6. Übungsblatt zu Mathematik für Informatiker I, WS 2003/04

JOACHIM VON ZUR GATHEN, OLAF MÜLLER, MICHAEL NÜSKEN

Abgabe bis Freitag, 5. Dezember 2003, 11^{11}
in den jeweils richtigen grünen oder roten Kasten auf dem D1-Flur.

Verfahrenstipp für Beweise: Überlege für jeden Schritt: Was ist bekannt? Was soll gezeigt werden? Die Antworten können einen Beweis ganz einfach machen. Auch beim Aufschreiben sorgt das für Klarheit...

Aufgabe 6.1 (Teilbarkeit). (2 Punkte)

Seien $s, t, x, y, d \in \mathbb{Z}$. Zeige:

(i) $d \mid x \wedge d \mid y \Longrightarrow d \mid (s \cdot x + t \cdot y)$.

(ii) $s \cdot x + t \cdot y = d \Longrightarrow \text{ggT}(x, y) \mid d$.

Aufgabe 6.2 (Primfaktorzerlegung, ggT, kgV). (7 Punkte)

(i) Seien $a, b \in \mathbb{R}$. Zeige: $a + b = \min\{a, b\} + \max\{a, b\}$.

Seien $r \in \mathbb{N}_{\geq 1}$, $p_1, \ldots, p_r$ prim und paarweise verschieden, $e_1, \ldots, e_r, f_1, \ldots, f_r \in \mathbb{N}$.

(ii) Zeige: Für $x \in \mathbb{N}$ gilt:

$$x \mid (p_1^{f_1} \cdot \ldots \cdot p_r^{f_r}) \iff \exists\, e_1, \ldots, e_r \in \mathbb{N} \quad x = p_1^{e_1} \cdot \ldots \cdot p_r^{e_r} \wedge e_1 \leq f_1 \wedge \ldots \wedge e_r \leq f_r.$$

Wir erinnern an die Definition des ggT:

Definition (ggT). *Seien $a, b \in \mathbb{N}$. Eine Zahl $g \in \mathbb{N}$ heißt* größter gemeinsamer Teiler von a und b *genau dann, wenn*

- $g \mid a$ *und* $g \mid b$ *gilt (g ist ein gemeinsamer Teiler), und*
- $\forall t \in \mathbb{N} \quad t \mid a \ \wedge \ t \mid b \Rightarrow t \mid g$ *gilt (jeder gemeinsame Teiler t teilt g).*

Wir schreiben dann auch $g = \text{ggT}(a, b)$.

(iii) Zeige: $\text{ggT}(p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}, p_1^{f_1} \cdot \ldots \cdot p_r^{f_r}) = p_1^{\min\{e_1, f_1\}} \cdot \ldots \cdot p_r^{\min\{e_r, f_r\}}$.

Die Definition des kgV ist ganz analog zu der des ggT:

Definition (kgV). *Seien $a, b \in \mathbb{N}$. Eine Zahl $k \in \mathbb{N}$ heißt* kleinstes gemeinsames Vielfaches von a und b *genau dann, wenn*

- $a \mid k$ *und* $b \mid k$ *gilt (k ist ein gemeinsames Vielfaches), und*
- $\forall v \in \mathbb{N} \quad a \mid v \ \wedge \ b \mid v \Rightarrow k \mid v$ *gilt (jedes gemeinsame Vielfache v ist ein Vielfaches von k).*

Wir schreiben dann auch $k = \mathrm{kgV}(a, b)$.

(iv) Zeige: $\mathrm{kgV}(p_1^{e_1} \cdot \ldots \cdot p_r^{e_r}, p_1^{f_1} \cdot \ldots \cdot p_r^{f_r}) = p_1^{\max\{e_1,f_1\}} \cdot \ldots \cdot p_r^{\max\{e_r,f_r\}}$.

(v) Seien $x, y \in \mathbb{N}$. Zeige: $\mathrm{ggT}(x, y) \cdot \mathrm{kgV}(x, y) = x \cdot y$.

(vi) Betrachte $x = 1\,639\,032\,613$ und $y = 3\,278\,156\,593$. Berechne (von Hand) $\mathrm{ggT}(x, y)$ und $\mathrm{kgV}(x, y)$. [*Tipp*: Primfaktorzerlegung ist hier nicht notwendig.]

Aufgabe 6.3 (Erweiterter Euklidischer Algorithmus). (5 Punkte)

Betrachte den folgenden Algorithmus:

Algorithmus. Erweiterter Euklidischer Algorithmus.
Eingabe: $a, b \in \mathbb{Z}$.
Ausgabe: $\ell \in \mathbb{N}$, $r_i, s_i, t_i \in \mathbb{Z}$ für $0 \le i \le \ell + 1$, und $q_i \in \mathbb{Z}$ für $1 \le i \le \ell$, wie unten berechnet.

1. $r_0 \leftarrow a, \quad r_1 \leftarrow b.$
2. $s_0 \leftarrow 1, \quad t_0 \leftarrow 0.$
3. $s_1 \leftarrow 0, \quad t_1 \leftarrow 1.$
4. $i \leftarrow 1.$
5. While $r_i \neq 0$ do 6–10
6. $\quad q_i \leftarrow r_{i-1}$ quo r_i.
7. $\quad r_{i+1} \leftarrow r_{i-1} - q_i r_i.$
8. $\quad s_{i+1} \leftarrow s_{i-1} - q_i s_i.$
9. $\quad t_{i+1} \leftarrow t_{i-1} - q_i t_i.$
10. $\quad i \leftarrow i + 1.$
11. $\ell \leftarrow i - 1.$
12. Return ℓ, r_i, s_i, t_i für $0 \le i \le \ell + 1$, und q_i für $1 \le i \le \ell$.

(i) Führe den Algorithmus für $a = 219\,215$ und $b = 807\,959$ durch. Notiere ℓ sowie in einer Tabelle i, r_i, q_i, s_i, t_i.

(ii) Zeige, dass für $0 \leq i \leq \ell + 1$ gilt: $r_i = s_i \cdot a + t_i \cdot b$.

(iii) Schließe, dass es ganze Zahlen $s, t \in \mathbb{Z}$ gibt mit $\mathrm{ggT}(a, b) = s \cdot a + t \cdot b$.

Aufgabe 6.4 (Mersenne-Zahlen). (4 Punkte)

Ziel dieser Aufgabe ist es folgenden Satz zu zeigen.

Satz. *Wenn die Mersenne-Zahl $2^k - 1$ prim ist, dann ist k prim.*

Dazu ist zu zeigen, dass für $a, b \in \mathbb{N}_{>1}$ die Zahl $2^{ab} - 1$ zusammengesetzt ist.

(i) Bestimme die Binärdarstellung von $2^k - 1$. (Mit Beweis!)

(ii) Bestimme die Binärdarstellung von $(2^7 - 1)(2^{42} + 2^{14} + 1)$.

(iii) Zerlege die Zahl
$a := (111\,1100\,0001\,1111\,1111\,1000\,0011\,1111\,1111\,0000\,0000\,0000\,0001\,1111)_2$
in Faktoren.

(iv) Bestimme die 2^5-adische Darstellung von $2^{35} - 1$. [Man könnte die Ziffern wiederum 2-adisch darstellen.]

(v) Schreibe $2^{35} - 1$ als echtes Produkt.

(vi) Bestimme die 2^a-adische Darstellung von $2^{ab} - 1$.

(vii) Schreibe $2^{ab} - 1$ als echtes Produkt. Beweise den Satz.

Aufgabe 6.5 (Induktion). (3 Punkte)

Sei φ eine Formel mit einem Parameter. Beweise:

$$\forall n \in \mathbb{N} \Big(\big(\forall i \in \mathbb{N}_{<n}\ \varphi(i)\big) \ \Rightarrow\ \varphi(n) \Big) \implies \forall n \in \mathbb{N}\ \varphi(n).$$

In Worten: Wenn für jedes $n \in \mathbb{N}$ aus der Gültigkeit der Formel φ für alle $i \in \mathbb{N}$ mit $i < n$ auf die Gültigkeit von φ für n geschlossen werden kann, dann gilt φ für alle natürlichen Zahlen.

Tipps: Was bedeutet die Voraussetzung für $n = 0$? Betrachte versuchsweise einige weitere kleine n. Bezeichne mit $\psi(n)$ die Aussage $\forall i \in \mathbb{N}_{<n}\ \varphi(i)$ und betrachte diese.

Bemerkung: Das ist eine abgewandelte Form der vollständigen Induktion. Hier kann man alle vorher erreichten Zwischenergebnisse im Induktionsschritt nutzen und braucht verblüffenderweise keinen separaten Induktionsanfang.

Aufgabe 6.6 (Erweiterter Euklidischer Algorithmus). (3 Punkte)

Berechne den ggT g von a und b und eine Darstellung der Form $g = sa + tb$.

- $a = 3\,795$ und $b = 2\,574$.
- $a = 5\,978$ und $b = 6\,699$.
- $a = 610$ und $b = 377$.

6. Übungsblatt zu Mathematik für Informatiker I, WS 2003/04, Mündlicher Teil

JOACHIM VON ZUR GATHEN, OLAF MÜLLER, MICHAEL NÜSKEN

Mündliche Aufgabe 6.7 (Teilbarkeit).

Seien $a, b, c, d, q, r \in \mathbb{Z}$. Zeige:

(i) $a \mid b \wedge c \mid d \implies (ac) \mid (bd)$.

(ii) $c \neq 0 \wedge ac \mid bc \implies a \mid b$.

(iii) $\text{ggT}(a, 0) = a$.

(iv) Wenn $a = q \cdot b + r$ ist, dann ist $\text{ggT}(a, b) = \text{ggT}(b, r)$.

(v) $(a, b) \neq (0, 0) \wedge \text{ggT}(a, b) = c \implies c \neq 0 \wedge \text{ggT}(\frac{a}{c}, \frac{b}{c}) = 1$.

Mündliche Aufgabe 6.8 (Primfaktorzerlegung, ggT, kgV).

Seien $r \in \mathbb{N}_{\geq 1}$, p prim, $e, f \in \mathbb{N}$. Zeige:

(i) Für $x \in \mathbb{N}$ gilt: $x \mid p^f \iff \exists e \in \mathbb{N} \quad x = p^e \wedge e \leq f$.

(ii) $\text{ggT}(p^e, p^f) = p^{\min\{e,f\}}$.

(iii) $\text{kgV}(p^e, p^f) = p^{\max\{e,f\}}$.

Mündliche Aufgabe 6.9 (Erweiterter Euklidischer Algorithmus).

Berechne den ggT g von a und b und eine Darstellung der Form $g = sa + tb$.

- $a = 2\,805$ und $b = 1\,001$.
- $a = 10\,013$ und $b = 9\,269$.
- $a = 47\,248$ und $b = 83\,740$.

Mündliche Aufgabe 6.10 (Repunits).

Ziel dieser Aufgabe ist es folgenden Satz zu zeigen.

Satz. *Wenn die Zahl $R_k = \frac{10^k-1}{10-1}$ prim ist, dann ist k prim.*

Bemerkung. *Bekannt ist derzeit nur, dass R_k prim ist für $k = 2$, $k = 19$, $k = 23$, $k = 317$ und $k = 1\,031$. Für $k = 49\,081$ und $k = 86\,453$ ist R_k vermutlich auch prim, dies ist aber nur mit sogenannten probabilistischen Tests überprüft worden: During 1999 Dubner discovered $R_{49\,081} = (10^{49\,081} - 1)/9$ was a probable prime. In October 2000, Lew Baxter discovered the next repunit probable prime is $R_{86\,453}$. It will be some time before this giant is proven prime! As the poet wrote:*

> *Ah, but a man's reach should exceed his grasp, or what's a heaven for? (Robert Browning)*

Für den Beweis des Satzes ist zu zeigen, dass für $a, b \in \mathbb{N}_{>1}$ die Zahl $\frac{10^{ab}-1}{10-1}$ zusammengesetzt ist.

(i) Bestimme die Dezimaldarstellung von $10^k - 1$. (Mit Beweis!)

(ii) Zerlege die Zahl

$$a := (217\,217\,000\,217\,000\,217\,000\,000\,217)_{10}$$

in Faktoren.

(iii) Bestimme die 10^3-adische Darstellung von $\frac{10^{15}-1}{10-1}$.

(iv) Schreibe $\frac{10^{15}-1}{10-1}$ als echtes Produkt.

(v) Bestimme die 10^a-adische Darstellung von $\frac{10^{ab}-1}{10-1}$.

(vi) Schreibe $\frac{10^{ab}-1}{10-1}$ als echtes Produkt. Beweise den Satz.

Mündliche Aufgabe 6.11 (Induktion rückwärts).

Sei φ eine Formel mit einem Parameter. Beweise:

$$\Big(\varphi(k) \ \wedge \ \forall j \in \mathbb{N}_{<k} \ \Big(\varphi(j+1) \Rightarrow \varphi(j)\Big)\Big) \implies \forall j \in \mathbb{N}_{\leq k} \ \varphi(j).$$

Das bedeutet wir führen eine Induktion rückwärts aus. In Worten: Wenn φ für den größten Wert gilt, und für alle geeigneten j aus $\varphi(j+1)$ die Gültigkeit von $\varphi(j)$ folgt, dann gilt φ für alle betrachteten j.