Übungsstunde 7

Dan Philipp

Nachbesprechung Bonus

- Kleine Begründung, warum eine Injektion zu finden die Uncountability beweist
- Alle Schritte genau ausführen
- Achtet auf die Domain/Codomain der Funktionen in A_ℓ

6.5 Countability ***(8 Points)***

Prove that for all $\ell \in \mathbb{N}$ with $\ell \geq 1$ the set

$$A_\ell := \left\{ f : \mathbb{N} \to \{0,1\} \;\middle|\; \sum_{i=0}^{k} f(i) \leq \frac{k}{\ell} + 1 \text{ for all } k \in \mathbb{N} \right\}. \tag{1}$$

is uncountable.

Hint: For all $\ell \geq 1$, explicitly write an injection from a known uncountable set into A_ℓ.

Aufgabe

Beweise oder widerlege:

$$S = \{f : \mathbb{N} \to \mathbb{N} \mid \forall x \forall y (x \leq y \to f(x) \leq f(y)\}$$

ist abzählbar.

Definition 3.42.

(i) Two sets A and B *equinumerous*[48], denoted $A \sim B$, if there exists a bijection $A \to B$.

(ii) The set B *dominates* the set A, denoted $A \preceq B$, if $A \sim C$ for some subset $C \subseteq B$ or, equivalently, if there exists an injective function $A \to B$.

(iii) A set A is called *countable*[49] if $A \preceq \mathbb{N}$, and *uncountable*[50] otherwise.[51]

Lemma 3.15. [52]

(i) The relation $\sim$ is an equivalence relation.

(ii) The relation $\preceq$ is transitive: $A \preceq B \wedge B \preceq C \implies A \preceq C$.

(iii) $A \subseteq B \implies A \preceq B$.

Theorem 3.22. *Let A and A_i for $i \in \mathbb{N}$ be countable sets.*

(i) For any $n \in \mathbb{N}$, the set A^n of n-tuples over A is countable.

(ii) The union $\cup_{i \in \mathbb{N}} A_i$ of a countable list $A_0, A_1, A_2, \ldots$ of countable sets is countable.

(iii) The set A^* of finite sequences of elements from A is countable.

Number Theory

Modulo rechnen

- $R_m(n) =$ der Rest, wenn wir n durch m teilen
- Beispiel: $R_5(13) = 3$

Für Addition und Multiplikation gilt:

$$R_m(n + l) = R_m(R_m(n) + R_m(l))$$
$$R_m(n * l) = R_m(R_m(n) * R_m(l))$$

- Formale Definition: $a \equiv_m b \Leftrightarrow m|(a - b)$

  (wichtig für Beweise)

Aufgabe

Berechne:

- $R_{31}(2^{1003})$
- $R_{80}(3^{1207})$
- $R_{9}(5^{123})$

Number Theory

- **Theorem 4.6**: Jede natürliche Zahl kann **eindeutig** in ein Produkt aus Primzahlen zerlegt werden

$$a = \prod_i p_i^{e_i}$$

- gcd(a,b): grösster gemeinsamer Teiler von a und b
- lcm(a,b): kleinstes gemeinsames Vielfaches von a und b

Euklidischer Algorithmus

- Ziel: gcd(a,b) berechnen
- Wir teilen die grössere Zahl durch die kleinere und notieren den Rest
- Wir wiederholen dies, bis eine der Zahlen 0 ist
- Die andere Zahl ist dann der gcd

Aufgabe

Berechne

- $\gcd(455, 182)$
- $\gcd(9^3, 12^2)$

Aufgabe

Zeige, dass keine $x, y \in \mathbb{Z}$ die Gleichung

$$x^3 - x = y^2 + 1$$

erfüllen

Ideal

- $(a) = \{u * a \mid u \in \mathbb{Z}\}$

  Beispiel: $(4) = \{\dots, -8, -4, 0, 4, 8, \dots\}$
- $(a, b) = \{u * a + v * b \mid u, v \in \mathbb{Z}\}$

  Beispiel: $(3,5) = \{\dots, -8, -5, -3, 0, 3, 5, 8, \dots\}$

Multiplikative Inverse

Lemma 4.18

$$a * x \equiv_m 1$$

hat nur eine Lösung genau dann wenn gcd(a,m)=1. Diese Lösung ist einzigartig.

Diese Lösung können wir mit dem erweiterten euklidischen Algorithmus berechnen.

Aufgabe

Berechne die multiplikative Inverse von 15 modulo 53

Chinese Remainder Theorem (CRT)

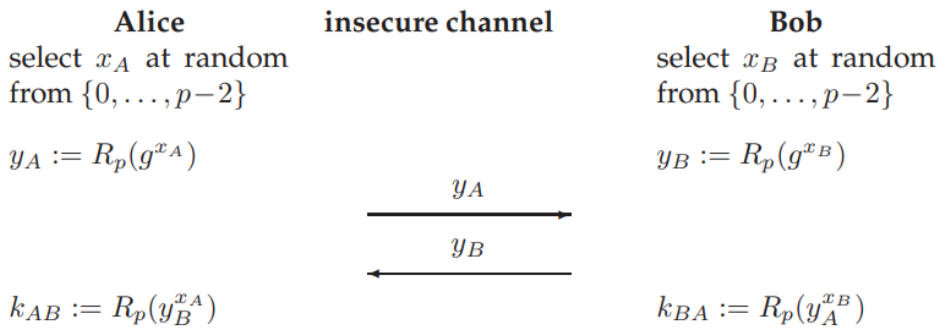
Wir haben mehrere modulare Kongruenzen mit einem x, das wir suchen:

$$x \equiv_2 1$$
$$x \equiv_5 3$$
$$x \equiv_7 2$$

Wichtig: Die Moduli (2,5,7) müssen paarweise teilerfremd sein.

Dann gilt: Es gibt eine eindeutige Lösung für x mit $0 \leq x < M$, wobei M=2*5*7=70

Diffie-Hellman Protokoll



$$k_{AB} \equiv_p y_B^{x_A} \equiv_p (g^{x_B})^{x_A} \equiv_p g^{x_A x_B} \equiv_p k_{BA}$$

- Anwendung in der Verschlüsselung
- Manchmal kommen in der Klausur Fragen zum Diffie-Hellman Protokoll
- Tipp: Schreibt euch die Funktionsweise des Protokolls auf euer Cheatsheet
- Hilfreiches Youtube Video zu dem Thema: https://www.youtube.com/watch?v=iHDNpH_Xw4Y