Anhang: Chebyshev-Polynome und Lucas-Folgen

Vorbemerkung: *Pafnuti Lwowitsch Tschebyschow* (1821-1894) war ein russischer Mathematiker, dessen Name an verschiedenen Stellen auftaucht. Hier wird die englische Schreibweise *Chebyshev* verwendet, es finden sich aber auch eine Reihe anderer Schreibweisen: Tchebychev, Čebyšev, Tchebychef, Tchebycheff, Tchebychev, Tschebyschef, Tschebyscheff, Tschebyschew, Tschebyschow. (Die letzte Schreibweise ist die aktuelle wissenschaftliche Transliteration.)

Die **Chebyshev-Polynome 1. Art** $T_n(x)$ werden rekursiv durch

$$T_0(x) = 1, \quad T_1(x) = x \quad \text{und} \quad T_n(x) = 2xT_{n-1}(x) - T_{n-2}(x) \text{ für } n \geq 2$$

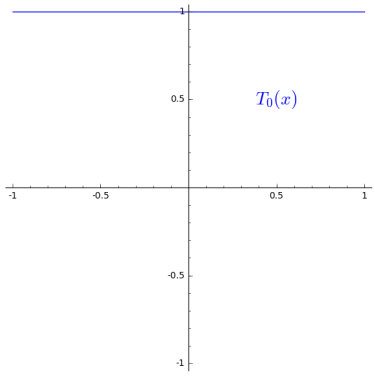
definiert. Die **Chebyshev-Polynome 2. Art** $U_n(x)$ werden durch

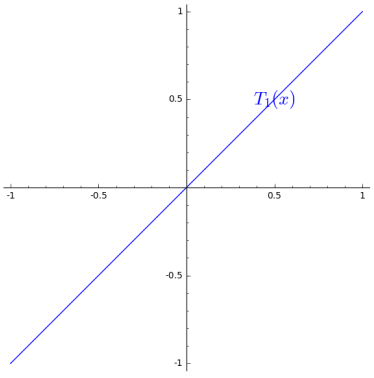
$$U_0(x) = 1, \quad U_1(x) = 2x, \quad U_n(x) = 2xU_{n-1}(x) - U_{n-2}(x) \text{ für } n \geq 2$$

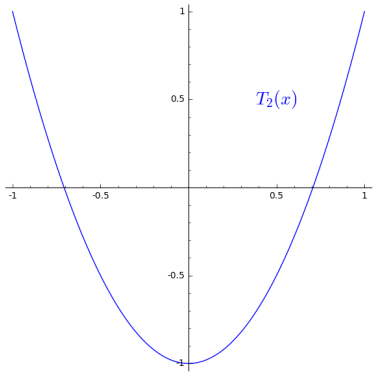
rekursiv definiert. SAGE kennt dafür die Befehle `chebyshev_T(n,x)` und `chebyshev_U(n,x)`. Wir werden hier aber nur die Polynome $T_n(x)$ betrachten. Die ersten 10 Polynome $T_n(x)$ sind:

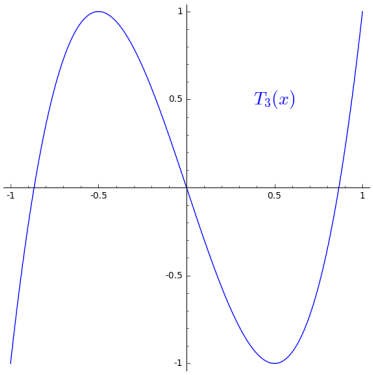
n	$T_n(x)$
0	1
1	x
2	$2x^2 - 1$
3	$4x^3 - 3x$
4	$8x^4 - 8x^2 + 1$
5	$16x^5 - 20x^3 + 5x$
6	$32x^6 - 48x^4 + 18x^2 - 1$
7	$64x^7 - 112x^5 + 56x^3 - 7x$
8	$128x^8 - 256x^6 + 160x^4 - 32x^2 + 1$
9	$256x^9 - 576x^7 + 432x^5 - 120x^3 + 9x$

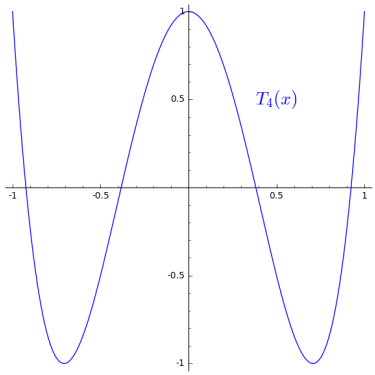
Man kann die Chebyshev-Polynome über einem beliebigen Körper betrachten.
Für die reellen Polynome erhält man folgende Bilder im Intervall $[-1, 1]$:

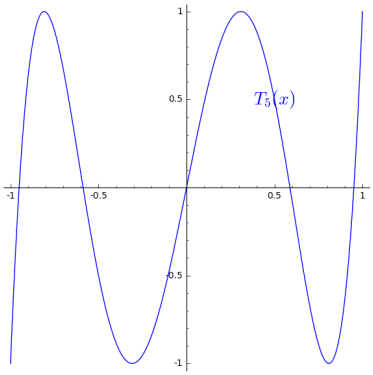


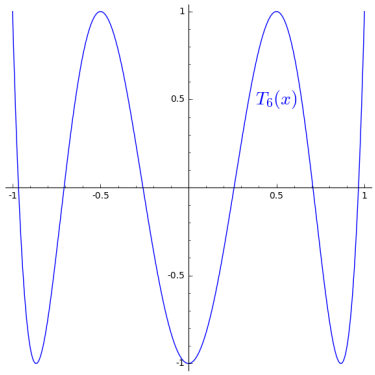


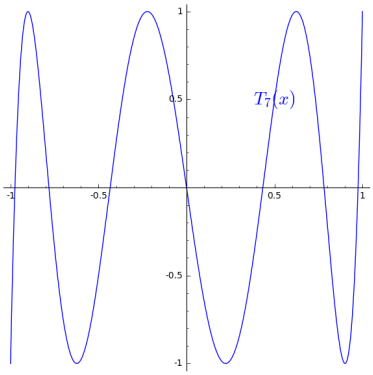

$T_2(x)$

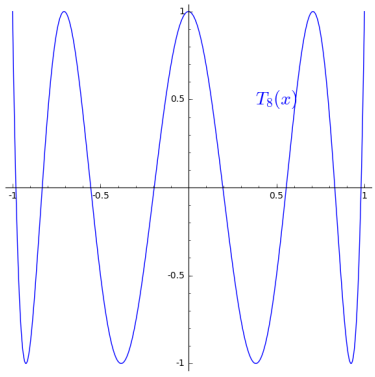

$T_3(x)$

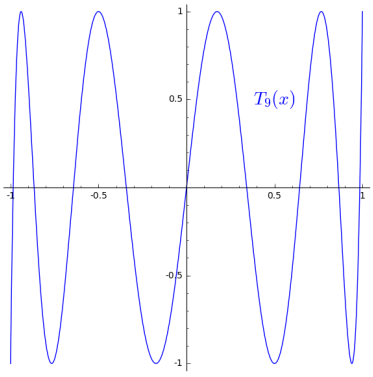

$T_4(x)$


$T_5(x)$

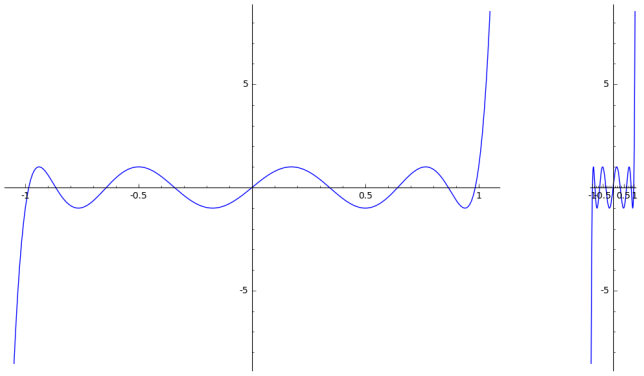

$T_6(x)$


$T_7(x)$


$T_8(x)$


$T_9(x)$

Die folgenden Bilder zeigen $T_9(x)$ im Intervall $[-1.05, 1.05]$, einmal nicht maßstabsgetreu, das zweite Mal maßstabsgetreu:



Die Chebyshev-Polynome haben eine Vielzahl interessanter Eigenschaften, von denen wir aber nur einige erwähnen. Das folgende Lemma stellt einen Zusammenhang zu den Lucas-Folgen her:

LEMMA. *Für die Lucas-Folge $V_n(P,Q)$ mit $P = 2x$ und $Q = 1$ gilt*

$$T_n(x) = \frac{1}{2}V_n(2x, 1).$$

Beweis: Es gilt $V_0(P,Q) = 2$, $V_1(P,Q) = P$ und

$$V_n(P,Q) = PV_{n-1}(P,Q) - QV_{n-2}(P,Q) \text{ für } n \geq 2.$$

Wir beweisen die Behauptung durch Induktion. Für $n = 0$ und $n = 1$ ist

$$T_0(x) = 1 = \frac{1}{2}V_0(2x, 1) \quad \text{und} \quad T_1(x) = x = \frac{1}{2}V_1(2x, 1).$$

Gilt die Aussage bereits für $n-2$ und $n-1$, so folgt

$$\begin{aligned} T_n(x) &= 2xT_{n-1}(x) - T_{n-2}(x) = 2x \cdot \frac{1}{2}V_{n-1}(2x,1) - \frac{1}{2}V_{n-2}(2x,1) = \\ &= \frac{1}{2}\left(2xV_{n-1}(2x,1) - V_{n-2}(2x,1)\right) = \frac{1}{2}V_n(2x,1), \end{aligned}$$

was die Behauptung nun durch Induktion beweist. ■

SATZ. *Für $m, n \geq 0$ gilt*

$$T_m(T_n(x)) = T_{mn}(x).$$

Beweis: Wir wissen, dass gilt

$$V_{mn}(P,Q) = V_m(V_n(P,Q), Q^m),$$

woraus für $Q = 1$

$$V_{mn}(P,1) = V_m(V_n(P,1),1)$$

folgt. Mit dem letzten Lemma erhalten wir

$$\begin{aligned} T_m(T_n(x)) &= \frac{1}{2}V_m(2 \cdot T_n(x), 1) = \frac{1}{2}V_m(V_n(2x,1),1) = \\ &= \frac{1}{2}V_{mn}(2x,1) = T_{mn}(x), \end{aligned}$$

wie behauptet. ■

LEMMA. *Ist K ein Körper der Charakteristik $\neq 2$ und $u \in K^*$, so gilt für $n \geq 0$*

$$T_n(\frac{1}{2}(u + \frac{1}{u})) = \frac{1}{2}(u^n + \frac{1}{u^n}).$$

Beweis: Nach dem letzten Lemma gilt

$$T_n(\frac{1}{2}(u+\frac{1}{u})) = \frac{1}{2}V_n(u+\frac{1}{u},1).$$

Wegen $x^2-(u+\frac{1}{u})x+1 = (x-u)(x-\frac{1}{u})$ sind u und $\frac{1}{u}$ die Nullstellen des Polynoms $x^2-(u+\frac{1}{u})x+1$, sodass gilt

$$V_n(u+\frac{1}{u},1) = u^n + (\frac{1}{u})^n.$$

Damit ergibt sich

$$T_n(\frac{1}{2}(u+\frac{1}{u})) = \frac{1}{2}V_n(u+\frac{1}{u},1) = \frac{1}{2}(u^n+\frac{1}{u^n}),$$

wie behauptet. ■

SATZ. *Für $K=\mathbb{R}$ und $\varphi\in\mathbb{R}$ gilt für alle $n\in\mathbb{N}_0$*

$$\cos(n\varphi) = T_n(\cos\varphi).$$

Beweis: Wir wenden das letzte Lemma für $K=\mathbb{C}$ auf $u=e^{i\varphi}$ an:

$$T_n(\cos\varphi) = T_n(\frac{1}{2}(e^{i\varphi}+e^{-i\varphi})) = \frac{1}{2}(e^{in\varphi}+e^{-in\varphi}) = \cos(n\varphi). \quad ■$$

Beispielsweise ist

$$\begin{aligned}\cos(2\varphi) &= T_2(\cos\varphi) = 2(\cos\varphi)^2-1\\ \cos(3\varphi) &= T_3(\cos\varphi) = 4(\cos\varphi)^3-3\cos\varphi.\end{aligned}$$

Der Satz liefert eine Charakterisierung der Chebyshev-Polynome über den reellen Zahlen.

Mit der folgenden Formel kann man die Chebyshev-Polynome für kryptographische Anwendungen schnell auswerten:

SATZ. *Für $n\geq 0$ gilt*

$$\begin{pmatrix} T_n(x)\\ T_{n+1}(x)\end{pmatrix} = \begin{pmatrix}0 & 1\\ -1 & 2x\end{pmatrix}^n \begin{pmatrix}1\\ x\end{pmatrix}.$$

Beweis: Dies beweist man durch Induktion. Der Induktionsanfang $n=0$ folgt aus der Definition. Der Schluss von n auf $n+1$ ergibt sich aus der Rekursionsformel:

$$\begin{aligned}\begin{pmatrix} T_{n+1}(x)\\ T_{n+2}(x)\end{pmatrix} &= \begin{pmatrix} T_{n+1}(x)\\ 2xT_{n+1}(x)-T_n(x)\end{pmatrix} = \begin{pmatrix}0 & 1\\ -1 & 2x\end{pmatrix}\begin{pmatrix} T_n(x)\\ T_{n+1}(x)\end{pmatrix} =\\ &= \begin{pmatrix}0 & 1\\ -1 & 2x\end{pmatrix}\begin{pmatrix}0 & 1\\ -1 & 2x\end{pmatrix}^n\begin{pmatrix}1\\ x\end{pmatrix} = \begin{pmatrix}0 & 1\\ -1 & 2x\end{pmatrix}^{n+1}\begin{pmatrix}1\\ x\end{pmatrix}.\end{aligned}$$

Dies beweist den Satz. ■