Diskrete Strukturen
Pflichtserie 12

Nikita Emanuel John Fehér, 3793479

27. Januar 2025
09:15-10:45 Dietzschold, Johannes

12.1
Zei $n \in \mathbb{N}$ mit $n > 1$, und sei $a \in \mathbb{Z}/n = \{0, 1, 2, ..., n-1\}$ so dass $\mathrm{ggt}(a, n) = 1$. Beweisen Sie, dass es existiert $b \in \mathbb{Z}/n$ so dass $ab \equiv 1 \mod n$.

$$\forall n \in \mathbb{N}, n > 0 : 1 \mod n = 1$$
$$\implies ab \equiv 1 \mod n$$

12.2

In der Vorlesung haben wir die Bezout-identität gesehen: falls $x, y \in \mathbb{N}$ und $\mathrm{ggt}(x, y) = 1$ dann wir können $u, v \in \mathbb{Z}$ finden mit $ux + vy = 1$. Wir haben auch gesehen, dass die Lösung (u, v) kann man effektiv finden, mitte des Euklidischen Algorthmus.

Seien jetzt $a, b \in \mathbb{N}$ mit $\mathrm{ggt}(a, b) = 1$, und seien $k \in \mathbb{Z}/a, l \in \mathbb{Z}/b$. Benutzen sie die Bezout-identität, um zu zeigen, dass es $X \in \mathbb{Z}$ existiert mit $X \equiv k \mod a$ and $X \equiv l \mod b$.

12.3

Seien p, q verschiedene Primzahlen and sei $n := pq$. Wie viele Elemente $a \in \mathbb{Z}/n$ gibt es mit der Eigenschaft $\mathrm{ggt}(a, pq) = 1$? Hinweis: betrachten Sie konkrete Beispiele von p und q um eine gute Hypothese erst zu stellen.

sei $X = |\{x \in \mathbb{Z}/p : \mathrm{ggt}(x, p) = 1\}|$
sei $Y = |\{y \in \mathbb{Z}/q : \mathrm{ggt}(y, q) = 1\}|$
sei $Z = |\{z \in \mathbb{Z}/pq : \mathrm{ggt}(z, pq) = 1\}|$

$$\begin{aligned}
\text{sei } p = 2, q = 3 : & \\
& X = 1, Y = 2, Z = 2 \\
\text{sei } p = 2, q = 5 : & \\
& X = 1, Y = 4, Z = 4 \\
\text{sei } p = 5, q = 7 : & \\
& X = 4, Y = 6, Z = 24 \\
\text{sei } p = 5, q = 11 : & \\
& X = 4, Y = 10, Z = 40
\end{aligned}$$

These: $Z = pq - \frac{pq}{p} - \frac{pq}{q} + 1 = pq - q - p + 1 = (p-1)(q-1)$

Herleitung

Die Herleitung dieser Formel basiert auf der Inklusions-Exklusionsregel:

1. $n = pq$ ist die Gesamtanzahl der Elemente in $\mathbb{Z}/n$.
2. Die Anzahl der Elemente, die durch p teilbar sind, ist $\frac{n}{p} = \frac{pq}{p} = q$.
3. Die Anzahl der Elemente, die durch q teilbar sind, ist $\frac{n}{q} = \frac{pq}{q} = p$.
4. Die Anzahl der Elemente, die durch beide teilbar sind, ist $\frac{n}{pq} = \frac{pq}{pq} = 1$.

Die Anzahl der Elemente, die durch keines der beiden teilbar sind, ist:

$$Z = pq - q - p + 1.$$

□