Diskrete Strukturen

Sommer 2019

Prof. Stefan Lucks, Jannis Bossert
<firstname>.<lastname>(at)uni-weimar.de

Bauhaus-Universität Weimar

November 26, 2019

Aufgabe 1: Primzahlen und k-glatte Zahlen

Sei $k \in \mathbb{N}$ und $\pi(k)$ die Anzahl der Primzahlen $p_1, \ldots, p_{\pi(k)} \leq k$ bis k. Zum Beispiel ist $\pi(5) = 3$. Eine Zahl $m \in \mathbb{N}$ heißt k-glatt wenn all ihre Primteiler kleiner gleich k sind:

$$m = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_{\pi(k)}^{e_{\pi(k)}}.$$

wobei $e_1, \ldots, e_{\pi(k)} \in \mathbb{N}_0$. Wir definieren $P_k := p_1 \cdot p_2 \cdot \cdots \cdot p_{\pi(k)}$.
Beweisen oder widerlegen Sie die folgenden Aussagen. Um eine Aussage zu widerlegen, reicht es aus, ein Gegenbeispiel zu nennen.

Aufgabe 1: Primzahlen und k-glatte Zahlen

Sei $k \in \mathbb{N}$ und $\pi(k)$ die Anzahl der Primzahlen $p_1, \ldots, p_{\pi(k)} \leq k$ bis k. Zum Beispiel ist $\pi(5) = 3$. Eine Zahl $m \in \mathbb{N}$ heißt k-glatt wenn all ihre Primteiler kleiner gleich k sind:

$$m = p_1^{e_1} \cdot p_2^{e_2} \cdot \cdots \cdot p_{\pi(k)}^{e_{\pi(k)}}.$$

wobei $e_1, \ldots, e_{\pi(k)} \in \mathbb{N}_0$. Wir definieren $P_k := p_1 \cdot p_2 \cdot \cdots \cdot p_{\pi(k)}$.
Beweisen oder widerlegen Sie die folgenden Aussagen. Um eine Aussage zu widerlegen, reicht es aus, ein Gegenbeispiel zu nennen.

Wir definieren $p_{\pi(k)}$ als die größte Primzahl kleiner gleich k.

Aufgabe 1: Primzahlen und k-glatte Zahlen

a) Für jedes $k \geq 3$ gibt es unendlich viele k-glatte Zahlen.

Aufgabe 1: Primzahlen und k-glatte Zahlen

a) Für jedes $k \geq 3$ gibt es unendlich viele k-glatte Zahlen.

Wahr: $\forall i \in \mathbb{N} : z_i = p^i_{\pi(k)}$

Aufgabe 1: Primzahlen und k-glatte Zahlen

a) Für jedes $k \geq 3$ gibt es unendlich viele k-glatte Zahlen.

Wahr: $\forall i \in \mathbb{N} : z_i = p^i_{\pi(k)}$

b) Für jedes $k \geq 3$ gibt es unendlich viele k-glatte Primzahlen.

Aufgabe 1: Primzahlen und k-glatte Zahlen

a) Für jedes $k \geq 3$ gibt es unendlich viele k-glatte Zahlen.

Wahr: $\forall i \in \mathbb{N} : z_i = p^i_{\pi(k)}$

b) Für jedes $k \geq 3$ gibt es unendlich viele k-glatte Primzahlen.

Falsch: Damit $p_{\pi(i)}$ k-glatt ist, muss gelten $p_{\pi(i)} \leq k$. Es gibt also genau $\pi(k)$ k-glatte Primzahlen.

Aufgabe 1: Primzahlen und k-glatte Zahlen

a) Für jedes $k \geq 3$ gibt es unendlich viele k-glatte Zahlen.

Wahr: $\forall i \in \mathbb{N} : z_i = p^i_{\pi(k)}$

b) Für jedes $k \geq 3$ gibt es unendlich viele k-glatte Primzahlen.

Falsch: Damit $p_{\pi(i)}$ k-glatt ist, muss gelten $p_{\pi(i)} \leq k$. Es gibt also genau $\pi(k)$ k-glatte Primzahlen.

c) Für jedes $k \geq 3$ gibt es unendlich viele Zahlen $m \in \mathbb{N}$, die nicht k-glatt sind.

Aufgabe 1: Primzahlen und k-glatte Zahlen

a) Für jedes $k \geq 3$ gibt es unendlich viele k-glatte Zahlen.

Wahr: $\forall i \in \mathbb{N} : z_i = p^i_{\pi(k)}$

b) Für jedes $k \geq 3$ gibt es unendlich viele k-glatte Primzahlen.

Falsch: Damit $p_{\pi(i)}$ k-glatt ist, muss gelten $p_{\pi(i)} \leq k$. Es gibt also genau $\pi(k)$ k-glatte Primzahlen.

c) Für jedes $k \geq 3$ gibt es unendlich viele Zahlen $m \in \mathbb{N}$, die nicht k-glatt sind.

Wahr: Zum Beispiel alle Primzahlen oder $p^i_{\pi(k)+1}, \forall i \in \mathbb{N}$.

Aufgabe 1: Primzahlen und k-glatte Zahlen

d) P_k ist die größte k-glatte Zahl.

Aufgabe 1: Primzahlen und k-glatte Zahlen

d) P_k ist die größte k-glatte Zahl.

Falsch: Aus **a)** folgt, dass es unendlich viele k-glatte Zahlen gibt. Folglich gibt es keine größte k-glatte Zahl.

Aufgabe 1: Primzahlen und k-glatte Zahlen

d) P_k ist die größte k-glatte Zahl.

Falsch: Aus **a)** folgt, dass es unendlich viele k-glatte Zahlen gibt. Folglich gibt es keine größte k-glatte Zahl.

e) Ist $m \in \mathbb{N}$ k-glatt, dann ist auch $(m \cdot P_k)$ k-glatt.

Aufgabe 1: Primzahlen und k-glatte Zahlen

d) P_k ist die größte k-glatte Zahl.

Falsch: Aus **a)** folgt, dass es unendlich viele k-glatte Zahlen gibt. Folglich gibt es keine größte k-glatte Zahl.

e) Ist $m \in \mathbb{N}$ k-glatt, dann ist auch $(m \cdot P_k)$ k-glatt.

Wahr: Alle Primfaktoren von m und P_k sind kleiner gleich k, dies gilt somit auch für das Produkt $m \cdot P_k$.

Aufgabe 1: Primzahlen und k-glatte Zahlen

d) P_k ist die größte k-glatte Zahl.

Falsch: Aus **a)** folgt, dass es unendlich viele k-glatte Zahlen gibt. Folglich gibt es keine größte k-glatte Zahl.

e) Ist $m \in \mathbb{N}$ k-glatt, dann ist auch $(m \cdot P_k)$ k-glatt.

Wahr: Alle Primfaktoren von m und P_k sind kleiner gleich k, dies gilt somit auch für das Produkt $m \cdot P_k$.

f) Ist $m \in \mathbb{N}$ $2k$-glatt, dann ist m k-glatt.

Aufgabe 1: Primzahlen und k-glatte Zahlen

d) P_k ist die größte k-glatte Zahl.

Falsch: Aus **a)** folgt, dass es unendlich viele k-glatte Zahlen gibt. Folglich gibt es keine größte k-glatte Zahl.

e) Ist $m \in \mathbb{N}$ k-glatt, dann ist auch $(m \cdot P_k)$ k-glatt.

Wahr: Alle Primfaktoren von m und P_k sind kleiner gleich k, dies gilt somit auch für das Produkt $m \cdot P_k$.

f) Ist $m \in \mathbb{N}$ $2k$-glatt, dann ist m k-glatt.

Falsch: Gegenbeispiel: $k = 3, m = 5$

Aufgabe 2: Multiplikatives Inverses

Im Folgenden seien Paare (a, b) mit $a, b \in \mathbb{Z}_n$ gegeben. Ermitteln Sie nachvollziehbar jeweils alle Werte für $n \in \mathbb{N}$ für die gilt: $a^{-1} \equiv b \bmod n$.

a) $(11, 13)$

b) $(7, 42)$

c) $(3, 25)$

d) $(17, 17)$

Aufgabe 2: Multiplikatives Inverses

Im Folgenden seien Paare (a, b) mit $a, b \in \mathbb{Z}_n$ gegeben. Ermitteln Sie nachvollziehbar jeweils alle Werte für $n \in \mathbb{N}$ für die gilt: $a^{-1} \equiv b \bmod n$.

a) $(11, 13)$

b) $(7, 42)$

c) $(3, 25)$

d) $(17, 17)$

Für n muss gelten dass

$$n \mid (a \cdot b) - 1 \qquad \text{und} \qquad a, b < n.$$

Aufgabe 2: Multiplikatives Inverses

a) $(11, 13)$

Aufgabe 2: Multiplikatives Inverses

a) $(11, 13)$
Wir haben $11 \cdot 13 - 1 = 142$.

$$n \mid 142$$

Dies gilt für $n \in \{71, 142\}$.

Aufgabe 2: Multiplikatives Inverses

a) $(11, 13)$
Wir haben $11 \cdot 13 - 1 = 142$.

$$n \mid 142$$

Dies gilt für $n \in \{71, 142\}$.

b) $(7, 42)$

Aufgabe 2: Multiplikatives Inverses

a) $(11, 13)$
Wir haben $11 \cdot 13 - 1 = 142$.

$$n \mid 142$$

Dies gilt für $n \in \{71, 142\}$.

b) $(7, 42)$
Es gilt $7 \cdot 42 - 1 = 293$.

$$n \mid 293$$

Dies gilt für $n \in \{293\}$.

Aufgabe 2: Multiplikatives Inverses

c) $(3, 25)$

Aufgabe 2: Multiplikatives Inverses

c) $(3, 25)$
Es gilt $3 \cdot 25 - 1 = 74$.

$$n \mid 74$$

Dies gilt für $n \in \{37, 74\}$.
d) $(17, 17)$

Aufgabe 2: Multiplikatives Inverses

c) $(3, 25)$
Es gilt $3 \cdot 25 - 1 = 74$.

$$n \mid 74$$

Dies gilt für $n \in \{37, 74\}$.
d) $(17, 17)$
Es gilt $17 \cdot 17 - 1 = 288$.

$$n \mid 288$$

Dies gilt für $n \in \{18, 24, 32, 36, 48, 72, 96, 144, 288\}$.

Aufgabe 3: Chinesischer Restsatz

Ermitteln Sie alle Zahlen $n < 500000$ für die gilt:

$$n \bmod 13 = 11$$
$$n \bmod 25 = 17$$
$$n \bmod 7 = 5$$
$$n \bmod 111 = 40.$$

Sollten Sie das multiplikative Inverse einer Zahl benötigen, verwenden Sie den erweiterten euklidischen Algorithmus und geben Sie Ihren Rechenweg an. Sie können Ihr Script aus Aufgabe 5 verwenden, stellen Sie jedoch sicher, dass dieses korrekt ist. Sollte Ihr Script für Aufgabe 5 fehlerhaft sein, werden hier entstehende Fehler nicht als Folgefehler gewertet!

Aufgabe 3: Chinesischer Restsatz

Mit dem chinesischen Restsatz lässt sich leicht Folgendes berechnen:

$$
\begin{aligned}
m_1 &= 13, & a_1 &= 11 \\
m_2 &= 25, & a_2 &= 17 \\
m_3 &= 7, & a_3 &= 5 \\
m_4 &= 111, & a_4 &= 40
\end{aligned}
$$

$$m = \prod m_i = 252525$$

Aufgabe 3: Chinesischer Restsatz

Mit dem chinesischen Restsatz lässt sich leicht Folgendes berechnen:

$$\begin{aligned} m_1 &= 13, & a_1 &= 11 \\ m_2 &= 25, & a_2 &= 17 \\ m_3 &= 7, & a_3 &= 5 \\ m_4 &= 111, & a_4 &= 40 \end{aligned}$$

$$m = \prod m_i = 252525$$

Mit dem erweiterten Euklid kann man $y_i = M_i^{-1}$ berechnen. $M_i = m/m_i$

$$\begin{aligned} M_1 &= 19425 & y_1 &= 9 & a_1 &= 11 \\ M_2 &= 10101 & y_2 &= 1 & a_2 &= 17 \\ M_3 &= 36075 & y_3 &= 2 & a_3 &= 5 \\ M_4 &= 2275 & y_4 &= 109 & a_4 &= 40 \end{aligned}$$

Aufgabe 3: Chinesischer Restsatz

Mit dem chinesischen Restsatz lässt sich leicht Folgendes berechnen:

$$m_1 = 13, \qquad a_1 = 11$$
$$m_2 = 25, \qquad a_2 = 17$$
$$m_3 = 7, \qquad a_3 = 5$$
$$m_4 = 111, \qquad a_4 = 40$$
$$m = \prod m_i = 252525$$

Mit dem erweiterten Euklid kann man $y_i = M_i^{-1}$ berechnen. $M_i = m/m_i$

$$M_1 = 19425 \qquad y_1 = 9 \qquad a_1 = 11$$
$$M_2 = 10101 \qquad y_2 = 1 \qquad a_2 = 17$$
$$M_3 = 36075 \qquad y_3 = 2 \qquad a_3 = 5$$
$$M_4 = 2275 \qquad y_4 = 109 \qquad a_4 = 40$$

Nun ergibt $\sum(a_i y_i M_i) \bmod m = 817$. Also sind alle $n < 500000, n \in \mathbb{N}$ die Folgenden: $817, 817 + 252525 = 253342$

Aufgabe 4: Gruppentheorie

Untersuchen Sie die folgenden Paare auf ihre Gruppeneigenschaften:

a) $(\mathbb{N}, *)$

b) $(\mathbb{Z}, *)$

c) $(\mathbb{Q} \setminus \{0\}, *)$

Geben Sie außerdem an, unter welchen Umständen $(\mathbb{Z}_n \setminus \{0\}, *)$ eine Gruppe ist.

Aufgabe 4: Gruppentheorie

a) $(\mathbb{N}, *)$

Aufgabe 4: Gruppentheorie

a) $(\mathbb{N}, *)$
Abgeschlossenheit (Gruppoid): Ja, das Produkt zweier natürlicher Zahlen ist definiert und liegt in $\mathbb{N}$.

Aufgabe 4: Gruppentheorie

a) $(\mathbb{N}, *)$
Abgeschlossenheit (Gruppoid): Ja, das Produkt zweier natürlicher Zahlen ist definiert und liegt in $\mathbb{N}$.

Assoziativität (Halbgruppe): Die Multiplikation ist assoziativ:
$a \cdot (b \cdot c) = (a \cdot b) \cdot c = a \cdot b \cdot c$

Aufgabe 4: Gruppentheorie

a) $(\mathbb{N}, *)$
Abgeschlossenheit (Gruppoid): Ja, das Produkt zweier natürlicher Zahlen ist definiert und liegt in $\mathbb{N}$.

Assoziativität (Halbgruppe): Die Multiplikation ist assoziativ:
$a \cdot (b \cdot c) = (a \cdot b) \cdot c = a \cdot b \cdot c$

Neutrales Element (Monoid): Das neutrale Element der Multiplikation ist 1. Für jede natürliche Zahl n gilt: $n \cdot 1 = 1 \cdot n = n$

Aufgabe 4: Gruppentheorie

a) $(\mathbb{N}, *)$
Abgeschlossenheit (Gruppoid): Ja, das Produkt zweier natürlicher Zahlen ist definiert und liegt in $\mathbb{N}$.

Assoziativität (Halbgruppe): Die Multiplikation ist assoziativ:
$a \cdot (b \cdot c) = (a \cdot b) \cdot c = a \cdot b \cdot c$

Neutrales Element (Monoid): Das neutrale Element der Multiplikation ist 1. Für jede natürliche Zahl n gilt: $n \cdot 1 = 1 \cdot n = n$

Inverses Element (Gruppe): Es gibt kein Inverses Element für jedes Element der Gruppe. Somit ist $(\mathbb{N}, *)$ keine Gruppe sondern nur ein Monoid.

Aufgabe 4: Gruppentheorie

b) $(\mathbb{Z}, *)$

Aufgabe 4: Gruppentheorie

b) $(\mathbb{Z}, *)$
Abgeschlossenheit (Gruppoid): Ja, das Produkt zweier ganzer Zahlen ist definiert und liegt in $\mathbb{Z}$.

Aufgabe 4: Gruppentheorie

b) $(\mathbb{Z}, *)$
Abgeschlossenheit (Gruppoid): Ja, das Produkt zweier ganzer Zahlen ist definiert und liegt in $\mathbb{Z}$.

Assoziativität (Halbgruppe): Die Multiplikation ist assoziativ:
$a \cdot (b \cdot c) = (a \cdot b) \cdot c = a \cdot b \cdot c$

Aufgabe 4: Gruppentheorie

b) $(\mathbb{Z}, *)$
Abgeschlossenheit (Gruppoid): Ja, das Produkt zweier ganzer Zahlen ist definiert und liegt in $\mathbb{Z}$.

Assoziativität (Halbgruppe): Die Multiplikation ist assoziativ:
$a \cdot (b \cdot c) = (a \cdot b) \cdot c = a \cdot b \cdot c$

Neutrales Element (Monoid): Das neutrale Element der Multiplikation ist 1. Für jede ganze Zahl n gilt: $n \cdot 1 = 1 \cdot n = n$

Aufgabe 4: Gruppentheorie

b) $(\mathbb{Z}, *)$

Abgeschlossenheit (Gruppoid): Ja, das Produkt zweier ganzer Zahlen ist definiert und liegt in $\mathbb{Z}$.

Assoziativität (Halbgruppe): Die Multiplikation ist assoziativ: $a \cdot (b \cdot c) = (a \cdot b) \cdot c = a \cdot b \cdot c$

Neutrales Element (Monoid): Das neutrale Element der Multiplikation ist 1. Für jede ganze Zahl n gilt: $n \cdot 1 = 1 \cdot n = n$

Inverses Element (Gruppe): Es gibt kein Inverses Element für jedes Element der Gruppe. Somit ist $(\mathbb{Z}, *)$ keine Gruppe sondern nur ein Monoid.

Aufgabe 4: Gruppentheorie

c) $(\mathbb{Q} \setminus \{0\}, *)$

Aufgabe 4: Gruppentheorie

c) $(\mathbb{Q} \setminus \{0\}, *)$
Abgeschlossenheit (Gruppoid): Ja, das Produkt zweier rationaler Zahlen ist definiert und liegt in $\mathbb{Q} \setminus \{0\}$.

Aufgabe 4: Gruppentheorie

c) $(\mathbb{Q} \setminus \{0\}, *)$
Abgeschlossenheit (Gruppoid): Ja, das Produkt zweier rationaler Zahlen ist definiert und liegt in $\mathbb{Q} \setminus \{0\}$.

Assoziativität (Halbgruppe): Die Multiplikation ist assoziativ:
$a \cdot (b \cdot c) = (a \cdot b) \cdot c = a \cdot b \cdot c$

Aufgabe 4: Gruppentheorie

c) $(\mathbb{Q} \setminus \{0\}, *)$
Abgeschlossenheit (Gruppoid): Ja, das Produkt zweier rationaler Zahlen ist definiert und liegt in $\mathbb{Q} \setminus \{0\}$.

Assoziativität (Halbgruppe): Die Multiplikation ist assoziativ:
$a \cdot (b \cdot c) = (a \cdot b) \cdot c = a \cdot b \cdot c$

Neutrales Element (Monoid): Das neutrale Element der Multiplikation ist 1. Für jede rationale Zahl n gilt: $n \cdot 1 = 1 \cdot n = n$

Aufgabe 4: Gruppentheorie

c) $(\mathbb{Q} \setminus \{0\}, *)$
Abgeschlossenheit (Gruppoid): Ja, das Produkt zweier rationaler Zahlen ist definiert und liegt in $\mathbb{Q} \setminus \{0\}$.

Assoziativität (Halbgruppe): Die Multiplikation ist assoziativ: $a \cdot (b \cdot c) = (a \cdot b) \cdot c = a \cdot b \cdot c$

Neutrales Element (Monoid): Das neutrale Element der Multiplikation ist 1. Für jede rationale Zahl n gilt: $n \cdot 1 = 1 \cdot n = n$

Inverses Element (Gruppe): Es gibt ein Inverses Element für jedes Element der Gruppe. Ist $n = \frac{a}{b}$, so ist $n^{-1} = \frac{b}{a} \in \mathbb{Q} \setminus \{0\}$. Somit ist $(\mathbb{Q} \setminus \{0\}, *)$ eine Gruppe.

Aufgabe 4: Gruppentheorie

Geben Sie außerdem an, unter welchen Umständen $(\mathbb{Z}_n \setminus \{0\}, *)$ eine Gruppe ist.

Aufgabe 4: Gruppentheorie

Geben Sie außerdem an, unter welchen Umständen $(\mathbb{Z}_n \setminus \{0\}, *)$ eine Gruppe ist.

$\mathbb{Z}_n \setminus \{0\} = \{1, 2, \ldots, n-1\}$, die Multiplikation ist also Modulo n
Es muss also gelten: $\forall a, b \in \mathbb{Z}_n \setminus \{0\} : a \cdot b \mod n > 0$.
Zusätzlich gilt als Voraussetzung für die Existenz von $a^{-1} \mod n$, dass ggT$(a, n) = 1$. Dies kann nur für alle $a \in \mathbb{Z}_n \setminus \{0\}$ gelten, wenn n prim ist.

Aufgabe 5: Erweiterter Euklid (Python)

Implementieren Sie den Erweiterten Euklidischen Algorithmus aus der Vorlesung (Kapitel 2.5, Folie 100ff.) in Python. Das Programm soll dabei zwei Zahlen x, y als Kommandozeilenparameter entgegennehmen und (d, a, b) zurückgeben mit $d = \text{ggT}(x, y)$ und $ax + by = d$.

Fragen?