Dr. S. Witzel WS 15/16

Diskrete Mathematik

Probeklausur

Ihre Antworten müssen immer begründet werden. Für nicht begründete Antworten erhalten Sie keine oder erheblich weniger Punkte.
Bearbeitungszeit: 105 Minuten.

Aufgabe 1 (Wochentage)

Wir identifizieren Wochentage mit den Zahlen $0, \ldots, 6$ wie folgt: 0 = Montag, 1 = Dienstag, ..., 6 = Sonntag.

a) Ein gewöhnliches Jahr hat 365 Tage. Wenn der 1.1. in einem gewöhnlichen Jahr Y auf einen Wochentag V fällt, auf welchen Wochentag W fällt der 1.1. im Jahr $Y + 1$?

b) Das Jahr Y ist ein Schaltjahr wenn Y durch 4 teilbar ist, aber nicht wenn Y durch 100 teilbar ist, aber doch wenn Y durch 400 teilbar ist. Wieviele der Jahre 1 bis 2015 waren Schaltjahre?

c) Der 1.1.2016 ist ein Freitag (= 4). Welcher Wochentag war der 1.1.1?

(2+2+2 Punkte)

Aufgabe 2 (Elementordnung)

Beweisen Sie den „kleinen Satz von Fermat“: Für eine Primzahl p und eine beliebige Zahl $a \in \mathbb{Z}$ gilt

$$a^p \equiv a \mod p.$$

Hinweis: Benutzen Sie den Satz von Lagrange **(4 Punkte)**

Aufgabe 3 (Klammerungen)

Wir betrachten die Anzahl C_n an Möglichkeiten, den Ausdruck

$$x_0 \cdot x_1 \cdot \ldots \cdot x_n$$

vollständig zu klammern (so dass er eine eindeutige Reihenfolge beschreibt, jeweils zwei Elemente zu multiplizieren).

Zum Beispiel ist $C_0 = C_1 = 1$, für $n = 2$ gibt es zwei Möglichkeiten: $x_0 \cdot (x_1 \cdot x_2)$ und $(x_0 \cdot x_1) \cdot x_2$. Für $n = 3$ gibt es fünf Möglichkeiten:

$$(x_0 \cdot (x_1 \cdot x_2)) \cdot x_3, \quad ((x_0 \cdot x_1) \cdot x_2) \cdot x_3,$$
$$(x_0 \cdot x_1) \cdot (x_2 \cdot x_3),$$
$$x_0 \cdot (x_1 \cdot (x_2 \cdot x_3)), \quad x_0 \cdot ((x_1 \cdot x_2) \cdot x_3)$$

a) Überlegen Sie sich, dass jeder Ausdruck durch die äußerste Multiplikation in zwei kürzere geklammerte Ausdrücke zerfällt. Folgern Sie daraus, wie sich C_n rekursiv in Abhängigkeit von $C_0, \ldots, C_{n-1}$ bestimmen lässt.

b) Beobachten Sie, dass das Ergebnis aus (a) eine Faltung ist leiten Sie daraus eine definierende Gleichung ab, die die erzeugende Funktion $\gamma(z) = \sum_{i=0}^{\infty} C_i z^i$ erfüllt.

(2+2 Punkte)

Aufgabe 4 (Türme)

Ein Schachbrett ist 8×8 Felder groß. Ein Turm auf einem Feld des Schachbretts bedroht alle Felder in derselben Reihe sowie alle Felder in derselben Spalte.

Wieviele Möglichkeiten gibt es, acht Türme auf einem Schachbrett zu positionieren, so dass keine zwei sich bedrohen?

(2 Punkte)

Aufgabe 5 (Kompression)

Wir bezeichnen mit $\{0,1\}^*$ die Menge aller endlichen $(0,1)$-Folgen und betrachten eine „Kompressionsfunktion“

$$\text{zip}\colon \{0,1\}^* \to \{0,1\}^*.$$

Wir nennen zip *verlustfrei* falls eine eine „Dekompressionsfunktion“ $\text{unzip}\colon \{0,1\}^* \to \{0,1\}^*$ gibt, so dass $\text{unzip}(\text{zip}(x)) = x$ für alle x.

Sei zip eine verlustfreie Kompressionsfunktion. Zeigen Sie, dass es ein $x \in \{0,1\}^*$ gibt, so dass $\text{zip}(x)$ mindestens so lang ist wie x. Gehen Sie dazu wie folgt vor:

a) Zeigen Sie, dass eine verlustfreie Kompressionsfunktion injektiv ist.

b) Führen Sie die Annahme, dass $\text{zip}(x)$ immer echt kürzer ist als x zu einem Widerspruch, indem Sie für ein $n \in \mathbb{N}$ die Einschränkung $\text{zip}\colon \{0,1\}^{n+1} \to \{0,1\}^n$ betrachten.

(2+2 Punkte)

Programmieraufgabe

Aufgabe 6* (Schnelle Exponentiation)

Sei a beliebig und $b \in \mathbb{N}$. Wenn wir b in Binärschreibweise schreiben als $b = \sum_{i=0}^{\ell} b_i 2^i$ (mit $b_i \in \{0,1\}$) gilt

$$a^b = a^{\sum_{i=0}^{\ell} b_i 2^i} = \prod_{i=0}^{\ell} a^{b_i 2^i} = \prod_{\substack{0 \le i \le \ell \\ b_i = 1}} a^{2^i}$$

Daraus ergibt sich ein sehr effiziente Methode Potenzen von a auszurechnen: man bestimmt sukzessive a, a^2, a^4, $\ldots$ (was jeweils eine Quadratur bedeutet) und parallel b_0, b_1, b_2 (was jeweils eine Division mit Rest bedeutet) und multipliziert a^{2^i} zum Ergebnis falls $b_i = 1$. Wenn a eine ganze Zahl ist, ist a^b naturgemäß sehr groß. Wenn a eine Restklasse ist, kann dagegen immer ein kleiner Repräsentant gewählt werden.

Implementieren Sie eine Funktion `fast_pow`(n, a, b), die Zahlen $n, a, b \in \mathbb{Z}$ mit $n \ge 2$ und $b \ge 0$ annimmt und mit der obigen Methode $a^b \mod n \in \{0, \ldots, n-1\}$ berechnet und zurückgibt.

Wenn Sie zusätzlich den erweiterten euklidischen Algorithmus implementieren, können Sie auch negative b erlauben. **(4*+3* Punkte)**