Fibonacci Numbers Modulo p

Brian Lawrence

April 14, 2014

Abstract

The Fibonacci numbers are ubiquitous in nature and a basic object of study in number theory. A fundamental question about the Fibonacci numbers is: which of them are multiples of a given prime p? In particular, we will see that either the p-th Fibonacci number, the one before it, or the one after it, is a multiple of p. Along the way we will use the arithmetic of finite fields, an essential tool in number theory, and perhaps even see some analogies with differential equations and linear algebra.

1 Introduction

Consider the Fibonacci sequence, defined recursively by $F_0 = 0$, $F_1 = 1$ and $F_i = F_{i-1} + F_{i-2}$ for $i \geq 2$.

Question 1.1. *For a given positive integer N, which Fibonacci numbers are divisible by N?*

It is enough to consider the case where N is a power of a prime. A reasonable approach to this problem is in two steps. First, find which F_i are divisible by the prime number p. Then, investigate what power of p divides each F_i. In this talk we will focus on the first step. So, we have the new question:

Question 1.2. *For a given prime number p, which Fibonacci numbers are divisible by p?*

2 Initial Examples and Periodicity

As a first example, consider the case $p = 2$. Which Fibonacci numbers are divisible by 2? Inspecting the table we see that F_i is divisible by 2 if and only if i is divisible by 3; we easily prove this by induction on i

Which Fibonacci numbers are divisible by 3?

Here we see that F_i is divisible by 3 if and only if i is divisible by 4. To prove this we note that

$$F_{i+8} \equiv F_i (\bmod 3),$$

so the set of i with F_i divisible by 3 will be a union of congruence classes modulo 8. But now we can check that the classes that arise are 0 and 4 mod 8, so F_i is divisible by 3 exactly when 4 divides i.

A priori, this argument showed only that that F_i is divisible by 3 for i in some union of arithmetic progressions modulo 8; we had to check by hand to see which progressions arise. It would be better to show directly that F_i is divisible by 3 exactly when i is a multiple of some 4.

When $p = 3$ we can get a dirce the *twisted periodicity* relation

$$F_{i+4} \equiv -F_i \pmod 3.$$

This is enough to show that F_i is a multiple of 3 exactly when i is a multiple of 4.

How much of this can we generalize to all p? We restate the two arguments above for general p.

Remark 2.1. *Fix some p. Suppose we can find some b such that*

$$F_b \equiv 0$$

and

$$F_{b+1} \equiv 1 \pmod p.$$

Then by induction on i we can show that

$$F_{b+i} \equiv F_i \pmod p,$$

so the Fibonacci sequence modulo p is periodic with period b.

Remark 2.2. *Under the assumption of Remark 2.1, let a be the smallest positive integer such that F_a is a multiple of p. (Such a exists by hypothesis). Then we can prove by induction on i the twisted periodicity relation*

$$F_{a+i} \equiv F_{a+1} F_i,$$

so in particular, F_{a+i} is a multiple of p if and only if F_i is a multiple of p. Thus we see that F_i is a multiple of p exactly when i is a multiple of a.

The argument that F_{a+i} is a multiple of p if and only if F_i is a multiple of p implicitly used the fact that F_{a+1} is not a multiple of p. One can show that F_{a+1} is not a multiple of p by the following argument: if F_a and F_{a+1} are both multiples of p then, using the Fibonacci recurrence backwards, one finds that F_i is a multiple of p for all $i < a$. But $F_1 = 1$ is not a multiple of p, for any prime p, a contradiction.

We are now ready to prove the following theorem.

Theorem 2.3. *Let p be a prime. Then there exist integers a_p and b_p such that the Fibonacci number F_i is a multiple of p if and only if i is a multiple of a_p, and the Fibonacci sequence modulo p is periodic with minimum period b_p. Furthermore, a_p divides b_p, and $b_p \leq p^2$.*

Proof. Consider the ordered pairs

$$(F_i, F_{i+1})$$

taken modulo p. There are only p^2 such pairs possible, so eventually some pair must repeat. That is, we must have

$$(F_i, F_{i+1}) = (F_j, F_{j+1})$$

for some

$$0 \leq i < j \leq p^2.$$

Now by reverse induction (that is, induction on k), we find that

$$F_{j-k} \equiv F_{i-k}$$

for $k \geq 0$. In particular, taking $k = i$ and $k = i - 1$, we have

$$F_{j-i} \equiv F_0 \equiv 0$$

and

$$F_{j-i+1} \equiv F_1 \equiv 1.$$

Taking

$$b_p = j - i$$

and using Remarks 2.1 and 2.2 above, we are done. □

2.1 Computing the Periods

(In the talk I showed a table of values of a_p and b_p at this point.)

For small values of p, one sees that a_p does not exceed $p + 1$, and it is a factor of p, $p - 1$ or $p + 1$. Also, b_p is a factor of $p^2 - 1$, except when $p = 5$. We will prove these observations below.

3 Aside: A Formula for Fibonacci Numbers

Theorem 3.1. *Suppose λ and μ are the two distinct roots of the equation*

$$x^2 = x + 1$$

in any field F in which the equation has two distinct roots. Set

$$C = \frac{1}{\mu - \lambda}.$$

Then (in the field F) the Fibonacci numbers are given by the formula

$$F_i = C(\mu^i - \lambda^i).$$

We will present two proofs of this fact. For both proofs, let

$$G_i = C(\mu^i - \lambda^i).$$

We want to prove that

$$F_i = G_i.$$

Proof. First proof: elementary, by induction.

We check the formula by hand for $i = 0$ and $i = 1$. Next, since

$$\lambda^2 = \lambda + 1,$$

we have

$$\lambda^i = \lambda^{i-1} + \lambda^{i-2}.$$

and a similar result for μ^i.

But since G_i is a linear combination of λ^i and μ^i, we have

$$G_i = G_{i-1} + G_{i-2},$$

so by induction we have

$$G_i = F_i.$$

□

There is some linear algebra happening behind the scenes, as our second proof will show.

Definition 3.2. *A* Fibonacci-type sequence *is a sequence $H_0, H_1, \ldots$ of 'numbers' (or, elements of some field F) such that*

$$H_i = H_{i-1} + H_{i-2}$$

for all $i \geq 2$.

Let V denote the set of Fibonacci-type sequences (over the field F).

Proposition 3.3. *V is a two-dimensional vector space (over F).*

Proof. Easy. □

Now we can return to the theorem.

Proof. Second proof: Vector spaces.

Note that λ^i and μ^i are two elements of the vector space V. They are obviously independent (since $\lambda \neq \mu$), so they form a basis for V. Thus the Fibonacci sequence F_i is a linear combination of λ^i and μ^i, and it is now a routine matter to determine the coefficients. □

Well, that was certainly more conceptual, but it still doesn't explain where the sequences λ^i and μ^i came from. We will now see that they are eigenvectors for a translation operator.

First note the following trivial fact: if H_i is a Fibonacci-type sequence, then the translated sequence $(TH)_i$ defined by

$$(TH)_i = H_{i+1}$$

is also a Fibonacci-type sequence.

Now this T is a linear map from V to V, so we can study it using linear algebra.

By the recurrence, we have

$$(TTH)_i = (TH)_i + H_i,$$

which is to say, we have

$$T^2 = T + 1.$$

It follows the eigenvalues of T must be roots λ and μ of the polynomial x^2-x-1, and by the way that T is diagonalizable, ie. that there is a basis of eigenvectors. In fact, by choosing a basis for V and writing down a matrix for T, we can see that $x^2 - x - 1$ is also the characteristic polynomial for T, so λ and μ are both eigenvalues, each with multiplicity one.

What are the eigenvectors of T? Take the eigenvalue λ, for example. We need to find an H such that

$$TH = \lambda H.$$

In other words, we want $H_{i+1} = \lambda H_i$. Of course, up to scaling we must take $H_i = \lambda^i$. Thus λ^i arises as an eigenvector for T, and similarly for μ^i.

Remark 3.4. *All this is very similar to the theory of linear ordinary differential equations of the type studied in calculus class, such as*

$$f''(x) - f'(x) - f(x) = 0.$$

For such equations there is a solution space V whose dimension equals the degree of the equation. But instead of a single translation operator, we can translate solutions by any real distance t, giving a family of translation operators T_t. Or we can consider differentiation D, also as an operator on V.

The eigenvalues of D are easily read off the differential equation itself. (In the above example,

$$D^2 - D - 1 = 0$$

and the eigenvalues are exactly the λ and μ from above.) In calculus class we show that the functions

$$e^{\lambda x}, e^{\mu x}$$

form a basis for the solution space V. But even if we didn't know the solution, we could derive *it from eigenvalue considerations, as in the third proof above.*

We want to find an eigenvector of D for some eigenvalue, say ν. If f is such an eigenvector, then f by definition satisfies the differential equation

$$f'(x) = \nu f(x)$$

for all x. The eigenspace is thus one-dimensional, so T_t must act by a constant. Let $\chi(\nu, t)$ be the eigenvalue of T_t on this space. That is, if f satisfies the equation above, then

$$f(x+t) = \chi(\nu, t) f(x).$$

What are these constants $\chi(\nu, t)$? By composing two translations, we find that

$$\chi(\nu, s+t) = \chi(\nu, s)\chi(\nu, t).$$

Comparing solutions to different differential equations (or, as the physicists would say, scaling the x-axis), we can also show that

$$\chi(\nu, t) = \chi(1, \nu t).$$

Thus, all these constants $\chi(\nu, t)$ are in fact determined from the one function $e(t) := \chi(1, t)$, which satisfies $e(s+t) = e(s) + e(t)$. Of course, this e is just the natural exponential function.

4 Return to the Periods

Suppose our prime p is such that the polynomial $x^2 - x - 1$ has two distinct roots λ and μ in the finite field $\mathbb{F}_p$. (For example, if we take $p = 11$, then 4 and 8 are two distinct roots.) By the theorem above, we can recover the Fibonacci numbers modulo p from the powers of λ and μ.

For example, modulo 11, the powers of 4 are given by

$$1, 4, 5, 9, 3, 1, 4, 5, 9, 3, 1, 4, 5, \ldots$$

and the powers of 8 are given by

$$1, 8, 9, 6, 4, 10, 3, 2, 5, 7, 1, 8, 9, \ldots.$$

Now if we take $\lambda = 4$, $\mu = 8$, then (working in the field of integers modulo 11)

$$C = \frac{1}{\mu - \lambda} = \frac{1}{4} = 3,$$

and taking three times the difference of the two sequences we recover the Fibonacci sequence modulo 11.

Note that the powers of 4 here are periodic with period 5, and the powers of 8 are periodic with period 10. We now apply the following well-known theorem of Fermat.

Theorem 4.1. *(Fermat's Little Theorem): For any a not divisible by a prime p, we have*

$$a^{p-1} \equiv 1 (\mathrm{mod}\, p).$$

That is, the powers of a, modulo p, are periodic with period dividing $p - 1$.

Thus, we see immediately that the Fibonacci numbers are periodic with period dividing $p - 1$, provided our quadratic equation has two distinct roots modulo p. For which primes p can we find these two roots? Another classic theorem, this one due to Gauss, gives the answer.

Theorem 4.2. *(Gauss's Quadratic Reciprocity): The polynomial $x^2 - x - 1$ has two distinct roots modulo p if and only if p is congruent to 1 or 4 modulo 5.*

(The first few such primes are $11, 19, 29, 31$. In general half of all primes have this property.)

Thus we have proved:

Theorem 4.3. *If p is a prime congruent to 1 or 4 modulo 5, then both a_p and b_p divide $p - 1$. In particular, F_{p-1} is divisible by p.*

If p is congruent to 2 or 3 modulo 5, then we have the following result.

Theorem 4.4. *If p is a prime congruent to 2 or 3 modulo 5, then a_p divides $p + 1$ and b_p divides $p^2 - 1$. Thus, F_{p+1} is divisible by p.*

Proof. In this case we know by Quadratic Reciprocity that the polynomial $x^2 - x - 1$ has no roots in $\mathbb{F}_p$, so we see easily that

$$\mathbb{F}_p[x]/(x^2 - x - 1)$$

is a field of order p^2 in which the polynomial has two roots. (In fact, there is only one such field, customarily denoted $\mathbb{F}_{p^2}$, but we will make no use of this fact.) Call the two roots λ and μ. All calculations below occur in this field.

We claim that

$$\lambda^p = \mu \text{ and } \mu^p = \lambda.$$

First we show that λ^p is a root of $x^2 - x - 1$. Indeed, by the Binomial Theorem in characteristic p, we have

$$\lambda^{2p} = (\lambda + 1)^2 = \lambda^p + 1.$$

Thus λ^p is either λ or μ. But the equation $x^p = x$ can have at most p roots in our field. We already know that the elements of $\mathbb{F}_p$ are roots of this equation, and there are p of them. So, since λ is not an element of $\mathbb{F}_p$, it is not a root of $x^p = x$. Thus we have $\lambda^p \neq \lambda$, so $\lambda^p = \mu$.

A similar argument shows that $\mu^p = \lambda$.

Now it follows that

$$\lambda^{p+1} = \lambda\mu = \mu^{p+1},$$

so by our formula for the Fibonacci numbers, we have that

$$F_{p+1} \equiv 0 (\operatorname{mod} p).$$

The assertion about b_p follows from the fact that for any nonzero x in a field of order p^2, we have

$$x^{p^2-1} = 1.$$

This is a consequence of Lagrange's Theorem in group theory. □

Combining the two theorems above (and the fact that $F_5 = 5$), we have proved the advertised result.

Theorem 4.5. *Let p be a prime number. Then one of the three Fibonacci numbers F_{p-1}, F_p and F_{p+1} is a multiple of p.*