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 $111 \cdot 67$ *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.