Rechnen modulo n

Bernhard Ganter

Institut für Algebra
TU Dresden
D-01062 Dresden
bernhard.ganter@tu-dresden.de

Kanonische Primfaktorzerlegung

Jede natürliche Zahl $n > 0$ kann auf eindeutige Weise in der Form

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$$

geschrieben werden, wobei

- $k \in \mathbb{N}$,
- $\alpha_i \in \mathbb{N} \setminus \{0\}$ für $i \in \{1, \ldots, k\}$ und
- $p_1 < p_2 < \cdots < p_k$ Primzahlen sind.

Dies ist die **kanonische Primfaktorzerlegung** von n.

ggT und kgV

Je zwei natürliche Zahlen n und m besitzen

- einen größten gemeinsamen Teiler $\mathrm{ggT}(m, n)$ und
- ein kleinstes gemeinsames Vielfaches $\mathrm{kgV}(m, n)$.

Zur Bestimmung des ggT kann man den Algorithmus der **Wechselwegnahme** benutzen:

```
while m ≠ n do
begin

  if m < n then n := n − m

  if n < m then m := m − n

end
output(‘‘ggT =’’, m).
```

Gauss–Klammer

Ist r eine reelle Zahl, dann bezeichnet $\lfloor r \rfloor$ die größte ganze Zahl, die kleiner oder gleich r ist.

Analog ist $\lceil r \rceil$ die kleinste ganze Zahl, die größer oder gleich r ist.

Sind a und b ganze Zahlen, $b \neq 0$, so ist

$$a \operatorname{div} b = \left\lfloor \frac{a}{b} \right\rfloor .$$

$z \mod n$

Ist z eine beliebige ganze Zahl und ist $n > 0$ eine natürliche Zahl, dann ist

$$z \mod n := z - n \cdot \left\lfloor \frac{z}{n} \right\rfloor .$$

Beispielsweise ist

- $17 \mod 5 = 2$ und
- $-17 \mod 5 = 3$.

In jedem Falle gilt $z \mod n \in \{0, 1, \ldots, n-1\}$.

Rechnen modulo n

Wenn man umfangreiche Rechnungen modulo n auszuführen hat, dann ist die **Homomorphieregel** außerordentlich hilfreich. Sie besagt, dass man auch Zwischenergebnisse modulo n rechnen darf, ohne dass sich das Endergebnis ändert. Formal besagt sie, dass für ganze Zahlen a, b stets folgendes gilt:

$$\begin{aligned}(a+b) \bmod n &= (a \bmod n + b \bmod n) \bmod n \\ (a-b) \bmod n &= (a \bmod n - b \bmod n) \bmod n \\ (a \cdot b) \bmod n &= (a \bmod n \cdot b \bmod n) \bmod n\end{aligned}$$

$a \equiv r \pmod{n}$

Der ständige Zusatz „mod n“ wird rasch lästig und gern weggelassen. Um Missverständnisse zu vermeiden, kann man ihn am Ende der Rechnung in Klammern angeben und die Gleichheitszeichen durch $\equiv$ ersetzen, wie im folgenden Beispiel:

$$(108 \cdot 33) - 22 \equiv (3 \cdot 3) + 3 \equiv 9 + 3 \equiv 2 \pmod{5}.$$

Statt $a \mod n = r$ schreibt man oft auch

$$a \equiv r \pmod{n}$$

und liest dies etwas altertümlich aber einprägsam als

a ist kongruent zu r modulo n.

Ein Satz von J.P.Fermat

> Eine Primzahl p ist genau dann nicht als Summe zweier Quadrate ganzer Zahlen darstellbar, wenn p kongruent zu 3 modulo 4 ist.

Solche Ergebnisse der elementaren Zahlentheorie haben in den letzten Jahren für die *Kryptologie* an Bedeutung gewonnen.

Rechnen modulo 5

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$-$	0	1	2	3	4
0	0	4	3	2	1
1	1	0	4	3	2
2	2	1	0	4	3
3	3	2	1	0	4
4	4	3	2	1	0

$\cdot$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Die Verknüpfungstafeln für die Rechenarten modulo 5.

Operationen auf einer Menge

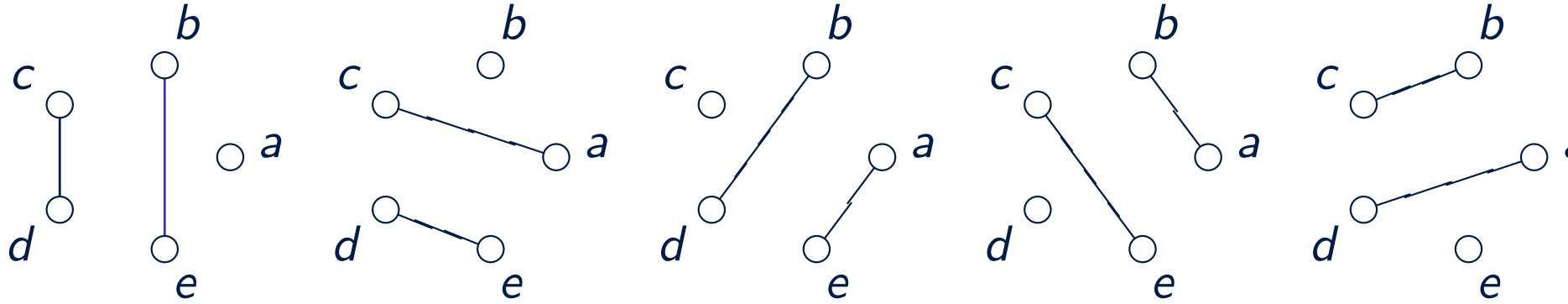
Grundsätzlich hat man nahezu unbegrenzte Freiheiten, sich neue Rechenstrukturen zu verschaffen: Man wählt sich eine Trägermenge und definiert darauf **Operationen**, beispielsweise indem man willkürlich Verknüpfungstafeln hinschreibt.

Operation und *Verknüpfung* bedeuten in diesem Zusammenhang dasselbe. Eine n-stellige Operation auf einer Trägermenge T nimmt als Input eine Folge von n Elementen aus T und gibt ein Element von T als Output zurück.

Eine n-stellige Operation auf T ist also eine Abbildung

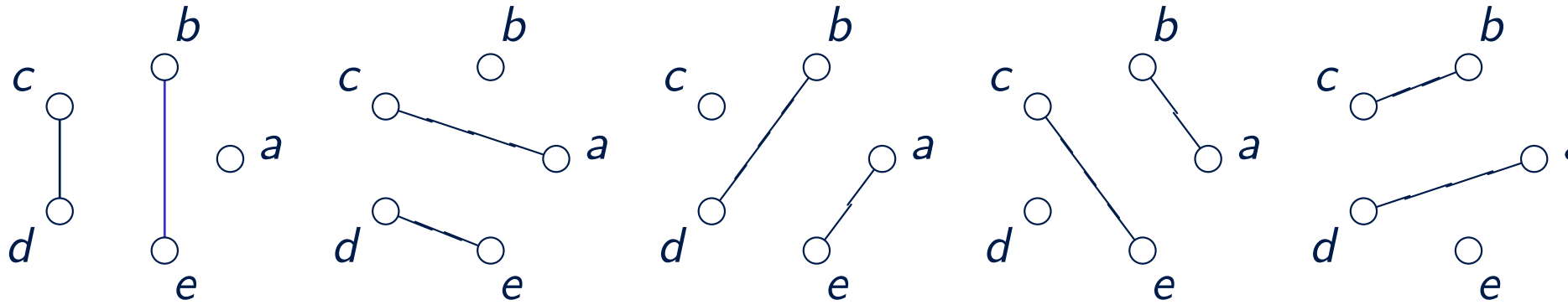
$$f : T^n \to T.$$

Tischtennisturniermultiplikation



$$x \circ y := \begin{cases} x & \text{falls } x = y \\ \text{der Spieler, der aussetzt, wenn } x \text{ gegen } y \text{ spielt} & \text{falls } x \neq y \end{cases}$$

Tischtennisturniermultiplikationstafel



$\circ$	a	b	c	d	e
a	a	d	b	e	c
b	d	b	e	c	a
c	b	e	c	a	d
d	e	c	a	d	b
e	c	a	d	b	e

Regeln (1) für das Rechnen modulo n

Die Addition

- ist assoziativ: es gilt $(a+b)+c = a+(b+c)$ für alle a, b, c,
- ist kommutativ: es gilt $a+b = b+a$ für alle a, b,
- ist **kürzbar**: aus $a+b = a+c$ folgt stets $b = c$. Das ist wichtig, wenn man Gleichungen lösen will.
- hat 0 als **neutrales Element**: $a+0 = 0+a = a$ gilt für alle a.
- hat **inverse Elemente**: Zu jedem a ist $-a := 0-a$ ein Element mit $a+(-a) = 0 = (-a)+a$. Daraus folgt übrigens die Kürzbarkeit.

$(\mathbb{Z}_n, +_{\bmod n}, -_{\bmod n}, 0)$ ist eine abelsche Gruppe.

Regeln (2) für das Rechnen modulo n

die Multiplikation

- ist assoziativ: es gilt $(a \cdot b) \cdot c = a \cdot (b \cdot c)$ für alle a, b, c,
- ist kommutativ: es gilt $a \cdot b = b \cdot a$ für alle a, b,
- hat 1 als neutrales Element: $a \cdot 1 = a = 1 \cdot a$ gilt für alle a.
- ist über der Addition distributiv: $a \cdot (b + c) = a \cdot b + a \cdot c$ gilt für alle a, b, c (Leseregel: „Punktrechnung vor Strichrechnung“).

$$\mathbb{Z}_n := (\mathbb{Z}_n, +_{\bmod n}, -_{\bmod n}, \cdot_{\bmod n}, 0, 1)$$

ist ein kommutativer Ring mit Eins.

Ein anderer Zugang zu $\mathbb{Z}_n$

Für Zahlenmengen $A, B \subseteq \mathbb{R}$ definiert man die **Komplexaddition** durch

$$A + B := \{a + b \mid a \in A, b \in B\}.$$

Entsprechend kann man eine **Komplexsubtraktion** und eine **Komplexmultiplikation** einführen.

So kommt man (wenn man noch Klammern einspart) für natürliche Zahlen n und r zu

$$n\mathbb{Z} + r := \{\ldots, r - 2n, r - n, r, r + n, r + 2n, \ldots\},$$

der **Restklasse** zum Rest r modulo n. Diese Menge enthält genau diejenigen ganzen Zahlen, die bei der ganzzahligen Division durch n den Rest r ergeben.

Restklassenringe

Man überzeugt sich, dass bei festem n die

- Komplexaddition,
- Komplexsubtraktion und
- Komplexmultiplikation

von Restklassen als Ergebnisse immer Restklassen liefern.

Die Restklassen modulo n bilden einen kommutativen Ring mit Eins, den **Restklassenring** der ganzen Zahlen modulo n.

Rechnen mit Repräsentanten

Jede Restklasse modulo n enthält genau eine der Zahlen $\{0, 1, \ldots, n-1\}$.

Deshalb rechnet man nicht wirklich mit den Restklassen, sondern mit ihren *Repräsentanten* aus $\mathbb{Z}_n$.

Das entspricht genau der oben eingeführten Rechenweise modulo n.

Der Restklassenring modulo n ist also isomorph zum Ring $\mathbb{Z}_n$ der ganzen Zahlen modulo n.

Rechnen modulo 2

Der für die Informatik wichtigste Fall ist natürlich $\mathbb{Z}_2$. In diesem Fall stimmen Addition und Subtraktion überein. Die beiden Restklassen sind die Menge der geraden und die der ungeraden Zahlen.

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Das Rechnen modulo 2.

Dividieren modulo n?

Eine *Division* modulo n kann man nicht ohne erhebliche Einschränkungen erfinden.

Das zeigt ein einfaches Beispiel: das Rechnen modulo 6.

Wenn es möglich wäre, eine Division durch 2 modulo 6 zu erfinden, dann sollte doch jedenfalls 2 geteilt durch 2 das Ergebnis 1 und 0 geteilt durch 2 das Ergebnis Null liefern.
Daraus erhält man die widersprüchliche Gleichung

$$3 \equiv 3 \cdot 1 \equiv 3 \cdot \frac{2}{2} \equiv \frac{3 \cdot 2}{2} \equiv \frac{0}{2} \equiv 0 \pmod 6.$$

So geht es also nicht!

Nullteiler

Man kann dieses Beispiel verallgemeinern.
Man nennt eine Zahl $a \neq 0$ (in einem Ring) einen **Nullteiler**, wenn es eine Zahl $b \neq 0$ mit $a \cdot b = 0$ gibt.

Im Ring $\mathbb{Z}_6$ ist diese Bedingung für $a = 2$ und $b = 3$ erfüllt:
2 ist also ein Nullteiler in $\mathbb{Z}_6$.

Die Argumentation der vorigen Seite zeigt:

eine Division durch Nullteiler
kann nicht sinnvoll definiert werden.

Einheiten

Eine Zahl a in einem Ring ist eine **Einheit**, wenn es eine Zahl b mit $a \cdot b = 1$ gibt.

Durch Einheiten kann man „dividieren“, denn b verhält sich ja wie ein Kehrwert zu a.

Man sagt, b sei *multiplikativ invers* zu a.

Man dividiert durch a, indem man mit b multipliziert.

Mittelwert mod 5

Auf diese Weise können wir z.B. einen „Mittelwert modulo 5“ definieren, nämlich die Operation

$$a \bullet b := 3(a + b) \bmod 5,$$

denn wegen $2 \cdot 3 \bmod 5 = 1$ ist $3(a + b)$ modulo 5 dasselbe wie $\frac{a+b}{2}$.

$\bullet$	0	1	2	3	4
0	0	3	1	4	2
1	3	1	4	2	0
2	1	4	2	0	3
3	4	2	0	3	1
4	2	0	3	1	4

.

Tischtennis mod 5

Auf diese Weise können wir z.B. einen „Mittelwert modulo 5“ definieren, nämlich die Operation

$$a \bullet b := 3(a + b) \bmod 5,$$

denn wegen $2 \cdot 3 \bmod 5 = 1$ ist $3(a + b)$ modulo 5 dasselbe wie $\frac{a+b}{2}$.

$\circ$	a	b	c	d	e
a	a	d	b	e	c
b	d	b	e	c	a
c	b	e	c	a	d
d	e	c	a	d	b
e	c	a	d	b	e

$\cong$

$\bullet$	0	1	2	3	4
0	0	3	1	4	2
1	3	1	4	2	0
2	1	4	2	0	3
3	4	2	0	3	1
4	2	0	3	1	4

.

Welche Zahlen sind Einheiten mod n?

Durch Einheiten kann man dividieren, durch Nullteiler nicht.

Es bleibt die Frage, wie man Einheiten und Nullteiler erkennt.

Modulo n ist das einfach:

Hilfssatz Eine Zahl $a \in \{1, \ldots, n-1\}$ ist genau dann eine Einheit modulo n, wenn a zu n teilerfremd ist.
Ist a keine Einheit, dann ist a ein Nullteiler.

Eulersche φ-Funktion

Die Eulersche φ-Funktion ist für $n \in \mathbb{N}$ folgendermaßen definiert:

$$\varphi(n) := |\{e \in \{0, \ldots, n-1\} \mid \mathrm{ggT}(e, n) = 1\}|.$$

$\varphi(n)$ gibt also die Anzahl der zu n teilerfremden natürlichen Zahlen an, die kleiner als n sind.

$\varphi(n)$ gibt also auch die Anzahl der Einheiten in $\mathbb{Z}_n$ an.

Eine Formel für $\varphi(n)$

Satz Ist

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_k^{\alpha_k}$$

die kanonische Primfaktorzerlegung von n, dann gilt

$$\varphi(n) = n \cdot (1 - \frac{1}{p_1}) \cdot (1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k}).$$

Beispiel: $1008 = 2^4 \cdot 3^2 \cdot 7$, deshalb
$\varphi(1008) = 1008 \cdot (1 - \frac{1}{2}) \cdot (1 - \frac{1}{3}) \cdot (1 - \frac{1}{7}) = 1008 \cdot \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{6}{7} = 288.$

Funktion Wegnahme

Input: Eine Menge $\{a, b\}$, bestehend aus natürlichen Zahlen a und b.

Output: $\mathrm{WN}(\{a, b\}) := \begin{cases} \{b, a - b\} & \text{falls } a \geq b \\ \{a, b - a\} & \textit{sonst}. \end{cases}$

Es wird also die größere der beiden Zahlen ersetzt durch die positive Differenz der beiden Zahlen. Das Ergebnis ist eine zwei- oder einelementige Menge.

Eigenschaften der Funktion Wegnahme

1. Ist
$$\{a_1, b_1\} = \mathrm{WN}(\{a, b\}),$$
dann gibt es ganze Zahlen $\lambda_1, \lambda_2, \lambda_3, \lambda_4$ mit
$$a_1 = \lambda_1 \cdot a + \lambda_2 \cdot b$$
und
$$b_1 = \lambda_3 \cdot a + \lambda_4 \cdot b.$$
2. Ist $\{a_1, b_1\} = \mathrm{WN}(\{a, b\})$ und ist d ein gemeinsamer Teiler von a_1 und b_1, dann ist d auch ein Teiler von a und von b.

Wechselwegnahme

Algorithmus Wechselwegnahme.
Input: Natürliche Zahlen a, b.

WHILE $|\{a, b\}| = 2$ do

$\{a, b\} := \mathrm{WN}(\{a, b\})$;

OUTPUT: a.

Weil bei jedem WHILE-Schritt die größere der beiden Zahlen verkleinert wird, terminiert dieser Algorithmus offenbar, d.h., er kommt zu einem Ergebnis.

Beispiel zur Wechselwegnahme

	Input:	154	238
$238 - 154 = 84$	also:	154	84
$154 - 84 = 70$	also:	84	70
$84 - 70 = 14$	also:	70	14
$70 - 14 = 56$	also:	56	14
$56 - 14 = 42$	also:	42	14
$42 - 14 = 28$	also:	28	14
$28 - 14 = 14$	also:	14	14
	stop.		

ggT-Berechnung

Hilfssatz Der Algorithmus **Wechselwegnahme** berechnet den größten gemeisamen Teiler (ggT).

Beweis Sei d das Ergebnis einer Ausführung des Algorithmus bei dem Input $\{a, b\}$. Wendet man die Beobachtungen 1) und 2) induktiv an, so erhält man:

1. Es gibt ganze Zahlen α, β mit $d = \alpha \cdot a + \beta \cdot b$,
2. d teilt a und b.

Das zweite zeigt, dass d ein gemeinsamer Teiler von a und b ist, und aus dem ersten folgt, dass jeder gemeinsame Teiler von a und b auch ein Teiler von d ist. Deshalb muss d der größte gemeinsame Teiler von a und b sein.

Beobachtung

Eine Erkenntnis aus dem Beweis wollen wir als Satz festhalten, weil sie oft sehr nützlich ist:

Satz Zu je zwei ganzen Zahlen a, b existieren ganze Zahlen α, β mit

$$\mathrm{ggT}(a, b) = \alpha \cdot a + \beta \cdot b.$$

Diese Zahlen α, β kann man durch „Rückwärtseinsetzen“ beim Algorithmus „Wechselwegnahme“ leicht bestimmen.

Beschleunigung der ggT-Berechnung

Am Beispiel erkennt man eine Möglichkeit, den Algorithmus zu beschleunigen: die letzten vier Schritte kann man zu einem einzigen zusammenfassen.

Funktion Mehrfachwegnahme.

Input: Natürliche Zahlen a und b mit $a \geq b$.

Output: $\mathrm{MW}(a, b) := (b, a \bmod b)$.

Es wird also die größere der beiden Zahlen ersetzt durch ihren Rest modulo der anderen.

Algorithmus (Euklidischer Algorithmus).

Input: Ganze Zahlen a, b mit $a \geq b \geq 0$

WHILE $b \neq 0$ do

$(a, b) := \mathrm{MW}(a, b)$;

Output: a.

. . . berechnet den ggT

Der Euklidische Algorithmus führt offenbar zum gleichen Ergebnis wie die Wechselwegnahme. Wir haben also:

Satz Der Euklidische Algorithmus berechnet den ggT.

Beispiel

a	b		
238	154	$238 \bmod 154 = 84$	

Beispiel

a	b		
238	154	$238 \bmod 154 = 84$	
154	84	$154 \bmod 84 = 70$	

Beispiel

a	b		
238	154	$238 \bmod 154 = 84$	
154	84	$154 \bmod 84 = 70$	
84	70	$84 \bmod 70 = 14$	

Beispiel

a	b		
238	154	$238 \bmod 154 = 84$	
154	84	$154 \bmod 84 = 70$	
84	70	$84 \bmod 70 = 14$	
70	14	$70 \bmod 14 = 0$	

Beispiel

a	b		
238	154	$238 \bmod 154 = 84$	
154	84	$154 \bmod 84 = 70$	
84	70	$84 \bmod 70 = 14$	
70	14	$70 \bmod 14 = 0$	$\mathrm{ggT}(238, 154) = 14$

Beispiel

a	b		
238	154	$238 \bmod 154 = 84$	
154	84	$154 \bmod 84 = 70$	
84	70	$84 \bmod 70 = 14$	$14 = 84 - 70$
70	14	$70 \bmod 14 = 0$	$\mathrm{ggT}(238, 154) = 14$

Beispiel

a	b		
238	154	$238 \bmod 154 = 84$	
154	84	$154 \bmod 84 = 70$	$70 = 154 - 84$
84	70	$84 \bmod 70 = 14$	$14 = 84 - 70$
70	14	$70 \bmod 14 = 0$	$\mathrm{ggT}(238, 154) = 14$

Beispiel

a	b		
238	154	$238 \bmod 154 = 84$	$84 = 238 - 154$
154	84	$154 \bmod 84 = 70$	$70 = 154 - 84$
84	70	$84 \bmod 70 = 14$	$14 = 84 - 70$
70	14	$70 \bmod 14 = 0$	$\mathrm{ggT}(238, 154) = 14$

Beispiel

a	b		
238	154	$84 = 238 - 154$	
154	84	$70 = 154 - 84$	
84	70	$14 = 84 - 70$	
70	14	$\mathrm{ggT}(238, 154) = 14$	

Beispiel

a	b		
238	154	$84 = 238 - 154$	
154	84	$70 = 154 - 84$	
84	70	$14 = 84 - 70$	$\mathrm{ggT} = 84 - 70$
70	14	$\mathrm{ggT}(238, 154) = 14$	

Beispiel

a	b		
238	154	$84 = 238 - 154$	
154	84	$70 = 154 - 84$	$\mathrm{ggT} = 2 \cdot 84 - 154$
84	70	$14 = 84 - 70$	$\mathrm{ggT} = 84 - 70$
70	14	$\mathrm{ggT}(238, 154) = 14$	

Beispiel

a	b		
238	154	$84 = 238 - 154$	$\mathrm{ggT} = 2 \cdot 238 - 3 \cdot 154$
154	84	$70 = 154 - 84$	$\mathrm{ggT} = 2 \cdot 84 - 154$
84	70	$14 = 84 - 70$	$\mathrm{ggT} = 84 - 70$
70	14	$\mathrm{ggT}(238, 154) = 14$	

Beweis des Hilfssatzes über die Einheiten

Beweis Wenn a zu n teilerfremd ist, dann gibt es nach dem Satz Zahlen α und β mit

$$\alpha \cdot a + \beta \cdot n = 1$$

und folglich

$$\alpha \cdot a \equiv 1 \pmod{n},$$

woraus

$$(\alpha \bmod n) \cdot a \equiv 1 \pmod{n}$$

folgt. $\alpha \bmod n$ ist dann multiplikativ invers zu a in $\mathbb{Z}_n$.
Ist $ggT(a, n) =: d > 1$, dann ist $b := \frac{n}{d}$ eine ganze Zahl in $\mathbb{Z}_n$, die von Null verschieden ist. Aber $a \cdot b$ ist dann ein Vielfaches von n und folglich $a \cdot b \equiv 0 \pmod{n}$, d.h. a ist ein Nullteiler oder gleich 0.

Inversenberechnung mod n

Aufgabe: Bestimme die Lösung der Gleichung

$$13 \cdot x \bmod 109 = 10.$$

Lösungsweg:

1. Zeige mit Hilfe des Euklidischen Algorithmus, dass $\mathrm{ggT}(109, 13) = 1$ gilt.
2. Berechne Zahlen α und β mit $1 = \alpha \cdot 13 + \beta \cdot 109$.
3. Multiplikativ invers zu 13 ist dann α mod 109.
4. Die (einzige) Lösung der Aufgabe ist daher

$$x = 10 \cdot \alpha \bmod 109.$$

$\mathrm{GF}(p)$

Wenn p eine Primzahl ist, dann ist jede Zahl in $\{1, 2, \ldots, p-1\}$ teilerfremd zu p.

Wenn p eine Primzahl ist, dann gibt es modulo p keine Nullteiler. Man kann durch alle Zahlen von $\mathbb{Z}_p$ (außer Null) modulo p dividieren.

Der Ring $\mathbb{Z}_p$, p prim, ist ein **Körper**!

Er wird auch mit dem Symbol $\mathrm{GF}(p)$ abgekürzt ("Galois-Field").