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.