Fibonacci-like sequences and greatest common divisors

H.R.MORTON

Department of Pure Mathematics, University of Liverpool,
PO Box 147, Liverpool, L69 3BX, UK.

It is a curious feature of the Fibonacci sequence $\{f_n\}$ that the greatest common divisor (f_m, f_n) of two terms in the sequence is itself the k-th term in the sequence, with $k = (m, n)$. This result and its extension to sequences satisfying the recurrence relation

$$f_{n+1} = af_n + bf_{n-1},$$

starting with $f_0 = 0$, when a and b are any coprime integers, is proved by Lucas [L1], [L2]. The traditional proof, which is nicely presented in Hardy and Wright [HW 148-9], uses relations between the sequence $\{f_n\}$ and an auxiliary sequence, describing both sequences in terms of the roots of the quadratic $t^2 - at - b$. The purpose of this article is to present a proof which uses only simple congruence features of the sequence $\{f_n\}$. The result is stated below as theorem A. It is deduced readily from theorem B, which shows that the terms f_N in the sequence which are divisible by any fixed d are regularly spaced.

Theorem A. *Let $\{f_n\}$ be the sequence of integers determined by the initial conditions $f_0 = 0$, $f_1 = 1$ and the recurrence relation*

$$f_{n+1} = af_n + bf_{n-1},$$

where a and b are any two coprime integers. Then $(f_m, f_n) = \pm f_{(m,n)}$.

Remark. The choice of $f_1 = 1$ is not important; any other choice will just result in a multiple of the same sequence.

Theorem B. *Let $\{f_n\}$ be the sequence of integers defined in theorem A. Let d be a positive integer, and let S be the set of integers N for which f_N is divisible by d. Then S consists of all multiples of some integer k, depending on d and the sequence.*

In what follows we shall use standard congruence notation and algebra; thus $f_n \equiv 0 \bmod d$ means that f_n is divisible by d. The only property of gcd which is needed is that every common divisor of two numbers also divides their gcd. In the case of general coprime coefficients a and b we need the result that if d divides bc and is coprime to b then d divides c, or equivalently, in the context of congruences, that any number coprime to d has an inverse $\bmod d$. In the case $b = \pm 1$ the proofs use more elementary arguments, involving only addition and multiplication $\bmod d$.

To appear in Amer. Math. Monthly

Deduction of theorem A from theorem B: Let d be a positive integer and let $f_m \equiv 0 \bmod d$ and $f_n \equiv 0 \bmod d$.

Consider the set S of integers N for which $f_N \equiv 0 \bmod d$. By theorem B this set consists of all multiples of some k. Now $m, n \in S$, by hypothesis. Thus m and n are each divisible by k and hence also their gcd, (m,n), is divisible by k. The integer (m,n) thus belongs to S, which in turn means that $f_{(m,n)} \equiv 0 \bmod d$.

Now choose $d = (f_m, f_n)$. Then f_m and f_n are both divisible by d. The argument above shows that $f_{(m,n)}$ is also divisible by $d = (f_m, f_n)$.

Conversely, choose $d = f_{(m,n)}$ and again consider the set S of integers N for which $f_N \equiv 0 \bmod d$. Then S consists, by theorem B, of all multiples of some k. Clearly $(m,n) \in S$, since $f_{(m,n)}$ is divisible by d, and hence (m,n) is a multiple of k. Now m and n are multiples of (m,n), and hence are also multiples of k. So $m, n \in S$ and thus f_m and f_n are both divisible by d. It follows at once that their gcd, (f_m, f_n), is divisible by $d = f_{(m,n)}$.

We have already established that $f_{(m,n)}$ is divisible by (f_m, f_n). Thus $f_{(m,n)} = \pm(f_m, f_n)$, as claimed. □

It remains to establish theorem B. This is most simply done in the case $b = \pm 1$, when a can be any integer, by extending the sequence to include terms f_n for negative integers n also. The proof follows from two simple propositions; modifications of these needed to prove the general case are then given. Finally an alternative proof of theorem B is indicated, along lines suggested by the referee.

Proposition 1. *Let $\{f_n\}$ be a sequence of integers satisfying the recurrence relation $f_{n+1} = af_n + bf_{n-1}$, where a and b are integers. Suppose that $f_n \equiv 0 \bmod d$. Then for every $k \leq n$ the terms $f_{n\pm k}$ are related by*

$$f_{n+k} + (-b)^k f_{n-k} \equiv 0 \bmod d.$$

Proof: By induction on k. It is clearly true for $k = 0, 1$. Now

$$\begin{aligned} f_{n+k+1} + (-b)^{k+1} f_{n-k-1} &= af_{n+k} + bf_{n+k-1} + (-b)^k af_{n-k} + b(-b)^{k-1} f_{n-k+1} \\ &\equiv 0 \bmod d \end{aligned},$$

by the induction hypothesis. □

In general, proposition 1 shows that $f_{n+k} \equiv \pm b^k f_{n-k} \bmod d$ with $n \geq k$, assuming that $f_n \equiv 0 \bmod d$.

Suppose now that $b = \pm 1$. The relation can be read in the opposite direction as $f_{n-1} = -abf_n + bf_{n+1}$, since $b^{-1} = b$. Integers f_n satisfying the recurrence relation may then be defined for all negative integers n also. Proposition 1 holds for all k in this case, showing that $f_{n+k} \equiv \pm f_{n-k} \bmod d$ for all k, where $f_n \equiv 0 \bmod d$. Then $f_{n-k} \equiv 0 \bmod d$ if and only if $f_{n+k} \equiv 0 \bmod d$.

The set S of all integers N (positive and negative) for which $f_N \equiv 0 \bmod d$ is thus invariant under 'reflection' in any of its elements $n \in S$, where reflection in n interchanges the integers $n \pm k$.

Theorem B now follows from the geometrically obvious proposition 2.

Proposition 2. *Any set S of integers which contains 0 and is invariant under reflection in each element of S consists of all multiples of some fixed integer k.*

Proof: Either $S = \{0\}$ or we can take $k > 0$ as the least distance between any two elements of S, which we can write as n and $n+k$. Symmetry of S under reflection in $n+k$ shows that $n+2k \in S$. By induction on r, symmetry about $n+(r-1)k$ shows that $n+rk \in S$ for all positive integers r. Symmetry about n extends this to show that $n+rk \in S$ for all integers r. Because k is the least distance between any two integers in S there are no further elements of S. Given that $0 \in S$ we can then write $0 = n+rk$ for some r, so that n is a multiple of k, and hence S consists of the multiples of k. □

In the general case of coprime a and b proposition 2 holds, when restricted to positive integers n only. In this case the reflection invariance for the set S should be taken as saying that if $n \in S$ and $n \geq k$ then $n+k \in S$ if and only if $n-k \in S$. Proposition 1 shows that $f_{n+k} \equiv \pm b^k f_{n-k} \bmod d$ with $n \geq k$ when $f_n \equiv 0 \bmod d$. Hence the set S of integers $N \geq 0$ with $f_N \equiv 0 \bmod d$ does have the modified reflection invariance, *provided that b and d are coprime.* Theorem B then follows in the case that d is coprime to b.

In the remaining cases, when b and d have a common factor, $c > 1$ say, the recurrence relation gives $f_{n+1} \equiv af_n \bmod c$, and hence $f_n \equiv a^{n-1} \bmod c$. Now a and b are coprime, and hence a and c are coprime, so f_n is never divisible by c for any $n > 0$. The terms f_n with $n > 0$ are then never divisible by d; in these cases the set S consists only of 0, and again satisfies theorem B, taking $k = 0$.

Sketch of an alternative proof of theorem B: Observe that if $f_n \equiv 0 \bmod d$ then the sequence $f_n, f_{n+1}, \ldots, f_{n+k}, \ldots$ is a multiple of the sequence $f_0, f_1, \ldots, f_k, \ldots$ $\bmod d$. Explicitly, an easy induction on k, using the recurrence relation, shows that $f_{n+k} \equiv f_{n+1} f_k \bmod d$. After another induction to prove that f_n and f_{n+1} are coprime, and hence that f_{n+1} is coprime to d, it follows that when $n \in S$ then $k \in S$ if and only if $n+k \in S$. The set S thus has the property that if $m, n \in S$ with $m \geq n$ then $m \pm n \in S$. Theorem B follows readily.

Remarks. It is interesting to look explicitly at the sequences given by small choices of a and b, besides the Fibonacci sequence with $a = b = 1$, and the integers, with $a = 2, b = -1$.

It is shown above that the terms f_n with $n > 0$ are never divisible by any prime factor of b. On the other hand Lucas showed that each prime p which is coprime to b divides some term f_n in the sequence, with $n > 0$, and hence divides infinitely many terms.

Values of n for which f_n is divisible by p can be found as follows, although these are not always the smallest possible. Set $\Delta = a^2 + 4b$ and let p be any prime not dividing Δ or b. If Δ is a square $\bmod p$ then f_{p-1} is divisible by p, while if Δ is not a square $\bmod p$ then f_{p+1} is divisible by p. If p divides Δ then f_p is divisible by p. Explicit details of this and other divisibility properties of Lucas are reported in [D] and [HW].

Acknowledgments.

This proof was developed in 1993 as a result of conversations with Rob Baston, with whom I was sharing the teaching of an elementary course involving congruences and divisibility properties of integers. I am grateful to him and to Kit Nair and Alastair King for provoking me to complete this proof as a means of avoiding the more complicated induction proofs. I must thank the referee for suggestions which allowed me to extend my original presentation with $b = \pm 1$ to the general case, and for the outline of the alternative proof of theorem B.

References.

[D] L.E.Dickson, History of the Theory of Numbers, vol 1, 1919, (Chelsea reprint, New York 1971).

[L1] E.Lucas, Sur les rapports qui éxistent entre la théorie des nombres et le calcul intégral. Comptes Rendus, Paris 82 (1876), 1303-5.

[L2] E.Lucas, Sur la théorie des nombres premiers, Atti R. Accad Sc. Torino (Math), 11 (1875-6), 928-937

[HW] G.H.Hardy and E.M.Wright, Introduction to the Theory of Numbers. OUP, 1938.

H.R.Morton, Sept. 1994, revised Jan. 1995, April 1995.

Fibonacci-like sequences and greatest common divisors

H.R.Morton

Department of Pure Mathematics, University of Liverpool,
PO Box 147, Liverpool, L69 3BX, UK.

It is a curious feature of the Fibonacci sequence $\{f_n\}$ that the greatest common divisor (f_m, f_n) of two terms in the sequence is itself the k-th term in the sequence, with $k = (m, n)$. This result and its extension to sequences satisfying the recurrence relation

$$f_{n+1} = af_n + bf_{n-1},$$

starting with $f_0 = 0$, when a and b are any coprime integers, is proved by Lucas [L1], [L2]. The traditional proof, which is nicely presented in Hardy and Wright [HW 148-9], uses relations between the sequence $\{f_n\}$ and an auxiliary sequence, describing both sequences in terms of the roots of the quadratic $t^2 - at - b$. Alternative proofs generally use more or less elaborate induction methods. The purpose of this article is to present a proof which uses only simple congruence features of the sequence $\{f_n\}$. The result is stated below as theorem A. It is deduced readily from theorem B, which shows that the terms f_N in the sequence which are divisible by any fixed d are regularly spaced.

Theorem A. *Let $\{f_n\}$ be the sequence of integers determined by the initial conditions $f_0 = 0$, $f_1 = 1$ and the recurrence relation*

$$f_{n+1} = af_n + bf_{n-1},$$

where a and b are any two coprime integers. Then $(f_m, f_n) = \pm f_{(m,n)}$.

Remark. The choice of $f_1 = 1$ is not important; any other choice will just result in a multiple of the same sequence.

Theorem B. *Let $\{f_n\}$ be the sequence of integers defined in theorem A. Let d be a positive integer, and let S be the set of integers N for which f_N is divisible by d. Then S consists of all multiples of some integer k, depending on d and the sequence.*

In what follows we shall use standard congruence notation and algebra; thus $f_n \equiv 0 \bmod d$ means that f_n is divisible by d. The only property of gcd which is needed is that every common divisor of two numbers also divides their gcd. In the case of general coprime coefficients a and b we need the result that if d divides bc and is coprime to b then d divides c, or equivalently, in the context of congruences, that any number coprime to d has an inverse $\bmod d$. In the case $b = \pm 1$ the proofs use more elementary arguments, involving only addition and multiplication $\bmod d$.

To appear in Amer. Math. Monthly

Deduction of theorem A from theorem B: Let d be a positive integer and let $f_m \equiv 0 \bmod d$ and $f_n \equiv 0 \bmod d$.

Consider the set S of integers N for which $f_N \equiv 0 \bmod d$. By theorem B this set consists of all multiples of some k. Now $m, n \in S$, by hypothesis. Thus m and n are each divisible by k and hence also their gcd, (m,n), is divisible by k. The integer (m,n) thus belongs to S, which in turn means that $f_{(m,n)} \equiv 0 \bmod d$.

Now choose $d = (f_m, f_n)$. Then f_m and f_n are both divisible by d. The argument above shows that $f_{(m,n)}$ is also divisible by $d = (f_m, f_n)$.

Conversely, choose $d = f_{(m,n)}$ and again consider the set S of integers N for which $f_N \equiv 0 \bmod d$. Then S consists, by theorem B, of all multiples of some k. Clearly $(m,n) \in S$, since $f_{(m,n)}$ is divisible by d, and hence (m,n) is a multiple of k. Now m and n are multiples of (m,n), and hence are also multiples of k. So $m, n \in S$ and thus f_m and f_n are both divisible by d. It follows at once that their gcd, (f_m, f_n), is divisible by $d = f_{(m,n)}$.

We have already established that $f_{(m,n)}$ is divisible by (f_m, f_n). Thus $f_{(m,n)} = \pm(f_m, f_n)$, as claimed. □

It remains to establish theorem B. This is most simply done in the case $b = \pm 1$, when a can be any integer, by extending the sequence to include terms f_n for negative integers n also. The proof follows from two simple propositions; modifications of these needed to prove the general case are then given. Finally an alternative proof of theorem B is indicated, along lines suggested by the referee.

Proposition 1. *Let $\{f_n\}$ be a sequence of integers satisfying the recurrence relation $f_{n+1} = af_n + bf_{n-1}$, where a and b are integers. Suppose that $f_n \equiv 0 \bmod d$. Then for every $k \le n$ the terms $f_{n\pm k}$ are related by*

$$f_{n+k} + (-b)^k f_{n-k} \equiv 0 \bmod d.$$

Proof: By induction on k. It is clearly true for $k = 0, 1$. Now

$$\begin{aligned} f_{n+k+1} + (-b)^{k+1} f_{n-k-1} &= af_{n+k} + bf_{n+k-1} + (-b)^k af_{n-k} + b(-b)^{k-1} f_{n-k+1} \\ &\equiv 0 \bmod d \end{aligned},$$

by the induction hypothesis. □

In general, proposition 1 shows that $f_{n+k} \equiv \pm b^k f_{n-k} \bmod d$ with $n \ge k$, assuming that $f_n \equiv 0 \bmod d$.

Suppose now that $b = \pm 1$. The relation can be read in the opposite direction as $f_{n-1} = -abf_n + bf_{n+1}$, since $b^{-1} = b$. Integers f_n satisfying the recurrence relation may then be defined for all negative integers n also. Proposition 1 holds for all k in this case, showing that $f_{n+k} \equiv \pm f_{n-k} \bmod d$ for all k, where $f_n \equiv 0 \bmod d$. Then $f_{n-k} \equiv 0 \bmod d$ if and only if $f_{n+k} \equiv 0 \bmod d$.

The set S of all integers N (positive and negative) for which $f_N \equiv 0 \bmod d$ is thus invariant under 'reflection' in any of its elements $n \in S$, where reflection in n interchanges the integers $n \pm k$.

Theorem B now follows from the geometrically obvious proposition 2.

Proposition 2. *Any set S of integers which contains 0 and is invariant under reflection in each element of S consists of all multiples of some fixed integer k.*

Proof: Either $S = \{0\}$ or we can take $k > 0$ as the least distance between any two elements of S, which we can write as n and $n+k$. Symmetry of S under reflection in $n+k$ shows that $n+2k \in S$. By induction on r, symmetry about $n+(r-1)k$ shows that $n+rk \in S$ for all positive integers r. Symmetry about n extends this to show that $n+rk \in S$ for all integers r. Because k is the least distance between any two integers in S there are no further elements of S. Given that $0 \in S$ we can then write $0 = n+rk$ for some r, so that n is a multiple of k, and hence S consists of the multiples of k. □

In the general case of coprime a and b proposition 2 holds, when restricted to positive integers n only. In this case the reflection invariance for the set S should be taken as saying that if $n \in S$ and $n \geq k$ then $n+k \in S$ if and only if $n-k \in S$. Proposition 1 shows that $f_{n+k} \equiv \pm b^k f_{n-k} \bmod d$ with $n \geq k$ when $f_n \equiv 0 \bmod d$. Hence the set S of integers $N \geq 0$ with $f_N \equiv 0 \bmod d$ does have the modified reflection invariance, *provided that b and d are coprime.* Theorem B then follows in the case that d is coprime to b.

In the remaining cases, when b and d have a common factor, $c > 1$ say, the recurrence relation gives $f_{n+1} \equiv af_n \bmod c$, and hence $f_n \equiv a^{n-1} \bmod c$. Now a and b are coprime, and hence a and c are coprime, so f_n is never divisible by c for any $n > 0$. The terms f_n with $n > 0$ are then never divisible by d; in these cases the set S consists only of 0, and again satisfies theorem B, taking $k = 0$.

Alternative proof of theorem B: Observe that if $f_n \equiv 0 \bmod d$ then the sequence $f_n, f_{n+1}, \ldots, f_{n+k}, \ldots$ is a multiple of the sequence $f_0, f_1, \ldots, f_k, \ldots \bmod d$. Explicitly, an easy induction on k shows that $f_{n+k} \equiv f_{n+1} f_k \bmod d$. After another induction to prove that f_n and f_{n+1} are coprime, and hence that f_{n+1} is coprime to d, it follows that when $n \in S$ then $k \in S$ if and only if $n+k \in S$. The set S thus has the property that if $m, n \in S$ with $m \geq n$ then $m \pm n \in S$. Theorem B follows readily.

Remarks. It is interesting to look explicitly at the sequences given by small choices of a and b, besides the Fibonacci sequence with $a = b = 1$, and the integers, with $a = 2, b = -1$.

Lucas shows that each prime p which is coprime to b divides some term f_n in the sequence, with $n > 0$, and hence divides infinitely many terms. Values of n for which f_n is divisible by p can be found as follows, although these are not always the smallest possible. Set $\Delta = a^2 + 4b$ and let p be any prime not dividing Δ or b. If Δ is a square $\bmod p$ then f_{p-1} is divisible by p, while if Δ is not a square $\bmod p$ then f_{p+1} is divisible by p. If p divides Δ then f_p is divisible by p. Explicit details of this and other divisibility properties of Lucas are reported in [D] and [HW].

Acknowledgments.

This proof was developed in 1993 as a result of conversations with Rob Baston, with whom I was sharing the teaching of an elementary course involving congruences and divisibility properties of integers. I am grateful to him and to Kit Nair and Alastair King for provoking me to complete this proof as a means of avoiding the more complicated induction proofs. I must thank the referee for suggestions which allowed me to extend my original presentation with $b = \pm 1$ to the general case, and for the outline of the alternative proof of theorem B.

References.

[D] L.E.Dickson, History of the Theory of Numbers, vol 1, 1919, (Chelsea reprint, New York 1971).

[L1] E.Lucas, Sur les rapports qui éxistent entre la théorie des nombres et le calcul intégral. Comptes Rendus, Paris 82 (1876), 1303-5.

[L2] E.Lucas, Sur la théorie des nombres premiers, Atti R. Accad Sc. Torino (Math), 11 (1875-6), 928-937

[HW] G.H.Hardy and E.M.Wright, Introduction to the Theory of Numbers. OUP, 1938.

H.R.Morton, Sept. 1994, revised Jan. 1995