Diskrete Mathematik Übungsstunde Zusammenfassung

Leon Kolmanić

06.11.2023

1 Organisation

1.1 Dateigrössenlimit

Bei der Abgabe von den Bonusaufgaben gibt es ein Limit für die Grösse der Dateien. Dieses ist sehr grosszügig gewählt, es sollte also jedem möglich sein durch Komprimierung die Dateien klein genug zu bekommen. Ab jetzt werden zu grosse Abgaben, die deshalb per E-Mail zugeschickt werden, nicht mehr akzeptiert.

1.2 Cheat Sheet

Ihr dürft an die Klausur 6 A4 Seiten Notizen mitbringen. Das Cheat Sheet muss komplett von euch selbst verfasst werden. Ausserdem müsst ihr es handgeschrieben verfassen, also auf Papier oder einem Tablet mit Stift. Es ist nicht erlaubt, Grafiken oder Bilder einzufügen. Durch das Schreiben des Cheat Sheets geht ihr nochmal den ganzen Stoff detailliert durch, meiner Erfahrung nach werdet ihr viel davon profitieren euch eins selber zu schreiben.

1.3 Abschreiben beim Bonus

Bei den Bonusaufgaben ist es verboten, mit anderen zusammenzuarbeiten. Ihr müsst eure Lösung komplett selber verfassen. Ich kann euch sehr empfehlen, die Aufgaben selber abzugeben und von dem Feedback zu lernen. Davon werdet ihr mit Blick auf die Prüfung viel mehr profitieren, als wenn ihr euch die 0.25 Bonus durch Abschreiben sichert.

2 Besprechung Bonusaufgabe

a)

Häufige Fehler

Hier wurde öfters folgende Umformung gemacht:

$$A \text{ ist überabzählbar} \stackrel{\cdot}{\iff} \mathbb{N} \preceq A$$

Diese Umformung kann man so nicht machen. $\mathbb{N} \preceq A$ bedeutet lediglich, dass es eine Injektion von den natürlichen Zahlen nach A gibt. Aber es gibt auch beispielsweise eine Injektion von $\mathbb{N}$ nach $\mathbb{N}$, und zwar die Identitätsfunktion. Also gilt $\mathbb{N} \preceq \mathbb{N}$. Aber natürlich ist $\mathbb{N}$ nicht überabzählbar. Die folgende Umformung ist auch nicht möglich:

$$\text{nicht } A \preceq \mathbb{N} \stackrel{\cdot}{\Longrightarrow} A \succ \mathbb{N}$$

Diese Umformung ist aus zwei Gründen falsch: Zunächst mal definieren wir die Zeichen $\succ$ und $\prec$ nicht, wenn wir diese im Kontext von (Über)abzählbarkeit verwenden. Diese Zeichen benutzen wir nur, wenn $\preceq$ eine Ordnungsrelation ist. Aber die "Dominanz-Relation" auf den Mengen ist keine Ordnungsrelation, weil sie nicht antisymmetrisch ist. Es gilt z.B. $\mathbb{Z} \preceq \mathbb{N}$ und $\mathbb{N} \preceq \mathbb{Z}$, aber $\mathbb{Z} \neq \mathbb{N}$. Generell ist es eine gute Idee, nicht zu viel in die verwendeten Zeichen reinzuinterpretieren. Bevor ihr eine Umformung macht, solltet ihr immer überprüfen, ob diese durch ein Lemma/Theorem aus dem Skript gerechtfertigt ist oder ihr eine andertweitige Begründung angeben könnt. Das zweite Problem ist, dass wir im Skript nie bewiesen haben, dass für zwei Mengen A und B $A \preceq B$ oder $B \preceq A$ gilt. Für die Mengen, die wir in diesem Kurs betrachten, gilt immer eine der beiden Aussagen, aber das formal zu zeigen ist nicht möglich ohne in die axiomatische Mengenlehre einzusteigen. In diesem Kurs machen wir das nicht.

Proof Pattern bei Implikationen

Ich habe bei den Abgaben gemerkt, dass viele Leute Schwierigkeiten bei der Anwendung von Proof Pattern haben. Bei Aufgaben wie dieser ist es entscheidend, das richtige Proof Pattern zu wählen. Man konnte hier einen sehr eleganten Beweis führen, wenn man einen indirekten Beweis oder Beweis durch Widerspruch gemacht hat, aber mit einem direkten Beweis war das nicht möglich. Ich kann sehr empfehlen, sich bei einer Aufgabe für mehrere Proof Pattern den Beweisansatz zu überlegen und sich dann für den einfachsten zu entscheiden.
Es hatten vor allem Leute Schwierigkeiten mit dem Beweis durch Widerspruch, deshalb erkläre ich ihn hier noch einmal. Bei einer Implikation $S \Longrightarrow T$ funktioniert ein Beweis durch Widerspruch wie folgt: Wir nehmen an, dass in einem konkreten Fall die Implikation nicht gilt. Hier war die Aussage zum Beispiel "für alle Mengen A und B gilt:". Also nehmen wir bei einem Beweis durch Widerspruch an, dass es Mengen A und B gibt, sodass S wahr ist und T falsch ist. Konkret würde das so aussehen:

Beweis. Assume towards a contradiction that there are sets A and B such that A is uncountable, $A \preceq B$ and B is countable. By the definition of countability $B \preceq \mathbb{N}$ follows. From $A \preceq B$ and $B \preceq \mathbb{N}$ we can deduce $A \preceq \mathbb{N}$ with lemma 3.15. This means A is countable by definition of countability. We have arrived at a contradiction which concludes the proof. □

b)

Bei der b) war es entscheidend, eine korrekte Injektion zu konstruieren. Wenn die Injektion nur "fast richtig" war oder nur eine intuitive Begründung für die Überabzählbarkeit von S geliefert wurde, gab es nicht die volle Punktzahl. Einige von euch haben mit Cantors Diagonalisierungsargument argumentiert. Ich würde euch sehr stark davon abraten dies zu tun, weil es mit dem Diagonalisierungsargument mehr Aufwand ist, die Überabzählbarkeit zu zeigen. Ausserdem kann es sein, dass solche Lösungen strikter bewertet werden, weil sie nicht in das erwartete Lösungsschmema passen. Übt für die Klausur die Methode der Konstruktion einer Injektion. Diese funktioniert immer gleich und wenn man viele solche Aufgaben geübt hat, hat man damit nicht mehr so grosse Schwierigkeiten.

3 Reste berechnen und modulare Arithmetik

In der Zahlentheorie wollen wir manchmal den Rest von Zahlen berechnen. Das funktioniert genauso, wie die Division, die man in der Grundschule lernt. Um den Rest von einer Zahl n wenn wir sie durch m teilen zu notieren, schreiben wir $R_m(n)$. Wir überlegen uns, wie oft m in n reinpasst, und schreiben dann die Differenz auf. Also ist $R_5(13)$ zum Beispiel 3, weil die 5 zweimal in die 13 passt, aber dann noch 3 fehlt. $R_2(101) = 1$, weil 100 genau durch 2 teilbar ist und dann 1 übrig bleibt.
In der Prüfung gibt es oft Aufgaben, bei denen man den Rest von sehr grossen Zahlen berechnen muss. Hier kann man sich einige Tricks der modularen Arithmetik zunutze machen. Modulare Arithmetik bedeutet einfach, dass wenn wir bei einer Rechnung nur an dem Resultat modulo m interessiert sind, Summanden und Faktoren durch andere Zahlen ersetzen können, solange diese andere Zahlen kongruent modulo m sind zu den ursprünglichen Zahlen. Es gilt zum Beispiel $3 + 5 \equiv_3 0 + 8$, weil $3 \equiv_3 0$ und $5 \equiv_3 8$.
In diesem Fall kann man sich die Rechnung sehr vereinfachen: $R_{12345}(12344^{12345})$. Weil $12344 \equiv_{12345} -1$ (anders gesagt: $12345 \mid 12344 - (-1)$) und -1 hoch eine ungerade Zahl wieder -1 ist, können wir so vorgehen:

$$12344^{12345} \equiv_{12345} (-1)^{12345} \equiv_{12345} -1 \equiv_{12345} 12344$$

Also $R_{12345}(12344^{12345}) = 12344$.
In diesem Beispiel funktioniert der gleiche Trick, aber diesmal ist er nicht so

offensichtlich: $R_{31}(2^{100003})$.

$$\begin{aligned} 2^{100003} &\equiv_{31} 2^{100000} \cdot 8 \equiv_{31} (2^5)^{20000} \cdot 8 \\ &\equiv_{31} 32^{20000} \cdot 8 \equiv_{31} 1^{20000} \cdot 8 \equiv_{31} 8 \end{aligned}$$

Also $R_{31}(2^{100003}) = 8$.

4 Nichtexistenz von Lösungen einer Gleichung beweisen

In den meisten zahlentheoretischen Beweisen in diesem Kurs kann man Tricks der modularen Arithmetik anwenden. Wir wollen zum Beispiel folgendes Theorem zeigen:

Theorem. *Es gibt keine $x, y \in \mathbb{Z}$, die die Gleichung*

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

erfüllen.

Um so eine Aussage zu zeigen, muss man nur den richtigen Modulus betrachten. In diesem Fall funktioniert $m = 3$. Den richtigen Modulus kann man nur durch Ausprobieren findet. Wenn wir ein beliebiges $x \in \mathbb{Z}$ betrachten, tritt einer der Fälle $x \equiv_3 0$, $x \equiv_3 1$ oder $x \equiv_3 2$ ein. Analoges gilt für y. Wir berechnen jetzt in einer Tabelle, was der modulus 3 der beiden Seiten der Gleichung in diesen Fällen ist.

$x \equiv_3$	$x^3 \equiv_3$	$x^3 - x \equiv_3$
0	0	0
1	1	0
2	2	0

Wir füllen die Tabelle wie folgt aus: Wenn wir z.B. in der letzten Zeile sind, wissen wir, dass $x \equiv_3 2$. Wir wollen nun wissen, was x^3 modulo 3 ist. Wir dürfen dafür x durch 2 ersetzen (modulare Arithmetik), weil $x \equiv_3 2$ gilt. Also $x^3 \equiv_3 2^3 \equiv_3 8 \equiv_3 2$. Die letzte Kongruenz gilt, weil die Differenz von 2 und 8 ein Vielfaches von dem Modulus 3 (6) ist. Wir gehen analog für die rechte Seite vor:

$y \equiv_3$	$y^2 \equiv_3$	$y^2 + 1 \equiv_3$
0	0	1
1	1	2
2	1	2

Jetzt bemerken wir folgendes: Die linke Seite der Gleichung ist immer kongruent zu 0 modulo 3, während die rechte Seite immer kongruent zu 1 oder

2 modulo 3 ist. Also können die beiden Seiten der Gleichung nie gleich sein. Falls sie für eine bestimmte Wahl von x und y erfüllt wäre, müsste es zumindest einen Fall geben, in dem sie den gleichen Modulos 3 haben. Man muss hier aber aufpassen: Gibt es auch nur eine einzige Zahl, die sowohl in der rechten Spalte der ersten Tabelle und der rechten Spalte der zweiten Tabelle ist, kann man nicht folgern, dass die Gleichung keine Lösungen hat. Es ist nicht erforderlich, dass die Zahlen auf der gleichen Zeile übereinstimmen, weil x und y ja völlig unabhängig gewählt werden können.

5 Euklidischer Algorithmus

In der Prüfung ist es oft erforderlich, den grössten gemeinsamen Teiler von zwei Zahlen zu finden oder das modulare Inverse einer Zahl. Es gibt zwei Methoden, wie man beides systematisch bestimmen kann.

5.1 Einfacher euklidischer Algorithmus

Wenn wir den grössten gemeinsamen Teiler von zwei Zahlen n und m bestimmen wollen, gehen wir wie folgt vor: Wir teilen die grössere der beiden Zahlen durch die kleinere und notieren den Rest. Das wiederholen wir so lange, bis eine der Zahlen 0 ist. Dann ist die andere Zahl der grösste gemeinsame Teiler. Ein Beispiel:

$$\begin{aligned}\gcd(284, 384) &= \gcd(284, 100) = \gcd(84, 100) = \gcd(84, 16)\\ &= \gcd(4, 16) = \gcd(4, 0) = 4\end{aligned}$$

5.2 Erweiterter euklidischer Algorithmus

Wenn wir das modulare Inverse einer Zahl finden wollen, dann reicht der einfache euklidische Algorithmus nicht aus. Hier müssen wir den erweiterten euklidischen Algorithmus verwenden. Das modulare Inverse einer Zahl a modulo m zu finden bedeutet, eine Zahl $0 \leq x < m$ zu finden, sodass $ax \equiv_m 1$ gilt. Zum Beispiel ist das modulare Inverse von 5 modulo 7 3, weil $3 \cdot 5 \equiv_7 15 \equiv_7 1$. Nun sollen wir zum Beispiel das modulare Inverse von 15 modulo 53 finden. Wir führen jetzt den euklidischen Algorithmus durch, notieren aber zusätzlich noch die Divisionen, um den Rest zu bestimmen, explizit. Im ersten Schritt teilen wir also 53 durch 15, nur das wir jetzt zusätzlich die vollständige Rechnung ausschreiben.

$$\begin{aligned} 53 &= 3 \cdot 15 + 8 && \gcd(53, 15)\\ 15 &= 1 \cdot 8 + 7 && \gcd(8, 15)\\ 8 &= 1 \cdot 7 + 1 && \gcd(8, 7)\end{aligned}$$

Wenn wir diesen Prozess durchführen, erhalten wir irgendwann den Rest 1. Dann beginnen wir von der 1 aus, rückwärts umzuformen. Wir fangen also mit der untersten Gleichung an, und setzen dann die Gleichungen nacheinander

ein. Nachdem wir jede Gleichung einsetzen, bringen wir gemeinsame Faktoren zusammen. Wir schreiben also die 1 auf eine immer umständlich werdendere Weise. Ich habe jeweils die Zahl markiert, die im nächsten Schritt ersetzt wird.

$$\begin{aligned} 1 &= 8 - 1 \cdot 7 \\ &= 8 - 1 \cdot (15 - 1 \cdot 8) \\ &= 2 \cdot 8 - 15 \\ &= 2 \cdot (53 - 3 \cdot 15) - 15 \\ &= 2 \cdot 53 - 7 \cdot 15 \end{aligned}$$

Wenn wir alle Gleichungen eingesetzt haben, erhalten wir einen Ausdruck mit den zwei ursprünglichen Zahlen 53 und 15. Die Zahl, die vor der 15 steht, in diesem Fall die -7, ist die gesuchte Lösung. Man kann verifizieren: $-7 \cdot 15 \equiv_{53} 1$. Aber für das modulare Inverse verlangen wir immer die eindeutige Zahl im Bereich $0 \leq x < 53$. Nach den Regeln der modularen Arithmetik dürfen wir unsere Lösung -7 durch eine andere Zahl ersetzen, sofern diese kongruent zu -7 modulo 53 ist, ohne die Bedingung $15x \equiv_{53} 1$ zu verletzen. Also wählen wir als Lösung $-7 + 53 = 46$, da 46 im gewünschten Bereich liegt und $46 \equiv_{53} -7$ gilt.

6 Der chinesische Restsatz (CRT)

Der chinesische Restsatz sieht auf den ersten Blick sehr komplex aus, aber er sagt etwas einfaches aus. Wir betrachten ein System von modularen Kongruenzen mit einer Variablen, also einfach mehrere modulare Kongruenzen, die gleichzeitig erfüllt sein sollen und auf deren linker Seite immer x steht. Ein Beispiel für so ein System ist:

$$\begin{aligned} x &\equiv_2 0 \\ x &\equiv_6 0 \end{aligned}$$

Das System hat mehrere Lösungen im Bereich $0 \leq x < 6 \cdot 2 = 12$, weil 0 und 6 das System beide lösen. Der chinesische Restsatz sagt nun über solche Systeme etwas aus, die eine besondere Bedingung erfüllen: Die Moduli sind alle teilerfremd. Das bedeutet: Wenn wir je zwei der Moduli betrachten, ist der grösste gemeinsame Teiler 1. In dem obigen System ist das nicht erfüllt, weil 2 und 6 als grössten gemeinsamen Teiler 2 haben. In diesem System ist das aber zum Beispiel erfüllt, weil $\gcd(2, 3) = 1$:

$$\begin{aligned} x &\equiv_2 1 \\ x &\equiv_3 2 \end{aligned}$$

Wenn diese Bedingung für ein System erfüllt ist, dann garantiert das CRT, dass es eine einzigartige Lösung $0 \leq x < M$ gibt, wobei M das Produkt aller Moduli ist. Also in diesem Fall ist $M = 2 \cdot 3 = 6$. Die einzigartige Lösung bei

letzterem System ist 5. Indem wir alle anderen Zahlen im Bereich $0 \leq x < 6$ überprüfen, sehen wir, dass es keine andere Lösung gibt.

Man kann den Satz verwenden, wenn man herausfinden möchte, wie viele Lösungen ein System modularer Kongruenzen hat, auch wenn die Moduli nicht teilerfremd sind. Dazu teilen wir Moduli in mehrere kleinere Moduli auf, die dann jeweils teilerfremd sind. Sei zum Beispiel dieses System gegeben:

$$\begin{aligned} x &\equiv_2 1 \\ x &\equiv_6 5 \end{aligned} \tag{1}$$

Wir wollen nur herausfinden, wie viele Lösungen es im Bereich $0 \leq x < 12$ gibt. Damit wir das CRT anwenden können, formen wir das System zu diesem um:

$$\begin{aligned} x &\equiv_2 1 \\ x &\equiv_2 5 \\ x &\equiv_3 5 \end{aligned}$$

Weil das modulare Kongruenzen sind, können wir die rechten Seiten durch kongruente Zahlen ersetzen. Mit $5 \equiv_2 1$ und $5 \equiv_3 2$ erhalten wir:

$$\begin{aligned} x &\equiv_2 1 \\ x &\equiv_2 1 \\ x &\equiv_3 2 \end{aligned}$$

Nun sehen wir, dass die erste Gleichung doppelt vorkommt. Deshalb dürfen wir diese streichen. Übrig bleibt das System

$$\begin{aligned} x &\equiv_2 1 \\ x &\equiv_3 2 \end{aligned} \tag{2}$$

Für System 2 wissen wir von oben schon, dass die einzige Lösung im Bereich $0 \leq x < 6$ 5 ist. Weil wir die Systeme ineinander umgeformt haben, sind sie äquivalent. Jede Lösung von System 1 ist auch eine von System 2 und umgekehrt. Wir können weitere Lösungen für System 2 erhalten, indem wir zu 5 Vielfache des Produktes aller Moduli addieren, also wenn wir zu 5 Vielfache von $2 \cdot 3 = 6$ addieren. Zum Beispiel ist 11 auch eine Lösung von System 2. Weil 5 und 11 die einzigen Lösungen von 2 sind, die im Bereich $0 \leq x < 12$ liegen, sind dies auch die einzigen Lösungen von System 1 in diesem Bereich.
Bei einem System mit so kleinen Zahlen ist es natürlich einfacher, für alle Zahlen im Bereich $0 \leq x < 12$ zu prüfen, ob diese Lösungen sind. In der Klausur gibt es aber manchmal Aufgaben mit solchen Systemen, bei denen die Zahlen so gross sind, dass eine Überprüfung von allen zu lange dauern würde. Diese Aufgaben gehören aber zu den schwierigeren in der Klausur, also **keine Panik, wenn das Beispiel von oben nicht zu 100% klar war!** Die Methode, um solche Aufgaben zu lösen, also die Gleichungen aufzuteilen, unnötige zu streichen und

dann das CRT anzuwenden, ist immer gleich. Diese wird einem erst richtig klar, wenn man diese an paar alten Prüfungsaufgaben geübt hat. Ich wollte sie in dieser Zusammenfassung trotzdem vorstellen, damit man sie zumindest einmal gesehen hat und die Lösungen von den Altklausuren nachvollziehen kann. In der Klausur ist nicht die Erwartung, dass man alle Aufgaben schafft, selbst wenn man eine sehr gute Note haben will. Wenn einem also dieser Aufgabentyp zum Beispiel nicht liegt, gibt es genügend andere Aufgaben, um das zu kompensieren.