On the periodicity of the Fibonacci sequence modulo p

Kyle Miller

May 16, 2017

Recall that the Fibonacci sequence is $f_n = f_{n-1} + f_{n-2}$ with $f_0 = 0$ and $f_1 = 1$. A midterm question asked why it was that $3 \mid f_n$ if $4 \mid n$. In discussion, I asked whether this could be extended to primes other than 3, since we noticed that the tables were periodic far sooner than the pigeonhole principle guarantees, and for the primes we tried the period was $2(p+1)$. Jiahan Du figured it out and wrote up a solution. For those who are interested in abstract algebra, I've rewritten it using some field theory.

Theorem 1. *Let p be an odd prime not equal to 5. Then*

1. *if $p \equiv \pm 1 \pmod 5$, $f_n \equiv f_{n+p-1} \pmod p$ for all n; and*
2. *if $p \equiv \pm 2 \pmod 5$, $f_n \equiv -f_{n+p+1} \pmod p$ for all n.*

Of course, by requiring odd primes the congruences are $p \equiv \pm 1 \pmod{10}$ and $p \equiv \pm 3 \pmod{10}$, respectively.

For the midterm question, since $3 \equiv -2 \pmod 5$, the second case applies, and thus $f_{4k} \equiv -f_{4k+4} \pmod 3$ for all n. Since $f_0 = 0$, it follows that $3 \mid f_n$ if $4 \mid n$.

Definition 2. *For p a prime, the set $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is the field of integers modulo p.*

A field is a number system with addition, subtraction, multiplication, and division. Division can be done in $\mathbb{F}_p$ due to the existence of multiplicative inverses through Bézout's lemma.

Temporarily, we will speak about a general field k. The set of polynomials with coefficients in k and indeterminate x is called $k[x]$. Here is a quick overview of some properties we might care about for a polynomial $f(x) \in k[x]$:

- If $f(x) = g(x)h(x)$ for some $g(x), h(x) \in k[x]$, with neither $g(x)$ nor $h(x)$ a constant polynomial, then $f(x)$ is called *reducible*. Otherwise, $f(x)$ is called *irreducible*.
- If for all $g(x), h(x) \in k[x]$ such that $f(x) \mid g(x)h(x)$ then $f(x) \mid g(x)$ or $f(x) \mid h(x)$, then $f(x)$ is called *prime*. Because of polynomial long division, *prime* is equivalent to *irreducible*.
- If $f(x)$ has a root $\alpha \in k$, then through polynomial long division $f(x) = (x - \alpha)q(x)$ for some quotient $q(x) \in k[x]$. This means (1) if $f(x)$ is irreducible then $f(x)$ has no roots, and (2) $f(x)$ has at most $\deg f(x)$ roots.

If $f(x)$ is irreducible, there is a standard construction to create a new field in which $f(x)$ has a root. The set $k[x]/(f(x))$ is the set of polynomials modulo $f(x)$, and if $[x]$ is the equivalence class of x in $k[x]/(f(x))$, then $f([x]) = [0]$. Through polynomial long division, it's not hard to show that $[x]$ has a multiplicative inverse.

Definition 3. *Given a field k and a field K such that $k \subset K$, then K is called a* field extension *of k. If $\alpha \in K$, the smallest field extension of k containing α is called $k[\alpha]$, the* adjunction of k by α.

Lemma 4. *If $f(x) \in k[x]$ is irreducible, then there is a field extension of k such that $f(x)$ has a root. In particular, $k[x]/(f(x))$ with $\alpha = [x]$.*

For example, $\mathbb{C} = \mathbb{R}[i]$, and $x^2 + 1$ is an irreducible polynomial over $\mathbb{R}$, and $\mathbb{C} \cong \mathbb{R}[x]/(x^2+1)$, with $i = [x]$. In math, a thing *is* what it *does*: i is just a thing that when you square it you get -1, and we have $x^2 \equiv -1 \pmod{x^2+1}$.

It is OK to adjoin an element which already exists in k, you just won't get something that is bigger. For instance, $\mathbb{R}[\sqrt{5}] = \mathbb{R}$. The polynomial $x^2 - 5$ is not irreducible, and factors as $(x-\sqrt{5})(x+\sqrt{5})$, and $\mathbb{R}[\sqrt{5}] \cong \mathbb{R}[x]/(x-\sqrt{5})$.

Definition 5. *If K is a field extension of k, then K can be thought of as a vector space over k. The* degree *of the extension is $\dim_k K$.*

The $\mathbb{C} = \mathbb{R}[i]$ example gives that the degree of $\mathbb{C}$ over $\mathbb{R}$ is two. In general, the degree of the extension is the degree of the corresponding irreducible polynomial, if the extension is finite, hence why it is called "degree."

Now let us go back to $k = \mathbb{F}_p$.

Lemma 6. *If K is a finite field extension of $\mathbb{F}_p$, then the map $F : K \to K$ defined by $F(x) = x^p$ is an automorphism. Furthermore, for $a \in K$, $F(a) = a$ if and only if $a \in \mathbb{F}_p$; which is to say $\mathbb{F}_p$ is the* fixed field *of F. The map F is called the* Frobenius automorphism.

Proof. A *field automorphism* is a map which is a field homomorphism ($F(1) = 1$, $F(a+b) = F(a)+F(b)$ and $F(ab) = F(a)F(b)$), which has the domain equaling the codomain, and which is a bijection. Multiplication is clear:

$$F(ab) = (ab)^p = a^p b^p = F(a)F(b).$$

Addition is trickier:

$$F(a+b) = (a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i} b^i$$

Excercise for the reader: for prime p and $1 \le i \le n-1$, then $p \mid \binom{p}{i}$. Then we continue:

$$= a^p + b^p = F(a) + F(b)$$

The fact it is a bijection is because it is injective and $|K|$ is finite. Injectivity is because if $F(a) = 0$ with $a \neq 0$, then $F(1) = F(aa^{-1}) = F(a)F(a^{-1}) = 0F(a^{-1}) = 0$, contradicting the fact that $F(1) = 1$.

If $a \in \mathbb{F}_p$, then Fermat's little theorem says $a^p \equiv a \pmod{p}$, so $\mathbb{F}_p$ is certainly fixed by F. For the converse, an element $a \in K$ is fixed by F if $a^p - a = 0$, which is to say if it is a root of $x^p - x$. Since we know $0, \dots, p-1 \in \mathbb{F}_p$ are roots of $x^p - x$, there can be no other roots. □

An interesting thing about a field automorphism is that, if the coefficients of a polynomial are fixed by the automorphism, then roots get sent to roots. For, if $f(x) = c_0 + c_1 x + \cdots + c_n x^n$, $c_0, \dots, c_n \in \mathbb{F}_p$, and α a root of f,

$$\begin{aligned} 0 = F(0) = F(f(\alpha)) &= F(c_0 + c_1\alpha + \cdots + c_n\alpha^n) \\ &= F(c_0) + F(c_1)F(\alpha) + \cdots + F(c_n)F(\alpha)^n \\ &= c_0 + c_1 F(\alpha) + \cdots + c_n F(\alpha)^n = f(F(\alpha)). \end{aligned}$$

Now to our original problem. One way to study the Fibonacci sequence is as a linear system

$$\begin{pmatrix} f_{n+1} \\ f_{n+2} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} f_n \\ f_{n+1} \end{pmatrix},$$

which in closed form is

$$\begin{pmatrix} f_n \\ f_{n+1} \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}^n \begin{pmatrix} 0 \\ 1 \end{pmatrix}.$$

With φ the root of the characteristic polynomial $x^2 - x - 1$ over $\mathbb{F}_p$, the transition matrix A is readily diagonalized over $\mathbb{F}_p[\varphi]$:

$$A = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ \varphi & 1-\varphi \end{pmatrix} \begin{pmatrix} \varphi & 0 \\ 0 & 1-\varphi \end{pmatrix} \begin{pmatrix} 1 & 1 \\ \varphi & 1-\varphi \end{pmatrix}^{-1}$$

(Using the modulo idea, we can get many relations on φ. For instance, $\varphi^2 = \varphi + 1$, $\varphi(\varphi - 1) = 1$ so $\varphi^{-1} = \varphi - 1$, and $(1-\varphi)^{-1} = -\varphi$.) The diagonalization yields a periodicity if $\varphi^n = (1-\varphi)^n = 1$, or an "odd periodicity" if $\varphi^n = (1-\varphi)^n = -1$.

If $\varphi \in \mathbb{F}_p$, then by Fermat's little theorem, $\varphi^{p-1} = 1$ and $(1-\varphi)^{p-1} = 1$, since $\varphi, 1-\varphi$ are not zero in $\mathbb{F}_p$. Then, the period must divide $p-1$. There is a paper on "Fibonacci primitive roots"[1] which says that the period might not equal $p-1$, for instance $p = 29$ has $\varphi^{14} = 1$.

If $\varphi \notin \mathbb{F}_p$, then $F(\varphi) \neq \varphi$, yet $F(\varphi)$ must still be a root of the characteristic polynomial, so $F(\varphi)$ must be the other root $1-\varphi$. Since this means $\varphi^p = 1-\varphi$ and $(1-\varphi)^p = \varphi$, we have

$$\begin{aligned} \varphi^{p+1} &= \varphi(1-\varphi) = -1 \\ (1-\varphi)^{p+1} &= (1-\varphi)\varphi = -1. \end{aligned}$$

Thus, the period must divide $2(p+1)$, with an "odd period" dividing $p+1$.

Now to characterize the condition $\varphi \in \mathbb{F}_p$. The quadratic formula gives $\varphi = \frac{1}{2}(1+\sqrt{5})$, so for an odd prime $p \neq 5$, $\mathbb{F}_p[\varphi] = \mathbb{F}_p[\sqrt{5}]$. This is simply the question of whether $x^2 - 5$ is an irreducible polynomial in $\mathbb{F}_p$, or rather whether 5 is not a quadratic residue. Using quadratic reciprocity of the Jacobi symbol,

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

which is 1 if $p \equiv \pm 1 \pmod 5$ and which is -1 if $p \equiv \pm 2 \pmod 5$. Hence:

1. If $p \equiv \pm 1 \pmod 5$, then $\mathbb{F}_p$ contains a square root of 5, in which case $A^{p-1} = I_2$.

2. If $p \equiv \pm 2 \pmod 5$, then $\mathbb{F}_p$ does not contain a square root of 5, in which case $A^{p+1} = -I_2$.

This completes the proof.

Question: Can the actual period be characterized further?

[1] `http://www.fq.math.ca/Scanned/10-2/shanks-a.pdf`