Übung 7

Nachbesprechung

- Immer alles Beweisen was nicht direkt als Lemma oder Theorem im Skript vorkommt und jeden Schritt begründen! Auch an der Prüfung
- Verwendet keine Symbole, die nicht im Skript vorkommen
  z.B. $A \subset B$ für Mengen A, B

Countability

Sei $S = \{f \in \{0,1\}^{\mathbb{N}} \mid \forall x \exists y\ (x < y \wedge f(x) = f(y))\}$. Beweise, dass S überabzählbar ist.
Für jedes $f \in S$ gilt, dass wenn $f(x) = 1$, so gibt es $y > x$ mit $f(y) = 1$ und wenn $f(x) = 0$, so gibt es $y > x$ mit $f(y) = 0$. Also ist $f \equiv 0$ oder $f \equiv 1$ oder f wird nie konstant.

überabzählbar

Injektive Funktion $g: \{0,1\}^{\infty} \to S$ finden, $f_b := g(b)$ für $b \in \{0,1\}^{\infty}$

$$f_b(i) = \begin{cases} b_i & i = 3k \text{ für } k \in \mathbb{N} \\ 1 & i = 3k+1 \quad \text{=//=} \\ 0 & i = 3k+2 \quad \text{=//=} \end{cases}$$

wobei b_i die i-te Stelle des Bitstrings b bezeichnet

Beweis $f_b \in S$ für alle $b \in \{0,1\}^{\infty}$: Sei $b \in \{0,1\}^{\infty}$ beliebig. $f := g(b)$
Sei $x \in \mathbb{N}$ beliebig. zu zeigen: $\exists y\,(y > x \wedge f(y) = f(x))$
Fall $x = 3k+1$: $f(x+3) = 1 = f(x)$
Fall $x = 3k+2$: $f(x+3) = 0 = f(x)$
Fall $x = 3k$: Wenn $f(x) = 1$, dann ist $f(x+1) = 1 = f(x)$
Wenn $f(x) = 0$, dann ist $f(x+2) = 0 = f(x)$

Injektivität von g beweisen:
Seien $b, c \in \{0,1\}^{\infty}$ beliebig und nehmen wir an $b \neq c$.
$\Rightarrow \exists i\ b_i \neq c_i$
$\Rightarrow f_b(3i) = b_i \neq c_i = f_c(3i)$
$\Rightarrow g(b) = f_b \neq f_c = g(c)$

Daraus folgt $\{0,1\}^{\infty} \leq S$

Number Theory

Theorie über $\mathbb{Z}$

Theorem 4.6. Jede natürliche Zahl kann eindeutig in ihre Primfaktoren zerlegt werden

z.B. $60 = 2^2 \cdot 3 \cdot 5 = \prod_i p_i^{e_i}$

$126 = 2 \cdot 3^2 \cdot 7 = \prod_i p_i^{f_i}$

Der grösste gemeinsame Teiler von $a, b \in \mathbb{Z}$ ist die grösste Zahl d, die a und b teilt (grösste bezüglich Teilbarkeitsrel., also muss d jeden weiteren Teiler von a und b teilen)

gcd ist definiert als positive grösste gemeinsame Vielfache

$\gcd(60,126) = \prod_i p_i^{\min(e_i, f_i)} = 2^{\min(2,1)} \cdot 3^{\min(1,2)} \cdot 5^{\min(1,0)} \cdot 7^{\min(0,1)}$

$= 2 \cdot 3 = 6$

analog gilt $\text{lcm}(60,126) = \prod_i p_i^{\max(e_i, f_i)}$

Aus der Primfaktorenzerlegung zweier Zahlen kann man einfach ihren gcd und lcm berechnen

Ohne Primfaktorenzerlegung kann man den Euklidean alg. für gcd verwenden:

Bsp. $\gcd(24,70) = \gcd(24, 70-2\cdot 24) = \gcd(24,22) = \gcd(24-22, 22)$

$= \gcd(2,22) = 2$

zudem gilt immer $a \cdot b = \gcd(a,b) \cdot \text{lcm}(a,b)$

Aufg. Berechne die Primfaktorenzerlegung von $\text{lcm}(9 \cdot 2^4, 3^6) \cdot \gcd(9^3, 12^2)$.

$\text{lcm}(9 \cdot 2^4, 3^6) = \text{lcm}(3^2 \cdot 2^4, 3^6) = 3^{\max(2,6)} \cdot 2^{\max(4,0)} = 3^6 \cdot 2^4$

$\gcd(9^3, 12^2) = \gcd(3^6, 3^2 \cdot 4^2) = 3^{\min(6,2)} \cdot 2^{\min(0,4)} = 3^2$

$\Rightarrow \text{lcm}(9 \cdot 2^4\ 3^6) \cdot \gcd(9^3, 12^2) = 3^8 \cdot 2^4$

Def. ideal generiert von a und b für $a,b \in \mathbb{Z}$ ist definiert als $(a,b) = \{ua + vb \mid u,v \in \mathbb{Z}\} = \{ud \mid u \in \mathbb{Z}\} = (d)$ für $d := \gcd(a,b)$

z.B. $(4,6) = \{\ldots, -4, -2, 0, 2, 4, \ldots\} = (2)$

Aufg. Let $m,n \in \mathbb{N}$. Prove that $(n) \subseteq (m) \iff m \mid n$

Def. $m \mid n$: there exists $u \in \mathbb{Z}$ s.t. $m \cdot u = n$

Let $m,n \in \mathbb{N}$ be arbitrary.

($\Rightarrow$) Assume $(n) \subseteq (m)$. It holds $n \in (n)$. From the assumption follows $n \in (m)$. Thus $n = u \cdot m$ for some $u \in \mathbb{Z}$. This is equivalent to $m \mid n$.

($\Leftarrow$) Assume $m \mid n$. Thus $n = u \cdot m$ for some $u \in \mathbb{Z}$. Let $x \in \mathbb{Z}$ be arbitrary.

$x \in (n) \Rightarrow x = k \cdot n$ for some $k \in \mathbb{Z}$ (def. ideal)

$\Rightarrow x = k \cdot u \cdot m$ for some $k \in \mathbb{Z}$ (ass.)

$\Rightarrow x = v \cdot m$ for $v = k \cdot u \in \mathbb{Z}$ ($k \cdot u \in \mathbb{Z}$)

$\Rightarrow x \in (m)$ (def. ideal)

Thus, $(n) \subseteq (m)$, which concludes the proof.

Modulare Arithmetik

Mit $R_n(a)$ wird der Rest bezeichnet, wenn man a durch n teilt.

Wichtig: $R_n(a) \in \{0, \dots, n-1\}$ für alle $a \in \mathbb{Z}$

Korollar 4.17. $R_n(f(a_1,\dots,a_m)) = R_n(f(R_n(a_1),\dots,R_n(a_m)))$ for Polynom f.

z.B. $R_n(a_1 \cdot a_2 + a_3^3) = R_n(R_n(a_1) \cdot R_n(a_2) + R_n(a_3)^3)$

aber nicht ... $R_n(a_3)^{R_n(3)})$ Rest n vom Exponent nicht erlaubt

Aufg. Beweise $R_{13}(3^{n+2} + 4^{2n+1}) = 0$ für alle $n \in \mathbb{N}$

Sei $n \in \mathbb{N}$ beliebig.

$R_{13}(3^{n+2} + 4^{2n+1}) = R_{13}(9 \cdot 3^n + 4 \cdot 16^n) = R_{13}(9 \cdot 3^n + 4 \cdot R_{13}(16)^n)$

↑ Corollary 4.17.

$= R_{13}(9 \cdot 3^n + 4 \cdot 3^n) = R_{13}(13 \cdot 3^n) = 0$

Aufg. Berechne $R_{11}(2^{1408})$

Ziel: finde x so dass $2^x \equiv_{11} 1$ oder $2^x \equiv_{11} -1$. So kann man viel einfacher weiterrechnen

Es gilt $2^5 \equiv_{11} 32 \equiv_{11} 10 \equiv_{11} -1$

exponent gerade oder ungerade?

$R_{11}(2^{1408}) = R_{11}(2^3 \cdot 2^{1405}) = R_{11}(8 \cdot (2^5)^{281}) = R_{11}(8 \cdot (-1)^{281}) =$

$R_{11}(8 \cdot -1) = R_{11}(-8 + 11) = 3$ wobei Korollar 4.17. verwendet wurde

Def. Für $a, b, m \in \mathbb{Z}$ mit $m \geq 1$ $a \equiv_m b \overset{\text{def}}{\iff} m \mid (a-b)$

Aufg. Zeige, dass gilt $10 \mid (43^{43} - 17^{17})$

Es gilt $10 \mid (43^{43} - 17^{17})$

$\iff 43^{43} \equiv_{10} 17^{17}$ (def. $\equiv_{10}$)

$\iff R_{10}(43^{43}) = R_{10}(17^{17})$ (Lemma 4.16.ii.)

$R_{10}(43^{43}) = R_{10}(3^{43}) = R_{10}(3^{4 \cdot 10 + 3}) = R_{10}(R_{10}(3^4)^{10} \cdot 3^3) = R_{10}(1^{10} \cdot 27) = 7$

$R_{10}(17^{17}) = R_{10}(R_{10}(7)^{17}) = R_{10}(7^{17}) = R_{10}(7^{2 \cdot 8} \cdot 7) = R_{10}(R_{10}(49)^8 \cdot 7) =$

$R_{10}(-1^8 \cdot 7) = 7$. $R_{10}(43^{43}) = R_{10}(17^{17}) \Rightarrow 10 \mid (43^{43} - 17^{17})$

Aufg. Berechne die multiplikative Inverse von 11 mod 26.

Also $11 \cdot u \equiv_{26} 1$

Nach Lemma 4.18 gilt: die Gleichung (*) hat eine Lösung genau dann wenn $\gcd(11,26) = 1$ gilt. u ist eindeutig ($u \in \mathbb{Z}_{26}$)

u kann mit Hilfe des Erweiterten Euklidischen Alg. berechnet werden.

Lemma 4.2.: Für alle $m, n, q \in \mathbb{Z}$ gilt $\gcd(m,n) = \gcd(m, n-qm)$

$$\gcd(26,11) = \gcd(26-2\cdot 11, 11) = \gcd(4,11) = \gcd(4, 11-2\cdot 4) = \gcd(4,3)$$
$$= \gcd(4-3, 3) = \gcd(1,3) = 1$$

Wir wollen $u, v \in \mathbb{Z}_{26}$ finden, so dass $1 = u \cdot 11 + v \cdot 26$ gilt (Inverse)

$$\Rightarrow 1 = 4-3 = 4-(11-2\cdot 4) = (26-2\cdot 11) - (11 - 2\cdot(26-2\cdot 11))$$
$$= 26 - 2\cdot 11 - 11 + 2\cdot 26 - 4\cdot 11$$
$$= 3\cdot 26 + (-7)\cdot 11$$

$-7 \equiv_{26} 19$, also ist $u = 19$ die Inverse von 11 mod 26

Aufg. Finde zwei Lösungen x_1, x_2 für $2x^2 + 8 \equiv_{13} 6$

$2x^2 + 8 \equiv_{13} 6$

$\Rightarrow 2x^2 \equiv_{13} 6 - 8 \equiv_{13} -2$

$\Rightarrow 14x^2 \equiv_{13} -14$ ($\cdot 7$, 7 mult. inv. von 2 mod 13 (*))

$\Rightarrow x^2 \equiv_{13} -1 \equiv_{13} 12 \equiv_{13} 25$

$\Rightarrow x_1 = 5$

Wenn x_1 eine Lösung ist für $x^2 \equiv_{13} 12$, so ist $-x_1$ auch eine Lösung

$x_2 \equiv_{13} -5 \equiv_{13} 8 \Rightarrow x_2 = 8$

(*) Finde $u, v \in \mathbb{Z}_{13}$, so dass $2\cdot u + 13 \cdot v = 1$ gilt

$\gcd(2,13) = \gcd(2, 13-6\cdot 2) = \gcd(2,1) = 1$

$1 = 13 - 6\cdot 2 = 1\cdot 13 + (-6)\cdot 2 \Rightarrow u = 7$ da $-6 \equiv_{13} 7$

CRT

$m_1, m_2, \dots, m_r$ teilerfremd. $M = \prod_{i=1}^{r} m_i$

$X \equiv_{m_1} a_1$

$\dots$

$X \equiv_{m_r} a_r$ es existiert eine eindeutige Lösung $x \in \{0, \dots, M-1\}$

Bsp. $X \equiv_3 1$, $X \equiv_4 2$, $X \equiv_5 4$. Finde $x \in \mathbb{Z}_{60}$

1.) $M = \prod_{i=1}^{n} m_i$ $\quad M = 3 \cdot 4 \cdot 5 = 60$

2.) $M_i = M / m_i$ $\quad M_1 = 20,\ M_2 = 15,\ M_3 = 12$

3.) Find N_i s.t. $M_i N_i \equiv_{m_i} 1$

$20 \cdot N_1 \equiv_3 1 \Rightarrow N_1 = 2$

$15 \cdot N_2 \equiv_4 1 \Rightarrow N_2 = 3$

$12 \cdot N_3 \equiv_5 1 \Rightarrow N_3 = 3$

4.) $x = R_M\left(\sum_{i=1}^{r} a_i M_i N_i\right)$ $\quad R_{60}(1 \cdot 2 \cdot 20 + 2 \cdot 3 \cdot 15 + 4 \cdot 3 \cdot 12) = 34$

Diffie-Hellman Key-Agreement

Idee: Wenn x bekannt ist, dann kann $R_p(g^x)$ schnell berechnet werden.
Gegeben $y = R_p(g^x)$, p, g ist es aber schwer x zu berechnen

Alice		Bob
$x_A \in \{0, \dots, p-2\}$		$x_B \in \{0, \dots, p-2\}$
$y_A := g^{x_A}$	$\xrightarrow{y_A}$	$y_B := g^{x_B}$
	$\xleftarrow{y_B}$	
$k_{AB} := y_B^{x_A}$		$k_{AB} := y_A^{x_B}$

↖ secret key, nur Alice und Bob kennen ihn