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

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.

$Z_m^* := \{r \in Z_m \,|\, ggT(r,m)=1\}$ =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

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

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

$$\Rightarrow (p_g \,|\, a \wedge p_g \,|\, m) \vee (p_g \,|\, b) \wedge p_g \,|\, m) \Rightarrow p_g \,|\, ggT(a,m) \vee p_g \,|\, ggT(b,m)$$ 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)