In dem grundlegenden Zahlentheoriebuch von Hasse (1898-1979) ist im Inhaltsverzeichnis der Liebe Gott als mathematischer Autor aufgeführt. Sieht man auf Seite 3 nach, so liest man: "Die natürlichen Zahlen haben wir vom Lieben Gott". Andere Mathematiker haben eine axiomatische Definition den natürlichen Zahlen gegeben (Peano-Axiome) oder eine Fundierung durch eine "Nachfolgerfunktion" vorgeschlagen. Wir folgen Hasse und gehen davon aus, dass wir sie recht gut kennen. Lediglich heben wir hervor:

Prinzip vom minimalen Element: Jede Teilmenge der natürlichen Zahlen hat ein kleinstes Element. Übrigens hat sie nicht unbedingt ein größtes Element. Die Bruchzahlen aber z.B. haben Teilmengen ohne kleinstes Element.

Grundlegendes zur Teilbarkeit

Def.: $a, b \in \mathbb{Z}$ Man sagt: **a teilt b** genau dann, wenn es eine ganze Zahl q gibt, so dass das q-fache von a die Zahl b ergibt. Kurz: $a \mid b \Leftrightarrow \exists q \in \mathbb{Z}: \quad b = q \cdot a$

$15 \mid 165 \Leftrightarrow \exists\, 11 \in \mathbb{Z} : 165 = 11 \cdot 15$, oder auch $165 : 15 = 11$ ohne Rest.

ebenso $-3 \mid 15$, $-3 \mid -15$, aber $3 \nmid 55$. Es gilt $a \nmid (a+1)$ für $a \neq 1$.

Man kann sich für $a \mid b$ auch vorstellen, dass eine Länge b in Stücke der Länge a genau aufgeteilt werden kann, oder dass b Stifte ohne Rest in Päckchen zu a Stück verpackt werden können. So lassen sich viele Aussagen der elementaren Zahlentheorie gut verstehen. Der Vorteil algebraischer Beweise liegt einmal darin, dass die Aussagen dann auch für negative Zahlen gelten, zum anderen bleibt es ja nicht allein bei diesen Grundlagen. Als Lehrer aber sollte man nie so tun, als "müsse" man die einfachsten Dinge "beweisen". Da mit $a \mid b$ auch $a \mid -b$, $-a \mid b$ und $-a \mid -b$ gilt, reicht es nämlich doch, bei Teilbarkeitsfragen vor allem für natürliche Zahlen zu betrachten. Man mache sich das Folgende also klar:

$$(a \mid v \ \ und \ \ a \mid w) \Rightarrow a \mid (v+w) \quad \text{und} \quad (a \mid v \ \ und \ \ a \mid w) \Rightarrow a \mid (v-w)$$

aber $a \mid (v+w) \not\Rightarrow (a \mid v \ \ und \ \ a \mid w)$. In Worten: Wenn a zwei Zahlen teilt, dann teilt a auch deren Summe und deren Differenz. Das gilt aber nicht umgekehrt. Auch dafür mache man sich Beispiele. $7 \mid (15+6) \not\Rightarrow (a \mid 15 \ \ und \ \ a \mid 6)$

Algebraischer Beweis für die erste Behauptung.

$(a \mid v \ \ und \ \ a \mid w) \Rightarrow \exists q, p : v = qa \wedge w = pa \Rightarrow v + w = qa + pa = (q+p)a \ \ mit \ (q+p) \in \mathbb{Z}$ q.e.d.

Satz von der Division mit Rest:

Seien a und b positive natürliche Zahlen mit $a < b$. Dann gibt es eindeutig bestimmte natürliche Zahlen q und r mit $b = q \cdot a + r \ \ mit \ 0 \leq r < a$.

r heißt "Rest, den b beim Teilen durch a lässt."

Später schreiben wir $b = r \ \bmod \ a$ oder $b \underset{a}{\equiv} r$ lies: b = r modulo a .

Man kann sich den Sachverhalt leicht am Zahlenstrahl klar machen.

Der Satz gilt sogar auch für ganzzahlige a und b, mit $a \neq 0 \ und \ \ 0 \leq r < |a|$.

$15 < 55 \Rightarrow 55 = 3 \cdot 15 + 10$, aber auch $a = 15; b = -27 \Rightarrow -27 = -2 \cdot 15 + 3$

Definitionen:

Teilermenge $T_n = \textit{Menge der Teiler von } n = \{t \mid \exists\, k \in N \text{ mit } t \cdot k = n\}$

Vielfachenmenge $V_n = \{v \mid \exists\, k \in N \text{ mit } k \cdot n = v\}$

Größter gemeinsamer Teiler $ggT(a,b) = \max(T_a \cap T_b)$ englisch gcd(a,b)

Kleinstes gemeinsames Vielfaches $kgV(a,b) = \min(V_a \cap V_b)$ =lcm(a,b)

Ist ggT(a,b)=1, dann sagt man “a ist teilerfremd zu b” oder “a ist relativ prim zu b”.

Algorithmen zur Bestimmung des ggT:

TI: gcd(45,63) oder ggte(45,63) ergibt {9,3,-2,}

Wechselwegnahme

$45 \mid 63$ $45 \mid 18$ $27 \mid 18$ $9 \mid 18$	ggT(45,63)=? Man schreibt die beiden Zahlen in eine Tabelle und zieht solange immer die kleinere von der größeren ab, bis die kleinere die größere teilt. Dann ist diese letzte kleinere Zahl der ggT. ggT(45,63)=9	$15 \mid 22$ $15 \mid 7$ $8 \mid 7$ $1 \mid 7$	Das klappt, weil jeder gemeinsame Teiler jede Differenz teilt.

Dass man dabei nicht auf einen kleineren gemeinsamen Teiler kommen kann, merkt man, wenn man weiter abzieht.

Euklidischer Algorithmus

$63 = 1 \cdot 45 + 18$ $45 = 2 \cdot 18 + \boxed{9}$ $18 = 2 \cdot 9 + 0$ $ggT(63,45) = 9$	$220 = 2 \cdot 75 + 70$ $75 = 1 \cdot 70 + \boxed{5}$ $70 = 12 \cdot 5 + 0$ $ggT(220,75) = 5$	ggT(a,b)=? Sei a>b. Man teilt a durch b mit Rest r_1. Man teilt b durch r_1 mit Rest r_2. Man teilt r_1 durch r_2 mit Rest r_3. und so fort.... bis ein Rest 0 ist. Der vorige Rest ist dann der ggT(a,b).

Ersichtlich ist der Euklidische Algorithmus eine Abkürzung der Wechselweg-nahme. Gemeinsame Teiler werden auf die Reste “durchgereicht”.

Erweiterter Euklidischer Algorithmus zur Erzeugung der **Vielfachsummendarstellung** des ggT, d.h.

$\exists s,t \in Z \text{ mit } ggT(a,b) = s \cdot \boxed{a} + t \cdot \boxed{b}$, **Linearkombination** von a und b

$ggT(63,45) = 9$ $9 = 45 - 2 \cdot 18$ $9 = 45 - 2 \cdot (63 - 1 \cdot 45)$ $\boxed{9} = -2 \cdot \boxed{63} + 3 \cdot \boxed{45}$	Man verfolgt die Zeilen des Euklidischen Algorithmus termmäßig ohne auszurechnen rückwärts. Günstig ist es, stets den größeren Rest links zu schreiben. Ersichtlich entstehen so die gesuchten Linearfaktoren s und t. Die Existenz dieser Darstellung heißt auch “Lemma von Bezoût”.

!

Euklidischer Algorithmus

676, 182

$676 = 3 \cdot 182 + 130 \qquad 26 = -2 \cdot 182 + 3 \cdot (676 - 3 \cdot 182) = 3 \cdot 676 - 11 \cdot 182$

$182 = 1 \cdot 130 + 52 \qquad 26 = 130 - 2 \cdot (182 - 1 \cdot 130) = -2 \cdot 182 + 3 \cdot 130$

$130 = 2 \cdot 52 + \boxed{26} \rightarrow 26 = 130 - 2 \cdot 52$

$52 = 2 \cdot 26 + 0$

$26 = 3 \cdot 676 - 11 \cdot 182$

$\gcd(a,b) = s \; a + t \; b$

6885, 3465

$6885 = 1 \cdot 3465 + 3420 \qquad 45 = 3465 - 1(6885 - 1 \cdot 3465) = -1 \cdot 6885 + 2 \cdot 3465$

$3465 = 1 \cdot 3420 + \boxed{45} \rightarrow 45 = 3465 - 1 \cdot 3420$

$3420 = 86 \cdot 45 + 0 \qquad 45 = -1 \cdot 6885 + 2 \cdot 3465$

374 272

$374 = 272 + 102 \qquad 34 = -1 \cdot 272 + 3(374 - 272) = 3 \cdot 374 - 4 \cdot 272$

$272 = 2 \cdot 102 + 68 \qquad 34 = 102 - 1 \cdot (272 - 2 \cdot 102) = -1 \cdot 272 + 3 \cdot 102$

$102 = 1 \cdot 68 + \boxed{34} \qquad 34 = 102 - 1 \cdot 68$

$68 = 2 \cdot 34 + 0 \qquad 34 = 3 \cdot 374 - 4 \cdot 272$

von oben nach unten

$102 = 374 - 272$

$68 = 272 - 2 \cdot 102$

$= 272 - 2(374 - 272)$

$= -2 \cdot 374 + 3 \cdot 272$

$34 = 102 - 1 \cdot 68$

$= 374 - 272 - 1 \cdot (-2 \cdot 374 + 3 \cdot 272)$

$= 3 \cdot 374 - 4 \cdot 272$

223 70

$223 = 3 \cdot 70 + 13 \qquad 1 = -5 \cdot 70 + 27(223 - 3 \cdot 70) = 27 \cdot 223 - 86 \cdot 70$

$70 = 5 \cdot 13 + 5 \qquad 1 = 2 \cdot 13 - 5 \cdot (70 - 5 \cdot 13) = -5 \cdot 70 + 27 \cdot 13$

$13 = 2 \cdot 5 + 3 \qquad 1 = -1 \cdot 5 + 2(13 - 2 \cdot 5) = 2 \cdot 13 - 5 \cdot 5$

$5 = 1 \cdot 3 + 2 \qquad 1 = 3 - 1 \cdot (5 - 1 \cdot 3) = -1 \cdot 5 + 2 \cdot 3$

$3 = 1 \cdot 2 + \boxed{1} \qquad 1 = 3 - 1 \cdot 2$

$2 = 2 \cdot 1 + 0 \qquad 1 = 27 \cdot 223 - 86 \cdot 70$

MuPAD igcdex(374, 272) → [34, 3, −4]

gcd s t

Zahlentheorie Primzahlen

Prof. Dr. Dörte Haftendorn, www.uni-lueneburg.de/mathe-lehramt

Definition: Natürliche Zahlen mit genau zwei natürlichen Teilern heißen Primzahlen.

Genau die Primzahlen p haben keine echten Teiler, also keine Teiler t mit 1<t<p.

Hilfssatz: Jede natürliche Zahl n größer 1 hat mindestens einen Primteiler.

Bew: Es gibt, da $T_n\backslash\{1\}$ endlich ist, ein kleinstes Element m in $T_n\backslash\{1\}$. Ein echter Teiler von m wäre auch Teiler von n, also hat m keine echten Teiler, ist also Primteiler. q.e.d.

Fundamental-Lemma über Primzahlen:

Wenn eine Primzahl ein Produkt teilt, dann teilt sie mindestens einen Faktor.

Kurz: $p \ prim \ \wedge \ p \mid a \cdot b \Rightarrow p \mid a \ \vee \ p \mid b$

Bew.: Angenommen $p \nmid a \Rightarrow ggT(p,a) = 1 \Rightarrow \exists s,t \in Z: \ 1 = s \cdot p + t \cdot a$ als Linearkombination nach dem erweiterten Euklid-Algorithmus. Multipliation mit b ergibt

$b = s \cdot p \cdot b + t \cdot a \cdot b = s \cdot p \cdot b + t \cdot p \cdot k = p \cdot (s \cdot b + t \cdot k)$ mit

$k \in N \wedge (s \cdot b + t \cdot k) \in Z \Rightarrow p \mid b$. **Es reicht, wenn p relativ prim zu a ~~und~~ oder b ist**. q.e.d.

$ggT(p,a)=1$ ...

Fundamentalsatz der Zahlentheorie

Jede natürliche Zahl größer 1 hat eine eindeutige Primfaktor-Zerlegung, PFZ.

$n > 1, \Rightarrow \exists p_i \ prim \wedge \alpha_i \in N: \ n = \prod_i p_i^{\alpha_i}$ Die Primfaktoren und ihre Exponenten sind bis auf die Reihenfolge eindeutig bestimmt.

Beweis der Existenz: Angenommen es gibt Zahlen ohne PFZ, dann sei m die kleinste dieser Zahlen. Nach obigem Hilfssatz hat m einen Primteiler p und des gilt m=p m* und m*<m. Damit muss m* eine PFZ haben, denn m war ja minimal. p m* ist ein Produkt und somit hat m selbst eine PFZ im Widerspruch zur Annahme. q.e.d. (Existenz)

Beweis der Eindeutigkeit: Angenommen es existiert ein m mit nichteindeutiger PFZ und m sei minimal mit dieser Eigenschaft. Dann gilt $m = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$, Vielfachheiten ausgeschrieben. Fall 1: $p_1 = q_k \Rightarrow m = p_1 m^* = q_k m^{\sim} \| : p_1 \Rightarrow m^* = m^{\sim}$ Diese beiden Zahlen sind aber beide kleiner als m, haben daher eine eindeutige PFZ, sind also bei passender Sortierung völlig gleich. Damit ist auch die Zerlegung von m eindeutig, Widerspruch, q.e.d. (Fall1).

Fall 2: $p_1 \neq q_k \forall k \Rightarrow m = p_1 m^* = q_1 m^{\sim} \Rightarrow p_1 \mid m^{\sim}$ nach dem Fundamental-Lemma. Da wieder $m^{\sim}$ eine eindeutige PFZ hat, muss p_1 einer dier Primfaktoren sein und das ist ein Widerspruch zu $p_1 \neq q_k \forall k$. Also kann es gar kein solches m geben. q.e.d (Fall2 und Satz).

Satz (Euklid): Es gibt unendlich viele Primzahlen

Bew.: Angenommen es gibt nur endlich viele Primzahlen $p_1, p_2, \cdots, p_n$. Wir betrachten $m = p_1 p_2 \cdots p_n + 1$. Fall 1: m ist selbst prim. Wegen $m > p_i \ \forall i$ ist m dann eine neue Primpzahl und wir haben einen Widerspruch. Q.e.d.(Fall1)

Fall 2: m ist nicht selbst prim. Dann hat m nach dem Hilfssatz einen Primteiler q. Gilt nun $q = p_i$ für einen Index i, o.B.d.A. $q = p_1$, dann folgt $m = q \cdot k = p_1 p_2 \cdots p_n + 1$ und damit $q \cdot (k - p_2 \cdots p_n) = 1$, ein Widerspruch. Damit ist auch in diesem Fall eine neue Primzahl nötig und der Satz ist bewiesen.

Satz von der Division mit Rest:(s.o.)

$\forall m \in N, b \in N_0 \quad \exists_{\text{eindeutig}} \; q, r \in N_0: \; b = q \cdot m + r \;\; mit \;\; 0 \le r < m$

Definition der Kongruenz von a und b modulo m.

$\forall m \in N, \;\; a, b \in N_0 : a \underset{m}{\equiv} b \Leftrightarrow \; m \mid (a-b) \Leftrightarrow \exists \; k \in Z: \; m \cdot k = a - b$

Man schreibt dann $a = b \;\; \mathbf{mod} \;\; m$ oder $a \underset{m}{\equiv} b$ lies: $a = b \;\; \mathbf{modulo} \;\; m$

In obigem Satz gilt $q \cdot m = b - r \;\; mit \;\; 0 \le r < m$, also gilt:

$b = r \;\; \mathbf{mod} \;\; m$ oder $b \underset{m}{\equiv} r$ lies: $b = r \;\; \mathbf{modulo} \;\; m$ d.h. Jede Zahl ist kongruent zu ihrem Rest modulo m.

Satz: $a \underset{m}{\equiv} b \Leftrightarrow \left(a \underset{m}{\equiv} r \;\; \wedge \;\; b \underset{m}{\equiv} r \right)$ d.h. a und b sind kongruent modulo m genau dann, wenn sie beim Teilen durch m denselben nicht-negeativenRest lassen.

Bew.: $"\Rightarrow"_{o.B.d.A} \; a > b \quad a \underset{m}{\equiv} b \Rightarrow m \cdot k = a - b \Rightarrow a = k \cdot m + b$. Für b existiert eine Darstellung mit Rest $b = q \cdot m + r \;\; mit \;\; 0 \le r < m$, also bleibt zu zeigen, dass a auch diesen Rest hat: $a = k \cdot m + b = k \cdot m + q \cdot m + r = (k+q) \cdot m + r \;\; mit \;\; 0 \le r < m$ q.e.d ($"\Rightarrow"$)

Bew.: $"\Leftarrow"_{o.B.d.A.} \; a > b \quad \left(a \underset{m}{\equiv} r \;\; \wedge \;\; b \underset{m}{\equiv} r \right) \Rightarrow a = k \cdot m + r \;\; \wedge b = q \cdot m + r \Rightarrow$

$\Rightarrow a - b = (k - q) \cdot m \Rightarrow a \underset{m}{\equiv} b$ mit natürlichen Zahlen k und q. q.e.d ($"\Leftarrow"$) q.e.d.

Bemerkung: In der Schule nimmt man diesen Satz als Definition und macht alle Zusammenhänge an Beispielen, an Strecken und an Bündelungen klar.

Durch diesen Satz wird offensichtlich, dass die Kongruenz modulo m ein Äquivalenzrelation ist (reflexiv, symmetrisch, transitiv), die zugehörigen Klassen heißen Restklassen modulo m.

In der **Zahlentheorie** ist es üblich, die Klasse von a mit $\bar{a}$ zu bezeichnen.
Bevorzugter Repräsentant der Klasse ist der nicht-negative Rest r, denn alle Elemente gemeinsam haben, $\bar{a} = \bar{r}$.

In der funktionalen Sicht betrachtet man die Funktion

$\mathbf{Mod}: \;\; Z \to Z_m := \{0, 1, ..., m-1\}$, die jeder ganzen Zahl ihren Rest modulo m zuordnet. $\mathbf{Mod}(a, m) := r \;\; mit \;\; a = r \;\; \mathbf{mod} \;\; m \;\; \wedge 0 \le r < m$

Diese Sicht passt zur Beschaffung der Reste mit Computerwerkzeugen:
Mathematica: Mod(27,5) ergibt 2 // TI, Derive, GTR mod(27,5)
MuPad modp(27,6) Das p steht für “positiv” , dort auch mods(28,6) ergibt -2.
In mehreren Werkzeugen ist außer der funktionalen Schreibweise mit vorn stehendem Funktionssymbol (Präfix-Schreibweise) auch die Infix-Schreibweise möglich: Maple, MuPAD 27 mod 5 , Mathematica 27 ~Mod~ 5,
Dabei steht der Operator zwischen den Operanden.

In algebraischer Sicht betrachtet man $Z_m := \{0, 1, ..., m-1\}$ einfach als eine Menge, für die es nun gilt Verknüpfungen zu definieren.

In zahlentheoretischer Sicht setzt man $\overline{a} + \overline{b} := \overline{a+b}$ und muss als erstes zeigen, dass damit eine Addition der Klassen "wohldefiniert" ist, d.h. dass das Verküpfungsergebnis nicht von der Wahl der Repräsentanten der Klassen abhängt.

Bew.: Wähle a', b' mit $\overline{a'} = \overline{a} = \overline{r_a}$, $\overline{b'} = \overline{b} = \overline{r_b}$ Zu zeigen ist: $\overline{a'} + \overline{b'} = \overline{a} + \overline{b}$.

Die Voraussetzung lässt sich auch schreiben als

$a' = k'm + r_a,\quad a = km + r_a,\quad b' = q'm + r_b,\quad b = qm + r_b.$

Fall A $r_a + r_b < m \Rightarrow r_a + r_b = r_{a+b}$, Fall B $m \le r_a + r_b < 2m \Rightarrow r_a + r_b = m + r_{a+b}$

Damit gilt:

$$\overline{a'} + \overline{b'} \underset{per\ def}{=} \overline{k'm + r_a + q'm + r_b} = \overline{(k'+q')\cdot m + r_a + r_b} \underset{per\ def\ \equiv}{=} \overline{(k+q)\cdot m + r_a + r_b}$$

$$\begin{cases} \underset{\text{Fall A}}{=} \overline{(k+q)\cdot m \quad + r_{a+b}} \underset{per\ def\ \equiv}{=} \overline{a+b} \underset{per\ def\ +}{=} \overline{a} + \overline{b} \\ \underset{\text{Fall B}}{=} \overline{(k+q+1)\cdot m + r_{a+b}} \underset{per\ def\ \equiv}{=} \overline{a+b} \underset{per\ def\ +}{=} \overline{a} + \overline{b} \end{cases}$$

Also ist die Addition wohldefiniert.

Abgeschlossenheit liegt vor, weil Definition als Ergebnis ja eine Klasse angibt. Damit ist die Menge der Restklassen bzgl. der Addition eine algebraische Struktur. Mit Blick auf allgemeinere algebraische Sichtweisen kann man die Restklassen auch so schreiben: $\overline{0} = Z \cdot m = mZ,\ \overline{1} = mZ + 1,\ \overline{2} = mZ + 2, ...$ Dabei ist $mZ = V_m$, die Menge der Vielfachen von m. $(mZ, +)$ ist eine Gruppe, wie man sich leicht überlegt, und damit eine Untergruppe von $(Z, +)$, den ganzen Zahlen. Die Restklassen sind dann die additiven Nebenklassen. Diesen Begriff gibt es allgemein in der Gruppentheorie und daher kommt die Bezeichnung Z / mZ für die Menge der Restklassen. (Lies Z $nach$ mZ)

In funktionaler Sicht ist die Abbildung Mod damit ein Homomorphismus bzgl. +, das Bild einer Summe ist die Summe der Bilder.

Im Modul 5: $\overline{47} + \overline{11} = \overline{47+11} = \overline{58} = \overline{3}$, aber auch $\overline{47} + \overline{11} = \overline{2} + \overline{1} = \overline{2+1} = \overline{3}$

In algebraischer Sicht betrachtet man $Z_m := \{0, 1, ..., m-1\}$ einfach als eine Menge, für die es nun gilt Verknüpfungen zu definieren.

Definition $a, b \in Z_m := \{0, 1, ..., m-1\}$ $\quad a + b := c$ mit $c = r_{a+b} \bmod m$

Da nach dem Satz der Divison mit Rest

$c = r_{a+b} \bmod m$ mit $0 \le c \le m-1$ eindeutig bestimmt ist, ist die Addition in Z_m wohldefiniert und abgeschlossen. $(Z_m, +)$ ist eine algebraische Struktur.

Satz: $(Z_m, +) \cong (Z / mZ, +)$ Die Menge der Reste und die Restklassen sind bzgl. + isomorph, d.h. strukturgleich, beides modulo m betrachtet.

Bew.: Offensichtlich haben sie beide m Elemente und für die Übertragung sorgt der oben bewiesene Homomorphismus von Z auf Z / mZ, der nun zum Isomorphismus zwischen Z / mZ und Z_m wird.

In zahlentheoretischer Sicht setzt man $\overline{a}\cdot\overline{b} := \overline{a\cdot b}$ und muss als erstes zeigen, dass damit eine Multiplikation der Klassen jeweils "wohldefiniert" ist, d.h. dass das Verküpfungsergebnis nicht von der Wahl der Repräsentanten der Klassen abhängt. !!

Bew.: Wähle $a',b'\ mit\ \overline{a'}=\overline{a}=\overline{r_a},\ \overline{b'}=\overline{b}=\overline{r_b}$ Zu zeigen ist: $\overline{a'}\cdot\overline{b'}=\overline{a}\cdot\overline{b}$.

Die Voraussetzung lässt sich auch schreiben als

$$a'=k'm+r_a,\quad a=km+r_a,\quad b'=q'm+r_b,\quad b=qm+r_b.$$

Für $r_a\cdot r_b$ gibt es nach dem Satz von der Division mit Rest eine eindeutige Darstellung

$r_a\cdot r_b = s_r\cdot m + r_{ab}\quad mit\, 0\le r_{ab}<m$ (*) Damit gilt:

$$\overline{a'}\cdot\overline{b'} \underset{per\ def}{=} \overline{(k'm+r_a)(q'm+r_b)} = \overline{s'\cdot m + r_a\cdot r_b} \underset{per\ def\ \equiv}{=} \overline{s\cdot m + r_a\cdot r_b}$$

$$\underset{(*)}{=}\overline{s\cdot m+s_r m+r_{ab}} \underset{per\ def\ \equiv}{=} \overline{a\cdot b} \underset{per\ def\ \bullet}{=} \overline{a}\cdot\overline{b}$$ Also ist die Multiplikation wohldefiniert.

Abgeschlossenheit liegt vor, weil Definition als Ergebnis ja eine Klasse angibt.
Damit ist die Menge der Restklassen $(Z/mZ,\bullet)$ bzgl. der Multiplikation eine algebraische Struktur. !

In funktionaler Sicht ist die Abbildung Mod damit ein Homomorphismus bzgl. $\bullet$, das Bild eines Produktes ist das Produkt der Bilder. !!

Im Modul 5: $\overline{7}\cdot\overline{11}=\overline{7\cdot 11}=\overline{77}=\overline{2}$, aber auch $\overline{7}\cdot\overline{11}=\overline{2}\cdot\overline{1}=\overline{2\cdot 1}=\overline{2}$

In algebraischer Sicht betrachtet man $Z_m := \{0,1,....,m-1\}$ einfach als eine Menge, für die es nun gilt die Verknüpfung $\bullet$ zu definieren.

Definition $a,b\in Z_m := \{0,1,....,m-1\}\quad a\cdot b := c\ \ mit\ \ c = r_{a\cdot b}\ \mathbf{mod}\ m$

Da nach dem Satz von der Divison mit Rest $c = r_{a\cdot b}\ \mathbf{mod}\ m\ \ mit\ \ 0\le c\le m-1$ eindeutig bestimmt ist, ist die Miltiplikaition in Z_m wohldefiniert und abgeschlossen. $(Z_m,\cdot)$ ist eine algebraische Struktur.

Satz: $(Z_m,\bullet)\cong(Z/mZ,\bullet)$ Die Menge der Reste und die Restklassen sind bzgl. $\bullet$ isomorph, d.h. strukturgleich, beides modulo m betrachtet. !

Bew.: Offensichtlich haben sie beide m Elemente, und für die Übertragung sorgt der oben bewiesene Homomorphismus von Z auf Z/mZ, der nun zum Isomorphismus zwischen Z/mZ und Z_m wird.

Folgerung aus den Isomorphiesätzen für + und $\bullet$ ist, dass man große Freiheit bei der Notation hat. In der Kryptographie ist die algebraische Schreibweise ohne die Querstriche üblich. Der betrachtete Modul m ergibt sich aus dem Kontext.
Für die Lehre ist die Schreibweise mit den drei Strichen oft günstig, da sie den Zusammenhang besser beleuchtet.

Im Modul 11: $7+5=1$ oder $7+5\underset{11}{\equiv}1$ oder $7+5=1\ \ \mathbf{mod}\ \ 11$ oder $\overline{7}+\overline{5}=\overline{1}$

$7^2+5^2\underset{11}{\equiv}5+3=8$ oder $7^2+5^2=49+25=74\underset{11}{\equiv}8$ oder $\overline{7^2}+\overline{5^2}=\overline{49}+\overline{25}=\overline{5}+\overline{3}=\overline{8}$

Die Definition der Restklassen wird in "natürlicher Weise" auf die ganzen Zahlen zurückgeführt. Daher überträgt sich die Assoziativität und die Kommutativität sowohl für + als auch für $\bullet$. $(Z,+,\bullet)$ ist ein Ring, es gilt das Distributivgesetz $a\cdot(b+c)=a\cdot b+a\cdot c$ in $(Z,+,\bullet)$. Wegen der Homomorphie in beiden Operationen überträgt sich auch dieses auf die Restklassenstrukturen. Neutrale Elemente sind die Bilder von 0 und 1, also wieder 0 und 1 in $(Z_m,+,\bullet)$ b.z.w $\bar{0}$ *und* $\bar{1}$ *in* $(Z/_{mZ},+,\bullet)$ Zusammengefasst:

$(Z_m,+,\bullet)$ und $(Z/_{mZ},+,\bullet)$ sind untereinander isomorphe kommutative Ringe mit Einselement, die sogenannten "Restklassenringe".

*Ein **Ring ist eine algebraische Struktur** mit zwei Verknüpfungen, genannt Addition und Multiplikation, gekoppelt mit dem Distributivgesetz. Bezüglich der Addition wird eine kommutative Gruppe verlangt, bzgl. der Multiplikation reicht eine Halbgruppe. Sie braucht keine 1 zu haben und muss nicht kommutativ sein (dann werden aber beide Distributivgestze gefordert).* Die ganzen Zahlen und die Restklassenringe sind die bekanntesten Ringe.

Bemerkung: In der Schule lassen sich die Eigenschaften der Restklassenringe sehr schön an Verknüpfungstafeln erkunden.

Eigenschaften: Die (+)-Tafeln sind alle gleich aufgebaut, es entstehen immer Diagonalen mit gleichen Zahlen. Man kann bald ohne zu rechnen weiterschreiben. $(Z_m,+)$ heißt zyklische Gruppe. Die Ursache dafür ist, dass die Zahlen aus der 1 additiv entstanden sind. Ganz allgemein heißen Gruppen, die von einem Element erzeugt werden können, "zyklische Gruppen". Es ist ein Satz der Algebra, dass alle zyklischen Gruppen zu $(Z_m,+)$ oder $(Z,+)$ isomorph sind.

Interessanter sind die Mal-Tafeln. In Ringen sind Nullelemente stets anullierend, d.h. $a\cdot 0=0 \quad \forall a$. Darum lässt man bei Mal-Tafeln die 0-Zeile und die 0-Spalte weg. Dennoch kommt die 0 als Ergebnis zustande z.B. $2\cdot 3\underset{6}{\equiv}0$. Lernende finden leicht heraus, dass es solche "Nullteiler" genau dann gibt, wenn der Modul keine Primzahl ist. (2 und 3 heißen in dem Beispiel Nullteiler, weil aus z.B. aus $\boxed{2*3=6}$ folgt, dass 2 und 3 die 6 teilen). und 6 =0 modulo 6.

Satz: $(Z_m,+,\cdot)$ ist genau dann nullteilerfrei, wenn m eine Primzahl p ist.

Folgerung Dann ist $(Z_p,+,\cdot)$ ein Körper, ein primer Restklassenkörper.

*Ein **Körper** ist ein Ring, bei dem auch die multiplikative Struktur eine Gruppe ist.*

Bew.: $"\Leftarrow"\quad p\ \ prim\ \wedge\ a\cdot b\underset{p}{\equiv}0\Rightarrow a\cdot b=k\cdot p\underset{Fund.L.}{\Rightarrow}\ p|a\vee p|b$. Widerspruch. zu $0<a,b<p$

$"Nullteilerfrei\Rightarrow prim"$ Ist logisch gleichwertig mit

$"nicht\ \ prim\Rightarrow nicht\ \ Nullteilerfrei"$ Sei also $m=a\cdot b\Rightarrow 0\underset{m}{\equiv}a\cdot b$ q.e.d.

Beweis "Körper".: Es fehlt nur die Inverseneigenschaft. p sei prim. Behauptung: in jeder Zeile der Tafel kommen alle Elemente vor. [Gäbe es zwei gleiche $ab=ac\Rightarrow ab-ac=0\Rightarrow a(b-c)=0$ Nullteiler gibt es aber nicht]. Also kommt auch die 1 vor, also gibt es für jedes a ein Inverses. Die Betrachtung der Zeilen reicht wegen der Kommutativität. Rechnungen erlaubt, da Ring gesichert. (Der Beweis hätte auch über die Vielfachsummendarstellung geführt werden können, s.u.)

Prof. Dr. Dörte Haftendorn, www.uni-lueneburg.de/mathe-lehramt Mai 05

In der Kryptographie spielt nur die Multiplikation in den "primen Restklassen-Gruppen" eine Rolle. Daher sollen deren Eigenschaften herausgearbeitet werden.

$Z_m := \{0,1,....,m-1\}$ = Menge der Reste modulo m.

$Z_m^* := \{r \in Z_m \mid ggT(r,m)=1\}$ =Menge der zu m teilerfremden Reste modulo m. Zahlen a und b mit ggT(a,b)= 1 heißen sie "teilerfremd" oder "relativ prim".

Ersichtlich ist $Z_m^* \subseteq Z_m$ Die Multiplikation ist damit erklärt, es fragt sich aber, ob Z_m^* bzgl. der Multiplikation abgeschlossen ist. Antwort gibt der folgende

Satz $(Z_m^*,\bullet)$ ist Gruppe, die "prime Restklassen-Gruppe modulo m"

Beweis $a,b \in Z_m^* \Leftrightarrow ggT(a,m)=1 \wedge ggT(b,m)=1$. Angenommen $g = ggT(ab,m)$ und p_g sei ein Primteiler von g .(Existenz s.o.) Dann gilt

$$p_g \mid ab \wedge p_g \mid m \underset{Fundam.Lemma}{\Rightarrow} (p_g \mid a \vee p_g \mid b) \wedge p_g \mid m$$

Formal-logisch notiert!
Schreiben Sie das in Text um.

$\Rightarrow (p_g \mid a \wedge p_g \mid m) \vee (p_g \mid b) \wedge p_g \mid m) \Rightarrow p_g \mid ggT(a,m) \vee p_g \mid ggT(b,m)$ Widerspruch zu $ggT(a,m)=1 \wedge ggT(b,m)=1$ und damit zu $a,b \in Z_m^*$. Also muss $ggT(ab,m)=1$ sein, d.h. $a \cdot b \in Z_m^*$ Die Multiplikation in Z_m^* ist also abgeschlossen. Die Assoziativität wird aus $(Z_m,\bullet)$ übertragen, wegen $ggT(1,m)=1$ ist die 1 enthalten und damit ist $(Z_m^*,\bullet)$ kommutative Halbgruppe mit 1-Element. Es gibt die Vielfachsummendarstellung in $(Z,+,\bullet)$

$ggT(a,m)=1=s\boxed{a}+t\boxed{m} \underset{m}{\equiv} r_s\boxed{a}+0=r_s\boxed{a}$ mit $r_s \underset{m}{\equiv} s$ Also ist r_s das Inverse von a in $(Z_m,\bullet)$. Zu zeigen bleibt, dass $r_s \in (Z_m^*,\bullet)$ ist. Leicht ist zu sehen, dass $ggT(s,m)=1$, denn wäre $ggT(s,m)=g$, könnte man oben g ausklammern und g hätte ein Inverses in $(Z,+,\bullet)$, d.h. $g=1 \vee g=-1$, letzteres entfällt, da m positiv ist, ersteres ist die Behauptung für s, wegen $r_s \underset{m}{\equiv} s$ gilt das auch für r_s .q.e.d.

Bemerkung: Z_m^* ist bzgl. + i.a. gar nicht abgeschlossen, daher lohnt die Betrachtung von + nicht, wenn m keine Primzahl ist.

Die Beschaffung von Z_m^* kann für kleine m durch "Durchforsten" geschehen: (siehe Extraseite). Beim TI-voyage liefert der der Befehl (Tool s.u.) zstern(m) die Liste der Teilerfremden von n.

Für größere m ist nur noch die **Anzahl der Elemente in** Z_m^* wichtig, sie wird durch die **Eulersche φ -Funktion** angegeben. Diese Funktion ist in dem TI-Tool als euler(m) zu haben, in MuPAD als numlib::phi(m), in Maple with(numtheory): phi(m) Z_m^* erhält man mit invphi(m)

Prime Restklassengruppen $\left(Z_m^*,\cdot\right)$ Mal- und Potenztafeln.

Potenz-Tafel von Zstern modulo 6
Zstern(6 *) hat* 2 *Elemente*

1	5
1	1

Potenz-Tafel von Zstern modulo 7
Zstern(7 *) hat* 6 *Elemente*

1	2	3	4	5	6
1	4	2	2	4	1
1	1	6	1	6	6
1	2	4	4	2	1
1	4	5	2	3	6
1	1	1	1	1	1

Potenz-Tafel von Zstern modulo 8
Zstern(8 *) hat* 4 *Elemente*

1	3	5	7
1	1	1	1
1	3	5	7
1	1	1	1

Malstern-Tafel modulo 6
Zstern(6 *) hat* 2 *Elemente*

1	5
5	1

Malstern-Tafel modulo 7
Zstern(7 *) hat* 6 *Elemente*

1	2	3	4	5	6
2	4	6	1	3	5
3	6	2	5	1	4
4	1	5	2	6	3
5	3	1	6	4	2
6	5	4	3	2	1

Malstern-Tafel modulo 8
Zstern(8 *) hat* 4 *Elemente*

1	3	5	7
3	1	7	5
5	7	1	3
7	5	3	1

Malstern-Tafel modulo 11
Zstern(11 *) hat* 10 *Elemente*

1	2	3	4	5	6	7	8	9	10
2	4	6	8	10	1	3	5	7	9
3	6	9	1	4	7	10	2	5	8
4	8	1	5	9	2	6	10	3	7
5	10	4	9	3	8	2	7	1	6
6	1	7	2	8	3	9	4	10	5
7	3	10	6	2	9	5	1	8	4
8	5	2	10	7	4	1	9	6	3
9	7	5	3	1	10	8	6	4	2
10	9	8	7	6	5	4	3	2	1

Malstern-Tafel modulo 12
Zstern(12 *) hat* 4 *Elemente*

1	5	7	11
5	1	11	7
7	11	1	5
11	7	5	1

Malstern-Tafel modulo 9
Zstern(9 *) hat* 6 *Elemente*

1	2	4	5	7	8
2	4	8	1	5	7
4	8	7	2	1	5
5	1	2	7	8	4
7	5	1	8	4	2
8	7	5	4	2	1

Potenz-Tafel von Zstern modulo 9
Zstern(9 *) hat* 6 *Elemente*

1	2	4	5	7	8
1	4	7	7	4	1
1	8	1	8	1	8
1	7	4	4	7	1
1	5	7	2	4	8
1	1	1	1	1	1

Potenz-Tafel von Zstern modulo 11
Zstern(11 *) hat* 10 *Elemente*

1	2	3	4	5	6	7	8	9	10
1	4	9	5	3	3	5	9	4	1
1	8	5	9	4	7	2	6	3	10
1	5	4	3	9	9	3	4	5	1
1	10	1	1	1	10	10	10	1	10
1	9	3	4	5	5	4	3	9	1
1	7	9	5	3	8	6	2	4	10
1	3	5	9	4	4	9	5	3	1
1	6	4	3	9	2	8	7	5	10
1	1	1	1	1	1	1	1	1	1

Malstern-Tafel modulo 10
Zstern(10 *) hat* 4 *Elemente*

1	3	7	9
3	9	1	7
7	1	9	3
9	7	3	1

Potenz-Tafel von Zstern modulo 10
Zstern(10 *) hat* 4 *Elemente*

1	3	7	9
1	9	9	1
1	7	3	9
1	1	1	1

Potenz-Tafel von Zstern modulo 12
Zstern(12 *) hat* 4 *Elemente*

1	5	7	11
1	1	1	1
1	5	7	11
1	1	1	1

Malstern-Tafel modulo 13
Zstern(13 *) hat* 12 *Elemente*

1	2	3	4	5	6	7	8	9	10	11	12
2	4	6	8	10	12	1	3	5	7	9	11
3	6	9	12	2	5	8	11	1	4	7	10
4	8	12	3	7	11	2	6	10	1	5	9
5	10	2	7	12	4	9	1	6	11	3	8
6	12	5	11	4	10	3	9	2	8	1	7
7	1	8	2	9	3	10	4	11	5	12	6
8	3	11	6	1	9	4	12	7	2	10	5
9	5	1	10	6	2	11	7	3	12	8	4
10	7	4	1	11	8	5	2	12	9	6	3
11	9	7	5	3	1	12	10	8	6	4	2
12	11	10	9	8	7	6	5	4	3	2	1

Potenz-Tafel von Zstern modulo 13
Zstern(13 *) hat* 12 *Elemente*

1	2	3	4	5	6	7	8	9	10	11	12
1	4	9	3	12	10	10	12	3	9	4	1
1	8	1	12	8	8	5	5	1	12	5	12
1	3	3	9	1	9	9	1	9	3	3	1
1	6	9	10	5	2	11	8	3	4	7	12
1	12	1	1	12	12	12	12	1	1	12	1
1	11	3	4	8	7	6	5	9	10	2	12
1	9	9	3	1	3	3	1	3	9	9	1
1	5	1	12	5	5	8	8	1	12	8	12
1	10	3	9	12	4	4	12	9	3	10	1
1	7	9	10	8	11	2	5	3	4	6	12
1	1	1	1	1	1	1	1	1	1	1	1

Malstern-Tafel modulo 18
Zstern(18 *) hat* 6 *Elemente*

1	5	7	11	13	17
5	7	17	1	11	13
7	17	13	5	1	11
11	1	5	13	17	7
13	11	1	17	7	5
17	13	11	7	5	1

Potenz-Tafel von Zstern modulo 18
Zstern(18 *) hat* 6 *Elemente*

1	5	7	11	13	17
1	7	13	13	7	1
1	17	1	17	1	17
1	13	7	7	13	1
1	11	13	5	7	17
1	1	1	1	1	1

Malstern-Tafel modulo 14
Zstern(14 *) hat* 6 *Elemente*

1	3	5	9	11	13
3	9	1	13	5	11
5	1	11	3	13	9
9	13	3	11	1	5
11	5	13	1	9	3
13	11	9	5	3	1

Potenz-Tafel von Zstern modulo 14
Zstern(14 *) hat* 6 *Elemente*

1	3	5	9	11	13
1	9	11	11	9	1
1	13	13	1	1	13
1	11	9	9	11	1
1	5	3	11	9	13
1	1	1	1	1	1

Malstern-Tafel modulo 16
Zstern(16 *) hat* 8 *Elemente*

1	3	5	7	9	11	13	15
3	9	15	5	11	1	7	13
5	15	9	3	13	7	1	11
7	5	3	1	15	13	11	9
9	11	13	15	1	3	5	7
11	1	7	13	3	9	15	5
13	7	1	11	5	15	9	3
15	13	11	9	7	5	3	1

Malstern-Tafel modulo 15
Zstern(15 *) hat* 8 *Elemente*

1	2	4	7	8	11	13	14
2	4	8	14	1	7	11	13
4	8	1	13	2	14	7	11
7	14	13	4	11	2	1	8
8	1	2	11	4	13	14	7
11	7	14	2	13	1	8	4
13	11	7	1	14	8	4	2
14	13	11	8	7	4	2	1

Potenz-Tafel von Zstern modulo 15
Zstern(15 *) hat* 8 *Elemente*

1	2	4	7	8	11	13	14
1	4	1	4	4	1	4	1
1	8	4	13	2	11	7	14
1	1	1	1	1	1	1	1
1	2	4	7	8	11	13	14
1	4	1	4	4	1	4	1
1	8	4	13	2	11	7	14
1	1	1	1	1	1	1	1

Potenz-Tafel von Zstern modulo 16
Zstern(16 *) hat* 8 *Elemente*

1	3	5	7	9	11	13	15
1	9	9	1	1	9	9	1
1	11	13	7	9	3	5	15
1	1	1	1	1	1	1	1
1	3	5	7	9	11	13	15
1	9	9	1	1	9	9	1
1	11	13	7	9	3	5	15
1	1	1	1	1	1	1	1

Malstern-Tafel modulo 17
Zstern(17 *) hat* 16 *Elemente*

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	4	6	8	10	12	14	16	1	3	5	7	9	11	13	15
3	6	9	12	15	1	4	7	10	13	16	2	5	8	11	14
4	8	12	16	3	7	11	15	2	6	10	14	1	5	9	13
5	10	15	3	8	13	1	6	11	16	4	9	14	2	7	12
6	12	1	7	13	2	8	14	3	9	15	4	10	16	5	11
7	14	4	11	1	8	15	5	12	2	9	16	6	13	3	10
8	16	7	15	6	14	5	13	4	12	3	11	2	10	1	9
9	1	10	2	11	3	12	4	13	5	14	6	15	7	16	8
10	3	13	6	16	9	2	12	5	15	8	1	11	4	14	7
11	5	16	10	4	15	9	3	14	8	2	13	7	1	12	6
12	7	2	14	9	4	16	11	6	1	13	8	3	15	10	5
13	9	5	1	14	10	6	2	15	11	7	3	16	12	8	4
14	11	8	5	2	16	13	10	7	4	1	15	12	9	6	3
15	13	11	9	7	5	3	1	16	14	12	10	8	6	4	2
16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Potenz-Tafel von Zstern modulo 17
Zstern(17 *) hat* 16 *Elemente*

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	4	9	16	8	2	15	13	13	15	2	8	16	9	4	1
1	8	10	13	6	12	3	2	15	14	5	11	4	7	9	16
1	16	13	1	13	4	4	16	16	4	4	13	1	13	16	1
1	15	5	4	14	7	11	9	8	6	10	3	13	12	2	16
1	13	15	16	2	8	9	4	4	9	8	2	16	15	13	1
1	9	11	13	10	14	12	15	2	5	3	7	4	6	8	16
1	1	16	1	16	16	16	1	1	16	16	16	1	16	1	1
1	2	14	4	12	11	10	8	9	7	6	5	13	3	15	16
1	4	8	16	9	15	2	13	13	2	15	9	16	8	4	1
1	8	7	13	11	5	14	2	15	3	12	6	4	10	9	16
1	16	4	1	4	13	13	16	16	13	13	4	1	4	16	1
1	15	12	4	3	10	6	9	8	11	7	14	13	5	2	16
1	13	2	16	15	9	8	4	4	8	9	15	16	2	13	1
1	9	6	13	7	3	5	15	2	12	14	10	4	11	8	16
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Malstern-Tafel modulo 21
Zstern(21 *) hat* 12 *Elemente*

1	2	4	5	8	10	11	13	16	17	19	20
2	4	8	10	16	20	1	5	11	13	17	19
4	8	16	20	11	19	2	10	1	5	13	17
5	10	20	4	19	8	13	2	17	1	11	16
8	16	11	19	1	17	4	20	2	10	5	13
10	20	19	8	17	16	5	4	13	2	1	11
11	1	2	13	4	5	16	17	8	19	20	10
13	5	10	2	20	4	17	1	19	11	16	8
16	11	1	17	2	13	8	19	4	20	10	5
17	13	5	1	10	2	19	11	20	16	8	4
19	17	13	11	5	1	20	16	10	8	4	2
20	19	17	16	13	11	10	8	5	4	2	1

Potenz-Tafel von Zstern modulo 21
Zstern(21 *) hat* 12 *Elemente*

1	2	4	5	8	10	11	13	16	17	19	20
1	4	16	4	1	16	16	1	4	16	4	1
1	8	1	20	8	13	8	13	1	20	13	20
1	16	4	16	1	4	4	1	16	4	16	1
1	11	16	17	8	19	2	13	4	5	10	20
1	1	1	1	1	1	1	1	1	1	1	1
1	2	4	5	8	10	11	13	16	17	19	20
1	4	16	4	1	16	16	1	4	16	4	1
1	8	1	20	8	13	8	13	1	20	13	20
1	16	4	16	1	4	4	1	16	4	16	1
1	11	16	17	8	19	2	13	4	5	10	20
1	1	1	1	1	1	1	1	1	1	1	1

Zstern(19) *hat* 18 *Elemente*

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	4	6	8	10	12	14	16	18	1	3	5	7	9	11	13	15	17
3	6	9	12	15	18	2	5	8	11	14	17	1	4	7	10	13	16
4	8	12	16	1	5	9	13	17	2	6	10	14	18	3	7	11	15
5	10	15	1	6	11	16	2	7	12	17	3	8	13	18	4	9	14
6	12	18	5	11	17	4	10	16	3	9	15	2	8	14	1	7	13
7	14	2	9	16	4	11	18	6	13	1	8	15	3	10	17	5	12
8	16	5	13	2	10	18	7	15	4	12	1	9	17	6	14	3	11
9	18	8	17	7	16	6	15	5	14	4	13	3	12	2	11	1	10
10	1	11	2	12	3	13	4	14	5	15	6	16	7	17	8	18	9
11	3	14	6	17	9	1	12	4	15	7	18	10	2	13	5	16	8
12	5	17	10	3	15	8	1	13	6	18	11	4	16	9	2	14	7
13	7	1	14	8	2	15	9	3	16	10	4	17	11	5	18	12	6
14	9	4	18	13	8	3	17	12	7	2	16	11	6	1	15	10	5
15	11	7	3	18	14	10	6	2	17	13	9	5	1	16	12	8	4
16	13	10	7	4	1	17	14	11	8	5	2	18	15	12	9	6	3
17	15	13	11	9	7	5	3	1	18	16	14	12	10	8	6	4	2
18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Zstern(19) *hat* 18 *Elemente*

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
1	4	9	16	6	17	11	7	5	5	7	11	17	6	16	9	4	1
1	8	8	7	11	7	1	18	7	12	1	18	12	8	12	11	11	18
1	16	5	9	17	4	7	11	6	6	11	7	4	17	9	5	16	1
1	13	15	17	9	5	11	12	16	3	7	8	14	10	2	4	6	18
1	7	7	11	7	11	1	1	11	11	1	1	11	7	11	7	7	1
1	14	2	6	16	9	7	8	4	15	11	12	10	3	13	17	5	18
1	9	6	5	4	16	11	7	17	17	7	11	16	4	5	6	9	1
1	18	18	1	1	1	1	18	1	18	1	18	18	18	18	1	1	18
1	17	16	4	5	6	7	11	9	9	11	7	6	5	4	16	17	1
1	15	10	16	6	17	11	12	5	14	7	8	2	13	3	9	4	18
1	11	11	7	11	7	1	1	7	7	1	1	7	11	7	11	11	1
1	3	14	9	17	4	7	8	6	13	11	12	15	2	10	5	16	18
1	6	4	17	9	5	11	7	16	16	7	11	5	9	17	4	6	1
1	12	12	11	7	11	1	18	11	8	1	18	8	12	8	7	7	18
1	5	17	6	16	9	7	11	4	4	11	7	9	16	6	17	5	1
1	10	13	5	4	16	11	12	17	2	7	8	3	15	14	6	9	18
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Potenz-Tafel von Zstern modulo 31

Zstern(31) *hat* 30 *Elemente*

(%o152)

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
1	4	9	16	25	5	18	2	19	7	28	20	14	10	8	8	10	14	20	28	7	19	2	18	5	25	16	9	4	1
1	8	27	2	1	30	2	16	16	8	29	23	27	16	27	4	15	4	8	2	23	15	15	29	1	30	29	4	23	30
1	16	19	8	5	25	14	4	20	18	9	28	10	7	2	2	7	10	28	9	18	20	4	14	25	5	8	19	16	1
1	1	26	1	25	26	5	1	25	25	6	26	6	5	30	1	26	25	5	25	6	6	30	26	5	6	30	5	30	30
1	2	16	4	1	1	4	8	8	2	4	2	16	8	16	16	8	16	2	4	2	8	8	4	1	1	4	16	2	1
1	4	17	16	5	6	28	2	10	20	13	24	22	19	23	8	12	9	7	18	11	21	29	3	25	26	15	14	27	30
1	8	20	2	25	5	10	16	28	14	19	9	7	18	4	4	18	7	9	19	14	28	16	10	5	25	2	20	8	1
1	16	29	8	1	30	8	4	4	16	23	15	29	4	29	2	27	2	16	8	15	27	27	23	1	30	23	2	15	30
1	1	25	1	5	25	25	1	5	5	5	25	5	25	1	1	25	5	25	5	5	5	1	25	25	5	1	25	1	1
1	2	13	4	25	26	20	8	14	19	24	21	3	9	15	16	22	28	10	7	12	17	23	11	5	6	27	18	29	30
1	4	8	16	1	1	16	2	2	4	16	4	8	2	8	8	2	8	4	16	4	2	2	16	1	1	16	8	4	1
1	8	24	2	5	6	19	16	18	9	21	17	11	28	27	4	3	20	14	10	22	13	15	12	25	26	29	7	23	30
1	16	10	8	25	5	9	4	7	28	14	18	19	20	2	2	20	19	18	14	28	7	4	9	5	25	8	10	16	1
1	1	30	1	1	30	1	1	1	1	30	30	30	1	30	1	30	1	1	1	30	30	30	30	1	30	30	1	30	30
1	2	28	4	5	25	7	8	9	10	20	19	18	14	16	16	14	18	19	20	10	9	8	7	25	5	4	28	2	1
1	4	22	16	25	26	18	2	19	7	3	11	17	10	23	8	21	14	20	28	24	12	29	13	5	6	15	9	27	30
1	8	4	2	1	1	2	16	16	8	2	8	4	16	4	4	16	4	8	2	8	16	16	2	1	1	2	4	8	1
1	16	12	8	5	6	14	4	20	18	22	3	21	7	29	2	24	10	28	9	13	11	27	17	25	26	23	19	15	30
1	1	5	1	25	5	5	1	25	25	25	5	25	5	1	1	5	25	5	25	25	25	1	5	5	25	1	5	1	1
1	2	15	4	1	30	4	8	8	2	27	29	15	8	15	16	23	16	2	4	29	23	23	27	1	30	27	16	29	30
1	4	14	16	5	25	28	2	10	20	18	7	9	19	8	8	19	9	7	18	20	10	2	28	25	5	16	14	4	1
1	8	11	2	25	26	10	16	28	14	12	22	24	18	27	4	13	7	9	19	17	3	15	21	5	6	29	20	23	30
1	16	2	8	1	1	8	4	4	16	8	16	2	4	2	2	4	2	16	8	16	4	4	8	1	1	8	2	16	1
1	1	6	1	5	6	25	1	5	5	26	6	26	25	30	1	6	5	25	5	26	26	30	6	25	26	30	25	30	30
1	2	18	4	25	5	20	8	14	19	7	10	28	9	16	16	9	28	10	7	19	14	8	20	5	25	4	18	2	1
1	4	23	16	1	30	16	2	2	4	15	27	23	2	23	8	29	8	4	16	27	29	29	15	1	30	15	8	27	30
1	8	7	2	5	25	19	16	18	9	10	14	20	28	4	4	28	20	14	10	9	18	16	19	25	5	2	7	8	1
1	16	21	8	25	26	9	4	7	28	17	13	12	20	29	2	11	19	18	14	3	24	27	22	5	6	23	10	15	30
1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1

Malstern-Tafel modulo 20

Zstern(20) *hat* 8 *Elemente*

1	3	7	9	11	13	17	19
3	9	1	7	13	19	11	17
7	1	9	3	17	11	19	13
9	7	3	1	19	17	13	11
11	13	17	19	1	3	7	9
13	19	11	17	3	9	1	7
17	11	19	13	7	1	9	3
19	17	13	11	9	7	3	1

Potenz-Tafel von Zstern modulo 2

Zstern(20) *hat* 8 *Elemente*

1	3	7	9	11	13	17	19
1	9	9	1	1	9	9	1
1	7	3	9	11	17	13	19
1	1	1	1	1	1	1	1
1	3	7	9	11	13	17	19
1	9	9	1	1	9	9	1
1	7	3	9	11	17	13	19
1	1	1	1	1	1	1	1

Algebra, Theorie endlicher Gruppen $(G,\cdot)$, Einselement sei als 1 notiert.

Das Folgende gilt für alle endlichen Gruppen:

(1) Satz: $\boxed{\forall a \in G\ \exists\, k \in \mathbb{N}:\ a^k = 1}$ Für jedes Element a gibt einen Exponenten k, so dass die Potenz 1 ist.

Beweis: $\exists \bar{a} : a\bar{a} = 1$. Sei $a^i = a^j$ mit $i < j$. Dann folgt $1 = a^i \bar{a}^i = a^j \bar{a}^i = a^{j-i} = a^k$. q.e.d

(2) Def.: Sei $a \in G$. Die kleinste natürliche Zahl (>0) mit $a^k = 1$ heißt Ordnung von a, kurz $ord(a)$.

(3) Satz und Def.: $\langle a \rangle := \left\{1, a, a^2, \dots, a^{ord(a)-1}\right\}$ ist eine Gruppe.

$\langle a \rangle$ heißt „von a erzeugte Untergruppe“.

Beweis: Abgeschlossenheit: $a^i a^j = a^{i+j} = a^{ord(a)+r} = a^{ord(a)} a^r = a^r$, notiert für $i + j \ge ord(a)$, da sonst klar.

Inverses zu a^i ist $a^{ord(a)-i}$, denn $a^i a^{ord(a)-i} = a^{ord(a)} = 1$. q.e.d.

(4) Def.: Die Ordnung einer Gruppe ist die Anzahl ihrer Elemente, also $ord(G) = |G|$, damit auch $ord\left(\langle a \rangle\right) = ord(a)$.

(5) Def.: Sei $g \in G$. Die Menge $g\langle a \rangle := \left\{g, g\,a, g\,a^2, \dots, g\,a^{ord(a)-1}\right\}$ heißt Nebenklasse von a.

(6) Satz: a) Jede Nebenklasse $g\langle a \rangle$ hat genau $ord(a)$ Elemente.

b) Zwei Nebenklassen sind entweder gleich oder disjunkt.

Beweis a) Mehr Elemente können es ja nicht sein, aber evt. weniger. Sei

Sei $\bar{g}\,g = 1$ und $g\,a^i = g\,a^j$, dann folgt $\bar{g}\,g\,a^i = \bar{g}\,g a^j$ also $a^i = a^j$. Letzteres ist in $\langle a \rangle$ für $i \ne j$ nicht möglich, also sind es auch $ord(a)$ Elemente.

b) Sei $g\,a^i = h\,a^j$ mit $i < j$ ein Element aus beiden Nebenklassen. Dann folgt

$g = h\,a^{j-i} \in h\langle a \rangle$ also auch $\forall r\ \ g a^r \in h\langle a \rangle$ und damit $g\langle a \rangle \subseteq h\langle a \rangle$. Weiter folgt

$g\,a^i a^{ord(a)-j} = h\,a^j a^{ord(a)-j} = h$, damit wie oben

$h\langle a \rangle \subseteq g\langle a \rangle$, also $g\langle a \rangle = h\langle a \rangle$. Ein gemeinsames Element erzwingt also schon, dass die Nebenklassen gleich sind. Kein gemeinsames Element heißt „disjunkt“ q.e.d

(7) Hauptsatz zur Ordnung von Gruppen und Elementen

a. $ord(a) \,|\, ord(G)$, jede Elementordnung teilt die Gruppenordnung

b. $\forall a:\ a^{ord(G)} = 1$, ein Element hoch Gruppenordnung ist immer 1.

c. $e = q \cdot ord + r$, dann gilt $a^e = a^r$. Dabei kann man als ord die Elementordnung oder die Gruppenordnung nehmen.

Beweis: a) Die Vereinigung aller Nebenklassen –es gebe z Stück- ist die ganze Gruppe und alle Nebenkassen haben gleich viele Elemente, nämlich $ord(a)$. Dann ist

$z \cdot ord(a) = ord(G)$. b) $a^{ord(G)} = a^{z \cdot ord(a)} = \left(a^{ord(a)}\right)^z = 1^z = 1$=1 c) klar. qed

Algebra-Zahlentheorie, die $\left(\mathbb{Z}_m^*, \cdot\right)$ als Gruppen

Gemeint sind die primen Restklassengruppen von Seite 11. Dort ist unten schon von der Anzahl ihrer Elemente die Rede-

(4) Def.: Die Anzahl der zu m teilerfremden Elemente in $\mathbb{Z}(m)$ ist $\varphi(m)$.

a. Satz: Ist $m = p$ eine Primzahl, dann ist $\varphi(m) = p-1$.

b. Satz: Ist $m = p \cdot q$ ein Primzahlprodukt, dann ist $\varphi(m) = (p-1)\cdot(q-1)$

Beweis auf Extraseite

c. Sonst ist $\varphi(m)$ für kleine m durch Hinsehen, für größere m mit Computern mit euler(m), eulerphi(m), phi(m) o.ä. zu beschaffen.

d. Mit Seite 12 a,b,c kann man $\langle a \rangle$ für einzelne a bilden. Die Zahl der Elemente darin ist Ordnung von a.

(5) Die Nebenklassen zu einem Element a lassen sich mit Hilfe der Seiten 12 a,b,c leicht bestimmen. (Übungsaufgaben)

(6) Die Zahl der Elemente in $g\langle a \rangle$ kann man sehen. Dass zwei Nebenklassen entweder zusammenfallen oder gar kein gemeinsames Element haben, merkt man beim Ausrechnen. (Übungsaufgaben)

(7) Eulerscher Satz $a^{\varphi(m)} \underset{m}{\equiv} 1 \quad \text{für} \quad a \in \mathbb{Z}_m^*$

(8) Kleiner Fermatscher Satz Wenn p Primzahl ist, gilt $a^{p-1} \underset{p}{\equiv} 1$ für $a \in \mathbb{Z}_p^*$.

Beweise: Der Eulersche Satz ist eine direkte Folge des Hauptsatze der Gruppentheorie zur Ordnung, Nr. (7) aus Seite 13. und obiger Definition (4), denn die zu m teilerfremden Elemente bilden eine Gruppe und diese hat $\varphi(m)$ Elemente. Der Kleine Fermatsche Satz folgt daraus mit (4)a.

(9) Primzahlsuche mit dem Kleinen Fermatschen Satz.

Findet man für ein $a \in \mathbb{Z}_p^*$, dass $a^{p-1} \underset{p}{\not\equiv} 1$ ist, dann kann p keine Primzahl sein. Wenn aber $a^{p-1} \underset{p}{\equiv} 1$ für $a \in \mathbb{Z}_p^*$ erfüllt ist, bleibt p ein Primzahlkandidat. Erst nimmt man ein anderes a. Wenn wieder 1 heraus kommt, wendet man schließlich aufwendigere Primzahlprüfer auf p an.

(10) Def.: Nicht-Primzahlen, die für ein $a \in \mathbb{Z}_p^*$ liefern, dass $a^{p-1} \underset{p}{\equiv} 1$ ist, heißen fermatsche Pseudoprimzahlen. Erfüllen sie die Fermatsche Gleichung immer, ohne, dass sie selbst Primzahlen sind, heißen sie Carmichael-Zahlen. (Info Wikipedia)

Beispiele 341 ist Pseudoprimzahl, denn 341=11*31, also keine Primzahl. Dennoch gilt $2^{340} \underset{341}{\equiv} 1$, geprüft mit TI pmod(2,340,341), aber mit Basis 3 hat man schon Erfolg.

561, 1105, 1729, 2465, 2821, sind Carmichael-Zahlen, probieren sie einige Beispiele.

Algebra: Inversenbestimmung und Gleichungen in $\mathbb{Z}_m^*$

Alle primen Restklassengruppen $\left(\mathbb{Z}_m^*,\cdot\right)$ sind wirklich Gruppen im Sinne der Algebra, also gibt es zu jedem Element a ein Inverses $\overline{a}$ mit $a\cdot\overline{a}=1$

Man schreibt auch oft a^{-1} statt $\overline{a}$, jedoch denken Unerfahrene dann an Brüche, die gibt es aber in der Zahlentheorie nicht.

Beschaffung von Inversen:

(1) In den **Maltafeln** findet man bei jeder 1 in der Tafel ein Paar von zueinander inversen Elementen beim Zeilen- und Spalteneingang. Z. B. sind 5 und 7 zueinander invers in $\mathbb{Z}_{17}^*$, Probe $5\cdot 7=35=34+1\underset{17}{\equiv}1$

(2) In den **Potenz-Tafeln** stehen in vorletzten Zeile die Inversen zu den Elementen in der Eingangszeile.

Zu a ist $a^{\varphi(m)-1}$ invers, denn nach dem Eulerschen Satz ist das Produkt dieser beiden Elemente 1.

Auch **ohne Potenzentafel** kann man $a^{\varphi(m)-1}$ berechnen und hat dann das Inverse zu a. Nehmen wir z.B. $m=143=11\cdot 13$ Dann ist nach Seite 14 (4)b $\varphi(m)=(p-1)\cdot(q-1)=10\cdot 12=120$. Zu $a=111$ ist dann

$\overline{a}=111^{119}\bmod 143=67$ das Inverse. (Berechnet mit pmod(111,67,143))

Probe $111\cdot 67\ \mathit{modulo}\ 143=1$ (Berechnet mit mod(111*67,143))

Kennt man m aber nicht $\varphi(m)$, so beschafft man es mit eulerphi(m)

(3) Man kann das Inverse mit dem **erweiterten Euklidischen Algorithmus** und der Vielfachsummendarstellung beschaffen. Zu m und a bestimmt man $1=s\cdot m+t\cdot a$ Mit ggte(m,a) erhält man die Liste [1,s,t]. Wenn t positiv ist, ist es das Inverse, anderenfalls ist $t+m$ das Inverse.

Beweis: $1=s\cdot m+t\cdot a\underset{m}{\equiv}0+t\cdot a=t\cdot a$. Im Beispiel: ggte(143,111) ergibt [1, -52, 67], also ist 67 das Inverse zu 111.

In den großen CAS ist der erweiterte Euklidische Algorithmus vorgesehen: In maxima: gcdex(143,111) ergibt [-52,67,1] , in MuPAD igcdex(….) in Mathematica ExtendedGCD[143,111] ergibt {1,{-52,67}}

Am TI (alle CAS-Versionen) ist ggte(…) zusätzlich programmiert, download von obiger Site. Das gilt auch für pmod, das in maxima, MuPAD und Mathematica powermod heißt.

(4) Gleichungen der Bauart $a\cdot x=c$ in $\mathbb{Z}_m^*$ werden nach x aufgelöst durch $x=\overline{a}\cdot c$.

(5) Für Gleichungen der Bauart $x^2=c$ oder $x^k=c$ oder $a^x=c$ gibt es in $\mathbb{Z}_m^*$ keine Lösungsverfahren außer dem Nachsehen in Tafeln und dem Probieren. Man sagt: diskretes Wurzelziehen und diskretes Logarithmieren sind nicht effektiv möglich.

Algebra Speziell für Kryptografie $\mathbb{Z}_n^*$ mit $n = p \cdot q$ Primzahlprodukt

Zahlen-Tafel bis 5 *mal* 7

$$(\%o14)\quad \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 8 & 9 & 10 & 11 & 12 & 13 & 14 \\ 15 & 16 & 17 & 18 & 19 & 20 & 21 \\ 22 & 23 & 24 & 25 & 26 & 27 & 28 \\ 29 & 30 & 31 & 32 & 33 & 34 & 35 \end{bmatrix}$$

ZahlenTafel modulo 5

$$(\%o15)\quad \begin{bmatrix} 1 & 2 & 3 & 4 & 0 & 1 & 2 \\ 3 & 4 & 0 & 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 & 4 & 0 & 1 \\ 2 & 3 & 4 & 0 & 1 & 2 & 3 \\ 4 & 0 & 1 & 2 & 3 & 4 & 0 \end{bmatrix}$$

ZahlenTafel modulo 7

$$(\%o16)\quad \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 0 \end{bmatrix}$$

Zahlen-Tafel bis 3 *mal* 5

$$(\%o9)\quad \begin{bmatrix} 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 10 \\ 11 & 12 & 13 & 14 & 15 \end{bmatrix}$$

ZahlenTafel modulo 3

$$(\%o10)\quad \begin{bmatrix} 1 & 2 & 0 & 1 & 2 \\ 0 & 1 & 2 & 0 & 1 \\ 2 & 0 & 1 & 2 & 0 \end{bmatrix}$$

ZahlenTafel modulo 5

$$(\%o11)\quad \begin{bmatrix} 1 & 2 & 3 & 4 & 0 \\ 1 & 2 & 3 & 4 & 0 \\ 1 & 2 & 3 & 4 & 0 \end{bmatrix}$$

$p = 3 \quad q = 5$

Es gibt $n = p \cdot q = 15$ Zahlen in der Tafel, 3 Zeilen, 5 Spalten. Es gibt in jeder Spalte ein Vielfaches von 3, sichtbar an der 0 in der zweiten Tafel, also 5 Vielfache von 3. Es gibt 3 Zeilen, an jedem Zeilenende steht ein Vielfaches von 5, also 3 Nullen in der dritten Tafel. Also gibt es zusammen 5+3-1=7 Nullen, wenn man die Ecke rechts unten nicht doppelt zählt. Bleiben 15-7= 8 Zahlen, die teilefremd zu 15 sind.

Allgemein:

$\varphi(n) = \varphi(p \cdot q) =$

$p \cdot q - (q + p - 1) =$

$p \cdot q + q - p + 1 =$

$(p-1) \cdot (q-1)$

Zahlen-Tafel bis 11 *mal* 13

$$(\%o24)\quad \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 13 \\ 14 & 15 & 16 & 17 & 18 & 19 & 20 & 21 & 22 & 23 & 24 & 25 & 26 \\ 27 & 28 & 29 & 30 & 31 & 32 & 33 & 34 & 35 & 36 & 37 & 38 & 39 \\ 40 & 41 & 42 & 43 & 44 & 45 & 46 & 47 & 48 & 49 & 50 & 51 & 52 \\ 53 & 54 & 55 & 56 & 57 & 58 & 59 & 60 & 61 & 62 & 63 & 64 & 65 \\ 66 & 67 & 68 & 69 & 70 & 71 & 72 & 73 & 74 & 75 & 76 & 77 & 78 \\ 79 & 80 & 81 & 82 & 83 & 84 & 85 & 86 & 87 & 88 & 89 & 90 & 91 \\ 92 & 93 & 94 & 95 & 96 & 97 & 98 & 99 & 100 & 101 & 102 & 103 & 104 \\ 105 & 106 & 107 & 108 & 109 & 110 & 111 & 112 & 113 & 114 & 115 & 116 & 117 \\ 118 & 119 & 120 & 121 & 122 & 123 & 124 & 125 & 126 & 127 & 128 & 129 & 130 \\ 131 & 132 & 133 & 134 & 135 & 136 & 137 & 138 & 139 & 140 & 141 & 142 & 143 \end{bmatrix}$$

ZahlenTafel modulo 11

$$(\%o25)\quad \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 0 & 1 & 2 \\ 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 0 & 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 & 9 & 10 & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\ 7 & 8 & 9 & 10 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 9 & 10 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 0 & 1 \\ 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 & 8 & 9 & 10 & 0 & 1 & 2 & 3 & 4 & 5 \\ 6 & 7 & 8 & 9 & 10 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 8 & 9 & 10 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 10 & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 0 \end{bmatrix}$$

$$\boxed{\varphi(p \cdot q) = (p-1) \cdot (q-1)}$$

ZahlenTafel modulo 13

$$(\%o26)\quad \begin{bmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 0 \\ 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 & 0 \end{bmatrix}$$

Wenn die Nullen der modulo-p-Tafel alle in die letzte Zeile sacken und man sie dann in die letzte Zeile der modulo-q-Tafel schreibt, hat man ein Zahlenfeld von $(p-1)(q-1)$ Zahlen ohne Nullen.

Algebra-Aufgaben zum Kryptografie-Heft Seiten 13 und 14

kry\malstern(22) und kry\potstern(22) sind hier rechts angegeben.
Stellen Sie jeweils die Maltafel der von a erzeugten Untergruppe auf.

$$\begin{bmatrix} 1 & 3 & 5 & 7 & 9 & 13 & 15 & 17 & 19 & 21 \\ 3 & 9 & 15 & 21 & 5 & 17 & 1 & 7 & 13 & 19 \\ 5 & 15 & 3 & 13 & 1 & 21 & 9 & 19 & 7 & 17 \\ 7 & 21 & 13 & 5 & 19 & 3 & 17 & 9 & 1 & 15 \\ 9 & 5 & 1 & 19 & 15 & 7 & 3 & 21 & 17 & 13 \\ 13 & 17 & 21 & 3 & 7 & 15 & 19 & 1 & 5 & 9 \\ 15 & 1 & 9 & 17 & 3 & 19 & 5 & 13 & 21 & 7 \\ 17 & 7 & 19 & 9 & 21 & 1 & 13 & 3 & 15 & 5 \\ 19 & 13 & 7 & 1 & 17 & 5 & 21 & 15 & 9 & 3 \\ 21 & 19 & 17 & 15 & 13 & 9 & 7 & 5 & 3 & 1 \end{bmatrix}$$

$$\begin{bmatrix} 1 & 1 & 3 & 5 & 7 & 9 & 13 & 15 & 17 & 19 & 21 \\ 2 & 1 & 9 & 3 & 5 & 15 & 15 & 5 & 3 & 9 & 1 \\ 3 & 1 & 5 & 15 & 13 & 3 & 19 & 9 & 7 & 17 & 21 \\ 4 & 1 & 15 & 9 & 3 & 5 & 5 & 3 & 9 & 15 & 1 \\ 5 & 1 & 1 & 1 & 21 & 1 & 21 & 1 & 21 & 21 & 21 \\ 6 & 1 & 3 & 5 & 15 & 9 & 9 & 15 & 5 & 3 & 1 \\ 7 & 1 & 9 & 3 & 17 & 15 & 7 & 5 & 19 & 13 & 21 \\ 8 & 1 & 5 & 15 & 9 & 3 & 3 & 9 & 15 & 5 & 1 \\ 9 & 1 & 15 & 9 & 19 & 5 & 17 & 3 & 13 & 7 & 21 \\ 10 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{bmatrix}$$

1.) Wählen Sie drei verschiedene a, die die Ordnung 2 , 5 und 10 haben sollen.
Übrigens: seq(mod(a^k,m),k,1,m), aber eine „von Hand“:

2.) Woran erkennen Sie, dass es sich um Gruppen handelt?

3.) Schreiben Sie jeweils alle Nebenklassen auf.

4.) Machen Sie sich klar: Nach der Definition in S.13 (5) ist auch <a> selbst eine Nebenklasse von <a>. Nennen wir die anderen Nebenklassen "echte Nebenklassen".

5.) Wieviele Elemente haben die Nebenklassen aus 3) und wieviele Nebenklassen gibt es jeweils?

6.) Warum kann man wirklich das Wort "Klassen" für die Nebenklassen verwenden?

7.) Machen Sie sich den Zusammenhang zwischen den Anzahlen der Elemente in <a>, Anzahl der Nebenklassen von <a>, Anzahl der Element in G, Anzahl der Elemente in den Nebenklassen, Anzahl der echten Nebenklassen und der Ordnung von a für Ihre drei a oben und allgemein klar.

8.) Gibt es in $\mathbb{Z}_{22}^{*}$ eine Zahl. die den Kleinen Fermatsche Satz $\boxed{a^{20} \underset{22}{\equiv} 1}$ erfüllt? Suchen Sie in den Potenztafeln der Seiten 12 a,b,c Zahlen, die $\boxed{a^{m-1} \underset{m}{\equiv} 1}$ erfüllen. Können Sie eine Vermutung äußern?

9.) Bestätigen Sie die Behauptung Seite 14 Satz 4b an den Beispielen der Seiten 12 a,b,c. Sehen Sie sich sorgfältig den Beweis dieses Stzes auf Seite 16 an. Geben Sie eine verbale Begründung.

Algebra-Zahlentheorie Aufgaben

(1) Führen Sie den erweiterten euklidischen Algorithmus vollständig von Hand durch für das Zahlenpaar (223, 70)
Prüfen Sie mit TI durch Eingabe von ggte(223,70)
Prüfen Sie in wxMaxima mit gcdex(223,70)
gcd=greatest common divisor=ggt, ex=extended=erweitert)
Bestimmen Sie von Hand 223 modulo 70.
TI: mod(223,70) wxMaxima mod(223,70)

“von Hand” heißt: mit allen Zwischenschritten

(2) Bestimmen Sie auf alle!!! auf Seite 15 vorgestellten Arten das Inverse von 13 modulo 70 und prüfen Sie von Hand.

(3) Zerlegen Sie 70 in Primfaktoren (sinnvoll von Hand).
Mit CAS: factor(70)
Geben Sie begründet (mit systematischer Primfaktoren-Auswahl) alle Teiler von 70 an. Mit TI teiler(70) (Ha-Krypto-Tool) wxMaxima divisors(70)

(4) Geben Sie von Hand durch einige Worte begründet die ersten 10 zu 70 teilerfremden Zahlen an.
Bestimmen Sie mit CAS die Menge Z*(70).
Mit TI zstern(70) (Ha-Krypto-Tool) mit wxMaxima zstern(70) (Ha-entpr. Datei)

(5) Bestimmen Sie mit CAS die Anzahl der zu 70 teilerfremden Zahlen.
Mit TI euler(70), wxMaxima eulerphi(70) (Ha-entpr. Datei)

(6) Geben Sie eine Liste der Potenzen von 13 modulo 70 an.
TI: seq (mod(13^k ,70) , k, 0,24) seq=sequence=Folge
wxMaxima makelist(mod(13^k, 70) ,k,0,24)

(7) Lesen Sie aus ihrer Liste die Ordnung von 13 in Z*(70) ab.
Mit TI ordo(13,17) (Ha-Krypto-Tool) wxMaxima ordo(13,70)

(8) Taufen Sie die von 13 in Z*(70) erzeugte Untergruppe grup.
Bestimmen Sie die Nebenklassen von <13> in Z*(70)
Verwenden Sie bei TI mod(a*grup,70) bei wxMaxima mod(a*grup,70)

(9) Lösen Sie von Hand in Z*(70) die Gleichung 13*x=19.

(10) Geben Sie in Z*(70) einige Quadratzahlen an, die in Z nicht Quadratzahlensind. (Von Hand)

(11) Wählen Sie selbst teilerfremde Zahlenpaare (nicht zu klein) entsprechend (223,70) und (13,70), bearbeiten Sie die Seite ebenso.
Prüfen Sie alles selbst.