Beweis des Lemmas

Wir beginnen mit der ersten Aussage, der Surjektivität von π:

Zu gegebenen ganzen Zahlen y und z suchen wir eine ganze Zahl x, so dass $\pi(x) = (y + m\mathbb{Z}, z + n\mathbb{Z})$ gilt.

Per Definition ist $\pi(x) = (x + m\mathbb{Z}, x + n\mathbb{Z})$. Zu zeigen ist also, dass es eine ganze Zahl x gibt, so dass $x + m\mathbb{Z} = y + m\mathbb{Z}$ und $x + n\mathbb{Z} = z + n\mathbb{Z}$, d.h. m teilt $x - y$ und n teilt $x - z$.

Da m und n teilerfremd sind, gibt es a, b mit $am + bn = 1$.

Wir wählen $x = zam + ybn$ und überprüfen, dass diese Zahl tatsächlich unsere Bedingungen erfüllt.

$$x - y = zam + y(bn - 1) = zam - yam = (za - ya)m$$
$$x - z = z(am - 1) + ybn = -zbn + ybn = (yb - zb)n$$

Also ist m Teiler von $x - y$ und n Teiler von $x - z$, wie verlangt.

Beweis (Forts.)

Nun fehlt noch der Beweis, dass die Einschränkung auf $\mathbb{Z}/mn\mathbb{Z}$ bijektiv ist.

1. Injektivität:

Sei $(x + m\mathbb{Z}, x + n\mathbb{Z}) = (y + m\mathbb{Z}, y + n\mathbb{Z})$, d.h. m teilt $x - y$ und n teilt $x - y$.
Da m und n teilerfremd sind, teilt auch mn die Differenz $x - y$.
Aber das bedeutet, dass in $\mathbb{Z}/mn\mathbb{Z}$ die Gleichheit $x = y$ gilt.

2. Surjektivität:

Sowohl der Urbildbereich $\mathbb{Z}/mn\mathbb{Z}$, wie auch der Bildbereich $\mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ haben mn Elemente. Bei endlichen gleichgroßen Bereichen ist aber jede injektive Abbildung automatisch auch surjektiv.

Damit ist die Bijektivität gezeigt.

Anwendungen der modularen Arithmetik

Schon die Zahlendarstellung im modernen Rechner stellt eine Anwendung modularer Arithmetik dar. Ein Byte hat z.B. 8 Bit. Wenn man nur mit Bytes rechnet, muss man modulo 256 rechnen. Allgemein: Bei einer sog. *Wortlänge* von k Bits rechnet man generell modulo 2^k. Details hierzu möge man dem Buch von Diekert, Kufleitner und Rosenberger entnehmen.

Stichwort: *Zweierkomplement.*

Weiteres Beispiel: Fehlererkennung bei Artikelnummern (EAN)
(13-stellig mit *13-Regel*)

Und auch die Matrikelnummern der Uni Stuttgart verwenden modulare Arithmetik, um eine Prüfnummer zu ermitteln – übrigens wird hier ein ähnliches Schema verwendet, wie bei Ausweisprüfnummern und bei Bahn-Card-Nummern, die sogenannte 137-Regel:

Eigentlich 6-stellige Nummer sei 471174. Mache daraus 471174p, so dass
$1 \cdot 4 + 3 \cdot 7 + 7 \cdot 1 + 1 \cdot 1 + 3 \cdot 7 + 7 \cdot 4 + 1 \cdot p \equiv 0 \bmod 10$

Lösung: $p = 8$

ISBN, IBAN

Recht bekannt ist die Prüfsumme beim ISBN-Code:

Eine korrekte 10-stellige ISBN (International Standard Book Numbering) ist eine Zahl $x_1x_2x_3x_4x_5x_6x_7x_8x_9x_{10}$, die die folgende Bedingung erfüllt:

$$1 \cdot x_1 + 2 \cdot x_2 + \cdots + 9 \cdot x_9 + 10 \cdot x_{10} \equiv 0 \mod 11$$

Dabei stehen die ersten 9 Ziffern für die sachlich-inhaltliche Einordnung (Land, Verlag, Buchnummer). Die letzte Ziffer ist die Prüfnummer, die aus dem Bereich $0, \ldots, 10$ kommt – da x_{10} manchmal den Wert 10 annimmt, muss für diesen das Zeichen X verwendet werden.

Die IBAN (International Bank Account Number) wird aus der BBAN (BLZ und 10-stellige Kontonummer) so gebildet: Vorangestellt zwei Buchstaben als Ländercode und eine zweistellige Prüfziffer PP, wobei die folgende 24-stellige Zahl kongruent zu 1 modulo 97 wird: BBBBBBBBKKKKKKKKKKLLCCPP.
In Deutschland (Code DE) ist LLCC=1314, allgemein A=10, B=11, etc.

Beispiel für simultane Kongruenz

Jetzt wollen wir das Lemma der letzten Einheit anwenden. Wenn man eine Zahl sucht, die kongruent zu y modulo m und kongruent zu z modulo n ist, so nehme man

$$zam + ybn$$

wobei $am + bn = 1$ gemäß dem Euklidischen Algorithmus.

Sei also $m = 9$ und $n = 11$, dann ist $5m - 4n = 1$.
Die Kongruenzen $x \equiv y \bmod 9$ und $x \equiv z \bmod 11$ werden also immer durch die Zahl $z \cdot 5m - y \cdot 4n$ gelöst.

Wollen wir also ein x mit $x \equiv 3 \bmod 9$ und $x \equiv 6 \bmod 11$, so wählen wir $x = 6 \cdot 45 - 3 \cdot 44 = 270 - 132 = 138$.

Da $mn = 99$ ist, können wir auch $138 - 99 = 39$ nehmen. Prüfen Sie das Resultat!