Fibonacci periods and multiples

G. J. O. JAMESON

Introduction

The well-known Fibonacci numbers F_n are defined by the recurrence relation

$$F_n = F_{n-1} + F_{n-2}. \tag{1}$$

together with the starting values $F_0 = 0$, $F_1 = 1$, or equivalently $F_1 = F_2 = 1$. We record the first few:

n	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14
F_n	0	1	1	2	3	5	8	13	21	34	55	89	144	233	377

The recurrence relation can also be applied backwards in the form $F_n = F_{n+2} - F_{n+1}$ to define F_n for $n < 0$. An easy induction verifies that $F_{-n} = (-1)^{n-1} F_n$ for $n > 0$.

There is, of course, a massive literature about the Fibonacci numbers, including the books by Vajda [1] and Koshy [2], and chapters or sections in many other books, as well as a vast number of articles in journals.

Here we focus on the following property, which was already noted by E. Lucas [3] in 1878: *for each positive integer m, some F_n is a multiple of m.* The statement is actually obtained as a consequence of another one, the fact that (F_n) is periodic modulo m. Both statements are established by a neat application of the pigeon-hole principle, as follows.

Theorem 1: Given any positive integer m, there exists k such that $1 \leqslant k \leqslant m^2$ and:

(i) $F_{n+k} \equiv F_n \bmod m$ for all n,

(ii) F_k is a multiple of m.

Proof: Consider the pairs $(F_j, F_{j+1}) \bmod m$ for $0 \leqslant j \leqslant m^2$. There are $m^2 + 1$ such pairs, but only m^2 possible pairs of values mod m. By the pigeon-hole principle, two of the pairs considered must coincide, so there exist j in $[0, m^2]$ and k in $[1, m^2]$ such that $F_j \equiv F_{j+k}$ and $F_{j+1} \equiv F_{j+k+1} \bmod m$. Adding these two statements and applying (1), we see that $F_{j+2} \equiv F_{j+k+2} \bmod m$, and, repeating this, that $F_{n+k} \equiv F_n \bmod m$ for all $n \geqslant j$. Equally, by (1) and subtraction, we find that $F_{j-1} \equiv F_{j+k-1}$, and $F_{n+k} \equiv F_n \bmod m$ for all $n < j$ (including 0 and negative n). In particular, $F_k \equiv F_0 = 0 \bmod m$, so F_k is a multiple of m.

Let us distinguish the two properties of k seen in Theorem 1. Clearly, (i) says that (F_n) is periodic mod m: any k satisfying (i) will be called a *period* of (F_n) mod m. Clearly, any period satisfies (ii). More exactly, the relationship is as follows.

https://doi.org/10.1017/mag.2018.8 Published online by Cambridge University Press

Lemma 1: A positive integer k is a period for (F_n) mod m if, and only if, $F_k \equiv 0$ and $F_{k+1} \equiv 1 \bmod m$ (or equivalently $F_k \equiv 0$ and $F_{k-1} \equiv 1 \bmod m$).

Proof: If k is a period, then $F_k \equiv F_0 = 0$ and $F_{k+1} \equiv F_1 = 1 \bmod m$. Conversely, we saw in the proof of Theorem 1 that this pair of conditions implies that k is a period. Further, given that $F_k \equiv 0 \bmod m$, it follows from (1) that $F_{k+1} \equiv F_{k-1} \bmod m$.

We denote the *smallest* period mod m by $k(m)$. Some writers reserve the term 'period' for $k(m)$, but it will suit our purposes to use the word in the way we have described. Also, we denote the smallest positive k that satisfies (ii) by $r(m)$. Clearly $r(m) \leqslant k(m)$.

The pigeon-hole principle gives a neat proof of the existence of $k(m)$ and $r(m)$, but gives no further information about them. It is easy enough to find them for any given m (some examples follow shortly), but it is natural to ask whether there is an expression applying for general m. For *prime* m, there is indeed an explicit expression for a period (not necessarily the least period); it was already known to Lucas, and is reproduced in many books.

Other interesting results about these numbers, including a rather satisfactory description of how they relate to each other, have been given in a sucession of articles by various writers, including [4, 5, 6, 7, 8]. These results have not been accorded much coverage in subsequent books and surveys. Here we outline a selection of them, with some minor refinements. In a few cases, we offer a more elementary proof. Our exposition supplements the *Gazette* articles [9] and [10], with some overlap where desirable for continuity. Finally, we describe some applications of Lucas's theorem on explicit values. One consequence is that the bound $k(m) \leqslant m^2$ seen in Theorem 1 can be greatly improved.

Finding particular values

A trivial observation is: $r(F_n) = n$, since $F_j < F_n$ (so is not a multiple of F_n) for $j < n$. So, for example, $r(3) = 4$ and $r(13) = 7$. However, this only applies to the integers m that happen to be Fibonacci numbers, and doesn't reveal $k(m)$ even for these numbers. In general, the way to find $r(m)$ and $k(m)$ is to consider successive values of F_n mod m, using (1) to reduce mod m at each step: we do not need the actual values of F_n (which rapidly grow large). We use Lemma 1 to detect $k(m)$. Let us give some examples.

$m = 2$: Since $F_1 = F_2 = 1$ and $F_3 = 2 \equiv 0 \bmod 2$, we have $r(2) = k(2) = 3$. Note that it follows that F_n is even exactly when n is a multiple of 3.

https://doi.org/10.1017/mag.2018.8 Published online by Cambridge University Press

$m = 4$: (For further examples, we tabulate the values of $F_n \bmod m$.)

n	1	2	3	4	5	6
$F_n \bmod 4$	1	1	2	3	1	0

This shows that $r(4) = k(4) = 6$.

$m = 11$:

n	1	2	3	4	5	6	7	8	9	10
$F_n \bmod 11$	1	1	2	3	5	8	2	10	1	0

Hence $r(11) = k(11) = 10$.

In all these examples, $k(m) = r(m)$. Another lemma identifies a wide class of cases where $k(m) = 2r(m)$, and enables us to recognise them as soon as we have found $r(m)$.

Lemma 2: Let $r(m) = r$. If $F_{r-1} \equiv -1 \bmod m$, then $k(m) = 2r$.

Proof: Then $F_{r+1} \equiv -1 \bmod m$. By (1) and an easy induction, as before, it follows that $F_{r+j} \equiv -F_j \bmod m$ for all $j > 0$. In particular, $F_{2r} \equiv -F_r \equiv 0$ and $F_{2r+1} \equiv -F_{r+1} \equiv 1 \bmod m$, so $2r$ is a period, by Lemma 1. Also, F_{r+j} is not a multiple of m for $1 \leqslant j < r$, so $2r$ is the smallest period.

We give a few examples of this type.

$m = 3$: Since $F_4 = 3$ and $F_3 = 2 \equiv -1 \bmod 3$, we have $r(3) = 4$ and $k(3) = 8$.

$m = 7$:

n	1	2	3	4	5	6	7	8
$F_n \bmod 7$	1	1	2	3	5	1	6	0

Since $6 \equiv -1 \bmod 7$, this shows that $r(7) = 8$ and $k(7) = 16$.

$m = 9$:

n	1	2	3	4	5	6	7	8	9	10	11	12
$F_n \bmod 9$	1	1	2	3	5	8	4	3	7	1	8	0

Hence $r(9) = 12$ and $k(9) = 24$.

$m = 5$:

n	1	2	3	4	5	6	7	8	9	10
$F_n \bmod 5$	1	1	2	3	0	3	3	1	4	0

So $r(5) = 5$ and by an obvious slight variant of Lemma 2, $k(5) = 20$. We shall see later that this case has a rather special status.

https://doi.org/10.1017/mag.2018.8 Published online by Cambridge University Press

We include two rather more adventurous examples illustrating the fact that $k(m)$ can be considerably smaller than m. Taking advantage of the original table of values, we shorten the tabulation by starting with the last two values of F_n that are smaller than m.

$m = 47$:

n	8	9	10	11	12	13	14	15	16
$F_n \bmod 47$	21	34	8	42	3	45	1	46	0

so $r(47) = 16$ and $k(47) = 32$.

$m = 199$:

n	11	12	13	14	15	16	17	18	19	20	21	22
$F_n \bmod 199$	89	144	34	178	13	191	5	196	2	198	1	0

so $r(199) = k(199) = 22$.

Note: For $k = k(m)$, we have $F_{k-n} \equiv F_{-n} = (-1)^{n-1}F_n \bmod m$. This shows up clearly in the tabulation for 199, read backwards.

Some facts about the Fibonacci numbers

We shall make repeated use of some well-known results about the Fibonacci numbers. The proofs are short, so we include them for completeness.

Theorem 2 (the addition formula): For all integers m, n,

$$F_{m+n} = F_{m-1}F_n + F_mF_{n+1}. \tag{2}$$

Proof: This is proved by induction on n (in both directions) for fixed m. For $n = 0$, the right-hand side is $F_mF_1 = F_m$, so (2) holds. For $n = 1$, it equates to (1). Now suppose that (2) holds for $n = k - 1$ and $n = k$, so that

$$F_{m+k-1} = F_{m-1}F_{k-1} + F_mF_k,$$

$$F_{m+k} = F_{m-1}F_k + F_mF_{k+1}.$$

Addition gives (2) for $n = k + 1$, and subtraction gives (2) for $n = k - 2$. So easy induction, both forwards and backwards, gives (2) for all n.

Corollary 2.1: For all integers m, n,

$$(-1)^{n-1}F_{m-n} = F_{m-1}F_n - F_mF_{n-1}. \tag{3}$$

Proof: Replace n by $-n$ in (2), recalling that $F_n = (-1)^{n-1}F_n$. We obtain

$$F_{m-n} = (-1)^{n-1}F_{m-1}F_n + (-1)^nF_mF_{n-1},$$

which is equivalent to (3).

https://doi.org/10.1017/mag.2018.8 Published online by Cambridge University Press

Taking $m = n + 1$, we find:

Corollary 2.2: For all n,

$$F_{n+1}F_{n-1} - F_n^2 = (-1)^n. \tag{4}$$

Theorem 3: For positive integers k and n, F_{kn} is a multiple of F_n.

Proof: Induction on k (this time, forwards only) for fixed n. Assume the statement for a certain k. Then by (2),

$$F_{(k+1)n} = F_{kn+n} = F_{kn-1}F_n + F_{kn}F_{n+1},$$

so is also a multiple of F_n.

Of course, it follows that for all composite n except 4, F_n is composite. In other words, for $n > 4$, F_n can only be prime when n is prime (rather like the Mersenne numbers $2^n - 1$). In fact, F_p is prime for all primes p from 3 to 17, but $F_{19} = 4181 = 37 \times 113$.

First results for $k(m)$ and $r(m)$

Obviously, any multiple of $k(m)$ is a period mod m. The converse is true as well:

Theorem 4: Every period for (F_n) mod m is a multiple of $k(m)$.

Proof: Write $k(m) = k_0$, and let k be another period. Let $k = qk_0 + s$, where $0 \leqslant s < k_0$. Then, for all n,

$$F_n \equiv F_{n+k} = F_{n+s+qk_0} \equiv F_{n+s} \bmod m,$$

so if $s > 0$, then s is a period. By the definition of k_0, it follows that $s = 0$, so $k = qk_0$.

We write $[m, n]$ for the least common multiple of m and n.

Corollary 4.1: Let $\gcd(m, n) = 1$. Then $k(mn) = [k(m), k(n)]$.

Proof: Any period mod mn is obviously a period mod m and mod n. Conversely, let k be a period mod m and mod n. Since $[m, n] = mn$, we then have $F_{N+k} \equiv F_N \bmod mn$ for all N, so k is a period mod mn. Hence the periods mod mn are the integers k that are multiples of both $k(m)$ and $k(n)$: the least one is $[k(m), k(n)]$.

Analogous statements apply to $r(m)$, though for different reasons. We will use the notation $R(m)$ for the set of all integers n such that F_n is a multiple of m.

https://doi.org/10.1017/mag.2018.8 Published online by Cambridge University Press

Theorem 5: $R(m)$ consists of exactly the multiples of $r(m)$.

Proof: Write $r(m) = r_0$. By Theorem 3, if n is a multiple of r_0, then F_n is a multiple of m, so $n \in R(m)$. Conversely, suppose that $n \in R(m)$. Let $n = qr_0 + s$, where $0 \leqslant s < r_0$. By (3),

$$F_s = F_{n-qr_0} = (-1)^{qr_0-1}\left(F_{n-1}F_{qr_0} - F_nF_{qr_0-1}\right),$$

so F_s is a multiple of m. By the definition of r_0, it follows that $s = 0$, so $n = qr_0$.

In particular, $k(m)$ is a multiple of $r(m)$.

Corollary 5.1: Let $\gcd(m, n) = 1$. Then $r(mn) = [r(m), r(n)]$.

Proof: F_r is a multiple of mn if, and only if, it is a multiple of both m and n. This occurs exactly when r is a multiple of both $r(m)$ and $r(n)$.

Using our earlier examples (which were all for primes or powers of primes), we can now read off the values of $r(m)$ and $k(m)$ for various composite m. For example:

m	factors	$r(m)$	$k(m)$
6	2×3	$[3, 4] = 12$	$[3, 8] = 24$
10	2×5	$[3, 5] = 15$	$[3, 20] = 60$
22	2×11	$[3, 10] = 30$	$[3, 10] = 30$
36	4×9	$[6, 12] = 12$	$[6, 24] = 24$

Recall from (4) that $F_{r+1}F_{r-1} - F_r^2 = (-1)^r$. We record an immediate consequence.

Theorem 6: If $F_r \equiv 0$ and $F_{r+1} \equiv c \bmod m$, then $c^2 \equiv (-1)^r \bmod m$.

Proof: Then also $F_{r-1} \equiv c \bmod m$, so the statement follows at once from (4).

Two further conclusions follow easily.

Corollary 6.1: For all $m > 2$, $k(m)$ is even.

Proof: (Longer proofs can be seen in some books!) Apply Theorem 6 with $r = k(m)$. Then $c = 1$, so $(-1)^r \equiv 1 \bmod m$. If r is odd, this says $1 \equiv -1 \bmod m$, so m is 1 or 2.

Corollary 6.2: Suppose that m has a prime factor q congruent to $-1 \bmod 4$. Then $r(m)$ is even.

Proof: If $r = r(m)$ is odd, then $c^2 = -1 \bmod m$, hence also mod q. But by a well-known result of number theory, no such c exists when $q \equiv -1 \bmod 4$.

https://doi.org/10.1017/mag.2018.8 Published online by Cambridge University Press

We now turn to our main objective, which is to express $k(m)$ in terms of $r(m)$. In all the examples we have seen, $k(m)$ is either $r(m)$, $2r(m)$ or $4r(m)$. This is indeed always the case. It was stated in simultaneous articles by Vinson [5] and Robinson [6], but may have been known for longer. The key step is the next result, which extends Lemma 2 and shows how we can always determine $k(m)$ once we know $r(m)$.

Theorem 7: Suppose that $F_r \equiv 0$ and $F_{r+1} \equiv c \bmod m$. Then

$$F_{nr+1} \equiv c^n \bmod m$$

for all $n \geqslant 1$. So nr is a period mod m if, and only if, $c^n \equiv 1 \bmod m$, and if $r = r(m)$, then $k(m) = nr(m)$ for the smallest such n.

Proof: Induction on n. The case $n = 1$ is the hypothesis. Assume the statement for n. Then by (2),

$$F_{(n+1)r+1} = F_{nr+(r+1)} = F_{nr}F_r + F_{nr+1}F_{r+1} \equiv 0 + c^{n+1} \mod m.$$

This proof differs from both [6], which uses a matrix method, and [5], where the result is derived from the rather ponderous identity

$$F_{nr+s} = \sum_{j=0}^{n} \binom{n}{j} F_r^j F_{r-1}^{n-j} F_{j+s}. \tag{5}$$

Example: As an immediate application of Theorem 7, take $m = 8$. Since $8 = F_6$, we have $r(8) = 6$. Also, $F_5 = 5$ and $5^2 = 25 \equiv 1 \bmod 8$, hence $k(8) = 2 \times 6 = 12$.

By Theorem 6, in all cases, we have $c^4 \equiv 1 \bmod m$, so $k(m)$ divides $4r(m)$, hence is $jr(m)$, where $j = 1$, 2 or 4. Further, if $r(m)$ is even, then $c^2 = 1$, so j is 1 or 2. However, before we state this as a theorem, we will refine it with the help of another result, which generalises the fact, noted earlier, that $F_{k-s} \equiv (-1)^{s-1}F_s \bmod m$. Here we diverge again from [5] and [6].

Theorem 8: Suppose that $F_r \equiv 0$ and $F_{r+1} \equiv c \bmod m$. Then for all $s \geqslant 1$,

$$F_{r-s} \equiv (-1)^{s-1} cF_s \bmod m. \tag{6}$$

Proof: Then $F_{r-1} \equiv c \bmod m$, so by (3),

$$F_{r-s} = (-1)^{s-1}\left(F_{r-1}F_s - F_rF_{s-1}\right) \equiv (-1)^{s-1} cF_s \bmod m.$$

The next Corollary looks rather special, but it is just what we will need, several times.

https://doi.org/10.1017/mag.2018.8 Published online by Cambridge University Press

Corollary 8.1: Suppose that $r = 2t$ and that $F_r \equiv 0$ and $F_{r+1} \equiv (-1)^t \bmod m$. Then $F_t \equiv 0 \bmod m$.

Proof: By (6),

$$F_{t-1} = F_{r-(t+1)} \equiv (-1)^t (-1)^t F_{t+1} = F_{t+1} \bmod m,$$

so $F_t = F_{t+1} - F_{t-1} \equiv 0 \bmod m$.

We are now ready to present the basic theorem relating $k(m)$ and $r(m)$.

Theorem 9:

(i) if $r(m)$ is a multiple of 4, then $k(m) = 2r(m)$;

(ii) if $r(m) \equiv 2 \bmod 4$, then $k(m)$ is either $r(m)$ or $2r(m)$;

(iii) if $m > 2$ and $r(m)$ is odd, then $k(m) = 4r(m)$.

Proof: In the following, all congruences are mod m. Write $r(m) = r$, and let $F_{r+1} \equiv c$.

If r is even, then, by Theorem 6, $c^2 \equiv 1$, so by Theorem 7, $k(m)$ divides $2r$, so is either r or $2r$. Suppose now that $r = 4s$. If $k(m) = r$, then $c = 1$, so by Corollary 8.1 (with $t = 2s$), $F_{2s} \equiv 0$, contradicting $r(m) = 4s$. This proves (i) and (ii).

If r is odd, then $c^2 \equiv -1$ and $c^4 \equiv 1$. So $k(m) = jr(m)$, where $j = 1$, 2 or 4. For $m > 2$, c^2 (hence also c) is not congruent to 1. Hence $k(m) = 4r$.

Clearly, cases (i) and (iii) give the value of $k(m)$ instantly once we know $r(m)$. For example, it is clear from the original table that $r(17) = 9$, so $k(17) = 36$. A pleasant application is the precise evaluation of $k(F_n)$ for all n:

Corollary 9.1: Let $n \geqslant 4$. Then $k(F_n)$ equals $2n$ for even n and $4n$ for odd n.

Proof: Since $r(F_n) = n$, the statement follows at once when n is odd or a multiple of 4. Now let $n = 2s$, where s is odd. By case (ii), $k(F_n)$ is either $2s$ or $4s$. But $k(F_s) = 4s$, and $k(F_n)$ is a multiple of $k(F_s)$, since F_n is a multiple of F_s. So $k(F_n) = 4s$.

We can resolve case (ii) fully for *prime* moduli:

Theorem 10: If p is prime and $r(p) \equiv 2 \bmod 4$, then $k(p) = r(p)$.

Proof: Congruences are mod p. Let $r = 4s + 2$ and $F_{r+1} \equiv c$. By Theorem 6, $c^2 \equiv 1$. Since p is prime, it follows that $c \equiv \pm 1$. If $c \equiv -1$, then Corollary 8.1 applies, with $t = 2s + 1$, to give $F_{2s+1} \equiv 0$, contradicting $r(p) = 4s + 2$. Hence $c \equiv 1$, so $k(p) = r$.

https://doi.org/10.1017/mag.2018.8 Published online by Cambridge University Press

For composite m, both possibilities can occur in case (ii). For example, as seen above, $r(22) = k(22) = 30$, while $r(8) = 6$ and $k(8) = 12$. At the cost of more work, the cases where $k(m) = r(m)$ are identified in [5] in terms of the prime factorisation.

The modulus m^j

We now establish a result on periods and multiples for m^j, by a rather more elementary method than [4]. We start with a Lemma extending Theorem 6 to the modulus m^2:

Lemma 3: Suppose that $F_r = am$ and $F_{r+1} = bm + c$, where $1 \leqslant c < m$. Then

$$F_{nr} \equiv nac^{n-1}m \mod m^2, \tag{7}$$

$$F_{nr+1} \equiv nbc^{n-1}m + c^n \mod m^2. \tag{8}$$

Proof: Assume (7) and (8) for a certain value of n. Note that $F_{r-1} = (b - a)m + c$. By (2),

$$\begin{aligned} F_{(n+1)r} = F_{nr+r} &= F_{nr}F_{r-1} + F_{nr+1}F_r \\ &\equiv nac^{n-1}m\big((b-a)m + c\big) + \big(nbc^{n-1}m + c^n\big)am \\ &\equiv (n+1)ac^n m \mod m^2 \end{aligned}$$

and

$$\begin{aligned} F_{(n+1)r+1} = F_{nr+(r+1)} &= F_{nr}F_r + F_{nr+1}F_{r+1} \\ &\equiv \big(nac^{n-1}m\big)am + \big(nbc^{n-1}m + c^m\big)(bm + c) \\ &\equiv (n+1)bc^n m + c^{n+1} \mod m^2, \end{aligned}$$

so (7) and (8) hold for $n + 1$.

Theorem 11: For any $m \geqslant 2$ and $j \geqslant 1$,

(i) $m^{j-1}r(m)$ is in $R(m^j)$;

(ii) $m^{j-1}k(m)$ is a period for $(F_n) \mod m^j$.

Proof:

(i) This will follow if we can show that if $r \in R(m^j)$, then $mr \in R(m^{j+1})$. Take $r \in R(m^j)$. By (7), with m replaced by m^j, we have $F_{nr} \equiv nac^{n-1}m^j \mod m^{2j}$. Hence $F_{mr} \equiv 0 \mod m^{j+1}$, so $mr \in R(m^{j+1})$. (Note that the value of c doesn't matter.)

(ii) Similarly, we show that if r is a period mod m^j, then mr is a period mod m^{j+1}. By (8) applied to m^j, with $c = 1$, we have $F_{nr+1} \equiv nbm^j + 1 \mod m^{2j}$, hence $F_{mr+1} \equiv 1 \mod m^{j+1}$, as required.

https://doi.org/10.1017/mag.2018.8 Published online by Cambridge University Press

Theorem 11 does not assert that the stated values are minimal, equating to $r(m^j)$ and $k(m^j)$ respectively. This would say, for example, that $r(m^2) = mr(m)$. For composite m, this is a non-starter: we have seen that $r(36) = r(6) = 12$. However, for *prime* p, the question becomes more interesting. Write $r(p^j) = r^j$. Then r_{j+1} is either r_j or pr_j, since it is a multiple of r_j and (as shown in the proof) a divisor of pr_j. It remains a famously unsolved problem whether there are *any* primes p such that $r_2 = r_1$. The alternative is $r_2 = pr_1$, and for $p > 2$ one can show that in this case $r_j = p^{j-1}r_1$ for all j, either by revisiting the proof above or by formulae like (5) (for two versions, see [4, 5]).

The case $p = 2$ is special: indeed, $r(8) = r(4) = 6$. However, one can show that $r(2^j) = 3{\cdot}2^{j-2}$ for all $j \geqslant 3$.

Similar remarks apply to $k(p^j)$, but $k(8) = 12$ and, by Theorem 9 and the values just given for $r(2^j)$, we have $k(2^j) = 3{\cdot}2^{j-1}$ for all $j \geqslant 2$.

Explicit values for prime moduli

We now state the theorem for prime moduli which, in its essentials, was already known to Lucas. It identifies both a period (though not necessarily the least period) and a member of $R(p)$ explicitly. It is rather intriguing that different answers apply for different values of p mod 5.

Theorem 12: Let $p \neq 5$ be prime. If $p \equiv \pm 1 \bmod 5$, then $F_p \equiv 1$ and $F_{p-1} \equiv 0 \bmod p$, hence $p - 1$ is a period for $(F_n) \bmod p$.

If $p \equiv \pm 2 \bmod 5$, then $F_p \equiv -1$ and $F_{p+1} \equiv 0 \bmod p$, hence $p + 1$ is in $R(p)$ and $2p + 2$ is a period for $(F_n) \bmod p$.

The proof can be seen in numerous books and articles, e.g. [11, p. 150], [1, pp. 78-79] and [9], so we will not repeat it here. We just mention that it uses Binet's formula

$$F_n = \frac{1}{\sqrt{5}}\left(\phi^n - \psi^n\right),$$

where $\phi = \frac{1}{2}(1 + \sqrt{5})$ and $\psi = \frac{1}{2}(1 - \sqrt{5})$, and some non-trivial results from number theory.

Note that for primes $p \neq 2$, the condition $p \equiv \pm 1 \bmod 5$ is equivalent to $p \equiv 1$ or $9 \bmod 10$, and $p \equiv \pm 2 \bmod 5$ is equivalent to $p \equiv 3$ or $7 \bmod 10$.

Of course, this theorem leaves out $p = 5$. We dealt with this case above: $r(5) = 5$ and $k(5) = 20$. Clearly, this is the only case where $r(p)$ is a multiple of p.

We mentioned earlier that $r(p^2)$ is either $r(p)$ or $pr(p)$, and that it is not known whether there are any primes for which $r(p^2) = r(p)$. By Theorem 12, $r(p)$ divides $p + \varepsilon$, where ε is either 1 or -1. Now $pr(p)$ does not divide $p + \varepsilon$, so the statement $r(p^2) = r(p)$ is equivalent to $F_{p+\varepsilon}$ being a multiple of p^2. The problem is often stated in this form.

https://doi.org/10.1017/mag.2018.8 Published online by Cambridge University Press

We now describe some developments and applications of Theorem 12. First, using Theorem 8 and Corollary 8.1, we refine the result by showing that $\frac{1}{2}(p+\varepsilon) \in R(p)$ in the cases where $p \equiv 1 \bmod 4$; this seems to be less well known. The possible values of p mod 4 and mod 5 give us four classes mod 20, and we can determine the value of $r(p)$ mod 4, and hence also of $k(p)/r(p)$, in three of the cases. These values were derived by rather different methods in [5, Theorem 4].

Theorem 13:

(i) If $p \equiv 1$ or 9 mod 20, then $\frac{1}{2}(p-1) \in R(p)$.

(ii) If $p \equiv 13$ or 17 mod 20, then $\frac{1}{2}(p+1) \in R(p)$, $r(p)$ is odd and $k(p) = 4r(p)$.

(iii) If $p \equiv 11$ or 19 mod 20, then $\frac{1}{2}(p-1) \notin R(p)$, $r(p) \equiv 2 \bmod 4$ and $k(p) = r(p)$.

(iv) If $p \equiv 3$ or 7 mod 20, then $\frac{1}{2}(p+1) \notin R(p)$, $r(p)$ is a multiple of 4 and $k(p) = 2r(p)$.

Proof: All congruences are mod p. In cases (i) and (ii), p is of the form $4s+1$. In case (i), by Theorem 12, $F_{p-1} \equiv 0$ and $F_p \equiv 1$. By Corollary 8.1, with $r = p-1 = 4s$, we have $F_{2s} \equiv 0$, so $2s = \frac{1}{2}(p-1) \in R(p)$.

In case (ii), Theorem 12 says that $F_{p+1} \equiv 0$ and $F_{p+2} \equiv -1$. Corollary 8.1, with $r = p+1 = 4s+2$, now applies to give $F_{2s+1} \equiv 0$. So $r(p)$ divides $2s+1$, hence is odd, and $k(p) = 4p(r)$, by Theorem 9.

In cases (iii) and (iv), p is of the form $4s-1$. In case (iii), we know from Corollary 6.2 that $r(p)$ is even, while $\frac{1}{2}(p-1)$ is odd. Also, $r(p)$ divides $p-1$, which is not a multiple of 4. So $r(p) \equiv 2 \bmod 4$, and $k(p) = r(p)$, by Theorem 10.

In case (iv), $F_{p+1} \equiv 0$ and $F_{p+2} \equiv -1$. By Theorem 8, with $r = p+1 = 4s$, we have $F_{2s+1} = F_{r-(2s-1)} \equiv -F_{2s-1} \equiv a$ (say). Then $F_{2s} \equiv 2a$. If $2a \equiv 0$, then $a \equiv 0$ (since p is odd), so $F_{2s} \equiv F_{2s+1} \equiv 0$. But this is not true, since it implies that $F_n \equiv 0$, so is a multiple of p, for all n! Hence $2s \notin R(p)$. So $r(p)$ divides $4s$ but not $2s$, so is a multiple of 4. By Theorem 9, $k(p) = 2r(p)$.

We now give examples of all four types showing that $r(p)$ (and the implied value of $k(p)$) can be either equal to the value indicated by Theorems 12 and 13, or smaller. Most of the examples have already been mentioned above; the reader may care to verify the others.

Type (i):	$r(29) = 14$,	$r(41) = 20$,	$r(89) = 11$.
Type (ii):	$r(13) = 7$,	$r(233) = 13$.	
Type (iii):	$r(11) = 10$,	$r(199) = 22$.	
Type (iv):	$r(3) = 4$,	$r(47) = 16$.	

This also shows that type (i) allows all possibilities for $r(p)$ mod 4.

https://doi.org/10.1017/mag.2018.8 Published online by Cambridge University Press

Of course, in case (ii), if $\frac{1}{2}(p+1)$ happens to be prime, then $r(p)$ has this value. So, for example, $r(37) = 19$ and $r(73) = 37$.

Wall [4] lists 99 primes $p < 2000$ for which $k(p)$ is less than the value stated in Theorem 16 (leaving 202 others for which it is the same).

Another result, which we will not prove here, is Carmichael's theorem: *For every n except* 1, 2, 6, 12, *there is a prime p such that* $r(p) = n$. In other words, F_n has a prime factor that is not a factor of any earlier F_k. A proof can be seen in [7].

Upper bounds for $k(m)$ *and* $r(m)$

The prime factorisation of a general integer m expresses it in the form $q_1q_2\ldots q_j$, where the q_j are powers of distinct primes (so mutually coprime). By Theorems 11 and 12, we have an expression for a period mod q_j and a member of $R(q_j)$. Common multiples of these expressions give, respectively, a period mod m and a member of $R(m)$. The expressions are too unpleasant to write out explicitly in the form of a general formula, but they are used implicitly in the result that follows.

Theorem 14: For all positive integers m, we have $k(m) \leqslant 6m$ and $r(m) \leqslant 2m$.

Proof: Write the prime factorisation of m as

$$m = 2^a 5^b Q_1 Q_2,$$

where $Q_1 = q_1q_2\ldots q_s$, $Q_2 = q_{s+1}\ldots q_t$, in which $q_j = p_j^{a_j}$ for each j and $p_j \equiv \pm 1 \bmod 5$ for $1 \leqslant j \leqslant s$ and $p_j \equiv \pm 2 \bmod 5$ for $s+1 \leqslant j \leqslant t$. (If there are no factors of the type listed, then Q_1 or Q_2 is 1.) We know that periods for these components are as follows:

$$k^*(2^a) = 3\cdot 2^{a-1},$$

$$k^*(5^b) = 4\cdot 5^b,$$

$$k^*(q_j) = (p_j - 1)p_j^{a_j-1}, \text{ for } 1 \leqslant j \leqslant s,$$

$$k^*(q_j) = 2(p_j + 1)p_j^{a_j-1}, \text{ for } s+1 \leqslant j \leqslant t.$$

(We use the notation k^* because these are not necessarily the least periods.) Let $k^*(Q_1) = \prod_{j=1}^{s} k^*(q_j)$. For $1 \leqslant j \leqslant s$, we have $k^*(q_j) < q_j$, so $k^*(Q_1) < Q_1$. For $s+1 \leqslant j \leqslant t$, write $p_j + 1 = 2u_j$. Then $u_j \leqslant p_j$ and $k^*(q_j) = 4u_jp_j^{a_j-1}$. So a common multiple of $k^*(5^b)$ and these numbers $k^*(q_j)$ is

$$4\cdot 5^b \prod_{j=s+1}^{t} u_j p_j^{a_j-1} \leqslant 4\cdot 5^b \prod_{j=s+1}^{t} p_j^{a_j} = 4\cdot 5^b Q_2.$$

https://doi.org/10.1017/mag.2018.8 Published online by Cambridge University Press

Hence a common multiple of all the elements of the type $k^*(q)$, in other words a period for m, is not greater than

$$3 \cdot 2^{a-1} \cdot 4 \cdot 5^b Q_1 Q_2 = 6m.$$

For $r(m)$, we replace $k^*(5^b)$ by $r^*(5^b)$ and $k^*(q_j)$ for $s+1 \leqslant j \leqslant t$ by $r^*(q_j) = (p_j+1)p_j^{a_j-1} = 2u_j p_j^{a_j-1}$. A common multiple of these numbers $r^*(q_j)$ is $2\prod_{j=s+1}^{t} u_j p_j^{a_j-1}$: denote this by R_2. Then

$$\frac{R_2}{Q_2} = 2\prod_{j=s+1}^{t} \frac{u_j}{p_j}.$$

Now $\dfrac{u_j}{p_j} = \dfrac{2}{3}$, attained when $p_j = 3$, so $R_2 \leqslant \frac{4}{3}Q_2$ (if $Q_2 = 1$, then $R_2 = 1$). So

$$r(m) \leqslant 3 \cdot 2^{a-1} \cdot 5^b Q_1 \left(\tfrac{4}{3}Q_2\right) = 2m.$$

Since $k(10) = 60$ and $r(6) = 12$, the factors 6 and 2 are optimal.

A rather more sophisticated proof of the statement for $k(m)$ is given in [8]. I do not know an explicit reference for the result on $r(m)$.

Generalised Fibonacci sequences; Lucas numbers

Any sequence (G_n) satisfying the recurrence relation $G_n = G_{n-1} + G_{n-2}$ is called a 'generalised Fibonacci sequence'. Clearly (G_n) is fully determined once the values $G_0 = a$ and $G_1 = b$ are specified: in fact,

$$G_n = aF_{n-1} + bF_n, \tag{9}$$

since the right-hand side has the required values a and b at 0 and 1.

A case of particular interest is the sequence (L_n) of *Lucas numbers* defined by $L_0 = 2, L_1 = 1$, so that

$$L_n = 2F_{n-1} + F_n = F_{n+1} + F_{n-1}.$$

The first few are:

n	0	1	2	3	4	5	6	7	8	9	10
L_n	2	1	3	4	7	11	18	29	47	76	123

Numerous identities link the Lucas and Fibonacci numbers, for example $L_{n+1} + L_{n-1} = 5F_n$ and $F_{2n} = L_n F_n$. Also, $L_n = \phi^n + \psi^n$.

We conclude with some very brief remarks about periods and multiples for such sequences (a thorough study can be seen in [4]). If (G_n) is any generalised Fibonacci sequence, then (9) shows that any period for (F_n) mod m is a period for (G_n). However, (G_n) may have a smaller period. Either way, Theorem 4 still applies. It follows from Theorem 12 (or can be proved in a similar way) that for all primes p, $L_p \equiv 1 \bmod p$. Meanwhile, if a and b

https://doi.org/10.1017/mag.2018.8 Published online by Cambridge University Press

are not zero, there is no guarantee that any G_n is a multiple of m, so the results on $r(m)$ have no counterpart.

These observations are illustrated by the Lucas numbers, with $m = 5$. Since $L_4 \equiv 2$ and $L_5 \equiv 1 \bmod 5$ (replicating L_0 and L_1), (L_n) has period 4 mod 5, while (F_n) has period 20. Further, since L_0, L_1, L_2 and L_3 are not multiples of 5, no L_n is a multiple of 5.

References

1. Steven Vajda, *Fibonacci and Lucas numbers and the Golden Section*, Dover (1989).
2. Thomas Koshy, *Fibonacci and Lucas numbers with Applications*, Wiley Interscience, New York (2001).
3. E. Lucas, Théorie des fonctions numériques simplement périodiques, *American J. Math.* **1** (1878) pp. 184-240, 289-321.
4. D. D. Wall, Fibonacci series modulo *m*, *American Math. Monthly* **67** (1960) pp. 525-532.
5. John Vinson, The relation of the period modulo *m* to the rank of apparition of *m* in the Fibonacci sequence, *Fibonacci Quart.* **1** (2) (1963) pp. 37-45.
6. D. W. Robinson, The Fibonacci matrix modulo *m*, *Fibonacci Quart.* **1** (2) (1963) pp. 29-36.
7. John H. Halton, On the divisibility properties of Fibonacci numbers, *Fibonacci Quart.* **4** (1966) pp. 217-240.
8. Kevin Brown, The period of Fibonacci sequences modulo *m*, solution to Problem E3410, *American Math. Monthly* **99** (1992) pp. 278-279.
9. John H. Jaroma, On a generalised divisibility property of primes and the Fibonacci numbers, *Math. Gaz.* **87** (2003) pp. 486-491.
10. Dominic Vella and Alfred Vella, Some properties of finite Fibonacci sequences, *Math. Gaz.* **88** (2004) pp. 494-500.
11. G. H. Hardy and E. M. Wright, *An Introduction to the theory of Numbers* (5th edn.),Oxford University Press (1979).

10.1017/mag.2018.8

G. J. O. JAMESON
Dept. of Mathematics and Statistics, Lancaster University, Lancaster LA1 4YF
e-mail: *g.jameson@lancaster.ac.uk*

https://doi.org/10.1017/mag.2018.8 Published online by Cambridge University Press