Beweis

Für $n = 1$ existiert nur die Darstellung $1 = \prod p^0$, d.h. $n_p = 0$ für alle Primzahlen p.
Sei nun $n > 1$, dann existiert eine Primzahl p, die n teilt.
Nach Induktionsvoraussetzung hat n/p eine Primfaktorzerlegung, also auch n, da es $p \cdot (n/p)$ ist. Zu zeigen bleibt die Eindeutigkeit:

Angenommen, es gibt zwei verschiedene Primfaktorzerlegungen von n, etwa

$$\prod p^{n_p} = \prod p^{n'_p}$$

dann dividieren wir beide Seiten durch gemeinsame Primteiler, bis es keine solchen mehr gibt. Nun haben wir zwei Produkte von Primzahlen, wobei keine Primzahl auf beiden Seiten vorkommt. Andererseits können beide Produkte nicht leer sein, ihr Wert ist also größer als 1. Ein beliebiger Primteiler des einen Produkts teilt aber nach der Folgerung aus Bézout's Lemma das andere Produkt nicht, da er keine der darin enthaltenen Primzahlen teilt, und folglich auch nicht deren Produkt.

Das ist ein Widerspruch, da beide Seiten gleich sind!

Modulare Arithmetik

Wir rechnen mit den sogenannten *Restklassen:*

Es sei $n \in \mathbb{N}$, $n \geq 1$. Betrachte für $k \in \mathbb{Z}$ die Menge $k + n\mathbb{Z}$:

$$k + n\mathbb{Z} = \{\ldots, k-2n, k-n, k, k+n, k+2n, k+3n, \ldots\}$$

Beachte: $(k + n\mathbb{Z}) \cap (\ell + n\mathbb{Z}) \neq \emptyset \iff k + n\mathbb{Z} = \ell + n\mathbb{Z} \iff n \,|\, (k - \ell)$

Wir definieren die Äquivalenzrelation $\equiv \pmod{n}$ durch

$$k \equiv \ell \mod n \iff k \in \ell + n\mathbb{Z}$$

Man überprüfe, dass das wirklich eine Äquivalenzrelation ist.

Zur Beachtung: Das ist zu unterscheiden von der Informatik-spezifischen Notation bei der durch $k \bmod n$ die eindeutig bestimmte nichtnegative Zahl kleiner als n gemeint ist, die in $k + n\mathbb{Z}$ liegt.

Restklassenring $\mathbb{Z}/n\mathbb{Z}$

Aus den Restklassen bilden wir den *Restklassenring* $\mathbb{Z}/n\mathbb{Z}$:

Addition:

$$(k + n\mathbb{Z}) + (\ell + n\mathbb{Z}) = k + \ell + n\mathbb{Z}$$

Für diese Definitionen ist jeweils die Wohldefiniertheit zu prüfen. (Bitte selbst machen.)

Multiplikation:

$$(k + n\mathbb{Z}) \cdot (\ell + n\mathbb{Z}) = k \cdot \ell + n\mathbb{Z}$$

Die Gültigkeit der Ringaxiome ist leicht nachzuweisen.

Die *multiplikative Gruppe* in $\mathbb{Z}/n\mathbb{Z}$ besteht aus den invertierbaren Elementen (bzgl. der Multiplikation), bezeichnet mit $(\mathbb{Z}/n\mathbb{Z})^*$.

Die Elemente von $(\mathbb{Z}/n\mathbb{Z})^*$ werden auch als *Einheiten* im Ring $\mathbb{Z}/n\mathbb{Z}$ bezeichnet.

Wichtige Eigenschaften

Für den Ring $\mathbb{Z}/n\mathbb{Z}$ und seine Einheitengruppe $(\mathbb{Z}/n\mathbb{Z})^*$ gilt:

Satz: a) $(\mathbb{Z}/n\mathbb{Z})^* = \{k + n\mathbb{Z} \mid ggT(k,n) = 1\}$

b) $\mathbb{Z}/n\mathbb{Z}$ ist Körper, gdw. n ist Primzahl

c) $x \mapsto kx$ auf $\mathbb{Z}/n\mathbb{Z}$ bijektiv, gdw. $ggT(k,n) = 1$

Beweis: a) k ist invertierbar genau dann, wenn ein a existiert mit $ak \equiv 1 \bmod n$, also genau dann, wenn a und b existieren mit $ak = 1 + bn$, also genau dann, wenn 1 eine Linearkombination von k und n ist, also genau dann, wenn k und n teilerfremd sind.

b) $\mathbb{Z}/n\mathbb{Z}$ ist Körper genau dann, wenn alle $k \in \mathbb{Z}/n\mathbb{Z} \setminus \{0\}$ invertierbar sind, also genau dann, wenn alle k mit $1 \leq k < n$ teilerfremd zu n sind, also genau dann, wenn n eine Primzahl ist.

c) Wenn $ggT(k,n) = 1$ ist, hat k ein Inverses, d.h. $x \mapsto kx$ hat eine Umkehrabbildung. Also ist die Abbildung bijektiv.
Wenn aber $ggT(k,n) = m > 1$, dann ist $k \cdot n/m = 0 = k \cdot 0$, d.h. die Abbildung ist nicht injektiv, da $0 < n/m < n$, also $n/m \neq 0$.

Ein zentrales Lemma

Lemma: Es seien m, n zwei teilerfremde ganze Zahlen.
Die folgende Abbildung π ist surjektiv:

$$\pi\colon\ \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$$
$$x \mapsto (x + m\mathbb{Z}, x + n\mathbb{Z})$$

Zwischen $\mathbb{Z}/mn\mathbb{Z}$ und $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ wird dadurch eine bijektive Abbildung induziert:

$$(x \bmod mn) \mapsto (x \bmod m, x \bmod n)$$

Die erste Aussage besagt, dass für $ggT(m, n) = 1$ zwei gleichzeitige Kongruenzen in $\mathbb{Z}$ immer lösbar sind, d.h. $\forall a, b \in \mathbb{Z}\ \exists x \in \mathbb{Z}$, so dass $x \equiv a \bmod m$ und $x \equiv b \bmod n$.

Die zweite Aussage bedeutet, dass die Abbildung surjektiv bleibt, wenn man sich auf die Zahlen $\{0, \ldots, mn - 1\}$ beschränkt. In diesem Fall wird die Abbildung sogar injektiv, also ist sie bijektiv.