

**Remark** As a bonus, we have another proof of integral (4) deduced from series (6).

We have seen a variety of evaluations of the Poisson integral. The interested reader is encouraged to investigate additional approaches.

**Acknowledgment.** I wish to thank Brian Bradie and the referees for their helpful suggestions.

## REFERENCES

1. D. Logan, *Applied Partial Differential Equations*, Springer, New York, 1998.
2. G. Tolstov, *Fourier Series*, Dover Books, New York, 1962.
3. J. E. Marsden & M. J. Hoffman, *Basic Complex Analysis*, Freeman, New York, 1987.

# Cycles in the Generalized Fibonacci Sequence modulo a Prime

DOMINIC VELLA

ALFRED VELLA

194 Buckingham Rd.  
Bletchley, Milton Keynes, UK, MK3 5JB  
Fibonacci@thevellas.com

Since their invention in the thirteenth century, Fibonacci sequences have intrigued mathematicians. As well as modeling the population patterns of overly energetic rabbits, however, they have sparked developments in more serious mathematics. For example, generalized Fibonacci sequences crop up in all manner of situations, from fiber optic networks [3] to computer algorithms [1] to probability theory [2].

In this article, we study generalized Fibonacci sequences  $\{G(n)\}$ , given by the recurrence relation:  $G(n) = aG(n-1) + bG(n-2)$  for  $a, b, G(0)$  and  $G(1)$  integers. We also study the periods of repetition in such sequences when considered modulo  $p$ , a prime. For one particular class of generalized Fibonacci numbers, we find a surprising connection with Fermat's Last Theorem. Other connections between these two seemingly unrelated subjects have been discovered in the past [8], but the one unearthed here allows us to calculate the length of these repetitions or *cycles* exactly.

**Some useful results** When working with the generalized Fibonacci sequences described above, we will need some results to make our lives easier. It is well known that the usual Fibonacci numbers (that is  $a = b = 1$ ,  $G(0) = 0$ ,  $G(1) = 1$ ) can be expressed using Binet's formula [5]:

$$\sqrt{5}G(n) = \left(\frac{1 + \sqrt{5}}{2}\right)^n - \left(\frac{1 - \sqrt{5}}{2}\right)^n.$$

This is easily derived by guessing a solution to the recurrence of the form  $G(n) = \lambda^n$ , solving for  $\lambda$ , and matching with the initial conditions. In a similar way, many number theory texts (see for example, Niven and Zuckermann [7]) prove that the analogous Binet formula for our sequence is

$$(A - B)G(n) = G(1)(A^n - B^n) + G(0)(AB^n - BA^n), \quad (1)$$

where

$$A = \frac{a + \sqrt{a^2 + 4b}}{2}, B = \frac{a - \sqrt{a^2 + 4b}}{2},$$

provided  $a^2 + 4b \neq 0$ .

In this article, we will focus on those generalized Fibonacci sequences where  $A$  and  $B$  are both integers. We do this because it will lead us to nicer and more exact results later, but first we should investigate what it means for our sequence. If  $a^2 + 4b = x^2$  (where  $x$  is an integer) then  $x$  has the same parity as  $a$ . The fact that  $A$  and  $B$  are both integers follows immediately from this. Conversely, since  $a^2 + 4b = (2A - a)^2$ , then if  $A$  and  $B$  are both integers it is clear that  $a^2 + 4b$  is a perfect square. This is the first of our useful results and we summarize it as:

(I)  $A$  and  $B$  are integers if and only if  $a^2 + 4b \neq 0$  is a perfect square.

In order to obtain more results concisely, we can also use Fibonacci matrices that are defined to be

$$\mathbf{G}_k = \begin{pmatrix} G(k+2) & G(k+1) \\ G(k+1) & G(k) \end{pmatrix}, \mathbf{M} = \begin{pmatrix} a & b \\ 1 & 0 \end{pmatrix}.$$

A simple induction shows that  $\mathbf{G}_n = \mathbf{M}^n \mathbf{G}_0$ . If we then take determinants of this equation we have the second of our results:

(II)  $G(n+2)G(n) - G(n+1)^2 = (-b)^n(G(2)G(0) - G(1)^2)$ .

Now that we have these results at our disposal, we can begin to answer the real question we are interested in: What can we say about these generalized Fibonacci sequences when looking at them modulo  $p$ ?

**Finding points of repetition in the sequence** Using (1) in conjunction with the result (I), we are able to discover some interesting divisibility properties of this class of Fibonacci sequence. Central to much of this work is Fermat's Little Theorem, which states that  $x^p \equiv x \pmod{p}$  for all primes  $p$  and integers  $x$ . Because this result only works for integers, we need to ensure that  $A$  and  $B$  are both integers, that is, that  $a^2 + 4b = x^2$ , for some nonzero integer  $x$ , and we shall continue to do so for the rest of the article. Reducing the Binet analog (Equation 1) modulo  $p$ , and using Fermat's Little Theorem, it is easy to show that  $G(p) \equiv G(1) \pmod{p}$  if  $(x, p) = 1$ . A similar argument, involving such easy formulas as  $A^2 - B^2 = ax$ , shows that

$$G(p+1) \equiv (aG(1) + bG(0)) \pmod{p} \equiv G(2) \pmod{p}.$$

But,  $G(p+1) = aG(p) + bG(p-1)$ , so that

$$bG(p-1) \equiv G(2) - aG(1) \pmod{p} \equiv bG(0).$$

If  $(b, p) = 1$ , we can conclude that  $G(p-1) \equiv G(0) \pmod{p}$ . The conditions  $(x, p) = (b, p) = 1$  are so important in the work we do that if  $p$  is a prime satisfying them, we say that  $p$  is a *Level 1 prime with respect to the sequence generated by  $a$  and  $b$*  abbreviated to " $p$  is LI wrt  $a, b$ ." The last result can now be written:

(III) If  $p$  is LI wrt  $a, b$  then  $G(p-1) \equiv G(0) \pmod{p}$  and  $G(p) \equiv G(1) \pmod{p}$ .

**What about cycles then?** Before we begin to think about cycles, it is important to have clear in our minds what we mean by the cycle length of the generalized Fibonacci

sequence. In general, sequences that eventually settle down into nice cycles can exhibit strange behavior for a finite number of terms. So we define the set  $\mathcal{C}_p$  as follows, in order to identify *eventual* cycles in the sequence:

$$\mathcal{C}_p = \{c > 0 \mid G(n+c) \equiv G(n), G(n+c+1) \equiv G(n+1), \text{ for } n \text{ sufficiently large}\}$$

Here, as in the rest of the paper, all equivalences are to be understood as being mod  $p$ . Then we set  $C(p) = \min \mathcal{C}_p$ ; this is what we mean by the cycle length of a particular sequence repeating modulo  $p$ . (The dependence of  $C(p)$  on  $a$  and  $b$  is implicit.)

The most interesting results are obtained by considering only the Level I primes with respect to the sequences generated by  $a$  and  $b$ . Perhaps the most obvious questions to ask about the sequences reduced modulo these primes are (i) Did we really need to worry about cycles beginning far out on the sequence? and (ii) Is there a finite cycle length at all?

The answer is affirmative to each of these questions and, at least for question (ii), it is not too hard to see why. There are only a total of  $p^2$  different pairings of numbers in the sequence (since we are dealing only with the numbers  $0, \dots, (p-1)$ ) and so we must have  $C(p) \leq p^2$ .

Question (i) is a little harder to answer, so we shall do this more slowly! Suppose that the cyclic behavior begins with the  $n$ th term, so that

$$G(n+c) \equiv G(n), \text{ and } G(n+c+1) \equiv G(n+1),$$

but  $G(n-1+c) \not\equiv G(n-1)$ . Expressing  $G(n+c-1)$  and  $G(n-1)$  in terms of their successors, using the recursion relation, gives  $bG(n+c-1) \equiv bG(n-1)$ . As  $(b, p) = 1$ , we see that the cycle must begin at the beginning, with  $G(C(p)) \equiv G(0)$ ,  $G(C(p)+1) \equiv G(1)$ , as we would have liked.

**$p^2$  can't be the best bound!** There is indeed a better bound on the cycle length than  $p^2$  (We already knew this for Level I primes, since by (3) a cycle must have occurred by  $p-1$ ). In fact, we can do substantially better than that and in some cases, we can even calculate the exact cycle length, but that will have to wait for a few more sections. In the meantime, we shall obtain results analogous to those obtained by many other people for the normal and generalized Fibonacci sequences. The seminal articles on this subject are those by Wall [9] (who invented the subject!) and Li [6], although the results we obtain are in some ways nicer.

To demonstrate this kind of sequence, we look at the case  $a = 1, b = 2$  with  $G(0) = 0, G(1) = 1$ . This gives us the generalized Fibonacci sequence beginning

$$0, 1, 1, 3, 5, 11, 21, 43, \dots$$

Reduced modulo 11, which is LI wrt 1, 2, we have the sequence  $0, 1, 1, 3, 5, 0, -1, -1, -3, -5, 0, 1, 1, 3, 5, \dots$

This sequence clearly repeats every tenth term, so we write  $C(11) = 10$ . The result we now obtain will help to explain why the answer here is 10, though we will not know the full story until later. By (3), we know that  $C(p) \leq p-1$ , and we can write

$$G(kC(p)) \equiv G(p-1) \quad \text{for all integers } k \geq 0.$$

If we assume that  $C(p)$  is not a divisor of  $p-1$  and let  $j$  be the floor of  $(p-1)/C(p)$ , that is,

$$j = \left\lfloor \frac{p-1}{C(p)} \right\rfloor \neq \frac{p-1}{C(p)},$$

then we find that we have a repetition in the Fibonacci sequence between  $G(jC(p))$  and  $G(p-1)$  that is shorter than  $C(p)$ . This contradicts the fact that  $C(p)$  was taken to be the smallest cycle length, and so we conclude that  $C(p) \mid p-1$ . This gives us one of our most important results:

(IV) For all LI primes  $p$  wrt  $a, b$ ,  $C(p) \mid p-1$ .

The theorem corresponding to this last result in Wall's 1960 paper [9] on the normal Fibonacci numbers has a more complicated result than ours, as we had the luxury of looking at the case where  $A$  and  $B$  are integers. The reason we say our results are nicer is that  $a^2 + 4b = x^2$  and so is a quadratic residue of all primes whereas 5 (which is  $a^2 + 4b$  for the usual Fibonacci numbers) is only a quadratic residue of primes of the form  $10n \pm 1$ .

In the example at the beginning of this section we had  $a = 1$ ,  $b = 2$ ,  $G(0) = 0$ ,  $G(1) = 1$ , and  $C(11) = 10$ . In this case, our upper bound for  $C(p)$  is met but for the time being we are unable to provide a similar lower bound. As we shall see, however, it is no accident that in this particular case the upper bound is met.

**Another viewpoint on cycles** If we want to progress much farther, it is useful to try and understand what causes a Fibonacci cycle. This is a very deep question and we can only partially answer it here. Primarily, we are interested in the order of  $A$  and  $B$  modulo  $p$  ( $\text{ord}_p(A)$ , etc.), where the *order* is the smallest nontrivial exponent  $e$  such that, for example,  $A^e \equiv 1 \pmod{p}$ . If  $\text{ord}_p(A) \mid r$  and  $\text{ord}_p(B) \mid r$ , then the Binet analog shows that terms  $r$  and  $(r+1)$  of our sequence are

$$G(r) \equiv \frac{1}{A-B} (G(1)(1-1) + G(0)(A-B)) \equiv G(0)$$

$$G(r+1) \equiv \frac{1}{A-B} (G(1)(A-B) + G(0)(AB-BA)) \equiv G(1)$$

so that a cycle begins at  $r$ .

Conversely, if  $G(r) \equiv G(0)$ ,  $G(r+1) \equiv G(1)$ , then we have:

$$G(0)(A-B) \equiv G(1)(A^r - B^r) + G(0)(AB^r - BA^r)$$

$$G(1)(A-B) \equiv G(1)(A^{r+1} - B^{r+1}) + G(0)(AB^{r+1} - BA^{r+1})$$

$$\Rightarrow (A-B)(G(1) - AG(0)) \equiv G(1)(B^r A - B^{r+1})$$

$$\quad + G(0)(AB^{r+1} - B^r A^2)$$

$$\Rightarrow G(1)(A-B)(B^r - 1) + AG(0)(A-B)(1 - B^r) \equiv 0$$

$$\Rightarrow (G(1) - AG(0))(A-B)(B^r - 1) \equiv 0$$

Thus  $B^r \equiv 1$ , that is,  $\text{ord}_p(B) \mid r$ , or  $G(1) \equiv AG(0)$ . By the symmetry of the equations we also have:  $A^r \equiv 1$ , that is,  $\text{ord}_p(A) \mid r$ , or  $G(1) \equiv BG(0)$ . However, we can rule out these possibilities by insisting that our sequence is such that  $(G(1) - AG(0), p) = 1$  and similarly for the second condition. Level I primes that satisfy these conditions as well are known as *Level II primes wrt the sequence generated by  $a, b, G(0)$  and  $G(1)$* . We will abbreviate this in a way similar to that for LI primes: we say that  $p$  is LII wrt  $a, b, G(0)$  and  $G(1)$ . Under this new requirement, we can

also deduce easily that  $C(p) = [\text{ord}_p(A), \text{ord}_p(B)]$  where  $[x, y]$  denotes the lowest common multiple of  $x$  and  $y$ , giving us result (5):

(V) For  $p$ , LII wrt  $a, b, G(0)$  and  $G(1)$ , a cycle begins at  $r$  iff  $\text{ord}_p(A) \mid r$  and  $\text{ord}_p(B) \mid r$ . Furthermore,  $C(p) = [\text{ord}_p(A), \text{ord}_p(B)]$ .

This result reduces to the question of cycle lengths to another well-established one in number theory. As yet, there is no answer to the seemingly simple question of determining  $\text{ord}_p(n)$ , although we can answer the question of what the cycle length is in some cases, as we shall see in the last section. First, however, it is interesting to note that this result implies that the cycle length for these kinds of sequence is independent of the starting points  $G(0)$  and  $G(1)$  (as long as the conditions are met of course!) since it depends only on the orders of  $A$  and  $B$ .

**A strange connection with Fermat's Last Theorem?!** So far we have been unable to calculate the exact cycle length of a generalized Fibonacci sequence modulo any prime. However, for many values of  $A$  and  $B$  (and hence  $a$  and  $b$ ) it is possible to prove that the order of at least one of  $A$  and  $B$  will be even for any prime. Perhaps the most obvious example of this is when one of  $A$  or  $B$  is  $-1$ . It is interesting to see what the condition  $A = -1$  or  $B = -1$  really means for the kind of Fibonacci recurrence relation we are interested in. This is a simple matter as we may take (without loss of generality)  $B = -1$ . The numbers  $a$  and  $b$  are given in terms of  $A$  as follows:

$$-b = AB = -A \text{ and } a = A + B = A - 1 = b - 1,$$

so that all recurrence relations of the form

$$G(n) = aG(n-1) + (a+1)G(n-2) \tag{2}$$

have one of  $A$  or  $B = -1$ . By result (IV) in the last section, this in turn means that the cycle lengths for these types of sequence are always even (for any prime  $p$ ). This result, innocuous as it may seem, will now enable us to calculate the exact cycle length of this type of sequence for certain primes. This will require a new definition and will reveal a slightly surprising link with Fermat's Last Theorem!

**DEFINITION.** If  $p$ , a prime, is such that  $p = 2q + 1$  where  $q$  is also a prime, then  $q$  is a *Sophie Germain prime* of the first kind and  $p$  is a reverse Sophie Germain prime. Sophie Germain used her primes (see Wells [10] for a list) to prove a particular case of Fermat's Last Theorem, a strategy that was later developed by Lagrange to include more cases. Since Wiles' proof of this theorem, however, the study of these primes is now little more than a mathematical curiosity. However, it is the concept of reverse Sophie Germain primes that interests us here. If we are looking at a generalized Fibonacci sequence (of the type described above) modulo  $p$ , where  $p$  is a reverse Sophie Germain prime, then since  $C(p) \mid p - 1 (= 2q)$  and  $C(p)$  must be even, the only options for the cycle length are  $C(p) = 2, C(p) = p - 1$ . If we can eliminate the first of these possibilities then we will know the exact cycle length for a whole host of primes! The shortest way to do this is simply to state as a condition that  $C(p) \neq 2$ , although it is not too difficult (using Cramer's rule) to show that an equivalent set of conditions on  $a, b, G(0)$  and  $G(1)$  is

$$\begin{aligned} a + b &\not\equiv 1, \text{ if } G(0) \equiv G(1) \\ b - a &\not\equiv 1 \text{ if } G(0) \equiv -G(1) \\ \text{and } a &\not\equiv 0 \text{ or } b \not\equiv 1 \text{ if } G(0) \not\equiv \pm G(1). \end{aligned}$$

With this condition we have the surprising result:

**(VI)** If we have a generalized Fibonacci sequence given by (2), then for reverse Sophie Germain primes,  $C(p) = p - 1$ , subject to the condition that  $C(p) \neq 2$  and that  $p$  is also LII wrt  $a, b, G(0)$  and  $G(1)$ .

It is now clear that the particular sequence we looked at earlier (with  $a = 1, b = 2, G(0) = 0, G(1) = 1$  and  $p = 11$ ) is one of these sequences and so we could have predicted that  $C(11) = 10$  after only having checked that  $C(11) \neq 2$  (we could do this by calculating the third and fourth terms of the sequence).

In the interests of being able to apply this result to a whole host of primes for a particular sequence we have neglected the fact that we can also have, in exactly the same way:

**(VII)** If  $A \equiv -1 \pmod{p}$  or  $B \equiv -1 \pmod{p}$ , then  $C(p)$  is even. Further, if  $p$  is a reverse Sophie Germain prime then  $C(p) = p - 1$ , provided that  $C(p) \neq 2$  and that  $p$  is LII wrt  $a, b, G(0)$  and  $G(1)$ .

It is believed that there may be infinitely many Sophie Germain primes (and hence reverse Sophie Germain primes!). The question of whether this is true is related to the conjecture that there are infinitely many twin primes and, like it, does not yet have a solution. However, a great deal of work has been carried out on the calculation of large Sophie Germain primes [4]. Because of this a very large number of such primes are known and hence we can calculate the exact cycle length of a large number of primes for certain generalized Fibonacci sequences.

Although we have only been interested in the case where  $a^2 + 4b$  is a perfect square, it is possible to replace this by looking only at the prime residue systems in which  $a^2 + 4b$  is a quadratic residue. The results we have obtained all follow through in this case, it is just more complicated to state them and give their proofs although the keen reader will have little trouble in verifying this.

**Note** One interesting reference not referred to in the text is Neil Sloane's homepage (<http://www.research.att.com/~njas>) which has links to his encyclopedia of number sequences. Here there are many examples of Fibonacci (and Lucas) sequences as well as some examples of Sophie Germain primes and related sequences called Cunningham chains (the Cunningham chain with the smallest elements is  $2, 5 = 2 \times 2 + 1, 11 = 2 \times 5 + 1, 23 = 2 \times 11 + 1, 47 = 2 \times 23 + 1$ ).

**Acknowledgment.** We would like to thank the anonymous referees whose valuable suggestions have helped improve the clarity of this note.

## REFERENCES

1. J. Atkins and R. Geist, Fibonacci numbers and computer algorithms, *College Math. J.* **18** (1987), 328–337.
2. C. Cooper, Classroom capsules: Application of a generalized Fibonacci sequence, *College Math. J.* **15** (1984), 145–148.
3. W. Dotson, F. Norwood and C. Taylor, Fiber optics and Fibonacci, this MAGAZINE **66** (1993), 167–174.
4. H. Dubner, Large Sophie Germain primes, *Math. Comp.* **65**:213 (1996), 393–396.
5. R. J. Hendel, Approaches to the formula for the  $n$ th Fibonacci number, *College Math. J.* **25** (1994), 139–142.
6. Hua-Chieh Li, Complete and reduced residue systems of second-order recurrences modulo  $p$ , *Fibonacci Quart.* **38** (2000), 272–281.
7. I. Niven and H. S. Zuckerman, *An Introduction to the Theory of Numbers*, 2nd ed., Wiley, New York, 1966.
8. Zhi-Hong Sun and Zhi-Wei Sun, Fibonacci numbers and Fermat's last theorem, *Acta Arith.* **60** (1992), 371–388.
9. D. D. Wall, Fibonacci series modulo  $m$ , *Amer. Math. Monthly* **67** (1960), 525–532.
10. D. Wells, *The Penguin Dictionary of Curious and Interesting Numbers*, Revised Edition, Penguin Books, London, 1997.