Fibonacci sequences

Jonathan L.F. King
squash@ufl.edu
Webpage http://squash.1gainesville.com/
12 May, 2024 (at *12:09*)

See also *Problems/Algebra/LinearAlg/linear-recurr.latex*

GCD. We'll sometimes use a red under-bracket for *greatest common divisor*, e.g, $\underline{n,m} := \text{GCD}(n,m)$.

Prolegomenon. The famous ***Fibonacci sequence*** $\vec{f} := (\mathsf{f}_n)_{n=-\infty}^{\infty}$ is defined by $\mathsf{f}_0 := 0$, $\mathsf{f}_1 := 1$ and

1a: $$\mathsf{f}_{n+1} = \mathsf{f}_n + \mathsf{f}_{n-1},$$

producing this doubly-∞ sequence:

n ...	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7	8	9	10 ...
f_n ...	5	-3	2	-1	1	0	1	1	2	3	5	8	13	21	34	55 ...

Let $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ be the positive and negative roots of the ***characteristic polynomial*** of $\vec{f}$, which is

$$\text{Fib}(x) := x^2 - x - 1 \overset{\text{note}}{=\!=} [x-\boldsymbol{\alpha}][x-\boldsymbol{\beta}].$$ *So*

1b: $$\boldsymbol{\alpha}+\boldsymbol{\beta} = 1 \quad \textit{and} \quad \boldsymbol{\alpha}\cdot\boldsymbol{\beta} = -1.$$ *Moreover*

$$\boldsymbol{\alpha}^2 = \boldsymbol{\alpha}+1,\ \boldsymbol{\beta}^2 = \boldsymbol{\beta}+1 \textit{ and } \boldsymbol{\alpha},\boldsymbol{\beta} = \tfrac{1}{2}[1 \pm \sqrt{5}].$$

For future reference,

1c: $$\boldsymbol{\alpha} > 1 > |\boldsymbol{\beta}|.$$

Binet Formula. Let $\varphi := \sqrt{5}$. [Mnemonic "phi" to evoke "five".] Our $\vec{f}$ is some linear combination $A\cdot[n \mapsto \boldsymbol{\alpha}^n] + B\cdot[n \mapsto \boldsymbol{\beta}^n]$. Easily, $-B = A = \frac{1}{\varphi}$, so

2: $$\forall n \in \mathbb{Z}: \quad \mathsf{f}_n = \frac{1}{\varphi}\cdot[\boldsymbol{\alpha}^n - \boldsymbol{\beta}^n],$$

since this formula gives correct values for f_0 and f_1.

2a: Lemma. *Courtesy Binet:*

†: $$\forall n \in \mathbb{Z}: \quad \boldsymbol{\alpha}^n = \mathsf{f}_n\boldsymbol{\alpha} + \mathsf{f}_{n-1}.$$ *Also,*

‡: $$5\boldsymbol{\alpha}^2 = [\boldsymbol{\alpha}+2]^2.$$

Each of these holds with $\boldsymbol{\alpha}$ replaced by $\boldsymbol{\beta}$. ♢

Pf of (†). We prove (†) for n positive. The base case is $\boldsymbol{\alpha}^1 = 1\cdot\boldsymbol{\alpha} + 0 = \mathsf{f}_1\cdot\boldsymbol{\alpha} + \mathsf{f}_0$. Inductively

$$\begin{aligned} \boldsymbol{\alpha}^{n+1} = \boldsymbol{\alpha}\cdot[\mathsf{f}_n\boldsymbol{\alpha} + \mathsf{f}_{n-1}] &= \mathsf{f}_n\boldsymbol{\alpha}^2 + \mathsf{f}_{n-1}\boldsymbol{\alpha} \\ &= \mathsf{f}_n[\boldsymbol{\alpha}+1] + \mathsf{f}_{n-1}\boldsymbol{\alpha} \\ &= [\mathsf{f}_n + \mathsf{f}_{n-1}]\boldsymbol{\alpha} + \mathsf{f}_n \end{aligned}$$

which equals $\mathsf{f}_{n+1}\boldsymbol{\alpha} + \mathsf{f}_n$, as desired. ♦

Pf (‡). Squaring, $[\boldsymbol{\alpha}+2]^2 = \boldsymbol{\alpha}^2 + 4[\boldsymbol{\alpha}+1] = \boldsymbol{\alpha}^2 + 4\boldsymbol{\alpha}^2$. ♦

Recurrence doubling

A fibonacci-like sequence $\vec{\mathbf{z}} := (z_n)_{n=0}^{\infty}$ is defined via (possibly complex) numbers $\mathcal{P}$ and $\mathcal{S}$, by

3.1: $$z_{n+2} := \mathcal{S}z_{n+1} - \mathcal{P}z_n\,,$$

and some initial condition (z_1, z_0). With

3.2: $$\mathsf{G} := \begin{bmatrix} \mathcal{S} & -\mathcal{P} \\ 1 & 0 \end{bmatrix}, \quad \text{then } \begin{bmatrix} z_{n+1} \\ z_n \end{bmatrix} = \mathsf{G}^n \cdot \begin{bmatrix} z_1 \\ z_0 \end{bmatrix},$$

for each integer n.

A number $r{\neq}0$ engenders seq $n \mapsto r^n$. It satisfies recurrence (3.1) IFF r is a root of polynomial

$$f(x) := x^2 - \mathcal{S}x + \mathcal{P} \overset{\text{factored}}{=\!=} [x-\boldsymbol{\mu}][x-\boldsymbol{\nu}]\,.$$

Equating coeffs in the polynomial gives:

3.3: $$\boldsymbol{\mu} + \boldsymbol{\nu} = \mathcal{S}\,. \qquad \text{(Sum)}$$
$$\boldsymbol{\mu} \cdot \boldsymbol{\nu} = \mathcal{P}\,. \qquad \text{(Product)}$$

3.4: $$\boldsymbol{\mu}^2 = \mathcal{S}\boldsymbol{\mu} - \mathcal{P} \quad \text{and} \quad \boldsymbol{\nu}^2 = \mathcal{S}\boldsymbol{\nu} - \mathcal{P}\,.$$

Henceforth, we require $\boldsymbol{\mu} \neq \boldsymbol{\nu}$, i.e $\mathcal{S}^2 \neq 4\mathcal{P}$; this, since $\text{Discr}(f) \overset{\text{note}}{=\!=} \mathcal{S}^2 - 4\mathcal{P}$. *We want $\boldsymbol{\mu} \neq \boldsymbol{\nu}$ so that every seq satisfying (3.1) has its n^{th}-term equal a linear combination of $\boldsymbol{\mu}^n$ and $\boldsymbol{\nu}^n$.*

Doubling. Sequences $(z_e)_{e\text{ even}}$ and $(z_d)_{d\text{ odd}}$ will satisfy *some* two-term linear recurrence. [The same recurrence.] We seek numbers $\widehat{\mathcal{S}}$ and $\widehat{\mathcal{P}}$ such that for r equaling either $\boldsymbol{\mu}^2$ or $\boldsymbol{\nu}^2$,

$$r^2 = \widehat{\mathcal{S}}r^1 - \widehat{\mathcal{P}}r^0\,.$$

I.e, that polynomial

$$x^2 - \widehat{\mathcal{S}}x + \widehat{\mathcal{P}} \overset{\text{factors}}{=\!=} [x - \boldsymbol{\mu}^2]\cdot[x - \boldsymbol{\nu}^2]\,.$$

Squaring eqn $\boldsymbol{\mu}^2 = \mathcal{S}\boldsymbol{\mu} - \mathcal{P}$ gives

$$\boldsymbol{\mu}^4 = \mathcal{S}^2\boldsymbol{\mu}^2 - 2\mathcal{P}\mathcal{S}\boldsymbol{\mu} + \mathcal{P}^2.$$

As $\mathcal{S}\boldsymbol{\mu} = \boldsymbol{\mu}^2 + \mathcal{P}$, so $2\mathcal{P}\mathcal{S}\boldsymbol{\mu} = 2\mathcal{P}\boldsymbol{\mu}^2 + 2\mathcal{P}^2$. Thus

$$\boldsymbol{\mu}^4 = \overbrace{[\mathcal{S}^2 - 2\mathcal{P}]}^{\widehat{\mathcal{S}}}\boldsymbol{\mu}^2 - \overbrace{\mathcal{P}^2}^{\widehat{\mathcal{P}}}\,.$$

3.5: Doubling thm. *Sequence $\vec{\mathbf{z}} := (z_n)_{n=0}^{\infty}$ satisfies recurrence*

$$z_{n+2} := \mathcal{S}z_{n+1} - \mathcal{P}z_n\,, \quad \text{where } \mathcal{S},\mathcal{P} \in \mathbb{C}.$$

Then sequence $(z_{2n})_{n\in\mathbb{N}}$ and $(z_{2n+1})_{n\in\mathbb{N}}$ each satisfy recurrence

$$\square_{n+2} = \widehat{\mathcal{S}} \cdot \square_{n+2} - \widehat{\mathcal{P}} \cdot \square_n$$

where $\widehat{\mathcal{S}} := \mathcal{S}^2 - 2\mathcal{P}$ and $\widehat{\mathcal{P}} := \mathcal{P}^2$.

[If $\mathcal{P}{\neq}0$, then $\vec{\mathbf{z}}$ can be extended backwards to $\vec{\mathbf{z}} := (z_n)_{n=-\infty}^{\infty}$, and the doubling result holds.] ♢

Proof. The foregoing argument used $\mathcal{S}^2 \neq 4\mathcal{P}$. Since sequence-values vary continuously with $\mathcal{S}$ and $\mathcal{P}$, it suffices to obtain an $\mathcal{S}^2 = 4\mathcal{P}$ pair as a limit of pairs where the inequality holds. ♦

Fib example. The Fib-seq has $\mathcal{S} = 1$ and $\mathcal{P} = $-$1$. Hence $\widehat{\mathcal{S}} = 1^2 - $-$2 = 3$, and $\widehat{\mathcal{P}} = [$-$1]^2$. So $(\mathsf{f}_{2n})_{n\in\mathbb{Z}}$ and $(\mathsf{f}_{2n+1})_{n\in\mathbb{Z}}$ each satisfy $z_{n+2} = 3z_{n+1} - z_n$.

Starting an any index, then taking every 4^{th}-term, gives a seq satisfying $z_{n+2} = 7z_{n+1} - z_n$, since $3^2 - 2{\cdot}1 = 7$ and $1^2 = 1$. □

3.6: Speed-up thm. *Sequence $\vec{\mathbf{z}} := (z_n)_{n=0}^{\infty}$ satisfies recurrence $z_{n+2} := \mathcal{S}z_{n+1} - \mathcal{P}z_n$.*

For posint K and natnum $\mathbf{b}$, subsequence $(z_{nK+\mathbf{b}})_{n=0}^{\infty}$ satisfies $\square_{n+2} = \widehat{\mathcal{S}} \cdot \square_{n+2} - \widehat{\mathcal{P}} \cdot \square_n$, where $x^2 - \widehat{\mathcal{S}}x + \widehat{\mathcal{P}}$ is the characteristic polynomial of K^{th}-power

$$\mathsf{G}^K = \begin{bmatrix} \mathcal{S} & -\mathcal{P} \\ 1 & 0 \end{bmatrix}^K.$$ ♢

Pf. Use $x^2 - \widehat{\mathcal{S}}x + \widehat{\mathcal{P}}$ for the charpoly of $\mathsf{M} := \mathsf{G}^K$. Cayley-Hamilton asserts $\mathsf{M}^2 = \widehat{\mathcal{S}}{\cdot}\mathsf{M} - \widehat{\mathcal{P}}{\cdot}\mathbf{I}$. Applying both sides to colvec $\begin{bmatrix} z_1 \\ z_0 \end{bmatrix}$, the bottom entry asserts $z_{2K} = \widehat{\mathcal{S}}{\cdot}z_K - \widehat{\mathcal{P}}{\cdot}z_0$. ♦

4: Theorem. *For each integer N:*

4a: $$[\mathsf{f}_N]^2 + [\mathsf{f}_{N-1}]^2 = \mathsf{f}_{2N-1}\,. \quad \diamond$$

Inefficient proof. Always, LhS(4a) is non-negative. And RhS(4a) is non-neg, even when $N \in \mathbb{Z}_-$, since f_{Odd} is always non-neg. So ISTProve that the squares of LhS(4a) and RhS(4a) are equal. To this end, define

4b: $$\mathcal{L} := \varphi^2 \cdot \left[[\mathsf{f}_N]^2 + [\mathsf{f}_{N-1}]^2\right] \qquad \textit{and}$$
$$\mathcal{R} := \varphi^2 \cdot [\mathsf{f}_{2N-1}] \stackrel{\text{note}}{=\!=} \varphi\cdot[\alpha^{2N-1} - \beta^{2N-1}]\,.$$

Leftside. By (2), $\varphi\cdot\mathsf{f}_N = \alpha^N - \beta^N$. So $\varphi^2\cdot{\mathsf{f}_N}^2$ equals
$$\alpha^{2N} + \beta^{2N} - 2[\alpha\beta]^N\,.$$

But $\alpha\beta = \text{-}1$, and N and $N-1$ have opposite parities. Thus $\mathcal{L}$ equals
$$\alpha^{2N} + \beta^{2N} + \alpha^{2[N-1]} + \beta^{2[N-1]}$$
$$= \alpha^{2[N-1]}[\alpha^2 + 1] + \bullet\bullet\bullet\,,$$
where the "$\bullet\bullet\bullet$" represents a copy of all the α-terms to its left, but with "α" replaced by "β".

By (1b), note, $\alpha^2 + 1 = \alpha + 2$. Thus
$$\mathcal{L} = \alpha^{2[N-1]}[\alpha + 2] + \beta^{2[N-1]}[\beta + 2]\,.$$

Squaring $\mathcal{L}$ will give twice this cross-term:
$$[\alpha\beta]^{2[N-1]}\cdot[\alpha+2][\beta+2] = 1\cdot[\alpha+2][\beta+2]$$
$$= \alpha\beta + 2[\alpha+\beta] + 4$$
$$= \text{-}1 + 2 + 4 = 5\,.$$

Also note $[\alpha+2]^2 = \alpha^2 + 4[\alpha+1] = 5\alpha^2$. Thus
$$\mathcal{L}^2 = \alpha^{4[N-1]}\cdot 5\alpha^2 + \bullet\bullet\bullet + 5\cdot 2\,.$$

Consequently

4c: $$\tfrac{1}{5}\cdot\mathcal{L}^2 = \alpha^{4N-2} + \beta^{4N-2} + 2\,.$$

Rightside of (4a). Square $\mathcal{R}$ and divide by 5. Since $5 = \varphi^2$,
$$\tfrac{1}{5}\cdot\mathcal{R}^2 = \left[\alpha^{2N-1} - \beta^{2N-1}\right]^2.$$

The cross-term is $\text{-}2[\alpha\beta]^{2N-1} = \text{-}2\cdot[\text{-}1]^{2N-1} = 2$, since $2N-1$ is odd. We have thus shown that

4d: $$\tfrac{1}{5}\cdot\mathcal{R}^2 = \alpha^{4N-2} + \beta^{4N-2} + 2\,.$$

And this equals RhS(4c), as desired. ♦

Ahem. It's a proof, but the next is a *prettier proof.* □

Dot-product proof

Fix three integers $S = j + k$. Evidently the dot-product
$$\mathsf{f}_{j+1}\mathsf{f}_k + \mathsf{f}_j\mathsf{f}_{k-1} = \mathsf{f}_{j+1}[\mathsf{f}_{k-1} + \mathsf{f}_{k-2}] + \mathsf{f}_j\mathsf{f}_{k-1}$$
$$= [\mathsf{f}_{j+1} + \mathsf{f}_j]\mathsf{f}_{k-1} + \mathsf{f}_{j+1}\mathsf{f}_{k-2}$$
$$= \mathsf{f}_{j+2}\mathsf{f}_{k-1} + \mathsf{f}_{j+1}\mathsf{f}_{k-2}\,.$$

This last dot-product is the same as the first, but with "$j + k = S$" replaced by "$[j+1] + [k-1] = S$". Thus, for all $j \in \mathbb{Z}$, expression $\mathsf{f}_{j+1}\cdot\mathsf{f}_k + \mathsf{f}_j\cdot\mathsf{f}_{k-1}$ depends only on S.

5: Theorem. *For all triples of integers $S = j + k$:*

5a: $$\mathsf{f}_{j+1}\cdot\mathsf{f}_k + \mathsf{f}_j\cdot\mathsf{f}_{k-1} = \mathsf{f}_S\,.$$

In particular, (4a) holds. ◊

Proof. Setting $j := 0$ in LhS(5a) results in
$$\mathsf{f}_1\mathsf{f}_S + \mathsf{f}_0\mathsf{f}_{S-1} = 1\cdot\mathsf{f}_S + 0\cdot\mathsf{f}_{S-1} = \mathsf{f}_S\,.$$

Hence (5a). To obtain (4a) from (5a), set $S := 2N-1$ and $j := N-1$. ♦

Alt Pf. Looking ahead to matrix $\mathsf{A} := \left[\begin{smallmatrix}1 & 1\\ 1 & 0\end{smallmatrix}\right]$ from Cassini, the $(1,2)$-entry of matrix $\mathsf{A}^S = \mathsf{A}^j\mathsf{A}^k$ is $(*)$. ♦

5b: Duplication identity. *For each integer n,*

$*$: $$\mathsf{f}_{2n} = \mathsf{f}_n\cdot[\mathsf{f}_{n+1} + \mathsf{f}_{n-1}] = \mathsf{f}_n\cdot[\mathsf{f}_n + 2\mathsf{f}_{n-1}]\,. \quad \diamond$$

Proof. Apply (5a) with $j := n-1$ and $k := n+1$. Then $\mathsf{f}_{2n} = \mathsf{f}_n\mathsf{f}_{n+1} + \mathsf{f}_{n-1}\mathsf{f}_n = \mathsf{f}_n\cdot[\mathsf{f}_{n+1} + \mathsf{f}_{n-1}]$. So f_{2n} equals
$$\mathsf{f}_n\cdot\Big[[\mathsf{f}_n + \mathsf{f}_{n-1}] + \mathsf{f}_{n-1}\Big] = \text{RhS}(*)\,. \quad ♦$$

5c: Cassini's identity. *For all n,*

£: $$f_{n+1} \cdot f_{n-1} = {f_n}^2 + [-1]^n . \qquad \diamond$$

Pf. Let $\mathbf{v}_n := \begin{bmatrix} f_n \\ f_{n-1} \end{bmatrix}$. With $A := \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}$, our recurrence says $A\mathbf{v}_n = \mathbf{v}_{n+1}$. Id-matrix $\mathbf{I} = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} f_1 & f_0 \\ f_0 & f_{-1} \end{bmatrix}$; i.e A^0 is 2×2 matrix $[\mathbf{v}_1\ \mathbf{v}_0]$. Thus A^n equals $\begin{bmatrix} f_{n+1} & f_n \\ f_n & f_{n-1} \end{bmatrix}$. Equation $\mathrm{Det}(A^n) = [\mathrm{Det}(A)]^n$ yields (£). ♦

5d: 1-3-1 Fib lemma. *Fibonacci sequence $\vec{f}$ satisfies*

££: $$[f_{n+1}]^2 - 3[f_n]^2 + [f_{n-1}]^2 = 2 \cdot [-1]^n . \qquad \diamond$$

Proof. Squaring $f_n = f_{n+1} - f_{n-1}$ implies

$$\begin{aligned} {f_n}^2 &= {f_{n+1}}^2 + {f_{n-1}}^2 - 2f_{n+1} \cdot f_{n-1} \\ &\overset{\text{Cassini}}{=\!=} {f_{n+1}}^2 + {f_{n-1}}^2 - 2\big[{f_n}^2 + [-1]^n\big] \\ &= {f_{n+1}}^2 + {f_{n-1}}^2 - 2{f_n}^2 - 2[-1]^n . \end{aligned}$$ ♦

6: Lemma. $\forall n \in \mathbb{N}$: $[f_1]^2 + [f_2]^2 + \ldots + [f_n]^2 = f_n f_{n+1}$. ◊

Pf. Easy induction. Even nicer, $f_n f_{n+1}$ is the area of a $f_n \times f_{n+1}$ business card. Decompose it into squares. ♦

Perodicity mod a prime. Working mod-5, note

$$(f_{10}, f_{11}) = (55, 89) \equiv_5 (0, -1) = [-1] \cdot (f_0, f_1) .$$

Mod-5, then, Fib-seq $\vec{f}$ has a nega-period of length 10, whence $\vec{f}_{\text{Mod-5}}$ has 20 as a period: $f_{20+n} \equiv_5 f_n$.

[Eventually adjoin material wrt other primes.]

Divisibility

Integer-sequence $\vec{\boldsymbol{\sigma}} = \boldsymbol{(}\sigma_1, \sigma_2, \ldots\boldsymbol{)}$ is a ***divisibility sequence*** [***div-seq***] if $\forall_{\text{indices}}\, j,k \in \mathbb{Z}_+$: If $j \bullet\!| \; k$ then $\sigma_j \bullet\!| \; \sigma_k$.

Our $\vec{\boldsymbol{\sigma}}$ is a ***strong div-seq*** if $\forall j,k$:

$$\dagger: \qquad \sigma_{\mathrm{GCD}(j,k)} = \mathrm{GCD}(\sigma_j, \sigma_k).$$

Why does *strong div-seq* implies *div-seq*? When $j \bullet\!| \; k$, then $\mathrm{GCD}(j,k) = j$. Hence $\mathrm{GCD}(\sigma_j, \sigma_k) = \sigma_j$. And this implies $\sigma_j \bullet\!| \; \sigma_k$.

Strong div-seq implies, for each list $k_1, \ldots, k_N$,

$$\ddagger: \qquad \sigma_{\mathrm{GCD}(k_1,\ldots,k_N)} = \mathrm{GCD}(\sigma_{k_1}, \ldots, \sigma_{k_N})\,.$$

Using underline for GCD, note $\underline{a,c,e} = \underline{\underline{a,c},\, e}$. Hence,

$$\begin{aligned} \sigma_{\underline{a,c,e}} = \sigma_{\underline{\underline{a,c},\,e}} &\overset{\text{by }(\dagger)}{=\!=} \underline{\sigma_{\underline{a,c}},\ \sigma_e} \\ &\overset{\text{by }(\dagger)}{=\!=} \underline{\underline{\sigma_a, \sigma_c},\ \sigma_e} \\ &= \underline{\sigma_a, \sigma_c, \sigma_e}\,. \end{aligned}$$

8.1: Lemma. *For integers $b > a \geq 0$, values $\sigma_n := b^n - a^n$ form a divisibility sequence.* ♢

Proof. Given $j \bullet\!| \; k$, write $k = \boldsymbol{\rho}\cdot j$, and set $B := b^j$ and $A := a^j$. So

$$\frac{\sigma_k}{\sigma_j} = \frac{B^{\boldsymbol{\rho}} - A^{\boldsymbol{\rho}}}{B - A} = \sum_{\substack{\mathsf{v}+\mathsf{u} = \boldsymbol{\rho}-1 \\ \mathsf{v},\mathsf{u} \geq 0}} B^{\mathsf{v}} A^{\mathsf{u}}\,.$$ ♦

8.2: *Obs.* Div-seq $\sigma_n = b^n - a^n$ need not be a strong div-sequence. E.g, with $b := 4$ and $a := 2$, note

$$\mathrm{GCD}(\sigma_6, \sigma_4) = \mathrm{GCD}(4032, 240) = 48\,.$$

Yet $\sigma_{\mathrm{GCD}(6,4)} = \sigma_2 = 12$. □

8.3: ? Fact ? *For integers $b > a \geq 1$, if $b \perp a$ then sequence $\sigma_n := b^n - a^n$ is a strong divisibility-sequence.* ♢

Proof. ?? See proof of (11). ♦

9: Theorem. *Fibonacci seq* $\vec{\boldsymbol{f}} = (\mathsf{f}_1, \mathsf{f}_2, \mathsf{f}_3, \ldots)$ *is a divisibility-sequence.* ♢

Pf. Fix posint P. For $n = 1, 2, \ldots$, we prove $\mathsf{f}_P \bullet\!| \; \mathsf{f}_{nP}$. The base-case is $\mathsf{f}_P \bullet\!| \; \mathsf{f}_{1 \cdot P}$.

We apply Thm 5,

$$*: \qquad \mathsf{f}_{j+k} = \mathsf{f}_{j+1} \cdot \mathsf{f}_k + \mathsf{f}_j \cdot \mathsf{f}_{k-1},$$

with $j := nP$ and $k := P$. Inductively, quotient $Q := \mathsf{f}_{nP}/\mathsf{f}_P$ is an integer. Our $(*)$ says

$$\begin{aligned} \mathsf{f}_{[n+1]P} &= \mathsf{f}_{nP+1}\mathsf{f}_P + \mathsf{f}_{nP}\mathsf{f}_{P-1} \\ &= \mathsf{f}_{nP+1}\mathsf{f}_P + Q\mathsf{f}_P\,\mathsf{f}_{P-1} \\ &= \mathsf{f}_P \cdot [\mathsf{f}_{nP+1} + Q\,\mathsf{f}_{P-1}]. \end{aligned}$$

And $\mathsf{f}_{nP+1} + Q\,\mathsf{f}_{P-1}$ is an integer. ♦

10.1: Prop. *For integers* δ, β, D*: If* $\delta \,|\!\bullet\, D$*, then*

$$\mathrm{GCD}(\delta + \beta,\, D) = \mathrm{GCD}(\beta, D). \qquad \text{[Exercise]}$$ ♢

10.2: Prop. *For* n *an integer:* $\mathsf{f}_{n+1} \perp \mathsf{f}_n$. [Exercise] ♢

11: Fib strong-div. *Divide* $\mathsf{u} \neq 0$ *into* v [*both integers*] *to get quotient and remainder,* $\mathsf{v} = q\mathsf{u} + \mathsf{r}$. *Then*

11a: $\mathrm{GCD}(\mathsf{f}_\mathsf{v}, \mathsf{f}_\mathsf{u}) = \mathrm{GCD}(\mathsf{f}_\mathsf{u}, \mathsf{f}_{\mathsf{v}-\mathsf{u}})$;

11b: $\mathrm{GCD}(\mathsf{f}_\mathsf{v}, \mathsf{f}_\mathsf{u}) = \mathrm{GCD}(\mathsf{f}_\mathsf{u}, \mathsf{f}_\mathsf{r})$;

11c: $\mathrm{GCD}(\mathsf{f}_\mathsf{v}, \mathsf{f}_\mathsf{u}) = \mathsf{f}_{\mathrm{GCD}(\mathsf{v},\mathsf{u})}$.

Thus $\mathsf{f}_1, \mathsf{f}_2, \mathsf{f}_3, \ldots$ *is a strong divisibility-sequence.* ♢

Pf 11a. We apply Thm 5 with $j := \mathsf{v} - \mathsf{u}$ and $k := \mathsf{u}$. So

$$\mathsf{f}_\mathsf{v} = \mathsf{f}_{\mathsf{v}-\mathsf{u}+1}\,\mathsf{f}_\mathsf{u} + \mathsf{f}_{\mathsf{v}-\mathsf{u}}\,\mathsf{f}_{\mathsf{u}-1}.$$

Since f_u divides $\mathsf{f}_{\mathsf{v}-\mathsf{u}+1}\,\mathsf{f}_\mathsf{u}$, our Prop 10.1 says

$$\underline{\mathsf{f}_\mathsf{v}, \mathsf{f}_\mathsf{u}} = \underline{\mathsf{f}_{\mathsf{v}-\mathsf{u}}\mathsf{f}_{\mathsf{u}-1},\, \mathsf{f}_\mathsf{u}} = \underline{\mathsf{f}_{\mathsf{v}-\mathsf{u}},\, \mathsf{f}_\mathsf{u}},$$

since $\mathsf{f}_{\mathsf{u}-1} \perp \mathsf{f}_\mathsf{u}$. [Argument works also for $\mathsf{u}=0$.] ♦

Pf 11b. Applying (11a) q times gives $\underline{\mathsf{f}_\mathsf{v}, \mathsf{f}_\mathsf{u}} = \underline{\mathsf{f}_\mathsf{u}, \mathsf{f}_{\mathsf{v}-q\mathsf{u}}}$. ♦

Pf 11c. Recall the *update rule* in the Euclidean algorithm (Lightning Bolt) when seeding LBolt with $r_0 := \mathsf{v}$ and $r_1 := \mathsf{u}$. Observe that the r of decomposition $\mathsf{v} = q\mathsf{u} + \mathsf{r}$ is the r_2 of LBolt. Thus (11b) says

$$\underline{\mathsf{f}_{r_0}, \mathsf{f}_{r_1}} = \underline{\mathsf{f}_{r_1}, \mathsf{f}_{r_2}}.$$

But *this* is the update rule when seeded with f_{r_0} and f_{r_1}. Consequently, letting $\boldsymbol{g} := \underline{\mathsf{v}, \mathsf{u}}$,

$$\underline{\mathsf{f}_\mathsf{v}, \mathsf{f}_\mathsf{u}} = \underline{\mathsf{f}_{\boldsymbol{g}}, \mathsf{f}_0} = \underline{\mathsf{f}_{\boldsymbol{g}}, 0} \stackrel{\text{note}}{=\!=} \mathsf{f}_{\boldsymbol{g}}.$$ ♦

Can complex analysis Fib?

What is the RoC of

$$\dagger: \qquad \mathcal{F}(z) := \sum_{n\geq 0} \mathsf{f}_n z^n ,$$

the ***generating function*** of the fibonacci sequence?

Recurrence $\mathsf{f}_{n+2} = \mathsf{f}_{n+1} + \mathsf{f}_n$, and that $\mathsf{f}_n \geq 0$ for $n \geq 0$ show that sequence $\vec{\boldsymbol{f}}$ is non-decreasing. For $n \geq 2$, the sequence is positive, so recurrence (1a) gives

$$2\mathsf{f}_{n-2} \leq \mathsf{f}_n \leq 2\mathsf{f}_{n-1} . \quad \textit{Hence}$$

$$\text{Const} \cdot [\sqrt{2}]^n \leq \mathsf{f}_n \leq \text{Const} \cdot 2^n . \quad \textit{Thus}$$

$$\frac{1}{\sqrt{2}} \geq \mathsf{RoC}(\mathcal{F}) \geq \frac{1}{2} .$$

In particular, $\mathcal{F}$ is analytic in a nbhd of zero.

Shh... In fact we know that

$$**: \qquad \mathsf{f}_n = \frac{1}{\sqrt{5}} \cdot [\boldsymbol{\alpha}^n - \boldsymbol{\beta}^n], \qquad \textit{where}$$

$$\boldsymbol{\alpha} = \tfrac{1}{2}[1+\sqrt{5}] \quad \textit{and} \quad \boldsymbol{\beta} = \tfrac{1}{2}[1-\sqrt{5}] .$$

Here, $\boldsymbol{\alpha}$ and $\boldsymbol{\beta}$ are the *golden/silver* ratios, respectively. We thus have that

$$\text{Shh!:} \qquad \mathsf{RoC}(\mathcal{F}) = 1/\boldsymbol{\alpha} = \frac{2}{1+\sqrt{5}} .$$

Source. Online book **A First Course in Complex Analysis**, made freely available by Matthias Beck, Gerald Marchesi, Dennis Pixton & Lucas Sabalka, has the below problem in §*10.3* of their text. □

A formula for $\mathcal{F}$. [Below, I'll use $\mathcal{F}$ to abbreviate $\mathcal{F}(z)$.] By defn,

$$z^0 \cdot \sum_{n\geq 0} \mathsf{f}_{n+2} \cdot z^{n+2} = \mathcal{F} - \mathsf{f}_0 \cdot z^0 - \mathsf{f}_1 \cdot z^1 \stackrel{\text{note}}{=\!=} \mathcal{F} - z;$$

$$z^1 \cdot \sum_{n\geq 0} \mathsf{f}_{n+1} \cdot z^{n+1} = z \cdot [\mathcal{F} - \mathsf{f}_0 \cdot z^0] \stackrel{\text{note}}{=\!=} z \cdot \mathcal{F};$$

$$z^2 \cdot \sum_{n\geq 0} \mathsf{f}_n \cdot z^n = z^2 \cdot \mathcal{F} .$$

From the top equality, we subtract the other two. The lefthand side of the result is

$$\sum_{n\geq 0} [\mathsf{f}_{n+2} - \mathsf{f}_{n+1} - \mathsf{f}_n] z^{n+2} \stackrel{\text{note}}{=\!=} 0 ,$$

since $\mathsf{f}_{n+2} = \mathsf{f}_{n+1} + \mathsf{f}_n$. From the righthand sides, then, $0 = [1 - z - z^2]\mathcal{F} - z$. Hence

$$\ddagger: \quad \mathcal{F}(z) = \frac{z}{D(z)} , \quad \textit{where} \quad D(z) := 1 - z - z^2 .$$

Easily, $D(z) = z^2 \cdot \text{Fib}(\frac{1}{z}) = z^2 \cdot [\frac{1}{z} - \boldsymbol{\alpha}][\frac{1}{z} - \boldsymbol{\beta}]$. Rewriting, $D(z) = [\boldsymbol{\alpha} z - 1][\boldsymbol{\beta} z - 1]$. Thus

$$D(z) = \boldsymbol{\alpha\beta}[z - \tfrac{1}{\boldsymbol{\alpha}}][z - \tfrac{1}{\boldsymbol{\beta}}] \stackrel{\text{note}}{=\!=} \text{-}1 \cdot [z + \boldsymbol{\beta}][z + \boldsymbol{\alpha}] .$$

Residues. With $H_n(z) := \frac{1}{z^n D(z)} \stackrel{\text{def}}{=\!=} \frac{\mathcal{F}(z)}{z^{n+1}}$, note

$$\operatorname*{Res}_{z=0}(H_n) =\!=\!= \operatorname*{Res}_{z=0}\Big(\frac{\mathcal{F}(z)}{z^{n+1}}\Big) \underset{P.30}{\stackrel{\text{PlexNotes}}{=\!=\!=}} \frac{1}{n!} \cdot \mathcal{F}^{(n)}(0) = \mathsf{f}_n .$$

Looking ahead, $\frac{1}{\boldsymbol{\beta}^n} - \frac{1}{\boldsymbol{\alpha}^n} = \frac{\boldsymbol{\alpha}^n - \boldsymbol{\beta}^n}{[\boldsymbol{\alpha\beta}]^n} = \frac{\boldsymbol{\alpha}^n - \boldsymbol{\beta}^n}{[\text{-}1]^n}$. So

$$\yen: \qquad \frac{1}{[\text{-}\boldsymbol{\beta}]^n} - \frac{1}{[\text{-}\boldsymbol{\alpha}]^n} = \boldsymbol{\alpha}^n - \boldsymbol{\beta}^n .$$

Contour integral. Let $\mathsf{C}_r := \text{Sph}_r(0)$. Since $n \geq 0$, the degree of $z^n D(z)$ is at least 2, whence

$$\lim_{r \nearrow \infty} \frac{1}{2\boldsymbol{\pi}\mathbf{i}} \oint_{\mathsf{C}_r} H_n = 0 .$$

As the singularities of H_n are $0, \text{-}\boldsymbol{\beta}, \text{-}\boldsymbol{\alpha}$,

$$0 = \text{Res}(H_n, 0) + \text{Res}(H_n, \text{-}\boldsymbol{\beta}) + \text{Res}(H_n, \text{-}\boldsymbol{\alpha}) , \textit{ i.e}$$

$$*: \quad \mathsf{f}_n = \text{Res}(-H_n, \text{-}\boldsymbol{\beta}) + \text{Res}(-H_n, \text{-}\boldsymbol{\alpha}) .$$

Writing $-H_n(z) = \frac{1/[z^n[\boldsymbol{\alpha} + z]]}{z - \text{-}\boldsymbol{\beta}}$, the CIF gives

$$\text{Res}(-H_n, \text{-}\boldsymbol{\beta}) = 1/[[\text{-}\boldsymbol{\beta}]^n[\boldsymbol{\alpha} - \boldsymbol{\beta}]] . \quad \textit{Similarly,}$$

$$\text{Res}(-H_n, \text{-}\boldsymbol{\alpha}) = 1/[[\text{-}\boldsymbol{\alpha}]^n[\boldsymbol{\beta} - \boldsymbol{\alpha}]] .$$

Their sum equals

$$\frac{1}{\boldsymbol{\alpha} - \boldsymbol{\beta}} \cdot \Big[\frac{1}{[\text{-}\boldsymbol{\beta}]^n} - \frac{1}{[\text{-}\boldsymbol{\alpha}]^n}\Big] \stackrel{\text{by }(\yen)}{=\!=\!=} \frac{1}{\boldsymbol{\alpha} - \boldsymbol{\beta}} \cdot [\boldsymbol{\alpha}^n - \boldsymbol{\beta}^n] .$$

Plugging this into (∗), yields (∗∗) –which we supposedly didn't know.

Tribonacci sequence

The bi-infinite ***Trib sequence*** is

$$*: \quad (t_0, t_1, t_2) := (0,0,1) \quad \textit{and} \quad t_{n+3} := t_{n+2} + t_{n+1} + t_n,$$

for $n \in \mathbb{Z}$. The resulting Trib sequence is

n:	...	-9	-8	-7	-6	-5	-4	-3	-2	-1	0	1	2	3	4	5	6	7 ...
t_n:	...	81	44	24	13	7	4	2	1	1	0	0	1	1	2	4	7	13 ...

A nz-complex ω engenders seq $n \mapsto \omega^n$, which satisfies the recurrence part of $(*)$ IFF ω is a zero of $\text{Trb}(z) := z^3 - z^2 - z - 1$.

Zeros of $\text{Trb}()$. As $\text{Trb}(1) < 0 < \text{Trb}(2)$, value $\text{Trb}(\boldsymbol{p})$ is zero for some posreal $1<\boldsymbol{p}<2$. The remaining Trb-zeros form a complex-conjugate pair $\boldsymbol{w} \neq \overline{\boldsymbol{w}}$.

To see this last, ISTShow that $\text{Trb}|_{\mathbb{R}}$ has but one zero. Its derivative equals

$$\text{Trb}'(x) = 3x^2 - 2x - 1 = 3[z-1][z+\tfrac{1}{3}].$$

At the Trb()-critical-points, each of $\text{Trb}(1) = \text{-}2$ and $\text{Trb}(\frac{-1}{3}) = \frac{-22}{27}$ is negative. Hence $\text{Trb}(x)$ is negative for $x < \boldsymbol{p}$, and is positive for $x > \boldsymbol{p}$.

12: Prop'n. *Sum* $\boldsymbol{w} + \overline{\boldsymbol{w}} + \boldsymbol{p} = 1$, *product* $\boldsymbol{w} \cdot \overline{\boldsymbol{w}} \cdot \boldsymbol{p} = 1$. *Also*, $\boldsymbol{p} > 1 > |\boldsymbol{w}| = |\overline{\boldsymbol{w}}| = \frac{1}{\sqrt{\boldsymbol{p}}}$. ◊

Pf. Write $z^3 - 1z^2 - z - 1 = [z - \boldsymbol{w}][z - \overline{\boldsymbol{w}}][z - \boldsymbol{p}]$ and equate coeffs. ♦

Trib GF. The *generating function* of Trib-seq is

$$\dagger: \quad \mathcal{T}(z) := \sum_{n \geq 0} t_n z^n. \quad \square$$

12a: Lemma. *The* $\text{RoC}(\mathcal{T})$ *is* $1/|\boldsymbol{p}|$. *Proof.* Exercise. ◊

"Cheating". Cardano's formula gives

$$\boldsymbol{p} = \tfrac{1}{3}[1 + S^+ + S^-],$$
$$\boldsymbol{w} = \tfrac{1}{6}[2 + \boldsymbol{\mu} S^+ + \overline{\boldsymbol{\mu}} S^-],$$
$$\overline{\boldsymbol{w}} = \tfrac{1}{6}[2 + \overline{\boldsymbol{\mu}} S^+ + \boldsymbol{\mu} S^-],$$

where

$$\boldsymbol{\mu} := \text{-}1 + \mathbf{i}\sqrt{3}, \qquad S^+ := \sqrt[3]{19 + 3\sqrt{33}},$$
$$\overline{\boldsymbol{\mu}} := \text{-}1 - \mathbf{i}\sqrt{3}, \qquad S^- := \sqrt[3]{19 - 3\sqrt{33}}.$$

Values $S^+ > S^-$ are real. And $\text{Im}(\boldsymbol{w}) > 0 > \text{Im}(\overline{\boldsymbol{w}})$. Approximately $\boldsymbol{p} \approx 1.839$ and $\boldsymbol{w} \approx \text{-}0.419 + 0.606\mathbf{i}$. *However*, we eschew this information FtTBeing. □

A formula for $\mathcal{T}$. [Below, $\mathcal{T}$ abbreviates $\mathcal{T}(z)$.] By defn,

$$z^0 \cdot \sum_{n \geq 0} t_{n+3} \cdot z^{n+3} = \mathcal{T} - t_0 \cdot z^0 - t_1 \cdot z^1 - t_2 \cdot z^2 \overset{\text{note}}{=\!=} \mathcal{T} - z^2;$$

$$z^1 \cdot \sum_{n \geq 0} t_{n+2} \cdot z^{n+2} = z \cdot [\mathcal{T} - t_0 \cdot z^0 - t_1 \cdot z^1] \overset{\text{note}}{=\!=} z \cdot \mathcal{T};$$

$$z^2 \cdot \sum_{n \geq 0} t_{n+1} \cdot z^{n+1} = z^2 \cdot [\mathcal{T} - t_0 \cdot z^0] \overset{\text{note}}{=\!=} z^2 \cdot \mathcal{T};$$

$$z^3 \cdot \sum_{n \geq 0} t_n \cdot z^n = z^3 \cdot \mathcal{T}.$$

From the top equality, subtracting the lower three gives this LhS,

$$\sum_{n \geq 0} [t_{n+3} - t_{n+2} - t_{n+1} - t_n] z^{n+3} \overset{\text{note}}{=\!=} 0,$$

by $(*)$. Hence $0 = [1 - z - z^2 - z^3]\mathcal{T} - z^2$, from the RhS. Consequently,

$$\ddagger: \quad \mathcal{T}(z) = \frac{z^2}{E(z)}, \textit{ where } E(z) := 1 - z - z^2 - z^3.$$

Zeros of $E()$. As $E(z) = \text{Trb}(\frac{1}{z}) \cdot z^3$, the zeros of $E()$ are reciprocals $\boldsymbol{b} := 1/\boldsymbol{p}$, $\boldsymbol{m} := 1/\boldsymbol{w}$ and $\overline{\boldsymbol{m}}$. Thus

$$E(z) = \text{-}1 \cdot [z - \boldsymbol{b}][z - \boldsymbol{m}][z - \overline{\boldsymbol{m}}].$$

Residues. As $\mathsf{RoC}(\mathcal{T})$ is positive, $\operatorname*{Res}_{z=0}\left(\frac{\mathcal{T}(z)}{z^{n+1}}\right) = \mathsf{t}_n$ for $n=0,1,\ldots$, courtesy (†).

Ratio $\frac{\mathcal{T}(z)}{z^{n+1}} \stackrel{\text{by } (\ddagger)}{=\!=} \frac{z}{z^n E(z)} =: H_n(z)$ is a rational function satisfying $\operatorname{Deg}(\text{Denominator}) \geq \operatorname{Deg}(\text{Numerator}) + 2$. Consequently, $\lim_{r \nearrow \infty} \int_{\mathsf{C}_r} H_n(z)\,\mathrm{d}z$ is zero.

For r large, circle C_r encloses $0, \boldsymbol{b}, \boldsymbol{m}, \overline{\boldsymbol{m}}$, the four singularities of H_n. Hence their H_n-residues sum to zero. Recall that the $z=0$ residue is t_n. So...

$$\mathsf{t}_n = \operatorname*{Res}_{z=\boldsymbol{b}}(-H_n) + \operatorname*{Res}_{z=\boldsymbol{m}}(-H_n) + \operatorname*{Res}_{z=\overline{\boldsymbol{m}}}(-H_n)$$

where $$-H_n(z) = z \Big/ \left(z^n[z-\boldsymbol{b}][z-\boldsymbol{m}][z-\overline{\boldsymbol{m}}]\right).$$

The sum of these three residues is

$$\frac{\boldsymbol{b}}{\boldsymbol{b}^n[\boldsymbol{b}-\boldsymbol{m}][\boldsymbol{b}-\overline{\boldsymbol{m}}]} + \frac{\boldsymbol{m}}{\boldsymbol{m}^n[\boldsymbol{m}-\boldsymbol{b}][\boldsymbol{m}-\overline{\boldsymbol{m}}]} + \frac{\overline{\boldsymbol{m}}}{\overline{\boldsymbol{m}}^n[\overline{\boldsymbol{m}}-\boldsymbol{b}][\overline{\boldsymbol{m}}-\boldsymbol{m}]}$$
$$= Q\cdot\boldsymbol{p}^n + U\cdot\boldsymbol{w}^n + \overline{U}\cdot\overline{\boldsymbol{w}}^n$$
$$= Q\cdot\boldsymbol{p}^n + \operatorname{Re}\left(U \cdot 2\,\boldsymbol{w}^n\right), \quad \textit{where}$$

$$Q = \frac{1/\boldsymbol{p}}{[1/\boldsymbol{p}-1/\boldsymbol{w}][1/\boldsymbol{p}-1/\overline{\boldsymbol{w}}]} = \frac{\boldsymbol{p}\boldsymbol{w}\overline{\boldsymbol{w}}}{[\boldsymbol{w}-\boldsymbol{p}][\overline{\boldsymbol{w}}-\boldsymbol{p}]} \stackrel{\text{note}}{=\!=} \frac{1}{[\boldsymbol{p}-\boldsymbol{w}]\cdot[\boldsymbol{p}-\overline{\boldsymbol{w}}]},$$
$$U = \frac{1/\boldsymbol{w}}{[1/\boldsymbol{w}-1/\boldsymbol{p}][1/\boldsymbol{w}-1/\overline{\boldsymbol{w}}]} = \frac{\boldsymbol{p}\boldsymbol{w}\overline{\boldsymbol{w}}}{[\boldsymbol{p}-\boldsymbol{w}][\overline{\boldsymbol{w}}-\boldsymbol{w}]} \stackrel{\text{note}}{=\!=} \frac{1}{[\boldsymbol{p}-\boldsymbol{w}][\overline{\boldsymbol{w}}-\boldsymbol{w}]}.$$

12b: **Theorem.** *For each $n \in \mathbb{Z}$:*

$$\mathsf{t}_n = \frac{\boldsymbol{p}^n}{[\boldsymbol{p}-\boldsymbol{w}][\overline{\boldsymbol{w}}-\boldsymbol{w}]} + \operatorname{Re}\left(\frac{2\,\boldsymbol{w}^n}{[\boldsymbol{p}-\boldsymbol{w}][\overline{\boldsymbol{w}}-\boldsymbol{w}]}\right). \diamondsuit$$

After typing up this Tribonacci *task, now I find the following webpage:*

https://en.wikipedia.org/wiki/Generalizations_of_Fibonacci_numbers#Tribonacci_numbers

Number theory of Fib sequence

T.fol problem and soln is from Stack Exchange.

13: Five-Fib thm. *For prime p, fibonacci number f_{p-1} is divisible by p IFF $p \equiv_5 \pm 1$.* ◊

Note. The result holds for $p=2$, as both parts fail. Henceforth, p is an odd prime. □

Pf ($\Leftarrow$). Suppose $p \equiv_5 +1$ or $p \equiv_5 -1$. Then p is a 5-QR. Courtesy Quadratic Reciprocity, 5 is a p-QR; this, since 5 is 4Pos.

Henceforth, $\equiv$ means $\equiv_p$, and $\langle\cdot\rangle$ means $\langle\cdot\rangle_p$.

Let $\boldsymbol{\sigma}$ be such that $\boldsymbol{\sigma}^2 \equiv 5$; use $\widehat{\boldsymbol{\sigma}} := \langle 1 \div \boldsymbol{\sigma}\rangle$ for its reciprocal. Let $\widehat{2} := \langle 1 \div 2\rangle$. Binet's formula for f_n is

$$f_n = \frac{1}{\varphi}\cdot[\boldsymbol{\alpha}^n - \boldsymbol{\beta}^n], \quad \textit{where}$$
$$\boldsymbol{\alpha},\boldsymbol{\beta} = (1 \pm \varphi)\cdot\frac{1}{2}, \quad \textit{where } \varphi := \sqrt{5}.$$

The Idea. Follow Binet by mimicking f_n in $\mathbb{Z}_p$:

$$*: \quad g_n := \widehat{\boldsymbol{\sigma}}\cdot\Big[([1+\boldsymbol{\sigma}]\cdot\widehat{2})^n - ([1-\boldsymbol{\sigma}]\cdot\widehat{2})^n\Big] = \widehat{\boldsymbol{\sigma}}\cdot\Big[(1+\boldsymbol{\sigma})^n - (1-\boldsymbol{\sigma})^n\Big]\cdot\widehat{2}^n.$$

Fermat's Little Thm. There is <u>*no*</u> oddprime p for which $5 \equiv 1$. Hence the above $\boldsymbol{\sigma} \not\equiv \pm 1$. Thus $1+\boldsymbol{\sigma}$ and $1-\boldsymbol{\sigma}$ are p-units, as is $\widehat{2}$.

We may thus apply FLiT to conclude that

$$**: \quad g_{p-1} \equiv \widehat{\boldsymbol{\sigma}}\cdot\Big[([1+\boldsymbol{\sigma}]\cdot\widehat{2})^{p-1} - ([1-\boldsymbol{\sigma}]\cdot\widehat{2})^{p-1}\Big] \stackrel{\text{FLit}}{=\!=} \widehat{\boldsymbol{\sigma}}\cdot[1-1] = 0.$$

Showing $g_N \equiv f_N$. ISTEstablish $2^N g_N \stackrel{?}{\equiv} 2^N f_N$, since $2 \perp p$. To this end, let H be the largest integer with $2H+1 \le N$. Then $\varphi\cdot 2^N f_N$ equals

$$(1+\varphi)^N - (1-\varphi)^N = \sum_{j=0}^{N}\binom{N}{j}\cdot[1-(-1)^j]\varphi^j = \sum_{d=0}^{H}\binom{N}{2d+1}\cdot 2\varphi^{2d+1} = 2\varphi\cdot\sum_{d=0}^{H}\binom{N}{2d+1}\cdot 5^d.$$

Hence $2^N f_N$ equals

$$\frac{1}{\varphi}\cdot\Big[(1+\varphi)^N - (1-\varphi)^N\Big] = 2\sum_{d=0}^{H}\binom{N}{2d+1}\cdot 5^d \stackrel{\text{note}}{\equiv} 2N.$$

The same algebra shows $2^N g_N$ is mod-5 congruent to

$$\widehat{\boldsymbol{\sigma}}\cdot\Big[(1+\boldsymbol{\sigma})^N - (1-\boldsymbol{\sigma})^N\Big] \equiv 2\sum_{d=0}^{H}\binom{N}{2d+1}\cdot 5^d \equiv 2N. ♦$$

Pf ($\Rightarrow$). ?? ♦

13a: Corollary. *For n a natnum: $2^n\cdot f_n \equiv_5 2n$.* ◊