Periods of Fibonacci Sequences Mod m

Given a positive integer m, let f(m) denote the period length of the Fibonacci sequence 0, 1, 1, 2, 3, 5, ... taken modulo m. Peter Freyd challenged the readers of the American Mathematical Monthly (E3410, March 92) to prove that f(m) is less than or equal to 6m for all m, and that equality holds for infinitely many values of m.

Let the prime factorization of m be

$$m = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

For the period length of a linear recurring sequence modulo m it is immediate that

$$f(m) = \mathrm{LCM}\left[f\left(p_j^{a_j}\right)\right]$$

which is less than or equal to

$$\mathrm{LCM}\left[p_j^{a_j - 1} f\left(p_j\right)\right]$$

Thus, a bound for f(m) is determined by the periods of the recurrence in the finite fields Z_p for each p dividing m.

The characteristic polynomial for the Fibonacci and Lucas sequences is

$$q(x) = x^2 - x - 1$$

which splits in the field Z_{p^2} into linear factors x - a and x - b. If a is not equal to b, then the nth element in the sequence has the form

$$F_n = Aa^n + Bb^n$$

for constants A and B (determined by the initial values). If q(x) splits in Z_p, then a,b are elements of Z_p, and f(p) divides p - 1 by Fermat's Little Theorem. On the other hand, if q(x) is irreducible in Z_p, then the order of the roots of q(x) can be found by noting that

$$a^p = b \qquad -1 = ab = a^{p+1}$$

implying that $a^{2(p+1)} = 1$. Thus f(p) divides 2(p+1) for "irreducible" primes. By the quadratic reciprocity law q(x) is irreducible over Z_p if p = ±2 (mod 5), and q(x) splits into distinct linear factors over Z_p if p = ±1 (mod 5).

The remaining case is when q(x) has multiple conjugate roots in Z_{p^2}, which implies that a = b in Z_p. This occurs if and only if p divides the discriminant of q(x), that is, if and only if p = 5. Then the nth term of the sequence is

$$F_n = (A + Bn)a^n$$

where the constants A and B are again determined by the initial values. Since the periods of A + Bn and a^n divide p and p - 1 respectively, the sequence in this case has period dividing

$p(p - 1) = 20$. Indeed, for the Fibonacci sequence we have $f(5) = 20$, whereas for the Lucas sequence the initial values are such that $B = 0$ and we have $f(5) = 4$.

Now, to maximize the value of $f(m)/m$ we should exclude any prime factors p for which $q(x)$ splits into distinct factors in Z_p, since they contribute at best a factor of $(p - 1)/p$. Therefore, we need consider only products of "irreducible" primes and the special prime 5. If m is a product of only odd irreducible primes, then

$$f(m) \le \mathrm{LCM}\left[\left(\frac{p_j+1}{2}\right)p_j^{a_j-1}\right] \le 4m\prod\frac{p_j-1}{2p_j}$$

which proves that the ratio is less than 4 in this case. So, in view of the facts that

$$f(3^n) = 8\cdot 3^{n-1} \qquad\qquad f(2^n) = 3\cdot 2^{n-1}$$

for both the Lucas and Fibonacci sequences and

$$f(5^n) = \begin{cases} 4\cdot 5^n & \text{for Fibonacci sequence} \\ 4\cdot 5^{n-1} & \text{for Lucas sequence} \end{cases}$$

we see that for the Fibonacci sequence the maximum value of $f(m)/m$ is 6, which occurs if and only if $m = 2\cdot 5^n$ where n is any positive integer. On the other hand, for the Lucas sequence 2,1,3,4,7,... the maximum value of $f(m)/m$ is 4, which occurs if and only if $m = 6$.

Return to MathPages Main Menu