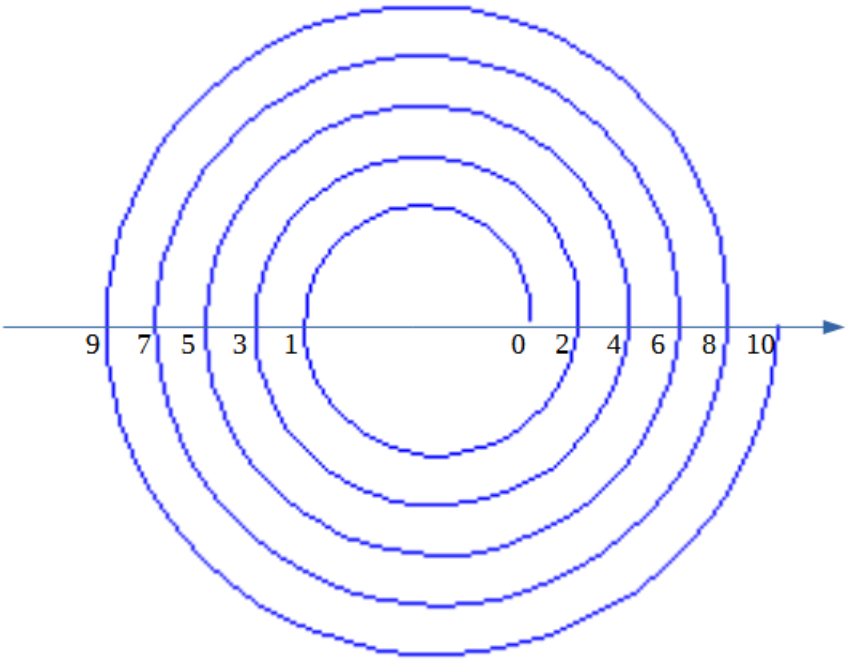
Modulrechnung



Anzahl der vollen Zyklen ↓ | modulo ↓ | Rest ↓

$$\begin{pmatrix} 1= & 0 & \cdot & 2 & + & 1 \\ 2= & 1 & \cdot & 2 & + & 0 \\ 3= & 1 & \cdot & 2 & + & 1 \\ 4= & 2 & \cdot & 2 & + & 0 \\ 5= & 2 & \cdot & 2 & + & 1 \end{pmatrix}$$

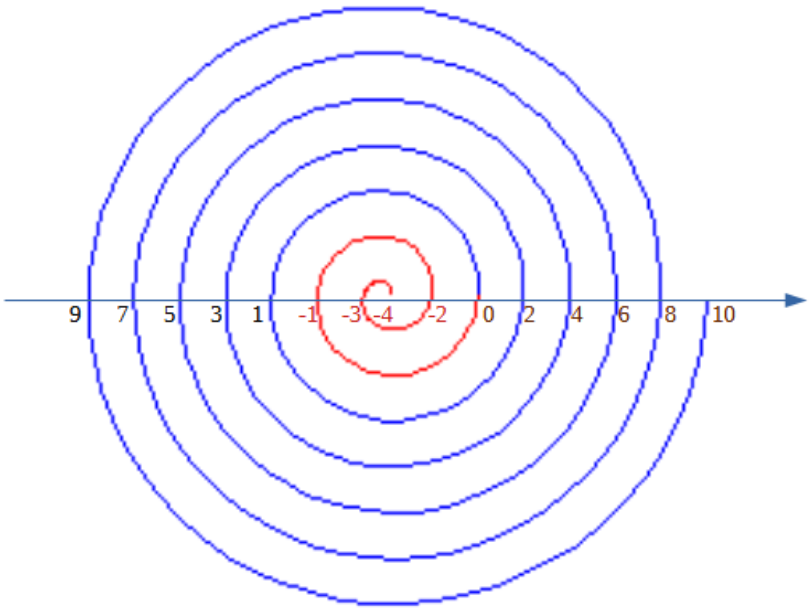
Hier gibt es zwei **Restklassen** (das, was zum vollen Zyklus fehlt bzw. allgemeiner, was über den vollen Zyklus hinausweist als Anfang einer neuen Vollendung) **modulo 2**:

Die Restklasse, die die Zahl 0 enthält: $[0]=\{0,2,4,6,8,10,12,...\}=[2]=[4]=[6]=...$
und die Restklasse, die die 1 enthält: $[1]=\{1,3,5,7,9,11,13,...\}=[3]=[5]=[7]=...$

Man sieht auch, dass zwei Zahlen a und b in die gleiche Restklasse gehören, wenn ihre Differenz ein Vielfaches von 2 ist: $10-4=6=3\cdot 2$, also $10-4$ ist das Dreifache von 2 und 10 und 4 gehören also zur gleichen Klasse: $[10]=[0]$ und $[4]=[0]$ Oder $9-5=4=2\cdot 2$, also gehören 9 und 5 in die gleiche Restklasse, also $[9]=[1]=[5]$. Aber $12-7=5$ ist kein Vielfaches von 2, gehören also zu verschiedenen Restklassen: $[12]=[0]\neq[7]=[1]$.

Diese Rechnung wird auch auf negative ganze Zahlen erweitert, indem man nicht mit Null anfängt, sondern mit beliebigen negativen Zahlen:

$$\begin{pmatrix} 0=\ 0\cdot 2+0 \\ -1=-1\cdot 2+1 \\ -2=-1\cdot 2+0 \\ -3=-2\cdot 2+1 \\ -4=-2\cdot 2+0 \\ -5=-3\cdot 2+1 \end{pmatrix}$$



$[-1]=[1]$, da auch hier der Unterschied ein Vielfaches (Einfaches) von 2 ist: $1-(-1)=1+1=2$

$[-2]=[0]$, $0-(-2)=0+2=2$

$[-3]=[1]$, $1-(-3)=1+3=4=2\cdot 2$

$[-4]=[0]$, $0-(-4)=4=2\cdot 2$

$[-5]=[1]$, $1-(-5)=1+5=6=3\cdot 2$.

Man hat gesehen, dass die Menge $[1]=\{\ldots,-9,-7,-5,-3,-1,1,3,5,7,9,\ldots\}$ aus allen ganzen Zahlen besteht, die bei der Division durch 2 den gleichen Rest 1 ergeben:

$3/2=1$ (Rest 1) oder schöner in ganzen Zahlen und als richtige Gleichung geschrieben $3=1\cdot 2+1$
$5/2=1$ (Rest 1) oder eben $5=2\cdot 2+1$
$-7/2=1$ (Rest 1) oder $-7=-4\cdot 2+1$ usw.

Man schreibt die Menge auch als $\mathbb{Z}\cdot 2+1$ (oder wie üblich $1+2\mathbb{Z}$), da sich alle Zahlen dieser Menge in der Form $z\cdot 2+1$ darstellen lassen mit einem jeweils passenden $z\in\mathbb{Z}$. So ist bei -7 die passende ganze Zahl -4: $-7=-4\cdot 2+1$.

Man sagt, zwei Zahlen $n_1, n_2\in\mathbb{Z}$ seien **äquivalent**, wenn sie zu dieser Menge $1+2\mathbb{Z}$ gehören und man schreibt: $n_1\equiv_{(2)} n_2 \Leftrightarrow n_1\in 1+2\mathbb{Z}\wedge n_2\in 1+2\mathbb{Z}\Leftrightarrow n_1\equiv n_2\ \ (mod\ 2)\Leftrightarrow \bigvee_{k\in\mathbb{Z}} n_1-n_2=k\cdot 2$.

Allgemein nennt man zwei Objekte a und b äquivalent, wenn ihre Beziehung R (geschrieben aRb oder $(a,b)\in\mathbb{R}$) symmetrisch ($aRb\Leftrightarrow bRa$, transitiv ($a\,Rb, bRc\Rightarrow aRc$ für jedes weitere Objekt c) und reflexiv (aRa) ist.

Das trifft auf obige Relation zu: Symmetrie ist klar, da $\wedge$ symmetrisch; Transitivität:
$n_1\equiv n_2\wedge n_2\equiv n_3\Rightarrow n_1-n_2=k_1\cdot 2\wedge n_2-n_3=k_2\cdot 2\Rightarrow n_1-n_3=(n_1-n_2)+(n_2-n_3)=k_1\cdot 2+k_2\cdot 2=(k_1+k_2)\cdot 2\Rightarrow n_1\equiv n_3$
und Reflexivität: $n\equiv n\Leftrightarrow n-n=0\cdot 2$.

Allgemein ist eine Restklasse zu n modulo $m\neq 0$ die Menge aller ganzer Zahlen z , die bei der Division durch m den gleichen Rest n ergeben:

$$[n]_m=\{\ z\in Z/\ \bigvee_{k\in\mathbb{Z}} z=n+km\ \}=\{\ z\in Z/\ \text{z} \equiv \text{n (mod m)}\ \}=n+m\mathbb{Z}$$

Die **Menge aller Restklassen modulo m** wird mit $\mathbb{Z}/m\mathbb{Z}=\mathbb{Z}_m$ bezeichnet.

Modulo 2 gibt es genau 2 Restklassen: $\mathbb{Z}_2=\{\ [0]_2,[1]_2\ \}$, die Menge die aus der Restklasse aller geraden Zahlen und die aller ungeraden Zahlen besteht. Die ganzen Zahlen werden also durch die Restklassen (disjunkt) zerlegt: $\mathbb{Z}=[0]_2\cup[1]_2$.

Modulo 3 gibt es genau 3 Restklassen: $\mathbb{Z}_3=\{\ [0]_3,[1]_3,[2]_3\}$
$[0]_3=\{\ ...,-12,-9,-6,-3,0,3,6,9,12,...\}$ die durch 3 teilbaren Zahlen ohne Rest (Rest 0),
$[1]_3=\{\ ...,-14,-11,-8,-5,-2,1,4,7,10,13,...\}$
$[2]_3=\{\ ...,-13,-10,-7,-4,-1,2,5,8,11,14,...\}$

Also auch hier gilt, dass $\mathbb{Z}=[0]_3\cup[1]_3\cup[2]_3$ in diese drei Restklassen zerlegt wird.

Allgemein werden die ganzen Zahlen bzgl. jedem Modul m in Restklassen zerlegt:

$$\mathbb{Z}=[0]_m\cup[1]_m\cup...\cup[m-1]_m$$

Um die Struktur der ganzen Zahlen auf die Restklassen zu übertragen, kann man nun versuchen eine **Addition von zwei Restklassen** zu definieren:

Ansatz: $[x]+[y]:=[x+y]$, also beim Modul 2:

$[0]+[0]:=[0+0]=[0]$
$[0]+[1]:=[0+1]=[1]$

$[1]+[0]:=[1+0]=[1]$

$[1]+[1]:=[1+1]=[2]=[0]$

Oder wenn man es in einer **Tabell**e übersichtlich zusammenfassen will:

+	[0]	[1]
[0]	[0]	[1]
[1]	[1]	[0]

Damit wird bspw. folgendermaßen gerechnet:

$[5]+[10]=[5+10]=[15]=[1]$ oder auch $[5]+[10]=[1]+[0]=[1]$

$[-5]+[2]=[-5+2]=[-3]=[1]$ und $[-1]+[-3]=[-1+(-3)]=[-4]=[0]$

Man nennt die Klasse $[0]$ das bezüglich der Addition **neutrale Element** oder **Nullelement**, da die Addition mit $[0]$ nichts verändert: $[0]+[0]=[0]$, $[1]+[0]=[1]$.

Ergibt die Addition zweier Klassen die Klasse $[0]$, also $[0]+[0]=[0]$ oder $[1]+[1]=[0]$, dann nennt man die rote Klasse die bzgl. der Addition inverse Klasse, sozusagen die Minusklasse der links stehenden schwarzen Klasse. Also hier (nicht sehr schön) $[0]=-[0]$ und $[1]=-[1]$. Die Klasse Null ist also ihr eigenes Inverses und ebenso ist die Klasse Eins ihr eigenes Inverses. Das ist bei anderen Modulen schöner. Holt man bspw. modulo 3:

$\ldots,-3,-2,-1,0,1,2,3,4,5,6,7,8,9,10,11,12,13,14,15,16,\ldots$

Zur Klasse 0 gehören $[0]=\{\ \ldots,-6,-3,0,3,6,9,12,15,\ldots\}=[-6]=[-3]=[3]=[6]=\ldots$
Zur Klasse 1 gehören $[1]=\{\ \ldots,-2,1,4,7,10,13,16,\ldots\}=[-2]=[4]=[7]=\ldots$
Zur Klasse 2 gehören $[2]=\{\ -4,-1,2,5,8,11,14,\ldots\}=[-4]=[5]=[8]=\ldots$

Ist die Differenz zweier Zahlen ein Vielfaches von 3, dann gehören sie zur gleichen Restklasse.
Man definiert wieder analog die Addition zweier Restklassen

$[a]+[b]:=[a+b]$, also

$[0]+[0]:=[0+0]=[0]$
$[0]+[1]:=[0+1]=[1]$
$[0]+[2]:=[0+2]=[2]$
$[1]+[0]:=[1+0]=[1]$
$[1]+[1]:=[1+1]=[2]$
$[1]+[2]:=[1+2]=[3]=[0]$
$[2]+[0]:=[2]$
$[2]+[1]:=[3]=[0]$
$[2]+[2]:=[4]=[1]$

oder wieder mit einer Tabelle:

+	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

Ergibt eine Summe wieder das neutrale Element $[0]$ wie bei $[1]+[2]=[0]$, dann ist $[2]$ das Inverse zu $[1]$: $[2]=-[1]$ etc. Hier ist das Inverse eine andere Klasse und nicht wie bei modulo 2 die gleiche. Praktisch eine Befreiung aus dem Solipsismus :)

Man versucht nun auch eine **Multiplikation** bzgl. zweier Klassen einzuführen.
Es liegt nahe, das wie bei der Addition zu machen: $[a]\cdot[b]:=[a\cdot b]$, also bei den Restklassen modulo 2:

$[0]\cdot[0]:=[0\cdot 0]=[0]$
$[0]\cdot[1]:=[0]$
$[1]\cdot[0]:=[0]$
$[1]\cdot[1]:=[1]$

Tabelle:

$\cdot$	$[0]$	$[1]$
$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$

Das neutrale Element bei der Multiplikation ist $[1]$, da sie nichts verändert: $[1]\cdot[a]=[a]$.

Ist das Produkt zweier Klassen $[1]$, also das neutrale Element, dann ist mit $[a]\cdot[b]=[1]$, $[b]$ das Inverse von $[a]$bzgl. der Multiplikation $[b]$ und das Inverse von $[b]$ eben auch $[a]$.
Hier ist also wieder $[1]$ das Inverse von sich selbst.

Bei den Restklassen modulo 3 gebe ich gleich die Tabelle an:

$\cdot$	$[0]$	$[1]$	$[2]$
$[0]$	$[0]$	$[0]$	$[0]$
$[1]$	$[0]$	$[1]$	$[2]$
$[2]$	$[0]$	$[2]$	$[1]$

Hier hat man wieder Inverse, aber auch nur selbstinvers: $[1]\cdot[1]=[1]$, $[2]\cdot[2]=[1]$. Man schreibt auch wie bei den reellen oder rationalen Zahlen für das Inverse bzgl. der Multiplikation:

$3\cdot\frac{1}{3}=1$, also ist 1/3 das Inverse zu 3 und umgekehrt. Man schreibt für das Inverse auch $\frac{1}{3}=3^{-1}$.

So kann man das auch bei Restklassen machen: $[2]^{-1}=[2]$ ist das Inverse von $[2]$. Und $[1]^{-1}=[1]$

Ein Beispiel für Restklassen modulo 3: $[4]\cdot[5]=[1]\cdot[2]=[2]$ oder $[4]\cdot[5]=[20]=[2]$, da $20-2=18=6\cdot 3$, also ein Vielfaches von 3. 20 und 2 gehören also zur gleichen Restklasse modulo 3.
Die Menge $\mathbb{Z}_2$ aller Restklassen modulo 2 bzw. die Menge $\mathbb{Z}_3$ aller Restklassen modulo 3 mit der Addition und Multiplikation bilden einen **kommutativen Ring mit Einselement** $[1]$, den sogenannten Restklassenring, ja sogar einen **kommutativen Körper**. Letzteres gilt für alle Mengen $\mathbb{Z}_p$ der Restklassen mit Primzahlmodul p (wie 2 und 3).

Lineare diophantische Gleichungen mit zwei Variablen

Bsp1: $17m=5n+3,\ m,n\in\mathbb{Z}$

Man zerlegt 17 in Vielfaches von 5 + Rest: $17=3\cdot 5+2$; $(17\in[2]_5)$

$(3\cdot 5+2)m=5n+3\Leftrightarrow 5(\underbrace{3m-n}_{=:r})=3-2m\Leftrightarrow 5r=3-2m\ \ (*)\wedge 3m-n=r$

Man zerlegt wieder $5=2\cdot 2+1$:

$(*)\Leftrightarrow(2\cdot 2+1)r=3-2m \Leftrightarrow 2(\underbrace{2r+m}_{=:s})=3-r\Leftrightarrow r=3-2s(**)\wedge s=2r+m$

Setzt $s:=1\Rightarrow r=3-2=1\Rightarrow m=s-2r=1-2=-1\Rightarrow$ wegen $3m-n=r:-3-n=1\Rightarrow n=-4$

Also hat man die Lösung $m=-1\wedge n=-4$.

Alle anderen Lösungen erhält man indem man $m=-1\pm k\cdot 5,\ k\in\mathbb{Z}$ und $n=-4\pm 17\cdot k$ setzt,

denn sind m_0 und n_0 Lösungen von der obigen Gleichung: $17m_0=5n_0+3$, so gilt

$17(m_0\pm 5k)=5(n_0\pm 17k)+3\Leftrightarrow 17m_0\pm 17\cdot 5k=5n_0\pm 5\cdot 17k+3\Leftrightarrow 17m_0=5n_0+3$, also sind

mit m_0 und n_0 auch $m_0\pm 5k$ und $n_0\pm 17k$ Lösungen der Gleichung.

Will man also nur Lösungen aus $\mathbb{N}$, so addiert man zu -1 5 und zu -4 17: $m_1=4,\ n_1=13$.

Probe: $17\cdot 4=5\cdot 13+3$ oder $68=68$.

Allgemein (noch ungefähr): Hat man eine diophantische Gleichung $a\cdot m=b\cdot n+c$ mit den gesuchten Zahlen m,n und ist oBdA $a>b$, sonst stellt man um, falls $a<b: b\cdot n=a\cdot m-c$ und argumentiert wie oben. Ist $a=b$ und ist c nicht durch a teilbar, gibt es keine Lösung, ist c aber teilbar durch a, also $c=a\cdot d$, dann lautet die Gleichung $m=n+d$ und die Lösungsmenge ist somit klar.

Im erstgenannten Fall zerlegt man: $a=s\cdot b+r$ und erhält $b(\underbrace{sm-n}_{\alpha})=c-rm\Rightarrow b\cdot\alpha=-rm+c$

Diese Gleichung ist von gleicher Art wie die Ausgangsgleichung mit $b<a$ und $r<b$. Man wiederholt diesen Prozess (endlich viele Schritte) bis man bei einer Gleichung ist, bei der nach einer Variablen aufgelöst ist. Entweder ist diese Gleichung lösbar oder nicht. Falls diese Gleichung lösbar ist, setzt man die zweite Variable 1 und berechnet rückwärts alle eingeführten Variablen bis man m und n hat. Mit m und n sind dann auch $m+k\cdot b$ und $n+k\cdot a,\ k\in\mathbb{Z}$ Lösungen.

Bsp2: $5m=\frac{4}{5}\left[\frac{4}{5}(n-1)-1\right]\Rightarrow 500m=16n-36\Rightarrow 125m=4n-9\Rightarrow(31\cdot 4+1)m=4n-9\Rightarrow$
$\Rightarrow 4(\underbrace{31m-n}_{\alpha})=-m-9\Rightarrow 4\alpha=-m-9\Rightarrow m=-4\alpha-9,\ \alpha:=1\Rightarrow m=-13\Rightarrow 31\cdot(-13)-n=1\Rightarrow$
$\Rightarrow n=-404, m=-13$. Positive Lösungen: $n=-404+4\cdot 125=96$ und $m=-13+4\cdot 4=3$.

Bsp3: Der Affe und die Kokosnüsse (von Martin Gardner):
Fünf Piraten und ein Affe erleiden Schiffbruch und stranden auf einer Insel. Die Seeleute verbringen ihren Tag damit Kokosnüsse zu sammeln. Nachts wacht einer misstrauisch auf und holt sich seinen Anteil, d.h. er teilt die Nüsse in fünf gleichgroße Haufen und da eine übrig bleibt, legt er sie für den Affen beiseite. Kurz danach macht ein zweiter Pirat das Gleiche, d.h. er teilt den Rest in fünf Teile und abermals bleibt eine Nuss übrig, die er ebenfalls dem Affen zuteilt. Und so geht es weiter bis zum fünften Piraten, ebenfalls mit einer übrigen Kokosnuss für den Affen. Am Morgen teilen sie die noch übrig gebliebenen Nüsse in fünf gleiche Teile, diesmal aber ohne Rest. Wieviele Kokosnüsse hatten sie gesammelt?

$$\frac{5}{4}\left(\frac{5}{4}\left(\frac{5}{4}\left(\frac{5}{4}\left(\frac{5}{4}\cdot 5m+1\right)+1\right)+1\right)+1\right)+1=n\Rightarrow\frac{5}{4}\left(\frac{5}{4}\left(\frac{5}{4}\left(\frac{5}{4}\cdot 5m+1\right)+1\right)+1\right)+1=\frac{4}{5}n-\frac{4}{5}\Rightarrow$$

$$\frac{5}{4}\left(\frac{5}{4}\left(\frac{5}{4}\cdot 5m+1\right)+1\right)+1=\frac{16}{25}(n-1)-\frac{4}{5}\Rightarrow\frac{5}{4}\left(\frac{5}{4}\cdot 5m+1\right)+1=\left(\frac{4}{5}\right)^3(n-1)-\left(\frac{4}{5}\right)^2-\frac{4}{5}\Rightarrow$$

$$\frac{5}{4}\cdot 5m+1=\left(\frac{4}{5}\right)^4(n-1)-\left(\frac{4}{5}\right)^3-\left(\frac{4}{5}\right)^2-\frac{4}{5}\Rightarrow 5m=\left(\frac{4}{5}\right)^5(n-1)-\left(\frac{4}{5}\right)^4-\left(\frac{4}{5}\right)^3-\left(\frac{4}{5}\right)^2-\frac{4}{5}\Rightarrow$$

$$15625m=1024(n-1)-1280-1600-2000-2500\Rightarrow\ 15625m=1024n-8404\Rightarrow$$

Nun folgt eine Dekonstruktion hinunter zur elementaren Ebene bis ein Koeffizient 1 ist (falls eine Lösung existiert bzw. evident ist, dass keine Lösung existiert:

$$(15\cdot 1024+265)m=1024n-8404\Rightarrow 1024\underbrace{(15m-n)}_{\alpha}=-8404-265m\Rightarrow 1024\alpha=-265m-8404\Rightarrow$$

$$(3\cdot 265+229)\alpha=-265m-8404\Rightarrow 265\underbrace{(3\alpha+m)}_{\beta}=-229\alpha-8404\Rightarrow 265\beta=-229\alpha-8404\Rightarrow$$

$$(229+36)\beta=-229\alpha-8404\Rightarrow 229\underbrace{(\beta+\alpha)}_{\gamma}=-36\beta-8404\Rightarrow 229\gamma=-36\beta-8404\Rightarrow$$

$$(6\cdot 36+13)\gamma=-36\beta-8404\Rightarrow 36\underbrace{(6\gamma+\beta)}_{\delta}=-13\gamma-8404\Rightarrow 36\delta=-13\gamma-8404\Rightarrow$$

$$(2\cdot 13+10)\delta=-13\gamma-8404\Rightarrow 13\underbrace{(2\delta+\gamma)}_{\epsilon}=-10\delta-8404\Rightarrow 13\epsilon=-10\delta-8404\Rightarrow$$

$$(10+3)\epsilon=-10\delta-8404\Rightarrow 10\underbrace{(\epsilon+\delta)}_{\theta}=-3\epsilon-8404\Rightarrow 10\theta=-3\epsilon-8404\Rightarrow(3\cdot 3+1)\theta=-3\epsilon-8404\Rightarrow$$

$$3\underbrace{(3\theta+\epsilon)}_{\phi}=-\theta-8404\Rightarrow 3\phi=-\theta-8404\Rightarrow\theta=-3\phi-8404\ \text{ Setze }\phi:=1\Rightarrow\theta=-8407$$

Nun folgt eine Rekonstruktion hinauf auf die komplexe Ebene:

$$3\theta+\epsilon=\phi\Rightarrow\epsilon=1+3\cdot 8407=25222\quad\theta=\epsilon+\delta\Rightarrow\delta=\theta-\epsilon=-8407-25222=-33629$$

$$2\delta+\gamma=\epsilon\Rightarrow\gamma=\epsilon-2\delta=25222-2\cdot(-33629)=92480$$

$$6\gamma+\beta=\delta\Rightarrow\beta=\delta-6\gamma=-33629-6\cdot 92480=-588509$$

$$\beta+\alpha=\gamma\Rightarrow\alpha=\gamma-\beta=92480+588509=680989$$

$$3\alpha+m=\beta\Rightarrow m=\beta-3\alpha=-588509-3\cdot 680989=-2631476$$

$\alpha=15m-n\Rightarrow n=15m-\alpha=15\cdot(-2631476)-680989=-40153129$, also hat die Gleichung

$15625m=1024n-8404$ die Lösungen $m=-2631476$ und $n=-40153129$.

Gesucht sind noch die kleinsten positiven Lösungen:

$$m=-2631476+1024k>0\Rightarrow k=2570\Rightarrow m=204$$

$n=-40153129+15625k=-40153129+15625\cdot 2570=3121\Rightarrow n=3121.$

Also hat man $m=204$ und $n=3121$. Sie hatten 3121 Kokosnüsse gesammelt.

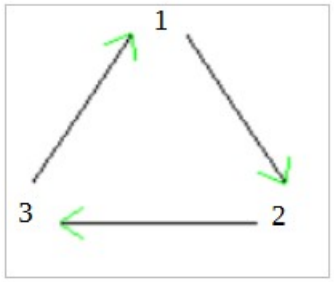
Zeitzyklen

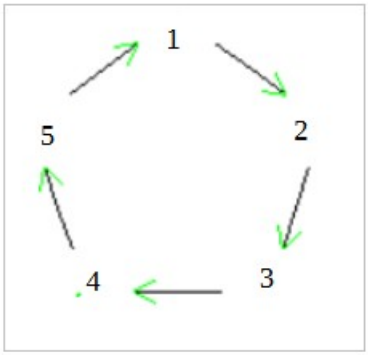
1 Monat = 30,4 Tage
1 Jahr = 365,25 Tage

10 M= 304 T;
5 M = 152 T
100 J = 36525 T;
$4J=1461T$
ggT(1461, 152)=1 1461 = 3 * 487, 487 ist Primzahl, 152 = 2*2*2*19

$1461\cdot 152=222072$
$5M=152T \overset{\cdot 1461}{\Rightarrow} 7305M=222072T$
$4J=1461T \overset{\cdot 152}{\Rightarrow} 608J=222072T$
$\Rightarrow 7305M=608J\Rightarrow 1J\approx 12{,}015M \quad 7305=3\cdot 5\cdot 487;\ 608=2^5\cdot 19\Rightarrow ggT(7305,608)=1$

Bsp: Ein Dreieckzyklus und ein Fünferzyklus starten beide bei 1 und legen in einer Zeiteinheit jeweils eine Kante zurück. Wann sind sie wieder beide gleichzeitig bei 1.



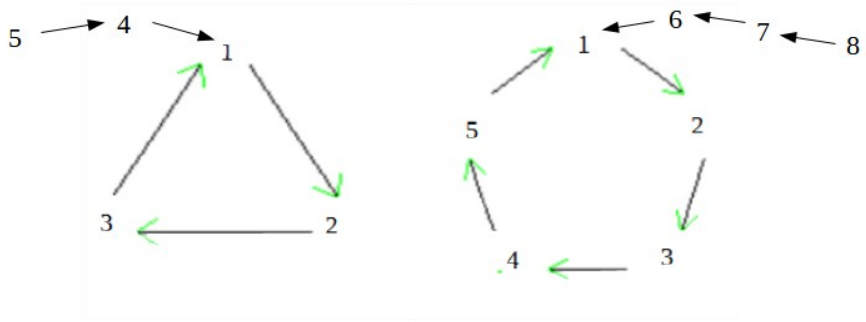


Ist der Dreierzyklus das erste Mal wieder bei 1, so ist der Fünferzyklus bei 4.
Der Dreierzyklus muss 5 mal vollständige Zyklen durchlaufen und der Fünferzyklus 3 mal.

$3\cdot m=5\cdot n$. Links ist mit 3 der Dreierzyklus und rechts mit 5 der Fünferzyklus notiert.

Also $m=5$ und $n=3$, da ggT(3,5)=1. Demnach sind sie nach $15=3\cdot 5$ Zeiteinheiten wieder zeitgleich bei 1.

Der Dreierzyklus soll nun zu Anfang bei 3 sein und der Fünferzyklus bei 1. Wann sind sie zeitgleich bei 1? Es gilt dann $3\cdot m+1=5\cdot n$ mit den Lösungen m = 3 und n = 2. Also nach $3\cdot 3+1=10$ Zeiteinheiten sind sie zeitgleich bei 1.

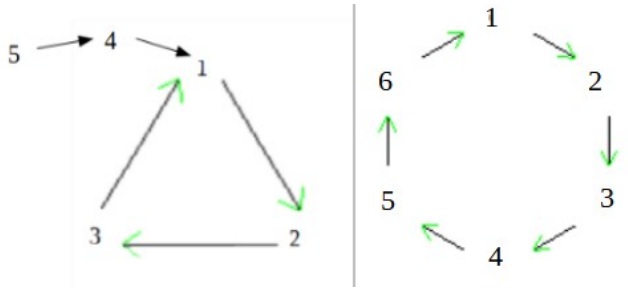


Hat man Zyklen mit Einzugsgebieten (Vorzyklen), etwa wie in der Graphik Dreierzyklus mit 2-Vorzyklus ($5 \to 4 \to$) und Fünfzyklus mit 3-Vorzyklus ($8 \to 7 \to 6 \to$), so ändert sich die diophantische Gleichung:

$3 \cdot m+2=5 \cdot n+3$ mit der kleinsten positiven Lösung $m=2 \wedge n=1$ und somit sind beide Zyklen nach $3 \cdot 2+2=8$ Zeiteinheiten synchron bei 1.

Allgemein hat man also bei einem q-Zyklus mit s-Vorzyklus und einem r-Zyklus mit t-Vorzyklus bei $q \cdot m+s=r \cdot n+t$ oder $q \cdot m=r \cdot n+t-s$ oder mit c = t-s $q \cdot m=r \cdot n+c$ Zeiteinheiten synchron die 1, falls die Gleichung lösbar ist. Die Gleichung ist nicht lösbar, wenn c nicht durch den ggT von q und r teilbar ist: $\neg \bigvee_{z \in \mathbb{Z}} c=z \cdot ggT(q,r)$. In diesem Fall laufen die Zyklen ständig parallel (ohne je die 1 synchron zu erhalten (oder eine andere Zahl). Es ist das zyklische Analogon zu den parallelen Geraden, die sich nicht schneiden.

Bsp (parallel laufende Zyklen)**:** $6m=3n+2$



1,2,3,4,5,6,1,2,3,4,5,6,1,2,3,4,5,6,…
5,4,1,2,3,1,2,3,1,2,3,1,2,3,1,2,3,1,…

Die beiden Zyklen kommen nie bei 1 (oder einer anderen Zahl) zusammen.
Entsprechend ist die Gleichung $6m=3n+2$ nicht lösbar, da $3=ggT(6,3)$ die Zahl 2 nicht teilt.

Oder so: $3(2m-n)=2 \Leftrightarrow 3r=2 \wedge r=2m-n$, aber für r gibt es keine ganzzahlige Lösung.

Oder so: $[6m]_3=[2]_3 \Rightarrow [6m-2m \cdot 3]=[2]_3 \Rightarrow [0]_3=[2]_3$ das aber sind verschiedene Restklassen mod 3

Allgemein: Gegeben sei die Gleichung $q \cdot m = r \cdot n + c$ in der Form $q_0 \cdot s_1 + q_1 \cdot s_0 = c$ (damit man eine Rekursion aufstellen kann):

Zunächst seien die Koeffizienten q_0, q_1 positiv.

Fall 1: Sei $ggT(q_0, q_1) = (q_0, q_1) = 1$.

Fall 1a: $q_0 = q_1 = 1 \Rightarrow s_1 + s_0 = c$, die Lösungen sind klar.

Fall 1b: oBdA $q_1 < q_0$. $q_0 = a_1 q_1 + q_2$, wobei $q_2 < q_1$, sonst vertauschen $q_1 := q_0, q_0 := q_1$ und $s_1 := s_0, s_0 := s_1$.

$$q_0 s_1 + q_1 s_0 = c \Rightarrow (a_1 q_1 + q_2) s_1 + q_1 s_0 = c \Rightarrow q_1 (\underbrace{a_1 s_1 + s_0}_{=: s_2}) + q_2 s_1 = c \Rightarrow$$

$q_1 s_2 + q_2 s_1 = c$ $q_1 = a_2 q_2 + q_3$ mit $q_3 < q_2$

$$q_1 s_2 + q_2 s_1 = c \Rightarrow (a_2 q_2 + q_3) s_2 + q_2 s_1 = c \Rightarrow q_2 (\underbrace{a_2 s_2 + s_1}_{=: s_3}) + q_3 s_2 = c \Rightarrow$$

$q_2 s_3 + q_3 s_2 = c$ $q_2 = a_3 q_3 + q_4$ mit $q_4 < q_3$

…

$q_{n-1} s_n + q_n s_{n-1} = c$ $q_{n-1} = a_n q_n + q_{n+1}$ mit $q_{n+1} < q_n$

$q_n s_{n+1} + q_{n+1} s_n = c$ (*)

Das sind Gleichungen mit $q_0 > q_1 > ... > q_n > q_{n+1}$. Da dies natürliche Zahlen sind, endet diese Folge.

Sei (*) die letzte Gleichung dieser Folge.
Dann ist $q_{n+1} = 1$. Wäre dies nicht der Fall, also $1 < q_{n+1} = 2 + d$ mit $d \geq 0$. Da $q_n > q_{n+1}$, sei $q_n = 2 + e$

mit $e > d$. Dann ist $q_n s_{n+1} + q_{n+1} s_n = c \Rightarrow (2+e) s_{n+1} + (2+d) s_n = c \Rightarrow 2 (\underbrace{s_{n+1} + s_n}_{=: s_{n+s}}) + e s_{n+1} + d s_n = c \Rightarrow$

$$2 s_{n+2} + e s_{n+1} + d s_n = c \Rightarrow 2 s_{n+2} + \underbrace{q_{n+2}}_{1} s_{n+1} = c \Rightarrow s_{n+1} = e s_{n+1} + d s_n \overset{s_n, s_{n+1} \text{unabhängig}}{\Rightarrow} e = 1, d = 0 \Rightarrow$$

$2 s_{n+2} + 1 s_{n+1} = c$. Also ist (*) nicht im Gegensatz zur Setzung die letzte Gleichung. Also ist Annahme dass $q_{n+1} > 1$ *falsch*.

Weiter vererbt sich die Teilerfremdheit von einer Gleichung auf die folgende: Sei also

$(q_{n-1}, q_n) = 1$. Wäre $(q_n, q_{n+1}) > 1 \Rightarrow q_n = z \cdot \alpha, q_{n+1} = z \cdot \beta$ mit $z > 1$. .

Da $q_{n-1} = a_n q_n + q_{n+1} = a_n z \cdot \alpha + z \cdot \beta = z \cdot (a_n \cdot \alpha + \beta)$ und $q_n = z \cdot \alpha \Rightarrow (q_{n-1}, q_n) > 1$ *Wid*.

Fall 2: $ggT(q_0, q_1) = (q_0, q_1) = d > 1 \Rightarrow q_0 = d \cdot \gamma \wedge q_1 = d \cdot \delta$ mit $(\gamma, \delta) = 1$.

$q_0 s_1 + q_1 s_0 = c \Leftrightarrow d\gamma s_1 + d\delta s_0 = c$

Fall 2a: $c = d \cdot \epsilon : d\gamma s_1 + d\delta s_0 = d\epsilon \Rightarrow \gamma s_1 + \delta s_0 = \epsilon$ und das ist Fall 1.

Fall 2b: $c \neq d \cdot \epsilon \Rightarrow$ c nicht durch d teilbar, dann ist die Gleichung nicht lösbar.

Man kann auch zeigen, dass der $ggT(r_1, r_2) =: g$ zweier Zahlen r_1 und r_2 sich darstellen lässt als Linearkombination (LK) von r_1 und r_2: $\bigvee_{\alpha,\beta \in \mathbb{Z}} g = \alpha r_1 + \beta r_2$. Das ist bekannt als das Lemma von Étienne Bézout.

Sei oBdA $0 < r_2 < r_1$:
1.
$r_1 = z_1 r_2 + r_3,\ r_3 < r_2$
$r_2 = z_2 r_3 + r_4,\ r_4 < r_3$
$r_3 = z_3 r_4 + r_5,\ r_5 < r_4$
…
$r_\mu = z_\mu r_{\mu+1} + r_{\mu+2},\ r_{\mu+2} < r_{\mu+1}$
...
$r_{n-3} = z_{n-3} r_{n-2} + r_{n-1},\ r_{n-1} < r_{n-2}$
$r_{n-2} = z_{n-2} r_{n-1} + r_n,\quad r_n < r_{n-1}$
$r_{n-1} = z_{n-1} r_n + r_{n+1},\quad r_{n+1} < r_n$
$r_n \quad = z_n r_{n+1} + r_{n+2},\quad r_{n+2} < r_{n+1}$

Da die Kette der r_ν abbrechen muss, sei $r_{n+2} = 0$, also der letzte Rest.
Nun geht man wieder zurück, um r_{n+1} als LK von a und b zu bestimmen. Ich löse dazu die vorletzte Gleichung nach r_{n+1} auf:

$r_{n+1} = r_{n-1} - z_{n-1} r_n$, d.h. $r_{n+1} = LK(r_{n-1}, r_n)$ und aus der vorvorletzten Gleichung folgt analog
$r_n = r_{n-2} - z_{n-2} r_{n-1}$ und damit
$r_{n+1} = r_{n-1} - z_{n-1}(r_{n-2} - z_{n-2} r_{n-1})$ oder vereinfacht
$r_{n+1} = -z_{n-1} r_{n-2} + (1 + z_{n-1} z_{n-2}) r_{n-1}$, d.h. $r_{n+1} = LK(r_{n-2}, r_{n-1})$ und im nächsten Schritt folgt nach Auflösung nach r_{n-1} aus der vorvorvorletzten Gleichung:
$r_{n+1} = (1 + z_{n-1} z_{n-2}) r_{n-3} - (z_{n-1} + (1 + z_{n-1} z_{n-2}) z_{n-3}) r_{n-2}$ oder mit $\gamma := 1 + z_{n-1} z_{n-2}$
$r_{n+1} = \gamma r_{n-3} - (z_{n-1} + \gamma z_{n-3}) r_{n-2}$, d.h. $r_{n+1} = LK(r_{n-3}, r_{n-2})$.

Das ist wieder ein rekursiver Prozess $r_{n+1} = LK(r_{n-\mu}, r_{n-\mu+1})$, $1 \leq \mu \leq n-1$, der schließlich mit $\mu = n-1$ bei $r_{n+1} = LK(r_1, r_2)$ endet.

2. Der ggT vererbt sich aber von $r_\mu, r_{\mu+1}$ auf $r_{\mu+1}, r_{\mu+2}$:
Sei zum **Beweis** $g = ggT(r_\mu, r_{\mu+1})$, d.h. $r_\mu = g \cdot a$ und $r_{\mu+1} = g \cdot b$ mit $ggT(a,b) = 1$.
Da $r_{\mu+2} = r_\mu - z_\mu r_{\mu+1}$ gilt $r_{\mu+2} = g a - z_\mu g b = g(a - z_\mu b)$ und $r_{\mu+1} = g \cdot b$.
Wäre $ggT(b, a - z_\mu b) > 1$, also $ggT(r_{\mu+1}, r_{\mu+2}) > g$, so gäbe es ein $h > 1$ mit $b = h \cdot c$ und $a - z_\mu b = h \cdot d \Rightarrow a - z_\mu (h \cdot c) = h \cdot d \Rightarrow a = h(z_\mu c + d)$ und da $b = h \cdot c$, wären a und b nicht teilerfremd, was ein Widerspruch ist. Also ist $ggT(r_{\mu+1}, r_{\mu+2}) = g$ und die Vererbung sichergestellt.
Also ist g auch der $ggT(r_{n-1}, r_n)$ und $ggT(r_n, r_{n+1})$

3. r_{n+1} ist aber der $ggT(r_1,r_2)=g$: Da $ggT(r_n,r_{n+1})=g \Rightarrow r_n=b\cdot g$, $r_{n+1}=c\cdot g$ mit $ggT(b,c)=1$ und $r_n=z_n r_{n+1}$ folgt $r_n=z_n\cdot c\cdot g$ und $r_{n+1}=c\cdot g$. Da $ggT(r_n,r_{n+1})=g$, muss gelten $c=1$, also $r_{n+1}=g$.

Man kann damit leicht zeigen, dass die diophantische Gleichung $am=bn+c$ genau dann lösbar ist, wenn der $g=ggT(a,b)$ auch c teilt, wenn also gilt: $c=g\cdot z$ mit geeignetem z.

Beweis: (1) Sei $am=bn+c$ lösbar und $g=ggT(a,b)$, also ist $a=g\cdot x$ und $b=g\cdot y$. Daraus folgt $gx\,m-gy\,n=c$ oder $g(xm-yn)=c$, also teilt g auch c.
(2) Sei $c=g\cdot z$. Da $g=ggT(a,b)\Rightarrow g=\alpha a+\beta b$ und also $c=a\,\alpha z+b\,\beta z$. Also hat man Lösungen für $c=a\,m-bn$: $m=\alpha z$ und $n=-\beta z$.

Man kann die diophantische Gleichung auch durch Restklassen lösen, falls sie lösbar ist:

Bsp2: $125\,m=4\,n-9$ $ggT(125,4)=1$, also lösbar: modulo des kleineren Koeffizienten, also mod 4:

$$[125\,m]_4=[-9]_4\Leftrightarrow[125\,m-4\cdot(31\,m)]_4=[-9+4\cdot 3]_4\Leftrightarrow[m]_4=[3]_4\Rightarrow m=3+4\cdot r$$

Eingesetzt in diophantische Gleichung: $125(3+4\,r)=4\,n-9\Rightarrow n=96+125\cdot r$.

Eine Lösung für $r=0: m=3, n=96$.

Bsp3: $15625\,m=1024\,n-8404$ modulo 1024:
$$[15625\,m]_{1024}=[-8404]_{1024}\Leftrightarrow[15625\,m-1024\cdot(15\,m)]_{1024}=[-8404+9\cdot 1024]_{1024}\Leftrightarrow[265\,m]_{1024}=[812]_{1024}$$

$265\,m=812+1024\,r\Leftrightarrow 1024\,r=265\,m-812$ modulo 265:
$$[1024\,r]_{265}=[-812]_{265}\Leftrightarrow[1024\,r-265\cdot 3\,r]_{265}=[-812+265\cdot 4]_{265}\Leftrightarrow[229\,r]_{265}=[248]_{265}$$

$229\,r=248+265\,s\Leftrightarrow 265\,s=229\,r-248$ modulo 229:
$$[265\,s]_{229}=[-248]_{229}\Leftrightarrow[265\,s-229\,s]_{229}=[-19]_{229}\Leftrightarrow[36\,s]_{229}=[-19]_{229}$$

$36\,s=-19+229\,t\Leftrightarrow 229\,t=36\,s+19$ modulo 36:
$$[229\,t]_{36}=[19]_{36}\Leftrightarrow[229\,t-36\cdot 6\,t]_{36}=[19]_{36}\Leftrightarrow[13\,t]_{36}=[19]_{36}$$

$13\,t=19+36\,u\Leftrightarrow 36\,u=13\,t-19$ modulo 13:
$$[36\,u]_{13}=[-19]_{13}\Leftrightarrow[36\,u-13\cdot 2\,u]_{13}=[-19+2\cdot 13]_{13}\Leftrightarrow[10\,u]_{13}=[7]_{13}$$

$10\,u=7+13\,v\Leftrightarrow 13\,v=10\,u-7$ modulo 10:
$$[13\,v]_{10}=[-7]_{10}\Leftrightarrow[13\,v-10\,v]_{10}=[-7+10]_{10}\Leftrightarrow[3\,v]_{10}=[3]_{10}$$

$3\,v=3+10\,w\Leftrightarrow 10\,w=3\,v-3$ modulo 3
$[10\,w]_3=[-3]_3\Leftrightarrow[10\,w-3\cdot 3\,w]_3=[-3+3]_3\Leftrightarrow[w]_3=[0]_3$ d.h. $w=3\,x$

Setze $x:=1\Rightarrow w=3\Rightarrow v=11\Rightarrow u=15\Rightarrow t=43\Rightarrow s=273\Rightarrow r=317\Rightarrow m=1228\Rightarrow n=18746$

Die kleinsten positiven Lösungen sind: $m=1228-1024=204$, $n=18746-15625=3121$.

Diese Methode bietet keinen Vorteil gegenüber meiner zuerst angegebenen Methode, die durchsichtiger ist.

Ich vermute, dass man die Gleichung auch ohne Rekursion, rein algebraisch lösen kann. Bin mir aber nicht ganz sicher.

Allgemein ohne Rekursion:

$am=bn+c$ bzw. $bn=am-c$

Fall0: Ist c nicht durch $ggT(a,b)$ teilbar, dann keine Lösung.

Fall1: Ist $b+c$ durch a teilbar, dann $[0]_a \cap [c]_b = [c+b]_{a\cdot b}$ bzw.
ist in der äquivalenten Umstellung a-c durch b teilbar, dann $[0]_b \cap [-c]_a = [a-c]_{a\cdot b}$

Fall2: Ist b+c nicht durch a teilbar, bzw. ist a-c nicht durch b teilbar,. dann entweder

Fall2.1: $[0]_a \cap [c]_b = [\pm a\cdot c]_{a\cdot b}$ bzw. $[0]_b \cap [-c]_a = [\pm b\cdot c]_{ab}$

Fall 2.2: geht mit erstem positiven Rest bzw. anderem Restglied als c $[0]_a \cap [c]_b = [c \pm b]_{a\cdot b}$

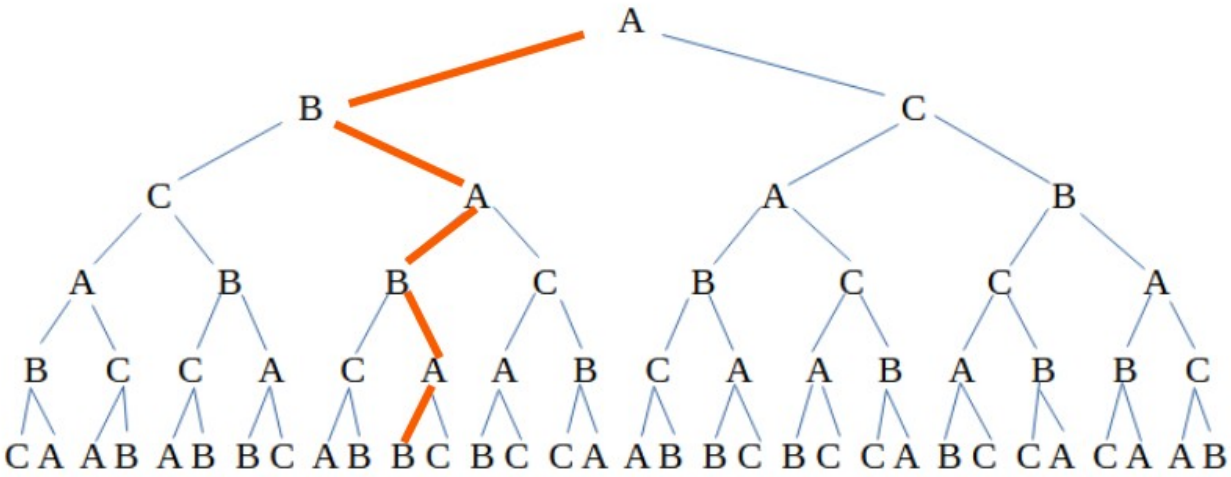
Bsp2 oben Seite 6: $125m=4n-9$: $[0]_{125} \cap [-9]_4 = [0]_{125} \cap [3]_4 = [125\cdot 3]_{125\cdot 4} = [375]_{500}$ das ist Fall2.1
Sollte die Vermutung falsch sein, dann ist das auch interessant, da hier zwei Gesichtspunkte angewandt wurden, eine diachrone, evolutionäre (Dekonstruktion und Rekonstruktion (Rekursion)) und eine synchrone, die algebraische. Das wäre ein Beispiel dafür, dass die Diachronie eine verkürzte und demnach unvollständige Sicht gegenüber der evolutionären vollständigen ist.
Ich habe dies mehrfach bemerkt[1]. Vgl. mein Essay über das Hebelgesetz (Schwerpunkt), meine Ausführungen über den freien Willen, der ebenfalls nur diachron verstehbar ist, die natürlichen Zahlen, denen eine Konstruktion, Begriffsbildung zweiten Grades zugrunde liegt und demnach nicht peanomäßig oder analog betrachtet werden kann, das arithmetische Unendliche in der Mathematik, das Prozess und Ergebnis identifiziert, Zeichentheorie, die das Problem der Bedeutung nicht erfassen kann, wenn sie das Zeichen bereits triadisch sieht, der Raumbegriff, für den die Verschränkung ein Rätsel bleibt, wenn er nicht evolutionär betrachtet wird, etc.. Der synchrone Aspekt ist sozusagen eine Projektion eines mehrdimensionalen Problems (des diachronen) auf eine geringere Dimension, sozusagen auf eine reduzierende Ebene. Vgl. hierzu auch das Höhlengleichnis von Platon.

Zyklen, Ketten, Determinismus, Zufall

Alle ungestörten Prozesse (wohlmöglich sehr lange endliche, unendliche gibt es nicht) sind Ketten oder Zyklen in der Regel mit Vorzyklen (Einzugsgebieten). Viele enden in Einerzyklen, die dann stationär sind. Jede Veränderung ist entweder unregelmäßig (Kette) oder regelmäßig (Zyklus). Das Konstante ist ein Spezialfall der zyklischen Veränderung. Was keiner internen Regel folgt, nannten die Griechen alogon und die Römer nach ihnen irrational. Diese Sicht spiegelt sich bei der Benennung der Zahlen wider. Nimmt man eine hinreichend interessante Welt an, in der zwei Zustände existieren, A und B und sonst nichts und die nicht gleich in Todesstarre fällt, so sieht die erste potenzielle „Uhr“ oder der einzig mögliche Prozess folgendermaßen aus: A B A B A …. Also ein 2-Zyklus. Eine Folge wie A B A A A B … etc kann nicht existieren, da sich AAA von A nicht unterscheidet. Dazu bräuchte es einen zweiten vom ersten unabhängigen Zyklus.

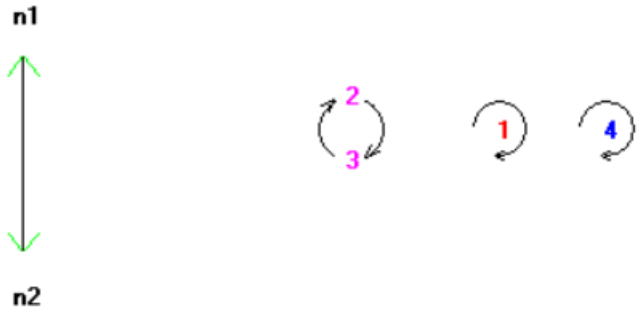
Wie sieht es in einer Welt mit drei Zuständen aus?

1 Bspw. in „Der genetische Gesichtspunkt“

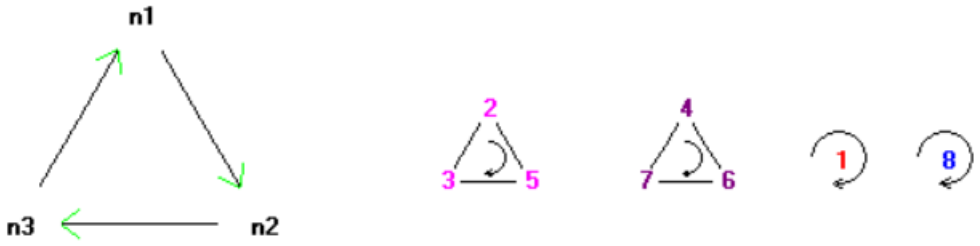


Hier ist der Determinismus schon zu Ende. Betrachtet man den „orangenen“ Prozess ABABAB, den bisherigen 2-Zyklus im Nachhinein, wie die Erkenntnis (Eule) es so zu machen pflegt, so hat man den Eindruck eines deterministischen Prozesses, eines Gesetzes. Hier gibt es keinen internen Grund (einen externen gibt es in dieser Konstellation ohnehin nicht), dass nicht jederzeit diese Folge hätte anders verlaufen können. Sie ist eine Zufallsfolge wie jede andere Folge in diesem Diagramm auch. Das ändert sich mit vier oder mehreren Zuständen nicht. Die Anzahl drei ist sozusagen die magische Anzahl. Mit der Anzahl eins gibt es keinen Prozess, mit der Anzahl zwei beginnt der Prozess, der aber deterministisch ist und mit der Anzahl drei wird der Prozess zufällig. Es sind sozusagen alles irrationale Prozesse.

Wie kommt es dann zu relativ regelhaften oder relativ stabilen Prozessen, zu internen Zyklen? Dazu bedarf es der **Beziehungen**. Die Welt muss komplexer werden. Es muss mindestens zwei Bereiche (Entitäten) n_1, n_2 geben, in denen jeweils mindestens zwei Zustände A und B existieren und eine Wirkung der beiden Entitäten aufeinander. Den kombinierten Zustand (A, A) bezeichne ich mit 1, die Zustandskombination (A, B) mit 2, (B, A) mit 3 und (B, B) mit 4. Dann ist folgender Prozess (rechts im Bild) gegeben. Bei diesem und den folgenden Diagrammen ist ein externer Zeittakt vorausgesetzt:

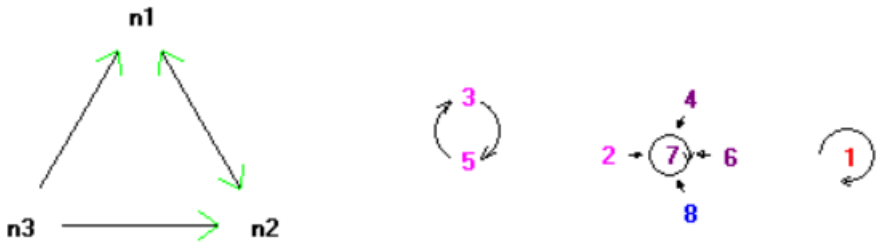


Mit (2,3) hat man einen intern stabilen 2-Zyklus und mit (1) bzw. (4) einen stabilen 1-Zyklus oder stationären Zustand. Gibt es eine weitere Entität mit Wirkung auf die beiden ersten, so kann – wenn man nur das System der beiden ersten in den Blick nimmt – ein Zyklus in einen anderen überspringen. Ist der Blick auf dem System mit den drei Entitäten und wirken sie analog des ersten Falls aufeinander, so ergibt sich folgende Dynamik (rechts):

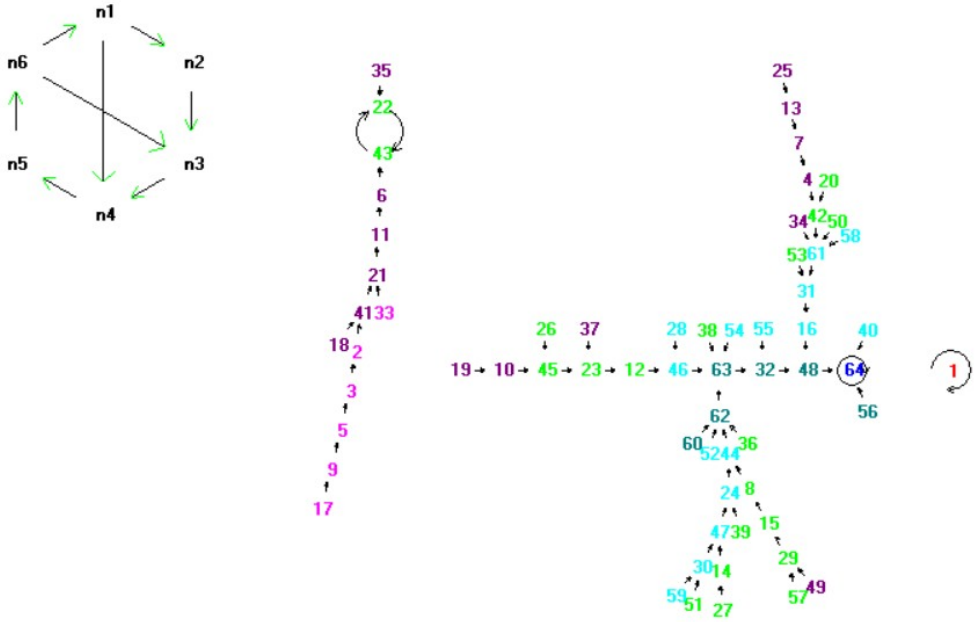


wobei folgende Bezeichnungen gelten: $1=(A,A,A);2=(A,A,B);\ 3=(A,B,A);\ 4=(A,B,B)$
$5=(B,A,A);\ 6=(B,A,B);\ 7=(B,B,A);\ 8=(B,B,B)$.

Im Fall, dass wie im ersten Beispiel die beiden ersten Entitäten gegenseitig aufeinander wirken und die dritte auf die beiden ersten, so ergibt das (das System aller drei betrachtet) mit den gleichen Bezeichnungen wie soeben:

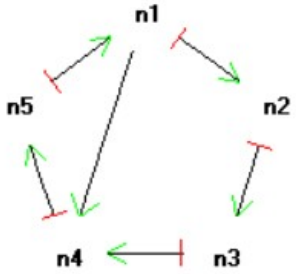


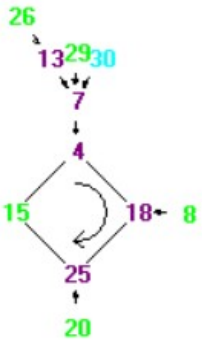
Wie man erkennt, wirkt die dritte Entität auf die beiden anderen derart stabilisierend, dass der 1-Zyklus bzw. der stationäre Zustand 7 entsteht.
Um noch ein komplexeres Beispiel anzugeben mit leicht zu erratenden Bezeichnungen:

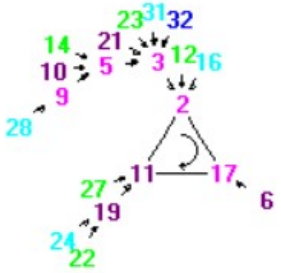


Das ist ein allgemeines Bild: Zustandskombinationen (hier $2^6=64$) enden entweder in 1-Zyklen, d.h. stationären Zuständen (hier 64) oder in Zyklen hier im 2-Zyklus (22, 43).

Zur Verdeutlichung noch ein letztes Beispiel, diesmal mit zwei antagonistischen Wirkungen:


n1
n2
n3
n4
n5


26
13
29
30
7
4
15
18
8
25
20


23
31
32
14
21
10
5
3
12
16
9
2
28
11
17
6
27
19
24
22


1