32. Die multiplikative Gruppe

Schreibweise:
$g \in G, n \in \mathbb{N}$
$g^n = g \circ ... \circ g$ (n-mal)
$g^\circ = e$ (neutrales Element)
$g^{n+1} := g^n \circ g$
$n \in \mathbb{Z} : g^n := (g^{-n})^{-1} \quad (n < 0)$
$\mathbb{Z}_6 \to 2$ hat kein Inverses

Definition: Eine Zahl $a \in \mathbb{Z}_n \ \{0\}$ heißt Nullteiler, wenn es ein $b \in \mathbb{Z}_n \ \{0\}$ gibt, sodass $a \cdot b = 0 (mod\ n)$.

Beispiel: 2 ist Nullteiler von $\mathbb{Z}_6$.

Definition: Eine Zahl $a \in \mathbb{Z}_n$ heißt Einheit, wenn es eine Zahl $b \in \mathbb{Z}_n$ gibt mit $a \cdot b \equiv 1 (mod\ n)$.

Lemma: Eine Zahl $m \in \mathbb{Z}_n \ \{0\}$ ist Einheit genau dann, wenn m und n teilerfremd.
Beweis: ($\Rightarrow$) Es gibt ein $b \in \mathbb{Z}_n$ mit $m \cdot b \equiv 1\ mod\ n$
$m \cdot b - 1 = a \cdot n$ für alle $a \in \mathbb{Z}$
$1 = mb - an$
$\Rightarrow ggt(m, n) = 1$
($\Leftarrow$) Seien m und n teilerfremd.
Bézout: $a \cdot m + b \cdot n = 1 \qquad (a, b \in \mathbb{Z})$
Behauptung: a ist multiplikatives Inverses zu m
$m \cdot a = 1 - bn$
$\equiv 1\ mod\ n \qquad \square$
Die Menge aller Einheiten bildet bzgl. der Multiplikation eine Gruppe $\mathbb{Z}_n^* (in\ \mathbb{Z}_n)$

1. Assoziativgesetz vererbt sich
2. neutrales Element
3. inverses Element: zu a gibt es b (Inverses) mit $a \cdot b \equiv 1\ mod\ n$
4. $G^2 \mapsto G$
5. a,b Einheiten zz.: $a \cdot b$ Einheit. Es gibt a^{-1}, b^{-1} mit $aa^{-1} = 1 = bb^{-1}$

Inverse: $(a \cdot b) \cdot (b^{-1} \cdot a^{-1} = \frac{a \cdot (bb^{-1}{}^{-1}}{a} 1$
$= aa^{-1}$
$= 1$

Inverses: $(a \cdot b)^{-1} := b^{-1}a^{-1}$

Eulersche Φ-Funktion

Wie groß ist die multiplikative Gruppe $\mathbb{Z}_n^*$ von $\mathbb{Z}$?

n	2	3	4	5	6
$\Phi(n)$	1	2	2	4	2

$= |\mathbb{Z}_n^*|$

Hat $n \in \mathbb{N}$ die Primfaktorzerlegung $n = p_1^{\alpha_1} \cdot (...) \cdot p_n^{\alpha_n}$
dann gilt: $\Phi(n) = (p_1 - 1)p_1^{\alpha_1 - 1} \cdot (...) \cdot (p_{n-1})p_n^{\alpha_n - 1}$

Beispiel: $n = 6 = 2(= p_1) \cdot 3(= p_2)$
$\Phi(6) = (2-1) \cdot 2^0 \cdot (3-1) \cdot 3^0 = 1 \cdot 2 \cdot 1 = 2$

Für kleine n einfache Formel. Für große n Problem, da Primfaktorzerlegung (noch) nicht berechenbar.