4-1-2012

Splitting Fields and Periods of Fibonacci Sequences Modulo Primes

Sanjai Gupta
Irvine Valley College

Parousia Rockstroh '08
Harvey Mudd College

Francis E. Su
Harvey Mudd College

REFERENCES

1. Ward Cheney and Will Light, *A Course in Approximation Theory*, American Mathematical Society, Providence, RI, 2009
2. Dan Kalman, The Generalized Vandermonde Matrix, *Math. Mag.* **28** (1984) 15–21; http://dx.doi.org/10.2307/2690290.
3. Allan Klinger, The Vandermonde Matrix, *Amer. Math. Monthly* **74** (1967) 571–574; http://dx.doi.org/10.2307/2314898.
4. David C. Lay, *Linear Algebra and its Applications*, Addison-Wesley, 1994.
5. Joseph J. Rushanan, On the Vandermonde Matrix, *Amer. Math. Monthly* **96** (1989) 921–924; http://dx.doi.org/10.2307/2324589.
6. Mariam Schapiro Grosof and Geraldine Taiani, Vandermonde Strikes Again, *Amer. Math. Monthly* **100** (1993) 575–577; http://dx.doi.org/10.2307/2324617.

Summary Let $a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_n$ be real numbers and the $n \times n$ matrix C be defined with entries $c_{ij} = (a_i + b_j)^k$, where k is a positive integer. If $n > k + 1$, then $\det(C) = 0$, and if $n = k + 1$, then $\det(C)$ is a product involving two Vandermonde determinants.

Splitting Fields and Periods of Fibonacci Sequences Modulo Primes

SANJAI GUPTA
Irvine Valley College
Irvine, CA 92618
sgupta@ivc.edu

PAROUSIA ROCKSTROH
Simon Fraser University
Burnaby, British Columbia V5A 1S6, Canada
parousia_rockstroh@sfu.ca

FRANCIS EDWARD SU
Harvey Mudd College
Claremont, CA 91711
su@math.hmc.edu

The Fibonacci sequence defined by $F_0 = 0$, $F_1 = 1$, $F_{n+1} = F_n + F_{n-1}$ is clearly periodic when reduced modulo an integer m, since there are only finitely many possible pairs of consecutive elements chosen from $\mathbb{Z}/m\mathbb{Z}$ (in fact, m^2 such pairs) and any such pair determines the rest of the sequence, both forwards and backwards. What is the period of this sequence?

An upper bound is $m^2 - 1$ (since the sequence does not have a consecutive pair of 0's), but the period is often much smaller. As examples, the Fibonacci sequence mod 11 is:

$$0, 1, 1, 2, 3, 5, 8, 2, 10, 1, 0, 1, 1, \ldots$$

and has period 10; the Fibonacci sequence mod 7 is:

$$0, 1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, 1, 1, \ldots$$

and has period 16.

Math. Mag. **85** (2012) 130–135. doi:10.4169/math.mag.85.2.130.

This problem was first considered by Wall [**8**] and shortly thereafter by Robinson [**5**]. Among other cases, they studied the Fibonacci sequence for prime moduli, and showed that for primes p that are congruent to 1 or 4 (mod 5) the period length of the Fibonacci sequence mod p divides $p-1$, while for primes p that are congruent to 2 or 3 (mod 5) the period length divides $2(p+1)$. The examples above illustrate these facts. As we will see, the prime $p=5$ is a special case with period 20; the prime $p=2$ is also special in some ways with period 3.

Wall's proofs use different combinatorial techniques for each of these classes of primes. Robinson proves these results by appealing to a directed graph of points formed by multiplication by a *Fibonacci matrix*. In this paper, we give alternative proofs of these results that also use the Fibonacci matrix, but unlike Robinson, we place the roots of its characteristic polynomial in an appropriate splitting field. This allows us to obtain bounds for the periods of the more general recurrence

$$E_{n+1} = AE_n + BE_{n-1}$$

modulo a prime, which neither Wall nor Robinson consider.

Vella and Vella [**7**] consider general recurrences, but only in the special case where the roots of the characteristic polynomial are integers. Using sophisticated methods, Pinch [**3**] proves general results about multiple-term recurrences with prime power moduli, but does not produce specific bounds of the kind that we consider here. Li [**4**] reviews prior work on period lengths of general recurrences in the context of a different problem: determining which residue classes appear in recurrence sequences.

The purpose of our brief paper is to illustrate an accessible, motivated treatment of this classical topic using only ideas from linear and abstract algebra (rather than the case-by-case analysis found in many papers on the subject, or techniques from graduate number theory). Our methods extend to general recurrences with prime moduli and provide some new insights, e.g., Theorem 8, below. And our treatment highlights a nice application of the use of splitting fields (explained below) that might be suitable to present in an undergraduate course in abstract algebra or Galois theory.

Eigenvalues of the Fibonacci matrix

Let p be an odd prime.

In accordance with previous literature [**5, 8**] we define $k(p)$, the *period* of the Fibonacci sequence mod p, to be the smallest positive index i such that $F_i \equiv 0 \bmod p$ and $F_{i+1} \equiv 1 \bmod p$. In our examples above, $k(11) = 10$, while $k(7) = 16$. Following Robinson [**5**], we consider the Fibonacci matrix:

$$U = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}.$$

This is a matrix over some field $\mathbb{F}$ that we should be careful to specify. If we choose $\mathbb{F} = \mathbb{R}$, then

$$U^n = \begin{bmatrix} F_{n+1} & F_n \\ F_n & F_{n-1} \end{bmatrix}.$$

And if we choose $\mathbb{F} = \mathbb{F}_p$, the finite field of order p (also known as $\mathbb{Z}/p\mathbb{Z}$, the integers mod p) then the entries of U^n are elements of the Fibonacci sequence mod p, the desired objects of study.

It is natural to consider the eigenvalues of the matrix U, which are roots of its characteristic polynomial $x^2 - x - 1$. If eigenvalues $\lambda, \bar{\lambda}$ exist in $\mathbb{F}_p$ and are distinct,

then $U = CDC^{-1}$ where D is the diagonal matrix

$$D = \begin{bmatrix} \lambda & 0 \\ 0 & \bar{\lambda} \end{bmatrix} \tag{1}$$

and C is a matrix with the corresponding eigenvectors as columns. Then $U^k = CD^kC^{-1}$. We see that for $k = k(p)$, we have $U^k = I$, the identity matrix. Therefore $D^k = C^{-1}U^kC$ is also I. We observe that the exponent $k = k(p)$ is the smallest non-zero exponent n such that $D^n = I$. Thus:

LEMMA 1. *The period $k(p)$ must divide any n that satisfies $D^n = I$.*

When do the eigenvalues $\lambda, \bar{\lambda}$ exist in $\mathbb{F}_p$? The quadratic formula shows that $ax^2 + bx + c$ has roots in the field $\mathbb{F}_p$ as long as the discriminant $\Delta = b^2 - 4ac$ is a square in $\mathbb{F}_p$; hence the characteristic polynomial $x^2 - x - 1$ has roots in $\mathbb{F}_p$ if and only if $\Delta = 5$ is a square. Quadratic reciprocity [**6**] shows that if p is an odd prime, then 5 is a square in $\mathbb{F}_p$ if and only if $p \equiv 0, 1, 4 \bmod 5$. And as long as $p \neq 5$, the eigenvalues are distinct. Hence:

THEOREM 2. *If p is an odd prime and p is congruent to* 1 *or* 4 *(*mod 5*), then $k(p)$ divides $p - 1$. In particular, $k(p) \leq p - 1$.*

Proof. The eigenvalues $\lambda, \bar{\lambda}$ of U are non-zero (since U is invertible) and distinct (since $p \neq 5$). Since p is prime, Fermat's (little) theorem implies both $\lambda^{p-1} = 1$ and $\bar{\lambda}^{p-1} = 1$. Hence $D^{p-1} = I$ and Lemma 1 gives the desired conclusion. ∎

When $p = 5$, the eigenvalues are not distinct (they are both 3) and D is not diagonal, so $D^4 \neq I$ even though $\lambda^4 = \bar{\lambda}^4 = 1$. One finds that $D^{20} = I$ and $k(5) = 20$.

A splitting field for the eigenvalues

The case of remaining classes of odd primes, $p \equiv 2, 3 \bmod 5$, requires more work, because for these primes, the characteristic polynomial $x^2 - x - 1$ is *irreducible.* It does not have roots in $\mathbb{F}_p$ unless we enlarge the field.

We can do this by a standard construction: to the field $\mathbb{F}_p$, we "adjoin" an element γ that has the property that $\gamma^2 = \gamma + 1$, and consider the set of linear combinations of 1 and γ over $\mathbb{F}_p$ with the natural arithmetic.

Let's make this construction more precise. As a set, the enlarged field has p^2 elements:

$$\mathbb{F}_{p^2} = \{a + b\gamma : a, b \in \mathbb{F}_p\}$$

We may regard these as formal expressions or as a particular way to write ordered pairs (a, b). They are added and multiplied as if γ were a number satisfying $\gamma^2 - \gamma - 1 = 0$. Here's a sample calculation: $(1 - \gamma)(\gamma) = \gamma - \gamma^2 = \gamma - (\gamma + 1) = -1$. With these operations, $\mathbb{F}_{p^2}$ is a field. In fact it is the unique finite field of size p^2 and some may recognize it also as the quotient field $\mathbb{F}_p[x]/(x^2 - x - 1)$, though this insight is not needed in what follows.

Note that the expressions of the form $a + 0\gamma$ (with $b = 0$) form a subfield identical to $\mathbb{F}_p$ itself. In this way we regard $\mathbb{F}_p$ as a subfield of $\mathbb{F}_{p^2}$. We note that this subfield obeys Fermat's theorem, so

$$a^p = a$$

holds for all $a \in \mathbb{F}_p$.

By construction, γ is automatically a root of $x^2 - x - 1$ in $\mathbb{F}_{p^2}$. One may check that

$$\bar{\gamma} = 1 - \gamma$$

is another root, distinct from γ. We will need the fact that $\gamma\bar{\gamma} = -1$, which follows from the sample calculation above.

Also by construction, $\mathbb{F}_{p^2}$ has *characteristic* p: any element $a + b\gamma$ multiplied by p (e.g., added to itself p times) is 0, since the coefficients a, b come from $\mathbb{F}_p$. So the following nifty fact holds, sometimes facetiously called "freshman exponentiation" [**1**, p. 422]: if $\mu, \nu \in \mathbb{F}_{p^2}$, then

$$(\mu + \nu)^p = \mu^p + \nu^p. \tag{2}$$

This follows from the binomial theorem. When p is prime and k is not equal to 0 or p, the binomial coefficient $\binom{p}{n}$ is divisible by p. Therefore all of the intermediate terms of the binomial expansion of $(\mu + \nu)^p$ vanish, and (2) holds.

This is the basis of an important lemma. We briefly consider an arbitrary polynomial in $\mathbb{F}_p$:

LEMMA 3. *If $P(x)$ is an irreducible polynomial in $\mathbb{F}_p$ that has a root γ in $\mathbb{F}_{p^2}$, then γ^p must be a different root of $P(x)$.*

(This is a standard fact in Galois theory: the *Frobenius map* $x \to x^p$ transitively permutes the roots of irreducible polynomials, though we have avoided that language here to keep this treatment friendly.)

Proof. Let $P(x) = a_n x^n + \cdots + a_0$ where $a_i \in \mathbb{F}_p$, and suppose γ is a root. Then

$$\begin{aligned} P(\gamma^p) &= a_n\gamma^{pn} + \cdots + a_0 \\ &= a_n^p\gamma^{np} + \cdots + a_0^p \\ &= (a_n\gamma^n + \cdots + a_0)^p \\ &= 0^p = 0. \end{aligned}$$

The second line follows because Fermat's theorem ($a = a^p$) holds for elements of $\mathbb{F}_p$, and the third line follows from freshman exponentiation.

So γ^p is a root of $P(x)$. Further, $\gamma^p \neq \gamma$, because there are at most p solutions to the equation $x^p = x$, and Fermat's theorem shows they are all the elements of the subfield $\mathbb{F}_p$. Therefore γ is not a solution, and γ^p must be a different root of $P(x)$. ∎

Returning to the case of $P(x) = x^2 - x - 1$, we immediately obtain:

LEMMA 4. *If $p \equiv 2, 3 \bmod 5$, then*

$$\gamma^p = \bar{\gamma} \quad \text{and} \quad \bar{\gamma}^p = \gamma.$$

Proof. These statements follow from the fact that $x^2 - x - 1$ is irreducible in $\mathbb{F}_p$ when $p \equiv 2, 3 \bmod 5$, but has exactly two roots γ and $\bar{\gamma}$ in $\mathbb{F}_{p^2}$. ∎

Now we may determine the desired bound:

THEOREM 5. *Let p be an odd prime that is congruent to 2 or 3 (*mod 5*) then $k(p)$ divides $2(p + 1)$. In particular, $k(p) \leq 2(p + 1)$.*

Proof. We appeal to Lemma 1, now viewing the matrices U and D in the prior discussion with elements from the enlarged field $\mathbb{F}_{p^2}$. Note that the diagonal entries $\lambda, \bar{\lambda}$ of D in (1) are then the roots $\gamma, \bar{\gamma}$ of $x^2 - x - 1$.

Applying Lemma 4 ($\gamma^p = \bar{\gamma}$) and the fact that $\gamma\bar{\gamma} = -1$, we see that

$$\gamma^{2(p+1)} = (\gamma^p)^2\gamma^2 = \bar{\gamma}^2\gamma^2 = (-1)^2 = 1. \tag{3}$$

By reversing roles of $\gamma, \bar{\gamma}$ we see that $\bar{\gamma}^{2(p+1)} = 1$ as well. These conclusions show that $D^{2(p+1)} = I$, as desired in Lemma 1. ∎

As Wall [**8**] notes, the upper bounds of Theorems 2 and 5 are tight for many small odd primes $p \neq 5$ (for $p < 100$, the only exceptions are 29, 47, and 89). The bounds appear to be less tight for larger p. Wall also shows for prime powers, $k(p^t) \leq p^{t-1}k(p)$ with equality if $k(p^2) \neq k(p)$. It is believed the latter condition always holds; see [**2**] for partial results. Combining knowledge of $k(p^t)$ with the fact that $\text{lcm}[k(m), k(n)] = k(\text{lcm}[m, n])$, one can obtain a bound on $k(m)$ for each positive integer m.

The general recurrence

Our methods can be adapted to obtain bounds for the period of the general recurrence

$$E_{n+1} = AE_n + BE_{n-1}$$

modulo a prime p, with $E_0 = 0$ and $E_1 = 1$. Let $k_{A,B}(p)$ be the period of E_n mod p. The analog of the Fibonacci matrix becomes

$$U = \begin{bmatrix} A & B \\ 1 & 0 \end{bmatrix},$$

and the eigenvalues $\lambda, \bar{\lambda}$ are roots of the characteristic polynomial $x^2 - Ax - B$. This has roots in $\mathbb{F}_p$ as long as the discriminant

$$\Delta = A^2 + 4B$$

is a square in $\mathbb{F}_p$ (a *quadratic residue* mod p), and they are distinct if $\Delta \not\equiv 0 \bmod p$. The same arguments as in Theorem 2 will yield:

THEOREM 6. *If p is an odd prime and Δ is a non-zero quadratic residue mod p, then $k_{A,B}(p)$ divides $p - 1$. In particular $k_{A,B}(p) \leq p - 1$.*

For example, consider $E_{n+1} = 3E_n + 2E_{n-1}$ mod 13. Then $A = 3$, $B = 2$, and $\Delta = 17$. Since $\Delta \equiv 2^2 \bmod 13$, Δ is a non-zero quadratic residue mod 13. Our theorem shows that $k_{3,2}(13) \leq 12$ (and, in fact, it is 12).

A curious consequence of our theorem is that the sequence $E_{n+1} = E_n + 2E_{n-1}$ mod p has small period (that divides $p - 1$) for *every* odd prime p except 3 (since $\Delta = 3^2$ is always a square and the only prime p that divides Δ is 3).

If the discriminant Δ is not a square in $\mathbb{F}_p$, we consider U as a matrix with entries from $\mathbb{F}_{p^2}$, the splitting field of $x^2 - Ax - B$ obtained by adjoining an element γ that satisfies $\gamma^2 = A\gamma + B$. The roots of the characteristic polynomial $x^2 - Ax - B$ in $\mathbb{F}_{p^2}$ are then γ and $\bar{\gamma} = A - \gamma$. The irreducibility of $x^2 - Ax - B$ over $\mathbb{F}_p$ and Lemma 3 show that

LEMMA 7. *If Δ is a quadratic nonresidue mod p, then*

$$\gamma^p = \bar{\gamma} \quad \text{and} \quad \bar{\gamma}^p = \gamma.$$

We can now obtain the following result. Let $\text{ord}(n)$ denote the *multiplicative order* of n: the smallest positive integer t such that $n^t \equiv 1 \bmod p$.

THEOREM 8. *If Δ is a quadratic nonresidue mod p, then $k_{A,B}(p)$ is a divisor of $2(p+1)\cdot \operatorname{ord}(B^2)$. In particular,*

$$k_{A,B}(p) \le 2(p+1)\cdot \operatorname{ord}(B^2).$$

Proof. We mimic the proof of Theorem 5. In light of Lemma 1, our goal is to show that

$$\gamma^{2(p+1)} = \bar{\gamma}^{2(p+1)} = B^2.$$

But these follow easily by noting $\gamma\bar{\gamma} = -B$, using Lemma 7, and repeating a similar calculation as (3). ∎

Note that if $B = 1$, then the original bound $2(p+1)$ still holds. For example, consider $E_{n+1} = 3E_n + E_{n-1} \bmod 19$. Then $A = 3$, $B = 1$, and $\Delta = 13$. Since 13 is a nonresidue mod 19, our theorem shows $k_{3,1}(19)$ divides 40 (and, in fact, it is 40). For the same sequence mod 11, we find that 13 is a nonresidue mod 11, so $k_{3,1}(11)$ divides $2(11+1) = 24$ (and, in fact, it is 8).

For a general example where $B \neq 1$, consider $E_{n+1} = 3E_n + 2E_{n-1} \bmod 7$. Then $A = 3$, $B = 2$, and $\Delta = 17$. Since 17 is a nonresidue mod 7, and $B^2 = 4$ satisfies $4^3 \equiv 1 \bmod 7$, our theorem shows that the period $k_{3,2}$ divides $2(7+1)\cdot 3 = 48$ (and, in fact, is 48).

In general, we note that $\operatorname{ord}(B^2)$ is at most $(p-1)/2$ by Fermat's theorem, so the bound in Theorem 8 could be as high as $2(p+1)(p-1)/2 = p^2 - 1$, the bound at the beginning of this paper. This bound is actually achieved by $E_{n+1} = 3E_n + 2E_{n-1} \bmod 37$, the sequence

$$0, 1, 3, 11, 2, 28, 14, 24, 26, 15, 23, 25, 10, 6, 1, 15, 10, 23, 15, 17, \ldots$$

which has period $1368 = (37+1)(37-1)$, and indicates that all possible consecutive pairs other than 0, 0 appear in this sequence mod 37.

Acknowledgment Francis Edward Su was supported in part by NSF DMS-0701308 and NSF DMS-1002938.

REFERENCES

1. J. B. Fraleigh, *A First Course in Abstract Algebra*, 7th ed., Addison Wesley, Boston, 2003.
2. S. E. Mamangakis, Remarks on the Fibonacci series modulo m, *Amer. Math. Monthly* **68** (1961) 648–649; http://dx.doi.org/10.2307/2311514.
3. R. G. E. Pinch, Recurrent sequences modulo prime powers, in *Cryptography and coding, III* (*Cirencester, 1991*), 297–310, *Inst. Math. Appl. Conf. Ser. New Ser.*, **45**, Oxford University Press, New York, 1993.
4. H. C. Li, Complete and reduced residue systems of second-order recurrences modulo p, *Fib. Quart.* **38** (2000) 272–281.
5. D. W. Robinson, The Fibonacci matrix modulo m, *Fib. Quart.* **1** (1963) 29–36.
6. W. Stein, *Elementary Number Theory: Primes, Congruences, and Secrets*, Springer, New York, 2008.
7. D. Vella and A. Vella, Cycles in the generalized Fibonacci sequence modulo a prime, *Math. Mag.* **75** (2002) 294–299; http://dx.doi.org/10.2307/3219168.
8. D. D. Wall, Fibonacci series modulo m, *Amer. Math. Monthly* **67** (1960) 525–532; http://dx.doi.org/10.2307/2309169.

Summary We consider the period of a Fibonacci sequence modulo a prime and provide an accessible, motivated treatment of this classical topic using only ideas from linear and abstract algebra. Our methods extend to general recurrences with prime moduli and provide some new insights. And our treatment highlights a nice application of the use of splitting fields that might be suitable to present in an undergraduate course in abstract algebra or Galois theory.