Kapitel 1

ZAHLENTHEORIE

by BRUNO

1.1 Körper

Definition

Ein Körper ist eine Menge K, versehen mit zwei inneren zweistelligen Verknüpfungen $+$ und $\cdot$, also Addition und Multiplikation, für welche eine Addition

$$\oplus \quad : \quad K \times K \to K \qquad ; \qquad (a;b) \longmapsto a+b$$

und eine Multiplikation

$$\odot \quad : \quad K \times K \to K \qquad ; \qquad (a;b) \longmapsto a \cdot b$$

gegeben sind, sodass folgende Gesetze bewisen sind:

Assoziativgesetz	(A1)	$a+(b+c)=(a+b)+c$
Kommutativgesetz	(A2)	$a+b=b+a$
Neutrales Element	(A3)	$\exists!\quad 0$ mit:
		$a+0=0+a=a$
Inverses Element	(A4)	$\forall a \in K \quad \exists! -a \in K$ mit:
		$a+(-a)=0$
Assoziativgesetz	(M1)	$a \cdot (b \cdot c)=(a \cdot b) \cdot c$
Kommutativgesetz	(M2)	$a \cdot b=b \cdot a$
Neutrales Element	(M3)	$\exists!\quad 1 \in K$ mit
		$1 \cdot a=a \cdot 1=a$
Inverses Element	(M4)	$\exists!\quad \frac{1}{a}$ zu jedem $a \in K \backslash \{0\}$ mit:
		$a \cdot \frac{1}{a}=1$
Distributivgesetz	(D)	a$\cdot(b+c)=ab+ac$

Dies erfüllen $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{R}^n$ (Vektorräume), $\mathbb{C}$, Matritzen, prime Restklassengruppen $\mathbb{Z}/p\mathbb{Z}$ ...

1.2 Teilbarkeit

1.2.1 Teilbarkeitseigenschaften

Definition

Die ganze Zahl $a \in \mathbb{Z}$ teilt $b \in \mathbb{Z}$, wenn es ein x gibt, mit $b = a \cdot x$. Man schreibt:

$$a \mid b$$

a ist ein **Teiler** von b und b ist **Vielfaches** von a

Zwei Zahlen $a, b \in \mathbb{Z}$ sind **teilerfremd**, wenn aus $c \mid a$ und $c \mid b$ folgt $|c| = 1$

Theorem

Aus dieser Teilbarkeitsrelation ergeben sich mehrere Eigenschaften:
Sei $a, b, c, t \in \mathbb{Z}$ und $t \neq 0$:

(0) $a \mid b$ und a$\mid c$ $dann$ a $\mid b \pm c$
(1) $a \mid b$ und $b \mid c$ dann $a \mid c$
(2) $a \mid b$ dann $a \mid bc$
(3) $at \mid bt \Leftrightarrow a \mid b$
(4) $a \mid b$ dann $b = 0$ oder $|a| \leq |b|$
(5) $a \mid b$ und $b \mid a$ dann $a = \pm b$

Beweis

- (1) Wenn $a \mid b$ und $b \mid c$, dann gibt es $x, y \in \mathbb{Z}$ mit $b = a \cdot x$ und $c = b \cdot y$. Also gilt auch $c = b \cdot y = a \cdot (xy)$ und somit $a \mid c$
- (2) Weil offensichtlich $b \mid bc$ gilt, folgt die Aussage sofort aus Aussage (3)
- (3) $at \mid bt \Leftrightarrow \exists x \in \mathbb{Z} : bt = atx \Leftrightarrow b = ax \Leftrightarrow a \mid b$
- (4) Sei $b = ax$ mit $x \in \mathbb{Z}$. Wenn $x = 0$, dann ist $b = 0$. In alles anderen Fällen ist $|x| > 1$ und daher $|b| = |a| \cdot |x| \geq |a|$
- (5) Wenn weder $a = 0$ noch $b = 0$ ist, dann folgt aus (4) $|a| \geq |b| \geq |a|$ und daher $a = \pm b$. Wenn also $a = 0$, dann folgt $b = 0$

□

1.2.2 Euklidische Division

Definition

Seien a und b zwei natürliche Zahlen. Es gibt dann immer $q, r \in \mathbb{N}$ sodass

$$a = b \cdot q + r \qquad 0 \leq r < b$$

q heißt **Quotient** und r heißt **Rest**. Man schreibt: $q = a \div b$ und $r \equiv a \mod b$

1.3 Primzahlen

Hier die Liste der Primzahlen bis 100:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97

Definition

Eine natürliche Zahl heißt Primzahl, wenn sie in $\mathbb{N}$ genau zwei Teiler besitzt.

Theorem

Es gibt unendlich viele Primzahlen

Beweis

Es gibt unendlich viele Primzahlen: Beweis nach Euklid

Jede ganze Zahl $n > 1$ ist durch eine Primzahl teilbar. Entweder ist n selber eine Primzahl oder $n = a \cdot b$ mit $a, b \in \mathbb{N}$.
Also ist $1 < a = \frac{n}{b} < n$. Wenn man diesen Schritt endlich oft macht, kommt man am Ende auf ein neues $a' \in \mathbb{P}$.
$\mathbb{A}$: Nehmen wir jetzt an, es gäbe nur endlich viele Primzahlen $p_1, p_2, ..., p_{r-1}, p_r$.

Dann ist

$$N = p_1 \cdot p_2 \cdot ... \cdot p_{r-1} \cdot p_r + 1 = \left(\prod_{r=1}^{r} P_r \right) + 1$$

eine ganze Zahl > 1 und hat daher mindestens einen Primteiler $p_l \in \mathbb{P}$ und $l \in \{1, 2, ..., r-1, r\}$ Dann hat man:

$$\Rightarrow \begin{cases} p_l & | \quad p_1 \cdot p_2 \cdot ... \cdot p_{r-1} \cdot p_r \\ p_l & | \quad p_1 \cdot p_2 \cdot ... \cdot p_{r-1} \cdot p_r + 1 \end{cases}$$

$$\Leftrightarrow p_l \mid p_1 \cdot p_2 \cdot ... \cdot p_{r-1} \cdot p_r - (p_1 \cdot p_2 \cdot ... \cdot p_{r-1} \cdot p_r + 1)$$

$\Leftrightarrow p_l \mid (-1)$ oder $p_l \mid 1$ WIDERSPRUCH, da $p_l = 1$ aber $1 \notin \mathbb{P}$

N muss also einen Primteiler haben ungleich $p_r \quad mit \quad r \in \{1, 2, 3, ..., r-1, r\}$ oder **selber prim sein**. □

Theorem

Jede natürliche Zahl $n \geq 2$, die nicht prim ist, besitzt einen Primfaktor p, für den gilt

$$p^2 \leq n \quad \Leftrightarrow \quad p \leq \sqrt{n}$$

Also lässt sich jede Zahl, die nicht prim ist, in Primfaktoren zerlegen.

Jede natürliche Zahl $n \geq 2$ besitzt eine eindeutige **Primfaktorzerlegung** der Form

$$n = (p_1)^{a_1} \cdot (p_2)^{a_2} \cdot ... \cdot (p_{k-1})^{a_{k-1}} \cdot (p_k)^{a_k}$$

mit $p_1 < p_2 < ... < p_{k-1} < p_k$ und $\{p_1, p_2, ..., p_{k-1}, p_k\} \in \mathbb{P}$ und $a_1, a_2, ...a_{k-1}, a_k \in \mathbb{N}$

1.4 Restklassen oder Kongruenzklassen

Definition

Seien drei natürliche Zahlen $a, b, n \in \mathbb{N}$ mit $n \geq 2$.
Wenn $a = q_1 \cdot n + r_1$ und $b = q_2 \cdot n + r_2$ und $r_1 = r_2$, also falls a und b bei der euklidischen Division durch n den gleichen Rest besitzen, dann gilt

$$a \equiv b \mod n$$

Beispiel:

- $29 \equiv -121 \mod 5$ da $29 \equiv 5 \cdot 5 + 4$ und $-121 = 5 \cdot (-25) + 4$
- $88 \equiv 24 \mod 8$ da $8 \mid 88$ und $8 \mid 24$
- $87 \equiv 23 \mod 8$

Theorem

Seien a, b zwei ganze Zahlen und $n \in \mathbb{N}$ mit $n \geq 2$, dann gilt

(1) $a \equiv b \mod n \quad \Leftrightarrow \quad n \mid (a - b)$
(2) $a \equiv 0 \mod n \quad \Leftrightarrow \quad n \mid a$
(3) falls $n' \geq 2$ und $n' \mid n$ dann gilt: $a \equiv b \mod n \quad \Rightarrow \quad a \equiv b \mod n'$

Beweis

- (1) $a \equiv b \mod n \quad \Leftrightarrow \quad a - b \equiv 0 \mod n \quad \Leftrightarrow \quad n$ teilt $(a - b)$

□

Beispiel:

- (1) $61 \equiv 29 \mod 8$ (Rest 5) $\Leftrightarrow \quad 8 \mid (61 - 29) = 32$
- (3) $4 \geq 2$ und $4 \mid 12 \quad 43 \equiv 67 \mod 12 \quad (r = 7) \quad \Rightarrow \quad 43 \equiv 67 \mod 4$

Theorem

Für jedes $n \in \mathbb{N}$ mit $n \geq 2$ gilt:
Jede ganze Zahl a ist modulo n kongruent zu einer natürlichen Zahl r mit $0 \geq r \geq n - 1$

Anders gesagt gibt es zu jeder Zahl immer Kongruenzklassen.

Definition

Es seien $n \in \mathbb{N}$ mit $n \geq 2$ und $r \in \mathbb{N}$ mit $0 \leq r < n$
Die Menge $[r] \mod n$ ist die Menge aller ganzen Zahlen z, die bei der euklidischen Division durch n den Rest r liefern.

Sie ist eine Menge von Zahlen, die den Abstand n zueinander haben.

Kongruenzen sind mit der Addition und der Multiplikation verträglich. Seien a, b, a^*, b^* ganze Zah-

len:

$$\Rightarrow \begin{cases} a & \equiv & a^* \mod n \\ b & \equiv & b^* \mod n \end{cases}$$

$$\Rightarrow a+b \equiv a^*+b^* \mod n \quad \text{und} \quad a \cdot b \equiv a^* \cdot b^* \mod n$$

Beispiel:

- $[1] \mod 4 = \{..., -7, -3, 1, 5, 9, ...\}$
- $[2] \mod 4 = \{..., -6, -2, 2, 6, 10, ...\}$
- $[3] \mod 4 = \{..., -5, -1, 3, 7, 11, ...\}$
- $[4] \mod 4 = [0] \mod 4 = \{..., -8, -4, 0, 4, 8, 12, ...\}$

Theorem

Seien $a, b \in \mathbb{N}$ mit $a, b \geq 2$ und $a \mid b$, dann gilt

$$[r] \mod b \subseteq [r] \mod a$$

($\subseteq$ heißt "Teilmenge")

Beispiel:
So gilt zum Beispiel:

$$[2] \mod 10 \subseteq [2] \mod 5$$

$$\Leftrightarrow \{..., -28, -18, -8, 2, 12, 22, ...\} \subseteq \{..., -18, -13, -8, -3, 2, 7, 12, 17, ...\}$$

1.4.1 Mit Kongruenzen rechnen und beweisen

Definition

Kongruenzen sind mit der Addition und der Multiplikation verträglich. Daraus folgen diese Eigenschaften:

Sei $n \in \mathbb{N}$ mit $n \geq 2$. a und a^* zwei (beliebige) ganze Zahlen.

1. Für jede ganze Zahl k gilt:
$$a \equiv a^* \mod n \Rightarrow k \cdot a \equiv k \cdot a^* \mod n$$
2. Für jede natürliche Zahl $p \in \mathbb{N} \setminus \{0\}$ gilt:
$$a \equiv a^* \mod n \Rightarrow a^p \equiv a^{*p} \mod n$$

Diese Eigenschaften sind **keine** Äquivalenzen, sondern Folgerungen! Bei Beweisen kann man also nicht vom Ergebnis ausgehen, und dann durch das dividieren auf beiden Seiten des Kongruenzzeichens auf ein einfaches Ergebnis kommen. Man muss von etwas einfachem ausgehen, und das dann so umformen, dass man auf die gewünschte Kongruenz kommt.

Beispiel:

$\mathbb{Z}$: $35^{228} + 84^{501} \equiv 0 \mod 17$

$$\begin{array}{rrcl|rrcl} \Rightarrow & 35 & = & 34+1 = 17\cdot 2+1 & \Rightarrow & 84 & = & 85-1 = 17\cdot 5-1 \\ \Rightarrow & 35 & \equiv & 1 \mod 17 & \Rightarrow & 84 & \equiv & -1 \mod 17 \\ \Rightarrow & 35^{228} & \equiv & 1 \mod 17 & \Rightarrow & 84^{501} & \equiv & -1 \mod 17 \end{array}$$

$$\Rightarrow \quad 35^{228}+84^{501} \quad \equiv \quad 1-1 \mod 17 \quad \equiv \quad 0 \mod 17$$

Definition

Es seien a und b zwei natürliche Zahlen größer Null mit $a > b$. r sei der Rest der Euklidischen Division von a durch b. Dann gilt:

1. Wenn $r = 0$, dann sind die gemeinsamen Teiler von a und b die Teiler von b. Da die Division aufgeht, teilt b die Zahl a. a ist also ein Vielfaches von b, deshalb sind die Teiler von a auch die Teiler von b.
2. Wenn $r \neq 0$, dann sind die gemeinsamen Teiler von a und b gerade die gemeinsamen Teiler von b und r. (Äquivalenz $\Leftrightarrow$)

Beweis

Die Euklidische Division sagt $a = b \cdot q + r$

$$\begin{array}{lll} \text{n | a} \quad \wedge \quad n|b \Rightarrow n|q\cdot b & \Rightarrow & n|a-q\cdot b \\ & \Rightarrow & n|r \end{array}$$

Alle Teiler n haben die Eigeschaften: $n|a$, $n|b$ und $n|r$. n ist also Teiler von a, b und r.

Umgekehrt gilt: wenn $n|b$ und $n|r$:

$\Rightarrow$ n | q $\cdot b + r$
$\Rightarrow$ $n|a$
□

1.4.2 Der Euklidische Algorithmus

Der Euklidische Algorithmus ist eine effiziente Methode um den ggT (größter gemeinsamer Teiler) zweier Zahlen zu finden, wenn die Primfaktorzerlegung nicht vorliegt.

Definition

Seien $a, b \in \mathbb{N}$. Sei a die größere Zahl, also $a > b$. Sei b kein Teiler von a. Nun wiederholt man immer wieder die Euklidische Division mit den Resten der vorherigen Division. Nach diesem Satz sind die Teiler von a und b auch die Teiler von b und r. Man möchte ja den ersten gemeinsamen Teiler der Zahlen a und b finden.

$$\begin{array}{rcll} a & = & q_1\cdot b + r_1 & 0 < r_1 < b \\ b & = & q_2\cdot r_1 + r_2 & 0 < r_2 < r_1 \\ r_1 & = & q_3\cdot r_2 + r_3 & 0 < r_3 < r_2 \\ & & \vdots & \\ r_{n-2} & = & q_n\cdot r_{n-1} + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} & = & q_{n+1}\cdot r_n + 0 & \end{array}$$

Deshalb ist r_n der größte gemeinsame Teiler der Zahlen a und b:

Die Folge der Reste $r_k \in \mathbb{N}$ mit $k = \{1, 2, ..., n-1, n\}$ ist streng monoton fallend. Diese Folge hat den Grenzwert $g = 0$. Deshalb gibt es immer **ein** letztes r_n der Folge.

Die **Existenz** von der letzten Zahl r_n ist sicher, da $b \nmid a$. Die Teiler von a und b sind also auch die Teiler von b und r_1. Da die Folge der Reste monoton fallend ist, kommt man am Ende auf jeden Fall

auf eine Zahl r_n, die Teilerin von a und b ist. (zum Satz)

Theorem

Aus vorheriger Definition des Euklidischen Algorithmus ergeben sich diese Eigenschaften der Zahl r_n:

1. r_n ist gleichzeitig Teiler von a und b.
2. Jeder andere Teiler von a und b ist auch Teiler von r_n

r_n ist der größte gemeinsame Teiler von a und b. $\quad \text{ggT}(a\,;b) = r_n$. Es gilt also:

- $\text{ggT}(a\,;b) = \text{ggT}(b\,;a)$
- $a|c$ und $b|d \quad \Rightarrow \quad \text{ggT}(a\,;b)|\ \text{ggT}(c\,;d)$
- $\text{ggT}(a^2;b^2) = (\text{ggT}(a;b))^2$

Beispiel:

Man sucht den ggT von $a = 780$ und $b = 567$.

$$\left.\begin{array}{rcrcr} 780 & = & 1\cdot 567 & + & 213 \\ 567 & = & 2\cdot 213 & + & 141 \\ 213 & = & 1\cdot 141 & + & 72 \\ 141 & = & 1\cdot 72 & + & 69 \\ 72 & = & 1\cdot 69 & + & 3 \\ 69 & = & 23\cdot 3 & + & 0 \end{array}\right\} \quad ggT(780;567) = ggT(567;780) = 3$$

Jetzt sucht man den ggT von $c = 3\cdot 780 = 2340$ und $d = 567\cdot 5 = 2835$.

$$\left.\begin{array}{rcrcr} 2835 & = & 1\cdot 2340 & + & 495 \\ 2340 & = & 4\cdot 495 & + & 360 \\ 495 & = & 1\cdot 360 & + & 135 \\ 360 & = & 2\cdot 135 & + & 90 \\ 135 & = & 1\cdot 90 & + & 45 \\ 90 & = & 2\cdot 45 & + & 0 \end{array}\right\} \quad \text{ggT}(2340;2835) = \text{ggT}(2835;2340) = 45$$

Aus $\quad 780\,|\,2340$ und $567|2835 \quad$ folgt $\quad \text{ggT}(780,567)\,|\ \text{ggT}(2340;2385) \quad$ oder auch $3\,|\,45$

1.4.3 Der kleine Satz von Fermat

Definition

Sei a eine ganze Zahl und $p \in \mathbb{P}$ kein Teiler von a. Dann gilt

$$a^{p-1} \equiv 1 \mod p$$

$$\Rightarrow a^p \equiv a \mod p$$

Beweis

Seien p eine Primzahl und $a \in Z$ und zwei Listen (oder Mengen) von Zahlen

$$M : a, 2a, 3a, 4a, ..., (p-2)a, (p-1)a$$

$$N : 1, 2, 3, 4, ..., (p-2), (p-1)$$

Erst wird bewiesen, dass bei der Division von 2 Zahlen $k, k' \in \mathbb{N}$ mit $k \neq k'$ ein anderer Rest rauskommt.

Dies wird und später hilfreich sein.

$$\begin{array}{rrcll} \Rightarrow & k & \not\equiv & k' \mod p & \text{(da } k \neq k' \text{ und } k < p \text{ und } k' < p\text{)} \\ \Rightarrow & k \cdot a & \not\equiv & k' \cdot a \mod p & \end{array}$$

Die Reste von beliebigen Zahlen $x \in M$ durch $p \in \mathbb{P}$ ergeben genau die Zahlen $y \in N$, da in beiden Mengen genau $(p-1)$ verschiedene Elemente sind und da gerade gezeigt wurde dass jedes Element aus M bei der Division durch p einen unterschiedlichen Rest hat. Die Reihenfolge der zu $x \in M$ zugehörigen Reste $y \in N$ ist natürlich nicht klar (ganz normal bei Mengen).

Wir benennen um, damit es klarer wird:

$$\begin{array}{rcll} \text{a} & \equiv & r_1 & \mod p \\ \text{2a} & \equiv & r_2 & \mod p \\ \text{3a} & \equiv & r_3 & \mod p \\ & & \vdots & \\ \text{(p - 2)a} & \equiv & r_{p-2} & \mod p \\ \text{(p - 1)a} & \equiv & r_{p-1} & \mod p \end{array}$$

$r_1, r_2, ..., r_{p-1}$ sind alle voneinander verschieden ($\widehat{=}$ paarweise verschieden) und sind genau alle Elemente aus der Menge N

Demnach gilt die Schreibweise:

$$r_1 \cdot r_2 \cdot r_3 \cdot ... \cdot r_{p-2} \cdot r_{p-1} \quad = \quad 1 \cdot 2 \cdot 3 \cdot ... \cdot (p-2) \cdot (p-1) \quad = \quad (p-1)!$$

Daraus folgt:

$$\begin{array}{rcll} \text{a} \cdot 2a \cdot 3a \cdot ... \cdot (p-1)a & \equiv & r_1 \cdot r_2 \cdot r_3 \cdot ... \cdot r_{p-1} & \mod p \\ \text{(p-1)! a}^{p-1} & \equiv & (p-1)! & \mod p \end{array}$$

Da ggT$((p-1)!; p) = 1$, kann man durch (p-1)! teilen, ohne dass sich das Modulo verändert

$\Rightarrow a^{p-1} \equiv 1 \mod p$

□

1.4.4 Zusammenhänge zwischen ggT und kgV

Theorem

Das kgV besitzt ähnliche Eigenschaften wie der ggT Seien a, b, c, d, k ganze Zahlen ungleich Null. Dann gilt:

1. kgV$(a; b)$ = kgV$(b; a)$
2. kgV$(k \cdot a; k \cdot b)$ = $|k|$· kgV $(a; b)$
3. Falls $a|c$ und $b|d$, dann gilt auch kgV$(a; b)$ | kgV$(c; d)$

Eine wichtige Eigenschaft, die oft benutzt wird, ist folgende:

$$\text{ggT}(a; b) \cdot \text{kgV}(a; b) = |a \cdot b|$$

Eine andere Art, den ggT und den kgV zu ermitteln ist die über die Primfaktorzerlegung. Diese wird gleich mithilfe eines Beispiels erklärt.

Beispiel:

$$\begin{array}{rcccl} \text{a = 12474} & = & 2 \cdot 3^4 \cdot 7 \cdot 11 & = & 2^1 \cdot 3^4 \cdot 5^0 \cdot 7^1 \cdot 11^1 \cdot 17^0 \\ \text{b = 33320} & = & 2^3 \cdot 5 \cdot 7^2 \cdot 17 & = & 2^3 \cdot 3^0 \cdot 5^1 \cdot 7^2 \cdot 11^0 \cdot 17^1 \end{array}$$

Daraus ergeben sich
ggT$(a;b) = 2^1 \cdot 7^1 \quad = \quad 14$
kgV$(a;b) = 2^3 \cdot 3^4 \cdot 5^1 \cdot 7^2 \cdot 11^1 \cdot 17^1 \quad = \quad 29688120$

1.4.5 Die Sätze von Bézout, Gauß und der Fundamentalsatz des ggT

Definition

Der **Fundamentalsatz des ggT** besagt, dass für $a, b \in \mathbb{N}$ ganze Zahlen u und v exisitieren, sodass gilt:

$$a \cdot u + b \cdot v \; = \; \text{ggT(a; b)}$$

Wenn a und b teilerfremd sind, dann gilt im Sonderfall: $\exists u, v \in \mathbb{Z}$:

$$a \cdot u + b \cdot v \; = \; \text{ggT(a; b)} \; = \; 1$$

Daraus folgt der **Satz von Bézout**. Zwei ganze Zahlen ungleich Null sind genau dann teilerfremd, wenn $\exists u, v \in \mathbb{Z}$ gibt, sodass gilt:

$$a \cdot u + b \cdot v \; = \; 1$$

Der **Satz von Gauß** ist bei diophantischen Gleichungen nützlich: Es seien a, b und c ganze Zahlen ungleich Null und seien a und b teilerfremd.

$$a|bc \quad \Rightarrow \quad a|c$$

Daraus folgt:

$$\text{ggT(a; } b_1) \quad \text{und} \quad \text{ggT(a; } b_2) \qquad \Leftrightarrow \qquad \text{ggT(a; } b_1 \cdot b_2)$$

Beispiel:
Musterlösung einer diophantischen Gleichung:

$$(1) \qquad 12597a - 3813b = 3$$

Enweder man sucht mit dem Taschenrechner eine Lösung oder man verwendet den oft längen Weg mit einer hohen Vorzeichenfehlerwahrscheinlichkeit. Wir sind mutig und die Zahken sind groß, deshalb nehmen wir den Weg mit dem Gaus'schen Algorithmus. Man merkt dass 12597, 3813 mit 3 gekürzt werden kann.

$$(1) \quad \Leftrightarrow \quad 4199a - 1271b = 1$$

$$\begin{aligned} 4199 &= 3 \cdot 1271 + 386 \\ 1271 &= 3 \cdot 386 + 113 \\ 386 &= 3 \cdot 113 + 47 \\ 113 &= 2 \cdot 47 + 19 \\ 47 &= 2 \cdot 19 + 9 \\ 19 &= 2 \cdot 9 + 1 \end{aligned}$$

Jetzt wird zurück eingesetzt, um auf eine Lösung zu kommen

$$
\begin{aligned}
1 &= 19 - 2 \cdot (9) \\
1 &= 19 - 2 \cdot (47 - 2 \cdot 19) = 5 \cdot 19 - 2 \cdot 47 \\
1 &= 5 \cdot (113 - 2 \cdot 47) - 2 \cdot 47 = 5 \cdot 113 - 12 \cdot 47 \\
1 &= 5 \cdot 113 - 12 \cdot (386 - 3 \cdot 113) = 41 \cdot 113 - 12 \cdot 386 \\
1 &= 41 \cdot (1271 - 3 \cdot 386) - 12 \cdot 386 = 41 \cdot 1271 - 135 \cdot 386 \\
1 &= 41 \cdot 1271 - 135 \cdot (4199 - 3 \cdot 1271) = 446 \cdot 1271 - 135 \cdot 4199
\end{aligned}
$$

Eine Lösung dieser Gleichung ist also das Zahlentupel $(-135; -446)$. Jetzt zieht man eine Gleichung von der anderen ab:

$$
\begin{aligned}
&\Rightarrow \quad 4199(a + 135) - 1271(b + 446) = 0 \\
&\Leftrightarrow \quad 4199(a + 135) = 1271(b + 446)
\end{aligned}
$$

Unter Verwendung des Satzes von Gauß folgert man

$$
\begin{aligned}
&\Rightarrow \quad 4199 | b + 446 \\
&\Rightarrow \quad 4199k = b + 446 \\
&\Leftrightarrow \quad b = 4199k - 446
\end{aligned}
$$

Jetzt wird eingesetzt

$$
\begin{aligned}
&\Rightarrow \quad 4199a + 135 \cdot 4199 = 1271(4199k - 446 + 446) = 1271 \cdot 4199k \\
&\Leftrightarrow \quad a = 1271k - 135
\end{aligned}
$$

Die Lösungsmenge Für die Geichung (1) lautet

$$\mathbb{L} = \{(1271k - 135; 4199k - 446); \quad k \in \mathbb{Z}\}$$

Jetzt kann man jede ganze Zahl F durch unendlich viele Linearkombinationen von 1271 und 4199 darstellen. Sei die Aufgabe

$$4199a - 1271b = F$$

$$\mathbb{L}_F = \{(1271k - (F \cdot 135); 4199k - (F \cdot 446)); \quad k \in \mathbb{Z}\}$$

1.4.6 Das RSA Verschlüsselungsverfahren

Die RSA-Verschlüsselung ist eine sehr sichere Verschlüsselungsmethode, welche auch sehr viele Kommunikationsdienste benutzen. Mit einem langen Schlüssel kann ein brute force Angriff (Rumprobieren) mehrere Generationen dauern und noch ist kein Algorithmus (öffentlich) bekannt, der entschlüsseln kann.

Konstruktion der Schlüssel

1. Man nimmt 2 sehr große Primzahlen p und q, die privat bleiben.

2. Man rechnet das Rsa-Modul $N = p \cdot q$ aus. N ist ein Teil des öffentlichen Schlüssels und hat mehrere hunderte von Dezimalstellen

3. Man bestimmt die Anzahl der zu N teilerfremden Zahlen. Wenn man dazu nur N kennt, brauchen Computer Jahre. Da wir aber die Primfaktorzerlegung haben, ist $\varphi(N) = (p-1) \cdot (q-1)$. φ sei die Funktion die die Anzahl an teilerfremden Zahlen angibt. Die Anzahl der zu N teilerfremden Zahlen ist das Produkt der zu p teilerfremden Zahlen mit den zu q teilerfremden Zahlen. p und q sind prim, deshalb ist $\varphi(p) = (p-1)$.

4. Man wählt eine Zahl e mit $1 < e < (p-1) \cdot (q-1)$ mit ggT$(e; (p-1)(q-1)) = 1$. Sie ist also teilerfremd mit $\varphi(N)$
   Der öffentliche Schlüssel ist (e, N). Geheim bleiben p, q, und $(p-1) \cdot (q-1)$.

5. Jetzt bestimmt man eine Zahl d mit $e \cdot d \equiv 1 \mod (p-1)(q-1)$. Man bestimmt also das Inverse Element zu e bei der Rechnung mit $\mod (p-1)(q-1)$. Dies macht man mithilfe des Euklidischen Algorithmus:

   $e \cdot d \equiv 1 \mod (p-1)(q-1)$

   $\Leftrightarrow (p-1)(q-1) \cdot k = e \cdot d - 1 \qquad (k \in \mathbb{Z})$

   $\Leftrightarrow e \cdot d - k \cdot (p-1)(q-1) = 1$ Eine lösbare Diophantische Gleichung! (ggT($e; (p-1)(q-1)) = 1$))

   $\Leftrightarrow e \cdot d + k \cdot (p-1)(q-1) = 1$ da $k \in \mathbb{Z}$

   Der private Schlüssel ist (d, N)

Ver- und Entschlüsselung der Nachricht

Sei T der Klartext, also der unverschlüsselte Text und G der geheime, verschlüsselte Text.

- Verschlüsselung: $G = T^e \mod N$
- Entschlüsselung: $T = G^d \mod N$

Damit diese Rechnung funktioniert, muss $(T^e)^d \equiv T \mod N$ gelten. Um dies zu prüfen, schauen wir uns die Ausgangsgleichheiten an:

$$e \cdot d \equiv 1 \mod (p-1)(q-1) \quad \Leftrightarrow \quad e \cdot d = r \cdot (p-1)(q-1) + 1 \qquad r \in \mathbb{Z}$$

Und es sei die (Eulersche) Formel gegeben (Vorraussetzung: ggT($a; pq) = 1$):

$$a^{(p-1)(q-1)} \equiv 1 \mod pq$$

Dann müssen nur Potenzgesetze angewandt werden:

$$\begin{aligned} (T^e)^d = T^{e \cdot d} &= T^{r \cdot (p-1)(q-1)+1} \\ &= T^{r \cdot (p-1)(q-1)} \cdot T \\ &= \left(T^{(p-1)(q-1)}\right)^r \cdot T \\ &\equiv 1^r \cdot T \mod pq \\ &\equiv T \mod N \end{aligned}$$

Beispiel:
Nehmen wir zur Veranschaulichung lieber kleine Primzahlen

1. $p = 7$ und $q = 23$
2. $N = p \cdot q = 161$
3. $\varphi(N) = (p-1)(q-1) = 132$
4. $e = 5$ passt, da ggT$(5; 161) = 1$ und $1 < 5 < 132$
5. Sei d mit $5d \equiv 1 mod 132$ oder auch äquivalent $5d + 132r = 1$. Ein Lösungstupel ist $(53; -2)$.

Der öffentliche Schlüssel ist $(5; 161)$ und der geheime Schlüssel ist $(53; 161)$

Nun verschlüsseln wir die Nachricht „ADVENT“. Der Absender bekommt den öffentlichen Schlüssel.

Nachricht	A	D	V	E	N	T
Zugehörige Zahl	1	4	22	5	14	20
$G = T^5 \mod 161$	1	58	22	66	84	125
Übermittlung der Nachricht						
$T = G^{53} \mod 161$	1	4	22	5	14	20
Entschlüsselte Nachricht	A	D	V	E	N	T

1.5 Die vollständige Induktion

Die vollständige Induktion ist eine mathematische Beweismethode, nach der eine Aussage für alle natürlichen Zahlen bewiesen wird, die größer oder gleich einem bestimmten Startwert sind.
Daher wird der Beweis in zwei Etappen durchgeführt; mit dem **Induktionsanfang** beweist man die Aussage für die kleinste Zahl, mit dem **Induktionsschritt** für die nächste Zahl, also logischerweise für alle darauffolgenden Zahlen.

Beweis

Beweis der Gaußschen Summenformel

$\not\exists : S(n) = \sum_{i=1}^{n} i = \frac{n(n+1)}{2}$

Induktionsanfang : 1= $\frac{1(1+1)}{2} = 1$

Induktionsvorraussetzung : für ein beliebiges, aber festes $k \in \mathbb{N}$ gilt: $\sum_{i=1}^{k} = \frac{k(k+1)}{2}$

Induktionsbehauptung : man behauptet, dass $\forall n \in \mathbb{N}$ gilt: $\sum_{i=1}^{n+1} = \frac{(n+1)((n+1)+1)}{2}$ □

Induktionsschluss : $\sum_{i=1}^{n} +(n+1) = \frac{n(n+1)}{2} + \frac{2(n+1)}{2} = \frac{(n+1)((n+1)+1)}{2}$

Beweis

Beweis der Summe ungerader Zahlen

$\not\exists\, \forall n \in \mathbb{N} : \sum_{k=1}^{n} (2k-1) = n^2$

Induktionsanfang : $\sum_{k=1}^{1}(2k-1) = 2\cdot 1 - 1 = 1 = 1^2$

Induktionsvorraussetzung : für ein beliebiges, aber festes $i \in \mathbb{N}$ gilt: $\sum_{k=1}^{i}(2k-1) = i^2$

Induktionsbehauptung : man behauptet, dass $\forall n \in \mathbb{N} : \sum_{k=1}^{n+1}(2k-1) = (n+1)^2$

Induktionsschluss : $\sum_{k=1}^{n+1}(2k-1) = \sum_{k=1}^{n}(2k-1) + 2(n+1) - 1 = n^2 + 2n + 1 = (n+1)^2$

□

Beweis

Beweis der Bernoullischen Ungleichung

Zz : $\forall n \in \mathbb{N} \quad n > 0 : \qquad (1+x)^n \geq 1 + nx \qquad ; x \geq -1$

Induktionsanfang : $(1+x)^0 = 1 \geq 1 = 1 + 0x$

Induktionsvorraussetzung : Es gelte nun: $(1+x)^n \geq 1 + nx; n \in \mathbb{N}_0$

Induktionsbehauptung : $(1+x)^{n+1} \geq 1 + (n+1)x$

Induktionsschluss : $(1+x)^{n+1} = (1+x)^n \cdot (1+x) \overset{\text{I.V.}}{\geq} (1+nx)\cdot(1+x) = nx^2 + nx + x + 1$

$\geq 1 + x + nx = 1 + (n+1)x$

□

Beweis

Beweis der Summe der Quadratzahlen

Mittels Induktion lässt sich ”nur” eine vorhandene Formel beweisen.

Zz : $S(n) = \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6}$

Induktionsanfang : $S(1) = \sum_{i=1}^{1} i^2 = 1^2 = 1 = \frac{1(1+1)(2+1)}{6}$

Induktionsvorraussetzung : keine Ahnung was hier rein soll

Induktionsbehauptung : $S(n+1) = \sum_{i=1}^{n+1} i^2 = \frac{(n+1)(n+2)(2(n+1)+1)}{6}$

Induktionsschluss : $S(n) + (n+1)^2 = \frac{n(n+1)(2n+1)}{6} + (n+1)^2 = \frac{2n^3+9n^2+13n+6}{6}$

$\frac{(n+1)(n+2)(2(n+1)+1)}{6} = \frac{2n^3+9n^2+13n+6}{6}$

□

Beweis

Beweis für eine Abschätzung der Summe der Quadratzahlen

$$\text{Z}: \sum_{i=1}^{n} i^2 > \frac{n^3}{3}$$

Induktionsanfang : $1^2 > \frac{1^3}{3}$

Induktionsvorraussetzung : für ein beliebiges, aber festes $k \in \mathbb{N}$ gilt: $\sum_{i=1}^{k} i^2 > \frac{k^3}{3}$

Induktionsbehauptung : man behauptet, dass $\forall n \in \mathbb{N}$ gilt: $\sum_{i=1}^{n+1} i^2 > \frac{(n+1)^3}{3}$

Induktionsschluss:

$$\sum_{i=1}^{n+1} i^2 = \overbrace{\sum_{i=1}^{n} i^2}^{> \frac{n^3}{3}} + (n+1)^2 > \frac{n^3}{3} + (n+1)^2$$

$$= \frac{n^3 + 3n^2 + 6n + 3}{3}$$

$$= \frac{n^3 + 3n^2 + 3n + 1 + 3n + 2}{3}$$

$$= \frac{(n+1)^3}{3} + \frac{3n+2}{3} \overbrace{>}^{n \geq 0} \frac{(n+1)^3}{3}$$

□

Beweis

Beweis einer Abschätzung der Fakultät

$$\forall n \in \mathbb{N}, \quad n \geq 4 : \quad n! > n^2$$

Induktionsanfang : $\text{n}_o = 4 : \quad 4! = 4 \cdot 3 \cdot 2 \cdot 1 \cdot 0! = 24 > 16 = 4^2$

Induktionsvorraussetzung : $\exists n \in \mathbb{N}, \quad n \geq 4 : \quad n! > n^2$

Induktionsbehauptung : $\text{n}! \geq n^2 \Rightarrow (n+1)! > (n+1)^2 = (n+1) \cdot (n+1)$

Induktionsschluss : $(\text{n+1})! = (\text{n+1}) \cdot n! \quad > \quad (n+1) \cdot n^2$

$$\Rightarrow n^2 \overset{?}{>} (n+1)$$

Mini-induktion : $\text{n}_0 = 4 : \quad 4^2 = 16 > 5 = 4 + 1$

$$\Rightarrow (n^2)' \overset{?}{>} (n+1)'$$

$$\Leftrightarrow 2n \overset{!}{>} 1 \qquad \forall n \in \mathbb{N}$$

□