Dr. Silke Hartlieb, Prof. Dr. Luise Unger

Modul 61115

Mathematische Grundlagen der Kryptografie

LESEPROBE

Fakultät für
Mathematik und Informatik

FernUniversität in Hagen

Inhaltsverzeichnis

Studierhinweise

In dieser Kurseinheit werden wir grundlegende Definitionen und Eigenschaften von Ringen untersuchen und ein erstes Public-Key-Kryptosystem vorstellen.

Nachdem wir in Abschnitt 5.1 einige grundlegende Begriffe und Beispiele behandelt haben, wird in Abschnitt 5.2 eine ganz wichtige Konstruktion vorgestellt, wie wir aus Ringen neue Ringe herstellen können. Es geht um so genannte Faktorringe modulo einem Ideal. Diese Konstruktion ist analog zu Konstruktionen, die Sie im Laufe des Studiums schon kennen gelernt haben: In der Linearen Algebra haben Sie Faktorräume modulo einem Unterraum und in Kurseinheit 2 Faktorgruppen modulo einem Normalteiler gesehen. Die Konstruktion eines Faktorringes modulo einem Ideal ist ganz ähnlich, nur dass eben auf die besondere Situation, dass wir mit Ringen arbeiten, eingegangen wird. Sie kennen schon Beispiele für Faktorringe. Die Ringe $\mathbb{Z}/n\mathbb{Z}$ sind Faktorringe, mit denen Sie schon seit dem ersten Semester arbeiten. Die wichtigsten Faktorringe in der Kryptografie sind die Ringe $\mathbb{Z}/n\mathbb{Z}$ und gewisse Faktorringe von Polynomringen $\mathbb{F}_p[T]$, wobei p eine Primzahl ist. Letztere werden benötigt, um die endlichen Körper zu konstruieren, die nicht von der Form $\mathbb{F}_p$, p eine Primzahl sind. Diesen Körpern wird sich die Kurseinheit 5 widmen.

In Abschnitt 5.3 geht es um Ringhomomorphismen. Das sind Abbildungen zwischen Ringen, die die Ringstrukturen respektieren. Nichts in diesem Abschnitt ist wirklich überraschend. Sie werden viele Analogien zwischen Vektorraumhomomorphismen (linearen Abbildungen) und Gruppenhomomorphismen feststellen.

Abschnitt 5.4 widmet sich einem klassischen Satz der elementaren Zahlentheorie, dem so genannten Chinesischen Restsatz. Dieser Satz gibt Antwort auf die Frage, wie gewisse Kongruenzen simultan gelöst werden können. Dieser Satz ist schon seit etwa 2000 Jahren bekannt, ist aber alles andere als ein alter Hut. Er hat wichtige Anwendungen in der Computeralgebra und der Kryptografie.

In Abschnitt 5.5 werden wir spezielle Unterringe von Ringen untersuchen, die so genannten Primringe. Diese sind in gewisser Weise die „kleinsten Unterringe“ von Ringen. Primringe werden bei der Konstruktion der endlichen Körper in Kursein-

heit 5 wieder eine Rolle spielen.

Besonders wichtige Ringe in der Kryptografie sind der Ring $\mathbb{Z}$ und Polynomringe über endlichen Körpern sowie Faktorringe dieser Ringe. Diese Ringe sind kommutativ. Wir werden daher in Abschnitt 5.6 auf diese spezielle Situation eingehen und Ideale und Faktorringe kommutativer Ringe näher betrachten.

Abschnitt 5.7 widmet sich Polynomringen. Hier werden wir unter anderem einige Fakten aus der Linearen Algebra II wiederholen, wo Polynome im Zusammenhang mit dem charakteristischen Polynom einer Matrix oder eines Endomorphismus studiert werden. Dieser Abschnitt ist im gewissen Sinne schon der Auftakt zu Kurseinheit 5.

Nach all der Mathematik geht es in Abschnitt 5.8 dann endlich wieder zum zentralen Thema dieses Kurses: der Kryptografie. Dieser Abschnitt behandelt das RSA-Kryptosystem. Dieses System wurde schon 1978 entdeckt, spielt aber immer noch eine zentrale Rolle in der Public-Key-Kryptografie. Wir werden in Abschnitt 5.8 nur sagen wie und warum es funktioniert. Warum es wirklich „gut“, das heißt „schnell“ ist, wird in Kurseinheit 4 präzisiert und erklärt.

Kapitel 5

Ringe

5.1 Notation und Beispiele

Obgleich Sie Ringe schon kennen, wiederholen wir noch einmal die Definition:

5.1.1 Definition Ein **Ring** $(R, +, \cdot)$ ist eine Menge R mit zwei Verknüpfungen $+$ und $\cdot$, so dass folgende Bedingungen erfüllt sind:

(i) $(R, +)$ ist eine abelsche Gruppe.

(ii) $\cdot$ ist assoziativ, und es gibt ein **neutrales Element** der Multiplikation $e \in R$, so dass $a \cdot e = e \cdot a = a$ für alle $a \in R$ gilt.

(iii) Es gelten die **Distributivgesetze**, das heißt, für alle $a, b, c \in R$ gilt

(a) $a(b + c) = ab + ac$

(b) $(a + b)c = ac + bc$.

Wenn R zusätzlich noch die Bedingung

(iv) Für alle $a, b \in R$ gilt $a \cdot b = b \cdot a$

erfüllt, so wird R ein **kommutativer Ring** genannt.

Hier gleich eine **Warnung**: Es gibt konkurrierende Definitionen von Ringen. Oft wird die Bedingung (ii) dahingehend abgeschwächt, dass die Existenz eines neutralen Elementes der Multiplikation nicht gefordert wird. Wenn Sie zusätzliche Literatur lesen, müssen Sie also immer nachsehen, welche Definition für einen Ring benutzt wird.

5.1.2 Beispiele (a) $(\mathbb{Z}, +, \cdot)$ ist ein kommutativer Ring.

(b) Für alle $n \in \mathbb{N}$, $n > 1$, ist $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ ein kommutativer Ring.

(c) Sei $R = \{0\}$. Dann ist R ein Ring. Das neutrale Element der Addition und der Multiplikation ist in beiden Fällen das Element 0.

(d) Sei R ein Ring. Der Polynomring $R[T]$ ist ein Ring, und $R[T]$ ist genau dann kommutativ, wenn R kommutativ ist. Dies haben wir in der Linearen Algebra I, Kurseinheit 2, gezeigt.

(e) Sei R ein kommutativer Ring, und seien $\mathrm{M}_{nn}(R)$ die $n \times n$-Matrizen über R. Mit der Addition und der Multiplikation von Matrizen ist $\mathrm{M}_{nn}(R)$ ein Ring. Für $n > 1$ ist dieser Ring nicht kommutativ.

(f) Sei R die Menge der Funktionen von $\mathbb{R}$ nach $\mathbb{R}$. Für alle $f, g \in R$ definieren wir $f + g : \mathbb{R} \to \mathbb{R}$ durch $(f + g)(x) = f(x) + g(x)$ und $f \cdot g : \mathbb{R} \to \mathbb{R}$ durch $(f \cdot g)(x) = f(x) \cdot g(x)$ für alle $x \in \mathbb{R}$. Mit diesen Verknüpfungen ist $(R, +, \cdot)$ ein kommutativer Ring.

5.1.3 Notationen Wir behalten die Notationen bei, die wir in 4.1.4 bei den Gruppen bereits eingeführt haben. Sei $(R, +, \cdot)$ ein Ring.

(a) Das neutrale Element in $(R, +)$ wird mit 0 bezeichnet. Ist $a \in R$, so bezeichnen wir das inverse Element zu a in $(R, +)$ mit $-a$. An Stelle von $b+(-a)$ schreiben wir $b - a$. Ist $n \in \mathbb{N}$, so schreiben wir na für die Summe $a + \cdots + a$ mit n Summanden a und $(-n)a = n(-a)$. Ferner ist $0a = 0$.

(b) Das neutrale Element der Multiplikation wird mit 1 bezeichnet. An Stelle von $a \cdot b$ schreiben wir nur ab. Ist $a \in R$ bezüglich der Multiplikation invertierbar, so bezeichnen wir das inverse Element mit a^{-1}. Ist $n \in \mathbb{N}$, so schreiben wir a^n für das Produkt $a \cdot \cdots \cdot a$ von n Faktoren a. Ist a invertierbar, so wird a^0 als 1 und a^{-m} als $(a^{-1})^m$ definiert.

Analog zu Produkten von Gruppen (vergleichen Sie Abschnitt 4.9) können wir Produkte von Ringen definieren.

Dazu seien $(R_1, +_1, \cdot_1), \ldots, (R_n, +_n, \cdot_n)$ Ringe. Wir betrachten das cartesische Produkt

$$\prod_{i=1}^{n} R_i = R_1 \times \cdots \times R_n = \{(r_1, \ldots, r_n) \mid r_i \in R_i, 1 \leq i \leq n\}.$$

Auf $\prod_{i=1}^{n} R_i$ definieren wir zwei Verknüpfungen

$$\begin{array}{rccccc} + : & (R_1 \times \cdots \times R_n) & \times & (R_1 \times \cdots \times R_n) & \to & (R_1 \times \cdots \times R_n) \\ & ((r_1, \ldots, r_n), & & (r'_1, \ldots, r'_n)) & \mapsto & (r_1 +_1 r'_1, \ldots, r_n +_n r'_n) \end{array}$$

und

$$\begin{array}{rccccc} \cdot : & (R_1 \times \cdots \times R_n) & \times & (R_1 \times \cdots \times R_n) & \to & (R_1 \times \cdots \times R_n) \\ & ((r_1, \ldots, r_n), & & (r'_1, \ldots, r'_n)) & \mapsto & (r_1 \cdot_1 r'_1, \ldots, r_n \cdot_n r'_n). \end{array}$$

Mit diesen Verknüpfungen ist $\prod_{i=1}^{n} R_i$ ein Ring mit neutralem Element $(0, \ldots, 0)$ der Addition und neutralem Element $(1, \ldots, 1)$ der Multiplikation.

5.1.4 Definition Der Ring $\prod_{i=1}^{n} R_i$ wird das **direkte Produkt** der Ringe $R_1, \ldots, R_n$ genannt.

Je nachdem, welche zusätzlichen Eigenschaften Ringe besitzen, werden weitere Definitionen eingeführt.

5.1.5 Definitionen (a) Ein kommutativer Ring $(R, +, \cdot)$ mit $1 \neq 0$ heißt **Integritätsbereich**, wenn aus $ab = 0$ folgt, dass $a = 0$ oder $b = 0$ ist.

(b) Ein Ring $(R, +, \cdot)$ heißt **Schiefkörper**, wenn $(R \setminus \{0\}, \cdot)$ eine Gruppe ist.

(c) Ein kommutativer Schiefkörper wird ein **Körper** genannt.

5.1.6 Aufgabe Beweisen Sie, dass in jedem Schiefkörper aus $ab = 0$ folgt, dass $a = 0$ oder $b = 0$ gilt.

5.1.7 Beispiele (a) Der Ring $\mathbb{Z}$ der ganzen Zahlen ist ein Integritätsbereich.

(b) Jeder Körper ist ein Integritätsbereich.

(c) Sei $\mathbb{K}$ ein Körper. Dann ist der Polynomring $\mathbb{K}[T]$ ein Integritätsbereich.

(d) Sei $n \in \mathbb{N}$, und sei $n = ab$ für Elemente $a \neq 1$ und $b \neq 1$ in $\mathbb{N}$. Dann ist $\mathbb{Z}/n\mathbb{Z}$ kein Integritätsbereich, denn $ab = 0$ in $\mathbb{Z}/n\mathbb{Z}$, aber $a \neq 0$ und $b \neq 0$.

(e) Sie haben in Kurseinheit 7 der Linearen Algebra I mit den Quaternionen $\mathbb{H}$ einen Schiefkörper kennen gelernt, der kein Körper ist.

5.1.8 Aufgabe Seien $R_1, \ldots, R_n$ Ringe. Beweisen oder widerlegen Sie folgende Aussagen.

(a) $\prod_{i=1}^{n} R_i$ ist genau dann ein Integritätsbereich, wenn alle R_i, $1 \leq i \leq n$ Integritätsbereiche sind.

(b) $\prod_{i=1}^{n} R_i$ ist genau dann ein Körper, wenn alle R_i, $1 \leq i \leq n$ Körper sind.

(c) $\prod_{i=1}^{n} R_i$ ist genau dann kommutativ, wenn alle R_i, $1 \leq i \leq n$ kommutativ sind.

Jeder Körper ist ein Schiefkörper, und er ist, wie wir oben in Aufgabe 5.1.6 bereits festgestellt haben, ein Integritätsbereich. Die Umkehrung gilt nicht. Beispielsweise ist $\mathbb{Z}$ ein Integritätsbereich, der kein Körper ist. Ist R ein endlicher Integritätsbereich, so gilt die Umkehrung allerdings schon:

5.1.9 Proposition Jeder Integritätsbereich, der nur endlich viele Elemente enthält, ist ein Körper.

Beweis: Sei $R = \{a_1, \ldots, a_n\}$ ein Integritätsbereich. Sei $a \in R$, $a \neq 0$. Wir bilden $aa_1, \ldots, aa_n$. Diese Elemente sind verschieden, denn aus $aa_i = aa_j$ folgt $aa_i - aa_j = a(a_i - a_j) = 0$. Da R ein Integritätsbereich ist, folgt dann $a = 0$ oder $a_i - a_j = 0$. Die Annahme $a \neq 0$ impliziert $a_i - a_j = 0$, also $a_i = a_j$. Die n Elemente $aa_1, \ldots, aa_n$ sind damit alle Elemente aus R, das heißt, jedes Element in R ist von der Form aa_i. Dies trifft insbesondere für das Element 1 zu. Zu $a \in R$, $a \neq 0$ gibt es also ein $a_i \in R$ mit $aa_i = 1$. Da R kommutativ ist, folgt auch $a_i a = 1$. Somit hat jedes Element in $R \setminus \{0\}$ ein inverses Element, und es folgt, dass $(R \setminus \{0\}, \cdot)$ eine abelsche Gruppe, also $(R, +, \cdot)$ ein Körper ist. □

5.2 Ideale und Faktorringe

5.2.1 Definition Sei $(R, +, \cdot)$ ein Ring. Eine Teilmenge R' von R heißt **Unterring** von R, wenn R' mit den Verknüpfungen $+$ und $\cdot$ in R ein Ring ist, und wenn $1 \in R'$ ist.

Wenn R' ein Unterring von R ist, dann ist $(R', +)$ eine Untergruppe von $(R, +)$.

5.2.2 Beispiele (a) Sei $\mathbb{Q}$ der Körper der rationalen Zahlen. Dann ist $\mathbb{Z}$ ein Unterring von $\mathbb{Q}$.

(b) Sei $\mathbb{K}$ ein Körper. Dann ist $\mathbb{K}$ ein Unterring des Polynomringes $\mathbb{K}[T]$.

(c) Sei $\mathrm{M}_{nn}(\mathbb{K})$ die Menge der $n \times n$-Matrizen über einem Körper $\mathbb{K}$. Sei $\mathrm{B}_{nn}(\mathbb{K})$ die Teilmenge der oberen Dreiecksmatrizen. Da das Produkt von zwei oberen Dreiecksmatrizen eine obere Dreiecksmatrix ist, ist $\mathrm{B}_{nn}(\mathbb{K})$ ein Unterring von $\mathrm{M}_{nn}(\mathbb{K})$.

(d) Sei $n \in \mathbb{N}$, $n > 1$. Dann ist $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ **kein** Unterring von $\mathbb{Z}$. Zwar ist $(n\mathbb{Z}, +)$ eine Untergruppe von $(\mathbb{Z}, +)$, und es gilt auch $(nz)(nz') = n(nzz') \in n\mathbb{Z}$, aber $1 \notin n\mathbb{Z}$. Somit ist $n\mathbb{Z}$ kein Ring.

5.2.3 Definition Sei $(R, +, \cdot)$ ein Ring. Ein **Ideal** I in R ist eine Untergruppe von $(R, +)$, so dass für alle $a \in I$ und alle $b \in R$ die Elemente ab und ba in I liegen. Ist I ein Ideal in R, so schreiben wir $I \lhd R$.

5.2.4 Beispiele (a) Sei $n \in \mathbb{N}$, $n > 1$. Dann ist $n\mathbb{Z} = \{nz \mid z \in \mathbb{Z}\}$ ein Ideal in $\mathbb{Z}$.

(b) Sei R ein kommutativer Ring, und sei $x \in R$. Dann ist $(x) = \{xr \mid r \in R\}$ ein Ideal in R.

Beachten Sie, dass das Beispiel (a) ein Spezialfall dieses Beispiels ist. In (a) ist $R = \mathbb{Z}$ und $x = n$. Ein weiterer wichtiger Spezialfall ist der, wenn $R = \mathbb{K}[T]$, $\mathbb{K}$ ein Körper, und $f = \sum_{i=0}^{n} a_i T^i$ ein Polynom in $\mathbb{K}[T]$ ist. Dann ist $(f) = \{fg \mid g \in \mathbb{K}[T]\}$ ein Ideal in $\mathbb{K}[T]$.

(c) Sei $R = \mathbb{Q}$. Zwar ist $\mathbb{Z}$ ein Unterring von $\mathbb{Q}$, allerdings kein Ideal. Es ist beispielsweise $1 \in \mathbb{Z}$, $\frac{1}{2} \in \mathbb{Q}$, aber $1 \cdot \frac{1}{2} \notin \mathbb{Z}$.

5.2.5 Aufgaben

1. Sei $(R, +, \cdot)$ ein Ring, und sei I ein Ideal in R. Beweisen Sie, dass $I = R$ ist, falls $1 \in I$ gilt.
2. Sei R ein Ring, und seien I_1, I_2 Ideale in R. Beweisen Sie, dass $I_1 \cap I_2$ ein Ideal in R ist.
3. Sei R ein kommutativer Ring, und sei I ein Ideal in R. Sei $\mathrm{M}_{nn}(I)$ die Menge der $n \times n$-Matrizen, deren Einträge in I liegen. Beweisen Sie, dass $\mathrm{M}_{nn}(I)$ ein Ideal in $\mathrm{M}_{nn}(R)$ ist.

Mit Hilfe von Idealen in kommutativen Ringen können wir eine Charakterisierung von Körpern geben:

5.2.6 Proposition (Charakterisierung von Körpern)

Ein kommutativer Ring $R \neq \{0\}$ ist genau dann ein Körper, wenn $\{0\}$ und R die einzigen Ideale in R sind.

Beweis: Sei R ein Körper, und sei $I \neq \{0\}$ ein Ideal in R. Sei $a \in I$, $a \neq 0$. Da R ein Körper ist, ist a invertierbar. Da I ein Ideal ist, folgt $aa^{-1} = 1 \in I$. Dann gilt $r \cdot 1 = r \in I$ für alle $r \in R$, also $R \subseteq I$. Da auch $I \subseteq R$, folgt $R = I$. Dies zeigt, dass $\{0\}$ und R die einzigen Ideale in R sind.

Sei umgekehrt $R \neq \{0\}$ ein kommutativer Ring, dessen einzige Ideale $\{0\}$ und R sind. Sei $a \in R$, $a \neq 0$. Dann ist $(a) \neq \{0\}$, denn $a \in (a)$. Es folgt $(a) = R$. Somit ist jedes Element $r \in R$ von der Form $r = ax$ mit $x \in R$. Insbesondere gibt es $x \in R$ mit $ax = 1$. Es gilt auch $xa = 1$, denn R ist kommutativ. Somit ist jedes $a \neq 0$ in R invertierbar, und es folgt, dass R ein Körper ist. □

Sei $(R, +, \cdot)$ ein Ring, und sei I ein Ideal in R. Da Ideale Normalteiler (vergleichen Sie bitte mit Definition 4.6.3 und Proposition 4.6.4) von $(R, +)$ sind, erhalten wir eine Klasseneinteilung auf R mit Nebenklassen $r + I = \{r + s \mid s \in I\}$ modulo I. Wir bezeichnen eine solche Nebenklasse mit $[r]$, also

$$[r] = \{r + s \mid s \in I\}.$$

5.2.7 Definition Sei R ein Ring, und sei I ein Ideal in R. Zwei Elemente $a, b \in R$ heißen **kongruent modulo** I, wenn sie in derselben Nebenklasse modulo I liegen. Sind a und b kongruent modulo I, so schreiben wir $a \equiv b (\mathrm{mod} I)$.

5.2.8 Aufgabe Sei R ein Ring, und sei I ein Ideal in R.

1. Seien $a, b \in R$. Beweisen Sie, dass $a \equiv b (\mathrm{mod} I)$ genau dann, wenn $a - b \in I$ gilt.
2. Sei $U \subseteq R^\times$ die Menge der Einheiten $a \in R^\times$ mit $a \equiv 1 (\mathrm{mod} I)$. Beweisen Sie, dass U ein Normalteiler von $R^\times$ ist.

5.2.9 Proposition (Rechenregeln für Kongruenzen)

Sei R ein Ring, und sei I ein Ideal in R. Seien $a, b, r, s \in R$. Dann gilt:

(a) Die folgenden Aussagen sind äquivalent:

(1) $[a] = [b]$.

(2) $a \equiv b (\mathrm{mod} I)$.

(3) $a - b \in I$.

(b) Wenn $a \equiv b(\mathrm{mod} I)$, so gilt

(1) $a + r \equiv b + r(\mathrm{mod} I)$.

(2) $ar \equiv br(\mathrm{mod} I)$.

(3) $na \equiv nb(\mathrm{mod} I)$ für alle $n \in \mathbb{Z}$.

(c) Wenn $a \equiv b(\mathrm{mod} I)$ und $r \equiv s(\mathrm{mod} I)$, so gilt

(1) $a + r \equiv b + s(\mathrm{mod} I)$.

(2) $ar \equiv bs(\mathrm{mod} I)$.

Beweis:

(a) Sei $[a] = [b]$. Da $a \in [a]$ und $b \in [b]$, folgt $a, b \in [a]$. Somit liegen a und b in derselben Nebenklasse modulo I, und es folgt $a \equiv b(\mathrm{mod} I)$, also (1)⇒(2).

Es gilt

$$\begin{array}{rcl} a \equiv b(\mathrm{mod} I) & \Leftrightarrow & \text{es gibt ein } x \in R \text{ mit } a, b \in [x] \\ & \Leftrightarrow & a = x + s \text{ und } b = x + s' \text{ für } s, s' \in I \\ & \Leftrightarrow & a - b = s - s' \in I. \end{array}$$

Insbesondere gilt (2)⇒(3).

Sei $a - b \in I$. Dann gilt $a = b + s$ für ein $s \in I$. Es folgt $a \in [b]$. Es gilt auch $a \in [a]$, und da Nebenklassen gleich oder disjunkt sind, folgt $[a] = [b]$, also (3)⇒(1).

(b) Sei $a \equiv b(\mathrm{mod} I)$, also $a - b \in I$ mit (a).

(1) Es ist $(a + r) - (b + r) = a - b \in I$. Mit (a) folgt $a + r \equiv b + r(\mathrm{mod} I)$.

(2) Es ist $ar - br = (a - b)r \in I$, denn $(a - b) \in I$ und I ist ein Ideal. Mit (a) folgt die Behauptung.

(3) Es ist $na - nb = n(a - b)$ und $a - b \in I$. Da $(I, +)$ eine Gruppe ist, folgt $n(a - b) \in I$. Wieder folgt mit (a) die Behauptung.

(c) Seien $a \equiv b(\mathrm{mod} I)$ und $r \equiv s(\mathrm{mod} I)$, also $a - b, r - s \in I$.

(1) Es gilt $(a+r)-(b+s) = (a-b)+(r-s) \in I$, denn $(I, +)$ ist eine Gruppe.

(2) Es gilt

$$\begin{array}{rcl} ar - bs & = & ar - bs - as + as \\ & = & a(r - s) + (a - b)s. \end{array}$$

Da I ein Ideal ist, folgt $a(r-s) \in I$ und $(a-b)s \in I$. Da $(I,+)$ eine Gruppe ist, gilt $a(r-s)+(a-b)s \in I$. Mit (a) folgt die Behauptung.

□

Sei R ein Ring, und sei $I \lhd R$. Sei R/I die Menge der Nebenklassen modulo I, also

$$R/I = \{[r] \mid r \in R\}.$$

Für zwei Nebenklassen $[a], [b] \in R/I$ definieren wir

$$[a]+[b] = [a+b] \text{ und } [a] \cdot [b] = [ab].$$

Wir zeigen, dass $+$ und $\cdot$ wohldefiniert sind. Dazu seien $[a] = [a']$ und $[b] = [b']$. Mit Proposition 5.2.9 (a) folgt $a \equiv a' (\mathrm{mod} I)$ und $b \equiv b' (\mathrm{mod} I)$. Mit Proposition 5.2.9 (c) gilt $a+b \equiv a'+b' (\mathrm{mod} I)$ und $ab \equiv a'b' (\mathrm{mod} I)$, also $[a+b] = [a'+b']$ und $[ab] = [a'b']$. Somit sind $+$ und $\cdot$ Verknüpfungen auf R/I. Ein Standardbeweis zeigt, dass R/I mit diesen Verknüpfungen ein Ring ist.

5.2.10 Definition Sei R ein Ring, und sei $I \lhd R$. Der Ring R/I wird **Faktorring von R modulo I** oder **Restklassenring von R modulo I** genannt.

In dem folgenden Beispiel werden wir den Ring $\mathbb{Z}/n\mathbb{Z}$ neu entdecken.

5.2.11 Beispiel Sei $R = \mathbb{Z}$, und sei $I = n\mathbb{Z}$ für ein $n \in \mathbb{N}$, $n > 1$. Wir haben in 5.2.4 gesehen, dass I ein Ideal in $\mathbb{Z}$ ist. Somit ist $\mathbb{Z}/n\mathbb{Z} = \{[a] \mid a \in \mathbb{Z}\}$. Weiter gilt $[a] = [a']$ genau dann, wenn $a - a' \in n\mathbb{Z}$, wenn also n ein Teiler von $a - a'$ ist.

Sei $[a] \in \mathbb{Z}/n\mathbb{Z}$. Wir dividieren a durch n mit Rest und erhalten

$$a = xn + a \,\mathrm{mod} n \text{ für ein } x \in \mathbb{Z},$$

also $a - a \,\mathrm{mod} n = xn \in n\mathbb{Z}$, und damit $[a] = [a \,\mathrm{mod} n]$. Es folgt

$$\mathbb{Z}/n\mathbb{Z} = \{[0], \ldots, [n-1]\}.$$

Seien $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$. Mit der Definition der Verknüpfungen in $\mathbb{Z}/n\mathbb{Z}$ folgt

$$[a]+[b] = [a+b] = [(a+b)\mathrm{mod} n] \text{ und } [a] \cdot [b] = [ab] = [(ab)\mathrm{mod} n].$$

Bis auf die Klammerschreibweise der Elemente in $\mathbb{Z}/n\mathbb{Z}$, die wir in den bisherigen Kapiteln nicht benutzt haben, liefert die Konstruktion der Bildung des Restklassenringes modulo einem Ideal also gerade den Ring $\mathbb{Z}/n\mathbb{Z}$, mit dem wir in den vorigen Kapiteln und in der Linearen Algebra I bereits gearbeitet haben.

5.3 Ringhomomorphismen

Wie bei Vektorräumen und Gruppen interessieren wir uns bei Ringen für strukturerhaltende Abbildungen zwischen Ringen.

5.3.1 Definition Seien R und R' Ringe. Eine Abbildung $\phi : R \to R'$ heißt ein **Ringhomomorphismus** oder kurz ein **Homomorphismus**, wenn für alle $r_1, r_2 \in R$ gilt:

(i) $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$, und

(ii) $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$, und

(iii) $\phi(1) = 1$.

Injektive Ringhomomorphismen werden **Monomorphismen** und surjektive **Epimorphismen** genannt. Ist $\phi : R \to R'$ ein bijektiver Ringhomomorphismus, so wird ϕ ein **Isomorphismus** genannt, und wir sagen, dass R und R' **isomorph** sind. Sind R und R' isomorph, so schreiben wir $R \simeq R'$. Ist ϕ ein Isomorphismus, und ist $R = R'$, so wird ϕ ein **Automorphismus** genannt.

5.3.2 Aufgabe Sei $\phi : R \to R'$ ein Ringhomomorphismus. Sei $\phi|_{R^\times} : R^\times \to R'$ definiert durch $\phi|_{R^\times}(r) = \phi(r)$ für alle $r \in R^\times$.

(a) Beweisen Sie, dass $\phi|_{R^\times}(r) \in R'^\times$ für alle $r \in R^\times$ ist.

(b) Beweisen Sie, dass $\phi|_{R^\times} : R^\times \to R'^\times$ ein Gruppenhomomorphismus ist.

Wenn $\phi : R \to R'$ ein Ringhomomorphismus ist, dann ist ϕ ein Gruppenhomomorphismus von $(R, +)$ nach $(R', +)$. Analog zu Kern und Bild von Gruppenhomomorphismen definieren wir Kern und Bild von Ringhomomorphismen:

5.3.3 Definition Sei $\phi : R \to R'$ ein Ringhomomorphismus. Das **Bild** und der **Kern** von ϕ sind folgende Teilmengen von R beziehungsweise R':

$$\text{Bild}(\phi) = \{r' \in R' \mid \text{ es gibt ein } r \in R \text{ mit } \phi(r) = r'\} \subseteq R'$$

$$\text{Kern}(\phi) = \{r \in R \mid \phi(r) = 0\} \subseteq R.$$

Völlig analog zu 4.5.7 gilt:

5.3.4 Proposition Sei $\phi : R \to R'$ ein Ringhomomorphismus. Dann gilt:

(a) Bild(ϕ) ist ein Unterring von R'.

(b) Kern(ϕ) ist ein Ideal in R.

(c) Der Homomorphismus ϕ ist genau dann injektiv, wenn Kern(ϕ) = $\{0\}$ ist.

Beweis:

(a) Da ϕ ein Gruppenhomomorphismus ist, ist (Bild(ϕ), +) mit 4.5.7 eine Untergruppe von $(R', +)$. Diese Gruppe ist auch abelsch, denn $(R', +)$ ist abelsch.

Seien $a', b' \in$ Bild(ϕ). Dann gibt es $a, b \in R$ mit $a' = \phi(a)$ und $b' = \phi(b)$. Es folgt

$$a'b' = \phi(a)\phi(b) = \phi(ab) \in \text{Bild}(\phi),$$

und dies zeigt, dass die Multiplikation eine Verknüpfung in Bild(ϕ) ist. Das Assoziativgesetz der Multiplikation gilt für alle Elemente in R', also gilt es insbesondere in Bild(ϕ). Da $\phi(1) = 1$, liegt das neutrale Element der Multiplikation in Bild(ϕ).

Die Distributivgesetze gelten in R', also insbesondere in Bild(ϕ).

Es folgt, dass Bild(ϕ) ein Unterring von R' ist.

(b) Mit Proposition 4.5.7 ist (Kern(ϕ), +) eine Untergruppe von $(R, +)$. Sei $a \in$ Kern(ϕ), und sei $r \in R$. Dann gilt $\phi(ar) = \phi(a)\phi(r) = 0 \cdot \phi(r) = 0$, also $ar \in$ Kern(ϕ). Analog folgt $ra \in$ Kern(ϕ). Somit ist Kern(ϕ) ein Ideal in R.

(c) Diese Behauptung ist gerade Proposition 4.5.7 (c).

□

Sei $\phi : R \to R'$ ein Ringhomomorphismus. Da Kern(ϕ) ein Ideal in R ist, können wir den Restklassenring $R/$Kern(ϕ) bilden.

Völlig analog zum Homomorphiesatz von Gruppen 4.6.7 gilt:

5.3.5 Satz (Homomorphiesatz für Ringe)

Sei $\phi : R \to R'$ ein Ringhomomorphismus. Dann ist $R/$Kern(ϕ) isomorph zu Bild(ϕ). Genauer, es ist

$$\begin{array}{rccc} \Phi: & R/\text{Kern}(\phi) & \to & \text{Bild}(\phi) \\ & [r] & \mapsto & \phi(r) \end{array}$$

ein Isomorphismus von Ringen.

Beweis:

1. Wir zeigen zunächst, dass Φ wohldefiniert ist. Dazu sei $[r] = [s]$. Mit den Rechenregeln für Kongruenzen, 5.2.9 (a), gilt $r - s \in \text{Kern}(\phi)$. Es folgt $\phi(r) - \phi(s) = \phi(r - s) = 0$, also $\phi(r) = \phi(s)$. Dies zeigt $\Phi([r]) = \Phi([s])$.

2. Wir zeigen nun, dass Φ ein Ringhomomorphismus ist. Dazu seien $[r], [s] \in R/\text{Kern}(\phi)$. Dann gilt

$$\Phi([r] + [s]) = \Phi([r + s]) = \phi(r + s) = \phi(r) + \phi(s) = \Phi([r]) + \Phi([s])$$

und

$$\Phi([r][s]) = \Phi([rs]) = \phi(rs) = \phi(r)\phi(s) = \Phi([r])\Phi([s])$$

und

$$\Phi([1]) = \phi(1) = 1.$$

Es folgt, dass Φ ein Homomorphismus ist.

3. Nun zeigen wir, dass Φ injektiv ist. Sei $[r] \in \text{Kern}(\Phi)$. Dann gilt $\phi(r) = 0$, also $r \in \text{Kern}(\phi)$. Somit gilt $r - 0 \in \text{Kern}(\phi)$, also $[r] = [0]$ mit den Rechenregeln für Kongruenzen 5.2.9 (a). Mit Proposition 5.3.4 folgt, dass Φ injektiv ist.

4. Sei $\phi(r) \in \text{Bild}(\phi)$. Dann ist $[r]$ ein Urbild von $\phi(r)$ unter Φ. Dies zeigt, dass Φ surjektiv ist.

□

Jedes Ideal ist der Kern eines Ringhomomorphismus, wie das folgende Ergebnis zeigt.

5.3.6 Proposition Sei R ein Ring und sei I ein Ideal in R. Sei

$$\pi : R \to R/I \text{ definiert durch } \pi(r) = [r] \text{ für alle } r \in R.$$

Dann ist π ein Epimorphismus, und $\text{Kern}(\pi) = I$.

Beweis: Dass π ein Homomorphismus ist, folgt unmittelbar aus der Definition der Addition und der Multiplikation von Elementen in R/I. Ebenfalls ist klar, dass π surjektiv, also ein Epimorphismus ist.

Sei $s \in I$. Dann gilt $\pi(s) = [s]$, und mit den Rechenregeln für Kongruenzen 5.2.9 (a) folgt $[s] = [0]$, denn $s - 0 \in I$. Es folgt $I \subseteq \text{Kern}(\pi)$. Sei umgekehrt $r \in \text{Kern}(\pi)$. Dann gilt $[r] = [0]$, also $r - 0 = r \in I$ mit den Rechenregeln für Kongruenzen 5.2.9 (a). Es folgt $\text{Kern}(\pi) \subseteq I$, und damit $\text{Kern}(\pi) = I$. □

5.3.7 Definition Sei R ein Ring und sei I ein Ideal in R. Sei

$$\pi : R \to R/I \text{ definiert durch } \pi(r) = [r] \text{ für alle } r \in R.$$

Dann wird π der **kanonische Epimorphismus** von R nach R/I genannt.

Wir werden in Proposition 5.3.9 das Ergebnis folgender Aufgabe benötigen:

5.3.8 Aufgabe Sei $\phi : R \to R'$ ein Epimorphismus, und sei $I \lhd R$ ein Ideal in R. Sei

$$\phi(I) = \{s' \in R' \mid \text{ es gibt ein } s \in I \text{ mit } \phi(s) = s'\}.$$

Beweisen Sie, dass $\phi(I)$ ein Ideal in R' ist.

5.3.9 Proposition Sei $\phi : R \to R'$ ein Epimorphismus, und sei $I \lhd R$ ein Ideal in R, das Kern(ϕ) enthält. Sei $I' = \phi(I)$. Dann ist

$$f : R/I \to R'/I', \text{ definiert durch } f([r]) = [\phi(r)] \text{ für alle } [r] \in R/I,$$

ein Isomorphismus von Ringen.

Beweis: Mit Aufgabe 5.3.8 ist I' ein Ideal in R', und wir können R'/I' bilden.

1. Wir zeigen, dass f wohldefiniert ist.

   Sei $[r] = [s]$, also $r - s \in I$. Es folgt $\phi(r - s) = \phi(r) - \phi(s) \in I'$, also $[\phi(r)] = [\phi(s)]$ mit den Rechenregeln für Kongruenzen 5.2.9 (a).

2. Wir zeigen nun, dass f ein Homomorphismus ist.

   Seien $r, s \in R$. Dann gilt

   $$\begin{aligned} f([r] + [s]) &= f([r + s]) \\ &= [\phi(r + s)] \\ &= [\phi(r) + \phi(s)] \\ &= [\phi(r)] + [\phi(s)] \\ &= f([r]) + f([s]). \end{aligned}$$

   Analog folgt $f([r][s]) = f([r])f([s])$. Es gilt $f([1]) = [\phi(1)] = [1]$, und dies zeigt, dass f ein Homomorphismus ist.

3. In diesem Schritt zeigen wir, dass f injektiv ist.

   Sei $[r] \in$ Kern(f), also $[\phi(r)] = [0]$. Dann gilt $\phi(r) = 0 + \phi(s)$ für ein $s \in I$. Es folgt

   $$\phi(r) - \phi(s) = \phi(r - s) = 0,$$

also $r - s \in \text{Kern}(\phi)$. Da $\text{Kern}(\phi) \subseteq I$, gilt damit $r - s \in I$. Mit den Rechenregeln für Kongruenzen 5.2.9 (a) folgt $[r] = [s] = [0]$, also $\text{Kern}(f) = \{[0]\}$. Proposition 5.3.4 impliziert, dass f injektiv ist.

4. Sei $[r'] \in R'/I'$. Da ϕ surjektiv ist, gibt es ein $r \in R$ mit $\phi(r) = r'$. Es folgt $[r'] = [\phi(r)]$, und $[r]$ ist ein Urbild von $[r']$ unter f.

□

Diese Proposition wird manchmal der „Erste Isomorphiesatz für Ringe“ genannt.

5.3.10 Aufgabe Sei R ein kommutativer Ring, und sei I ein Ideal in R. Sei $\mathrm{M}_{nn}(I)$ die Menge der $n \times n$-Matrizen, deren Einträge in I liegen. Sie haben in Aufgabe 5.2.5 gezeigt, dass $\mathrm{M}_{nn}(I)$ ein Ideal in $\mathrm{M}_{nn}(R)$ ist. Verwenden Sie den Homomorphiesatz für Ringe um zu zeigen, dass $\mathrm{M}_{nn}(R)/\mathrm{M}_{nn}(I)$ isomorph zu $\mathrm{M}_{nn}(R/I)$ ist.

5.4 Der Chinesische Restsatz

In diesem Abschnitt werden wir einen speziellen Isomorphismus für ganz spezielle Ringe konstruieren. Die Konstruktion ist etwa 2000 Jahre alt (bevor bekannt war, was ein Ring ist) und hat wichtige Anwendungen in der Computer Algebra. Wir werden am Ende des Abschnitts näher auf diesen Sachverhalt eingehen.

Wir haben im Abschnitt 4.9 in Satz 4.9.7 beziehungsweise in Korollar 4.9.8 gesehen, dass die Gruppe $\mathbb{Z}/n\mathbb{Z}$ isomorph zu $\prod_{i=1}^{r} \mathbb{Z}/p_i^{s_i}\mathbb{Z}$ ist, sofern $n = \prod_{i=1}^{r} p_i^{s_i}$, $p_i \neq p_j$ für $i \neq j$, die Primfaktorzerlegung von n ist. Allerdings war der Beweis des Satzes nicht konstruktiv, das heißt, wir haben keinen expliziten Isomorphismus von $\mathbb{Z}/n\mathbb{Z}$ nach $\prod_{i=1}^{r} \mathbb{Z}/p_i^{s_i}\mathbb{Z}$ angegeben. Wir werden das in diesem Kapitel nachholen, und darüberhinaus zeigen, dass $\mathbb{Z}/n\mathbb{Z}$ und $\prod_{i=1}^{r} \mathbb{Z}/p_i^{s_i}\mathbb{Z}$ als Ringe isomorph sind.

Dieses Ergebnis ist unter dem Namen „Chinesischer Restsatz“ bekannt.

Wenn Sie es vielleicht selbst einmal probieren wollen? Unser Ziel ist es, eine bijektive, strukturverträgliche Abbildung

$$\phi : \mathbb{Z}/n\mathbb{Z} \to (\mathbb{Z}/p_1^{s_1}\mathbb{Z}) \times (\mathbb{Z}/p_2^{s_2}\mathbb{Z}) \times \cdots \times (\mathbb{Z}/p_{r-1}^{s_{r-1}}\mathbb{Z}) \times (\mathbb{Z}/p_r^{s_r}\mathbb{Z})$$

zu definieren. Dazu müssen wir also jedem $x \in \{0, \ldots, n-1\}$ ein r-Tupel von Elementen in $\mathbb{Z}/p_1^{s_1}\mathbb{Z}, \ldots, \mathbb{Z}/p_r^{s_r}\mathbb{Z}$ zuordnen. Mit der Einstellung „Das Bild muss was mit x und den individuellen $\mathbb{Z}/p_i^{s_i}\mathbb{Z}$ zu tun haben“, werden Sie vermutlich

$$\phi(x) = (x \bmod p_1^{s_1}, x \bmod p_2^{s_2}, \ldots, x \bmod p_{r-1}^{s_{r-1}}, x \bmod p_r^{s_r})$$

vorschlagen. Und das ist auch richtig. Wir werden zunächst nur zeigen, dass ϕ surjektiv ist. Da $\mathbb{Z}/n\mathbb{Z}$ und $\prod_{i=1}^{r} \mathbb{Z}/p_i^{s_i}\mathbb{Z}$ gleich viele Elemente enthalten, folgt aus der Surjektivität schon die Bijektivität.

Wir beginnen mit einigen Vorbemerkungen. Stehende Annahme in diesem Abschnitt ist, dass $n = \prod_{i=1}^{r} p_i^{s_i}$, $p_i \neq p_j$ für $i \neq j$, die Primfaktorzerlegung von n ist. Für alle $1 \leq i \leq r$ sei $q_i = \prod_{\substack{j=1 \\ j \neq i}}^{r} p_j^{s_j}$.

5.4.1 Bemerkung Für alle $1 \leq i \leq r$ gilt $\mathrm{ggT}(q_i \bmod p_i^{s_i}, p_i^{s_i}) = 1$, insbesondere ist $q_i \bmod p_i^{s_i}$ in $\mathbb{Z}/p_i^{s_i}\mathbb{Z}$ invertierbar.

Beweis: Angenommen, $\mathrm{ggT}(q_i \bmod p_i^{s_i}, p_i^{s_i}) = d > 1$. Da $d | p_i^{s_i}$, folgt $p_i | d$. Sei

$$q_i = \prod_{\substack{j=1 \\ j \neq i}}^{r} p_j^{s_j} = x p_i^{s_i} + q_i \bmod p_i^{s_i}$$

mit $x \in \mathbb{Z}$. Da $p_i | q_i \bmod p_i^{s_i}$ und $p_i | p_i^{s_i}$, folgt $p_i | \prod_{\substack{j=1 \\ j \neq i}}^{r} p_j^{s_j}$, ein Widerspruch. Es folgt $d = 1$. Mit Korollar 2.4.12 folgt, dass $q_i \bmod p_i^{s_i}$ in $\mathbb{Z}/p_i^{s_i}\mathbb{Z}$ invertierbar ist. □

5.4.2 Notation Für alle $1 \leq i \leq r$ bezeichnen wir das zu $q_i \bmod p_i^{s_i}$ in $\mathbb{Z}/p_i^{s_i}\mathbb{Z}$ inverse Element mit r_i.

5.4.3 Bemerkung Für alle $i \neq j$ gilt $q_i \bmod p_j^{s_j} = 0$.

Beweis: Offenbar, denn q_i ist für alle $i \neq j$ ein Vielfaches von $p_j^{s_j}$. □

5.4.4 Satz (Chinesischer Restsatz)

Die Abbildung

$$\begin{array}{rccccccc} \phi: & \mathbb{Z}/n\mathbb{Z} & \to & \mathbb{Z}/p_1^{s_1}\mathbb{Z} & \times & \ldots & \times & \mathbb{Z}/p_r^{s_r}\mathbb{Z} \\ & x & \mapsto & (x \bmod p_1^{s_1} & , & \ldots & , & x \bmod p_r^{s_r}) \end{array}$$

ist bijektiv. Das Urbild eines Elementes $(x_1, \ldots, x_r) \in \prod_{i=1}^{r} \mathbb{Z}/p_i^{s_i}\mathbb{Z}$ unter ϕ ist $\left(\sum_{i=1}^{r} x_i q_i r_i\right) \bmod n$.

Beweis: Sei $(x_1, \ldots, x_r) \in \prod_{i=1}^{r} \mathbb{Z}/p_i^{s_i}\mathbb{Z}$, und sei $x = \left(\sum_{i=1}^{r} x_i r_i q_i\right) \bmod n$.

Wir untersuchen den k-ten Eintrag $x \bmod p_k^{s_k}$ von $\phi(x)$.

$$\begin{aligned} x \bmod p_k^{s_k} &= \left(\left(\sum_{i=1}^{r} x_i q_i r_i\right) \bmod n\right) \bmod p_k^{s_k} \\ &= \left(\left(\sum_{i=1}^{r} x_i q_i r_i\right) - tn\right) \bmod p_k^{s_k} \text{ für ein } t \in \mathbb{Z} \\ &= \left(\sum_{i=1}^{r} x_i q_i r_i\right) \bmod p_k^{s_k}, \text{ denn } p_k^{s_k} | n \\ &= \sum_{i=1}^{r} (x_i q_i r_i) \bmod p_k^{s_k} \\ &= x_k q_k r_k \bmod p_k^{s_k}, \text{ denn } q_i \bmod p_k^{s_k} = 0 \text{ für } i \neq k \\ &= x_k, \text{ denn } q_k r_k \bmod p_k^{s_k} = 1. \end{aligned}$$

Es folgt $\phi(x) = (x_1, \ldots, x_r)$, das heißt, ϕ ist surjektiv. Wie wir oben bereits überlegt haben, folgt, dass ϕ bijektiv ist. □

Wieso heißt der Chinesische Restsatz Chinesischer Restsatz? Erklären wir zunächst einmal den Begriff „Restsatz“. Nehmen wir an, wir hätten r verschiedene Primzahlen $p_1, \ldots p_r$ und r Reste $x_1 \bmod p_1^{s_1}, \ldots, x_r \bmod p_r^{s_r}$ gegeben. Wir können uns die

Frage stellen, ob es eine ganze Zahl x gibt, die beim Teilen durch $p_1^{s_1}, \ldots, p_r^{s_r}$ mit Rest die vorgegebenen Reste

$$x \mathrm{mod} p_1^{s_1} = x_1 \mathrm{mod} p_1^{s_1}, \ldots, x \mathrm{mod} p_r^{s_r} = x_r \mathrm{mod} p_r^{s_r}$$

besitzt. Der Chinesische Restsatz gibt eine Antwort auf diese Frage. Ja, genauer, es gibt genau ein $x \in \{0, \ldots, \prod_{i=1}^{r} p_i^{s_i} - 1\}$ mit dieser Eigenschaft. Und mit der in der Formulierung des Satzes genannten Formel für das Urbild von $(x_1, \ldots, x_r)$ unter ϕ können wir das x berechnen. Da das Verfahren, wie man ein solches x finden kann, bereits im ersten Jahrhundert unserer Zeitrechnung dem chinesischen Mathematiker Sun-Tsu bekannt war, wurde der Satz eben Chinesischer Restsatz genannt.

5.4.5 Aufgabe Bestimmen Sie die kleinste ganze Zahl x für die gilt:

$$\begin{aligned} x &\equiv 2 (\bmod 3) \\ x &\equiv 1 (\bmod 5) \\ x &\equiv 6 (\bmod 7). \end{aligned}$$

Woran Sun-Tsu sicher nicht im Traum gedacht hat, ist, dass der Chinesische Restsatz etwa 2000 Jahre später hoch aktuell in der Computeralgebra und Kryptografie werden würde. Und das liegt an Folgendem: Die im Chinesischen Restsatz angegebene Abbildung ist weit mehr als irgendeine Bijektion. Es gilt nämlich:

5.4.6 Proposition Sei $\phi : \mathbb{Z}/n\mathbb{Z} \to \prod_{i=1}^{r} \mathbb{Z}/p_i^{s_i}\mathbb{Z}$ die Abbildung wie im Chinesischen Restsatz. Dann gilt für alle $x, y \in \mathbb{Z}/n\mathbb{Z}$

$$\begin{aligned} \phi(x+y) &= \phi(x) + \phi(y) \text{ und} \\ \phi(xy) &= \phi(x)\phi(y) \text{ und} \\ \phi(1) &= 1, \end{aligned}$$

das heißt, ϕ ist ein Isomorphismus von Ringen.

Bevor wir dieses Ergebnis beweisen, wollen wir zunächst einmal klären, wieso dies so wichtige Folgerungen in der Computeralgebra hat.

Wenn wir mit dem Rechner $x + y$ oder xy mit $x, y \in \mathbb{Z}$ berechnen wollen, dann ist es völlig egal, ob wir diese Rechnung in $\mathbb{Z}$ durchführen oder in $\mathbb{Z}/n\mathbb{Z}$, so lange das Ergebnis kleiner als n ist. Wenn x und y, und damit n nun riesig groß sind, so kann es Zeit und Speicher sparender sein, die Rechnung auszulagern und viele kleinere

Rechnungen zu machen. Mit anderen Worten, wir können ein großes n, dessen Primfaktorzerlegung $n = \prod_{i=1}^{r} p_i^{s_i}$ wir kennen, wählen, und an Stelle von $x+y$ oder xy berechnen wir einfach $((x+y) \bmod p_1^{s_1}, \ldots, (x+y) \bmod p_r^{s_r})$ beziehungsweise $(xy \bmod p_1^{s_1}, \ldots, xy \bmod p_r^{s_r})$. Die einzelnen Einträge können sogar parallel berechnet werden. Der Chinesische Restsatz garantiert, dass wir das Ergebnis mit der im Satz angegebenen Formel wieder zusammensetzen können und das Ergebnis in $\mathbb{Z}/n\mathbb{Z}$ erhalten.

Beweis: (**Proposition 5.4.6)** Seien $x, y \in \mathbb{Z}/n\mathbb{Z}$. Dann gilt

$$\begin{aligned} \phi(x+y) &= ((x+y) \bmod p_1^{s_1}, \ldots, (x+y) \bmod p_r^{s_r}) \\ &= ((x \bmod p_1^{s_1} + y \bmod p_1^{s_1}) \bmod p_1^{s_1}, \ldots, (x \bmod p_r^{s_r} + y \bmod p_r^{s_r}) \bmod p_r^{s_r}) \end{aligned}$$

und

$$\begin{aligned} \phi(x) + \phi(y) &= (x \bmod p_1^{s_1}, \ldots, x \bmod p_r^{s_r}) + (y \bmod p_1^{s_1}, \ldots, y \bmod p_r^{s_r}) \\ &= ((x \bmod p_1^{s_1} + y \bmod p_1^{s_1}) \bmod p_1^{s_1}, \ldots, (x \bmod p_r^{s_r} + y \bmod p_r^{s_r}) \bmod p_r^{s_r}), \end{aligned}$$

also $\phi(x+y) = \phi(x) + \phi(y)$.

Analog wird gezeigt, dass auch $\phi(xy) = \phi(x)\phi(y)$ gilt.

Da $1 \bmod p_i^{s_i} = 1 \in \mathbb{Z}/p_i^{s_i}\mathbb{Z}$ für alle $1 \leq i \leq r$, folgt $\phi(1) = (1, \cdots, 1) = 1 \in \prod_{i=1}^{r} \mathbb{Z}/p_i^{s_i}\mathbb{Z}$. □

5.5 Der Primring eines Ringes

Wir werden den Homomorphiesatz für Ringe, Satz 5.3.5, dazu benutzen, den „kleinsten“ Unterring $P(R)$ eines Ringes R zu bestimmen. Dabei soll der kleinste Unterring bedeuten, dass $P(R)$ ein Ring ist, der in allen Unterringen von R enthalten ist. Zunächst einmal ist gar nicht klar, dass es immer einen Unterring von R gibt, der in allen Unterringen von R enthalten ist. Klar ist hingegen, dass ein Unterring mit dieser Eigenschaft eindeutig ist, falls er denn existiert. Denn seien S und S' Unterringe von R, die in allen Unterringen von R enthalten sind. Dann gilt $S \subseteq S'$ und $S' \subseteq S$, also $S = S'$.

Sei nun also $(R, +, \cdot)$ ein Ring. Um Verwirrungen zu vermeiden, bezeichnen wir das neutrale Element der Multiplikation in R mit e.

Wir definieren eine Abbildung $\phi : \mathbb{Z} \to R$ durch $\phi(n) = ne$ für alle $n \in \mathbb{Z}$. Hierbei benutzen wir die in 5.1.3 festgelegte Notation. Für alle $m, n \in \mathbb{Z}$ gilt dann

$$\phi(m+n) = (m+n)e = me + ne = \phi(m) + \phi(n)$$

und

$$\phi(mn) = (mn)e = (mn)e^2 = (me)(ne) = \phi(m)\phi(n).$$

Weiter gilt $\phi(1) = 1e = e$, und es folgt

5.5.1 Bemerkung Die Abbildung $\phi : \mathbb{Z} \to R$, definiert durch $\phi(n) = ne$ für alle $n \in \mathbb{Z}$, ist ein Homomorphismus von Ringen mit $\text{Bild}(\phi) = \mathbb{Z}e = \{ne \mid n \in \mathbb{Z}\}$. □

Mit Proposition 5.3.4 ist $\text{Bild}(\phi)$ ein Unterring von R. Sei S ein weiterer Unterring von R. Dann gilt $e \in S$, denn S enthält das neutrale Element der Multiplikation. Da $+$ eine Verknüpfung auf S ist, gilt $ne \in S$ für alle $n \in \mathbb{Z}$. Es folgt $\text{Bild}(\phi) = \mathbb{Z}e \subseteq S$. Wir haben also gezeigt:

5.5.2 Bemerkung Es ist $\mathbb{Z}e$ ein Unterring von R, und für alle Unterringe S von R gilt $\mathbb{Z}e \subseteq S$. □

Damit haben wir den kleinsten Unterring von R gefunden, und wir definieren:

5.5.3 Definition Sei R ein Ring, und sei e das neutrale Element der Multiplikation in R. Der Unterring $\mathbb{Z}e$ von R wird der **Primring** von R genannt und mit $P(R)$ bezeichnet.

Mit dem Homomorphiesatz für Ringe, Satz 5.3.5, gilt $\text{Bild}(\phi) = \mathbb{Z}e \simeq \mathbb{Z}/\text{Kern}(\phi)$. Weiter wissen wir mit Proposition 5.3.4, dass $\text{Kern}(\phi)$ ein Ideal in $\mathbb{Z}$ ist. Dies zeigt

5.5.4 Bemerkung Sei R ein Ring, und sei $P(R)$ der Primring von R. Dann gilt $P(R) \simeq \mathbb{Z}/I$, und I ist ein Ideal in $\mathbb{Z}$. □

Wie sehen nun die Ideale I in $\mathbb{Z}$ aus? Zunächst einmal haben wir die Ideale $\{0\}$ und $\mathbb{Z}$ in $\mathbb{Z}$. Weiter wissen wir, dass $(I, +)$ eine Untergruppe von $(\mathbb{Z}, +)$ ist. Da $\mathbb{Z}$ zyklisch ist, folgt mit Proposition 4.8.5, dass $(I, +)$ zyklisch ist. Sei I ein Ideal in $\mathbb{Z}$ mit $I \neq \{0\}$. Sei $k \in I$, $k \neq 0$. Mit k liegt auch $-k$ in I, und es folgt, dass I eine positive Zahl enthält. Sei m die kleinste positive Zahl in I. Dann gilt

$$(m) = \{mn \mid n \in \mathbb{Z}\} = m\mathbb{Z} \subseteq I.$$

Sei umgekehrt $z \in I$. Wir teilen z durch m mit Rest und erhalten $z = xm + r$ mit $x, r \in \mathbb{Z}$ und $0 \leq r < m$. Ist $r \neq 0$, so gilt $z - xm = r \in I$, ein Widerspruch, denn m war die kleinste positive Zahl in I. Somit gilt $z \in m\mathbb{Z}$, also $I = m\mathbb{Z}$. Ist $m = 1$, so ist $m\mathbb{Z} = \mathbb{Z}$. Wir haben hiermit gezeigt:

5.5.5 Bemerkung Die Ideale in $\mathbb{Z}$ sind $m\mathbb{Z}$ mit $m \geq 0$. □

Ist $I = \{0\}$, so ist $\mathbb{Z}/I$ isomorph zu $\mathbb{Z}$. Kombinieren wir nun die Bemerkungen 5.5.4 und 5.5.5, so erhalten wir:

5.5.6 Bemerkung Sei R ein Ring, und sei $P(R)$ der Primring von R. Dann gilt $P(R) \simeq \mathbb{Z}$ oder $P(R) \simeq \mathbb{Z}/m\mathbb{Z}$ für ein $m > 0$. □

Ist $R = \{0\}$, dann ist $P(R) = \{0\} = R \simeq \mathbb{Z}/1 \cdot \mathbb{Z}$. Wir betrachten also nun den Fall $R \neq 0$. Wie können wir dann entscheiden, welcher der beiden Fälle vorliegt? Hierzu betrachten wir den Isomorphismus

$$\begin{array}{rccc} \Phi: & \mathbb{Z}/\mathrm{Kern}(\phi) & \to & \mathrm{Bild}(\phi) = P(R) \\ & [n] & \mapsto & \phi(n) = ne \end{array}$$

aus dem Homomorphiesatz 5.3.5 für Ringe.

Ist $\mathrm{Kern}(\phi) = \{0\}$, also $\mathbb{Z}/\mathrm{Kern}(\phi) \simeq \mathbb{Z}$, so ist $\Phi([n]) = ne \neq 0$ für alle $n \in \mathbb{Z}$, $n \neq 0$, denn Φ ist injektiv.

Ist $\mathrm{Kern}(\phi) = m\mathbb{Z}$ für ein $m > 0$, so sind

$$\Phi([1]) = e \neq 0, \ldots, \Phi([m-1]) = (m-1)e \neq 0,$$

und es ist $\Phi([m]) = \Phi([0]) = 0$. Somit ist m die kleinste positive Zahl mit $me = 0$.

Fassen wir unsere Überlegungen zusammen, so erhalten wir:

5.5.7 Proposition (Klassifikation der Primringe)

Sei R ein Ring mit Primring $P(R)$, und sei e das neutrale Element der Multiplikation in R. Dann gilt $P(R) \simeq \mathbb{Z}$ oder $P(R) \simeq \mathbb{Z}/m\mathbb{Z}$ für ein $m > 0$.

(a) Ist $P(R) \simeq \mathbb{Z}$, so gilt $ne \neq 0$ für alle $n \neq 0$.

(b) Ist $P(R) \simeq \mathbb{Z}/m\mathbb{Z}$ für ein $m > 0$, so ist m die kleinste positive Zahl mit $me = 0$. □

5.5.8 Aufgabe Geben Sie ein Beispiel für einen Ring R, der unendlich viele Elemente enthält und dessen Primring endlich ist.

5.5.9 Korollar Sei R ein Ring mit Primring $P(R) \simeq \mathbb{Z}/m\mathbb{Z}$ für ein $m > 0$. Dann gilt $na = 0$ für alle $a \in R$ und alle Vielfachen n von m.

Beweis: Sei $n = xm$ für ein $x \in \mathbb{Z}$. Es ist $na = xma = x(me)a = x(0a) = x0 = 0$ für alle $a \in R$. □

5.5.10 Definition Sei R ein Ring mit Primring $P(R)$.

(i) Wenn $P(R) \simeq \mathbb{Z}$ ist, dann sagen wir, dass R die **Charakteristik** 0 hat und schreiben $\text{char}(R) = 0$.

(ii) Wenn $P(R) \simeq \mathbb{Z}/m\mathbb{Z}$ für ein $m > 1$ ist, dann sagen wir, dass R die **Charakteristik** m hat, beziehungsweise, dass R **positive Charakteristik** hat, und schreiben $\text{char}(R) = m$.

Für den Ring $R = \{0\}$ ist keine Charakteristik definiert.

5.5.11 Proposition Sei R ein Integritätsbereich mit $\text{char}(R) = m > 0$. Dann ist m eine Primzahl.

Beweis: Da Integritätsbereiche Elemente $\neq 0$ enthalten (vergleichen Sie mit Definition 5.1.5), ist $m \geq 2$. Angenommen, m ist keine Primzahl. Dann gibt es $s > 1$ und $t > 1$ in $\mathbb{N}$ mit $m = st$, und es sind $s < m$ und $t < m$. Sei e das neutrale Element der Multiplikation in R. Dann gilt

$$0 = me = (st)e = (se)(te).$$

Da R ein Integritätsbereich ist, folgt $se = 0$ oder $te = 0$. Dies ist ein Widerspruch, denn m ist die kleinste positive Zahl mit $me = 0$. □

Da Körper Integritätsbereiche sind, folgt

5.5.12 Korollar Sei $\mathbb{K}$ ein Körper mit $\text{char}(\mathbb{K}) = m > 0$. Dann ist m eine Primzahl. □

5.5.13 Korollar Die Charakteristik eines endlichen Körpers $\mathbb{K}$ ist eine Primzahl.

Beweis: Mit Korollar 5.5.12 reicht es zu zeigen, dass endliche Körper eine positive Charakteristik haben. Wir betrachten die Elemente $e, 2e, \ldots$. Da $\mathbb{K}$ nur endlich viele Elemente enthält, gibt es positive Zahlen k und m mit $k < m$ und $ke = me$. Es folgt $me - ke = (m - k)e = 0$ und $m - k \neq 0$. Mit Proposition 5.5.7 folgt $\text{char}(\mathbb{K}) \neq 0$. □

Nicht jeder Ring hat Primzahl-Charakteristik. Beispielsweise ist 6 die Charakteristik von $\mathbb{Z}/6\mathbb{Z}$.

5.5.14 Aufgabe Ein Ring R heißt **einfach**, falls $R \neq \{0\}$, und falls $\{0\}$ und R die einzigen Ideale in R sind. Beweisen Sie, dass einfache kommutative Ringe die Charakteristik 0 oder p haben, wobei p eine Primzahl ist.

Sei $\mathbb{K}$ ein endlicher Körper. Der Primring $P(\mathbb{K})$ ist mit Korollar 5.5.13 ein Körper mit p Elementen, p eine Primzahl. Damit ist $\mathbb{K}$ ein Vektorraum über $P(\mathbb{K})$. Da $\mathbb{K}$ nur endlich viele Elemente enthält, ist die Dimension von $\mathbb{K}$ über $P(\mathbb{K})$ endlich, etwa $\dim_{P(\mathbb{K})}(\mathbb{K}) = n$. Es gibt also $b_1, \ldots, b_n \in \mathbb{K}$, so dass jedes Element $b \in \mathbb{K}$ eindeutig in der Form $b = a_1 b_1 + \cdots + a_n b_n$ mit $a_1, \ldots, a_n \in P(\mathbb{K})$ geschrieben werden kann. Für jedes a_i haben wir p Möglichkeiten, und es folgt

5.5.15 Satz (Ordnung endlicher Körper)

Ein endlicher Körper hat p^n Elemente, wobei p eine Primzahl und $n \in \mathbb{N}$ ist. □

Insbesondere gibt es keine Körper mit 15 Elementen, denn 15 ist keine Primzahlpotenz. Bisher kennen Sie nur endliche Körper mit p Elementen, nämlich die Körper $\mathbb{Z}/p\mathbb{Z}$, p eine Primzahl. Wir werden in Kurseinheit 5 zeigen, dass es zu jeder Primzahl p und jeder natürlichen Zahl n einen Körper mit p^n Elementen gibt.

In kommutativen Ringen R mit $\mathrm{char}(R) = p$, p eine Primzahl, kann man die binomische Formel so einfach ausrechnen – jedenfalls für p-Potenzen – wie man es sich immer wünscht. Zunächst aber eine Erinnerung an die Lineare Algebra. Sie haben in der Linearen Algebra II, Kurseinheit 3, folgendes Ergebnis kennengelernt:

5.5.16 Satz (Binomische Formel)

Sei R ein Ring, und seien $a, b \in R$ zwei Ringelemente, für die $ab = ba$ gilt. Sei $n \in \mathbb{N}_0$. Dann gilt

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k}.$$

□

Dabei bezeichnet $\binom{n}{k}$ den so genannten Binomialkoeffizienten, also $\binom{n}{k} = \dfrac{n!}{k!(n-k)!}$ für alle $0 \leq k \leq n$ und $\binom{n}{k} = 0$ für alle $k > n$. Es sind $0! = 1$ und $n! = n(n-1)\cdots 2 \cdot 1$ für alle $n \in \mathbb{N}$. Mit der binomischen Formel, Satz 5.5.16, folgt

5.5.17 Proposition Sei R ein kommutativer Ring der Charakteristik $p > 0$, und sei p eine Primzahl. Dann gilt

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}$$

für alle $a, b \in R$ und alle $n \in \mathbb{N}$.

Beweis: Wir beweisen die Behauptung mit Induktion nach n. Sei $n = 1$. Da $ab = ba$ für alle $a, b \in R$, können wir die binomische Formel anwenden, und es gilt

$$(a+b)^p = a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k b^{p-k} + b^p.$$

Es ist $\binom{p}{k} k!(p-k)! = p!$, und für $1 \leq k \leq p-1$ sind weder $k!$ noch $(p-k)!$ durch p teilbar. Da $p!$ durch p teilbar ist, folgt, dass $\binom{p}{k}$ durch p teilbar ist. Mit Korollar 5.5.9 gilt $\binom{p}{k} a^k b^{p-k} = 0$ für alle $1 \leq k \leq p-1$, und es folgt die Behauptung. Sei nun $n \geq 1$. Dann gilt

$$(a+b)^{p^{n+1}} = \left((a+b)^{p^n}\right)^p = (a^{p^n} + b^{p^n})^p = a^{p^{n+1}} + b^{p^{n+1}}.$$

□

5.5.18 Aufgabe Sei R ein kommutativer Ring der Charakteristik $p > 0$. Seien $a_1, \ldots, a_m \in R$. Beweisen Sie, dass

$$(a_1 + \cdots + a_m)^{p^n} = a_1^{p^n} + \cdots + a_m^{p^n}$$

für alle $m, n \in \mathbb{N}$ gilt.

5.5.19 Korollar Wenn $\mathbb{K}$ ein endlicher Körper der Charakteristik $p > 0$ ist, dann ist die Abbildung $\sigma : \mathbb{K} \to \mathbb{K}$, definiert durch $\sigma(a) = a^p$ für alle $a \in \mathbb{K}$, ein Automorphismus.

Beweis: Mit Proposition 5.5.17 gilt $\sigma(a+b) = (a+b)^p = a^p + b^p = \sigma(a) + \sigma(b)$ für alle $a, b \in \mathbb{K}$. Es gilt auch $\sigma(ab) = (ab)^p = a^p b^p = \sigma(a)\sigma(b)$ und $\sigma(1) = 1^p = 1$. Somit ist σ ein Homomorphismus. Es ist $\mathrm{Kern}(\sigma) = \{0\}$, und es folgt, dass σ injektiv ist. Da $\mathbb{K}$ endlich ist, folgt, dass σ auch surjektiv, also ein Automorphismus ist. □

Der Automorphismus σ aus Korollar 5.5.19 wird zu Ehren des Mathematikers Ferdinand Georg Frobenius (1849 – 1917) auch **Frobenius Automorphismus** genannt.

5.6 Ideale in kommutativen Ringen

In diesem Abschnitt sei R ein kommutativer Ring. Wir werden spezielle Ideale in R betrachten, die wir in Kurseinheit 5 für die Konstruktion der endlichen Körper benötigen werden.

5.6.1 Definition Sei R ein kommutativer Ring. Ein Element $a \in R$ heißt **Teiler** eines Elementes $b \in R$, wenn es ein $c \in R$ gibt, so dass $ac = b$ ist. Zwei Elemente $a, b \in R$ heißen **assoziiert**, wenn es eine Einheit $\epsilon \in R^\times$ gibt, so dass $a = b\epsilon$ ist. Ein Element $c \in R$ heißt **Primelement**, wenn c keine Einheit ist, und wenn c nur die Einheiten und die zu c assoziierten Elemente als Teiler besitzt.

5.6.2 Beispiel Sei $R = \mathbb{Z}$. Die Einheiten in $\mathbb{Z}$ sind 1 und -1. Somit sind a und b in $\mathbb{Z}$ genau dann assoziiert, wenn sie gleich sind oder sich nur durch das Vorzeichen unterscheiden. Die Primelemente in $\mathbb{Z}$ sind die Primzahlen und die Negativen der Primzahlen.

5.6.3 Definition Sei R ein kommutativer Ring. Ein Ideal $P \neq R$ in R heißt **Primideal**, wenn für alle $a, b \in R$ mit $ab \in P$ folgt, dass a oder b in P liegen.

5.6.4 Beispiele (a) Sei $R = \mathbb{Z}$. Dann ist $\{0\}$ ein Primideal in $\mathbb{Z}$, denn $\mathbb{Z}$ ist ein Integritätsbereich.

(b) Sei $R = \mathbb{Z}$, und sei $p \in \mathbb{Z}$ eine Primzahl. Sei $P = p\mathbb{Z} = \{pz \mid z \in \mathbb{Z}\}$. Dann ist P ein Primideal, denn wenn $a, b \in \mathbb{Z}$ und $ab \in P$, so gilt $p|ab$, und es folgt $p|a$ oder $p|b$. Im ersten Fall liegt a in P, im zweiten Fall gilt $b \in P$.

(c) Sei $R = \mathbb{Z}$, und seien $a \neq 0$ und $b \neq 0$ Elemente in $\mathbb{Z}$, die beide keine Einheiten sind. Sei $n = ab$. Dann ist $I = n\mathbb{Z}$ kein Primideal, denn $ab \in I$, aber $a \notin I$ und $b \notin I$.

5.6.5 Definition Sei R ein kommutativer Ring. Ein Ideal $M \neq R$ in R heißt **maximales** Ideal, wenn für jedes Ideal I in R mit $M \subseteq I$ folgt, dass $M = I$ oder $I = R$ ist.

5.6.6 Aufgabe Sei $R = \mathbb{Z}$, und seien $m\mathbb{Z}$ und $n\mathbb{Z}$ Ideale in $\mathbb{Z}$. Beweisen Sie:

1. Genau dann gilt $m\mathbb{Z} \subseteq n\mathbb{Z}$, wenn n ein Teiler von m ist.
2. Genau dann gilt $m\mathbb{Z} = n\mathbb{Z}$, wenn m und n assoziiert sind.
3. Genau dann ist $n\mathbb{Z}$ ein maximales Ideal, wenn n ein Primelement in $\mathbb{Z}$ ist.

5.6.7 Aufgabe Geben Sie ein Beispiel für ein Primideal, das nicht maximal ist.

5.6.8 Definition Sei R ein kommutativer Ring. Ein Ideal I in R heißt **Hauptideal**, wenn es ein $a \in I$ gibt, so dass $I = (a) = \{ar \mid r \in R\}$ ist. Ein Ring R heißt **Hauptidealring**, wenn R ein Integritätsbereich ist, und wenn alle Ideale in R Hauptideale sind.

5.6.9 Beispiel Mit Bemerkung 5.5.5 sind die Ideale in $\mathbb{Z}$ von der Form $n\mathbb{Z}$, $n > 0$ und $\{0\} = 0\mathbb{Z}$. Somit ist $\mathbb{Z}$ ein Hauptidealring.

5.6.10 Satz (Faktorringe von kommutativen Ringen)

Sei R ein kommutativer Ring. Dann gilt:

(a) Ein Ideal M in R ist genau dann maximal, wenn R/M ein Körper ist.

(b) Ein Ideal P in R ist genau dann ein Primideal, wenn R/P ein Integritätsbereich ist.

(c) Jedes maximale Ideal in R ist ein Primideal.

(d) Wenn R ein Hauptidealring ist, der kein Körper ist, so ist $R/(c)$ genau dann ein Körper, wenn c ein Primelement in R ist.

Beweis:

(a) Sei M ein maximales Ideal in R. Wir müssen zeigen, dass jedes Element $[a] \neq [0]$ in R/M invertierbar ist. Mit den Rechenregeln für Kongruenzen, 5.2.9 (a), ist $[a] \neq [0]$ genau dann, wenn $a \notin M$. Da $M \neq R$ gibt es Elemente $a \notin M$. Sei also $a \notin M$. Sei

$$I = \{ar + m \mid r \in R \text{ und } m \in M\}.$$

Das Ideal M ist in I enthalten. Wir zeigen, dass I ein Ideal in R ist. Mit dem Untergruppenkriterium, 4.2.4, ist $(I, +)$ eine Untergruppe von $(R, +)$. Seien $ar + m \in I$ und $b \in R$. Dann gilt $(ar + m)b = a(br) + mb$, denn R ist kommutativ. Da M ein Ideal ist, gilt $mb \in M$. Es folgt, dass $(ar + m)b \in I$, und analog $b(ar + m) \in I$. Somit ist I ein Ideal. Das Ideal I enthält a. Da $a \notin M$, ist M in I echt enthalten. Da M maximal ist, folgt $I = R$. Jedes Element in R, also auch das Element 1, hat damit eine Darstellung der Form $ar + m$ mit $r \in R$ und $m \in M$. Sei also $ar + m = 1$ für gewisse $r \in R$ und $m \in M$. Dann gilt

$$[a][r] = (a+M)(r+M) = ar+M = (1-m)+M = (1+M)-(m+M) = 1+M = [1],$$

und es folgt, dass $[a]$ invertierbar ist. Somit ist R/M ein Körper.

Sei umgekehrt R/M ein Körper. Sei I ein Ideal in R, welches M echt enthält. Sei $a \in I$, $a \notin M$. Dann ist $[a] \neq [0]$, und es folgt, dass es ein $r \in R$ mit $[a][r] = ar + M = 1 + M$ gibt. Es folgt $ar + m = 1$ für ein $m \in M$. Da $a \in I$ und $m \in I$, gilt $ar + m \in I$, also $1 \in I$. Es folgt $(1) = R \subseteq I$, also $I = R$. Somit ist M ein maximales Ideal in R.

(b) Sei P ein Primideal in R. Da $P \neq R$, gilt $1 \notin P$, also mit den Rechenregeln für Kongruenzen, 5.2.9 (a), $[1] \neq [0] \in R/P$. Seien $[a][b] = [0]$ in R/P, also $ab \in P$. Dann gilt $a \in P$ oder $b \in P$, und damit $[a] = [0]$ oder $[b] = [0]$ in R/P. Somit ist R/P ein Integritätsbereich.

Sei umgekehrt R/P ein Integritätsbereich. Sei $ab \in P$. Dann gilt $[0] = [ab] = [a][b]$, und es folgt $a \in P$ oder $b \in P$. Somit ist P ein Primideal.

(c) Diese Behauptung folgt aus (a) und (b), denn jeder Körper ist ein Integritätsbereich.

(d) Sei R ein Hauptidealring, der kein Körper ist.

Sei (c) ein Ideal in R, und sei $R/(c)$ ein Körper. Wenn c eine Einheit in R ist, so gilt $1 \in (c)$, also $(c) = R$, ein Widerspruch. Somit ist c keine Einheit in R. Es kann auch nicht $c = 0$, sein, denn $R/(0) \simeq R$ ist kein Körper. Wenn c weder eine Einheit, noch das Nullelement noch ein Primelement in R ist, so gibt es einen Teiler a von c, der weder eine Einheit noch assoziiert zu c ist und für den $a \neq 0$ gilt. Wir schreiben $c = ab$ mit $b \in R$. Angenommen, $a \in (c)$. Dann gibt es ein $d \in R$ mit $a = cd = abd$, also $a(1 - bd) = 0$. Da Hauptidealringe Integritätsbereiche sind, folgt $1 - bd = 0$, also $bd = 1$. Es folgt, dass d eine Einheit ist, ein Widerspruch, denn dann sind $a = cd$ und c assoziiert. Dieser Widerspruch zeigt $a \notin (c)$. Es folgt $(c) \subsetneq (a)$. Da a keine Einheit in R ist, gilt auch $(a) \subsetneq R$. Somit ist (c) nicht maximal. Dies ist ein Widerspruch, denn mit (a) ist $R/(c)$ kein Körper. Der Widerspruch zeigt, dass c ein Primelement ist.

Sei umgekehrt c ein Primelement in R. Da c keine Einheit ist, gilt $(c) \neq R$. Sei I ein Ideal, das (c) enthält. Da R ein Hauptidealring ist, folgt $I = (a)$ für ein $a \in R$. Es folgt $c \in (a)$, das heißt, a ist ein Teiler von c. Somit ist a eine Einheit, und damit $(a) = R$, oder a ist assoziiert zu c, also $I = (c)$. Dies zeigt, dass (c) ein maximales Ideal ist, und mit (a) folgt die Behauptung.

□

Als Folgerung etwas, das wir seit grauer Vorzeit schon wissen:

5.6.11 Korollar Sei $n \in \mathbb{Z}$. Genau dann ist $\mathbb{Z}/n\mathbb{Z}$ ein Körper, wenn n assoziiert zu einer Primzahl ist.

Beweis: Die Primelemente in $\mathbb{Z}$ sind die Assoziierten der Primzahlen. Die Behauptung folgt nun mit 5.6.10 (d). □

5.7 Der Ring $\mathbb{K}[T]$

In Kurseinheit 2 der Linearen Algebra II haben Sie bereits Polynomringe über Ringen kennen gelernt. Wir werden in der Kryptologie vornehmlich an Polynomringen über Körpern interessiert sein. Faktorringe von Polynomringen über endlichen Körpern $\mathbb{Z}/p\mathbb{Z}$, p eine Primzahl, spielen eine zentrale Rolle bei der Konstruktion der endlichen Körper, die nicht von der Form $\mathbb{Z}/p\mathbb{Z}$ sind. In Kurseinheit 1 der Linearen Algebra II haben wir Polynomringe über Körpern im Zusammenhang mit dem charakteristischen Polynom studiert. Viele der dort hergeleiteten Ergebnisse werden wir auch hier benötigen, und wir werden, ohne Beweis, einige der Resultate wiederholen.

Zunächst erinnern wir an einige Begriffe.

5.7.1 Definition Sei R ein Ring, und sei $f = \sum_{i=0}^{n} a_i T^i \in R[T]$ ein Polynom, das nicht das Nullpolynom ist. Wir können annehmen, dass $a_n \neq 0$ ist. Dann wird a_n der **Leitkoeffizient** von f und a_0 der **konstante Term** von f genannt. Die Zahl n heißt der **Grad** von f, abgekürzt $\mathrm{Grad}(f) = n$. Den Grad des Nullpolynoms definieren wir als $-\infty$. Polynome vom Grad ≤ 0 werden **konstante** Polynome genannt. Ist $a_n = 1$, so sagen wir, dass das Polynom f **normiert** ist.

Sei $\mathbb{K}$ ein Körper. Dann ist $\mathbb{K}[T]$ ein Integritätsbereich, und $\mathbb{K}[T]^\times = \mathbb{K}^\times$. Die invertierbaren Elemente in $\mathbb{K}[T]$ sind also die Polynome vom Grad 0.

Wir erinnern an die Division mit Rest in $\mathbb{K}[T]$:

5.7.2 Proposition (Division mit Rest in $\mathbb{K}[T]$)

Zu Polynomen $f, g \in \mathbb{K}[T]$ mit $f \neq 0$ gibt es eindeutig bestimmte Polynome $q, r \in \mathbb{K}[T]$ mit

$$g = qf + r \quad \text{und} \quad \mathrm{Grad}(r) < \mathrm{Grad}(f).$$

Beweis: Lineare Algebra II, Kurseinheit 1. □

Diese Proposition impliziert, dass jedes Ideal in $\mathbb{K}[T]$ ein Hauptideal ist:

5.7.3 Proposition Der Ring $\mathbb{K}[T]$ ist ein Hauptidealring. Genauer, ist $I \neq (0)$ ein Ideal in $\mathbb{K}[T]$, so gibt es ein eindeutig bestimmtes, normiertes Polynom $g \in \mathbb{K}[T]$ mit $I = (g)$.

Beweis: Wir wissen bereits, dass $\mathbb{K}[T]$ ein Integritätsbereich ist. Sei $I \neq (0)$ ein Ideal in $\mathbb{K}[T]$. Sei $h \neq 0$ ein Polynom vom kleinsten Grad in I, und sei b der Leitkoeffizient von h. Dann ist $b^{-1}h = g$ ein normiertes Polynom in I und $\mathrm{Grad}(h) = \mathrm{Grad}(g)$. Sei f ein beliebiges Polynom in I. Wir teilen f durch g mit Rest und erhalten $f = qg + r$ mit $\mathrm{Grad}(r) < \mathrm{Grad}(g)$. Da I ein Ideal ist, gilt $f - qg = r \in I$. Da $h \neq 0$ ein Polynom vom kleinsten Grad in I ist, folgt $r = 0$, also $I = (g)$. Sei $g' \in I$ ein weiteres normiertes Polynom mit $I = (g')$. Dann gilt $g' = c_1 g$ und $g = c_2 g'$. Es folgt $g' = c_1 c_2 g'$, also $c_1 c_2 = 1$, und c_1, c_2 sind konstant. Da g' und g normiert sind, folgt $g = g'$. □

5.7.4 Satz Seien $f_1, \ldots, f_n$ Polynome in $\mathbb{K}[T]$, die nicht alle 0 sind. Dann gibt es ein eindeutig bestimmtes, normiertes Polynom $d \in \mathbb{K}[T]$ mit folgenden Eigenschaften:

(i) d teilt f_i für alle $1 \leq i \leq n$, und

(ii) jedes Polynom $c \in \mathbb{K}[T]$, das alle f_i, $1 \leq i \leq n$, teilt, ist auch ein Teiler von d.

Das Polynom d kann in der Form

$$d = b_1 f_1 + \cdots + b_n f_n \text{ mit } b_1, \ldots, b_n \in \mathbb{K}[T]$$

geschrieben werden.

Beweis: Sei $I = \{c_1 f_1 + \cdots + c_n f_n \mid c_1, \ldots, c_n \in \mathbb{K}[T]\}$. Dann ist I ein Ideal in $\mathbb{K}[T]$. Da nicht alle f_i das Nullpolynom sind, ist $I \neq (0)$. Mit Proposition 5.7.3 folgt, dass es ein eindeutig bestimmtes normiertes Polynom $d \in \mathbb{K}[T]$ gibt, so dass $I = (d)$ ist. Dieses Polynom d hat die Eigenschaft (i) der Behauptung, und es gilt $d = b_1 f_1 + \cdots + b_n f_n$ für gewisse $b_1, \ldots, b_n \in \mathbb{K}[T]$. Wenn c jedes Polynom f_i, $1 \leq i \leq n$ teilt, so teilt c auch $d = b_1 f_1 + \cdots + b_n f_n$. Es bleibt zu zeigen, dass d eindeutig ist. Sei d_1 ein weiteres normiertes Polynom mit den Eigenschaften (i) und (ii). Es folgt $d | d_1$ und $d_1 | d$, also $(d) = (d_1) = I$. Mit Proposition 5.7.3 folgt $d = d_1$. □

5.7.5 Definition Seien $f_1, \ldots, f_n$ und d in $\mathbb{K}[T]$ wie in Satz 5.7.4. Dann wird d **größter gemeinsamer Teiler** von $f_1, \ldots, f_n$ genannt und mit $\mathrm{ggT}(f_1, \ldots, f_n)$ bezeichnet. Ist $\mathrm{ggT}(f_1, \ldots, f_n) = 1$, so sagt man, dass $f_1, \ldots, f_n$ **teilerfremd** sind. Sie werden **paarweise teilerfremd** genannt, wenn $\mathrm{ggT}(f_i, f_j) = 1$ ist für alle $1 \leq i, j \leq n$ und $i \neq j$.

Sie haben in der Linearen Algebra II, Kurseinheit 1, gesehen, dass der größte gemeinsame Teiler von zwei Polynomen $f, g \in \mathbb{K}[T]$ mit Hilfe des Euklidischen Algorithmus berechnet werden kann.

Dazu seien $f, g \in \mathbb{K}[T]$. Wir können voraussetzen, dass $g \neq 0$, und dass g kein Teiler von f ist. Wir benutzen wiederholte Division mit Rest und erhalten

$$\begin{array}{lcll} f & = & q_1 g + r_1 & 0 \leq \mathrm{Grad}(r_1) < \mathrm{Grad}(g) \\ g & = & q_2 r_1 + r_2 & 0 \leq \mathrm{Grad}(r_2) < \mathrm{Grad}(r_1) \\ r_1 & = & q_3 r_2 + r_3 & 0 \leq \mathrm{Grad}(r_3) < \mathrm{Grad}(r_2) \\ & \vdots & & \\ r_{s-2} & = & q_s r_{s-1} + r_s & 0 \leq \mathrm{Grad}(r_s) < \mathrm{Grad}(r_{s-1}) \\ r_{s-1} & = & q_{s+1} r_s. & \end{array}$$

Dabei sind $q_1, \ldots, q_{s+1}$ und $r_1, \ldots, r_s$ Polynome in $\mathbb{K}[T]$. Da der Grad von g endlich ist, muss der Prozess des wiederholten Teilens mit Rest abbrechen. Wenn r_s, der kleinste Rest $\neq 0$, den Leitkoeffizienten b hat, so ist $\mathrm{ggT}(f, g) = b^{-1} r_s$. Um den größten gemeinsamen Teiler von $f_1, \ldots, f_n$ mit $n > 2$ zu bestimmen, berechnet man zunächst $\mathrm{ggT}(f_1, f_2)$, dann $\mathrm{ggT}(\mathrm{ggT}(f_1, f_2), f_3)$, und so weiter.

5.7.6 Aufgabe Berechnen Sie den größten gemeinsamen Teiler von $f = 2T^6 + T^3 + T^2 + 2 \in \mathbb{F}_3[T]$ und $g = T^4 + T^2 + 2T \in \mathbb{F}_3[T]$.

Den Gegenpart zum größten gemeinsamen Teiler von Polynomen $f_1, \ldots, f_n$ in $\mathbb{K}[T]$ spielt das kleinste gemeinsame Vielfache von $f_1, \ldots, f_n$.

5.7.7 Proposition Seien $f_1, \ldots, f_n$ Polynome $\neq 0$ in $\mathbb{K}[T]$. Dann gibt es ein eindeutig bestimmtes normiertes Polynom $h \in \mathbb{K}[T]$, so dass gilt:

(i) h ist Vielfaches von jedem f_i, $1 \leq$i$\leq n$, und

(ii) wenn $b \in \mathbb{K}[T]$ ein Vielfaches von allen f_i, $1 \leq i \leq n$, ist, dann ist b Vielfaches von h.

Beweis: Sei $I = (f_1) \cap \cdots \cap (f_n)$. Mit Aufgabe 5.2.5 ist der Durchschnitt von Idealen ein Ideal, und es folgt, dass I ein Ideal in $\mathbb{K}[T]$ ist. Es gibt also ein eindeutig

bestimmtes normiertes Polynom h mit $(f_1) \cap \cdots \cap (f_n) = (h)$. Da $h \in (f_i)$ für alle $1 \leq i \leq n$, ist h ein Vielfaches aller f_i. Jedes weitere gemeinsame Vielfache h' aller f_i liegt in $I = (h)$, ist also ein Vielfaches von h. □

5.7.8 Definition Seien $f_1, \ldots, f_n$ und h wie in Proposition 5.7.7. Dann wird h das **kleinste gemeinsame Vielfache** von $f_1, \ldots, f_n$ genannt und mit $\mathrm{kgV}(f_1 \ldots, f_n)$ bezeichnet.

Die Primelemente in $\mathbb{K}[T]$ werden irreduzible Elemente genannt. Weil dieser Begriff so wichtig ist, wiederholen wir die Definition.

5.7.9 Definition Ein Polynom $p \in \mathbb{K}[T]$ heißt **irreduzibel über** $\mathbb{K}$ oder **irreduzibel in** $\mathbb{K}[T]$ oder **Primelement in** $\mathbb{K}[T]$, wenn $\mathrm{Grad}(p) > 0$, und wenn $p = ab$ mit $a, b \in \mathbb{K}[T]$ impliziert, dass a oder b konstant sind. Ein Polynom von positivem Grad, das nicht irreduzibel ist, wird reduzibel genannt.

Ob ein Polynom irreduzibel ist oder nicht hängt ganz entscheidend von dem Körper $\mathbb{K}$ ab. Beispielsweise ist T^2-2 irreduzibel in $\mathbb{Q}[T]$, aber $T^2-2 = (T+\sqrt{2})(T-\sqrt{2})$ ist reduzibel in $\mathbb{R}[T]$.

Normierte irreduzible Polynome spielen in $\mathbb{K}[T]$ in etwa die Rolle, die Primzahlen in $\mathbb{Z}$ spielen. In Analogie zu 4.4.6 gilt etwa

5.7.10 Lemma Sei $p \in \mathbb{K}[T]$ irreduzibel und seien $f_1, \ldots, f_n \in \mathbb{K}[T]$. Wenn p das Produkt $\prod_{i=1}^{n} f_i$ teilt, dann teilt p einen der Faktoren f_i.

Beweis: Sei p ein Teiler von $\prod_{i=1}^{n} f_i$. Dann gilt

$$(f_1 + (p)) \cdots (f_n + (p)) = \prod_{i=1}^{n} f_i + (p) = 0 + (p)$$

im Faktorring $\mathbb{K}[T]/(p)$. Da $\mathbb{K}[T]/(p)$ mit Satz 5.6.10 ein Körper ist, folgt $f_i + (p) = 0 + (p)$ für ein $1 \leq i \leq n$. Dies bedeutet $f_i \in (p)$, und somit ist p ein Teiler von f_i. □

Weiter gilt in $\mathbb{K}[T]$ ein Analogon zur eindeutigen Primfaktorzerlegung in $\mathbb{Z}$:

5.7.11 Satz (Eindeutige Zerlegung von Polynomen in irreduzible Faktoren)

Jedes Polynom $f \in \mathbb{K}[T]$ mit $\mathrm{Grad}(f) \geq 1$ lässt sich als Produkt $f = ep_1^{s_1} \cdots p_n^{s_n}$ schreiben, wobei $e \in \mathbb{K}^\times$, $s_1, \ldots, s_n \in \mathbb{N}$ und $p_1, \ldots, p_n$ verschiedene normierte und irreduzible Polynome sind. Die Einheit e, die Zahlen $s_1, \ldots, s_n$ und die Polynome $p_1, \ldots, p_n$ sind (bis auf die Reihenfolge) eindeutig bestimmt. □

Eine Beweis dieses Satzes wurde in der Linearen Algebra II, Kurseinheit 1, erbracht.

5.7.12 Notation Wir nennen eine Zerlegung von f wie in 5.7.11 eine **kanonische Zerlegung von** f.

Es ist eine wichtige Frage über Polynome in $\mathbb{K}[T]$, zu entscheiden, ob sie irreduzibel sind oder nicht. In der Kryptografie ist insbesondere der Fall interessant, in dem der Körper $\mathbb{K}$ ein endlicher Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ ist, wobei p eine Primzahl ist. In einer solchen Situation können wir im Prinzip alle irreduziblen Polynome von einem vorgegebenen Grad n bestimmen. Man macht eine Liste aller Polynome vom Grad n (es gibt nur endlich viele), dann berechnet man alle Produkte von Polynomen kleineren Grades und erstellt auf diese Weise eine Liste der reduziblen Polynome vom Grad n. Nun eliminiert man die reduziblen Polynome vom Grad n von der Liste aller Polynome vom Grad n. Übrig bleiben die irreduziblen vom Grad n. Wenn n oder p groß sind, eine zugegebenermaßen mühsame Arbeit.

5.7.13 Aufgabe Bestimmen Sie alle irreduziblen Polynome vom Grad 4 in $\mathbb{F}_2[T]$.

Wir haben in der Linearen Algebra II bereits Körperelemente in Polynome eingesetzt, indem wir die Unbestimmte T durch ein Körperelement x ersetzt haben. Genauer, wenn $f = \sum_{i=0}^{n} a_i T^i$ ein Polynom in $\mathbb{K}[T]$ und $x \in \mathbb{K}$ ist, so bezeichnen wir mit $f(x)$ das Element $\sum_{i=0}^{n} a_i x^i$ in $\mathbb{K}$.

Eine wichtige Rolle spielen die so genannten Nullstellen eines Polynoms $f \in \mathbb{K}[T]$.

5.7.14 Definition Ein Element $\lambda \in \mathbb{K}$ heißt **Nullstelle** oder **Wurzel** eines Polynoms $f \in \mathbb{K}[T]$, wenn $f(\lambda) = 0$ ist.

Wir hatten in der Linearen Algebra II gesehen:

5.7.15 Proposition (Nullstellen und irreduzible Faktoren)

Ein Element $\lambda \in \mathbb{K}$ ist genau dann Nullstelle von $f \in \mathbb{K}[T]$, wenn $f = (T - \lambda)q$ für ein Polynom $q \in \mathbb{K}[T]$ ist. □

5.7.16 Definition Sei λ eine Nullstelle von $f \in \mathbb{K}[T]$. Die größte natürliche Zahl v, so dass $(T - \lambda)^v$ ein Teiler von f ist, wird die **Vielfachheit** von λ genannt und mit $\alpha(\lambda)$ bezeichnet. Wenn $\alpha(\lambda) > 1$ ist, dann sagen wir, dass λ eine **mehrfache Nullstelle** von f ist.

Die folgenden Korollare aus Proposition 5.7.15 wurden in der Linearen Algebra II, Kurseinheit 1, bewiesen:

5.7.17 Korollar Seien $\lambda_1, \ldots, \lambda_s$ verschiedene Nullstellen von $f \in \mathbb{K}[T]$ mit Vielfachheiten $\alpha(\lambda_1), \ldots, \alpha(\lambda_s)$. Dann gibt es ein Polynom $q \in \mathbb{K}[T]$, so dass

$$f = (T - \lambda_1)^{\alpha(\lambda_1)} \cdots (T - \lambda_s)^{\alpha(\lambda_s)} q$$

ist. □

5.7.18 Korollar (Anzahl der Nullstellen von Polynomen)

Ein Polynom $f \in \mathbb{K}[T]$, $f \neq 0$, vom Grad n hat höchstens n verschiedene Nullstellen. □

Unmittelbar aus Korollar 5.7.17 folgt

5.7.19 Korollar Sei f ein Polynom in $\mathbb{K}[T]$ vom Grad n. Seien $\lambda_1, \ldots, \lambda_s$ verschiedene Nullstellen von $f \in \mathbb{K}[T]$ mit Vielfachheiten $\alpha(\lambda_1), \ldots, \alpha(\lambda_s)$. Dann gilt $\sum_{i=1}^{s} \alpha(\lambda_i) \leq n$. □

Ob ein Polynom $f \in \mathbb{K}[T]$ mehrfache Nullstellen hat, können wir an der Ableitung von f ablesen.

5.7.20 Definition Sei $f = \sum_{i=0}^{n} a_i T^i$ ein Polynom in $\mathbb{K}[T]$. Die **Ableitung** f' von f ist das Polynom $f' = \sum_{i=1}^{n} i a_i T^{i-1}$.

Es gelten die üblichen Rechenregeln

$$\begin{aligned} (af + bg)' &= af' + bg' \\ (fg)' &= f'g + fg' \end{aligned}$$

für alle $a, b \in \mathbb{K}$ und alle $f, g \in \mathbb{K}[T]$.

5.7.21 Proposition Genau dann ist $\lambda \in \mathbb{K}$ eine mehrfache Nullstelle eines Polynoms $f \in \mathbb{K}[T]$, wenn λ eine Nullstelle von f und von f' ist.

Beweis: Sei λ eine Nullstelle von f mit $\alpha(\lambda) \geq 2$. Mit Korollar 5.7.17 ist f von der Form

$$f = (T - \lambda)^{\alpha(\lambda)} q,$$

wobei q ein Polynom in $\mathbb{K}[T]$ ist. Es folgt

$$f' = \alpha(\lambda)(T - \lambda)^{\alpha(\lambda)-1} q + (T - \lambda)^{\alpha(\lambda)} q'.$$

Somit ist λ auch eine Nullstelle von f'.

Sei umgekehrt λ eine Nullstelle von f und von f'. Mit Proposition 5.7.15 folgt $f = (T-\lambda)g$ für ein $g \in \mathbb{K}[T]$. Somit gilt $f' = g+(T-\lambda)g'$, also $g = f'-(T-\lambda)g'$. Da λ eine Nullstelle von f' ist, teilt $T - \lambda$ die rechte Seite dieser Gleichung, also auch die linke. Es folgt $g = (T - \lambda)h$ für ein $h \in \mathbb{K}[T]$. Somit gilt

$$f = (T - \lambda)g = (T - \lambda)^2 h,$$

und es folgt, dass λ eine mehrfache Nullstelle von f ist. □

Es gibt einen Zusammenhang zwischen der Nicht-Existenz von Nullstellen und Irreduzibilität. Wenn f ein irreduzibles Polynom vom Grad ≥ 2 ist, dann besagt 5.7.15, dass f keine Wurzel in $\mathbb{K}$ besitzt. Die Umkehrung gilt für Polynome vom Grad 2 oder 3, aber nicht notwendigerweise für Polynome höheren Grades.

5.7.22 Proposition Ein Polynom f in $\mathbb{K}[T]$ vom Grad 2 oder 3 ist genau dann irreduzibel, wenn es keine Nullstelle in $\mathbb{K}$ hat.

Beweis: Sei $f \in \mathbb{K}[T]$ ein Polynom vom Grad 2 oder 3. Wenn f reduzibel ist, so hat f einen Teiler g vom Grad 1. Dieser hat die Form $aT - b = a(T - \frac{b}{a})$ für $a, b \in \mathbb{K}$, $a \neq 0$. Es folgt, dass $\frac{b}{a}$ eine Nullstelle von f ist. Umgekehrt, wenn f eine Nullstelle besitzt, so besagt 5.7.15 gerade, dass f reduzibel ist. □

Diese Beobachtung ermöglicht uns, irreduzible Polynome vom Grad ≤ 3 über Körpern $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, p eine Primzahl, zu bestimmen. Wir setzen die endlich vielen Elemente ein; bekommen wir 0 raus, so ist das Polynom reduzibel, ist das Ergebnis immer $\neq 0$, so ist das Polynom irreduzibel. Folgendes Beispiel mag das veranschaulichen.

5.7.23 Beispiel Wir bestimmen alle irreduziblen Polynome vom Grad ≤ 3 in $\mathbb{F}_2[T]$.

Zunächst einmal sind alle Polynome vom Grad 1 irreduzibel. Diese sind $f_1 = T$ und $f_2 = T + 1$.

Es gibt folgende Polynome vom Grad 2: $g_1 = T^2$, $g_2 = T^2 + 1$, $g_3 = T^2 + T$, und $g_4 = T^2 + T + 1$. Es ist $g_1(0) = 0$, also ist g_1 reduzibel (wofür wir natürlich keine Theorie brauchen, um das zu sehen). Es ist $g_2(1) = 1 + 1 = 0$, also ist auch g_2 reduzibel. Es ist $g_3(0) = 0$, also ist g_3 ebenfalls reduzibel. Es ist $g_4(0) = 1$ und $g_4(1) = 1 + 1 + 1 = 1$. Somit ist g_4 irreduzibel in $\mathbb{F}_2[T]$.

Es gibt folgende Polynome vom Grad 3 in $\mathbb{F}_2[T]$: $h_1 = T^3$, und h_1 ist reduzibel. $h_2 = T^3 + 1$, und $h_2(1) = 0$, das heißt, h_2 ist reduzibel. $h_3 = T^3 + T$, offenbar reduzibel. $h_4 = T^3 + T^2$, ebenfalls reduzibel. $h_5 = T^3 + T + 1$; es sind $h_5(0) = 1$ und $h_5(1) = 1$. Somit ist h_5 irreduzibel. Analog ist $h_6 = T^3 + T^2 + 1$ irreduzibel. Das Polynom $h_7 = T^3 + T^2 + T$ ist offenbar durch T teilbar. Auch $h_8 = T^3 + T^2 + T + 1$ ist reduzibel, denn $h_8(1) = 0$.

Wir erhalten also folgende irreduzible Polynome vom Grad ≤ 3: $T, T + 1, T^2 + T + 1, T^3 + T + 1$ und $T^3 + T^2 + 1$.

5.8 Das RSA-Kryptosystem

Das RSA-Kryptosystem ist ein Beispiel für ein Public-Key-Kryptosystem, wie wir sie in Kapitel 1 allgemein eingeführt haben. Zur Erinnerung, in einem Public-Key-Kryptosystem werden die Schlüssel K und die Chiffrierungsregeln e_K nicht geheim gehalten. Es ist ausreichend, Zusatzinformation – so genannte geheime Schlüssel – zu verbergen.

Das RSA-Kryptosystem ist nach seinen Entdeckern Ronald Rivest, Adi Shamir und Leonard Adleman [RSA] benannt, und ist, obwohl es schon 1978 publiziert wurde, das wohl bekannteste und heute noch am häufigsten eingesetzte Public-Key-Verfahren.

Die mathematischen Grundlagen dieses Systems sind spezielle Eigenschaften der Restklassenringe $\mathbb{Z}/n\mathbb{Z}$, die in dieser und der letzten Kurseinheit hergeleitet wurden.

Beschreiben wir zunächst, wie Alice in die Liste der befugten Teilnehmerinnen und Teilnehmer des RSA-Verfahrens aufgenommen wird.

Alice wählt zwei große, verschiedene Primzahlen p und q und bildet $m = pq$. Die Primzahlen p und q hält sie geheim. Weiter berechnet sie $\varphi(m) = (p-1)(q-1)$ und wählt eine Zahl e mit $\mathrm{ggT}(e, \varphi(m)) = 1$. Dabei bezeichnet φ die Eulersche φ-Funktion. Da $\mathrm{ggT}(e, \varphi(m)) = 1$, ist e in $\mathbb{Z}/\varphi(m)\mathbb{Z}$ invertierbar. Alice berechnet $d \in \mathbb{Z}/\varphi(m)\mathbb{Z}$, so dass $e \cdot d = 1$ in $\mathbb{Z}/\varphi(m)\mathbb{Z}$ ist. Dann gilt $ed = r\varphi(m) + 1$ für ein $r \in \mathbb{Z}$.

So weit die Vorbereitungen.

Das Paar (m, e) ist der öffentliche Schlüssel von Alice.

Die Primzahlen p, q und die Zahl d bilden den geheimen Schlüssel von Alice.

Die Klartextmenge und die Geheimtextmenge in Alice' Kryptosystem ist die Menge $\mathbb{Z}/m\mathbb{Z}$.

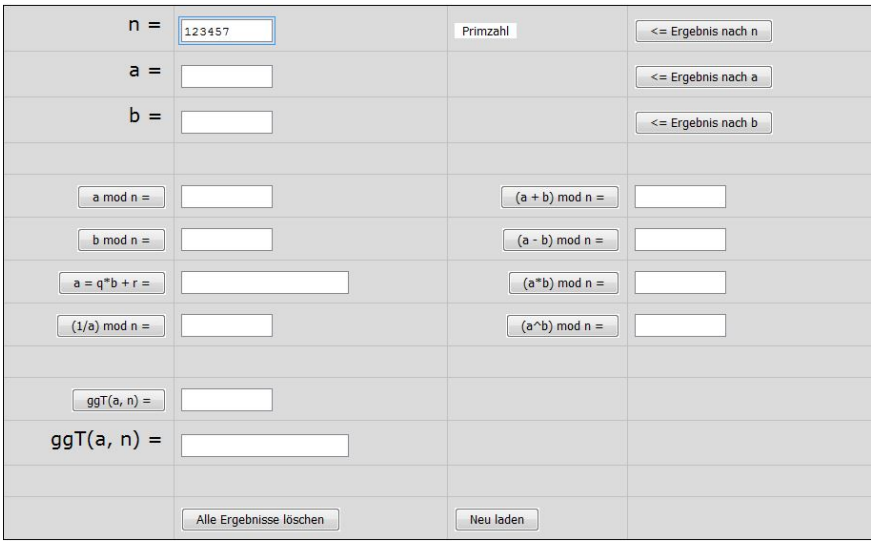
Chiffrierung im RSA-Verfahren: Will Bob an Alice die Nachricht $x \in \mathbb{Z}/m\mathbb{Z}$ schicken, so bildet er $y = x^e$ in $\mathbb{Z}/m\mathbb{Z}$ und schickt y an Alice.

Dechiffrierung im RSA-Verfahren: Alice hat eine Nachricht $y \in \mathbb{Z}/m\mathbb{Z}$ empfangen. Diese ist von der Form $y = x^e$ in $\mathbb{Z}/m\mathbb{Z}$, wobei x der Klartext ist. Sie bildet $y^d = (x^e)^d = x^{ed}$ in $\mathbb{Z}/m\mathbb{Z}$. Da $ed = r\varphi(m) + 1$, folgt mit der Folgerung 4.4.13 aus dem Kleinen Satz von Fermat, dass $y^d = x$ ist, und sie erhält Bobs Klartext.

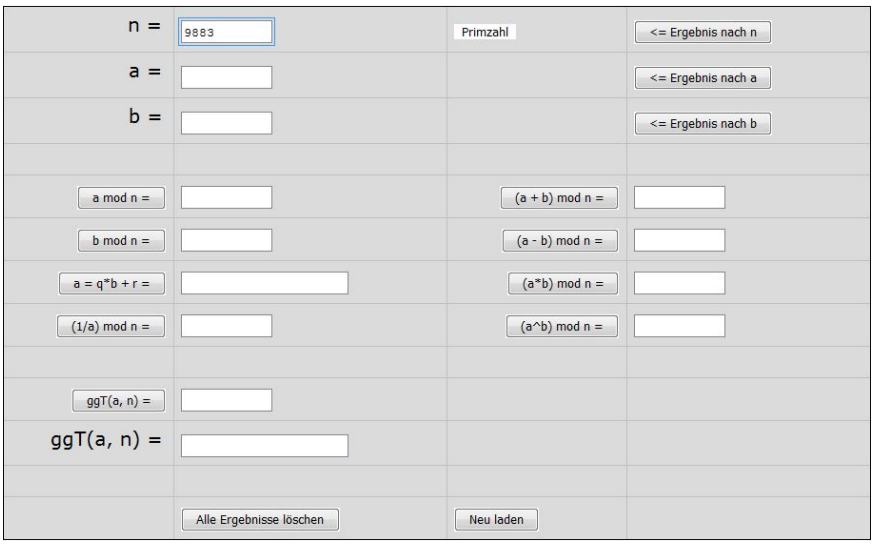
Warum das RSA-Verfahren schnell und sicher ist, werden wir später sehen. Wenden wir uns zunächst einem Beispiel zu. Dabei benutzen wir für die Rechnungen den Taschenrechner für modulare Arithmetik, der im virtuellen Studienplatz bereit steht. Hier wird er in Form von Screenshots eingebunden.

5.8.1 Ein Beispiel

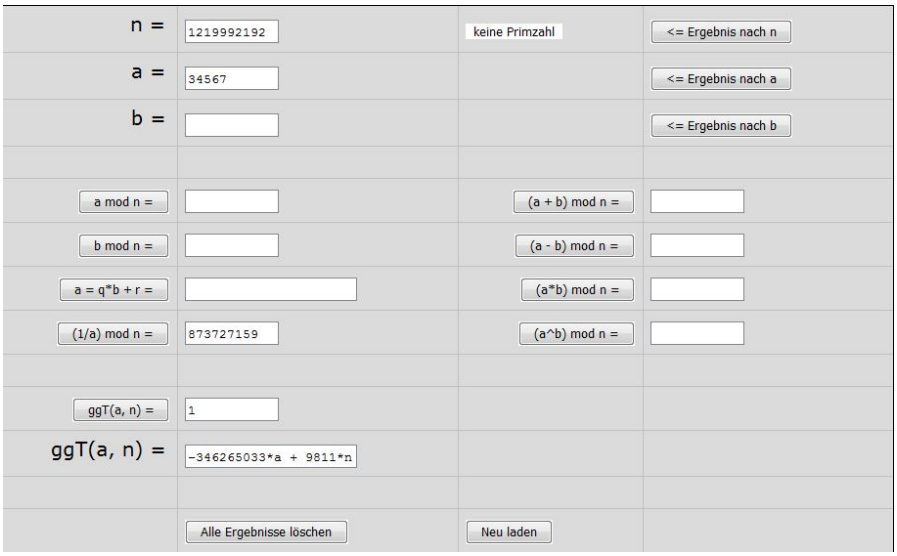
Als Primzahl p wählen wir $p = 123457$.



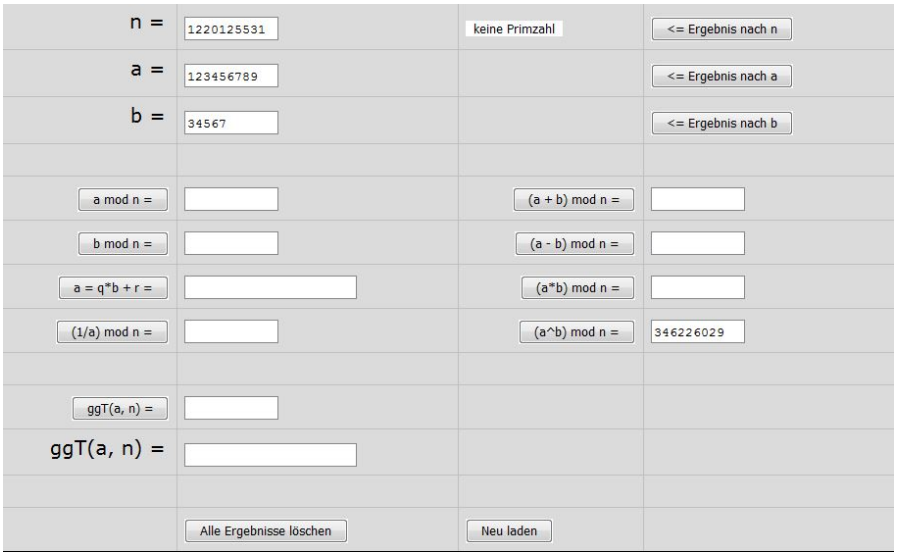
Als Primzahl q wählen wir $q = 9883$.



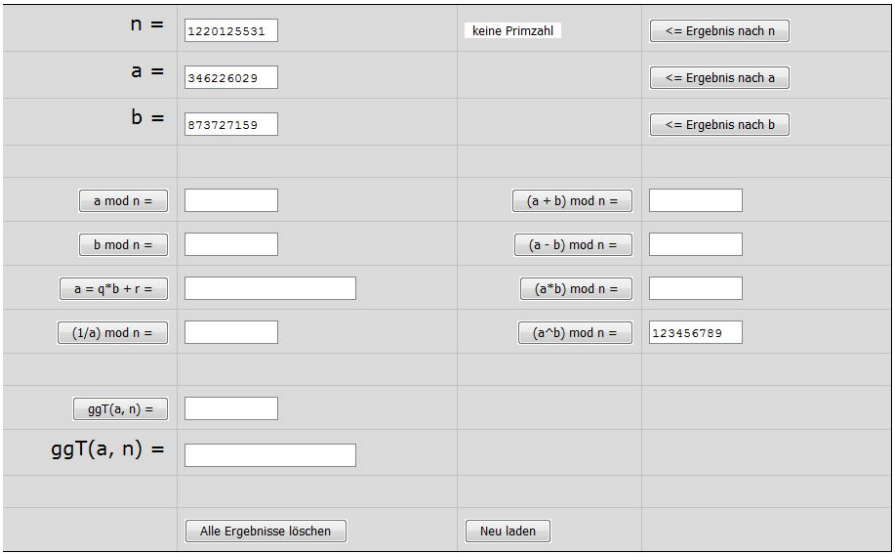
Weiter berechnen wir, etwa mit dem Taschenrechner des Computers, $m = pq = 1220125531$ und $\varphi(m) = (p-1)(q-1) = 1219992192$. Wir wählen $e = 34567$. Um zu überprüfen, ob wirklich $\mathrm{ggT}(e, \varphi(m)) = 1$ gilt, tragen wir $\varphi(m)$ als n und e als a in den Taschenrechner ein und berechnen $\mathrm{ggT}(a, n)$. Jetzt berechnen wir das zu e inverse Element in $\mathbb{Z}/\varphi(m)\mathbb{Z}$. Wir erhalten $d = 873727159$.



Jetzt haben wir alle Bestandteile des Schlüssels zusammen: der öffentliche Schlüssel ist $m = pq = 1220125531$ und $e = 34567$, und der geheime Schlüssel ist $p = 123457$, $q = 9883$ und $d = 873727159$. Nun können wir chiffrieren und dechiffrieren. Wir tragen $m = pq = 1220125531$ als n in den Taschenrechner ein. Die Zahl 123456789 wird dann als $123456789^{34567} = 346226029$ in $\mathbb{Z}/m\mathbb{Z}$ chiffriert.



Um zu überprüfen, ob das Verfahren in diesem Beispiel geklappt hat, müssen wir das Ergebnis in die 873727159-te Potenz erheben:



Wir erhalten die Ausgangsnachricht 123456789.

5.8.2 Analyse des RSA-Verfahrens, oder, wo ist der Trick?

Wir hatten in Kapitel 1 gewisse Forderungen an ein Public-Key-Kryptosystem gestellt. Wir werden in diesem Abschnitt erklären, warum das RSA-Verfahren diesen Anforderungen genügt.

Wiederholen wir aber zunächst noch einmal die Forderungen:

1. Für alle Klartexte $x \in \mathcal{P}$ muss sich $e_K(x)$ sehr schnell berechnen lassen.
2. **Ohne** den geheimen Schlüssel lässt sich das Urbild eines Geheimtextes $y \in \mathcal{C}$ unter e_K praktisch – das heißt, in angemessener Zeit – nicht berechnen, selbst dann nicht, wenn K und e_K bekannt sind.
3. Dazu Befugte können aus dem öffentlichen Schlüssel K den geheimen Schlüssel schnell herleiten.
4. **Mit** dem geheimen Schlüssel lässt sich $d_K(y)$ für alle Geheimtexte y sehr schnell berechnen.

Wenden wir uns zunächst Punkt 3. zu, also der Konstruktion des öffentlichen und des geheimen Schlüssels. Diese Konstruktion darf nur wenig Speicherplatz und Rechenzeit beanspruchen.

Alice, die befugte Teilnehmerin des RSA-Kommunikationsnetzes muss zwei verschiedene große Primzahlen wählen.

Dies geschieht in der Regel so, dass ein Zufallszahlengenerator zwei große ungerade Zahlen p und q vorschlägt, von denen aber nicht klar ist, ob diese wirklich Primzahlen sind oder nicht. Alice unterwirft diese Zahlen einem so genannten „probabilistischen Primzahltest“, dazu sagen wir in der folgenden Kurseinheit mehr. Wenn das Ergebnis dieses Testes lautet: „p ist keine Primzahl“, dann setzt Alice p auf $p+2$ und unterzieht diese Zahl erneut einem probabilistischen Primzahltest. Dies setzt sie so lange fort, bis das Ergebnis des Testes lautet: „p ist eine Primzahl“. Analog verfährt sie mit der Zahl q. Die Zahlen p und q, beziehungsweise die Zahlen $p-1$ und $q-1$ miteinander zu multiplizieren, ist kein Problem.

Ein probabilistischer Primzahltest ist ein schnell durchführbarer Algorithmus, in den eine ungerade Zahl n eingesetzt wird, und der als Ergebnis die Antworten „n ist keine Primzahl“ oder „n ist eine Primzahl“ liefert. Dabei ist das Ergebnis „n ist keine Primzahl“ immer richtig. Lautet die Antwort „n ist eine Primzahl“, so können wir allerdings nicht völlig sicher sein, dass die Antwort richtig ist.

Kommen wir zurück zur Schlüsselkonstruktion im RSA-Kryptosystem. Sie haben bisher gesehen, wie die Wahl von zwei großen Primzahlen erfolgt. Als nächsten Schritt muss Alice eine Zahl e so wählen, dass $\mathrm{ggT}(e, \varphi(m)) = 1$ ist. Wieder schlägt ein Zufallszahlengenerator eine Zahl e vor. Mit Hilfe des euklidischen Algorithmus, der ein wirklich schnell durchführbarer Algorithmus ist, berechnet Alice $\mathrm{ggT}(e, \varphi(m))$. Ist das Ergebnis $\neq 1$, so setzt sie e auf $e+1$ und versucht es erneut. Nach wenigen Schritten wird sie eine Zahl e gefunden haben, die $\mathrm{ggT}(e, \varphi(m)) = 1$ erfüllt.

Die Berechnung des zu e in $\mathbb{Z}/\varphi(m)\mathbb{Z}$ inversen Elements d erfolgt wieder mit dem Euklidischen Algorithmus.

So weit zur Schlüsselerzeugung. Wenden wir uns den Punkten 1. und 4. zu, also der Chiffrierung und Dechiffrierung. Beide erfolgen mit Hilfe des so genannten „wiederholten Quadrierungsalgorithmus“, den wir in der folgenden Kurseinheit vorstellen werden. Dieser Algorithmus ist schnell durchführbar.

Es bleibt zu klären, warum Oscar, der Lauscher an der unsicheren Leitung, ein ernst zu nehmendes Problem hat.

Das Problem besteht darin, dass Oscar nur $m = pq$ kennt, nicht aber die Faktoren p und q von m, die er zur Berechnung von d (bzw. $\varphi(m)$) benötigt. Oscar sieht sich also mit dem Problem konfrontiert, die Zahl m in Primfaktoren zu zerlegen. Dieses Problem wird in der Zahlentheorie schon seit Jahrhunderten untersucht, und es gilt als ein sehr schweres Problem. Bis heute sind keine schnellen Algorithmen bekannt, mit deren Hilfe Zahlen als Produkte von Primfaktoren geschrieben werden können. Zwar können probabilistische Primzahltests dazu eingesetzt werden, zu

entscheiden, ob eine gegebene Zahl n eine Primzahl ist oder nicht, aber keiner dieser Tests liefert einen Faktor von n.

Die Sicherheit des RSA-Verfahrens beruht also darauf, dass keine schnellen Algorithmen bekannt sind, eine Zahl m als Produkt ihrer Faktoren zu schreiben.

Es ist ein offenes mathematisches Problem, ob es schnelle (dieser Begriff ist natürlich zu präzisieren) Faktorisierungsalgorithmen gibt oder nicht. Es wird vermutet, dass dies nicht der Fall ist. Außerdem ist auch nicht bekannt, ob wirklich die Zahl m faktorisiert werden muss, um das RSA-Kryptosystem zu brechen.

5.8.3 Realistische Größen bei der Nutzung des RSA-Verfahrens

Die Sicherheit des RSA-Verfahrens beruhte auf dem Problem, eine große natürliche Zahl in ihre Primfaktoren zu zerlegen. Daher darf die Schlüssellänge nicht zu klein gewählt werden. Die Länge eines Schlüssels wird gemessen in der Anzahl der Speicherbits, die benötigt werden, um diesen Wert im Computer darzustellen.

Mit welchen Schlüssellängen das RSA-Verfahren im Herbst 2004 als sicher galt, wird hier aus den Richtlinien des Bundesamtes für Sicherheit in der Informationstechnik `http://www.bsi.de/` zitiert:

„Werden bei asymmetrischer Verschlüsselungs- und Signaturverfahren Algorithmen eingesetzt, deren Sicherheit auf dem Problem des Faktorisierens großer Zahlen basiert, so wird heute angenommen, daß Schlüssellängen von weniger als 1024 Bit als unsicher zu betrachten sind. Dies begründet sich in den Fortschritten bei der Entwicklung effizienter Faktorisierungsalgorithmen, die heute unter massivem Rechnereinsatz Faktorisierungen von Zahlen mit rund 500 Bit erlauben. Daneben ist die mögliche Entwicklung von opto-elektronischen Beschleunigern für einen wesentlichen Teil- Rechenschritt bei diesen Verfahren in Betracht zu ziehen, was diese wesentlich beschleunigen würde.

...

Betroffen ist der RSA-Algorithmus, der als asymmetrisches Verfahren auf dem Faktorisierungsproblem basiert. Wird dieser mit einer Schlüssellänge unter 768 Bit betrieben, kann von potentiellen Unsicherheiten ausgegangen werden. Für die nächsten Jahre wird eine Schlüssellänge von mehr als 1024 Bit als ausreichend sicher angesehen.“

Eine Zahl mit 1024 Bit Länge hat etwa 300 Stellen.

In den USA ist nur eine Schlüssellänge von 512 Bit erlaubt.

5.8.4 Neuere und neuste Geschichte des RSA-Kryptosystems

In den USA war das RSA-Verfahren patentiert. Das Patent hatte die Firma RSA Security vom Massachusetts Institute of Technology (MIT) erworben, bei dem die Entdecker Rivest, Shamir und Adleman angestellt waren. Kommerzielle RSA-Nutzer in den USA mussten Lizenzgebühren zahlen, auch wenn keine Implementierung durch RSA Security erfolgte. Europäische Software kostete deutlich mehr oder konnte gar nicht erst vertrieben werden. Am 20. September 2000 lief das Patent aus, und das RSA-Verfahren wurde Allgemeingut.

Es wird immer wieder davon berichtet, dass das RSA-Kryptosystem gebrochen worden wäre. So wird etwa über Angriffe auf RSA durch Einsatz spezieller Hardware oder durch Anwendung cleverer mathematischer Verfahren berichtet.

Es gab spezielle RSA-Challenges, in denen wissenschaftliche Institutionen aber auch Individuen aufgefordert wurden, speziell vorgegebene Zahlen zu faktorisieren. Dies diente unter anderem auch dazu, herauszufinden, wie groß die Schlüssellängen gewählt werden müssen, damit das RSA-Verfahren noch als sicher angesehen werden kann. Der Wettbewerb wurde 1991 ausgerufen und 2007 nach der erfolgreichen Faktorisierung einer 1039-Bit-Zahl eingestellt. Bis dahin wurden 30100 US-Dollar an Preisgeldern ausgezahlt.

Es gibt heute Public-Key-Verfahren, die als genauso sicher wie RSA gelten, die aber mit deutlich geringerer Schlüssellänge auskommen. Diese Verfahren beruhen auf der mathematischen Theorie elliptischer Kurven, die wir in Kurseinheit 6 vorstellen werden.

5.8.5 Aufgaben

5.8.1 Aufgabe Übernehmen Sie die Rolle von Alice. Sie möchten in die Liste derer aufgenommen werden, die mit Hilfe des RSA-Verfahrens miteinander kommunizieren. Der Zufallszahlengenerator hat Ihnen als Primzahlen p und q die Zahlen $p = 2345$ und $q = 76543$ vorgeschlagen, und als zu $(p-1)(q-1)$ teilerfremde Zahl e die Zahl $e = 97251$.

Nehmen Sie die vorgeschlagenen Zahlen als Basis zur Konstruktion des geheimen und des öffentlichen Schlüssels im RSA-Kryptosystem.

Wie lautet Ihr geheimer, wie Ihr öffentlicher Schlüssel? Wie wird dechiffriert?

In den beiden folgenden Aufgaben werden wir Buchstaben wie folgt mit Zahlen

identifizieren:

$a \leftrightarrow 01$	$b \leftrightarrow 02$	$c \leftrightarrow 03$	$d \leftrightarrow 04$	$e \leftrightarrow 05$	$f \leftrightarrow 06$	$g \leftrightarrow 07$	$h \leftrightarrow 08$
$i \leftrightarrow 09$	$j \leftrightarrow 10$	$k \leftrightarrow 11$	$l \leftrightarrow 12$	$m \leftrightarrow 13$	$n \leftrightarrow 14$	$o \leftrightarrow 15$	$p \leftrightarrow 16$
$q \leftrightarrow 17$	$r \leftrightarrow 18$	$s \leftrightarrow 19$	$t \leftrightarrow 20$	$u \leftrightarrow 21$	$v \leftrightarrow 22$	$w \leftrightarrow 23$	$x \leftrightarrow 24$
$y \leftrightarrow 25$	$z \leftrightarrow 26$						

Eine Leerstelle werden wir mit 00 identifizieren. Wir fassen dann den Text in Blöcke der Länge 2 zusammen, und erhalten Ziffernfolgen der Länge 4 (möglicherweise mit führender Null). Diese Ziffernfolgen werden wir chiffrieren beziehungsweise dechiffrieren. Ein Beispiel: „Es geht los“ wird zu 0519 0007 0508 2000 1215 1924. Dabei haben wir, da der Text aus einer ungeraden Anzahl von Buchstaben/Leerstellen bestand, den Text am Ende um ein x verlängert.

5.8.2 Aufgabe Übernehmen Sie die Rolle von Bob. Sie möchten Alice die Botschaft „wie immer um Mitternacht“ übermitteln. Alice' öffentlicher Schlüssel ist $(2923, 725)$.

Chiffrieren Sie die Nachricht mit Alice' öffentlichem Schlüssel.

5.8.3 Aufgabe Sie sind Oscar, und Sie haben folgende Nachricht von Bob an Alice abgefangen:

2201	2352	1458	0207	2417
1951	0717	0795	1442	0876
2730	1205	0795.		

Der öffentliche Schlüssel von Alice ist $(2881, 137)$. Wie lautet der Klartext?

Lösungen der Aufgaben

Aufgabe 5.1.6

Behauptung In jedem Schiefkörper R folgt aus $ab = 0$, dass $a = 0$ oder $b = 0$ gilt.

Beweis: Sei R ein Schiefkörper. Wir zeigen zunächst, dass $r \cdot 0 = 0$ ist, für alle $r \in R$.

Es gilt $r \cdot 0 = r \cdot (0 + 0) = r \cdot 0 + r \cdot 0$. Wir subtrahieren auf beiden Seiten der Gleichung $r \cdot 0$ und erhalten $0 = r \cdot 0$.

Seien nun $a, b \in R$ mit $ab = 0$. Wenn $a = 0$, so sind wir fertig. Sei also $a \neq 0$. Wir müssen zeigen, dass $b = 0$ ist. Wir multiplizieren die Gleichung $ab = 0$ auf beiden Seiten mit a^{-1}. Dann folgt $a^{-1}ab = b = 0$, und wir sind fertig. □

Aufgabe 5.1.8 Seien $R_1, \ldots, R_n$ Ringe.

(a) **Behauptung** $\prod_{i=1}^{n} R_i$ ist in der Regel kein Integritätsbereich, wenn $R_1, \ldots, R_n$ Integritätsbereiche sind.

Beweis: Sei etwa $R_1 = R_2 = \mathbb{Z}$. Dann sind R_1 und R_2 Integritätsbereiche. Der Ring $\mathbb{Z} \times \mathbb{Z}$ ist kein Integritätsbereich, denn $(1, 0)$ und $(0, 1)$ sind $\neq 0$, aber $(1, 0)(0, 1) = (0, 0)$. □

(b) **Behauptung** $\prod_{i=1}^{n} R_i$ ist in der Regel kein Körper, wenn alle R_i, $1 \leq i \leq n$ Körper sind.

Beweis: Sei etwa $R_1 = R_2 = \mathbb{R}$. Dann liegen $(1, 0)$ und $(0, 1)$ in $\mathbb{R} \times \mathbb{R}$, und es gilt $(1, 0)(0, 1) = (0, 0)$. Somit ist $\mathbb{R} \times \mathbb{R}$ kein Integritätsbereich. Mit Aufgabe 5.1.6 folgt, dass $\mathbb{R} \times \mathbb{R}$ kein Körper ist. □

(c) **Behauptung** $\prod_{i=1}^{n} R_i$ ist genau dann kommutativ, wenn alle R_i, $1 \leq i \leq n$ kommutativ sind.

Beweis: Seien $R_1, \ldots, R_n$ kommutativ. Dann gilt für alle $a_i, b_i \in R_i, 1 \leq i \leq n$:

$$\begin{aligned} & a_i b_i = b_i a_i \\ \Leftrightarrow \quad & (a_1 b_1, \ldots, a_n b_n) = (b_1 a_1, \ldots, b_n a_n) \\ \Leftrightarrow \quad & (a_1, \ldots, a_n)(b_1, \ldots, b_n) = (b_1, \ldots, b_n)(a_1, \ldots, a_n) \\ \Leftrightarrow \quad & \prod_{i=1}^{n} R_i \text{ ist kommutativ.} \end{aligned}$$

□

Aufgabe 5.2.5

1. Sei $(R, +, \cdot)$ ein Ring, und sei I ein Ideal in R.

   Behauptung Falls $1 \in I$, so gilt $I = R$.

   Beweis: Sei $1 \in I$. Nach Definition gilt $r \cdot 1 = 1 \cdot r = r \in I$ für alle $r \in R$. Es folgt $R \subseteq I$, also $R = I$. □

2. Sei R ein Ring, und seien I_1, I_2 Ideale in R.

   Behauptung $I_1 \cap I_2$ ist ein Ideal in R.

   Beweis: Mit dem Untergruppenkriterium folgt, dass $(I_1 \cap I_2, +)$ eine abelsche Untergruppe von $(R, +)$ ist. Sei $x \in I_1 \cap I_2$. Sei $r \in R$. Dann gilt $rx, xr \in I_1$, denn I_1 ist ein Ideal in R. Analog gilt $xr, rx \in I_2$. Es folgt $rx, xr \in I_1 \cap I_2$, das heißt, $I_1 \cap I_2$ ist ein Ideal in R. □

3. Sei R ein kommutativer Ring, und sei I ein Ideal in R. Sei $\mathrm{M}_{nn}(I)$ die Menge der $n \times n$-Matrizen, deren Einträge in I liegen.

   Behauptung Es ist $\mathrm{M}_{nn}(I)$ ein Ideal in $\mathrm{M}_{nn}(R)$.

   Beweis: Mit dem Untergruppenkriterium folgt, dass $(\mathrm{M}_{nn}(I), +)$ eine abelsche Untergruppe von $\mathrm{M}_{nn}(R)$ ist. Sei $A = (a_{ij}) \in \mathrm{M}_{nn}(I)$, und sei $B = (b_{ij}) \in \mathrm{M}_{nn}(R)$. Seien $C = (c_{ij}) = AB$ und $D = (d_{ij}) = BA$. Dann gelten $c_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj} \in I$ und $d_{ij} = \sum_{k=1}^{n} b_{ik} a_{kj} \in I$ für alle $1 \leq i, j \leq n$, denn I ist ein Ideal in R. Es folgt $AB, BA \in \mathrm{M}_{nn}(I)$. Somit ist $\mathrm{M}_{nn}(I)$ ein Ideal in $\mathrm{M}_{nn}(R)$. □

Aufgabe 5.2.8 Sei R ein Ring, und sei I ein Ideal in R.

1. Seien $a, b \in R$.

   Behauptung Es ist $a \equiv b(\mathrm{mod} I)$ genau dann, wenn $a - b \in I$ gilt.

   Beweis: Es gilt

   $$\begin{aligned} a \equiv b(\mathrm{mod} I) &\Leftrightarrow a = b + c \text{ für ein } c \in I \\ &\Leftrightarrow a - b = c \text{ für ein } c \in I \\ &\Leftrightarrow a - b \in I. \end{aligned}$$

   □

2. Sei $U \subseteq R^\times$ die Menge der Einheiten $a \in R^\times$ mit $a \equiv 1(\mathrm{mod} I)$.

   Behauptung U ist ein Normalteiler von $R^\times$.

   Beweis: Wir zeigen zunächst mit dem Untergruppenkriterium, dass U eine Untergruppe von $R^\times$ ist.

   Die Menge U ist nicht leer, denn $1 \in U$.

   Seien $a, b \in U$. Dann ist ab^{-1} eine Einheit in R. Seien $a = 1 + c$ und $b = 1 + c'$ für Elemente $c, c' \in I$. Indem wir die zweite Gleichung mit b^{-1} multiplizieren, erhalten wir $1 = b^{-1} + b^{-1}c'$, wobei $d = b^{-1}c' \in I$ gilt. Es folgt $ab^{-1} = (1 + c)(1 - d) = 1 + (c - d - cd)$, und $c - d - cd \in I$. Somit gilt $ab^{-1} \in U$, und mit dem Untergruppenkriterium folgt, dass U eine Untergruppe von $R^\times$ ist.

   Zum Beweis, dass U ein Normalteiler von $R^\times$ ist, benutzen wir die zweite Bedingung von Proposition 4.6.4. Dazu seien $r \in R^\times$ und $x = 1 + c \in U$ mit $c \in I$. Dann gilt $rxr^{-1} = r(1 + c)r^{-1} = 1 + rcr^{-1} \in U$, denn $rxr^{-1} \in R^\times$ und $rcr^{-1} \in I$. Es folgt $rUr^{-1} \subseteq U$, und dies impliziert die Behauptung. □

Aufgabe 5.3.2 Sei $\phi : R \to R'$ ein Ringhomomorphismus. Sei $\phi|_{R^\times} : R^\times \to R'$ definiert durch $\phi|_{R^\times}(r) = \phi(r)$ für alle $r \in R^\times$.

(a) **Behauptung** Es gilt $\phi|_{R^\times}(r) \in R'^\times$ für alle $r \in R^\times$.

Beweis: Sei r eine Einheit in R. Dann gilt $rr^{-1} = 1$ und $1 = \phi(1) = \phi(rr^{-1}) = \phi(r)\phi(r^{-1})$. Analog folgt, dass $\phi(r^{-1})\phi(r) = 1$ gilt. Somit ist $\phi(r)$ invertierbar. Es folgt, dass $\phi|_{R^\times}$ invertierbare Elemente in R auf invertierbare Elemente in R' abbildet. □

(b) **Behauptung** Es ist $\phi|_{R^\times} : R^\times \to R'^\times$ ein Gruppenhomomorphismus.

Beweis: Wir haben im ersten Teil der Aufgabe gesehen, dass $\phi|_{R^\times}$ eine Abbildung von $R^\times$ nach $R'^\times$ ist. Da $\phi|_{R^\times}(rs) = \phi|_{R^\times}(r)\phi|_{R^\times}(s)$ für alle $r, s \in R^\times$, folgt, dass $\phi|_{R^\times}$ ein Gruppenhomomophismus ist. □

Aufgabe 5.3.8 Sei $\phi : R \to R'$ ein Epimorphismus, und sei $I \lhd R$ ein Ideal in R. Sei

$$\phi(I) = \{s' \in R' \mid \text{ es gibt ein } s \in I \text{ mit } \phi(s) = s'\}.$$

Behauptung Es ist $\phi(I)$ ein Ideal in R'.

Beweis: Da ϕ ein Ringhomomorphismus ist, folgt mit dem Untergruppenkriterium, dass $(\phi(I), +)$ eine abelsche Untergruppe von $(R', +)$ ist. Sei $\phi(c) \in \phi(I)$, und sei $r' \in R'$. Da ϕ surjektiv ist, gibt es ein $r \in R$ mit $\phi(r) = r'$. Dann gilt

$$\phi(c)r' = \phi(c)\phi(r) = \phi(cr) \in \phi(I),$$

denn $cr \in I$. Analog folgt, dass $r'\phi(c)$ in $\phi(I)$ liegt. Somit ist $\phi(I)$ ein Ideal in R'. □

Aufgabe 5.3.10 Sei R ein kommutativer Ring, und sei I ein Ideal in R. Sei $\mathrm{M}_{nn}(I)$ die Menge der $n \times n$-Matrizen, deren Einträge in I liegen.

Behauptung $\mathrm{M}_{nn}(R)/\mathrm{M}_{nn}(I)$ ist isomorph zu $\mathrm{M}_{nn}(R/I)$.

Beweis: Wir definieren $\phi : \mathrm{M}_{nn}(R) \to \mathrm{M}_{nn}(R/I)$ durch $\phi((a_{ij})) = ([a_{ij}])$ für alle $A = (a_{ij}) \in \mathrm{M}_{nn}(R)$.

Die Abbildung ϕ ist ein Epimorphismus, und

$$\mathrm{Kern}(\phi) = \{A = (a_{ij}) \in \mathrm{M}_{nn}(R) \mid a_{ij} \in I \text{ für alle } 1 \leq i, j \leq n\} = \mathrm{M}_{nn}(I).$$

Mit dem Homomorphiesatz folgt die Behauptung. □

Aufgabe 5.4.5

Gesucht ist die kleinste ganze Zahl x für die gilt:

$$\begin{aligned} x &\equiv 2 (\bmod 3) \\ x &\equiv 1 (\bmod 5) \\ x &\equiv 6 (\bmod 7). \end{aligned}$$

Wir berechnen das Urbild von $(2 \bmod 3, 1 \bmod 5, 6 \bmod 7)$ unter der Abbildung ϕ des chinesischen Restsatzes.

Es ist $n = 3 \cdot 5 \cdot 7 = 105$. Weiter sind $q_1 = 35$, $q_2 = 21$ und $q_3 = 15$. Die r_i berechnen wir mir dem Euklidischen Algorithmus oder durch scharfes Hinsehen (hier entscheiden wir uns für die letztere Variante): $r_1 = 2$, $r_2 = 1$ und $r_3 = 1$.

Es folgt

$$x = (2 \cdot 35 \cdot 2 + 1 \cdot 21 \cdot 1 + 6 \cdot 15 \cdot 1) \bmod 105 = 251 \bmod 105 = 41.$$

Das gesuchte x ist somit $x = 41$. □

Aufgabe 5.5.8 Sei $R = \mathbb{F}_2[T]$. Der Ring R hat unendlich viele Elemente, und sein Primring $\mathbb{F}_2$ hat 2 Elemente. □

Aufgabe 5.5.14

Behauptung Einfache, kommutative Ringe haben die Charakteristik 0 oder p, wobei p eine Primzahl ist.

Beweis: Sei R ein kommutativer Ring, und sei 1 das neutrale Element der Multiplikation in R. Angenommen, $\mathrm{char}(R) = m$, und $m = st$, mit $s, t \neq 1$. Dann gilt $0 = m \cdot 1 = (s \cdot 1)(t \cdot 1)$ mit $s \cdot 1 \neq 0$ und $t \cdot 1 \neq 0$. Sei $I = (s \cdot 1)$ das von $s \cdot 1$ erzeugte Ideal. Dann gilt $I \neq \{0\}$, denn $s \cdot 1 \in I$. Angenommen, $I = R$. Dann gilt $1 \in I$, also $1 = s \cdot 1r$ für ein $r \in R$. Dann folgt $0 = (t \cdot 1)(s \cdot 1)r = t \cdot 1$, ein Widerspruch. Somit ist I ein Ideal, das $\{0\}$ echt enthält und das in R echt enthalten ist. Es folgt, dass R nicht einfach ist. □

Aufgabe 5.5.18 Sei R ein kommutativer Ring der Charakteristik $p > 0$. Seien $a_1, \ldots, a_m \in R$.

Behauptung Es gilt $(a_1 + \cdots + a_m)^{p^n} = a_1^{p^n} + \cdots + a_m^{p^n}$ für alle $m, n \in \mathbb{N}$.

Beweis: Wir beweisen die Behauptung mit Induktion nach m. Ist $m = 1$, so ist die Behauptung offenbar richtig. Sei $m > 1$. Dann gilt

$$\begin{aligned}(a_1 + \cdots + a_m)^{p^n} &= ((a_1 + \cdots + a_{m-1}) + a_m)^{p^n} \\ &= (a_1 + \cdots + a_{m-1})^{p^n} + a_m^{p^n} \text{ mit der Binomischen Formel} \\ &= a_1^{p^n} + \cdots + a_m^{p^n} \text{ mit der Induktionsvoraussetzung.}\end{aligned}$$

□

Aufgabe 5.6.6 Sei $R = \mathbb{Z}$, und seien $m\mathbb{Z}$ und $n\mathbb{Z}$ Ideale in $\mathbb{Z}$.

1. **Behauptung** Genau dann gilt $m\mathbb{Z} \subseteq n\mathbb{Z}$, wenn n ein Teiler von m ist.

   Beweis: Sei $m\mathbb{Z} \subseteq n\mathbb{Z}$. Da $m \in m\mathbb{Z}$, folgt $m \in n\mathbb{Z}$, also $m = xn$ für ein $x \in \mathbb{Z}$. Somit ist n ein Teiler von m.

Sei umgekehrt n ein Teiler von m, also $m = xn$, $x \in \mathbb{Z}$. Dann gilt $my = nxy \in n\mathbb{Z}$ für alle $my \in m\mathbb{Z}$. Es folgt $m\mathbb{Z} \subseteq n\mathbb{Z}$. □

2. **Behauptung** Genau dann gilt $m\mathbb{Z} = n\mathbb{Z}$, wenn m und n assoziiert sind.

   Beweis: Seien m und n assoziiert. Dann gilt $m = \pm n$, und es folgt $m\mathbb{Z} = n\mathbb{Z}$.

   Sei umgekehrt $m\mathbb{Z} = n\mathbb{Z}$. Mit dem ersten Teil der Aufgabe gilt $m|n$ und $n|m$. Es folgt, dass m und n assoziiert sind. □

3. **Behauptung** Genau dann ist $n\mathbb{Z}$ ein maximales Ideal, wenn n ein Primelement in $\mathbb{Z}$ ist.

   Beweis: Sei n kein Primelement. Dann gibt es $s \neq 1$ und $t \neq 1$ mit $n = st$. Dann ist $n\mathbb{Z}$ echt in $s\mathbb{Z}$ enthalten, und es folgt, dass $n\mathbb{Z}$ nicht maximal ist.

   Sei umgekehrt n ein Primelement. Sei $I \neq \mathbb{Z}$ ein Ideal in $\mathbb{Z}$, das $n\mathbb{Z}$ enthält. Dann ist I von der Form $m\mathbb{Z}$, und mit dem ersten Teil der Aufgabe folgt $n\mathbb{Z} = m\mathbb{Z}$. □

Aufgabe 5.6.7

Sei $R = \mathbb{Z}$, und sei $I = \{0\}$. Dann ist I ein Primideal, denn wenn $ab \in I$ für $a, b \in R$, so folgt $a = 0$ oder $b = 0$. Das Nullideal ist aber nicht maximal. □

Aufgabe 5.7.6

$$\begin{aligned} 2T^6 + T^3 + T^2 + 2 &= (2T^2 + 1)(T^4 + T^2 + 2T) + T + 2 \\ T^4 + T^2 + 2T &= (T^3 + T^2 + 2T + 1)(T + 2) + 1 \\ T + 2 &= (T + 2) \cdot 1. \end{aligned}$$

Die Polynome f und g sind somit teilerfremd. □

Aufgabe 5.7.13 Die Polynome vom Grad 4 über $\mathbb{F}_2$ sind:

T^4, $T^4 + 1$, $T^4 + T$, $T^4 + T^2$, $T^4 + T^3$, $T^4 + T + 1$, $T^4 + T^2 + 1$, $T^4 + T^3 + 1$, $T^4 + T^2 + T$, $T^4 + T^3 + T$, $T^4 + T^3 + T^2$, $T^4 + T^2 + T + 1$, $T^4 + T^3 + T + 1$, $T^4 + T^3 + T^2 + 1$, $T^4 + T^3 + T^2 + T$, $T^4 + T^3 + T^2 + T + 1$.

Die meisten der Polynome können wir durch Überlegen schon als reduzibel aussortieren. Wenn ein Polynom 2 oder 4 Summanden besitzt, dann ist es reduzibel, denn dann sind 0 oder 1 Nullstellen. Auch jedes Polynom ohne konstanten Term 1 ist reduzibel, denn dann ist T ein Faktor. Somit bleiben uns noch folgende Polynome:

$T^4 + T + 1$, $T^4 + T^2 + 1$, $T^4 + T^3 + 1$, $T^4 + T^3 + T^2 + T + 1$.

Ein reduzibles Polynom vom Grad 4 ist Produkt von zwei Polynomen vom Grad 2 oder Produkt eines Polynomes vom Grad 1 mit einem vom Grad 3. Die Polynome vom Grad 2 sind T^2, T^2+1, T^2+T, T^2+T+1. Keiner der vier Kandidaten oben ist durch T^2 oder T^2+T teilbar. Die verbleibenden Produkte von Polynomem vom Grad 2 sind:

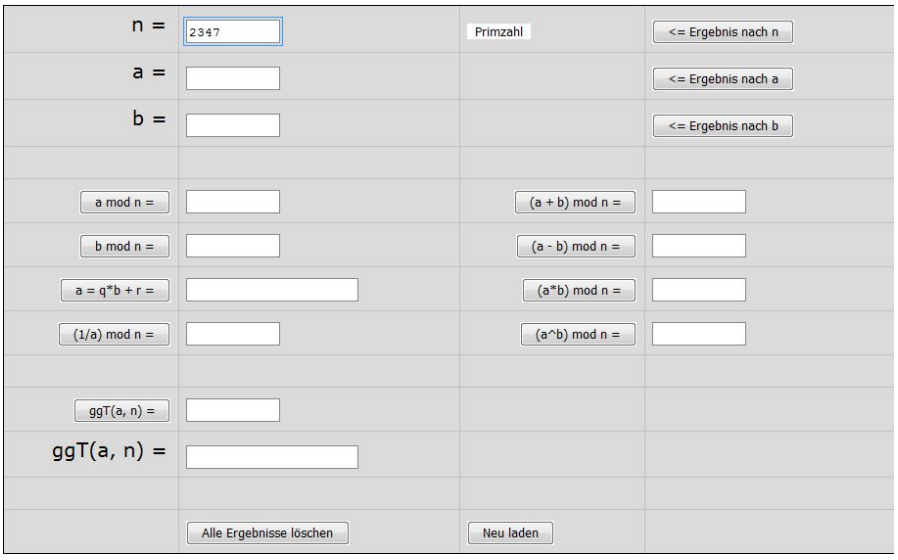
$(T^2+1)^2 = T^4+1$, $(T^2+1)(T^2+T+1) = T^4+T^3+T+1$ und $(T^2+T+1)^2 = T^4+T^2+1$.

Damit verkürzt sich unsere Liste auf

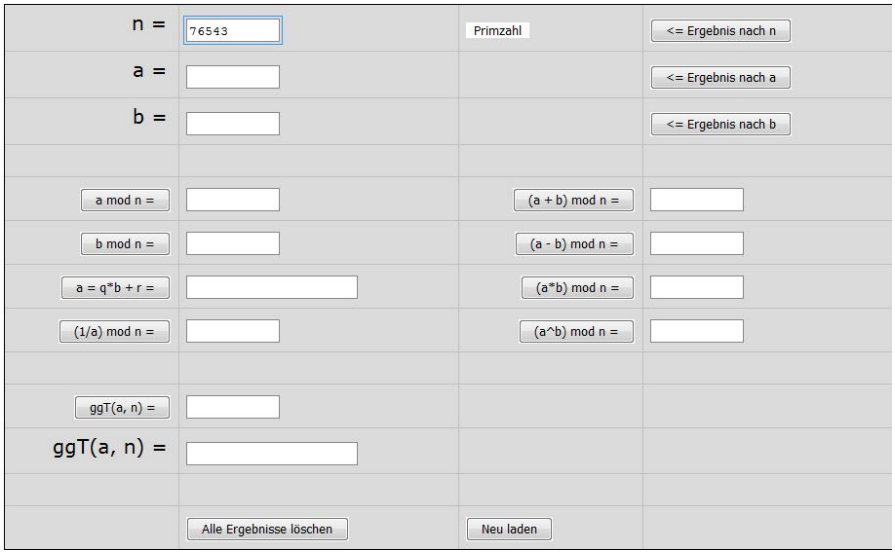
T^4+T+1, T^4+T^3+1, $T^4+T^3+T^2+T+1$.

Diese Polynome sind irreduzibel oder das Produkt eines Polynoms vom Grad 3 mit einem Polynom $\neq T$ vom Grad 1. Im letzteren Fall hätten die Polynome Nullstellen. Wir setzen die Elemente von $\mathbb{F}_2$ ein und stellen fest, dass sie keine Nullstellen haben. Somit sind sie irreduzibel. Die irreduziblen Polynome vom Grad 4 sind damit T^4+T+1, T^4+T^3+1, $T^4+T^3+T^2+T+1$. □

Aufgabe 5.8.1 Die Zahl 2345 ist natürlich keine Primzahl. Wir erhöhen um 2 und setzen die Zahl 2347 als n in den Taschenrechner zum Rechnen in $\mathbb{Z}/n\mathbb{Z}$ ein. Glück gehabt, 2347 ist eine Primzahl, und wir setzen $p = 2347$.

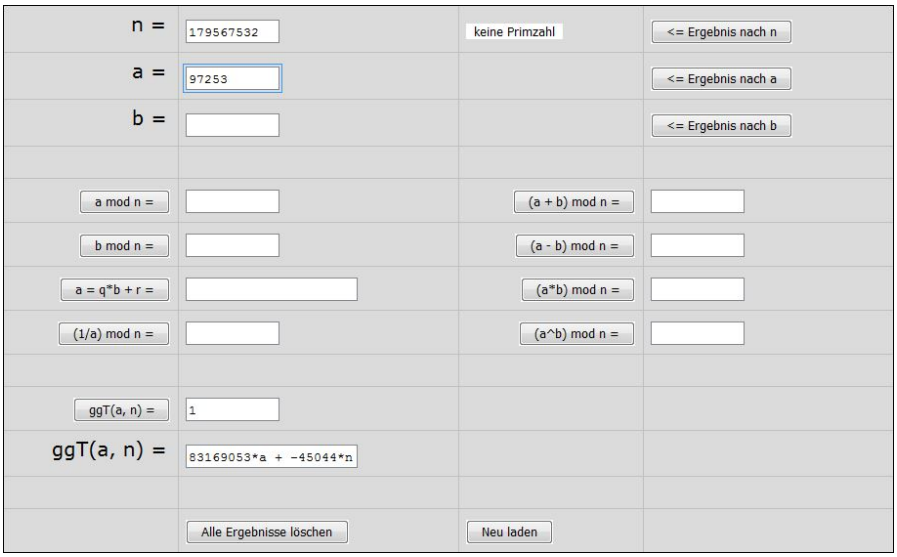


Wir setzen 76543 als n in den Taschenrechner ein.



Es zeigt sich, dass 76543 eine Primzahl ist, und wir setzen $q = 76543$.

Wir berechnen $\varphi(m) = (p-1)(q-1) = 179567532$ und setzen diese Zahl als n in den Taschenrechner ein. Es ist $\mathrm{ggT}(97251, 179567532) = 3$. Wir erhöhen die vorgeschlagene Zahl $e = 97251$ um 2 und erhalten $\mathrm{ggT}(97253, 179567532) = 1$.



Das zu e in $\mathbb{Z}/179567532\mathbb{Z}$ inverse Element ist $d = 83169053$.

Wir berechnen $m = pq = 2347 \cdot 76543 = 179646421$.

Der öffentliche Schlüssel ist $(179646421, 97253)$.

Der geheime Schlüssel ist $(2347, 76543)$ beziehungsweise 83169053.

Zum Dechiffrieren werden die Geheimtextzahlen in $\mathbb{Z}/179646421\mathbb{Z}$ in die 83169053-te Potenz erhoben.

Aufgabe 5.8.2 Wir übersetzen zunächst den Text in Zahlen:

$$\begin{array}{cccccc} 2309 & 0500 & 0913 & 1305 & 1800 & 2113 \\ 0013 & 0920 & 2005 & 1814 & 0103 & 0820. \end{array}$$

Wir geben 2923 als n und 725 als b in den Taschenrechner ein. Dann setzen wir die vierstelligen Zahlen, die unserem Klartext entsprechen jeweils als a in den Taschenrechner ein und bilden a^b. Wir erhalten die Ziffernfolge:

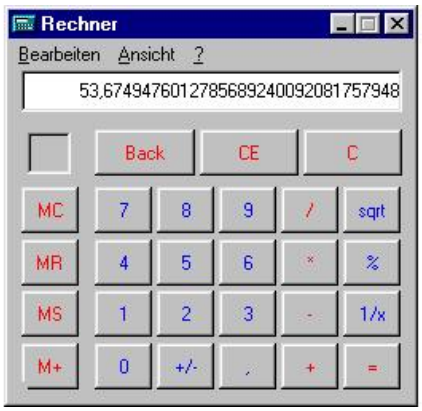
$$\begin{array}{cccccc} 1800 & 1280 & 1362 & 1987 & 0890 & 1135 \\ 1589 & 1685 & 1785 & 1111 & 2900 & 1153. \end{array}$$

Dies ist der Geheimtext, und den schicken wir an Alice.

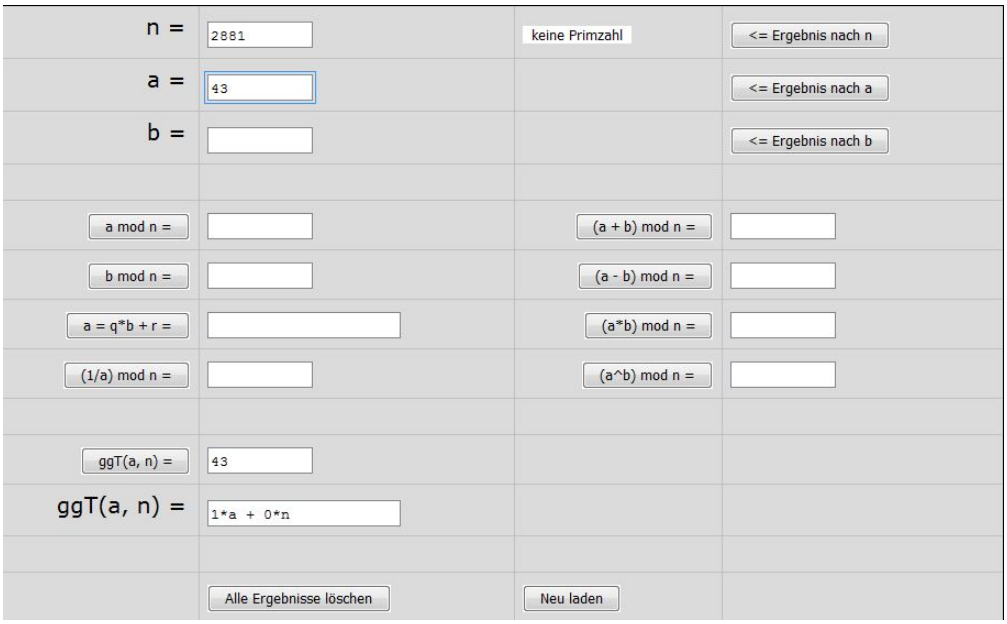
Aufgabe 5.8.3 Wir müssen versuchen, Alice' geheimen Schlüssel herzuleiten.

Wir wissen, dass $m = pq$ ist, wobei p und q verschiedene Primzahlen sind. Wie groß können diese Teiler von m maximal werden? Mit Hilfe des Taschenrechners (zum Beispiel dem des Computers) berechnen wir

$\sqrt{2881} =$

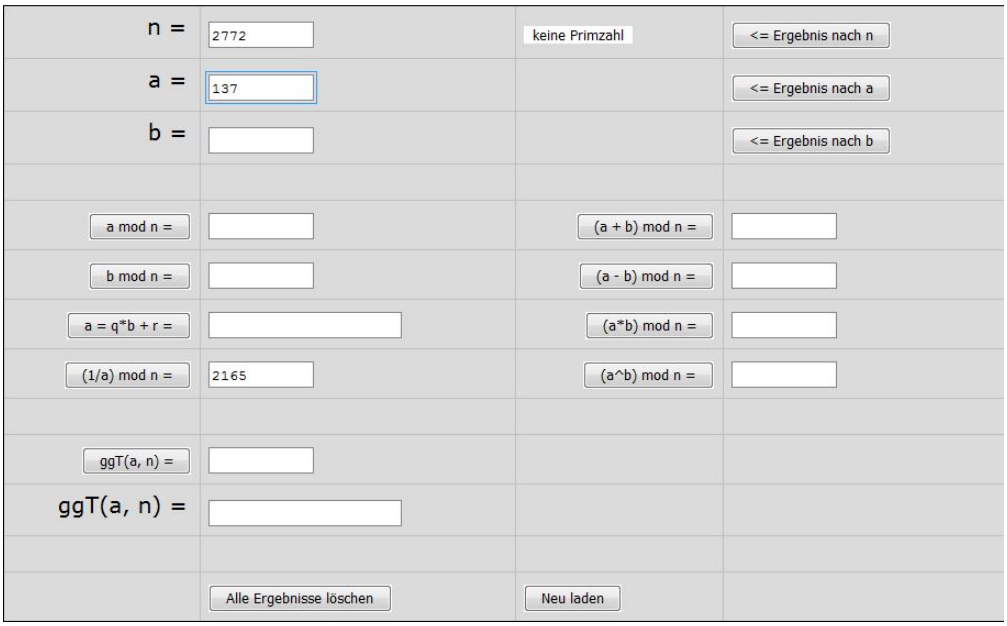


Einer der beiden Teiler von m muss daher eine Primzahl sein, die kleiner als 54 ist. Um einen solchen Teiler zu bestimmen, können wir den Taschenrechner benutzen. Wir geben 2881 als n ein. Als a geben wir Primzahlen ein, die kleiner als 54 sind und berechnen $\mathrm{ggT}(a, n)$. Nach einigen Versuchen finden wir:



Somit ist 43 ein Teiler von m, und es gilt $m = 43 \cdot 67$.

Als nächstes berechnen wir $(p-1)(q-1) = 42 \cdot 66 = 2772$. Diese Zahl tragen wir als n in den Taschenrechner ein. Weiter tragen wir die Zahl $e = 137$ als a in den Taschenrechner ein und berechnen das zu a inverse Element in $\mathbb{Z}/2772\mathbb{Z}$.



Es ist also $d = 2165$, und wir dechiffrieren, indem wir die abgefangenen Zahlen in

$\mathbb{Z}/2881\mathbb{Z}$ in die 2165-te Potenz erheben. Wir erhalten

$$\begin{array}{lllll} 0409 & 0519 & 0500 & 2601 & 0812 \\ 0514 & 0019 & 0914 & 0400 & 2621 \\ 0011 & 1205 & 0914. & & \end{array}$$

Die führenden Nullen müssen wir natürlich selbst einfügen.

In Buchstaben übersetzt erhalten wir den Klartext: „Diese Zahlen sind zu klein“.