Beweis des Satzes von Euler

$(\mathbb{Z}/n\mathbb{Z})^*$ hat $\varphi(n)$ Elemente $g_1, g_2, \ldots, g_{\varphi(n)}$.

Nach Teil c) des Satzes aus Einheit 26 definiert $x \mapsto ax$ eine Bijektion auf $\mathbb{Z}/n\mathbb{Z}$ und daher auch auf $(\mathbb{Z}/n\mathbb{Z})^*$.

Also gilt:

$$(\mathbb{Z}/n\mathbb{Z})^* = \{g_1, g_2, \ldots, g_{\varphi(n)}\} = \{ag_1, ag_2, \ldots, ag_{\varphi(n)}\}$$

Wir definieren g als das Produkt aller Elemente von $(\mathbb{Z}/n\mathbb{Z})^*$. Dann folgt:

$$g = \prod_{i=1}^{\varphi(n)} ag_i = a^{\varphi(n)} \prod_{i=1}^{\varphi(n)} g_i = a^{\varphi(n)} g$$

Diese Berechnungen sind natürlich modulo n zu verstehen.

Da g invertierbar ist, folgt die Behauptung.

Wie berechnet man $\varphi(n)$?

Wir zeigen zunächst, dass für teilerfremde Zahlen m und n gilt:

$$\varphi(mn) = \varphi(m)\varphi(n)$$

Denn der Isomorphismus zwischen $\mathbb{Z}/mn\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, den wir aus dem Chinesischen Restsatz kennen, bildet Einheiten auf Einheiten ab. Also liefert die Einschränkung auf $(\mathbb{Z}/mn\mathbb{Z})^*$ einen Isomorphismus zwischen $(\mathbb{Z}/mn\mathbb{Z})^*$ und $(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*$, d.h.

$$\varphi(mn) = |(\mathbb{Z}/mn\mathbb{Z})^*| = |(\mathbb{Z}/m\mathbb{Z})^* \times (\mathbb{Z}/n\mathbb{Z})^*| = \varphi(m)\varphi(n)$$

Daher gilt mit der Primfaktorzerlegung $n = p_1^{e_1} \cdots p_r^{e_r}$ die Formel:

$$\varphi(n) = \varphi(p_1^{e_1}) \cdots \varphi(p_r^{e_r})$$

und aus der letzten Einheit kennen wir bereits die Werte $\varphi(p^e)$ für Primzahlen p. Daraus folgt die Formel $\varphi(n) = n \cdot \prod_{p|n} (1 - \frac{1}{p})$

Noch ein Satz über die φ-Funktion

Satz: $\sum_{t|n} \varphi(t) = n$

Beachte, dass t hier von 1 bis n alle Teiler von n durchläuft!

Zum Beweis betrachtet man die Menge $N = \{\frac{0}{n}, \frac{1}{n}, \ldots, \frac{n-1}{n}\}$.

Nun kürzen wir alle Brüche in N, dann erhalten wir Brüche, deren Nenner Teiler von n sind und deren Zähler teilerfremd zum jeweiligen Nenner sind.

Für jeden Teiler t von n enthält N genau $\varphi(t)$ viele Brüche mit Nenner t. Und insgesamt sind es n Brüche.

Damit folgt die Behauptung!

Beispiel: $n = 12$, $N = \{\frac{0}{1}, \frac{1}{12}, \frac{1}{6}, \frac{1}{4}, \frac{1}{3}, \frac{5}{12}, \frac{1}{2}, \frac{7}{12}, \frac{2}{3}, \frac{3}{4}, \frac{5}{6}, \frac{11}{12}\}$

Verallgemeinerung des Satzes von Euler

Der folgende Satz verallgemeinert den kleinen Satz von Fermat und den Satz von Euler:

Satz: Für jede kommutative Gruppe G und jedes $a \in G$ gilt: $a^{|G|} = 1$

Wie in den Spezialfällen beweisen wir auch diesen Satz, indem wir die Gruppe G einmal als $\{b_1, \ldots, b_{|G|}\}$ schreiben, und dann als $\{ab_1, \ldots, ab_{|G|}\}$. Da a invertierbar ist, sind diese beiden Mengen gleich, d.h. das Produkt aller Elemente hat jeweils den selben Wert. Daher muss $a^{|G|} = 1$ gelten.

Dieser Satz gilt übrigens auch für beliebige endliche Gruppen.

In dieser allgemeineren Form heißt er Satz von Lagrange.

Ein exaktes Primzahlzertifikat

Satz: Es sei $n \geq 2$, $n \in \mathbb{N}$. Falls für alle Primzahlen p mit $n \equiv 1 \bmod p$ eine Zahl $a \in \mathbb{Z}$ existiert, so dass

$$a^{n-1} \equiv 1 \bmod n \quad \text{und} \quad a^{\frac{n-1}{p}} \not\equiv 1 \bmod n$$

gilt, dann ist n eine Primzahl.

Bemerkung (ohne Beweis): Dieses Kriterium erfüllen alle Primzahlen.

Zum Beweis des Satzes genügt es zu zeigen, dass $\varphi(n)$ durch $n-1$ teilbar ist. Dazu zeigen wir für jede Primzahl p:

$$p^r \mid n-1 \quad \Longrightarrow \quad p^r \mid \varphi(n)$$

Denn daraus folgt, dass $n-1$ ein Teiler von $\varphi(n)$ ist, aber es gilt ja immer $\varphi(n) < n$, also folgt $\varphi(n) = n-1$, d.h. n ist prim.

Beweis

Sei p ein beliebiger Primteiler von $n-1$, und sei p^r die größte Potenz von p, die in $n-1$ aufgeht. Wir wählen eine ganze Zahl a gemäß der Voraussetzung, d.h. $a^{n-1} \equiv 1 \bmod n$, aber $a^{\frac{n-1}{p}} \not\equiv 1 \bmod n$. Ferner sei m die *Ordnung von* a, d.h. die kleinste positive ganze Zahl mit $a^m \equiv 1 \bmod n$.

Da a teilerfremd zu n ist, gilt auch $a^{\varphi(n)} \equiv 1 \bmod n$.

Damit ist m sowohl Teiler von $n-1$, als auch Teiler von $\varphi(n)$.
Andererseits ist m nicht Teiler von $\frac{n-1}{p}$, daher teilt p^r auch m.

Nun ist p^r ein Teiler von m und m ein Teiler von $\varphi(n)$, also teilt p^r auch $\varphi(n)$, wie zu beweisen war.