DIVISIBILITY SEQUENCES FROM STRONG DIVISIBILITY SEQUENCES

PETER BALA, Mar 2014

Let $\mathrm{S}(n)$ be a (non-vanishing) strong divisibility sequence. If p and q are relatively prime positive integers we show that the sequence $\mathrm{S}(pn)\mathrm{S}(qn)/\mathrm{S}(n)$ is a divisibility sequence. We give some examples of divisibility sequences of bivariate polynomials constructed by this method. Specializing these polynomials leads us to families of linear divisibility sequences over $\mathbb{Z}$, that is, integer divisibility sequences whose terms obey a linear recurrence equation having integer coefficients. The natural setting for defining a strong divisibility sequence is that of a GCD domain. We begin by recalling the basic theory of these domains.

1. GCD domains

An integral domain D (commutative ring with unity and no zero divisors) is a GCD domain if every pair a, b of nonzero elements has a greatest common divisor, denoted by $\gcd(a, b)$. The greatest common divisor satisfies the universal property that $\gcd(a, b)$ is a divisor of a and b and if d divides both a and b (written $d \mid a$ and $d \mid b$) then d divides $\gcd(a, b)$. The element $\gcd(a, b)$ is not unique but only determined up to a unit of D.

Every UFD is a GCD domain. So, for example, the ring of integers $\mathbb{Z}$ is a GCD domain as are the polynomial rings $\mathbb{Z}[x]$ and $\mathbb{Z}[x, y]$. We gather together the results we need concerning GCD domains in the form of a Lemma. See Woo [4] for the proof that every GCD domain is also a LCM domain.

Lemma 1.1 *Let D be a GCD domain.*

(i) $\gcd(ab, ac) = a\gcd(b, c) \qquad a, b, c \in D$

(ii) *The gcd is a multiplicative function; that is, if* $gcd(a_1, a_2) = 1$ *then*

$$gcd(a_1a_2, b) = gcd(a_1, b)gcd(a_2, b).$$

(iii) *D is a LCM domain; that is, every pair a, b of nonzero elements in D has a least common multiple, denoted by $lcm(a, b)$ (determined only up to a unit of D). There holds*

$$lcm(a, b)gcd(a, b) = ab$$

(iv) *If $a \mid a^{'}$ and $b \mid b^{'}$ in the domain D then $lcm(a, b) \mid lcm(a^{'}, b^{'})$ in D.* $\square$

Note, due to the ambiguity in the choice of the lcm and the gcd, the above equations are really equivalence relations whose lhs and rhs differ by a unit of the domain D. The same remark applies to other equations throughout the document involving the gcd or lcm functions.

2. Divisibility and strong divisibility sequences

A sequence $\{a(n)_{n\geq 1}\}$, where the terms $a(n)$ belongs to an integral domain, is called a divisibility sequence if $a(n)$ divides $a(nm)$ for all natural numbers n and m and $a(n) \neq 0$.

A sequence $\{a(n)\}_{n\geq 1}$ of elements of a GCD domain D is said to be strong divisibility sequence (SDS for short) if for all natural numbers n and m we have $\gcd(a(n), a(m)) = a(\gcd(n, m))$. Note the abuse of notation here: the gcd on the lhs of the equation refers to the domain D while the gcd on the rhs is taken in $\mathbb{Z}$. A strong divisibility sequence is also a divisibility sequence since for all natural numbers n and m we have $\gcd(a(n), a(nm)) = a(\gcd(n, nm)) = a(n)$. Thus $a(n) \mid a(nm)$.

Proposition 2.1 *Let $S(n)$ be a strong divisibility sequence of nonzero elements of a GCD domain D. Let p and q be relatively prime positive integers. Then the sequence $\{X(n)\}_{n\geq 1}$ defined by*

$$X(n) = \frac{S(pn)S(qn)}{S(n)}$$

is a divisibility sequence in D.

Proof

Since a strong divisibility sequence is also a divisibility sequence we have $\mathrm{S}(n) \mid \mathrm{S}(pn)$ in D for all natural numbers n. Hence $\mathrm{X}(n)$ belongs to D for every n. We need to show that $\mathrm{X}(n) \mid \mathrm{X}(nm)$ in D for all natural numbers n and m.

Now by the assumption on S we have

$$\gcd(\mathrm{S}(pn), \mathrm{S}(qn)) = \mathrm{S}(\gcd(pn, qn)) = \mathrm{S}(n).$$

It follows that

$$\begin{aligned} \mathrm{X}(n) &= \frac{\mathrm{S}(pn)\mathrm{S}(qn)}{\mathrm{S}(n)} \\ &= \frac{\mathrm{S}(pn)\mathrm{S}(qn)}{\gcd(\mathrm{S}(pn), \mathrm{S}(qn))} \\ &= \mathrm{lcm}(\mathrm{S}(pn), \mathrm{S}(qn)) \end{aligned}$$

by Lemma 1.1 (iii). Therefore

$$\frac{\mathrm{X}(nm)}{\mathrm{X}(n)} = \frac{\mathrm{lcm}(\mathrm{S}(pnm), \mathrm{S}(qnm))}{\mathrm{lcm}(\mathrm{S}(pn), \mathrm{S}(qn))},$$

which belongs to the domain D by Lemma 1.1 (iv), since $\mathrm{S}(pn) \mid \mathrm{S}(pnm)$ and $\mathrm{S}(qn) \mid \mathrm{S}(qnm)$ in D. Thus $\mathrm{X}(n) \mid \mathrm{X}(nm)$ in D for all natural numbers n and m. □

Example 2.1 The sequence of Fibonacci numbers $\mathrm{F}(n)$ is a SDS. Therefore, for each pair of coprime positive integers p and q, the sequence $\mathrm{F}(pn)\mathrm{F}(qn)/\mathrm{F}(n)$ is an integer divisibility sequence.

Example 2.2 The sequence of Mersenne numbers $2^n - 1$ is a SDS. Therefore, for fixed odd q, the sequence $(2^n + 1)(2^{qn} - 1)$ is an integer divisibility sequence.

In order to apply Proposition 2.1 to produce divisibility sequences we need a supply of strong divisibility sequences.

Proposition 2.2 *Let D be a GCD domain. Let a and b be relatively prime elements in $D-\{0\}$, that is, $gcd(a,b)=1$. The sequence $S(n)$ defined by the second-order linear recurrence*

$$S(n) = aS(n-1) + bS(n-2), \qquad [S(0)=0, S(1)=1]$$

is a strong divisibility sequence, that is,

$$gcd(S(n), S(m)) = S(gcd(n,m))$$

for all natural numbers n and m.

Lucas [2] gave a proof of this result when the domain D $= \mathbb{Z}$. Norfleet [3, Theorem 3] proved the result for the domain D $= \mathbb{Z}[x]$. If we examine Norfleet's proof we see that it only uses the fact that the domain $\mathbb{Z}[x]$ is a GCD domain and so his proof can be immediately extended to prove Propostion 2.2. We present a modified version of Norfleet's proof in the Appendix.

3. Divisibility sequences of polynomials

In this section we apply the results of Section 2 to the particular GCD domain $\mathbb{Z}[x,y]$ to produce examples of divisibility sequences of bivariate polynomials.

Proposition 3.1

(i) The sequence of homogeneous bivariate polynomials $U(n) \equiv U(n,x,y)$ defined by

$$U(n,x,y) = \frac{x^n - y^n}{x-y} \tag{1}$$

is a strong divisibility sequence of polynomials in the domain $\mathbb{Z}[x,y]$.

(ii) The sequence of homogeneous bivariate polynomials $L(n) \equiv L(n,x,y)$ defined by

$$L(n,x,y) = \begin{cases} \frac{x^n-y^n}{x-y} & n \text{ odd} \\ \\ \frac{x^n-y^n}{x^2-y^2} & n \text{ even} \end{cases} \tag{2}$$

is a strong divisibility sequence of polynomials in the domain $\mathbb{Z}[x,y]$.

Proof

(i) This well-known result is an immediate consequence of Proposition 2.2 since one easily verifies that U(n) satisfies the second-order linear recurrence

$$\mathrm{U}(n+1) = (x+y)\mathrm{U}(n) - xy\mathrm{U}(n-1)$$

with U(0) = 0, U(1) = 1.

(ii) The sequence of polynomials L(n) satisfies the fourth-order linear recurrence

$$\mathrm{L}(n) = (x^2+y^2)\mathrm{L}(n-2) - (xy)^2\mathrm{L}(n-4)$$

with initial conditions $\mathrm{L}(0) = 0,\ \mathrm{L}(1) = 1,\ \mathrm{L}(2) = 1$ and $\mathrm{L}(3) = x^2 + xy + y^2$, so we can't apply Proposition 2.2. However, we clearly have $\mathrm{L}(n) = \mathrm{U}(n)$ when n is odd and $(x+y)\mathrm{L}(n) = \mathrm{U}(n)$ when n is even. The strong divisibility property $\gcd(\mathrm{L}(n), \mathrm{L}(m)) = \mathrm{L}(\gcd(n, m))$ of the sequence $\mathrm{L}(n)$ will follow from part (i) of the Proposition. We need to examine various cases.

Firstly, consider the case where both n, m are odd. Then

$$\begin{aligned}\gcd(\mathrm{L}(n), \mathrm{L}(m)) &= \gcd(\mathrm{U}(n), \mathrm{U}(m)) \\ &= \mathrm{U}(\gcd(n, m)) \qquad \text{by part (i)} \\ &= \mathrm{L}(\gcd(n, m))\end{aligned}$$

since $\gcd(n, m)$ is odd.

Secondly, suppose both n, m are even. We have

$$\begin{aligned}(x+y)\gcd(\mathrm{L}(n), \mathrm{L}(m)) &= \gcd((x+y)\mathrm{L}(n), (x+y)\mathrm{L}(m)) \\ &= \gcd(\mathrm{U}(n), \mathrm{U}(m)) \\ &= \mathrm{U}(\gcd(n, m)).\end{aligned}$$

Therefore

$$\begin{aligned}\gcd(\mathrm{L}(n), \mathrm{L}(m)) &= \frac{\mathrm{U}(\gcd(n, m))}{x+y} \\ &= \mathrm{L}(\gcd(n, m))\end{aligned}$$

since $\gcd(n, m)$ is even.

Finally, consider the case where n, m are of different parity, say, n odd and m even. We have

$$\begin{aligned}\gcd(\mathrm{L}(n), (x+y)\mathrm{L}(m)) &= \gcd(\mathrm{U}(n), \mathrm{U}(m)) \\ &= \mathrm{U}(\gcd(n, m)) \\ &= \mathrm{L}(\gcd(n, m)) \qquad (3)\end{aligned}$$

since $\gcd(n, m)$ is odd.

Now it is easy to see that $x + y$ is coprime to $\mathrm{L}(n) = (x^n - y^n)/(x - y)$ since n is odd, and also coprime to $\mathrm{L}(m) = (x^m - y^m)/(x^2 - y^2)$ since m is even . Therefore, since gcd is a multiplicative function (Lemma 1 (ii)), we have

$$\begin{aligned}\gcd(\mathrm{L}(n), (x+y)\mathrm{L}(m)) &= \gcd(\mathrm{L}(n), x+y)\gcd(\mathrm{L}(n), \mathrm{L}(m)) \\ &= \gcd(\mathrm{L}(n), \mathrm{L}(m)). \qquad (4)\end{aligned}$$

Comparing (3) and (4) we see that for this case we again have $\gcd(\mathrm{L}(n), \mathrm{L}(m)) = \mathrm{L}(\gcd(n, m))$ and the proof that $\mathrm{L}(n)$ is a strong divisibility sequence is complete. □

Applying Proposition 2.1 to the strong divisibility sequences $\mathrm{U}(n)$ and $\mathrm{L}(n)$ from Proposition 3.1 yields the following result.

Proposition 3.2 *Let p, q be a pair of coprime positive integers. The pair of sequences of homogeneous polynomials $A(n) \equiv A(n,x,y)$ and $B(n) \equiv B\ (n,x,y)$ in $\mathbb{Z}[x,y]$ defined by*

$$\begin{aligned} A(n) &= \frac{U(pn)\,U(qn)}{U(n)} \\ &= \frac{(x^{pn}-y^{pn})(x^{qn}-y^{qn})}{(x^n-y^n)(x-y)} \end{aligned} \tag{5}$$

and

$$B(n) = \frac{L(pn,x,y)L(qn,x,y)}{L(n,x,y)} \tag{6}$$

are divisibility sequences of polynomials in $\mathbb{Z}[x,y]$. $\square$

By calculating the ordinary generating function (ogf) of the sequence $\mathrm{A}(n)$ (resp. $\mathrm{B}(n)$) it can be shown that $\mathrm{A}(n)$ (resp. $\mathrm{B}(n)$) satisfies a linear recurrence of order $2\min(p,q)$ (resp. $4\min(p,q)$). The following example illustrates this point.

Example 3.1 Take $p = 2$ and $q = 3$. Find the ogf of the normalized sequence $\mathrm{A}(n)/\mathrm{A}(1)$. We have from (5)

$$\begin{aligned} \frac{\mathrm{A}(n)}{\mathrm{A}(1)} &= \frac{(x-y)(x^{2n}-y^{2n})(x^{3n}-y^{3n})}{(x^n-y^n)(x^2-y^2)(x^3-y^3)} \\ &= \frac{(x^n+y^n)(x^{3n}-y^{3n})}{(x+y)(x^3-y^3)} \\ &= c(x,y)((x^4)^n+(x^3y)^n-(xy^3)^n-(y^4)^n), \end{aligned} \tag{7}$$

where

$$c(x,y) = \frac{1}{(x+y)(x^3-y^3)}\,.$$

It follows from (7) that the ogf

$$\sum_{n\geq 1} \frac{\mathrm{A}(n)}{\mathrm{A}(1)} z^n,$$

of the normalized sequence $\mathrm{A}(n)/\mathrm{A}(1)$ is a sum of four geometric series, and so will be a rational function of the form $z\mathrm{N}(z)/\mathrm{D}(z)$ for polynomials $\mathrm{N}(z)$ and $\mathrm{D}(z)$. A short calculation yields

$$N(z) = 1 - 2xy(x^2-xy+y^2) + (xy)^4z^2$$

$$D(z) = (1-x^4z)(1-x^3yz)(1-xy^3z)(1-y^4z).$$

From the form of the denominator polynomial $\mathrm{D}(z)$ we see that the normalized sequence $\mathrm{A}(n)/\mathrm{A}(1)$, and hence also the sequence $\mathrm{A}(n)$, satisfies a linear recurrence of order 4 ($= 2\min(p,q)$), whose coefficients are polynomials in $\mathbb{Z}[x,y]$.

4. Integer divisibility sequences

Clearly, we can obtain integer linear divisibility sequences from the polynomials $\mathrm{A}(n,x,y)$ in (5) and $\mathrm{B}(n,x,y)$ in (6) simply by specializing x and y to be distinct integers. In fact, we can relax the requirement that x and y be integers and still get integer sequences. This is because of the symmetries satisfied by the polynomials $\mathrm{A}(n,x,y)$ and $\mathrm{B}(n,x,y)$. Recall the following simple consequences of the fundamental theorem of symmetric polynomials:

Any symmetric polynomial P(x,y) in $\mathbb{Z}[x,y]$ can be expressed as a polynomial with integer coefficients in the elementary symmetric polynomials $x+y$ and xy. If the symmetric polynomial $\mathrm{P}(x,y)$ is also invariant under change of sign of the variables x and y, that is, $\mathrm{P}(x,y)=\mathrm{P}(-x,-y)$, then $\mathrm{P}(x,y)$ can be expressed as a polynomial with integer coefficients in the elementary symmetric polynomials $(x+y)^2$ and xy.

A) Firstly, we consider integer divisibility sequences obtained by specializing the polynomials $\mathrm{B}(n,x,y)$. Observe from (2) that for each n, $\mathrm{L}(n,x,y)$ is a symmetric polynomial that is also invariant under change of sign of the variables x and y

$$\mathrm{L}(n,x,y)=\mathrm{L}(n,y,x)=\mathrm{L}(n,-x-y).$$

Clearly, the same symmetries also hold for the polynomials $\mathrm{B}(n,x,y)$ in (6) and for the polynomials $\mathrm{B}(nm,x,y)/\mathrm{B}(n,x,y)$ for all natural numbers n,m. Therefore, by the above remark, these polynomials can be written as a polynomials with integer coefficients in the symmetric functions$(x+y)^2$ and xy. Thus in order for $\mathrm{B}(n,x,y)$ to be an integer divisibility sequence it suffices to choose values for x and y so that both $(x+y)^2$ and xy are integers.

To this end, let P and Q be nonzero integers and define complex numbers α and β by

$$\begin{aligned}(\alpha+\beta)^2 &= \mathrm{P}\\ \alpha\beta &= \mathrm{Q}\end{aligned}\tag{8}$$

so that α and β are the roots of the quadratic equation $x^2-\sqrt{\mathrm{P}}x+\mathrm{Q}=0$. We also assume that α/β is not equal to a root of unity. Then we conclude that

$$\mathrm{B}(n,\alpha,\beta)=\frac{\mathrm{L}(pn,\alpha,\beta)\mathrm{L}(qn,\alpha,\beta)}{\mathrm{L}(n,\alpha,\beta)}$$

is a well-defined linear divisibility sequence of integers of order $4\min(p,q)$. The particular case $p=q=1$ gives the Lehmer numbers $\mathrm{L}(n,\alpha,\beta)$ [1].

B) Next, we consider integer divisibility sequences obtained by specializing the polynomials $\mathrm{A}(n,x,y)$. There are two cases to consider according as to whether $p+q$ is odd or $p+q$ is even.

(i) Suppose first that $p+q$ is odd.

Observe that in this case the polynomial $\mathrm{A}(n,x,y)$ given by (5), and the polynomials $\mathrm{A}(nm,x,y)/\mathrm{A}(n,x,y)$ for $n,m\in\mathbb{N}$, in addition to being symmetric in x and y, are also invariant under change of sign of the variables x and y since

$$\mathrm{A}(n,-x,-y)=(-1)^{n(p+q+1)}\mathrm{A}(n,x,y)=\mathrm{A}(n,x,y).$$

Therefore, by the above remark, $\mathrm{A}(n,x,y)$ can be written as a polynomial with integer coefficients in the symmetric polynomials $(x+y)^2$ and xy. The same is true for the polynomial $\mathrm{A}(nm,x,y)/\mathrm{A}(n,x,y)$ for all natural numbers n,m. Thus $\mathrm{A}(n,x,y)$ will be an integer divisibility sequence if x and y are chosen so that both $(x+y)^2$ and xy are integers. Accordingly, let P and Q be nonzero integers and define complex numbers α and β by (8). We again require that α/β is not equal to a root of unity. Then

$$\mathrm{A}(n,\alpha,\beta)=\frac{(\alpha^{pn}-\beta^{pn})(\alpha^{qn}-\beta^{qn})}{(\alpha^n-\beta^n)}$$

is a well-defined integer linear divisibility sequence of order $2\min(p,q)$. Of course, the same holds true for the normalized sequence

$$\frac{\mathrm{A}(n,\alpha,\beta)}{\mathrm{A}(1,\alpha,\beta)}=\frac{(\alpha-\beta)(\alpha^{pn}-\beta^{pn})(\alpha^{qn}-\beta^{qn})}{(\alpha^n-\beta^n)(\alpha^p-\beta^p)(\alpha^q-\beta^q)}.$$

Example 4.1 Let $p=3$ and $q=4$; take $\mathrm{P}=5$ and $\mathrm{Q}=1$.
The roots α,β of the quadratic equation $x^2-\sqrt{5}x+1=0$ are given by

$$\alpha=\frac{1+\sqrt{5}}{2},\quad \beta=\frac{\sqrt{5}-1}{2}.$$

For convenience we work with the normalized sequence

$$\begin{aligned}\frac{\mathrm{A}(n,\alpha,\beta)}{\mathrm{A}(1,\alpha,\beta)} &= \frac{(\alpha-\beta)(\alpha^{3n}-\beta^{3n})(\alpha^{4n}-\beta^{4n})}{(\alpha^n-\beta^n)(\alpha^3-\beta^3)(\alpha^4-\beta^4)}\\ &= \frac{\alpha^{6n}+\alpha^{4n}+\alpha^{2n}-\beta^{6n}-\beta^{4n}-\beta^{2n}}{12\sqrt{5}}.\end{aligned}$$

The sequence begins $[1,14,228,3948,69905,1248072,22352707,400808856,...]$. The sequence satisfies a linear recurrence of order $2\min\{p,q\}=6$, as shown by calculating the ogf

$$\sum_{n\geq 1}\frac{\mathrm{A}(n,\alpha,\beta)}{\mathrm{A}(1,\alpha,\beta)}z^n=\frac{z(1-14z+40z-14z^3+z^4)}{(1-3z+z^2)(1-7z+z^2)(1-18z+z^2)}.\square$$

(ii) Suppose now that $p+q$ is even.
In this case, the polynomials $\mathrm{A}(n,x,y)$ given by (5), and the polynomials $\mathrm{A}(nm,x,y)/\mathrm{A}(n,x,y)$ for $n,m\in\mathbb{N}$, are symmetric in x and y (but not invariant under change of sign of the variables) and so can be written as polynomials with integer coefficients in the elementary symmetric functions $x+y$ and xy. Thus in order for $\mathrm{A}(n,x,y)$ to be an integer divisibility sequence it suffices to choose values for x and y so that both $x+y$ and xy are integers. Accordingly, let P and Q be nonzero integers and now define complex numbers α and β by

$$\begin{aligned}\alpha+\beta &= \mathrm{P}\\ \alpha\beta &= \mathrm{Q}\end{aligned}$$

so that α and β are the roots of the quadratic equation $x^2 - Px + Q = 0$. We also require that α/β is not equal to a root of unity.. Then for each n

$$\mathrm{A}(n, \alpha, \beta) = \frac{(\alpha^{pn} - \beta^{pn})(\alpha^{qn} - \beta^{qn})}{\alpha^n - \beta^n}$$

is a well-defined integer and forms the terms of an integer divisibility sequence. In the particular case $p = q = 1$, the normalized sequence $\mathrm{A}(n, \alpha, \beta)/\mathrm{A}(1, \alpha, \beta)$ becomes the Lucas sequence $(\alpha^n - \beta^n)/(\alpha - \beta)$ [2].

Example 4.2 Let $p = 3$ and $q = 5$; take $\mathrm{P} = 1$ and $\mathrm{Q} = -1$.
The roots α, β of the quadratic equation $x^2 - x - 1 = 0$ are given by

$$\alpha = \frac{1 + \sqrt{5}}{2}, \quad \beta = \frac{1 - \sqrt{5}}{2}.$$

The normalized sequence

$$\begin{aligned} \frac{\mathrm{A}(n, \alpha, \beta)}{\mathrm{A}(1, \alpha, \beta)} &= \frac{(\alpha - \beta)(\alpha^{3n} - \beta^{3n})(\alpha^{5n} - \beta^{5n})}{(\alpha^n - \beta^n)(\alpha^3 - \beta^3)(\alpha^5 - \beta^5)} \\ &= \frac{\alpha^{7n} + (-\alpha)^{5n} + \alpha^{3n} - \beta^{7n} - (-\beta)^{5n} - \beta^{3n}}{10\sqrt{5}} \end{aligned}$$

begins $[1, 44, 1037, 32472, 915305, 26874892, 776952553, 22595381424, ...]$ (see A238601). The sequence satisfies a linear recurrence of order $2\min\{p, q\} = 6$, as shown by calculating the ogf

$$\sum_{n \geq 1} \frac{\mathrm{A}(n, \alpha, \beta)}{\mathrm{A}(1, \alpha, \beta)} z^n = \frac{z(1 + 22z - 181z^2 - 22z^3 + z^4)}{(1 - 4z - z^2)(1 + 11z - z^2)(1 - 29z - z^2)}.$$

Appendix

We give a proof of Proposition 2.2 following Norfleet [3, Theorem 3].

Proposition 2.2 *Let D be a GCD domain. Let a and b be relatively prime elements in D−{0}, that is, gcd(a, b) = 1. The sequence S(n) defined by the second-order linear recurrence*

$$S(n+1) = aS(n) + bS(n-1), \qquad [S(0) = 1, S(1) = 1]$$

is a strong divisibility sequence, that is,

$$gcd(S(n), S(m)) = S(gcd(n, m)) \tag{9}$$

for all natural numbers n and m.

We shall make use of the following simple properties of the gcd function in the domain D:

$$\text{if } \gcd(a, b) = 1 \text{ then } \gcd(a, bc) = \gcd(a, c) \tag{10}$$

$$\text{if } a = cb + r \text{ then } \gcd(a, b) = \gcd(b, r). \tag{11}$$

We will need two preliminary results about the sequence $S(n)$.

Proposition A2 For $n \geq 1$ we have

(i)

$$\gcd(S(n), b) = 1 \tag{12}$$

(ii)

$$\gcd(S(n+1), S(n)) = 1. \tag{13}$$

Proof

(i) By induction. Clearly, $\gcd(S(1), b) = 1$ and

$$\begin{aligned} \gcd(S(n+1), b) &= \gcd(aS(n) + bS(n-1), b) \\ &= \gcd(aS(n), b) \quad \text{by (11)} \\ &= \gcd(S(n), b) \quad \text{by (10)} \end{aligned}$$

and the induction goes through.

(ii) By induction. Clearly, $\gcd(S(2), S(1)) = 1$ and

$$\begin{aligned} \gcd(S(n+1), S(n)) &= \gcd(aS(n) + bS(n-1), S(n)) \\ &= \gcd(bS(n-1), S(n)) \quad \text{by (11)} \\ &= \gcd(S(n-1), S(n)) \quad \text{by (10) and part (i)}, \end{aligned}$$

and the induction goes through. □

Proposition A3 For $k = 1, 2, 3, \ldots$ we have

$$S(n+k) = S(k+1)S(n) + bS(k)S(n-1). \tag{14}$$

Proof We use strong induction on k. The case $k = 1$ is simply the defining recurrence equation for the sequence $S(n)$. Assume (14) holds true up to k then

$$\begin{aligned} S(n+k+1) &= aS(n+k) + bS(n+k-1) \\ &= a(S(k+1)S(n) + bS(k)S(n-1)) + b(S(k)S(n) + bS(k-1)S(n-1)) \\ &= S(k+2)S(n) + bS(k+1)S(n-1) \end{aligned}$$

and the induction goes through. □

Proof of Proposition 2.2

We need to establish the strong divisibility property

$$\gcd(S(n), S(m)) = S(\gcd(n, m)) \tag{15}$$

for all natural numbers n, m. We can assume without loss of generality that $n \geq m$. Let $k = n - m$. We begin by establishing the result

$$\gcd(S(n), S(m)) = \gcd(S(n-m), S(m)). \tag{16}$$

This holds because

$$\begin{aligned}
\gcd(S(n), S(m)) &= \gcd(S(m+k), S(m)) \\
&= \gcd(S(k+1)S(m) + bS(k)S(m-1), S(m)) \quad \text{by (14)} \\
&= \gcd(bS(k)S(m-1), S(m)) \quad \text{by (11)} \\
&= \gcd(S(k)S(m-1), S(m)) \quad \text{by (10) and (12)} \\
&= \gcd(S(k), S(m)) \quad \text{by (10) and (13)} \\
&= \gcd(S(n-m), S(m)).
\end{aligned}$$

We are now ready to prove (15) by means of a strong induction argument on $n+m$. Clearly, (15) is true for the base case $n = m = 1$. We make the inductive hypothesis that (15) is true for all n, m with $n + m \leq N$. Then if $n + m = N + 1$

$$\begin{aligned}
\gcd(S(n), S(m)) &= \gcd(S(n-m), S(m)) \text{ by (16)} \\
&= S(\gcd(n-m, m)) \quad \text{by the inductive hypothesis} \\
&= S(\gcd(n, m))
\end{aligned}$$

and hence the induction goes through. □

Example A1 Define a sequence $U(n)_{n\geq 1}$ in the ring of Gaussian integers $\mathbb{Z}[i]$ by the recurrence $U(n) = (1+i)U(n-1) + U(n-2)$ with $U(0) = 0$ and $U(1) = 1$. By Proposition 2.2 this will be a strong divisibility sequence in the GCD domain $\mathbb{Z}[i]$.

The sequence begins $[1, 1+i, 1+2i, 4i, -3+6i, -9+7i, -19+4i, -32-8i, ...]$. It is not difficult to check that the sequence $|U(n)|^2$ beginning $[1, 2, 5, 16, 45, 130, 377, 1088, ...]$ is a divisibility sequence of integers obeying a fourth-order linear recurrence. It is A138573 in the database.

REFERENCES

[1] D. H. Lehmer, An extended theory of Lucas' Functions, Annals of Mathematics Second Series, Vol. 31, No. 3 (July 1930), 419-448.

[2] E. Lucas, Théorie des Fonctions Numériques Simplement Périodiques.

[3] M. Norfleet, Characterization of second-order strong divisibility sequences of polynomials, The Fibonacci Quarterly, Vol. 43, No. 2 (May 2005), 166-169.

[4] C. Woo, An integral domain is lcm iff it is gcd.