Altes Beispiel: $b = 133$, $a = 84$

$133 : 84 = 1 \quad q_0$
$\underline{84}$
$84 : 49 = 1 \quad q_1$
$\underline{49}$
$49 : 35 = 1 \quad q_2$
$\underline{35}$
$35 : 14 = 2 \quad q_3$
$\underline{28}$
$14 : 7 = 2 \quad q_4$

			q_0	q_1	q_2	q_3	q_4
q			1	1	1	2	2
c	0	1	1	2	3	8	19
d	1	0	1	1	2	5	12
$\frac{c}{d}$			$\frac{1}{1}$	$\frac{2}{1}$	$\frac{3}{2}$	$\frac{8}{5}$	$\frac{19}{12}$

$\frac{1}{1} < \frac{3}{2} < \frac{19}{12} < \frac{8}{5} < \frac{2}{1}$
$\qquad\qquad\quad \| \quad a$

$n = 4$, $r_n = 7$

$8 \cdot 84 - 5 \cdot 133 = 7$, denn

allgemein für $\frac{b}{a}$ mit $a > 0$:

$\frac{b}{a} = \frac{r_n b'}{r_n a'}$ $\quad b' = c_n$, $a' = d_n$. Nach F7 gilt

$d_n c_{n-1} - c_n d_{n-1} = (-1)^n$, wegen $b' = c_n$, $a' = d_n$ also

$c_{n-1} a' - d_{n-1} b' = (-1)^n$, mult. mit r_n

(45) $\boxed{c_{n-1} a - d_{n-1} b = (-1)^n r_n}$

Aus obigem Schema kann man also eine Lösung x, y der Gleichung

$x a + y b = d \qquad d = r_n$

direkt ablesen!

Ein ergiebiges Beispiel: Betrachte den Kettenbruch

$$\alpha = [1; 1, 1, 1, \ldots]$$

$c_n = q_n c_{n-1} + c_{n-2} = c_{n-1} + c_{n-2}$
$d_n = q_n d_{n-1} + d_{n-2} = d_{n-1} + d_{n-2}$ $\quad n = 0, 1, 2, \ldots$

c_{-2}	c_{-1}	c_0	c_1	c_2	$\ldots$
0	1	1	2	3	$\ldots$
d_{-1}	d_0	d_1	d_2	d_3	$\ldots$

$\boxed{u_n := d_{n-1} = c_{n-2}}$ $n \geq 0$

also

$d_n = u_{n+1}$, $c_n = u_{n+2}$

u_0	u_1	u_2	u_3	u_4	u_5	u_6	u_7	u_8	u_9	u_{10}	u_{11}	$\ldots$
0	1	1	2	3	5	8	13	21	34	55	89	$\ldots$

u_{12}	u_{13}	u_{14}	u_{15}	u_{16}	u_{17}	u_{18}	u_{19}	$\ldots\ldots$
144	233	377	610	987	1597	2584	4181	$\ldots\ldots$

Fibonacci = Leonardo von Pisa (1180? – 1250?)

$(u_n)_{n \geq 0}$ Folge der Fibonacci-Zahlen u_n n-te Fibonacci-Zahl

$$\boxed{u_{n+1} = u_n + u_{n-1} \quad n \geq 1 \quad ; \quad u_0 = 0, u_1 = 1}$$

$u_{n-1} = u_{n+1} - u_n$ $\qquad u_{-1} := u_1 - u_0 = 1$

u_n rekursiv für alle $n < 0$ definiert. Übrigens: Für $n < 0$ gilt $u_{-n} = (-1)^{n+1} u_n$ [für $n = 1$ ✓ Beweis durch Induktion]

$$\frac{u_{n+1}}{u_n} = \frac{c_{n-1}}{d_{n-1}} \qquad n \geq 1$$

(46) $$\begin{pmatrix} u_{n+2} \\ u_{n+1} \end{pmatrix} = \underbrace{\begin{pmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{pmatrix}}_{M_n} \begin{pmatrix} 1 \\ 1 \end{pmatrix} \quad \text{alle } n \in \mathbb{Z}.$$

(47) Für $n \geq 1$: $$\begin{pmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{pmatrix} = M_n \overset{(F7)}{=} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \cdots \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n$$

gilt auch für alle $n \leq 0$, ÜA

Wir wissen, daß $\frac{u_{n+1}}{u_n} = \frac{c_{n-1}}{d_{n-1}}$ gegen ein $\alpha \in \mathbb{R}$ konvergiert.

Berechnung von α: $\quad \xi_1 = \alpha$! $\quad \overset{\xi_1 > 0}{\Longrightarrow} \alpha > 0$

$$\alpha = q_0 + \frac{1}{\xi_1} = 1 + \frac{1}{\alpha} \quad , \Rightarrow$$

(48) $$\boxed{\alpha^2 - \alpha - 1 = 0} \quad , \Rightarrow \alpha = \tfrac{1}{2} \pm \sqrt{\tfrac{1}{4}+1} = \tfrac{1}{2} \pm \tfrac{1}{2}\sqrt{5}$$

Da $\alpha > 0$, folgt $\boxed{\alpha = \frac{1}{2} + \frac{1}{2}\sqrt{5}}$, somit

(49) $$\frac{1}{2} + \frac{1}{2}\sqrt{5} = [1; 1, 1, 1, \dots]$$

Die "andere Nullstelle" ist $\beta := \frac{1}{2} - \frac{1}{2}\sqrt{5}$, und es folgt $\alpha + \beta = 1$ sowie

(50) $$\alpha\beta = -1 \quad , \quad \beta = -\frac{1}{\alpha} \qquad (\Rightarrow |\beta| < 1)$$

Wegen $\alpha^2 = \alpha + 1$, $\beta^2 = \beta + 1$ ist $\alpha^{n+2} = \alpha^{n+1} + \alpha^n$, $\beta^{n+2} = \beta^{n+1} + \beta^n$, also

$$\begin{pmatrix} \alpha^{n+2} & \alpha^{n+1} \\ \beta^{n+2} & \beta^{n+1} \end{pmatrix} = \begin{pmatrix} \alpha^{n+1} & \alpha^n \\ \beta^{n+1} & \beta^n \end{pmatrix} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix} \overset{\text{ind.}}{=} \begin{pmatrix} \alpha & 1 \\ \beta & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n+1}$$

$$\overset{(47)}{=} \begin{pmatrix} \alpha & 1 \\ \beta & 1 \end{pmatrix} \begin{pmatrix} u_{n+2} & u_{n+1} \\ u_{n+1} & u_n \end{pmatrix}, \text{ mithin}$$

$$\begin{pmatrix} u_{n+2} & u_{n+1} \\ u_{n+1} & u_n \end{pmatrix} = \begin{pmatrix} \alpha & 1 \\ \beta & 1 \end{pmatrix}^{-1} \begin{pmatrix} \alpha^{n+2} & \alpha^{n+1} \\ \beta^{n+2} & \beta^{n+1} \end{pmatrix} = \frac{1}{\alpha - \beta} \begin{pmatrix} 1 & -1 \\ -\beta & \alpha \end{pmatrix} \begin{pmatrix} \alpha^{n+2} & \alpha^{n+1} \\ \beta^{n+2} & \beta^{n+1} \end{pmatrix}$$

$$= \frac{1}{\alpha - \beta} \begin{pmatrix} \alpha^{n+2} - \beta^{n+2} & * \\ * & * \end{pmatrix}, \Rightarrow u_{n+2} = \frac{\alpha^{n+2} - \beta^{n+2}}{\alpha - \beta}$$

Wegen $\alpha - \beta = \sqrt{5}$ erhalten wir die "endgültige Formel":

(51) $$\boxed{u_n = \frac{\alpha^n - \beta^n}{\sqrt{5}} = \frac{\left(\frac{1}{2} + \frac{1}{2}\sqrt{5}\right)^n - \left(\frac{1}{2} - \frac{1}{2}\sqrt{5}\right)^n}{\sqrt{5}}} \qquad n \geq 0$$

(gilt für alle $n \in \mathbb{Z}$)

Aus (46), (47) folgt:

$$\begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n-1} \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad \begin{pmatrix} u_{n+k+2} \\ u_{n+k} \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n+k-2} \begin{pmatrix} 1 \\ 1 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{k} \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{n-1} \begin{pmatrix} 1 \\ 1 \end{pmatrix} =$$

$$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^{k} \begin{pmatrix} u_{n+2} \\ u_n \end{pmatrix} = \begin{pmatrix} u_{k+1} & u_k \\ u_k & u_{k-1} \end{pmatrix} \begin{pmatrix} u_{n+1} \\ u_n \end{pmatrix}$$

somit

$$\begin{array}{rcl} u_{n+k} & = & u_k\, u_{n+1} + u_{k-1}\, u_n \\ \| & & \\ u_{k+n} & & \end{array}$$

F16: Für die "Folge" $(u_n)_{n\in\mathbb{Z}}$ der Fibonacci-Zahlen gilt u.a.:

(i) $\dfrac{u_{n+2}}{u_{n+1}}$ ist der n-te Näherungsbruch von $\alpha = [1;1,1,\ldots]$ $\quad n \geq -2$

(ii) $\alpha = \frac{1}{2} + \frac{1}{2}\sqrt{5}$

(iii) $u_n = \dfrac{\alpha^n - \beta^n}{\sqrt{5}}$ mit $\beta = \frac{1}{2} - \frac{1}{2}\sqrt{5}$ $\quad (n \in \mathbb{Z})$

(iv) $u_{m+n} = u_m\, u_{n+2} + u_{m-2}\, u_n$ $\quad (m, n \in \mathbb{Z})$

Für $m = n+2$:

(iv$_a$) $u_{2n-1} = u_n^2 + u_{n-1}^2$, z.B. $u_{19} = u_{10}^2 + u_9^2 = 55^2 + 34^2 = 4181$

[durch Determ.-bildung aus $\begin{pmatrix} u_{n+1} & u_n \\ u_n & u_{n-1} \end{pmatrix} = M_n = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}^n$]

(v) $u_{n+1}\, u_{n-1} - u_n^2 = (-1)^n$ bzw. [folgt auch aus F7(iii)]

(v') $u_n^2 = u_{n-1}\, u_{n+1} + (-1)^{n+1}$

etc.

Bem. u_n ist die zu $\frac{\alpha^n}{\sqrt{5}}$ nächstgelegene ganze Zahl. $(n \geq 0)$

Bew. $\left| \underbrace{\frac{\alpha^n - \beta^n}{\sqrt{5}} - \frac{\alpha^n}{\sqrt{5}}} \right| = \frac{|\beta|^n}{\sqrt{5}} \leq \frac{1}{\sqrt{5}} < \frac{1}{2}$

übrigens: konvergiert gegen 0 für $n \to \infty$.

$\frac{\alpha^{12}}{\sqrt{5}} = 144,00138\ldots$, $u_{12} = 144$

Wieviel Stellen hat u_n für $n = 1000$? Antwort: 209 Stellen

[Stellenzahl minus 1 von $\frac{\alpha^n}{\sqrt{5}}$ ist $\left[{}^{10}\log \frac{\alpha^n}{\sqrt{5}}\right] = \left[n\,{}^{10}\log\alpha - {}^{10}\log\sqrt{5}\right]$

für $n = 1000$: $[208,98\ldots - 0,349] = 208$, also hat $\frac{\alpha^{1000}}{\sqrt{5}}$ 209 Stellen.

u_{1000} hat die gleiche Stellenzahl, denn hier ist (da 1000 gerade!)

$$u_{1000} < \frac{\alpha^{1000}}{\sqrt{5}} < u_{1000} + \frac{1}{2} \qquad u_{1000} \in \mathbb{N}\,!$$]

F17. Für $a, b \in \mathbb{Z}$ gilt $(u_a, u_b) = u_{(a,b)}$, insb.

$a \mid b \Rightarrow u_a \mid u_b$.

Bew. ① $u_m \mid u_{xm}$ für alle $m, x \in \mathbb{Z}$.

$u_{-n} = (-1)^{n+1} u_n$

o.E. $m, x \in \mathbb{N}$. Ind. nach x: $x = 1$ ✓

$u_{(x+1)m} = u_{xm+m} \overset{F16}{=} u_{xm} \cdot u_{m+1} + u_{xm-1} u_m$ teilbar durch u_m.

② Sei $d = (a,b)$. Aus ① folgt $u_d \mid u_a$, $u_d \mid u_b$, also $u_d \mid (u_a, u_b)$.

$d = xa + yb$ mit $x, y \in \mathbb{Z}$. Es folgt

(*) $u_d = u_{xa+yb} = u_{xa} u_{yb+1} + u_{xa-1} u_{yb}$

Sei nun c ein gem. Teiler von u_a, u_b. z.Z. $c \mid u_d$

Klar nach (*) wegen ①.

Bem. u_n Primzahl $\overset{F17}{\Longrightarrow}$ n Primzahl (≥ 3), mit Ausnahme von $n=4$: $u_4 = 3$.

Frage: p Primzahl >2 $\Longrightarrow$ u_p Primzahl? Nein!

u_3	u_5	u_7	u_{11}	u_{13}	u_{17}	mit Primzahlen,
2	5	13	89	233	1597	

aber $u_{19} = 4181 = 37 \cdot 113$ keine Primzahl!

Auch $u_{31} = 557 \cdot 2417 = 1.346.269$ keine Primzahl.

$u_{23} = 28657$ ist Primzahl

Probleme: Gibt es unendlich viele Fibonacci-Primzahlen?
Ist u_p für unendlich viele Primzahlen p keine Primzahl?

§3 Kongruenzrechnung

Zur Motivation:

Satz 1 (Fermat): p Primzahl. Für jede ganze Zahl a mit $p \nmid a$ gilt dann

$$p \mid a^{p-1} - 1 ,$$

d.h. a^{p-1} läßt bei Division durch p stets den Rest 1.

z.B. $17 \mid 2^{16} - 1$ $\qquad$ $89 \mid 89093^{88} - 1$

Beweis: $M_1 = \{1, 2, \ldots, p-1\}$. Für jedes $k \in M$ ist

(*) $\quad ak = q_k p + r_k$ mit $r_k \in M$ (denn $r_k \neq 0$)

Beh. $M = \{r_1, r_2, \ldots, r_{p-1}\}$ **q.z.z.** $r_j \neq r_k$ für $j \neq k$.

Sei $r_k = r_j$ und o.E. $k > j$. Es folgt $a(k-j) = (q_k - q_j)p$,

$\overset{p \text{ prim}}{\underset{p \nmid a}{\Longrightarrow}}$ $p \mid k-j$, $\overset{0 \leq k-j < p}{\Longrightarrow}$ $k = j$.

Jetzt: $\underbrace{(p-1)!}_{} = \prod_{k \in M} k \overset{!}{=} \prod_{k \in M} r_k = \prod_{k=1}^{p-1} (ak - q_k p) =$

$$\prod_{k=1}^{p-1} (ak) + cp \quad \text{mit einem } c \in \mathbb{Z} \qquad = \quad a^{p-1} \prod_{k=1}^{p-1} k + cp = \underbrace{a^{p-1}(p-1)! + cp}_{},$$

$$\Rightarrow \; p \mid a^{p-1}(p-1)! - (p-1)! , \; \Rightarrow p \mid (p-1)!(a^{p-1} - 1) \overset{p \text{ prim}}{\Longrightarrow}$$

$$p \mid a^{p-1} - 1 \qquad \text{q.e.d.}$$