Diskrete Mathematik

Anna-Lena Rädler
Christina Kohl
Georg Moser
Christian Sternagel
Vincent van Oostrom

Sommersemester 2018

Zusammenfassung der letzten LVA

Definition

- Für eine Folge $f: \mathbb{N} \to \mathbb{R}$ heißt die Potenzreihe $F(x) := \sum_{n=0}^{\infty} f(n) \cdot x^n$ die erzeugende Funktion von f
- Die Methode der erzeugenden Funktionen versucht geschlossene Formeln für $f(n)$ zu finden, indem nach $F(x)$ gelöst wird

Satz (Master-Theorem)

Sei $T(n)$ eine wachsende Funktion, die folgende Rekurrenzgleichungen erfüllt

$$T(n) = \begin{cases} c & n = 1 \\ aT(\frac{n}{b}) + f(n) & n = b^k,\ k = 1, 2, \ldots \end{cases}$$

wobei $a \geqslant 1$, $b > 1$, $c > 0$. Wenn $f \in \Theta(n^s)$, wobei $s \geqslant 0$, dann gilt: (i) $T(n) \in \Theta(n^{\log_b a})$, wenn $a > b^s$; (ii) $T(n) \in \Theta(n^s \log n)$, wenn $a = b^s$; (iii) $T(n) \in \Theta(n^s)$, wenn $a < b^s$.

Zusammenfassung der letzten LVA

Definition

- Für eine Folge $f: \mathbb{N} \to \mathbb{R}$ heißt die Potenzreihe $F(x) := \sum_{n=0}^{\infty} f(n) \cdot x^n$ die erzeugende Funktion von f
- Die Methode der erzeugenden Funktionen versucht geschlossene Formeln für $f(n)$ zu finden, indem nach $F(x)$ gelöst wird

Satz (Master-Theorem)

Sei $T(n)$ eine wachsende Funktion, die folgende Rekurrenzgleichungen erfüllt

$$T(n) = \begin{cases} c & n = 1 \\ aT(\frac{n}{b}) + f(n) & n = b^k,\ k = 1, 2, \ldots \end{cases}$$

wobei $a \geqslant 1$, $b > 1$, $c > 0$. Wenn $f \in \Theta(n^s)$, wobei $s \geqslant 0$, dann gilt: (i) $T(n) \in \Theta(n^{\log_b a})$, wenn $a > b^s$; (ii) $T(n) \in \Theta(n^s \log n)$, wenn $a = b^s$; (iii) $T(n) \in \Theta(n^s)$, wenn $a < b^s$.

Inhalte der Lehrveranstaltung

Beweismethoden

deduktive Beweise, Beweise von Mengeninklusionen, Kontraposition, Widerspruchsbeweise, vollständige Induktion, wohlfundierte Induktion, strukturelle Induktion, Gegenbeispiele

Relationen, Ordnungen und Funktionen

Äquivalenzrelationen, partielle Ordnungen, Wörter, asymptotisches Wachstum von Funktionen

Graphentheorie

gerichtete Graphen, ungerichtete Graphen

Zähl- und Zahlentheorie

Aufzählen und Nummerien von Objekten, Abzählbarkeit, Wahrscheinlichkeitstheorie, Lösen von Rekursionsformeln, Rechnen mit ganzen Zahlen, euklidischer Algorithmus, Primzahlen, Restklassen

Inhalte der Lehrveranstaltung

Beweismethoden

deduktive Beweise, Beweise von Mengeninklusionen, Kontraposition, Widerspruchsbeweise, vollständige Induktion, wohlfundierte Induktion, strukturelle Induktion, Gegenbeispiele

Relationen, Ordnungen und Funktionen

Äquivalenzrelationen, partielle Ordnungen, Wörter, asymptotisches Wachstum von Funktionen

Graphentheorie

gerichtete Graphen, ungerichtete Graphen

Zähl- und Zahlentheorie

Aufzählen und Nummerien von Objekten, Abzählbarkeit, Wahrscheinlichkeitstheorie, Lösen von Rekursionsformeln, Rechnen mit ganzen Zahlen, euklidischer Algorithmus, Primzahlen, Restklassen

Rechnen mit ganzen Zahlen

Definition (Ziffernoperationen)

Sei b eine natürliche Zahl $\geqslant 2$. Für Zahlen $u, v \in \{0, 1, \ldots, b-1\}$ und $w \in \{0, 1\}$ heißt $C(u, v, w) := (u + v + w) \operatorname{div} b$ der Übertrag (carry) modulo b und $S(u, v, w) := (u + v + w) \bmod b$ die Summe modulo b.

Lemma

Es gilt $u + v + w < 2b$ und somit $C(u, v, w) \in \{0, 1\}$ also kann Übertrag und Summe wie folgt definiert werden

$$C(u, v, w) := \begin{cases} 0 & \text{falls } u + v + w < b \\ 1 & \text{sonst} \end{cases}$$

$$S(u, v, w) := \begin{cases} u + v + w & \text{falls } u + v + w < b \\ u + v + w - b & \text{sonst} \end{cases}$$

Satz (Addition natürlicher Zahlen in Zifferndarstellung)

Es seien x und y natürliche Zahlen mit Ziffern $x_k x_{k-1} \cdots x_0$ bzw. $y_\ell y_{\ell-1} \cdots y_0$ zur Basis $b \geqslant 2$. ObdA nehmen wir $k \geqslant \ell$ an und setzen

$$y_{\ell+1} := 0\,,\ y_{\ell+2} := 0\,, \ldots,\ y_k := 0$$

Dann können die Ziffern der Summe $x + y =: z$ durch den folgenden Algorithmus mit $O(k)$ Ziffernoperationen berechnet werden:

Setze $c_0 = 0$.

Für i *von* 0 *bis* k *wiederhole:*

Setze $z_i = S(x_i, y_i, c_i)$.

Setze $c_{i+1} = C(x_i, y_i, c_i)$.

Falls $c_{k+1} \neq 0$, *setze* $z_{k+1} = c_{k+1}$.

Satz (schnelles Potenzieren)

Sei x eine ganze Zahl oder allgemeiner ein Element eines Ringes, und sei e eine positive ganze Zahl mit Binärziffern

$$e_t e_{t-1} \cdots e_0$$

wobei $e_t = 1$. Dann kann die Potenz $y := x^e$ durch t-faches Quadrieren (und eventuell Multiplizieren) berechnet werden:

Setze $y = x$.

Für i von $t-1$ hinab bis 0 wiederhole:

Setze $y = y^2$.

Falls $e_i = 1$, setze $y = y * x$.

Beweis.

- Induktion über t; für $t = 0$ gilt $e = 1$ und laut Algorithmus $x^1 = x$
- Für $t > 0$ schreiben wir

$$e = \sum_{i=0}^{t} e_i 2^i = d \cdot 2 + e_0 \quad \text{mit} \quad d = \sum_{i=1}^{t} e_i 2^{i-1} = \sum_{i=0}^{t-1} e_{i+1} 2^i$$

Nach Induktionshypothese berechnet die ersten $t - 1$ Schleifendurchläufe den Wert x^d; daher berechnet der letzte Durchlauf ($i = 0$) das folgende Resultat

$$(x^d)^2 \cdot x^{e_0} = x^e$$

Beweis.

- Induktion über t; für $t = 0$ gilt $e = 1$ und laut Algorithmus $x^1 = x$
- Für $t > 0$ schreiben wir

$$e = \sum_{i=0}^{t} e_i 2^i = d \cdot 2 + e_0 \quad \text{mit} \quad d = \sum_{i=1}^{t} e_i 2^{i-1} = \sum_{i=0}^{t-1} e_{i+1} 2^i$$

Nach Induktionshypothese berechnet die ersten $t - 1$ Schleifendurchläufe den Wert x^d; daher berechnet der letzte Durchlauf ($i = 0$) das folgende Resultat

$$(x^d)^2 \cdot x^{e_0} = x^e$$

Beweis.

- Induktion über t; für $t = 0$ gilt $e = 1$ und laut Algorithmus $x^1 = x$
- Für $t > 0$ schreiben wir

$$e = \sum_{i=0}^{t} e_i 2^i = d \cdot 2 + e_0 \quad \text{mit} \quad d = \sum_{i=1}^{t} e_i 2^{i-1} = \sum_{i=0}^{t-1} e_{i+1} 2^i$$

Nach Induktionshypothese berechnet die ersten $t - 1$ Schleifendurchläufe den Wert x^d; daher berechnet der letzte Durchlauf ($i = 0$) das folgende Resultat

$$(x^d)^2 \cdot x^{e_0} = x^e$$

Beispiel

Es gilt: $3^9 = 3^8 \cdot 3^1 = ((3^2)^2)^2 \cdot 3 = 19683$. Für die Berechnung sind 4 Multiplikationen nötig, davon 3 für das Quadrieren.

Definition

- $d \in \mathbb{Z}$ heißt Teiler von $a \in \mathbb{Z}$, wenn es $c \in \mathbb{Z}$ gibt mit $a = c \cdot d$
- „d teilt a“, „a ist Vielfaches von d“ $d \mid a$
- die Teiler $\pm 1, \pm a$ nennt man triviale Teiler von a

Definition

- $d \in \mathbb{Z}$ heißt Teiler von $a \in \mathbb{Z}$, wenn es $c \in \mathbb{Z}$ gibt mit $a = c \cdot d$
- „d teilt a“, „a ist Vielfaches von d“ $d \mid a$
- die Teiler $\pm 1, \pm a$ nennt man triviale Teiler von a

Definition

Seien $a, b \in \mathbb{Z}$, $a, b \neq 0$

- Der größte gemeinsame Teiler $\mathrm{ggT}(a, b)$ von a und b teilt a und b und für alle $c \mid a$, $c \mid b$ gilt $c \mid \mathrm{ggT}(a, b)$
- $\gcd(a, b)$, „greatest common divisor“

Definition

- $d \in \mathbb{Z}$ heißt Teiler von $a \in \mathbb{Z}$, wenn es $c \in \mathbb{Z}$ gibt mit $a = c \cdot d$
- „d teilt a“, „a ist Vielfaches von d“ $d \mid a$
- die Teiler $\pm 1, \pm a$ nennt man triviale Teiler von a

Definition

Seien $a, b \in \mathbb{Z}$, $a, b \neq 0$

- Der größte gemeinsame Teiler $\mathrm{ggT}(a, b)$ von a und b teilt a und b und für alle $c \mid a$, $c \mid b$ gilt $c \mid \mathrm{ggT}(a, b)$
- $\gcd(a, b)$, „greatest common divisor“
- Das kleinste gemeinsame Vielfache $\mathrm{kgV}(a, b)$ von a und b ist sowohl Vielfaches von a als auch Vielfaches von b und für alle c, sodass $a \mid c$ und $b \mid c$, gilt $\mathrm{kgV}(a, b) \mid c$
- $\mathrm{lcm}(a, b)$, „least common multiple“

Satz

Seien $a, b, c \in \mathbb{Z}$ *mit* $a \neq 0$, $b \neq 0$ *und* $a \neq c \cdot b$; *dann gilt*

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(|a|, |b|) \quad \textit{und} \quad \mathrm{ggT}(a, b) = \mathrm{ggT}(a - c \cdot b, b)$$

Satz

Seien $a, b, c \in \mathbb{Z}$ *mit* $a \neq 0$, $b \neq 0$ *und* $a \neq c \cdot b$; *dann gilt*

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(|a|, |b|) \quad \textit{und} \quad \mathrm{ggT}(a, b) = \mathrm{ggT}(a - c \cdot b, b)$$

Beweis.

- Wenn $dc = a$, dann auch $d(-c) = -a$, also stimmen die Teiler von a und $|a|$ überein

Satz

Seien $a, b, c \in \mathbb{Z}$ *mit* $a \neq 0$, $b \neq 0$ *und* $a \neq c \cdot b$; *dann gilt*

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(|a|, |b|) \quad \textit{und} \quad \mathrm{ggT}(a, b) = \mathrm{ggT}(a - c \cdot b, b)$$

Beweis.

- Wenn $dc = a$, dann auch $d(-c) = -a$, also stimmen die Teiler von a und $|a|$ überein
- Wenn eine ganze Zahl d die Zahlen a und b teilt, dann teilt sie auch die Zahl $a - c \cdot b$ und umgekehrt wenn d, $a - c \cdot b$ und b teilt, dann gilt auch $d \mid a$

Satz

Seien $a, b, c \in \mathbb{Z}$ *mit* $a \neq 0$, $b \neq 0$ *und* $a \neq c \cdot b$; *dann gilt*

$$\mathrm{ggT}(a, b) = \mathrm{ggT}(|a|, |b|) \quad \textit{und} \quad \mathrm{ggT}(a, b) = \mathrm{ggT}(a - c \cdot b, b)$$

Beweis.

- Wenn $dc = a$, dann auch $d(-c) = -a$, also stimmen die Teiler von a und $|a|$ überein
- Wenn eine ganze Zahl d die Zahlen a und b teilt, dann teilt sie auch die Zahl $a - c \cdot b$ und umgekehrt wenn d, $a - c \cdot b$ und b teilt, dann gilt auch $d \mid a$
- die gemeinsamen Teiler von a und b mit den gemeinsamen Teilern von $a - c \cdot b$ und b überein, und die größten gemeinsamen Teiler sind gleich

Satz (euklidischer Algorithmus für ganze Zahlen)

Der größte gemeinsame Teiler zweier ganzer Zahlen ungleich Null kann wie folgt berechnet werden:

Ersetze die Zahlen durch ihre Beträge.

Solange die Zahlen verschieden sind, wiederhole:

Ersetze die größere der Zahlen durch die Differenz der größeren und der kleineren.

Die resultierende Zahl ist dann der größte gemeinsame Teiler.

Satz (euklidischer Algorithmus für ganze Zahlen)

Der größte gemeinsame Teiler zweier ganzer Zahlen ungleich Null kann wie folgt berechnet werden:

> *Ersetze die Zahlen durch ihre Beträge.*
>
> *Solange die Zahlen verschieden sind, wiederhole:*
>
> > *Ersetze die größere der Zahlen durch die Differenz der größeren und der kleineren.*
>
> *Die resultierende Zahl ist dann der größte gemeinsame Teiler.*

Ersetzt man mehrfaches Abziehen derselben Zahl durch eine Division mit Rest, erhält man den folgenden Algorithmus, der eine komprimierte Berechnung erlaubt

Satz (euklidischer Algorithmus für ganze Zahlen)

Der größte gemeinsame Teiler zweier ganzer Zahlen ungleich Null kann wie folgt berechnet werden:

> *Ersetze die Zahlen durch ihre Beträge.*
>
> *Solange die Zahlen verschieden sind, wiederhole:*
>
> > *Ersetze die größere der Zahlen durch die Differenz der größeren und der kleineren.*
>
> *Die resultierende Zahl ist dann der größte gemeinsame Teiler.*

Ersetzt man mehrfaches Abziehen derselben Zahl durch eine Division mit Rest, erhält man den folgenden Algorithmus, der eine komprimierte Berechnung erlaubt

Satz (Variante)

Ersetze die Zahlen durch ihre Beträge.

Solange keine der zwei Zahlen ein Teiler der anderen ist, wiederhole:

Ersetze die größere der Zahlen durch ihren Rest

nach Division durch die kleinere.

Der resultierende Teiler ist dann der größte gemeinsame Teiler.

Satz (Variante)

Ersetze die Zahlen durch ihre Beträge.

Solange keine der zwei Zahlen ein Teiler der anderen ist, wiederhole:

Ersetze die größere der Zahlen durch ihren Rest

nach Division durch die kleinere.

Der resultierende Teiler ist dann der größte gemeinsame Teiler.

Beweis.

- Nach dem vorigen Satz bleiben bei jedem Schritt die größten gemeinsamen Teiler der beiden Zahlen gleich, somit folgt Korrektheit

Satz (Variante)

Ersetze die Zahlen durch ihre Beträge.

Solange keine der zwei Zahlen ein Teiler der anderen ist, wiederhole:

Ersetze die größere der Zahlen durch ihren Rest

nach Division durch die kleinere.

Der resultierende Teiler ist dann der größte gemeinsame Teiler.

Beweis.

- Nach dem vorigen Satz bleiben bei jedem Schritt die größten gemeinsamen Teiler der beiden Zahlen gleich, somit folgt Korrektheit
- In jedem Schleifendurchlauf die Zahlen positiv bleiben, aber ihr Maximum um mindestens 1 sinkt, bricht der Algorithmus nach endlich vielen Schritten ab, somit folgt Termination

Satz (Variante)

Ersetze die Zahlen durch ihre Beträge.

Solange keine der zwei Zahlen ein Teiler der anderen ist, wiederhole:

Ersetze die größere der Zahlen durch ihren Rest

nach Division durch die kleinere.

Der resultierende Teiler ist dann der größte gemeinsame Teiler.

Beweis.

- Nach dem vorigen Satz bleiben bei jedem Schritt die größten gemeinsamen Teiler der beiden Zahlen gleich, somit folgt Korrektheit
- In jedem Schleifendurchlauf die Zahlen positiv bleiben, aber ihr Maximum um mindestens 1 sinkt, bricht der Algorithmus nach endlich vielen Schritten ab, somit folgt Termination

Beispiel

Es gilt $\mathrm{ggT}(138, -48) = 6$, denn die erste Methode liefert

$$\begin{aligned}\mathrm{ggT}(138, -48) &= \mathrm{ggT}(138, 48) = \mathrm{ggT}(90, 48) = \mathrm{ggT}(42, 48)\\ &= \mathrm{ggT}(42, 6) = \mathrm{ggT}(36, 6) = \mathrm{ggT}(30, 6)\\ &= \mathrm{ggT}(24, 6) = \mathrm{ggT}(18, 6) = \mathrm{ggT}(12, 6)\\ &= \mathrm{ggT}(6, 6) = 6\end{aligned}$$

Beispiel

Es gilt $\mathrm{ggT}(138, -48) = 6$, denn die erste Methode liefert

$$\begin{aligned}\mathrm{ggT}(138, -48) &= \mathrm{ggT}(138, 48) = \mathrm{ggT}(90, 48) = \mathrm{ggT}(42, 48)\\ &= \mathrm{ggT}(42, 6) = \mathrm{ggT}(36, 6) = \mathrm{ggT}(30, 6)\\ &= \mathrm{ggT}(24, 6) = \mathrm{ggT}(18, 6) = \mathrm{ggT}(12, 6)\\ &= \mathrm{ggT}(6, 6) = 6\end{aligned}$$

Die zweite Methode liefert

$$\mathrm{ggT}(138, -48) = \mathrm{ggT}(138, 48) = \mathrm{ggT}(42, 48) = \mathrm{ggT}(42, 6) = 6\,.$$

Satz (erweiterter euklidischer Algorithmus, Lemma von Bézout)

Seien a und b ganze Zahlen ungleich Null. Dann gibt es ganze Zahlen u und v mit

$$u \cdot a + v \cdot b = \mathrm{ggT}(a, b)$$

Diese Zahlen u und v können durch folgenden Algorithmus berechnet werden:

Setze $A = (|a|, 1, 0)$ *und* $B = (|b|, 0, 1)$.

Solange B_1 *die Zahl* A_1 *nicht teilt, wiederhole:*

- *Berechne den ganzzahligen Quotienten* q *von* A_1 *und* B_1.
- *Setze* $C = B$.
- *Setze* $B = A - q \cdot C$ *(komponentenweise gerechnet)*
- *Setze* $A = C$.

Setze $u = \mathrm{vz}(a) \cdot B_2$ *und* $v = \mathrm{vz}(b) \cdot B_3$.

Beweis.

- Sei $T = (T_1, T_2, T_3)$ ein Tripel ganzer Zahlen und $(*)$ die Eigenschaft

$$T_1 = |a| \cdot T_2 + |b| \cdot T_3 \qquad (*)$$

Beweis.

- Sei $T = (T_1, T_2, T_3)$ ein Tripel ganzer Zahlen und $(*)$ die Eigenschaft

$$T_1 = |a| \cdot T_2 + |b| \cdot T_3 \qquad (*)$$

- Wenn die Zahlentripel A und B die Eigenschaft $(*)$ haben, dann auch alle Tripel $A - q \cdot B$ mit $q \in \mathbb{Z}$.

Beweis.

- Sei $T = (T_1, T_2, T_3)$ ein Tripel ganzer Zahlen und $(*)$ die Eigenschaft

$$T_1 = |a| \cdot T_2 + |b| \cdot T_3 \qquad (*)$$

- Wenn die Zahlentripel A und B die Eigenschaft $(*)$ haben, dann auch alle Tripel $A - q \cdot B$ mit $q \in \mathbb{Z}$.
- Die ersten zwei Tripel im Algorithmus haben diese Eigenschaft, daher auch alle anderen auftretenden Tripel. In der ersten Komponente der Tripel wird der euklidische Algorithmus durchgeführt, für das letzte Tripel B gilt daher

$$\mathrm{ggT}(a,b) = B_1 = |a| \cdot B_2 + |b| \cdot B_3 = \underbrace{(\mathrm{vz}(a) \cdot B_2)}_{u} \cdot a + \underbrace{(\mathrm{vz}(b) \cdot B_3)}_{v} \cdot b$$

Beweis.

- Sei $T = (T_1, T_2, T_3)$ ein Tripel ganzer Zahlen und $(*)$ die Eigenschaft

$$T_1 = |a| \cdot T_2 + |b| \cdot T_3 \qquad (*)$$

- Wenn die Zahlentripel A und B die Eigenschaft $(*)$ haben, dann auch alle Tripel $A - q \cdot B$ mit $q \in \mathbb{Z}$.
- Die ersten zwei Tripel im Algorithmus haben diese Eigenschaft, daher auch alle anderen auftretenden Tripel. In der ersten Komponente der Tripel wird der euklidische Algorithmus durchgeführt, für das letzte Tripel B gilt daher

$$\mathrm{ggT}(a,b) = B_1 = |a| \cdot B_2 + |b| \cdot B_3 = \underbrace{(\mathrm{vz}(a) \cdot B_2)}_{u} \cdot a + \underbrace{(\mathrm{vz}(b) \cdot B_3)}_{v} \cdot b$$

Beispiel

Für $a = 138$ und $b = -48$ liefert der erweiterte euklidische Algorithmus $u = -1$ und $v = -3$ und $\mathrm{ggT}(138, -48) = 6$

Beispiel

Für $a = 138$ und $b = -48$ liefert der erweiterte euklidische Algorithmus $u = -1$ und $v = -3$ und $\mathrm{ggT}(138, -48) = 6$

A	B	q
$(138, 1, 0)$	$(48, 0, 1)$	2
$(48, 0, 1)$	$(42, 1, -2)$	1
$(42, 1, -2)$	$(6, -1, 3)$	

Beispiel

Für $a = 138$ und $b = -48$ liefert der erweiterte euklidische Algorithmus $u = -1$ und $v = -3$ und $\mathrm{ggT}(138, -48) = 6$

A	B	q
$(138, 1, 0)$	$(48, 0, 1)$	2
$(48, 0, 1)$	$(42, 1, -2)$	1
$(42, 1, -2)$	$(6, -1, 3)$	

Satz (binärer erweiterter euklidischer Algorithmus)

Seien a und b positive ganze Zahlen mit höchstens n Binärziffern. Dann können

$$g := \mathrm{ggT}(a, b) \quad \textit{und} \quad u, v \in \mathbb{Z} \quad \textit{mit} \quad u \cdot a + v \cdot b = g$$

durch Additionen, Subtraktionen und Shifts mit $O(n^2)$ Bitoperationen berechnet werden

Algorithmus

1. Setze $e = 0$
2. Solange a und b gerade sind, wiederhole:

   Setze $a = a/2$, $b = b/2$ und $e = e + 1$
3. Setze $A = (a, 1, 0)$ und $B = (b, 0, 1)$
4. Solange A_1 gerade ist, wiederhole:

   Setze $A_1 = A_1/2$.

   Falls A_2 und A_3 gerade sind

   setze $A_2 = A_2/2$ und $A_3 = A_3/2$

   ansonsten falls $A_2 > 0$ ist

   setze $A_2 = (A_2 - b)/2$ und $A_3 = (A_3 + a)/2$

   ansonsten

   setze $A_2 = (A_2 + b)/2$ und $A_3 = (A_3 - a)/2$

Algorithmus (cont'd)

5. Solange B_1 gerade ist, wiederhole:

   Setze $B_1 = B_1/2$

   Wenn B_2 und B_3 gerade sind

   setze $B_2 = B_2/2$ und $B_3 = B_3/2$

   ansonsten falls $B_2 > 0$ ist

   setze $B_2 = (B_2 - b)/2$ und $B_3 = (B_3 + a)/2$

   ansonsten

   setze $B_2 = (B_2 + b)/2$ und $B_3 = (B_3 - a)/2$

6. Falls $A_1 > B_1$, setze $A = A - B$ und gehe zu Schritt 4
7. Falls $A_1 < B_1$, setze $B = B - A$ und gehe zu Schritt 5
8. Setze $g = B_1 \cdot 2^e$, $u = B_2$ und $v = B_3$

Beweis der Korrektheit.

- ObdA nehmen wir an, dass a oder b ungerade sind (Schritt 2 fällt aus)
- Zur Analyse der Schritte 3-7 betrachten wir die Eigenschaft

$$T_1 = a \cdot T_2 + b \cdot T_3 \quad T = (T_1, T_2, T_3) \qquad (*)$$

Beweis der Korrektheit.

- ObdA nehmen wir an, dass a oder b ungerade sind (Schritt 2 fällt aus)
- Zur Analyse der Schritte 3-7 betrachten wir die Eigenschaft

$$T_1 = a \cdot T_2 + b \cdot T_3 \quad T = (T_1, T_2, T_3) \qquad (*)$$

- Startwerte für A und B in Schritt 3 haben die Eigenschaft $(*)$

Beweis der Korrektheit.

- ObdA nehmen wir an, dass a oder b ungerade sind (Schritt 2 fällt aus)
- Zur Analyse der Schritte 3-7 betrachten wir die Eigenschaft

$$T_1 = a \cdot T_2 + b \cdot T_3 \quad T = (T_1, T_2, T_3) \qquad (*)$$

- Startwerte für A und B in Schritt 3 haben die Eigenschaft $(*)$
- Wenn A und B die Eigenschaft $(*)$ besitzen, dann auch die Tripel $A - B$, bzw $B - A$ (Schritt 6,7)

Beweis der Korrektheit.

- ObdA nehmen wir an, dass a oder b ungerade sind (Schritt 2 fällt aus)
- Zur Analyse der Schritte 3-7 betrachten wir die Eigenschaft

$$T_1 = a \cdot T_2 + b \cdot T_3 \quad T = (T_1, T_2, T_3) \qquad (*)$$

- Startwerte für A und B in Schritt 3 haben die Eigenschaft $(*)$
- Wenn A und B die Eigenschaft $(*)$ besitzen, dann auch die Tripel $A - B$, bzw $B - A$ (Schritt 6,7)
- Wenn A_1, A_2 und A_3 gerade sind, dann hat auch $(A_1/2, A_2/2, A_3/2)$ Eigenschaft $(*)$
- Wenn A_1 gerade ist, A_2 oder A_3 ungerade sind, dann sind $A_2 - b$ und $A_3 + a$ gerade, außerdem folgt aus $A_2 > 0$, dass $A_3 \leqslant 0$ gilt
- Somit gilt Eigenschaft $(*)$ auch für $(A_1/2, (A_2 - b)/2, (A_3 + a)/2)$ (Schritt 4)

Beweis der Korrektheit.

- ObdA nehmen wir an, dass a oder b ungerade sind (Schritt 2 fällt aus)
- Zur Analyse der Schritte 3-7 betrachten wir die Eigenschaft

$$T_1 = a \cdot T_2 + b \cdot T_3 \quad T = (T_1, T_2, T_3) \qquad (*)$$

- Startwerte für A und B in Schritt 3 haben die Eigenschaft $(*)$
- Wenn A und B die Eigenschaft $(*)$ besitzen, dann auch die Tripel $A - B$, bzw $B - A$ (Schritt 6,7)
- Wenn A_1, A_2 und A_3 gerade sind, dann hat auch $(A_1/2, A_2/2, A_3/2)$ Eigenschaft $(*)$
- Wenn A_1 gerade ist, A_2 oder A_3 ungerade sind, dann sind $A_2 - b$ und $A_3 + a$ gerade, außerdem folgt aus $A_2 > 0$, dass $A_3 \leqslant 0$ gilt
- Somit gilt Eigenschaft $(*)$ auch für $(A_1/2, (A_2 - b)/2, (A_3 + a)/2)$ (Schritt 4)
- Schließlich gilt für $A_1 = B_1$ in Schritt 8, $g = a \cdot B_2 + b \cdot B_3$ ■

Satz (Berechnung des kleinsten gemeinsamen Vielfachen)

Seien a und b ganze Zahlen ungleich Null. Dann gilt

$$\mathrm{kgV}(a,b) = \frac{|a| \cdot |b|}{\mathrm{ggT}(a,b)} .$$

Satz (Berechnung des kleinsten gemeinsamen Vielfachen)

Seien a und b ganze Zahlen ungleich Null. Dann gilt

$$\mathrm{kgV}(a,b) = \frac{|a| \cdot |b|}{\mathrm{ggT}(a,b)}\,.$$

Beweis.

Offensichtlich ist

$$m := \frac{|b|}{\mathrm{ggT}(a,b)} \cdot |a| = \frac{|a|}{\mathrm{ggT}(a,b)} \cdot |b|$$

ein Vielfaches sowohl von a als auch von b und somit ein gemeinsames Vielfaches. Wir zeigen, dass m das kleinste gemeinsame Vielfache von a und b ist. Sei dazu eine positive ganze Zahl z gemeinsames Vielfaches von a und b. Dann gibt es ganze Zahlen c, d mit

$$z = c \cdot a \quad \text{und} \quad z = d \cdot b$$

Beweis (Fortsetzung).

Nach dem vorigen Satz existieren Zahlen u, v mit

$$u \cdot a + v \cdot b = \mathrm{ggT}(a, b)$$

Es folgt

$$z = \frac{u \cdot a + v \cdot b}{\mathrm{ggT}(a,b)} \cdot z = \frac{u \cdot a}{\mathrm{ggT}(a,b)} \cdot z + \frac{v \cdot b}{\mathrm{ggT}(a,b)} \cdot z =$$
$$\frac{u \cdot a \cdot d \cdot b}{\mathrm{ggT}(a,b)} + \frac{v \cdot b \cdot c \cdot a}{\mathrm{ggT}(a,b)} = \frac{a \cdot b}{\mathrm{ggT}(a,b)} \cdot (u \cdot d + v \cdot c) =$$
$$m \cdot \mathrm{vz}(a \cdot b) \cdot (u \cdot d + v \cdot c)$$

und damit ist z ein Vielfaches von m.

Beweis (Fortsetzung).

Nach dem vorigen Satz existieren Zahlen u, v mit

$$u \cdot a + v \cdot b = \mathrm{ggT}(a, b)$$

Es folgt

$$z = \frac{u \cdot a + v \cdot b}{\mathrm{ggT}(a,b)} \cdot z = \frac{u \cdot a}{\mathrm{ggT}(a,b)} \cdot z + \frac{v \cdot b}{\mathrm{ggT}(a,b)} \cdot z =$$
$$\frac{u \cdot a \cdot d \cdot b}{\mathrm{ggT}(a,b)} + \frac{v \cdot b \cdot c \cdot a}{\mathrm{ggT}(a,b)} = \frac{a \cdot b}{\mathrm{ggT}(a,b)} \cdot (u \cdot d + v \cdot c) =$$
$$m \cdot \mathrm{vz}(a \cdot b) \cdot (u \cdot d + v \cdot c)$$

und damit ist z ein Vielfaches von m. Aus $z, m > 0$ folgt $\mathrm{vz}(a \cdot b) \cdot (u \cdot d + v \cdot c) > 0$, somit $z \geqslant m$ und wegen der Totalität von $>$ ist m das kleinste gemeinsame Vielfache von a und b.

Beweis (Fortsetzung).

Nach dem vorigen Satz existieren Zahlen u, v mit

$$u \cdot a + v \cdot b = \mathrm{ggT}(a, b)$$

Es folgt

$$z = \frac{u \cdot a + v \cdot b}{\mathrm{ggT}(a,b)} \cdot z = \frac{u \cdot a}{\mathrm{ggT}(a,b)} \cdot z + \frac{v \cdot b}{\mathrm{ggT}(a,b)} \cdot z =$$
$$\frac{u \cdot a \cdot d \cdot b}{\mathrm{ggT}(a,b)} + \frac{v \cdot b \cdot c \cdot a}{\mathrm{ggT}(a,b)} = \frac{a \cdot b}{\mathrm{ggT}(a,b)} \cdot (u \cdot d + v \cdot c) =$$
$$m \cdot \mathrm{vz}(a \cdot b) \cdot (u \cdot d + v \cdot c)$$

und damit ist z ein Vielfaches von m. Aus $z, m > 0$ folgt $\mathrm{vz}(a \cdot b) \cdot (u \cdot d + v \cdot c) > 0$, somit $z \geqslant m$ und wegen der Totalität von $>$ ist m das kleinste gemeinsame Vielfache von a und b. ∎

Definition

Eine natürliche Zahl p heißt Primzahl, wenn $p \notin \{0, 1\}$ und p nur die trivialen Teiler besitzt.

Definition

Eine natürliche Zahl p heißt Primzahl, wenn $p \notin \{0, 1\}$ und p nur die trivialen Teiler besitzt.

Satz

Sei p eine Primzahl und seien $a, b \in \mathbb{Z}$. Wenn p das Produkt $a \cdot b$ teilt, dann teilt p auch einen der Faktoren a oder b.

Definition

Eine natürliche Zahl p heißt Primzahl, wenn $p \notin \{0, 1\}$ und p nur die trivialen Teiler besitzt.

Satz

Sei p eine Primzahl und seien $a, b \in \mathbb{Z}$. Wenn p das Produkt $a \cdot b$ teilt, dann teilt p auch einen der Faktoren a oder b.

Beweis.

Sei $c \in \mathbb{Z}$ mit $c \cdot p = a \cdot b$. Wenn p die Zahl a teilt, sind wir fertig. Wenn p die Zahl a nicht teilt, dann ist $\mathrm{ggT}(a, p) = 1$. Daher gibt es ganze Zahlen u und v mit $1 = u \cdot a + v \cdot p$; es folgt

$$b = b \cdot u \cdot a + b \cdot v \cdot p = u \cdot c \cdot p + b \cdot v \cdot p = (u \cdot c + b \cdot v) \cdot p\,,$$

somit ist p ein Teiler von b

Definition

Eine natürliche Zahl p heißt Primzahl, wenn $p \notin \{0, 1\}$ und p nur die trivialen Teiler besitzt.

Satz

Sei p eine Primzahl und seien $a, b \in \mathbb{Z}$. Wenn p das Produkt $a \cdot b$ teilt, dann teilt p auch einen der Faktoren a oder b.

Beweis.

Sei $c \in \mathbb{Z}$ mit $c \cdot p = a \cdot b$. Wenn p die Zahl a teilt, sind wir fertig. Wenn p die Zahl a nicht teilt, dann ist $\mathrm{ggT}(a, p) = 1$. Daher gibt es ganze Zahlen u und v mit $1 = u \cdot a + v \cdot p$; es folgt

$$b = b \cdot u \cdot a + b \cdot v \cdot p = u \cdot c \cdot p + b \cdot v \cdot p = (u \cdot c + b \cdot v) \cdot p\,,$$

somit ist p ein Teiler von b ∎

Satz (Fundamentalsatz der Arithmetik)

Jede ganze Zahl größer als 1 *kann als Produkt von Primzahlen geschrieben werden. Diese Primzahlen heißen Primfaktoren der Zahl und sind bis auf die Reihenfolge eindeutig bestimmt.*

Satz (Fundamentalsatz der Arithmetik)

Jede ganze Zahl größer als 1 *kann als Produkt von Primzahlen geschrieben werden. Diese Primzahlen heißen Primfaktoren der Zahl und sind bis auf die Reihenfolge eindeutig bestimmt.*

Beweis.

Es genügt zu beweisen, dass die Primfaktoren eindeutig bestimmt sind (Induktion nach a); seien also

$$a = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$$

zwei Zerlegungen von a in Primfaktoren.

Satz (Fundamentalsatz der Arithmetik)

Jede ganze Zahl größer als 1 *kann als Produkt von Primzahlen geschrieben werden. Diese Primzahlen heißen Primfaktoren der Zahl und sind bis auf die Reihenfolge eindeutig bestimmt.*

Beweis.

Es genügt zu beweisen, dass die Primfaktoren eindeutig bestimmt sind (Induktion nach a); seien also

$$a = p_1 p_2 \cdots p_k = q_1 q_2 \cdots q_\ell$$

zwei Zerlegungen von a in Primfaktoren. Wir zeigen die Behauptung durch wohlfundierte Induktion nach $<$. Da p_1 das Produkt $q_1 q_2 \cdots q_\ell$ teilt, gibt es nach dem vorigen Satz eine Zahl $j \in \{1, \ldots, \ell\}$ mit $p_1 = q_j$, $p_1 \geqslant 2$; somit ist

$$p_2 \cdots p_k = \prod_{\substack{1 \leqslant i \leq \ell \\ i \neq j}} q_i$$

die Behauptung folgt aus IH. ∎

Folgerung

Seien a und b positive ganze Zahlen mit Primfaktorzerlegungen $a = \prod_{i=1}^{n} p_i^{e_i}$ und $b = \prod_{i=1}^{n} p_i^{f_i}$, wobei $p_1, \ldots, p_n$ paarweise verschiedene Primzahlen und $e_1, \ldots, e_n, f_1, \ldots, f_n$ natürliche Zahlen sind. Dann gilt

$$\mathrm{ggT}(a,b) = \prod_{i=1}^{n} p_i^{\min(e_i,f_i)} \quad \textit{und} \quad \mathrm{kgV}(a,b) = \prod_{i=1}^{n} p_i^{\max(e_i,f_i)}$$

wobei $\min(e_i, f_i)$ bzw. $\max(e_i, f_i)$ die kleinere bzw. die größere der zwei Zahlen e_i und f_i bezeichnet.

Folgerung

Seien a und b positive ganze Zahlen mit Primfaktorzerlegungen $a = \prod_{i=1}^{n} p_i^{e_i}$ und $b = \prod_{i=1}^{n} p_i^{f_i}$, wobei $p_1, \ldots, p_n$ paarweise verschiedene Primzahlen und $e_1, \ldots, e_n, f_1, \ldots, f_n$ natürliche Zahlen sind. Dann gilt

$$\mathrm{ggT}(a,b) = \prod_{i=1}^{n} p_i^{\min(e_i,f_i)} \quad \textit{und} \quad \mathrm{kgV}(a,b) = \prod_{i=1}^{n} p_i^{\max(e_i,f_i)}$$

wobei $\min(e_i, f_i)$ bzw. $\max(e_i, f_i)$ die kleinere bzw. die größere der zwei Zahlen e_i und f_i bezeichnet.

Beweis für $\mathrm{ggT}(a, b)$.

- $d := \prod_{i=1}^{n} p_i^{\min(e_i,f_i)}$ teilt a und b
- Nach dem Satz ist die Primfaktorenzerlegung von a und b eindeutig, also kann d nur die Primfaktoren $p_1, \ldots, p_n$ enthalten
- Nach Def. darf aber p_i in $\mathrm{ggT}(a, b)$ nur $\min(e_i, f_i)$-mal auftreten: $d = \mathrm{ggT}(a, b)$

Satz

Es gibt unendlich viele Primzahlen.

Satz

Es gibt unendlich viele Primzahlen.

Beweis.

- Wir nehmen an, die Zahlen $p_1, p_2, \ldots, p_n$ wären sämtliche Primzahlen, sei

$$q := \prod_{i=1}^{n} p_i$$

- Dann ist $q + 1$ größer als jede Primzahl und somit keine Primzahl
- Nach der Primfaktorzerlegung gibt es eine Primzahl p_j, die $q + 1$ teilt
- Da p_j auch q teilt, würde p_j auch 1 teilen, was im Widerspruch zur Primheit von p_j steht

Satz

Es gibt unendlich viele Primzahlen.

Beweis.

- Wir nehmen an, die Zahlen $p_1, p_2, \ldots, p_n$ wären sämtliche Primzahlen, sei

$$q := \prod_{i=1}^{n} p_i$$

- Dann ist $q + 1$ größer als jede Primzahl und somit keine Primzahl
- Nach der Primfaktorzerlegung gibt es eine Primzahl p_j, die $q + 1$ teilt
- Da p_j auch q teilt, würde p_j auch 1 teilen, was im Widerspruch zur Primheit von p_j steht

Definition

- Sei n eine positive ganze Zahl. Zwei ganze Zahlen a, b heißen kongruent modulo n, in Zeichen $a \equiv_n b$ wenn ihre Reste nach Division durch n a mod n und b mod n gleich sind
- Kongruenz modulo n ist eine Äquivalenzrelation; die Äquivalenzklasse einer ganzen Zahl a ist

$$\overline{a} := \{a + z \cdot n \mid z \in \mathbb{Z}\}$$

  und wird die Restklasse von a modulo n genannt
- Die Menge aller Restklassen modulo n wird mit $\mathbb{Z}/n$ bezeichnet

Definition

- Sei n eine positive ganze Zahl. Zwei ganze Zahlen a, b heißen kongruent modulo n, in Zeichen $a \equiv_n b$ wenn ihre Reste nach Division durch n a mod n und b mod n gleich sind
- Kongruenz modulo n ist eine Äquivalenzrelation; die Äquivalenzklasse einer ganzen Zahl a ist

$$\overline{a} := \{a + z \cdot n \mid z \in \mathbb{Z}\}$$

  und wird die Restklasse von a modulo n genannt
- Die Menge aller Restklassen modulo n wird mit $\mathbb{Z}/n$ bezeichnet

Bemerkung

Als Repräsentantensysteme verwenden wir üblicherweise die kleinsten nicht-negativen Reste $\{0, 1, 2, \ldots, n-1\}$ oder die absolut-kleinsten Reste

$$\begin{cases} \{-n/2+1, \ldots, -1, 0, 1, \ldots, n/2\} & \text{falls } n \text{ gerade} \\ \{-(n-1)/2, \ldots, -1, 0, 1, \ldots, (n-1)/2\} & \text{falls } n \text{ ungerade.} \end{cases}$$

Satz

Die Abbildungen

$$+ \colon \mathbb{Z}/n \times \mathbb{Z}/n \to \mathbb{Z}/n\,,\ (\overline{a},\overline{b}) \mapsto \overline{a} + \overline{b} := \overline{a+b}\,,$$

und

$$\cdot \colon \mathbb{Z}/n \times \mathbb{Z}/n \to \mathbb{Z}/n\,,\ (\overline{a},\overline{b}) \mapsto \overline{a} \cdot \overline{b} := \overline{a \cdot b}\,,$$

sind wohldefiniert und $(\mathbb{Z}/n; \overline{0}, \overline{1})$ *ist ein kommutativer Ring*

Satz

Die Abbildungen

$$+ \colon \mathbb{Z}/n \times \mathbb{Z}/n \to \mathbb{Z}/n\,,\ (\overline{a},\overline{b}) \mapsto \overline{a} + \overline{b} := \overline{a+b}\,,$$

und

$$\cdot \colon \mathbb{Z}/n \times \mathbb{Z}/n \to \mathbb{Z}/n\,,\ (\overline{a},\overline{b}) \mapsto \overline{a} \cdot \overline{b} := \overline{a \cdot b}\,,$$

sind wohldefiniert und $(\mathbb{Z}/n; \overline{0}, \overline{1})$ *ist ein kommutativer Ring* ■

Beispiel

Es gilt $\mathbb{Z}/5 = \{\overline{0},\overline{1},\overline{2},\overline{3},\overline{4}\} = \{\overline{-2},\overline{-1},\overline{0},\overline{1},\overline{2}\}$; weiters gilt $\overline{0} = \{0,5,10,15,\ldots\} = \overline{5}$ und $\overline{2}+\overline{4} = \overline{6} = \overline{1}$.

Definition

Eine Restklasse $\overline{a}$ modulo n heißt invertierbar, wenn es eine Restklasse $\overline{b}$ (mod n) gibt mit $\overline{a} \cdot \overline{b} = \overline{1}$ (mod n)

Satz

Sei n eine positive ganze Zahl und a eine ganze Zahl ungleich Null.

(1) *Die Restklasse von a modulo n ist genau dann invertierbar, wenn* $\mathrm{ggT}(a, n) = 1$ *; in diesem Fall können mit dem erweiterten euklidischen Algorithmus ganze Zahlen u, v mit $u \cdot a + v \cdot n = 1$ berechnet werden, und dann ist $\overline{a}^{-1} = \overline{u}$*

(2) *$\mathbb{Z}/n$ ist ein Körper gdw n eine Primzahl*

Satz

Sei n eine positive ganze Zahl und a eine ganze Zahl ungleich Null.

(1) *Die Restklasse von a modulo n ist genau dann invertierbar, wenn* $\mathrm{ggT}(a,n)=1$ *; in diesem Fall können mit dem erweiterten euklidischen Algorithmus ganze Zahlen u,v mit $u\cdot a+v\cdot n=1$ berechnet werden, und dann ist $\overline{a}^{-1}=\overline{u}$*

(2) *$\mathbb{Z}/n$ ist ein Körper gdw n eine Primzahl*

Beweis.

(1) Wenn $\mathrm{ggT}(a,n)=1$ und $u\cdot a+v\cdot n=1$ ist, dann ist $\overline{1}=\overline{u}\cdot\overline{a}+\overline{v}\cdot\overline{n}=\overline{u}\cdot\overline{a}+\overline{v}\cdot\overline{0}=\overline{u}\cdot\overline{a}$. Wenn umgekehrt $\overline{a}$ invertierbar ist, dann gibt es eine ganze Zahl b mit $\overline{a}\cdot\overline{b}=\overline{1}$, also $\overline{ab-1}=\overline{0}$; somit ist n ein Teiler von $ab-1$. Da $\mathrm{ggT}(a,n)$ sowohl a als auch $ab-1$ teilt, ist $\mathrm{ggT}(a,n)=1$

(2) Sei n eine Primzahl und a eine ganze Zahl. Dann ist entweder a ein Vielfaches von n oder $\mathrm{ggT}(a,n)=1$; die Behauptung aus (1)

Satz

Sei n eine positive ganze Zahl und a eine ganze Zahl ungleich Null.

(1) *Die Restklasse von a modulo n ist genau dann invertierbar, wenn* $\mathrm{ggT}(a,n)=1$ *; in diesem Fall können mit dem erweiterten euklidischen Algorithmus ganze Zahlen u,v mit $u\cdot a+v\cdot n=1$ berechnet werden, und dann ist $\overline{a}^{-1}=\overline{u}$*

(2) *$\mathbb{Z}/n$ ist ein Körper gdw n eine Primzahl*

Beweis.

(1) Wenn $\mathrm{ggT}(a,n)=1$ und $u\cdot a+v\cdot n=1$ ist, dann ist $\overline{1}=\overline{u}\cdot\overline{a}+\overline{v}\cdot\overline{n}=\overline{u}\cdot\overline{a}+\overline{v}\cdot\overline{0}=\overline{u}\cdot\overline{a}$. Wenn umgekehrt $\overline{a}$ invertierbar ist, dann gibt es eine ganze Zahl b mit $\overline{a}\cdot\overline{b}=\overline{1}$, also $\overline{ab-1}=\overline{0}$; somit ist n ein Teiler von $ab-1$. Da $\mathrm{ggT}(a,n)$ sowohl a als auch $ab-1$ teilt, ist $\mathrm{ggT}(a,n)=1$

(2) Sei n eine Primzahl und a eine ganze Zahl. Dann ist entweder a ein Vielfaches von n oder $\mathrm{ggT}(a,n)=1$; die Behauptung aus (1) ∎

Beispiel

Die Zahl 6 ist nicht invertierbar modulo 26, das Inverse von 5 modulo 26 ist 21. Der Ring $\mathbb{Z}/2$ ist ein Körper mit zwei Elementen, der Ring $\mathbb{Z}/256$ ist kein Körper.

Satz (der kleine Satz von Fermat)

Sei p eine Primzahl und sei a eine ganze Zahl, die nicht von p geteilt wird. Dann gilt

$$a^{p-1} \equiv_p 1\,.$$

Beispiel

Die Zahl 6 ist nicht invertierbar modulo 26, das Inverse von 5 modulo 26 ist 21. Der Ring $\mathbb{Z}/2$ ist ein Körper mit zwei Elementen, der Ring $\mathbb{Z}/256$ ist kein Körper.

Satz (der kleine Satz von Fermat)

Sei p eine Primzahl und sei a eine ganze Zahl, die nicht von p geteilt wird. Dann gilt

$$a^{p-1} \equiv_p 1\,.$$

Beweis.

Die Restklassen $\overline{1a}, \overline{2a}, \ldots, \overline{(p-1)a}$ sind alle von $\overline{0}$ und untereinander verschieden und damit eine Permutation von $\overline{1}, \overline{2}, \ldots, \overline{p-1}$ Somit ist

$$\overline{1 \cdot 2 \cdots (p-1)} \cdot \overline{a^{p-1}} = \overline{1a} \cdot \overline{2a} \cdots \overline{(p-1)a} = \overline{1 \cdot 2 \cdots (p-1)} \cdot \overline{1}$$

Kürzen liefert den Satz ∎

Satz (chinesischer Restsatz)

Seien p und q positive ganze Zahlen mit $\mathrm{ggT}(p,q) = 1$, und seien a und b beliebige ganze Zahlen. Dann hat das Kongruenzensystem

$$x \equiv_p a$$
$$x \equiv_q b$$

die eindeutige Lösung $x \equiv_{pq} vqa + upb$ wobei die ganzen Zahlen u und v mit $up + vq = 1$ durch den erweiterten euklidischen Algorithmus berechnet werden können.

Satz (chinesischer Restsatz)

Seien p und q positive ganze Zahlen mit $\mathrm{ggT}(p,q) = 1$, und seien a und b beliebige ganze Zahlen. Dann hat das Kongruenzensystem

$$x \equiv_p a$$
$$x \equiv_q b$$

die eindeutige Lösung $x \equiv_{pq} vqa + upb$ wobei die ganzen Zahlen u und v mit $up + vq = 1$ durch den erweiterten euklidischen Algorithmus berechnet werden können.

Beweis.

Nach Konstruktion gilt
$x \equiv_p a \equiv_p 1a \equiv_p (vq + up)a \equiv_p (vqa + upa) \equiv_p vqa$ und
$x \equiv_q b \equiv_q 1b \equiv_q (vq + up)b \equiv_q (vqb + upb) \equiv_q upb$

Satz (chinesischer Restsatz)

Seien p und q positive ganze Zahlen mit $\mathrm{ggT}(p,q) = 1$, und seien a und b beliebige ganze Zahlen. Dann hat das Kongruenzensystem

$$x \equiv_p a$$
$$x \equiv_q b$$

die eindeutige Lösung $x \equiv_{pq} vqa + upb$ wobei die ganzen Zahlen u und v mit $up + vq = 1$ durch den erweiterten euklidischen Algorithmus berechnet werden können.

Beweis.

Nach Konstruktion gilt
$x \equiv_p a \equiv_p 1a \equiv_p (vq + up)a \equiv_p (vqa + upa) \equiv_p vqa$ und
$x \equiv_q b \equiv_q 1b \equiv_q (vq + up)b \equiv_q (vqb + upb) \equiv_q upb$ ∎

Beispiel

Die eindeutige Lösung des Kongruenzensystems

$$x \equiv_5 1$$
$$x \equiv_7 2$$

ist $x \equiv_{35} 16$

Beispiel

Die eindeutige Lösung des Kongruenzensystems

$$x \equiv_5 1$$
$$x \equiv_7 2$$

ist $x \equiv_{35} 16$
Wir berechnen mit dem erweiterten euklidischen Algorithmus ganze Zahlen u und v, sodass $u \cdot 5 + v \cdot 7 = \text{ggT}(5,7)$.

$A = (5,1,0)$	$B = (7,0,1)$	$q = 0$
$A = (7,0,1)$	$B = (5,1,0)$	$q = 1$
$A = (5,1,0)$	$B = (2,-1,1)$	$q = 2$
$A = (2,-1,-1)$	$B = (1,3,-2)$	$q = 2$

Somit ist $u = 3$ und $v = -2$ und $\text{ggT}(5,7) = 3 \cdot 5 - 2 \cdot 7 = 1$ und deshalb ist $-2 \cdot 7 \cdot 1 + 3 \cdot 5 \cdot 2 = 16$ und die Lösung $x \equiv_{35} 16$ eindeutig