vhb - Kurs: Grundlagen der elementaren Zahlentheorie

III.4. Rechnen mit Restklassen - Exkurs: Wichtige Sätze zu Restklassen

Das von Gauß eingeführte Restklassenkalkül erweist sich als äußerst nützlich in der Zahlentheorie. Um noch weiter Eigenschaften von Restklassen kennenzulernen, klassifizieren wir diese wie folgt: Eine Restklasse a mod m heißt **prim**, wenn a und m teilerfremd sind. Wegen ggT$(a+km,m)$=ggT(a,m) ist entweder jedes Element einer Restklasse oder keines teilerfremd zum Modul m. Die primen Restklassen modulo $m=8$ sind damit

$$1,\ 3,\ 5,\ 7 \mod 8$$

Die Menge der primen Restklassen modulo m ist offensichtlich multiplikativ abgeschlossen (denn mit a und b ist auch das Produkt ab teilerfremd zu m). Die Anzahl $\varphi(m)$ der primen Restklassen mod m zählt die **Eulersche φ -Funktion**. Es gelten

$$\varphi(8)=4\,,\ \varphi(10)=4 \quad \text{und} \quad \varphi(2^k)=2^{k-1}$$

bzw.

$$\varphi(p)=p-1 \quad \text{und} \quad \varphi(p^k)=p^k(1-1/p)$$

für Primzahlen p.

Satz (Satz von Euler, 1750): Für teilerfremde a und m gilt

$$a^{\varphi(m)} \equiv 1 \bmod m.$$

Beweis. Es sei

$$A := \prod_{\substack{1\le b<m,\\ ggT(b,m)=1}} b$$

das Produkt aller primen Restklassen b mod m. Weil mit b auch ab alle primen Restklassen modulo m durchläuft (da a zu m teilerfremd ist), gilt

$$\prod_{\substack{1\le b<m,\\ ggT(b,m)=1}} b \equiv \prod_{\substack{1\le b<m,\\ ggT(b,m)=1}} ab = a^{\varphi(m)} \prod_{\substack{1\le b<m,\\ ggT(b,m)=1}} b \mod m$$

bzw.

$$A \equiv a^{\varphi(m)} A \mod m\ .$$

Weil A (faktorweise) teilerfremd zu m ist, folgt nach Kürzen $1 \equiv a^{\varphi(m)}$ mod m, also die Behauptung.

Korollar (Kleiner Fermatscher Satz): Sei p eine Primzahl und p teilerfremd zu a. Dann gilt

$$a^{p-1} \equiv 1 \bmod p\ .$$

Ohne Voraussetzung an a kann man dies auch so formulieren: $a^p \equiv a \mod p$.

Der irreführende Name 'kleiner Fermat' bezieht sich auf den so genannten 'großen Fermatschen Satz', die Fermatsche Vermutung, die erst seit einigen Jahren tatsächlich diesen Namen tragen darf (weil sie zuvor nur eine unbewiesene Vermutung war).

Mit dem folgenden Satz lassen sich Primzahlen charakterisieren:

Satz (Satz von Wilson): Es ist p genau dann eine Primzahl, wenn

$$(p-1)! \equiv -1 \mod p.$$

Beweis. Besitzt p einen echten Primteiler q, so kommt dieser unter den Faktoren von $(p-1)!$ vor und es gilt $q|(p-1)!$. Insbesondere folgt $(p-1) \not\equiv -1 \mod p$ (denn $-1 \mod p$ ist eine prime Restklasse). Ist hingegen $p > 2$ prim, dann können wir Paare von Restklassen a, $b \mod p$ finden, so dass $ab \equiv 1 \mod p$ gilt; b ist dann das multiplikativ Inverse von $a \mod p$ und umgekehrt. Damit entstehen viele Paare, deren Produkt jeweils $\equiv 1 \mod p$ ist. Hiervon sind lediglich jene Restklassen auszuschließen, für die $a^2 \equiv 1 \mod p$ gilt (denn diese sind 'selbstinvers'). Nun ist

$$a^2 \equiv 1 \quad \Leftrightarrow \quad (a-1)(a+1) = a^2 - 1 \equiv 0 \mod p,$$

was auf $a \equiv 1$ oder aber $a \equiv p-1 \mod p$ führt. Damit gilt also $(p-1)! \equiv (p-1) \equiv -1 \mod p$ und der Satz ist bewiesen.

Welche linearen Kongruenzen sind lösbar? Hierzu liefert der nächste Satz eine Lösung:

Satz: Die Kongruenz

$$aX \equiv b \mod m$$

ist genau dann lösbar, wenn $ggT(a,m)|b$. In diesem Fall gibt es genau $ggT(a,m)$ inkongruente Lösungen modulo m.

Beweis. Nach dem Satz von Bezout ist die lineare diophantische Gleichung $aX = b + mY$ bzw. $aX - mY = b$ genau dann lösbar, wenn b ein Vielfaches von $ggT(a,m)$ ist. In diesem Fall existieren also ganze Zahlen x und y, so dass $ax = b + my$ bzw. $ax \equiv b \mod m$. Damit ist eine lösende Restklasse modulo m gefunden. Die weiteren Lösungen ergeben sich mittels der Kürzungsregel für Kongruenzen.