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 $ab \equiv 1 \bmod n$.

Solution. Z.B.: mit Bezout-identität finden wirh $x, y \in \mathbb{Z}$ mit $xa + yn = 1$. Dann ist $xa \equiv 1 \bmod n$.

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 $X \equiv l \bmod b$.

Solution. Mit der Bezout-identität finden wir $x, y \in \mathbb{Z}$ mit $xa + yb = 1$. Dann $X := xal + ybk$ ist eine Lösung: modulo a haven wir $X \equiv xal + ybk \equiv xak + ybk \equiv 1 \cdot k$. Ähnlich modulo b haben wir $X \equiv k$.

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.

Solution. Die Elemente a für die $ggt(a, pg) > 1$ gilt sind

$$\{0, p, 2p, \ldots, (q-1)p\} \cup \{0, q, 2q, \ldots, (p-1)q\}.$$

.

Die Zwei Mengen die wir vereinigen sind jedoch nicht disjunkt: Das element 0 ist in beiden, sonst gibt's keine andere, da wenn $p \mid x$ und $q \mid x$, dann $pq \mid x$, weil p, q Primzahlen sind.

Also wir haben genau $q+p-1$ solche Elemente. Deswegen die Antwort ist $pq-p-q+1 = (p-1)(q-1)$.

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.

Solution. Wir wissen dass G genau 24 Elemente hat. Wir checken dass $2^1 2 \equiv 1 \bmod 35$ und $2^k \not\equiv 1 \bmod 35$ wenn $1 \leq k \leq 12$. Deswegen Die Untergruppe $\{1, 2, 4, \ldots, 2^{11}\} \subset G$ ist eine Untergruppe die zu $\mathbb{Z}/12$ isomorph ist.

Wir checken auch direkt dass $6 \notin \{1, 2, 4, \ldots, 2^{11}\}$, und $\{1, 6\} \subset G$ ist eine Untergruppe die zu $\mathbb{Z}/2$ ismorph ist.

Wir möchten beweisen dass G ist isomorph zu $\mathbb{Z}/12 \times \mathbb{Z}/2$. Isomoprhismus ist: $f\colon \{1, 2, 4, \ldots, 2^{11}\} \times \{1, 6\} \to G$, gegeben als $f(x, y) = xy$. Das f ist ein Homomorphismus, folg daraus dass wenn $\alpha\colon A \to C$ und $\beta\colon B \to C$ sind homomoprhismen zwischen kommutativen Gruppen, dann auch $A \times B \to C$, $(x, y) \mapsto \alpha(x)\beta(x)$ ist ein Homomorphismus.

Nach dem vorherigen Übungsblatt brauchen wir nur zu prüfen, ob $\ker f = (1, 1)$. Nehmen wir also an, dass $f(x, y) = 1$, d.h. $2^k 6^l \equiv 1 \bmod 35$ und $k \leq 11$, $l \leq 2$. Für $l = 1$ haben wir bereits geprüft, dass $2^k \equiv 1$ nur wenn $k = 0$. Für $l = 1$ folgern wir, dass $2^k 6^2 \equiv 6$ und damit $2^k \equiv 6$. Wir prüfen auch direkt, dass es kein solches k gibt.

(Natürlich solche Aufgabe wäre zu lang für die Klausur)

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 Algorithmus 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 $+ \bmod n$. (z.B. $a \cdot a \cdot a + a$ sind "drei Schritte").

Solution. Seien $k_{d-1}k_{d-2}\ldots k_0$ die Dezimalstellen von k, so dass $k = \sum_{j=0}^{d-1} k_j 10^j$.

Um $\bar{a}_j := a^{k_j 10^j}$ zu berechnen, rechnen wir wie folgt: $a_0 := a$, $a_1 := a^{10}$, $a_2 := a_1^{10}$,..., $a_j := a_{j-1}^1 0$, $\bar{a}_j := a_j^{k_j}$.

Dazu brauchen wir nur $10j + k_j$, also weniger als $10(j + 1)$, Operationen.

Wir sehen jetzt $a^k = \bar{a}_{d-1} \cdot \bar{a}_{d-2} \cdot \ldots \cdot \bar{a}_0$, und dazu brauchen wir zusätzlich $d-1$ Operationen.

Auf erstes Blick haben wir alles zusammen weniger als $\sum_{j=0}^{d-1} 10(j + 1) + d$ Operationen, was gibt uns Cd^2.

Jedoch, sehen wir dass wir die Zahlen $a_0, \ldots, a_j$ nicht neu berechnen müssen, wenn wir $\bar{a}_j$ berechnen. Deswegen brauchen wir nur Cd Operationen.

(Die Konstante C ist hier von n unabhängig. Jedoch wenn wir diesen Algorithmus als Computer-programm schreiben, müssen wir modulo n reduzieren, sobald wir irgenwo eine Zahl grössere als n bekommen. Sonst werden die Zahlen zu groß. Davon kommt die Abhängikeit der Konstante C von n in Anwendungen).

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")

Solution. Z.B. $p = 3$, $p = 5$ (und auch $p = 11$ abder nicht $p = 7$).