

Formelsammlung MP4-IT3

Geometrische Folgen:

Kennzeichen: Jedes Glied ist um einen konstanten Faktor q ($q > 0$) grösser (wenn $q > 1$) oder kleiner (wenn $q < 1$) als das vorherige Glied.

Explizite Darstellung: $a_n = a_1 \cdot q^{n-1}$

Rekursive Darstellung: $a_1 = \dots, a_n = q \cdot a_{n-1}$

Quotient a_n/a_j : $a_n/a_j = q^{n-j}$ Bsp.: $a_{17}/a_{11} = q^{17-11} = q^6$
 $\rightarrow q = \sqrt[6]{a_{17}/a_{11}}$

Exponentielles Wachstum (od. Zerfall, wenn $q < 1$):

(Zinsezins)

$$X_n = X_0 \cdot q^n,$$

Wobei $q = 1 \pm \frac{p}{100}$

(beginnt bei null!)
 $n =$ Anzahl Wachstumsperioden

z. B. 5% Wachstum $\rightarrow q = 1 + 5/100 = 1.05$ od
 6% Abnahme $\rightarrow q = 1 - 6/100 = 0.94$

Unterjährigere Verzinsung: Es sei m die Anzahl Zinsperioden pro Jahr und p sei der Nominalzins (p.a.), dann

- ▶ Zinssatz durch m dividieren
- ▶ Anzahl Zinsperioden mit m multiplizieren

Merke: X_n ist der Kontostand (eines ruhenden Guthabens). Der Zins ist

$$Z_n = X_n - X_0 = X_0 [q^n - 1]$$

Potenzgleichungen: $a \cdot x^n = b \rightarrow x = \sqrt[n]{b/a}$, z. B.
 $3 \cdot x^5 = 11 \rightarrow x = \sqrt[5]{11/3} = 1.2967$

Exponentialgleichungen: $c \cdot a^x = b \Leftrightarrow x = \frac{\log(b/c)}{\log a}$

z.B. $3 \cdot 2^x = 5 \Leftrightarrow x = \log(5/3) / \log 2 = 0.7370$

Umformung: $c \cdot a^x = d \cdot b^x \rightarrow (a/b)^x = d/c \Leftrightarrow$
 $x = \log(d/c) / \log(a/b)$

Punkte auf der Secp256k1 (Bitcoin):

$$y^2 = x^3 + 7$$

Geg. $x \rightarrow y = \pm \sqrt{x^3 + 7}$ zwei Lösungen!

Geg. $y \rightarrow x = \sqrt[3]{y^2 - 7} = (y^2 - 7)^{1/3}$

Punkte addieren:

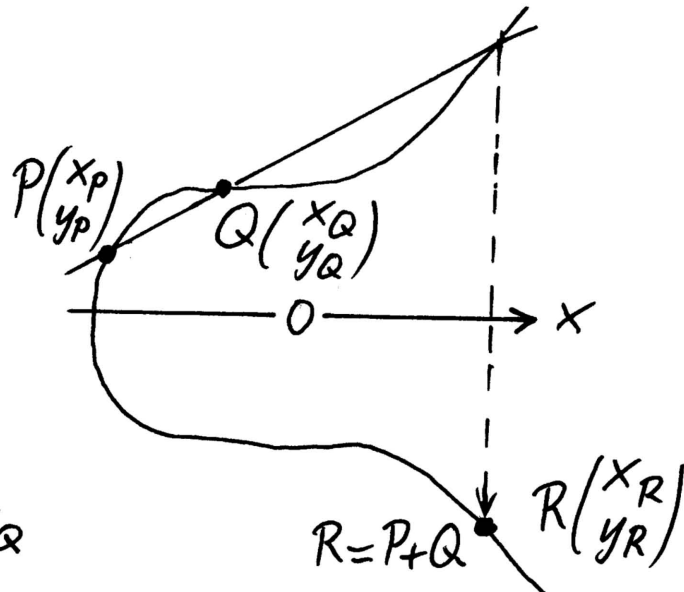
$$m = \frac{y_Q - y_P}{x_Q - x_P}$$

$$x_R = m^2 - x_P - x_Q$$

$$y_R = m(x_P - x_R) - y_P$$

oder

$$y_R = m(x_Q - x_R) - y_Q$$



Skalare Multiplikation von Punkten: (Nur Verdoppelung, d.h. $P+P$)

$$m = \frac{3x_P^2}{2y_P}$$

$$x_R = m^2 - 2x_P$$

$$y_R = m(x_P - x_R) - y_P$$

