CALCULATING EXACT CYCLE LENGTHS IN THE GENERALIZED FIBONACCI SEQUENCE MODULO p

DOMINIC VELLA AND ALFRED VELLA

1. Introduction

The cycles that occur in the Fibonacci sequence $\{F_n\}_{n=0}^{\infty}$ when it is reduced modulo a prime, p, have been extensively studied starting with the work of Wall [6]. In particular, it has been shown that the resulting sequence is periodic and thus forms a cycle with a well-defined cycle length, which we denote by $C(p)$. In this article, we shall extend some of these results to the cycles that occur in the generalized Fibonacci sequence $\{G_n\}_{n=0}^{\infty}$, which is defined by the second-order recurrence relation:

$$G_n = aG_{n-1} + bG_{n-2} \tag{1}$$

where a and b are non-zero integers. So that we get the conventional Fibonacci sequence $0, 1, 1, 2, ...$ with $a = 1$ and $b = 1$, we also take the starting values $G_0 = 0$, $G_1 = 1$. Since we shall be concerned with the generalized Fibonacci sequence once reduced modulo p, the condition that a and b be non-zero integers requires that $(a, p) = (b, p) = 1$. This in turn ensures that the sequences studied are actually second order sequences rather than first order sequences in disguise.

As we shall see, it is relatively easy to obtain upper bounds for $C(p)$ in general and in some special cases it is possible to calculate the value of $C(p)$ exactly. We will show how this can be achieved by extending some of the ideas that have previously been exploited in more specialised cases (see [4, 5]).

To appear in *The Mathematical Gazette*, March 2006.

2. Some Preliminary Results

Given a and b, the recurrence relation (1) can be solved by looking for solutions of the form $G_n = A\lambda^n$. The values of λ must be chosen to satisfy the auxiliary equation $\lambda^2 - a\lambda - b = 0$, which then, along with the initial conditions, gives the Binet formula:

$$G_n = \frac{1}{2^n \Delta^{1/2}} \left((a + \Delta^{1/2})^n - (a - \Delta^{1/2})^n \right) \tag{2}$$

where $\Delta = a^2 + 4b$ is the discriminant of the auxiliary equation. Throughout, we shall take p to be an odd prime and use $\equiv$ to denote congruence modulo p.

We now prove some results that we will use later on. The first of these is a simple Lemma, which is of such importance later that it is explicitly stated here.

Lemma 1. *If $G_n \equiv 0$, then $G_{n+k} \equiv bG_{n-1}G_k$ for $k \in \mathbb{N}$.*

Proof. Using a proof by induction (or, more elegantly, Fibonacci matrices [4]), it is easy to show that:

$$G_{n+k} = G_n G_{k+1} + bG_{n-1}G_k$$

Reducing this expression modulo p and using the fact that $G_n \equiv 0$, the result follows. □

Lemma 1 formalises the obvious idea that a reduced generalised Fibonacci sequence repeats in blocks, each of which is the previous block multiplied by bG_{n-1}. This result will be invaluable throughout but as a first application we have the following Theorem, which we have been unable to find in the literature:

Theorem 2. *If $G_n \equiv 0$, then $G_{n+1}^2 \equiv (-b)^n$. Further, if z is the smallest such $n \in \mathbb{N}$, then $C(p) = kz$ for k, the smallest positive solution of:*

$$G_{z+1}^k \equiv 1 \tag{3}$$

Proof. For the generalized Fibonacci sequence $\{G_m\}_{m=0}^{\infty}$, we have the modified Cassini relationship (see, for example, [4]):

$$G_{m+1}G_{m-1} - G_m^2 = -(-b)^{m-1} \tag{4}$$

With $m = n + 1$, this can be reduced modulo p to give:

$$G_{n+1}^2 \equiv (-b)^n \tag{5}$$

and so the first part of the Theorem follows. For the second part, Lemma 1 gives that:

$$G_{kz+1} \equiv G_{z+1}^k \tag{6}$$

Using Lemma 1 again, we must have $z|C(p)$ and thus $C(p) = kz$ for the least possible value of k. This value of k must be determined by the constraint that $G_{kz+1} = 1$, which leads immediately to the condition in (3) and the Theorem is proved. □

The following Corollary of Theorem 2 concerns the question of when $C(p)$ is even, and results in a condition on the order of $-b$ modulo p (denoted by $\mathrm{ord}_p(-b)$) which is the least $n \in \mathbb{N}$ such that $(-b)^n \equiv 1$.

Corollary 3. *$ord_p(-b)|C(p)$, the cycle length. In particular, $C(p)$ is even if $ord_p(-b)$ is even.*

Proof. We have from Theorem 2 that $G_{z+1}^2 \equiv b^z$ so that we have immediately $G_{z+1}^{2k} \equiv b^{zk}$ from which it follows that $\mathrm{ord}_p(-b)|zk = C(p)$. □

Corollary 3 can also be proved as a direct consequence of Theorem 3.6 of [1] or from first principles. The proof given above, however, gives a nice application of Theorem 2. We are now in a position to return to our main topic of interest: the value of $C(p)$.

3. Upper Bounds for the Cycle Length

Since each element of the generalized Fibonacci sequence is determined by the two preceeding elements, an application of the *pigeonhole principle* makes it clear that the sequence reduced modulo p must repeat after at most p^2 terms, so that $C(p) \leq p^2$. It is also easy to see that the sequence must return to the starting values $0, 1$ when it repeats. If, on the contrary, the cyclic behaviour started at the nth term then we could write:

$$G_{n+c} \equiv G_n, \qquad G_{n+c+1} \equiv G_{n+1}$$

(where $c = C(p)$) but with $G_{n-1+c} \not\equiv G_{n-1}$ since the cycle had to start at n. However, we may use the recurrence relation (1) to express G_{n+c-1} and G_{n-1} in terms of their successors which would then yield $bG_{n+c-1} \equiv bG_{n-1}$. Since $(b, p) = 1$ we see that we must have the cycle returning to the beginning and so $G_c \equiv 0$ and $G_{c+1} \equiv 1$.

It is also clear that finding an n such that $G_n \equiv 0$ and $G_{n+1} \equiv 1$ is enough to show that $C(p)|n$ using Lemma 1 and the above argument. Bearing this result in mind, we now proceed to obtain better upper bounds for the cycle length than the bound $C(p) \leq p^2$ obtained so far. The corresponding results are divided into two classes depending on whether Δ is, or is not, a quadratic residue modulo p (i.e. whether $\Delta \equiv x^2$ for some x, or not).

Many of the questions that we consider in this section were first considered by Wall [6] in the more familiar setting of the Fibonnaci sequence $\{F_n\}_{n=0}^{\infty}$ (so that $a = b = 1$ in our notation). Wherever possible, we simply translate the arguments given by Wall [6] into the generalized notation that interests us here. Adopting this strategy immediately yields:

Theorem 4. *If Δ is a quadratic non-residue modulo p, then $C(p)|(ord_p(-b)(p+1))$.*

Proof. By expanding the Binet formula (2) using the Binomial Theorem, we can write the general term of the generalized Fibonacci sequence as:

$$G_n = 2^{1-n}\left(\binom{n}{1}a^{n-1} + \binom{n}{3}\Delta a^{n-3} + \binom{n}{5}\Delta^2 a^{n-5} + ...\right) \tag{7}$$

We can then substitute the values $n = p$ and $n = p+1$ into (7) in turn and reduce modulo p, making extensive use of Fermat's Little Theorem (that $a^{p-1} \equiv 1$ if $(a, p) = 1$) and the fact that $\Delta^{\frac{p-1}{2}} \equiv -1$ (since Δ is a quadratic non-residue modulo p) to show that:

$$G_p \equiv 2^{1-p}\binom{p}{p}\Delta^{\frac{p-1}{2}} \equiv \Delta^{\frac{p-1}{2}} \equiv -1 \tag{8}$$

and also:

$$G_{p+1} \equiv 2^{-p}\left(\binom{p+1}{1}a^p + \binom{p+1}{p}a\Delta^{\frac{p-1}{2}}\right) \equiv 0 \tag{9}$$

From Lemma 1, we then have that the sequence will be repeated from here but is multiplied by $-b$ so that we must have a complete cycle after at most $\text{ord}_p(-b)$ blocks of $p+1$ elements. Using Lemma 1 again, the Theorem follows. □

Remark. From Fermat's Little Theorem, we know that $\text{ord}_p(-b)|p-1$ so that the longest possible cycle length is $(p-1)(p+1)$, which almost achieves the naive upper bound from earlier, namely $C(p) \leq p^2$. Of course, Theorem 4 is better than being just an upper bound since we know that $C(p)|p^2-1$ but taking $a=3$, $b=2$ and $p=7$ (so that $\text{ord}_p(-b)=6=p-1$ and $\Delta=17$ is a quadratic non-residue modulo p) it is easy to calculate the sequence and check that $C(p)=(p-1)(p+1)$ so that this upper bound can indeed be met.

The proof of Theorem 4 involved showing that $G_p \equiv -1$; a fact that can be utilized to show the following Corollary, whose importance shall become apparent later.

Corollary 5. *If $ord_p(-b)=2^k$, for some $k \in \mathbb{N}$, and Δ is a quadratic non-residue modulo p, then $4|C(p)$.*

Proof. From Theorem 4, we know that $C(p)|2^k(p+1)$ so that if the claim were not true we would have $C(p)|p+1$ and so $G_{p+2} \equiv 1$. However, from (8) we have that $G_p \equiv -1$ and so $G_{p+2} \equiv -b \not\equiv 1$ since, by the condition of the Corollary, $\text{ord}_p(-b) > 1$, which is a contradiction. □

In the case where Δ *is* a quadratic residue modulo p we can use some of the ideas developed in the proof of Theorem 4 to show:

Theorem 6. *If Δ is a quadratic residue modulo p then $C(p)|(p-1)$.*

Proof. Rather than using the approach adopted by Wall [6], we rewrite (8) and (9) but now with $\Delta^{\frac{p-1}{2}} \equiv 1$ (because Δ is now a quadratic residue modulo p) so that:

$$G_p \equiv 2^{1-p}\binom{p}{p}\Delta^{\frac{p-1}{2}} \equiv 1 \tag{10}$$

and:

$$G_{p+1} \equiv 2^{-p}\left(\binom{p+1}{1}a^p + \binom{p+1}{p}a\Delta^{\frac{p-1}{2}}\right) \equiv \frac{1}{2}(p+1)2a \equiv a \tag{11}$$

Since $(b, p) = 1$, (1) then implies that $G_{p-1} \equiv 0$ and so a cycle must have occured by $n = p - 1$ and the Theorem follows. □

Before going on to use Theorems 4 and 6 to calculate the exact cycle length for particular primes p, we first note another Corollary of these two Theorems due to Lucas [3].

Corollary 7. *Let z be the smallest $n \in \mathbb{N}$ such that $G_n \equiv 0$. Then:*

(i) $z|p+1$, if Δ is a quadratic non-residue modulo p

(ii) $z|p-1$, if Δ is a quadratic residue modulo p

(iii) $z = p$, if $p|\Delta$.

Proof. For (i) we note, from the Proof of Theorem 4 that $G_{p+1} \equiv 0$ in this situation, and similarly for (ii) we note that $G_{p-1} \equiv 0$ in this case. (iii) follows from (7) since we have in this case that $G_p \equiv 0$ and so $z|p$ (using Lemma 1) from which the result follows, since p is prime. □

4. Calculating the Exact Cycle Length

In this section, we shall show how it is possible to calculate the exact cycle length in certain situations. The first of these results is a simple consequence of Theorem 6:

Theorem 8. *If $\mathrm{ord}_p(-b) = p-1$ and Δ is a quadratic residue modulo p, then $C(p) = p-1$.*

Proof. From Corollary 3 we have that $p-1|C(p)$ but from Theorem 6 that $C(p)|p-1$ and so the result follows. □

Example 1. *Take $a = 1$, $b = 3$ so that $\Delta = 13$ and use the prime $p = 29$ as the base. Then a calculation shows that Δ is a quadratic residue modulo p and also that $ord_{29}(-b) = 28$ so that Theorem 8 gives $C(p) = p - 1 = 28$, as can easily be checked by computer.*

By making the following adaptation of the well-known (see for example [7]) notion of a Sophie Germain Prime, we can also prove a number of other results.

Definition. *A prime, p, is said to be a Reverse Positive (Negative) Sophie Germain Prime if $p = 2q + (-)1$ for some odd prime, q.*

With this definition, we are now in a position to prove two results that allow us to say when the upper bounds derived earlier are achieved.

Theorem 9. *If $b \equiv 1$ and Δ is a quadratic non-residue modulo a Reverse Negative Sophie Germain Prime p, then $C(p) = 2p + 2$.*

Proof. We have that $C(p)$ must be a multiple of 4 (by Corollary 5) and that $2p + 2 = 4q$ so that the only possible cycle lengths are (by Theorem 4 with $\mathrm{ord}_p(-b) = 2$) $C(p) = 4$ or $C(p) = 4q = 2p + 2$. The first of these possibilities can be ruled out by establishing the conditions under which $G_4 \not\equiv 0$ *or* $G_5 \not\equiv 1$. Using (7) we see that $G_4 = a^3 + 2ab \equiv a(a^2 + 2)$ and $G_5 = a^4 + 3a^2b + b^2 \equiv a^2(a^2 + 3) + 1$. Since $(a, p) = 1$, the condition that $C(p) \neq 4$ reduces to $a^2 \not\equiv -2$ or $a^2 \not\equiv -3$, at least one of which must *always* be true and so the Theorem follows. □

Remark. We cannot use the full power of Corollary 5 to prove an analogous result for cases other than $\mathrm{ord}_p(-b) = 2$ because it is not possible to have a prime q such that $4q = 2^k(p + 1)$ unless $k = 1$. Despite this, the Theorem is still of considerable use as is illustrated in the following example, which uses some of the authors' favourite numbers, although many other examples may easily be constructed.

Example 2. *Look at the generalized Fibonacci sequence generated by $a = 9$, $b = 14$ modulo $p = 13$. Now, 13 is a Reverse Negative Sophie Germain Prime since $13 = 2 \times 7 - 1$. Also, $\Delta = 9^2 + 4 \times 14 = 137 \equiv 7$ from which it is easy to show that Δ is a quadratic non-residue modulo p. Theorem 9 gives us immediately $C(13) = 28$. Using a computer, it is a simple matter to calculate the generalized Fibonacci sequence in this case reduced modulo 13:*

$$0, 1, 9, 4, 6, 6, 8, 0, 8, 7, 6, 9, 9, 12, 0, 12, 4, 9, 7, 7, 5, 0, 5, 6, 7, 4, 5, 1, 0, 1, 9, 4, ...$$

so that we do indeed have $C(13) = 2 \times 13 + 2 = 28$.

Using the same sort of ideas that gave us Theorem 9 we can also pin down the cycle length in the case where Δ is a quadratic residue modulo p to give:

Theorem 10. *If $b \equiv 1$ and Δ is a quadratic residue modulo a Reverse Positive Sophie Germain Prime p, then $C(p) = p - 1$.*

Proof. By Theorem 6 we have that $C(p)|p-1$ and also that $p - 1 = 2q$ for some prime q. But also, by Corollary 3, $2|C(p)$. Since $(a, p) = 1$, we cannot have $C(p) = 2$ so that the only possibility is $C(p) = p - 1$ as desired. □

Remark. The Proof of Theorem 10 requires only that $\mathrm{ord}_p(-b)$ be even. However, we have that $\mathrm{ord}_p(-b)|p-1 = 2q$ (in this case) and so the only possible even orders of $-b$ are 2 and $2q$. The latter of these possibilities is dealt with in more generality by Theorem 8 and so the only other case of interest is $\mathrm{ord}_p(-b) = 2$, i.e. $b \equiv 1$.

It is also easy to find examples in which Theorem 10 gives the value of $C(p)$ explicitly with very little calculation required.

Example 3. *Take $p = 47 = 2 \times 23 + 1$ with $b = 1$ and $a = 7$ so that $\Delta \equiv 6$ which is a quadratic residue modulo p. In this case we then see from Theorem 10 that $C(p) = 46$.*

Conclusions

Having seen the ease with which Theorems 9 and 10 allow us to calculate the exact cycle length in a couple of instances, it remains to understand how these results fit in with earlier work. To our knowledge, there have only been two earlier attempts to calculate the exact value of $C(p)$ (see [4, 5]). In [4] the value of Δ was restricted to a perfect square so that it was always a quadratic residue modulo p but the results obtained are very similar in spirit to Theorem 10. In the usual Fibonacci sequence, with $a = b = 1$, it is also reassuring to note that Theorems 9 and 10 specialise to the results given in [5].

The utilility of the results presented here depends primarily on how many reverse Sophie Germain primes there are. It is not yet known whether there are infinitely many Sophie Germain primes (and hence reverse Sophie Germain primes) but there is certainly a very large number of them, with ten appearing in the first one hundred natural numbers.

The main results considered in this article (Theorems 9 and 10) have allowed us to calculate the exact cycle lengths for these periodic sequences in particular cases and represent a generalisation of earlier results on this topic. These results could be used to strengthen existing results in other, related, Fibonacci topics. For example, the major results of Li [2] depend on the fact that $C(p) = p - 1$ for some primes p and generalized Fibonacci sequences $\{G_n\}_{n=0}^{\infty}$. Our work allows these results to be stated in terms of the defining parameters of the sequence a, b and p.

Acknowledgements. We thank Robin Grayson and Colin Roberts for suggesting cycles in reduced Fibonacci sequences as an interesting problem and we are grateful to the referee for helpful comments.

References

[1] H. -C. Li, "On Second-Order Linear Recurrence Sequences: Wall and Wyler Revisited." *The Fibonacci Quarterly* **37.4** (1999): 342-349.

[2] H. -C. Li, "Conditions for the Existence of Generalized Fibonacci Primitive Roots." *The Fibonacci Quarterly* **38.3** (2000): 244-249.

[3] E. Lucas, "Theorie des fonctions numeriques implement periodiques." *Amer. J. Math.* **1** (1878): 184–240, 289-321.

[4] D. Vella and A. Vella, "Cycles in the Generalized Fibonacci Sequence Modulo a Prime." *Math. Mag.* **75** (2002): 294-299.

[5] D. Vella and A. Vella, "Some Properties of Finite Fibonacci Sequences." To appear in *The Mathematical Gazette*, November 2004.

[6] D. D. Wall, "Fibonacci Series Modulo m." *Amer. Math. Monthly* **67** (1960): 525-532.

[7] D. Wells, "The Penguin Dictionary of Curious and Interesting Numbers." Revised Edition (1997), Penguin Books, London.

194 Buckingham Road, Bletchley, Milton Keynes, MK3 5JB

E-mail address: fibonacci@thevellas.com