Prof. Dr. W. Buchholz

Vorlesung *Diskrete Strukturen*
Sommersemester 2009

Lösungsvorschläge für die Übungsblätter und Ergänzungen

Uwe Lück

12. Juli 2009

Blatt 1, Aufgabe 1a: Für $n \in \mathbb{N}_1 := \mathbb{N} \setminus \{0\}$ seien:[1] 2009/05/08

$$F(n) := \frac{1}{n(n+2)} \qquad G(n) := \frac{3}{4} - \frac{2n+3}{2(n+1)(n+2)}$$

Z. z.: $\mathcal{A}(n)$: $\boxed{\sum_{k=1}^{n} F(k) = G(n)}$ für $n \in \mathbb{N}_1$. *Induktionsanfang* ist $\mathcal{A}(1)$.

Im *Induktionsschritt* ist $\sum_{k=1}^{n+1} F(k) = G(n+1)$ aus $\mathcal{A}(n)$ zu folgern.

$$\sum_{k=1}^{n+1} F(k) \overset{def}{=} \sum_{k=1}^{n} F(k) + F(n+1) \overset{IH}{=} G(n) + F(n+1)$$

daher z. z: $\boxed{F(n+1) = G(n+1) - G(n)}$

$G(n+1) = \frac{3}{4} - \frac{2n+5}{2(n+2)(n+3)}$, daher

$$G(n+1) - G(n) = \frac{(n+3)(2n+3) - (n+1)(2n+5)}{2(n+1)(n+2)(n+3)}$$

Der Zähler dieses Bruchs ist $2n+4 = 2(n+2)$, daher

$$G(n+1) - G(n) = \frac{1}{(n+1)(n+3)} = F(n+1) \quad \square$$

– Das ist nicht richtiger als andere Lösungen, aber vielleicht klarer.

Die abgegebenen Lösungen formen typischerweise die Behauptung um und enden auf „$1/3 = 1/3$“. Es ist etwas seltsam, wenn in einem Beweis die Voraussetzung am Schluss und der Schluss aus der Voraussetzung am Anfang steht. Aber OK, wenn jeweils „ist äquivalent zu“ oder „zu zeigen also“ angedeutet wird, z. B. durch Fragezeichen über dem Gleichheitszeichen.

[1] $\mathbb{N}^+$ wegen *Aufgabe 10* nachträglich in $\mathbb{N}_1$ abgeändert.

Blatt 1, Aufgabe 1b: Hier ist es besonders wichtig, sich die zu betrachtenden Aussagen klarzumachen. Zu zeigen ist, dass

$$\mathcal{A}(n): \quad \boxed{a_n = 2^n + (-1)^n}$$

für alle $n \in \mathbb{N}$ gilt.

Die Rekursionsgleichung bestimmt a_n erst ab $n \geq 2$, daher müssen $\mathcal{A}(0)$ und $\mathcal{A}(1)$ „zu Fuß ausgerechnet“ werden, was auch kein Problem ist. Zu zeigen bleibt $\mathcal{A}(m)$ für $m \geq 2$. Für diesen Fall ergibt die Rekursionsgleichung

$$a_m \overset{def}{=} a_{m-1} + 2\,a_{m-2} \overset{IH}{=} [2^{m-1} + (-1)^{m-1}] + 2\,[2^{m-2} + (-1)^{m-2}]$$

Wegen $2 \cdot 2^{k+1} \overset{def}{=} 2^k$, $(-1)^{m-2} = (-1)^m$ und $(-1)^{m-1} + (-1)^m \overset{[def]}{=} 0$:

$$a_m = 2^{m-1} + 2^{m-1} + (-1)^m = 2^m + (-1)^m,$$

also $\mathcal{A}(m)$.

Ich habe plötzlich statt „n“ das Variablensymbol „m“ verwendet – aus zwei Gründen: (i) um Verwirrung bei Anwendung der Rekursionsgleichung zu vermeiden; (ii) um nun zu diskutieren, inwiefern es sich um eine Induktion oder überhaupt um einen Beweis handelt.

Ich habe *nicht* „von n auf $n+1$“ geschlossen. $\mathcal{A}(m)$ wurde auch nicht nur aus $\mathcal{A}(m-1)$ abgeleitet, vielmehr ging weiter $\mathcal{A}(m-2)$ wesentlich ein – als *„IH“*.

Es handelt sich also nicht um eine *vollständige Induktion* im ursprünglichen Sinne.

Die „Rettung“ des Beweises ist die $<_{\mathbb{N}}$-*Induktion* – Korollar zu Satz 1.1 der Vorlesung. Auf $\mathcal{A}(m)$ konnte unter der Voraussetzung geschlossen werden, dass $\mathcal{A}(k)$ für alle $k < m$ gilt – wobei für $\mathcal{A}(m)$ bei $m \geq 2$ die Voraussetzung $\mathcal{A}(k)$ nur mit $k = m-1$ und $k = m-2$ erforderlich war und $\mathcal{A}(0)$ und $\mathcal{A}(1)$ ganz *ohne* einen solchen Rückgriff auskamen.

Diese Betrachtung führt den Beweis zu einem glücklichen Ende.

Blatt 1, Aufgabe 2 (Fibonacci-Zahlen): Die „Mustererkennung“ im „Indexsalat“ ist oft mühsam, zumal wenn die Indizes auch nur mühsam zu entziffern sind. Hilfreich wären Hinweise, was für eine Umformung jeweils vorgenommen wurde.

Für $0 \leq k < n$ $\boxed{G_n(k) := a_k\, a_{n-k-1} + a_{k+1}\, a_{n-k}}$ z. z.: $\boxed{a_n = G_n(k)}$

Induktionsschritt: Der Schluss ist nur für $k+1 < n$ zu führen. In $G_n(k+1)$ kann die Rekursionsgleichung auf a_{k+2} angewandt werden, danach ergibt sich eine weitere Anwendung auf a_{n-k}:

$$\begin{aligned} G_n(k+1) &= a_{k+1}\, a_{n-k-2} + a_{k+2}\, a_{n-k-1} \\ &\overset{def}{=} a_{k+1}\, a_{n-k-2} + (a_k + a_{k+1})\, a_{n-k-1} \\ &= a_k\, a_{n-k-1} + a_{k+1}\, (a_{n-k-2} + a_{n-k-1}) \\ &\overset{def}{=} a_k\, a_{n-k-1} + a_{k+1}\, a_{n-k} \quad = \quad G_n(k) \quad \overset{IH}{=} \quad a_n \quad \square \end{aligned}$$

Speziell folgt $a_{2n} = G_{2n}(n)$, also

$$a_{2n} = a_n\, a_{2n-n-1} + a_{n+1}\, a_{2n-n} = a_n\, a_{n-1} + a_{n+1}\, a_n = a_n\, (a_{n-1} + a_{n+1})$$

somit $a_n \mid a_{2n}$ (Diesen Aufgabenteil habe ich in der Übung vergessen!)

Blatt 1, Aufgabe 4a: unproblematisch, nur zum späteren Rückverweis:

$$\boxed{\textstyle\sum_i^n (a_i + b_i) = \sum_i^n a_i + \sum_i^n b_i}$$

Induktionsanfang ist in dieser Aufgabe immer $\mathcal{A}(0)$.

Blatt 1, Aufgabe 4b: Beim Schritt

$$\textstyle\sum_j^m \sum_i^n a_{ij} + \sum_j^m a_{n+1,j} = \sum_j^m \sum_i^{n+1} a_{ij}$$

wird durchgehend geschummelt, zum Teil wie Forster, *Analysis I*, 4. Aufl., S. 12 (Appell an die Vorstellung einer allgemeinen Summe vieler Summanden, Pünktchen-Notation). Korrekt sollte auf *Aufgabe 4a* verwiesen werden. *Damit*

$$\textstyle\sum_j^m \sum_i^n a_{ij} + \sum_j^m a_{n+1,j} \overset{4a}{=} \sum_j^m (\sum_i^n a_{ij} + a_{n+1,j}) \overset{def}{=} \sum_j^m \sum_i^{n+1} a_{ij} \quad \square$$

Blatt 1, Aufgabe 4c: Analog zu 1a etwa:

$$G(n+1) - G(n) = (a_{n+2} - a_0) - (a_{n+1} - a_0) = a_{n+2} - a_{n+1} = F(n+1) \quad \square$$

Blatt 1, Aufgabe 3: Vorab leicht zu verifizieren (3 Fälle):

$$\overline{sg}(0) = 1 \qquad \text{und} \qquad \overline{sg}(x) = 0 \quad \text{für } x \in \mathbb{N}_1.$$

$sg(x) = 1 \dot{-} \overline{sg}(x)$, daher

$$sg(0) = 0 \qquad \text{und} \qquad sg(x) = 1 \quad \text{für } x \in \mathbb{N}_1.$$

Bemerkung: In Bezug auf $\mathbb{N}$ ist sg die *charakteristische Funktion* oder *Indikatorfunktion*[2] $\mathbf{1}_{\mathbb{N}_1}$ von $\mathbb{N}_1$, $\overline{sg}$ ist die charakteristische Funktion $\mathbf{1}_{\{0\}}$ der Komplement(är)menge $\{0\} = \mathbb{N} \setminus \mathbb{N}_1$. Außerdem ist sg die Einschränkung der *Signumfunktion* (und auch der *Heaviside-Funktion* Θ_0) auf $\mathbb{N}$.

Für $y \in \mathbb{N}_1$ wird

$$\mathcal{A}(x): \quad \boxed{r(x,y) < y \quad \text{und} \quad F_y(x) := y \cdot q(x,y) + r(x,y) = x}$$

durch vollständige Induktion nach x bewiesen.

$\mathcal{A}(0)$ gilt trivial wegen $r(0,y) := 0 =: q(0,y)$. $\mathcal{A}(x+1)$ aus $\mathcal{A}(x)$:

Es sei $\boxed{G_y(x) := y \dot{-} [r(x,y)+1].}$ Aus $\mathcal{A}(x)$ folgt $r(x,y)+1 \leq y$.

Falls $\boxed{r(x,y)+1 < y}$: $G_y(x) > 0 = \overline{sg}(G_y(x))$, $sg(G_y(x)) = 1$,

$$r(x+1,y) \overset{def}{=} r(x,y)+1 \overset{Fall}{<} y$$
$$F_y(x+1) \overset{def}{=} y \cdot q(x,y) + [r(x,y)+1] \overset{IH}{=} x+1$$

Andernfalls $\boxed{r(x,y)+1 = y}$; $G_y(x) = 0 = sg(G_y(x))$, $\overline{sg}(G_y(x)) = 1$,

$$r(x+1,y) \overset{def}{=} 0 < y$$
$$F_y(x+1) \overset{def}{=} y \cdot [q(x,y)+1] = y \cdot q(x,y) + y \overset{Fall}{=} y \cdot q(x,y) + [r(x,y)+1] \overset{IH}{=} x+1$$

Bemerkungen: (i) $x \mapsto r(x,y)$ ist eine „diskrete Sägezahnfunktion“, die Schritt für Schritt um 1 wächst, wenn sie nicht bei Teilern von y auf 0 „zurückfällt“. – (ii) $x \mapsto q(x,y)$ ist eine „diskrete Treppenfunktion“, die konstant bleibt, wenn sie nicht bei Teilern von y um 1 ansteigt. – Vgl. Lemma 1.6 im Skriptum– x geteilt durch y ist $q(x,y)$ mit Rest $r(x,y)$![3]

[2] Bedeutsam in der Maßtheorie, der Rekursionstheorie und der Beweistheorie.

[3] Die Aufgabe zeigt letzlich, dass die Division mit Rest auf $\mathbb{N}$ *primitiv-rekursiv* ist, vgl. H. Hermes, *Aufzählbarkeit, Entscheidbarkeit, Berechenbarkeit*, 1971, S. 65ff.

Blatt 2, Aufgabe 5a: Mit $\boxed{G_n(k) := x^{n-k}\, y^k}$ $(0 \le k \le n)$ ist 2009/05/15

$$\mathcal{A}(n; x, y): \quad \boxed{(x-y) \cdot \sum_{k=0}^{n} G_n(k) = x^{n+1} - y^{n+1}} \quad \text{für } n \in \mathbb{N}$$

sinnvoll und z. z.; IA also $\mathcal{A}(0; x, y)$. IS: $G_{n+1}(k) = x \cdot G_n(k)$, daher

$$\begin{aligned}
(x-y) \cdot \sum_{k=0}^{n+1} G_{n+1}(k) &\overset{def}{=} (x-y) \cdot \left(\sum_{k=0}^{n} G_{n+1}(k) + G_{n+1}(n+1) \right) \\
&= x\,(x-y) \sum_{k=0}^{n} G_n(k) + (x-y)\, x^0\, y^{n+1} \\
&\overset{IH}{=} x\,(x^{n+1} - y^{n+1}) + x\, y^{n+1} - y^{n+2} \\
&= x^{n+2} - y^{n+2} \quad \square
\end{aligned}$$

Blatt 2, Aufgabe 5b: $\boxed{M_n := 2^n - 1}$ ist die *n-te Mersenne-Zahl.*[4] Wir beweisen die zur Behauptung äquivalente Aussage

Ist n keine Primzahl, so ist M_n keine Primzahl.

Diese Aussage trifft für $n = 0$ und $n = 1$ zu, weil $M_0 = 0$ und $M_1 = 1$ keine Primzahlen sind. Ist $n \in \mathbb{N}\backslash\{0, 1\} =: \mathbb{N}_2$[5] keine Primzahl, so gibt es $r, s \in \mathbb{N}_2$[6] mit $n = rs$. $\mathcal{A}(s-1; 2^r, 1^r)$ gemäß *Aufgabe 5a* ergibt dann

$$M_n = (2^r)^s - (1^r)^s = (2^r - 1) \cdot \sum_{k=0}^{s-1} (2^r)^{s-1-k}$$

Wegen $1 < 2^r < 2^{rs}$ sind dann sowohl $2^r - 1$ als auch die Summe positive nicht-triviale Teiler von M_n, d. h. sie sind größer als 1 und kleiner als M_n. $\square$

[4] *Marin Mersenne* 1588–1648, frz. Mönch, Priester, Mathematiker, Musiktheoretiker.
[5] $\mathbb{N}^{++}$ wegen *Aufgabe 10* nachträglich in $\mathbb{N}_2$ abgeändert.
[6] bzw. Skriptum: $r, s < n$ ...

Blatt 2, Aufgabe 6: a und b lösen $x^2 - x - 1 = 0$:[7]

$$\left(\frac{1 \pm \sqrt{5}}{2}\right)^2 = \frac{1}{4} + \frac{5}{4} \pm \frac{\sqrt{5}}{2} = 1 + \frac{1 \pm \sqrt{5}}{2}$$

Äquivalent zur Behauptung[8] ist

$$\mathcal{A}(n): \quad \boxed{\sqrt{5}\, F_n = a^n - b^n} \quad \text{für } n \in \mathbb{N}_1$$

$\mathcal{A}(0)$ und $\mathcal{A}(1)$ sind klar. Für $n \in \mathbb{N}_2$:

$$\begin{array}{rcl} a^n - b^n & = & a^2\, a^{n-2} - b^2\, b^{n-2} \quad = \quad (a+1)\, a^{n-2} - (b+1)\, b^{n-2} \\ & = & a^{n-1} - b^{n-1} + a^{n-2} - b^{n-2} \\ & \overset{IV}{=} & \sqrt{5}\,(F_{n-1} + F_{n-2}) \quad \overset{def}{=} \quad \sqrt{5}\, F_n \end{array}$$

In diese Betrachtung sind als *„IV“* $\mathcal{A}(n-1)$ und $\mathcal{A}(n-2)$, eingeflossen, was wie in *Aufgabe 1b* als $<_{\mathbb{N}}$-Induktion rechtfertigt werden kann. $\square$[9]

[7] a (oder manchmal b) wird *Goldener Schnitt* genannt, weil bei Streckenverhältnissen $c : d = (c+d) : c$ die Gleichung $\frac{c}{d} = \frac{c+d}{c} = a$ erfüllt wird.

[8] Formel von *de Moivre* (1730) bzw. *Binet* (1843).

[9] Im Wikipedia-Artikel *Fibonacci-Folge* gibt es noch „elegantere“ Herleitungen.

$$(x_0,\dots,x_n) \sqsubset (y_0,\dots,y_n) \;:\Longleftrightarrow\; (\exists k \le n)\Big(x_k < y_k \;\&\; (\forall i < k)(x_i = y_i)\Big)$$

Blatt 2, Aufgabe 7 – Lösung „n fest“. *Idee:* Zu einer nicht-leeren Teilmenge M von $\mathbb{N}^{n+1}$ werden nacheinander m_0, m_1, … so bestimmt, dass $(m_0,\dots,m_n)$ kleinstes Element von M ist. 2009/05/15 nur angedeutet.

Kleine Abkürzung: Seien $s = (x_0,\dots,x_n)$ und $t = (y_0,\dots,y_n) \in \mathbb{N}^{n+1}$. $s =^k t$ heißt $\forall i \le k\colon\ x_i = y_i$. Damit

$$s \sqsubset t \iff (\exists k \le n)(x_k < y_k \;\&\; x =^{k-1} y)$$

Sei $\emptyset \neq M \subseteq \mathbb{N}^{n+1}$. Wir definieren rekursiv *nicht-leere* Teilmengen M_k von M, $0 \le k \le n$, die für $k > 0$ die Eigenschaft haben, unter $=^{k-1}$ „abgeschlossen“ zu sein in folgendem Sinne:

$$s \in M_k \;\&\; t \in M \;\&\; s =^{k-1} t \implies t \in M_k \qquad (\mathcal{A}(k))$$

– $M_k \neq \emptyset$ und $\mathcal{A}(k)$ sind durch vollständige Induktion nachzuweisen.

Es sei $M_0 := M$ $(\neq \emptyset)$.

Ist M_k definiert $(0 \le k \le n)$ und nicht leer, so sei für $m \in \mathbb{N}$

$$M_{k,m} := \{\, (x_0,\dots,x_n) \in M_k : x_k = m \,\}$$

M_k hat (IV) mindestens ein Element $(y_0,\dots,y_n)$, ein solches ist in M_{k,y_k}. Daher ist $\{\, m \in \mathbb{N} : M_{k,m} \neq \emptyset \,\}$ nicht-leere Teilmenge von $\mathbb{N}$ und hat wegen des *Prinzips vom kleinsten Element* (Skriptum Satz 1.3) ein *kleinstes* Element m_k. Wir setzen $M_{k+1} := M_{k,m_k}$.

Ist $(x_0,\dots,x_n) \in M_1$, so ist $x_0 = m_0$, und alle $(y_0,\dots,y_n)$ mit $y_0 = m_0 = x_0$ sind in M_1, also $\mathcal{A}(1)$. Gilt $\mathcal{A}(k)$ für $k \ge 1$, und ist $s = (x_0,\dots,x_n) \in M_{k+1}$ und $t = (y_0,\dots,yn) \in M$ mit $s =^k t$, so gilt auch $s =^{k-1} t$, und t ist nach $\mathcal{A}(k)$ wie s in M_k. Außerdem gilt wegen $s =^k t$ $x_k = y_k$, und t ist nach Konstruktion in M_{k+1} – damit $\mathcal{A}(k+1)$.

Nach Konstruktion ist $M_{n+1} = \{(m_0,\dots,m_n)\}$, dieses Element von M_{n+1} heiße u. Es bleibt zu zeigen, dass u das *kleinste* Element von M ist. Sei $s = (x_0,\dots,x_n)$ ein *anderes* Element von M. Dann $\exists k, 0 \le k \le n$, $x_k \neq m_k$, d. h. $A := \{\, k \in \mathbb{N} : k \le n \;\&\; x_k \neq m_k \,\} \neq \emptyset$. Wieder nach dem *Prinzip vom kleinsten Element* gibt es ein *kleinstes* Element k_0 von A. Demnach $s =^{k_0-1} u$, und nach $\mathcal{A}(k_0)$ ist $s \in M_{k_0}$. Nach der Wahl von m_{k_0} ist dann $m_{k_0} < x_{k_0}$, damit $u \sqsubset s$. □

Blatt 2, Aufgabe 7 – Lösung „Induktion nach n“. Wir bezeichnen die lexikografische Ordnung auf $\mathbb{N}^{n+1}$ als $\sqsubset^{n+1}$ und beweisen durch Induktion nach n, dass jede nicht-leere Teilmenge von $\mathbb{N}^{n+1}$ ein kleinstes Element bezüglich $\sqsubset^{n+1}$ hat.

IA: $n = 0$. *Vorbetrachtung:* $\forall (x_0), (y_0) \in \mathbb{N}^1\colon\ (x_0) \sqsubset^1 (y_0) \iff x_0 < y_0$.

Seien $M \subseteq \mathbb{N}^1$, $M \neq \emptyset$ und $M' := \{\, x_0 \in \mathbb{N} : (x_0) \in M \,\}$. $M' \neq \emptyset$ wegen $M \neq \emptyset$, nach *Prinzip vom kleinsten Element* hat M' ein Element m_0 mit $\forall m \in M', m \neq m_0\colon\ m_0 < m$. Für jedes $(x_0) \in M \setminus \{(m_0)\}$ gilt $(m_0) \sqsubset^1 (x_0)$, d. h. (m_0) ist kleinstes Element von M bezüglich $\sqsubset^1$.

IS: Es seien $\emptyset \neq M \subseteq \mathbb{N}^{n+2}$ und

$$M' := \{\, (x_0, \ldots, x_n) \in \mathbb{N}^{n+1} : \exists x_{n+1} \in \mathbb{N}\colon (x_0, \ldots, x_n, x_{n+1}) \in M \,\}$$

Ist $(y_0, \ldots, y_{n+1}) \in M$, so ist $(y_0, \ldots, y_n) \in M'$, daher $\emptyset \neq M' \subseteq \mathbb{N}^{n+1}$, nach IV hat M' ein kleinstes Element $u' = (u_0, \ldots, u_n)$ bezüglich $\sqsubset^n$. Nach Konstruktion ist $\{\, m \in \mathbb{N} : (u_0, \ldots, u_n, m) \in M \,\} \neq \emptyset$ und hat nach *Prinzip vom kleinsten Element* ein *kleinstes* Element u_{n+1}.

Zu zeigen bleibt, dass $u := (u_0, \ldots, u_{n+1})$ kleinstes Element von M ist. Sei $s = (x_0, \ldots, x_{n+1})$ ein *anderes* Element von M. Dann $\exists k$, $0 \leq k \leq n+1$: $x_k \neq u_k$, d. h. $A := \{\, k \in \mathbb{N} : k \leq n \;\&\; x_k \neq u_k \,\} \neq \emptyset$. Wieder nach *Prinzip vom kleinsten Element* hat A ein *kleinstes* Element k_0.

Ist $k_0 \leq n$, so ist $s' := (x_0, \ldots, x_n) \in M'$, und $u' \sqsubset^{n+1} s'$ gilt nach Wahl von u', dies impliziert $u \sqsubset^{n+2} s$. Ist $k_0 = n+1$, so ist $s' = u'$, und $u_{n+1} < x_{n+1}$ gilt nach Wahl von u_{n+1}, damit ebenfalls $u \sqsubset^{n+2} s$. □

Blatt 2, Aufgabe 7 – Lösung „Induktion nach n *extra*“.[10] Mit Abkürzungen aus §2 der Vorlesung betrachten wir für $n \in \mathbb{N}$ $(n+1)$-Tupel $t = (x_0, \ldots, x_n) \in \mathbb{N}^{n+1}$ als durch $t(k) = x_k$ definierte Abbildungen $t : I_{n+1} \to \mathbb{N}$, also $\mathbb{N}^{n+1}$ als $\mathbb{N}^{I_{n+1}}$. $\sqsubset^{n+1}$ bezeichnet die lexikografische Ordnung auf $\mathbb{N}^{n+1}$.

2009/05/15 nicht vorgetragen.

[10] Geht auf verschiedene Konstrukte der Vorlesung ein, die für die Aufgabe nicht unbedingt nötig wären. Inhaltlich, also von Notationstricks abgesehen, lehnt sich der Beweis an die vorhergehende Version an.

Weiter ist $()$ das „0-Tupel“ bzw. die „leere Abbildung“ $e : I_0 \to \mathbb{N}$ mit $I_0 = \emptyset$ gemäß Vorlesung. $\mathbb{N}^0$ sei $\{()\}$. Die „lexikografische“ Ordnung $\sqsubset^0$ ist eine „leere“ Relation auf $\mathbb{N}^0$, die durch $() \not\sqsubset^0 ()$ definiert ist, auch gemäß der Aufgabenstellung. Die einzige nicht-leere Teilmenge $\{()\}$ von $\mathbb{N}^0$ hat $()$ als kleinstes Element bezüglich $\sqsubset^0$.[11]

Durch vollständige Induktion nach n zeigen wir, dass jede nicht-leere Teilmenge von $\mathbb{N}^n$ ein kleinstes Element bezüglich $\sqsubset^n$ hat – $\mathcal{A}(n)$. $\mathcal{A}(0)$ haben wir eben erklärt.

Für $t \in \mathbb{N}^{n+1}$ sei $t^* := t\big|_{I_n}$ (Einschränkung auf I_n, $t(n)$ wird „entfernt“, eventuell $t^* = ()$.) Für $t \in \mathbb{N}^n$ und $m \in \mathbb{N}$ sei $t * (m)$ die durch $t(n) := m$ definierte Erweiterung von t auf I_{n+1} ($\Longrightarrow$ $t * (m) \in \mathbb{N}^{n+1}$).[12]

IS: Wir zeigen $\mathcal{A}(n) \implies \mathcal{A}(n+1)$. Es seien $\emptyset \neq M \subseteq \mathbb{N}^{n+1}$ und $M' := \{ t^* : t \in M \}$. $M \neq \emptyset \implies M' \neq \emptyset$; u' sei das *kleinste* Element von M' – ein solches existiert nach $\mathcal{A}(n)$. $u' = s^*$ für ein $s \in M$ nach Konstruktion von M', damit

$$s(n) \in A := \{ m \in \mathbb{N} : u' * (m) \in M \}$$

also $A \neq \emptyset$, und nach *Prinzip vom kleinsten Element* hat A ein kleinstes Element u_n.

Zu zeigen bleibt, dass $u := u' * (u_n)$ kleinstes Element von M ist. Sei $u \neq t \in M$.[13] Dann $\exists k,\ 0 \leq k \leq n$: $t(k) \neq u(k)$, d. h.

$$B := \{ k \in \mathbb{N} : k \leq n \ \&\ t(k) \neq u(k) \} \neq \emptyset$$

Wieder nach *Prinzip vom kleinsten Element* hat B ein *kleinstes* Element k_0. Ist $k_0 < n$, so ist $t^* \in M'$, und $u^* = u' \sqsubset^n t^*$ gilt nach Wahl von u', dies impliziert $u \sqsubset^{n+1} t$. Ist $k_0 = n$, so ist $t^* = u^*$, und $u(n) = u_n < t(n)$ gilt nach Wahl von u_n, damit ebenfalls $u \sqsubset^{n+1} t$. □

[11] Diese Betrachtung ist auch für die „b-adische Darstellung“ (Skriptum 1.6f.) von Interesse.

[12] Vgl. Skriptum: Bemerkung zu Satz 1.7. $s := t * (m) \implies s(k) = t(k)$, $k \in I_n$. Man könnte auch $t \frown (m)$ schreiben. Die Schreibweisen ersparen das Ausschreiben von „$(x_0, \ldots, x_n)$“ und machen Formeln übersichtlicher. Auch die Verwirrung, die durch das mit 0 beginnende Numerieren der Folgenglieder wird gemildert. All die Tricks machen den Beweis zwar insgesamt sogar *länger*, nützen vielleicht *dennoch* – fürs bessere Verständnis und für später.

[13] D. h. t ist ein *anderes* Element von M.

Blatt 2, Aufgabe 8b. ($\boxed{I_n := \{\, k \in \mathbb{N} : k < n \,\}}$ gemäß Vorlesung §2.)

Die Voraussetzung $D(b^{k+1}; a) = (c_n, \ldots, c_0)$ bedeutet nach Vorl., Satz 1.7 und den dort anschließenden Bemerkungen

$$\boxed{a = \sum_{i=0}^{n} c_i (b^{k+1})^i} \qquad \text{mit} \quad \forall i \le n : c_i \in I_{b^{k+1}} \quad \& \quad c_n > 0 \qquad (a)$$

Die Voraussetzung $D(b; c_n) = (c_{nm}, \ldots, c_{n0})$ bedeutet analog

$$\boxed{c_n = \sum_{j=0}^{m} c_{nj} b^j} \qquad \text{mit} \quad \forall j \le m : c_{nj} \in I_b \quad \& \quad c_{nm} > 0 \qquad (b)$$

Vorausgesetzt wird schließlich noch

$$\forall i \in I_n \qquad \boxed{c_i = \sum_{j=0}^{k} c_{ij} b^j} \qquad \text{mit} \quad \forall j \le k : c_{ij} \in I_b \qquad (c)$$

Die *Behauptung*

$$\begin{array}{ccccccccccccccc} D(b;a) = (c_{nm}, \ldots, c_{n0}, & c_{n-1,k}, \ldots, & c_{n-1,0}, \ldots\ldots\ldots, & c_{1k}, \ldots, & c_{10}, & c_{0k}, \ldots, & c_{00}) \\ \| & \| \quad \| & \| & \| & \| & \| \quad \| & \| \\ \gamma_{N+m} & \gamma_N \quad \gamma_{N-1} & \gamma_{(n-1)(k+1)} & \gamma_{2k+1} & \gamma_{k+1} & \gamma_k \quad \gamma_0 \end{array}$$

bedeutet analog mit $\boxed{N := n\,(k+1)}$

$$\boxed{a = \sum_{\nu=0}^{N+m} \gamma_\nu b^\nu} \quad \text{mit} \quad \gamma_\nu = \begin{cases} c_{n,\nu-N} & \text{für} \quad N \le \nu \le N+m \\ c_{ij} & \text{für} \quad 0 \le \nu = i\,(k+1) + j < N, \\ & \qquad i < n, \quad j \le k \end{cases}$$

– dabei sind i, j nach Lemma 1.5 eindeutig bestimmt durch *„ν geteilt durch $k+1$ ist i, Rest j“*, etwa mit den Funktionen q und r aus *Aufgabe 3*: $i = q(\nu, k+1)$ und $j = r(\nu, k+1)$. Die Behauptung impliziert *darüber hinaus* wesentlich $\gamma_{N+m} = c_{nm} > 0$, was aber schon aus (b) unmittelbar folgt.

2009/05/18 nicht vorgetragen.

Einsetzen von (b) und (c) in (a) ergibt

$$\begin{aligned} a &= \left(\sum_{i=0}^{n-1} \left(\sum_{j=0}^{k} c_{ij} b^j \right) b^{(k+1)i} \right) + \left(\sum_{j=0}^{m} c_{nj} b^j \right) b^{(k+1)n} \\ &= \sum_{i=0}^{n-1} \sum_{j=0}^{k} c_{ij} b^{i(k+1)+j} + \sum_{j=0}^{m} c_{nj} b^{n(k+1)+j} \\ &= \sum_{\nu=0}^{N-1} c_{q(\nu,k+1),r(\nu,k+1)} b^\nu + \sum_{\nu=N}^{N+m} a_\nu b^\nu \quad = \quad \sum_{\nu=0}^{N+m} a_\nu b^\nu \end{aligned}$$

Zur Umwandlung $\sum\sum \mapsto \sum$ beweist man notfalls als Lemma etwa 2009/05/15 nur angedeutet.

$$\sum_{\kappa=0}^{q(\mu,\beta)-1}\sum_{\lambda=0}^{\beta-1}\gamma_{\kappa,\lambda} + \sum_{\lambda=0}^{r(\mu,\beta)-1}\gamma_{q(\mu,\beta),\lambda} = \sum_{\nu=0}^{\mu-1}\gamma_{q(\nu,\beta),r(\nu,\beta)}$$

durch vollständige Induktion nach μ ähnlich wie in *Aufgabe 3* und setzt $\beta = k+1$ und $\mu = N$ ein (dann $q(\mu,\beta) = n$ und $r(\mu,\beta) = 0$). Tatsächlich gelten in der Aufgabe $0 < c_{nm} \implies b^m \le c_{nm}b^m \le c_n < b^{k+1} \implies m \le k \implies m+1 = r(N+m+1, k+1)$,[14] was man für a schon eine Zeile früher anwenden kann. □

Blatt 2, Aufgabe 8a. Automatisch erzeugt: 2009/05/18 nicht vorgetragen.

$D(9; 893) = (1, 2, 0, 2)$

$D(2; 2009) = (1, 1, 1, 1, 1, 0, 1, 1, 0, 0, 1)$

$D(8; 2009) = (3, 7, 3, 1)$

$D(16; 2009) = (7, 13, 9)$ [= `7D9`]

$D(2; 13466917) = (1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 0, 1)$

$D(16; 13466917) = (12, 13, 7, 13, 2, 5)$ [= `CD7D25`]

[14] 2009/05/15 vorgetragen.

Blatt 3, Aufgabe 9. $f : \mathbb{Z}^2 \to \mathbb{Z}^2$ ist definiert durch $\boxed{f(x_1, x_2) = (y_1, y_2)}$ 2009/05/15 mit

$$\boxed{\text{(Y1)} \quad y_1 = 3x_1 + 2x_2} \quad \& \quad \boxed{\text{(Y2)} \quad y_2 = 7x_1 + 5x_2}$$

Sind $y_1, y_2 \in \mathbb{Z}$ gegeben, so zeigt Addition von $5 \cdot$ (Y1) und $-2 \cdot$ (Y2) bzw. von $-7 \cdot$ (Y1) und $3 \cdot$ (Y2), dass nur

$$\boxed{\text{(X1)} \quad x_1 = 5y_1 - 2y_2} \quad \& \quad \boxed{\text{(X2)} \quad x_2 = -7y_1 + 3y_2}$$

die Gleichungen (Y1) und (Y2) erfüllen – f ist *injektiv*.

$\boxed{g(y_1, y_2) := (x_1, x_2) \quad \text{gemäß (X1) und (X2)}}$ liefert offenbar $g : \mathbb{Z}^2 \to \mathbb{Z}^2$.

Für $x_1, x_2 \in \mathbb{Z}$ folgt aus (Y1), (Y2), (X1), (X2) $g(f(x_1, x_2)) = (x_1, x_2)$, also $g \circ f = \mathrm{id}_{\mathbb{Z}^2}$.

In Matrizenschreibweise[15] werden (X1) und (X2) durch

$$\begin{pmatrix} x_1 \\ x_2 \end{pmatrix} = \begin{pmatrix} 5 & -2 \\ -7 & 3 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

und (Y1) und (Y2) durch $\begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix} \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}$ ausgedrückt. Setzt man $\boxed{(z_1, z_2) := f(g(y_1, y_2))}$, so errechnet man mit denselben beiden 2×2-Matrizen

$$\begin{pmatrix} z_1 \\ z_2 \end{pmatrix} = \begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix} \begin{pmatrix} 5 & -2 \\ -7 & 3 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \end{pmatrix} = \begin{pmatrix} y_1 \\ y_2 \end{pmatrix}$$

(Dies steht in engem Zusammenhang mit $\begin{pmatrix} 3 & 2 \\ 7 & 5 \end{pmatrix} \begin{pmatrix} 5 & -2 \\ -7 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ – Assoziativität der Matrizenmultiplikation, die beiden linken Matrizen sind invers zueinander.)

Zu gegebenen $y_1, y_2 \in \mathbb{Z}$ ist daher $(x_1, x_2) := g(y_1, y_2)$ ein Element von $\mathbb{Z}^2$, für das $f(x_1, x_2) = (y_1, y_2)$. f bildet also $\mathbb{Z}^2$ *surjektiv* auf sich selbst ab, gleichzeitig haben wir $f \circ g = \mathrm{id}_{\mathbb{Z}^2}$.

Insgesamt ist also $f : \mathbb{Z}^2 \leftrightarrow \mathbb{Z}^2$ mit *Umkehrabbildung* g. □

[15] Für die Aufgabe genügt schlichtes Ausrechnen von $f(g(y_1, y_2))$, die Matrizenschreibweise fördert lediglich das Verständnis.

Blatt 3, Aufgabe 10. *Folgende Darstellung beruht wesentlich auf*

`http://www.mathematik.uni-muenchen.de/~buchholz/DS09/loes3.pdf`

$6\mathbb{N} := \{\, 6n : n \in \mathbb{N} \,\}$ ist die Menge der durch 6 teilbaren natürlichen Zahlen.

(a) $h(x) = x^3 - x = x \cdot (x^2 - 1) = (x-1) \cdot x \cdot (x+1) \implies$

$h(x)$ hat Nullstellen -1, 0, $+1$; $h(0) = 0 = h(1) \implies$ *h nicht injektiv.*

Genau eine der Zahlen in $\{(x-1), x, (x+1)\}$ ist durch 3 teilbar, und mindestens eine ist durch 2 teilbar $\implies$ das Produkt $h(x)$ ist sowohl durch 3 als auch durch 2 teilbar [...], also auch durch 6[16] $\implies$ $h(x) \in 6\mathbb{N}$. □

(b) $h_1 : \mathbb{N}_1 \to 6\mathbb{N}$ ist die Einschränkung $h\big|_{\mathbb{N}_1}$ von $h : \mathbb{N} \to \mathbb{N}$ auf $\mathbb{N}_1 := \{\, n \in \mathbb{N} : n \geq 1 \,\}$. Im Gegensatz zu h im vorigen Aufgabenteil hat h_1 daher nur noch *eine* Nullstelle. Für *Injektivität* von h_1 bleibt zu zeigen, dass auch $k \in \mathbb{N}_1$ nur noch von *einem* l durch $h(l) = k$ „getroffen“ wird. Die *Grundidee* ist, dass *streng monotone* Abbildungen *injektiv* sind.

Es seien $x, y \in \mathbb{N}_1$. *Ohne Beschränkung der Allgemeinheit* $0 < y < x$. Laut *Hinweis* $x^3 - y^3 = (x-y)\,(x^2 + xy + y^2) \implies$

$$\begin{aligned} h(x) - h(y) &= (x^3 - x) - (y^3 - y) \\ &= (x-y)\,(x^2 + xy + y^2) - (x-y) \\ &= (x-y)\,(x^2 + xy + y^2 - 1) \quad > \quad 0 \end{aligned}$$

– die letzte Zeile beruht auf $x - y > 0$ und $x^2 + xy + y^2 \geq 4 + 2 + 1 > 1$. Somit $h_1(x) \neq h_1(y)$, h_1 injektiv.

Nicht surjektiv: $h_1(1) = 0$, $h_1(2) = 6$ $h_1(3) = 24$; für $x > 3$ ist $h_1(x) > h(3)$, wie eben zur Injektivität gezeigt. □

[16] Wird im Anschluss an *Aufgabe 18a* nachgetragen!

Blatt 3, Aufgabe 11a: Es werden *zwei* Beweise vorgestellt.[17]

Schreibweisen:
$$\boxed{\begin{array}{l}\mathcal{P}_g(M) := \{\, U \in \mathcal{P}(M) : |U| \text{ gerade} \,\} \\ \mathcal{P}_u(M) := \{\, U \in \mathcal{P}(M) : |U| \text{ ungerade} \,\} \\ A = B \,\dot\cup\, C :\Longleftrightarrow\ A = B \cup C \ \ \& \ \ B \cap C = \emptyset\end{array}}$$

$B \,\dot\cup\, C$ wird als *disjunkte Vereinigung* von B und C bezeichnet.

Erster Beweis durch vollständige Induktion nach $|M|$:

Nach Aufgabenstellung $M \neq \emptyset \implies$ IA $|M| = 1 \implies \mathcal{P}_g(M) = \{\emptyset\}$ & $\mathcal{P}_u(M) = \{M\} \implies |\mathcal{P}_g(M)| = |\mathcal{P}_u(M)|$.

IS: Wähle $a \in M$, $\boxed{M' := M \setminus \{a\}}$ Damit

$$\mathcal{P}_g(M) = \mathcal{P}_g(M') \,\dot\cup\, \{\, U \cup \{a\} : U \in \mathcal{P}_u(M') \,\}$$

Die Abbildung $U \mapsto U \cup \{a\} = U \,\dot\cup\, \{a\}$ für $U \subseteq M'$ ist *injektiv* $\implies$

$$\begin{aligned} |\mathcal{P}_g(M)| &\overset{L.2.2}{=} \left|\mathcal{P}_g(M')\right| + \left|\{\, U \cup \{a\} : U \in \mathcal{P}_u(M') \,\}\right| \\ &\overset{L.2.5(a)}{=} |\mathcal{P}_g(M')| + |\mathcal{P}_u(M')| \end{aligned}$$

Nach IV $\boxed{m^* := |\mathcal{P}_g(M')| = |\mathcal{P}_u(M')|} \implies |\mathcal{P}_g(M)| = 2m^*$. Analog

$$|\mathcal{P}_u(M)| = \left|\mathcal{P}_u(M') \,\dot\cup\, \{\, U \cup \{a\} : U \in \mathcal{P}_g(M') \,\}\right| = m^* + |\mathcal{P}_g(M')| = 2m^* \quad \square$$

[17] Beide skizziert von Prof. Buchholz, siehe Link in *Aufgabe 10*.

Zweiter Beweis mithilfe *Lemma 2.7 (b):* Es sei[18]

2009/05/18 nicht vorgetragen.

$$\boxed{n^* := \left\lfloor \frac{|M|}{2} \right\rfloor = \max\{\, n \in \mathbb{N} : 2n < |M| \,\} \iff 2n^* \le |M| \le 2n^* + 1}$$

Analog zur Betrachtung von $\mathcal{P}(X)$ als *disjunkter Vereinigung* der $\mathcal{P}_k(X)$, $k \in I_{|X|}$, im Beweis von *Lemma 2.7* ist $\mathcal{P}_g(M)$ disjunkte Vereinigung der $\mathcal{P}_k(M)$ mit *geraden* $k \in I_{|M|}$ $\Longrightarrow$

$$\begin{aligned} |\mathcal{P}_g(M)| &= \sum_{k=0}^{n^*} |\mathcal{P}_{2k}(M)| \overset{L.2.7(b)}{=} \sum_{k=0}^{n^*} \binom{|M|}{2k} \\ &\overset{L.2.7(a)}{=} 1 + \sum_{k=1}^{n^*} \left[\binom{|M|-1}{2k-1} + \binom{|M|-1}{2k} \right] = \sum_{k=0}^{|M|-1} \binom{|M|-1}{k} \end{aligned}$$

(Für $|M|$ gerade ist $\binom{|M|-1}{2n^*} = 0$.)

Analog zu oben ist $\mathcal{P}_u(M)$ disjunkte Vereinigung der $\mathcal{P}_k(M)$ mit *ungeraden* $k \in I_{|M|}$ $\Longrightarrow$ (für $|M|$ gerade ist das letzte Summenglied 0)

$$\begin{aligned} |\mathcal{P}_u(M)| &= \sum_{k=0}^{n^*} |\mathcal{P}_{2k+1}(M)| \overset{L.2.7(b)}{=} \sum_{k=0}^{n^*} \binom{|M|}{2k+1} \\ &\overset{L.2.7(a)}{=} \sum_{k=0}^{n^*} \left[\binom{|M|-1}{2k} + \binom{|M|-1}{2k+1} \right] = \sum_{k=0}^{|M|-1} \binom{|M|-1}{k} \quad \square \end{aligned}$$

Somit $|\mathcal{P}_g(M)| = |\mathcal{P}(M')| = \mathcal{P}_u(M)$ mit $M' = M \setminus \{a\}$ für irgendein $a \in M$ – man vergleiche den *ersten* Beweis.

Blatt 3, Aufgabe 11b: *Empfehlung der Aufgabenstellung:*[19]

$$\boxed{M_k := \{\, X \subseteq \{1, \ldots, n\} : |X| = 3 \;\;\&\;\; \min X = k \,\}}$$

$\mathcal{P}_3(\{1, \ldots, n\})$ ist disjunkte Vereinigung der M_k mit $1 \le k \le n-2$.

$M_k = \{\, Y \cup \{k\} : Y \in \mathcal{P}_2(\{k+1, \ldots, n\}) \,\} \Longrightarrow |M_k| = \binom{n-k}{2} \Longrightarrow$

$$\binom{n}{3} = |\mathcal{P}_3(\{1, \ldots, n\})| = \sum_{k=1}^{n-2} |M_k| = \sum_{k=1}^{n-2} \binom{n-k}{2} \quad \square$$

[18] „Gaußklammer“

[19] Wie Prof. Buchholz, Link in Aufgabe 10.

Blatt 3, Aufgabe 11b, Alternative durch Rechnen: Einige haben vollständige Induktion nach n verwendet:

2009/05/18 nicht vorgetragen.

IA $n = 3$: $\sum_{k=1}^{3-2} \binom{3-k}{2} = \binom{2}{2} = 1 = \binom{3}{3}$.

IS $n \to n+1$: $\sum_{k=1}^{n-1} \binom{n+1-k}{2} = \sum_{k=1}^{n-1} \left[\binom{n-k}{1} + \binom{n-k}{2}\right] = \sum_{k=1}^{n-1}(n-k) + \sum_{k=1}^{n-2} \binom{n-k}{2} + \binom{1}{2} = \frac{n\,(n-1)}{2} + \binom{n}{3} = \binom{n}{2} + \binom{n}{3} = \binom{n+1}{3}$ □

Blatt 3, Aufgabe 12a. $\boxed{G_n(k) := \binom{n-k+1}{k}}$ für $0 \le k \le n$.

2009/05/18 11 Uhr 40 – einige müssen während des Vortrags gehen.

$$\boxed{\mathcal{P}_k^*(\{1,\ldots,n\}) := \{\, X \in \mathcal{P}_k(\{1,\ldots,n\}) : (\forall i \in X)(i+1 \notin X) \,\}}\ [20]$$

Z. z. $\mathcal{A}(n)$: $\boxed{f_{n,k} := |\mathcal{P}_k^*(\{1,\ldots,n\})| = G_k(n)}$ für $0 \le k \le n$.

Tatsächlich kommt es in Teil (b) auf $f_{0,0}$ an, hierfür kann $\{1,\ldots,0\}$ als $\emptyset$ verstanden werden.[21]

... Induktion nach n:

(1) Zunächst für $k = 0$ und *alle* n: $\mathcal{P}_0^*(\{1,\ldots,n\}) = \{\emptyset\} \implies f_{0,0} = 1 = \binom{n+1}{0} = G_n(0) \implies \mathcal{A}(0)$.[22] In der Folge wird $k > 0$ vorausgesetzt.

(2) Nun wird $0 < k = n$ für *alle* n abgehandelt.

Grundsätzlich erfüllen einelementige Mengen die Zusatzbedingung $\implies \mathcal{P}_1^*(\{1\}) = \mathcal{P}_1(\{1\}) = \{\{1\}\} \implies f_{1,1} = 1 = \binom{1}{1} = G_1(1) \implies \mathcal{A}(1)$.

Für $n > 1$ enthält jedoch das einzige Element $\{1,\ldots,n\}$ von $\mathcal{P}_n(\{1,\ldots,n\})$ 1 zusammen mit $1+1=2$ und verletzt dadurch die Zusatzbedingung $\implies f_{n,n} = 0 = \binom{1}{n} = G_n(n)$.[23]

---

[20] Schreibweise und Gedankengang übernommen von Prof. Buchholz, siehe Link in *Aufgabe 10* oben.

[21] Oder man versteht $f_{n,k}$ als $|\{\, X \in \mathcal{P}_k(I_{n+1} \cap \mathbb{N}_1) : (\forall i \in X)(i+1 \notin X) \,\}|$ ($\mathbb{N}_1 = \{\, n \in \mathbb{N} : n \ge 1 \,\}$ gemäß *Aufgabe 10*).

[22] An der Tafel stand vorübergehend fälschlich $\binom{n}{0}$.

[23] An der Tafel stand vorübergehend fälschlich $f_{1,n}$.

(3) IS: Es bleibt $\mathcal{A}(n)$ für $0 < k < n$ zu zeigen.

$$\mathcal{P}_k^*(\{1,\dots,n\}) = \mathcal{P}_k^*(\{1,\dots,n-1\}) \dot\cup \{\, X \cup \{n\} : X \in \mathcal{P}_{k-1}^*(\{1,\dots,n-2\}) \,\}$$

$$\Longrightarrow \quad \boxed{f_{n,k} = f_{n-1,k} + f_{n-2,k-1}} \quad \Longrightarrow \qquad (*)$$

$f_{n,k} \overset{IH}{=} G_{n-1}(k) + G_{n-2}(k-1) = \binom{n-k}{k} + \binom{n-k}{k-1} \overset{P.\Delta}{=} \binom{n-k+1}{k} = G_k(n).$

Verwendet wurden $\mathcal{A}(n-1)$ und $\mathcal{A}(n-2)$, der Beweis ist eine $<_{\mathbb{N}}$-Induktion. □

Blatt 3, Aufgabe 12b:[24] Beh.: $\boxed{\sum_{k=0}^{n} f_{n,k} = F_{n+2}}$ – F_n Fibonacci-Zahlen. 2009/05/18 nicht vorgetragen.

IA: $f_{0,0} = |\mathcal{P}_0^*(\{\})| = 1 = F_2, \quad f_{1,0} + f_{1,1} = |\{\emptyset\}| + |\{\{1\}\}| = 1+1 = 2 = F_3.$

IS: $\sum_{k=0}^{n} f_{n,k} \overset{(*)}{=} 1 + \sum_{k=1}^{n-1}(f_{n-1,k} + f_{n-2,k-1}) = 1 + \sum_{k=1}^{n-1} f_{n-1,k} + \sum_{k=1}^{n-1} f_{n-2,k-1}.$

Nach (1) ist $f_{n,0} = 1 = f_{n-1,0}$, und durch „Variablensubstitution“ in der rechten Summe ergibt sich

$$\sum_{k=0}^{n} f_{n,k} = \sum_{k=0}^{n-1} f_{n-1,k} + \sum_{k=0}^{n-2} f_{n-2,k} \overset{IH}{=} F_{n+1} + F_n \overset{def}{=} F_{n+2}$$

Als IH wurde hier wieder auf die Fälle „$n-1$“ und „$n-2$“ zurückgegriffen – $<_{\mathbb{N}}$-Induktion. □

[24] Ganz wie Prof. Buchholz, siehe Link in Aufgabe 10.

Blatt 4, Aufgabe 13. Für die Dauer der Behandlung der Aufgabe heiße

2009/05/25 angedeutet, loes4.pdf vorgetragen

$$\boxed{B \subseteq \mathbb{N}\ m\text{-zulässig } (m \in \mathbb{N}_1) \quad :\Longleftrightarrow \quad \forall i \in B : i + m \notin B}$$

Für $M := \{\, n \in \mathbb{N} : 1 \leq n \leq 100 \,\}$ (Aufgabenstellung) sei

$$\boxed{z(m) := \max \{\, |A| : A \subseteq M \ m\text{-zulässig} \,\}}$$

Aufgabenteil (a) ergibt $\boxed{|A| = 55 \implies A \text{ nicht mehr 9-zulässig}}$ – also $z(9) < 55$, während für (b) ein 9-zulässiges $A' \subseteq M$ zeigt, dass $z(9) = 54$.[25] — Bearbeiter (m/w) X. Y.[26] aus Z. meinte, $z(10)$ sei $=44$ (oder kleiner?), tatsächlich ist $z(10) = 50$, wie in der Folge skizziert.

Für die Suche nach der größtmöglichen Mächtigkeit m-zulässiger Mengen kann man sich auf *maximal* m-zulässige Mengen beschränken. B heiße *m-maximal in C*, wenn $B \subseteq C \subseteq M$ und $\boxed{\forall c \in C \setminus B\colon \{c - m, c + m\} \cap B \neq \emptyset}$
Lemma: $z(m) = \{\, |A| : A \subseteq M,\ A\ m\text{-maximal in } M \,\}$.

Die Suche wird weiter einfacher durch Betrachtung der „Restklassen“ $\subseteq M$ *modulo* m. Für $\boxed{k \in \{1, \ldots, m\}}$ sei $\boxed{M_{m,k} := \{\, k + im \in M : i \in \mathbb{N} \,\}}$[27]
Lemma: A ist m-maximal in $M \iff \forall k \in \{1, \ldots, m\} : A \cap M_{m,k}$ ist m-maximal in $M_{m,k}$.

In *Aufgabe 12* kam sinngemäß 1-Zulässigkeit vor. Darauf lässt sich m-Zulässigkeit zurückspielen: Für $B \subseteq M$ sei $\boxed{R_{m,k}(B) := \{\, i \in \mathbb{N} : k + im \in B \,\}}$
Lemma: B ist m-maximal in $M_{m,k} \iff R_{m,k}(B)$ ist 1-maximal in $R_{m,k}(M)$.

Falls $m \mid 100$, so ist $R_{m,k}(M) = \{0, \ldots, \frac{100}{m} - 1\}$. Falls $100 \equiv k_0 \bmod m$, $1 \leq k_0 < m$, so $R_{m,1}(M) = R_{m,2}(M) = \ldots = R_{m,k_0}(M) = \{0, \ldots, \lfloor \frac{100}{m} \rfloor\}$, während $R_{m,k_0+1}(M) = \ldots = R_{m,m}(M) = \{0, \ldots, \lfloor \frac{100}{m} \rfloor - 1\}$.

---

[25] Siehe Lösung von Prof. Buchholz,
http://www.mathematik.uni-muenchen.de/~buchholz/DS09/loes4.pdf

[26] Name von der Redaktion geändert! Urheberrechtlich: Der vorstehende Witz stammt von Freimut Wössner. Dank für den Lösungsversuch: Erst deshalb (und auf Marco Rauscheckers Bericht hin) habe ich mir die Mühe hier gegeben, die Aufgabe besser zu verstehen.

[27] Die $M_{m,k}$, $k \in \{1, \ldots, m\}$, sind die „Bahnen“ einer „lokalen Gruppe“, die von $1 \mapsto 1 + m$ erzeugt wird und auf M operiert – vgl.
http://de.wikipedia.org/wiki/Gruppenoperation
Allgemein bilden *Bahnen* eine *Zerlegung* der Menge, auf der eine Gruppe operiert.

Lemma: 1-maximale Teilmengen von $R_{m,k}(M)$ enthalten 0 oder 1 sowie mit i auch $i+2$ oder $i+3$ (falls noch in $R_{m,k}(M)$).

$$\boxed{R^*_{m,k} := \{\, 2j : j \in \mathbb{N} \;\;\&\;\; k + 2jm \in M \,\}}$$

hat jedenfalls maximale Mächtigkeit unter den 1-zulässigen Teilmengen von $R_{m,k}(M)$, daher

$$\boxed{z(m) = \left| \bigcup_{k=1}^{m} \{\, k + im : i \in R^*_{m,k} \,\} \right| = \sum_{k=1}^{m} |R^*_{m,k}|}$$

Tatsächlich sind alle $R^*_{9,k} = \{0, 2, 4, 6, 8, 10\}$, $z(9) = 6 \cdot 9 = 54$,

$$\begin{aligned} A' &:= \bigcup_{k=1}^{9} \{\, k + 9i : i \in R^*_{9,k} \,\} \\ &= \{1, 2, \ldots, 9, 19, 20, \ldots, 91, 92, \ldots, 99\} \end{aligned}$$

ist 9-zulässig. — $R^*_{10,k} = \{0, 2, 4, 6, 8\}$, daher $z(10) = 5 \cdot 10 = 50$,

$$\begin{aligned} A'' &:= \bigcup_{k=1}^{10} \{\, k + 10i : i \in R^*_{10,k} \,\} \\ &= \{1, 2, \ldots, 10, 21, 22, \ldots, 30, \ldots 81, 82, \ldots, 90\} \end{aligned}$$

ist 10-zulässig. □

Blatt 4, Aufgabe 14a. Mit $\boxed{G_k(i) := \binom{i}{k}}$

2009/05/25 wohl ohne G_k etc. vorgetragen

z. z.: $\mathcal{A}_k(n)$: $\boxed{\sum_{i=k}^{n} G_k(i) = \sum_{i=k}^{n} \binom{i}{k} = \binom{n+1}{k+1} =: H_k(n)}$ $(k \leq n)$

IA: $n = 0 \implies k = 0 \implies$

$$\sum_{i=k}^{n} G_k(i) = \sum_{i=0}^{0} \binom{i}{0} = \binom{0}{0} = 1 = \binom{0+1}{0+1} = H_0(0) = H_k(n)$$

$\implies \mathcal{A}_0(0)$.

IS: Wir gehen von $\mathcal{A}_k(n)$ für $k \leq n$ aus:

$$\begin{aligned} H_k(n+1) &= \binom{n+2}{k+1} \overset{P.\Delta}{=} \binom{n+1}{k+1} + \binom{n+1}{k} = H_k(n) + \binom{n+1}{k} \\ &\overset{HV}{=} \sum_{i=k}^{n} \binom{i}{k} + \binom{n+1}{k} = \sum_{i=k}^{n+1} \binom{i}{k} = \sum_{i=k}^{n+1} G_k(i) \end{aligned}$$

Hierbei fällt allerdings $\mathcal{A}_{n+1}(n+1)$ unter den Tisch, also noch

2009/05/25 allerdings

$$\sum_{i=n+1}^{n+1} G_{n+1}(i) = \binom{n+1}{n+1} = 1 = \binom{n+2}{n+2} = H_{n+1}(n+1) \quad \square$$

2009/05/25 ansonsten entlang loes4.pdf.

Blatt 4, Aufgabe 16. Kleine Ergänzungen[28] zu den Lösungsvorschlägen von Prof. Buchholz:[29]

(c) $c \neq 0 \;\&\; x(bc) = ac \implies xb = a \mid a$ – vielleicht mit *Lemma 1.5* (Eindeutigkeit der Division mit Rest).

(d) $xb = a \implies (-x)(-b) = a$; $x(-b) = a \implies xb = -a$; $xb = -a \implies (-x)b = a$ – der Kreis schließt sich. □

(f) Beh. $a \mid 1 \implies a \in \{1, -1\}$: Sei $xa = 1$. Dann $a \neq 0 \neq x$, $|a| \geq 0 \leq |x|$. Wäre $|a| > 1$, so wäre $|xa| = |x| \cdot |a| > 1$. Also $|a| = 1$, $a \in \{1, -1\}$. □

(i) Falls $a \neq 0 \neq b$, so folgen mit (h) $|b| \leq |a|$ aus $b \mid a$ und $|a| \leq |b|$ aus $a \mid b$, also $|a| = |b|$. □

(j) Seien $a, b \in \mathbb{Z}$ mit denselben positiven Teilern.

1. Ist $a = 0$, so ist jedes $k \in \mathbb{N}_1$ Teiler von a und damit auch von b. Wäre $b \neq 0$, so wäre auch $|b| + 1$ Teiler von b, und mit (h) würde $\big||b| + 1\big| \leq |b|$ folgen – Widerspruch. Es bleibt $b = 0$, damit $|b| = 0 = |a|$.

2. Ist $a \neq 0$, so ist $|a|$ positiver Teiler von a (denn $1 \cdot |a| = a$ oder $(-1) \cdot |a| = a$), und damit auch von b und wegen (d) von $|b|$. Wäre $b = 0$, so wäre (analog zu 1.) jedes $k \in \mathbb{N}_1$ Teiler von a, und a wäre 0 im Widerspruch zur Voraussetzung. $|b|$ ist daher positiver Teiler von b und schließlich auch von $|a|$. Aus (i) folgt $|a| = \big||a|\big| = \big||b|\big| = |b|$. □

2009/05/25 11:43 fertig!

[28] getippt 2009/06/07

[29] loes4.pdf, siehe Link in Fußnote zu *Aufgabe 13*!

Blatt 5, Aufgabe 17 = *Lemma 3.5* der Vorlesung, Skriptum S. 10, wird dort bewiesen, hier kleine Ergänzungen dazu, alternative Beweise, historische Bemerkungen. 2009/06/08

Blatt 5, Aufgabe 17a. *Behauptung:*

$$\boxed{a \mid bc \;\;\&\;\; \mathsf{ggT}(a,b) = 1 \implies a \mid c}$$

Beweis im Skriptum: Mit *Lemma 3.3* folgt aus $\mathsf{ggT}(a,b) = 1$ Existenz von x, y mit $\boxed{xa + yb = 1}$. Dann $a \mid xac$, und wegen $a \mid bc$ und $bc \mid ybc$ aus (a) von *Aufgabe 16* = Skriptum S. 8 auch $a \mid ybc$. Mit (b) von dort folgt $a \mid xac + ybc = c$. □

Direkterer Beweis: $1 = xa + yb$ wie zuvor, zudem $az = bc$ für $a \mid bc$. Dann $c = (xa+yb)\,c = xac+ybc = axc+yaz = a\,(xc+yz)$, also $a \mid c$. □

Bemerkung: Varianten von $a \mid bc \implies a \mid c$ mit „a, b Primzahlen“ (statt wie hier nur „relativ prim“) oder auf *Hauptidealbereiche*[30] ausgedehnt sind als *„Lemma von Euklid“* bekannt – nicht zu verwechseln mit dem *„Satz von Euklid“*, Skriptum Satz 3.9. Der zweite Beweis oben verwendet das *„Lemma von Bézout“* ($1 = xa+yb$), das in *Lemma 3.3* verallgemeinert wird. – Jeweils zu ergoogeln bei *Wikipedia* und *Wikiversity*.[31] 2009/06/08 nur Namen

Ü-Lemma 5.1 = $(*)$ im Skriptum zum Beweis von *Lemma 3.5 (c)*.[32]

$$\boxed{a \mid c \;\;\&\;\; b \mid c \;\;\&\;\; \mathsf{ggT}(a,b) = 1 \implies ab \mid c}$$

Beweis aus (a): $b \mid c \implies c = by \implies a \mid by \overset{\text{(a)}}{\implies} a \mid y \implies y = az \implies c = baz \implies ab \mid c$ □

Beweis nach Skriptum mit Lemma 3.3: $ua = c = vb \;\;\&\;\; 1 = xa + yb \implies c = (xa + yb) \cdot c = xavb + ybua = (xv + yu) \cdot ab \implies ab \mid c$ □

Blatt 3, Aufgabe 10, Nachtrag: In der Übung vom 18. Mai wurden $2 \mid h(x)$ und $3 \mid h(x)$ gezeigt. Um $\boxed{h(x) \in 6\mathbb{N}}$ zu folgern, wurde eigentlich auf „Ü-Lemma 5.1“ vorgegriffen.

[30] Vgl. *Satz 3.1* der Vorlesung.

[31] Vor allem `http://de.wikiversity.org/Zahlentheorie/Teilbarkeit/Lemma_von_Euklid/Fakt_mit_Beweisklappe`

[32] Zum Vergleich mit (a) vorgezogen.

Man hätte sofort wie folgt vorgehen können:

$2 \mid h(x) \implies \exists a \in \mathbb{N} : h(x) = 2a$; $3 \mid h(x) \implies \exists b \in \mathbb{N} : h(x) = 3b$. Also $2a = h(x) = 3b \implies a = (3-2)a = 3a - 3b \implies h(x) = 2a = 6(a-b) \implies 6 \mid h(x) \implies h(x) \in 6\mathbb{N}$. □

Dies ist einfach dem zweiten Beweis von *Aufgabe 17a* abgeschaut (*Wikiversity*) bzw. ein Spezialfall des ersten Beweises von „Ü-Lemma 5.1“, gleichzeitig ein einfaches Anwendungsbeispiel der vorigen Aussagen.

Prof. Buchholz hat in seiner Übung so dem Problem Rechnung getragen, dass Lemma 3.5 für Aufgabe 10 noch nicht zur Verfügung stand: $3 \mid h(x) \implies \exists a \in \mathbb{N} : h(x) = 3a$. Wäre 2 *nicht* Teiler von a, so wären a und damit $h(x) = 3a$ ungerade, Widerspruch; es gibt also ein b mit $a = 2b$, also $h(x) = 3 \cdot 2 \cdot b$.[33] 2009/06/08 ausgelassen

Dabei bedeutet „ungerade“ zunächst „hat Gestalt $2k+1$“. Dass „ungerade“ in diesem Sinne dasselbe ist wie Teilbarkeit durch 2, ging schon aus *Lemma 1.5* (Eindeutigkeit der Division mit Rest) hervor. □

Ü-Lemma 5.2 (eigene Ergänzung). Für jede Primzahl p und jede ganze Zahl a: $\mathsf{ggT}(p,a) = p \iff p \mid a$; $\mathsf{ggT}(p,a) = 1 \iff p \notin T(a)$. 2009/06/08 ausgelassen

Beweis: $p \mid a \implies p \in T(p,a)$. Wegen Folgerung (g) (Skriptum S. 8 bzw. Aufgabe 16) $p = \mathsf{ggT}(p)$, also $\mathsf{ggT}(p,a) = p$. $p \notin T(a) \implies 1$ ist größter Teiler von p außer p, siehe Beweis von *Lemma 3.6a = Aufgabe 19a* (schon hier ausführbar). Wegen $1 \mid a$ daher $\mathsf{ggT}(p,a) = 1$. □

Ü-Lemma 5.3 = (∗) im Skriptum zum Beweis von *Lemma 3.5 (b).*

$$\underbrace{\mathsf{ggT}(a,c) = 1 = \mathsf{ggT}(b,c)}_{(**)} \implies \mathsf{ggT}(ab,c) = 1$$

Beweis wie im Skriptum mit Lemma 3.3: Wegen (∗∗) gibt es u, v, x, y mit $\boxed{ua + vc = 1 = xb + yc}$. Damit

$$1 = 1 \cdot 1 = (ua + vc)(xb + yc) = ux \cdot ab + (uay + vxb + vcy) \cdot c$$

Mit Lemma 3.3 folgt $\mathsf{ggT}(ab,c) = 1$. □

[33] Soweit habe ich es in der Übung vom 18. Mai erzählt. Den folgenden wichtigen Zusatz hat mir Herr Buchholz noch hinterher erklären müssen.

Beweis aus (a): Es sei $\boxed{d := \mathsf{ggT}(ab, c)}$, und es gelte $(**)$.

zur Abschreckung – 2009/06/08 ausgelassen

$d = 0$ würde $c = 0$ implizieren, was der Voraussetzung $\mathsf{ggT}(a, c) = 1$ widerspräche.[34]

Andere Annahme: $d > 1$. Nach *Satz 1.2* der Vorlesung (Existenz einer Primfaktorzerlegung) hat d irgendeine *Primzahl* $d^* > 1$ als Teiler, notfalls $d^* = d$. Wegen *Lemma 3.2 (c)*[35] $d^* \in T(ab, c)$, während wegen $\mathsf{ggT}(a, c) = 1$ $d^* \notin T(a, c)$. Also $d^* \notin T(a)$. Wegen $\mathsf{ggT}(a, c) = 1$ $a \neq 0$, und da d^* als *Primzahl* gewählt wurde, $\mathsf{ggT}(d^*, a) = 1$ („Ü-Lemma“ 5.2). Wegen $d^* \in T(ab, c)$ gilt $d^* \mid ab$. Nach Aufgabenteil (a) somit $d^* \mid b$. Allerdings eben auch $d^* \mid c$, also $\mathsf{ggT}(b, c) \geq d^* > 1$ im Widerspruch zu $(**)$.

Daher bleibt nur $\mathsf{ggT}(ab, c) = d = 1$. □

Die „Ü-Lemmata“ 5.1 und 5.3 werden im Rest der Aufgabe auf längere Produkte verallgemeinert. Die Gedankengänge sind exakt die des Skriptums.

Blatt 5, Aufgabe 17b. Wie Skriptum lasse ich a_0 weg!

$$\boxed{\forall i \in \{1, \ldots, n\} : \mathsf{ggT}(a_i, b) = 1 \implies \mathsf{ggT}(a_1 \cdots a_n, b) = 1}$$

wird durch vollständige Induktion nach n gezeigt. $n = 1$ trivial. IS: Es gelte $\boxed{\forall i \in \{1, \ldots, n+1\} : \mathsf{ggT}(a_i, b) = 1}$. Wegen der $i \in \{1, \ldots, n\}$ liefert IH $\mathsf{ggT}(a_1 \cdots a_n, b) = 1$, außerdem folgt $\mathsf{ggT}(a_{n+1} = 1)$. Daher ergibt „Ü-Lemma 5.3“ $\mathsf{ggT}(a_1 \cdots a_{n+1}, b) = \mathsf{ggT}((a_1 \cdots a_n) \cdot a_{n+1}, b) = 1$. □

Blatt 5, Aufgabe 17c. Wie Skriptum lasse ich a_0 weg!

$$\boxed{a_i,\ i \in \{1, \ldots, n\}, \text{ paarweise teilerfremd sowie } \in T(b) \implies a_1 \cdots a_n \mid b}$$

wird durch vollständige Induktion nach n gezeigt. $n = 1$ trivial. IS: Es gelte $\boxed{\forall i, j \in \{1, \ldots, n+1\} \, [\, \mathsf{ggT}(a_i, a_j) = 1 \ \ \& \ \ a_i \mid b \,]}$. Wegen der $i, j \in \{1, \ldots, n\}$ liefert IH $\underline{a_1 \cdots a_n \mid b}$, außerdem folgt $\underline{a_{n+1} \mid b}$. Weiter

$$\mathsf{ggT}(a_1, a_{n+1}) = \cdots = \mathsf{ggT}(a_n, a_{n+1}) = 1$$

daher aus Aufgabenteil (b) $\underline{\mathsf{ggT}(a_1 \cdots a_n, a_{n+1}) = 1}$. Daher ergibt „Ü-Lemma 5.1“ (angewandt auf $a_1 \cdots a_n$, a_{n+1}, b) $a_1 \cdots a_{n+1} = (a_1 \cdots a_n) \cdot a_{n+1} \mid b$. □

[34] $\mathsf{ggT}(b_1, \ldots, b_k) = 0 \iff \forall i \in \{1, \ldots, k\} : b_i = 0$

[35] Teiler von gemeinsamen Teilern sind gemeinsame Teiler.

Blatt 5, Aufgabe 18a = *Bemerkung* auf S. 10 im Skriptum. Kleine Ergänzung des dortigen Beweises:

Mit $d := \mathsf{ggT}(a_1, \ldots, a_{n-1})$, $c := \mathsf{ggT}(d, a_n)$, $b := \mathsf{ggT}(a_1, \ldots, a_n)$, $T_n := T(a_1, \ldots, a_n)$ gilt nach *Lemma 3.3* $T(d) = T(a_1, \ldots, a_{n-1})$ und daher

$$T_n = T(a_1, \ldots, a_{n-1}) \cap T(a_n) = T(d) \cap T(a_n) = T(d, a_n)$$

Wie zur Definition des ggT im Skript auf S. 8 unten *bemerkt*, folgt wie gewünscht $b = c$, denn *entweder* ist $T_n = T(d, a_n) = \mathbb{Z}$ (alle $a_i = 0$), so dass $b = 0 = c$, *oder* $b = \max T_n = \max T(d, a_n) = d$. □

Blatt 5, Aufgabe 18b. Nach Aufgabenteil (a) gilt

$$\begin{aligned} \mathsf{ggT}(7469, 2464, 4515, 2639) &= \mathsf{ggT}(\mathsf{ggT}(7469, 2464, 4515), 2639) \\ &= \mathsf{ggT}(\mathsf{ggT}(\mathsf{ggT}(7469, 2464), 4515), 2639) \end{aligned}$$

Mit der Bezeichnungsweise der *Vorlesung*, S. 9 unten:

2009/06/08 „1.“ angeschrieben, „2.“ Zeilenzahl und Ergebnis, „3.“ gekürzt angeschrieben

1.

	$r_n = q_n \cdot r_{n+1} + r_{n+2}$		
$(*_0)$	$r_0 = 7469 =$	$3 \cdot 2464 +$	77
$(*_1)$	$r_1 = 2464 = 32 \cdot$	$77 +$	0
		r_2	r_3

$\mathsf{ggT}(7469, 2464) = 77$

2.

	$r_n = q_n \cdot r_{n+1} + r_{n+2}$			
$(*_0)$	$r_0 = 4515 = 58 \cdot$	$77 +$	49
$(*_1)$	$r_1 = 77 = 1 \cdot$	$49 +$	28
$(*_2)$	$r_2 = 49 = 1 \cdot$	$28 +$	21
$(*_3)$	$r_3 = 28 = 1 \cdot$	$21 +$	7
$(*_4)$	$r_4 = 21 = 3 \cdot$	$7 +$	0
		r_5	r_6

$\mathsf{ggT}(4515, 77) = 7$

3.

	$r_n = q_n \cdot r_{n+1} + r_{n+2}$		
$(*_0)$	$r_0 = 2639 = 377 \cdot$	$7 +$	0
		r_1	r_2

$\mathsf{ggT}(2639, 7) = 7$

Damit

$$\begin{aligned} \mathsf{ggT}(7469, 2464, 4515, 2639) &= \mathsf{ggT}(\mathsf{ggT}(77, 4515), 2639) \\ &= \mathsf{ggT}(7, 2639) = 7 \end{aligned}$$

Blatt 5, Aufgabe 18c.

2009/06/08 erwähnt

		r_n	$=$	$q_n \cdot r_{n+1}$	$+$	r_{n+2}
$(*_0)$	$r_0 = 632$	$=$	$1\cdot$	547	$+$	85
$(*_1)$	$r_1 = 547$	$=$	$6\cdot$	85	$+$	37
$(*_2)$	$r_2 = 85$	$=$	$2\cdot$	37	$+$	11
$(*_3)$	$r_3 = 37$	$=$	$3\cdot$	11	$+$	4
$(*_4)$	$r_4 = 11$	$=$	$2\cdot$	4	$+$	3
$(*_5)$	$r_5 = 4$	$=$	$1\cdot$	3	$+$	1
$(*_6)$	$r_6 = 3$	$=$	$3\cdot$	1	$+$	0
				r_7		r_8

$\mathsf{ggT}(632, 547) = 1$

Bestimmung einer Linearkombination gemäß Vorlesung: „k“ wird durch $r_{k+1} = 0$ bestimmt, also $\boxed{k = 7}$. Um x, y mit

$$\mathsf{ggT}(632, 547) = 1 = x \cdot 632 + y \cdot 547$$

zu bestimmen, beginnt man bei $(*_{k-2}) = (*_5)$. Die Werte der r_n werden unterstrichen; sie werden nicht aufgelöst, sondern eliminiert:

$$\begin{aligned}
\underline{1} &\overset{(*_5)}{=} \underline{4} - \underline{3} \overset{(*_4)}{=} \underline{4} - (\underline{11} - 2\cdot\underline{4}) = 3\cdot\underline{4} - \underline{11}\\
&\overset{(*_3)}{=} 3\cdot(\underline{37} - 3\cdot\underline{11}) - \underline{11} = 3\cdot\underline{37} - 10\cdot\underline{11}\\
&\overset{(*_2)}{=} 3\cdot\underline{37} - 10\cdot(\underline{85} - 2\cdot\underline{37}) = 23\cdot\underline{37} - 10\cdot\underline{85}\\
&\overset{(*_1)}{=} 23\cdot(\underline{547} - 6\cdot\underline{85}) - 10\cdot\underline{85} = 23\cdot\underline{547} - 148\cdot\underline{85}\\
&\overset{(*_0)}{=} 23\cdot\underline{547} - 148\cdot(\underline{632} - \underline{547}) = \boxed{171}\cdot\underline{547} + \boxed{-148}\cdot\underline{632},
\end{aligned}$$

also $\boxed{x = -148, \quad y = 171}$

Durchsichtigere Alternative: In den Beweis der *Vorlesung* (Skriptum S. 10 oben) kann man Indizes für x und y einfügen, so dass $\boxed{r_k = x_n r_n + y_n r_{n+1}}$. Gesucht sind x_0, y_0. $x_{k-2} = 1$, $y_{k-2} = -q_{k-2}$,[36]

$$x_n = y_{n+1}, \qquad y_n = x_{n+1} - y_{n+1}q_n = y_{n+2} - y_{n+1}q.$$

Man kann sich $y_{k-1} = 1$ und $y_k = 0$ hinzudenken. Damit $y_{k-2} = y_5 = -q_5 = -1$, $y_4 = 1+q_4 = 3$, $y_3 = -1-3q_3 = -1-3\cdot 3 = -10$, $y_2 = 3+10q_2 = 23$,

$$\begin{aligned}
x &= x_0 = y_1 = -10 - 23q_1 = -10 - 138 = \boxed{-148}\\
y &= y_0 = 23 - 148q_0 = \boxed{171}
\end{aligned}$$

Bemerkung: Während man hier „von unten nach oben“ rechnet, kann man auch „von oben nach unten“ u_n, v_n mit $r_n = u_n r_0 + v_n r_1$ bestimmen und

[36] Im Skriptum steht (2009/06/06) auf S. 10 oben, 2.1, fälschlich q_{k-1} statt q_{k-2}. 2009/06/08 korrigiert.

erhält schließlich $r_k = u_k r_0 + v_k r_1$ aus $u_{n+2} = u_n - q_n u_{n+1}$ und $v_{n+2} = v_n - q_n v_{n+1}$, – von Hand mehr zu tun, aber einfacher zu programmieren, vgl. *Wikipedia: „Erweiterter euklidischer Algorithmus“.*[37]

Blatt 5, Aufgabe 18d. Für $n \in \mathbb{N}_1$ ist mit $\boxed{a_n := n! + 1}$ die Aussage $\boxed{\mathsf{ggT}(a_{n+1}, a_n) = 1}$ zu zeigen, d. h. a_{n+1}, a_n sind *teilerfremd.* 2009/06/08 angedeutet

$a_1 = 2$, $a_2 = 3$, $a_3 = 7$, die Behauptung ist deshalb klar für $n = 1$ und $n = 2$. In der Folge setzen wir $n > 2$ voraus. Wir verwenden den euklidischen Algorithmus mit $\boxed{r_0 := a_{n+1} = (n+1)! + 1}$ und $\boxed{r_1 := a_n = n! + 1}$.

Zur Erinnerung: $(*_n)$ ist $\boxed{r_n = q_n r_{n+1} + r_{n+2}}$ mit $\boxed{r_{n+2} < r_{n+1}}$.

$(n+1)! = n!(n+1) = n!n + n - n + n! = n(n! + 1) - n + n!$, daher

$$r_0 = nr_1 - n + n! + 1 = nr_1 - n + r_1$$

Wegen $n > 2$ ist $r_1 - n < r_1$, also gilt $(*_0)$ mit $q_0 = n$ und $\boxed{r_2 = r_1 - n}$.

Wegen $n > 2$ ist $2n \leq n!$, daher $n < 2n+1-n \leq n!+1-n = r_1-n = r_2$, daher gilt $r_1 = r_2 + n$ und ist gerade $(*_1)$ mit $q_1 = 1$ und $\boxed{r_3 = n}$.

Nun

$$r_2 = n! + 1 - n = (n-1)!n + 1 - n = ((n-1)! - 1)n + 1 = q_2 r_3 + 1$$

mit $q_2 = (n-1)! - 1$. Wegen $1 < n = r_3$ ist das $(*_2)$ mit $\boxed{r_4 = 1}$.

Nun terminiert der Algorithmus mit $(*_3)$ $r_3 = nr_4$, also ist gemäß Vorlesung $\boxed{\mathsf{ggT}(r_0, r_1) = r_k = r_4 = 1}$. □

Zusammenfassung des Rechenverlaufs:

		$r_n =$	$q_n \cdot$	$r_{n+1} +$	r_{n+2}
$(*_0)$	$r_0 = (n+1)! + 1 =$		$n \cdot$	$(n! + 1) + n! + 1 - n$	
$(*_1)$	$r_1 =$	$n! + 1 =$	$1 \cdot$	$(n! + 1 - n) +$	n
$(*_2)$	$r_2 =$	$n! + 1 - n = ((n-1)! - 1) \cdot$		$n +$	1
$(*_3)$	$r_3 =$	$n =$	$n \cdot$	$1 +$	0
				r_4	r_5
$\mathsf{ggT}((n+1)! + 1, n! + 1) = 1$					

Blatt 5, Aufgabe 19 = *Lemma 3.6f.* Skriptum, folgende Beweise wie dort, nur etwas ausführlicher.) niemand da 2009/06/15

$\boxed{\mathbb{P} := \{\, n \in \mathbb{N} : 2 \le n \;\;\&\;\; \neg(\exists m, k < n)(n = mk) \,\}}$ (Primzahlen)

Blatt 5, Aufgabe 19a = *Lemma 3.6 (a)* Skriptum.

Beh.: $\boxed{\forall p \in \mathbb{P} : T(p) \cap \mathbb{N} = \{1, p\}}$

Bew.: $a \mid p \overset{Skr.S.8(g)}{\Longrightarrow} \boxed{1 \le a \le p} \;\&\; \exists k \in \mathbb{N} : \boxed{ka = p}$.

Annahme 1: $\boxed{1 < a < p}$. Wäre auch noch (*Annahme 2*) $\boxed{k \ge p}$, so wäre $p = ak \ge 2k \overset{k \ge 2}{>} k \ge p$, d. h. $p > p$, Widerspruch aus Annahme 2, also $k < p$. Dann aber ist p Produkt zweier Zahlen $< p \implies p \notin \mathbb{P}$ – Widerspruch aus Annahme 1. Von $1 \le a \le p$ bleibt daher nur $a \in \{a, p\}$. □

Ü-Lemma 5.2*. $\boxed{\forall p \in \mathbb{P}: \quad p \notin T(a) \iff \mathsf{ggT}(a, p) = 1}$

Beweis: Zu *Ü-Lemma 5.2* wurde schon $p \mid a \implies \mathsf{ggT}(a, p) = p$ gezeigt.[38] [nachholen!] – Ist p dagegen *nicht* Teiler von a, so ist nach *Aufgabe 19a* 1 der einzige natürliche Teiler von p, der auch a teilt, d. h. $1 = \mathsf{ggT}(a, p)$. □

Bemerkung: $p \in \mathbb{P}$ ist als Voraussetzung wesentlich, denn z. B. $6 \notin T(8)$, aber $\mathsf{ggT}(6, 8) = 2$.

Blatt 5, Aufgabe 19b = *Lemma 3.6 (b)* Skriptum.

Beh.: $\boxed{\forall p \in \mathbb{P}: \quad p \mid a_0 \cdots a_k \implies (\exists i \le k)(p \mid a_i)}$[39]

Bew.: Umgekehrt $\forall i \le k : p \notin T(a_i) \overset{Ü.-L.5.2^*}{\Longrightarrow} \forall i \le k : \mathsf{ggT}(a_i, p) = 1$ $\overset{L.3.5b=A.17b}{\Longrightarrow} \mathsf{ggT}(a_0 \cdots a_n, p) = 1 \overset{Ü.-L.5.2^*}{\Longrightarrow} p \notin T(a_0 \cdots a_n)$. □

[37] `http://de.wikipedia.org/wiki/Erweiterter_euklischer_Algorithmus`
[38] vor *Aufgabe 17b.*
[39] Nun wird wieder ab 0 gezählt!

$$\boxed{v_p(a) := \max\{\, m \in \mathbb{N} : p^m \mid a \,\}} \quad (p \in \mathbb{P},\ a \in \mathbb{Z} \setminus \{0\})$$

Blatt 5, Aufgabe 19c = *Lemma 3.7* Skriptum.

Hilfssatz: $\boxed{a = p_0^{n_0} \cdots p_k^{n_k}}$ mit $\{p_0, \ldots, p_k\} \subseteq \mathbb{P}$ & $(i \neq j \Rightarrow p_i \neq p_j) \implies$

$$\forall p \in \mathbb{P}: \quad \boxed{p \mid a \iff (\exists i \leq k)\,(p = p_i \ \ \& \ \ n_i > 0)} \tag{1}$$

Beweis des Hilfssatzes: „$\Leftarrow$“ gilt wegen Skriptum S. 8 (a) (Transitivität der Relation *„ist Teiler von“*, $p \mid p_i^{n_i} \mid a \implies p \mid a$, darauf kommt es hier aber nicht an). – Weiter ganz wie im Skriptum:

$p \mid a \overset{L.3.6b}{\implies} (\exists i \leq k : p \mid p_i^{n_i})$.[40] $p \mid p_i^{n_i} \overset{S.8(g)}{\implies} 1 < p \leq p_i^{n_i} \implies \underline{n_i > 0}$.
$p \mid p_i^{n_i}$ & $n_i > 0 \overset{L.3.6b}{\implies} p \mid p_i \overset{L.3.6a}{\implies} \underline{p = p_i}$. Damit ist (1) bewiesen.

Behauptung der Aufgabe bzw. von 3.7: $\boxed{a = p_0^{n_0} \cdots p_k^{n_k}}$ mit $\{p_0, \ldots, p_k\} \subseteq \mathbb{P}$ & $(i \neq j \Rightarrow p_i \neq p_j) \implies$

$$\forall p \in \mathbb{P}: \quad \boxed{v_p(a) = \begin{cases} 0 & \text{für } p \notin \{p_0, \ldots, p_k\} \quad (*^-) \\ n_i & \text{für } p = p_i,\ i \leq k \quad (*^+) \end{cases}}$$

Die Umkehrung von (1) „$\Rightarrow$“ besagt $p \notin \{p_0, \ldots, p_k\} \implies p \notin T(a) \implies v_p(a) \overset{def}{=} \max\{\, m \in \mathbb{N} : p^m \mid a \,\} = 0$, also $(*^-)$.

Zu $(*^+)$: $\boxed{p = p_i}$, $i \leq k$, $\implies p_i^{n_i} \mid a$, d. h. $\underline{v_p(a) \geq n_i}$.

Angenommen, auch $p_i^{n_i+1} \mid a$, $a = p_i^{n_i+1} \cdot c$. O. E. (d. h. ggf. nach Umnumerierung) $i = 0$. Dann $p_0 \cdot p_1 \cdots p_k = p_0^{n_0+1} \cdot c$ und (etwa wegen Lemma 1.5: Eindeutigkeit der Division mit Rest) $p_1 \cdots p_k = p_0 \cdot c$. Demnach $p_0 \mid p_1 \cdots p_k$, und der „Hilfssatz“ (mit $p_1 \cdots p_k$ für „a“) ergibt $p_0 \in \{p_1, \ldots, p_k\}$ – im Widerspruch zur Voraussetzung, dass die p_j „paarweise verschieden“ sind. Daher $p_i^{n_i+1} \notin T(a)$ (wegen Transitivität überhaupt $p_i^m \notin T(a)$ für $m > n_i$), $v_p(a) \overset{def}{=} \max\{\, m \in \mathbb{N} : p^m \mid a \,\} = n_i$ gemäß $(*^+)$. □

[40] Tippfehler „k_i“ im Skriptum (2009/06/12).

Korollar: „Fundamentalsatz der Arithmetik“.[41] *Jede natürliche Zahl* $a > 1$ *lässt sich* eindeutig *(bis auf die Reihenfolge der Faktoren) als Produkt von Primzahlen darstellen* („Primfaktorzerlegung“), d. h.: es gibt Primzahlen $p_0, \dots, p_k$, so dass $a = p_0 \cdots p_k$; und gilt auch $a = q_0 \cdots q_l$ mit Primzahlen $q_0, \dots, q_l$, so sind $k = l$, $\{p_0, \dots, p_k\} = \{q_0, \dots, q_l\}$, und jede Primzahl $p_i = q_j$ kommt in $p_0 \cdots p_k$ ebenso häufig vor wie in $q_0 \cdots q_l$, nämlich $v_{p_i}(a) = v_{q_j}(a)$-mal. Außerdem kommen alle Primzahlen, die a teilen, sowohl in $p_0 \cdots p_k$ als auch in $q_0 \cdots q_l$ vor.

In der *kanonischen Primfaktorzerlegung* werden die Primzahlen, die n teilen, aufsteigend als $\bar{p}_0, \dots, \bar{p}_{\bar{k}}$ (paarweise verschieden) angeordnet, die Zerlegung ist dann $a = \bar{p}_0^{v_{\bar{p}_0}(a)} \cdots \bar{p}_{\bar{k}}^{v_{\bar{p}_{\bar{k}}}(a)}$.

Beweis: Dass es Primzahlen $p_0, \dots, p_k$ $(k \in \mathbb{N})$ mit $a = p_0 \cdots p_k$ *gibt*, ist im Skriptum *Satz 1.2.* [Die Numerierung kann so gewählt werden, dass $p_i \leq p_{i+1}$ (falls $k > i \geq 0$; aufsteigende Anordnung, *„kanonische Darstellung“.*)] Wir wählen p_i aus, die *„paarweise verschieden“* sind.

Es sei $P_a := \{p_0, \dots, p_k\}$ die *Menge* der (*„paarweise verschiedenen“*) Primzahlen, die in $p_0 \cdots p_k$ vorkommen, $|P_a| \leq k + 1$; im allgemeinen *nicht* $|P_a| = k + 1$, da manche Primzahlen $\in P_a$ in $p_0 \cdots p_k$ *mehrfach* vorkommen.

Es sei $\bar{p}_0 := \min P_a$; falls $j + 1 < |P_a|$, sei $\bar{p}_{j+1} := \min \{\, p \in P_a : p > \bar{p}_j \,\}$. Die $\bar{p}_j$, $j < |P_a|$, sind dann *paarweise verschieden*, tatsächlich $j < j' \Rightarrow \bar{p}_j < \bar{p}_{j'}$. $P_a = \{\, \bar{p}_j : j < |P_a| \,\}$.

Für $j < |P_a|$ sei $u_j := |\{\, i \in \{0, \dots, k\} : p_i = \bar{p}_j \,\}|$ – Häufigkeit/„Vielfachheit“ von $\bar{p}_j$ in $p_0 \cdots p_k$. Dann ist $\boxed{a = \bar{p}_0^{u_0} \cdots \bar{p}_{|P_a|-1}^{u_{|P_a|-1}}}$.[42] Aus Lemma 3.7 = Aufgabe 19c folgt $u_j = v_{\bar{p}_j}(a)$ für $j < |P_a|$, außerdem folgt $v_p(a) = 0$ für $p \notin P_a$, d. h. $\mathbb{P} \cap T(a) = P_a$. Beginnt man das vorige Verfahren mit einer *anderen* Darstellung $a = q_0 \cdots q_l$, so ist $\{q_0, \dots, q_l\} = P_a$ (dieselbe Menge), und man erhält dieselben Exponenten wie vorher. □

Bemerkung: Auch 1 hat eine solche Darstellung, z. B. $1 = 2^0 \cdot 3^0$; $v_p(1) = 0$.

[41] Steht nicht im Skriptum, ich schreibe es der Deutlichkeit halber auf.

[42] Noch genauer sollte man vielleicht eine Induktion nach k durchführen.

Blatt 5, Aufgabe 20 = *Lemma 3.8*, allerdings wurde im Skriptum eine weitere Aussage als „(a)“ eingefügt, so dass sich die alfabetische Zählung der weiteren Aussagen verschob.

Für den Rest des Übungsblatts seien $\boxed{a, b \in \mathbb{N}_1}$. M sei die Menge der Primzahlen, die a *oder* b teilen,[43] d. h. $\boxed{M := \mathbb{P} \cap (T(a) \cup T(b))}$. Falls $M = \emptyset$ $(a = 1 = b)$, $k := 0$, $p_0 := 2$. Andernfalls sei $k := |M| - 1$ und $p_0, \ldots, p_k$ eine Aufzählung von M durch paarweise verschiedene p_i, etwa wie oben $p_0 := \min M$ und $p_{i+1} := \min\{\, p \in M : p > p_i \,\}$; letztlich $\boxed{M = \{p_0, \ldots, p_k\}}$. Nach Lemma 3.7 bzw. der vorigen Aufgabe gelten $\boxed{(*_a)\ a = p_0^{n_0} \cdots p_k^{n_k}}$ mit $\boxed{n_i := v_{p_i}(a)}$ und $\boxed{(*_b)\ b = p_0^{m_0} \cdots p_k^{m_k}}$ mit $\boxed{m_i := v_{p_i}(b)}$. Es folgt noch:

$$p \in \mathbb{P} \setminus M \implies v_p(a) = 0 = v_p(b) \qquad (*_\infty)$$

Lemma 3.8 (a): *Beh.:* $a = b \iff \forall p \in \mathbb{P} : v_p(a) = v_p(b)$. – *Bew.:* „$\Rightarrow$“ ist eine logische Trivialität. – Gilt anders herum $\forall p \in \mathbb{P} : v_p(a) = v_p(b)$, so insbesondere $\forall i \in \{0, \ldots, k\} : n_i = v_{p_i}(a) = v_{p_i}(b) = m_i \implies a = b$. □

Blatt 5, Aufgabe 20a = Lemma 3.8 (b). Aus $(*_a)$ und $(*_b)$ folgt $a \cdot b = p_0^{n_0+m_0} \cdots p_k^{n_k+m_k}$. Aus der Lemma 3.7 (c) (für $a \cdot b$) folgt $v_p(a \cdot b) = n_i + m_i$ für $p = p_i \in M$. – Eine Primzahl, die $a \cdot b$ teilt, teilt nach Lemma 3.6 (b) a oder b, ist also Element von M.[44] Für $p \in \mathbb{P} \setminus M$ ist also $p \notin T(a \cdot b) \implies v_p(a \cdot b) = 0 \overset{(*_\infty)}{=} v_p(a) + v_p(b)$ auch für $p \in \mathbb{P} \setminus M$. □

Blatt 5, Aufgabe 20b = Lemma 3.8 (c). „$\Rightarrow$“: $xa = b \implies v_p(a) \leq v_p(x) + v_p(a) \overset{L.3.8b=A.20a}{=} v_p(b)$. – „$\Leftarrow$“: $\forall i \in \{0, \ldots, k\} : n_i \leq m_i \implies c := p_0^{m_0-n_0} \cdots p_k^{m_k-n_k} \in \mathbb{N} \implies a \cdot c = p_0^{m_0} \cdots p_k^{m_k} = b$, also $a \mid b$. □

Blatt 5, Aufgabe 20c = Lemma 3.8 (d). $d \in T(a, b) \overset{A.20b+(*_\infty)}{\iff} \forall i \in \{0, \ldots, k\} : v_{p_i}(d) \leq \min(n_i, m_i) \overset{L.3.7}{\iff} \forall i \in \{0, \ldots, k\} : v_{p_i}(d) \leq v_{p_i}(c) \overset{A.20b+(*_\infty)}{\iff} d \in T(c)$ mit $c := p_0^{\min(n_0,m_0)} \cdots p_k^{\min(n_k,m_k)}$. Mit Lemma 3.3 folgt $c = \mathsf{ggT}(a, b)$, mit $(*_\infty)$ $\forall p \in \mathbb{P} : v_p(c) = \min(v_p(a), v_p(b))$. □

[43] Ansatz etwas anders als im Skriptum, ansonsten handelt es sich nur um Ausschmückungen und minimale Korrekturen der Beweise des Skriptums.

[44] Diese Überlegung scheint im Skriptum (2009/06/13) zu fehlen.

Prof. Buchholz' loes6.pdf etwas verändert dargestellt (unterschiedliche Betonungen): nicht vorgetragen

Blatt 6, Aufgabe 21a. $\underline{\mathsf{ggT}(a_1,\ldots,a_n) = \mathsf{ggT}(a_1,s_2,\ldots,s_n)}$ folgt mit der Bemerkung im Skript auf S. 8 unten aus

$$\begin{aligned} T(a_1,\ldots,a_n) &= T(a_1,a_2)\cap\ldots\cap T(a_1,a_n) \\ &\overset{L.3.4}{=} T(a_1,s_2)\cap\ldots\cap T(a_1,s_n) = T(a_1,s_2,\ldots,s_n) \quad \square \end{aligned}$$

Blatt 6, Aufgabe 21b. $\underline{\mathsf{ggT}(ac,bc) = \mathsf{ggT}(a,b)\cdot c}$ folgt mit *Lemma 3.8 (a)* aus $(\forall p \in \mathbb{P})$

$$\begin{aligned} v_p\big(\mathsf{ggT}(ac,bc)\big) &\overset{L.3.8b,d}{=} \min\big(v_p(a)+v_p(c), v_p(b)+v_p(c)\big) \\ &\overset{2Fälle}{=} \min\big(v_p(a),v_p(b)\big) + v_p(c) \\ &\overset{L.3.8b,d}{=} v_p\big(\mathsf{ggT}(a,b)\cdot c\big) \quad \square \end{aligned}$$

Blatt 6, Aufgabe 21c. $\underline{c \mid ab} \overset{L.3.8b,c}{\Longrightarrow} \forall p\in\mathbb{P}: \boxed{(\dagger)\ \ v_p(c) \le v_p(a)+v_p(b)}$.
Wegen *Lemma 3.8* (b), (d) (*Aufgabe 20b,c*) gilt

$$\boxed{u_p := v_p\big(\mathsf{ggT}(a,c)\cdot\mathsf{ggT}(b,c)\big) = \min\big(v_p(a),v_p(c)\big) + \min\big(v_p(b),v_p(c)\big)}$$

$\underline{\mathsf{ggT}(a,b)=1} \implies \min\big(v_p(a),v_p(b)\big) \overset{L.3.8d}{=} v_p(\mathsf{ggT}(a,b)) = v_p(1) = 0 \implies \boxed{v_p(a)=0 \ \text{ oder } \ v_p(b)=0}$. Falls $\boxed{v_p(a)=0}$, so folgt aus (†) $v_p(c)\le v_p(b)$, also $\underline{u_p} = 0+\min\big(v_p(b),v_p(c)\big) \underline{= v_p(c)}$. Falls $\boxed{v_p(b)=0}$, so folgt aus (†) $v_p(c)\le v_p(a)$, also $\underline{u_p} = \min\big(v_p(a),v_p(c)\big)+0 \underline{= v_p(c)}$ wie zuvor. Mit *Lemma 3.8* (a) folgt $\underline{\mathsf{ggT}(a,c)\cdot\mathsf{ggT}(b,c)=c}$. $\square$

Blatt 6, Aufgabe 23b: An der Tafel standen ein paar Striche falsch! Also noch einmal: 2009/06/29 wg. Korrekturbericht zu P5b; TODO „$\mathbb{Q}$“ + P5b

Zu zeigen: $x' \sim x \prec y \sim y' \implies x' \prec y' \quad (x, x', y, y' \in M)$.

Es seien $x = (a, n)$, $x' = (a', n')$, $y = (b, m)$, $y' = (b', m')$. Damit $an' = a'n$ & $am < bn$ & $bm' = b'm$; z. z.: $a'm' < b'n'$. Dies folgt wegen $nm > 0$ aus (abwechselnd umordnen und Voraussetzung einsetzen) $(a'm')(nm) = (a'n)(mm') \overset{s.o.}{=} (an')(mm') = (am)(mm') \overset{s.o.}{<} (bn)(mm') = (bm')(nm) \overset{s.o.}{=} (bm)(nm') = (bm')(nm) \overset{s.o.}{=} (b'm)(nm)$. □

Die Frage, ob man hier (sinngemäß ungefähr:) nm trickhalber herbeigezaubert hat, hätte ich eigentlich bejahen sollen.

Blatt 8, Aufgabe P4a: *Hinweis:* In Prof. Buchholz' loes8.pdf muss es „4.6a“ statt „4.5a“ heißen. D. h. mit $a^k \equiv_m 1$ ist a^{k-1} ein a' so dass $aa' \equiv_m 1$, $\mathsf{ggT}(a, m) = 1$ folgt daher unmittelbar aus Lemma 4.6 (b) des Vorlesungsskriptums. – *Alternativ* gibt loes8.pdf als „zu-Fuß“-Überlegung an: $a^k \equiv_m 1$ bedeutet, dass es ein x mit $a^k - 1 = xm$ gibt, damit $1 = a^{k-1} - xm$, also (da 1 jede ganze Zahl teilt) $1 \in T(a, m) \cap (\mathbb{Z}a + \mathbb{Z}m)$ und nach Lemma 3.3 $1 = \mathsf{ggT}(a, m)$ (vgl. zweite Bemerkung auf S. 10 des Skriptums). □ nicht vorgetragen

Blatt 8, Aufgabe P4b: *Hinweis:* Die Aufgabenstellung wurde zwischenzeitlich abgeändert. Man muss zusätzlich $n > 3$ voraussetzen. Ausführlicher: 2009/06/29 nur Notwendigkeit des Zusatzes angedeutet

Für $n \in \mathbb{N}$ sei $\mathcal{A}(n)$: $\boxed{n + 1 \notin \mathbb{P} \implies n + 1 \mid n!}$

(Jawohl, $a \equiv 0 \bmod b$ ist nur eine umständliche Ausdrucksweise für $b \mid a$.)

$\mathcal{A}(0)$ trifft wegen $0! = 1 \mid 1 = 1!$ zu. Da 2 und 3 keine Primzahlen sind, sind $\mathcal{A}(1)$ und $\mathcal{A}(2)$ trivialerweise wahr. 4 ist *keine* Primzahl und teilt $3! = 6$ *nicht*, daher ist $\mathcal{A}(3)$ *falsch!*

Erläuterung des Beweises in loes8.pdf: Es sei $n + 1 \notin \mathbb{P}$. Es wird gezeigt, dass $\{1, \ldots, n\}$ Elemente $\boxed{m_1 \neq m_2}$ hat, die $m_1 \cdot m_2 = n + 1$ erfüllen. Ist m_3 dann das Produkt der Elemente von $\{1, \ldots, n\} \setminus \{m_1, m_2\}$, so gilt $(n + 1) \cdot m_3 = m_1 m_2 m_3 = n!$, also $n + 1 \mid n!$.

Wegen $n + 1 \notin \mathbb{P}$ gibt es $k, m < n + 1$ mit $n + 1 = k \cdot m$. *Falls* $k \neq m$, so hat man bereits $m_1 = k$ und $m_2 = m$ wie oben. *Andernfalls* $n + 1 = k^2$ und $\boxed{k > 2}$, weil sonst $n = k^2 - 1 \leq 3$ wäre. Daher $k < 2k < k^2 = n + 1$, also $k < 2k \leq n$, und man hat $m_1 = k$ und $m_2 = 2k$ wie oben. □

Blatt 8, Aufgabe P6: Die Aufgabe verlangte keine Begründungen!

(1) Richtig, Beweis: [Verbesserung gegenüber Übung 2009/06/29:] Aus L. 2.5b folgt für $f : X \to X$: f injektiv $\iff$ f surjektiv. □

(2) Falsch, Gegenbeispiel: $f : \{0, 1\} \to \{0\}$ surjektiv, nicht injektiv.

(3) Richtig, Beweis: $d \in \mathbb{Z}a + \mathbb{Z}b$ bedeutet Existenz von $x, y \in \mathbb{Z}$ mit $d = xa + yb$, nach (b) von S. 8 bzw. Aufg. 16 daher $T(a, b) \subseteq T(d)$, insbesondere $\mathsf{ggT}(a, b) \mid d$. □

(4) Falsch: Nach Korollar 1 ist die Euler-Funktion φ zwar „multiplikativ“, $\varphi(m_1 \cdot m_2) = \varphi(m_1) \cdot \varphi(m_2)$ gilt aber nur unter der Voraussetzung $\mathsf{ggT}(m_1, m_2) = 1$. Für z. B. $m_1 = 3 = m_2$ ist dagegen $\varphi(m_1) = \varphi(m_2) = |\{1, 2\}| = 2$, also $\varphi(m_1 \cdot m_2) = \varphi(9) = |\{1, 2, 4, 5, 7, 8\}| = 6 \neq 4 = \varphi(m_1) \cdot \varphi(m_2)$.

(5) Falsch, Gegenbeispiel: $\{1, 5\}$ ist primes Restsystem modulo 6 (nur $[1]_6$ und $[5]_6$ sind prim modulo 6, und sie sind verschieden), nicht aber $\{2\cdot 1, 2\cdot 5\}$, da $[2]_6$ nicht prim modulo 6 ist ($\mathsf{ggT}(2, 6) = 2$).

(6) Richtig, folgt aus der Betrachtung zu (5) wegen $11 \equiv_6 5$ und $55 \equiv_6 = 1$.

„Ausflug“ hierzu: $11 \in [-1]_6$ ist mir „sonnenklar“, wenn ich an $11 = 12 - 1$ denke – aber wie komme ich dazu? [Konnte ich 2009/06/29 nicht erklären] Vielleicht so: $x + y = am \implies m \mid x - (-y) \implies x \in [-y]_m$; im Beispiel $a = 2$, $m = 6$, $x = 11$, $y = 1$.

Blatt 9, Aufgabe 29 Wir benennen die Knoten jeweils oben beginnend im Uhrzeigersinn als A_1, A_2 A_3 A_4 A_5. Falls ein Isomorphismus angegeben wird, geht man für den Beweis die 5 Kanten von G bzw. von $\overline{G}$ durch.

2009/07/06 zunächst Aufgabe 31 vorgezogen

1. Ist G der *links* dargestellte Graph, so erhält man einen Isomorphismus auf $\overline{G}$ durch $A_i \mapsto A_{\mathbf{r}_5(2i-1)}$ (vgl. Vorlesungsskriptum S. 13 bzw. Aufgabe 22c; Permutationszyklen-Schreibweise: (1 3 5 2 4)).

2. Ist $G = (V, E)$ der in der *Mitte* dargestellte Graph, so ist G *nicht* zu $\overline{G}$ isomorph.

Annahme: $f : V \mapsto V$ wäre Isomorphismus. In G ist A_1 der einzige Knoten mit Grad 1, in $\overline{G}$ ist A_4 der einzige Knoten mit Grad 1. Wegen *Lemma 5.1* des Vorlesungsskripts muss daher $\boxed{f(A_1) = A_4}$ gelten. Wegen Isomorphie muss $\{f(A_1), f(A_5)\}$ Kante von $\overline{G}$ sein, es kommt nur $\{A_4, A_1\}$ in Frage, also $\boxed{f(A_5) = A_1}$. A_5 hat in G Grad 2, $f(A_5) = A_1$ hat in $\overline{G}$ dagegen Grad 3 – *Widerspruch* mit Lemma 5.1, f ist *doch* kein Isomorphismus, es gibt keinen.

3. Ist G der *rechts* dargestellte Graph, so gibt es *zwei* Isomorphismen von G auf $\overline{G}$, weil beide Graphen einen Isomorphismus auf sich selbst haben, der A_1 mit A_2 und A_3 mit A_5 vertauscht. Beide bilden A_4 auf A_4 ab. Einer bildet weiter $A_1 \mapsto A_3 \mapsto A_2 \mapsto A_5 \mapsto A_1$ ab, als Permutationszykel (1 3 2 5). Der andere entspricht dem Permutationszykel (1 5 2 3).

zuerst falsche Abbildung angegeben

Ü-Lemma 9.1 (eigene Ergänzung zur Vorbereitung von *Aufgabe 30a*): Es seien $G = (V, E)$, $G' = (V', E')$ $\boxed{\textit{isomorphe}}$ Graphen mit endlicher Eckenzahl. Dann $|V| = |V'|$ und $\boxed{|E| = |E'|}$.

2009/07/06 ausgelassen

Drei Beweise:

Erster Beweis: Ist f Isomorphismus von G auf G', so folgt aus Lemmata 5.1 und 5.2 des Skriptums

Erst hinterher entdeckt!

$$2 \cdot |E| \overset{5.2}{=} \sum_{A \in V} \text{grad}_G(A) \overset{5.1}{=} \sum_{A \in V} \text{grad}_{G'}(f(A)) \overset{f \text{ bij.}}{=} \sum_{A' \in V'} \text{grad}_{G'}(A') \overset{5.2}{=} 2 \cdot |E'|$$

□

Zweiter Beweis: Sei $f : V \to V'$ Isomorphismus von (V, E) auf (V', E'). Nach Definition von „Isomorphismus“ auf S. 18 (einschließlich der Bemerkung [„d.h. ...“]) wird dann durch $f^*(A, B) := \{f(A), f(B)\}$ eine surjektive Abbildung f^* von E auf E' definiert. f^* ist auch injektiv, denn aus $f(A_0), f(A_1) = f(A'_0), f(A'_1)$ folgt $f(A_i) = f(A'_0)$ oder $f(A_i) = f(A'_1)$ und somit (da f injektiv) $A_1, A_2 \in A'_0, A'_1$; ebenso folgt $A'_0, A'_1 \in A_0, A_1$; insgesamt also $A_0, A_1 = A'_0, A'_1$. □

Von Prof. Buchholz 2009/07/10 mitgeteilt

Dritter Beweis (aus Definition von Isomorphismus „ganz zu Fuß“): Zunächst kann jeder Abbildung $h : V \to V'$ eine durch

$$h^*(\{A, B\}) := \{h(A), h(B)\}$$

definierte Abbildung $h^* : \mathcal{P}_2(V) \to \mathcal{P}_1(V') \cup \mathcal{P}_2(V')$ zugeordnet werden. Ist $\{A, B\} \in E$ und $h(A) = h(B)$ (h *nicht* injektiv), so ist $h^*(\{A, B\}) \in \mathcal{P}_1(V')$, auf keinen Fall eine Kante von G'.

2009/07/06 im Zusammenhang mit Aufgabe 29

Wegen Isomorphie existiert hier jedoch eine *Bijektion* $f : V \to V'$, so dass

$$\forall X \in \mathcal{P}_2(V)) : \big(X \in E \iff f^*(X) \in E'\big) \qquad (*)$$

f^* bildet also schon einmal Kanten auf Kanten ab, sogar $\boxed{\textit{injektiv}}$, denn sind $\{A, B\}$ und $\{A', B'\}$ *verschiedene* Kanten von G, so $|\{A, A', B, B'\}| \geq 3$ und wegen wegen Injektivität von f auch $|\{f(A), f(A'), f(B), f(B')\}| \geq 3$, was $f^*(\{A, B\}) = f^*(\{A', B'\})$ ausschließt.

Ist zudem (A', B') irgendeine Kante von G', so gibt es wegen der *Surjektivität* von f $A, B \in V$ mit $f(A) = A'$ und $f(B) = B'$, also $f^*(\{A, B\}) = \{A', B'\}$. Wegen $(*)$ ist dann auch (A, B) eine *Kante* von G. Zu jeder Kante X' von G' *gibt* es also eine Kante X von G, so dass $f^*(X) = X'$.

Damit ist die *Einschränkung* von f^* auf E, also die durch $f^{**}(X) := f^*(X)$ für $X \in E$ definierte Abbildung f^{**} eine *Bijektion* von E auf E'. Nach Lemma 2.4 des Vorlesungsskriptums daher $|E| = |E'|$ (und $|V| = |V'|$ sowieso, weil f bijektiv). □

Blatt 9, Aufgabe 30a. (wie Prof. Buchholz' loes9.pdf) 2009/07/06 ausgelassen
Es seien $G = (V, E)$ selbstkomplementär und V endlich mit $n := |V| \geq 1$. Nach obigem Lemma $|E| = |\mathcal{P}_2(V) \setminus E| = \binom{n}{2} - |E|$, $4 \cdot |E| = n\,(n-1)$, also $4 \mid n\,(n-1)$. Ist n ungerade, so $\mathsf{ggT}(4, n) = 1$ und nach *Lemma 3.5* (a) (= *Aufgabe 17*) $4 \mid n-1$, also $n \equiv_4 1$. Andernfalls analog $4 \mid n$, d. h. $n \equiv_4 0$. □

Blatt 9, Aufgabe 30b. (etwas ausführlicher als loes9.pdf:) 2009/07/06 ausgelassen
Erneut sei $G = (V, E)$ selbstkomplementär, diesmal aber $n = |V| \geq 2$.

Annahme: Für ein $A \in V$ wäre $\mathrm{grad}_G(A) = 0$. Dann $\forall B \in V \setminus \{A\}$: $\{A, B\} \notin E$, d. h. $\{A, B\} \in \mathcal{P}_2(V) \setminus E$. Damit nicht nur $\forall B \in V \setminus \{A\}$: $\mathrm{grad}_{\overline{G}}(B) \geq 1$, sondern auch $\mathrm{grad}_{\overline{G}}(A) = n - 1 \overset{n \geq 2}{\geq} 1$. Für jede Abbildung $f : V \to V$ gilt daher $\mathrm{grad}_{\overline{G}}(f(A)) \geq 1 > 0 = \mathrm{grad}_G(A)$, f kann wegen *Lemma 5.1* also kein Isomorphismus $G \to \overline{G}$ sein – *Widerspruch!* – also doch $\forall A \in E : \mathrm{grad}_G(A) \geq 1$. □

Blatt 9, Aufgabe 31 – Vorbemerkungen 1: Zerlegungen. Unter einer *Zerlegung* oder *Partition* einer Menge M versteht man eine Menge $\mathcal{M}$ von nicht-leeren Teilmengen von M, die paarweise disjunkt sind und sich zu ganz M vereinigen. Im (zweit?-)einfachsten Fall ist $\mathcal{M} = \{M_1, M_2\}$, $(M_1 \neq M_2)$ $M = M_1 \dot\cup M_2$ – Schreibweise für $M = M_1 \cup M_2$ & $M_1 \cap M_2 = \emptyset$. Ganz allgemein schreibt man $M = \dot\bigcup \mathcal{M}$ (gleich wieder vergessen!). 2009/07/06 hiermit begonnen

Ist M *endlich* und $\{M_1, M_2\}$ $(M_1 \neq M_2)$ eine Zerlegung von M, so gilt nach *Lemma 2.2* $|M| = |M_1| + |M_2|$. Durch vollständige Induktion folgt

$$\boxed{|M| = \sum_{i=1}^{k} |M_i|}, \text{ wenn } \{M_1, \ldots, M_k\} \text{ eine Zerlegung von } M \text{ ist.}$$

Lemma 4.1 besagt, dass *Äquivalenzklassen* bezüglich einer Relation R auf M eine *Zerlegung* von M bilden. Nach *Aufgabe 22* (a) induziert eine Zerlegung $\mathcal{M}$ von M umgekehrt eine Äquivalenzrelation auf M, bezüglich der die Elemente von $\mathcal{M}$ die Äquivalenzklassen sind.

Blatt 9, Aufgabe 31 – Vorbemerkungen 2: Zusammenhangskomponenten. *Drei Zugänge:*

1. Die *„verbindbar“*-Relation der Vorlesung in Bezug auf Graphen bildet eine *Äquivalenzrelation* auf der Knotenmenge, wenn man dazusagt, dass jeder Knoten mit sich selbst verbindbar genannt werden soll – siehe Nachtrag unten! So ist die Relation auch *reflexiv*, während sie andernfalls nur *symmetrisch* und *transitiv* wäre. – Diese Äquivalenzklassen werden in der Vorlesung als *Zusammenhangskomponenten* oder *Komponenten* bezeichnet.

$\Delta_M := \{\,(x,x) : x \in M\,\}$ ist die *„Diagonale“* von M, die Identitätsrelation eingeschränkt auf M. Ist R eine symmetrische und transitive Relation auf M, so ist $R \cup \Delta_M$ eine Äquivalenzrelation.

Tatsächlich aber ist Skriptum S. 21 oben so zu verstehen, dass $\{A_i, A_{i+1}\}$ *für* $0 \le i \le n-1$ *(äquivalent* $i \in I_n$ *gemäß Skriptum S. 4) auch im Falle* $n = 0$ *hinreichend und notwendig für Vorliegen eines Kantenzugs* $(A_0, \ldots, A_n)$ *(*$n \in \mathbb{N}$*!),* (A) *also für jeden Knoten* A *trivialerweise Kantenzug ist!* von Prof. Buchholz 2009/07/10 mitgeteilt

2. Eine Komponente U eines Graphen (V, E) ist gleichzeitig eine *„maximal zusammenhängende“* Teilmenge von V, d. h. jede *echte Obermenge* W von U – $U \subset W \subseteq V$ – ist nicht mehr zusammenhängend, oder einfach: kein Knoten aus $V \setminus U$ ist mit einem Knoten aus U über Kanten aus E verbindbar. 2009/07/06 nur angedeutet

3. Ist $G = (V, E)$ ein Graph, so sei für $A \in V$: $\mathcal{C}_0(A) := \{A\}$ und für $i \in \mathbb{N}$: $\mathcal{C}_{i+1}(A) := \mathcal{C}_i(A) \cup \{\,B \in V : (\exists C \in \mathcal{C}_i(A))(\{B, C\} \in E)\,\}$. Dann ist $\mathcal{C}(A) := \bigcup_{i\in\mathbb{N}} \mathcal{C}_i(A)$ die Komponente „von A“, d. h. die Zusammenhangskomponente von G, die A enthält. Ist V endlich, so ist „spätestens“ $\mathcal{C}(A) = \bigcup_{i=0}^{|V|-1} \mathcal{C}_i(A)$. (Hierbei kommt *„verbindbar“* gar nicht vor!) $\{\,\mathcal{C}(B) : B \in V\,\}$ ist die Menge der Komponenten von G, wobei natürlich $\mathcal{C}(B)$ und $\mathcal{C}(B')$ zusammenfallen, wenn B mit B' verbindbar ist. 2009/07/06 grob angedeutet

Blatt 9, Aufgabe 31 – Voraussetzungen: Es sei $G = (V, E)$ ein Graph mit endlicher Eckenzahl $n = |V|$, $\overline{G} = (V, \overline{E})$ mit $\overline{E} = \mathcal{P}_2(V) \setminus E$ der komplementäre Graph. 2009/07/06 Fortsetzung

Blatt 9, Aufgabe 31a. *Behauptung:* G oder $\overline{G}$ ist zusammenhängend. *Beweis:* Gleichbedeutend ist:

$$G \textit{ nicht} \text{ zusammenhängend} \implies \overline{G} \text{ zusammenhängend}$$

Sei also G *nicht* zusammenhängend. Es geht etwas anders als in loes9.pdf weiter. Weiter seien $A, B \in V$, $A \neq B$; z. z.: A, B sind in $\overline{G}$ verbindbar. *Fallunterscheidung:*

1. Sind A, B *nicht* in G verbindbar, so insbesondere *nicht* $\{A, B\} \in E$, das bedeutet aber $\{A, B\} \in \overline{E}$, und A, B sind in $\overline{G}$ („direkt“) verbindbar (*Kantenzug* (A, B)).

2. Seien A, B nun *doch* in G verbindbar. Da G nicht zusammenhängend ist, gibt es ein $C \in V$, das in G *nicht* mit A verbindbar ist – wären in G alle D, D' mit A verbindbar, so wären D, D' „via A“ [*Transitivät!* + Symmetrie] verbindbar, im Gegensatz zur Annahme, dass G *nicht* zusammenhängend ist. C ist dann ebensowenig mit B verbindbar. Insbesondere sind weder $\{A, C\}$ noch $\{B, C\}$ Kanten in E. Dann sind aber $\{A, C\}$ und $\{B, C\}$ Kanten in $\overline{E}$, und (A, C, B) ist ein *Kantenzug* in $\overline{G}$, der A und B verbindet. □

Alternative zu 2.: A, B gehören zur selben Komponente V_1 in G, dann sind A, B in $\overline{G}$ über ein $C \in G \setminus V_1$ verbindbar.

Blatt 9, Aufgabe 31b. Etwas anders als loes9.pdf: Wir zeigen die Umkehrung: Ist G *nicht* zusammenhängend, so gibt es A mit $\text{grad}_G(A) < \frac{n-1}{2}$. – Sei G nicht zusammenhängend. G hat dann mindestens *zwei* Komponenten. Wir wählen eine Komponente V_1 mit *minimaler* Mächtigkeit $|V_1|$. Die übrigen Komponenten seien $V_2, \ldots, V_k$, nach Wahl von V_1 $|V_i| \leq |V_1|$, nach der Summenformel für Zerlegungen (oben) daher $n = \sum_{i=1}^{k} |V_i| \geq k \cdot |V_1| \geq 2|V_1|$. Ist $A \in V_1$, so gibt es Kanten $\{A, B\} \in E$ allenfalls mit Knoten $B \in V_1 \setminus \{A\}$, also $\text{grad}_G(A) \leq |V_1| - 1 \leq \frac{n}{2} - 1 < \frac{n-1}{2}$ – und $\exists A \in V_1$! □ Fehler und Holprigkeiten des Vortrags behoben