**Kleiner Satz von Fermat**



Hilfssatz: $\binom{n}{m}$ ist durch n teilbar, sofern n eine Primzahl und $0 < m < n$ ist.

Beweis: $\binom{n}{m} = \frac{n!}{(n-m)!\ m!} = \frac{n(n-1)(n-2)\ldots(n-m+1)}{1\cdot 2\cdot 3\cdot\ldots\cdot m}$ ist in jedem Fall ganzzahlig.

Falls n prim und m<n, findet sich im Nenner kein Faktor zum Kürzen von n im Zähler.
Also muß nach vollständigem Kürzen aller Faktoren des Nenners n noch Teiler sein.

Satz (Fermat): $\mathbf{k^p \equiv k \bmod p}$

Beweis (Vollständige Induktion über k):

Induktions-Anfang: k=0: $0^p = 0 \equiv 0 \bmod p$

Induktions-Schritt: $k^p \equiv k \bmod p \Rightarrow (k+1)^p \equiv k+1 \bmod p$:

$$(k+1)^p = \binom{p}{0}k^p + \binom{p}{1}k^{p-1} + \binom{p}{2}k^{p-2} + \ldots + \binom{p}{p-1}k^1 + \binom{p}{p}k^0 \qquad \text{(Binomischer Lehrsatz)}$$

$$= 1\cdot k^p + p\cdot k^{p-1} + \binom{p}{2}k^{p-2} + \ldots + p\cdot k + 1\cdot k^0$$

$$= \underbrace{k^p}_{\equiv k \text{ nach Induktions-voraussetzung}} + \underbrace{p\cdot k^{p-1} + \binom{p}{2}k^{p-2} + \ldots + p\cdot k}_{\text{alle Summanden sind teilbar durch p wegen der Binomialkoeffizienten (s.o.: Hilfssatz)}} + 1$$

$$\equiv k + 0 + 0 + \ldots + 0 + 1 \bmod p$$

$$\equiv k+1 \bmod p$$

$\Rightarrow k^p \equiv k \bmod p \quad \forall\, k \geq 0$ und p prim

bzw.

$k^{p-1} \equiv 1 \bmod p$ (falls $k \not\equiv 0 \bmod p$. Das folgt nach Division durch k aus der ersten Version)

Bsp.:

| | | | | |
|---|---|---|---|---|
| $0^7 =$ | $0 =$ | $0\cdot 7 + 0$ | $\Rightarrow$ | $0^7 \equiv 0 \bmod 7$ |
| $1^7 =$ | $1 =$ | $0\cdot 7 + 1$ | $\Rightarrow$ | $1^7 \equiv 1 \bmod 7$ |
| $2^7 =$ | $128 =$ | $18\cdot 7 + 2$ | $\Rightarrow$ | $2^7 \equiv 2 \bmod 7$ |
| $3^7 =$ | $2187 =$ | $312\cdot 7 + 3$ | $\Rightarrow$ | $3^7 \equiv 3 \bmod 7$ |
| $4^7 =$ | $16384 =$ | $2340\cdot 7 + 4$ | $\Rightarrow$ | $4^7 \equiv 4 \bmod 7$ |
| $5^7 =$ | $78125 =$ | $11160\cdot 7 + 5$ | $\Rightarrow$ | $5^7 \equiv 5 \bmod 7$ |
| $6^7 =$ | $279936 =$ | $39990\cdot 7 + 6$ | $\Rightarrow$ | $6^7 \equiv 6 \bmod 7$ |