involve
a journal of mathematics

Bounds for Fibonacci period growth

Chuya Guo and Alan Koch

mathematical sciences publishers

2009 Vol. 2, No. 2

INVOLVE 2:2(2009)

Bounds for Fibonacci period growth

Chuya Guo and Alan Koch

(Communicated by Arthur T. Benjamin)

We study the Fibonacci sequence mod n for some positive integer n. Such a sequence is necessarily periodic; we introduce a function $Q(n)$ which gives the ratio of the length of this period to n itself. We compute $Q(n)$ in certain cases and provide bounds for it which depend on the nature of the prime divisors of n.

1. Introduction

Any sequence of integers which satisfy a recurrence relation becomes periodic when reduced modulo n for any positive integer n. Here we investigate the behavior of the length of the period of the Fibonacci sequence modulo n, $n \in \mathbb{Z}^+$. We shall denote this length by $k(n)$, and call it the Fibonacci period mod n. This sequence was first studied by Wall [1960], and since that time many interesting properties of $k(n)$ have been discovered. For example, if m and n are relatively prime then $k(mn) = \operatorname{lcm}(k(m), k(n))$. Thus it seems reasonable to compute $k(n)$ using its prime power factorization: if $n = p_1^{e_1} \cdots p_t^{e_t}$ then $k(n) = \operatorname{lcm}(k(p_1^{e_1}), \ldots k(p_t^{e_t}))$. Assuming one can find the prime power factorization of n in a reasonable amount of time, two problems remain: there is no known formula for $k(p)$ when p is a prime, and though it is generally believed that $k(p^e) = p^{e-1}k(p)$ it has not been proven.

While $\{k(n)\}$ is not an increasing sequence it tends to grow as n does, in the sense that for $\{a_r\}$ an infinite sequence of positive integers we have that $\{k(a_r)\}$ is unbounded. A study of $k(n)$ makes it clear that certain such $\{a_r\}$ lead to period lengths which blow up much faster that others — two extreme examples being $\{2 \cdot 5^r\}$ and $\{F_r\}$.

In order to study the growth rates of such sequences we introduce the Fibonacci Q-function. The notion of this ratio is implicit in previous words — often n is compared to $k(n)$; for example, see [Coleman et al. 2006, Fig. 1] for a plot of $k(p)$

MSC2000: primary 11B39; secondary 11B50.

Keywords: Fibonacci sequence, Fibonacci periods, growth of Fibonacci periods, Fibonacci period mod n.

versus p, p prime. For all n we define $Q(n)$ to be the ratio of period length to modulus. We will see that for all $r \in \mathbb{Z}^+$ we have $Q(2 \cdot 5^r) = 6$ and $Q(F_r) \to 0$, where F_r is the r^{th} Fibonacci number. Using new and known results about Fibonacci periods we will compute $Q(n)$ for many classes of integers, including some classes of prime numbers as well as Fibonacci and Lucas numbers. Additionally, viewing Q as a function on positive integers, we will show that the image of Q, denoted $\mathfrak{Q}$, is contained in but not equal to $[0, 6] \cap \mathbb{Q}$. It turns out that $\mathfrak{Q}$ is infinite, as is its complement in $[0, 6] \cap \mathbb{Q}$. It is interesting as well to note that $1, 2, 3, 4$, and 6 are all in $\mathfrak{Q}$ – $Q(24) = 1$, $Q(60) = 2$, $Q(20) = 3$, $Q(5) = 4$, and $Q(10) = 6$ – but $5 \notin \mathfrak{Q}$.

We also establish bounds for $Q(n)$ which depend on the number t_1 of prime factors of n whose last digits are either 3 or 7. The bounds are given explicitly and depend on $\gcd(10, n)$. These bounds are useful when n has a small number of such factors, but the bound increases with t_1 and eventually exceeds 6. We also examine the *unit disk preimage* $U = \{n \in \mathbb{Z}^+ \mid Q(n) < 1\}$, showing it is closed under multiplication by relatively prime numbers, and give a sufficient (but not necessary) criterion for a number to be in U.

We finish with a number of open questions concerning values of $Q(n)$ and topological properties of $\mathfrak{Q}$. Perhaps the most famous conjecture concerning k is that $k(p^e) = p^{e-1}k(p)$ when p is a prime. Using the Q-function the conjecture becomes $Q(p^e) = Q(p)$, and it is no surprise that our conjecture is equivalent the one on k. We will show that this conjecture holds in the case where p is a Fibonacci prime. We will see that the answers to many of our other open questions on values of $Q(n)$ will follow immediately from other famous conjectures. For example, we conjecture that there are infinitely many primes p such that $Q(p) = 2(1 + 1/p)$ and infinitely many primes p such that $Q(p) = 1 - 1/p$. With the exception of $p = 5$ we have $Q(p) \leq 2(1 + 1/p)$, and if there are an infinite number of Mersenne Primes whose last digit is 3 or 7 then there are an infinite number of points where we have equality. Also, if $p \equiv \pm 1 (\text{mod } 10)$ then $Q(p) \leq 1 - 1/p$, and if there are an infinite number of Sophie Germaine primes then U contains infinitely many primes (primes which, in fact, are safe rather than Sophie Germaine).

2. Preliminaries

Consider the recurrence relation

$$a_n = a_{n-1} + a_{n-2},\ n \geq 2.$$

If we set $a_0 = 0$ and $a_1 = 1$ we obtain the Fibonacci sequence, which we denote by $\{F_n\}$. Each F_n is a Fibonacci number, and if F_n is prime then it is called a *Fibonacci prime*. Examples of Fibonacci primes include $2, 3, 5, 13$, and 89. It is

well known (see, for example, [Hardy and Wright 1954, Theorem 179 (iv)]) that if $m \mid n$ then $F_m \mid F_n$, hence if F_q is a Fibonacci prime, $q > 4$ then q is also prime. It is conjectured that there are an infinite number of Fibonacci primes. We may extend the Fibonacci sequence to negative indices. If we define $F_{-n} = (-1)^{n-1} F_n,\ n \geq 1$ then $F_n = F_{n-1} + F_{n-2}$ for all integers n.

While the Fibonacci sequence is the focus here, we will also need to consider the Lucas sequence $\{L_n\}$, obtained by $L_0 = 2,\ L_1 = 1$, and the recurrence relation above. Note that $L_n = F_{n+1} - F_{n-1}$. In a manner similar to F_n we may define $L_{-n} = (-1)^n L_n$, and we may then extend the identity $L_n = L_{n-1} + L_{n-2}$ to all $n \in \mathbb{Z}$.

For any $n \geq 0$ we define $k(n)$ to be the smallest positive integer such that

$$F_{k(n)} \equiv 0 \text{ and } F_{k(n)+1} \equiv 1 (\mathrm{mod}\, n).$$

The number $k(n)$ is called the *Fibonacci period* mod n. Notice that this term is appropriate because, mod n, the sequence of Fibonacci numbers is necessarily a periodic sequence mod n, i.e. $F_{k(n)+i} \equiv F_i \ (\mathrm{mod}\, n)$. Periodicity is guaranteed since there are only n^2 possibilities for F_i and F_{i+1}, and if

$$F_i \equiv F_j (\mathrm{mod}\, n) \qquad \text{and} \qquad F_{i+1} \equiv F_{j+1} (\mathrm{mod}\, n),$$

then it is easy to show (by repeated subtraction) that

$$F_{i-j} \equiv 0 (\mathrm{mod}\, n) \qquad \text{and} \qquad F_{i-j+1} \equiv 1 (\mathrm{mod}\, n).$$

Example 2.1. Modulo 2 the Fibonacci sequence is $0, 1, 1, 0, 1, 1, \ldots$ and thus $k(2) = 3$. Modulo 3 we have the sequence

$$0, 1, 1, 2, 0, 2, 2, 1, 0, 1, \ldots$$

hence $k(3) = 8$. The sequence mod 4 is

$$0, 1, 1, 2, 3, 1, 0, 1, \ldots$$

and $k(4) = 6$. If we take the sequence mod 5 we get

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

and thus $k(5) = 20$.

There is no known formula for $k(n)$, however many of its properties are known. The result below summarizes the facts that we will need. Proofs of each can be found in [Renault 1996], although many are first described in Wall's original paper.

Lemma 2.2. *Let $p, n \in \mathbb{Z}^+$, p prime. The length of a Fibonacci period satisfies all of the following.*

(1) *For $n > 2$, $k(n)$ is even.*

(2) *If* $p \equiv \pm 1 \pmod{10}$ *then* $k(p) \mid p-1$.

(3) *If* $p \equiv \pm 3 \pmod{10}$ *then* $k(p) \mid 2(p+1)$ *and* $k(p) \nmid (p+1)$.

(4) *Let* t *be the largest integer such that* $k(p^t) = k(p)$. *Then for all* $e \geq t$, $k(p^e) = p^{e-t}k(p)$.

(5) *For* $\gcd(m,n) = 1$ *we have* $k(mn) = \operatorname{lcm}(k(m), k(n))$.

(6) *Suppose* $n \geq L_t$. *Then* $k(n) \geq 2t$.

(7) *Let* $a(n)$ *be the smallest positive integer such that* $F_{a(n)} \equiv 0 \pmod{n}$, *and let* $b(n)$ *be the number of indices* $1 \leq i \leq k(n)$ *with* $F_i \equiv 0 \pmod{n}$. *Then* $k(n) = a(n)b(n)$ *and* $b(n) = 1, 2,$ *or* 4.

(8) *For all* $e \geq 1$, $b(p^e) = b(p)$.

Throughout the paper, the numbers $a(n)$ and $b(n)$ will be as described above.

It was conjectured by Wall that $k(p^2) = pk(p)$, and it is only a slight generalization to conjecture $k(p^e) = p^{e-1}k(p)$, i.e. that $t = 1$ in the fourth statement above. This is the most famous conjecture related to the study of $k(n)$, and we will refer to this as Wall's Conjecture. As mentioned in the introduction, we will show it is true for Fibonacci primes.

Notice that, for any given prime, Lemma 2.2 (6) implies that one need only check a finite number of exponents to establish Wall's Conjecture for a given prime. For example, one can directly compute $k(17) = 36$. To show

$$k(17^e) = 17^{e-1}k(17) = 36 \cdot 17^{e-1},$$

notice that $L_{19} = 9349$. Then for each $n \geq 9349$ we have $k(n) \geq 2 \cdot 19 = 38$, hence if $17^t \geq 9349$ then $k(17^t) \geq 38 > 36 = k(17)$. Thus since $17^2 = 289$, $17^3 = 4913$, and $17^4 = 83521 > 9349$ one needs to check that $k(17^2)$ and $k(17^3)$ are not 36 — they are, in fact, 612 and 10404, as expected.

We are now ready to formally introduce the tool we will use to study Fibonacci periods mod n.

Definition 2.3. *For any* $n \in \mathbb{Z}^+$ *let*

$$Q(n) = \frac{k(n)}{n}.$$

Q *is called the* Fibonacci Q-Function.

Example 2.4. $Q(2) = 3/2$, $Q(3) = 8/3$, $Q(4) = 3/2$, and $Q(5) = 4$. Notice that $Q(2) = Q(4)$ and that $Q(5)$ is much larger than the others – we will discuss both of these observations later.

Example 2.5. For all e, $Q(17^e) = Q(17) = 36/17$.

3. Points

The rest of the paper is an investigation of the properties of $Q(n)$. In the previous section we computed $Q(n)$ for numbers at most 5 (note that $Q(1) = 1$). Here we will look at certain classes of numbers for which we can compute $Q(n)$ exactly. Perhaps the easiest numbers to study are the Fibonacci numbers themselves.

Example 3.1. The numbers 8 and 11 are both Fibonacci numbers: $8 = F_6$ and $13 = F_7$. Clearly $a(8) = 6$ since $F_6 \equiv 8 \equiv 0 (\mathrm{mod}\, 8)$ and since $F_n < 8$ for $1 \leq n \leq 5$ this is the smallest Fibonacci number for which we get zero mod 8. By Lemma 2.2 (7)–(8) we know that $k(8) = 6$, 12, or 24. Since $F_7 = F_6 + F_5$ we have

$$F_6 + 1 < F_7 < 2 \cdot F_6$$

and hence F_7 is not 1 mod 8, i.e. $k(8) \neq 6$. Finally, note

$$F_{-6} = (-1)^5 F_6 = -8 \equiv 0 (\mathrm{mod}\, 8)$$
$$F_{-5} = (-1)^4 F_5 = F_5 \equiv F_7 (\mathrm{mod}\, 8)$$

since $F_7 = F_5 + F_6 \equiv F_5 (\mathrm{mod}\, F_6)$. Thus the sequence is periodic, period 12, so $k(8) = 12$. Similarly, $a(13) = 7$ and thus $k(13) = 7$, 14, or 28. Since

$$F_7 + 1 < F_8 < 2 \cdot F_9$$

we know $k(13) \neq 7$. In this case note that $F_{-7} = F_7$ and $F_{-6} = -F_6$ which is not congruent to $F_8 (\mathrm{mod}\, 11)$ since then $F_6 \equiv F_8 \equiv -F_6 (\mathrm{mod}\, 11)$ and this implies $2 \cdot F_6 = F_7$ which cannot occur. Thus $k(13) = 28$.

We have $Q(8) = 3/2$ and $Q(13) = 28/13$. We can use the results on these Fibonacci numbers to help us compute $Q(n)$ for other numbers. For example,

$$Q(104) = \frac{k(104)}{104} = \frac{\mathrm{lcm}(k(8), k(13))}{104} = \frac{\mathrm{lcm}(2 \cdot 6, 4 \cdot 7)}{104} = \frac{21}{26}.$$

Note that the Q-function has an interesting property on this product:

$$Q(104) = Q(8)Q(13)/4.$$

More generally, we have

Theorem 3.2. *Let $n \geq 3$ be an integer.*

(1) *If n is even, then $Q(F_n) = 2n/F_n$. If n is odd, $Q(F_n) = 4n/F_n$.*

(2) *If n is even, then $Q(L_n) = 4n/F_n$. If n is odd, $Q(L_n) = 2n/F_n$.*

(3) *If $F_q = p$ is an odd prime, then $Q(p^e) = Q(p) = 4q/p$. Also, $Q(2^e) = 3/2$.*

(4) *Let* $\{n_1, n_2, \ldots, n_t\}$ *be a sequence of positive integers such that* $\gcd(n_i, n_j) \leq 2$, $t > 1$. *Then*

$$Q(F_{n_1} F_{n_2} \cdots F_{n_t}) = 4^{1-t} Q(F_{n_1}) \cdots Q(F_{n_t}).$$

Proof. A proof of Theorem 3.2 (1) is omitted, however it may be obtained by generalizing the previous example. Also, (2) is similar to (1) and is also omitted.

For Theorem 3.2 (3), by Lemma 2.2 (4) we know that $k(p^e) = p^{e-t} k(p)$, where t is the largest positive integer such that $k(p^t) = k(p)$. Since $p^e > p = F_q$ for all $e > 1$ it is clear that $a(p^e) > a(p)$. Since $b(p^e) = b(p)$ we see that $k(p^t) > k(p)$ unless $t = 1$. Thus

$$Q(p^e) = \frac{p^{e-1} k(p)}{p^e} = \frac{k(p)}{p} = \frac{4q}{p}.$$

To show that $Q(2^e) = 3/2$, it suffices to show that $k(2^e) > 3$ for all $e > 1$. But since $2^e > 3 = L_2$ we know that $k(2^e) \geq 2 \cdot 3$ and we are done.

We now prove Theorem 3.2 (4). Note that $\gcd(n_i, n_j) \leq 2$ implies that

$$\gcd(F_{n_i}, F_{n_j}) = 1$$

since

$$\gcd(F_{n_i}, F_{n_j}) = F_{\gcd(n_i, n_j)}.$$

Suppose $n_1, n_2, \ldots, n_s$ are all even and $n_{s+1}, n_{s+2}, \ldots, n_t$ are all odd. Then we have

$$\begin{aligned} Q(F_{n_1} F_{n_2} \cdots F_{n_t}) &= \frac{\operatorname{lcm}(k(F_{n_1}), \ldots, k(F_{n_t}))}{F_{n_1} F_{n_2} \cdots F_{n_t}} \\ &= \frac{\operatorname{lcm}(2n_1, 2n_2, \ldots, 2n_s, 4n_{s+1}, \ldots, 4n_t)}{F_{n_1} F_{n_2} \cdots F_{n_t}} \\ &= 4\left(\frac{\operatorname{lcm}(n_1/2, n_2/2, \ldots, n_s/2, n_{s+1}, \ldots, n_t)}{F_{n_1} F_{n_2} \cdots F_{n_t}}\right) \\ &= 4 \frac{n_1 n_2 \cdots n_t}{2^s F_{n_1} F_{n_2} \cdots F_{n_t}}, \end{aligned}$$

the last equality since the set $\{n_1/2, n_2/2, \ldots, n_s/2, n_{s+1}, \ldots, n_t\}$ is pairwise relatively prime. Note that $n_i / F_{n_i} = Q(F_{n_i})/2$ for $i \leq s$ and $n_i / F_{n_i} = Q(F_{n_i})/4$ otherwise. Thus

$$\begin{aligned} Q(F_{n_1} F_{n_2} \cdots F_{n_t}) &= \frac{4}{2^s}((Q(F_{n_1})/2) \cdots (Q(F_{n_s})/2))((Q(F_{n_{s+1}})/4) \cdots (Q(F_{n_t})/4)) \\ &= \frac{4}{2^s} \frac{1}{2^s} (Q(F_{n_1}) \cdots Q(F_{n_s})) \frac{1}{4^{t-s}} (Q(F_{n_{s+1}}) \cdots Q(F_{n_t})) \\ &= \frac{4}{4^t} Q(F_{n_1}) \cdots Q(F_{n_t}) = 4^{1-t} Q(F_{n_1}) \cdots Q(F_{n_t}). \end{aligned}$$

□

Remark 3.3. Note that Theorem 3.2 (4) does not extend to powers of Fibonacci numbers since $Q(45) = 8/3$ and $(1/4)Q(3)Q(5) = 8$. Nonetheless, it remains easy to compute $Q(n)$ whenever n is a product of powers of relatively prime Fibonacci numbers.

We will now try to compute $Q(p)$ when p is in one of a few well-known classes of primes. Let $p \equiv \pm 3 (\mathrm{mod}\ 10)$. From Lemma 2.2 (3) we see that $k(p) \mid 2(p+1)$. To find a class of primes where we can explicitly compute $Q(p)$ we can consider primes such that $p+1$ has few divisors. Thus it is natural to consider Mersenne primes, primes of the form $2^q - 1$ for some q. It is well known that q must be prime for $2^q - 1$ to be prime: see, for example, [Rosen 2000, Theorem 7.11]. On the other hand, if $p \equiv \pm 1 (\mathrm{mod}\ 10)$ then $k(p) \mid (p-1)$, so any prime of this form that also satisfies $p = 2q+1$, q prime will have few divisors.

Theorem 3.4. *Let p be prime.*

(1) *If p is a Fibonacci prime, say $p = F_q$ with $q > 4$ then $Q(p) = 4q/p$.*

(2) *If p is a Mersenne prime, $p = 2^q - 1$, such that $q \equiv 3 (\mathrm{mod}\ 4)$ then $Q(p) = 2(1 + 1/p) = 2^{q+1}/p$.*

(3) *If p is a safe prime i.e. $p = 2q + 1$ for some Sophie Germaine prime q such that $q \equiv -1 (\mathrm{mod}\ 10)$ then $Q(p) = 1 - 1/p = 2q/p$.*

Proof. Notice that Theorem 3.4 (1) is a special case of Theorem 3.2 (1) and (3).

We now prove Theorem 3.4 (2). If $q = 4s + 3$ then since the last digit of 6^s is 6 we get

$$p = 2^{4s+3} - 1 = 16^s \cdot 8 - 1 \equiv 6^s \cdot 8 - 1 \equiv 47 \equiv 7 (\mathrm{mod}\ 10)$$

and so $k(p) \mid 2(p+1)$, i.e. $k(p) \mid 2^{q+1}$. But $k(p) \nmid (p+1)$, i.e. $k(p) \nmid 2^q$, thus $k(p) = 2^{q+1}$ and $Q(p) = 2(1 + 1/p) = 2^{q+1}/p$.

Finally, if $p = 2q + 1$ with $q \equiv -1 (\mathrm{mod}\ 10)$ then $p \equiv 2(-1) + 1 \equiv -1 (\mathrm{mod}\ 10)$, thus $k(p) \mid p - 1$. But $p - 1 = 2q$, so $k(p) = 1, 2, q$, or $2q$. Since $k(p)$ is even and $k(p) > 2$ we must have $k(p) = 2q$, hence $Q(p) = 1 - 1/p = 2q/p$ and Theorem 3.4 (3) is proven. □

Example 3.5. The largest known Mersenne prime of the form above is

$$M_{42} = 2^{25964951} - 1.$$

The Fibonacci Q-function of this 7,816,230-digit number is

$$Q(M_{42}) = \frac{2^{25964952}}{2^{25964951} - 1} \approx 2 + 10^{-7816230}.$$

This is the largest prime for which we know $Q(p)$, and we do not know a prime p such that $Q(p)$ is closer to 2 than $Q(M_{42})$. (We do, however conjecture that for all $\varepsilon > 0$ there is a prime p within ε of 2.)

We now investigate certain values of the Q function.

Theorem 3.6. *Let $r \geq 1$. Then*

(1) $Q(n) = 1$ *if and only if* $n = 24 \cdot 5^{r-1}$.

(2) $Q(n) = 3/2$ *if* $n = 10^{r+2}$.

(3) $Q(n) = 6$ *if and only if* $n = 2 \cdot 5^r$.

Proof. The "if" portions of each of these can be determined by direct calculations since each prime factor is a Fibonacci prime. For example,

$$Q(10^n) = \frac{\operatorname{lcm}(k(2^n), k(5^n))}{10^n} = \frac{\operatorname{lcm}(2^{n-1} \cdot 3, 5^{n-1} \cdot 20)}{10^n} = \frac{2^{n-1} \cdot 3 \cdot 5^n}{2^n 5^n} = \frac{3}{2}$$

establishes Theorem 3.6 (2). The "only if" portions of Theorem 3.6 (1) and (3) follow from the results presented in [Fulton and Morris 1969/1970] and [Brown 1992] respectively. □

In fact, [Brown 1992] proves something stronger: the author shows that $k(n) \leq 6n$ with equality if and only if $n = 24 \cdot 5^{r-1}$. This will be useful when we construct bounds for $Q(n)$ in the next section.

Note that there is no "only if" in Theorem 3.6 (2) since, for example, $Q(2) = 3/2$. It would be interesting to be able to describe the set $Q^{-1}(3/2)$.

Having determined some of the values of Q, it is worth describing certain rational numbers in $[0, 6]$ which are not values of Q. Clearly $Q(n) \neq 0$ for all n since $k(n) \geq 1$ for all $n \in \mathbb{Z}^+$. The following gives an infinite number of other rationals in this interval which are not values of Q.

Theorem 3.7. *Let n be a positive integer. Then*

(1) $Q(n) \neq 5$.

(2) *For each Fibonacci prime p, $Q(n) \neq \frac{t}{p^j u}$ for any t, u relatively prime to p and $j \geq 2$.*

Proof. Let n be the smallest positive integer so that $Q(n) = 5$. Then $k(n) = 5n$, and since $n > 2$ we know that $k(n)$ is even, hence $5n$ is be even. Write $n = 2^i s$, s odd, $i \in \mathbb{Z}^+$. Then

$$5 \cdot 2^i s = k(n) = \operatorname{lcm}(2^{i-1} \cdot 3, k(s)).$$

Since 3 divides the right-hand side we see that $3 \mid s$. Write $s = 3^j t$, t odd, $j \in \mathbb{Z}^+$, $3 \nmid t$. Then

$$5(2^i \cdot 3^j \cdot t) = k(n) = \operatorname{lcm}(2^{i-1} \cdot 3, 3^{j-1} \cdot 8, k(t)).$$

From this we see that $5t \mid k(t)$. Note that if $5t < k(t)$ then $k(t) \geq 10t > 6t$ which cannot occur by [Brown 1992]. Thus $k(t) = 5t$. But $t < n$, contradicting the minimality of n. Thus Theorem 3.7 (1) is proved.

For Theorem 3.7 (2), the trick is that the denominator, before cancellation, is always n. Suppose $Q(n) = t/p^j u$. Then $p^j u \mid n$, so we can write $n = p^i um$ for some $i \geq j$ and $\gcd(p, um) = 1$. Then

$$\frac{t}{p^j u} = Q(n) = \frac{\operatorname{lcm}(k(p^i), k(um))}{p^i um} = \frac{\operatorname{lcm}(p^{i-1}k(p), k(um))}{p^i um}.$$

Cross-multiplying gives

$$tp^i um = p^j u \operatorname{lcm}(p^{i-1}k(p), k(um)).$$

The right-hand side is clearly divisible by p^{i+j-1}, however since $i + j - 1 \geq i + 1$ and $p \nmid mtu$ we see that the left hand side is not divisible by p^{i+j-1}, a contradiction. Thus such an n cannot occur and we are done. □

4. Bounds

In general, it is no easier to compute $Q(n)$ than $k(n)$. However, it is more natural to describe bounds on the Q-function than it is on the period. For example, the statement $k(n) \leq 6n$ can be stated more naturally as $Q(n) \leq 6$. This fact, together with Lemma 2.2 (6) gives

Proposition 4.1. $L_t/(2n) \leq Q(n) \leq 6$, *where* $n \geq L_t$.

To show that these are the best bounds possible in general we have

Corollary 4.2. $\sup\{Q(n)\} = 6$ *and* $\inf\{Q(n)\} = 0$.

Proof. The sequence $\left\{Q(2 \cdot 5^{r-1})\right\}$ is a sequence of 6's and hence converge to 6. The sequence $\{Q(F_n)\}$ converges to 0. □

We can get a better upper bound if we restrict ourselves to certain classes of integers. The natural place to start is to find an upper bound for Q restricted to primes. We already know the result in this case.

Lemma 4.3. *Let* p *be prime.*

(1) $Q(2) = 3/2$ *and* $Q(5) = 4$.

(2) *Suppose* $p \equiv \pm 1 \pmod{10}$. *Then* $Q(p) \leq 1 - 1/p$.

(3) *Suppose* $p \equiv \pm 3 \pmod{10}$. *Then* $Q(p) \leq 2(1 + 1/p)$.

Proof. Of course, Lemma 4.3 (1) was stated before — is included here only for completeness. Lemma 4.3 (2) and (3) follow immediately from Lemma 2.2 (2) and (3). □

Note that $p = 3$ and 11 give the largest possible value for $Q(p)$ under the conditions in Lemma 4.3 (3) and (2), respectively. Combining those two parts gives

Corollary 4.4. *For $p \neq 5$ a prime $Q(p) \leq 2(1+1/p)$.*

We now consider powers of primes. With the exception of $p = 5$ there is a universal bound for such numbers.

Lemma 4.5. *For any prime $p \neq 5$ we have $Q(p^e) \leq Q(p) \leq 8/3$; furthermore $Q(5^e) = Q(5) = 4$.*

Proof. If $p = 2$ then $Q(p) = 3/2 \leq 8/3$. Furthermore, since 2 is a Fibonacci prime we know $Q(2^e) = Q(2) = 3/2$. Likewise, $Q(3^e) = Q(3) = 8/3$ and $Q(5^e) = Q(5) = 4$. We shall assume $p \geq 7$. Then $Q(p) \leq 2(1+1/p) \leq 2(1+1/7) = 16/7 < 8/3$, so it remains to show $Q(p^e) \leq Q(p)$ for $e > 1$.

Suppose $a = a(p)$ and $a' = a(p^e)$. Since $F_{a'} \equiv 0 (\mathrm{mod}\, p^e)$ we know $F_{a'} \equiv 0 (\mathrm{mod}\, p)$ and hence a' is a multiple of a. We claim that $F_{p^{e-1}a} \equiv 0 (\mathrm{mod}\, p^e)$, and hence $a' \leq p^{e-1}a$. Applying the well-known identity

$$F_{mn} = \sum_{i=1}^{m} \binom{m}{i} F_i F_n^i F_{n-1}^{m-i}$$

we have

$$F_{p^{e-1}a} = \sum_{i=1}^{p^{e-1}} \binom{p^{e-1}}{i} F_i F_a^i F_{a-1}^{p^{e-1}-i}.$$

For $1 \leq i \leq p^{e-1}$ we clearly have $p^i \mid F_a^i$. If we write $i = p^f j$, $p \nmid j$ it can be shown that $p^{e-f-1} \mid \binom{p^{e-1}}{i}$. Thus $p^{e-f-1+i}$ divides the i^{th} term in the series above. Since $i > 0$ we have $i \geq f+1$ and so each term is divisible by p^e, hence $F_{p^{e-1}a} \equiv 0 (\mathrm{mod}\, p^e)$.

Thus,

$$Q(p^e) = \frac{a'b(p^e)}{p^e} \leq \frac{(p^{e-1}a)b(p)}{p^e} = \frac{k(p)}{p} = Q(p). \qquad \square$$

Next, we look at how Q behaves with relatively prime numbers.

Lemma 4.6. *For $\gcd(m,n) = 1$ we have $Q(mn) \leq Q(m)Q(n)$. If furthermore $m, n > 2$ then $Q(mn) \leq \frac{1}{2}Q(m)Q(n)$.*

Proof. For m and n relatively prime we have

$$\begin{aligned} Q(mn) &= \frac{\mathrm{lcm}(k(m), k(n))}{mn} = \frac{k(m)k(n)}{mn \gcd(k(m), k(n))} \\ &= \frac{1}{\gcd(k(m), k(n))} Q(m)Q(n) \leq Q(m)Q(n). \end{aligned}$$

If $m, n > 2$ then $k(m)$ and $k(n)$ are both even, hence $\gcd(k(m), k(n)) \geq 2$ and we are done. $\square$

Before continuing to generalize n, we note that this lemma gives us insight into the structure of the *unit disk preimage*.

Corollary 4.7. *Let* $U = \left\{n \in \mathbb{Z}^+ \mid Q(n) < 1\right\}$. *Then* U *is infinite, and is closed under multiplication by relatively prime elements.*

Proof. Certainly $p \in U$ for all primes $p \equiv \pm 1 (\mathrm{mod}\, 10)$, and by Lemma 4.5 we have $p^e \in U$ for all e hence U is infinite. (One could obtain a different proof using Dirichlet's Theorem on Primes in Arithmetic Progressions.) That U is closed under multiplication by relatively prime elements is clear from the previous result. □

Finally, we are ready to consider arbitrary n. For the remainder of the section we write

$$n = 2^r 5^s p_1^{r_1} \cdots p_t^{r_t},\ m = p_1^{r_1} \cdots p_t^{r_t},\ \gcd(10, m) = 1$$

and we let

$$t_0 = \#\left\{i \mid p_i \equiv \pm 1 (\mathrm{mod}\, 10)\right\} \text{ and } t_1 = \#\left\{i \mid p_i \equiv \pm 3 (\mathrm{mod}\, 10)\right\}.$$

Proposition 4.8. *We have* $Q(m) \leq Q(p_1) \cdots Q(p_t)/2^{t-1}$.

Proof. Immediate from Lemmas 4.5 and 4.6. □

Theorem 4.9. *We have* $Q(m) \leq 2^{2t_1 - t_0 + 1}/3^{t_1}$. *Furthermore,*

$$Q(5^s m) \leq \frac{2^{2t_1 - t_0 + 2}}{3^{t_1}},\ Q(2^r m) \leq \frac{2^{2t_1 - t_0}}{3^{t_1 - 1}},\ \text{and } Q(2^r 5^s m) \leq \frac{2^{2t_1 - t_0 + 1}}{3^{t_1 - 1}}.$$

Proof. Since $Q(p_i) \leq 8/3$ when $p_i \equiv \pm 3 (\mathrm{mod}\, 10)$ and $Q(p_i) < 1$ when $p_i \equiv \pm 1 (\mathrm{mod}\, 10)$ we have

$$Q(m) \leq \frac{1^{t_0} (\frac{8}{3})^{t_1}}{2^{t-1}} = (\frac{8}{3})^{t_1} \frac{1}{2^{t-1}} = \frac{2^{3t_1}}{3^{t_1} \cdot 2^{t_0 + t_1 - 1}} = \frac{2^{2t_1 - t_0 + 1}}{3^{t_1}}.$$

Similarly we have

$$Q(5^s m) \leq \frac{1}{2} Q(5^s) Q(m) = 2Q(m) \leq \frac{2^{2t_1 - t_0 + 2}}{3^{t_1}}.$$

and

$$Q(2^r m) \leq \frac{3}{2} Q(m) \leq \frac{2^{2t_1 - t_0}}{3^{t_1 - 1}},$$

and

$$Q(2^r 5^s m) \leq 3Q(m) \leq \frac{2^{2t_1 - t_0 + 1}}{3^{t_1 - 1}}.$$ □

One can obtain an overall bound by taking the largest of the four expressions.

Corollary 4.10. *For any* n *we have*

$$Q(n) \leq \frac{2^{2t_1 - t_0 + 1}}{3^{t_1 - 1}}.$$

Notice that this bound is quite significant if n has a lot of primes of the form $p \equiv \pm 1 (\mathrm{mod}\, 10)$, however there will also be cases where the bound does not provide useful information. For example, if $t_0 = 0$ and $t_1 = 7$ we have $Q(m) \leq 7.5$, which we already knew.

We can use Theorem 4.9 to obtain a sufficient, though not necessary, criterion for a number to be in the *unit disk preimage*.

Corollary 4.11. *If*

$$t_0 \geq t_1 \frac{\ln 4/3}{\ln 2} + 1,$$

then $m \in U$. *If*

$$t_0 \geq t_1 \frac{\ln 4/3}{\ln 2} + 2,$$

then $5^s m \in U$. *If*

$$t_0 \geq t_1 \frac{\ln 4/3}{\ln 2} + \ln 3,$$

then $2^r m \in U$. *Finally, if*

$$t_0 \geq t_1 \frac{\ln 4/3}{\ln 2} + \ln 3 + 1,$$

then $n \in U$.

Proof. Obtained by setting each of the bounds equal to 1 and solving for t_0. For example, if we set

$$Q(m) \leq \frac{2^{2t_1 - t_0 + 1}}{3^{t_1}} \leq 1,$$

we get

$$\begin{aligned} 2^{2t_1 - t_0 + 1} &\leq 3^{t_1} \\ (2t_1 - t_0 + 1) \ln 2 &\leq t_1 \ln 3 \\ (2 \ln 2 - \ln 3) t_1 + \ln 2 = \ln(4/3) t_1 + \ln 2 &\leq t_0 \ln 2 \\ t_0 &\geq t_1 \frac{\ln 4/3}{\ln 2} + 1. \end{aligned}$$

The others are similar. □

Notice that if $t_0 = 0$ and $t_1 = 2$, Theorem 4.9 gives $Q(m) \leq 32/9$. However, it is clear we can do better since $Q(p) = 8/3$ only when $p = 3$. In fact, we have

$$Q(m) \leq \frac{1}{2} \frac{8}{3} \frac{16}{7} = \frac{64}{21} < 3.048$$

This leads to a stronger bound.

Theorem 4.12. *For $t_1 > 2$,*

$$Q(m) \le \frac{2^{6-t_0}}{21} \prod_{i=3}^{t_1} \left(\frac{5i-12}{5i-13} \right).$$

Proof. Assume that $3 \le p_1 < p_2 < \cdots < p_t$. Again if $p_i \equiv \pm 1 (\mathrm{mod}\, 10)$ then $Q(p_i) \le 1$. If $p_i \equiv \pm 3 (\mathrm{mod}\, 10)$ then $Q(p_i) \le 2(1+1/p_i)$. If we write $p_i = 10h \pm 3$ then $h \ge (i/2 - 1)$ since there are at most two such primes between $10z$ and $10(z+1)$. Thus

$$p_i = 10h \pm 3 \ge 10h - 3 \ge 10(i/2 - 1) - 3 = 5i - 13$$

and hence

$$Q(p_i) \le 2\left(1 + \frac{1}{5i-13}\right) = 2\left(\left(\frac{5i-12}{5i-13}\right)\right)$$

for $i \ge 3$. Since $Q(p_1) \le 8/3,\ Q(p_2) \le 16/7$ we have

$$\begin{aligned} Q(m) &\le \frac{1}{2^{t-1}} \frac{8}{3} \frac{16}{7} \prod_{i=3}^{t_1} 2\left(\frac{5i-12}{5i-13}\right) = \frac{2^7}{2^{t_0-1+t_1} \cdot 21} 2^{t_1-2} \prod_{i=3}^{t_1} \left(\frac{5i-12}{5i-13}\right) \\ &= \frac{2^{6-t_0}}{21} \prod_{i=3}^{t_1} \left(\frac{5i-12}{5i-13}\right). \end{aligned}$$

□

Here is a table of bounds for m when $t_0 = 0$; similar tables for $2^r 5^s m$ can be constructed. For the second bound, we use $8/3$ and $64/21$ when $t = 1$ and 2 respectively.

t_1	1	2	3	4	5	6	7
First Bound	2.667	3.556	4.741	(over 6)			
Second Bound	2.667	3.048	4.572	5.225	5.660	5.993	(over 6)

We could, with much work, obtain progressively sharper bounds for large t_1 by noticing that our bounds constructed above use the fact that there are at most two primes whose last digit is 3 or 7 between $10z$ and $10(z+1)$; there may be fewer, e.g. when $z = 2$ or 3.

5. Questions

We conclude with several conjectures and questions. Many of the these relate directly to Wall's conjecture or other well-known questions. We start with the obvious

Conjecture 5.1. $Q(p^e) = Q(p)$ for all primes p.

Notice that this is equivalent to Wall's conjecture since if

$$Q(p^e) = k(p^e)/p^e = k(p)/p = Q(p)$$

then $k(p^e) = p^{e-1}k(p)$.

Theorem 3.7 established that the image of Q , viewed as a function $\mathbb{Z}^+ \to \mathbb{Q}$, does not include numbers which cannot be expressed with denominators divisible by a Fibonacci prime power greater than one. It seems likely that this result extends.

Conjecture 5.2. For any prime p, $Q(n) \neq \frac{t}{p^j u}$ for all n and any t relatively prime to p, and $j \geq 2$.

If Conjecture 5.1 is true, then by Theorem 3.7 (2) so is this one. There is a partial converse.

Proposition 5.3. *If Conjecture 5.2 is true, then Wall's Conjecture is true when either $e \neq 2$ or $p \equiv \pm 1 (\mathrm{mod}\ 10)$.*

Proof. Suppose Conjecture 5.2 holds. We know Wall's Conjecture holds when $p = 2$, so hereafter we assume $p \neq 2$. We have

$$Q(p^e) = \frac{k(p^e)}{p^e}.$$

Since the denominator, when reduced, can have at most one power of p we see that p^{e-1} must divide the numerator. Thus $k(p^e) \geq p^{e-1}$. If $e \geq 3$ then

$$k(p^e) \geq p^{e-1} \geq p^2 > 2(p+1) \geq k(p)$$

since $p \geq 3$. Thus if $k(p^t) = k(p)$ then $t = 1$ or 2. Finally, if $e \geq 2$ and $p \equiv \pm 1 (\mathrm{mod}\ 10)$ then

$$p^{e-1} \geq p > p - 1 \geq k(p)$$

and hence $k(p^t) = k(p)$ can only occur if $t = 1$. □

We saw that the "unit disk preimage" U is closed under multiplication by relatively prime numbers, and Lemma 4.5 can be used to show that U is closed under powers, i.e. $u \in U$ implies $u^i \in U$ for all $i \geq 1$. This suggests that the following may be true.

Conjecture 5.4. If $m, n \in U$, then $mn \in U$.

Note that the converse to this is not true: $Q(3) = 8/3$ and $Q(7) = 16/7$, so $3, 7 \notin U$; however $Q(21) = 16/21$ and hence $21 \in U$. If this conjecture is true then U is a semigroup; furthermore $V := \{n \in \mathbb{Z}^+ \mid Q(n) \leq 1\}$ is a monoid since $Q(1) = 1$.

The final two conjectures are motivated by the empirical observation that $k(p)$ is often $p - 1$ or $2(p + 1)$.

Conjecture 5.5. There are an infinite number of primes with $Q(p) = 2(1 + 1/p)$.

If there are an infinite number of Mersenne primes $2^q - 1$ with $q \equiv 3 (\mathrm{mod}\, 4)$ then this conjecture is true.

Conjecture 5.6. There are an infinite number of primes with $Q(p) = (1 - 1/p)$.

If there are an infinite number of Sophie Germaine primes with $q \equiv -1 (\mathrm{mod}\, 10)$ then this conjecture is true. Alternatively, if one could show that there are an infinite number of length four Cunningham chains of the first kind then the conjecture would be proved.

Finally, viewing Q once again as a function $\mathbb{Z}^+ \to \mathbb{Q}$ we can ask a variety of questions about the image. Let $\mathfrak{Q}$ be the image of Q, and let $I = [0, 6] \cap \mathbb{Q}$. What are the topological properties of $\mathfrak{Q}$ as a subset of I? Is it dense? What are its limit points? We know that 0 is an accumulation point since $\{Q(F_{2k+1})\}$ is a strictly decreasing sequence in $\mathfrak{Q}$ converging to 0. (This also establishes that $\mathfrak{Q}$ is infinite.) Thus $\mathfrak{Q}$ is certainly not a closed set – what is its closure in I?. If there are an infinite number of Fibonacci primes then 0 would be a boundary point since $\frac{1}{p^2} \notin \mathfrak{Q}$ for all Fibonacci primes. (In fact we have that every point in $\mathfrak{Q}$ is a boundary point since for each $q \in \mathfrak{Q}$ any each $\varepsilon > 0$ there exists a $t/2^i$, t odd, $i \geq 2$ such that $\left|q - t/2^i\right| < \varepsilon$.) The two previous conjectures would also imply that 1 and 2 are accumulation points. Are there others? Is 6 an isolated point? What about 4? If these points are isolated than $\mathfrak{Q}$ cannot be open in I. A topological study of $\mathfrak{Q}$ seems to be interesting in its own right, as well as a useful way to gain more insight into $k(n)$.

References

[Brown 1992] K. Brown, "The period of Fibonacci sequences modulo m", *American Mathematical Monthly* **99**:3 (1992), 278. problem E3410.

[Coleman et al. 2006] D. A. Coleman, C. J. Dugan, R. A. McEwen, C. A. Reiter, and T. T. Tang, "Periods of (q, r)-Fibonacci sequences and elliptic curves", *Fibonacci Quart.* **44**:1 (2006), 59–70. MR 2006j:11019 Zbl 1133.11009

[Fulton and Morris 1969/1970] J. D. Fulton and W. L. Morris, "On arithmetical functions related to the Fibonacci numbers", *Acta Arith.* **16** (1969/1970), 105–110. MR 40 #4193

[Hardy and Wright 1954] G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, Oxford, at the Clarendon Press, 1954. 3rd ed. MR 16,673c Zbl 0058.03301

[Renault 1996] M. Renault, *Properties of the Fibonacci sequence under various moduli*, Master's thesis, Wake Forest University, 1996.

[Rosen 2000] K. H. Rosen, *Elementary number theory and its applications*, Fourth ed., Addison-Wesley, Reading, MA, 2000. MR 2000i:11001 Zbl 0964.11002

[Wall 1960] D. D. Wall, "Fibonacci series modulo m", *Amer. Math. Monthly* **67** (1960), 525–532. MR 22 #10945 Zbl 0101.03201

Received: 2008-08-22 Revised: Accepted: 2008-12-05

cguo@agnesscott.edu *Agnes Scott College, Department of Mathematics, 141 E. College Ave., Decatur, GA 30030, United States*

akoch@agnesscott.edu *Agnes Scott College, Department of Mathematics, 141 E. College Ave., Decatur, GA 30030, United States*