	3	2	1	676	27					
821	4	1	1	49	576					
829	3	2	1	289	108					
	4	1	1	9	784					
859	11	1	1024	1	319	3146	9438	9317	1331	
881	5	2	16	3721	1450	125				
911	13	1	102400	1	182	10595	222404	1595191	3405350	1373125
919	3	2	1	784	27					
	9	2	64	1	153	2187	27			
953	3	1	1	169	108					
	9	1	64	361	585	243	27			
967	11	1	32768	1	1551	105754	642510	286165	1331	
977	3	1	1	1	972					
991	5	2	16	3481	1850	125				

Comments on Table:

1) As can be seen whenever k is an odd prime c_{k-1} is divisible by k^3.

2) If k is an odd prime $\sum b_i \equiv 0 \pmod{k}$ will ensure that c_{k-1} be divisible by k^3.

3) If one sums the coefficients in the table without first multiplying by powers of five one obtains k-th power residues of two.

Some of this has undoubtedly been observed before and even probably proved but we have no idea how much.

We have enjoyed playing around with these concepts and actually suspect much more than we have indicated here. If anyone is interested in pursuing this further, we shall be glad to hear from him.

XXXXXXXXXXXXXXX

LETTER TO THE EDITOR

Lenard Weinstein
Massachusetts Institute of Technology

Conjecture 2., made by Mr. Thoro, on page 186 of the October issue, follows immediately from the following theorem found on page 126 of W. J. Leveque, Topics in Number Theory, Vol. I:

Definition

A representation of a positive integer n as a sum of two squares, say $n = x^2 + y^2$ is termed proper if $(x, y) = 1$.

Theorem

If p is a prime of the form $4k + 3$ and $p \mid n$, then n has no proper representation.

Since $F_{2n+1} = F_n^2 + F_{n+1}^2$, and $(F_n, F_{n+1}) = 1$, F_{2n+1} always has a proper representation. Therefore, by the above theorem, no prime of the form $4k + 3$ can divide F_{2n+1}.

XXXXXXXXXXXXXXX