
MATH 47a Congruence and Divisibility Problems Spring, 2000

Let $P(m)$ be the period of the Fibonacci sequence modulo m .

Here are some hints in studying $P(m)$: First look at the case in which m is prime. The Binet formula can be useful, as can the formula obtained from the Binet formula by expanding α^n and β^n with the binomial theorem. To use the Binet formula you will need something to take the place of $\sqrt{5}$. Another useful fact is that F_{n+1} is “almost” determined by F_n : take the identity $F_n^2 - F_{n-1}F_{n+1} = (-1)^{n-1}$, and express F_{n-1} in terms of F_n and F_{n+1} to get an identity involving only F_n and F_{n+1} .

1. What can you say about $P(m)$. Hint: Look at prime moduli first, and then prime powers.
2. Let $Z(m)$ be the least positive k such that $F_k \equiv 0 \pmod{m}$. Can you find any connection between $Z(m)$ and $P(m)$?
3. Is there any connection between $P(m_1)$, $P(m_2)$, and $P(m_1m_2)$? What if m_1 and m_2 are relatively prime?
4. There are m^2 different generalized Fibonacci sequences (g_n) modulo m , corresponding to the m^2 possible values for g_0 and g_1 . Suppose we consider two of these generalized Fibonacci sequences to be equivalent if one can be obtained by shifting the other. Thus if $m = 3$ then there are only two equivalence classes, corresponding to the trivial sequence $(0, 0, \dots)$ and to the sequence $(0, 1, 1, 2, 0, 2, 2, 1, 0, 1, 1, \dots)$. If $m = 4$, there are four equivalence classes: have $(0, 0, \dots)$, $(0, 1, 1, 2, 3, 1, 0, 1, \dots)$, $(0, 2, 2, 0, 2, \dots)$, and $(0, 3, 3, 2, 1, 3, 0, 3, \dots)$.
 - (a) How many equivalence classes are there in general?
 - (b) When (i.e., for which m) are the Fibonacci and Lucas sequences in the same equivalence class?
 - (c) When do all nontrivial equivalence classes have the same period?
 - (d) How many different periods are possible? If there is more than one, must there be any relation among them?
5.
 - (a) Show that if m divides n then F_m divides F_n .
 - (b) Show that $\gcd(F_m, F_n) = F_{\gcd(m, n)}$, where $\gcd(a, b)$ is the greatest common divisor of a and b .
 - (c) Is there anything similar that you can say for Lucas numbers? For other generalized Fibonacci sequences?
6. Does every generalized Fibonacci sequence contain infinitely many primes?