Diskrete Strukturen (WS 2023-24) - Halbserie 12

12.1 **[3]**

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

12.2 **[4]**

In der Vorlesung haben wir die Bezout-identität gesehen: falls $x, y \in \mathbb{N}$ und $ggt(x, y) = 1$ 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 $ggt(a, b) = 1$, 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 $X \equiv k \bmod a$ and $X \equiv l \bmod b$.

12.3 **[3]**

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

12.4 Sei G die multiplikative Gruppe modulo 35, d.h. die Elemente sind $a \in \mathbb{Z}/35$ mit $ggt(a, 35) = 1$ und die Operation ist $x \oplus y := xy \bmod 35$. Aus den obigen Aufgaben wissen wir dass das tatsätzlich eine Gruppe ist, und auch wie viele Elemente diese Gruppe hat. Finden Sie ein kartesiches Produkt $H := \mathbb{Z}/n_1 \times \ldots \times \mathbb{Z}/n_k$ sodasss G und H isomorph sind.

12.5 Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}/n$. Sei $k \in \mathbb{N}$ eine Zahl mit d Dezimalstellen. Finden Sie ein algorthmus um $a^k \bmod n$ zu berechnen, der effizient ist, im folgenden Sinn: es existiert eine konstante C (von n abhängig), so dass der Algorithmus brauch nicht mehr als Cd Schritte, vobei ein Schritt ist eine operation $\cdot$ oder $+$ mod n. (z.B. $a \cdot a \cdot a + a$ sind "drei Schritte").

12.6 Finden Sie zwei verschieden Primzahlen p mit der Eigenschaft dass $\forall a \in \mathbb{Z}/p^*$ existiert n mit $a \equiv 2^n \bmod p$. (Es ist unbekannt ob es unendlich viele solche Primzahlen gibt. Die Vermutung dass es so ist heißt "Artins Vermutung")