Ein Algorithmus zur Zerlegung von Primzahlen in Primideale

Diplomarbeit

von

Damian Weber

nach einem Thema von Prof. Dr. Johannes Buchmann
Fachbereich 14 – Informatik
Universität des Saarlandes

April 1993

Eidesstattliche Erklärung

Hiermit versichere ich an Eides Statt, daß ich für die Anfertigung dieser Arbeit keine anderen als die angegebenen Quellen verwendet habe.

Saarbrücken, im April 1993

Damian Weber

Mein Dank richtet sich in besonderer Weise an Herrn Professor Buchmann. Er gab mir die Anregung, an diesem interessanten Thema zu arbeiten und hat mich in zahlreichen Gesprächen durch wertvolle Ratschläge unterstützt.

Außerdem gilt mein Dank Christine Hollinger, Erik Scheid und Georg Lay für das sorgfältige und kritische Durchsehen des Manuskriptes.

Schließlich danke ich meiner Freundin Karen Blaich für das eingehende Prüfen der syntaktischen Korrektheit und ihrer Geduld in der arbeitsreichen Zeit der Fertigstellung dieser Arbeit.

Inhaltsverzeichnis

Kapitel 1

Einführung

1.1 Einleitung

In dieser Arbeit wird ein Algorithmus zur Zerlegung von Primzahlen p innerhalb von p–maximalen Ordnungen $\mathcal{O}$ algebraischer Zahlkörper vorgestellt.

Ein algebraischer Zahlkörper $\mathcal{K}$ ist eine endliche Körpererweiterung über dem Körper der rationalen Zahlen und $\mathcal{O}_{\mathcal{K}}$ der Ring der ganzen algebraischen Zahlen von $\mathcal{K}$. Wir verstehen unter einer p–maximalen Ordnung $\mathcal{O}$ einen Teilring von $\mathcal{O}_{\mathcal{K}}$, in dem die Primzahl p eindeutig als Produkt von Primidealen darstellbar ist. Unser Verfahren ist in der Hinsicht allgemein, daß damit jede Primzahl p in jeder Teilordnung $\mathcal{O}$ von $\mathcal{O}_{\mathcal{K}}$ zerlegt werden kann, sofern diese p–maximal ist. Insbesondere sind hiermit auch Teiler des Index $[\mathcal{O}_{\mathcal{K}} : \mathbb{Z}[\rho]]$ zerlegbar, was mit dem bekannten Satz von Dedekind[1] über die Faktorisierung des Körperpolynoms über $\mathbb{F}_p$ nicht möglich ist.

Ein wichtiges Problem, zu dessen Lösung die Kenntnis der Primidealzerlegung der Primzahl p vonnöten ist, ist die Berechnung der Klassengruppe beliebiger Zahlkörper, siehe z.B. [Schm1], [Schm2] oder [Sche]. Die Klassengruppe wird nämlich gerade von den Primidealen der Zerlegung von $p\mathcal{O}_{\mathcal{K}}$ erzeugt, wobei $p < O(\log^2 \Delta)$.

Eine weitere Anwendung ist die Berechnung von Euler–Produkten[2], die die Werte der auf Ideale verallgemeinerten Riemann'schen ζ–Funktion[3] liefern und damit unter Benutzung der analytischen Klassenzahlformel eine Approximation der Klassenzahl liefern [Stew].

Die Kenntnis der Klassenzahl kann dazu verwendet werden, spezielle Diophantische Gleichungen[4] zu lösen — wie beispielsweise $y^2+4 = z^3$ — mit der sich schon Fermat[5]

---

[1] Richard Dedekind, 1831–1916
[2] Leonhard Euler, 1707–1783
[3] Bernhard Riemann, 1826–1866
[4] Diophantos von Alexandria, um 250 n. Chr.
[5] Pierre de Fermat, 1601–1665

beschäftigte, oder $x^2 + 7 = 2^n$ (Ramanujan[6]) und sogar zur Lösung von Fermats letztem Problem $x^n + y^n = z^n$ im Falle regulärer Primzahlen n beitragen [Stew].

Der Zusammenhang zwischen Zahlkörpern und elliptischen Kurven basiert auf der Tatsache, daß die Anzahl der Idealklassen der Ordnung $\mathcal{O}$ eines algebraischen Zahlkörpers gleich der Anzahl der Isomorphieklassen elliptischer Kurven über $\mathbb{Q}$ ist, deren Endomorphismenringe isomorph zu $\mathcal{O}$ sind [Shi].

Die endgültige Form unseres Algorithmus benutzt Ideen von J. Buchmann und H.W. Lenstra, die in [BuLen] beschrieben sind. Unter Zuhilfenahme praktischer Tests konnte das dort vorgestellte Grundverfahren entscheidend verbessert werden. Das Verfahren beruht wesentlich auf der R–Modulstruktur der Ordnungen $\mathcal{O}$ und verwendet daher vor allem Techniken aus der Linearen Algebra.

Die objektorientierte Implementierung erlaubt die Verwendung von algebraischen Strukturen in einer Programmiersprache. Die zugehörigen Operationen sind so realisiert worden, daß die Arithmetik mit Elementen algebraischer Strukturen in gewohnter Weise mit den Symbolen { +,–,∗ } dargestellt werden kann.
Die hier neu definierten abstrakten Datentypen — wie beispielsweise Elemente und Ideale von Ordnungen oder Matrizen und Vektoren über Körpern — können dann wie die Standarddatentypen behandelt werden.
Aufbauend auf diesen Datentypen können Algorithmen der algebraischen Zahlentheorie und der Linearen Algebra in bequemer Weise implementiert werden.

1.2 Der Aufbau dieser Arbeit

Im weiteren Verlauf dieses Kapitels werden die verwendeten mathematischen Symbole sowie die Darstellung der beschriebenen Algorithmen eingeführt. Letztere werden in einer einheitlichen, an [Meh] angelehnten, aber weiterentwickelten Form dargeboten.

In Kapitel 2 werden die notwendigen Begriffe und Resultate der algebraischen Zahlentheorie zusammengestellt, die überwiegend verbreiteten Standardwerken entnommen wurden.

Kapitel 3 beschäftigt sich mit der algorithmischen Seite der algebraischen Zahlentheorie und stellt in der Hauptsache Verfahren vor, die der Realisierung der Arithmetik in der Ordnung eines algebraischen Zahlkörpers dienen.

Schließlich kann in Kapitel 4 — aufbauend auf den in Kapitel 2 eingeführten Begriffen und den in Kapitel 3 beschriebenen Operationen — die Grundidee des gesamten Verfahrens vorgestellt werden; dies bietet auch gleichzeitig einen Überblick über die

[6] Srinivasa Ramanujan, 1887–1920

zu bewältigenden Teilaufgaben. Danach wird jeder Schritt des Verfahrens ausführlich beschrieben.

In Kapitel 5 wird eingehend auf die Implementierung in der Programmiersprache C++ eingegangen. Es werden die Vorteile gegenüber der Verwendung von reinem C–Code herausgestellt; außerdem werden die Konzepte objektorientierter Programmierung in Verbindung mit Algorithmen der algebraischen Zahlentheorie verdeutlicht.

Abschließend beinhaltet das Kapitel 6 eine kurze Diskussion über die worst–case–Laufzeit, die Zusammenstellung von praktischen Tests und eine heuristische Aussage über die erwartete Laufzeit.

1.3 Bezeichnungen

Wir benutzen die für Zahlenmengen üblichen Bezeichnungen:

$\mathbb{N}$ – die Menge der natürlichen Zahlen

$\mathbb{N}_0$ – die Menge der natürlichen Zahlen einschließlich der 0

$\mathbb{Z}$ – die Menge der ganzen Zahlen

$\mathbb{Q}$ – die Menge der rationalen Zahlen

$\mathbb{R}$ – die Menge der reellen Zahlen

$\mathbb{C}$ – die Menge der komplexen Zahlen

$\mathbb{F}_p$ – der Primkörper der Charakteristik p mit p Elementen

Für eine Matrix A in ${\mathbb{F}_p}^{m \times n}, \mathbb{Z}^{m \times n}$ oder $\mathbb{Q}^{m \times n}$ verwenden wir die übliche Schreibweise a_{ij} für das Element in der i-ten Zeile und j-ten Spalte.

Außerdem wird, da wir uns oft auf Spalten von Matrizen beziehen werden, mit A_j die j-te Spalte von A bezeichnet.

In einem R-Modul V wird mit

$$\langle v_1, v_2, \ldots, v_n \rangle_R \quad \text{mit } v_i \in V, 1 \leq i \leq n$$

die Menge

$$\left\{ \sum_{i=1}^{n} r_i v_i \mid r_i \in R \right\}$$

bezeichnet.

1.4 Darstellung der Algorithmen

Die Beschreibung der verwendeten Algorithmen wurde nach dem Muster in [Meh] durchgeführt. Diese Form eines an höhere Programmiersprachen angelehnten Pseudo-Codes wird seit Jahren in der zweisemestrigen Vorlesung 'Algorithmen und Komplexität' an der Universität des Saarlandes benutzt. Aus diesem Pseudo-Code lassen sich auf einfache Weise Programme in den Programmiersprachen PASCAL, C und C++ erzeugen.

Zu Beginn eines Algorithmus wird ein Programmkopf erzeugt, der seinen Namen und die Spezifikation der Ein– und Ausgabedaten enthält.

Algorithmus PROGRAMMNAME

Eingabe: Eingabedaten

Ausgabe: Ausgabedaten

Danach folgen durchnumerierte Zeilen, die jeweils eine Anweisung enthalten.

Es werden drei verschiedene Typen von Schleifen verwendet:

1. die **for**-Schleife

   (a) mit inkrementierter Schleifenvariable

   for $z \leftarrow a$ **to** e **do**
   Anweisung 1
   $\vdots$
   Anweisung n
   od

   Hierbei sind a und e arithmetische Ausdrücke in Variablen und Konstanten; die Variable z wird auf den Wert a gesetzt und bei **od** jeweils inkrementiert. Falls zu Beginn $a > e$ gilt, wird der Anweisungsblock nicht ausgeführt.

   (b) mit dekrementierter Schleifenvariable

   for $z \leftarrow a$ **down to** e **do**
   Anweisung 1
   $\vdots$
   Anweisung n
   od

   Hierbei sind a und e arithmetische Ausdrücke in Variablen und Konstanten; die Variable z wird auf den Wert e gesetzt und bei **od** jeweils dekrementiert. Falls zu Beginn $a < e$ gilt, wird der Anweisungsblock nicht ausgeführt.

2. die **while-do**-Schleife

   while *Bedingung* **do**
           Anweisung 1
           ⋮
           Anweisung n
           od

   Dieses ist eine *pre-checked loop.* Zuerst wird die Gültigkeit der Bedingung geprüft, und danach werden im Falle der Gültigkeit die Anweisungen solange ausgeführt, bis die Bedingung ungültig ist.

3. die **do-while**-Schleife

   do
       Anweisung 1
       ⋮
       Anweisung n
   while *Bedingung*

   Dieses ist eine *post-checked loop.* Zuerst werden die Anweisungen einmal ausgeführt; danach wird die Gültigkeit der Bedingung geprüft. Solange die Bedingung gültig bleibt, werden die Anweisungen wiederholt.
   In manchen Veröffentlichungen wird hierfür das Konstrukt **repeat–until** verwendet. Die hier eingesetzte Form steht jedoch der Sprache C näher, weshalb auf **repeat–until** verzichtet wurde.

Zum Zwecke einer übersichtlichen Darstellung wurde der **break**–Befehl aufgenommen, der eine sofortige Beendigung der aktuellen Schleife bewirkt.

Programmverzweigungen werden mit Hilfe von

if *Bedingung* **then**
        Anweisung 1
        ⋮
        Anweisung n
        else
        Anweisung 1'

(7) $\vdots$
(8) *Anweisung n'*
(9) **fi**

---

dargestellt und bedürfen keiner weiteren Erläuterung. Bei einem leeren **else**-Teil wird dieser weggelassen.

Die hinter **Ausgabe** angegebenen Ausgabedaten eines Algorithmus werden mit Hilfe der **return**–Anweisung der aufrufenden Prozedur zur Verfügung gestellt. Eine **return**–Anweisung beendet einen solchen Teilalgorithmus.

Kommentare schließen wir durch '**co** Kommentar **oc**' ein.

Kapitel 2

Algebraische Zahlkörper

2.1 Bezeichnungen

Wir stellen einige Begriffe und bekannte Resultate der Algebra — insbesondere der algebraischen Zahlentheorie — zusammen, die den Werken [Hun, Hor, Stew, PohZa] entnommen wurden. Nähere Einzelheiten sowie Beweise zu den aufgeführten Sätzen sind dort enthalten.

2.1 Definition *Eine Zahl $\alpha \in \mathbb{C}$ heißt* algebraisch *über $\mathbb{Q}$, falls es ein vom Nullpolynom verschiedenes Polynom*

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n \in \mathbb{Q}[X]$$

gibt mit $f(\alpha) = 0$. Falls f irreduzibel über $\mathbb{Q}$ ist und $a_n = 1$ gilt, so heißt f das Minimalpolynom *von α. In diesem Falle heißt n der* Grad *von α.*

2.2 Definition *Ein Teilkörper $\mathcal{K}$ von $\mathbb{C}$ heißt* algebraischer Zahlkörper, *falls für die Dimension des Vektorraums $\mathcal{K}$ über $\mathbb{Q}$*

$$dim_{\mathbb{Q}}\mathcal{K} < \infty$$

gilt.

Man sieht leicht, daß algebraische Zahlkörper nur algebraische Zahlen enthalten können.
Da wir eine Primzahl p in einem Ring aus ganzalgebraischen Zahlen zerlegen wollen, benötigen wir die folgende Definition.

2.3 Definition *Sei $\alpha \in \mathbb{C}$. Falls es ein vom Nullpolynom verschiedenes Polynom*

$$f(X) = a_0 + a_1X + a_2X^2 + \cdots + a_{n-1}X^{n-1} + X^n \in \mathbb{Z}[X] \tag{2.1}$$

mit $f(\alpha) = 0$ gibt, so heißt α eine ganzalgebraische *oder* ganze algebraische *Zahl.*

2.4 Beispiel Sei $\rho = \sqrt[3]{19}$.

ρ ist eine ganzalgebraische Zahl wegen $\rho^3 - 19 = 0$.

Es ist

$$\vartheta := \frac{1 + \rho + \rho^2}{3}$$

eine ganzalgebraische Zahl wegen $\vartheta^3 - \vartheta^2 - 6\vartheta - 12 = 0$.

2.5 Definition *Seien $n \in \mathbb{N}$ und X eine Menge algebraischer Zahlen.*
Dann bedeutet

$$\mathbb{Q}(X) := \bigcap_{\substack{L \text{ Körper} \\ X \subset L}} L.$$

Offensichtlich wird im Spezialfall von $X = \{\alpha\}$ der Körper $\mathcal{K} = \mathbb{Q}(\alpha)$ von allen Potenzen von α über $\mathbb{Q}$ erzeugt:

2.6 Lemma *Sei α algebraisch vom Grad n über $\mathbb{Q}$.*
Dann ist $\mathbb{Q}(\alpha) =< 1, \alpha, \alpha^2, \ldots, \alpha^{n-1} >_{\mathbb{Q}}$.

Der bekannte Satz vom primitiven Element berechtigt dazu, jeden algebraischen Zahlkörper auf diese Weise darzustellen [Stew, Th. 2.2.].

2.7 Satz *Sei $\mathcal{K}$ ein algebraischer Zahlkörper. Dann gibt es eine algebraische Zahl α, so daß*

$$\mathcal{K} = \mathbb{Q}(\alpha).$$

Im wichtigen Anwendungsfall der Klassengruppenberechnung hat man diese Darstellung von $\mathcal{K}$ durch ein α definierendes Polynom gegeben.

2.2 Der Ganzheitsring $\mathcal{O}_{\mathcal{K}}$ von $\mathcal{K}$

Wir führen nun mit $\mathcal{O}_{\mathcal{K}}$ den Ring der ganzalgebraischen Zahlen von $\mathcal{K}$ ein und beschreiben einige seiner wesentlichen Eigenschaften.

2.8 Definition *Sei $\mathcal{O}$ ein beliebiger Teilring von $\mathcal{K}$, der nur ganzalgebraische Zahlen enthält. Dann heißt $\mathcal{O}$ eine* Ordnung *von $\mathcal{K}$.*

2.9 Bemerkung Die $\subseteq$–Relation definiert eine partielle Ordnung auf der Gesamtheit der Ordnungen von $\mathcal{K}$. Bezüglich dieser Ordnungen gibt es ein maximales Element; dazu geben wir die folgende Definition.

2.10 Definition *Sei $\mathcal{O}$ eine Ordnung in $\mathcal{K}$. Falls es keine Ordnung $\mathcal{O}'$ in $\mathcal{K}$ gibt mit $\mathcal{O} \subsetneqq \mathcal{O}'$, so heißt $\mathcal{O}$ die* Maximalordnung *oder der* Ganzheitsring *von $\mathcal{K}$ und wird mit $\mathcal{O}_{\mathcal{K}}$ bezeichnet.*

2.11 Bemerkung Damit die Zerlegung der Primzahl p in Primideale eindeutig ist, muß man als Zahlenbereich nicht unbedingt die Maximalordnung verlangen; es genügt, wenn die Primzahl p den Index $[\mathcal{O}_{\mathcal{K}} : \mathcal{O}]$ nicht teilt (vgl. [BuLen, Kap. 6]). Der Index ist folgendermaßen definiert.

2.12 Definition *Sei $\mathcal{O}_{\mathcal{K}}$ die Maximalordnung von $\mathcal{K}$. Für jede Ordnung $\mathcal{O}$ von $\mathcal{K}$ bezeichnen wir mit*

$$[\mathcal{O}_{\mathcal{K}} : \mathcal{O}] := dim_{\mathcal{O}}\mathcal{O}_{\mathcal{K}}$$

den Index von $\mathcal{O}$ in $\mathcal{O}_{\mathcal{K}}$.

Die uns interessierenden Ordnungen charakterisieren wir durch p–Maximalität.

2.13 Definition *Sei $\mathcal{O}$ eine Ordnung in $\mathcal{K}$ und p eine Primzahl. Dann heißt die Ordnung $\mathcal{O}$* p-maximal, *falls p den Index $[\mathcal{O}_{\mathcal{K}} : \mathcal{O}]$ nicht teilt.*

2.14 Bemerkung Wegen $[\mathcal{O}_{\mathcal{K}} : \mathcal{O}_{\mathcal{K}}] = 1$ ist insbesondere $\mathcal{O}_{\mathcal{K}}$ für alle Primzahlen p schon p–maximal.

Wir betrachten nun die uns interessierenden Teilmengen von $\mathcal{O}$. Der Begriff Ideal steht für eine Teilstruktur des Rings $\mathcal{O}$, für die dort neben den bekannten Eigenschaften in allgemeinen Ringen weitere Beziehungen gelten.

2.15 Definition *Sei R ein kommutativer Ring. Ein* Ideal *in R ist eine Teilmenge I von R mit folgenden Eigenschaften:*

1. *$(I, +)$ ist eine abelsche Gruppe.*
2. *$r \in R, a \in I \Rightarrow ra \in I$*

Man schreibt $I \trianglelefteq R$.

2.16 Bemerkung Offensichtlich ist ein Ideal I des kommutativen Ringes R mit Einselement 1 genau dann gleich R, wenn $1 \in I$ gilt.

2.17 Lemma *Sei R ein kommutativer Ring mit Einselement und seien $I, J \trianglelefteq R$ Ideale. Dann ist auch $I \cap J$ ein Ideal in R.*

Der Beweis ergibt sich direkt aus der Idealeigenschaft von I und J.

Als Beispiele für den Begriff des Ideals führen wir für ein Element $c \in R$ die Menge aller Vielfachen cR und den Annullator $Ann\ c$ ein.

2.18 Definition *Sei R ein kommutativer Ring mit Einselement. Dann bezeichnen wir mit*

$$cR := \{cr \mid r \in R\}$$

die Menge aller Vielfachen von c und mit

$$Ann_R\ c := \{r \in R \mid cr = 0\}$$

den Annullator von c in R.

2.19 Bemerkung Falls aus dem Zusammenhang klar ist, daß der Ring R gemeint ist, schreiben wir auch kurz $Ann\ c$ für $Ann_R\ c$.

Die in Definition 2.18 erklärten Teilmengen von R sind sogar Ideale in R. Wir notieren dies in dem folgenden

2.20 Lemma *Sei R ein kommutativer Ring mit Einselement und sei $c \in R$. Dann sind cR und $Ann\ c$ Ideale in R.*

Beweis: Seien $a, b \in cR$, $a = ca'$ und $b = cb'$. Dann folgt $a - b = ca' - cb' = c(a' - b') \in cR$. Also ist $(cR, +)$ Untergruppe von $(R, +)$. Weiter haben wir $ra = rca' = cra' \in cR$ für jedes $r \in R$ und damit Bedingung (2) von Definition 2.15 gezeigt.

Sind nun $a, b \in Ann\ c$, so gilt $ca = cb = 0$, also auch $c(a - b) = ca - cb = 0$ und $(Ann\ c, +)$ ist Untergruppe von $(R, +)$. Weiterhin gilt $cra = rca = r0 = 0$ für jedes $r \in R$, daher ist auch $Ann\ c$ ein Ideal von R. ■

Wir werden die Idealeigenschft dieser beiden Mengen benutzen, um Quotientenstrukturen zu bilden. Dabei tritt der wichtige Fall auf, daß c ein Nullteiler in R ist. Man gewinnt dadurch eine leicht verschärfte Aussage, die wir in dem nächsten Lemma festhalten.

2.21 Lemma *Sei R ein kommutativer Ring mit Einselement und sei $c \in R$ ein Nullteiler. Dann sind cR und $Ann\ c$ echte Ideale in R, also*

$$\begin{array}{cccc} (0) \subsetneqq & cR & \subsetneqq & R \\ (0) \subsetneqq & Ann\ c & \subsetneqq & R. \end{array}$$

Beweis: Sei $0 \neq a \in R$ so gewählt, daß $ca = 0$. Unter Verwendung von Bemerkung 2.16 sieht man

1. $(0) \subsetneqq cR$ wegen $c \in cR$
2. $cR \subsetneqq R$, da $1 \in cR$ sofort $a = 1a = cra = rca = r0 = 0$ zur Folge hätte
3. $(0) \subsetneqq Ann\ c$ wegen $0 \neq a \in Ann\ c$
4. $Ann\ c \subsetneqq R$, da wegen $1c = c \neq 0$ schon $1 \notin Ann\ c$ gilt.

■

Die Verwendung von Algorithmen der Linearen Algebra zur Ausführung der Idealarithmetik beruht wesentlich auf der R-Modul-Struktur von $\mathcal{O}$ [Stew, Th.2.15]:

2.22 Satz *Seien $\mathcal{K}$ ein algebraischer Zahlkörper vom Grad n, $\mathcal{O}_\mathcal{K}$ sein Ganzheitsring und I ein Ideal in $\mathcal{O}_\mathcal{K}$. Dann sind $\mathcal{O}_\mathcal{K}$ und I freie $\mathbb{Z}$-Moduln vom Rang n.*

Wir halten einen wichtigen Spezialfall davon fest, da wir nicht nur die Maximalordnung betrachten.

2.23 Korollar *Jede Ordnung $\mathcal{O}$ von $\mathcal{K}$ ist ein freier $\mathbb{Z}$-Modul vom Rang n.*

2.24 Definition *Sei $\mathcal{O}_\mathcal{K}$ der Ganzheitsring des algebraischen Zahlkörpers $\mathcal{K}$. Eine $\mathbb{Z}$-Basis für $\mathcal{O}_\mathcal{K}$ heißt* Ganzheitsbasis.

2.25 Beispiel Eine Ganzheitsbasis für $\mathbb{Q}(\sqrt{5})$ ist

$$\left\{1, \frac{1+\sqrt{5}}{2}\right\}.$$

Die Berechnung einer Ganzheitsbasis eines gegebenen algebraischen Zahlkörpers ist ein nichttriviales Problem. Da unser Algorithmus jedoch als Eingabe eine Ordnung benötigt, wird diese mit Hilfe einer Multiplikationstabelle angegeben, die aus einer vorberechneten Ganzheitsbasis gebildet werden kann. Zur Berechnung von Ganzheitsbasen haben wir uns des Programmpaketes [PARI] bedient.

2.3 Ideale in $\mathcal{O}$

2.3.1 Multiplikation von Idealen, Teilbarkeit

Wir sind interessiert an einem Produkt von Idealen, das gleich dem Ideal $p\mathcal{O} \trianglelefteq \mathcal{O}$ ist. Die Multiplikationsvorschrift entnimmt man der folgenden

2.26 Definition *Seien $I, J \trianglelefteq \mathcal{O}$ Ideale mit $\mathbb{Z}$-Basen*

$$\begin{aligned} I &= <\alpha_1, \alpha_2, \ldots, \alpha_n>_\mathbb{Z} \\ J &= <\beta_1, \beta_2, \ldots, \beta_n>_\mathbb{Z}. \end{aligned}$$

Dann ist

$$I \cdot J := <\alpha_1 \cdot \beta_1, \alpha_1 \cdot \beta_2, \ldots, \alpha_i \cdot \beta_j, \ldots, \alpha_n \cdot \beta_n>_\mathbb{Z}. \tag{2.2}$$

Analog zu der bekannten Teilbarkeitstheorie über Elemente in $\mathbb{Z}$ legen wir einen Teilbarkeitsbegriff für Ideale fest.

2.27 Definition *Seien $A, B \trianglelefteq \mathcal{O}$ Ideale. Dann bedeutet*

$$A \mid B :\Longleftrightarrow \exists C \trianglelefteq \mathcal{O}, \quad \textit{so daß} \quad B = A \cdot C. \tag{2.3}$$

In diesem Falle sagt man A teilt *B.*

Wir benutzen oft, ohne es besonders zu erwähnen, das

2.28 Lemma *Seien $A, B \trianglelefteq \mathcal{O}$ Ideale. Dann gilt*

$$A \mid B \iff B \subseteq A.$$

2.3.2 Primideale und maximale Ideale

Analog zu Primzahlen und irreduziblen Elementen definiert man die Begriffe Primideal und maximales Ideal.

2.29 Definition *Sei R ein kommutativer Ring. Ein Ideal $P \trianglelefteq R$ heißt* Primideal, *wenn $P \neq R$ und für alle $A, B \trianglelefteq R$ gilt*

$$A \cdot B \subseteq P \Rightarrow A \subseteq P \vee B \subseteq P. \tag{2.4}$$

2.30 Beispiel Das Ideal (3) ist Primideal in $\mathbb{Z}$, aber nicht das Ideal (15), da

$$(3) \cdot (5) = (15),$$

aber $(3) \not\subseteq (15)$ und $(5) \not\subseteq (15)$.

2.31 Definition *Sei R ein kommutativer Ring. Ein Ideal $M \trianglelefteq R$ heißt* maximales Ideal, *wenn $M \neq R$ und für jedes Ideal $A \trianglelefteq R$ mit $M \subseteq A \subseteq R$*

$$A = R \textit{ oder } A = M \tag{2.5}$$

gilt.

2.32 Beispiel Das Ideal (2) ist maximal in $\mathbb{Z}$, aber nicht das Ideal (4), da

$$(4) \subsetneqq (2) \subsetneqq \mathbb{Z}.$$

Da $\mathcal{O}$ ein kommutativer Ring mit Einselement ist, gilt [Hun, Th.III,2.19]

2.33 Lemma *Jedes maximale Ideal in $\mathcal{O}$ ist ein Primideal.*

Da wir interessiert sind, maximale Ideale zu finden, die $p\mathcal{O}$ teilen, benötigen wir einen effektiven Maximalitätstest für ein gegebenes Ideal M. Dieser verwendet eine Tatsache, die wir in dem folgenden Satz [Hor, Satz 41.1] festhalten.

2.34 Satz *Sei $M \trianglelefteq R$ ein Ideal des kommutativen Rings R mit Einselement. Dann gilt*

$$M \quad maximal \iff {}^{R}\!/_{M} \quad Körper. \tag{2.6}$$

Die Charakterisierung von Primidealen durch Quotientenbildung erfolgt in ähnlicher Weise [Hor, Satz 40.1].

2.35 Satz *Sei $P \trianglelefteq R$ ein Ideal des kommutativen Ringes R mit Einselement. Dann gilt*

$$P \quad Primideal \iff {}^{R}\!/_{P} \quad Integritätsring. \tag{2.7}$$

In $\mathcal{O}$ können wir nun die Begriffe maximales Ideal und Primideal synonym benutzen, da für jedes Ideal I der Restklassenring $\mathcal{O}/I$ endlich ist. Dies schließt man unter Verwendung der Tatsache, daß endliche Integritätsringe stets Körper sind. Es gilt nämlich

$$\begin{array}{lcl} & P \text{ Primideal} & \\ \Rightarrow & \mathcal{O}/P & \text{Integritätsring} \\ \Rightarrow & \mathcal{O}/P & \text{Körper} \\ \Rightarrow & P & \text{maximales Ideal.} \end{array}$$

Da $\mathcal{O}$ insbesondere ein kommutativer Ring mit Einselement ist, haben wir die Möglichkeit, statt der Idealzerlegung auch eine Zerlegung von Faktorringen zu bestimmen. Aus den Faktorringen können danach die gesuchten Ideale konstruiert werden. Von dieser Möglichkeit wird in beiden Varianten des Algorithmus Gebrauch gemacht, die Grundlage dafür bildet eine Spezialisierung eines Korollares aus [Hun, Cor.III.2.27]:

2.36 Satz *Seien $I_1, I_2, \ldots, I_n$ Ideale in einem Ring R mit Einselement mit*

$$I_j + I_k = R \text{ für } 1 \leq j < k \leq n.$$

Dann gilt die Isomorphie

$$ {}^{R}\!/_{I_1 \cdot I_2 \cdots I_n} \quad \cong \quad {}^{R}\!/_{I_1} \times {}^{R}\!/_{I_2} \times \cdots \times {}^{R}\!/_{I_n}. \tag{2.8}$$

Der Ring $\mathcal{O}_K$ hat einige Eigenschaften, die kommutative Ringe im allgemeinen nicht besitzen. Da Dedekind durch die Untersuchung von Ringen ganzer algebraischer Zahlen den Grundstein für die algebraische Zahlentheorie legte, wurden diese Ringe nach ihm benannt [Hun, Def. VIII.6.1].

2.37 Definition *Ein* Dedekind-Ring *ist ein Integritätsbereich R, in dem sich jedes von R verschiedene Ideal in ein endliches Produkt von Primidealen zerlegen läßt.*

Es ist folgende Tatsache bekannt [PohZa]:

2.38 Satz *Für jeden algebraischen Zahlkörper $\mathcal{K}$ ist sein Ganzheitsring $\mathcal{O}_{\mathcal{K}}$ ein Dedekind-Ring.*

Wir zitieren die für uns notwendigen Eigenschaften eines Dedekind–Ringes (vgl. [Hun, Th.VIII.6.10]).

2.39 Satz *Für einen Dedekind–Ring R gelten:*

1. *R ist noethersch, d.h. jedes Ideal in R ist endlich erzeugt,*
2. *Jedes echte Ideal in R ist eindeutig als Produkt von Primidealen darstellbar.*

2.3.3 Addition von Idealen, ggT

Man erklärt die Summe zweier Ideale A, B eines Ringes R als Menge aller endlichen Summen von Produkten eines Elements aus A mit einem Element aus B. Liegt die Primidealzerlegung von A und B vor, so erinnert die Summenbildung an die ggT-Bildung in $\mathbb{Z}$.

2.40 Definition *Seien R ein kommutativer Ring mit Einselement und $A, B \trianglelefteq R$ Ideale. Dann heißt*

$$A + B := \{\sum_{i=1}^{k} a_i b_i \mid k \in \mathbb{N}, a_i \in A, b_i \in B, 1 \leq i \leq k\} \tag{2.9}$$

die Summe der Ideale A und B.

In einem Dedekind–Ring kann man $A + B$ als den größten gemeinsamen Teiler von A und B charakterisieren. Dies wird gerechtfertigt durch den

2.41 Satz *Seien R ein Dedekind–Ring und $A, B \trianglelefteq R$ Ideale mit eindeutiger Primidealzerlegung*

$$\begin{aligned} A &= \prod_P P^{e_P} \\ B &= \prod_P P^{e'_P}. \end{aligned}$$

Dann ist

$$A + B = \prod_P P^{min(e_P, e'_P)}. \tag{2.10}$$

2.3.4 Das p–Radikal I_p

Eine erste Information über die Zerlegung von $p\mathcal{O}$ wird durch das p–Radikal von $\mathcal{O}$ geliefert, das definiert ist als das Produkt aller maximalen Ideale, die $p\mathcal{O}$ teilen.

2.42 Definition *Seien R ein kommutativer Ring und I ein Ideal in R. Dann heißt*

$$Rad\ I := \bigcap_{\substack{P \supseteq I \\ P\, Primideal}} P \tag{2.11}$$

das Radikal *von I.*

Als Durchschnitt von Idealen ist auch $Rad\ I$ wieder ein Ideal von R (Lemma 2.17). Wir halten dies fest in folgendem

2.43 Lemma *Seien R ein kommutativer Ring und I ein Ideal in R. Dann ist $Rad\ I$ ebenfalls ein Ideal in R.*

Wir interessieren uns speziell für $Rad\ p\mathcal{O}$ und definieren

2.44 Definition *Für eine Ordnung $\mathcal{O}$ von $\mathcal{K}$ heißt*

$$I_p := Rad\ p\mathcal{O}$$

das p–Radikal *von $\mathcal{O}$.*

2.45 Bemerkung Da in $\mathcal{O}$ Teilbarkeit dasselbe wie Teilmengenbeziehung und Schnittmengenbildung dasselbe wie Bildung des kleinsten gemeinsamen Vielfachen bedeuten, gilt für I_p die folgende Beziehung:

$$I_p = \prod_{M | p\mathcal{O}} M.$$

Hierbei durchläuft M alle maximalen Ideale, die $p\mathcal{O}$ teilen.

2.46 Beispiel In einer p–maximalen Ordnung $\mathcal{O}$ sei die eindeutige Primidealzerlegung von $p\mathcal{O}$ gegeben durch

$$p\mathcal{O} = P^2 \cdot Q^2.$$

Dann ist

$$I_p = P \cap Q = P \cdot Q.$$

2.4 Idealarithmetik in $\mathcal{O}$ und $\mathcal{O}/p\mathcal{O}$

Wenn man Idealarithmetik in $\mathcal{O}$ über $\mathbb{Z}$ betreibt, so entsteht bei der Berechnung der Hermite-Normalform einer Matrix (siehe Def.2.52) das Phänomen der sogenannten Entry–Explosion [Schm1]. Dies bedeutet, man hat keine Kontrolle über die Größe der Zwischenergebnisse. Da wir nur Ideale betrachten, die $p\mathcal{O}$ enthalten, können wir dies umgehen, indem wir den Ring $\mathcal{O}$ nach $\mathcal{O}/p\mathcal{O}$ homomorph abbilden, die Operationen dort ausführen und dann wieder den Homomorphismus umkehren.

Da wir dieses Verfahren häufig benutzen, legen wir den kanonischen Epimorphismus

$$\begin{aligned} \Phi: \quad & \mathcal{O} && \to \mathcal{O}/p\mathcal{O} \\ & \alpha && \mapsto \overline{\alpha} := \alpha + p\mathcal{O} \end{aligned} \tag{2.12}$$

für das gesamte Verfahren fest.

Dieser Epimorphismus vermittelt eine effizient berechenbare bijektive Zuordnung zwischen den Idealen, die $p\mathcal{O}$ teilen, und den Idealen in $\mathcal{O}/p\mathcal{O}$. Sie beruht auf folgendem

2.47 Satz *Sei I ein Ideal eines Ringes R. Dann gibt es eine bijektive Zuordnung zwischen der Menge aller Ideale, die I enthalten und der Menge aller Ideale in R/I. Daher ist jedes Ideal in R/I von der Form J/I, wobei J ein Ideal in R ist.*

Zum Beweis siehe [Hun, Th.III.2.13].

Dem Satz ist zu entnehmen, daß für $I \trianglelefteq \mathcal{O}$ mit $p\mathcal{O} \subseteq I$ das entsprechende Ideal in $\mathcal{O}/p\mathcal{O}$ durch $\Phi(I) \trianglelefteq \mathcal{O}$ berechnet werden kann. Man kann umgekehrt auch I aus $\Phi(I)$ berechnen; dies benötigen wir jedoch erst im letzten Schritt des Algorithmus und verweisen für nähere Informationen auf Abschnitt 4.2.4.

Zur Struktur von $\mathcal{O}/p\mathcal{O}$ beweisen wir die folgende, leicht verallgemeinerte Aussage.

2.48 Satz *Sei $\mathcal{O}$ eine Ordnung in einem algebraischen Zahlkörper $\mathcal{K}$ und p eine Primzahl. Für ein Ideal I mit $p\mathcal{O} \trianglelefteq I \trianglelefteq \mathcal{O}$ ist dann der Restklassenring $\mathcal{O}/I$ ein $\mathbb{F}_p$–Vektorraum.*

Beweis:

Aus der $\mathbb{Z}$–Moduleigenschaft von $\mathcal{O}$ ergibt sich zunächst die $\mathbb{Z}$–Moduleigenschaft von $\mathcal{O}/I$.

Seien nun $a, b \in \mathbb{Z}$ mit gleicher Restklasse modulo p gegeben, also $b-a = kp,\ k \in \mathbb{Z}$. Dann gilt für die Multiplikation von a und b mit Elementen w aus $\mathcal{O}/I$:

$$b(w+I) = (a+kp)(w+I) = aw + \underbrace{pkw}_{\in p\mathcal{O}} + I = aw + I = a(w+I),$$

woraus man ablesen kann, daß der $\mathbb{Z}$–Modul $\mathcal{O}/I$ zum $\mathbb{F}_p$– Vektorraum $\mathcal{O}/I$ isomorph ist. ■

Für $\mathcal{O}/p\mathcal{O}$ schreiben wir auch gelegentlich $\overline{\mathcal{O}}$. Wir haben bei der Berechnung von Idealprodukten und Idealdivisionen stets folgende Situation gegeben:

Gegeben sind Ideale A, B mit $p\mathcal{O} \trianglelefteq A, B \trianglelefteq \mathcal{O}$. Gesucht ist $\overline{C} \trianglelefteq \mathcal{O}/p\mathcal{O}$ mit $C = \frac{B}{A}$, falls $A \mid B$, oder $C = B \cdot A$.

Es zeigt sich, daß zur Lösung dieser Aufgabe lediglich Grundalgorithmen der Linearen Algebra herangezogen werden müssen. Die Vorgehensweise orientiert sich an den Aussagen der folgenden Sätze, von denen die beiden ersten [BuLen, Kap. 4] entnommen wurden:

2.49 Satz *Seien $A, B \trianglelefteq \mathcal{O}$ Ideale mit $A, B \supseteq p\mathcal{O}$ und $A \mid B$. Sei C das Ideal in $\mathcal{O}$, so daß $A \cdot C = B$.*
Dann ist $\overline{C}$ der Kern der folgenden Abbildung

$$\begin{array}{rcl} \overline{\mathcal{O}} & \to & (\overline{A} \to \overline{\mathcal{O}}/\overline{B}) \\ \overline{\gamma} & \mapsto & (\overline{\alpha} \mapsto \overline{\gamma\alpha}). \end{array} \tag{2.13}$$

2.50 Satz *Seien $A, B \trianglelefteq \mathcal{O}$ Ideale mit $A, B \supseteq p\mathcal{O}$, und $\overline{A}, \overline{B}$ seien durch*

$$\begin{array}{rcl} \overline{A} & = & \langle \overline{\alpha_1}, \overline{\alpha_2}, \dots, \overline{\alpha_n} \rangle_{\mathbb{F}_p} \\ \overline{B} & = & \langle \overline{\beta_1}, \overline{\beta_2}, \dots, \overline{\beta_n} \rangle_{\mathbb{F}_p} \end{array}$$

gegeben.

Sei C das Ideal in $\mathcal{O}$, so daß $C = A \cdot B + p\mathcal{O}$.
Dann ist

$$\overline{C} := \langle \overline{\alpha_1 \cdot \beta_1}, \overline{\alpha_1 \cdot \beta_2}, \dots, \overline{\alpha_i \cdot \beta_j}, \dots, \overline{\alpha_n \cdot \beta_n} \rangle_{\mathbb{F}_p}. \tag{2.14}$$

2.51 Satz *Seien $A, B \trianglelefteq \mathcal{O}$ Ideale mit $A, B \supseteq p\mathcal{O}$, und $\overline{A}, \overline{B}$ seien durch*

$$\begin{array}{rcl} \overline{A} & = & \langle \overline{\alpha_1}, \overline{\alpha_2}, \dots, \overline{\alpha_k} \rangle_{\mathbb{F}_p} \\ \overline{B} & = & \langle \overline{\beta_1}, \overline{\beta_2}, \dots, \overline{\beta_l} \rangle_{\mathbb{F}_p} \end{array}$$

gegeben.

Sei C das Ideal in $\mathcal{O}$, so daß $C = A + B$.
Dann ist

$$\overline{C} := \langle \overline{\alpha}_1, \ldots, \overline{\alpha}_k, \overline{\beta}_1, \ldots, \overline{\beta}_l \rangle_{\mathbb{F}_p}. \tag{2.15}$$

Beweis: Das Ideal C ist als größter gemeinsamer Teiler von A und B erst recht ein Teiler von $p\mathcal{O}$ und gehört somit zu den Idealen von $\mathcal{O}$, die durch Φ bijektiv nach $\mathcal{O}/p\mathcal{O}$ abgebildet werden. Daher wird $\overline{C}$ über $\mathbb{F}_p$ vom Bild von $A + B$ unter Φ erzeugt; dieses ist aber durch

$$\langle \overline{\alpha_1}, \overline{\alpha}_2, \ldots, \overline{\alpha}_k, \overline{\beta}_1, \overline{\beta}_2, \ldots, \overline{\beta}_l \rangle_{\mathbb{F}_p} \tag{2.16}$$

gegeben. ■

2.5 Darstellung der Elemente von $\mathcal{K}$ und $\mathcal{O}$

In diesem Abschnitt sei $\mathcal{K} = \mathbb{Q}(\rho)$ ein algebraischer Zahlkörper vom Grad n und $\mathcal{O}$ eine Ordnung in $\mathcal{K}$. Wir stellen die Elemente von $\mathcal{K}$, $\mathcal{O}$ und $\mathcal{O}/p\mathcal{O}$ als Tupel über $\mathbb{Z}$ bzw. $\mathbb{F}_p$ dar:

Sei $\alpha \in \mathcal{K}$,

$$\alpha = \frac{1}{d} \sum_{i=0}^{n-1} a_i \rho^i, d \in \mathbb{N}, a_i \in \mathbb{Z} \; mit \; \mathrm{ggT}(d, a_0, \ldots, a_{n-1}) = 1.$$

Dann wird α eindeutig repräsentiert durch den Vektor

$$(a_0, \ldots, a_{n-1}, d) \in \mathbb{Z}^{n+1}.$$

Sei $\{\omega_1, \ldots, \omega_n\}$ eine $\mathbb{Z}$–Basis für $\mathcal{O}$ und

$$\beta \in \mathcal{O}, \beta = \sum_{i=1}^{n} b_i \omega_i, \text{ mit } b_i \in \mathbb{Z}, 1 \leq i \leq n.$$

Dann repräsentieren wir β eindeutig durch den Vektor $(b_1, \ldots, b_n) \in \mathbb{Z}^n$.

Sei $\overline{\beta} \in \mathcal{O}/p\mathcal{O}$,

$$\overline{\beta} = \sum_{i=1}^{n} \overline{b_i}\overline{\omega_i}, \; \overline{b_i} \in \mathbb{F}_p, \; 1 \leq i \leq n.$$

Dann wird β eindeutig repräsentiert durch den Vektor $(\overline{b_1}, \ldots, \overline{b_n}) \in {\mathbb{F}_p}^n$.

2.6 Darstellung von Idealen in $\mathcal{O}$ und $\mathcal{O}/p\mathcal{O}$

Sei $\mathcal{O}$ wie im letzten Abschnitt gegeben, $I \trianglelefteq \mathcal{O}$ ein Ideal und $\overline{I} \trianglelefteq \mathcal{O}/p\mathcal{O}$ sein Bild unter Φ. Dann gibt es nach Satz 2.22 eine $\mathbb{Z}$–Basis von n Elementen für I.

Sei also $I = \langle v_1, \ldots, v_n \rangle_{\mathbb{Z}}$, wobei

$$v_i = \sum_{j=1}^{n} v_{ij} w_j \qquad 1 \leq i \leq n. \tag{2.17}$$

Dann stellen wir das Ideal I durch die Matrix $V := (v_{ij})_{1 \leq i,j \leq n}$ dar.Wir nennen eine solche Matrix *Darstellungsmatrix* des Ideals I und bezeichnen sie mit M_I. Entsprechend stellen wir das Ideal $\overline{I}$ durch die Matrix $\overline{V} := (\overline{v_{ij}})_{i,j}$ dar, wobei das Überstreichen Restklassenbildung nach $\mathbb{Z}/p\mathbb{Z}$ bedeutet. Falls alle Komponenten eines v_i durch p teilbar sind, entstehen bei der Restklassenbildung Spalten, die gleich 0 sind. Diese werden bei der Darstellung nicht berücksichtigt.

Die $\mathbb{Z}$-Basis-Darstellung eines Ideals ist nicht eindeutig, da für jedes $a \in \mathbb{Z}$ auch

$$I =< v_1, \ldots, v_i + av_j, \ldots, v_j, \ldots, v_n >_{\mathbb{Z}} \tag{2.18}$$

eine Basisdarstellung für I ist.

Dies liegt daran, daß sich Basen von $\mathbb{Z}$-Modulen durch Folgen unimodularer Spaltenoperationen ineinander überführen lassen.

Eine *unimodulare* Spaltenoperation ist eine der folgenden Operationen:

1. Addition eines Vielfachen einer Spalte zu einer anderen
2. Multiplikation einer Spalte mit -1
3. Vertauschung zweier Spalten.

Man sieht leicht, daß eine Folge unimodularer Operationen auf $A \in \mathbb{Z}^{m \times n}$ auch durch Multiplikation von A mit einer Matrix $T \in \mathcal{SL}(n, \mathbb{Z})$ bewerkstelligt werden kann. Dabei ist $\mathcal{SL}(n, \mathbb{Z})$ die Gruppe der invertierbaren Matrizen in $\mathbb{Z}^{n \times n}$. Eine eindeutige Darstellung für Ideale in $\mathcal{O}$ erhält man, wenn man die sogenannte Hermite–Normalform der $\mathbb{Z}$–Basis–Darstellung fordert. Diese besitzt untere Dreiecksgestalt; jeder Zeileneintrag ist nicht negativ und kleiner als das jeweils positive Diagonalelement.

2.52 Definition *Eine Matrix* $H \in \mathbb{Z}^{n\times n}$ *hat* Hermite-Normalform (HNF), *wenn gilt:*

$$\begin{array}{rl} h_{ij} = 0 & (1 \le i < j \le n) \\ h_{ii} > 0 & (1 \le i \le n) \\ 0 \le h_{ij} < h_{ii} & (1 \le j < i \le n). \end{array}$$

Daß man zu jeder quadratischen Matrix mit vollem Rang eine äquivalente Matrix in HNF finden kann, garantiert die folgende Aussage [Düll].

2.53 Satz *Zu jeder regulären Matrix* $A \in \mathbb{Z}^{n\times n}$ *gibt es eine Matrix* $K \in \mathcal{SL}(n, \mathbb{Z})$*, so daß* $H := AK$ *Hermite-Normalform besitzt.*

2.54 Bemerkung Da $\mathcal{O}$ ein freier $\mathbb{Z}$–Modul vom Rang n ist, kann man zu jedem Erzeugendensystem eines Teilmoduls I von $\mathcal{O}$, das aus $m > n$ Elementen besteht, eine Basis aus n Elementen finden. Somit existiert sogar zu jeder Matrix $A \in \mathbb{Z}^{n\times m}, m > n$ eine Matrix A' in HNF mit $Bild\ A = Bild\ A'$.

Wir benutzen HNF-Berechnung zur Bestimmung einer $\mathbb{Z}$–Basis der gefundenen Primideale in der Zerlegung von $p\mathcal{O}$.

2.7 Die Norm eines Ideals

Um eine Möglichkeit zu schaffen, Probleme betreffend Ideale des Rings $\mathcal{O}$ dadurch zu vereinfachen, daß sie über den ganzen Zahlen $\mathbb{Z}$ betrachtet werden können, führt man die ganzzahlige Norm eines Ideals ein und zeigt, daß diese multiplikativ ist. Wir beziehen uns auf [Hua].

2.55 Definition *Sei* $I \trianglelefteq \mathcal{O}$ *ein Ideal und sei* $\mathcal{O}/I$ *der zugehörige Restklassenring. Dann nennen wir seine Elementanzahl*

$$N(I) := \left| {}^{\mathcal{O}}\!/_{I} \right|$$

die Norm des Ideals I.

Die Norm eines Ideals I läßt sich bei Vorliegen der Darstellungsmatrix M_I leicht angeben. Es gilt nämlich der folgende Satz.

2.56 Satz *Sei* $\{\omega_1, \ldots, \omega_n\}$ *eine* $\mathbb{Z}$*–Basis von* $\mathcal{O}$ *und sei* $\{\alpha_1, \ldots, \alpha_n\}$ *eine* $\mathbb{Z}$*–Basis des Ideals* $I \trianglelefteq \mathcal{O}$. *Falls*

$$\alpha_i = \sum_{j=1}^{n} a_{ij}\omega_j, \quad 1 \leq i \leq n,$$

so gilt für die Norm von I

$$N(I) = |det(a_{ij})|.$$

2.57 Beispiel Da sich im Ganzheitsring $\mathcal{O}_{\mathcal{K}}$ eines Zahlkörpers $\mathcal{K}$ vom Grad 3 eine Darstellungsmatrix von $p\mathcal{O}_{\mathcal{K}}$ leicht in der Form

$$\begin{pmatrix} p & 0 & 0 \\ 0 & p & 0 \\ 0 & 0 & p \end{pmatrix}$$

angeben läßt, gilt $N(p\mathcal{O}_{\mathcal{K}}) = p^3$.

Um die Norm eines Produktes von Idealen zu berechnen, verwendet man den

2.58 Satz *Seien* $I, J \trianglelefteq \mathcal{O}$ *Ideale. Dann gilt*

$$N(IJ) = N(I)N(J).$$

Daraus erschließt man für die Zerlegung von $p\mathcal{O}$ sofort einige einfache Tatsachen, die wir in folgendem Korollar festhalten.

2.59 Korollar *Sei in der* p*–maximalen Ordnung* $\mathcal{O}$*eines Zahlkörpers vom Grad* n *die eindeutige Primidealzerlegung von* $p\mathcal{O}$ *folgendermaßen gegeben:*

$$p\mathcal{O} = M_1^{e_1} \cdot M_2^{e_2} \cdots M_r^{e_r}.$$

Dann gilt

1. *die Norm von* $p\mathcal{O}$ *ist* $N(p\mathcal{O}) = p^n$
2. *die Norm jedes* M_j, $1 \leq j \leq r$ *ist eine Potenz von* p
3. *die Summe der Exponenten ist beschränkt durch* n

$$e_1 + e_2 + \ldots e_r \leq n$$

4. *die Anzahl der* $p\mathcal{O}$ *teilenden Primideale ist höchstens* n.

Beweis:

1. Dies folgt direkt aus Satz 2.56.
2. Wegen $p^n = N(p\mathcal{O}) = N(M_1)^{e_1} \cdot N(M_2)^{e_2} \cdots N(M_r)^{e_r} \qquad (*)$

   kommen als Teiler von p^n für die Normen der Primideale M_j nur p–Potenzen in Frage.
3. Sei $N(M_j) = p^{f_j}$. Damit erhält man aus der Darstellung $(*)$

   $$e_1 f_1 + e_2 f_2 + \ldots + e_r f_r = n$$

   mit $f_j \geq 1,\ 1 \leq j \leq r$.
4. Dies folgt direkt aus Punkt 3.

■

2.60 Bemerkung Die im Beweis zu Korollar 2.59 auftretenden Größen e_j und f_j werden in der Literatur oft als Verzweigungsgrad e_j von M_j über p und der Restklassengrad f_j von M_j über $\mathbb{F}_p$ bezeichnet.

Im Falle $\mathcal{O}$=$\mathcal{O}_\mathcal{K}$ läßt sich die Primzahl p im allgemeinen auf einfache Weise zerlegen. Dazu benötigen wir den Begriff der Polynomdiskriminante.

2.61 Definition *Sei $f \in \mathbb{Q}[X]$ ein Polynom vom Grad n und L der Zerfällungskörper von f über $\mathbb{Q}$. Seien $\xi_1, \xi_2, \ldots, \xi_n \in L$ die Nullstellen von f in L.*

Dann heißt

$$d(f) := \prod_{1 \leq i < k \leq n} (\xi_i - \xi_k)^2$$

die Polynomdiskriminante *von f.*

Das sich aus [PohZa, Th. 2.27,Le. 2.29] unmittelbar ergebende Resultat formulieren wir als

2.62 Satz *Seien $\mathcal{K} = \mathbb{Q}(\rho)$ ein algebraischer Zahlkörper, $f \in \mathbb{Z}[X]$ das Minimalpolynom von ρ, $\mathcal{O}_\mathcal{K}$ sein Ganzheitsring und p eine $d(f)$ nicht teilende Primzahl.*

Dann ergibt sich die Zerlegung von $p\mathcal{O}_\mathcal{K}$ folgendermaßen:
es sei

$$\overline{f}(X) \equiv \overline{f}_1^{e_1}(X) \cdots \overline{f}_r^{e_r}(X)$$

die eindeutige Primfaktorzerlegung von f modulo p über $\mathbb{Z}/p\mathbb{Z}$; dann hat $p\mathcal{O}_K$ die eindeutige Primidealdarstellung

$$p\mathcal{O}_K = \prod_{j=1}^{r} P_j^{e_j},$$

wobei die Primideale $P_j \trianglelefteq \mathcal{O}_K$ durch

$$P_j = p\mathcal{O}_K + f_j(\rho)\mathcal{O}_K \qquad 1 \leq j \leq n$$

gegeben sind.

Kapitel 3

Operationen in $\mathcal{O}$

In diesem Kapitel beschreiben wir die arithmetischen Operationen in einer Ordnung $\mathcal{O}$ des algebraischen Zahlkörpers $\mathcal{K}$vom Grad n und geben Algorithmen zu ihrer Realisierung an. Dabei wird ausführlich auf die Verwendung Linearer Algebra bei der Behandlung der auftretenden Teilprobleme eingegangen, und es werden Algorithmen zu ihrer Lösung angegeben.

Wir repräsentieren die Ordnung $\mathcal{O}$ durch eine Multiplikationstabelle

$$w_{ijk},\ 1 \le i, j, k \le n,$$

die unser Algorithmus entweder direkt als Eingabe erhält oder aus anderen Eingabedaten berechnet (s.u.). Diese liegt somit zu Beginn des Verfahrens vor. Sie ist durch die n^2 Gleichungen

$$\omega_i \omega_j = \sum_{k=1}^{n} w_{ijk}\omega_k, \quad 1 \le i, j \le n$$

definiert.

Um bei der Benutzung des Algorithmus eine komfortable Eingabe zu ermöglichen, erlauben wir zusätzlich die Angabe von $\mathcal{O}$ durch eine $\mathbb{Z}$–Basis ganzalgebraischer Zahlen und im Spezialfall einer ρ–Potenzbasis — hier ist ρ eine ganzalgebraische Zahl — die Eingabe des Minimalpolynoms von ρ.

3.1 Beispiel Wir beginnen mit der Angabe einer Multiplikationstabelle.

$$\begin{array}{ll} w_{111} = 1 & w_{112} = 0 \\ w_{121} = 0 & w_{122} = 1 \\ w_{211} = 0 & w_{212} = 1 \\ w_{221} = 2 & w_{222} = 0 \end{array}$$

Dieses ist die Multiplikationstabelle von $\mathcal{O} = \langle 1, \sqrt{2} \rangle$.

Da dies sogar eine ρ–Potenzbasis mit $\rho = \sqrt{2}$ ist, können wir $\mathcal{O}$ ebensogut durch $f(X) = X^2 - 2 \in \mathbb{Z}[X]$ festlegen.

Wir haben schon in Kapitel 2 gesehen, daß sich die Darstellung von Idealen, die $p\mathcal{O}$ teilen, auf die Darstellung von Idealen in $\mathcal{O}/p\mathcal{O}$ reduzieren läßt. Es wurde gezeigt, daß auch die Arithmetik in den für uns interessanten Fällen im Ring $\mathcal{O}/p\mathcal{O}$ ausgeführt werden kann. Daher benötigen wir eine Elementarithmetik in $\mathcal{O}/p\mathcal{O}$.

3.1 Elementarithmetik

Sei

$$\{\overline{\omega}_1, \ldots, \overline{\omega}_n\}$$

die durch Restklassenbildung modulo $p\mathcal{O}$ aus $\mathcal{O}$ hervorgegangene $\mathbb{F}_p$–Basis von $\mathcal{O}/p\mathcal{O}$.

Seien $\overline{\alpha}, \overline{\beta} \in \overline{\mathcal{O}}$ mit

$$\overline{\alpha} = \sum_{j=1}^{n} a_j \overline{\omega}_j$$

$$\overline{\beta} = \sum_{k=1}^{n} b_k \overline{\omega}_k,$$

wobei $a_j, b_j \in \mathbb{F}_p$ für $1 \le j \le n$.

Dann ist

$$\begin{aligned}
\overline{\alpha} + \overline{\beta} &= \sum_{k=1}^{n} (a_k + b_k) \overline{\omega}_k \\
\overline{\alpha} - \overline{\beta} &= \sum_{k=1}^{n} (a_k - b_k) \overline{\omega}_k \\
\overline{\alpha} \cdot \overline{\beta} &= \sum_{k=1}^{n} (\sum_{i=1}^{n} \sum_{j=1}^{n} (a_i \cdot b_j) w_{ijk}) \overline{\omega}_k,
\end{aligned}$$

wobei die Elemente $w_{ijk}, \quad 1 \le i, j, k \le n$ die zu Anfang des Kapitels eingeführte Multiplikationstabelle von $\mathcal{O}$ bilden.

Daher stellt die Ausführung der Ringoperationen in $\mathcal{O}/p\mathcal{O}$ kein algorithmisches Problem dar. Man beachte, daß $\overline{\alpha} \pm \overline{\beta}$ Vektorraumoperationen sind und daher die Arithmetik von ${\mathbb{F}_p}^n$ vererbt werden kann.

Nähere Einzelheiten zur Technik der Vererbung findet man in Kapitel 5.

3.2 Idealarithmetik

Wir möchten Ideale $A, B \trianglelefteq \mathcal{O}$ mit $A, B \supseteq p\mathcal{O}$ arithmetisch verknüpfen. Nach Satz 2.47 braucht die Verknüpfung lediglich in $\mathcal{O}/p\mathcal{O}$ statt in $\mathcal{O}$ stattzufinden.

Seien also $\overline{A} = \Phi(A), \overline{B} = \Phi(B) \trianglelefteq \overline{\mathcal{O}}$ Ideale mit

$$\begin{aligned}\overline{A} &= <\overline{\alpha}_1, \ldots, \overline{\alpha}_k>_{\mathbb{F}_p}\\ \overline{B} &= <\overline{\beta}_1, \ldots, \overline{\beta}_l>_{\mathbb{F}_p},\end{aligned}$$

wobei

$$\begin{aligned}\overline{\alpha}_j &= \sum_{i=1}^{n} a_{ij}\overline{\omega}_i \qquad 1 \leq j \leq k\\ \overline{\beta}_j &= \sum_{i=1}^{n} b_{ij}\overline{\omega}_i \qquad 1 \leq j \leq l.\end{aligned}$$

Die Darstellung erfolgt demzufolge durch Matrizen

$$\begin{aligned}M_{\overline{A}} &= (a_{ij}) \in {\mathbb{F}_p}^{n\times k}\\ M_{\overline{B}} &= (b_{ij}) \in {\mathbb{F}_p}^{n\times l}.\end{aligned}$$

3.2.1 Addition von Idealen

Es ist nach Satz 2.51

$$\overline{A} + \overline{B} = \langle \overline{\alpha}_1, \ldots, \overline{\alpha}_k, \overline{\beta}_1, \ldots, \overline{\beta}_l \rangle_{\mathbb{F}_p}. \tag{3.1}$$

Daher bilden die Spalten von $M_{\overline{A}}$ ergänzt durch die Spalten von $M_{\overline{B}}$ ein Erzeugendensystem von $\overline{A} + \overline{B}$. Aus diesem Erzeugendensystem eine Basis für $\overline{A} + \overline{B}$ zu berechnen, ist Aufgabe eines Grundalgorithmus aus dem Bereich der Linearen Algebra (Abschnitt 3.3.1).

3.2.2 Multiplikation von Idealen

Es ist nach Satz 2.50

$$\overline{A} \cdot \overline{B} = \langle \overline{\alpha}_1\overline{\beta}_1, \ldots, \overline{\alpha}_\kappa\overline{\beta}_\lambda, \ldots, \overline{\alpha}_k\overline{\beta}_l \rangle_{\mathbb{F}_p}. \tag{3.2}$$

Da die Elementarithmetik schon bekannt ist, sind hier lediglich die Vektoren der Produkte der $\overline{\alpha}_\kappa\overline{\beta}_\lambda$ zu einer Matrix zusammenzufassen. Damit hat man ein Erzeugendensystem für das Idealprodukt. Dieses in eine Basis umzuwandeln, ist Aufgabe eines Algorithmus im Bereich der Linearen Algebra (Abschnitt 3.3).

3.2.3 Division von Idealen

Nach Satz 2.49 ist für $A \mid B$ das ganze Ideal $\frac{B}{A}$ der Kern des folgenden Homomorphismus:

$$\begin{array}{rcl} \overline{\mathcal{O}} & \to & (\overline{A} \to \overline{\mathcal{O}}/\overline{B}) \\ \overline{\gamma} & \mapsto & (\overline{\alpha} \mapsto \overline{\gamma\alpha}). \end{array} \tag{3.3}$$

Dies bedeutet, daß für jedes Basiselement $\overline{\gamma} \in \overline{\mathcal{O}}$ die Abbildungsmatrix des Multiplikation–mit–$\overline{\gamma}$-Homomorphismus gebildet werden muß. Außerdem muß eine Basis des Quotientenmoduls $\overline{\mathcal{O}}/\overline{B}$ bestimmt werden (Beschreibung in Abschnitt 3.3.7). Als Elemente des $\mathbb{F}_p$-Vektorraums $Hom(\overline{A}, \overline{\mathcal{O}}/\overline{B})$ werden nun diese Matrizen als Vektoren aufgefaßt und aus ihnen die Matrix der Abbildung (3.3) zusammengestellt. Den Kern dieser Matrix auszurechnen, ist nun wieder Aufgabe eines Algorithmus im Bereich der Linearen Algebra (Abschnitt 3.3).

Damit sind alle für das Hauptverfahren notwendigen Idealoperationen beschrieben.

3.3 Lineare Algebra über $\mathbb{F}_p$

Wie aus dem letzten Abschnitt ersichtlich, sind zur Bewältigung der Idealoperationen eine Reihe von algorithmischen Grundproblemen aus dem Bereich der Linearen Algebra über dem endlichen Körper $\mathbb{F}_p$ zu lösen. Wir listen diese nun auf und geben Algorithmen zu ihrer Lösung an. Hierbei sei V ein Vektorraum über $\mathbb{F}_p$ und $A \in {\mathbb{F}_p}^{m\times n}$ eine Matrix.

1. aus einem gegebenen Erzeugendensystem eine Basis für V bestimmen (siehe Abschnitt 3.3.1)
2. eine Basis für *Bild* A bestimmen (siehe Abschnitt 3.3.2)
3. eine Basis für *Kern* A bestimmen (siehe Abschnitt 3.3.3)
4. den Rang von A berechnen (siehe Abschnitt 3.3.4)

5. Ergänzung einer linear unabhängigen Menge zu einer Basis von V (siehe Abschnitt 3.3.5)

6. Lösen eines linearen Gleichungssystems $Ax = b$ (siehe Abschnitt 3.3.6)

7. für einen Teilmodul $W \leq V$ den Quotientenmodul V/W berechnen (siehe Abschnitt 3.3.7).

Den Algorithmen hierzu liegt ein elementares Hilfsmittel zugrunde — die Berechnung der Spaltenstufenform einer Matrix. Dazu geben wir die folgende

3.2 Definition *Sei $B = (b_{ij}) \in \mathbb{F}_p{}^{m\times n}$ und*

$$m_j := \begin{cases} max\{i \mid b_{ij} \neq 0\}, & falls\ existent \\ 0 & sonst \end{cases}$$

für $1 \leq j \leq n$ und sei k der minimale Index, so daß $m_k \neq 0$.
Dann heißt B in Spaltenstufenform $:\Longleftrightarrow$

$$0 = m_1 = \ldots = m_{k-1} < m_k < m_{k+1} < \ldots < m_n.$$

3.3 Beispiel Folgende Matrix hat Spaltenstufenform

$$\begin{pmatrix} 0 & 0 & 4 & 0 & 0 & 6 \\ 0 & 0 & 5 & 1 & 0 & 3 \\ 0 & 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 2 & 4 & 4 \\ 0 & 0 & 0 & 0 & 4 & 3 \\ 0 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in \mathbb{F}_7^{8\times 6} \quad .$$

Mit den Bezeichnungen von Definition 3.2 gilt:

$$0 = m_1 = m_2 < m_3 = 2 < m_4 = 4 < m_5 = 6 < m_6 = 8, \quad k = 3.$$

3.4 Bemerkung Eine Matrix $A \in \mathbb{F}_p{}^{m\times n}$ kann mehrere Spaltenstufenformen A' mit $Bild\ A = Bild\ A'$ besitzen. Addiert man beispielsweise in Beispiel 3.3 die dritte Spalte zur vierten, erhält man eine solche äquivalente Spaltenstufenform.

Es ist üblich, diejenigen Matrizenoperationen, die den Kern und das Bild einer Matrix invariant lassen, als elementar zu bezeichnen. Wir formalisieren dies in der folgenden Definition.

3.5 Definition *Sei $A \in {\mathbb{F}_p}^{m\times n}$ und $A \to T(A)$ eine Operation von folgendem Typ:*

1. *Addition eines Vielfachen einer Spalte zu einer anderen*
2. *Vertauschung zweier Spalten.*

Dann nennen wir T eine elementare Spaltenoperation.

Wir werden einen Algorithmus angeben, der eine beliebige Matrix $A \in {\mathbb{F}_p}^{m\times n}$ durch elementare Spaltenoperationen in Spaltenstufenform überführt.

Es läßt sich durch direktes Nachrechnen bestätigen, daß jede elementare Spaltenoperation eine Multiplikation $A \cdot T$ mit einer regulären Matrix $T \in {\mathbb{F}_p}^{n\times n}$ bedeutet:

1. für $a \in \mathbb{F}_p$ addiere das a-fache der Spalte j zur Spalte i

$$T(A) = A \cdot \underbrace{\begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 1 & 0 & \cdots & \cdots & 0 \\ & & 1 & & & \\ & & & \ddots & & \\ & a & & & \ddots & \\ & & & & & 1 \end{pmatrix}}_{T}$$

   Hierbei steht a in der i–ten Spalte und j–ten Zeile.

2. vertausche die Spalten i und j

$$T(A) = A \cdot \underbrace{\begin{pmatrix} 1 & 0 & \cdots & \cdots & \cdots & 0 \\ 0 & 0 & \cdots & 0 & 1 & 0 \\ & & 1 & & & \\ & & & \ddots & & \\ & 1 & & & 0 & \\ & & & & & 1 \end{pmatrix}}_{T}$$

   Hier wurde die Multiplikation mit einer durch eine Vertauschung der Spalten i und j modifizierten Einheitsmatrix ausgeführt.

Offensichtlich ist T in beiden Fällen regulär. Aufeinanderfolgende elementare Spaltenoperationen liefern somit ein Produkt von regulären Transformationsmatrizen

$$T(A) = A \cdot \underbrace{T_1 \cdot T_1 \cdots T_s}_{T'} = A \cdot T'$$

mit einer regulären Matrix T'. Wir berechnen im Algorithmus 'column step form' sowohl $T(A)$ als auch T'.

Algorithmus COLUMN STEP FORM

Eingabe: $A \in {\mathbb{F}_p}^{m \times n}$

Ausgabe: eine Spaltenstufenform $T(A) \in {\mathbb{F}_p}^{m \times n}$ von A und eine Transformationsmatrix $T \in \mathcal{GL}(n, \mathbb{F}_p)$, so daß

$$T(A) = A \cdot T.$$

(1) $T \leftarrow I_n$
co *setze T auf die Einheitsmatrix von ${\mathbb{F}_p}^{n \times n}$* **oc**

(2) $i \leftarrow m$

(3) $j \leftarrow n$
co *wir beginnen bei dem Element in der rechten unteren Ecke der Matrix und bearbeiten die Matrix in Richtung linker oberer Ecke* **oc**

(4) **do**

(5) **if** $a_{ij} = 0$ **then**
co *wir ersetzen, falls möglich, die Spalte j durch eine Spalte mit einem von Null verschiedenen Element in Zeile i* **oc**

(6) **for** $k \leftarrow j - 1$ **down to** 1 **do**

(7) **if** $a_{ik} \neq 0$ **then**
co *eine geeignete Spalte k ist gefunden* **oc**

(8) *tausche(A,k,j)*

(9) *tausche(T,k,j)*

(10) **break**

(11) **fi**

(12) **od**

(13) **fi**

(14) **if** $a_{ij} \neq 0$ **then**
co *hier testen wir, ob erfolgreich getauscht wurde – falls ja, benutzen wir das invertierbare Element dazu, die Elemente in der gleichen Zeile mit kleinerem Spaltenindex zu annullieren und protokollieren diesen Vorgang in der Transformationsmatrix* **oc**

(15) **for** $k \leftarrow j-1$ **down to** 1 **do**
(16) $A_k \leftarrow A_k - a_{ik}a_{ij}^{-1}A_j$
(17) $T_k \leftarrow T_k - a_{ik}a_{ij}^{-1}T_j$
(18) **od**
(19) $j \leftarrow j-1$
co *nächste Spalte, falls das Annullieren durchgeführt wurde* **oc**
(20) **fi**
(21) $i \leftarrow i-1$
co *nächste Zeile* **oc**
(22) **while** $j > 1$ *and* $i > 0$
(23) **return** A, T

Zur Korrektheit beweisen wir zunächst das

3.6 Lemma *Nach Ausführung von Zeile (21) gilt* $a_{ij'} = 0$ *für* $1 \leq j' \leq j$.

Beweis: Wir nehmen induktiv an, daß für Zeilen $i' > i$ die Behauptung bereits gilt.

Falls es in Zeile (5) kein $a_{ij'}$ gibt mit $a_{ij'} \neq 0$, so ist die Bedingung in Zeile (14) falsch, und somit gilt die Aussage des Lemmas.

Sei nun k so gewählt, daß $a_{ik} \neq 0$, dabei k maximal mit $1 \leq k \leq j$. Ein solches k wird im Block (6)–(13) bestimmt, und es werden die Spalten k und j getauscht.

Ab diesem Zeitpunkt ist also $a_{ij} \neq 0$, und es kann a_{ij}^{-1} gebildet werden. So wird in Zeile (16) jedes a_{ik} folgendermaßen gesetzt:

$$a_{ik} \leftarrow a_{ik} - a_{ik}a_{ij}^{-1}a_{ij} \quad (=0).$$

Die Zeilen $i' > i$ bleiben unverändert, da nach Induktionsannahme dort schon alle Einträge gleich Null sind.

Damit ist das Lemma bewiesen. ∎

Wir vervollständigen die Korrektheitsaussage durch den folgenden Satz.

3.7 Satz *Der Algorithmus 'COLUMN STEP FORM' berechnet eine Spaltenstufenform $T(A)$ von $A \in {\mathbb{F}_p}^{m\times n}$ und liefert $T \in \mathcal{GL}(n, \mathbb{F}_p)$, so daß*

$$T(A) = A \cdot T. \tag{3.4}$$

Beweis: Nach dem obigen Lemma existiert nach Ausführung des Algorithmus für jede Zeile i ein $j(i)$, so daß $a_{ij} = 0$ für $1 \leq j < j(i)$. Wegen Zeile (19) gilt

$$j(1) \leq j(2) \leq \ldots \leq j(m), \tag{3.5}$$

wobei das Gleichheitszeichen für den jeweiligen Zeilenindex genau dann besteht, wenn die Bedingung in Zeile (14) falsch war.

Also läßt sich die Ungleichungskette (3.5) auch so schreiben:

$$j(1) = \ldots = j(l_0) < j(l_0 + 1) = \ldots = j(l_1) < j(l_1 + 1) = \ldots = j(l_2) < \ldots \tag{3.6}$$

für gewisse Indizes l_ν.

Nach ihrer Definition gilt dann auch $l_0 < l_1 < l_2 < \ldots$.

Nun kann man die Bezeichnungen der Definition 3.2 benutzen, und man sieht unmittelbar, daß

$$m_{t+\nu} = l_\nu,$$

wobei t der Index der ersten von Null verschiedenen Spalte von $T(A)$ ist.

Damit liefert der Algorithmus 'COLUMN STEP FORM' tatsächlich eine Spaltenstufenform von A.

Die Transformationsmatrix ist regulär, da sie aus der Einheitsmatrix I_n mittels elementarer Spaltenoperationen (Multiplikation mit einer regulären Matrix von rechts) hervorgegangen ist.

Die Gleichung (3.4) ist nach den Vorbemerkungen zum Algorithmus offensichtlich erfüllt. ∎

3.8 Bemerkung Der Algorithmus benutzt nur elementare Spaltenoperationen; daher bleibt *Bild A* invariant.

Betrachtet man die Schleife *(15)–(18)*, so kann man die Komplexität des Verfahrens direkt angeben. Es werden nämlich in den Schritten *(16),(17)* jeweils $n-1, n-2, \ldots, n-m+1$ Spaltenoperationen ausgeführt; diese sind wiederum durch m Operationen beschränkt. So hat man als Laufzeit für den Algorithmus 'COLUMN STEP FORM'

$$O(((m-1)n - (m-1)m/2)m) = O(m^2 n),$$

was der für Trigonalisierung von quadratischen Matrizen bekannten Laufzeit $O(n^3)$ entspricht.

Mit dem soeben zur Verfügung gestellten Hilfsmittel können die Lösungen der erwähnten algorithmischen Probleme aus der Linearen Algebra in übersichtlicher Form angegeben werden.

3.3.1 Basisberechnung aus einem Erzeugendensystem

Gegeben: ein Erzeugendensystem $\{w_1, \ldots, w_l\} \subset \mathbb{F}_p{}^n$ des $\mathbb{F}_p$–Vektorraums V

Gesucht: eine Basis für V

Idee: Wende auf $W := (w_1 \ldots w_l) \in \mathbb{F}_p{}^{n \times l}$ COLUMN STEP FORM an.

Die Vorgehensweise dazu wird suggeriert durch den

3.9 Satz *Sei $A \in \mathbb{F}_p{}^{m \times n}$, $T(A)$ eine Spaltenstufenform von A.*
Dann bilden die von Null verschiedenen Spalten von $T(A)$ eine Basis von Bild A.

Beweis: Wegen *Bild* $A =$ *Bild* $T(A)$ erzeugen die von Null verschiedenen Spalten von T(A) den Vektorraum *Bild* A. Diese sind wegen ihrer speziellen Form trivialerweise linear unabhängig. ■

Wir haben also insbesondere das

3.10 Korollar *Falls die Spalten von A ein Erzeugendensystem von $\mathbb{F}_p{}^m$ bilden, so bilden die von Null verschiedenen Spalten von $T(A)$ eine Basis von $\mathbb{F}_p{}^m$.*

Beweis: Die Spalten von A sind genau dann ein Erzeugendensystem von $\mathbb{F}_p{}^m$, wenn *Bild* $A = \mathbb{F}_p{}^m$. Daher folgt die Behauptung direkt aus dem Satz. ■

3.3.2 Berechnung des Bildes einer Matrix

Gegeben: eine Matrix $A \in {\mathbb{F}_p}^{m \times n}$

Gesucht: eine Basis für $Bild\ A = \{Ax \mid x \in {\mathbb{F}_p}^n\}$

Idee: Wende COLUMN STEP FORM an und extrahiere die von Null verschiedenen Spalten.

Die Vorgehensweise ist durch den Satz 3.9 unmittelbar ersichtlich.

Algorithmus IMAGE

Eingabe: $A \in {\mathbb{F}_p}^{m \times n}$

Ausgabe: Matrix B aus Spaltenvektoren, die eine Basis für $Bild\ A$ bilden

```
COLUMN STEP FORM(A)
j ← 1
while j < n and A_j = 0 do
        co suche die erste von Null verschiedene Spalte
        von A und speichere den Spaltenindex in j oc
        j ← j + 1
        od
if j = n and A_n = 0 then
        co falls A die Nullmatrix ist, setze j auf n + 1 oc
        j ← j + 1
        fi
for k ← j to n do
        co speichere die Basis von Bild A in B oc
        B_{k-j+1} ← A_k
        od
return B
```

3.3.3 Berechnung des Kerns einer Matrix

Gegeben: eine Matrix $A \in {\mathbb{F}_p}^{m \times n}$

Gesucht: eine Basis für $Kern\ A = \{x \in {\mathbb{F}_p}^n \mid Ax = 0 \in {\mathbb{F}_p}^m\}$

Idee: Wende COLUMN STEP FORM an und erhalte $T(A) = AT$.
Wenn nun l die Anzahl der Nullspalten in T(A) ist, so bildet $\{T_1, \ldots, T_l\}$ eine Basis von $Kern\ A$.

Wir formulieren diese Tatsache als

3.11 Satz *Sei $A \in {\mathbb{F}_p}^{m \times n}$, $T(A) = AT$ eine Spaltenstufenform von A und r der Rang von $T(A)$. Dann bildet $T_1, \ldots, T_{n-r}$ eine Basis für $Kern\ A$.*

Beweis: Es sind die Spalten $\{T_1, \ldots, T_{n-r}\}$ als Spalten der regulären Matrix T linear unabhängig. Außerdem gilt

$$AT_i = 0 \text{ wegen } AT = T(A).$$

Weiterhin haben wir

$$rang\ A = rang\ T(A) = r = n - dim\ Kern\ A \Rightarrow dim\ Kern\ A = n - r.$$

Aus diesem Grunde ist $\{T_1, \ldots, T_{n-r}\}$ eine maximale linear unabhängige Teilmenge von $Kern\ A$, also eine Basis. ∎

Daraus ergibt sich der

Algorithmus KERN

Eingabe: $A \in {\mathbb{F}_p}^{m \times n}$

Ausgabe: Matrix K aus Spaltenvektoren, die eine Basis für $Kern\ A$ bilden

(1) *erhalte aus COLUMN STEP FORM(A) eine Spaltenstufenform A' von A und die Transformationsmatrix T, so daß $A' = AT$*

(2) **if** $A'_n = 0$ **then**
  co *falls A'_n die Nullmatrix ist, so ist der Kern ganz ${\mathbb{F}_p}^n$* **oc**

return T
fi
$j \leftarrow 1$
while $A'_j = 0$ **do**
co *für jede Nullspalte von A' übernehme die entsprechende Spalte von T* **oc**
$K_j \leftarrow T_j$
$j \leftarrow j + 1$
od
return K

3.3.4 Berechnung des Rangs einer Matrix

Gegeben: eine Matrix $A \in {\mathbb{F}_p}^{m \times n}$

Gesucht: *rang* A ($=$ *dim Bild* A)

Idee: Berechne *Bild* A nach Abschnitt 3.3.2 und zähle die Basisvektoren.

Damit kann das kurze Verfahren direkt angegeben werden.

Algorithmus RANG

Eingabe: eine Matrix $A \in {\mathbb{F}_p}^{m \times n}$

Ausgabe: rang A

$B \leftarrow$ *Bild* A
return *Anzahl der Spalten von* B

3.3.5 Basisergänzung

Gegeben: eine Matrix $V \in {\mathbb{F}_p}^{n \times k}$, die linear unabhängige Spaltenvektoren enthält; daher also $k \leq n$

Gesucht: eine Matrix $V' \in {\mathbb{F}_p}^{n \times n}$, deren erste k Spalten mit V übereinstimmen und für die gleichzeitig $rang\ V' = n$ gilt, deren Spalten also eine Basis des ${\mathbb{F}_p}^n$ bilden

Idee: Bringe V auf Spaltenstufenform und lies an dieser ab, welche $n-k$ Einheitsvektoren ergänzt werden müssen, um eine Dreiecksgestalt zu erreichen.

Die zu ergänzenden Einheitsvektoren e_l sind demnach gerade diejenigen, deren Index l echt zwischen den letzten von Null verschiedenen Einträgen von benachbarten Vektoren in der Spaltenstufenform liegen.

3.12 Beispiel Wir betrachten die Matrix aus Beispiel 3.3.

$$\begin{pmatrix} 0 & 0 & 4 & 0 & 0 & 6 \\ 0 & 0 & 5 & 1 & 0 & 3 \\ 0 & 0 & 0 & 0 & 0 & 5 \\ 0 & 0 & 0 & 2 & 4 & 4 \\ 0 & 0 & 0 & 0 & 4 & 3 \\ 0 & 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix} \in \mathbb{F}_7^{8 \times 6}$$

Man sieht sofort, daß das Ergänzen der von Null verschiedenen Spalten durch die vier Einheitsvektoren

$$\begin{pmatrix} 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad \begin{pmatrix} 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \\ 0 \\ 0 \end{pmatrix} \qquad \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix}$$

eine Basis des $\mathbb{F}_7^8$ liefert.

Aus diesen Vorüberlegungen ergibt sich, daß der folgende Algorithmus eine korrekte Basisergänzung durchführt.

Algorithmus BASIS COMPLETION

Eingabe: $V \in {\mathbb{F}_p}^{n\times k}$ mit *vollem* Rang

Ausgabe: $V' \in \mathcal{GL}(n, \mathbb{F}_p)$ mit $V_j = V'_j$ für $1 \le j \le k$

if $k = n$ **then**
  co *falls* $rang\ V = n$, *so ist nichts zu ergänzen* **oc**
  return V
  fi
if $k = 0$ **then**
  co *falls eine leere Matrix übergeben wurde, geben wir die Standardbasis zurück* **oc**
  return I_n
  fi
for $j \leftarrow 1$ **to** k **do**
    co *wir übernehmen die ersten* k *Vektoren aus* V **oc**
    $V'_j \leftarrow V_j$
    od
$W \leftarrow COLUMN\ STEP\ FORM(V)$
$l \leftarrow k + 1$
for $i \leftarrow 1$ **to** k **do**
    co *ergänze die fehlenden Einheitsvektoren* **oc**
    for $j \leftarrow last(W_{i-1}) + 1$ **to** $last(W_i) - 1$ **do**
        $V'_l \leftarrow e_j$
        $l \leftarrow l + 1$
        od
    od

3.13 Bemerkung Im Algorithmus bezeichnen wir mit e_l, $1 \leq l \leq n$ den l–ten kanonischen Einheitsvektor des ${\mathbb{F}_p}^n$.
Mit dem Aufruf $last(v)$ erhalten wir den Index des letzten von Null verschiedenen Eintrags von v.

3.3.6 Lösung eines linearen Gleichungssystems

Gegeben: eine Matrix $A \in {\mathbb{F}_p}^{m \times n}$, $b \in {\mathbb{F}_p}^m$

Gesucht: eine Lösung der Gleichung $Ax = b$

Idee: Erhalte aus COLUMN STEP FORM $T(A) = AT$. Wegen der einfachen Gestalt von $T(A)$ erhält man durch sukzessives Einsetzen eine Lösung von

$$T(A)y = b.$$

Nun ist aber

$$b = T(A)y = (AT)y = A(Ty).$$

Dies bedeutet, daß Ty eine Lösung von $Ax = b$ ist.

Der folgende Algorithmus realisiert diese Idee. Seine Korrektheit ist offensichtlich.

Algorithmus SOLVE

Eingabe: $A \in {\mathbb{F}_p}^{m \times n}$, $b \in {\mathbb{F}_p}^m$

Ausgabe: ein $x \in {\mathbb{F}_p}^n$ mit $Ax = b$, falls diese Gleichung eine Lösung besitzt, andernfalls ‘UNLÖSBAR’

(1) *erhalte aus COLUMN STEP FORM in A eine Spaltenstufenform von A und in T die zugehörige Transformationsmatrix*

(2) $i \leftarrow m$

(3) $j \leftarrow n$

(4) **do**

  co *wir berechnen den Lösungsvektor y durch sukzessives Einsetzen* **oc**

(5) $s \leftarrow 0$

for $k \leftarrow j+1$ **to** n **do**
co *der schon bekannte Teil von* y $(y_{j+1}, \ldots, y_n)$ *wird benutzt, um die Komponente Nr.* j *von* y *auszurechnen* **oc**
$s \leftarrow s + a_{ik} y_k$
od
$a \leftarrow a_{ij}$
if $a \neq 0$ **then**
co *falls Dividieren durch* a *erlaubt ist* **oc**
$s \leftarrow \frac{b_i - s}{a}$
else
co *sonst ist das Gleichungssystem entweder mehrdeutig lösbar oder unlösbar* **oc**
if $b_i - s = 0$ **then**
$s \leftarrow 0$
else
return *'UNLÖSBAR'*
fi
fi
$y_j \leftarrow s$
co y_j *wurde berechnet und die Indizes werden auf den nächsten Eintrag gesetzt* **oc**
$i \leftarrow i - 1$
$j \leftarrow j - 1$
while $i \geq 1$ *and* $j \geq 1$
for $k \leftarrow j$ **to** 1 **do**
co *bei mehrdeutigen Lösungen setzen wir die nicht eindeutigen Komponenten auf* 0 **oc**
$y_k \leftarrow 0$
od
co *am Schluß wird die Lösung des transformierten Gleichungssystems in eine Lösung des ursprünglichen Gleichungssystems umgewandelt* **oc**
$x \leftarrow Ty$
return x

3.3.7 Bildung des Quotientenmoduls ${\mathbb{F}_p}^n/W$

Gegeben: eine Matrix $A \in {\mathbb{F}_p}^{n\times k}$,deren Spalten einen Teilvektorraum W von ${\mathbb{F}_p}^n$ bilden

Gesucht: eine Basis für ${\mathbb{F}_p}^n/W$

Idee: Ergänze die Basis von W zu einer Basis von ${\mathbb{F}_p}^n$, dann bilden die ergänzten Vektoren eine Basis von ${\mathbb{F}_p}^n/W$.

Diese Idee beruht auf dem folgenden

3.14 Satz *Sei V ein n-dimensionaler Vektorraum über $\mathbb{F}_p$ und sei $W \leq V$ ein Teilraum von V mit Basis $\{w_1,\ldots,w_m\}$. Seien die Vektoren $w_{m+1},\ldots,w_n \in {\mathbb{F}_p}^n$ so gewählt, daß $\{w_1,\ldots,w_n\}$ eine Basis von V ist, so bildet $\{w_{m+1}+W,\ldots,w_n+W\}$ eine Basis von V/W.*

Beweis: Betrachte den kanonischen Epimorphismus

$$\pi : V \to {}^{V}\!/_{W}$$

Dann gilt $Kern\ \pi = W$ und $dim\ Kern\ \pi + dim\ Bild\ \pi = dim\ V$. Daraus folgt

$$dim\ {}^{V}\!/_{W} = n - m.$$

Also hat man eine linear unabhängige Menge in $Bild\pi = V/W$ bestimmt, die $n-m$ Elemente besitzt. Somit ist

$$\{w_{m+1}+W,\ldots,w_n+W\} \subseteq {}^{{\mathbb{F}_p}^n}\!/_{W}$$

eine Basis für V/W. ■

3.15 Bemerkung Wir benötigen hiervon nur den Spezialfall der Bildung von ${\mathbb{F}_p}^n/W$.

Algorithmus QUOTIENT MODULE

Eingabe: $\{w_1,\ldots,w_m\}$ Basis von W als Matrix $A \in {\mathbb{F}_p}^{n\times m}$

Ausgabe: $\{w_1,\ldots,w_m,w_{m+1},\ldots,w_n\}$, so daß $\{w_{m+1}+W,\ldots,w_n+W\}$ eine Basis von ${\mathbb{F}_p}^n/W$ ist

(1) $B \leftarrow BASIS\ COMPLETION(A)$

(2) **return** B

3.4 Modulare Hermite-Normalform Berechnung

Die durch Definition 2.52 eingeführte Hermite–Normalform einer Matrix wird zur eindeutigen $\mathbb{Z}$–Basis–Darstellung von Idealen in $\mathcal{O}$ benötigt. Das in [Schm1] erwähnte Problem des Auftretens großer Zwischenergebnisse bei der HNF–Berechnung tritt in unserem Falle nicht auf, da die umzuformenden Matrizen von sehr spezieller Gestalt sind. Sie treten am Schluß des Verfahrens (Abschnitt 4.2.4) auf und sind von der folgenden Form:

$$\begin{pmatrix} * & \cdots & * & p & 0 & \cdots & 0 \\ \vdots & & \vdots & \vdots & p & & \vdots \\ \vdots & & \vdots & & \cdots & \ddots & \vdots \\ * & \cdots & * & 0 & \cdots & & p \end{pmatrix}$$

Hierbei ist p die zu zerlegende Primzahl und die mit '$*$' gekennzeichneten Elemente irgendwelche Zahlen in $\mathbb{N}_0$, die kleiner als p sind. Also ist pI_n ein Teil der Matrix, und es können beliebige Vielfache dieser Spalten zu anderen Spalten addiert werden, so daß bei der Umformung der Matrix o.B.d.A. modulo p gerechnet werden kann. Zusammen mit der Beschreibung der HNF–Berechnung aus [Düll] ergibt sich folgendes Verfahren:

Algorithmus HNF_mod_p

Eingabe: $A' \in \mathbb{Z}^{m\times n}$, wobei $pe_i \in Bild\ A$ für jeden i–ten Einheitsvektor $e_i \in \mathbb{Z}^m$

Ausgabe: $A \in \mathbb{Z}^{n\times n}$ in HNF, so daß $Bild\ A = Bild\ A'$

(1) $A \leftarrow A'$

(2) **for** $i \leftarrow 1$ **to** m **do**

co *sorge beim i–ten Schleifendurchlauf für* $a_{ii} \neq 0$ **oc**

(3) **if** $a_{ii} = 0$ **then**

```
            for j ← i+1 to n do
                if a_ij ≠ 0 then
                    tausche(A,i,j)
                    break
                fi
                od
            fi
        for j ← i+1 to n do
            co reduziere die Elemente der Zeile i
            in den Spalten i+1,...,n oc
            if a_ij ≠ 0 then
                co wir verwenden den erweiterten Euklidischen Algorithmus (siehe unten) oc
                (r,x,y) ← egcd(a_ii, a_ij)
                v ← xA_i + yA_j mod p
                w ← (a_jj/r)A_j − (a_ij/r)A_i mod p
                A_i ← v
                A_j ← w
                fi
            od
        od
    for i ← 2 to m do
        co sorge für 0 ≤ a_ij < a_ii, 1 ≤ j < i oc
        for j ← 1 to i−1 do
            q ← a_ij/a_ii
            A_j ← A_j − qA_i mod p
            od
        od
```

Es folgen einige Anmerkungen zu diesem Algorithmus.

- A_i bedeutet die i-te Spalte von A.

- Spaltenoperationen mod p bedeuten die elementweise Reduzierung jedes Spalteneintrags mod p.
- Die Funktion 'egcd(a_1, a_2)' in Zeile (13) liefert den ggT von a_1 und a_2 und Koeffizienten x, y, so daß

$$ggT(a_1, a_2) \equiv xa_1 + ya_2 \; mod \; p.$$

- Die worst-case-Komplexität ist $O(n^2m)$ Operationen modulo p [Düll].
- Der Benutzer der Prozedur hat zu prüfen, ob das Rechnen modulo p zur Bestimmung der HNF genügt.

Kapitel 4

Der Algorithmus

In diesem Kapitel stellen wir die Grundidee der Weiterentwicklung des in [BuLen] beschriebenen Zerlegungsverfahrens für die Primzahl p vor und geben damit einen Überblick über die zu lösenden Teilprobleme, die im Anschluß daran detailliert besprochen werden. Im letzten Abschnitt wird das Verfahren aus [BuLen] beschrieben und auf die Unterschiede eingegangen.

In diesem Kapitel gehen wir davon aus, daß die eindeutige Primidealzerlegung von $p\mathcal{O}$ in der p–maximalen Ordnung $\mathcal{O}$ von folgender Gestalt ist:

$$p\mathcal{O} = M_1^{e_1} \cdot M_2^{e_2} \cdots M_r^{e_r}. \tag{4.1}$$

Wir werden uns stets auf diese Darstellung von $p\mathcal{O}$ beziehen.

4.1 Vorbemerkung zum Rechnen in $\mathcal{O}/p\mathcal{O}$

Wir haben schon in Abschnitt 2.4 gezeigt, daß es für unsere Zwecke genügt, Ideale in $\mathcal{O}/p\mathcal{O}$ zu betrachten. An dieser Stelle soll der Zusammenhang zwischen $\mathcal{O}$ und $\mathcal{O}/p\mathcal{O}$ noch einmal kurz skizziert werden, damit in der Beschreibung der Idee des Algorithmus die Verwendung von Idealen in $\mathcal{O}$ und $\mathcal{O}/p\mathcal{O}$ gleichzeitig geschehen kann:

- außer im letzten Schritt werden alle Idealoperationen in $\mathcal{O}/p\mathcal{O}$ durchgeführt
- der kanonische Homomorphismus $\Phi : \mathcal{O} \to \mathcal{O}/p\mathcal{O}$ bildet Ideale, die $p\mathcal{O}$ teilen, bijektiv auf die Ideale von $\mathcal{O}/p\mathcal{O}$ ab (Satz 2.47)
- die Abbildung Φ verhält sich bei Idealmultiplikation solcher Ideale homomorph, falls das Ergebnis der Multiplikation noch $p\mathcal{O}$ teilt (Satz 2.50)

- für das Bild eines Elements $\alpha \in \mathcal{O}$ unter der Abbildung Φ, die nichts anderes als Restklassenbildung modulo $p\mathcal{O}$ bedeutet, schreiben wir auch oft $\overline{\alpha}$
- für $A \mid p\mathcal{O}$ ist A aus $\overline{A}$ effizient berechenbar (siehe Abschnitt 4.2.4)
- da Φ ein Homomorphismus ist, sind die Urbilder der maximalen Ideale von $\overline{\mathcal{O}}$ unter Φ gerade die maximalen Ideale von $\mathcal{O}$, die $p\mathcal{O}$ teilen.

4.2 Die Grundidee des Algorithmus

Wir werden nun die Idee des gesamten Verfahrens vorstellen und es dabei bewußt vermeiden, auf technische Einzelheiten einzugehen. Die Behandlung der einzelnen Schritte des Verfahrens erfolgt gesondert in den darauffolgenden Abschnitten. Die fundamentalen Inhalte der Idee stammen aus Zusammenhängen zwischen den ganzen Idealen von $\mathcal{O}$ und den durch sie gebildeten Faktorringen. Es wird Schritt für Schritt das Teilwissen über die Primidealzerlegung von $p\mathcal{O}$ zusammengesetzt.

Die erste Information erhält man durch Kenntnis des Ideals I_p, das das Produkt aller derjenigen Primideale ist, die in der Zerlegung von $p\mathcal{O}$ auftreten. Man bildet den Faktorring $\mathcal{O}/I_p$ und zerlegt diesen in Körper der Gestalt $\mathcal{O}/M_k$, aus denen man die Primideale M_k gewinnt. Schließlich erhält man durch die Bestimmung der Exponenten die vollständige Primidealzerlegung.

Algorithmus FACTOR_P

Eingabe: eine Primzahl p,
eine Multiplikationstabelle w_{ijk}, $1 \leq i, j, k \leq n$ der Ordnung (siehe Abschnitt 3.1)

Ausgabe: paarweise verschiedene Primideale $M_1, \ldots, M_r \trianglelefteq \mathcal{O}$ und Exponenten $e_1, \ldots, e_r \in \mathbb{N}$, so daß

$$(*) \qquad p\mathcal{O} = M_1^{e_1} \cdot M_2^{e_2} \cdots M_r^{e_r}$$

(1) **Berechnung des p–Radikals von $\mathcal{O}$**

Wir beginnen mit Schritt (1) *des Hauptverfahrens und rechnen das Bild $\overline{I_p}$ des p-Radikals I_p von $\mathcal{O}$ unter Φ aus. Dieses hat mit den Bezeichnungen von Gleichung $(*)$ die Primidealdarstellung*

$$\overline{I}_p = \overline{M}_1 \overline{M}_2 \cdots \overline{M}_r.$$

$\overline{I_p}$ ist das Nilradikal von $\overline{\mathcal{O}}$ und läßt sich als Kern von

$$\begin{array}{ccc} \mathcal{O}/p\mathcal{O} & \to & \mathcal{O}/p\mathcal{O} \\ \overline{\alpha} & \mapsto & \overline{\alpha}^{p^l} \end{array}$$

berechnen. Hierbei ist der Exponent l von p so zu wählen, daß $p^l \geq n$.

(2) **Zerlegung des p–Radikals in maximale Ideale**

Setze $\overline{I} := \overline{I_p}$ und betrachte $\overline{\mathcal{O}}/\overline{I}$. Dieses ist übrigens nach dem dritten Isomorphiesatz für Ringe [Hun, Th.III.2.12] gleich $\mathcal{O}/I$. Wir stellen nun fest, ob $\overline{\mathcal{O}}/\overline{I}$

1. *ein Körper oder*
2. *kein Körper*

ist.

Im ersten Fall ist auch $\mathcal{O}/I$ ein Körper und daher I maximal, also ein Primideal. Im zweiten Fall ist $\overline{I}$ zerlegbar, und es gibt einen Nullteiler $\gamma \in \overline{\mathcal{O}}/\overline{I}$. Nun zerlegt man $A := \overline{\mathcal{O}}/\overline{I}$ in

$$A \cong {}^{A}\!/\!{}_{\gamma A} \times {}^{A}\!/\!{}_{Ann\gamma}.$$

Wenn man diese Darstellung von A gefunden hat, kann man $\overline{I}$ zerlegen in

$$\overline{I} = \overline{I}_1 \overline{I}_2.$$

Es ist nämlich

$$\begin{array}{rcl} \overline{I}_1 & = & \Theta^{-1}(\gamma A) \\ \overline{I}_2 & = & \Theta^{-1}(Ann\gamma), \quad \textit{wobei} \end{array}$$

$$\Theta : \ \mathcal{O}/p\mathcal{O} \ \to A$$

die kanonische Restklassenbildung in $\mathcal{O}/p\mathcal{O}$ nach dem Ideal $\overline{I} \trianglelefteq \mathcal{O}/p\mathcal{O}$ bedeutet. Man setzt nun nacheinander $\overline{I} := \overline{I}_1$ und $\overline{I} := \overline{I}_2$ und führt Schritt 2 solange iterativ aus, bis jeder Durchlauf im Fall 1 abbricht, also jedes betrachtete Ideal maximal ist.

(3) **Bestimmung der Exponenten**

Wir kennen schon die maximalen Ideale $\overline{M_i}$, für die

$$\overline{I_p} = \overline{M}_1 \cdot \overline{M}_2 \cdots \overline{M}_r.$$

Aus dieser Zerlegung können wir die Exponenten $e_1, \ldots, e_r$ berechnen, für die

$$p\mathcal{O} = M_1^{e_1} \cdot M_2^{e_2} \cdots M_r^{e_r}.$$

Sei nun $\overline{M} := \overline{M}_i$ für ein i mit $1 \le i \le r$.
Wir bilden sukzessive $\overline{M}^j$ für $j \ge 2$. Ist nun $j = e_i$, so gilt

$$\overline{M}^{j+1} = \overline{M}^j.$$

Daher haben wir, sobald Gleichheit auftritt, mit $e_i := j$ den Exponenten für M_i bestimmt. Dies tun wir für $1 \le i \le r$.

(4) **Zerlegung in $\overline{\mathcal{O}} \to$ Zerlegung in $\mathcal{O}$**

Der dritte Schritt liefert uns

$$(\overline{0}) = \overline{M}_1^{e_1} \cdot \overline{M}_2^{e_2} \cdots \overline{M}_r^{e_r}$$

in $\mathcal{O}/p\mathcal{O}$. Wir wollen nun für $1 \le i \le r$ aus $\overline{M}_i \trianglelefteq \overline{\mathcal{O}}$ die Ideale $M_i \trianglelefteq \mathcal{O}$ bestimmen.
Da

$$\overline{M}_i = {}^{M_i}\!/_{p\mathcal{O}} =< \overline{\beta}_{i1}, \ldots, \overline{\beta}_{is_i} >_{\mathbb{F}_p}$$

ist, wird M_i von

$$\{\beta_{i1}, \ldots, \beta_{is_i}, p\omega_1, \ldots, p\omega_n\}$$

über $\mathbb{Z}$ erzeugt.
Daher muß man aus einem Erzeugendensystem eines freien $\mathbb{Z}$-Moduls eine Basis des $\mathbb{Z}$-Moduls bestimmen. Das Standardverfahren dazu ist das Bestimmen der Hermite-Normalform der Koeffizientenmatrix — siehe dazu Abschnitt 3.4. Nach diesem Schritt hat man die gewünschte Ausgabe.

In den folgenden Abschnitten besprechen wir die Einzelheiten der vorgestellten Idee, beweisen die verwendeten Tatsachen und schließen theoretische Aussagen über die Laufzeit an.

Zur Veranschaulichung führen wir in den einzelnen Schritten ein Beispiel mit, das die Zerlegung der Primzahl 3 im Ganzheitsring eines Körpers vom Grade 6 demonstriert.

Wir betrachten dabei $\mathbb{Q}(\rho)$, wobei ρ eine Nullstelle des über $\mathbb{Q}$ irreduziblen Polynoms X^6+2 ist. Der Ganzheitsring $\mathcal{O}_K$ wurde durch das Programmpaket [PARI] bestimmt und ist gleich $\mathbb{Z}[\rho]$. Dies gibt uns gleichzeitig die Gelegenheit, die Zerlegung einer Primzahl durch Anwendung des Satzes 2.62 zu erhalten und das Verhalten unseres Verfahrens schon mit dem Wissen um die Lösung zu beobachten.

Zerlegt man nämlich das erzeugende Polynom f über $\mathbb{F}_3$, so erhält man

$$X^6 + 2 \equiv (X+1)^3(X+2)^3 \; mod \; 3,$$

was schon die eindeutige Zerlegung von $3\mathcal{O}_\mathcal{K}$ in Primideale liefert:

$$3\mathcal{O}_\mathcal{K} = P_1^3 P_2^3 = (3\mathcal{O}_\mathcal{K} + (\rho+1)\mathcal{O}_\mathcal{K})^3 \cdot (3\mathcal{O}_\mathcal{K} + (\rho+2)\mathcal{O}_\mathcal{K})^3.$$

Als $\mathbb{Z}$–Basis für $\mathbb{Z}[\rho]$ wählen wir $\{1, \rho, \rho^2, \rho^3, \rho^4, \rho^5\}$ und haben damit gleichzeitig folgende Bezeichnungen festgelegt:

$$\omega_j = \rho^{j-1}, \quad 1 \leq j \leq 6.$$

Da wir zur Zerlegung von $3\mathcal{O}$ in $\mathcal{O}/3\mathcal{O}$ rechnen, legen wir zusätzlich

$$\overline{\omega}_j = \omega_j + 3\mathcal{O} \in {}^{\mathcal{O}}\!/_{3\mathcal{O}}, \quad 1 \leq j \leq 6$$

fest.

Die Multiplikationstabelle kann mit Blick auf das Polynom f und der Vorgabe $\mathcal{O} = \mathbb{Z}[\rho]$ direkt angegeben werden:

```
MUTAB in O/3O:
w11: 1 0 0 0 0 0
w12: 0 1 0 0 0 0
w13: 0 0 1 0 0 0
w14: 0 0 0 1 0 0
w15: 0 0 0 0 1 0
w16: 0 0 0 0 0 1
w21: 0 1 0 0 0 0
w22: 0 0 1 0 0 0
w23: 0 0 0 1 0 0
w24: 0 0 0 0 1 0
w25: 0 0 0 0 0 1
w26: 1 0 0 0 0 0
w31: 0 0 1 0 0 0
w32: 0 0 0 1 0 0
w33: 0 0 0 0 1 0
w34: 0 0 0 0 0 1
w35: 1 0 0 0 0 0
w36: 0 1 0 0 0 0
w41: 0 0 0 1 0 0
w42: 0 0 0 0 1 0
w43: 0 0 0 0 0 1
w44: 1 0 0 0 0 0
w45: 0 1 0 0 0 0
w46: 0 0 1 0 0 0
```

```
w51: 0 0 0 0 1 0
w52: 0 0 0 0 0 1
w53: 1 0 0 0 0 0
w54: 0 1 0 0 0 0
w55: 0 0 1 0 0 0
w56: 0 0 0 1 0 0
w61: 0 0 0 0 0 1
w62: 1 0 0 0 0 0
w63: 0 1 0 0 0 0
w64: 0 0 1 0 0 0
w65: 0 0 0 1 0 0
w66: 0 0 0 0 1 0
```

Hierbei bedeutet beispielsweise die vorletzte Zeile:

$$\overline{\omega}_6 \cdot \overline{\omega}_5 = 0\overline{\omega}_1 + 0\overline{\omega}_2 + 0\overline{\omega}_3 + 1\overline{\omega}_4 + 0\overline{\omega}_5 + 0\overline{\omega}_6.$$

4.2.1 Berechnung des p-Radikals I_p

Wir besprechen jetzt Schritt (1) des Hauptverfahrens.

Das p-Radikal I_p von $\mathcal{O}$ ist definiert als das Produkt aller maximalen Ideale, die $p\mathcal{O}$ teilen (Def. 2.42), also

$$I_p = M_1 M_2 \cdots M_r.$$

Nach den Vorbemerkungen in Abschnitt 4.1 wissen wir schon, daß es für $p\mathcal{O}$ teilende Ideale genügt, ihr Bild unter Φ in $\mathcal{O}/p\mathcal{O}$ zu betrachten. Daher sind wir interessiert an

$$\overline{I_p} = \overline{M}_1 \overline{M}_2 \cdots \overline{M}_r.$$

Da jedoch $\overline{M}_1, \overline{M}_2 \ldots, \overline{M}_r$ nicht bekannt sind, benötigen wir eine andere Charakterisierung von $\overline{I_p}$. Es wird sich zeigen, daß $\overline{I}_p$ gerade das Ideal aller nilpotenten Elemente in $\mathcal{O}/p\mathcal{O}$ ist. Dazu geben wir die folgende auf beliebige Ringe verallgemeinerte

4.1 Definition *Sei R ein Ring und sei $a \in R$. Dann heißt*

$$a \textit{ nilpotent} \iff \exists k \in \mathbb{N} \textit{ mit } a^k = 0.$$

Die zuvor erwähnte Aussage präzisieren wir durch die folgende Proposition.

4.2 Proposition *Sei I_p das p-Radikal von $\mathcal{O}$.*

Dann gilt für $\overline{I_p} = \Phi(I_p) \trianglelefteq \mathcal{O}/p\mathcal{O}$

$$\overline{I_p} = \{\overline{\alpha} \in \mathcal{O}/p\mathcal{O} \mid \overline{\alpha} \textit{ nilpotent } \}.$$

Beweis: Es ist zu zeigen, daß

$$\{\overline{\alpha} \in \mathcal{O}/p\mathcal{O} \mid \overline{\alpha}\ nilpotent\ \} = \overline{M}_1\overline{M}_2\cdots\overline{M}_r.$$

Dazu zeigen wir zunächst "$\subseteq$".

Es sei also $\overline{\alpha} \in \mathcal{O}/p\mathcal{O}$ nilpotent und $k \in \mathbb{N}$ ein Exponent von $\overline{\alpha}$, so daß $\overline{\alpha}^k = 0$ gilt.

$\Rightarrow$ für jeden Repräsentanten $\alpha \in \alpha + p\mathcal{O}$ gilt $\alpha^k \in p\mathcal{O}$

$\Rightarrow$ $\alpha^k\mathcal{O} \subseteq p\mathcal{O}$

$\Rightarrow$ $p\mathcal{O} | \alpha^k\mathcal{O}$

$\Rightarrow$ $M_i | \alpha^k\mathcal{O}$ $\quad 1 \leq i \leq r$

$\Rightarrow$ $M_i | \underbrace{\alpha\mathcal{O}\cdots\alpha\mathcal{O}}_{k-mal}$ $\quad 1 \leq i \leq r$

$\Rightarrow$ $M_i | \alpha\mathcal{O}$ $\quad 1 \leq i \leq r$, da M_i maximal

$\Rightarrow$ $M_i \supseteq \alpha\mathcal{O}$ $\quad 1 \leq i \leq r$

$\Rightarrow$ $\alpha \in M_i$ $\quad 1 \leq i \leq r$

$\Rightarrow$ $\alpha \in M_1 \cap \ldots \cap M_r = M_1 \cdot M_2 \cdots M_r$

$\Rightarrow$ $\alpha \in I_p$ $\quad$ für alle Repräsentanten α

$\Rightarrow$ $\overline{\alpha} \in \overline{I_p}$

Nun zeigen wir "$\supseteq$".

Sei also $\overline{\alpha} \in \overline{M}_1 \cdot \overline{M}_2 \cdots \overline{M}_r$.

$\Rightarrow$ für jeden Repräsentant $\alpha \in \mathcal{O}$ gilt $\alpha \in M_1 \cdot M_2 \cdots M_r$

$\Rightarrow$ $\alpha\mathcal{O} \subseteq M_1 \cdot M_2 \cdots M_r$

Sei nun $e := max\{e_i \mid 1 \leq i \leq r\}$

$\Rightarrow$ $\alpha^e\mathcal{O} \subseteq M_1^e \cdot M_2^e \cdots M_r^e \subseteq p\mathcal{O}$

$\Rightarrow$ $\overline{\alpha}^e = 0 \in \mathcal{O}/p\mathcal{O}$

$\Rightarrow$ $\overline{\alpha}$ nilpotent in $\mathcal{O}/p\mathcal{O}$

Damit ist die Proposition bewiesen. ■

Die Proposition rechtfertigt also die Bezeichnung Nilradikal für $\overline{I_p}$.

Die Berechnung von $\overline{I_p}$ beruht auf dem folgenden Satz, dessen Beweis im wesentlichen eine Anwendung der vorangehenden Proposition ist.

4.3 Satz *Sei folgender Endomorphismus in $(\mathcal{O}/p\mathcal{O},+)$ gegeben:*

$$\begin{aligned} \varphi : \mathcal{O}/p\mathcal{O} &\rightarrow \mathcal{O}/p\mathcal{O} \\ \overline{\alpha} &\mapsto \overline{\alpha}^{p^l}, \end{aligned} \tag{4.2}$$

wobei $l \in \mathbb{N}$ so gewählt ist, daß $p^l \geq dim_{\mathbb{F}_p} \mathcal{O}/p\mathcal{O}$.
Dann ist

$$\overline{I_p} = Kern\ \varphi.$$

Beweis: In Ringen R der Charakteristik p ist φ tatsächlich ein Endomorphismus der additiven abelschen Gruppe von R. Seien $\overline{\alpha}, \overline{\beta} \in R$, dann gilt

$$\begin{aligned} (\overline{\alpha} + \overline{\beta})^p &= \sum_{k=0}^{p} \binom{p}{k} \overline{\alpha}^k \overline{\beta}^{p-k} \\ &= \overline{\alpha}^p + \overline{\beta}^p. \end{aligned}$$

Das letzte Gleichheitszeichen gilt wegen $\binom{p}{k} \equiv 0\ mod\ p$ für $k \neq 0$ und $k \neq p$.

Zuerst zeigen wir $\overline{I_p} \subseteq Kern\ \varphi$:

$$\begin{array}{lll} \text{sei} & \overline{\alpha} \in \overline{I_p} & \text{und } n := dim_{\mathbb{F}_p} \mathcal{O}/p\mathcal{O} \\ \Rightarrow & \alpha \in I_p & \text{für jeden Repräsentanten } \alpha \\ \Rightarrow & \alpha^n \in I_p^n & \\ \Rightarrow & \alpha^n \mathcal{O} \subseteq I_p^n & \subseteq p\mathcal{O} \\ \Rightarrow & \overline{\alpha}^n = 0 & \text{in } \mathcal{O}/p\mathcal{O} \end{array}$$

Wegen $\overline{\alpha}^n = 0$ und $p^l \geq n$ gilt auch $\overline{\alpha}^{p^l} = 0$, woraus $\overline{\alpha} \in Kern\ \varphi$ folgt.

Ist umgekehrt $\overline{\alpha} \in Kern\ \varphi$, so ist $\overline{\alpha}$ nach Proposition 4.2 als nilpotentes Element von $\mathcal{O}/p\mathcal{O}$ auch in $\overline{I_p}$ enthalten.

Damit ist der Satz bewiesen. ■

Nach diesen Vorüberlegungen können wir jetzt den Algorithmus zur Bestimmung des p–Radikals/Nilradikals angeben.

Algorithmus P–RADICAL

Eingabe: eine Primzahl p

Ausgabe: das Nilradikal $\overline{I_p}$ von $\mathcal{O}/p\mathcal{O}$

(1) $n \leftarrow dim_{\mathbb{F}_p}\mathcal{O}/p\mathcal{O}$
co *berechne* $q = p^l$ *so, daß* $q \geq n$ **oc**
(2) $q \leftarrow p$
(3) **while** $q < n$ **do**
(4) $\quad q \leftarrow q \cdot p$
(5) $\quad$ **od**
co *berechne Bilder der Standardbasis von* $\mathcal{O}/p\mathcal{O}$*und erzeuge aus ihnen die Matrix der Abbildung* $\alpha \mapsto \alpha^q$ **oc**
(6) **for** $k \leftarrow 1$ **to** n **do**
(7) $\quad A_k \leftarrow$ *Koeffizientenvektor von* $\overline{\omega}_k^q$
(8) $\quad$ **od**
co *liefere den Kern der Abbildung als Ergebnis zurück* **oc**
(9) $I_p \leftarrow KERN(A)$
(10) **return** I_p

Zu diesem Algorithmus sind zwei Punkte anzumerken.

- Die in Schritt 7 erzeugte Matrix A ist die Abbildungsmatrix von φ.
- Die worst-case-Laufzeit für die Prozedur 'P–RADICAL' beträgt

$$O(n \cdot n^2 \cdot \log q + n^3) = O(n^3 \log n \log p)$$

Operationen in $\mathbb{F}_p$. Es müssen nämlich n Basiselemente potenziert werden. Jede Exponentiation besteht aus jeweils $O(\log q)$ Multiplikationen. Multiplikation in $\mathcal{O}/p\mathcal{O}$ braucht Zeit $O(n^2)$. Danach wird der Kern der erstellten Abbildungsmatrix in Zeit $O(n^3)$ berechnet.

Fortführung des Beispiels

Da in unserem Beispiel $3\mathcal{O}_\mathcal{K}$ in die beiden oben angegebenen Primideale vom Verzweigungsgrad 3 zerfällt, muß I_3 das Produkt

$$I_3 = 3\mathcal{O}_\mathcal{K} + (\rho+1)\mathcal{O}_\mathcal{K} \cdot (\rho+2)\mathcal{O}_\mathcal{K}$$

sein.
Wir erhalten in $I_3 + 3\mathcal{O}_\mathcal{K} \trianglelefteq \mathcal{O}/3\mathcal{O}$. Dies wurde berechnet als

```
p-radical:
(1)   (0)   (0)   (0)
(0)   (1)   (0)   (0)
(0)   (0)   (1)   (0)
(0)   (0)   (0)   (1)
(2)   (0)   (2)   (0)
(0)   (2)   (0)   (2)
```

Dies bedeutet, eine $\mathbb{F}_3$–Basis für $I_3 + 3\mathcal{O}$ ist

$$\{\overline{\omega}_1 + 2\overline{\omega}_5, \overline{\omega}_2 + 2\overline{\omega}_6, \overline{\omega}_3 + 2\overline{\omega}_5, \overline{\omega}_4 + 2\overline{\omega}_6\}$$

4.2.2 Zerlegung von I_p in maximale Ideale

Es folgt nun die Beschreibung von Schritt (2) des Hauptverfahrens, der mit rund 80% der gesamten Rechenzeit den aufwendigsten Teil bildet. Daher wurde gerade hier auf eine besonders sorgfältige Aufbereitung der Theorie und eine möglichst effiziente Implementierung Wert gelegt.

Wir skizzieren zunächst die zu lösende Aufgabenstellung.

Gegeben ist ein Produkt $\overline{I}$ aus paarweise verschiedenen maximalen Idealen

$$\overline{I} = \prod_{l=1}^{d} \overline{M}'_l,$$

das daher quadratfrei ist. Gesucht ist entweder

- ein Maximalitätsbeweis für $\overline{I}$, was gleichbedeutend ist mit $d = 1$, oder
- eine Zerlegung $\overline{I} = \overline{I}_1 \cdot \overline{I}_2$ in zwei nichttriviale Ideale $\overline{I}_1, \overline{I}_2$ im Falle $d \geq 2$.

Dazu wird zunächst die $\mathbb{F}_p$–Algebra

$$A := {}^{\overline{\mathcal{O}}}\!/_{\overline{I}} \tag{4.3}$$

gebildet, die genau dann ein Körper ist, wenn $\overline{I}$ ein maximales Ideal ist.

In diesem Falle wird die Prozedur mit dem Ergebnis '$\overline{I}$ maximal' abgebrochen. Im anderen Falle ist A kein Körper, das heißt es gibt echte Ideale $\overline{I}_1, \overline{I}_2$, so daß

$$A = {}^{\overline{\mathcal{O}}}\!/_{\overline{I}_1\overline{I}_2}.$$

Daher gilt für $\overline{\alpha} \in \overline{I}_1 \setminus \overline{I}$ und $\overline{\beta} \in \overline{I}_2 \setminus \overline{I}$

$$(\overline{\alpha} + \overline{I})(\overline{\beta} + \overline{I}) = 0 \in A$$

mit von Null verschiedenen Elementen $\overline{\alpha}$ und $\overline{\beta}$. Dies bedeutet jedoch, daß es in A Nullteiler geben muß. Hat man einen Nullteiler $\gamma \in A$ bestimmt, dann sind nach Lemma 2.21

$$Ann\ \gamma \quad \text{und} \quad \gamma A$$

echte Ideale in A mit

$$A = {}^{A}\!/_{(0)} = {}^{A}\!/_{(\gamma A\ \cdot\ Ann\ \gamma)} \cong {}^{A}\!/_{\gamma A} \times {}^{A}\!/_{Ann\ \gamma}. \tag{4.4}$$

Aus dieser Zerlegung von A rekonstruieren wir nun die zu γA und $Ann\ \gamma$ gehörigen Ideale $\overline{I}_1, \overline{I}_2$ von $\mathcal{O}/p\mathcal{O}$. Dann wenden wir für $\overline{I} := \overline{I}_1$ und $\overline{I} := \overline{I}_2$ das gleiche Verfahren erneut an, bis alle betrachteten Ideale maximal sind.
Zunächst zeigen wir die Existenz der Zerlegung (4.4) und beweisen in diesem Zusammenhang die folgende Aussage.

4.4 Satz *Sei A eine $\mathbb{F}_p$–Algebra und γ ein Nullteiler in A. Dann gilt*

$$A \cong {}^{A}\!/_{\gamma A} \times {}^{A}\!/_{Ann\ \gamma}.$$

Beweis: Wir beginnen mit der Tatsache $\gamma A \cdot Ann\ \gamma = (0)$:
es seien etwa $\eta_1 \in \gamma A$ und $\eta_2 \in Ann\ \gamma$, dann gilt $\eta_1 = \gamma\alpha$ für ein $\alpha \in A$ und $\gamma\eta_2 = 0$. Daraus folgt

$$\eta_1\eta_2 = \gamma\alpha\eta_2 = \gamma\eta_2\alpha = 0.$$

Das Idealprodukt, das aus den Summen solcher Elementprodukte besteht, kann also nur das Nullelement enthalten.

Damit haben wir

$$A \cong {}^{A}\!/_{(0)} \cong {}^{A}\!/_{\gamma A \cdot Ann\ \gamma}.$$

Es gilt weiter $\gamma A + Ann\ \gamma = A$, denn der Endomorphismus

$$\begin{aligned} \psi:\ A &\to\ A \\ \alpha &\mapsto\ \gamma\alpha \end{aligned}$$

hat als Bild γA und als Kern $Ann\ \gamma$, woraus nach dem ersten Homomorphiesatz für Gruppen [Hun, Cor.I.5.7.] die Beziehung

$$A/_{Ann\ \gamma} \cong \gamma A$$

folgt.
Es sind daher die Voraussetzungen des Satzes 2.36 erfüllt, und wir können

$$A \cong A/_{(0)} \cong A/_{\gamma A \cdot Ann\ \gamma} \cong A/_{\gamma A} \times A/_{Ann\ \gamma}$$

schließen. ■

Um festzustellen, ob A ein Körper ist, betrachte man die folgende Abbildung:

$$\begin{aligned} \vartheta: \quad A &\rightarrow \quad A \\ \alpha &\mapsto \quad \alpha^p - \alpha. \end{aligned} \tag{4.5}$$

Im Beweis zu Satz 4.3 haben wir schon gezeigt, daß in Ringen der Charakteristik p das Erheben in die p–te Potenz eine homomorphe Abbildung ist. Da die Endomorphismen eines Ringes ebenfalls einen Ring bilden und Subtraktion von α die Subtraktion der identischen Abbildung ist, ist auch ϑ ein Endomorphismus.
Wir rechnen den Kern von ϑ aus und betrachten zwei Fälle.

Fall a) A **ist ein Körper**

Dann ist es klar, daß das Polynom $F(X) := X^p - X$ höchstens p Nullstellen in A hat. Außerdem gilt jedoch $F(1) = 0$. Setzt man dies zusammen mit der Tatsache, daß ϑ homomorph ist, gilt $F(k) = 0$ für $0 \leq k \leq p-1$. Damit ergibt sich

$$\mathbb{F}_p = Kern\ \vartheta.$$

Also gilt das

4.5 Lemma

$$A\ Körper \Rightarrow dim_{\mathbb{F}_p} Kern\ \vartheta = 1.$$

Fall b) A **ist kein Körper**

Wegen $A = \mathcal{O}/I$ ist dann I nicht maximal. Da I das Produkt paarweise verschiedener maximaler Ideale ist, gilt nach Satz 2.36

$$A \cong \mathcal{O}/_{I_1} \times \mathcal{O}/_{I_2}. \tag{4.6}$$

Die Abbildung

$$\vartheta': \mathcal{O}/_{I_1} \times \mathcal{O}/_{I_2} \xrightarrow{\sim} A \xrightarrow{\vartheta} A \xrightarrow{\sim} \mathcal{O}/_{I_1} \times \mathcal{O}/_{I_2}$$

enthält im Kern die Menge $\mathbb{F}_p \times \mathbb{F}_p$, aber $dim_{\mathbb{F}_p} \mathbb{F}_p \times \mathbb{F}_p = 2$.
Daher gilt

$$dim_{\mathbb{F}_p} Kern\ \vartheta = dim_{\mathbb{F}_p} Kern\ \vartheta' \geq 2 > 1.$$

Damit haben wir das folgende Lemma.

4.6 Lemma

$$dim_{\mathbb{F}_p} Kern\ \vartheta = 1 \Rightarrow A\ Körper.$$

Setzt man die beiden letzten Lemmata zusammen, so ergibt sich ein handliches Kriterium, um die Körpereigenschaft von A zu überprüfen:

4.7 Satz *Mit den Bezeichnungen (4.3) für A und (4.5) für ϑ gilt:*
A ist genau dann ein Körper, wenn

$$dim_{\mathbb{F}_p} Kern\ \vartheta = 1.$$

Dieses Ergebnis legt die folgende Vorgehensweise nahe:

Wir berechnen die Abbildungsmatrix M_ϑ des Endomorphismus ϑ bezüglich der $\mathbb{F}_p$–Basis von A und bestimmen eine Basis B von $Kern\ \vartheta$. Enthält B nur ein Element, so liegt Fall a) vor, denn es ist

$$A = \mathcal{O}/I$$

als Körper erkannt, und wir können I mit der Information 'I maximal' zurückliefern.

Falls die Basis B aus mehreren Elementen besteht, gibt es eine Zerlegung (4.6). Wir haben schon beschrieben, daß eine solche Zerlegung durch Bestimmung eines Nullteilers in A ermöglicht wird. Durch die Überlegungen zu Anfang dieses Abschnitts ist es klar, daß es in A einen Nullteiler geben muß. Wir nutzen zu seiner Bestimmung eine Information aus, die durch die Abbildung ϑ geliefert wird.

Fortführung des Beispiels

Wir zerlegen I_3 in die zwei Primideale, aus denen es besteht.

```
factor Ip=
(1)   (0)   (0)   (0)
(0)   (1)   (0)   (0)
(0)   (0)   (1)   (0)
(0)   (0)   (0)   (1)
(2)   (0)   (2)   (0)
(0)   (2)   (0)   (2)
%%%%%%%%%%%%%%%%%%%%%%%%%%%% the decomposition
I[1]:=
(1)   (1)   (0)   (0)   (0)
(2)   (0)   (1)   (0)   (0)
(0)   (2)   (0)   (1)   (0)
(0)   (0)   (2)   (0)   (1)
(0)   (0)   (0)   (2)   (0)
(0)   (0)   (0)   (0)   (2)
---
I[2]:=
(1)   (1)   (0)   (0)   (0)
(1)   (0)   (1)   (0)   (0)
(0)   (2)   (0)   (1)   (0)
(0)   (0)   (2)   (0)   (1)
(0)   (0)   (0)   (2)   (0)
(0)   (0)   (0)   (0)   (2)
----------------------------
factor I[1]: I[1] is maximal
----------------------------
factor I[2]: I[2] is maximal
----------------------------
```

Die Darstellung von I_1 und I_2 erfolgte wie im Beispiel zu I_p.

Hierbei war der Ablauf folgendermaßen:
zunächst wurde erkannt, daß $\mathcal{O}/I_p$ kein Körper ist, danach ein Nullteiler in $\mathcal{O}/I_p$ bestimmt und daraus mit dem oben beschriebenen Verfahren die Ideale I_1 und I_2 bestimmt.

Diese wurden mit der Feststellung '$\mathcal{O}/I_1$ Körper' beziehungsweise '$\mathcal{O}/I_2$ Körper' als maximal erkannt und an das Hauptverfahren zurückgegeben.

Berechnung eines Nullteilers in $\mathcal{O}/I$

Wir kennen schon ein Produkt aus lauter von Null verschiedenen Termen in A, das gleich Null ist. Der Kern von ϑ hat nach Satz 4.7 eine von 1 verschiedene Dimension über $\mathbb{F}_p$. Also können wir aus seiner Basis K ein Element $\beta \notin \mathbb{F}_p$ wählen. Dies führt zu

$$0 = \beta^p - \beta = \beta(\beta - 1)(\beta - 2) \cdots (\beta - (p-1)).$$

Wegen $\beta - a \neq 0$ für alle $a \in \mathbb{F}_p$ gibt es mindestens zwei Terme $\beta - a_1, \beta - a_2$, die Nullteiler in A sein müssen. Die Methode, einen dieser Terme zu finden, benutzt die Berechnung des Minimalpolynoms von β über $\mathbb{F}_p$. Dieses ist das normierte Polynom $m(X) \in \mathbb{F}_p[X]$ minimalen Grades, so daß $m(\beta) = 0$. Seine Berechnung diskutieren wir im nächsten Abschnitt. Da $\mathbb{F}_p$ ein Körper, also $\mathbb{F}_p[X]$ ein euklidischer Ring ist, gilt

$$X^p - X = q(X)m(X) + r(X),\ deg\ r(X) < deg\ m(X)\ oder\ r(X) \equiv 0$$

mit eindeutig bestimmten Polynomem $q(X), r(X) \in \mathbb{F}_p[X]$.

Setzt man nun in diese Gleichung β ein, folgt

$$0 = \beta^p - \beta = q(\beta)\underbrace{m(\beta)}_{=0} + r(\beta).$$

und daher $r(\beta) = 0$. Da $r(X)$ einen kleineren Grad als das Minimalpolynom hat, muß $r \equiv 0$ gelten. Daher besteht $m(X)$ als Teiler von $X^p - X$ nur aus Linearfaktoren.

$$m(X) = (X - a_1) \cdots (X - a_{deg\ m})$$

Für jeden Linearfaktor $X - a_i$ von $m(X)$ gilt wegen der Minimaleigenschaft von $m(X)$, daß $\beta - a_i$ ein Nullteiler in A ist. Also reduziert sich das Problem, einen Nullteiler zu finden, auf das Problem, eine Nullstelle x_0 von $m(X)$ in $\mathbb{F}_p$ zu bestimmen. Das Verfahren dazu wird im übernächsten Abschnitt erläutert. Mit $\gamma := \beta - x_0 \in A$ ist also ein Nullteiler gefunden.

Die Zerlegung

$$A \cong A/\gamma A \times A/Ann\ \gamma$$

erhält man durch Berechnung von Kern und Bild des Endomorphismus

$$\begin{aligned} \Psi_\gamma :\ A &\to A \\ \alpha &\mapsto \gamma\alpha. \end{aligned} \tag{4.7}$$

Es ist nämlich

$$\begin{aligned} \gamma A &= \{\xi \in A \mid \exists \alpha \in A\ mit\ \xi = \gamma\alpha\} \\ &= Bild\ \Psi_\gamma \\ &=: A_1 \trianglelefteq A, \end{aligned}$$

$$\begin{aligned} Ann\ \gamma &= \{\alpha \in A \mid \gamma\alpha = 0\} \\ &= Kern\ \Psi_\gamma \\ &=: A_2 \trianglelefteq A. \end{aligned}$$

Also berechnen wir die Abbildungsmatrix von Ψ_γ und bestimmen Kern und Bild dieser Matrix. Hierzu wurden die jeweiligen Prozeduren zusammengefaßt, damit nur einmal die aufwendige Berechnung der Spaltenstufenform notwendig wird. Sind die Basen für A_1, A_2 bestimmt, so müssen aus der Beziehung

$$\mathcal{O}/I = (\mathcal{O}/I)/A_1 \times (\mathcal{O}/I)/A_2 = \mathcal{O}/I_1 \times \mathcal{O}/I_2$$

noch die Ideale I_1, I_2 konstruiert werden, für die dann

$$I = I_1 I_2$$

gilt. Man hat dazu zwei nicht wesentlich verschiedene Wege zur Verfügung, von denen einer jedoch bequemer zu beschreiten ist.

1. Wir betrachten dazu eine Verkettung kanonischer Epimorphismen

$$g_k : \mathcal{O} \to \mathcal{O}/I \to (\mathcal{O}/I)/A_k$$

für $k = 1, 2$ und wenden den ersten Isomorphiesatz für Ringe [Hun, CorIII.2.10] an. Damit erhalten wir

$$\mathcal{O}/Kern\ g_k \cong Bild\ g_k$$

Nun ist g_k surjektiv, also

$$Bild\ g_k = (\mathcal{O}/I)/A_k = \mathcal{O}/I_1 = \mathcal{O}/Kern\ g_k\ ,$$

was nichts anderes als

$$I_k = Kern\ g_k \qquad \text{für } k = 1, 2$$

bedeutet.

2. Algorithmisch einfacher ist es, das folgende äquivalente Problem zu lösen, da es dabei vermieden werden kann, die $\mathbb{F}_p$–Algebra

$$(\mathcal{O}/I)/A_k$$

zu bilden.

Seien $I = < \rho_1, \ldots, \rho_m >_{\mathbb{F}_p}$ und

$$A = \mathcal{O}/I = < \rho_1, \ldots, \rho_m, \omega_{\pi_1}, \ldots, \omega_{\pi_{n-m}} >_{\mathbb{F}_p}\ .$$

Der Index π_i gibt an, welche ω-Basisvektoren zu den Basisvektoren von I ergänzt werden müssen, um eine Basis für $\mathcal{O}$ zu erhalten.

Hieraus erhält man $\overline{I}_1, \overline{I}_2$ als Urbild von γA bzw. $Ann\ \gamma$ unter der Abbildung

$$\begin{array}{rccl} \psi : & \overline{\mathcal{O}} & \longrightarrow & A \\ & x_1\overline{\omega}_1 + \ldots + x_n\overline{\omega}_n & \mapsto & y_1\overline{\omega}_{\pi_1} + \ldots + y_{n-m}\overline{\omega}_{\pi_{n-m}} \ + \ I \end{array} \qquad (4.8)$$

Damit ist $I = I_1 I_2$ in zwei nichttriviale Ideale zerlegt.

Berechnung des Minimalpolynoms für $\beta \in A$

Gegeben: ein Element $\overline{\beta} + \overline{I} \in \overline{\mathcal{O}}/\overline{I}$, $n - l = dim_{\mathbb{F}_p} \overline{I}$

Gesucht: das Minimalpolynom $m(X) \in \mathbb{F}_p[X]$ von $\overline{\beta} + \overline{I}$

Idee: Berechne den Kern der Abbildung

$$\begin{aligned} \Lambda: \qquad {\mathbb{F}_p}^{l+1} &\longrightarrow A \\ (x_0, \ldots, x_l) &\mapsto \sum_{i=1}^{l} x_i \overline{\alpha}^i. \end{aligned} \tag{4.9}$$

Die $l + 1$ Potenzen $\overline{\beta}^0, \overline{\beta}^1, \ldots, \overline{\beta}^l$ müssen wegen $l = dim_{\mathbb{F}_p} A$ linear abhängig sein und liefern daher über $\mathbb{F}_p$ eine nichttriviale Linearkombination der 0.

Es sei dazu $\{\overline{\alpha}_1, \ldots, \overline{\alpha}_{n-l}\}$ eine Basis für $\overline{I}$. Diese ergänzen wir mit Hilfe der Standardbasis $\{\overline{\omega}_1, \ldots, \overline{\omega}_n\}$ von $\overline{\mathcal{O}}$ zu einer Basis von $\overline{\mathcal{O}}$ (siehe Abschnitt 3.3.5). Damit haben wir also eine zweite Darstellung für $\overline{\mathcal{O}}$:

$$\overline{\mathcal{O}} = < \underbrace{\overline{\beta}_1, \ldots, \overline{\beta}_{n-l}}_{\overline{I}}, \overline{\omega}_{\pi_1}, \ldots, \overline{\omega}_{\pi_l} >_{\mathbb{F}_p} .$$

Die π_i geben die Indizes der ergänzten Basisvektoren an.

Nun sind wir in der Lage, das Verfahren zu formulieren.

Algorithmus MINIMAL_POLYNOMIAL

Eingabe: $\overline{I}, \overline{\beta} \in \overline{\mathcal{O}}$

Ausgabe: das Minimalpolynom von $\overline{\beta} + \overline{I} \in A$ über $\mathbb{F}_p$

(1) *erhalte die Darstellung in A von $\overline{\beta} + \overline{I}$*

$$\overline{\beta} = \sum_{j=1}^{l} c_j \overline{\omega}_{\pi_j}$$

(2) **for** $k \leftarrow 0$ **to** l **do**

(3) *bilde*

$$\overline{\beta}^k + \overline{I} = \sum_{j=1}^{l} c_j^{(k)} + \overline{I}$$

(4) **od**

(5) *setze* $C \leftarrow (c_j^{(i)})_{i,j} = M_\Lambda$, *die Abbildungsmatrix von* Λ

(6) $C' \leftarrow Kern\ C$

(7) $C'' \leftarrow COLUMN\_STEP\_FORM(C')$

(8) *extrahiere den ersten von Null verschiedenen Spaltenvektor von* C''*, dieser sei*

$$(a_0, a_1, \ldots, a_s, 0, \ldots, 0) \in {\mathbb{F}_p}^{l+1}$$

(9) **return** $\frac{1}{a_s} \sum_{j=0}^{s} a_j X^j \in \mathbb{F}_p[X]$

Zur Korrektheit beweisen wir den folgenden Satz.

4.8 Satz *Für* $\overline{\beta} + \overline{I} \in A$ *berechnet der Algorithmus MINIMAL_POLYNOMIAL das Minimalpolynom über* $\mathbb{F}_p$.

Beweis: Der Kern K der Abbildung Λ — erzeugt durch die Spaltenvektoren von C' — beinhaltet alle Linearkombinationen von Potenzen von $\overline{\beta} + \overline{I}$, die Null ergeben. Dies ist ein Teilvektorraum des ${\mathbb{F}_p}^{l+1}$.

Hat man nun eine Spaltenstufenform C'' der Basis von K gegeben, so muß der erste dieser Vektoren die Koeffizienten eines Polynoms von minimalem Grad beinhalten, das $\overline{\beta} + \overline{I}$ als Nullstelle besitzt, denn alle anderen Elemente des Kerns liefern Polynome von größerem Grad.

Daher hat man nach der Normierung im letzten Schritt des Algorithmus das Minimalpolynom berechnet.

∎

Berechnung einer Nullstelle für $f(X) \in \mathbb{F}_p[X]$

In Schritt (3) unseres Hauptverfahrens tritt das Problem auf, eine Nullstelle eines Polynoms $f \in \mathbb{F}_p[X]$ zu bestimmen. Man hat die zusätzliche Information, daß f über $\mathbb{F}_p$ in Linearfaktoren zerfällt. Daher ist es nicht notwendig, einen Algorithmus zur Faktorisierung beliebiger Polynome über $\mathbb{F}_p$zu benutzen.
Es genügt, ein gängiges Verfahren für unsere Zwecke zu spezialisieren. Es ist entnommen aus [Zayer].

Grundlage des Verfahrens ist die Bildung des größten gemeinsamen Teilers von f mit den Polynomen $X^{(p-1)/2} \pm 1$. Bekanntlich ist $X^{p-1} - 1$ das Produkt aller normierten Linearfaktoren von $\mathbb{F}_p[X]$. Für ungerade Primzahlen p läßt sich dieses Polynom in trivialer Weise faktorisieren:

$$X^{p-1} - 1 = (X^{(p-1)/2} - 1) \cdot (X^{(p-1)/2} + 1).$$

Weiterhin überzeugt man sich unter Verwendung elementarer Eigenschaften quadratischer Reste modulo p, daß über $\mathbb{F}_p$

$$X^{(p-1)/2} - 1 = \prod_{\substack{c \; quadratischer \\ Rest}} X - c$$

und

$$X^{(p-1)/2} + 1 = \prod_{\substack{c \; quadratischer \\ Nichtrest}} X - c$$

gilt.

Man findet deshalb durch ggT–Bildung dieser beiden Polynome mit f schon einen Linearfaktor von f, falls genau ein quadratischer Rest oder genau ein quadratischer Nichtrest Nullstelle von f(X) ist.

Innerhalb einer Schleife wird dasselbe Verfahren angewendet, wobei jedoch für X der Ausdruck $X - a$ substituiert wird, was gerade dann zum Erfolg führt, wenn für die Nullstellen $x_1, x_2, \ldots, x_l$ genau einer der Ausdrücke $x_1 + a, x_2 + a, \ldots, x_l + a$ quadratischer Rest beziehungsweise Nichtrest ist.

Es versteht sich von selbst, daß bei Auffinden echter Faktoren von f das Verfahren mit dem Faktor kleinsten Grades fortgesetzt wird.

Wir formalisieren dies als Algorithmus.

Algorithmus ROOT

Eingabe: ein normiertes Polynom

$$f(X) = X^n + a_{n-1}X^{n-1} + \ldots + a_1X + a_0 \in \mathbb{F}_p[X],$$

das über $\mathbb{F}_p$ in Linearfaktoren zerfällt

Ausgabe: ein $x_0 \in \mathbb{F}_p$ mit $f(x_0) = 0$

(1) **if** $a_0 = 0$ **then**
(2) **return** 0
(3) **fi**
(4) $g(X) \leftarrow ggT(f, X^{(p-1)/2} - 1)$
(5) **if** *degree* $g(X) = 1$ **then**
co *falls wir hierdurch einen Linearfaktor abspalten können, kennen wir eine Nullstelle* **oc**
(6) **return** $-g_0$
co $g_0 = g(0)$ **oc**

(7) **fi**
(8) $d_1 \leftarrow degree(g)$
(9) $h(X) \leftarrow ggT(f, X^{(p-1)/2} + 1)$
(10) **if** *degree* $h(X) = 1$ **then**
co *falls wir hierdurch einen Linearfaktor abspalten können, kennen wir wie vorher eine Nullstelle* **oc**
(11) **return** $-h_0$
co $h_0 = h(0)$ **oc**

(12) **fi**
(13) $d_2 \leftarrow degree(h)$
(14) $d \leftarrow d_1 + d_2$
co *wir schließen nun mehrfaches Vorkommen von Linearfaktoren aus* **oc**
(15) $F(X) = g(X) \cdot h(X)$
(16) **for** $a \leftarrow 1$ **to** $p - 1$ **do**
(17) $g(X) \leftarrow ggT(F, (X-a)^{(p-1)/2} - 1)$
(18) **if** *degree* $g(X) = 1$ **then**
(19) **return** $-g_0$

fi

$d_1 \leftarrow degree(g)$

$h(X) \leftarrow ggT(F, (X-a)^{(p-1)/2}+1)$

if $degree\ h(X) = 1$ **then**

return $-h_0$

fi

$d_2 \leftarrow degree(h)$

co *falls wir eine echte Faktorisierung* $F = gh$ *gefunden haben, benutzen wir zur weiteren Zerlegung den kleineren Faktor* **oc**

if $d_1 \neq 0$ *and* $d_2 \neq 0$ **then**

if $d_1 < d_2$ **then**

$F(X) \leftarrow g(X)$

$d \leftarrow d_1$

else

$F(X) \leftarrow h(X)$

$d \leftarrow d_2$

fi

fi

od

co *die* **for**–*Schleife wird durch das Finden einer Nullstelle abgebrochen* **oc**

Wir kommentieren die wesentlichen Schritte des Verfahrens; für nähere Einzelheiten verweisen wir auf [Zayer].

- Die Potenzen von X werden, da jedesmal der ggT mit f gebildet wird, modulo $f(X)$ gebildet; der erste Schritt bei der ggT–Bildung ist nämlich gerade eine Polynomdivision durch f. Dadurch erreicht man, daß nur Polynome auftreten, die höchstens den Grad von $f(X)$ haben.

- In den praktischen Tests hat sich gezeigt, daß im Bereich $2 \leq p < 400$ das einfache Durchprobieren aller Elemente von $\mathbb{F}_p$ schneller zum Ergebnis kommt als der Algorithmus ROOT. Im Bereich $401 \leq p < 800$ hängt der Unterschied davon ab, ob die Nullstelle zu Beginn des Durchprobierens auftaucht, d.h. beide Verfahren sind hier etwa gleich schnell. Im Bereich $p > 800$ ist der Algorithmus ROOT bis auf wenige Ausnahmen besser. Daher wird in unserer Implementierung bei Primzahlen < 800 eine Prozedur ausgeführt, die das naive Einsetzungsverfahren durchführt.

4.2.3 Berechnung der Exponenten

Wir beschreiben jetzt den Schritt (3) des Hauptverfahrens. Wir kennen schon die maximalen Ideale M_i für $1 \leq i \leq r$ in der Zerlegung

$$\overline{I}_p = \prod_{i=1}^{r} M_i$$

und wollen Exponenten e_i, $1 \leq i \leq r$ berechnen, so daß

$$p\mathcal{O} = M_1^{e_1} \cdot M_2^{e_2} \cdots M_r^{e_r}.$$

Sei nun $\overline{M} := \overline{M}_i$ für ein i mit $1 \leq i \leq r$.
Wir bilden sukzessive $\overline{M}^j$ für $j \geq 2$. Ist nun $j = e_i$, so gilt wegen $M^{e_i+1} + p\mathcal{O} = M^{e_i} + p\mathcal{O}$

$$\overline{M}^{j+1} = \overline{M}^j.$$

Daher haben wir, sobald Gleichheit auftritt, mit $e_i := j$ den Exponenten für M_i bestimmt. Dies tun wir für $1 \leq i \leq r$.

Die Gleichheit der beiden Ideale $\overline{M}^{j+1}$ und $\overline{M}^j$ aus $\mathcal{O}/p\mathcal{O}$ läßt sich sogar in konstanter Zeit feststellen. Aus Teilbarkeitsgründen gilt nämlich

$$\overline{M}^{j+1} \subseteq \overline{M}^j.$$

Daher gilt für die Dimensionen der Teilvektorräume von $\mathcal{O}/p\mathcal{O}$

$$dim_{\mathbb{F}_p} \overline{M}^{j+1} \leq dim_{\mathbb{F}_p} \overline{M}^j.$$

Solange $\overline{M}^{j+1} \subsetneq \overline{M}^j$ gültig ist, muß auch

$$dim_{\mathbb{F}_p} \overline{M}^{j+1} < dim_{\mathbb{F}_p} \overline{M}^j$$

gelten, da dann mindestens einer der Basisvektoren von $\overline{M}^j$ nicht in $\overline{M}^{j+1}$ enthalten sein kann.

Wir haben gerade bewiesen:

4.9 Lemma *Ist $\overline{M}$ ein Ideal in $\overline{\mathcal{O}}$, so gilt*

$$\overline{M}^{j+1} = \overline{M}^j \iff dim_{\mathbb{F}_p} \overline{M}^{j+1} = dim_{\mathbb{F}_p} \overline{M}^j.$$

Der Idealvergleich besteht also lediglich aus dem Vergleich der Anzahl der Basisvektoren.

Eine weitere Abbruchbedingung bei der Exponentenberechnung erhält man durch Betrachten der Normen von $p\mathcal{O}$ und M_j $(1 \leq j \leq n)$.

Nach dem Beweis von Korollar 2.59 hat man für die Verzweigungsgrade e_j, die Restklassengrade f_j und den Körpergrad n die Beziehung

$$e_1 f_1 + e_2 f_2 + \ldots + e_r f_r = n.$$

Die Werte $f_j = dim_{\mathbb{F}_p} \overline{\mathcal{O}}/\overline{M}_j$ für $1 \leq j \leq r$ sind schon bekannt, denn es gilt der folgende

4.10 Satz *Sei $I \trianglelefteq \mathcal{O}$ ein Ideal und sei n die Dimension von $\mathcal{O}$ über $\mathbb{Z}$. Dann gilt für den Restklassengrad von I über $\mathbb{F}_p$*

$$f := dim_{\mathbb{F}_p} \overline{\mathcal{O}}/\overline{I}$$

und die Dimension $d := dim_{\mathbb{F}_p} \overline{I}$ die Beziehung

$$f = n - d. \tag{4.10}$$

Beweis: Man betrachte die lineare Abbildung

$$\begin{aligned} g:\ \overline{\mathcal{O}} &\to \overline{\mathcal{O}}/\overline{I} \\ \overline{\alpha} &\mapsto \overline{\alpha} + \overline{I}. \end{aligned}$$

Dann ergibt sich die Beziehung (4.10) direkt aus

$$dim\ kern\ g + dim\ Bild\ g = n.$$

■

Aus der Kenntnis der f_j für $1 \leq j \leq r$ ergibt sich jetzt folgendes. Wir nehmen induktiv an, die Exponenten e_j von M_j sind für $1 \leq j \leq r' < r$ schon bestimmt. Dann gilt für den Exponenten $e_{r'+1}$

$$1 \leq e_{r'+1} \leq \frac{n - \sum_{j=1}^{r'} e_j f_j - \sum_{j=r'+2}^{n} f_j}{f_{r'+1}}.$$

Diese Ungleichung setzen wir zusätzlich zur obigen Abbruchbedingung $\overline{M}^{j+1} = \overline{M}^j$ ein.

Fortführung des Beispiels

Aus dem letzten Schritt sind die Ideale M_1, M_2, aber noch nicht die Exponenten e_1, e_2 in der Zerlegung

$$3\mathcal{O} = M_1^{e_1} M_2^{e_2}$$

bekannt.
Die Exponenten e_1, e_2 werden jetzt bestimmt. Es gilt hier

$$\overline{M}_1 \subsetneqq \overline{M}_1^2 \subsetneqq \overline{M}_1^3 = \overline{M}_1^4$$

und

$$\overline{M}_2 \subsetneqq \overline{M}_2^2 \subsetneqq \overline{M}_2^3 = \overline{M}_2^4,$$

wodurch man $e_1 = e_2 = 3$ als Exponenten erhält.

Darstellung des Nullideals von $\mathcal{O}/p\mathcal{O}$ durch Primideale

Wir haben in den vorangegangenen Schritten alle Ideale durch Rechnen modulo $p\mathcal{O}$ bestimmt; deshalb erhalten wir nach dem letzten Schritt eine Darstellung des Nullideals von $\mathcal{O}/p\mathcal{O}$ durch alle maximalen Ideale von $\mathcal{O}/p\mathcal{O}$:

$$(\overline{0}) = \prod_{i=1}^{r} \overline{M}_i^{e_i}.$$

Um die entsprechenden Ideale in $\mathcal{O}$ zu erhalten, ist für jedes $\overline{M}_i$ der kanonische Homomorphismus Φ umzukehren, d.h. es muß

$$M_i = \Phi^{-1}(\overline{M}_i)$$

für $1 \leq i \leq r$ bestimmt werden.
Dies ist das Thema des nächsten Abschnitts.

4.2.4 Abbilden der Ideale von $\mathcal{O}/p\mathcal{O}$ nach $\mathcal{O}$

Der letzte Teil des Hauptverfahrens löst die Aufgabe, zu einem gegebenen Ideal $\overline{M} \trianglelefteq \mathcal{O}/p\mathcal{O}$ das Ideal $M \trianglelefteq \mathcal{O}$ zu finden, so daß

$$\overline{M} = \Phi(M),$$

wobei

$$\Phi : \mathcal{O} \to \mathcal{O}/p\mathcal{O}$$

der für das gesamte Verfahren fundamentale kanonische Homomorphismus ist, der insbesondere die uns interessierenden maximalen Ideale in der Zerlegung von $p\mathcal{O}$ injektiv nach $\mathcal{O}/p\mathcal{O}$ abbildet.

Sei also die $\mathbb{F}_p$–Basis–Darstellung von $\overline{M}$ gegeben durch

$$\overline{M} =< \overline{\beta}_1, \overline{\beta}_2, \ldots, \overline{\beta}_t >_{\mathbb{F}_p} .$$

Wegen

$$\overline{M} = {}^{M}\!/_{p\mathcal{O}} = \{m + p\mathcal{O} \mid m \in M\}$$

gilt

$$M =< \beta_1, \beta_2, \ldots, \beta_t, p\omega_1, \ldots, p\omega_n >_{\mathbb{Z}} .$$

Um eine Basis für M zu bestimmen, muß also eine $\mathbb{Z}$–Matrix der Form

$$\begin{pmatrix} * & \cdots & * & p & 0 & \cdots & 0 \\ \vdots & & \vdots & 0 & p & & \vdots \\ \vdots & & \vdots & \vdots & & \ddots & 0 \\ * & \cdots & * & 0 & \cdots & 0 & p \end{pmatrix}$$

auf Hermite-Normalform gebracht werden. Da jede Zeile die Primzahl p enthält, ist das Addieren beliebiger Vielfache von p zu einem beliebigen Matrizenelement eine unimodulare Spaltenoperation. Aus diesem Grunde kann jede Spaltenoperation der Hermite-Normalform modulo p ausgeführt werden. Auf dieses Verfahren wurde bereits in Abschnitt 3.4 eingegangen.

Da dieses Verfahren im wesentlichen Ausführung des Gauss–Algorithmus modulo p bedeutet, benötigt es

$$O(n^3)$$

Operationen in $\mathbb{F}_p$.

Fortführung des Beispiels

Nachdem die Zerlegung

$$(0) = \overline{M}_1^3 \overline{M}_2^3$$

in $\mathcal{O}/3\mathcal{O}$ gefunden ist, werden die zugehörigen Ideale in $\mathcal{O}$ durch Hermite–Normalform–Berechnung modulo 3 bestimmt. Als Ergebnis der Prozedur erhält man die $\mathbb{Z}$–Basen der Primideale, die im folgenden angegeben werden.

```
P1 prime ideal no. 1 power 3:
( 1 0 0 0 0 0 )
( 0 1 0 0 0 0 )
( 0 0 1 0 0 0 )
( 0 0 0 1 0 0 )
( 0 0 0 0 1 0 )
( 2 2 2 2 2 3 )
- - - - - - - - - - - - -
P2 prime ideal no. 2 power 3:
( 1 0 0 0 0 0 )
( 0 1 0 0 0 0 )
( 0 0 1 0 0 0 )
( 0 0 0 1 0 0 )
( 0 0 0 0 1 0 )
( 1 2 1 2 1 3 )
- - - - - - - - - - - - -
3O type 2 (3,3)  - time 3.89s
```

Man sieht leicht, daß

$$1 + \rho = \omega_1 + \omega_2 \in P_2$$

und

$$2 + \rho = 2\omega_1 + \omega_2 \in P_1.$$

Mit den Bezeichnungen aus Abschnitt 4.2 hat man deshalb $M_1 = P_2$ und $M_2 = P_1$, das heißt die Primidealzerlegung von $3\mathcal{O}$ ist als $M_1^3 M_2^3$ bestimmt.

4.3 Ein alternativer Algorithmus

Hier wird nun der Algorithmus beschrieben, der sich aus den Ideen der Veröffentlichung [BuLen] ergibt.
Es hat sich in den Laufzeittests (Abschnitt 6.2.4) gezeigt, daß der im letzten Abschnitt vorgestellte Algorithmus 'FACTOR_P' deutlich schneller zum Ergebnis kommt.

(1) *Berechnung von $\overline{I_p}$ wie in Algorithmus 'FACTOR_P'*

(2) **Zerlege $p\mathcal{O}$ nach Primidealpotenzen**

Ziel dieses Schrittes ist es, eine Zerlegung

$$p\mathcal{O} = \prod_{j=1}^{t} C_j^j \tag{4.11}$$

zu finden, wobei die C_j quadratfrei sind.
Dazu bildet man sukzessive

$$\begin{array}{rcll} \overline{A}_j & := & \overline{I_p}^j & 0 \leq j \leq e \\ \overline{B}_j & := & \overline{A}_j / \overline{A}_{j-1} & 1 \leq j \leq e \\ \overline{C}_j & := & \overline{B}_j / \overline{B}_{j+1} & 1 \leq j \leq e. \end{array}$$

Hierbei bedeutet e der minimale Index, so daß $\overline{A}_e = (\overline{0})$. Dann gilt nämlich (Lemma 4.11)

$$\overline{C}_j = \prod_{\overline{M}^j \| p\mathcal{O}} M$$

Also ist C_j gerade das Produkt der maximalen Ideale, die $p\mathcal{O}$ mit der j-ten Potenz exakt teilen. Damit hat man die Zerlegung (4.11) gefunden.

(3) *Zerlege jedes C_j nach der Methode der Zerlegung von I_p im Algorithmus 'FACTOR_P'.*

(4) *Gewinne aus der Zerlegung in $\mathcal{O}/p\mathcal{O}$ die Zerlegung in $\mathcal{O}$ wie im Algorithmus 'FACTOR_P'.*

Es ist noch die Behauptung zu beweisen, daß in Schritt 2 die angegebene Zerlegung erzeugt wird.

4.11 Lemma *Nach Ausführung von Schritt 2 hat man die Zerlegung*

$$p\mathcal{O} = \prod_j C_j^j,$$

wobei

$$\overline{C}_j = \prod_{\overline{M}^j || p\mathcal{O}} M.$$

Beweis: Es gilt $\overline{I_p} = \overline{M}_1 \cdot \overline{M}_2 \cdots \overline{M}_r$.

Seien I_1, I_2 zwei Ideale, die $p\mathcal{O}$ teilen. Dann gilt in $\mathcal{O}/p\mathcal{O}$

$$\overline{I}_1 \overline{I}_2 = \Phi(I_1 I_2 + p\mathcal{O}).$$

Also wird durch die ggT-Bildung der Primidealexponent von M_i in der Zerlegung von $\overline{I}_1\overline{I}_2$ durch e_i beschränkt.

Hieraus folgt nun, wenn man die Primidealpotenzen der A_j, B_j, C_j betrachtet:

$$\begin{aligned}
\overline{A}_j &= \overline{I_p}^j \\
&= \prod_{k=1}^{r} M_k^{min(j,e_k)} \\
\\
\overline{B}_j &= \overline{A}_j / \overline{A}_{j-1} \\
&= \frac{\prod_{k=1}^{r} M_k^{min(j,e_k)}}{\prod_{k=1}^{r} M_k^{min(j-1,e_k)}} \\
&= \prod_{M^j | p\mathcal{O}} M \\
\\
\overline{C}_j &= \overline{B}_j / \overline{B}_{j+1} \\
&= \frac{\prod_{M^j | p\mathcal{O}} M}{\prod_{M^{j+1} | p\mathcal{O}}} M \\
&= \overline{C}_j = \prod_{\overline{M}^j || p\mathcal{O}} M.
\end{aligned}$$

Damit ist das Lemma bewiesen. ∎

Kapitel 5

Objektorientierte Implementierung in C++

In diesem Kapitel wird die Begründung für die Wahl der objektorientierten Sprache C++ gegeben, die Vorteile gegenüber C herausgestellt und gezeigt, daß diese Sprache für die Behandlung von Problemen aus der algorithmischen algebraischen Zahlentheorie als besonders geeignet anzusehen ist.

Außerdem werden die benutzten Datenstrukturen in Form von Klassenhierarchien dargestellt und die Realisierung in der Programmiersprache exemplarisch aufgezeigt.

5.1 Programmierkonzepte von C++

Der beschriebene Algorithmus wurde auf mehreren binärkompatiblen Workstations des Typs Sun SLC und Sun ELC implementiert. Die Laufzeittests wurden jeweils mit ELC's (21 Mips) durchgeführt. Als Programmiersprache wurde die objektorientierte Sprache C++ gewählt, da diese die Vorteile von objektorientiertem Algorithmendesign und der maschinennahen Programmiersprache C, hier vor allem der effizienten Umsetzung in Maschinencode, vereint.
Dabei wurde möglichst von der Benutzung wesentlicher Elemente objektorientierter Programmierung, deren Sinn und Zweck ausführlich in [Mer] beschrieben wurde, Gebrauch gemacht. An dieser Stelle wird nun lediglich auf diejenigen Aspekte eingegangen, die für die Behandlung von Problemen aus der algorithmischen algebraischen Zahlentheorie relevant sind.

5.1.1 Definition abstrakter Datentypen (Klassen)

Durch die Möglichkeit, einen neuen Datentyp mit allen zu ihm gehörenden Operatoren zu definieren, braucht sich der Benutzer dieses Datentyps weder um die Aufrufstruktur der Operatoren noch um die Speicherverwaltung dynamischer Objekte zu kümmern. Außerdem wird die Lesbarkeit der Algorithmen deutlich erhöht. Weiterhin können einmal definierte Klassen wie Standarddatentypen behandelt werden, z.B.

Deklaration: `Matrix A`
Rückgabe: `return A`.

Diese Fähigkeiten von C++ bedeuten einen enormen Vorteil gegenüber der Verwendung einer Struktur (`struct`) in der Sprache C.

5.1.2 Verkapselung

Der *direkte* Zugriff auf die Komponenten einer Klasse – wie beispielsweise die Einträge einer Matrix – wird für den Benutzer durch die Schlüsselworte `private` und `protected` gesperrt. Stattdessen müssen entsprechende sogenannte Member–Funktionen aufgerufen werden, die gleichzeitig die Aufgabe haben, die Zulässigkeit der Zugriffe zu überprüfen. Eine Ausnahme von dieser Regel bilden die sog. `friend`-Funktionen, denen es explizit schon durch einen Vermerk in der Klassendefinition erlaubt ist, auf Member–Variablen zuzugreifen. Die Variablen, die die Informationen über ein Klassenelement beinhalten, heißen Member–Variablen.

5.1 Beispiel Durch `Z_matrix A(3,5)` wird eine ganzzahlige Matrix der Dimension 3×5 deklariert. Falls nun irrtümlicherweise auf das Element a_{36} zugegriffen würde, käme es in einem C-Programm beim Ausdruck `a[3][6]` zu keinem Fehler, aber es würden nicht definierte Speicherinhalte benutzt. In C++ hingegen ist der Benutzer gezwungen, die dafür durch die Klasse bereitgestellte Member–Funktion zu benutzen, die beim Aufruf `A.element(3,6)` in eine Fehlerbehandlung verzweigt.

Desweiteren wird durch dieses Konzept die *Portabilität* der Software erhöht, da bei einer Veränderung der Repräsentationen der Daten einer Klasse nur die Klassendefinition und nicht Teile des die Klasse benutzenden Programms ausgetauscht werden müssen.

5.1.3 Vererbung

Durch Vererbung kann man erstens die Definition bereits definierter Klassen bei der Definition neuer Klassen in bequemer Weise benutzen. Die neuen Klassen erben sowohl die Definitionen als auch die Operationen der schon definierten Klassen. Zum zweiten wird die hierarchische Denkweise bei der Konstruktion immer komplizierterer Objekte in natürlicher Weise unterstützt.

5.2 Beispiel Ein Element $\overline{\alpha} \in \mathcal{O}/p\mathcal{O}, \overline{\alpha} = \sum_i x_i \overline{\omega}_i$ kann als $\mathbb{F}_p$–Vektor repräsentiert werden

$$\overline{\alpha} \leftrightarrow (x_1, \dots, x_n) \in {\mathbb{F}_p}^n,$$

und es kann für die Addition von $\overline{\alpha}, \overline{\beta} \in \mathcal{O}/p\mathcal{O}$ die schon implementierte Vektoraddition benutzt werden.
Daher erbt die Klasse `order_mod_p`, die für Elemente $\in \mathcal{O}/p\mathcal{O}$ steht, die Speicherverwaltung und sämtliche Vektorraum–Operationen von der Klasse `FF_vector`, die Vektoren $\in {\mathbb{F}_p}^n$ realisiert.

5.1.4 Überladen von Operatoren

In der Sprache C++ können alle Standardoperatoren (+,–,*,/,%,...) überladen, d.h. als Klassenoperatoren definiert werden. Dadurch ist es beispielsweise möglich, Vektoren einfach durch '+' zu addieren.

5.3 Beispiel Vektoraddition

```
void main()
       {
       FF_vector u,v,w;  // creating three vectors over Fp
       ...
       cin >> v;  // read v from standard input
       cin >> w;  // read w from standard input
       ...
       u=v+w;
       ...
       cout << u; // print u on standard output
       }
```

Es können auch verschiedene Klassen mit den Standardoperatoren verknüpft werden, z.B. Multiplikation einer Matrix mit einem Vektor.

Diese dem Aufbau algebraischer Strukturen sehr ähnlichen Datenstrukturen erleichtern die Implementierung der Algorithmen, da mathematisch formulierte Verfahren auf einfache Weise in die Programmiersprache übertragen werden können.

5.4 Beispiel Das Berechnen des Bildes eines Elements $a_0 \in \mathcal{O}/p\mathcal{O}$ unter der Abbildung

$$\begin{aligned} \vartheta: \; A &\to \; A \\ \alpha &\mapsto \; \alpha^p - \alpha \end{aligned}$$

Implementierung

```
//-----------------------------------------------------

order_mod_p frobenius(const order_mod_p& a0)
        {
        order_mod_p a;              // an element in O/pO

        a=power(a0,p)-a0;           // compute a0^p-a0
        return a;
        }

//-----------------------------------------------------
```

Hieran erkennt man erstens die unkomplizierte Behandlung von Elementen aus $\mathcal{O}/p\mathcal{O}$ durch Potenzbildung und Subtraktion per '−'; zweitens wird das Ergebnis einfach durch die Anweisung '`return`' an die übergeordnete Prozedur zurückgeliefert. Ohne Verwendung von C++ hätte in dieser Funktion Speicherplatz für a bereitgestellt werden müssen, die Subtraktion wäre durch einen unhandlichen Funktionsaufruf realisiert worden und die Komponenten des Vektors, aus denen das Ergebnis besteht, hätten durch eine Schleife an die übergeordnete Prozedur zurückgegeben werden müssen.

Die Ersparnis dieser Verwaltungsaufgaben, die in C++ schon bei der Definition des Datentyps '`order_mod_p`' zusätzlich angegeben werden, führen selbst bei komplizierten Verfahren zu angenehmer Übersichtlichkeit.

Damit ein solch problemloser Umgang mit komplexen Datenstrukturen möglich wird, sind bei der Implementierung einer Klasse im wesentlichen drei Punkte zu beachten.

- Es müssen Prozeduren zur Deklaration einer Instanz der Klasse bereitgestellt werden. Diese haben auch Sorge dafür zu tragen, daß genügend Speicherplatz für die Datenstruktur angefordert wird. Dies sind die sogenannten *Konstruktoren*. Hier muß insbesondere die Möglichkeit geschaffen werden, ein Element der Klasse zu kopieren, damit

  - als Rückgabewert einer Funktion auch ein Klassenelement möglich ist (siehe Bsp. 5.4) und
  - call-by-value Funktionsaufrufe möglich sind.

  Zur Erledigung dieser Aufgabe ist die Implementierung des sogenannten *Copy–Konstruktors* notwendig, der bei allen im Rahmen dieser Arbeit implementierten Datenstrukturen verwendet wurde.

- Es muß eine Prozedur zur Freigabe von Speicherplatz bereitgestellt werden, damit nach Terminierung eines Unterprogramms der Speicherplatz der dort deklarierten lokalen Variablen automatisch – wie man es von den Standarddatentypen gewohnt ist – wieder für andere Daten zur Verfügung steht. Eine solche Prozedur wird *Destruktor* genannt.

- Es sollte der Zuweisungsoperator '=' überladen werden, der sowohl die Funktion des Destruktors zum Freigeben des durch den alten Wert belegten Speicherplatzes als auch die Funktion des Copy–Konstruktors zum Speichern des zuzuweisenden Wertes wahrzunehmen hat.

Sind diese Bestandteile der neuen Klasse einmal realisiert, kann diese wie ein vordefinierter Typ (z.B. `int`) benutzt werden. Da durch dieses Konzept der Vorrat an verfügbaren Standarddatentypen dynamisch ausgebaut werden kann, ist C++ gerade für die Realisierung abstrakter mathematischer Strukturen mit Operationen, die sich aus anderen Strukturen mit selbstdefinierten Operationen aufbauen, ein geeignetes Hilfsmittel.
Ein Beispiel hierfür ist der Matrizenring über $\mathbb{F}_p$, der zur Darstellung der benutzten Homomorphismen verwendet wird.

5.2 Die verwendete Klassenstruktur

Es wurden die folgenden Datentypen samt zugehöriger Operationen realisiert.

FF	–	eine Arithmetik in $\mathbb{Z}/n\mathbb{Z}$ bzw. $\mathbb{F}_p$
FF_vector	–	Vektoren über $\mathbb{F}_p$
FF_matrix	–	Matrizen über $\mathbb{F}_p$
FF_poly	–	Polynome über $\mathbb{F}_p$
Q	–	eine Arithmetik im rationalen Zahlkörper $\mathbb{Q}$
Q_vector	–	Vektoren über $\mathbb{Q}$
Q_matrix	–	Matrizen über $\mathbb{Q}$
Q_poly	–	Polynome über $\mathbb{Q}$
Z_vector	–	Vektoren über $\mathbb{Z}$
Z_matrix	–	Matrizen über $\mathbb{Z}$
Z_poly	–	Polynome über $\mathbb{Z}$
order_mod_p	–	Elemente in $\mathcal{O}/p\mathcal{O}$
ideal_mod_p	–	Ideale in $\mathcal{O}/p\mathcal{O}$

5.3 Die Klasse FF

Durch die Klasse FF (= finite field) wurde eine komplette Arithmetik im Ring/Körper $\mathbb{Z}/n\mathbb{Z}$ realisiert. Hierbei wird n in der globalen Variablen MODUL festgelegt.

Die Klasse FF ist folgendermaßen deklariert:

```
// -----------------------------------------------------------------
// The Header-File of the class of the ring/field Z/nZ
//
// the residue class, in which we compute, has to be stored in the
// global variable of type 'Int' named MODUL
//
// Operators:
// FF+FF,FF+int,int+FF,FF-FF,FF-int,int-FF,FF*FF,FF/FF
//
// Functions:
// inv(FF& a)        the inverse of a
// pow(FF& a,long n) the n-th power of a
// -----------------------------------------------------------------

#ifndef ZMZ_H
#define ZMZ_H

#include <stream.h>
#endif
      // -----------------------------------------

typedef unsigned long ULONG;

#include <stdlib.h>
#include "utils.h"
      // -----------------------------------------

extern Int MODUL;

      // -----------------------------------------

class FF   // finite field
      {
      Int a;

      public:
      // -----------------------------------------
      // Constructors
```

```
//
// FF a;       creates an element and
//                 initializes it with value 0
//
// FF a(int);  ... initializes it with the int value


FF();
FF(int k);
FF(long k);
FF(Int k);
FF(const FF& c);  // Copy constructor

// ------------------------------------------
// Operators
//
friend istream& operator>>(istream& in, FF& a);
friend ostream& operator<<(ostream& out, const FF& a);

friend Int entry(FF&);

friend FF operator+(const FF&, const FF&);
friend FF operator-(const FF&, const FF&);
friend FF operator*(const FF&, const FF&);
friend FF operator/(const FF&, const FF&);

friend int operator==(const FF&, const FF&);
friend int operator==(const FF&, int);
friend int operator==(int , const FF&);
friend int operator!=(const FF&, const FF&);
friend int operator!=(const FF&, int);
friend int operator!=(int, const FF&);

FF& operator=(int k);
FF& operator=(Int k);
FF& operator+=(const FF&);
FF& operator-=(const FF&);
FF& operator=(const FF& b);
FF& operator=(const Q& b);

// ---------------------------------
// Functions

friend FF power(const FF&, Int);
friend FF inv(const FF&);
```

```
    friend Int convert_to_Int(const FF &a)
      { return a.a; };
    };

#endif
```

Die Klasse FF besitzt nur eine Int-Komponente, die den Wert der Variablen enthält. Sie benötigt somit auch keinen Destruktor, denn der Int–Destruktor gibt schon den gesamten belegten Platz frei. Auch die Konstruktoren wären nicht unbedingt notwendig; jedoch wurde die Möglichkeit genutzt, die Klassenelemente mit dem Wert 0 zu initialisieren.

Der Typ Int wird in zweifacher Weise genutzt. Ohne besondere Zusätze beim Compileraufruf steht 'Int' für einen vorzeichenlosen 32-Bit-Wert. Im anderen Falle hat man die Möglichkeit, eine lange ganzzahlige Arithmetik einzubinden, die lange ganze Zahlen mit dem Klassennamen Int realisiert — beispielsweise die an der Universität Heidelberg entwickelte Bibliothek 'libI'.

Da unser Algorithmus ausnahmslos alle arithmetischen Operationen modulo der eingegebenen, zu faktorisierenden Primzahl p durchführen kann und somit Primzahlen $< 2^{32} - 1$ auch ohne Verwendung langer Arithmetik in Primideale zerlegt werden können, wurden die meisten Tests des Algorithmus mit Int='unsigned long' durchgeführt. Im übrigen befinden sich die zu zerlegenden Primzahlen im Falle der Klassengruppenberechnung im Bereich $< 12 \log^2 \Delta$ [Sche]. Daher können prinzipiell für $p < 2^{32} - 1$ die Klassenzahlen von Zahlkörpern mit 22000-stelligen Diskriminanten ohne Verwendung langer Arithmetik berechnet werden.

Deshalb wurde auf eine effiziente Behandlung von Restklassenringen $\mathbb{Z}/n\mathbb{Z}$ mit $n < 2^{32}$ Wert gelegt. Hierbei tritt das Problem möglicher 64-Bit großer Zwischenresultate auf. Obwohl die arithmetischen Verfahren sehr einfach sind, wurde ihre Beschreibung in diese Arbeit aufgenommen, um die Behandlung gerade dieses Problems zu demonstrieren.

5.3.1 Die Addition in FF

Algorithmus OPERATOR+

Eingabe: zwei 32-Bit-Zahlen a,b

Ausgabe: das 32-Bit-Ergebnis von $a + b$ modulo $MODUL$

5.5 Bemerkung Die Variablen a,b,c stehen alle für 32-Bit große Speicherplätze.

(1) $c \leftarrow a + b$
(2) **if** $c < b$ **then**
(3) $\quad c \leftarrow c + (\tilde{}MODUL) + 1$
(4) $\quad$ **fi**
(5) **if** $c \geq MODUL$ **then**
(6) $\qquad c \leftarrow c - MODUL$
(7) $\qquad$ **fi**
(8) **return** c

Hier bedeutet $\tilde{}x$ das Zweierkomplement von x. Falls das Ergebnis von $a+b$ den Wert 2^{32} überschreitet, haben wir nach der Ausführung von (1) in c den Wert $a+b-2^{32}$. Wir benötigen jedoch

$$c' := a + b - MODUL.$$

Wegen $c' = c + 2^{32} - MODUL$ und $2^{32} - MODUL = \tilde{}MODUL + 1$ wird in diesem Falle dieser Wert zu c addiert. Offensichtlich ist bei der Addition genau dann die Grenze von 2^{32} überschritten worden, wenn als Ergebnis von $a + b$ ein kleinerer Wert als b oder a berechnet wurde. Schritt (6) dient schließlich dazu, den kleinsten positiven Rest zurückzuliefern, damit die Elementdarstellung in $\mathbb{Z}/n\mathbb{Z}$ eindeutig ist.

Ähnliche Überlegungen führen zum Algorithmus für die Subtraktion.

5.3.2 Die Subtraktion in FF

Algorithmus OPERATOR–

Eingabe: zwei 32-Bit-Zahlen a,b

Ausgabe: das 32-Bit-Ergebnis von $a - b$ modulo $MODUL$

(1) $c \leftarrow a - b$
(2) **if** $c > a$ **then**
(3) $c \leftarrow c + MODUL$
(4) **fi**
(5) **return** c

Falls $b > a$ ist, hat man nach Ausführung von Zeile (1)

$$c = a - b + 2^{32};$$

daher berechnen wir in diesem Falle

$$c' := c - 2^{32} + MODUL = a - b + MODUL.$$

5.3.3 Die Multiplikation in FF

Bei der Multiplikation wurden zwei Ansätze verfolgt.

- Berechnung des 64–Bit Ergebnisses $c = ab$; danach eine Division von 64-Bit geteilt durch 32–Bit $c/MODUL$
- Multiplikation als Folge von Additionen mit Reduktion mod MODUL in jedem Schritt, falls das Ergebnis einer Addition den Wert MODUL überschreitet

Da es sich herausstellte, daß beide Algorithmen gleich schnell sind und der erste Ansatz nur auf eine sehr technische Weise beschrieben werden kann, wurde schließlich der zweite Ansatz vorgezogen.
Bei der Berechnung von $ab \ mod \ MODUL$ wird für $0 \leq i \leq 31$

$$a_i := 2^i \cdot a \ mod \ MODUL$$

berechnet und

$$s := a_{i_0} + a_{i_1} + \ldots + a_{i_l} \ mod \ MODUL$$

gebildet, wobei $i_0, i_1, \ldots, i_l$ die Nummern der gesetzten Bits von b sind. Die a_i werden folgendermaßen gebildet:

$$a_{i+1} = \begin{cases} 2a_i & 2a_i < MODUL \\ 2a_i - MODUL & sonst \end{cases} .$$

Falls $2a_i \geq 2^{32}$, kann dies vor der Multiplikation abgefangen werden, da in diesem Falle das 31. Bit von a_i gesetzt ist, so daß analog zur Addition das Ergebnis korrigiert werden kann. Daraus ergibt sich folgendes Verfahren:

Algorithmus OPERATOR$*$

Eingabe: zwei 32-Bit-Zahlen a, b

Ausgabe: das 32-Bit-Ergebnis von ab modulo $MODUL$

```
m_232 ← ~MODUL + 1
if a = 0 ∨ b = 0 then
                co Trivialfälle behandeln oc
                return 0
                fi
s ← 0
while b ≠ 0 do
            if b&1 then
                co b ungerade? oc
                s1 ← s + a
                if s1 < s then
                        co Überlauf? oc
                        s ← s1 + m_232
                        else
                        s ← s1
                        fi
                fi
            shift_right(b)
            if b = 0 then
                break
                fi
            co Multiplikation mit 2, Test auf Überlauf oc
            if msb(a) then
                shift_left(a)
                a ← a + m_232
                else
                shift_left(a)
                if a ≥ MODUL then
                                a ← a − MODUL
                                fi
                fi
            od
return s mod MODUL
```

Wir erläutern die verwendeten abkürzenden Schreibweisen

- '&' bedeutet bitweise logische AND–Verknüpfung, daher stellt der Ausdruck 'b&1' fest, ob die binär dargestellte Zahl b gerade oder ungerade ist.
- shift–right bzw. shift–left schieben die Ziffern des Argumentes um eine Stelle nach rechts bzw. links, was gleichbedeutend mit Halbierung bzw. Verdopplung des Argumentes ist.
- 'msb' (=most significant bit) ist das oberste Bit in der Binärdarstellung des Argumentes. Es wird dazu benutzt, um festzustellen, ob bei der Multiplikation mit 2 ein Überlauf auftritt.

5.3.4 Die Division in FF

Die Division wird durch die Berechnung des inversen Elementes auf die Multiplikation zurückgeführt. Bekanntlich ist $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ genau dann invertierbar, wenn $ggT(a, n) = 1$.

Also gibt es $x, y \in \mathbb{Z}$ mit $ax + ny = 1$, woraus sich in $\mathbb{Z}/n\mathbb{Z}$ die Kongruenz

$$\overline{ax} \equiv \overline{1} \ mod\ n$$

ergibt. Daraus kann man ablesen, daß $\overline{x}$ das zu $\overline{a}$ multiplikativ Inverse in $\mathbb{Z}/n\mathbb{Z}$ ist. Hierbei kann x durch den erweiterten Euklidischen Algorithmus berechnet werden, wobei es genügt, x modulo n zu bestimmen.
Diese Vorbemerkungen führen zu einem speziellen erweiterten Euklidischen Algorithmus, dessen Grundgedanke [Knu1, Section 1.2.1] entnommen wurde.

Algorithmus EGCD

Eingabe: $a, n \in \mathbb{N}$

Ausgabe: $ggT(a, n) \in \mathbb{N}, u \in \mathbb{Z}/n\mathbb{Z}$, s.d. $\overline{au} \equiv 1 \ mod\ n$

(1) $n_0 \leftarrow n$
co *die Operationen werden modulo n ausgeführt; da n jedoch verändert wird, speichern wir diesen Wert in n_0* **oc**

```
u ← 0
u' ← 1
if a ≠ 0 ∧ b ≠ 0 then
                co es liegt kein Trivialfall vor oc
                do
                    co es folgt die bekannte Schleife des erweiter-
                    ten Euklidischen Algorithmus, wobei die jeweiligen
                    Operationen modulo n_0 stattfinden oc
                    r ← a mod n
                    q ← a/n
                    a ← n
                    n ← r
                    h ← u mod n_0
                    u ← u' − qu mod n_0
                    u' ← h
                while r ≠ 0
                else
                co Trivialfälle oc
                if a = 0 then
                      u ← 0
                      return n,u
                      else
                      u ← 1
                      return a,u
                      fi
                fi
u ← u'
return a,u
```

Zur Korrektheit dieses Standardverfahrens siehe [Knu1].

5.3.5 Potenzieren in $\mathbb{Z}/n\mathbb{Z}$

Für die schnelle Exponentiation in einer beliebigen Halbgruppe H gibt es ein Standardverfahren, die Methode des wiederholten Quadrierens. So läßt sich für $a \in H$ und $m \in \mathbb{N}_0$ der Wert $a^m \in H$ in $O(\log |m|)$ Halbgruppenoperationen bestimmen.

Für $a \in \mathbb{Z}/n\mathbb{Z}$ und $m \in \mathbb{Z}$ bedeutet das Zeit $O(\log^2 n \log |m|)$. Wegen

$$a^{-m} = \frac{1}{a^m}$$

genügt es, $m \geq 0$ zu betrachten.

5.6 Beispiel Zu berechnen sei a^{70}.

$$a^{70} = a^{64} \cdot a^4 \cdot a^2$$

Dazu berechnet man sukzessive durch Quadrieren $a^2, a^4, a^8, a^{16}, a^{32}, a^{64}$ und benötigt statt 70 nur 8 Multiplikationen.

Formal läßt sich dieses Verfahren wie folgt beschreiben.

Algorithmus POWER

Eingabe: $a \in \mathbb{Z}/n\mathbb{Z}$ und $m \in \mathbb{Z}_{\geq 0}$

Ausgabe: $a^m \in \mathbb{Z}/n\mathbb{Z}$

(1) $q \leftarrow a$
(2) **if** m *ungerade* **then**
(3) $\quad p \leftarrow a$
(4) $\quad$ **else**
(5) $\quad p \leftarrow 1$
(6) $\quad$ **fi**
(7) $m \leftarrow m/2$
(8) **while** $m > 0$ **do**
(9) $\quad q \leftarrow q^2$
(10) $\quad$ **if** m *ungerade* **then**
(11) $\quad\quad p \leftarrow pq$

(12) **fi**
(13) $m \leftarrow m/2$
(14) **od**
(15) **return** p

Zur Korrektheit:

wenn die Binärdarstellung von m

$$m = m_0 2^0 + m_1 2^1 + m_2 2^2 + \ldots + m_k 2^k, \qquad m_i \in \{0, 1\}$$

ist, dann gilt

$$a^m = a^{\sum m_i 2^i} = \prod_{i=0}^{k} (a^{2^i})^{m_i} = \prod_{\substack{i=0 \\ m_i=1}}^{k} (a^{2^i}).$$

Im i–ten Schleifendurchlauf hat q den Wert a^{2^i}, und die Ziffer m_i gibt gerade an, ob m zu diesem Zeitpunkt ungerade ist. Weitere Hinweise zur schnellen Exponentiation — insbesondere zur Minimierung der notwendigen Multiplikationen — findet man in [Knu2, Section 4.6.3].

5.4 Die Klasse FF_vector

Diese Klasse realisiert die Arithmetik von Vektoren im ${\mathbb{F}_p}^n$, wobei n als Member–Variable (siehe Bsp. 5.1) für jeden Vektor frei wählbar ist. Vektoren gleicher Dimension können addiert, subtrahiert und skalar multipliziert werden, die zugehörigen Algorithmen sind trivial. Darüber hinaus stehen Vergleiche und Eingabe– und Ausgabefunktionen zur Verfügung.

Die Klasse FF_vector ist folgendermaßen deklariert:

```
// ----------------------------------------------------------------
// Headerfile for computations with  vectors over finite fields

#ifndef FFVECTOR_H
#define FFVECTOR_H

#include "zmz.h"                  // to use class FF
```

```
typedef unsigned long Int;

class FF_vector
      {
      protected:      // not private because of inheritance
                      // of class order_mod_p
      FF *b;          // contains the values
      int dim;        // dimension of the vector

      public:
      // Constructors:
      //
      // () creates a scalar
      // (int d) creates a vector of dimension d

      FF_vector();
      FF_vector(int d);

      // Destructor:
      ~FF_vector();

      // Copy constructor
      FF_vector(const FF_vector&);

      // Assignment operators
      FF_vector& operator=(const FF_vector&);
      FF_vector& operator=(int);


      friend FF element(const FF_vector& v,int nr)
                  { return v.b[nr]; };
      friend int get_dimension(const FF_vector& v)
                  { return v.dim; };
      friend void sto_element(FF_vector& v,int nr,FF e)
                  { v.b[nr]=e; } ;

      // addition, subtraction and dot product of vectors:
      FF_vector operator+(const FF_vector&);
      FF_vector operator-(const FF_vector&);
      friend FF operator*(const FF_vector&, const FF_vector&);

      // Multiplication with a scalar
      friend FF_vector operator*(FF, FF_vector&);

      // to compare two vectors:
      friend int operator==(const FF_vector&, const FF_vector&);
```

```
      friend int operator==(const FF_vector&, int);
      friend int operator!=(const FF_vector&, const FF_vector&);
      friend int operator!=(const FF_vector&, int);

      // input and output functions:
      friend istream& operator>>(istream&, FF_vector&);
      friend ostream& operator<<(ostream&, const FF_vector&);

      // creates a column of the identity matrix:
      friend FF_vector standard_basis_vector_FF(int,int);

      };
#endif
// ---------------------------------------------------------------
```

Es folgen einige Bemerkungen zur Deklaration dieser Klasse:

- Der `#include` - Befehl erlaubt die Benutzung der Klasse FF.
- Konstruktoren, Destruktoren und Zuweisungsoperatoren wurden nach den Prinzipien von Abschnitt 5.1.4 implementiert.
- Neben Ein-/ Ausgabeoperationen wurden die Operatoren +,–,∗ überladen, damit diese zur gewohnten Verknüpfung von Vektoren zur Verfügung stehen.
- Die Member–Variablen wurden als `protected` gekennzeichnet, damit die erbende Klasse von Elementen in $\mathcal{O}/p\mathcal{O}$ auf diese zugreifen kann. Falls man dieses nicht täte, wären sie als `private` markiert und somit für alle anderen – sogar erbenden – Klassen unantastbar.

5.5 Die Klasse FF_matrix

Diese Klasse realisiert die Arithmetik von Matrizen im ${\mathbb{F}_p}^{m\times n}$. Neben den Grundoperationen in der $\mathbb{F}_p$–Algebra ${\mathbb{F}_p}^{m\times n}$ stehen folgende Funktionen zur Verfügung:

column(A,j)	liefert die j–te Spalte der Matrix A als FF_vector
row(A,j)	liefert die j–te Zeile der Matrix A als FF_vector
column_step_form(A, V)	bringt A auf Spaltenstufenform A' und liefert V, s.d. A'=AV (siehe Abschnitt 3.3)
kern(A)	liefert eine Basis des Kerns von A als Matrix zurück
image(A)	liefert eine Basis des Bildes von A als Matrix zurück
kern_and_image(A)	kombiniert die beiden letzten Prozeduren und erspart eine Triangularisierung der Matrix
determinant(A)	berechnet die Determinante von $A \in \mathbb{F}_p{}^{n\times n}$
basis_completion(A)	führt eine Basisergänzung der (linear unabhängigen) Spalten von $A \in \mathbb{F}_p{}^{m\times n}$, $n \leq m$ durch, so daß man eine Basis des $\mathbb{F}_p{}^m$ erhält.
quotient_module(A)	faßt die Spalten von A als Basis eines Teilraums U von $\mathbb{F}_p{}^m$ auf und liefert eine Basis für $\mathbb{F}_p{}^m/U$ zurück.

Es folgt die Deklaration der beschriebenen Klasse.

```
//---------------------------------
#ifndef FFMATRIX_H
#define FFMATRIX_H

#include <stdlib.h>
#include <string.h>

#include "ffvector.h"
//---------------------------------

class FF_matrix

      {
      FF **a;

      int rows;
      int columns;
```

```
        void error(char *,char *) const;

      public:

      // Constructors:

      // (int r, int c) defines a matrix with r rows and c columns
      // (int r)        defines a vector with r entries
      // ()             defines a 1x1 Matrix

      friend class ideal_mod_p;

      FF_matrix(int , int);
      FF_matrix(int);
      FF_matrix();

      // Copy constructors
      FF_matrix(const FF_matrix&);
      FF_matrix(const ideal_mod_p&);

      // Destructor
      ~FF_matrix();

friend int number_of_rows(const FF_matrix& M)    { return M.rows;} ;
friend int number_of_columns(const FF_matrix& M) { return M.columns;} ;
friend int get_rows(const FF_matrix& M)    { return M.rows;} ;
friend int get_columns(const FF_matrix& M) { return M.columns;} ;
friend void set_rows(FF_matrix& A,int r)    { A.rows=r;} ;
friend void set_columns(FF_matrix& A,int c) { A.columns=c;} ;

      FF  element(int,int) const;  // to get a matrix element
      void sto(int,int,FF);        // to change a matrix elemnt

friend FF_vector column(const FF_matrix&,int);
friend FF_vector row(const FF_matrix&,int);

      void change_dimension(int,int);

friend void sto_column(FF_matrix&,const FF_vector&, int);
friend void sto_row(FF_matrix&,const FF_vector&, int);

friend void column_step_form(FF_matrix&,FF_matrix&);

friend FF_matrix kern(const FF_matrix&);
friend FF_matrix image(const FF_matrix&);
friend FF_matrix transponate(const FF_matrix&);
```

```
friend FF determinant(const FF_matrix&);

// input / output functions
friend ostream& operator<<(ostream&,const FF_matrix&);
friend istream& operator>>(istream&, FF_matrix&);

// arithmetic
friend FF_matrix operator+(const FF_matrix&,const FF_matrix&);
friend FF_matrix operator*(const FF_matrix&,const FF_matrix&);
friend FF_vector operator*(const FF_matrix&,const FF_vector&);

// comparison
friend int operator==(const FF_matrix&,const FF_matrix&);

// assignment
      FF_matrix& operator=(const FF_matrix&);
      FF_matrix& operator=(int);

friend FF_matrix quotient_module(FF_matrix&);
      };
FF_matrix basis_completion(const FF_matrix&);
void kern_and_image(const FF_matrix&,FF_matrix&,FF_matrix&);

#endif

//--------------------------------
```

5.6 Die Klasse FF_poly

Diese Klasse realisiert die Arithmetik von Polynomen in $\mathbb{F}_p[X]$. Da die Algorithmen für Addition und Subtraktion trivial sind, widmen wir uns im folgenden Abschnitt der Multiplikation.

5.6.1 Multiplikation in $\mathbb{F}_p[X]$

Seien $f, g \in \mathbb{F}_p[X]$ mit

$$\begin{aligned} f(X) &= \sum_{j=0}^{n} a_j X^j, \quad a_j \in \mathbb{F}_p \\ g(X) &= \sum_{k=0}^{m} b_k X^k, \quad b_k \in \mathbb{F}_p \end{aligned}$$

und h das Produkt von f und g

$$h(X) = f(X)g(X) = \sum_l c_l X^l \quad c_l \in \mathbb{F}_p.$$

Die Koeffizienten berechnet man nach der Formel

$$f(X)g(X) = \sum_{l=0}^{m+n} \underbrace{(\sum_{i=0}^{l} a_i b_{l-i})}_{=c_l} X^l.$$

Also können die c_l in $O((m+n)^2)$ vielen Operationen in $\mathbb{F}_p$ bestimmt werden.

5.6.2 Division mit Rest in $\mathbb{F}_p[X]$

Aus der Körpereigenschaft von $\mathbb{F}_p$ folgt, daß der Polynomring über $\mathbb{F}_p$ ein Euklidischer Ring ist, es also für gegebene Polynome $f, g \in \mathbb{F}_p[X]$ zwei eindeutig bestimmte Polynome $q, r \in \mathbb{F}_p[X]$ gibt mit

$$f(X) = q(X)g(X) + r(X) \quad \wedge \quad (deg\ r < deg\ g \vee r \equiv 0)$$

Das Standardverfahren zur Berechnung von q und r ist beschrieben in [Knu2, Section 4.6.1]

5.6.3 Weitere Funktionen in $\mathbb{F}_p[X]$

leading_coefficient	liefert den höchsten Koeffizienten
degree	liefert den Grad
derivative	liefert die erste (formale) Ableitung
FF_monom(int k)	liefert X^k
p_th_root	liefert für $g(X)^p$ das Polynom $g(X)$ bei Charakteristik p
evaluate(f,a)	wertet das Polynom f an der Stelle $a \in \mathbb{F}_p$ aus
gcd(f,g)	berechnet nach dem Euklidischen Algorithmus den größten gemeinsamen Teiler von f und g
power(f,n,g)	liefert $f(X)^n$ modulo dem Polynom $g(X)$
root(f)	liefert eine Nullstelle von f nach dem Verfahren aus Abschnitt 4.2.2
root1(f)	liefert eine Nullstelle von f durch Ausprobieren
factorize(f)	Faktorisierung von f mit dem Berlekamp–Algorithmus [Knu2]

5.7 Datenstrukturen über $\mathbb{Q}$

Zur Berechnung von Multiplikationstabellen aus gegebenen Ganzheitsbasen ist es bequem, wenn man die Möglichkeit hat, lineare Gleichungssysteme über $\mathbb{Q}$ zu lösen. Daher wurden analog zu `FF,FF_vector,FF_matrix` die Klassen `Q,Q_vector,Q_matrix` definiert, die mit denselben Operationen und Funktionen wie die entsprechenden Klassen über $\mathbb{F}_p$ ausgestattet wurden. Die zugrundeliegenden Verfahren sind identisch, da sowohl $\mathbb{F}_p$ als auch $\mathbb{Q}$ Körper sind.

Der Vollständigkeit halber wurde analog zur Klasse `FF_poly` die Klasse `Q_poly` zur Realisierung des Polynomrings $\mathbb{Q}[X]$ hinzugefügt.

5.8 Datenstrukturen über $\mathbb{Z}$

In Analogie zu $\mathbb{Q}$ und $\mathbb{F}_p$ wurden die Klassen `Z_vector,Z_matrix` entwickelt, wobei die Klasse `Z_matrix` allerdings den Algorithmus zur Bestimmung der Spaltenstufenform nicht enthält, da dieser wegen auftretender Divisionen nur in Körpern verwendbar ist. Stattdessen hat man hier den Algorithmus zur Bestimmung der Hermite–Normalform (Abschnitt 3.4) zur Verfügung. Falls in unserem Algorithmus der Ganzheitsring nicht durch eine Multiplikationstabelle beschrieben wird, kann alternativ ein erzeugendes Polynom des Zahlkörpers eingegeben werden. Aus diesem Polynom wird dann die Multiplikationstabelle von $\mathbb{Z}[\rho]$ gebildet.

Aus diesem Grunde wurde die Klasse `Z_poly` implementiert, die eine Polynomarithmetik in $\mathbb{Z}[X]$ darstellt.

5.9 Arithmetik im Ring $\mathcal{O}/p\mathcal{O}$

5.9.1 Elemente in $\mathcal{O}/p\mathcal{O}$

Der Körper $\mathbb{F}_p$ ist in kanonischer Weise in $\mathcal{O}/p\mathcal{O}$ eingebettet:

$$\begin{array}{rcl} \mathbb{F}_p & \to & \mathcal{O}/p\mathcal{O} \\ a & \mapsto & \underbrace{1 + \ldots + 1}_{a-mal} \end{array} \tag{5.1}$$

Daher ist $\mathcal{O}/p\mathcal{O}$ sogar eine $\mathbb{F}_p$–Algebra, insbesondere also $\mathbb{F}_p$–Vektorraum. Die Darstellung der Elemente in $\mathcal{O}/p\mathcal{O}$ kann man Abschnitt 2.5 entnehmen.

Somit ist es möglich, die gesamte Speicherverwaltung und Vektorraum–Arithmetik von ${\mathbb{F}_p}^n$ an $\mathcal{O}/p\mathcal{O}$ durch Vererbung zu übertragen. Dies spart auf effektive Weise Programmcode ein (Abschnitt 5.1.3).

Die Multiplikation in $\mathcal{O}$ ist gegeben durch eine Multiplikationstabelle

$$w_{ijk}, \quad 1 \leq i, j, k \leq n,$$

so daß

$$\omega_i \omega_j = \sum_{k=1}^{n} w_{ijk} \omega_k$$

Da $\mathcal{O}$ ein kommutativer Ring ist, läßt sich die Tabelle auf die Indizes $1 \leq i \leq j \leq n$ und $1 \leq k \leq n$ beschränken. Daher hat man nur

$$\frac{n^2(n+1)}{2}$$

belegte Speicherplätze statt deren n^3.

Damit kann man beliebige Produkte in $\mathcal{O}$ ausrechnen, wie in Abschnitt 3.1 beschrieben.

Die Potenzierung kann nach Abschnitt 5.3.5 in polynomieller Zeit ausgeführt werden.

5.9.2 Ideale in $\mathcal{O}/p\mathcal{O}$

In Abschnitt 3.2 wurde schon auf die Darstellung von Idealen eingegangen. Für $I \trianglelefteq \mathcal{O}/p\mathcal{O}$ haben wir eine Darstellungsmatrix

$$M_I = \begin{pmatrix} b_{11} & \cdots & b_{1m} \\ \vdots & & \vdots \\ b_{n1} & \cdots & b_{nm} \end{pmatrix} \in \mathbb{F}_p{}^{n \times n}$$

Aus diesem Grunde kann die Klasse `ideal_mod_p`, die für die Realisierung der Idealarithmetik in $\mathcal{O}/p\mathcal{O}$ zuständig ist, die Speicherverwaltung von der Klasse `FF_matrix` erben.

Für die in Abschnitt 3.2 kurz angesprochenen Operationen werden nun die entsprechenden Algorithmen angegeben.

Algorithmus OPERATOR+

Eingabe:

$$\begin{aligned} \overline{A}, \overline{B} &\trianglelefteq \overline{\mathcal{O}} \\ \overline{A} &= <\overline{\alpha}_1, \ldots, \overline{\alpha}_l>_{\mathbb{F}_p} \\ \overline{B} &= <\overline{\beta}_1, \ldots, \overline{\beta}_m>_{\mathbb{F}_p} \end{aligned}$$

Ausgabe: $\overline{C} := \overline{A} + \overline{B} = <\overline{\gamma}_1, \ldots, \overline{\gamma}_t>_{\mathbb{F}_p}$

(1) $\overline{C}' \leftarrow (\overline{\alpha}_1, \ldots, \overline{\alpha}_l, \overline{\beta}_1, \ldots, \overline{\beta}_m)$

(2) *column_step_form*($\overline{C}'$)

(3) *für* $\overline{C}' = (0, \ldots, 0, \overline{\gamma}_1, \ldots, \overline{\gamma}_t)$ *setze* $\overline{C} \leftarrow (\overline{\gamma}_1, \ldots, \overline{\gamma}_t)$

(4) **return** $\overline{C}$

5.7 Bemerkung Die $\overline{\alpha}_i, \overline{\beta}_i$ sind durch den Vererbungsmechanismus nicht nur als Elemente von $\mathcal{O}/p\mathcal{O}$, sondern auch als Vektoren des $\mathbb{F}_p{}^n$ zu verwenden. Insbesondere lassen sich aus ihnen Matrizen zusammensetzen. Ebenso lassen sich auf die Ideale Matrizenoperationen anwenden. In diesem Sinne sind die im Algorithmus auftretenden Zuweisungsoperationen zu verstehen.

Algorithmus OPERATOR$*$

Eingabe:

$$\begin{aligned} \overline{A}, \overline{B} &\trianglelefteq \overline{\mathcal{O}} \\ \overline{A} &= <\overline{\alpha}_1, \ldots, \overline{\alpha}_l>_{\mathbb{F}_p} \\ \overline{B} &= <\overline{\beta}_1, \ldots, \overline{\beta}_m>_{\mathbb{F}_p} \end{aligned}$$

Ausgabe: $\overline{C} := \overline{A} \cdot \overline{B} = <\overline{\gamma}_1, \ldots, \overline{\gamma}_t>_{\mathbb{F}_p}$

(1) $\overline{C}' \leftarrow (\overline{\alpha}_1\overline{\beta}_1, \ldots, \overline{\alpha}_i\overline{\beta}_j, \ldots, \overline{\alpha}_l\overline{\beta}_m)$

(2) *column_step_form*$(\overline{C}')$

(3) *für* $\overline{C}' = (0, \ldots, 0, \overline{\gamma}_1, \ldots, \overline{\gamma}_t)$ *setze* $\overline{C} \leftarrow (\overline{\gamma}_1, \ldots, \overline{\gamma}_t)$

(4) **return** $\overline{C}$

Wir betrachten bei der Division den für uns ausreichenden Spezialfall, der von zwei $p\mathcal{O}$ teilenden Idealen ausgeht und überdies als Resultat ein ganzes Ideal in $\mathcal{O}$ erwartet.

Algorithmus OPERATOR/

Eingabe:

$$\begin{aligned} \overline{A}, \overline{B} &\trianglelefteq \overline{\mathcal{O}} \\ \overline{A} &= <\overline{\alpha}_1, \ldots, \overline{\alpha}_l>_{\mathbb{F}_p} \\ \overline{B} &= <\overline{\beta}_1, \ldots, \overline{\beta}_m>_{\mathbb{F}_p} \end{aligned}$$

Ausgabe: $\overline{C} := \overline{A}/\overline{B} = <\overline{\gamma}_1, \ldots, \overline{\gamma}_t>_{\mathbb{F}_p}$

(1) **for** $j \leftarrow 1$ **to** n **do**
co *gehe alle Basiselemente von* $\overline{\mathcal{O}}$ *durch* **oc**

(2) *für* $\overline{\omega}_j \in \overline{\mathcal{O}}$ *bestimme die Matrix der Abbildung*

$$\begin{array}{ccc} \overline{A} & \to & \overline{\mathcal{O}}/\overline{B} \\ \overline{\alpha} & \mapsto & \overline{\alpha\omega_j} \end{array}$$

(3) *speichere M als Spalte j in der Matrix T*

(4) **od**

(5) $\overline{C} \leftarrow Kern\ T$

5.10 UNIX–Makefiles

Um einen möglichst übersichtlichen Aufbau der Implementierung zu erhalten, wurde jede neu definierte Klasse samt ihrer zugehörigen Funktionen in einer eigenen Datei abgelegt. Die Objekt-Codes sind in einer Bibliothek zusammengefaßt. Der Deklarationsteil jeder Klasse ist Bestandteil einer eigenen *Header-Datei.*
Diese Vorgehensweise bei der Erstellung größerer Programme ist schon lange verbreitet und nicht erst seit der Einführung objektorientierter Programmierkonzepte üblich. Die Benutzung einer Klasse wird damit durch Einbinden (`#include`) des entsprechenden Header-Files und Angabe der Bibliothek ermöglicht.

Kapitel 6

Laufzeitbetrachtungen

Wir leiten dieses Kapitels mit einer Aussage über die theoretische worst–case–Laufzeit des Algorithmus ein und vergleichen diese im folgenden mit den Ergebnissen der praktischen Tests, die eine heuristische Aussage über die zu erwartende Laufzeit erlauben.

Alle arithmetischen Operationen, die im Algorithmus ausgeführt werden, finden ausnahmslos modulo der eingegebenen Primzahl p statt. Deshalb werden wir die Laufzeit in Anzahl von $\mathbb{F}_p$– Operationen angeben, wobei die Grundoperationen $(+, -, \cdot, /)$ zweier Elemente $a, b \in \mathbb{F}_p$ in Zeit $O(\log^2 p)$ ausgeführt werden können.

6.1 Die worst-case Laufzeit

Berechnung des p–Radikals Es wird die Matrix einer Abbildung aufgestellt, deren Abbildungsvorschrift sich für jedes Element in Zeit $O(n^2 \log n)$ berechnen läßt. Dies müssen wir für n Basiselemente tun. Danach wird die Matrix in $O(n^3)$ Operationen auf Spaltenstufenform gebracht. Also benötigt der erste Schritt höchstens Zeit

$$O(n \cdot n^2 \log n + n^3) = O(n^3 \log n).$$

Zerlegung von I_p in maximale Ideale In algebraischen Zahlkörpern der Dimension n ist die Anzahl der $p\mathcal{O}$ teilenden Primideale aus Normgründen durch n beschränkt:

$$p^n = N(p\mathcal{O}) = N(\prod_{i=1}^{r} M_i^{e_i}) = \prod_{i=1}^{r} \underbrace{N(M_i)}_{\geq p}{}^{e_i}.$$

Es folgt sofort $r \leq n$. Deshalb wird zum Zerlegen von I_p höchstens n–mal ein Ideal faktorisiert.

Nach Kapitel 4.2.2 benötigt dieses Verfahren Zeit $O(n^6)$, also haben wir für den dritten Schritt Laufzeit
$$O(n^7).$$

Bestimmung der Ideale in $\mathcal{O}$ Die modulare Hermite–Normalform–Berechnung läuft ähnlich wie der Gauss–Algorithmus im Körper $\mathbb{F}_p$ ab und benötigt daher Zeit
$$O(n^3).$$

Insgesamt hat man durch den dominierenden zweiten Schritt eine Gesamtlaufzeit im schlechtesten Fall von
$$O(n^7).$$

Die Betrachtung des zweiten Schrittes läßt vermuten, daß je mehr Primideale in der Zerlegung von $p\mathcal{O}$ auftreten, desto mehr Zeit in diesem Schritt verbraucht wird. Weiterhin läßt der deutliche Unterschied zu den Laufzeiten der anderen Schritte schon ahnen, daß der größte Teil der Gesamtlaufzeit dort verbraucht wird. Diese schon aus der Theorie ablesbaren Resultate finden sich in den praktischen Tests bestätigt, die den Inhalt des nächsten Abschnitts bilden.

6.2 Ergebnisse der praktischen Tests

Zur Bestimmung der Laufzeiten verwenden wir einen Betriebssystem– Aufruf. Das ist ein sogenannter *system call.* Die Systemfunktion entnimmt aus internen Tabellen die tatsächlich vom Prozessor für diesen Prozeß verbrauchte Zeit (CPU–Zeit) in $\frac{1}{100}$ Sekunden.

Wir haben am Ende jeden Schrittes die bis zu diesem Zeitpunkt verbrauchte Zeit gemessen, wobei wir jeden Durchlauf eines Schrittes einzeln aufführen.

6.1 Beispiel Wir geben einen Kontrollausdruck der Zeitmessung bei Körpergrad 7 an.

Das den Zahlkörper erzeugende Polynom ist
$$f(x) = x^7 - 3x^6 - 4x^5 - 2x^4 + 9x^3 + 6x^2 + 17x - 6,$$
zerlegt wird das Ideal $19\mathcal{O}_K$.

```
**************************************
(1)   p-radical:         27
(2.1) factor (D):       174
(2.2) factor (M):       210
(2.3) factor (D):       272
(2.4) factor (M):       272
(2.5) factor (M):       272
(3.1) exp (=1):         272
(3.2) exp (=2):         325
(4.1) HNF:              326
(4.2) HNF:              328
(4.3) HNF:              329
              190 type 3 (1,2,1)  - time 329
**************************************
```

Dies bedeutet, daß nach 0.27s das p–Radikal berechnet war, fünfmal die 'factor'–Prozedur des Schrittes (2) bemüht wurde, davon zweimal, um ein Ideal zu zerlegen (D) und dreimal, um die Maximalität eines Ideals festzustellen (M). In Schritt (3) mußten zwei Exponenten ermittelt werden und in Schritt (4) für jedes in (2) gefundene Primideal die modulare Hermite–Normalform–Berechnung durchgeführt werden, die die $\mathbb{Z}$–Basis der Primideale in $\mathcal{O}$ erzeugt. Die Zerlegung von $19\mathcal{O}_\mathcal{K}$ ist hier

$$19\mathcal{O}_\mathcal{K} = M_1 M_2^2 M_3.$$

Um die Zeitmessung bei der Zerlegung mehrerer Primzahlen in der gleichen Ordnung $\mathcal{O}$ übersichtlich darzustellen, haben wir Tabellen benutzt, die die jeweiligen Angaben vergleichbar nebeneinander auflisten.

Zunächst haben wir die Primzahlen $p \leq 83$ in Maximalordnungen durch Polynome gegebener Zahlkörper $\mathbb{Q}(\rho)$ zerlegt, wobei die Polynomkoeffizienten zufällig gewählt wurden. Es wurden zu jedem Körpergrad jeweils sieben Ordnungen erzeugt.

Die Laufzeitergebnisse hierzu befinden sich in Abschnitt 6.2.1.

Die Ganzheitsbasis wurde jeweils durch das Programmpaket [PARI] bestimmt; diese war die Grundlage zur Erzeugung einer Multiplikationstabelle, die von unserem Hauptverfahren verwendet wurde.

Anschließend (Abschnitt 6.2.2) geben wir, statistisch gemittelt, die durchschnittliche Laufzeit für jeden Zerlegungstyp an, wobei für das jeweils erste Polynom aus dem vorangehenden Abschnitt die 9592 Primzahlen

$$\{p \ Primzahl \mid 2 \leq p \leq 100\,000\}$$

zerlegt werden.

Um zu demonstrieren, wie die Laufzeit sich bei der Wahl größerer Primzahlen verhält, haben wir die Laufzeit bei jeweils gleichem Zahlkörper vom Grad n und Zerlegungstyp ($p\mathcal{O} = M_1 M_2$ für $n = 2, 3$ und $p\mathcal{O} = M_1 M_2 M_3$ für $4 \leq n \leq 9$) gemessen und dabei die Primzahl p um jeweils eine Zehnerpotenz erhöht (Abschnitt 6.2.3).

Schließlich vergleichen wir die jetzige Version des Verfahrens mit einer Implementierung des Verfahrens, das sich aus den Ideen von [BuLen] ergibt, welches wir in Abschnitt 4.3 beschrieben haben (Abschnitt 6.2.4).

6.2 Beispiel Das erzeugende Polynom sei durch

$$f(x) = x^4 - 13x^3 - 2x^2 - 8x + 2$$

gegeben. Wir zerlegen alle Primzahlen $p \leq 997$ und erhalten folgende Auswertung (Zeiten in $\frac{1}{100}$s):

```
type | av. time  | number (of 168)
-----+-----------+----------------
   1 |       18  |     48
   2 |       47  |     75
   3 |       67  |     42
   4 |       70  |      3
```

Dies bedeutet, von den 168 untersuchten Primzahlen haben 48 nur ein Primideal als Teiler, d.h. p ist Primidealpotenz. Die benötigte Zeit ist im Mittel 0.18s. 75 Primzahlen zerfallen in zwei Primideale, die benötigte Zeit ist im Mittel 0.47s und so fort.

6.2.1 Detaillierte Laufzeitmessungen der einzelnen Schritte

Auf den nächsten Seiten folgen nun die Laufzeitmessungen für die Körpergrade $2 \leq n \leq 9$ und den Primzahlen $2 \leq p \leq 83$. Die Tabellen geben an, zu welchen Zeitpunkten die jeweiligen Schritte des Verfahrens abgeschlossen wurden.

Außerdem wurden einige Tests für die Körpergrade $30, 52, 70, 82$ durchgeführt. Wir haben in diesen Fällen als Zahlkörper $\mathcal{K} = \mathbb{Q}(\zeta)$ gewählt, wobei ζ eine primitive q–te Einheitswurzel ist ($q = 31, 53, 71, 83$). Es ist bekannt [Stew], daß für diese Zahlkörper $\mathcal{O}_{\mathcal{K}} = \mathbb{Z}[\zeta]$ gilt.

Tabelle 1

$f(x) = x^2 - 27x - 29$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	1	0	0	1	0	0	0	0	1	1	1	0
Schritt 2.1	2	1	0	2	4	1	1	4	2	5	5	2
Schritt 2.2	–	–	–	–	4	–	–	4	–	5	5	–
Schritt 3.1	–	–	1	–	–	–	–	–	–	–	–	–
Schritt 4.1	2	1	1	2	5	1	2	5	2	5	5	2
Schritt 4.2	–	–	–	–	5	–	–	5	–	5	5	–

Tabelle 2

$f(x) = x^2 - 27x - 29$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	1	1	1	1	1	1	1	0	1	1	1
Schritt 2.1	5	3	2	2	5	5	2	4	2	5	3
Schritt 2.2	5	–	–	–	5	5	–	4	–	5	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	5	3	2	2	5	5	2	4	2	5	3
Schritt 4.2	5	–	–	–	5	5	–	4	–	5	–

Tabelle 3

$f(x) = x^2 - 10x + 10$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	1	0	0	1	1	1	0	1	1	1	2	1
Schritt 2.1	1	0	0	4	4	2	3	2	2	2	3	2
Schritt 2.2	–	–	–	4	4	–	4	–	–	–	–	–
Schritt 3.1	1	1	0	–	–	–	–	–	–	–	–	–
Schritt 4.1	2	1	0	4	5	2	4	2	2	2	3	2
Schritt 4.2	–	–	–	4	5	–	4	–	–	–	–	–

Tabelle 4

$f(x) = x^2 - 10x + 10$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	1	1	1	1	1	1	1	1	1	0	1
Schritt 2.1	2	5	2	5	5	5	4	6	2	2	2
Schritt 2.2	–	5	–	5	5	5	4	6	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	2	5	2	5	6	5	4	6	2	2	2
Schritt 4.2	–	5	–	5	6	5	4	6	–	–	–

Tabelle 5

$f(x) = x^2 + 20x + 16$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	1	1	1	1	0	0	0	1	0	1	1	0
Schritt 2.1	2	1	5	1	2	2	5	2	2	2	2	4
Schritt 2.2	–	–	6	–	–	–	5	–	–	–	–	4
Schritt 3.1	–	1	–	1	–	–	–	–	–	–	–	–
Schritt 4.1	2	1	6	1	2	2	5	2	2	2	2	5
Schritt 4.2	–	–	6	–	–	–	5	–	–	–	–	5

Tabelle 6

$f(x) = x^2 + 20x + 16$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	1	1	1	1	0	1	1	1	1	1	1
Schritt 2.1	4	5	5	2	4	2	5	2	2	5	5
Schritt 2.2	4	5	5	–	4	–	5	–	–	5	5
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	5	5	5	3	5	2	5	2	2	6	5
Schritt 4.2	5	5	5	–	5	–	5	–	–	6	5

Tabelle 7

$f(x) = x^2 - 19x + 6$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	0	0	0	1	1	1	0	0	1	1	1	0
Schritt 2.1	4	4	1	5	2	5	1	1	2	2	2	4
Schritt 2.2	4	4	–	5	–	5	–	–	–	–	–	4
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	4	4	1	5	2	5	2	1	2	2	2	4
Schritt 4.2	5	5	–	5	–	6	–	–	–	–	–	4

Tabelle 8

$f(x) = x^2 - 19x + 6$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	1	1	1	1	1	1	1	1	1	1	1
Schritt 2.1	5	5	5	2	2	3	2	2	2	5	3
Schritt 2.2	5	5	5	–	–	–	–	–	–	5	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	6	5	6	2	2	3	2	2	2	5	3
Schritt 4.2	6	5	6	–	–	–	–	–	–	5	–

Tabelle 9

$f(x) = x^2 - 21x + 19$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	0	1	1	1	1	1	0	0	0	1	0	1
Schritt 2.1	1	2	1	5	2	5	5	4	2	2	1	2
Schritt 2.2	–	–	–	5	–	5	5	4	–	–	–	–
Schritt 3.1	–	–	1	–	–	–	–	–	–	–	–	–
Schritt 4.1	1	2	1	6	2	6	5	4	2	3	1	2
Schritt 4.2	–	–	–	6	–	6	6	4	–	–	–	–

Tabelle 10

$f(x) = x^2 - 21x + 19$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	1	1	1	1	1	1	1	1	1	1	1
Schritt 2.1	5	5	5	4	2	6	3	5	1	5	5
Schritt 2.2	5	6	5	4	–	6	–	5	–	5	5
Schritt 3.1	–	–	–	–	–	–	–	–	2	–	–
Schritt 4.1	5	6	5	5	2	6	3	6	2	6	5
Schritt 4.2	5	6	5	5	–	6	–	6	–	6	5

Tabelle 11

$f(x) = x^2 - 18x + 20$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	1	1	1	1	1	1	0	0	1	1	1	1
Schritt 2.1	2	5	5	2	2	5	2	4	2	2	3	2
Schritt 2.2	–	5	5	–	–	5	–	5	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	2	5	5	2	2	5	2	5	2	2	3	2
Schritt 4.2	–	5	5	–	–	6	–	5	–	–	–	–

Tabelle 12

$f(x) = x^2 - 18x + 20$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	1	1	1	1	1	1	1	1	1	1	1
Schritt 2.1	5	2	5	2	2	1	3	2	6	3	5
Schritt 2.2	5	–	5	–	–	–	–	–	6	–	6
Schritt 3.1	–	–	–	–	–	1	–	–	–	–	–
Schritt 4.1	5	2	6	2	2	1	3	2	6	3	6
Schritt 4.2	6	–	6	–	–	–	–	–	6	–	6

Tabelle 13

$f(x) = x^2 + 7x + 17$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	0	0	0	1	1	1	1	1	1	1	0	1
Schritt 2.1	2	2	4	5	5	2	5	1	6	2	2	2
Schritt 2.2	–	–	4	5	6	–	5	–	6	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	1	–	–	–	–
Schritt 4.1	2	2	5	5	6	2	5	1	6	2	2	2
Schritt 4.2	–	–	5	5	6	–	5	–	6	–	–	–

Tabelle 14

$f(x) = x^2 + 7x + 17$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	1	1	0	1	0	1	1	1	1	1	1
Schritt 2.1	3	5	5	2	1	6	2	2	6	3	7
Schritt 2.2	–	5	5	–	–	6	–	–	6	–	7
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	3	5	5	2	1	6	2	2	6	3	7
Schritt 4.2	–	6	5	–	–	6	–	–	6	–	7

Tabelle 15

$f(x) = x^2 + x + 30$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	0	1	1	1	1	1	0	1	1	1	1	0
Schritt 2.1	5	5	5	1	2	2	1	3	2	3	5	2
Schritt 2.2	5	5	5	–	–	–	–	–	–	–	5	–
Schritt 3.1	–	–	–	1	–	–	1	–	–	–	–	–
Schritt 4.1	5	5	6	1	2	3	1	3	2	3	5	2
Schritt 4.2	5	5	6	–	–	–	–	–	–	–	6	–

Tabelle 16

$f(x) = x^2 + x + 30$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	1	1	0	1	1	1	0	1	1	1	1
Schritt 2.1	5	5	1	6	3	5	5	3	5	2	2
Schritt 2.2	5	5	–	6	–	5	5	–	6	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	6	5	1	6	3	5	5	3	6	2	2
Schritt 4.2	6	6	–	6	–	5	5	–	6	–	–

Tabelle 17

$f(x) = x^2 - 7x - 21$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	0	0	1	1	1	1	1	0	1	1	1	1
Schritt 2.1	0	5	2	1	5	5	2	1	5	2	6	2
Schritt 2.2	–	5	–	–	5	5	–	–	5	–	6	–
Schritt 3.1	–	–	–	2	–	–	–	1	–	–	–	–
Schritt 4.1	0	5	2	2	6	5	2	1	6	2	6	2
Schritt 4.2	–	5	–	–	6	5	–	–	6	–	6	–

Tabelle 18

$f(x) = x^2 - 7x - 21$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	0	1	1	1	1	0	1	0	1	1	1
Schritt 2.1	4	5	3	2	6	1	2	1	2	2	2
Schritt 2.2	4	5	–	–	6	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	5	5	3	2	6	1	3	1	3	2	2
Schritt 4.2	5	5	–	–	6	–	–	–	–	–	–

Tabelle 19

$f(x) = x^2 + 11x - 25$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	0	1	0	1	1	1	0	1	1	0	1	0
Schritt 2.1	1	2	4	5	5	1	1	2	2	2	5	5
Schritt 2.2	–	–	4	5	5	–	–	–	–	–	5	5
Schritt 3.1	–	–	–	–	–	2	1	–	–	–	–	–
Schritt 4.1	1	2	4	5	5	2	1	2	2	2	5	5
Schritt 4.2	–	–	4	5	5	–	–	–	–	–	5	5

Tabelle 20

$f(x) = x^2 + 11x - 25$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	1	1	1	1	1	1	1	1	1	1	1
Schritt 2.1	5	5	2	6	3	2	3	5	5	2	2
Schritt 2.2	5	5	–	6	–	–	–	5	5	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	5	6	2	6	3	2	3	6	5	3	2
Schritt 4.2	5	6	–	6	–	–	–	6	5	–	–

Tabelle 21

$f(x) = x^2 + 11x + 25$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	0	0	1	0	1	0	0	1	1	1	1	1
Schritt 2.1	1	0	5	0	2	2	4	2	3	2	2	6
Schritt 2.2	–	–	5	–	–	–	5	–	–	–	–	6
Schritt 3.1	–	1	–	0	–	–	–	–	–	–	–	–
Schritt 4.1	2	1	5	0	2	2	5	2	3	2	2	6
Schritt 4.2	–	–	5	–	–	–	5	–	–	–	–	6

Tabelle 22

$f(x) = x^2 + 11x + 25$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	1	1	1	1	1	1	1	1	1	1	1
Schritt 2.1	6	6	6	3	5	3	5	2	3	6	6
Schritt 2.2	6	6	6	–	6	–	5	–	–	6	6
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	6	6	6	3	6	3	6	2	3	7	6
Schritt 4.2	6	6	6	–	6	–	6	–	–	7	6

Tabelle 23

$f(x) = x^2 - 17x - 15$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	0	0	0	1	1	0	0	1	1	1	1	1
Schritt 2.1	1	5	4	2	2	2	5	5	6	6	6	6
Schritt 2.2	–	5	4	–	–	–	5	6	6	6	6	6
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	1	5	4	2	2	2	5	6	6	6	6	6
Schritt 4.2	–	5	4	–	–	–	5	6	6	6	6	6

Tabelle 24

$f(x) = x^2 - 17x - 15$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	1	1	1	1	2	1	1	1	0	1	1
Schritt 2.1	6	3	3	2	3	3	6	2	5	3	6
Schritt 2.2	6	–	–	–	–	–	6	–	5	–	6
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	6	3	3	2	3	3	6	2	5	3	6
Schritt 4.2	6	–	–	–	–	–	7	–	5	–	6

Tabelle 25

$f(x) = x^2 - 27x + 14$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	1	1	0	0	1	1	1	1	0	0	2	1
Schritt 2.1	5	5	1	5	2	5	2	2	5	5	3	6
Schritt 2.2	5	5	–	5	–	5	–	–	5	5	–	6
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	5	6	1	5	2	5	2	3	5	5	3	6
Schritt 4.2	5	6	–	5	–	5	–	–	5	5	–	6

Tabelle 26

$f(x) = x^2 - 27x + 14$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	1	1	2	1	1	1	1	1	1	1	1
Schritt 2.1	3	2	3	5	2	2	3	2	5	3	5
Schritt 2.2	–	–	–	5	–	–	–	–	6	–	6
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	3	2	3	5	2	2	3	2	6	3	6
Schritt 4.2	–	–	–	5	–	–	–	–	6	–	6

Tabelle 27

$f(x) = x^3 + 10x^2 + 24x + 2$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	2	1	1	2	2	2	1	2	2	2	2	2
Schritt 2.1	2	4	4	11	6	11	11	11	11	5	12	12
Schritt 2.2	–	–	–	11	–	11	13	11	14	–	12	15
Schritt 2.3	–	–	–	20	–	13	14	20	15	–	15	15
Schritt 2.4	–	–	–	20	–	–	–	20	–	–	–	–
Schritt 3.1	4	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	4	4	4	21	6	13	14	20	15	6	15	15
Schritt 4.2	–	–	–	21	–	14	14	20	15	–	15	15
Schritt 4.3	–	–	–	21	–	–	–	21	–	–	–	–

Tabelle 28

$f(x) = x^3 + 10x^2 + 24x + 2$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	2	2	2	2	2	2	2	2	2	2	2
Schritt 2.1	12	11	6	11	12	11	5	11	11	11	11
Schritt 2.2	15	12	–	11	12	14	–	14	11	11	14
Schritt 2.3	15	20	–	14	21	14	–	14	14	14	14
Schritt 2.4	–	20	–	–	21	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	16	20	6	14	21	15	5	14	14	15	14
Schritt 4.2	16	20	–	14	21	15	–	15	14	15	15
Schritt 4.3	–	20	–	–	22	–	–	–	–	–	–

Tabelle 29

$f(x) = x^3 - 14x^2 - 10x + 27$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	1	2	1	1	1	2	2	2	2	2	2	2
Schritt 2.1	10	10	3	4	10	11	11	12	12	5	12	5
Schritt 2.2	10	10	–	–	13	14	11	15	12	–	12	–
Schritt 2.3	13	12	–	–	13	14	20	15	15	–	15	–
Schritt 2.4	–	–	–	–	–	–	20	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	13	12	3	4	13	15	20	15	15	5	16	5
Schritt 4.2	13	12	–	–	13	15	21	15	15	–	16	–
Schritt 4.3	–	–	–	–	–	–	21	–	–	–	–	–

Tabelle 30

$f(x) = x^3 - 14x^2 - 10x + 27$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	2	2	2	2	3	3	3	2	2	2	2
Schritt 2.1	10	11	5	11	13	6	6	6	5	6	6
Schritt 2.2	13	12	–	11	13	–	–	–	–	–	–
Schritt 2.3	13	19	–	14	16	–	–	–	–	–	–
Schritt 2.4	–	20	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	13	20	5	14	16	6	6	6	5	6	6
Schritt 4.2	13	20	–	14	16	–	–	–	–	–	–
Schritt 4.3	–	21	–	–	–	–	–	–	–	–	–

Tabelle 31

$f(x) = x^3 + 2x^2 - 10x - 19$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	1	1	1	2	2	2	2	2	2	2	2	2
Schritt 2.1	9	4	3	4	11	11	12	11	12	6	12	11
Schritt 2.2	9	–	–	–	11	11	12	12	12	–	12	15
Schritt 2.3	12	–	–	–	11	14	15	21	21	–	15	15
Schritt 2.4	–	–	–	–	–	–	–	21	21	–	–	–
Schritt 3.1	–	–	–	–	12	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	14	–	–	–	–	–	–	–
Schritt 4.1	12	4	3	4	14	14	15	21	22	6	15	15
Schritt 4.2	12	–	–	–	14	14	15	22	22	–	16	15
Schritt 4.3	–	–	–	–	–	–	–	22	22	–	–	–

Tabelle 32

$f(x) = x^3 + 2x^2 - 10x - 19$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	2	3	3	2	2	3	2	2	2	3	2
Schritt 2.1	5	13	13	13	5	6	5	12	5	13	6
Schritt 2.2	–	17	16	13	–	–	–	12	–	13	–
Schritt 2.3	–	17	16	17	–	–	–	15	–	16	–
Schritt 2.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	5	17	17	17	5	7	5	15	5	17	6
Schritt 4.2	–	17	17	17	–	–	–	16	–	17	–
Schritt 4.3	–	–	–	–	–	–	–	–	–	–	–

Tabelle 33

$f(x) = x^3 - 7x^2 + 16x - 7$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	1	1	1	1	2	2	2	1	2	2	2	3
Schritt 2.1	3	10	10	11	5	11	4	11	12	12	12	13
Schritt 2.2	–	10	10	11	–	11	–	14	12	15	15	13
Schritt 2.3	–	13	10	14	–	14	–	14	21	15	15	22
Schritt 2.4	–	–	–	–	–	–	–	–	21	–	–	22
Schritt 3.1	–	–	11	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	3	13	11	14	5	14	5	15	21	16	15	23
Schritt 4.2	–	13	12	14	–	14	–	15	22	16	15	23
Schritt 4.3	–	–	–	–	–	–	–	–	22	–	–	23

Tabelle 34

$f(x) = x^3 - 7x^2 + 16x - 7$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	2	2	3	2	2	2	2	2	3	3	2
Schritt 2.1	6	12	7	12	6	6	6	11	12	14	6
Schritt 2.2	–	13	–	15	–	–	–	12	12	14	–
Schritt 2.3	–	16	–	15	–	–	–	15	21	17	–
Schritt 2.4	–	–	–	–	–	–	–	–	21	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	6	16	7	15	6	6	6	15	22	18	6
Schritt 4.2	–	16	–	15	–	–	–	15	22	18	–
Schritt 4.3	–	–	–	–	–	–	–	–	22	–	–

Tabelle 35

$f(x) = x^3 + 17x^2 + x - 28$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	1	1	1	2	2	1	2	2	1	2	3	2
Schritt 2.1	9	10	9	10	10	11	11	12	4	5	13	13
Schritt 2.2	9	10	9	10	11	11	14	15	–	–	13	13
Schritt 2.3	12	12	9	12	13	19	14	15	–	–	22	22
Schritt 2.4	–	–	–	–	–	19	–	–	–	–	22	22
Schritt 3.1	–	–	10	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	12	–	–	–	–	–	–	–	–	–
Schritt 4.1	12	13	12	13	13	20	14	15	4	5	22	22
Schritt 4.2	12	13	12	13	14	20	14	15	–	–	23	22
Schritt 4.3	–	–	–	–	–	20	–	–	–	–	23	23

Tabelle 36

$f(x) = x^3 + 17x^2 + x - 28$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	2	2	3	3	2	2	2	2	2	3	2
Schritt 2.1	5	12	13	14	6	5	6	6	6	14	6
Schritt 2.2	–	16	17	17	–	–	–	–	–	14	–
Schritt 2.3	–	16	17	17	–	–	–	–	–	17	–
Schritt 2.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	5	16	17	17	6	5	6	6	6	18	6
Schritt 4.2	–	16	17	18	–	–	–	–	–	18	–
Schritt 4.3	–	–	–	–	–	–	–	–	–	–	–

Tabelle 37

$f(x) = x^3 - 10x^2 + 12x + 1$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	1	1	1	1	2	2	2	2	2	2	2	2
Schritt 2.1	10	3	4	11	12	11	5	12	6	12	12	13
Schritt 2.2	10	–	–	13	12	14	–	15	–	12	12	13
Schritt 2.3	13	–	–	14	15	14	–	15	–	15	20	16
Schritt 2.4	–	–	–	–	–	–	–	–	–	–	20	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	13	3	4	14	15	15	5	15	6	15	20	17
Schritt 4.2	14	–	–	14	16	15	–	16	–	16	20	17
Schritt 4.3	–	–	–	–	–	–	–	–	–	–	20	–

Tabelle 38

$f(x) = x^3 - 10x^2 + 12x + 1$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	2	3	3	3	3	2	2	3	2	3	2
Schritt 2.1	13	13	14	13	14	13	6	13	14	15	13
Schritt 2.2	16	14	15	16	18	17	–	13	18	18	13
Schritt 2.3	17	23	25	17	18	17	–	13	18	18	16
Schritt 2.4	–	23	25	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	14	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	17	24	25	17	18	17	6	15	18	19	17
Schritt 4.2	17	24	26	17	18	18	–	15	18	19	17
Schritt 4.3	–	24	26	–	–	–	–	–	–	–	–

Tabelle 39

$f(x) = x^3 + 28x^2 + 18x - 17$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	0	1	1	2	2	2	2	2	2	2	2	2
Schritt 2.1	10	10	11	12	11	11	12	13	13	13	6	6
Schritt 2.2	10	11	11	12	11	11	12	13	16	16	–	–
Schritt 2.3	12	13	14	14	14	14	21	17	16	17	–	–
Schritt 2.4	–	–	–	–	–	–	21	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	13	13	14	15	14	14	21	17	16	17	6	6
Schritt 4.2	13	14	14	15	14	14	21	17	16	17	–	–
Schritt 4.3	–	–	–	–	–	–	21	–	–	–	–	–

Tabelle 40

$f(x) = x^3 + 28x^2 + 18x - 17$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	2	2	3	2	3	3	2	3	3	3	2
Schritt 2.1	13	6	14	15	14	7	6	6	3	13	6
Schritt 2.2	16	–	17	15	14	–	–	–	–	17	–
Schritt 2.3	16	–	17	25	24	–	–	–	–	17	–
Schritt 2.4	–	–	–	25	24	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	5	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	16	6	17	26	25	7	6	6	5	17	7
Schritt 4.2	16	–	17	26	25	–	–	–	–	18	–
Schritt 4.3	–	–	–	26	25	–	–	–	–	–	–

Tabelle 41

$f(x) = x^4 - 13x^3 - 2x^2 - 8x + 2$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	3	3	3	3	4	3	3	4	4	4	5	5
Schritt 2.1	17	8	24	10	25	24	25	23	26	25	28	12
Schritt 2.2	17	–	24	–	25	24	25	23	26	26	28	–
Schritt 2.3	17	–	40	–	44	44	44	28	34	46	49	–
Schritt 2.4	–	–	40	–	44	48	49	–	–	47	49	–
Schritt 2.5	–	–	40	–	59	48	49	–	–	52	54	–
Schritt 2.6	–	–	–	–	59	–	–	–	–	–	–	–
Schritt 3.1	23	–	45	–	–	–	–	32	–	–	–	–
Schritt 3.2	–	–	48	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	24	8	48	10	60	48	49	33	34	52	54	12
Schritt 4.2	24	–	48	–	60	48	50	33	35	53	55	–
Schritt 4.3	–	–	49	–	60	49	50	–	–	53	55	–
Schritt 4.4	–	–	–	–	60	–	–	–	–	–	–	–

Tabelle 42

$f(x) = x^4 - 13x^3 - 2x^2 - 8x + 2$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	5	5	6	5	5	6	5	5	5	7	6
Schritt 2.1	13	30	15	30	30	32	31	15	30	17	32
Schritt 2.2	–	36	–	30	31	38	37	–	39	–	41
Schritt 2.3	–	41	–	38	54	55	43	–	39	–	41
Schritt 2.4	–	–	–	–	60	55	–	–	–	–	–
Schritt 2.5	–	–	–	–	60	55	–	–	–	–	–
Schritt 2.6	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	13	41	15	39	60	56	43	15	39	17	42
Schritt 4.2	–	41	–	39	60	56	44	–	39	–	42
Schritt 4.3	–	–	–	–	60	57	–	–	–	–	–
Schritt 4.4	–	–	–	–	–	–	–	–	–	–	–

Tabelle 43

$f(x) = x^4 + 6x^3 + 19x^2 - 21x + 18$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	2	4	2	3	4	4	3	4	4	4	5	5
Schritt 2.1	21	23	8	9	24	25	26	23	26	27	13	27
Schritt 2.2	21	28	–	–	24	32	32	24	26	27	–	32
Schritt 2.3	27	32	–	–	31	33	37	43	46	35	–	38
Schritt 2.4	–	–	–	–	–	–	–	43	46	–	–	–
Schritt 2.5	–	–	–	–	–	–	–	48	61	–	–	–
Schritt 2.6	–	–	–	–	–	–	–	–	61	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	27	32	8	9	31	33	37	49	62	36	13	38
Schritt 4.2	27	32	–	–	31	33	37	49	62	36	–	39
Schritt 4.3	–	–	–	–	–	–	–	49	62	–	–	–
Schritt 4.4	–	–	–	–	–	–	–	–	62	–	–	–

Tabelle 44

$f(x) = x^4 + 6x^3 + 19x^2 - 21x + 18$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	4	5	6	5	5	5	5	6	5	6	5
Schritt 2.1	26	28	28	27	13	30	29	29	27	28	30
Schritt 2.2	26	28	28	27	–	36	34	29	27	34	39
Schritt 2.3	47	50	50	48	–	41	39	38	43	49	39
Schritt 2.4	52	50	50	53	–	–	–	–	43	49	–
Schritt 2.5	53	56	55	53	–	–	–	–	43	49	–
Schritt 2.6	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	47	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	53	56	56	54	14	42	39	39	48	50	39
Schritt 4.2	53	57	56	54	–	42	40	39	48	50	40
Schritt 4.3	54	57	57	55	–	–	–	–	49	50	–
Schritt 4.4	–	–	–	–	–	–	–	–	–	–	–

Tabelle 45

$f(x) = x^4 - 1x^3 + 14x^2 - 9x + 20$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	2	3	3	3	5	4	4	4	5	4	5	5
Schritt 2.1	21	25	25	9	26	10	11	25	12	27	28	28
Schritt 2.2	21	25	25	–	26	–	–	32	–	32	33	36
Schritt 2.3	27	32	47	–	45	–	–	32	–	37	50	37
Schritt 2.4	–	–	53	–	50	–	–	–	–	–	50	–
Schritt 2.5	–	–	53	–	50	–	–	–	–	–	50	–
Schritt 2.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	27	33	53	9	50	10	11	32	13	37	50	37
Schritt 4.2	28	33	53	–	51	–	–	32	–	37	51	37
Schritt 4.3	–	–	53	–	51	–	–	–	–	–	51	–
Schritt 4.4	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 46

$f(x) = x^4 - 1x^3 + 14x^2 - 9x + 20$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	5	5	6	6	5	6	5	6	5	6	6
Schritt 2.1	28	14	28	28	28	28	13	28	26	31	28
Schritt 2.2	33	–	33	37	34	33	–	37	27	31	34
Schritt 2.3	48	–	49	37	49	39	–	37	48	53	39
Schritt 2.4	48	–	49	–	50	–	–	–	53	53	–
Schritt 2.5	48	–	49	–	50	–	–	–	53	69	–
Schritt 2.6	–	–	–	–	–	–	–	–	–	69	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	48	14	49	37	50	39	13	37	54	69	40
Schritt 4.2	48	–	50	37	51	39	–	38	54	70	40
Schritt 4.3	49	–	50	–	51	–	–	–	54	70	–
Schritt 4.4	–	–	–	–	–	–	–	–	–	71	–

Tabelle 47

$f(x) = x^4 - 8x^3 + 23x^2 + 13x + 11$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	2	3	3	4	3	4	4	4	5	5	5	5
Schritt 2.1	22	25	26	25	26	11	25	12	27	28	30	27
Schritt 2.2	22	25	26	25	26	–	25	–	28	28	36	35
Schritt 2.3	28	31	46	32	34	–	47	–	51	36	52	35
Schritt 2.4	–	–	50	–	–	–	52	–	51	–	52	–
Schritt 2.5	–	–	50	–	–	–	52	–	57	–	52	–
Schritt 2.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	29	32	51	32	34	11	53	12	57	37	52	35
Schritt 4.2	29	32	51	33	34	–	53	–	58	37	53	36
Schritt 4.3	–	–	51	–	–	–	54	–	58	–	53	–
Schritt 4.4	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 48

$f(x) = x^4 - 8x^3 + 23x^2 + 13x + 11$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	5	6	6	6	5	6	6	5	6	6	6
Schritt 2.1	29	31	14	30	30	31	15	30	29	16	32
Schritt 2.2	35	40	–	30	36	40	–	36	37	–	32
Schritt 2.3	40	40	–	39	43	40	–	53	37	–	41
Schritt 2.4	–	–	–	–	–	–	–	54	–	–	–
Schritt 2.5	–	–	–	–	–	–	–	54	–	–	–
Schritt 2.6	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	41	40	14	39	43	40	15	54	37	16	41
Schritt 4.2	41	41	–	39	44	40	–	55	37	–	42
Schritt 4.3	–	–	–	–	–	–	–	55	–	–	–
Schritt 4.4	–	–	–	–	–	–	–	–	–	–	–

Tabelle 49

$f(x) = x^4 + 15x^3 + 5x^2 - 1x - 21$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	2	3	3	3	3	3	4	4	4	5	5	5
Schritt 2.1	8	27	10	19	27	26	11	28	29	28	30	30
Schritt 2.2	–	27	–	19	34	27	–	28	35	28	39	30
Schritt 2.3	–	35	–	20	34	34	–	36	52	52	40	38
Schritt 2.4	–	–	–	–	–	–	–	–	52	52	–	–
Schritt 2.5	–	–	–	–	–	–	–	–	52	58	–	–
Schritt 2.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	24	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	31	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	8	35	10	31	34	35	11	36	53	58	40	38
Schritt 4.2	–	35	–	32	34	35	–	37	53	59	40	39
Schritt 4.3	–	–	–	–	–	–	–	–	54	59	–	–
Schritt 4.4	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 50

$f(x) = x^4 + 15x^3 + 5x^2 - 1x - 21$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	5	5	6	5	6	6	5	6	5	6	5
Schritt 2.1	27	29	15	28	15	29	14	30	28	29	30
Schritt 2.2	28	39	–	34	–	35	–	39	34	30	39
Schritt 2.3	44	39	–	39	–	40	–	39	39	54	39
Schritt 2.4	44	–	–	–	–	–	–	–	–	54	–
Schritt 2.5	44	–	–	–	–	–	–	–	–	60	–
Schritt 2.6	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	49	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	53	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	53	39	15	39	15	41	14	39	39	61	39
Schritt 4.2	53	40	–	39	–	41	–	40	39	61	39
Schritt 4.3	54	–	–	–	–	–	–	–	–	62	–
Schritt 4.4	–	–	–	–	–	–	–	–	–	–	–

Tabelle 51

$f(x) = x^4 + 27x^3 - 12x^2 - 19x + 16$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	–	4	3	3	4	4	4	4	5	5	5	5
Schritt 2.1	21	25	9	10	12	29	27	11	13	13	29	28
Schritt 2.2	21	25	–	–	–	37	27	–	–	–	29	28
Schritt 2.3	28	32	–	–	–	37	35	–	–	–	36	51
Schritt 2.4	–	–	–	–	–	–	–	–	–	–	–	57
Schritt 2.5	–	–	–	–	–	–	–	–	–	–	–	57
Schritt 2.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	28	32	9	10	12	38	35	11	13	13	37	57
Schritt 4.2	28	32	–	–	–	38	36	–	–	–	37	58
Schritt 4.3	–	–	–	–	–	–	–	–	–	–	–	58
Schritt 4.4	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 52

$f(x) = x^4 + 27x^3 - 12x^2 - 19x + 16$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	5	6	5	5	6	6	5	5	5	5	5
Schritt 2.1	28	26	29	29	30	15	14	29	14	14	31
Schritt 2.2	35	31	37	38	30	–	–	37	–	–	32
Schritt 2.3	35	36	37	38	53	–	–	38	–	–	58
Schritt 2.4	–	–	–	–	59	–	–	–	–	–	64
Schritt 2.5	–	–	–	–	59	–	–	–	–	–	64
Schritt 2.6	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	36	37	37	38	59	15	15	38	14	15	64
Schritt 4.2	36	37	37	39	60	–	–	38	–	–	65
Schritt 4.3	–	–	–	–	60	–	–	–	–	–	65
Schritt 4.4	–	–	–	–	–	–	–	–	–	–	–

Tabelle 53

$f(x) = x^4 + x^3 + 6x^2 - 27x - 1$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	–	3	3	3	3	4	4	4	5	5	5	5
Schritt 2.1	21	9	24	25	10	11	28	11	13	13	33	13
Schritt 2.2	22	–	24	32	–	–	35	–	–	–	33	–
Schritt 2.3	26	–	45	32	–	–	35	–	–	–	42	–
Schritt 2.4	–	–	45	–	–	–	–	–	–	–	–	–
Schritt 2.5	–	–	50	–	–	–	–	–	–	–	–	–
Schritt 2.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	30	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	30	9	51	32	10	11	35	11	13	13	42	13
Schritt 4.2	31	–	51	32	–	–	36	–	–	–	43	–
Schritt 4.3	–	–	52	–	–	–	–	–	–	–	–	–
Schritt 4.4	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 54

$f(x) = x^4 + x^3 + 6x^2 - 27x - 1$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	5	6	5	5	6	5	5	5	5	6	6
Schritt 2.1	28	30	30	27	15	14	13	29	30	30	15
Schritt 2.2	28	31	30	27	–	–	–	29	35	40	–
Schritt 2.3	51	39	53	49	–	–	–	52	41	40	–
Schritt 2.4	51	–	53	49	–	–	–	52	–	–	–
Schritt 2.5	68	–	70	54	–	–	–	58	–	–	–
Schritt 2.6	68	–	70	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	69	39	70	54	15	15	13	58	41	40	15
Schritt 4.2	69	39	71	55	–	–	–	59	41	41	–
Schritt 4.3	70	–	71	55	–	–	–	59	–	–	–
Schritt 4.4	70	–	71	–	–	–	–	–	–	–	–

Tabelle 55

$f(x) = x^5 - 13x^4 - 2x^3 - 8x^2 + x + 7$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	5	7	6	6	7	8	8	8	10	10	11	10
Schritt 2.1	5	17	46	44	47	48	48	23	53	55	57	53
Schritt 2.2	–	–	46	45	48	48	56	–	61	63	57	89
Schritt 2.3	–	–	59	86	62	63	89	–	73	77	101	97
Schritt 2.4	–	–	–	86	–	–	89	–	–	–	111	106
Schritt 2.5	–	–	–	120	–	–	96	–	–	–	119	106
Schritt 2.6	–	–	–	127	–	–	–	–	–	–	–	–
Schritt 2.7	–	–	–	127	–	–	–	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	28	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	28	17	60	128	63	64	97	23	73	77	120	107
Schritt 4.2	–	–	60	129	63	64	97	–	74	78	121	107
Schritt 4.3	–	–	–	129	–	–	98	–	–	–	121	108
Schritt 4.4	–	–	–	130	–	–	–	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 56

$f(x) = x^5 - 13x^4 - 2x^3 - 8x^2 + x + 7$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	10	11	12	11	13	12	13	12	11	14	12
Schritt 2.1	54	58	57	60	62	31	55	56	55	32	30
Schritt 2.2	63	58	66	60	113	–	69	75	65	–	–
Schritt 2.3	76	103	80	108	123	–	96	75	79	–	–
Schritt 2.4	–	103	–	109	123	–	97	–	–	–	–
Schritt 2.5	–	140	–	122	132	–	97	–	–	–	–
Schritt 2.6	–	140	–	–	–	–	–	–	–	–	–
Schritt 2.7	–	149	–	–	–	–	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	77	150	80	123	132	31	97	75	80	33	30
Schritt 4.2	77	151	81	124	133	–	98	76	80	–	–
Schritt 4.3	–	152	–	124	133	–	98	–	–	–	–
Schritt 4.4	–	152	–	–	–	–	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–

Tabelle 57

$f(x) = x^5 + 19x^4 - 21x^3 + 17x^2 - 1x + 15$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	6	7	6	7	7	7	8	9	9	10	11	10
Schritt 2.1	42	39	43	47	19	49	49	23	50	54	28	56
Schritt 2.2	48	39	68	54	–	57	57	–	58	68	–	74
Schritt 2.3	81	63	68	88	–	68	68	–	90	76	–	74
Schritt 2.4	81	63	100	88	–	–	–	–	98	–	–	–
Schritt 2.5	88	63	101	96	–	–	–	–	99	–	–	–
Schritt 2.6	–	–	101	–	–	–	–	–	–	–	–	–
Schritt 2.7	–	–	108	–	–	–	–	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	75	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	92	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	88	93	108	97	19	69	68	24	99	77	28	74
Schritt 4.2	89	93	109	97	–	69	69	–	100	77	–	75
Schritt 4.3	89	94	110	98	–	–	–	–	100	–	–	–
Schritt 4.4	–	–	110	–	–	–	–	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 58

$f(x) = x^5 + 19x^4 - 21x^3 + 17x^2 - 1x + 15$

Primzahl	41	43	47	53	59	61	67	71	73	79	101
Schritt 1	10	11	13	12	13	13	11	13	11	14	–
Schritt 2.1	55	57	60	57	59	62	55	60	57	64	–
Schritt 2.2	72	74	60	72	74	62	69	60	57	64	–
Schritt 2.3	73	74	80	102	84	110	95	108	102	114	–
Schritt 2.4	–	–	–	102	–	124	95	108	112	130	–
Schritt 2.5	–	–	–	102	–	125	95	123	139	130	–
Schritt 2.6	–	–	–	–	–	–	–	–	139	–	–
Schritt 2.7	–	–	–	–	–	–	–	–	139	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	73	75	80	103	84	125	96	124	140	131	–
Schritt 4.2	73	75	81	104	85	126	96	124	141	131	–
Schritt 4.3	–	–	–	104	–	127	97	125	142	132	–
Schritt 4.4	–	–	–	–	–	–	–	–	142	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–

Tabelle 59

$f(x) = x^5 - 9x^4 + 19x^3 - 8x^2 + 23x + 14$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	6	6	6	6	7	8	8	9	10	10	11	10
Schritt 2.1	46	17	49	51	56	56	57	60	62	58	63	60
Schritt 2.2	71	–	49	89	68	72	57	60	62	72	64	61
Schritt 2.3	71	–	64	89	76	72	74	112	114	101	116	112
Schritt 2.4	80	–	–	96	–	–	–	112	123	102	157	127
Schritt 2.5	81	–	–	107	–	–	–	125	132	102	167	127
Schritt 2.6	–	–	–	–	–	–	–	–	–	–	167	–
Schritt 2.7	–	–	–	–	–	–	–	–	–	–	168	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	81	17	64	108	76	73	75	125	132	102	168	128
Schritt 4.2	82	–	65	108	77	73	75	126	133	103	169	129
Schritt 4.3	82	–	–	109	–	–	–	127	134	104	170	129
Schritt 4.4	–	–	–	–	–	–	–	–	–	–	171	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 60

$f(x) = x^5 - 9x^4 + 19x^3 - 8x^2 + 23x + 14$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	10	12	13	12	13	12	12	12	13	15	13
Schritt 2.1	56	60	32	60	32	32	59	61	60	69	34
Schritt 2.2	65	82	–	61	–	–	69	81	75	69	–
Schritt 2.3	79	82	–	110	–	–	108	81	84	122	–
Schritt 2.4	–	–	–	111	–	–	118	–	–	137	–
Schritt 2.5	–	–	–	153	–	–	118	–	–	137	–
Schritt 2.6	–	–	–	154	–	–	–	–	–	–	–
Schritt 2.7	–	–	–	163	–	–	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	80	83	32	164	32	32	118	82	85	138	34
Schritt 4.2	80	83	–	165	–	–	119	82	85	138	–
Schritt 4.3	–	–	–	166	–	–	119	–	–	139	–
Schritt 4.4	–	–	–	166	–	–	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–

Tabelle 61

$f(x) = x^5 + 10x^4 + 15x^3 + 5x^2 - 1x - 21$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	5	7	5	7	7	8	8	8	9	11	11	10
Schritt 2.1	16	40	17	41	48	49	51	54	57	60	60	60
Schritt 2.2	–	40	–	41	60	49	59	54	66	78	61	60
Schritt 2.3	–	66	–	68	68	64	94	70	79	78	78	77
Schritt 2.4	–	66	–	68	–	–	94	–	–	–	–	–
Schritt 2.5	–	66	–	68	–	–	102	–	–	–	–	–
Schritt 2.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.7	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	78	–	80	–	–	–	–	–	–	–	–
Schritt 3.2	–	94	–	98	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	16	94	17	98	69	65	102	71	80	78	79	77
Schritt 4.2	–	95	–	99	69	65	103	71	80	79	80	78
Schritt 4.3	–	96	–	100	–	–	104	–	–	–	–	–
Schritt 4.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 62

$f(x) = x^5 + 10x^4 + 15x^3 + 5x^2 - 1x - 21$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	10	11	12	11	13	12	12	12	12	14	13
Schritt 2.1	55	59	60	62	62	61	62	60	63	64	63
Schritt 2.2	68	73	70	62	77	71	63	80	63	85	63
Schritt 2.3	76	82	85	110	87	110	113	80	102	85	111
Schritt 2.4	–	–	–	111	–	111	123	–	102	–	121
Schritt 2.5	–	–	–	125	–	121	133	–	112	–	130
Schritt 2.6	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.7	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	126	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	138	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	77	83	85	126	87	121	133	81	139	86	131
Schritt 4.2	77	83	86	127	88	122	133	81	139	86	132
Schritt 4.3	–	–	–	127	–	123	134	–	140	–	132
Schritt 4.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–

Tabelle 63

$f(x) = x^5 + 27x^4 - 12x^3 - 19x^2 + 15x + 2$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	6	6	5	7	7	7	7	8	10	9	10	10
Schritt 2.1	45	46	16	57	19	49	50	23	54	52	58	59
Schritt 2.2	69	59	–	69	–	64	74	–	54	60	59	73
Schritt 2.3	69	59	–	95	–	64	74	–	73	72	110	82
Schritt 2.4	75	–	–	96	–	–	82	–	–	–	124	–
Schritt 2.5	76	–	–	96	–	–	82	–	–	–	124	–
Schritt 2.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.7	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	87	–	–	–	–	–	94	–	–	–	–	–
Schritt 3.2	87	–	–	–	–	–	94	–	–	–	–	–
Schritt 3.3	98	–	–	–	–	–	110	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	98	60	16	96	19	65	111	24	73	73	125	83
Schritt 4.2	99	60	–	97	–	65	111	–	74	73	125	83
Schritt 4.3	100	–	–	97	–	–	111	–	–	–	126	–
Schritt 4.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 64

$f(x) = x^5 + 27x^4 - 12x^3 - 19x^2 + 15x + 2$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	10	11	12	12	13	12	11	12	11	13	12
Schritt 2.1	61	57	31	56	61	60	58	60	29	59	63
Schritt 2.2	70	76	–	56	61	60	66	69	–	74	64
Schritt 2.3	110	76	–	73	112	81	104	83	–	104	114
Schritt 2.4	119	–	–	–	113	–	113	–	–	104	114
Schritt 2.5	119	–	–	–	151	–	113	–	–	104	152
Schritt 2.6	–	–	–	–	151	–	–	–	–	–	162
Schritt 2.7	–	–	–	–	160	–	–	–	–	–	162
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	120	77	31	74	161	82	114	83	29	104	163
Schritt 4.2	120	77	–	74	162	82	114	84	–	105	164
Schritt 4.3	121	–	–	–	162	–	115	–	–	106	165
Schritt 4.4	–	–	–	–	162	–	–	–	–	–	165
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–

Tabelle 65

$f(x) = x^5 + 6x^4 - 27x^3 - 25x + 16$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	5	6	6	6	8	8	7	9	10	10	11	10
Schritt 2.1	46	18	48	18	49	49	46	62	26	54	62	57
Schritt 2.2	46	–	55	–	65	57	58	62	–	54	62	57
Schritt 2.3	60	–	65	–	65	69	83	98	–	101	113	93
Schritt 2.4	–	–	–	–	–	–	83	106	–	113	141	94
Schritt 2.5	–	–	–	–	–	–	83	106	–	113	141	119
Schritt 2.6	–	–	–	–	–	–	–	–	–	–	150	119
Schritt 2.7	–	–	–	–	–	–	–	–	–	–	150	119
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	118	–	–	–	130
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	61	18	65	18	66	69	84	119	26	114	150	131
Schritt 4.2	61	–	66	–	66	70	84	119	–	114	151	132
Schritt 4.3	–	–	–	–	–	–	84	120	–	115	152	132
Schritt 4.4	–	–	–	–	–	–	–	–	–	–	152	133
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 66

$f(x) = x^5 + 6x^4 - 27x^3 - 25x + 16$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	10	10	12	12	12	12	11	12	12	14	13
Schritt 2.1	56	59	60	61	63	57	29	30	53	33	34
Schritt 2.2	72	59	60	75	83	57	–	–	53	–	–
Schritt 2.3	73	78	80	84	84	104	–	–	97	–	–
Schritt 2.4	–	–	–	–	–	104	–	–	107	–	–
Schritt 2.5	–	–	–	–	–	143	–	–	134	–	–
Schritt 2.6	–	–	–	–	–	153	–	–	134	–	–
Schritt 2.7	–	–	–	–	–	153	–	–	135	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	73	79	81	84	84	153	30	30	135	33	34
Schritt 4.2	74	79	81	85	85	153	–	–	136	–	–
Schritt 4.3	–	–	–	–	–	154	–	–	137	–	–
Schritt 4.4	–	–	–	–	–	155	–	–	138	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–

Tabelle 67

$f(x) = x^5 - 10x^4 - 26x^3 - 29x^2 - 3x + 23$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	5	6	5	6	7	8	7	9	9	9	11	10
Schritt 2.1	43	44	37	19	46	48	20	53	43	59	55	55
Schritt 2.2	52	51	37	–	62	60	–	61	43	60	73	55
Schritt 2.3	60	81	44	–	62	84	–	96	68	110	73	72
Schritt 2.4	–	81	–	–	–	84	–	96	69	110	–	–
Schritt 2.5	–	87	–	–	–	84	–	104	69	148	–	–
Schritt 2.6	–	–	–	–	–	–	–	–	–	157	–	–
Schritt 2.7	–	–	–	–	–	–	–	–	–	157	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	55	–	–	–	–	–	80	–	–	–
Schritt 3.2	–	–	59	–	–	–	–	–	97	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	61	87	60	19	62	84	20	105	97	158	73	73
Schritt 4.2	61	88	60	–	63	85	–	105	98	159	74	73
Schritt 4.3	–	88	–	–	–	86	–	106	99	160	–	–
Schritt 4.4	–	–	–	–	–	–	–	–	–	160	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 68

$f(x) = x^5 - 10x^4 - 26x^3 - 29x^2 - 3x + 23$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	10	11	12	13	13	13	10	14	11	15	12
Schritt 2.1	56	60	59	30	59	59	57	63	59	34	61
Schritt 2.2	65	68	77	–	74	59	57	63	72	–	81
Schritt 2.3	79	104	77	–	102	79	104	115	81	–	81
Schritt 2.4	–	104	–	–	102	–	117	116	–	–	–
Schritt 2.5	–	113	–	–	102	–	117	152	–	–	–
Schritt 2.6	–	–	–	–	–	–	–	153	–	–	–
Schritt 2.7	–	–	–	–	–	–	–	162	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	79	113	78	30	103	80	118	162	82	34	81
Schritt 4.2	80	114	78	–	104	80	119	163	82	–	82
Schritt 4.3	–	115	–	–	104	–	119	164	–	–	–
Schritt 4.4	–	–	–	–	–	–	–	164	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–

Tabelle 69

$f(x) = x^5 + 18x^3 - 1x^2 + 26x - 20$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	5	6	6	6	7	7	7	8	10	9	11	9
Schritt 2.1	42	45	42	46	47	50	49	53	25	58	27	60
Schritt 2.2	77	75	42	46	80	58	49	53	–	59	–	73
Schritt 2.3	87	75	56	60	87	89	96	69	–	98	–	102
Schritt 2.4	93	75	–	–	111	89	104	–	–	107	–	102
Schritt 2.5	93	81	–	–	111	97	130	–	–	107	–	102
Schritt 2.6	–	–	–	–	111	–	130	–	–	–	–	–
Schritt 2.7	–	–	–	–	112	–	130	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	90	–	–	–	–	–	–	–	120	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	120	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	131	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	93	91	56	60	112	97	131	70	25	132	27	103
Schritt 4.2	93	92	57	61	113	98	131	70	–	133	–	104
Schritt 4.3	94	92	–	–	113	98	132	–	–	133	–	104
Schritt 4.4	–	–	–	–	114	–	133	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 70

$f(x) = x^5 + 18x^3 - 1x^2 + 26x - 20$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	10	10	11	11	12	13	11	12	11	13	12
Schritt 2.1	26	56	58	57	57	58	58	61	55	59	30
Schritt 2.2	–	56	73	58	58	58	73	61	55	68	–
Schritt 2.3	–	74	83	109	78	77	82	111	73	83	–
Schritt 2.4	–	–	–	119	–	–	–	111	–	–	–
Schritt 2.5	–	–	–	129	–	–	–	148	–	–	–
Schritt 2.6	–	–	–	–	–	–	–	149	–	–	–
Schritt 2.7	–	–	–	–	–	–	–	158	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	27	75	83	129	79	78	83	159	74	83	30
Schritt 4.2	–	76	84	130	79	78	83	159	75	84	–
Schritt 4.3	–	–	–	131	–	–	–	159	–	–	–
Schritt 4.4	–	–	–	–	–	–	–	160	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–

Tabelle 71

$f(x) = x^6 - 3x^5 - 4x^4 - 2x^3 + 9x^2 + 6x + 18$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	11	11	16	12	14	14	14	17	19	20	23	20
Schritt 2.1	81	86	84	82	91	91	40	93	106	102	108	50
Schritt 2.2	82	140	84	82	131	114	–	106	126	103	109	–
Schritt 2.3	99	140	109	111	131	126	–	131	168	191	144	–
Schritt 2.4	–	154	–	–	199	–	–	–	168	212	–	–
Schritt 2.5	–	154	–	–	211	–	–	–	168	254	–	–
Schritt 2.6	–	–	–	–	211	–	–	–	–	254	–	–
Schritt 2.7	–	–	–	–	224	–	–	–	–	254	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	124	181	–	–	–	–	–	–	168	–	–	–
Schritt 3.2	–	181	–	–	–	–	–	–	198	–	–	–
Schritt 3.3	–	207	–	–	–	–	–	–	223	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	125	208	110	112	225	126	40	132	224	256	146	50
Schritt 4.2	125	208	110	112	225	127	–	133	225	256	146	–
Schritt 4.3	–	209	–	–	226	–	–	–	226	257	–	–
Schritt 4.4	–	–	–	–	227	–	–	–	–	258	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 72

$f(x) = x^6 - 3x^5 - 4x^4 - 2x^3 + 9x^2 + 6x + 18$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	20	25	24	22	26	25	23	25	22	27	24
Schritt 2.1	103	107	108	107	115	113	107	114	104	66	109
Schritt 2.2	117	107	130	107	138	126	107	114	104	–	132
Schritt 2.3	188	191	186	194	162	200	142	203	188	–	155
Schritt 2.4	189	191	186	216	–	216	–	218	215	–	–
Schritt 2.5	247	220	201	257	–	231	–	275	216	–	–
Schritt 2.6	248	–	–	257	–	–	–	275	–	–	–
Schritt 2.7	261	–	–	257	–	–	–	290	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	262	221	202	258	162	232	144	291	217	66	156
Schritt 4.2	263	222	203	259	163	232	144	292	217	–	156
Schritt 4.3	264	222	204	260	–	233	–	293	218	–	–
Schritt 4.4	265	–	–	261	–	–	–	294	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–

Tabelle 73

$f(x) = x^6 - 5x^5 + 29x^4 - 19x^3 + 18x^2 - 23x + 26$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	9	12	15	11	13	13	14	16	18	18	21	18
Schritt 2.1	79	85	35	86	88	87	84	95	96	48	103	95
Schritt 2.2	79	85	–	97	116	87	96	125	123	–	137	95
Schritt 2.3	101	162	–	117	116	170	160	125	163	–	138	175
Schritt 2.4	–	172	–	–	–	170	179	–	163	–	–	188
Schritt 2.5	–	186	–	–	–	236	179	–	164	–	–	207
Schritt 2.6	–	–	–	–	–	249	–	–	–	–	–	–
Schritt 2.7	–	–	–	–	–	262	–	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	102	187	35	118	117	263	180	125	164	48	138	208
Schritt 4.2	102	188	–	119	117	264	181	126	165	–	139	209
Schritt 4.3	–	189	–	–	–	265	182	–	166	–	–	210
Schritt 4.4	–	–	–	–	–	266	–	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 74

$f(x) = x^6 - 5x^5 + 29x^4 - 19x^3 + 18x^2 - 23x + 26$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	18	21	23	21	23	24	20	24	21	26	24
Schritt 2.1	102	109	106	107	110	116	107	109	113	63	109
Schritt 2.2	136	109	127	121	124	131	144	142	114	–	138
Schritt 2.3	136	143	148	191	197	192	144	157	192	–	180
Schritt 2.4	–	–	–	213	218	206	–	–	192	–	180
Schritt 2.5	–	–	–	213	218	206	–	–	250	–	180
Schritt 2.6	–	–	–	–	–	–	–	–	250	–	–
Schritt 2.7	–	–	–	–	–	–	–	–	265	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	206	–	–	290	–	–
Schritt 3.2	–	–	–	–	–	206	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	231	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	137	144	149	214	218	232	144	158	291	63	180
Schritt 4.2	138	144	150	215	218	233	145	159	292	–	181
Schritt 4.3	–	–	–	216	219	234	–	–	293	–	182
Schritt 4.4	–	–	–	–	–	–	–	–	294	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–

Tabelle 75

$f(x) = x^6 - 24x^5 + 9x^4 + 23x^3 + 12x^2 + 21x + 6$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	10	10	15	12	14	14	15	16	19	19	21	18
Schritt 2.1	74	46	88	88	91	91	91	90	98	98	105	97
Schritt 2.2	151	46	88	109	117	92	91	102	133	98	105	109
Schritt 2.3	209	46	107	151	128	119	118	174	133	191	192	178
Schritt 2.4	209	–	–	151	–	–	–	192	–	191	206	197
Schritt 2.5	209	–	–	152	–	–	–	193	–	217	261	197
Schritt 2.6	218	–	–	–	–	–	–	–	–	–	261	–
Schritt 2.7	232	–	–	–	–	–	–	–	–	–	275	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	96	132	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	135	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	233	136	133	152	129	120	119	193	134	218	276	198
Schritt 4.2	234	137	133	154	130	120	120	194	134	219	277	199
Schritt 4.3	235	–	–	155	–	–	–	195	–	220	278	200
Schritt 4.4	235	–	–	–	–	–	–	–	–	–	279	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 76

$f(x) = x^6 - 24x^5 + 9x^4 + 23x^3 + 12x^2 + 21x + 6$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	20	21	25	22	24	24	22	25	22	27	25
Schritt 2.1	109	54	117	54	119	108	106	111	108	116	114
Schritt 2.2	136	–	139	–	119	139	107	125	129	147	114
Schritt 2.3	149	–	162	–	216	155	195	197	151	162	204
Schritt 2.4	–	–	–	–	216	–	224	198	–	–	204
Schritt 2.5	–	–	–	–	246	–	225	257	–	–	279
Schritt 2.6	–	–	–	–	–	–	–	271	–	–	279
Schritt 2.7	–	–	–	–	–	–	–	271	–	–	300
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	150	54	162	54	247	155	226	271	152	162	301
Schritt 4.2	150	–	162	–	248	156	226	273	152	163	302
Schritt 4.3	–	–	–	–	249	–	227	273	–	–	304
Schritt 4.4	–	–	–	–	–	–	–	274	–	–	304
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–

Tabelle 77

$f(x) = x^6 + 29x^5 - 15x^3 - 12x^2 - 7x + 14$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	8	12	15	12	14	14	14	16	18	19	20	18
Schritt 2.1	76	29	97	94	91	101	96	43	97	96	102	102
Schritt 2.2	111	–	115	95	120	113	96	–	110	121	116	102
Schritt 2.3	111	–	116	116	120	136	165	–	177	134	190	137
Schritt 2.4	128	–	–	–	–	–	165	–	190	–	190	–
Schritt 2.5	128	–	–	–	–	–	182	–	202	–	212	–
Schritt 2.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.7	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	116	139	–	–	207	–	–	–	–	–
Schritt 3.2	–	–	140	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	129	29	140	140	121	137	208	44	203	134	213	138
Schritt 4.2	129	–	141	140	122	138	209	–	203	135	214	138
Schritt 4.3	129	–	–	–	–	–	210	–	204	–	215	–
Schritt 4.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 78

$f(x) = x^6 + 29x^5 - 15x^3 - 12x^2 - 7x + 14$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	20	20	24	19	24	23	21	24	22	26	24
Schritt 2.1	101	98	59	104	57	112	115	111	111	62	58
Schritt 2.2	114	118	–	118	–	126	134	146	111	–	–
Schritt 2.3	181	138	–	191	–	204	175	146	207	–	–
Schritt 2.4	181	–	–	212	–	217	175	–	221	–	–
Schritt 2.5	234	–	–	212	–	231	175	–	242	–	–
Schritt 2.6	246	–	–	–	–	–	–	–	–	–	–
Schritt 2.7	246	–	–	–	–	–	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	175	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	201	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	247	139	60	213	58	232	202	146	243	62	58
Schritt 4.2	249	140	–	214	–	233	203	147	244	–	–
Schritt 4.3	249	–	–	215	–	234	204	–	244	–	–
Schritt 4.4	250	–	–	–	–	–	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–

Tabelle 79

$f(x) = x^6 - 8x^5 - 18x^4 - 3x^3 - 15x^2 + 23$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	8	11	16	12	13	13	15	16	18	21	23	18
Schritt 2.1	72	29	94	90	38	84	98	96	115	49	108	102
Schritt 2.2	72	–	94	101	–	111	98	108	115	–	129	135
Schritt 2.3	93	–	114	122	–	112	126	178	180	–	148	136
Schritt 2.4	–	–	–	–	–	–	–	178	198	–	–	–
Schritt 2.5	–	–	–	–	–	–	–	232	198	–	–	–
Schritt 2.6	–	–	–	–	–	–	–	233	–	–	–	–
Schritt 2.7	–	–	–	–	–	–	–	246	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	139	–	–	–	–	–	222	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	94	29	140	123	39	112	127	247	223	49	149	136
Schritt 4.2	94	–	140	124	–	113	127	248	224	–	150	137
Schritt 4.3	–	–	–	–	–	–	–	249	225	–	–	–
Schritt 4.4	–	–	–	–	–	–	–	250	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 80

$f(x) = x^6 - 8x^5 - 18x^4 - 3x^3 - 15x^2 + 23$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	19	23	23	21	24	23	20	23	21	26	24
Schritt 2.1	102	107	114	56	109	109	103	58	107	117	59
Schritt 2.2	128	134	114	–	132	149	117	–	135	156	–
Schritt 2.3	141	176	213	–	193	149	192	–	149	156	–
Schritt 2.4	–	176	213	–	193	–	205	–	–	–	–
Schritt 2.5	–	176	243	–	238	–	218	–	–	–	–
Schritt 2.6	–	–	–	–	238	–	–	–	–	–	–
Schritt 2.7	–	–	–	–	238	–	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	141	177	244	56	239	150	219	58	149	157	60
Schritt 4.2	142	178	245	–	240	150	220	–	150	158	–
Schritt 4.3	–	179	246	–	241	–	221	–	–	–	–
Schritt 4.4	–	–	–	–	242	–	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–

Tabelle 81

$f(x) = x^6 + 28x^5 - 13x^4 + 26x^3 - 19x^2 - 28x + 2$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	10	11	15	12	13	14	14	16	18	18	22	18
Schritt 2.1	62	80	81	89	94	89	97	44	102	99	117	101
Schritt 2.2	62	80	91	100	181	89	125	–	115	112	117	135
Schritt 2.3	71	153	157	122	181	119	125	–	142	185	154	135
Schritt 2.4	–	162	157	–	181	–	–	–	–	205	–	–
Schritt 2.5	–	176	204	–	207	–	–	–	–	205	–	–
Schritt 2.6	–	–	204	–	–	–	–	–	–	–	–	–
Schritt 2.7	–	–	214	–	–	–	–	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	113	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	124	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	125	177	215	123	208	120	126	44	143	206	155	135
Schritt 4.2	126	178	216	123	209	120	127	–	144	207	157	136
Schritt 4.3	–	179	217	–	210	–	–	–	–	208	–	–
Schritt 4.4	–	–	218	–	–	–	–	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 82

$f(x) = x^6 + 28x^5 - 13x^4 + 26x^3 - 19x^2 - 28x + 2$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	19	21	23	23	25	24	21	23	22	27	24
Schritt 2.1	105	103	115	52	60	116	101	110	102	117	105
Schritt 2.2	106	103	152	–	–	192	129	124	122	147	106
Schritt 2.3	195	197	152	–	–	192	141	153	178	160	191
Schritt 2.4	221	197	–	–	–	206	–	–	192	–	191
Schritt 2.5	221	226	–	–	–	227	–	–	192	–	219
Schritt 2.6	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.7	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	222	227	152	53	60	228	142	154	193	161	220
Schritt 4.2	222	228	153	–	–	229	143	155	194	162	221
Schritt 4.3	223	229	–	–	–	230	–	–	195	–	221
Schritt 4.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–

Tabelle 83

$f(x) = x^6 + 6x^5 - 15x^4 - 19x^3 - 5x^2 - 16x + 20$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	8	11	15	11	14	14	13	16	18	19	20	18
Schritt 2.1	89	93	98	84	88	90	106	42	112	99	53	48
Schritt 2.2	148	103	137	84	88	114	106	–	112	99	–	–
Schritt 2.3	148	151	137	175	177	125	129	–	184	194	–	–
Schritt 2.4	148	151	158	175	177	–	–	–	204	194	–	–
Schritt 2.5	160	160	158	194	248	–	–	–	204	219	–	–
Schritt 2.6	–	–	–	–	265	–	–	–	–	–	–	–
Schritt 2.7	–	–	–	–	266	–	–	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	186	160	–	–	–	–	156	–	237	–	–	–
Schritt 3.2	–	185	–	–	–	–	–	–	237	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	263	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	187	186	159	195	267	126	157	43	264	220	54	48
Schritt 4.2	188	187	159	196	268	127	158	–	265	221	–	–
Schritt 4.3	189	188	160	196	268	–	–	–	266	221	–	–
Schritt 4.4	–	–	–	–	269	–	–	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 84

$f(x) = x^6 + 6x^5 - 15x^4 - 19x^3 - 5x^2 - 16x + 20$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	19	21	23	22	23	23	21	25	22	26	24
Schritt 2.1	104	119	108	110	107	58	106	124	109	117	60
Schritt 2.2	125	119	108	144	108	–	135	155	129	133	–
Schritt 2.3	186	154	204	145	144	–	149	155	149	216	–
Schritt 2.4	187	–	220	–	–	–	–	–	–	216	–
Schritt 2.5	200	–	241	–	–	–	–	–	–	276	–
Schritt 2.6	–	–	–	–	–	–	–	–	–	291	–
Schritt 2.7	–	–	–	–	–	–	–	–	–	291	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	155	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	181	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	201	155	242	145	146	58	149	181	150	292	60
Schritt 4.2	202	156	243	146	146	–	150	182	150	293	–
Schritt 4.3	203	–	244	–	–	–	–	–	–	294	–
Schritt 4.4	–	–	–	–	–	–	–	–	–	295	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–

Tabelle 85

$f(x) = x^7 - 3x^6 - 4x^5 - 2x^4 + 9x^3 + 6x^2 + 17x - 6$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	2	19	27	19	24	24	25	27	33	34	41	33
Schritt 2.1	125	125	139	143	149	156	154	174	171	174	175	162
Schritt 2.2	176	125	162	218	167	199	179	210	172	204	195	204
Schritt 2.3	176	250	255	218	282	257	281	272	230	244	317	294
Schritt 2.4	278	251	278	313	282	258	306	272	–	–	338	316
Schritt 2.5	297	280	278	328	379	258	307	272	–	–	419	317
Schritt 2.6	297	–	–	344	404	–	–	–	–	–	439	–
Schritt 2.7	309	–	–	360	404	–	–	–	–	–	439	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.11	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.12	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	272	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	325	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	310	281	279	361	406	259	308	326	232	246	441	318
Schritt 4.2	311	281	280	362	407	260	309	328	233	246	442	319
Schritt 4.3	312	282	282	364	408	261	310	329	–	–	443	320
Schritt 4.4	313	–	–	365	410	–	–	–	–	–	445	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.7	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 86

$f(x) = x^7 - 3x^6 - 4x^5 - 2x^4 + 9x^3 + 6x^2 + 17x - 6$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	34	36	41	36	40	40	37	48	38	45	38
Schritt 2.1	168	167	185	175	189	98	179	187	178	108	186
Schritt 2.2	197	208	217	195	190	–	179	221	178	–	186
Schritt 2.3	235	237	260	319	349	–	335	263	325	–	343
Schritt 2.4	–	–	–	349	350	–	335	–	377	–	400
Schritt 2.5	–	–	–	369	481	–	387	–	377	–	400
Schritt 2.6	–	–	–	–	481	–	–	–	–	–	–
Schritt 2.7	–	–	–	–	584	–	–	–	–	–	–
Schritt 2.8	–	–	–	–	585	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	620	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.11	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.12	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.6	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	236	238	261	370	621	98	388	264	378	108	402
Schritt 4.2	236	239	262	371	623	–	390	264	379	–	403
Schritt 4.3	–	–	–	372	625	–	391	–	380	–	404
Schritt 4.4	–	–	–	–	627	–	–	–	–	–	–
Schritt 4.5	–	–	–	–	628	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.7	–	–	–	–	–	–	–	–	–	–	–

Tabelle 87

$f(x) = x^7 + 29x^6 - 19x^5 + 18x^4 - 23x^3 + 25x^2 - 24x + 10$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	2	20	27	22	24	25	25	29	32	33	38	33
Schritt 2.1	137	138	160	160	160	68	159	175	182	179	98	181
Schritt 2.2	137	152	160	160	178	–	208	176	201	199	–	202
Schritt 2.3	166	237	208	211	221	–	209	326	326	330	–	343
Schritt 2.4	–	238	–	–	–	–	–	352	326	359	–	374
Schritt 2.5	–	257	–	–	–	–	–	379	426	379	–	395
Schritt 2.6	–	–	–	–	–	–	–	–	454	–	–	–
Schritt 2.7	–	–	–	–	–	–	–	–	454	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.11	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.12	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	216	257	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	311	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	217	312	209	213	222	68	209	380	456	381	99	396
Schritt 4.2	217	313	209	213	223	–	210	381	457	382	–	397
Schritt 4.3	–	314	–	–	–	–	–	382	458	383	–	398
Schritt 4.4	–	–	–	–	–	–	–	–	460	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.7	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 88

$f(x) = x^7 + 29x^6 - 19x^5 + 18x^4 - 23x^3 + 25x^2 - 24x + 10$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	34	38	42	39	41	43	39	42	41	48	42
Schritt 2.1	90	193	189	187	190	192	192	104	198	115	195
Schritt 2.2	–	237	247	210	213	216	213	–	199	–	230
Schritt 2.3	–	331	270	344	270	357	266	–	354	–	277
Schritt 2.4	–	332	–	344	–	357	–	–	375	–	–
Schritt 2.5	–	354	–	460	–	402	–	–	486	–	–
Schritt 2.6	–	–	–	460	–	–	–	–	487	–	–
Schritt 2.7	–	–	–	492	–	–	–	–	520	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.11	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.12	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.6	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	91	354	271	493	271	403	267	104	522	116	278
Schritt 4.2	–	355	272	495	272	405	268	–	523	–	279
Schritt 4.3	–	356	–	496	–	406	–	–	525	–	–
Schritt 4.4	–	–	–	497	–	–	–	–	526	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.7	–	–	–	–	–	–	–	–	–	–	–

Tabelle 89

$f(x) = x^7 + 23x^6 + 12x^5 + 21x^4 + 5x^3 - 3x^2 - 16x + 12$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	2	19	27	20	26	24	24	28	33	33	38	34
Schritt 2.1	153	105	149	150	152	152	149	75	166	167	180	173
Schritt 2.2	153	106	149	151	152	169	228	–	166	196	180	222
Schritt 2.3	184	177	191	284	289	287	229	–	306	299	325	287
Schritt 2.4	–	177	–	315	409	305	327	–	343	318	368	287
Schritt 2.5	–	191	–	330	409	330	345	–	404	337	431	287
Schritt 2.6	–	–	–	–	409	–	362	–	404	–	431	–
Schritt 2.7	–	–	–	–	445	–	379	–	405	–	431	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.11	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.12	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	235	249	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	363	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	236	364	192	331	447	331	381	75	406	338	433	288
Schritt 4.2	237	366	193	331	448	332	382	–	407	340	434	289
Schritt 4.3	–	367	–	332	450	333	383	–	408	341	435	291
Schritt 4.4	–	–	–	–	450	–	384	–	410	–	437	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.7	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 90

$f(x) = x^7 + 23x^6 + 12x^5 + 21x^4 + 5x^3 - 3x^2 - 16x + 12$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	34	38	42	39	43	43	38	43	39	55	43
Schritt 2.1	179	181	187	185	107	184	170	200	191	205	193
Schritt 2.2	199	213	242	205	–	219	170	200	192	273	225
Schritt 2.3	249	325	263	335	–	263	319	328	251	273	332
Schritt 2.4	–	356	–	335	–	–	340	328	–	–	364
Schritt 2.5	–	357	–	379	–	–	379	439	–	–	364
Schritt 2.6	–	–	–	–	–	–	–	461	–	–	–
Schritt 2.7	–	–	–	–	–	–	–	520	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	520	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	520	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.11	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.12	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	579	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	637	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	637	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	689	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.6	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	250	358	264	381	107	265	381	691	253	274	365
Schritt 4.2	251	359	265	382	–	265	382	692	254	275	366
Schritt 4.3	–	360	–	383	–	–	383	694	–	–	368
Schritt 4.4	–	–	–	–	–	–	–	695	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	697	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.7	–	–	–	–	–	–	–	–	–	–	–

Tabelle 91

$f(x) = x^7 - 6x^6 - 9x^5 + 21x^4 + 29x^3 - 15x - 13$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	2	20	26	19	23	24	26	28	32	33	36	34
Schritt 2.1	126	133	59	133	63	149	157	157	167	162	90	162
Schritt 2.2	203	160	–	170	–	164	190	158	213	163	–	162
Schritt 2.3	203	179	–	185	–	274	215	306	231	312	–	301
Schritt 2.4	224	–	–	–	–	274	–	349	–	349	–	319
Schritt 2.5	224	–	–	–	–	308	–	349	–	367	–	358
Schritt 2.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.7	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.11	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.12	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	283	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	283	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	370	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	371	180	60	186	63	309	216	351	231	369	90	360
Schritt 4.2	372	181	–	187	–	310	217	351	232	370	–	361
Schritt 4.3	373	–	–	–	–	311	–	352	–	371	–	362
Schritt 4.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.7	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 92

$f(x) = x^7 - 6x^6 - 9x^5 + 21x^4 + 29x^3 - 15x - 13$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	34	36	41	38	41	42	37	42	38	46	42
Schritt 2.1	167	191	182	93	188	185	175	187	92	190	187
Schritt 2.2	194	211	182	–	209	185	206	188	–	190	230
Schritt 2.3	294	260	247	–	340	337	246	337	–	341	316
Schritt 2.4	312	–	–	–	360	358	–	381	–	341	316
Schritt 2.5	330	–	–	–	391	471	–	401	–	398	381
Schritt 2.6	–	–	–	–	–	471	–	–	–	–	381
Schritt 2.7	–	–	–	–	–	555	–	–	–	–	381
Schritt 2.8	–	–	–	–	–	575	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	575	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.11	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.12	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.6	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	331	261	248	93	392	576	247	402	93	399	382
Schritt 4.2	332	262	249	–	394	578	247	403	–	401	383
Schritt 4.3	334	–	–	–	395	580	–	404	–	402	385
Schritt 4.4	–	–	–	–	–	581	–	–	–	–	386
Schritt 4.5	–	–	–	–	–	583	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.7	–	–	–	–	–	–	–	–	–	–	–

Tabelle 93

$f(x) = x^7 - 7x^6 + 13x^5 - 8x^4 - 18x^3 - 3x^2 - 15x + 1$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	2	20	26	19	23	23	24	27	37	38	37	32
Schritt 2.1	117	132	144	126	152	149	148	148	167	173	167	176
Schritt 2.2	129	159	165	126	168	224	164	202	204	211	208	176
Schritt 2.3	242	229	193	258	278	242	281	202	280	288	284	294
Schritt 2.4	243	230	–	289	279	340	295	–	299	288	284	313
Schritt 2.5	268	243	–	303	376	367	374	–	299	307	303	342
Schritt 2.6	–	–	–	–	393	367	389	–	–	–	–	–
Schritt 2.7	–	–	–	–	409	367	389	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.11	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.12	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–	394
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	269	243	194	305	410	368	390	203	299	308	304	395
Schritt 4.2	270	244	195	306	411	369	391	204	300	310	305	397
Schritt 4.3	271	245	–	307	413	371	393	–	301	311	307	398
Schritt 4.4	–	–	–	–	414	372	394	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.7	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 94

$f(x) = x^7 - 7x^6 + 13x^5 - 8x^4 - 18x^3 - 3x^2 - 15x + 1$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	32	36	40	37	41	41	38	41	37	45	41
Schritt 2.1	168	171	177	174	178	191	181	174	170	195	99
Schritt 2.2	187	232	177	204	233	223	181	226	201	239	–
Schritt 2.3	311	232	241	243	254	269	328	247	305	273	–
Schritt 2.4	330	–	–	–	–	–	348	–	305	–	–
Schritt 2.5	411	–	–	–	–	–	451	–	334	–	–
Schritt 2.6	411	–	–	–	–	–	479	–	–	–	–
Schritt 2.7	431	–	–	–	–	–	480	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.11	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.12	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.6	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	432	233	243	245	254	270	481	247	336	274	100
Schritt 4.2	434	235	244	245	255	271	483	248	337	275	–
Schritt 4.3	435	–	–	–	–	–	484	–	338	–	–
Schritt 4.4	436	–	–	–	–	–	485	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.7	–	–	–	–	–	–	–	–	–	–	–

Tabelle 95

$f(x) = x^7 + 22x^6 + 28x^5 - 13x^4 + 26x^3 - 19x^2 - 28x + 2$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	2	21	27	21	25	25	25	29	33	32	37	33
Schritt 2.1	138	51	168	132	69	67	154	149	161	169	180	169
Schritt 2.2	138	–	266	133	–	–	154	149	216	208	222	218
Schritt 2.3	168	–	288	258	–	–	194	200	216	236	304	278
Schritt 2.4	–	–	314	274	–	–	–	–	–	–	304	278
Schritt 2.5	–	–	315	308	–	–	–	–	–	–	324	278
Schritt 2.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.7	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.11	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.12	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	219	–	315	–	–	–	248	–	–	–	–	–
Schritt 3.2	–	–	315	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	367	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	220	51	367	309	69	67	249	201	217	237	325	279
Schritt 4.2	221	–	368	310	–	–	249	202	218	238	326	280
Schritt 4.3	–	–	370	310	–	–	–	–	–	–	327	281
Schritt 4.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.7	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 96

$f(x) = x^7 + 22x^6 + 28x^5 - 13x^4 + 26x^3 - 19x^2 - 28x + 2$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	33	38	41	38	41	45	37	42	40	47	43
Schritt 2.1	167	197	189	176	183	197	173	191	191	206	214
Schritt 2.2	214	249	189	176	204	218	327	192	212	241	215
Schritt 2.3	272	269	333	319	337	273	328	349	346	356	393
Schritt 2.4	272	–	333	320	383	–	328	371	387	391	435
Schritt 2.5	272	–	387	370	384	–	379	482	387	391	457
Schritt 2.6	–	–	–	–	–	–	–	482	–	–	–
Schritt 2.7	–	–	–	–	–	–	–	573	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	596	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	596	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.11	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.12	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.6	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	272	269	388	372	386	275	380	598	388	392	459
Schritt 4.2	273	270	390	374	386	275	381	599	389	393	460
Schritt 4.3	274	–	391	374	388	–	382	601	391	394	461
Schritt 4.4	–	–	–	–	–	–	–	602	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	603	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.7	–	–	–	–	–	–	–	–	–	–	–

Tabelle 97

$f(x) = x^7 + 6x^6 - 15x^5 - 19x^4 - 5x^3 - 16x^2 + 19x + 10$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	2	20	27	20	24	24	24	29	33	32	37	33
Schritt 2.1	124	128	147	148	144	143	149	165	170	183	190	172
Schritt 2.2	195	151	148	171	193	177	175	165	170	233	190	172
Schritt 2.3	195	183	284	262	193	252	210	279	226	254	363	322
Schritt 2.4	221	–	284	279	–	252	–	279	–	–	402	340
Schritt 2.5	234	–	322	294	–	269	–	379	–	–	421	376
Schritt 2.6	–	–	–	–	–	–	–	379	–	–	–	–
Schritt 2.7	–	–	–	–	–	–	–	459	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	460	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	525	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	526	–	–	–	–
Schritt 2.11	–	–	–	–	–	–	–	526	–	–	–	–
Schritt 2.12	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	583	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	644	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	706	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	767	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	822	–	–	–	–
Schritt 3.6	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	235	184	323	295	193	270	211	824	228	254	423	377
Schritt 4.2	235	185	325	297	194	271	212	826	228	255	424	379
Schritt 4.3	236	–	325	298	–	272	–	828	–	–	425	379
Schritt 4.4	–	–	–	–	–	–	–	829	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	831	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	833	–	–	–	–
Schritt 4.7	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 98

$f(x) = x^7 + 6x^6 - 15x^5 - 19x^4 - 5x^3 - 16x^2 + 19x + 10$

Primzahl	41	43	47	53	59	61	67	71
Schritt 1	34	37	41	38	42	43	39	42
Schritt 2.1	175	172	102	176	190	191	191	188
Schritt 2.2	231	191	–	176	190	225	212	188
Schritt 2.3	231	316	–	329	258	270	343	340
Schritt 2.4	–	357	–	379	–	–	374	341
Schritt 2.5	–	357	–	379	–	–	394	467
Schritt 2.6	–	–	–	–	–	–	–	467
Schritt 2.7	–	–	–	–	–	–	–	574
Schritt 2.8	–	–	–	–	–	–	–	605
Schritt 2.9	–	–	–	–	–	–	–	605
Schritt 2.10	–	–	–	–	–	–	–	–
Schritt 2.11	–	–	–	–	–	–	–	–
Schritt 2.12	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–
Schritt 3.6	–	–	–	–	–	–	–	–
Schritt 4.1	231	358	103	381	260	271	396	606
Schritt 4.2	232	359	–	382	260	272	397	608
Schritt 4.3	–	361	–	383	–	–	398	610
Schritt 4.4	–	–	–	–	–	–	–	611
Schritt 4.5	–	–	–	–	–	–	–	612
Schritt 4.6	–	–	–	–	–	–	–	–
Schritt 4.7	–	–	–	–	–	–	–	–

Tabelle 99

$f(x) = x^8 + 10x^7 + 24x^6 + 29x^5 - 16x^4 - 12x^3 - 17$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	27	35	45	52	40	41	39	47	55	54	62	57
Schritt 2.1	180	204	239	264	234	236	241	260	265	260	276	266
Schritt 2.2	205	252	310	417	234	236	241	310	304	348	330	266
Schritt 2.3	246	280	310	418	394	456	398	455	367	348	480	505
Schritt 2.4	–	–	–	438	394	523	431	456	–	549	572	505
Schritt 2.5	–	–	–	479	439	523	508	564	–	549	572	590
Schritt 2.6	–	–	–	–	–	–	509	588	–	549	598	–
Schritt 2.7	–	–	–	–	–	–	509	588	–	723	599	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	723	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	–	873	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	913	–	–
Schritt 2.11	–	–	–	–	–	–	–	–	–	913	–	–
Schritt 2.12	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	587	620	–	685	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	247	281	311	589	622	525	687	589	368	915	600	592
Schritt 4.2	248	282	312	591	624	526	688	591	369	917	602	595
Schritt 4.3	–	–	–	592	625	528	690	593	–	919	603	595
Schritt 4.4	–	–	–	–	–	–	692	595	–	921	605	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	922	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	924	–	–
Schritt 4.7	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 100

$f(x) = x^8 + 10x^7 + 24x^6 + 29x^5 - 16x^4 - 12x^3 - 17$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	54	61	73	64	72	69	63	70	65	78	72
Schritt 2.1	264	277	307	274	293	299	282	297	292	316	172
Schritt 2.2	318	277	366	316	293	359	380	341	378	414	–
Schritt 2.3	374	379	514	489	524	508	380	527	468	505	–
Schritt 2.4	–	–	514	544	599	537	–	570	469	505	–
Schritt 2.5	–	–	559	544	628	564	–	599	469	506	–
Schritt 2.6	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	375	381	560	546	631	566	381	600	470	507	173
Schritt 4.2	376	382	562	547	632	568	382	602	472	508	–
Schritt 4.3	–	–	563	549	633	569	–	603	473	510	–
Schritt 4.4	–	–	–	–	–	–	–	–	–	–	–

Tabelle 101

$f(x) = x^8 - 2x^7 - 13x^6 - 11x^5 + 18x^4 - 27x^3 + 8x^2 - 8x + 6$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	–	33	42	51	39	40	40	46	51	64	59	54
Schritt 2.1	156	212	228	273	244	255	269	269	268	309	288	294
Schritt 2.2	230	212	229	273	281	279	343	269	320	337	330	295
Schritt 2.3	230	274	447	343	345	352	428	488	464	550	401	547
Schritt 2.4	247	–	585	–	–	–	428	488	491	551	–	633
Schritt 2.5	247	–	606	–	–	–	428	559	518	619	–	633
Schritt 2.6	–	–	722	–	–	–	–	–	–	–	–	–
Schritt 2.7	–	–	745	–	–	–	–	–	–	–	–	–
Schritt 2.8	–	–	767	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	768	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	477	–	–	451	–	–	–	–	–	–	–	–
Schritt 3.2	542	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	714	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	716	275	770	453	346	354	428	561	519	621	403	635
Schritt 4.2	717	276	771	453	347	355	430	564	520	623	404	636
Schritt 4.3	719	–	773	–	–	–	432	564	522	624	–	638
Schritt 4.4	–	–	775	–	–	–	–	–	–	–	–	–
Schritt 4.5	–	–	776	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 102

$f(x) = x^8 - 2x^7 - 13x^6 - 11x^5 + 18x^4 - 27x^3 + 8x^2 - 8x + 6$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	64	62	67	63	68	70	61	69	65	77	71
Schritt 2.1	289	149	163	284	306	305	304	328	311	333	311
Schritt 2.2	332	–	–	328	411	394	305	391	374	432	372
Schritt 2.3	406	–	–	512	411	482	405	557	539	464	432
Schritt 2.4	–	–	–	553	–	482	–	589	586	–	–
Schritt 2.5	–	–	–	581	–	483	–	620	586	–	–
Schritt 2.6	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	408	149	163	582	412	483	407	622	588	465	434
Schritt 4.2	409	–	–	584	413	485	408	623	589	466	435
Schritt 4.3	–	–	–	585	–	487	–	624	591	–	–
Schritt 4.4	–	–	–	–	–	–	–	–	–	–	–

Tabelle 103

$f(x) = x^8 + 9x^7 - 5x^6 - 26x^5 + 26x^4 + 18x^3 + 18x^2 + 20x - 5$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	–	31	44	51	40	39	40	47	54	54	61	56
Schritt 2.1	193	216	220	232	238	233	279	279	279	275	162	271
Schritt 2.2	193	233	367	446	272	468	279	280	401	363	–	300
Schritt 2.3	248	285	367	512	431	544	533	486	428	391	–	534
Schritt 2.4	–	–	367	512	467	545	556	486	613	–	–	534
Schritt 2.5	–	–	408	512	490	545	728	660	614	–	–	600
Schritt 2.6	–	–	–	–	–	–	729	697	614	–	–	–
Schritt 2.7	–	–	–	–	–	–	776	722	763	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	805	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	806	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	590	–	–	–	–	824	–	–	–	–
Schritt 3.2	–	–	691	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	250	286	693	513	492	546	778	827	808	392	162	602
Schritt 4.2	250	287	695	514	493	547	780	829	810	393	–	604
Schritt 4.3	–	–	696	516	495	549	782	830	812	–	–	605
Schritt 4.4	–	–	–	–	–	–	784	832	814	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	816	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 104

$f(x) = x^8 + 9x^7 - 5x^6 - 26x^5 + 26x^4 + 18x^3 + 18x^2 + 20x - 5$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	56	67	70	63	70	70	62	69	70	77	71
Schritt 2.1	266	282	293	157	298	170	276	291	291	308	296
Schritt 2.2	267	344	293	–	344	–	305	292	292	309	296
Schritt 2.3	358	495	528	–	530	–	511	523	518	425	403
Schritt 2.4	–	495	528	–	590	–	511	567	573	–	–
Schritt 2.5	–	536	741	–	591	–	588	628	690	–	–
Schritt 2.6	–	–	742	–	–	–	–	–	718	–	–
Schritt 2.7	–	–	927	–	–	–	–	–	718	–	–
Schritt 2.8	–	–	928	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	986	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	361	537	988	157	592	171	589	630	720	427	406
Schritt 4.2	362	539	991	–	593	–	592	631	722	427	406
Schritt 4.3	–	541	993	–	595	–	593	632	723	–	–
Schritt 4.4	–	–	995	–	–	–	–	–	725	–	–
Schritt 4.5	–	–	997	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–

Tabelle 105

$f(x) = x^8 + 3x^7 + 29x^6 - 27x^5 - 29x^4 - 16x^3 - 27x + 12$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	–	31	45	51	38	40	40	46	52	54	60	53
Schritt 2.1	190	220	249	108	229	240	244	259	278	265	286	273
Schritt 2.2	265	220	306	–	276	323	244	332	354	291	287	299
Schritt 2.3	265	372	306	–	323	323	488	417	380	507	527	379
Schritt 2.4	318	456	–	–	–	–	488	418	–	571	597	–
Schritt 2.5	319	456	–	–	–	–	563	418	–	571	623	–
Schritt 2.6	–	485	–	–	–	–	–	–	–	–	–	–
Schritt 2.7	–	485	–	–	–	–	–	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	594	307	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	765	408	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	320	767	409	108	325	324	565	419	380	573	626	381
Schritt 4.2	321	769	410	–	326	325	567	420	381	574	627	382
Schritt 4.3	323	770	–	–	–	–	568	422	–	576	628	–
Schritt 4.4	–	772	–	–	–	–	–	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 106

$f(x) = x^8 + 3x^7 + 29x^6 - 27x^5 - 29x^4 - 16x^3 - 27x + 12$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	55	62	70	63	69	71	62	70	65	76	72
Schritt 2.1	273	283	292	154	303	302	285	305	301	310	170
Schritt 2.2	299	355	292	–	332	302	354	407	343	340	–
Schritt 2.3	499	484	547	–	547	548	473	407	412	574	–
Schritt 2.4	526	485	591	–	548	592	502	–	–	575	–
Schritt 2.5	671	513	731	–	735	743	502	–	–	652	–
Schritt 2.6	671	–	775	–	735	771	–	–	–	–	–
Schritt 2.7	793	–	775	–	879	801	–	–	–	–	–
Schritt 2.8	793	–	–	–	922	–	–	–	–	–	–
Schritt 2.9	820	–	–	–	922	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	822	514	777	155	924	803	503	408	414	654	170
Schritt 4.2	824	516	779	–	926	804	505	409	415	656	–
Schritt 4.3	827	517	780	–	929	806	507	–	–	657	–
Schritt 4.4	829	–	782	–	931	808	–	–	–	–	–
Schritt 4.5	831	–	–	–	932	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–

Tabelle 107

$f(x) = x^8 + 21x^7 + 24x^6 + 27x^5 - 24x^4 - 6x^3 - 22x^2 - 25x - 23$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	–	32	45	52	41	42	41	47	54	56	62	56
Schritt 2.1	71	210	234	249	233	112	238	262	257	279	296	140
Schritt 2.2	–	251	266	411	256	–	239	287	257	363	323	–
Schritt 2.3	–	393	320	432	327	–	461	507	489	389	541	–
Schritt 2.4	–	393	–	538	–	–	596	573	489	–	610	–
Schritt 2.5	–	423	–	559	–	–	621	573	698	–	610	–
Schritt 2.6	–	–	–	589	–	–	657	–	698	–	–	–
Schritt 2.7	–	–	–	590	–	–	679	–	764	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	71	424	321	591	329	112	682	575	767	389	612	140
Schritt 4.2	–	426	321	592	330	–	683	576	769	391	613	–
Schritt 4.3	–	427	–	593	–	–	685	578	771	–	615	–
Schritt 4.4	–	–	–	595	–	–	686	–	772	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 108

$f(x) = x^8 + 21x^7 + 24x^6 + 27x^5 - 24x^4 - 6x^3 - 22x^2 - 25x - 23$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	57	68	70	63	71	71	63	70	63	89	71
Schritt 2.1	268	287	286	278	302	303	154	307	268	317	305
Schritt 2.2	336	345	287	305	347	304	–	307	311	397	305
Schritt 2.3	447	491	527	520	521	547	–	548	481	444	549
Schritt 2.4	447	492	615	520	521	548	–	637	482	–	609
Schritt 2.5	474	601	616	591	664	640	–	637	626	–	727
Schritt 2.6	–	602	–	–	692	–	–	–	627	–	729
Schritt 2.7	–	686	–	–	721	–	–	–	670	–	758
Schritt 2.8	–	686	–	–	–	–	–	–	–	–	–
Schritt 2.9	–	686	–	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	475	688	618	594	722	642	154	639	672	446	760
Schritt 4.2	477	690	619	596	724	645	–	639	674	447	761
Schritt 4.3	478	692	620	597	726	646	–	641	676	–	764
Schritt 4.4	–	694	–	–	728	–	–	–	678	–	765
Schritt 4.5	–	696	–	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–

Tabelle 109

$f(x) = x^9 + 10x^8 + 24x^7 + 29x^6 - 16x^5 - 12x^4 - 16x - 3$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	49	49	68	80	59	62	60	71	82	83	93	84
Schritt 2.1	281	291	327	170	333	348	339	374	399	398	433	407
Schritt 2.2	313	292	366	–	374	424	427	441	449	451	433	408
Schritt 2.3	379	378	439	–	619	606	564	664	712	554	807	762
Schritt 2.4	–	–	–	–	649	607	564	697	797	–	808	798
Schritt 2.5	–	–	–	–	824	754	593	843	798	–	944	1073
Schritt 2.6	–	–	–	–	825	785	–	876	–	–	–	1143
Schritt 2.7	–	–	–	–	869	785	–	876	–	–	–	1177
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	380	379	441	170	871	787	594	878	800	556	947	1180
Schritt 4.2	381	380	442	–	873	789	597	880	801	557	950	1183
Schritt 4.3	–	–	–	–	876	791	598	882	803	–	951	1184
Schritt 4.4	–	–	–	–	878	793	–	885	–	–	–	1186
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 110

$f(x) = x^9 + 10x^8 + 24x^7 + 29x^6 - 16x^5 - 12x^4 - 16x - 3$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	84	96	108	110	108	109	98	108	100	119	110
Schritt 2.1	407	432	453	430	262	460	440	455	252	473	455
Schritt 2.2	550	433	538	586	–	545	441	525	–	474	455
Schritt 2.3	550	787	798	587	–	803	809	810	–	859	617
Schritt 2.4	–	925	838	–	–	804	848	876	–	964	–
Schritt 2.5	–	925	1003	–	–	889	1139	937	–	1027	–
Schritt 2.6	–	–	1004	–	–	–	1200	–	–	–	–
Schritt 2.7	–	–	1043	–	–	–	1259	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	551	928	1044	588	263	891	1262	939	253	1030	621
Schritt 4.2	553	929	1046	589	–	894	1265	941	–	1032	621
Schritt 4.3	–	931	1049	–	–	896	1267	943	–	1033	–
Schritt 4.4	–	–	1051	–	–	–	1269	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–

Tabelle 111

$f(x) = x^9 + 10x^8 + 6x^7 + 5x^6 + 15x^5 + 3x^4 + 29x^3 - 27x^2 - 29x - 17$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	50	49	70	96	61	73	62	75	88	85	97	85
Schritt 2.1	303	291	155	384	338	367	356	192	401	205	399	389
Schritt 2.2	363	325	–	454	339	444	480	–	523	–	473	442
Schritt 2.3	643	540	–	512	463	506	481	–	556	–	572	706
Schritt 2.4	664	540	–	–	–	–	–	–	–	–	–	795
Schritt 2.5	720	724	–	–	–	–	–	–	–	–	–	795
Schritt 2.6	–	759	–	–	–	–	–	–	–	–	–	–
Schritt 2.7	–	781	–	–	–	–	–	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	722	783	155	513	465	508	481	192	557	205	574	797
Schritt 4.2	724	785	–	514	466	509	483	–	558	–	575	799
Schritt 4.3	726	787	–	–	–	–	–	–	–	–	–	801
Schritt 4.4	–	789	–	–	–	–	–	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 112

$f(x) = x^9 + 10x^8 + 6x^7 + 5x^6 + 15x^5 + 3x^4 + 29x^3 - 27x^2 - 29x - 17$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	86	98	109	99	109	111	99	110	101	122	112
Schritt 2.1	427	452	261	456	455	467	436	457	458	471	456
Schritt 2.2	570	490	–	552	739	606	473	458	459	512	517
Schritt 2.3	571	805	–	751	840	727	786	862	838	897	638
Schritt 2.4	–	902	–	808	898	727	882	1002	838	898	–
Schritt 2.5	–	939	–	808	898	727	918	1002	1185	1043	–
Schritt 2.6	–	–	–	–	–	–	–	–	1185	–	–
Schritt 2.7	–	–	–	–	–	–	–	–	1474	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	1513	–	–
Schritt 2.9	–	–	–	–	–	–	–	–	1719	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	1719	–	–
Schritt 2.11	–	–	–	–	–	–	–	–	1776	–	–
Schritt 2.12	–	–	–	–	–	–	–	–	–	–	–
Schritt 2.13	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	572	942	261	810	900	728	921	1005	1779	1046	641
Schritt 4.2	573	943	–	812	901	730	923	1007	1782	1049	642
Schritt 4.3	–	945	–	814	903	733	925	1009	1785	1050	–
Schritt 4.4	–	–	–	–	–	–	–	–	1787	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	1790	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	1792	–	–
Schritt 4.7	–	–	–	–	–	–	–	–	–	–	–

Tabelle 113

$f(x) = x^9 - 27x^7 + 11x^6 + 21x^5 + 24x^4 + 27x^3 - 24x^2 - 6x - 23$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	51	49	72	83	63	64	66	76	88	89	99	89
Schritt 2.1	317	84	157	393	170	375	363	378	406	431	421	412
Schritt 2.2	366	–	–	420	–	407	444	499	460	505	422	508
Schritt 2.3	438	–	–	712	–	708	508	534	733	743	791	708
Schritt 2.4	–	–	–	712	–	709	–	–	734	744	830	762
Schritt 2.5	–	–	–	967	–	808	–	–	951	930	1120	762
Schritt 2.6	–	–	–	1025	–	–	–	–	1031	967	1158	–
Schritt 2.7	–	–	–	1141	–	–	–	–	1031	1002	1362	–
Schritt 2.8	–	–	–	1141	–	–	–	–	–	–	1363	–
Schritt 2.9	–	–	–	1141	–	–	–	–	–	–	1422	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	169	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	440	170	157	1144	171	810	510	535	1033	1004	1425	764
Schritt 4.2	441	–	–	1146	–	813	511	536	1036	1007	1427	765
Schritt 4.3	–	–	–	1148	–	814	–	–	1038	1009	1429	768
Schritt 4.4	–	–	–	1151	–	–	–	–	1041	1011	1432	–
Schritt 4.5	–	–	–	1153	–	–	–	–	–	–	1434	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 114

$f(x) = x^9 - 27x^7 + 11x^6 + 21x^5 + 24x^4 + 27x^3 - 24x^2 - 6x - 23$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	91	100	115	101	115	114	101	114	104	127	116
Schritt 2.1	405	244	441	439	474	465	440	463	446	523	466
Schritt 2.2	406	–	524	518	475	626	577	545	590	567	526
Schritt 2.3	740	–	772	759	850	626	615	798	708	900	822
Schritt 2.4	777	–	772	759	932	–	–	879	709	901	822
Schritt 2.5	892	–	855	835	1134	–	–	879	709	1036	1064
Schritt 2.6	–	–	–	–	1135	–	–	–	–	–	1224
Schritt 2.7	–	–	–	–	1197	–	–	–	–	–	1263
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	1300
Schritt 2.9	–	–	–	–	–	–	–	–	–	–	1300
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	895	245	857	837	1200	627	616	881	710	1038	1302
Schritt 4.2	898	–	860	839	1201	629	617	883	712	1041	1304
Schritt 4.3	899	–	862	841	1204	–	–	885	714	1042	1307
Schritt 4.4	–	–	–	–	1206	–	–	–	–	–	1309
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	1312
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–

Tabelle 115

$f(x) = x^9 + 5x^8 - 25x^7 + 6x^6 - 5x^5 + 6x^4 + 24x^3 - 29x^2 - 27x - 3$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	50	49	69	80	58	61	61	71	82	84	95	84
Schritt 2.1	306	332	145	170	344	159	347	356	393	426	439	216
Schritt 2.2	359	332	–	–	435	–	406	482	426	551	597	–
Schritt 2.3	401	620	–	–	477	–	612	482	728	551	597	–
Schritt 2.4	–	666	–	–	–	–	641	–	762	–	–	–
Schritt 2.5	–	702	–	–	–	–	782	–	849	–	–	–
Schritt 2.6	–	–	–	–	–	–	783	–	–	–	–	–
Schritt 2.7	–	–	–	–	–	–	811	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	882	–	–	–	–	–	–	–	551	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	731	–	–
Schritt 3.3	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	402	885	145	170	479	160	813	483	851	732	598	216
Schritt 4.2	404	886	–	–	480	–	815	484	854	735	599	–
Schritt 4.3	–	888	–	–	–	–	818	–	855	–	–	–
Schritt 4.4	–	–	–	–	–	–	820	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 116

$f(x) = x^9 + 5x^8 - 25x^7 + 6x^6 - 5x^5 + 6x^4 + 24x^3 - 29x^2 - 27x - 3$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	86	96	107	97	109	111	98	109	99	121	110
Schritt 2.1	441	421	437	445	469	470	430	449	439	465	265
Schritt 2.2	476	556	602	557	532	573	467	450	440	466	–
Schritt 2.3	775	671	603	611	657	769	813	821	811	831	–
Schritt 2.4	775	671	–	–	–	770	971	963	866	832	–
Schritt 2.5	1092	672	–	–	–	829	1009	963	1102	982	–
Schritt 2.6	1126	–	–	–	–	–	1085	–	1158	–	–
Schritt 2.7	1195	–	–	–	–	–	1086	–	1195	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	1198	673	604	612	659	831	1088	966	1198	985	265
Schritt 4.2	1200	675	605	613	660	833	1091	967	1200	988	–
Schritt 4.3	1203	677	–	–	–	835	1093	969	1202	989	–
Schritt 4.4	1205	–	–	–	–	–	1096	–	1204	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–

Tabelle 117

$f(x) = x^9 - 4x^8 - 9x^7 - 28x^6 + 16x^5 + 29x^4 + 17x^3 + 13x^2 + 24x - 23$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	50	49	70	94	61	61	74	70	88	83	95	86
Schritt 2.1	287	351	162	196	349	358	373	385	413	402	437	411
Schritt 2.2	288	351	–	–	378	473	405	481	414	403	595	485
Schritt 2.3	378	442	–	–	679	474	719	530	802	745	595	720
Schritt 2.4	–	–	–	–	679	775	798	–	803	869	–	791
Schritt 2.5	–	–	–	–	771	776	830	–	1126	869	–	791
Schritt 2.6	–	–	–	–	–	776	–	–	1214	–	–	–
Schritt 2.7	–	–	–	–	–	867	–	–	1248	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	380	444	163	197	773	870	832	532	1251	872	596	793
Schritt 4.2	381	445	–	–	776	873	834	533	1254	873	598	795
Schritt 4.3	–	–	–	–	778	876	836	–	1256	875	–	797
Schritt 4.4	–	–	–	–	–	877	–	–	1258	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 118

$f(x) = x^9 - 4x^8 - 9x^7 - 28x^6 + 16x^5 + 29x^4 + 17x^3 + 13x^2 + 24x - 23$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	86	97	107	98	110	111	99	110	99	122	110
Schritt 2.1	423	478	453	438	262	503	439	470	426	475	471
Schritt 2.2	424	534	614	439	–	503	594	512	426	518	554
Schritt 2.3	791	777	615	590	–	915	595	851	581	674	811
Schritt 2.4	893	835	–	–	–	915	–	890	–	–	851
Schritt 2.5	949	958	–	–	–	1069	–	1136	–	–	1025
Schritt 2.6	–	959	–	–	–	–	–	1196	–	–	1064
Schritt 2.7	–	959	–	–	–	–	–	1317	–	–	1065
Schritt 2.8	–	–	–	–	–	–	–	1317	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	1317	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	959	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	959	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	1159	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	952	1161	616	593	262	1072	596	1320	584	677	1066
Schritt 4.2	953	1163	617	594	–	1075	597	1323	585	678	1068
Schritt 4.3	955	1165	–	–	–	1076	–	1325	–	–	1070
Schritt 4.4	–	1168	–	–	–	–	–	1328	–	–	1073
Schritt 4.5	–	–	–	–	–	–	–	1330	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–

Tabelle 119

$f(x) = x^9 - 6x^8 + 24x^7 + 23x^6 - 2x^5 + 21x^4 + 6x^3 - 1x^2 + 5x - 21$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	49	52	68	80	59	60	62	73	84	84	94	84
Schritt 2.1	230	371	382	390	359	361	348	366	429	223	429	442
Schritt 2.2	231	570	409	390	436	393	348	367	541	–	506	499
Schritt 2.3	266	570	692	510	497	710	709	695	593	–	766	806
Schritt 2.4	–	642	758	–	–	710	822	730	–	–	843	934
Schritt 2.5	–	698	873	–	–	967	823	1000	–	–	843	935
Schritt 2.6	–	–	873	–	–	1190	–	1037	–	–	–	1140
Schritt 2.7	–	–	874	–	–	1337	–	1110	–	–	–	1140
Schritt 2.8	–	–	–	–	–	1370	–	–	–	–	–	1140
Schritt 2.9	–	–	–	–	–	1371	–	–	–	–	–	1307
Schritt 2.10	–	–	–	–	–	1405	–	–	–	–	–	1308
Schritt 2.11	–	–	–	–	–	1405	–	–	–	–	–	1347
Schritt 2.12	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	812	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	814	700	876	512	498	1408	826	1113	594	223	845	1349
Schritt 4.2	816	701	877	513	500	1411	827	1116	596	–	847	1352
Schritt 4.3	–	703	879	–	–	1413	829	1118	–	–	849	1355
Schritt 4.4	–	–	882	–	–	1416	–	1120	–	–	–	1358
Schritt 4.5	–	–	–	–	–	1418	–	–	–	–	–	1361
Schritt 4.6	–	–	–	–	–	1421	–	–	–	–	–	1363
Schritt 4.7	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 120

$f(x) = x^9 - 6x^8 + 24x^7 + 23x^6 - 2x^5 + 21x^4 + 6x^3 - 1x^2 + 5x - 21$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	88	99	108	99	110	110	99	113	99	122	111
Schritt 2.1	455	515	495	484	528	494	477	478	447	556	274
Schritt 2.2	597	572	673	541	529	494	555	478	447	599	–
Schritt 2.3	598	852	673	822	981	940	804	892	841	755	–
Schritt 2.4	–	914	–	928	982	1008	804	979	901	–	–
Schritt 2.5	–	973	–	929	1125	1284	1036	1067	1167	–	–
Schritt 2.6	–	–	–	–	–	1349	1036	–	1167	–	–
Schritt 2.7	–	–	–	–	–	1492	1101	–	1247	–	–
Schritt 2.8	–	–	–	–	–	1492	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	1493	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	599	975	673	931	1128	1495	1102	1070	1250	758	274
Schritt 4.2	600	977	675	933	1131	1497	1105	1072	1252	759	–
Schritt 4.3	–	979	–	935	1132	1499	1109	1074	1255	–	–
Schritt 4.4	–	–	–	–	–	1502	1111	–	1257	–	–
Schritt 4.5	–	–	–	–	–	1504	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–

Tabelle 121

$f(x) = x^9 + 9x^8 - 11x^7 - 24x^6 - 17x^5 + 20x^4 + 20x^3 + 18x^2 + 10$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	50	50	70	82	60	60	63	75	83	86	97	86
Schritt 2.1	248	121	347	354	342	352	349	369	385	386	425	406
Schritt 2.2	357	–	545	396	342	415	380	452	386	387	464	497
Schritt 2.3	358	–	546	653	668	644	485	661	747	742	784	694
Schritt 2.4	392	–	678	759	669	709	–	695	783	742	785	695
Schritt 2.5	392	–	678	760	777	709	–	728	1050	1058	899	748
Schritt 2.6	–	–	735	814	–	–	–	–	1104	1058	–	–
Schritt 2.7	–	–	859	814	–	–	–	–	1157	1328	–	–
Schritt 2.8	–	–	860	–	–	–	–	–	–	1384	–	–
Schritt 2.9	–	–	860	–	–	–	–	–	–	1535	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	1535	–	–
Schritt 2.11	–	–	–	–	–	–	–	–	–	1569	–	–
Schritt 2.12	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	879	–	1045	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	881	121	1048	816	781	711	488	730	1159	1572	901	750
Schritt 4.2	883	–	1050	818	784	712	489	732	1162	1575	904	752
Schritt 4.3	885	–	1052	820	785	715	–	734	1164	1578	905	754
Schritt 4.4	–	–	1054	823	–	–	–	–	1166	1580	–	–
Schritt 4.5	–	–	1056	–	–	–	–	–	–	1583	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	1586	–	–
Schritt 4.7	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 122

$f(x) = x^9 + 9x^8 - 11x^7 - 24x^6 - 17x^5 + 20x^4 + 20x^3 + 18x^2 + 10$

Primzahl	41	43	47	53	59	61	67	71	73	79	83
Schritt 1	88	96	110	99	108	109	99	110	101	125	111
Schritt 2.1	400	421	446	415	491	510	452	486	455	508	500
Schritt 2.2	455	460	550	415	492	510	452	487	455	552	500
Schritt 2.3	567	793	761	766	889	923	842	916	618	945	679
Schritt 2.4	–	890	802	805	926	1065	919	955	–	945	–
Schritt 2.5	–	927	842	1084	1211	1065	1131	1077	–	1085	–
Schritt 2.6	–	–	–	1175	1212	–	1193	–	–	–	–
Schritt 2.7	–	–	–	1175	1314	–	1193	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	569	929	843	1178	1317	1068	1196	1080	621	1088	682
Schritt 4.2	571	931	845	1181	1319	1069	1198	1083	622	1091	683
Schritt 4.3	–	933	847	1182	1321	1071	1200	1084	–	1092	–
Schritt 4.4	–	–	–	1185	1323	–	1203	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–

Tabelle 123

$f(x) = x^{10} + x^9 + 5x^8 - 5x^7 - 4x^6 + 23x^5 - 7x^4 + 23x^3 - 7x^2 + 21x + 2$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	77	119	107	123	92	100	90	110	126	124	140	126
Schritt 2.1	436	554	485	518	497	546	516	590	608	574	631	310
Schritt 2.2	436	555	517	640	497	675	689	590	676	575	632	–
Schritt 2.3	563	955	900	698	945	951	729	1106	1094	1085	1144	–
Schritt 2.4	–	955	935	–	1079	995	–	1107	1238	1154	1320	–
Schritt 2.5	–	1309	1036	–	1118	1150	–	1276	1239	1525	1371	–
Schritt 2.6	–	1526	–	–	–	1150	–	–	–	1628	–	–
Schritt 2.7	–	1527	–	–	–	1150	–	–	–	1793	–	–
Schritt 2.8	–	1709	–	–	–	–	–	–	–	1794	–	–
Schritt 2.9	–	1710	–	–	–	–	–	–	–	1794	–	–
Schritt 2.10	–	1756	–	–	–	–	–	–	–	–	–	–
Schritt 2.11	–	1789	–	–	–	–	–	–	–	–	–	–
Schritt 2.12	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	2134	–	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	2473	–	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	2809	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	3126	–	–	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	566	3130	1039	700	1122	1152	730	1280	1241	1798	1374	310
Schritt 4.2	568	3133	1042	701	1124	1155	732	1284	1242	1801	1376	–
Schritt 4.3	–	3136	1043	–	1126	1158	–	1285	1245	1803	1378	–
Schritt 4.4	–	3139	–	–	–	1161	–	–	–	1806	–	–
Schritt 4.5	–	3142	–	–	–	–	–	–	–	1810	–	–
Schritt 4.6	–	3145	–	–	–	–	–	–	–	–	–	–
Schritt 4.7	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 124

$f(x) = x^{10} + x^9 + 5x^8 - 5x^7 - 4x^6 + 23x^5 - 7x^4 + 23x^3 - 7x^2 + 21x + 2$

Primzahl	41	43	47	53	59	61	67	71	73	79	83	89
Schritt 1	126	145	161	145	166	171	148	170	162	190	166	170
Schritt 2.1	593	628	390	637	727	680	653	691	674	727	686	712
Schritt 2.2	813	679	–	637	834	680	727	776	883	941	742	830
Schritt 2.3	813	1172	–	1189	1228	1224	1164	1233	932	1031	1269	1255
Schritt 2.4	–	1358	–	1396	1362	1305	1294	1394	–	–	1376	1338
Schritt 2.5	–	1358	–	1396	1362	1687	1347	1394	–	–	1658	1421
Schritt 2.6	–	–	–	–	–	1687	–	–	–	–	1710	–
Schritt 2.7	–	–	–	–	–	1824	–	–	–	–	1764	–
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	814	1362	390	1400	1365	1828	1350	1397	933	1033	1768	1423
Schritt 4.2	816	1363	–	1401	1367	1831	1352	1399	935	1035	1770	1425
Schritt 4.3	–	1366	–	1404	1370	1835	1355	1402	–	–	1773	1428
Schritt 4.4	–	–	–	–	–	1837	–	–	–	–	1776	–
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 125

$f(x) = x^{10} - 4x^9 + 22x^8 - 7x^7 - 17x^6 - 6x^5 - 28x^4 + 15x^3 - 10x^2 + 1$

Primzahl	2	3	5	7	11	13	17	19	23	29	31	37
Schritt 1	81	118	108	130	95	103	102	118	149	134	151	131
Schritt 2.1	468	504	546	269	528	518	267	571	635	333	620	614
Schritt 2.2	468	504	686	–	674	586	–	615	736	–	669	614
Schritt 2.3	599	863	687	–	740	1000	–	785	1086	–	1139	1119
Schritt 2.4	–	1161	–	–	–	1085	–	–	1210	–	1320	1166
Schritt 2.5	–	1192	–	–	–	1147	–	–	1210	–	1321	1594
Schritt 2.6	–	1193	–	–	–	–	–	–	–	–	–	1748
Schritt 2.7	–	1260	–	–	–	–	–	–	–	–	–	1748
Schritt 2.8	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	1604	687	–	–	–	–	–	–	–	–	–
Schritt 3.2	–	1835	1007	–	–	–	–	–	–	–	–	–
Schritt 3.3	–	2404	–	–	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	602	2407	1009	269	742	1150	267	789	1212	333	1324	1752
Schritt 4.2	603	2410	1011	–	744	1153	–	790	1214	–	1325	1756
Schritt 4.3	–	2413	–	–	–	1155	–	–	1218	–	1328	1757
Schritt 4.4	–	2415	–	–	–	–	–	–	–	–	–	1760
Schritt 4.5	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 126

$f(x) = x^{10} - 4x^9 + 22x^8 - 7x^7 - 17x^6 - 6x^5 - 28x^4 + 15x^3 - 10x^2 + 1$

Primzahl	41	43	47	53	59	61	67	71	73	79	83	89
Schritt 1	134	154	168	155	177	172	155	177	166	202	178	179
Schritt 2.1	628	368	397	677	710	659	668	674	668	729	715	698
Schritt 2.2	681	–	–	755	852	923	668	756	854	851	766	699
Schritt 2.3	1143	–	–	1196	1209	923	1246	1197	935	1262	1260	948
Schritt 2.4	1291	–	–	1197	1263	–	1385	1197	–	1263	1313	–
Schritt 2.5	1343	–	–	1586	1347	–	1490	1600	–	1420	1697	–
Schritt 2.6	–	–	–	1686	–	–	–	1657	–	–	1777	–
Schritt 2.7	–	–	–	1847	–	–	–	1774	–	–	1857	–
Schritt 2.8	–	–	–	1847	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	1847	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–	–	–	–	–
Schritt 4.1	1347	369	397	1850	1349	924	1494	1777	937	1423	1860	952
Schritt 4.2	1349	–	–	1854	1352	926	1496	1780	938	1426	1863	953
Schritt 4.3	1352	–	–	1856	1354	–	1498	1785	–	1428	1866	–
Schritt 4.4	–	–	–	1860	–	–	–	1787	–	–	1869	–
Schritt 4.5	–	–	–	1864	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–	–	–	–	–

Tabelle 127

$f(x) = x^{30} + x^{29} + x^{28} + \ldots + x + 1$

Primzahl	2	3	5	7	11	13	17
Schritt 1	67628	8933	11869	8015	11013	11006	11065
Schritt 2.1	86648	14933	32726	30954	20372	20307	20382
Schritt 2.2	100010	–	40542	36608	–	–	–
Schritt 2.3	101347	–	41566	42138	–	–	–
Schritt 2.4	114817	–	63217	–	–	–	–
Schritt 2.5	116190	–	64240	–	–	–	–
Schritt 2.6	126322	–	65262	–	–	–	–
Schritt 2.7	127676	–	84232	–	–	–	–
Schritt 2.8	137710	–	92009	–	–	–	–
Schritt 2.9	139056	–	93043	–	–	–	–
Schritt 2.10	140389	–	107824	–	–	–	–
Schritt 2.11	141737	–	117603	–	–	–	–
Schritt 2.12	–	–	118666	–	–	–	–
Schritt 2.13	–	–	119711	–	–	–	–
Schritt 2.14	–	–	127461	–	–	–	–
Schritt 2.15	–	–	128487	–	–	–	–
Schritt 2.16	–	–	136111	–	–	–	–
Schritt 2.17	–	–	137111	–	–	–	–
Schritt 2.18	–	–	138155	–	–	–	–
Schritt 2.19	–	–	139183	–	–	–	–
Schritt 2.20	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–
Schritt 4.1	141781	14940	139247	42169	20379	20314	20388
Schritt 4.2	141818	–	139310	42188	–	–	–
Schritt 4.3	141863	–	139373	–	–	–	–
Schritt 4.4	141906	–	139434	–	–	–	–
Schritt 4.5	141953	–	139496	–	–	–	–
Schritt 4.6	141989	–	139555	–	–	–	–
Schritt 4.7	–	–	139615	–	–	–	–
Schritt 4.8	–	–	139676	–	–	–	–
Schritt 4.9	–	–	139734	–	–	–	–
Schritt 4.10	–	–	139796	–	–	–	–
Schritt 4.11	–	–	–	–	–	–	–

Tabelle 128

$f(x) = x^{40} + x^{39} + x^{38} + \ldots + x + 1$

Primzahl	2	3	5	7	11	13	17
Schritt 1	278361	29127	38938	26072	35770	35776	35742
Schritt 2.1	334555	90640	104059	54039	64880	64576	64536
Schritt 2.2	346463	125830	119178	–	–	–	–
Schritt 2.3	358303	131160	134291	–	–	–	–
Schritt 2.4	–	178370	–	–	–	–	–
Schritt 2.5	–	213363	–	–	–	–	–
Schritt 2.6	–	218748	–	–	–	–	–
Schritt 2.7	–	224205	–	–	–	–	–
Schritt 2.8	–	229663	–	–	–	–	–
Schritt 2.9	–	235148	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–
Schritt 4.1	358353	235261	134354	54055	64896	64592	64553
Schritt 4.2	358392	235358	134393	–	–	–	–
Schritt 4.3	–	235463	–	–	–	–	–
Schritt 4.4	–	235556	–	–	–	–	–
Schritt 4.5	–	235655	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–

Tabelle 129

$f(x) = x^{52} + x^{51} + \ldots + x + 1$

Primzahl	2	3	5	7	11
Schritt 1	992883	81295	109138	126292	99416
Schritt 2.1	1035317	131712	169385	314384	294762
Schritt 2.2	–	–	–	361064	345813
Schritt 2.3	–	–	–	407618	399581
Schritt 2.4	–	–	–	–	–
Schritt 3.1	–	–	–	–	–
Schritt 4.1	1035351	131745	169419	407753	399722
Schritt 4.2	–	–	–	407829	399803
Schritt 4.3	–	–	–	–	–

Tabelle 130a

$f(x) = x^{70} + x^{69} + \ldots + x + 1$

Primzahl	2	3	5	7	11	13	17
Schritt 1	–	275676	367460	430707	338765	338769	338897
Schritt 2.1	–	825871	925797	659023	606413	607270	971517
Schritt 2.2	–	946076	1175644	–	–	–	1020315
Schritt 2.3	–	1069472	1195409	–	–	–	1688903
Schritt 2.4	–	–	1701153	–	–	–	1737067
Schritt 2.5	–	–	1949768	–	–	–	2307221
Schritt 2.6	–	–	1970435	–	–	–	2356207
Schritt 2.7	–	–	2180887	–	–	–	2838833
Schritt 2.8	–	–	2343821	–	–	–	2889321
Schritt 2.9	–	–	2363963	–	–	–	3268582
Schritt 2.10	–	–	2695996	–	–	–	3317348
Schritt 2.11	–	–	2715997	–	–	–	3583440
Schritt 2.12	–	–	2918421	–	–	–	3631874
Schritt 2.13	–	–	2938358	–	–	–	3680206
Schritt 2.14	–	–	2958086	–	–	–	–
Schritt 2.15	–	–	2977628	–	–	–	–
Schritt 2.16	–	–	3264410	–	–	–	–
Schritt 2.17	–	–	3284124	–	–	–	–
Schritt 2.18	–	–	3441384	–	–	–	–
Schritt 2.19	–	–	3461388	–	–	–	–
Schritt 2.20	–	–	3720901	–	–	–	–
Schritt 2.21	–	–	3741032	–	–	–	–
Schritt 2.22	–	–	3761281	–	–	–	–
Schritt 2.23	–	–	3963632	–	–	–	–
Schritt 2.24	–	–	3983978	–	–	–	–
Schritt 2.25	–	–	4154431	–	–	–	–
Schritt 2.26	–	–	4174861	–	–	–	–
Schritt 2.27	–	–	4195350	–	–	–	–
Schritt 2.28	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–

Tabelle 130b

$f(x) = x^{70} + x^{69} + \ldots + x + 1$

Schritt 4.1	–	1069765	4196122	659102	606493	607350	3680931
Schritt 4.2	–	1069948	4196850	–	–	–	3681650
Schritt 4.3	–	–	4197612	–	–	–	3682369
Schritt 4.4	–	–	4198305	–	–	–	3683065
Schritt 4.5	–	–	4199025	–	–	–	3683755
Schritt 4.6	–	–	4199784	–	–	–	3684437
Schritt 4.7	–	–	4200545	–	–	–	3685115
Schritt 4.8	–	–	4201227	–	–	–	–
Schritt 4.9	–	–	4201966	–	–	–	–
Schritt 4.10	–	–	4202643	–	–	–	–
Schritt 4.11	–	–	4203360	–	–	–	–
Schritt 4.12	–	–	4204037	–	–	–	–
Schritt 4.13	–	–	4204686	–	–	–	–
Schritt 4.14	–	–	4205383	–	–	–	–
Schritt 4.15	–	–	–	–	–	–	–

Tabelle 131

$f(x) = x^{82} + x^{81} + \ldots + x + 1$

Primzahl	2	3	5	7	11	13	17
Schritt 1	9408466	751543	693519	810118	634869	636836	637240
Schritt 2.1	9665137	1744588	1072203	1954505	1862811	1138321	1844158
Schritt 2.2	–	1972420	–	2243165	2183740	–	2157891
Schritt 2.3	–	2201451	–	2521361	2498009	–	2475471
Schritt 2.4	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–
Schritt 4.1	9665266	2201900	1072330	2521874	2498561	1138450	2476009
Schritt 4.2	–	2202172	–	2522156	2498845	–	2476287
Schritt 4.3	–	–	–	–	–	–	–

6.2.2 Gemittelte Laufzeiten für $2 \leq p \leq 100000$

Die in diesem Abschnitt vorgelegten Testergebnisse beziehen sich für jeden Körpergrad $2 \leq n \leq 6$ auf das jeweils erste Polynom des vorangehenden Abschnitts, wobei die Laufzeit für die 9592 Primzahlen $2 \leq p \leq 100000$ gemessen und nach den einzelnen Zerlegungstypen gemittelt wurde.

$f(x) = x^2 - 27x - 29$

Typ	Laufzeit	Anzahl
1	13	4815
2	53	4777

$f(x) = x^3 + 10x^2 + 24x + 2$

Typ	Laufzeit	Anzahl
1	19	3212
2	52	4799
3	84	1581

$f(x) = x^4 - 13x^3 - 2x^2 - 8x + 2$

Typ	Laufzeit	Anzahl
1	34	2427
2	76	4369
3	111	2405
4	156	391

$f(x) = x^5 - 13x^4 - 2x^3 - 8x^2 + x + 7$

Typ	Laufzeit	Anzahl
1	80	1946
2	166	3975
3	230	2779
4	292	784
5	371	108

$f(x) = x^6 - 3x^5 - 4x^4 - 2x^3 + 9x^2 + 6x + 18$

Typ	Laufzeit	Anzahl
1	158	1627
2	304	3666
3	407	2976
4	504	1137
5	606	176
6	733	10

6.2.3 Laufzeitmessung in Abhängigkeit der Primzahl p

Wir betrachten hier wieder den jeweils ersten Zahlkörper für jeden Polynomgrad n aus Abschnitt 6.2.1 und listen für gleiche Zerlegungstypen die Laufzeiten auf, wobei wir die Primzahl p um jeweils eine Zehnerpotenz erhöhen. Es folgen die entsprechenden Tabellen.

Tabelle 132

$f(x) = x^2 - 27x - 29$

Primzahl	11	101	1009	10009	100019	1000039	100000039
Schritt 1	1	1	1	3	2	2	3
Schritt 2.1	4	4	14	18	12	12	17
Schritt 2.2	5	4	14	18	12	12	17
Schritt 3.1	–	–	–	–	–	–	–
Schritt 4.1	5	5	14	18	12	13	17
Schritt 4.2	5	5	14	18	12	13	17

Tabelle 133

$f(x) = x^3 + 10x^2 + 24x + 2$

Primzahl	13	101	1039	10009	100019	1000037	10000103	100000037
Schritt 1	1	2	3	6	5	7	8	10
Schritt 2.1	10	11	23	21	23	29	36	33
Schritt 2.2	11	14	23	22	23	29	43	33
Schritt 2.3	13	14	27	26	28	35	43	41
Schritt 2.4	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–
Schritt 4.1	14	15	27	26	29	36	44	41
Schritt 4.2	14	15	27	27	29	36	44	41
Schritt 4.3	–	–	–	–	–	–	–	–

Tabelle 134

$f(x) = x^4 - 13x^3 - 2x^2 - 8x + 2$

Primzahl	19	103	1009	10039	100003	1000037	10000103	100000073
Schritt 1	4	6	10	15	15	20	24	30
Schritt 2.1	24	33	41	48	52	66	72	102
Schritt 2.2	25	42	41	61	53	84	86	118
Schritt 2.3	30	42	52	62	68	84	99	134
Schritt 2.4	–	–	–	–	–	–	–	–
Schritt 2.5	–	–	–	–	–	–	–	–
Schritt 2.6	–	–	–	–	–	–	–	–
Schritt 3.1	33	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–
Schritt 4.1	34	42	52	62	69	84	99	134
Schritt 4.2	34	43	52	62	69	85	99	135
Schritt 4.3	–	–	–	–	–	–	–	–
Schritt 4.4	–	–	–	–	–	–	–	–

Tabelle 135

$f(x) = x^5 - 13x^4 - 2x^3 - 8x^2 + x + 7$

Primzahl	17	113	1019	10009	100043	1000099	10000019	100000007
Schritt 1	8	13	23	29	36	44	55	70
Schritt 2.1	48	57	85	96	112	128	156	194
Schritt 2.2	55	67	86	96	140	129	180	223
Schritt 2.3	88	103	144	162	181	208	261	311
Schritt 2.4	88	113	144	163	181	241	261	311
Schritt 2.5	95	113	164	186	181	241	285	339
Schritt 2.6	–	–	–	–	–	–	–	–
Schritt 2.7	–	–	–	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–
Schritt 4.1	95	114	165	187	182	242	286	340
Schritt 4.2	96	114	166	188	183	243	287	341
Schritt 4.3	96	115	166	188	183	243	287	341
Schritt 4.4	–	–	–	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–

Tabelle 136

$f(x) = x^6 - 3x^5 - 4x^4 - 2x^3 + 9x^2 + 6x + 18$

Primzahl	43	101	1009	10039	100019	1000003	10000079	100000007
Schritt 1	22	26	42	67	78	91	124	154
Schritt 2.1	105	112	151	205	236	264	321	390
Schritt 2.2	105	112	151	231	237	264	321	438
Schritt 2.3	189	200	258	334	417	416	511	607
Schritt 2.4	189	201	259	373	462	448	552	656
Schritt 2.5	217	231	299	373	492	500	619	705
Schritt 2.6	–	–	–	–	–	–	–	–
Schritt 2.7	–	–	–	–	–	–	–	–
Schritt 2.8	–	–	–	–	–	–	–	–
Schritt 2.9	–	–	–	–	–	–	–	–
Schritt 2.10	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–
Schritt 3.2	–	–	–	–	–	–	–	–
Schritt 3.3	–	–	–	–	–	–	–	–
Schritt 3.4	–	–	–	–	–	–	–	–
Schritt 3.5	–	–	–	–	–	–	–	–
Schritt 4.1	218	232	301	374	493	502	621	707
Schritt 4.2	219	233	302	375	494	503	622	708
Schritt 4.3	220	234	303	376	495	504	623	709
Schritt 4.4	–	–	–	–	–	–	–	–
Schritt 4.5	–	–	–	–	–	–	–	–
Schritt 4.6	–	–	–	–	–	–	–	–

Tabelle 137

$f(x) = x^7 - 3x^6 - 4x^5 - 2x^4 + 9x^3 + 6x^2 + 17x - 6$

Primzahl	13	101	1019	10037	100003	1000117	10000103	100000007
Schritt 1	25	42	83	106	128	174	223	277
Schritt 2.1	157	185	269	325	365	465	567	700
Schritt 2.2	200	228	317	326	429	465	628	700
Schritt 2.3	258	310	447	542	592	741	894	1091
Schritt 2.4	258	310	477	620	656	741	894	1309
Schritt 2.5	258	332	507	656	656	886	1033	1309
Schritt 2.6	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–
Schritt 4.1	258	332	508	658	657	888	1035	1311
Schritt 4.2	259	334	509	659	658	890	1037	1311
Schritt 4.3	260	335	510	661	660	891	1038	1313
Schritt 4.4	–	–	–	–	–	–	–	–

Tabelle 138

$f(x) = x^8 + 10x^7 + 24x^6 + 29x^5 - 16x^4 - 12x^3 - 17$

Primzahl	13	101	1013	10093	100129	1000003	10000019	100000049
Schritt 1	41	72	137	195	216	281	370	487
Schritt 2.1	236	292	431	568	633	750	911	1171
Schritt 2.2	236	353	499	655	634	750	911	1349
Schritt 2.3	455	510	731	924	1024	1194	1439	1811
Schritt 2.4	523	539	823	977	1081	1315	1749	1991
Schritt 2.5	523	568	823	1061	1243	1473	1749	2098
Schritt 2.6	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–
Schritt 4.1	525	570	825	1063	1246	1476	1752	2100
Schritt 4.2	526	571	826	1065	1249	1478	1753	2102
Schritt 4.3	527	573	828	1066	1250	1479	1755	2104
Schritt 4.4	–	–	–	–	–	–	–	–

Tabelle 139

$f(x) = x^9 + 10x^8 + 24x^7 + 29x^6 - 16x^5 - 12x^4 - 16x - 3$

Primzahl	17	101	1019	10061	100049	1000003	10000121	100000081
Schritt 1	62	113	229	286	354	441	619	775
Schritt 2.1	341	468	759	831	987	1144	1486	1814
Schritt 2.2	429	550	760	902	1170	1362	1688	2472
Schritt 2.3	567	798	1276	1380	1572	1806	2347	2732
Schritt 2.4	567	880	1447	1621	1573	1807	2718	2732
Schritt 2.5	596	880	1543	1621	1758	2027	2718	2733
Schritt 2.6	–	–	–	–	–	–	–	–
Schritt 3.1	–	–	–	–	–	–	–	–
Schritt 4.1	597	882	1547	1624	1760	2029	2721	2734
Schritt 4.2	599	884	1548	1625	1763	2033	2722	2736
Schritt 4.3	601	887	1550	1627	1764	2035	2725	2738
Schritt 4.4	–	–	–	–	–	–	–	–

6.2.4 Vergleich des aktuellen und des alternativen Verfahrens

Wir vergleichen unser Verfahren 'FACTOR_P' (Abschnitt 4.2) mit dem alternativen Verfahren aus [BuLen], das wir hier 'ABC' nennen.

Hierzu haben wir als erzeugendes Polynom jeweils $f(x) = x^n + 2$ gewählt, dann die Laufzeit der beiden Verfahren für $2 \leq p \leq 997$ wieder nach den verschiedenen Zerlegungstypen gemittelt.

$f(x) = x^2 + 2$

Typ	Laufzeit ABC	Laufzeit FACTOR_P	Anzahl
1	4	4	87
2	10	9	81

$f(x) = x^3 + 2$

Typ	Laufzeit ABC	Laufzeit FACTOR_P	Anzahl
1	13	11	58
2	34	28	86
3	43	41	24

$f(x) = x^4 + 2$

Typ	Laufzeit ABC	Laufzeit FACTOR_P	Anzahl
1	25	28	44
2	83	75	66
3	98	90	44
4	128	122	14

$f(x) = x^5 + 2$

Typ	Laufzeit ABC	Laufzeit FACTOR_P	Anzahl
1	62	61	34
2	159	143	88
3	223	217	38
4	0	0	0
5	324	328	8

$f(x) = x^6 + 2$

Typ	Laufzeit ABC	Laufzeit FACTOR_P	Anzahl
1	186	122	31
2	410	280	27
3	559	421	56
4	610	500	43
5	0	0	0
6	775	683	11

$f(x) = x^7 + 2$

Typ	Laufzeit ABC	Laufzeit FACTOR_P	Anzahl
1	261	232	27
2	515	506	59
3	727	765	52
4	878	959	27
5	0	0	0
6	0	0	0
7	1352	1617	3

$f(x) = x^8 + 2$

Typ	Laufzeit ABC	Laufzeit FACTOR_P	Anzahl
1	565	350	44
2	1242	781	23
3	0	0	0
4	1989	1483	52
5	2095	1644	44
6	0	0	0
7	0	0	0
8	2756	2396	5

$f(x) = x^9 + 2$

Typ	Laufzeit ABC	Laufzeit FACTOR_P	Anzahl
1	989	569	58
2	0	0	0
3	2327	1509	63
4	0	0	0
5	3358	2499	45
6	0	0	0
7	0	0	0
8	0	0	0
9	4786	3987	2

6.2.5 Vergleich mit der Polynomfaktorisierung in $\mathbb{F}_p[X]$

Aus Satz 2.62 wissen wir, daß man die Zerlegung der Primzahl p durch Zerlegung des Körperpolynoms über $\mathbb{F}_p$ erhalten kann, falls $p \nmid d(f)$.

Wir zitieren die Ergebnisse eines Fortgeschrittenenpraktikums an unserem Lehrstuhl, in dem eine Implementierung des Cantor–Zassenhaus–Verfahrens entwickelt und getestet wurde [MüHü]. Es wurden wie bei der Zerlegung von $p\mathcal{O}$ ebenfalls Sparc–Workstations vom Typ ELC eingesetzt.

In den Tests zu dieser Implementierung wurden zufällig gewählte Polynome vom Grade $2 \leq n \leq 500$ über mehreren Primkörpern $\mathbb{F}_p$ zerlegt.

Es folgen die Tabellen für $p \in \{13, 101, 1583, 7384563493\}$, die Laufzeiten werden in Sekunden angegeben.

$p = 13$:

n	Laufzeit
10	0.16
20	0.98
50	8.50
100	52.22
200	378.01
500	5798.35

$p = 101$:

n	Laufzeit
10	0.22
20	1.40
50	20.55
100	163.53

$p = 1583$:

n	Laufzeit
10	0.29
20	1.65
50	22.03
100	179.18

$p = 7384563493$:

n	Laufzeit
5	0.56
10	1.02
50	51.56

Zieht man jetzt Abschnitt 6.2.1 zum Vergleich mit unserem Zerlegungsverfahren für $p\mathcal{O}$ heran, so läßt sich hieraus klar ablesen, daß im Falle $\mathcal{O} = \mathcal{O}_{\mathcal{K}}$ zur Zerlegung von Primzahlen p, die nicht $d(f)$ teilen, die Anwendung von Satz 2.62 das Mittel der Wahl ist.

6.2.6 Eine heuristische Aussage zur mittleren Laufzeit

Wir ziehen die Ergebnisse aus Abschnitt 6.2.4 heran, um in Abhängigkeit des Körpergrades n eine Konstante k zu bestimmen, so daß die erwartete Laufzeit als $O(n^k)$ angegeben werden kann.

Dazu wählen wir den jeweils schlechtesten Fall, nämlich wenn $p\mathcal{O}$ in n Primideale zerfällt.

Dividiert man die in Abschnitt 6.2.4 enthaltenen Laufzeiten für $2 \leq n \leq 9$ durch n^k für $k = 1, 1.05, 1.10, \ldots$, so erhält man für $k = 4.20$ eine annähernd stabile Ausgabe:

```
Exponent 4.20:
n = 2:  0.004897
n = 3:  0.004063
n = 4:  0.003612
n = 5:  0.003804
n = 6:  0.003683
n = 7:  0.004564
n = 8:  0.003859
n = 9:  0.003916
```

Daher ist die erwartete Laufzeit unseres Verfahrens etwa $O(n^{4.2})$ mit einer O–Konstante ≈ 0.004.

Literaturverzeichnis

[Bu1] Johannes Buchmann. Algebraic Number Theory. Saarbrücken, Script zur Vorlesung WS 89/90

[BuLen] Johannes Buchmann/Hendrik Lenstra. Computing maximal orders and decomposing primes in number fields, 1991

[Cohen] Henri Cohen. A course in computational algebraic number theory. Buch-Manuskript, Bordeaux, 1991

[Cohen] Henri Cohen. A course in computational algebraic number theory. Buch-Manuskript, Bordeaux, 1991

[Düll] Stefan Düllmann. Ein Algorithmus zur Bestimmung der Klassengruppe positiv definiter binärer quadratischer Formen. Dissertation, Saarbrücken, 1991

[Eck1] Bruce Eckel. C++ Inside Out. McGraw-Hill, 1993

[Eck2] Bruce Eckel. Using C++. McGraw-Hill, 1989

[GIS] Gottwald/Ilgauds/Schlote. Lexikon bedeutender Mathematiker. Verlag Harri Deutsch, Thun, 1990

[Hor] Bernhard Hornfeck. Algebra. De Gruyter-Verlag, Berlin, 1976

[Hua] Hua Loo Keng. Introduction to Number Theory. Springer-Verlag, New York, 1982

[Hun] Thomas W. Hungerford. Algebra. Springer-Verlag, New York, 1974

[Knu1] Donald E. Knuth. The Art of Computer Programming I, Addison-Wesley, 1981

[Knu2] Donald E. Knuth. The Art of Computer Programming II, Addison-Wesley, 1981

[Kob] Neal Koblitz. A Course in Number Theory and Cryptography. Springer Verlag, New York, 1987

[Lang] Serge Lang. Algebraic Number Theory. Springer-Verlag, New York, 1986

[LenPo] Hendrik W. Lenstra/Michael Pohst. Computational algebraic number theory. Birkhäuser, 1991

[Lor1] Falko Lorenz. Lineare Algebra I. Bibl. Inst. Mannheim, 1981

[Lor2] Falko Lorenz. Lineare Algebra II. Bibl. Inst. Mannheim, 1981

[Meh] Kurt Mehlhorn. Datenstrukturen und effiziente Algorithmen I. Teubner-Verlag, Stuttgart, 1986

[Mer] Patrick Merscher. Standards für Objektorientierte Programmierung in der Computeralgebra. Diplomarbeit. Saarbrücken, 1992

[Mes] Herbert Meschkowski. Mathematiker–Lexikon. BI–Wissenschaftsverlag. Zürich, 1980

[Min] Hermann Minkowski. Diophantische Approximationen. Teubner-Verlag, 1907

[Mol] Richard A. Mollin. Number Theory and Applications. ASI Series, 1989

[MüHü] Andreas Müller/Michael Hürter. Der Berlekamp–Algorithmus und der Algorithmus von Cantor–Zassenhaus. Fortgeschrittenenpraktikum, Saarbrücken, 1992

[PARI] Batut/Bernardi/Cohen/Olivier. User's Guide to PARI-GP Version 1.37. Bordeaux, 1992

[PohZa] Michael Pohst/Hans Zassenhaus. Algorithmic Algebraic Number Theory. Cambridge University Press, 1989

[RSV] Reiffen/Scheja/Vetter. Algebra. Bibl. Inst. Band 110, Mannheim, 1984

[Sche] Erik Scheid. Ein neuer Algorithmus zur Berechnung der Klassenzahl algebraischer Zahlkörper. Diplomarbeit, Saarbrücken, 1993

[Schm1] Johannes Graf von Schmettow. Zur Berechnung der Klassengruppe algebraischer Zahlkörper. Diplomarbeit, Düsseldorf, 1987

[Schm2] Johannes Graf von Schmettow. Beiträge zur Klassengruppenberechnung Dissertation, Düsseldorf, 1991

[Shi] Goro Shimura. Introduction to the arithmetic theory of automorphic functions. Princeton University Press, 1971

[Stew] Ian Stewart/David Tall. Algebraic Number Theory. Chapman and Hall, Cambridge, 1987

[Zayer] Jörg Zayer. Die Theorie des Number Field Sieve. Diplomarbeit, Saarbrücken, 1991