

Tutorium: Diskrete Mathematik

Vorbereitung der Klausur am 17.02.2020
(Teil 1, Lösungen)

12. Februar 2020

Steven Köhler

mathe@stevenkoehler.de

mathe.stevenkoehler.de

Aufgabe 1

a) Die höchste in $a(x) \cdot b(x)$ vorkommende Potenz ist $x^9 \cdot x^{10} = x^{19}$; der Grad von $a(x) \cdot b(x)$ ist folglich 19.

b) Berechnen und Aufsummieren aller Terme, die x^{13} ergeben:

$$x^9 \cdot (-4x^4) + 2x^7 \cdot 2x^6 + 2x^4 \cdot (-5x^9) + (-x^3) \cdot x^{10} = -11x^{13}.$$

Der gesuchte Koeffizient lautet folglich -11.

Aufgabe 2 I

$$a(x) = 2x^6 + 4x^5 + 3x^4 + 4x^3 + x^2 + 1$$

$$b(x) = 4x^2 + 4.$$

Es ergibt sich die folgende Zerlegung mit Rest:

$$a(x) = q(x) \cdot b(x) + r(x)$$

mit

$$q(x) = 3x^4 + x^3 + 4x^2$$

$$r(x) = 1$$

Aufgabe 2 II

Das Ergebnis wurde über die folgende Polynomdivision erhalten:

$$\begin{array}{r} (2x^6 + 4x^5 + 3x^4 + 4x^3 + x^2 + 1) : (4x^2 + 4) = 3x^4 + x^3 + 4x^2 \\ -(2x^6 \quad + 2x^4) \\ \hline 4x^5 + x^4 + 4x^3 + x^2 + 1 \\ -(4x^5 \quad + 4x^3) \\ \hline x^4 + x^2 + 1 \\ -(x^4 + x^2) \\ \hline 1 \end{array}$$

Aufgabe 3 I

Anwendung des Euklidischen Algorithmus ergibt:

$$\begin{aligned} 2x^3 + 2x^2 + x + 1 &\stackrel{(1)}{=} (2x - 2) \cdot (x^2 + 2x + 1) + 3x + 3 \\ x^2 + 2x + 1 &\stackrel{(2)}{=} \left(\frac{1}{3}x + \frac{1}{3}\right) \cdot (3x + 3) + 0 \end{aligned}$$

Ein größter gemeinsamer Teiler ist folglich $3x + 3$. Als normierter größter gemeinsamer Teiler ergibt sich demnach $x + 1$.

Aufgabe 3 II

Polynomdivision für (1):

$$\begin{array}{r} (2x^3 + 2x^2 + x + 1) : (x^2 + 2x + 1) = 2x - 2 \\ -(2x^3 + 4x^2 + 2x) \\ \hline -2x^2 - x + 1 \\ -(-2x^2 - 4x - 2) \\ \hline 3x + 3 \end{array}$$

Aufgabe 3 III

Polynomdivision für (2):

$$\begin{array}{r} (x^2 + 2x + 1) : (3x + 3) = \frac{1}{3}x + \frac{1}{3} \\ -(x^2 + x) \\ \hline x + 1 \\ -(x + 1) \\ \hline 0 \end{array}$$

Aufgabe 4 I

Mithilfe einer Primfaktorzerlegung von $N = 247$ müssen zunächst die ursprünglichen Primzahlen p und q bestimmt werden. Es gilt

$$247 = 13 \cdot 19.$$

Mit $p = 13$ und $q = 19$ kann nun $\varphi(N)$ berechnet werden. Es gilt

$$\varphi(247) = \varphi(13) \cdot \varphi(19) = 12 \cdot 18 = 216.$$

Zur Berechnung des privaten Schlüssels ($d, 243$) muss nun das multiplikative Inverse von $e = 23$ bezüglich $\varphi(N)$ mithilfe des erweiterten Euklidischen Algorithmus berechnet werden.

Aufgabe 4 II

Bestimmen von ggT(216, 23) mit dem Euklidischen Algorithmus:

$$216 = 9 \cdot 23 + 9$$

$$23 = 2 \cdot 9 + 5$$

$$9 = 1 \cdot 5 + 4$$

$$5 = 1 \cdot 4 + 1$$

Rückwärtseinsetzen ergibt:

$$1 = 5 - 1 \cdot 4$$

$$= 5 - 1 \cdot (9 - 1 \cdot 5)$$

$$= -1 \cdot 9 + 2 \cdot 5$$

$$= -1 \cdot 9 + 2 \cdot (23 - 2 \cdot 9)$$

$$= 2 \cdot 23 - 5 \cdot 9$$

$$= 2 \cdot 23 - 5 \cdot (216 - 9 \cdot 23)$$

$$= -5 \cdot 216 + 47 \cdot 23$$

Aufgabe 4 III

Es ist 47 das gesuchte Inverse von 23 in \mathbb{Z}_{216} . Somit ergibt sich der folgende Schlüssel:

- ▶ privater Schlüssel: (47, 247)

Entschlüsseln mithilfe des privaten Schlüssels liefert

$$42^{47} \equiv 35 \pmod{247}.$$

Aufgabe 4 IV

Berechnen von $42^{47} \pmod{247}$ mithilfe des Square & Multiply Verfahrens:

$$\begin{array}{ll} 42^{47} \equiv 42 \cdot 42^{46} & 42^2 \equiv 35 \\ 42^{46} \equiv (42^{23})^2 & 42^4 \equiv 237 \\ 42^{23} \equiv 42 \cdot 42^{22} & 42^5 \equiv 74 \\ 42^{22} \equiv (42^{11})^2 & 42^{10} \equiv 42 \\ 42^{11} \equiv 42 \cdot 42^{10} & 42^{11} \equiv 35 \\ 42^{10} \equiv (42^5)^2 & 42^{22} \equiv 237 \\ 42^5 \equiv 42 \cdot 42^4 & 42^{23} \equiv 74 \\ 42^4 \equiv (42^2)^2 & 42^{46} \equiv 42 \\ 42^2 \equiv (42^1)^2 & 42^{47} \equiv 35 \end{array} \Rightarrow$$

Aufgabe 5

Zum Nachweis sind 2 Dinge zu zeigen:

- ▶ $a, b \in G \cap H \Rightarrow a \star b, b \star a \in G \cap H$
- ▶ $a \in G \cap H \Rightarrow a^{-1} \in G \cap H$

Zum Nachweis der ersten Eigenschaft genügt die folgende Begründung:

$$\begin{aligned} & a, b \in G \cap H \\ \Rightarrow & a, b \in G \quad \text{und} \quad a, b \in H \\ \Rightarrow & a \star b, b \star a \in G \quad \text{und} \quad a \star b, b \star a \in H \\ \Rightarrow & a \star b, b \star a \in G \cap H \end{aligned}$$

Der Nachweis der zweiten Eigenschaft erfolgt analog.

Es handelt sich bei $(G \cap H, \star)$ folglich um eine Untergruppe von \mathcal{G} und \mathcal{H} .

Aufgabe 6 I

Nach dem Satz von Lagrange gilt: $|G \cap H|$ teilt $|G|$ und $|G \cap H|$ teilt $|H|$. Als mögliche Ordnung von $G \cap H$ kommt also 2, 4 und 8 infrage.

Diese Fälle müssen separat betrachtet werden.

Fall 1: $|G \cap H| = 2$:

Nach dem Satz von Lagrange können die Elemente nur Ordnung 1 oder 2 haben. Ordnung 1 kommt stets nur für das neutrale Element infrage. Das zweite Element muss Ordnung 2 haben.

Aufgabe 6 II

Fall 2: $|G \cap H| = 4$:

Nach dem Satz von Lagrange können die Elemente nur Ordnung 1, 2 oder 4 haben. Ordnung 1 kommt stets nur für das neutrale Element infrage. Die weiteren Elemente müssen Ordnung 2 oder Ordnung 4 haben. Für den Fall Ordnung 2 sind wir fertig. Hat ein Element a hingegen Ordnung 4, lässt sich mit a^2 ein Element der Ordnung 2 finden:

$$a^4 = (a^2)^2 = 1.$$

Fall 3: $|G \cap H| = 8$:

Dieser Fall funktioniert analog zu Fall 2.

Für jeden Fall lässt sich also zeigen, dass immer ein Element der Ordnung 2 existiert. \square

Aufgabe 7

Die Isomorphie kann direkt über die Angabe einer strukturerhaltenden, bijektiven Abbildung zwischen den beiden Trägermengen G und H gezeigt werden:

$$f : \frac{G \parallel 1 \mid a \mid b \mid c}{H \parallel 1 \mid \diamond \mid \triangle \mid \square}$$

Durch Nachrechnen kann leicht überprüft werden, dass für alle Elemente $x, y \in G$ stets $f(x \star y) = f(x) \circ f(y)$ gilt.

Aufgabe 8

Bei der durch den Zyklus (123) erzeugten Untergruppen handelt es sich um

$$H = \langle (123) \rangle = \{id, (123), (132)\}.$$

Es ergeben sich die folgenden Nebenklassen:

$$\begin{aligned} idH &= Hid = \{id, (123), (132)\} \\ (12)H &= H(12) = \{(12), (13), (23)\}. \end{aligned}$$

Aufgabe 9 I

- a) Zunächst wird mit der Siebformel die Anzahl der durch 2, 3 oder 7 teilbaren Elemente zwischen 1 und 42 bestimmt:

$$\left\lfloor \frac{42}{2} \right\rfloor + \left\lfloor \frac{42}{3} \right\rfloor + \left\lfloor \frac{42}{7} \right\rfloor - \left\lfloor \frac{42}{2 \cdot 3} \right\rfloor - \left\lfloor \frac{42}{2 \cdot 7} \right\rfloor - \left\lfloor \frac{42}{3 \cdot 7} \right\rfloor + \left\lfloor \frac{42}{2 \cdot 3 \cdot 7} \right\rfloor = 30.$$

Bei den verbleibenden $42 - 30 = 12$ Elementen handelt es sich um die Elemente, die weder durch 2, 3 oder 7 teilbar sind. Diese bilden die Einheitengruppe $E(\mathbb{Z}_{42})$.

- b) Mithilfe der Eulerschen φ -Funktion kann die Anzahl der zu 42 teilerfremden Zahlen bestimmt werden; diese bilden die Einheitsgruppe.

$$\varphi(42) = \varphi(2 \cdot 3 \cdot 7) = \varphi(2) \cdot \varphi(3) \cdot \varphi(7) = (2-1) \cdot (3-1) \cdot (7-1) = 12$$

Aufgabe 9 II

- b) Die Einheitengruppe $E(\mathbb{Z}_{42})$ besitzt die in \mathbb{Z}_{42} invertierbaren Elemente:

$$E(\mathbb{Z}_{42}) = \{1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41\}$$

- c) Die Ordnung von $E(\mathbb{Z}_{42})$ ist 12. Mögliche Ordnungen der Elemente sind 1, 2, 3, 4, 6 und 12. Die Gruppe ist nicht zyklisch, da kein Element die Ordnung 12 besitzt.

$$\begin{array}{lll} 5^6 \equiv 1 \pmod{42} & 19^6 \equiv 1 \pmod{42} & 31^6 \equiv 1 \pmod{42} \\ 11^6 \equiv 1 \pmod{42} & 23^6 \equiv 1 \pmod{42} & 37^3 \equiv 1 \pmod{42} \\ 13^2 \equiv 1 \pmod{42} & 25^3 \equiv 1 \pmod{42} & 41^2 \equiv 1 \pmod{42} \\ 17^6 \equiv 1 \pmod{42} & 29^2 \equiv 1 \pmod{42} & \end{array}$$

Aufgabe 10a-e

- a) $\pi = (132)(4576)(89)$.
b) $\pi = (12)(13)(46)(47)(45)(89)$;
Alternativ: $\pi = (13)(32)(45)(57)(76)(89)$.
c) π besteht aus 6 Transpositionen, ist also gerade.
d) $\text{sign } \pi = +1$.
e) π ist eine gerade, ρ ist eine ungerade Permutation mit 13 Transpositionen. Diese können nicht identisch sein, da gerade Permutationen nur durch andere gerade Permutationen dargestellt werden können; analog für ungerade Permutationen.

Aufgabe 10f

f) Bei π handelt es sich um die folgende Permutation:

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Bei φ handelt es sich um die folgende Permutation:

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 2 & 3 \end{pmatrix}$$

Die Permutationen π und φ sind also nicht identisch.