Elementare Zahlentheorie

Fabian Januszewski

11. Februar 2021

Inhaltsverzeichnis

Vorwort

Dieses Skriptum begleitet die Vorlesung Elementare Zahlentheorie für das Lehramt an der Universität Paderborn im Wintersemester 2020/21.

Die Zahlentheorie blickt auf eine lange Geschichte zurück, welche wir in der ersten Vorlesung kurz anreißen werden. Sie gehört neben der Geometrie zu den ältesten Disziplinen der Mathematik und unterscheidet sich unter anderem dadurch von anderen Gebieten der Mathematik, daß ihr Name nicht die angewandte Methode beschreibt, sondern sich aus den Problemen beziehungsweise Objekten ableitet, welche studiert werden: den *ganzen Zahlen*.

Es gibt kaum ein mathematisches Teilgebiet, welches nicht in der Zahlentheorie Anwendung findet, was auf den ersten Blick widersprüchlich ist, denn die Zahlentheorie beschäftigt sich mit den augenscheinlich einfachsten Objekten der gesamten Mathematik: den natürlichen bzw. den ganzen Zahlen. Daß letztere derart tiefe Fragen aufwerfen, deren Beantwortung Erkenntnisse und Methoden aus einer Vielzahl mathematischer Bereiche wie Algebra, Analysis, Geometrie, Topologie, etc. erfordern, mag überraschen, macht jedoch auch den Reiz der Zahlentheorie aus. Kein geringerer als Carl Friedrich Gauß bezeichnete sie als „Königin der Mathematik“, zu einer Zeit wohlgemerkt, als die Mathematik selbst als „Königin der Wissenschaften“ angesehen wurde.

Die Probleme der Zahlentheorie, welche oft eine einfache allgemein verständliche Formulierung besitzen, aber nicht selten wie bereits angedeutet nur durch Anwendung schwieriger Resultate aus anderen mathematischen Gebieten bezwungen werden können — wenn sie nicht gar bis heute trotz jahrhundertelanger kollektiver Anstrengungen unbeantwortet geblieben sind — ziehen seit jeher prominente Mathematiker ihrer Zeit in ihren Bann.

Zusammengenommen führt dies zu einer sehr anspruchsvollen, schwierigen und tiefen Theorie, deren Verständnis einerseits eine große mathematische Breite erfordert und andererseits eine ausreichende Tiefe in der Materie selbst erzwingt.

Da diese Art der Zahlentheorie Studierenden nicht gerecht wird, hat sich im letzten Jahrhundert der Begriff der *Elementaren Zahlentheorie* herausgebildet. Er beschreibt einerseits das Teilgebiet der Zahlentheorie, welches mit elementaren Methoden zugänglich ist und andererseits eine Art von Lehrveranstaltung, welche ausgewählte Themen aus diesem Gebiet abhandelt. Hierbei kann es sich letztendlichr immer nur um eine Auswahl handeln, welche mehr oder weniger repräsentativ für die Zahlentheorie an sich steht.

Die vorliegende Vorlesung wurde insbesondere mit Blick auf das Lehramt und damit auch auf mögliche Anwendungen im Schulunterricht entworfen. Dabei werden sich die tatsächlichen Anwendungen im Unterricht in der Praxis wahrscheinlich auf die Beschreibung von hier abgehandelten Phänomenen beschränken, da selbst der Beweis des Chinesischen Restsatzes Schülern heutzutage als kaum zumutbar erscheint.

Das Adjektiv „elementar“ sollte nicht mißverstanden werden: „Elementar“ und „ein-

fach“ sind verschiedene Begriffe mit verschiedenen Bedeutungen. Ein elementarer Beweis in der elementaren Zahlentheorie kann schwieriger und anspruchsvoller sein, als sein nicht-elementares Pendant. Der Beweis des Primzahlsatzes ist hierfür ein prominentes Beispiel. Daher liegt es in der Verantwortung des Dozenten, hier eine geeignete angemessene Auswahl zu treffen.

Wie immer gilt: Die Hörerschaft muß sich auf die Inhalte intellektuell einlassen. Erst dann erschließen sich Sinn und Ästhetik, denn nur dann kann Verständnis möglich sein.

Paderborn, im Oktober 2020.

F. J.

Kapitel 1

Arithmetik

1.1 Kurzer Abriß der Geschichte der Zahlentheorie

Die Zahlentheorie blickt auf eine lange Geschichte zurück. Sie hat ihren Ursprung im *Zählen* und damit in den *natürlichen Zahlen*

$$1, 2, 3, 4, 5, \ldots$$

Die ersten natürlichen Zahlen spielen in der Evolution eine so wichtige Rolle, daß in verschiedenen Tierarten ein Sinn für die ersten natürlichen Zahlen nachweisbar ist. Raben, Tauben, Hunde, Rhesus-Affen und Schimpanzen haben alle einen natürlichen Sinn für die Zahlen 1,2,3, teilweise bis 4, welcher mit ausreichend Übung sogar erweitert werden kann. Ameisen können bis jenseits der 20 zählen und im Zahlbereich von 1 bis 5 addieren und subtrahieren. Ameisen bevölkern seit über 100 Millionen Jahren diesen Planeten, sodaß Zahlen deutlich um Größenordnungen älter sind die Menschheit insgesamt.

Daher überrascht es nicht, daß die natürlichen Zahlen historisch betrachtet die ersten mathematischen Objekte sind, mit welchen sich Menschen beschäftigt haben. Die Sumerer hatten bereits 3500 vor Christus einen Kalender, d. h. daß sie elementare Arithmetik beherrschten. Die ersten dokumentierten wissenschaftlichen mathematischen Erkenntnisse der Spezies homo sapiens aus Mesopotamien und werden auf das 18. Jahrhundert vor Christus datiert, sind also knapp 4000 Jahre alt. Diese befinden sich auf einer Tontafel der Babylonier, welche *pythagoreische Tripel* auflistet.

Ein pythagoreisches Tripel besteht aus drei positiven natürlichen Zahlen $a, b, c \in \mathbf{N}$, derart, daß

$$a^2 + b^2 = c^2. \tag{1.1}$$

Beispielsweise ist $a = 3$, $b = 4$ und $c = 5$ ein pythagoreisches Tripel. Die Tripel auf der erhaltenen Tontafel aus Mesopotamien sind zu groß, als daß sie durch reines Ausprobieren hätten gefunden werden können, weswegen davon ausgegangen wird, daß die Babylonier zahlentheoretische Kenntnisse besaßen, welche über die elementare Arithmetik der drei Grundrechenarten hinausgehen.

Pythagoreische Tripel sind insbesondere dank des *Satzes von Pythagoras* von praktischer Bedeutung: Sie reduzieren die Konstruktion rechter Winkel auf die Konstruktion von Dreiecken mit Seitenlängen a, b, c, welche wiederum der Relation (1.1) genügen, was insbesondere im Baugewerbe von Bedeutung ist.

Über die Zahlentheorie der Babylonier ist leider nicht mehr bekannt. Sie verfügten jedoch über eine sehr gut entwickelte Algebra und verschiedene Quellen legen nahe, daß Pythagoras und Thales Mathematik von den Babyloniern lernten.

Die antike griechische Mathematik griff dies auf und führte zu einer ersten Blüte der Mathematik, welche in den bekannten dreizehn Bänden der „Elemente“ von *Euklid von Alexandria* kulminierte, welche auf 300 vor Christus datiert werden. Die Elemente gelten als Keimzelle der modernen Mathematik: Die allgemeine Struktur *Definition*, *Satz*, *Beweis* wird dort konsequent umgesetzt und der einzigartige kulturelle Einfluß dieses Werkes kann nicht überschätzt werden. Sie fanden über 2000 Jahre lang als Lehrbücher im Mathematikunterricht Anwendung und waren bis weit ins 19. Jahrhundert hinein nach der Bibel das meistverbreitete Werk der Weltliteratur.

Die Elemente befassen sich mit Geometrie und Zahlentheorie. Der Geometrie der *Euklidischen Ebene* widmen sich Bände 1–3 sowie Band 10 und der Geometrie im Raum sind die Bände 11–13 gewidmet. Die Zahlentheorie umfaßt die Bände 5–9. Hier findet sich beispielsweise der Beweis der Irrationalität von $\sqrt{2}$ (Buch 5), Teilbarkeitslehre inklusive Primzahlbegriff (Band 7), sowie Euklids Beweis der Unendlichkeit der Menge der Primzahlen (Band 9).

Die folgenden Jahrhunderte brachten keinen erähnenswerten Fortschritt mit sich. Dabei muß das Mittelalter als Tiefpunkt betrachtet werden, zumindest aus europäischer Sicht[1].

Erst mit *Pierre de Fermat* (1607–1665)[2] wendet sich das Blatt. Nach einem umfassenden Studium der antiken griechischen Mathematik und insbesondere der klassischen Arbeiten von *Diophantos von Alexandria* gelangen Fermat bahnbrechende Entdeckungen, welche die Forschung in der Zahlentheorie bis in die Gegenwart beeinflussen. Fermat gilt als Begründer der modernen Zahlentheorie.

Fermat zeigte beispielsweise, daß jede Primzahl p der Form $p = 4n + 1$ wie $5, 13, 17, 29, ...$ eine Summe zweier Quadrate ist:

$$5 = 1^2 + 2^2, \quad 13 = 2^2 + 3^2, \quad 17 = 1^2 + 4^2, \quad 29 = 2^2 + 5^2, \ldots$$

Er behauptete auch, daß jede natürliche Zahl eine *Dreieckszahl* ist, oder eine Summe aus zwei oder drei Dreieckszahlen. Dabei ist die n-te Dreieckszahl $\Delta_n := \frac{n\cdot(n+1)}{2}$. Sie entspricht der Anzahl von Kugeln in einem gleichseitigen Dreieck, dessen Seiten jeweils aus n Kugeln bestehen. Analog lassen sich *Vierecks-* und *Fünfeckszahlen* und allgemein *n-Eckzahlen* definieren. Dabei sind Viereckszahlen nichts anderes als Quadratzahlen. Der Überbegriff für diese Zahlen ist *Polygonalzahl*. Fermat behauptete, daß jede natürliche Zahl stets Summe aus höchstens n n-Eckzahlen ist. Insbesondere sollte also jede natürliche Zahl eine Summe aus höchstens vier Quadraten sein. Die allgemeine Behauptung Fermats wird als *Fermats Polygonalzahlsatz* bezeichnet.

Nach Fermat ist der *kleine Satz von Fermat* benannt, welchen wir noch kennenlernen werden. Er entwickelte weiterhin die *Methode des unendlichen Abstiegs*, welche äquivalent zum Wohlordnungsprinzip ist und nutzte sie erfolgreich, um beispielsweise die Unlösbarkeit der Gleichung

$$X^4 + Y^4 = Z^4$$

[1] Im fernen Osten hingegen scheint die Zahlentheorie zwischen dem 5. und 12. Jahrhundert jedoch eine gewisse Blüte erlebt zu haben.

[2] Oft wird 1601 als Geburtsjahr Fermats angegeben, was jedoch nach aktuellem Kenntnisstand inkorrekt ist.

mit $X, Y, Z \in \mathbf{Z} \setminus \{0\}$ zu zeigen. In einer Randnotiz bemerkte er, daß er einen Beweis für die Unlösbarkeit der allgemeineren Gleichung

$$X^n + Y^n = Z^n$$

für $n > 2$ mit $X, Y, Z \in \mathbf{Z} \setminus \{0\}$ gefunden hätte, dieser allerdings nicht auf den entsprechenden Rand passen würde. Diese Aussage, als *Fermats großer Satz* und *Fermats letzten Satz* bekannt, blieb sehr lange Zeit eine offene Vermutung, trotz kollektiver Anstrengungen von Generationen von Mathematikern. Erst 1994 gelang Andrew Wiles in Kollaboration mit Richard Taylor ein Beweis unter Verwendung modernster Methoden, welche trotzdem um viele neue Techniken erweitert werden mußten, um das Ziel zu erreichen. Selbst 25 Jahre nach Veröffentlichung dieses Beweises ist er bis heute nicht unwesentlich vereinfacht worden und es gilt als unwahrscheinlich, daß Fermat einen Beweis kannte. Es ist ausgeschlossen, daß er den von Wiles geführten Beweis kannte.

Fermats letzter Satz beleuchtet folgendes Dilemma: Wenn eine Lösung existiert, dann kann sie durch naives Ausprobieren in endlicher Zeit gefunden werden. Im Fall der Unlösbarkeit nützen aber alle Lösungsversuche nichts, da wir stets nur endlich viele Fälle in endlicher Zeit abhandeln können. Die Unlösbarkeit einer Gleichung zu beweisen ist damit im allgemeinen ein schwierigeres Problem, als die Lösbarkeit nachzuweisen. Für letztere genügt es, eine Lösung anzugeben, für erstere müß mathematisch korrekt argumentiert werden.

Nach Fermat betrat *Leonhard Euler* (1707–1783) die Bühne, welchem als erster einen *analytischen Beweis* der unendlichkeit der Primzahlen gelang. Neben zahlreichen Beiträgen zur Zahlentheorie ist er insbesondere für die Lösung des sogenannten *Basel-Problems* bekannt. Euler zeigte, daß

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Daß es sich hierbei um ein zahlentheoretisch relevantes Resultat handelt, ist auf den ersten Blick nicht klar und es benötigte weitere Jahrhunderte, um herauszukristallisieren, was π^2 und $\frac{1}{6}$ in Eulers Formel bedeuten.

Um 1760 bewies *Johann Heinrich Lambert* (1728–1777) die *Irrationalität* von π, d. h. daß π keine rationale Zahl ist.

Nachfolger von Euler als Direktor der Königlich-Preußischen Akademie der Wissenschaften war *Joseph-Louis Lagrange* (1736–1813), welchem 1770 der Beweis des Spezialfalls der Quadratzahlen in Fermats Polygonalzahlsatz gelang: Jede natürliche Zahl ist Summe von höchstens vier Quadraten.

Das erste Lehrbuch zur Zahlentheorie verfaßte *Adrien-Marie Legendre* (1752–1833), welches 1798 erschien. Das *Legendre-Symbol* wird uns in dieser Vorlesung noch begegnen.

Ein unbestreitbarer Höhepunkt sind die Beiträge von *Johann Carl Friedrich Gauß* (1777–1855) zur Zahlentheorie. Obwohl Gauß bedeutende Beiträge zu allen damaligen Disziplinen der Mathematik leistete, betrachtete er sein Buch *Disquisitiones arithmeticae* als seinen wichtigsten Beitrag zur Mathematik.

In der Tat zehren wir bis heute von den Erkenntnis von Gauß und es kommt bisweilen vor, daß eine Bemerkung von Gauß neue Forschungsergebnisse inspiriert. Vieles, selbst

modernste Resultate, waren, wenn auch in anderem Gewand, trotzdem Gauß oftmals bereits bekannt, zumindest in speziellen Fällen.

Im Jahr 1796 gelang Gauß der Beweis des Spezialfalls der Dreieckszahlen von Fermats Polygonalzahlsatz: Jede natürliche Zahl ist Summe von höchstens drei Dreieckszahlen. Gauß kommentierte diese Erkenntnis in seinem Tagebuch mit den Worten „*Eureka!*“ Daher wird dieser Satz bisweilen auch als *Eureka-Satz* bezeichnet.

Im selben Jahr gelang Gauß im Alter von 18 Jahren der erste Beweis des *quadratischen Reziprozitätsgesetzes*, welches bereits von Euler vermutet worden und welcher hierzu wiederum durch Arbeiten von Fermat inspiriert worden war.

Das quadratische Reziprozitätsgesetz hat eine Symmetrie zwischen zwei Primzahlen p, q im Kontext der Fragestellung zum Inhalt, ob der Rest der Division von p durch q mit dem Rest eines Quadrates nach Division durch q übereinstimmt. In moderner Notation geht es also um die Frage, ob die Gleichung

$$p \equiv x^2 \pmod{q}$$

für ein $x \in \mathbf{Z}$ lösbar ist oder nicht. Das quadratische Reziprozitätsgesetz besagt beispielsweise, daß im Fall $p \equiv q \pmod 4$ diese Frage äquivalent ist zur Fragestellung, ob

$$q \equiv y^2 \pmod{p}$$

für ein $y \in \mathbf{Z}$ lösbar ist.

Eine derartige Symmetrie ist alles andere als offensichtlich und Gauß bezeichnete seine Erkenntnis in seinem Tagebuch als *Aureum Theorema*, d. h. als *goldenen Satz*. Inwieweit Gauß in seinen Fähigkeiten seinen Zeitgenossen überlegen war, manifestiert sich auch darin, daß er nicht nur als erster einen, sondern 8 (!) Beweise des quadratischen Reziprozitätsgesetzes fand und die aktuellen bis zum heutigen Tage andauernden Anstrengungen, dies zu verallgemeinern, sind eine der zentralsten Fragestellungen der modernen Zahlentheorie überhaupt.

Nach Gauß bereiteten *Augustin-Louis Cauchy* (1789–1857) und *Peter Gustav Lejeune Dirichlet* (1805–1859) den Boden für *analytische Methoden* in der Zahlentheorie. Cauchy gelang 1813 der vollständige Beweis von Fermats Polygonalzahlsatz und Dirichlet bewies unter Verwendung von Analysis, daß zu gegebenen teilerfremden $0 < k < n$ stets unendlich viele Primzahlen der Form $p = k + \ell \cdot n$ existieren. Mit anderen Worten es existieren unendlich viele Primzahlen, welche bei Division durch n Rest k hinterlassen. Dirichlet zeigte sogar, daß sich zu gegebenem n die Primzahlen asymptotisch gleichmäßig auf alle möglichen[3] Reste k verteilen.

Georg Friedrich Bernhard Riemann (1826–1866) leistete neben Beiträgen zur Integrationstheorie (*Riemannintegral*), Funktionentheorie (*Riemannsche Flächen*) und Differentialgeometrie (*Riemannsche Geometrie*) auch wichtige Beiträge zur Zahlentheorie. In seiner 9-seitigen Arbeit „Über die Anzahl der Primzahlen unter einer gegebenen Größe“, welche 1859 in den Monatsberichten der Königlich-Preußischen Akademie der Wissenschaften zu Berlin erschien, griff er die bereits von Euler studierte Funktion

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$$

[3] d. h. zu n teilerfremden

auf. Hatte Euler s als *reellen* Parameter betrachtet, faßte Riemann s als eine *komplexe* Variable auf. Dies erlaubte es ihm, funktionentheoretische Methoden auf das Studium der inzwischen nach ihm benannten *Riemannschen ζ-Funktion* $\zeta(s)$ anzuwenden. Insbesondere unter Verwendung von Fourier-Analysis und der Poissonschen Summenformel wies Riemann die Existenz einer tiefliegenden Symmetrie von ζ nach und gab weiterhin eine Formel für die Primzahlzählfunktion

$$\pi(x) \;:=\; \#\{p \text{ prim} \mid p \leq x\}$$

unter Verwendung der nichttrivialen Nullstellen ρ von $\zeta(s)$ an. Riemann bemerkte in seiner Arbeit „*... es ist sehr wahrscheinlich, daß alle Wurzeln reell sind. Hiervon wäre allerdings ein strenger Beweis zu wünschen; ich habe indes die Aufsuchung desselben nach einigen flüchtigen vergeblichen Versuchen vorläufig beiseite gelassen, da er für den nächsten Zweck meiner Untersuchung entbehrlich schien.*“

Diese als *Riemannsche Vermutung* bekannte Aussage ist bis heute unbeantwortet: Wir wissen nicht, ob sämtliche nichttrivialen Nullstellen ρ auf der kritischen Geraden $\frac{1}{2} + i\mathbf{R}$ liegen, wie Riemann mutmaßt. Sie läßt sich äquivalent in eine Aussage über die Asymptotik der Primzahlen übersetzen, denn in gewissem Sinne lassen sich die Nullstellen ρ der ζ-Funktion als *Frequenzen* der Primzahlen interpretieren.

Enrico Bombieri (1940–; Fieldsmedaille 1974) schrieb: „*Riemann's insight was that the frequencies of the basic waveforms that approximate the ψ-function are determined by the places where the ζ-function is equal to zero. [...] To me, that the distribution of prime numbers can be so accurately represented in a harmonic analysis is absolutely amazing and incredibly beautiful. It tells of an arcane music and a secret harmony composed by the prime numbers.*“

Erst 1882, also über einhundert Jahre nach Lamberts Beweis der Irrationalität von π gelang *Carl Louis Ferdinand von Lindemann* (1852–1939) der Beweis der *Transzendenz* von π, d. h. daß π keine Nullstelle eines Polynoms mit rationalen Koeffizienten ist.

Um diese Historie kurz zu halten, verzichten wir auf die genauere Diskussion der Entwicklungen im 20. und 21. Jahrhundert. Zusammenfassend gibt es zwei große Bereiche, auf welche sich die aktive Forschung fokussiert: Die analytische Zahlentheorie, welche Fragestellungen rund um Primzahlverteilungen, die ζ-Funktion und verwandter Funktionen studiert, sowie das *Langlandsprogramm*, welches seine Ursprünge in einem Brief von *Robert Phelan Langlands* (1936–) an *André Weil* (1906–1998) im Jahr 1967 hat. Es postuliert die Existenz einer allgemeinen Korrespondenz zwischen *arithmetischer Geometrie* auf der einen Seite und sogenannten *automorphen Darstellungen* auf der anderen. Bei ersteren handelt es sich um durch multivariate Polynomgleichungen mit ganzen oder rationalen Koeffizienten beschriebene Objekten und bei letzteren handelt es sich um gewisse ausgezeichnete Unterräume gewisser (meist unendlichdimensionaler) Hilberträume. Das Langlandsprogramm postuliert die Existenz einer Brücke zwischen Arithmetik und Analysis.

Diese Korrespondenz ist eine drastische Verallgemeinerung des quadratischen Reziprozitätsgesetzes und auch Andrew Wiles' Beweis von Fermats letztem Satz ist in diesem Kontext einzuordnen: Wiles bewies einen Spezialfall einer Korrespondenz, was letztendlich Fermats letzten Satz als Konsequenz hatte.

1.2 Die natürlichen Zahlen

Wir bezeichnen die Menge der natürlichen Zahlen mit $\mathbf{N} = \{0, 1, 2, 3, \dots\}$ und weisen darauf hin, daß 0 in dieser Vorlesung als natürliche Zahl angesehen wird[4]. Damit entspricht $\mathbf{N}$ der Menge der endlichen Kardinalzahlen[5]. Natürliche Zahlen werden etwas ausführlicher in Abschnitt 1.1.12 im Skriptum zur Linearen Algebra diskutiert. Hier fassen wir lediglich zusammen, was wir im Folgenden benötigen.

Es gelten:

Satz 1.2.1 (Induktionsprinzip; vgl. Satz 1.1.27 im Skriptum zur Linearen Algebra)**.** *Ist für jedes $n \in \mathbf{N}$ eine Aussage $A(n)$ gegeben und gelten weiterhin*

(i) $A(0)$ *ist wahr (Induktionsanfang),*

(ii) $\forall n \in \mathbf{N}$:

$$A(n) \text{ ist wahr} \quad \Rightarrow \quad A(n+1) \text{ ist wahr},$$

(Induktionsschritt),

so ist $A(n)$ für alle $n \in \mathbf{N}$ wahr.

Es bezeichne $S : \mathbf{N} \to \mathbf{N}, n \mapsto n + 1$ die Nachfolgerabbildung. Äquivalent zum Induktionsprinzip ist

Satz 1.2.2 (Universelle Eigenschaft von $\mathbf{N}$; vgl. Definition 1.1.24 sowie Satz 1.1.25 im Skriptum zur Linearen Algebra)**.** *Das Tripel $(\mathbf{N}, S, 0)$ besitzt folgende universelle Eigenschaft: Für jede Menge M, jede Abbildung $s : M \to M$ und jedes $m_0 \in M$ existiert eine eindeutig bestimmte Abbildung $f : \mathbf{N} \to M$ mit den beiden Eigenschaften*

(i) $f(0) = m_0$,

(ii) $f \circ S = s \circ f$, *d. h.* $\forall n \in \mathbf{N}$:

$$f(n+1) = s(f(n)).$$

Ebenfalls äquivalent ist das

Satz 1.2.3 (Wohlordnungsprinzip; vgl. Satz 1.1.37 im Skriptum zur Linearen Algebra)**.** *In jeder nichtleeren Teilmenge $M \subseteq \mathbf{N}$ existiert ein minimales Element $m \in M$, d. h.*

$$\forall n \in M : \quad m \leq n.$$

Wir werden von allen drei Sätzen Gebrauch machen. Das Induktionsprinzip als auch das Wohlordnungsprinzip sind sehr nützliche Beweismethoden. Dabei wird das *Induktionsprinzip* üblicherweise in konstruktiven Situationen angewandt. Das *Wohlordnungsprinzip* kommt oft in Widerspruchsbeweisen zur Anwendung: Man wählt M als die Menge der Ausnahmen, welche es auszuschließen gilt. Den Fall, daß M nicht leer ist, d. h. der Fall, daß es eine Ausnahme gibt, wird dann zum Widerspruch geführt, indem gezeigt wird, daß

[4] Diesbezüglich gibt es verschiedene Konventionen

[5] Für eine kurze Einführung in Kardinalzahlen verweisen wir auf Abschnit 1.1.11 im Skriptum zur Linearen Algebra.

es kein minimales $m \in M$ geben kann, weil es für jedes Element $n \in M$ ein echt kleineres $n' \in M$ gibt, was dem Wohlordnungsprinzip widerspricht. Pierre der Fermat nannte dies die *Methode des unendlichen Abstiegs*.

Die *universelle Eigenschaft* der natürlichen Zahlen ist konstruktiver Natur. Sie erlaubt uns *rekursive Definitionen* der Art:

$$\begin{aligned} a_0 &:= 2, \\ a_{n+1} &:= 2 \cdot a_n - 1 \quad \text{für } n \geq 0. \end{aligned}$$

Denn genau genommen suchen wir in diesem Fall eine Abbildung $f : \mathbf{N} \to \mathbf{N}$ mit den beiden Eigenschaften

$$f(0) = 2, \tag{1.2}$$
$$f(n+1) = 2 \cdot f(n) - 1 \quad \text{für } n \geq 0. \tag{1.3}$$

Dabei entspricht $f(n)$ dem n-ten Folgenglied a_n.

Daß es genau eine Abbildung f mit den beiden Eigenschaften (1.2) und (1.3) gibt, wird durch die universelle Eigenschaft garantiert: Die zweite rekursive Bedingung läßt sich via der Abbildung

$$s : \mathbf{N} \to \mathbf{N}, \quad k \mapsto 2 \cdot k - 1$$

kodieren, sodaß f genau dann obiger Rekursionsgleichung genügt, wenn $f(n+1) = s(f(n))$ für alle $n \in \mathbf{N}$ gilt.

Die Eindeutigkeit von f besagt, daß die charakterisierenden Eigenschaften der Folge a_n diese eindeutig bestimmen und die Existenz von f besagt, daß es derartige solche Folge tatsächlich gibt. In der Praxis gibt man sich üblicherweise mit der rekursiven Definition der Folge $(a_n)_{n \in \mathbf{N}}$ zufrieden und läßt die formale Übersetzung in die universelle Eigenschaft von $\mathbf{N}$ unter den Tisch fallen. Trotzdem wendet wird bei rekursiven Definitionen ein fundamentales Prinzip angewandt, welches Äquivalent zum Prinzip der vollständigen Induktion ist — also keineswegs vernachlässigbar. Wir weisen ebenfalls darauf hin, daß der Beweis der universellen Eigenschaft mittels vollständiger Induktion schwieriger ist als es auf den ersten Blick erscheint.

Addition als auch Multiplikation auf $\mathbf{N}$ werden rekursiv mittels der universellen Eigenschaft definiert, wobei hier erschwerend hinzukommt, daß zur Definition der Summe $m+n$ zweier natürlicher Zahlen rekursiv in *beiden* Argumenten vorgegangen werden muß:

Die *Addition* ist die eindeutig bestimmte Abbildung

$$\alpha : \mathbf{N} \times \mathbf{N} \to \mathbf{N}, \quad (m, n) \mapsto \alpha(m, n) =: m + n,$$

welche folgenden drei Eigenschaften genügt[6]:

$$\alpha(0, 0) = 0, \tag{1.4}$$
$$\alpha(m+1, n) = \alpha(m, n) + 1, \qquad \text{für alle } m, n \in \mathbf{N}, \tag{1.5}$$
$$\alpha(m, n+1) = \alpha(m, n) + 1, \qquad \text{für alle } m, n \in \mathbf{N}. \tag{1.6}$$

[6]Wir heben hervor, daß $m + n$ erst via α definiert wird.

Die Existenz und Eindeutigkeit der Addition ergeben sich aus der universellen Eigenschaft des direkten Produktes $\mathbf{N} \times \mathbf{N}$ (vgl. Satz 1.1.32 im Skriptum zur Linearen Algebra), welche wiederum eine Konsequenz der universellen Eigenschaft von $\mathbf{N}$ ist[7].

Unter Rückgriff auf die Addition wird schließlich analog die *Multiplikation* definiert. Diese ist die eindeutig bestimmte Abbildung

$$\mu : \mathbf{N} \times \mathbf{N} \to \mathbf{N}, \quad (m, n) \mapsto \mu(m, n) =: m \cdot n,$$

welche folgenden drei Eigenschaften genügt:

$$\mu(0, 0) = 0, \tag{1.7}$$
$$\mu(m + 1, n) = \alpha(m, n) + n, \qquad \text{für alle } m, n \in \mathbf{N}, \tag{1.8}$$
$$\mu(m, n + 1) = \alpha(m, n) + m, \qquad \text{für alle } m, n \in \mathbf{N}. \tag{1.9}$$

Die bekannten elementaren Eigenschaften der Addition natürlicher Zahlen werden in Satz 1.1.35 im Skriptum zur Linearen Algebra zusammengefaßt, was wir hier zitieren:

Satz 1.2.4 (Eigenschaften der Addition; vgl. Satz 1.1.35 im Skriptum zur Linearen Algebra)**.** *Es gelten:*

(a) 0 *ist* neutral *für* $+$*:*

$$\forall n \in \mathbf{N} : \quad n + 0 \;=\; n \;=\; 0 + n.$$

(b) $+$ *ist* assoziativ*:*

$$\forall m, n, k \in \mathbf{N} : \quad m + (n + k) \;=\; (m + n) + k.$$

(c) $+$ *ist* kommutativ*:*

$$\forall m, n \in \mathbf{N} : \quad m + n \;=\; n + m.$$

(d) Es gilt die Kürzungsregel*:*

$$\forall m, n, k \in \mathbf{N} : \quad m + k \;=\; n + k \quad \Rightarrow \quad m = n.$$

Analog formulieren wir ohne Beweis

Satz 1.2.5 (Eigenschaften der Multiplikation)**.** *Es gelten:*

(a) 1 *ist* neutral *für die Multiplikation:*

$$\forall n \in \mathbf{N} : \quad n \cdot 1 \;=\; n \;=\; 1 \cdot n.$$

(b) Die Multiplikation natürlicher Zahlen ist assoziativ*:*

$$\forall m, n, k \in \mathbf{N} : \quad m \cdot (n \cdot k) \;=\; (m \cdot n) \cdot k.$$

(c) Die Multiplikation natürlicher Zahlen ist kommutativ*:*

$$\forall m, n \in \mathbf{N} : \quad m \cdot n \;=\; n \cdot m.$$

[7] Eine alternative Definition ist Gleichung (1.57) im Skriptum zur Linearen Algebra, welche lediglich die universelle Eigenschaft von $\mathbf{N}$ verwendet.

(d) Es gilt die Kürzungsregel*:*

$$\forall m, n, k \in \mathbf{N},\, k > 0 : \quad m \cdot k \;=\; n \cdot k \quad \Rightarrow \quad m = n.$$

(e) Addition und Multiplikation sind distributiv:

$$\forall m, n, k \in \mathbf{N} : \quad (m + n) \cdot k \;=\; m \cdot k + n \cdot k.$$

Die Voraussetzung $k > 0$ in (d) ist notwendig, da 0 ganz $\mathbf{N}$ *annuliert*:

$$\forall n \in \mathbf{N} : \quad n \cdot 0 \;=\; 0 \;=\; 0 \cdot n.$$

Exemplarisch zeigen wir, wie sich diese Aussage induktiv anhand der Definition der Multiplikation beweisen läßt:

Per Definitionem gilt $0 \cdot 0 = 0$, vgl. (1.7). Sei nun $n \in \mathbf{N}$ beliebig und sei weiterhin $n \cdot 0 = 0$. Dann erhalten wir mit (1.8), daß

$$(n + 1) \cdot 0 \;=\; n \cdot 0 + 0 \;=\; 0 + 0 \;=\; 0,$$

wobei sich die letzte Identität aus Aussage (a) aus Satz 1.2.4 ergibt oder alternativ unmittelbar aus der Definition der Addition, vgl. (1.4). Dank Induktionsprinzip gilt damit $n \cdot 0 = 0$ für alle natürlichern Zahlen $n \in \mathbf{N}$. Analog ergibt sich $0 \cdot n = 0$ für alle $n \in \mathbf{N}$, wenn man hierfür nicht auf die Kommutativität der Multiplikation zurückgreifen möchte, um $0 \cdot n = 0$ auf die Aussage $n \cdot 0 = 0$ zu reduzieren.

1.3 Die ganzen Zahlen

Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.
Leopold Kronecker (1823–1891)

Aus den natürlichen Zahlen $\mathbf{Z}$ werden schlußendlich die ganzen Zahlen konstruiert. Hierbei ist es unerheblich, ob man mit den natürlichen Zahlen ausgehend von 0 oder mit den natürlichen Zahlen ausgehend von 1 ausgeht: Das Ergebnis $\mathbf{Z}$ ist in beiden Fällen das gleiche[8].

Die Konstruktion von $\mathbf{Z}$ wird dadruch motiviert, daß die Addition in $\mathbf{N}$ im Allgemeinen nicht umkehrbar ist, oder anders ausgedrückt ist Subtraktion keine wohldefinierte Abbildung $\mathbf{N} \times \mathbf{N} \to \mathbf{N}$, denn wenn wir n von 0 subtrahieren und $n > 0$, so macht die Differenz „$0 - n$“ als natürliche Zahl keinen Sinn.

Die Lösung dieses Problems ist so einfach wie sie elegant ist: Wir definieren $\mathbf{Z}$ als Menge *aller Differenzen* „$m - n$“ natürlicher Zahlen $m, n \in \mathbf{N}$. Das klingt jetzt tautologisch: Wir müssen die Differenzen erst definieren, bevor wir über sie sprechen können. Das ist aber kein Problem, denn gedanklich können wir uns von dieser Idee leiten lassen, um

[8]Das ist mit Vorsicht zu genießen. Genau genommen erhalten wir trotzdem *zwei verschiedene* Mengen, je nachdem, ob wir bei 0 oder bei 1 beginnen. Das Ergebnis ist *eindeutig bis auf eindeutige Isomorphie* abelscher Gruppen. Daher spielt es letztendlich doch keine Rolle, was wir wählen. Bemerkenswert ist, daß im Fall der natürlichen Zahlen ab 1 trotzdem die 0 als Element von $\mathbf{Z}$ quasi aus dem Nichts heraus entsteht.

Differenzen korrekt zu definieren. Zunächst geben zwei natürliche Zahlen $m, n \in \mathbf{N}$ jeweils Anlaß zu einer Differenz und jede Differenz entsteht als solche als Differenz natürlicher Zahlen. Daher entsprechen Differenzen also *Paaren* $(m, n) \in \mathbf{N} \times \mathbf{N}$ im direkten Produkt von $\mathbf{N}$ mit sich selbst. Es stellt sich nun die Frage, wann zwei Differenzen *gleich* sind, d. h. wann die Differenzen von $m_1, n_1 \in \mathbf{N}$ und $m_2, n_2 \in \mathbf{N}$ übereinstimmen. Da wir im Allgemeinen nicht subtrahieren dürfen bzw. können, behelfen wir uns damit, daß wir statt der Subtraktion die *Addition* verwenden: Wir sagen, daß (m_1, n_1) und (m_2, n_2) die selbe Differenz repräsentieren, wenn[9]

$$m_1 + n_2 \;=\; m_2 + n_1. \tag{1.10}$$

Auf diese Weise erhalten wir eine Äquivalenzrelation $\sim$ auf $\mathbf{N} \times \mathbf{N}$, deren Äquivalenzklassen aus den Paaren (m, n) bestehen, welche sämtlich die selbe Differenz repräsentieren, d. h. daß genau dann $(m_1, n_1) \sim (m_2, n_2)$, wenn (1.10) gilt[10]. Schlußendlich definieren wir damit die ganzen Zahlen als die Menge

$$\mathbf{Z} \;:=\; \mathbf{N} \times \mathbf{N} / \sim$$

der Äquivalenzklassen von Paaren $(m, n) \in \mathbf{N} \times \mathbf{N}$. Gedanklich steht die Äquivalenzklasse $[(m, n)]_\sim$ eines Paares (m, n) für den Wert der Differenz $m - n$, weswegen wir eine Abbildung

$$\iota : \mathbf{N} \to \mathbf{Z}, \quad n \mapsto [(n, 0)]_\sim$$

erhalten. Man rechnet nach, daß dank der Kürzungseigenschaft der Addition natürlicher Zahlen (vgl. Eigenschaft (d) aus Satz 1.2.4) die Abbildung ι injektiv ist. Mithin können wir $\mathbf{N}$ als Teilmenge von $\mathbf{Z}$ auffassen.

Addition und Multiplikation setzen sich nun eindeutig auf $\mathbf{Z}$ fort (vgl. Satz 1.2.18 im Skriptum zur Linearen Algebra bzw. das darauffolgende Beispiel $\mathbf{Z} = G(\mathbf{N})$). Wir erhalten auf diese Weise einen *kommutativen nullteilerfreien Ring*[11] $(\mathbf{Z}, +, \cdot)$ mit Einselement 1.

Die Allgegenwärtigkeit von $\mathbf{Z}$ in der Mathematik wird unter anderem durch die beiden universellen Eigenschaft erklärt, welche $\mathbf{Z}$ genügt.

Einerseits ist $(\mathbf{Z}, +)$ eine abelsche Gruppe, welche frei von $\{1\}$ erzeugt wird, womit für jede Gruppe $(G, \cdot\,)$ und jedes Element $g \in G$ ein eindeutig bestimmter Gruppenhomomorphismus $\phi_g : \mathbf{Z} \to G$ existiert mit $\phi_g(1) = g$ (vgl. Proposition 1.2.19 im Skriptum zur Linearen Algebra). Üblicherweise schreiben wir g^n anstatt $\phi_g(n)$ und stellten uns g^n als n-faches Produkt von g mit sich selbst vor, bei negativem Exponenten als n-faches Produkt des zu g inversen Elementes g^{-1}.

Andererseits hat $(\mathbf{Z}, +, 1)$ als ein Ring mit Eins mit folgende universelle Eigenschaft (vgl. Proposition 1.2.56 im Skriptum zur Linearen Algebra): Für jeden Ring $(R, +, \cdot)$ mit Eins existiert ein eindeutig bestimmter Ringhomomorphismus[12] $\phi : \mathbf{Z} \to R$. Bezeichnet $1_R \in R$ das Einselement in R, dann ist $\phi = \phi_{1_R}$ mit dem Gruppenhomomorphismus ϕ_{1_R} aus der ersten universellen Eigenschaft von $(\mathbf{Z}, +)$ als Gruppe. Man rechnet nach, daß

[9] Diese Bedingung wird dadurch motiviert, daß sie äquivalent zu $m_1 - n_1 = m_2 - n_2$ ist, wenn man alle Differenzen bereits zur Verfügung hätte. Dies erschließt sich via beidseitiger Addition von $n_1 + n_2$.

[10] Für den Nachweis, daß $\sim$ tatsächlich eine Äquivalenzrelation ist, verweisen wir auf den Beweis von Satz 1.2.18 im Skriptum zur Linearen Algebra.

[11] vgl. Definitionen 1.2.53 und 1.2.65 im Skriptum zur Linearen Algebra.

[12] Welcher 1 auf das Einselement $1_R \in R$ abbildet.

ϕ ein Ringhomomorphismus ist. Damit hat jede ganze Zahl $n \in \mathbf{Z}$ eine Interpretation $n \cdot 1_R = \phi(n)$ in einem beliebigen Ring R mit Eins. Oft schreiben wir einfach $n \in R$, anstatt $n \cdot 1_R$ oder $\phi(n)$, wohlwissen, daß für $n \neq 0$ in $\mathbf{Z}$ in R trotzdem $n = 0_R$ gelten kann.

Abschließend erinnern wir an die Definition des Absolutbetrages und der Ordnungsrelation auf $\mathbf{Z}$: F ur $n \in \mathbf{Z}$ gelte

$$|n| := \begin{cases} n, & \text{sofern } n \in \mathbf{N}, \\ -n, & \text{sofern } n \notin \mathbf{N}. \end{cases}$$

Für beliebige $m, n \in \mathbf{Z}$ sei weiterhin

$$m \leq n \quad :\Leftrightarrow \quad \exists k \in \mathbf{N} : \; m + k = n.$$

Diese ist eine totale Ordnungsrelation (vgl. Definition 1.1.16 und Proposition 1.1.36 aus Abschnit 1.1.10 im Skriptum zur Linearen Algebra), welche mit Addition und Multiplikation in folgendem Sinne verträglich ist:

(a) $\forall m, n, k \in \mathbf{Z}$:
$$m \leq n \quad \Rightarrow \quad m + k \leq n + k,$$

(b) $\forall m, n \in \mathbf{Z}$, $k \in \mathbf{N}$:
$$m \leq n \quad \Rightarrow \quad m \cdot k \leq n \cdot k,$$

(c) $\forall m, n \in \mathbf{Z}$:
$$m, n \leq 0 \quad \Rightarrow \quad m \cdot n \geq 0.$$

Außerdem haben wir für beliebiges $n \in \mathbf{Z}$ die Äquivalenz

$$0 \leq n \quad \Leftrightarrow \quad n \in \mathbf{N}.$$

Für den Betrag gelten dann die wichtigen Eigenschaften

(a) Homogenität: $\forall m, n \in \mathbf{Z}$:
$$|m \cdot n| \; = \; |m| \cdot |n|, \tag{1.11}$$

(b) Dreiecksungleichung: $\forall m, n, k \in \mathbf{Z}$:
$$|m - n| \; \leq \; |m - k| + |k - n|, \tag{1.12}$$

(c) Archimedisches Axiom: $\forall n \in \mathbf{N} \; \exists m \in \mathbf{Z}$:
$$n \; < \; |m|. \tag{1.13}$$

1.4 Teilbarkeitslehre

Die multiplikative Struktur von $\mathbf{N}$ beziehungsweise $\mathbf{Z}$ spielt in der Zahlentheorie eine fundamentale Rolle. Eines unserer Ziele in diesem Abschnitt wird es sein, den Fundamentalsatz der Arithmetik über die Existenz und Eindeutigkeit der Primzerlegung zu beweisen. Hierzu benötigen wir jedoch einige Hilfsmittel.

1.4.1 Division mit Rest

Es seien $n \in \mathbf{N}$ und $d \in \mathbf{N}$ natürliche Zahlen mit $d \neq 0$. Wir setzen $n_0 := n$. Wenn $n = n_0 > d$, können wir d von n abziehen und erhalten eine Zahl $n_1 = n - d$. Sofern $n_1 > d$, können wir wieder d von n_1 abziehen und erhalten

$$n_2 \;=\; n_1 - d \;=\; (n-d) - d \;=\; n - 2d.$$

Diesen Prozeß können wir so lange wiederholen, bis in der k-ten Iteration $n_k < d$ gilt. Da im k-ten Schritt wegen $d > 0$ die Zahl n_k echt kleiner als n_{k-1} ist, muß dieser Prozeß abbrechen, dank des Wohlordnungsprinzips: Die Menge

$$M \;:=\; \{n_k | n_k \text{ wie oben}\}$$

ist nicht leer und enthält aufgrund des Wohlordnungsprinzips (Satz 1.2.3) ein minimales Element n_m. Aufgrund obiger Betrachtung, daß die Folge $n_0, n_1, \ldots$ streng monoton fallend ist, muß m automatisch ein maximaler Index sein, mit anderen Worten: M ist endlich, sodaß obiges Verfahren in der Tat abbricht und $n_m < d$ gilt.

Fassen wir die iterativen Subtraktionen von d zu einer einzigen zusammen, so erhalten wir

$$n_m \;=\; n - m \cdot d.$$

Zusammenfassend gilt damit

$$n \;=\; m \cdot d + n_m$$

mit $n_m < d$.

Satz 1.4.1 (Division mit Rest in $\mathbf{Z}$)**.** *Es seien $n, d \in \mathbf{Z}$ mit $d \neq 0$. Dann existieren eindeutig bestimmte $q, r \in \mathbf{Z}$ mit*

$$n \;=\; q \cdot d + r, \tag{1.14}$$

und $0 \leq r < |d|$.

Wir nennen r den *Rest* der Division von n durch d.

Beweis. Die *Existenz* im Fall $n, d \in \mathbf{N}$ haben wir bereits im Vorfeld abgehandelt. Die anderen Fälle lassen sich auf diesen reduzieren, was wir der geneigten Leserschaft als Übungsaufgabe überlassen.

Die *Eindeutigkeit* ergibt sich wie folgt: Sei $n = q \cdot d + r = q' \cdot d + r'$ mit $q, q', r, r' \in \mathbf{Z}$ und $0 \leq r, r' < |d|$. Dann erhalten wir durch Umstellen dieser Identität

$$q \cdot d - q' \cdot d \;=\; r' - r,$$

also

$$(q - q') \cdot d \;=\; r' - r.$$

Einerseits dürfen wir annehmen, daß $r \leq r'$, sodaß $0 \leq r' - r < |d|$. Andererseits zeigt die letzte Gleichung, daß die Differenz von r' und r ein Vielfaches von d ist.

Bis auf einen Vorzeichenwechsel bei q und q' dürfen wir annehmen, daß d positiv ist. Dann gilt für die linke Seite $0 \leq (q - q') \cdot d$, sodaß auch $0 \leq q - q'$ gilt. Wenn $q \neq q'$ ist, ergibt sich hieraus $q - q' \geq 1$, was $d \leq (q - q') \cdot d$ zur Folge hat. Wegen $(q - q') \cdot d = r' - r < d$ kann dieser Fall nicht eintreten. Es gilt also $q = q'$ und damit auch zwangsläufig wegen $r' - r = 0$ auch $r = r'$, was zu zeigen war. □

1.4.2 Teiler

Definition 1.4.2 (Teiler)**.** Es sei $n \in \mathbf{Z}$. Wir nennen ein $d \in \mathbf{Z}$ einen *Teiler* von n, wenn ein $q \in \mathbf{Z}$ mit $n = q \cdot d$ existiert. Wir nennen dann q den *Quotienten* der Division von n durch d. Wir sagen in diesem Fall auch, daß d die Zahl n *teilt* und schreiben für diese Aussage symbolisch $d \mid n$. Entsprechend bezeichne $d \nmid n$ ihre Negation: d teilt n *nicht*.

Beispiel 1.4.3. Die Zahl $n = 6$ besitzt die Teiler $d = 1, 2, 3, 6$ mit entsprechenden Quotienten $q = 6, 3, 2, 1$. Weitere Teiler sind entsprechend $d = -1, -2, -3, -6$.

Beispiel 1.4.4. $d = 1$ ist Teiler eines jeden $n \in \mathbf{Z}$ und 0 wird von jedem $n \in \mathbf{Z}$ geteilt: $0 = 0 \cdot n$.

Bemerkung 1.4.5. Aufgrund der Eindeutigkeit des Restes bei Division mit Rest teilt d genau dann n, wenn der Rest r der entsprechenden Division 0 ist.

Proposition 1.4.6 (Teilbarkeit als Relation)**.** *Teilbarkeit definiert auf* $\mathbf{Z}$ *eine Relation mit folgenden Eigenschaften:*

(a) Reflexivität: $\forall n \in \mathbf{Z}$:

$$n \mid n.$$

(b) Transitivität: $\forall m, n, k \in \mathbf{Z}$:

$$m \mid n \ \wedge \ n \mid k \quad \Rightarrow \quad m \mid k.$$

(c) Schwache Antisymmetrie: $\forall m, n \in \mathbf{Z}$:

$$m \mid n \ \wedge \ n \mid m \quad \Rightarrow \quad m = \pm n.$$

Weiterhin gelten:

(d) Verträglichkeit mit Addition: $\forall d, m, n \in \mathbf{Z}$:

$$d \mid m \ \wedge \ d \mid n \quad \Rightarrow \quad d \mid (m \pm n).$$

(e) Verträglichkeit mit Multiplikation: $\forall d, e, m, n \in \mathbf{Z}$:

$$d \mid m \ \wedge \ e \mid n \quad \Rightarrow \quad d \cdot e \mid m \cdot n.$$

Beweis. Die *Reflexivität* ist klar, da $n = 1 \cdot n$, mithin $n \mid n$ für jedes $n \in \mathbf{Z}$.

Die *Transitivität* ist eine Konsequenz der Assoziativität der Multiplikation: Wenn $m \mid n$ und $n \mid k$, so finden wir $d, e \in \mathbf{Z}$ mit $n = d \cdot m$ und $k = e \cdot n$. Hieraus ergibt sich schließlich

$$k \ = \ e \cdot n \ = \ e \cdot (d \cdot m) \ = \ (e \cdot d) \cdot m,$$

was $m \mid k$ nachweist.

Die *Schwache Antisymmetrie* ergibt sich wie folgt: Seien $m, n \in \mathbf{Z}$ mit $m \mid n$ und $n \mid m$. Dann finden wir als wie zuvor $d, e \in \mathbf{Z}$ mit $n = d \cdot m$ und $m = e \cdot n$. Ist $m = 0$, so

ergibt sich hiermit $n = 0$ und umgekehrt. Im Fall $m \neq 0$ erhalten wir analog zum Beweis der Transitivität

$$m \;=\; e \cdot n \;=\; e \cdot (d \cdot m) \;=\; (e \cdot d) \cdot m,$$

also dank der Kürzungseigenschaft in $\mathbf{N}$ (deren Gültigkeit sich auf $\mathbf{Z}$ erweitert und welche anwendbar ist, da $m \neq 0$)

$$e \cdot d \;=\; 1.$$

Damit sind $d, e \in \mathbf{Z}^\times$ Einheiten des Ringes $\mathbf{Z}$. Die einzigen Einheiten sind jedoch ± 1, was $d = e = \pm 1$ zeigt. Damit gilt $m = \pm n$, was zu zeigen war.

Die Beweise von (d) und (e) verlaufen analog. □

Bemerkung 1.4.7. Die Teilbarkeitsrelation genügt gemäß Proposition 1.4.6 allen Axiomen einer Ordnungsrelation, abgesehen von der Antisymmetrie. Schränken wir die Teilbarkeitsrelation auf die natürlichen Zahlen $\mathbf{N}$ ein, dann zeigt die schwache Antisymmetrie in (c), daß wir tatsächlich eine Ordnungsrelation erhalten. Diese ist jedoch keine totale Ordnungsrelation, d. h. nicht alle Paare von Elementen sind vergleichbar: Es gilt beispielsweise weder $2 \mid 3$ noch $3 \mid 2$. Diese Problematik führt uns zum Begriff des größten gemeinsamen Teilers: Dieser quantifiziert, was zwei ganze Zahlen „gemeinsam“ haben.

1.4.3 Größte gemeinsame Teiler

Definition 1.4.8 (Größter gemeinsamer Teiler)**.** Es sei $M \subseteq \mathbf{Z}$ eine Teilmenge. Wir nennen ein $d \in \mathbf{Z}$ einen *gemeinsamen Teiler* der Elemente aus M, für alle $n \in M$ stets $d \mid n$ gilt. Ein $d \in \mathbf{Z}$ heißt ein *größter gemeinsamer Teiler*, wenn d ein gemeinsamer Teiler der Elemente aus M ist und wenn für *jeden* gemeinsamen Teiler d' der Elemente aus M stets $d' \mid d$ gilt.

Bemerkung 1.4.9. Wir sprechen explizit *nicht* von *dem* größten gemeinsamen Teiler, da für jeden (größten) gemeinsamen Teiler d auch $-d$ ein (größter) gemeinsamer Teiler ist. Letztendlich liegt diese Ambiguität darin begründet, daß die Teilbarkeitsrelation auf $\mathbf{Z}$ nicht antisymmetrisch ist. Da wir bereits wissen, daß ihre Einschränkung auf $\mathbf{N}$ antisymmetrisch ist, macht es Sinn, von *dem* größten gemeinsamen *positiven* Teiler zu sprechen: Denn sind $d, d' \in \mathbf{N}$ größte gemeinsame Teiler einer Menge M, so ergibt sich hieraus per Definitionem $d \mid d'$ und $d' \mid d$, mithin also $d = d'$.

Bevor wir die Existenz größter gemeinsamer Teiler beweisen können, müssen wir einige Eigenschaften gemeinsamer Teiler erarbeiten.

Proposition 1.4.10. *Es sei $M \subseteq \mathbf{Z}$ eine Teilmenge. Dann besitzen folgende Mengen jeweils die selben gemeinsamen Teiler:*

(i) Wenn $0 \in M$, so besitzen M und $M \setminus \{0\}$ die selben gemeinsamen Teiler.

(ii) Wenn $m \in M$, so besitzen M und $M' := \{n - m \mid n \in M,\, n \neq m\} \cup \{m\}$ die selben gemeinsamen Teiler.

(iii) Wenn $m \in M$, so besitzen M und $M \setminus \{m\} \cup \{-m\}$ die selben gemeinsamen Teiler.

Die selben Aussagen gelten mutatis mutandis auch für größte gemeinsame Teiler.

Beweis. Ad (i): Wir beobachten zunächst, daß per Definitionem *jedes* $d \in \mathbf{Z}$ ein Teiler von 0 ist, denn $0 = 0 \cdot n$. Damit besitzen M und $M \setminus \{0\}$ stets die selben gemeinsamen Teiler.
Ad (ii): Wenn d ein gemeinsamer Teiler zweier Elemente $m, n \in \mathbf{Z}$ ist, dann ist d gemäß Aussage (d) aus Proposition 1.4.6 auch ein Teiler von $m - n$, mithin ein gemeinsamer Teiler von m und $n - m$. Ist umgekehert d ein gemeinsamer Teiler von m und $n - m$, so ist d wieder dank Aussage (d) aus selbiger Propsition ebenfalls ein gemeinsamer Teiler von m und $(n - m) + m = n$. Das zeigt, daß wir in der Menge M das Element n durch die Differenz $n - m$ ersetzen dürfen, ohne dabei die Menge der gemeinsamen Teiler zu verändern. Das zeigt (ii).
Ad (iii): Da für jedes $m \in M$ die Elemente m und $-m$ die selben Teiler besitzen (man nutze $-m = (-1) \cdot m$ und $m = (-1) \cdot (-m)$ aus), dürfen wir in M jedes Element durch seine Negation ersetzen, ohne die Menge der gemeinsamen Teiler dabei zu verändern. Mithin gilt (iii).

Daß Mengen, deren Elemente die selben gemeinsamen Teiler besitzen die selben größten gemeinsamen Teiler besitzen (sofern diese existieren), ergibt sich aus der Definition der größten gemeinsamen Teiler. □

Proposition 1.4.10 erlaubt es uns, die Bestimmung bzw. den Nachweis der Existenz eines größten gemeinsamen Teilers von M auf einfachere Fälle zu reduzieren. Dies führt uns zur ersten Formulierung des *Euklidischen Algorithmus*, welcher die Existenz eines größten gemeinsamen Teilers für beliebige Teilmengen $M \subseteq \mathbf{Z}$ sicherstellt und zugleich einen Algorithmus zur Bestimmung eines größten gemeinsamen Teilers darstellt:
Sei $M \subseteq \mathbf{Z}$ eine Teilmenge.

(i) Wir dürfen annehmen, daß sämtliche Elemente in M nichtnegativ sind, indem wir negative Elemente durch ihre Negationen ersetzen.

(ii) Ist $M = \emptyset$ leer, so ist $d = 0$ ein größter gemeinsamer Teiler.

(iii) Gilt $M = \{n\}$ mit $n \neq 0$, so sind $\pm n$ die größten gemeinsamen Teiler.

(iv) Ist $0 \in M$, so dürfen wir 0 aus M entfernen, d. h. wir ersetzen M durch $M \setminus \{0\}$ und prüfen, ob (ii) oder (iii) zutrifft. Andernfalls führen wir Schritt (v) aus:

(v) Sei $m \in M$ ein minimales Element. Wir ersetzen alle von m verschiedenen Elemente n aus M durch die Differenzen $n - m$ oder, etwas effizienter, durch den Rest r der Division von n durch m. Danach springen wir zurück zu Schritt (iv).

Es gilt, sich zu überzeugen, daß obiger Algorithmus korrekt ist und stets terminiert. Die *Korrektheit* der Schritte (ii) und (iii) ist klar. Die Korrektheit der Schritte (i), (iv) und (v) ergibt sich unmittelbar aus Proposition 1.4.10. Wir bemerken, daß aufgrund von (i) und der Operationen in (iv) und (v) stets garantiert werden kann, daß die Elemente in M *nichtnegativ sind*. Es gilt also stets $M \subseteq \mathbf{N}$ in den Schritten (ii) bis (v). Damit existiert das minimale Element m in (v) dank des Wohlordnungsprinzips stets und aufgrund von (iv) gilt stets $m > 0$, weswegen die Division durch m in (v) wohldefiniert ist.

Es bleibt also zu zeigen, daß wir in endlich vielen Iterationen eine Menge M entsteht, auf welche (ii) oder (iii) anwendbar ist, da in diesen beiden Schritte jeweils einen größten gemeinsamen Teiler bzw. sogar alle größten gemeinsamen Teiler bestimmt werden.

Wir bemerken vorweg, daß M unendlich sein kann[13]. Sei also M zunächst beliebig. Schritt (v) sorgt dafür, daß die Elemente in M nach einer Iteration von (v) sämtlich zwischen 0 und m liegen, sofern wir Division durch m mit Rest auf alle von m verschiedenen Elemente in M anwenden und diese durch den entsprechenden Rest ersetzen (vgl. Satz 1.4.1). Insbesondere produziert Schritt (v) eine Menge $M \subseteq \{0, 1, 2, \ldots, m\}$, welche die selben Teiler und damit auch die selben größten gemeinsamen Teiler besitzt wie die Ausgangsmenge. Insbesondere ist dieses neue M endlich.

So lange $|M| \geq 2$ nach Anwendung von Schritt (iv), d. h. so lange M mindestens zwei Elemente enthält, nachdem eine möglicherweise enthaltene Null aus M gestrichen wurde, führt jede weitere Iteration von Schritt (v) dazu, daß das minimale Element der $k+1$-ten Iteration *echt kleiner ist* als das minimale Element der vorangegangenen k-ten Iteration, denn aus dem minimalen Element m zu Beginn in der k-ten Iteration wird nach Anwendung von (v) ein maximales Element und so lange $|M| \geq 2$, gibt es also ein echt kleineres Element als m in der Ausgabemenge $M \subseteq \{0, 1, 2, \ldots, m\}$ der k-ten Iteration von Schritt (v).

Damit muß aufgrund des Wohlordnungsprinzips der Algorithmus nach endlich vielen Schritten eine Menge M produzieren, welche nur noch ein oder kein Element enthält, womit dann automatisch (ii) oder (iii) zutrifft, was zu zeigen war.

Korollar 1.4.11 (Existenz größter gemeinsamer Teiler)**.** *Jede Teilmenge $M \subseteq \mathbf{Z}$ besitzt einen größten gemeinsamen Teiler.*

Konkret im Fall einer zweielementigen Menge $M = \{x, y\}$ sieht der Euklidische Algorithmus wie folgt aus:

(i) Wenn $x < 0$, ersetze x durch $-x$, wenn $y < 0$, ersetze y durch $-y$.

(ii/iii/iv) Ist $x = 0$, so ist $d = y$ ein größter gemeinsamer Teiler. Ist $y = 0$, so ist $d = x$ ein größter gemeinsamer Teiler. Ist $M = \{x\}$ einelementig, so ist $d = x$ ein größter gemeinsamer Teiler.

(v) Wir nehmen oBdA an, daß $x \geq y$. Teile x durch y, um Rest r mit $0 \leq r < y$ zu erhalten (es gilt dann $x = q \cdot y + r$), ersetze x durch y und y durch r, d. h. ss gilt nach diesem Schritt $M = \{y, r\}$. Springe zurück zu (ii/iii).

Wir bemerken, daß durch Schritt (i) die Menge M einelementig werden kann: Wenn z. B. $M = \{3, -3\}$, so wird hieraus in Schritt (i) die Menge $M = \{3\}$.

Im Folgenden bezeichnen wir mit $\operatorname{ggT} M$ den eindeutig bestimmten *nichtnegativen größten gemeinsamen Teiler* einer Teilmenge $M \subseteq \mathbf{N}$. Wenn $M = \{x_1, \ldots, x_n\}$ endlich ist, schreiben wir auch $\operatorname{ggT}(x_1, \ldots, x_n)$ anstatt $\operatorname{ggT}\{x_1, \ldots, x_n\}$, wobei in $(x_1, \ldots, x_n)$ ein Eintrag mehrfach vorkommen kann.

Beispiel 1.4.12. Wir möchten den größten gemeinsamen Teiler von 20 und 15 bestimmen.

[13] z. B. ist $M = \mathbf{Z}$ zulässig!

Wir wenden den Euklidischen Algorithmus an:

$$\begin{aligned}
\mathrm{ggT}(20,15) &= \mathrm{ggT}(1\cdot 15+5,15) && (\text{da } 20 = 1\cdot 15+5)\\
&= \mathrm{ggT}(5,15)\\
&= \mathrm{ggT}(15,5)\\
&= \mathrm{ggT}(3\cdot 15+0,5) && (\text{da } 15 = 3\cdot 15+0)\\
&= \mathrm{ggT}(0,5)\\
&= \mathrm{ggT}(5)\\
&= 5.
\end{aligned}$$

Beispiel 1.4.13. Wir bestimmen analog den größten gemeinsamen Teiler von 187 und 51:

$$\begin{aligned}
\mathrm{ggT}(187,51) &= \mathrm{ggT}(3\cdot 51+34,51) && (\text{da } 187 = 3\cdot 51+34)\\
&= \mathrm{ggT}(34,51)\\
&= \mathrm{ggT}(51,34)\\
&= \mathrm{ggT}(1\cdot 34+17,34) && (\text{da } 51 = 1\cdot 34+17)\\
&= \mathrm{ggT}(17,34)\\
&= \mathrm{ggT}(34,17)\\
&= \mathrm{ggT}(2\cdot 17+0,17) && (\text{da } 32 = 2\cdot 17+0)\\
&= \mathrm{ggT}(0,17)\\
&= 17.
\end{aligned}$$

Bemerkung 1.4.14. Es ist bemerkenswert, daß wir den größten gemeinsamen Teiler von 187 und 51 bestimmen konnten, **ohne** eine Primfaktorzerlegung beider Zahlen zu kennen.

Bemerkung 1.4.15. Rechnen wir rückwärts, so ergibt sich aus der letzten Rechnung exemplarisch:

$$\begin{aligned}
17 &= 0+17 && (0 \text{ war der Rest der letzten Division})\\
&= (34-2\cdot 17)+17 && (\text{da } 0 = 34-2\cdot 17)\\
&= 34-1\cdot 17 && (\text{Zusammenfassen})\\
&= 34-1\cdot(51-1\cdot 34) && (17 = 51-1\cdot 34)\\
&= 2\cdot 34-1\cdot 51 && (\text{Zusammenfassen})\\
&= 2\cdot(187-3\cdot 51)-1\cdot 51 && (34 = 187-3\cdot 51)\\
&= 2\cdot 187-7\cdot 51 && (\text{Zusammenfassen})
\end{aligned}$$

Damit haben wir den größten gemeinsamen Teiler 17 als **Z**-Linearkombination der Eingabe 187 und 51 dargestellt:

$$\mathrm{ggT}(187,51) = 17 = 2\cdot 187-7\cdot 51.$$

Die Verallgemeinerung dieses Vorgehens auf den allgemeinen Euklidischen Algorithmus wird als *erweiterter Euklidischer Algorithmus* bezeichnet. Hier wird in jedem Schritt

zusätzlich Buch geführt, sodaß die Koeffizienten einer Linearkombination des größten gemeinsamen Teilers durch die Eingabe en passant bestimmt werden können.

Der Übersichtlichkeit zubliebe diskutieren wir hier den *binären Fall*, d. h. den erweiterten Euklidischen Algorithmus mit zwei ganzen Zahlen als Eingabe.

Seien $x, y \in \mathbf{Z}$ zwei ganze Zahlen. Wir nehmen an, daß $x, y \neq 0$ und definieren

$$r_0 := x, \quad r_1 := y, \tag{1.15}$$

sowie

$$s_0 := 1, \quad s_1 := 0, \tag{1.16}$$

$$t_0 := 0, \quad t_1 := 1. \tag{1.17}$$

Bis $r_{k+1} = 0$, bestimmen wir in der k-ten Iteration den Rest r_{k+1}, sowie den Koeffizienten s_{k+1} rekursiv wie folgt:
Es bezeichne $q_k \in \mathbf{Z}$ der Quotienten der Division mit Rest von r_{k-1} durch r_k, d. h. es gelte

$$r_{k-1} = q_k r_k + r_{k+1}, \quad \text{mit } 0 \leq r_{k+1} < |r_k|. \tag{1.18}$$

Dann gilt bzw. wir definieren definieren weiterhin

$$r_{k+1} = r_{k-1} - q_k r_k, \quad s_{k+1} = s_{k-1} - q_k s_k, \quad t_{k+1} = t_{k-1} - q_k t_k. \tag{1.19}$$

Satz 1.4.16 (Erweiterter Euklidischer Algorithmus)**.** *Der erweiterte Euklidische Algorithmus bestimmt zu gegebenen ganzen Zahlen $x, y \in \mathbf{Z}$ mit $x, y \neq 0$ einen größten gemeinsamen Teiler $d = r_\ell$ und es gilt weiterhin*

$$d = s_\ell \cdot x + t_\ell \cdot y, \tag{1.20}$$

wenn der Algorithmus nach ℓ Schritten terminiert, d. h. wenn $r_{\ell+1} = 0$.

Beweis. Wir überzeugen uns zunächst davon, daß der Algorithmus nach endlich vielen Schritten terminiert und r_ℓ ein größter gemeinsamer Teiler ist.

Hierzu beobachten wir, daß im Gegensatz zum zuvor formulierten Algorithmus folgende Unterschiede gegeben sind: Es wird auf den ersten Blick nicht sichergestellt, daß $r_k \geq 0$. Weiterhin wird nicht explizit in jeder Iteration durch das Minimum geteilt.

In der Tat ist der Fall $y < 0$ möglich, womit per Definitinem auch $r_1 = y < 0$. Andererseits gilt ab der ersten Iteration, daß stets $r_k \geq 0$ für $k \geq 2$ ist, denn für $k \geq 2$ ist r_k per Definition Rest einer Division mit Rest und damit automatisch nichtnegativ.

Die Bedingung in Gleichung (1.18), daß $r_{k+1} < |r_k|$ ist, garantiert ebenfalls, daß ab der zweiten Iteration stets durch das Minimum geteilt wird, wie es der ursprüngliche Algorithmus forciert.

Im Fall, daß $|x| < |y|$ und $x \geq 0$, so gilt der ersten Iteration

$$r_0 = x = 0 \cdot y + x, \quad 0 \leq x < |r_0|,$$

was zeigt, daß sich hier $q_1 = 0$ und $r_2 = x$ ergibt (Eindeutigeit der Division mit Rest, vgl. Satz 1.4.1), womit automatisch $|r_2| < |r_1|$, d. h. die erste Iteration führt in diesem Falld dazu, daß die Reihenfolge von x und y vertauscht wird, sodaß ab diesem Zeitpunkt stets durch das Minimum geteilt werden kann.

Wenn $|x| < |y|$ und $x < 0$, so erhalten wir in der ersten Iteration

$$r_0 \;=\; (\pm 1) \cdot y - x \;=\; |y| - x, \quad 0 \leq |y| - x < |r_0|,$$

womit hier $q_1 = \pm 1$ (abhängig vom Vorzeichen von y) und $r_2 = |y| - x$ gilt, was wieder die Korrektheit der folgenden Iterationen garantiert.

Letzendlich der Algorithmus, weil er wie soeben beobachtet ab der zweiten Iteration stimmt er mit dem ursprünglichen Algorithmus übereinstimmt, wobei ggf. x durch $|y| - x$ ersetzt wird, was dank Proposition 1.4.10 (ii) und (iii) zulässig ist.

Um schlußendlich Identität (1.20) einzusehen, so genügt es diesbezüglich zu zeigen, daß in der k-ten Iteration stets

$$r_k \;=\; s_k \cdot x + t_k \cdot y$$

garantiert werden kann. In der Tat: Im Fall $k = 0$ gilt per Definition $s_0 = 1$ und $t_0 = 0$, was

$$r_0 \;=\; x \;=\; 1 \cdot x + 0 \cdot y \;=\; s_0 \cdot x + t_0 \cdot y$$

zeigt. Im Fall $k = 1$ gilt per Definition $s_1 = 0$ und $t_1 = 1$, was

$$r_1 \;=\; y \;=\; 0 \cdot x + 1 \cdot y \;=\; s_1 \cdot x + t_1 \cdot y$$

zeigt.

Die anderen Fälle ergeben sich nun mittels vollständiger Induktion. Seien also

$$r_{k-1} \;=\; s_{k-1} \cdot x + t_{k-1} \cdot y$$

und

$$r_k \;=\; s_k \cdot x + t_k \cdot y$$

jeweils für ein gegebenes $k \geq 1$ zutreffend. Dann erhalten wir aufgrund der Definition der Koeffizienten s_{k+1} und t_{k+1} in (1.19):

$$\begin{aligned}
s_{k+1} \cdot x + t_{k+1} \cdot y \;&=\; (s_{k-1} - q_k s_k) \cdot x \;+\; (t_{k-1} - q_k t_k) \cdot y \\
&=\; s_{k-1}x - q_k s_k x \;+\; t_{k-1}y - q_k t_k y && \text{(Ausmultiplizieren)} \\
&=\; s_{k-1}x + t_{k-1}y - q_k s_k x - q_k t_k y && \text{(Umstellen)} \\
&=\; \underbrace{s_{k-1}x + t_{k-1}y}_{=r_{k-1}} - q_k \cdot \underbrace{(s_k x - t_k y)}_{=r_k} && \text{(Ausklammern)} \\
&=\; r_{k-1} - q_k r_k && \text{(Induktionsvoraussetzung)} \\
&=\; r_{k+1}, && \text{(Definition } r_{k+1} \text{ in (1.18))}
\end{aligned}$$

was den Induktionsschritt vollzieht. □

Beispiel 1.4.17. Wir wenden den erweiterten Euklidischen Algorithmus auf $x = 3131$ und $y = 2418$ an:

k	r_k	q_k	s_k	t_k
0	3131		1	0
1	2418	1	0	1
2	713	3	1	-1
3	279	2	-3	4
4	155	1	7	-9
5	124	1	-10	13
6	31	4	17	-22
7	0			

Wir erhalten also

$$\mathrm{ggT}(3131, 2418) \;=\; 31 \;=\; 17 \cdot 3131 - 22 \cdot 2418.$$

Korollar 1.4.18. *Es seien $x_1, \ldots, x_n \in \mathbf{Z}$ gegeben. Dann ist für $y \in \mathbf{Z}$ die Gleichung*

$$y \;=\; \alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + \cdots + \alpha_n \cdot x_n$$

genau dann mit $\alpha_1, \ldots, \alpha_n \in \mathbf{Z}$ lösbar, wenn y ein Vielfaches eines größten gemeinsamen Teilers von $x_1, \ldots, x_n$ ist. Insbesondere ist der größte gemeinsame Teiler d von $x_1, \ldots, x_n$ eine $\mathbf{Z}$-Linearkombination von $x_1, \ldots, x_n$.

Beweis. Sei zunächst obige Gleichung lösbar, d. h. sei explizit

$$y \;=\; \alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + \cdots + \alpha_n \cdot x_n.$$

Dann teilt jeder größte gemeinsame Teiler d von $x_1, \ldots, x_n$ jedes $x_1, \ldots, x_n$ und damit aufgrund von Proposition 1.4.6 (d) daher auch die rechte Seite dieser Gleichung. Das zeigt $d \mid y$.

Sei umgekehrt $d \mid y$ mit einem größten gemeinsamen Teiler d von $x_1, \ldots, x_n$ als wie zuvor. Wir gehen induktiv vor, um uns auf den Fall $n = 2$ zurückzuziehen. Hierzu definieren wir zunächst rekursiv eine Folge d_k wie folgt:

$$d_1 := x_1, \quad d_{k+1} = \mathrm{ggT}(d_k, x_{k+1}) \text{ für } 1 \leq k < n.$$

Iterative Anwendung von Aufgabe 4 des Übgungsblattes 1 zeigt, daß dann $d_k = \mathrm{ggT}(x_1, \ldots, x_k)$, womit oBdA $d_n = d$ gilt.

Satz 1.4.16 beschert uns dann für jedes $1 \leq k < n$ ganze Zahlen $\beta_k, \gamma_k \in \mathbf{Z}$ mit

$$d_{k+1} \;=\; \beta_k \cdot d_k + \gamma_k \cdot x_{k+1}. \tag{1.21}$$

Da $d_1 = x_1$ sehen wir, daß (1.21) im Fall $k = 1$ die Gestalt

$$d_2 = \beta_1 \cdot x_1 + \gamma_1 \cdot x_2$$

annimmt. Setzen wir diese Relation für d_2 in Relation (1.21) im Fall $k = 2$ ein, erhalten wir

$$d_2 \;=\; \beta_2 \cdot (\beta_1 \cdot x_1 + \gamma_1 \cdot x_2) + \gamma_k \cdot x_{k+1} \;=\; \beta_2\beta_1 \cdot x_1 + \beta_2\gamma_1 \cdot x_2 + \gamma_2 \cdot x_3.$$

Insbesondere ist d_2 eine ganzzahlige Linearkombination von x_1, x_2, x_3.

Fahren wir so fort, indem wir eine Darstellung von d_k als Linearkombinatikon von $x_1, x_2, \ldots, x_{k+1}$ in (1.21) im Fall k einsetzen, so sehen wir induktiv, daß $d = d_n$ eine ganzzahlige Linearkombination von $x_1, \ldots, x_n$ ist. Damit ist auch jedes ganzzahlige Vielfache y von d eine ganzzahlige Linearkombination von $x_1, \ldots, x_n$, was zu zeigen war. □

1.4.4 Teilerfremde Zahlen

Eine erste wichtige Anwendung des Euklidischen Algorithmus liegt im Studium teilerfremder Zahlen.

Definition 1.4.19 (Teilerfremdheit)**.** Wir nennen ganze Zahlen $x_1, \ldots, x_n \in \mathbf{Z}$ *teilerfremd*, wenn $\mathrm{ggT}(x_1, \ldots, x_n) = 1$.

Folgende Aussage ist eine wichtige Anwendung des erweiterten Euklidischen Algorithmus.

Proposition 1.4.20 (Teilerfremdheitskriterium)**.** *Seien $x_1, \ldots, x_n$ ganze Zahlen. Dann sind $x_1, \ldots, x_n$ genau dann teilerfremd, wenn es $\alpha_1, \ldots, \alpha_n \in \mathbf{Z}$ gibt, mit*

$$\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + \cdots + \alpha_n \cdot x_n \;=\; 1.$$

Beweis. Seien zunächst $x_1, \ldots, x_n$ teilerfremd. Dann folgt die behauptete Existenz von $\alpha_1, \ldots, \alpha_n \in \mathbf{Z}$ aus Satz 1.4.16 bzw. Korollar 1.4.18.

Seien umgekehrt $\alpha_1, \ldots, \alpha_n \in \mathbf{Z}$ derart, daß

$$\alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + \cdots + \alpha_n \cdot x_n \;=\; 1.$$

Dann zeigt Korollar 1.4.18, daß 1 ein Vielfaches des größten gemeinsamen Teilers d von $x_1, \ldots, x_n$ ist. Insbesondere ergibt sich damit $d \mid 1$, was wegen $1 \mid d$ zeigt, daß $d = \pm 1$, was zu zeigen war. □

Eine erste Anwendung ist die nützliche

Proposition 1.4.21. *Seien $x_1, \ldots, x_n$ ganze Zahlen, welche nicht sämtlich 0 sind. Dann gilt $d := \mathrm{ggT}(x_1, \ldots, x_n) \neq 0$ und $\frac{x_1}{d}, \ldots, \frac{x_n}{d}$ sind teilerfremd.*

Beweis. Zunächst beobachten wir, daß 0 kein größter gemeinsamer Teiler von $x_1, \ldots, x_n$ ist, wenn nicht $x_1 = \cdots = x_n = 0$ gilt, was wir ausgeschlossen hatten.

Wir wenden zunächstSatz 1.4.16 bzw. Korollar 1.4.18 an: Es existieren $\alpha_1, \ldots, \alpha_n \in \mathbf{Z}$ mit

$$d \;=\; \alpha_1 \cdot x_1 + \alpha_2 \cdot x_2 + \cdots + \alpha_n \cdot x_n.$$

Teilen wir beide Seiten durch d, so erhalten wir

$$1 \;=\; \alpha_1 \cdot \frac{x_1}{d} + \alpha_2 \cdot \frac{x_2}{d} + \cdots + \alpha_n \cdot \frac{x_n}{d}.$$

Damit folgt aus Proposition 1.4.20, daß $\frac{x_1}{d}, \ldots, \frac{x_n}{d}$ teilerfremd sind. □

Der Beweis illustriert sehr schön, wie mithilfe einer $\mathbf{Z}$-Linearkombination argumentiert werden kann. Einerseits nutzen wir ihre Existenz für d, welche durch den erweiterten Euklidischen Algorithmus garantiert wird, und andererseits nutzen wir dann die resultierende Linearkombination für $d/d = 1$, um auf die Teilerfremdheit von $\frac{x_1}{d}, \ldots, \frac{x_n}{d}$ zu schließen.

Proposition 1.4.22. *Seien x, y_1, y_2 jeweils ganze Zahlen. Wenn x, y_1 teilerfremd und x, y_2 teilerfremd, so sind auch x, $y_1 \cdot y_2$ teilerfremd.*

Mit anderen Worten: Zu gegebenem $x \in \mathbf{Z}$ ist die Menge $\{y \in \mathbf{Z} \mid \mathrm{ggT}(x, y) = 1\}$ der zu x teilerfremden Zahlen unter Multiplikation abgeschlossen, d. h. für Elemente y_1, y_2 dieser Menge ist auch das Produkt $y_1 \cdot y_2$ ein Element dieser Menge.

Beweis. Seien x, y_1 und x, y_2 jeweils teilerfremd. Laut Satz 1.4.16 finden wir $\alpha_1, \alpha_2, \beta_1, \beta_2 \in \mathbf{Z}$ mit

$$\alpha_1 \cdot x + \alpha_2 \cdot y_1 \;=\; 1, \quad \text{und} \quad \beta_1 \cdot x + \beta_2 \cdot y_2 \;=\; 1.$$

Betrachten wir das Produkt dieser beiden Gleichungen, so erhalten wir

$$\begin{aligned}
1 &= 1 \cdot 1 \\
&= (\alpha_1 \cdot x + \alpha_2 \cdot y_1) \cdot (\beta_1 \cdot x + \beta_2 \cdot y_2) \\
&= \alpha_1 \cdot \beta_1 \cdot x^2 + \alpha_1 \cdot \beta_2 \cdot x \cdot y_2 + \alpha_2 \cdot \beta_1 \cdot y_1 \cdot x + \alpha_2 \cdot \beta_2 \cdot y_1 \cdot y_2 \quad \text{(Ausmultiplizieren)} \\
&= \underbrace{(\alpha_1 \cdot \beta_1 \cdot x + \alpha_1 \cdot \beta_2 \cdot y_2 + \alpha_2 \cdot \beta_1 \cdot y_1)}_{=:\gamma_1} \cdot x + \underbrace{\alpha_2 \cdot \beta_2}_{=:\gamma_2} \cdot y_1 \cdot y_2 \qquad (x \text{ ausklammern}) \\
&= \gamma_1 \cdot x + \gamma_2 \cdot y_1 \cdot y_2,
\end{aligned}$$

mit $\gamma_1, \gamma_2 \in \mathbf{Z}$. Damit sind x und das Produkt $y_1 \cdot y_2$ gemäß Proposition 1.4.20 teilerfremd, was zu zeigen war. □

1.4.5 Primzahlen

Mit den Erkenntnissen aus dem vorigen Abschnitt in der Hand, können wir uns Primzahlen und der Primzahlzerlegung widmen.

Klassisch werden *Primzahlen* als natürliche Zahlen $p > 1$ definiert, welche lediglich 1 und p als positive Teiler besitzen. Bei Polynom führt die analoge Definition zu *irreduziblen Polynomen*, weswegen man im Fall eines allgemeinen nullteilerfreien Ringes auch von *irreduziblen Elementen* spricht. Primzahlen sind also irreduzible Elemente in $\mathbf{Z}$. Aber was sind Primelemente?

Definition 1.4.23 (Primzahl)**.** Eine natürliche Zahl $p \in \mathbf{N}$ heißt *Primzahl* wenn $p \neq 1$ und wenn für alle $d \in \mathbf{N}$:

$$d \mid p \quad \Rightarrow \quad d = 1 \;\vee\; d = p. \tag{1.22}$$

Übersetzt in die ganzen Zahlen bedeutet (1.22)

$$\forall d \in \mathbf{Z}: \quad d \mid p \quad \Rightarrow \quad d = \pm 1 \;\vee\; d = \pm p, \tag{1.23}$$

d. h. (1.22) und (1.23) sind äquivalent.

Für Primzahlen ist Teilerfremdheit einfach zu prüfen.

Proposition 1.4.24 (Teilerfremdheitskriterium für Primzahlen)**.** *Es seien $p \in \mathbf{N}$ eine Primzahl und $n \in \mathbf{Z}$ sei beliebig. Dann sind äquivalent*

(i) $p \nmid n$, d. h. p ist kein Teiler von n.

(ii) p und n sind teilerfremd.

Beweis. Die Implikation (ii) ⇒ (i) ist klar, da $p > 1$.

Die Implikation (i) ⇒ (ii) ergibt sich wie folgt. Es bezeichne $d \geq 0$ einen größten gemeinsamen Teiler von p und n. Da d ein Teiler von p ist, gilt entweder $d = 1$ oder $d = p$, da p eine Primzahl ist. Da sich im zweiten Fall $d = p$ automatisch $p \mid n$ ergibt, muß im Fall $p \nmid n$ stets $d = 1$ gelten, mithin sind p und n in diesem Fall teilerfremd, was zu zeigen war. □

Proposition 1.4.25 (Primzahlkriterium)**.** *Für $p \in \mathbf{N}$ sind äquivalent:*

(i) p ist eine Primzahl.

(ii) Es gilt $p \neq 1$ und für alle $a, b \in \mathbf{Z}$ gilt die Implikation

$$p \mid a \cdot b \quad \Rightarrow \quad p \mid a \vee p \mid b. \tag{1.24}$$

Beweis. Sei zunächst p eine Primzahl. Dann gilt $p \neq 1$ per Definitionem und wenn $a, b \in \mathbf{Z}$ gegeben sind, dann ergibt sich aus $p \nmid a$ und $p \nmid b$ jeweils die Teilerfremdheit von p, a und p, b (vgl. Proposition 1.4.24). Damit sind auch p und $a \cdot b$ teilerfremd (Proposition 1.4.22), was zeigt, daß (1.24) gilt. Mithin gilt die Implikation (i) $\Rightarrow$ (ii).

Sei umgekehrt p eine natürliche Zahl, welche der Bedingung in (ii) genügt. Sei $d \in \mathbf{N}$ ein Teiler von p, d. h. wir finden ein $k \in \mathbf{N}$ mit $p = d \cdot k$. Damit gilt $p \mid d \cdot k$, was wegen Bedingung (1.24) $p \mid d$ oder $p \mid k$ zur Folge hat. Das wiederum hat $p = d$ oder $p = k$ zur Folge (vgl. Aussage (c) in Proposition 1.4.6). Das zeigt, daß p eine Primzahl ist, mithin gilt (i). □

Korollar 1.4.26. *Es sei p eine Primzahl und es seien $q_1, \ldots, q_r \in \mathbf{Z}$ beliebig. Dann gilt*

$$p \mid q_1 \cdot q_2 \cdot \ldots \cdot q_r \quad \Rightarrow \quad \exists 1 \leq i \leq r : \; p \mid q_i.$$

Mit anderen Worten: Wenn eine Primzahl p ein Produkt teilt, dann teilt sie bereits einen der Faktoren.

Beweis. Der Fall $r = 1$ ist klar. Der allgemeine Fall ergibt sich induktiv: Sei $r \geq 2$ und es gelte die Behauptung für alle Produkte $q_1, \ldots, q_{r-1}$ mit $r - 1$ Faktoren. Sei also

$$p \mid q_1 \cdot q_2 \cdot \ldots \cdot q_r,$$

dann gilt auch

$$p \mid (q_1 \cdot q_2 \cdot \ldots \cdot q_{r-1}) \cdot q_r,$$

womit aufgrund von (1.24) aus Proposition 1.4.25

$$p \mid q_1 \cdot q_2 \cdot \ldots \cdot q_{r-1}, \quad \text{oder} \quad p \mid q_r.$$

Im letzteren Fall sind wir fertig, und im ersteren Fall schließen wir aus der Induktionshypothese, daß p einen der ersten $r - 1$ Faktoren teilt, was zu zeigen war. □

Bemerkung 1.4.27. Wenn $q_1, \ldots, q_r$ Primzahlen sind, besagt Korollar 1.4.26, daß jeder Primteiler p des Produktes $q_1 \cdot q_2 \cdot \ldots \cdot q_r$ bereits mit einem der Primfaktoren q_i übereinstimmt, denn die einzigen positiven Teiler von q_i sind in diesem Fall 1 und q_i selbst.

1.4.6 Primfaktorzerlegung

Wir verfolgen zwei Ziele: Wir möchten die *Existenz* einer Primfaktorzerlegung einer beliebigen ganzen Zahl $n \neq 0$ einsehen und ebenfalls die *Eindeutigkeit* einer solchen Primfaktorzerlegung garantieren. Die Eindeutigkeit wird sich induktiv aus Korollar 1.4.26 ergeben (vgl. Bemerkung 1.4.27). Für den Nachweis der Existenz benötigen wir folgendes

Lemma 1.4.28 (Existenz von Primteilern)**.** *Es sei $n > 1$ eine natürliche Zahl. Dann existiert eine Primzahl p, welche n teilt.*

Beweis. Sei $n > 1$ eine beliebige natürliche Zahl. Wir betrachten die Menge

$$T \;:=\; \{d \in \mathbf{N} \mid d > 1 \wedge d \mid n\}$$

der Teiler von n, welche größer als 1 sind. Da $n > 1$ liegt wegen $n \mid n$ die Zahl n selbst in T, sodaß $T \neq \emptyset$ gilt. Das Wohlordnungsprinzip garantiert nun, daß in T ein bzgl. $\leq$ minimales $p \in T$ existiert. Wir behaupten, daß p eine Primteiler von n ist. Da $p \in T$ ist p ein Teiler von n. Es bleibt also zu zeigen, daß p eine Primzahl ist.

Sei hierzu $d \in \mathbf{N}$ ein Teiler von p. Dann gilt $d \mid p$, was wegen $p \mid n$ auch $d \mid n$ impliziert. Wenn $d > 1$ folgt hieraus aufgrund der Definition von T automatisch $d \in T$. Die Minimalität von p garantiert $p \leq d$, was wegen $d \mid p$ automatisch $d = p$ zur Folge hat[14]. Das zeigt, daß entweder $d = 1$ oder $d = p$ gilt. Da $p > 1$ (wegen $p \in T$) schließen wir, daß p tatsächlich eine Primzahl ist (vgl. Definition 1.4.23). □

Satz 1.4.29 (Primfaktorzerlegung)**.** *Jede ganze Zahl $n \neq 0$ besitzt eine eindeutige* Primfaktorzerlegung *der folgenden Gestalt:*

$$n \;=\; \varepsilon \cdot p_1^{v_1} \cdot p_2^{v_2} \cdot \ldots \cdot p_r^{v_r}, \tag{1.25}$$

wobei $\varepsilon \in \{\pm 1\}$, $r \geq 0$, $v_1, \ldots, v_r \geq 1$ und $p_1, \ldots, p_r$ paarweise verschiedene Zahlen sind. Die Darstellung (1.25) *ist eindeutig bis auf Reihenfolge der Primzahlen $p_1, \ldots, p_r$.*

Wir bemerken, daß auch $n = \pm 1$ zulässig ist. Hier gilt $r = 0$ und das Produkt

$$p_1^{v_1} \cdot p_2^{v_2} \cdot \ldots \cdot p_r^{v_r}$$

ist in diesem Fall *per Definitionem*[15] gleich 1.

Beweis. Existenz: Die Existenz der Zerlegung (1.25) ergibt sich für gegebenes $n \in \mathbf{Z}$, $n \neq 0$ wie folgt. Durch geeignete Wahl von ε können wir uns zunächst auf den Fall $n > 0$ d. h,. $n \in \mathbf{N}$ zurückziehen (denn für $n < 0$ gilt $-n > 0$). D. h. wir müssen zeigen, daß jede natürliche Zahl $n > 0$ eine Primfaktorzerlegung besitzt.

Wir hatten bereits bemerkt, daß $n = 1$ eine Primfaktorzerlegung besitzt. Bezeichne also

$$M \;:=\; \{n \in \mathbf{N} \mid n > 1,\ n \text{ besitzt keine Primfaktorzerlegung}\}$$

die Menge der Ausnahmen, d. h. die Menge derjenigen positiven natürlichen Zahlen, für welche *keine* Zerlegung der Form (1.25) existiert.

Angenommen, der Fall $M \neq \emptyset$ tritt ein. Dann existiert in M aufgrund des Wohlordnungsprinzips ein minimales $n \in M$. Aufgrund der Definition von M gilt dann $n > 1$, sodaß Lemma 1.4.28 anwendbar ist: Es existiert also ein Primteiler $p \mid n$. Wegen $\frac{n}{p} < n$ liegt die natürliche Zahl $\frac{n}{p}$ *nicht* in M, besitzt also eine Primfaktorzerlegung:

$$\frac{n}{p} \;=\; p_1^{v_1} \cdot p_2^{v_2} \cdot \ldots \cdot p_r^{v_r},$$

[14] Denn $d \mid p$ impliziert seinerseits $d \leq p$ und $\leq$ ist als Ordnungsrelation antisymmetrisch, d. h. $d \leq p$ und $p \leq d$ implizieren zusammengenommen $d = p$.

[15] Dufgrund seiner rekursiven Definition im Allgemeinen, welche den Fall $r = 0$ als Ausgangspunkt nimmt.

mit $r \geq 0$ und paarweise verschiedenen Primzahlen $p_1, \ldots, p_r$ und positiven Exponenten $v_1, \ldots, v_r$. Multiplizieren wir diese Zerlegung mit p, so erhalten wir mit

$$n \;=\; p_1^{v_1} \cdot p_2^{v_2} \cdot \ldots \cdot p_r^{v_r} \cdot p$$

eine Primfaktorzerlegung von n, im Widerspruch dazu, daß $n \in M$.

Wir schließen hieraus, daß M leer sein muß und insbesondere jedes $0 \neq n \in \mathbf{N}$ eine Primfaktorzerlegung besitzt.

Eindeutigkeit: Um die Eindeutigkeit der Zerlegung (1.25) einzusehen, gehen wir induktiv vor. Da der Faktor ε aufgrund der Positivität der Faktoren $p_1, \ldots, p_r$ in der Zerlegung (1.25) eindeutig durch das Vorzeichen von n bestimmt ist, dürfen wir uns wieder auf den Fall $n \in \mathbf{N}$ zurückziehen.

Wir gehen nun induktiv vor. Der Fall $n = \pm 1$ ist klar. Sei also $n \in \mathbf{N}$, $n > 1$ und wir als Induktionshypothese nehmen an, daß alle positiven natürlichen Zahlen $< n$ die Eindeutigkeit der Zerlegung (1.25) gegeben ist.

Seien nun

$$n \;=\; p_1^{v_1} \cdot p_2^{v_2} \cdot \ldots \cdot p_r^{v_r} \;=\; q_1^{w_1} \cdot q_2^{w_2} \cdot \ldots \cdot q_s^{w_s},$$

zwei Zerlegungen der Gestalt (1.25), d. h. $p_1, \ldots, p_r$ und $q_1, \ldots, q_s$ sind jeweils paarweise verschiedene Primzahlen und $v_1, \ldots, v_r, w_1, \ldots, w_r \geq 1$.

Wegen $n > 1$ gilt jeweils $r, s \geq 1$ (ansonsten wäre $n = 1$!). Das bedeutet, daß mit p_r ein Primteiler von n existiert. Damit teilt p_r das Produkt $q_1^{w_1} \cdot q_2^{w_2} \cdot \ldots \cdot q_s^{w_s}$, also dank Korollar 1.4.26 auch einen der Primfaktoren $q_1, \ldots, q_r$. Deshalb stimmt p_r also mit einem q_i für geeignetes $1 \leq i \leq s$ überein (vgl. Bemerkung 1.4.27). Da wir die Reihenfolge der Primaktoren letztendlich irrelevant ist, dürfe wir annehmen, daß $i = s$ gilt, also $p_r = q_s$.

Zusammenfassend ergibt sich nach Teilen durch p_r, daß

$$\frac{n}{p_r} \;=\; p_1^{v_1} \cdot p_2^{v_2} \cdot \ldots \cdot p_{r-1}^{v_{r-1}} \cdot p_r^{v_r - 1} \;=\; q_1^{w_1} \cdot q_2^{w_2} \cdot \ldots \cdot q_{s-1}^{w_{s-1}} \cdot q_s^{w_s - 1}.$$

Nun ist die Primzerlegung von $\frac{n}{p_r}$ aufgrund unserer Induktionshypothese eindeutig, denn $\frac{n}{p_r} < n$. Das bedeutet, daß $r = s$ gelten muß und wir annehmen dürfen, daß $p_1 = q_1$, $p_2 = q_2, \ldots, p_{r-1} = q_{r-1}$ ($p_r = q_r$ wissen wir bereits!), sowie und $v_1 = w_1, \ldots, v_{r-1} = w_{r-1}$ und auch $v_r - 1 = w_r - 1$, was $v_r = w_r$ zur Folge hat. Hieraus ergibt sich unmittelbar, daß die beiden Primfaktorzerlegungen von n übereinstimmen, was den Eindeutigkeitsbeweis abschließt. □

Der Satz über die Existenz und Eindeutigkeit der Primfaktorzerlegung hat viele Anwendungen. Eine unmittelbare Anwendung ist

Korollar 1.4.30 (Teilerbestimmung)**.** *Es sei $n \neq 0$ eine ganze Zahl mit Primfaktorzerlegung* (1.25)*. Dann ist die Menge der Teiler von n explizit gegeben durch*

$$\{\pm p_1^{e_1} \cdot p_2^{e_2} \cdot \ldots \cdot p_r^{e_r} \mid 0 \leq e_1 \leq v_1,\, 0 \leq e_2 \leq v_2, \ldots,\, 0 \leq e_r \leq v_r\}.$$

Insbesondere besitzt n genau $2 \cdot (v_1 + 1) \cdot (v_2 + 1) \cdot \ldots \cdot (v_r + 1)$ paarweise verschiedene Teiler in $\mathbf{Z}$.

In $\mathbf{N}$ sind es entsprechend halb so viele Teiler: $(v_1 + 1) \cdot (v_2 + 1) \cdot \ldots \cdot (v_r + 1)$ um genau zu sein.

Beweis. Wenn $d \mid n$, so existiert ein $k \in \mathbf{Z}$ mit $n = d \cdot k$. Durch Vergleich der Primfaktorzerlegungen von n, d und k sowie unter Ausnutzung der Eindeutigkeit der Primfaktorzerlegungen ergibt sich die angegebende Menge von Teilern.

Die behauptete Anzahl $2 \cdot (v_1 + 1) \cdot (v_2 + 1) \cdot \ldots \cdot (v_r + 1)$ ergibt sich daraus, daß das Vorzeichen $\pm$ eines Teilers d beliebig ausfallen kann (dies erklärt den Faktor 2) und der Primfaktor p_i unabhängig von Vorzeichen und den anderen Primfaktoren mit einer beliebigen Vielfachheit $0 \leq e_i \leq v_i$ in d auftreten darf (dies erklärt den Faktor (v_i+1)). □

Die Primfaktorzerlegung in $\mathbf{Z}$ erlaubt uns ebenfalls eine Beschreibung rationaler Zahlen mithilfe von Primzahlen:

Korollar 1.4.31. *Jede rationale Zahl $0 \neq x \in \mathbf{Q}$ besitzt eine eindeutige Darstellung der Form*

$$x \;=\; \varepsilon \cdot p_1^{v_1} \cdot p_2^{v_2} \cdot \ldots \cdot p_r^{v_r}, \tag{1.26}$$

wobei $\varepsilon \in \{\pm 1\}$, $r \geq 0$, $0 \neq v_1, \ldots, v_r \in \mathbf{Z}$ und $p_1, \ldots, p_r$ paarweise verschiedene Zahlen sind. Die Darstellung (1.26) *ist eindeutig bis auf Reihenfolge der Primzahlen $p_1, \ldots, p_r$.*

Beweis. Wir schreiben $x = \frac{a}{b}$ mit $a \in \mathbf{Z}$ und $0 < b \in \mathbf{N}$. Da $x \neq 0$ gilt auch $a \neq 0$. Bezeichne $d = \mathrm{ggT}(a, b)$. Wegen

$$x \;=\; \frac{a}{b} \;=\; \frac{d \cdot a/d}{d \cdot b/d} \;=\; \frac{d}{d} \cdot \frac{a/d}{b/d} \;=\; \frac{a/d}{b/d}$$

dürfen wir a durch a/d und b durch b/d ersetzen. Insbesondere dürfen wir annehmen, daß a und b *teilerfremd* sind (vgl. Proposition 1.4.21).

Seien nun

$$a \;=\; \varepsilon \cdot p_1^{v_1} \cdot p_2^{v_2} \cdot \ldots \cdot p_r^{v_r},$$

und

$$b \;=\; q_1^{w_1} \cdot q_2^{w_2} \cdot \ldots \cdot q_s^{w_s},$$

jeweils Primfaktorzerlegungen von a und b. Dann erhalten wir

$$x \;=\; a \cdot b^{-1} \;=\; \varepsilon \cdot p_1^{v_1} \cdot p_2^{v_2} \cdot \ldots \cdot p_r^{v_r} \cdot q_1^{-w_1} \cdot q_2^{-w_2} \cdot \ldots \cdot q_s^{-w_s}.$$

Aufgrund der Teilerfremdheit von a und b sind die $r + s$ Primzahlen $p_1, \ldots, p_r, q_1, \ldots, q_s$ paarweise verschieden, womit wir eine Darstellung von x der Form (1.26) gefunden haben. Das weist die Existenz nach.

Umgekehrt erhalten durch Multiplikation aller Primzahlpotenzen $p_i^{-v_i}$ mit negativem Exponenten $v_i < 0$ in (1.26) eine Primfaktorzerlegung des Nenners b von x, was zeigt, daß diese Faktoren eindeutig durch b bestimmt sind. Analog erhalten wir aus dem Produkt von ε und den Primzahlpotenzen $p_i^{v_i}$ aus (1.26) mit positiven Exponenten $v_i > 0$ eine Primfaktorzerlegung des Zählers a von x, womit diese eindeutig durch a bestimmt sind. Das reduziert die Eindeutigkeit auf die bereits bekannte Eindeutigkeit der Primfaktorzerlegung in $\mathbf{Z}$ aus Satz 1.4.29, sowie die Eindeutigkeit von a und b.

Letztere ist noch zu beweisen. Seien $c \in \mathbf{Z}$ und $0 < d \in \mathbf{N}$ teilerfremd mit

$$\frac{a}{b} \;=\; \frac{c}{d}.$$

Aufgrund der Definition rationaler Zahlen ist dies (nach „Erweitern“) äquivalent zu

$$ad \;=\; bc.$$

Wir würden jetzt gerne schließen, daß sich heraus aufgrund der Teilerfremdheit von a und b ergibt, daß $a \mid c$ gelten muß. Das gilt in der Tat — folgt allerdings nicht unmittelbar, da a im Allgemeinen keine Primzahl ist.

Erst aus der Tatsache, daß a, b, c, d,sowie ad und bc jeweils eindeutige Primfaktorzerlegungen besitzen und einem Vergleich dieser Primfaktorzerlegungen läßt sich dann mithilfe der Teilerfremdheit von a und b folgern, daß $ad = bc$ impliziert, daß $a \mid c$ und umgekehrt $c \mid a$, sowie analog $d \mid b$ und $b \mid d$ folgen. Zusammenfassend ergibt sich daraus dann $a = c$ und $b = d$, was zu zeigen war. □

Weil sie so wichtig ist, halten wir die Beobachtung im letzten Beweis fest.

Korollar 1.4.32. *Es seien a, b, c jeweils von Null verschiedene ganze Zahlen. Wenn a und b teilerfremd sind, dann impliziert $a \mid b \cdot c$ bereits $a \mid c$.*

Beweis. Dies ergibt sich aus einem Vergleich der Primfaktorzerlegungen von a, b und c, vgl. Korollar 1.4.30.

Alternatives Argument mit implizitem Euklidischen Algorithmus: Es bezeichne $d = \mathrm{ggT}(a, c)$. Wir müssen zeigen, daß $a|d$ gilt, da genau dann $a \mid c$. Dann sind dank Proposition 1.4.21 a/d und c/d teilerfremd. Da a und b nach Voraussetzung teilerfremd sind, sind a/d und b ebenfalls teilerfremd, sodaß aufgrund von Proposition 1.4.22 auch a/d und bc/d teilerfremd sind. Andererseits ist wegen $a \mid bc$ auch a/d ein Teiler von bc/d, womit wir schließen, daß a/d den größten gemeinsamen Teiler 1 von a/d und bc/d teilt. Insbesondere gilt $a/d = \pm 1$, was $a = \pm d$ zeigt, was wiederum zu zeigen war.

Bei diesem Argument findet der Euklidische Algorithmus keine direkte Anwendung, aber er geht in die Beweise der beiden Propositionen 1.4.21 und 1.4.22 ein.

Alternatives Argument via Euklidischem Algorithmus: Der Beweis von Proposition 1.4.22 inspiriert folgendes direktes Argument.

Da a und b teilerfremd sind, finden wir $x, y \in \mathbf{Z}$ mit $xa + yb = 1$ (vgl. Satz 1.4.16). Dann erhalten wir

$$b \cdot c \;=\; a \cdot b \cdot c \;=\; (xa + yb) \cdot b \cdot c \;=\; x \cdot ab \cdot c + y \cdot b \cdot bc.$$

Hieraus schließen wir, daß $a \cdot b$ das Produkt $b \cdot c$ teilt, denn ab teilt den ersten Summanden und da $a \mid cb$ und $b \mid b$ teilt es auch den zweiten, also teilt es ebenfalls die Summe, welche mit bc üebereinstimmt (vgl. Proposition 1.4.6 (d)). Division durch b zeigt, daß die Teilbarkeitsrelation $ab \mid bc$ unmittelbar $a \mid c$ zur Folge hat, was zu zeigen war. □

Korollar 1.4.33 (k-te Potenzen)**.** *Sei $k \geq 1$ gegeben. Dann ist eine ganze Zahl $n \in \mathbf{Z}$ ist genau dann eine k-te Potenz, wenn entweder $n = 0$, oder wenn alle Exponenten $v_1, \ldots, v_r$ in der Primfaktorzerlegung* (1.25) *durch k teilbar sind, sowie zusätzlich n positiv ist, falls k gerade ist.*

Beweis. Der Fall $n = 0$ ist klar.

Angenommen $n \neq 0$ ist eine k-te Potenz. Dann gilt $n = m^k$ mit einem $0 \neq m \in \mathbf{Z}$. Dieses m besitzt eine Primfaktorzerlegung der Gestalt

$$m \;=\; \delta \cdot q_1^{w_1} \cdot q_2^{w_2} \cdot \ldots \cdot q_s^{w_s}$$

mit $\delta \in \{\pm 1\}$, $s \geq 0$, $w_1, \ldots, w_s \geq 1$ und paarweise verschiedenen Primzahlen $q_1, \ldots, q_s$. Dann erhalten wir mit

$$n \;=\; m^k \;=\; \delta^k \cdot q_1^{k \cdot w_1} \cdot q_2^{k \cdot w_2} \cdot \ldots \cdot q_s^{k \cdot w_s}$$

eine Primfaktorzerlegung von n. Aufgrund der Eindeutigkeit der Primfaktorzerlegung (1.25) von n ergeben sich hieraus $r = s$ und bis auf ggf. entsprechende Anpassung der Nummerierung

$$\varepsilon \;=\; \delta^k, \text{ sowie } p_i = q_i \text{ und } v_i = k \cdot w_i \text{ für } 1 \leq i \leq r.$$

Das zeigt, daß in diesem Fall alle Exponenten v_i durch k teilbar sind und $\varepsilon = 1$ sofern k gerade ist, womit dann automatisch $n > 0$ gilt.

Umgekehrt erhalten wir analog zu obiger Rechnung eine k-te Wurzel m von n, indem wir ausgehend von der Primfaktorzerlegung (1.25) von n unter den entsprechenden Voraussetzungen wie im Korollar

$$m \;:=\; \varepsilon \cdot p_1^{v_1/k} \cdot p_2^{v_2/k} \cdot \ldots \cdot p_r^{v_r/k}$$

definieren[16]. □

Ein Höhepunkt stellt klassisch die Charakterisierung der k-ten Potenzen in $\mathbf{Q}$ dar:

Korollar 1.4.34 (k-te Potenzen in $\mathbf{Q}$)**.** *Sei $k \geq 1$ gegeben. Dann ist eine rationale Zahl $x \in \mathbf{Q}$ ist genau dann eine k-te Potenz einer rationalen Zahl, wenn entweder $x = 0$, oder wenn alle Exponenten $v_1, \ldots, v_r$ in der verallgemeinerten Primfaktorzerlegung* (1.26) *von x durch k teilbar sind, sowie zusätzlich x positiv ist, falls k gerade ist.*

Beweis. Der Beweis verläuft mutatis mutandis wie der Beweis von Korollar 1.4.33, wobei anstatt auf Satz 1.4.29 entsprechend auf Korollar 1.4.31 zurückgegriffen wird. □

Bemerkung 1.4.35. Formal ist $x \in \mathbf{Q}$ genau dann eine k-te Potenz, wenn die Gleichung

$$x \;=\; y^k$$

mit einem $y \in \mathbf{Q}$ lösbar ist. Analoges gilt für k-te Potenzen in $\mathbf{Z}$. Insbesondere ergibt sich durch Vergleich der Korollare 1.4.33 und 1.4.34, daß diese Gleichung für ein gegebenes $x \in \mathbf{Z}$ genau dann mit einem $y \in \mathbf{Z}$ lösbar ist, wenn sie mit einem $y \in \mathbf{Q}$ lösbar ist. Dies läßt sich verallgemeinern:

Sei $f \in \mathbf{Z}[X]$ ein normiertes Polynom, d. h. $f = X^k + a_{k-1}X^{k-1} + \cdots + a_1 X + a_0$ mit $a_0, a_1, \ldots, a_{k-1} \in \mathbf{Z}$. Sei $y \in \mathbf{Q}$ eine Nullstelle von f, d. h.

$$f(y) \;=\; y^k + a_{k-1}y^{k-1} + \cdots + a_1 y + a_0 \;=\; 0.$$

Wir behaupten, daß y eine ganze Zahl ist. In der Tat: Sei $y = \frac{a}{b}$ mit teilerfemden $a, b \in \mathbf{Z}$, $b \neq 0$. Dann ergibt sich aus $f(y) = 0$, durch Erweitern mit b^k, daß

$$\begin{aligned} 0 \;&=\; \left(\frac{a}{b}\right)^k \cdot b^k + a_{k-1}\left(\frac{a}{b}\right)^{k-1} \cdot b^k + \cdots + a_1\left(\frac{a}{b}\right) \cdot b^k + a_0 b^k \\ &=\; a^k + a_{k-1}a^{k-1}b + \cdots + a_1 b^{k-1}y + a_0 b^k \end{aligned}$$

[16] Die Voraussetzung garantiert, daß die Exponenten $v_1/k, \ldots, v_r/k$ sämtlich natürliche Zahlen sind. Man prüft leicht nach, daß in den zugelassenden Fällen $\varepsilon^k = \varepsilon$ gilt.

Wenn nun $p \mid b$ ein Primteiler des Nenners von y ist, dann teilt p einerseits alle Summanden der letzten Gleichung, abgesehen von a^k. Andererseits teilt p die 0, womit p aber auch a^k teilen muß, Widerspruch. Es kann also keinen Primteiler p von b geben, womit $b = \pm 1$ gilt, was bedeutet, daß $y = \pm a \in \mathbf{Z}$, was wir zeigen wollten.

Dies illustriert die Nützlichkeit der Primfaktorzerlegung für das Studium von Gleichungen mit ganzzahligen Koeffizienten. Obiges Argument ist in Essenz eine Verallgemeinerung des klassischen Beweises, weswegen die Wurzel von 2 *irrational* ist: Hier wird $f = X^2 - 2$ betrachtet und dies hat aufgrund der Existenz und Eindeutigkeit der Primfaktorzerlegung in $\mathbf{Z}$ keine Nullstelle in $\mathbf{Z}$ (vgl. Korollar 1.4.33 im Fall $k = 2$). Im Grunde genügt zum Beweis der Irrationalität ein Verweis auf Korollar 1.4.34, da letzteres Korollar bereits impliziert, daß 2 keine rationale Wurzel besitzt.

Unabhängig hiervon führt uns obige Rechnung mit dem Polynom $f = X^2 - 2$ zu folgendem klassischen Argument: Sei $y = \frac{a}{b}$ eine Quadratwurzel von 2 in $\mathbf{Q}$. Dann gilt

$$y^2 - 2 \;=\; 0 \quad \Leftrightarrow \quad \left(\frac{a}{b}\right)^2 - 2 \;=\; 0 \quad \Leftrightarrow \quad a^2 - 2 \cdot b^2 \;=\; 0.$$

Damit muß 2 ein Teiler von a^2 sein, also auch von a (da 2 Primzahl, vgl. (1.24) aus Proposition 1.4.25). Es gilt also $a = 2 \cdot \widetilde{a}$. Damit erhalten wir

$$2^2 \cdot \widetilde{a}^2 - 2b^2 \;=\; 0 \quad \Leftrightarrow \quad 2 \cdot \widetilde{a}^2 - b^2 \;=\; 0.$$

Letztere Gleichung ist (bis auf das Vorzeichen) die selbe wie die Ausgangsgleichung

$$a^2 - 2 \cdot b^2 \;=\; 0,$$

mit dem Unterschied, daß b die ursprüngliche Rolle von a und $\widetilde{a}$ die ursprüngliche Rolle von b einnimmt. Wir schließen also analog, daß b durch 2 teilbar sein muß, was wiederum analog zu einer Gleichung der Art

$$\widetilde{a}^2 - 2 \cdot \widetilde{b}^2 \;=\; 0,$$

führt. Dies geht nun unendlich lange so weiter, d. h. a und b sind beide unendlich oft durch 2 teilbar, ein Widerspruch.

Man hätte diesen Widerspruch auch schon früher herbeiführen können, wenn man a und b als teilerfremd vorausgesetzt hätte, was wir im Beweis von Korollar 1.4.34 auch tatsächlich getan haben.

Eine weitere Anwendung der eindeutigen Primfaktorzerlegung ist folgendes

Beispiel 1.4.36. In der Universität Paderborn gibt es genau 100 Büros. Um den neuen Umweltauflagen gerecht zu werden, hat der Hausmeister folgenden Arbeitsplan für das Reinigungspersonal erdacht: Die erste Schicht schaltet in jedem Büro das Licht ein, aber nicht aus. Die zweite Schicht betätigt nach Reinigung eines Büros in jedem zweiten Büro den Lichtschalter. Die dritte Schicht betätigt in jedem dritten Büro den Lichtschalter, usw. usf. In welchen Büros brennt das Licht, nachdem die 100. Schicht ihren Dienst beendet hat?

1.4.7 Primzahlen die Zweite

Satz 1.4.37. *Die Menge* $\mathbf{P} = \{2, 3, 5, 7, 11, \dots\}$ *der Primzahlen ist unendlich.*

Beweis. Nach Euklid: Angenommen, $\mathbf{P}$ ist endlich. Dann ist

$$n \ := \ \prod_{p \in \mathbf{P}} p \ + \ 1$$

eine natürliche Zahl. Wir beobachten nun zwei Dinge:

1.) Da das Produkt über alle Primzahlen mindestens 1 ist und hierzu 1 addiert wird, gilt $n > 1$, sodaß Lemma 1.4.28 über die Existenz von Primteilern auf n anwendbar ist und zeigt, daß es ein $q \in \mathbf{P}$ geben muß, welches n teilt.

2.) Per Konstruktion von n gilt

$$n \ = \ \left(\prod_{\substack{p \in \mathbf{P} \\ p \neq q}} p \right) \cdot q \ + \ 1.$$

Damit bleibt nach Division von n durch q der Rest 1 übrig (es gilt $q > 1$!). Die Eindeutigkeit der Division mit Rest zeigt dann, daß deshalb $q \nmid n$ gelten muß, ein Widerspruch zu underer ersten Beobachtung. Deshalb kann $\mathbf{P}$ nicht endlich sein.

Nach Euler: Wir nehmen an, daß $\mathbf{P}$ endlich ist und beobachten zunächst, daß für jedes $p \in \mathbf{P}$ wegen $p > 1$ gilt

$$p^{-1} \ = \ \frac{1}{p} \ < \ 1.$$

Insbesondere $1 - p^{-1} \neq 0$, sodaß wir die reelle Zahl

$$\zeta(1) \ := \ \prod_{p \in \mathbf{P}} \frac{1}{1 - p^{-1}}$$

betrachten dürfen. Diese ist aufgrund der vorausgesetzten Endlichkeit von $\mathbf{P}$ ein endliches Produkt.

Weiterhin dürfen wir wegen $p^{-1} < 1$ jeden einzelnen Faktor als geometrische Reihe

$$\frac{1}{1 - p^{-1}} \ = \ \sum_{k=0}^{\infty} \left(p^{-1}\right)^k \ = \ \sum_{k=0}^{\infty} p^{-k}$$

interpretieren.

Es gilt also

$$\zeta(1) \ = \ \prod_{p \in \mathbf{P}} \sum_{k=0}^{\infty} p^{-k} \ = \ \prod_{p \in \mathbf{P}} \left(1 + p^{-1} + p^{-2} + \dots\right).$$

Die Beweisidee ist nun Folgende: Da die rechterhand auftretenden unendlichen Reihen sämtlich absolut konvergent sind, dürfen wir das endliche Produkt rechterhand ausmultiplizieren, womit wir

$$\zeta(1) \ = \ \sum_{(v_i)_i \in \mathbf{N}^r} \left(p_1^{v_1} p_2^{v_2} \cdot \dots \cdot p_r^{v_r}\right)^{-1}$$

erhalten, wenn $\mathbf{P} = \{p_1, p_2, \ldots, p_r\}$. Aufgrund der Existenz und Eindeutigkeit der eindeutigen Primfaktorzerlegung für natürliche Zahlen vereinfacht sich diese Summe zu

$$\zeta(1) \;=\; \sum_{n\geq 1} n^{-1} \;=\; \sum_{n\geq 1} \frac{1}{n}.$$

Hier liegt nun der Hund begraben: Die harmonische Reihe rechterhand divergiert, d. h. es gilt

$$\sum_{n\geq 1} \frac{1}{n} \;=\; \infty.$$

Damit kann $\zeta(1)$ keine endliche reelle Zahl sein, Widerspruch. Insbesondere kann $\mathbf{P}$ nicht endlich sein. □

Bemerkung 1.4.38. In allen obigen Argumenten ist der Fall $\mathbf{P} = \emptyset$ ist zuläßig. Insbesondere wird gezeigt, daß es *mindestens eine Primzahl* gibt. Allerdings wird in beiden Beweisen bereits vorausgesetzt, daß Primteiler einer natürlichen Zahl $n > 1$ stets existieren, was bereits sehr nah an der Existenz einer Primzahl ist da natürliche Zahlen $n > 1$ offensichtlich existieren. Das wahre Aufgabe in obigen Beweisen besteht darin, die Existenz von Primteilern bzw. im Fall von Eulers Argument die Existenz und Eindeutigkeit der Primfaktorzerlegung zusammen mit der Unendlichkeit der Menge der natürlichen Zahlen geschickt auszunutzen, um auf die Unendlichkeit von $\mathbf{P}$ schließen zu können.

Bemerkung 1.4.39. Euler betrachtete die inzwischen nach Riemann benannte Riemannsche ζ-Funktion

$$\zeta(s) \;:=\; \sum_{n\geq 1} \frac{1}{n^s}.$$

Diese konvergiert absolut für $s > 1$ und für derartige Argumente zeigte Euler, daß

$$\zeta(s) \;=\; \prod_{p\in\mathbf{P}} \frac{1}{1-p^{-s}}$$

ein gegebenenfalls unendliches aber stets absolut konvergentes Produkt ist. Aus diesem Grund sprechen wir hier heutzutage von einem *Eulerprodukt*. Aufgrund der Tatsache, daß die harmonische Reihe divergiert, was wir in obigem Beweis ausgenutzt haben, besitzt $\zeta(s)$ bei $s = 1$ einen Pol, in welchem sich die Unendlichkeit der Menge der Primzahlen manifestiert. Eine genauere Analyse dieses Zusammenhanges, insbesondere unter Einbeziehung komplexer Argumente $s \in \mathbf{C}\setminus\{1\}$, führt zu starken Aussagen über die Verteilung von Primzahlen und letztendlich zur Riemannschen Vermutung.

Bemerkung 1.4.40. Eine kleine Modifikation Euklids Arguments erlaubt es, beliebig viele Primzahlen rekursiv zu bestimmen: Angenommen, wir haben bereits Primzahlen $p_1, \ldots, p_r$ bestimmt, wobei $r = 0$ zuläßig ist.

Dann betrachten wir wie in Euklids Argument die Zahl

$$n_r \;:=\; p_1 \cdot p_2 \cdot \ldots \cdot p_r \;+\; 1.$$

Wir wissen, dank Division mit Rest, daß jeder Primteiler $p \mid n_r$ von $p_1, \ldots, p_r$ verschieden ist. Bestimmen wir z. B. einen minimalen Teiler $d > 1$ von n, so erhalten wir mit $p_{r+1} :=$

d eine weitere Primzahl (vgl. Beweis von Lemma 1.4.28). Dieses Verfahren können wir so lange wiederholen, bis wir so viele Primzahlen gesammelt haben, wie uns lieb ist. Effizienter ist natürlich, aus n_r nicht nur ein p_{r+1} zu extrahieren, sondern rekursive alle Primteiler von n zu bestimmen, indem zunächst ein minimaler Teiler $d' > 1$ von $n_r/p_{r+1}^{v_{r+1}}$ bestimmt wird, etc. pp.

Beispiel 1.4.41. Zu Beginn kennen wir noch keine Primzahlen, d. h. es gilt $r = 0$. Dann betrachten wir nach Euklid

$$n_0 \;=\; \prod_{i=1}^{0} p_i \;+\; 1 \;=\; 1 \;+\; 1 \;=\; 2.$$

Ein minimaler Teiler > 1 von 2 ist $p_1 := 2$. Das ist unsere erste Primzahl. Wegen $n_0/p_1 = 2/2 = 1$ können wir aus n_0 keine weiteren Primzahlen gewinnen.

Also betrachten wir im nächsten Schritt

$$n_1 \;=\; \prod_{i=1}^{1} p_i \;+\; 1 \;=\; p_1 \;+\; 1 \;=\; 2 \;+\; 1 \;=\; 3.$$

Da $2 \nmid 3$ (das wissen wir schon per Konstruktion!) ist $p_2 = 3$ ein minimaler Teiler > 1 und damit prim. Wieder erhalten wir wegen $n_1/p_2 = 3/3 = 1$ aus n_1 keine weiteren Primzahlen.

Also betrachten wir

$$n_2 \;=\; \prod_{i=1}^{2} p_i \;+\; 1 \;=\; p_1 \cdot p_2 \;+\; 1 \;=\; 2 \cdot 3 \;+\; 1 \;=\; 7.$$

Per Konstruktion gilt $2 \nmid 7$ und $3 \nmid 7$. Das schließt ebenfalls 4 und 6 als Teiler aus. Wegen $7 = 1 \cdot 5 + 2$ gilt $5 \nmid 7$, sodaß ist $p_3 = 7$ ein minimaler Teiler > 1 ist und damit unsere dritte Primzahl darstellt. Wieder erhalten wir wegen $n_2/p_3 = 7/7 = 1$ aus n_2 keine weiteren Primzahlen.

Analog ergibt sich

$$n_3 \;=\; \prod_{i=1}^{3} p_i \;+\; 1 \;=\; p_1 \cdot p_2 \cdot p_3 \;+\; 1 \;=\; 2 \cdot 3 \cdot 7 \;+\; 1 \;=\; 43.$$

Hier ist wieder $p_4 = 43$ der minimale Teiler > 1 und damit prim.

Analog ergibt sich

$$n_4 \;=\; \prod_{i=1}^{4} p_i \;+\; 1 \;=\; p_1 \cdot p_2 \cdot p_3 \cdot p_4 \;+\; 1 \;=\; 2 \cdot 3 \cdot 7 \cdot 43 \;+\; 1 \;=\; 1807.$$

Hier passiert es zum ersten Mal, daß mit $p_5 = 13$ der minimale Teiler > 1 von n nicht mit n übereinstimmt. Aus $n_4/p_5 = 139$ erhalten wir die weitere Primzahl $p_6 = 139$.

Bemerkung 1.4.42. In Beispiel 1.4.41 haben wir gesehen, daß die Bestimmung von Primzahlen mit obigem Verfahren nicht sehr effizient ist. Ein weiterer Nachteil besteht darin, daß die Primzahlen nicht in ihrer natürlichen Reihenfolge, d. h. nicht nach Größte geordnet entdeckt werden.

Bei der Suche nach Abhilfe stellen wir fest, daß anstatt des Produktes

$$n_r \ := \ p_1 \cdot p_2 \cdot \ldots \cdot p_r \ + \ 1.$$

ab $r \geq 2$ wir alternativ

$$n_r \ := \ p_1 \cdot p_2 \cdot \ldots \cdot p_r \ - \ 1.$$

betrachten könnten. Dann entdecken wir z. B. $p_3 = 5$ vor 7. Allerdings wächst n_r und damit auch der Aufwand sehr stark[17].

Grundsätzlich könnten wir ebenfalls größere Exponenten für $p_1, \ldots, p_r$ zulassen, wodurch jedoch noch größere Zahlen entstehen — es sei denn, wir betrachten für ein festes r mehrere Exponenten auf einmal.

Nachteil dieses Ansatzes wäre, daß wir gegebenenfalls Primzahlen doppelt entdecken würden, was wiederum eine gewisse Buchhaltung erfordern würde.

Spinnt man diesen Gedanken konsequent zu Ende und betrachtet alle möglichen Exponenten, stellt man fest, daß man den Spieß umdrehen sollte: Anstatt Zahlen zu konstruieren, aus welchen neue Primzahlen gewonnen werden, sollten stattdessen alle nicht-Primzahlen markiert werden. Das, was dann übrig bleibt, sind die Primzahlen. Dies führt uns zum *Sieb des Eratosthenes*:

(i) Liste alle positiven natürlichen Zahlen bis zu einer Schranke $N \geq 2$ auf:

$$M_0 \ := \ \{1, 2, 3, \ldots, N-1, N\}.$$

(ii) Entferne die 1 und erhalte:

$$M_1 \ := \ \{2, 3, \ldots, N\}.$$

Setze $k := 1$.

(iii) Das minimale Element p_k in M_k ist eine Primzahl.

(iv) Entferne p_k und alle seine Vielfachen $\geq N$ aus M_k und erhalte so eine Teilmenge $M_{k+1} \subsetneq M_k$.

(v) So lange $M_{k+1} \neq \emptyset$ ersetze k durch $k+1$ und wiederhole Schritt (iii).

Satz 1.4.43 (Sieb des Eratosthenes)**.** *Obiges Verfahren von Eratosthenes bricht nach einer endlichen Anzahl r von Iterationen ab. Die Ausgabe $p_1, p_2, \ldots, p_r$ besteht aus der austeigend geordneten Folge aller Primzahlen $\leq N$.*

Beweis. Zunächst beobachten wir, daß per Konstruktion die Streichung von p_k aus M_k in Schritt (iv) dazu führt, daß $\#M_{k+1} < \#M_k$. Damit garantiert das Wohlordnungsprinzip[18], daß der Fall $M_{k+1} = \emptyset$ nach einer endlichen Anzahl r von Iterationen eintritt.

Wir gehen nun induktiv vor: Wir behaupten, daß in der k-ten Iteration gilt: $p_1, \ldots, p_k$ sind sämtliche Primzahlen $\leq p_{k+1}$ bzw. $\leq N$ wenn $k = r$.

Induktionsanfang: Der Fall $k = 0$ ist klar.

[17] Da Primzahlen stets ≥ 2 sind und sogar $p_i > 2$ für $i > 1$ gilt stets $n_r > 2^r$.

[18] Angewandt auf die Menge $\{\#M_k \mid k = 0, 1, 2, \ldots \text{ wie im Algorithmus}\} \subseteq \mathbf{N}$.

Induktionsschritt: $p_1, \ldots, p_k$ sind sämtliche Primzahlen $\leq p_k$ bzw. $\leq N$ wenn $k = r$.

Der Fall $k < r$: Aufgrund der Induktionshypothese, daß $p_1, \ldots, p_k$ sämtliche Primzahlen $\leq p_k$ sind, sind drei Dinge zu zeigen: $p_{k+1} > p_k$, p_k ist prim und zwischen p_k und p_{k+1} liegt keine weitere Primzahl q. Dann sind automatisch $p_1, \ldots, p_{k+1}$ alle Primzahlen bis p_{k+1} in aufsteigender Reihenfolge.

Daß $p_{k+1} > p_k$ ist, folgt automatisch, sobald wir wissen, daß p_{k+1} prim ist und nicht mit einem $p_1, \ldots, p_k$ übereinstimmt, da durch $p_1, \ldots, p_k$ gemäß Induktionshpyothese alle Primzahlen bis p_k gegeben sind.

Per Konstruktion ist p_{k+1} die kleinste natürliche Zahl > 1, welche nicht durch die Primzahlen $p_1, \ldots, p_k$ teilbar ist und daher prim. Genauer: Sei $1 < d \mid p_{k+1}$ ein Teiler von p_{k+1}. Nun ist p_{k+1} wegen $p_{k+1} \in M_{k+1}$ durch keine der Primzahlen $p_1, \ldots, p_k$ teilbar (andernfalls wäre es in der i-ten Iteration in Schritt (iv) aus M_i entfernt worden). Damit gilt auch $p_1, \ldots, p_k \nmid d$ aufgrund der Transitivität der Teilbarkeitsrelation. Damit gilt $d \in M_{k+1}$, denn es kann somit nicht in Schritt (iv) der i-ten Iteration ($1 \leq i \leq k$) aus M_i getilgt worden sein. Also impliziert die Minimalität von p_{k+1} (Schritt (iii)) $d \geq p_{k+1}$, was $d = p_{k+1}$ zur Folge hat. Das zeigt, daß p_{k+1} prim ist.

Weiterhin ist aus selbigem Grund p_{k+1} die kleinste Primzahl, welche größer als p_k ist: Sei $p_k < q \leq p_{k+1}$ eine weitere Primzahl. Dann ergibt sich $q \in M_{k+1}$, da q in Schritt (iv) der i-ten Iteration ($1 \leq i \leq k$) nicht aus M_i entfernt worden ist: $p_1, \ldots, p_k$ sind prim, $< q$ und damit insbesondere zu q teilerfremd. Die Definition von p_{k+1} als minimales Element von M_{k+1} zeigt $p_{k+1} \leq q$, was $q = p_{k+1}$ zur Folge hat, was wiederum zu zeigen war.

Der Fall $k = r$: Aus den vorangegangenen Betrachtungen wir wissen bereits, daß $p_1, \ldots, p_r$ alle Primzahlen $\leq p_r$ sind und daß im Fall $k = r$ das Verfahren abbricht, da $M_{r+1} = \emptyset$ gilt, sodaß hier also zu zeigen ist, daß p_k die größte Primzahl $\leq N$ ist, was sich analog zu obigem Fall ergibt.

Zunächst argumentieren wir etwas unsauber, daß in Schritt (iv) der i-ten Iteration alle Vielfachen von p_i aus M_i getilgt werden, weswegen aufgrund von $M_{r+1} = \emptyset$ jedes Element in $M_1 = \{1, 2, \ldots, N\}$ ein Vielfaches mindestens einer der Primzahlen $p_1, \ldots, p_r$ sein muß. Daher kann es keine weitere Primzahl in M_1 geben, was zu zeigen war.

Etwas formaler läßt sich wie folgt argumentieren: Angenommen, q ist eine Primzahl mit $p_r \leq q \leq N$. Dann liegt diese Primzahl in M_1, womit ein maximaler Index $1 \leq i \leq r$ mit $q \in M_k$ existiert. Wegen $q \notin M_{r+1}$ (letzteres ist die leere Menge), gilt in allen Fällen $q \notin M_{i+1}$. Damit muß q in Schritt (iv) der i-ten Iteration aus M_i entfernt worden sein, ist also ein Vielfaches von p_i, was wegen $q \geq p_r$ nur im Fall $i = r$ möglich ist, was $q = p_r$ zur Folge hat. Damit existieren keine weiteren Primzahlen $\leq N$, was zu zeigen war. □

Beispiel 1.4.44. Wir betrachten das Sieb des Eratosthenes exemplarisch für $N = 20$.
Ausgangspunkt in Schritt (i) des Verfahrens ist

$$M_0 \;=\; \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20\},$$

was uns in
Schritt (ii)

$$M_1 \;=\; \{2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20\},$$

sowie $k = 1$ beschert.

Schritt (iii): $p_1 := \min M_1 = 2$ ist eine Primzahl.
Schritt (iv): Entferne $p_1 = 2$ sowie alle seine Vielfachen aus M_1 und erhalte

$$M_2 \;=\; \{3, 5, 7, 9, 11, 13, 15, 17, 19\}.$$

Schritt (v): Da $M_2 \neq \emptyset$ inkrementieren wir k zu $k = 2$ und springen zurück zu
Schritt (iii): $p_2 := \min M_2 = 3$ ist eine Primzahl.
Schritt (iv): Entferne $p_2 = 3$ sowie alle seine Vielfachen aus M_2 und erhalte

$$M_3 \;=\; \{5, 7, 11, 13, 17, 19\}.$$

Schritt (v): Da $M_3 \neq \emptyset$ inkrementieren wir k zu $k = 3$ und springen zurück zu
Schritt (iii): $p_3 := \min M_3 = 5$ ist eine Primzahl.
Schritt (iv): Entferne $p_3 = 5$ sowie alle seine Vielfachen aus M_3 und erhalte

$$M_4 \;=\; \{7, 11, 13, 17, 19\}.$$

Schritt (v): Da $M_4 \neq \emptyset$ inkrementieren wir k zu $k = 4$ und springen zurück zu
Schritt (iii): $p_4 := \min M_4 = 7$ ist eine Primzahl.
Schritt (iv): etc. pp.

Auf diese Weise erhalten wir schlußendlich $2, 3, 5, 7, 11, 13, 17, 19$ als aufsteigende Folge aller Primzahlen $\leq N = 20$.

Es ist hervorzuheben, daß in diesem besonderen Fall M_3 bereits ausschließlich aus Primzahlen besteht, was auf den ersten Blick daran liegt, daß $N = 20$ recht klein ist und zu Beginn Primzahlen in sehr kleinen Abständen auftreten.

Trotzdem gibt es ein einfaches Abbruchkriterium, was hier zum Tragen kommt: Sobald für die k-te Primzahl $p_k > \sqrt{N}$ gilt, besteht die Menge M_k *ausschließlich aus Primzahlen*: Denn wenn $1 \leq n \leq N$ ein Vielfaches von p_k ist, dann gilt $n = q \cdot p_k$ mit einem $q < \sqrt{N}$, also $q < p_k$, womit n durch mindestens eine Primzahl $p_j < p_k$ teilbar ist und damit bereits in j-ten Iteration aus M_k getilgt worden sein muß. Selbiges Argument ist auf alle weiteren Iterationen $> k$ anwendbar und zeigt letztendlich induktiv, daß M_k ausschließlich aus Primzahlen besteht.

Wir halten also im Fall von $N = 20$ fest:

$$\{p \in \mathbf{P} \mid p \leq 20\} \;=\; \{2, 3\} \cup M_3 \;= = \{2, 3, 5, 7, 11, 13, 17, 19\}.$$

Diese Beobachtung halten wir fest:

Proposition 1.4.45 (Abbruchkriterium für das Sieb des Eratosthenes)**.** *Sei $N \geq 2$ gegeben. Wenn in der k-ten Iteration des Siebes von Eratosthenes $p_k > \sqrt{N}$ gilt, so besteht M_k ausschließlich aus Primzahlen.*

Bemerkung 1.4.46. Es ist *nicht* notwendig, $\sqrt{N}$ zu bestimmen, da $p_k > \sqrt{N}$ äquivalent zu $p_k^2 > N$ ist, was sich leicht berechnen und prüfen läßt. Beispielsweise gilt in obigem Fall für $N = 10$ bereits $p_3^2 = 5^2 > 20$, was erklärt, weswegen M_5 ausschließlich aus Primzahlen besteht.

Beispiel 1.4.47. Im Fall $N = 100$ ergibt sich, wie leicht aus unserem Beispiel ersichtlich ist, in der fünften Iteration $p_5 = 11$, was $p_5^2 = 11^2 = 121 > 100$ zur Folge hat. Daher besteht hier M_5 bereits ausschließlich aus Primzahlen, daß fünf Iterationen bereits ausreichend sind, um sämtliche Primzahlen ≤ 100 zu bestimmen.

Bemerkung 1.4.48. Das Verfahren von Eratosthenes ist in Anbetracht dieses Abbruchkriteriums also sehr effizient und bis heute eines der effizientesten Verfahren zur Bestimmung aller Primzahlen $\leq N$. Effizientere Verfahren sind asymptotisch genauso aufwendig, optimieren jedoch den Siebschritt etwas, um die Anzahl an Operationen pro Zahl $\leq N$ zu reduzieren. In der Praxis wird die Anwendung des Siebes von Eratosthenes nicht durch seine Laufzeit, sondern durch den hohen Speicherbedarf begrenzt. Auf einer modernen CPU dauert es bei einer guten Implementierung wenige Sekunden, bis der vorhande Arbeitsspeicher erschöpft ist und das Sieben aus diesem Grund abbrechen muß.

Wir illustrieren dies anhand folgender Rechnung: Legen wir 64 Gigabyte Arbeitsspeicher zugrunde und nehmen wir an, daß dieser in seiner Gesamtheit als Liste von $N = 2^{6+30} = 2^{36}$ Bits für das Sieb genutzt werden kann. Dabei steht jedes Bit für eine positive natürliche Zahl $n \leq N$. Dann gilt $\sqrt{N} = 2^{18} = 262\,144$, sodaß also weniger als 262 144 Iterationen notwendig sind, um sämtliche Primzahlen $\leq 2^{36} = 68\,719\,476\,736$ zu bestimmen. Konkret sind genau $\pi(262144) = 23\,000$ Iterationen[19] notwendig, da dies die Anzahl der Primzahlen ≤ 262144 ist.

Durch gewisse Tricks läßt sich N noch etwas vergrößern, z. B. indem man sich von vornherein auf ungerade Zahlen beschränkt, was zu einer Verdoppelung von N führt. Bereits ein Streichen der 3 im Vorfeld erzwingt Modifikationen am Algorithmus, da bei Divsion durch 3 die beiden verschiedenen Reste 1 und 2 möglich sind: In der naiven Implementierung wird in der k-ten Iteration jedes p_k-te Bit auf 0 gesetzt, was auch nach Streichung der geraden Zahlen im Vorfeld korrekt ist. Wenn die durch drei teilbaren Zahlen im Vorfeld ebenfalls gestrichen werden, dann dürfen wir in der k-ten Iteration nicht einfach jedes p_k-te Bit auf 0 setzen, sondern müssen adäquat buchhalten: jeder zweite Schritt muß doppelt gezählt werden, da in jedem zweiten Schritt eine durch drei teilbare Zahl übersprungen wird.

Von großem Interesse ist in der Zahlentheorie die *Primzahlzählfunktion*

$$\pi : \mathbf{R}_{\geq 0} \to \mathbf{N}, \quad x \mapsto \pi(x) := \#\{p \in \mathbf{P} \mid p \leq x\}.$$

Es gilt beispielsweise aufgrund unserer obigen Bestimmung aller Primzahlen ≤ 20:

$$\pi(20) \;=\; \#\{p \in \mathbf{P} \mid p \leq 20\} \;=\; \#\{2, 3, 5, 7, 11, 13, 17, 19\} \;=\; 8.$$

Im Allgemeinen ist $\pi(x)$ schwer exakt zu bestimmen. Abgesehen von kombinatorischen Verfahren, mit welchen $\pi(x)$ bestimmt werden kann, spielen hier analytische Methoden, welche asymptotische aber teilweise auch exakte Werte liefern. Die wichtigste Asymptotik ist zweifellos der

Satz 1.4.49 (Primzahlsatz)**.** *Asymptotisch gilt*

$$\pi(x) \;\sim\; \frac{x}{\ln x},$$

[19] Es ist ein Zufall, daß $\pi(262144)$ eine derart glatte Zahl ist.

das heißt

$$\lim_{x\to\infty} \frac{\pi(x)}{\left(\frac{x}{\ln x}\right)} \;=\; 1.$$

Der Primzahlsatz besagt einerseits, daß mit wachsendem x die Primzahlen um x herum seltener werden, andererseits aber auch nicht zu selten:

Naiv betrachtet sind aufgrund des Primzahlsatzes etwa ein $(1/\ln x)$-tel aller Zahlen um x Primzahlen, d. h. die Wahrscheinlichkeit, daß eine zufällig um x herum gewählte natürliche Zahl prim ist, ist etwa $1/\ln x$. Diese Aussage ist jedoch in jedweder Hinsicht sehr schwammig: Wie groß muß das Intervall um x sein, damit eine derartige Aussage sinnvoll ist und wie groß ist die zu erwartende Abweichung von der idealen Wahrscheinlichkeit von $1/\ln x$? Auf diese Frage gibt uns obige Formulierung des Primzahlsatzes *keine* Antwort. Diese subtileren Fragestellungen führen zu weitreichenden Vermutungen, deren prominenteste Vertreterin zweifellos die *Riemannsche Vermutung* ist.

1.5 Kongruenzrechnung

Wir haben bereits ausgiebig die Existenz und Eindeutigkeit des Restes der Division ganzer Zahlen ausgenutzt. Einen „koordinatenfreier“ Zugang stellt in diesem Kontext die *Kongruenzrechnung* dar.

Definition 1.5.1 (Kongruenzrelation)**.** Es sei $n \in \mathbf{Z}$ beliebig. Wir nennen $a, b \in \mathbf{Z}$ *kongruent modulo* n, wenn $n \mid a - b$. In Zeichen schreiben wir dann $a \equiv b \pmod{n}$.

Beispiel 1.5.2. Im Fall $n = 0$ gilt $a \equiv b \pmod{0}$ genau dann, wenn $a = b$.
Im Fall $n = 1$ gilt $a \equiv b \pmod{1}$ für *alle* $a, b \in \mathbf{Z}$.
Im Fall $n = 2$ gilt $a \equiv b \pmod{2}$ genau dann, wenn a und b jeweils gerade oder wenn sie jeweils ungerade sind, d. h. wenn a, b den selben Rest bei Division durch 2 lassen.

Proposition 1.5.3. *Für* $0 \neq n \in \mathbf{Z}$ *sind für alle* $a, b \in \mathbf{Z}$ *äquivalent:*

(i) $a \equiv b \pmod{n}$

(ii) $\exists k \in \mathbf{Z}: \quad a = b + k \cdot n$

(iii) Bei Division durch n *hinterlassen* a *und* b *den selben Rest* $0 \leq r < |n|$.

Beweis. Aussage (ii) ist lediglich eine äquivalente Umformulierung von $n \mid a - b$, was per Definitionem äquivalent zu $a \equiv b \pmod{n}$ war. Das zeigt, daß (i) und (ii) äquivalent sind.

Seien nun $a, b \in \mathbf{Z}$, welche (ii) genügen und seien weiterhin $q, r \in \mathbf{Z}$ derart, daß $b = q \cdot n + r$ und $0 \leq r < |n|$ (vgl. Satz 1.4.1). Dann erhalten wir mittels der Identität aus (ii):

$$a \;=\; b + k \cdot n \;=\; q \cdot n + r + k \cdot n \;=\; (k + q) \cdot n + r,$$

womit wir aus der Eindeutigkeit der Division mit Rest folgern, daß a und b zum selben Rest r bei Division durch n führen. Das zeigt (ii) $\Rightarrow$ (iii).

Seien umgekehrt $a, b \in \mathbf{Z}$ derart, daß (iii) gilt, d. h. es existieren $q, q', r \in \mathbf{Z}$ mit

$$a = q \cdot n + r, \quad \text{und} \quad b = q' \cdot n + r, \quad \text{mit} \quad 0 \leq r < |n|.$$

Dann ergibt sich hieraus

$$a - b \;=\; q \cdot n + r - (q' \cdot n + r) \;=\; (q - q') \cdot n,$$

was $n \mid a - b$ nachweist. Mithin gilt (iii) $\Rightarrow$ (i), was den Beweis abschließt. □

Korollar 1.5.4. *Für jedes $n \in \mathbf{Z}$ ist die Kongruenzrelation modulo n eine Äquivalenzrelation auf $\mathbf{Z}$.*

Beweis. Der Fall $n = 0$ ist klar, da hier $a, b \in \mathbf{Z}$ genau dann kongruent modulo n sind, wenn $a = b$ und $=$ ist offensichtlich eine Äquivalenzrelation.

Im Fall $n \neq 0$ zeigt die Äquivalenz von (i) und (iii) in Proposition 1.5.3, daß $a, b \in \mathbf{Z}$ genau dann äquivalent sind, wenn ihre Reste bei Division durch n übereinstimmen. Da leztere wiederum mithilfe der tautologischen Äquivalenzrelation $=$ vergleichen werden, folgt auch in diesem Fall die Behauptung. □

Bemerkung 1.5.5. Es ist nicht schwierig und in der Tat eine schöne Übung, mithilfe der elementaren Eigenschaften der Teilbarkeitsrelation (Reflexivität, Transitivität, etc.) direkt nachzuweisen, daß $a \equiv b \pmod{n}$ eine Äquivalenzrelation auf $\mathbf{Z}$ definiert.

1.5.1 Der Restklassenring

Definition 1.5.6 (Restklassenring)**.** Zu gegebenem $n \in \mathbf{Z}$ bezeichne Menge $\mathbf{Z}/n\mathbf{Z}$ die Menge der *Restklassen* modulo n, d. h. die Menge der Äquivalenzklassen für die obige Äquivalenzrelation $\equiv$.

Da $(\mathbf{Z}, +)$ eine abelsche Gruppe ist und $n\mathbf{Z} \subseteq \mathbf{Z}$ eine Untergruppe, trägt $\mathbf{Z}/n\mathbf{Z}$ als Faktorgruppe selbst eine Gruppenstruktur (vgl. Abschnitt 1.2.5 im Skriptum zur Linearen Algebra), welche von $+$ auf $\mathbf{Z}$ induziert wird: Für zwei Restklassen $A, B \in \mathbf{Z}/n\mathbf{Z}$ seien $a \in A$ und $b \in B$ jeweils Vertreter. Dann ist die Restklasse

$$A + B \;:=\; (a + b) + n\mathbf{Z} \;=\; \{a + b + nk \mid k \in \mathbf{Z}\}$$

von der Wahl der Repräsentanten a, b unabhängig und definiert auf $\mathbf{Z}/n\mathbf{Z}$ eine Gruppenstruktur (vgl. Proposition 1.2.48 aus dem Skriptum zur Linearen Algebra). Weiterhin ist $f_n : \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z},\ a \mapsto a + n\mathbf{Z}$ ein surjektiver Gruppenhomomorphismus mit Kern $\ker f_n = n\mathbf{Z} = \{kn \mid k \in \mathbf{Z}\}$ (vgl. Homomorphiesatz, Satz 1.2.49 aus dem Skriptum zur Linearen Algebra und das darauffolgende Beispiel).

Das Beispiel nach Proposition 1.2.56 aus dem Skriptum zur Linearen Algebra zeigt, daß $\mathbf{Z}/n\mathbf{Z}$ nicht nur eine abelsche Gruppe bzgl. $+$ ist, sondern daß die Multiplikation in $\mathbf{Z}$ auf $\mathbf{Z}/n\mathbf{Z}$ eine Multiplikation induziert, bezüglich welcher $\mathbf{Z}/n\mathbf{Z}$ zu einem kommutativen Ring mit 1 wird. Dieser Ring ist kanonisch isomorph zum Endomorphismenring $\mathrm{End}(\mathbf{Z}/n\mathbf{Z})$ der abelschen Gruppe $\mathbf{Z}/n\mathbf{Z}$. Wir erinnern ebenfalls an Definition 1.2.61 aus dem Skriptum zur Linearen Algebra, in welcher die Einheitengruppe $R^\times$ eines Ringes R definiert wird. Im Fall eines kommutativen Ringes R gilt:

$$R^\times \;=\; \{x \in R \mid \exists y \in R :\ x \cdot y = 1_R\},$$

wobei $1_R \in R$ das Einselement in R bezeichnet. Dann ist $(R^\times, \cdot\,)$ eine Gruppe (siehe Proposition 1.2.62 aus dem Skriptum zur Linearen Algebra).

Proposition 1.5.7. *Für $0 < n \in \mathbf{N}$ gelten:*

(i) $\mathbf{Z}/n\mathbf{Z}$ *ist eine zyklische Gruppe der Ordnung*[20] n*, welche von* $1 + n\mathbf{Z}$ *erzeugt*[21] *wird.*

(ii) $\mathbf{Z}/n\mathbf{Z}$ *ist ein kommutativer Ring mit Einselement* $1_{\mathbf{Z}/n\mathbf{Z}} = 1 + n\mathbf{Z}$*.*

(iii) $(\mathbf{Z}/n\mathbf{Z})^\times = \{a + n\mathbf{Z} \in \mathbf{Z}/n\mathbf{Z} \mid \mathrm{ggT}(a, n) = 1\}$*.*

(iv) Für beliebiges $a + n\mathbf{Z}$ *gilt: Bezeichne* $d = \mathrm{ggT}(a, n)$*, dann ist das Erzeugnis*

$$\langle a + n\mathbf{Z}\rangle \;=\; \{k \cdot a + n\mathbf{Z} \mid k \in \mathbf{Z}\}$$

eine zyklische Untergruppe der Ordnung[22] n/d *von* $\mathbf{Z}/n\mathbf{Z}$*.*

(v) Jede Untergruppe U *von* $\mathbf{Z}/n\mathbf{Z}$ *ist zyklisch und durch ihre Ordnung bereits eindeutig bestimmt. Letztere ist ein Teiler von* n*.*

Beweis. Da $\mathbf{Z}$ als abelsche Gruppe von 1 erzeugt wird, wird $\mathbf{Z}/n\mathbf{Z}$ aufgrund der Surjektivität des Gruppenhomomorphismus $f_n : \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ von $f_n(1)$ erzeugt (vgl. Proposition 1.2.28 (i) im Skriptum zur Linearen Algebra) und ist damit zyklisch. Daß $\mathbf{Z}/n\mathbf{Z}$ Kardinalität n besitzt ergibt sich aus Proposition 1.5.3 Aussage (iii) zusammen mit der Definition des Restes: Es gibt genau n verschiedene mögliche Reste. Das weist (i) nach.

Aussage (ii) haben wir bereits im Vorfeld diskutiert.

Aussage (iii) ergibt sich wie folgt: Sei zunächst $a + n\mathbf{Z} \in (\mathbf{Z}/n\mathbf{Z})^\times$ eine Einheit. Dann existiert eine Restklasse $b + n\mathbf{Z} \in \mathbf{Z}/n\mathbf{Z}$ mit

$$a \cdot b + n\mathbf{Z} \;=\; (a + n\mathbf{Z}) \cdot (b + n\mathbf{Z}) \;=\; 1 + n\mathbf{Z}.$$

Da $a \cdot b$ und 1 die selbe Restklasse modulo n repräsentieren, existiert ein $k \in \mathbf{Z}$ mit $a \cdot b + n \cdot k = 1$. Insbesondere sind a und n also teilerfremd (vgl. das Teilerfremdheitskriterium aus Proposition 1.4.20).

Sei umgekehrt $a \in \mathbf{Z}$ teilerfremd zu n. Dann existieren gemäß obgenanntem Teilerfremdheitskritierum $b, k \in \mathbf{Z}$ mit $a \cdot b + n \cdot k = 1$, was modulo n, d. h. nach Anwendung des Ringhomomorphismus f_n auf beide Seiten dieser Gleichung

$$(a + n\mathbf{Z}) \cdot (b + n\mathbf{Z}) + (0 + n\mathbf{Z}) \;=\; 1 + n\mathbf{Z}$$

zur Folge hat, was zeigt, daß $a + n\mathbf{Z}$ eine Einheit in $\mathbf{Z}/n\mathbf{Z}$ ist, was zu zeigen war.

Um (iv) einzusehen, sei $a \in \mathbf{Z}$ beliebig und es bezeichne $d = \mathrm{ggT}(a, n)$. Wir schreiben $a = d \cdot \widetilde{a}$ und $n = k \cdot d$. Dann ergibt sich einerseits

$$\frac{n}{d} \cdot a \;=\; k \cdot a \;=\; k \cdot d \cdot \widetilde{a} \;=\; \widetilde{a} \cdot n,$$

mithin ist $\frac{n}{d} \cdot a$ ein Vielfaches von n, was zeigt, daß $\frac{n}{d} \cdot (a + n\mathbf{Z}) = n\mathbf{Z}$ neutral ist. Mithin ist die Ordnung von $a + n\mathbf{Z}$ in $\mathbf{Z}/n\mathbf{Z}$ höchstens $\frac{n}{d}$.

[20] Für eine Gruppe G ist ihre *Ordnung* als die Kardinalität $\#G$ definiert.

[21] Das *Erzeugnis* einer Teilmenge $E \subseteq G$ einer Gruppe G ist per Definitionem die bzgl. $\subseteq$ kleinste Untergruppe von G, welche E enthält. Diese ist beispielsweise durch den Schnitt $\bigcap_{E \subseteq U \subseteq G} U$ aller Untergruppen U von G, welche E enthalten, gegeben. Intuitiv besteht das Erzeugnis aus allen Elementen, welche mithile wiederholter Verknüpfung (und Inversion) von Elementen in E „konstruiert“ werden können.

[22] Mit anderen Worten: Das Element $a + n\mathbf{Z}$ hat Ordnung n/d als Element von $\mathbf{Z}/n\mathbf{Z}$.

Sei umgekehert $m \in \mathbf{Z}$ derart, daß $m \cdot (a + n\mathbf{Z})$ in $\mathbf{Z}/n\mathbf{Z}$ neutral, d. h. $n \mid m \cdot a$. Mit ober Zerlegung von a und n ergibt sich die Teilbarkeitsrelation $k \cdot d \mid m \cdot \widetilde{a} \cdot d$, was uns nach Kürzen von d

$$k \mid m \cdot \widetilde{a}$$

beschert. Nun sind k und $\widetilde{a}$ teilerfremd, da d der größte gemeinsame Teiler von a und n war (vgl. Proposition 1.4.21). Also zeigt Korollar 1.4.32, daß

$$k \mid m,$$

mithin folgt $\frac{n}{d} \mid m$.

Zusammenfassend zeigen diese Betrachtungen, daß $\frac{n}{d}$ die Ordnung von $a + n\mathbf{Z}$ ist. Es gilt also $\#\langle a + n\mathbf{Z}\rangle = \frac{n}{d}$.

Um (v) einzusehen, wollen wir (iv) nutzen.

Hierzu bringen wir zunächst mithilfe von Aussage (iii) das Element a aus (iv) auf eine günstige Form. Mit obiger Zerlegung von $a = d \cdot \widetilde{a}$ in $d = \mathrm{ggT}(a, n)$ und $\widetilde{a} \in \mathbf{Z}$, welches teilerfremd zu n ist, erhalten wir aus (iii) die Existenz eines $\ell \in \mathbf{Z}$ mit $(\widetilde{a}+n\mathbf{Z})\cdot(\ell+n\mathbf{Z}) = 1 + n\mathbf{Z}$, was zeigt, daß

$$\ell \cdot (a + n\mathbf{Z}) = \underbrace{\ell \cdot \widetilde{a}}_{\equiv 1 \pmod n} \cdot d + n\mathbf{Z} \;=\; d + n\mathbf{Z}.$$

Damit folgt $d \in \langle a + n\mathbf{Z}\rangle$ und umgekehrt ist $a + n\mathbf{Z}$ das $\widetilde{a}$-Fache von $d + n\mathbf{Z}$, womit $a \in \langle d + n\mathbf{Z}\rangle$, also zusammenfassend $\langle d + n\mathbf{Z}\rangle = \langle a + n\mathbf{Z}\rangle$.

Mit anderen Worten: jede zyklische Untergruppe von $\mathbf{Z}/n\mathbf{Z}$ der Ordnung $\frac{n}{d}$ wird von $d + n\mathbf{Z}$ erzeugt und ist damit insbesondere eindeutig durch ihre Ordnung bestimmt.

Sei U nun eine beliebige (nicht notwendigerweise zyklische!) Untergruppe. Aufgrund der obigen Betrachtungen genügt es zu zeigen, daß U zyklisch ist.

1. Argument: Wir nutzen den Euklidischen Algorithmus. Seien $u_1, \ldots, u_r \in \mathbf{Z}$ Repräsentanten der (endlich vielen) Elemente in U und bezeichne $d = \mathrm{ggT}(u_1, \ldots, u_r)$.

Dann ist einerseits jedes u_i ein Vielfaches von d, womit die Restklasse $u_i + n\mathbf{Z}$ im Erzeugnis $\langle d + n\mathbf{Z}\rangle$ von $d + n\mathbf{Z}$ liegt. Insbesondere gilt $U \subseteq \langle d + n\mathbf{Z}\rangle$.

Andererseits ist d dank des erweiterten Euklidischen Algorithmus selbst eine $\mathbf{Z}$-Linearkombination von $u_1, \ldots, u_r$ (vgl. Korollar 1.4.18). Insbesondere liegt also $d + n\mathbf{Z}$ im Erzeugnis der Elemente $u_1 + n\mathbf{Z}, \ldots, u_r + n\mathbf{Z}$, was jedoch mit U übereinstimmt. Das zeigt $\langle d + n\mathbf{Z}\rangle \subseteq U$, was letztendlich die Gleichheit impliziert. Mithin ist U zyklisch.

2. Argument: Bezeichne hierzu $f_n : \mathbf{Z} \to \mathbf{Z}/n\mathbf{Z}$ die Restklassenabbildung. Da diese ein Gruppenhomomorphismus ist, ist das Urbild $f^{-1}(U)$ eine Untergruppe von $\mathbf{Z}$. Diese enthält das Urbild $n\mathbf{Z}$ der Restklasse $0+n\mathbf{Z}$, also gilt $n\mathbf{Z} \subseteq f^{-1}(U)$, womit $f^{-1}(U) \neq \{0\}$.

Wir behaupten, daß $f^{-1}(U)$ von einem Element $b \in \mathbf{Z}$ erzeugt wird. Sei hierzu $b \in^{-1}(U) \cap \mathbf{N}$ minimal mit der Eigenschaft, daß $b > 0$ (vgl. Wohlordnungsprinzip). Wenn $c \in f^{-1}(U)$ beliebig ist, bezeichne $t = \mathrm{ggT}(b, c)$. Da t eine $\mathbf{Z}$-Linearkombination von b und c ist, liegt t in $f^{-1}(U)$, womit $t \geq b$ aufgrund der Minimalität von b gelten muß. Da $t \mid b$ zeigt das $t = b$. Damit folgt $b \mid c$, was zeigt, daß c im Erzeugnis $\langle b\rangle$ von b liegt. Wir schließen, daß $f^{-1}(U) = \langle b\rangle$, was zeigt, daß

$$U = f_n(\langle b\rangle) = \langle f_n(b)\rangle = \langle b + n\mathbf{Z}\rangle$$

selbst zyklisch ist (vgl. Proposition 1.2.28 (i) aus dem Skriptum zur Linearen Algebra).

□

Bemerkung 1.5.8. Im Beweis von Teil (v) haben wir implizit gezeigt, daß jede von 0 verschiedene Untergruppe von $\mathbf{Z}$ zyklisch ist.

Korollar 1.5.9. *Für jedes $0 < n \in \mathbf{N}$ gelten:*

(a) Es gilt

$$\#(\mathbf{Z}/n\mathbf{Z})^\times \;=\; \#\{a \mid 1 \leq a \leq n \wedge \mathrm{ggT}(a,n) = 1\},$$

und dies ist die Anzahl der Elemente in $\mathbf{Z}/n\mathbf{Z}$, welche $\mathbf{Z}/n\mathbf{Z}$ erzeugen.

(b) Es gibt in $\mathbf{Z}/n\mathbf{Z}$ zu jedem positiven Teiler $d \mid n$ genau $\#(\mathbf{Z}/d\mathbf{Z})^\times$ Elemente der Ordnung d.

Beweis. Die Identität in (a) ist eine unmittelbare Konsequenz der Aussage (iv) aus Proposition 1.5.7: Eine Restklasse $a + n\mathbf{Z}$ ist genau dann ein Erzeuger von $\mathbf{Z}/n\mathbf{Z}$, wenn $d := \mathrm{ggT}(a,n) = 1$ gilt, da nur dann die Ordnung $\frac{n}{d}$ des Erzeugnisses $\langle a + n\mathbf{Z}\rangle$ mit n übereinstimmt.

Analoges gilt für Aussage (b), wobei wir hier auf die Eindeutigkeitsaussage in (v) zurückgreifen müssen: Aus (b) wissen wir, daß zu gegebenem $d \mid n$ alle Elemente der Ordnung d in $\mathbf{Z}/n\mathbf{Z}$ in der selben zyklischen Gruppe $\langle \frac{n}{d} + n\mathbf{Z}\rangle$ liegen. Mit anderen Worten: Ein Element $a + n\mathbf{Z}$ hat genau dann Ordnung d, wenn es ein Erzeuger von $\langle \frac{n}{d} + n\mathbf{Z}\rangle$ ist. Letztere Gruppe ist jedoch zyklisch von Ordnung d und damit isomorph zu $\mathbf{Z}/d\mathbf{Z}$. Ergo zeigt Aussage (a), daß es in letzterer Gruppe genau $\#(\mathbf{Z}/d\mathbf{Z})^\times$ Erzeuger gibt. Mithin gibt es insgesamt genau $\#(\mathbf{Z}/d\mathbf{Z})^\times$ verschiedene Elemente der Ordnung d in $\mathbf{Z}/n\mathbf{Z}$, was zu zeigen war. □

1.5.2 Die Euler'sche φ-Funktion

Definition 1.5.10 (Euler'sche φ-Funktion)**.** Wir definieren die *Euler'sche φ-Funktion* als

$$\varphi : \mathbf{N}_{\geq 1} \to \mathbf{N}, \quad n \mapsto \varphi(n) := \#(\mathbf{Z}/n\mathbf{Z})^\times.$$

Proposition 1.5.11 (Gauß)**.** *Für jedes $n \in \mathbf{N}_{\geq 1}$ gilt*

$$n \;=\; \sum_{d \mid n} \varphi(d). \tag{1.27}$$

Beweis. Wir wissen bereits, daß n die Anzahl der Elemente in $\mathbf{Z}/n\mathbf{Z}$ ist (vgl. Proposition 1.5.7 Aussage (i)). Die Ordnung eines jeden Elementes $a + n\mathbf{Z} \in \mathbf{Z}/n\mathbf{Z}$ ist gemäß Proposition 1.5.7 ein Teiler d von n. Zudem gibt es laut Korollar 1.5.9 (b) in $\mathbf{Z}/n\mathbf{Z}$ genau $\varphi(d)$ Elemente der Ordnung d. Daher schließen wir, daß

$$n \;=\; \#\mathbf{Z}/n\mathbf{Z} \;=\; \sum_{d \mid n} \#\{a + n\mathbf{Z} \in \mathbf{Z}/n\mathbf{Z} \mid \mathrm{ord}(a + n\mathbf{Z}) = d\} \;=\; \sum_{d \mid n} \varphi(d),$$

was zu zeigen war. □

Unser Beweis von Proposition 1.5.11 basierte darauf, daß $\mathbf{Z}/n\mathbf{Z}$ eine zyklische Gruppe ist. Von Bedeutung ist ebenfalls folgende Umkehrung, dessen Beweis sich die Identität (1.27) aus Proposition 1.5.11 zunutze macht.

Satz 1.5.12. *Es sei G eine endliche Gruppe der Ordnung n. Wenn es zu jedem positiven Teiler $d \mid n$ in G höchstens $\varphi(d)$ Elemente der Ordnung d gibt, dann ist G zyklisch*[23].

Beweis. Der Satz von Lagrange (Satz 1.2.41 im Skriptum zur Linearen Algebra) impliziert, daß die Ordnung $\operatorname{ord} g$ eines beliebigen $g \in G$ ein Teiler d der Ordnung n von G ist.

Nehmen wir an, daß für jeden Teiler $d \mid n$ in G höchstens $\varphi(d)$ Elemente der Ordnung d existieren, so zeigt dies einerseits

$$n \;=\; \#G \;=\; \sum_{d|n} \underbrace{\#\{g \in G \mid \operatorname{ord} g = d\}}_{\leq \varphi(d)} \;\leq\; \sum_{d|n} \varphi(d).$$

Andererseits wissen wir dank Proposition 1.5.11, daß insgesamt Gleichheit gilt, sodaß auch für jeden Summanden zu $d \mid n$ die Ungleichung

$$\#\{g \in G \mid \operatorname{ord} g = d\} \;\leq\; \varphi(d)$$

eine Gleichheit sein muß. Insbesondere ergibt sich[24] für $d = n$

$$\#\{g \in G \mid \operatorname{ord} g = n\} \;=\; \varphi(n) \;\geq\; 1,$$

was zeigt, daß in G mindestens ein Element g der Ordnung n existiert. Dieses erzeugt G, mithin ist G zyklisch. □

1.5.3 Der chinesische Restsatz

Sei m ein positiver Teiler einer positiven natürlichen Zahl n. Dann können wir jede Restklasse modulo n zu einer Restklasse modulo m vergrößern und erhalten so einen Ringhomomorphismus

$$p_m^n :\; \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}, \quad a + n\mathbf{Z} \mapsto\; a + m\mathbf{Z}.$$

Dieser ist wohldefiniert, da für alle $a, b \in \mathbf{Z}$ stets $a \equiv b \pmod{n}$ die Kongruenz $a \equiv b \pmod{m}$ impliziert, da $m \mid n$ und $n \mid a - b$ (vgl. Transitivität der Teilbarkeitsrelation).

Satz 1.5.13 (Chinesischer Restsatz)**.** *Es sei $n = n_1 \cdot n_2 \cdot \cdots \cdot n_r$ ein Produkt paarweise teilerfremder natürlicher Zahlen $n_1, \ldots, n_r$. Dann induzieren die Abbildungen $p_{n_i}^n : \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/n_i\mathbf{Z}$ einen kanonischen Isomorphismus*

$$f :\; \mathbf{Z}/n\mathbf{Z} \;\to\; \mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z} \times \ldots \times \mathbf{Z}/n_r\mathbf{Z}, \quad a + n\mathbf{Z} \;\mapsto\; (a + n_1\mathbf{Z}, a + n_2\mathbf{Z}, \ldots, a + n_r\mathbf{Z})$$

von Ringen.

Beweis. Als Produkt der Ringhomomorphismen $p_{n_i}^n$ ist obige Abbildung f wohldefiniert und ein Homomorphismus von Ringen.

Es bleibt die Bijektivität zu zeigen. Hierzu konstruieren wir die Umkehrabbildung g zu f. Zu gegebenem $1 \leq i \leq r$ definieren wir hierzu zunächst

$$d_i \;:=\; n/n_i \;=\; \prod_{j \neq i} n_j.$$

[23] und automatisch die Anzahl der Elemente der Ordnung n nicht nur $\leq \varphi(d)$, sondern $= \varphi(d)$.

[24] Da $\mathbf{Z}/n\mathbf{Z}$ zyklisch ist und damit einen Erzeuger besitzt gilt stets $\varphi(n) \geq 1$.

Da n_i gemäß Voraussetzung zu jedem n_j teilerfremd ist, ist n_i damit zu d_i teilerfremd (vgl. Proposition 1.4.22). Damit beschert uns der erweiterte Euklidische Algorithmus $x_i, y_i \in \mathbf{Z}$ derart, daß

$$x_i n_i \ + \ y_i d_i \ = \ 1. \tag{1.28}$$

Zu einem gegebenem Tupel $\overline{a} = (a_i + n_i\mathbf{Z})_{1 \leq i \leq r}$ von Restklassen aus dem Produkt $\mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z} \times \ldots \times \mathbf{Z}/n_r\mathbf{Z}$ definieren wir zunächst die ganze Zahl

$$a \ := \ \sum_{i=1}^{r} a_i \cdot y_i \cdot d_i$$

und setzen daraufhin

$$g(\overline{a}) \ := \ a + n\mathbf{Z}.$$

Zunächst prüfen wir, daß $a + n\mathbf{Z}$ nicht von der Wahl der Repräsentanten a_i der Restklassen $a_i + n_i\mathbf{Z}$ abhängt. In der Tat, wenn $b_i = a_i + k_i n_i$, so erhalten wir gemäß obiger Konstruktion zunächst eine ganze Zahl

$$b \ := \ \sum_{i=1}^{r} b_i \cdot y_i \cdot d_i \ = \ \sum_{i=1}^{r} (a_i + k_i n_i) \cdot y_i \cdot d_i \ = \ \sum_{i=1}^{r} a_i \cdot y_i d_i + k_i n_i y_i d_i.$$

Da jeder der Summanden $k_i n_i y_i d_i$ wegen $n_i d_i = n$ ein Vielfaches von n ist, ergibt sich

$$a \equiv b \pmod{n},$$

was zu zeigen war. Also erhalten wir eine wohldefinierte Abbildung

$$g: \ \mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z} \times \ldots \times \mathbf{Z}/n_r\mathbf{Z} \ \to \ \mathbf{Z}/n\mathbf{Z}.$$

Wir behaupten, daß $f \circ g = \mathbf{1}_{\mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z} \times \ldots \times \mathbf{Z}/n_r\mathbf{Z}}$. Sei also

$$(a_i + n_i\mathbf{Z})_i \ \in \ \mathbf{Z}/n_1\mathbf{Z} \times \ldots \times \mathbf{Z}/n_r\mathbf{Z}$$

ein beliebiges Tupel von Restklassen. Gemäß obiger Konstruktion gilt dann

$$\begin{aligned} f(g((a_i + n_i\mathbf{Z})_i)) \ &= \ f(g(a_1 + n_1\mathbf{Z}, a_2 + n_2\mathbf{Z}, \ldots, a_2 + n_r\mathbf{Z})) \\ &= \ f\left(\sum_{i=1}^{r} a_i \cdot y_i \cdot d_i \ + \ n\mathbf{Z}\right) \\ &= \ (a_1 \cdot y_1 d_1 + n_1\mathbf{Z}, \ldots, a_r \cdot y_r d_r + n_r\mathbf{Z}). \end{aligned}$$

Gemäß (1.28) gilt für jeden Index $1 \leq i \leq r$:

$$y_i \cdot d_i \ = \ 1 - x_i \cdot n_i \ \equiv \ 1 \pmod{n_i},$$

was uns

$$(a_1 \cdot y_1 \cdot d_1 + n_1\mathbf{Z}, \ldots, a_r \cdot y_r \cdot d_r + n_r\mathbf{Z}) \ = \ (a_1 \cdot 1 + n_1\mathbf{Z}, \ldots, a_r \cdot 1 + n_r\mathbf{Z}) \ = \ (a_1 + n_1\mathbf{Z}, \ldots, a_r + n_r\mathbf{Z})$$

beschert, was zu zeigen war.

Ergo ist g ein Rechtsinverses zu f, was impliziert, daß f surjektiv ist (vgl. Proposition 1.1.4 im Skriptum zur Linearen Algebra). Nun gilt

$$\#\mathbf{Z}/n\mathbf{Z} \;=\; n \;=\; n_1 \cdot n_2 \cdot \ldots \cdot n_r \;=\; \#(\mathbf{Z}/n_1\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z}),$$

womit Definitionsbereich und Zielbereich von f von der selben endlichen Kardinalität sind. Mithin folgt aus der Surjektivität von f damit die Bijektivität, was den Beweis abschließt. □

Korollar 1.5.14 (Multiplikativität der Euler'schen φ-Funktion)**.** *Es sei $n = n_1 \cdot n_2 \cdot \ldots \cdot n_r \geq 1$ ein Produkt paarweise teilerfremder natürlicher Zahlen $n_1, \ldots, n_r$. Dann gilt*

$$\varphi(n) \;=\; \varphi(n_1) \cdot \varphi(n_2) \cdot \ldots \cdot \varphi(n_r).$$

Beweis. φ ist die Kardinalität der Einheitengruppe des Ringes $\mathbf{Z}/n\mathbf{Z}$ und das Produkt rechterhand ist analog die Kardinalität der Einheitengruppe des Ringes $\mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z} \times \ldots \times \mathbf{Z}/n_r\mathbf{Z}$ (vgl. Proposition 1.5.7 (iii)). Laut Satz 1.5.13 sind die betreffenden Ringe und damit auch ihre Einheitengruppen isomorph, womit sich die Behauptung wie folgt ergibt:

$$\begin{aligned}
\varphi(n) \;&=\; \#(\mathbf{Z}/n\mathbf{Z})^\times \\
&=\; \#\left(\mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z}\right)^\times && \text{(Chinesischer Restsatz)} \\
&=\; \#\left[(\mathbf{Z}/n_1\mathbf{Z})^\times \times (\mathbf{Z}/n_2\mathbf{Z})^\times \times \cdots \times (\mathbf{Z}/n_r\mathbf{Z})^\times\right] \\
&=\; \#(\mathbf{Z}/n_1\mathbf{Z})^\times \cdot \#(\mathbf{Z}/n_2\mathbf{Z})^\times \cdot \ldots \cdot \#(\mathbf{Z}/n_r\mathbf{Z})^\times \\
&=\; \varphi(n_1) \cdot \varphi(n_2) \cdot \ldots \cdot \varphi(n_r).
\end{aligned}$$

□

Bemerkung 1.5.15. In der Zahlentheorie werden *multiplikative* und *strikt multiplikative* Abbildungen $f : \mathbf{N}_{\geq 1} \to \mathbf{C}$ unterschieden.

Die *Multiplikativität* von φ bedeutet **nicht**, daß für *alle* $a, b \in \mathbf{N}_{\geq 1}$ die Relation

$$\varphi(a \cdot b) \;=\; \varphi(a) \cdot \varphi(b)$$

gilt. Sondern diese gilt **nur**, sofern $\mathrm{ggT}(a, b) = 1$.

Für eine *strikt multiplikative* Funktion $f : \mathbf{N}_{\geq 1} \to \mathbf{C}$ gilt hingegen, daß

$$f(a \cdot b) \;=\; f(a) \cdot f(b)$$

für alle $a, b \in \mathbf{N}_{\geq 1}$ gilt. Bei einer *multiplikativen* Funktion wird dies nur für teilerfremde a, b gefordert.

Obwohl φ nicht strikt multiplikativ ist, genügt die Multiplikativität, um $\varphi(n)$ mithilfe der Primfaktorzerlegung von n zu bestimmen.

Korollar 1.5.16 (Explizite Form von $\varphi(n)$)**.** *Es sei $n \geq 1$ eine natürliche Zahl mit Primfaktorzerlegung $n = p_1^{v_1} \cdot p_2^{v_2} \cdot \ldots \cdot p_r^{v_r}$. Dann gilt*

$$\varphi(n) \;=\; \prod_{i=1}^{r} (p_i - 1) \cdot p_i^{v_i - 1}.$$

Beweis. Korollar 1.5.14 impliziert, daß

$$\varphi(n) \;=\; \prod_{i=1}^{r} \varphi(p_i^{v_i}),$$

da in einer Primfaktorzerlegung in unserem Sinne die Primfaktoren $p_1, \ldots, p_r$ paarweise verschieden und damit teilerfremd sind. Weiterhin gilt $v_1, \ldots, v_r \geq 1$.

Gemäß Korollar 1.5.9 haben wir

$$\varphi(p_i^{v_i}) \;=\; \#(\mathbf{Z}/p_i^{v_i}\mathbf{Z})^\times \;=\; \#\{a \mid 1 \leq a \leq p_i^{v_i} \wedge \mathrm{ggT}(a, p_i^{v_i}) = 1\}.$$

Da $v_i \geq 1$ ist die Bedingung $\mathrm{ggT}(a, p_i^{v_i}) = 1$ ist äquivalent zu $\mathrm{ggT}(a, p_i) = 1$, was wiederum dank unserem Teilerfremdheitskriterium für Primzahlen als Proposition 1.4.24 äquivalent zu $p_i \nmid a$ ist. Wir erhalten damit

$$\begin{aligned}\{a \mid 1 \leq a \leq p_i^{v_i} \wedge \mathrm{ggT}(a, p_i^{v_i}) = 1\} &= \{a \mid 1 \leq a \leq p_i^{v_i} \wedge p_i \nmid a\} \\ &= \underbrace{\{a \mid 1 \leq a \leq p_i^{v_i}\}}_{\text{die Menge } \{1,\ldots,p_i^{v_i}\}} \setminus \underbrace{\{b \cdot p_i \mid 1 \leq b \leq p_i^{v_i-1}\}}_{\text{alle durch } p_i \text{ teilbaren Elemente}}.\end{aligned}$$

Diese Menge besitzt die Kardinalität

$$\varphi(p_i^{v_i}) \;=\; p_i^{v_i} - p_i^{v_i-1} \;=\; (p_i - 1) \cdot p_i^{v_i-1},$$

was zu zeigen war. □

Korollar 1.5.17 (Zyklizitätskriterium für Produkte zyklischer Gruppen)**.** *Es seien $n_1, \ldots, n_r \geq 1$ natürliche Zahlen. Dann ist das Produkt*

$$\mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z}$$

genau dann zyklisch, wenn $n_1, \ldots, n_r$ paarweise teilerfremd sind.

Beweis. Teilerfremdheit ist hinreichend: Angenommen, die Zahlen $n_1, \ldots, n_r$ sind paarweise teilerfremd. Dann besagt der chinesische Restsatz (Satz 1.5.13), daß die gegebene Gruppe zu $\mathbf{Z}/n_1n_2 \cdot \cdots \cdot n_r\mathbf{Z}$ isomorph ist. Da letztere Gruppe zyklisch ist, trifft Selbiges ebenfalls auf $\mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z}$ zu.

Notwendigkeit der Teilerfremdheit: Angenommen, es existieren zwei Indizes $i \neq j$ mit $1 < d = \mathrm{ggT}(n_i, n_j)$. Dann beobachten wir, zunächst, daß wir einen surjektiven Gruppenhomomorphmismus

$$f : \mathbf{Z}/n_1\mathbf{Z} \times \mathbf{Z}/n_2\mathbf{Z} \times \cdots \times \mathbf{Z}/n_r\mathbf{Z} \to \mathbf{Z}/d\mathbf{Z}^2, \quad (a_k + n_k\mathbf{Z})_k \mapsto (a_i + d\mathbf{Z}, a_j + d\mathbf{Z})$$

erhalten. Wäre nun der Definitionsbereich von f zyklisch, so wäre ebenfalls sein Bild $\mathbf{Z}/d\mathbf{Z}^2$ zyklisch (vgl. Proposition 1.2.28 (i) aus dem Skriptum zur Linearen Algebra), was nicht der Fall ist. Daher muß im zyklischen Fall stets $\mathrm{ggT}(n_i, n_i) = 1$ gelten. □

Beispiel 1.5.18 (Chinesischer Restsatz: Simultane Kongruenzen)**.** Es sei $n = 7 \cdot 11 = 77$ gegeben. Wir suchen das eindeutig bestimmte (!) $0 \leq a < 77$ mit

$$\begin{aligned} a &\equiv 3 \pmod 7 \\ a &\equiv 5 \pmod{11} \end{aligned}$$

Wir orientieren uns an der Konstruktion im Beweis des chinesischen Restsatzes. Insbesondere seien $n_1 = 7$, $n_2 = 11$, $a_1 = 3$, $a_2 = 5$. Dann ergibt sich $d_1 = n/n_1 = 11$ und $d_2 = 7$. Wie in (1.28) müssen wir nun mithilfe des erweiterten Euklidischen Algorithmus $x_1, x_2, y_1, y_2 \in \mathbf{Z}$ bestimmen mit mit

$$x_i n_i + y_i d_i = 1,$$

welche hier wegen $d_1 = n_2$ und $d_2 = n_1$ äquivalent zu

$$y_2 n_1 + y_1 n_2 = 1$$

ist. Konkret rechnen wir also

k	r_k	q_k	s_k	t_k
0	11		1	0
1	7	1	0	1
2	4	1	1	-1
3	3	1	-1	2
4	1	1	2	-3

ergo:

$$(-3) \cdot 7 + 2 \cdot 11 \;=\; 1,$$

womit $y_1 = 2$ und $y_2 = -3$. Mit dem Rezept aus dem Beweis ergibt sich damit

$$\begin{aligned} a &\equiv a_1 y_1 d_1 + a_2 y_2 d_2 && \pmod{77} \\ &\equiv 3 \cdot 2 \cdot 11 + 5 \cdot (-3) \cdot 7 && \pmod{77} \\ &\equiv 66 - 105 && \pmod{77} \\ &\equiv -39 && \pmod{77} \\ &\equiv 77 - 39 && \pmod{77} \\ &\equiv 38 && \pmod{77} \end{aligned}$$

also $a = 38$. Zur Probe führen wir Division mit Rest durch:

$$\begin{aligned} 38 &= 5 \cdot 7 + 3 \equiv 3 \pmod{7} \\ 38 &= 3 \cdot 11 + 5 \equiv 5 \pmod{11} \end{aligned}$$

wie gewünscht.

Beispiel 1.5.19 (Chinesischer Restsatz: Rechnen modulo n)**.** Wir bleiben im Kontext von $n = 7 \cdot 11 = 77$, da es dies uns erlaubt, die Berechnungen aus (1.5.18) weiterzuverwenden. Die erste Einsicht ist, daß wir mithilfe von y_1 und y_2 nun beliebige simultane Kongruenzen modulo 7 und modulo 11 lösen können: Sind $a_1, a_2 \in \mathbf{Z}$ gegeben, so suchen wir ein $a \in \mathbf{Z}$ mit

$$\begin{aligned} a &\equiv a_1 \pmod{7} \\ a &\equiv a_2 \pmod{11} \end{aligned}$$

Wegen $y_1 = 2$ und $y_2 = -3$ erhalten wir analog zum vorigen Beispiel

$$\begin{aligned} a &\equiv a_1 y_1 d_1 + a_2 y_2 d_2 && \pmod{77} \\ &\equiv a_1 \cdot 2 \cdot 11 + a_2 \cdot (-3) \cdot 7 && \pmod{77} \\ &\equiv 22 \cdot a_1 - 21 \cdot a_2 && \pmod{77} \end{aligned}$$

Dies läßt sich aufgrund der Homomorphie von p_m^n ausnutzen, um Rechnungen modulo 77 auf Rechnungen moduhlo 7 und modulo 11 zu reduzieren. Wollen wir beispielsweise $71 \cdot 53$ modulo 77 bestimmen, so berechnen wir zunächst das Ergebnis modulo 7 und modulo 11:

$$\begin{aligned} 71 \cdot 53 &\equiv 1 \cdot 4 \equiv 4 \pmod 7 \\ 71 \cdot 53 &\equiv 5 \cdot (-2) \equiv 1 \pmod{11} \end{aligned}$$

Daraufhin bestimmen wir $a \in \mathbf{Z}$ mit

$$\begin{aligned} a &\equiv 4 \pmod 7 \\ a &\equiv 1 \pmod{11} \end{aligned}$$

gemäß obiger expliziter Formel:

$$\begin{aligned} a &\equiv 22 \cdot 4 - 21 \cdot 1 && \pmod{77} \\ &\equiv 88 - 21 && \pmod{77} \\ &\equiv 67 && \pmod{77} \end{aligned}$$

Es gilt also

$$71 \cdot 53 \equiv 67 \pmod{77}.$$

Wir haben es auf diese Weise vermieden, zwei zweistellige Zahlen zu multiplizieren und insbesondere mit einem *vierstelligen* Zwischenergebnis zu arbeiten. Stattdessen mußten wir zwei mal einstellige Zahlen multiplizieren (Rechnen modulo 7 und modulo 11 involviert nur einstellige Zahlen wenn wir $10 \equiv -1 \pmod{11}$ ausnutzen). Allerdings mußten wir im letzten Schritt bei der Rekonstruktion von a die einstelligen Ergebnisse mit 22 und 21 multiplizieren. Trotzdem haben wir es zu jedem Zeitpunkt nur mit *zweistelligen* Zahlen zu tun gehabt. Weiterhin ist zu bemerken, daß wir vier Divisionen mit Rest angefallen sind, um 71 und 53 jeweils modulo 7 und modulo 11 zu minimieren.

Das Rechnen modulo 7 und 11 anstatt modulo 77 wird umso effizienter, je mehr Operationen wir mit 71 und 53 auszuführen haben, da jede einzelne Multiplikation, Addition, Division etc. modulo 7 und modulo 11 deutlich günstiger ist als modulo 77. Weiterhin muß in gewissen Situationen das Ergebnis a modulo 77 nicht rekonstruiert werden: Wollen wir beispielsweise prüfen, ob eine Gleichheit gilt, d. h. ob beispielsweise

$$53^3 \equiv 71^4 \pmod{77} \tag{1.29}$$

gilt, so genügt, es dank des chinesischen Restsatzes, dies modulo 7 und modulo 11 zu prüfen:

$$\begin{aligned} 53^3 &\equiv 4^3 \equiv 16 \cdot 4 \equiv 2 \cdot 4 \equiv 8 \equiv 1 \pmod 7 \\ 71^4 &\equiv 1^4 \equiv 1 \pmod 7 \end{aligned}$$

Modulo 11 ergibt sich:

$$\begin{aligned} 53^3 &\equiv (-2)^3 \equiv -8 \equiv 3 \pmod{11} \\ 71^4 &\equiv 5^4 \equiv 25^2 \equiv 3^2 \equiv 9 \not\equiv 3 \pmod{11} \end{aligned}$$

womit die Prüfung modulo 11zeigt, daß die Kongruenz (1.29) nicht gilt.

Beispiel 1.5.20 (Chinesischer Restsatz: Nullstellen modulo n)**.** Der chinesische Restsatz reduziert das Bestimmen von Lösungen algebraischer Gleichungen modulo n, d. h. äquivalent formuliert das Bestimmen von Nullstellen von Polynomgleichungen modulo n auf das Bestimmen der Lösungen selbiger Gleichungen modulo n_1, modulo n_2,..., modulo n_r.

Im Kontext unseres obigen Beispiels betrachten wir die lineare Gleichung

$$71 \cdot a \equiv 53 \pmod{77}.$$

Wir suchen alle $a \in \mathbf{Z}$, welche dieser Kongruenz genügen. Wir könnten unmittelbar den erweiterten Euklidischen Algorithmus auf 71 und 77 anwenden, um das multiplikativ Inverse von 71 zu bestimmen und auf diese Weise obige Kongruenz nach a aufzulösen.

Stattdessen betrachten wir obige Kongruenz zunächst modulo 7 und modulo 11:

$$\begin{aligned} 71 \cdot a &\equiv 53 \pmod{7} \\ 71 \cdot a &\equiv 53 \pmod{11} \end{aligned}$$

Wir kennen bereits kleine Repräsentanten für 71 und 53 modulo 7 und modulo 11, was uns die äquivalenten Kongruenzen

$$\begin{aligned} 1 \cdot a &\equiv 4 \pmod{7} \\ 5 \cdot a &\equiv -2 \pmod{11} \end{aligned}$$

beschert. Die erste Kongruenz ist zu

$$a \equiv 4 \pmod{7}$$

äquivalent und für die zweite berechnen wir mithilfe des Euklidischen Algorithmus

k	r_k	q_k	s_k	t_k
0	11		1	0
1	5	2	0	1
2	1		1	-2

also

$$1 \;=\; 1 \cdot 11 - 2 \cdot 5.$$

Mit anderen Worten: -2 repräsentiert das multiplikativ Inverse zu 5 modulo 11. Ergo ergibt sich

$$a \;\equiv\; (-2) \cdot 5 \cdot a \equiv (-2) \cdot (-2) \equiv 4 \pmod{11}$$

Zusammenfassend gilt also

$$\begin{aligned} a &\equiv 4 \pmod{7} \\ a &\equiv 4 \pmod{11} \end{aligned}$$

was uns offensichtlich[25]

$$a \equiv 4 \pmod{77}$$

[25] Es gilt stets $a \equiv a \pmod{n_i}$!

beschert. Alternativ nutzen wir die Rekonstruktion aus dem chinesischen Restsatz mithilfe von y_1 und y_2:

$$a \equiv 22 \cdot a_1 - 21 \cdot a_2 \equiv 22 \cdot 4 - 21 \cdot 4 \equiv 4 \pmod{77}$$

Diese Rechnung zeigt nebenbei, daß daß ein Repräsentant $b \in \mathbf{Z}$ des multiplikativ Inverse von 71 modulo 77 folgenden beiden Kongruenzen genügen muß:

$$\begin{aligned} b &\equiv 1 \pmod{7} \\ b &\equiv -2 \pmod{11} \end{aligned}$$

also

$$b \equiv 22 \cdot 1 - 21 \cdot (-2) \equiv 22 + 42 \equiv 64 \pmod{77}$$

1.5.4 Endliche Körper

Aus der Charakterisierung der Einheitengruppe in $\mathbf{Z}/n\mathbf{Z}$ in Proposition 1.5.7 (iii) erhalten wir

Proposition 1.5.21 (Endliche Primkörper)**.** *Für $n \geq 0$ ist der Ring $\mathbf{Z}/n\mathbf{Z}$ ist genau dann ein Körper, wenn n eine Primzahl ist.*

Im Fall $n = p$ prim definieren wir $\mathbf{F}_p := \mathbf{Z}/p\mathbf{Z}$.

Beweis. Sei n zunächst eine Primzahl. Wir wissen bereits, daß $\mathbf{Z}/n\mathbf{Z}$ ein kommutativer Ring mit Eins ist. Es bleibt daher zu zeigen, daß $(\mathbf{Z}/n\mathbf{Z})^\times = \{x+n\mathbf{Z} \mid x+n\mathbf{Z} \neq 0+n\mathbf{Z}\} = \mathbf{Z}/n\mathbf{Z} \setminus \{0+n\mathbf{Z}\}$. Wir wissen weiterhin, daß $\mathbf{Z}/n\mathbf{Z}$ eine n-elementige Menge ist, was uns wegen $\{0+n\mathbf{Z}\} \notin (\mathbf{Z}/n\mathbf{Z})^\times$ darauf reduziert zu zeigen, daß $\#(\mathbf{Z}/n\mathbf{Z})^\times = n-1$ gilt, wenn n eine Primzahl ist. Die explizite Formel in Korollar 1.5.16 zeigt, daß $\varphi(n) = n-1$ für n prim und da per Definition $\varphi(n) = \#(\mathbf{Z}/n\mathbf{Z})^\times$, zeigt dies, daß $\mathbf{Z}/n\mathbf{Z}$ ein Körper ist.

Sei umgekehrt $n \geq 0$ und $\mathbf{Z}/n\mathbf{Z}$ ein Körper. Wegen $\mathbf{Z} \cong \mathbf{Z}/0\mathbf{Z}$ gilt dann $n \geq 1$. Nun ist $\mathbf{Z}/1\mathbf{Z}$ der Nullring, welcher wegen $1 = 0$ kein Körper ist. Also gilt $n \geq 2$. Sei nun $a \mid n$ ein natürlicher Teiler von n, d. h. $n = a \cdot b$ mit natürlichen Zahlen $a, b \in \mathbf{N}$. Modulo n ergibt sich dann

$$a \cdot b \equiv 0 \pmod{n},$$

was in $\mathbf{Z}/n\mathbf{Z}$ bedeutet, daß $(a+n\mathbf{Z}) \cdot (b+n\mathbf{Z}) = 0$ gilt. Da $\mathbf{Z}/n\mathbf{Z}$ ein Körper ist, impliziert dies $a + n\mathbf{Z} = 0 + n\mathbf{Z}$ oder $b + n\mathbf{Z} = 0 + n\mathbf{Z}$. Der erstere Fall ist äquivalent zu $n \mid a$, also $n = a$ und der zweite zu $n \mid b$, also $n = b$. Damit besitzt n lediglich die natürlichen Teiler 1 und n und ist somit eine Primzahl (es gilt $n \geq 2$!). □

Bemerkung 1.5.22. Die zweite Implikation im Beweis von Proposition 1.5.21 läßt sich wie die erste ebenfalls aus der expliziten Formel für $\varphi(n)$ aus Korollar 1.5.16 ableiten: Nachdem man sich wegen $\mathbf{Z}/0\mathbf{Z} \cong \mathbf{Z}$ davon überzeugt hat, daß $n \geq 1$ ist, ist zu zeigen, daß $\varphi(n) = n-1$ impliziert, daß n eine Primzahl ist. Mithilfe der Formel für $\varphi(n)$ ergibt

sich mittels der Notation aus dem Korollar:

$$\begin{aligned}
n - \varphi(n) &= \prod_{i=1}^{r} p_i \cdot p_i^{v_i - 1} - \prod_{i=1}^{r} (p_i - 1) \cdot p_i^{v_i - 1} \\
&= p_1^{v_1 - 1} \cdot \left(p_1 \cdot \prod_{i=2}^{r} p_i \cdot p_i^{v_i - 1} - (p_1 - 1) \cdot \prod_{i=2}^{r} (p_i - 1) \cdot p_i^{v_i - 1} \right) \\
&= p_1^{v_1 - 1} p_2^{v_2 - 1} \cdot \left(p_1 p_2 \cdot \prod_{i=3}^{r} p_i \cdot p_i^{v_i - 1} - (p_1 - 1)(p_2 - 1) \cdot \prod_{i=3}^{r} (p_i - 1) \cdot p_i^{v_i - 1} \right) \\
&= \ldots \\
&= \prod_{i=1}^{r} p_i^{v_i - 1} \cdot \left(\prod_{i=1}^{r} p_i - \prod_{i=1}^{r} (p_i - 1) \right)
\end{aligned}$$

Dieser Ausdruck muß nach Voraussetzung den Wert 1 annehmen, sodaß

$$\prod_{i=1}^{r} p_i^{v_i - 1} = 1 \quad \text{und} \quad \prod_{i=1}^{r} p_i - \prod_{i=1}^{r} (p_i - 1) = 1$$

gelten müssen. Die erste Identität beschert uns $v_1 = v_2 = \cdots = v_r = 1$ und die zweite zeigt $r \geq 1$, da im Fall $r = 0$ die Differenz der Produkte 0 ist. Ein genaurerer Blick auf die zweite Identität zeigt, daß dank $r \geq 1$

$$\begin{aligned}
\prod_{i=1}^{r} p_i - \prod_{i=1}^{r} (p_i - 1) &= p_1 \cdot \prod_{i=2}^{r} p_i - (p_1 - 1) \prod_{i=2}^{r} p_i + (p_1 - 1) \cdot \prod_{i=2}^{r} p_i - \prod_{i=1}^{r} (p_i - 1) \\
&= \prod_{i=2}^{r} p_i + \underbrace{(p_1 - 1) \cdot \left(\prod_{i=2}^{r} p_i - \prod_{i=2}^{r} (p_i - 1) \right)}_{\geq 0} \\
&= 1,
\end{aligned}$$

was nur möglich ist, wenn[26] $r = 1$.

Satz 1.5.23 (Einheitengruppe eines endlichen Körper ist zyklisch)**.** *Es sei* $\mathbf{F}$ *eine endlicher Körper. Dann ist die Einheitengruppe* $\mathbf{F}^\times$ *zyklisch.*

Beweis. Wir wenden das Kriterium aus Satz 1.5.12 an. Sei hierzu $d \mid q - 1 = \#\mathbf{F}^\times$ ein Teiler der Gruppenordnung. Ein Element $x \in \mathbf{F}^\times$ der Ordnung d genügt der Gleichung

$$x^d = 1,$$

womit x Nullstelle des Polynoms $X^d - 1$ ist. Nun ist mit x auch jede Potenz x^k wegen

$$(x^k)^d = x^{k \cdot d} = x^{d \cdot k} = (x^d)^k = 1^k = 1$$

[26] Denn im Fall $r \geq 2$ ergibt sich: $\prod_{i=2} p_i = p_2 \cdot \prod_{i=3}^{r} p_i \geq p_2 \geq 2$,

eine Nullstelle von $X^d - 1$. Da ist jedes Element $y \in \langle x \rangle$ des Erzeugnisses von x ebenfalls eine Nullstelle von $X^d - 1$. Das zeigt

$$\langle x \rangle \ \subseteq \ \{z \in \mathbf{F} \mid z^d - 1 = 0\}. \tag{1.30}$$

Einerseits ist $\langle x \rangle$ eine d-elementige Menge. Andererseits besitzt das Polynom $X^d - 1$ in einem Körper höchstens d paarweise verschiedene Nullstellen, d. h.

$$\#\{z \in \mathbf{F} \mid z^d - 1 = 0\} \ \leq \ d.$$

Hieraus schließen wir mittels (1.30), daß

$$\langle x \rangle \ = \ \{z \in \mathbf{F} \mid z^d - 1 = 0\}$$

gelten muß. Es gibt in $\mathbf{F}^\times$ also höchstens eine zyklische Untergruppe der Ordnung d, womit es auch höchstens $\varphi(d)$ Elemente der Ordnung d geben kann. Das zeigt, daß die Voraussetzungen von Satz 1.5.12 erfüllt sind, woraus wir schließen, daß $\mathbf{F}^\times$ zyklisch ist. □

Bemerkung 1.5.24. Satz 1.5.23 besagt insbesondere, daß für jede Primzahl p die Einheitengruppe

$$\mathbf{F}_p^\times \ = \ (\mathbf{Z}/p\mathbf{Z})^\times \ = \ \{a + p\mathbf{Z} \mid 1 \leq a \leq p - 1\}$$

zyklisch. Insbesondere existiert ein Erzeuger $a + p\mathbf{Z}$, d. h. eine Einheit $a + p\mathbf{Z}$ mit der Eigenschaft, daß

$$\mathbf{F}_p^\times \ = \ \{a^k + p\mathbf{Z} \mid 0 \leq k < p - 1\}.$$

Mit anderen Worten: Jedes von 0 verschiedene Element $b + p\mathbf{Z}$ ist von der Form $b + p\mathbf{Z} = a^k + p\mathbf{Z}$. Äquivalent formuliert: Es existiert ein Element $1 \leq a \leq p - 1$ sodaß für jedes $b \in \mathbf{Z}$ mit $p \nmid b$ ein (eindeutig bestimmtes!) $0 \leq k < p - 1$ existiert mit

$$a^k \equiv b \pmod{p}.$$

Definition 1.5.25 (Primitivwurzeln)**.** Es sei p eine Primzahl. Ein Element $a \in \mathbf{F}_p$ (bzw. $a \in \mathbf{Z}$) heißt *Primitivwurzel* modulo p, wenn a (bzw. $a + p\mathbf{Z}$) ein Erzeuger von $\mathbf{F}_p^\times$ ist.

Bemerkung 1.5.26 (Existenz und Anzahl von Primitivwurzeln)**.** Satz 1.5.23 besagt, daß $\mathbf{F}_p^\times$ zyklisch ist. Als zyklische Gruppe der Ordnung $p - 1$ ist $\mathbf{F}_p^\times$ damit isomorph zu $\mathbf{Z}/(p-1)\mathbf{Z}$. In letzterer Gruppe gibt es laut Korollar 1.5.9 $\varphi(p-1)$ verschiedene Erzeuger. Daher gibt es für in $\mathbf{F}_p^\times$ genau $\varphi(p-1)$ paarweise verschiedene Primitivwurzeln.

Bemerkung 1.5.27 (Allgemeine Primitivwurzeln)**.** Obige Definition läßt sich auf beliebige endliche Körper $\mathbf{F}$ erweitern: Eine Primitivwurzel in $\mathbf{F}$ ist ein Erzeuger von $\mathbf{F}^\times$. Wenn q die Kardinalität von $\mathbf{F}$ bezeichnet, existieren in $\mathbf{F}^\times$ entsprechend $\varphi(q-1)$ paarweise verschiedene Primitivwurzeln.

Beispiel 1.5.28 (Primitivwurzeln modulo 3)**.** Es gilt

$$\mathbf{F}_3 = \{0 + 3\mathbf{Z}, 1 + 3\mathbf{Z}, 2 + 3\mathbf{Z}\} = \{0 + 3\mathbf{Z}, 1 + 3\mathbf{Z}, (-1) + 3\mathbf{Z}\}$$

und

$$\mathbf{F}_3^\times \ = \ \{\pm 1 + 3\mathbf{Z}\}$$

ist zyklisch von Ordnung 2. Das Element $a = (-1) + 3\mathbf{Z}$ ist ein Erzeuger der Einheitengruppe und damit eine Primitivwurzel. In diesem Fall ist dies die einzige Primitivwurzel.

Beispiel 1.5.29 (Primitivwurzeln modulo 5)**.** Es gilt

$$\mathbf{F}_5 = \{0+5\mathbf{Z}, 1+5\mathbf{Z}, 2+5\mathbf{Z}, 3+5\mathbf{Z}, 4+5\mathbf{Z}\} = \{0+5\mathbf{Z}, 1+5\mathbf{Z}, 2+5\mathbf{Z}, (-2)+5\mathbf{Z}, (-1)+5\mathbf{Z}\}$$

und damit

$$\mathbf{F}_5^\times = \{1+5\mathbf{Z}, 2+5\mathbf{Z}, (-2)+5\mathbf{Z}, (-1)+5\mathbf{Z}\}.$$

Wegen

$$2^2 = 4 \equiv -1 \pmod 5$$

ist $a = 2 + 5\mathbf{Z}$ eine Primitivwurzel: Wegen $2^2 \not\equiv 1$ gilt $\operatorname{ord} a > 2$. Da $\operatorname{ord} a \mid 4$ ergibt sich hieraus bereits $\operatorname{ord} a = 4$. Alternativ verifziert man händisch: $a^3 = 2^3 + 5\mathbf{Z} = 3 + 5\mathbf{Z} = (-2) + 5\mathbf{Z}$ und $a^4 = 2^4 + 5\mathbf{Z} = 1 + 5\mathbf{Z}$.

Analog überzeugt man sich davon, daß $-2 + 5\mathbf{Z}$ eine Primitivwurzel modulo 5 ist. Wegen $\varphi(\#\mathbf{F}_5^\times) = \varphi(5-1) = \varphi(4) = 2$ sind dies alle Primitivwurzeln in $\mathbf{F}_5$.

Beispiel 1.5.30 (Primitivwurzeln modulo 17)**.** Im Fall $p = 17$ ergibt sich $p-1 = 16 = 2^4$, womit analog zum Fall $p = 5$ ein Element $a \in \mathbf{Z}$ mit $17 \nmid a$ genau dann eine Primtivwurzel modulo 17 ist, wenn $a^8 \not\equiv 1 \pmod{17}$. Dies trifft beispielsweise auf $a = 3$ zu:

$$\begin{aligned} a^2 &\equiv 9 \equiv -8 \pmod{17} \\ a^4 &\equiv (a^2)^2 \equiv (-8)^2 \equiv 64 \equiv 13 \not\equiv 0 \pmod{17} \\ a^8 &\equiv ((a^2)^2)^2 \equiv 13^2 \equiv 16 \not\equiv 0 \pmod{77} \end{aligned}$$

Es gibt insgesamt $\varphi(16) = (2-1) \cdot 2^3 = 8$ Primitivwurzeln modulo 17. Die anderen erhalten wir wie folgt:

Zunächst nutzen wir den Isomorphismus

$$e : \mathbf{Z}/16\mathbf{Z} \to \mathbf{F}_{17}^\times, \quad k + 16\mathbf{Z} \mapsto 3^k \pmod{17}.$$

Dieser ist wohldefiniert, da $3^{16} \equiv 1 \pmod{17}$ und ein Isomorphismus von Gruppen, weil 3 eine Primtivwurzel modulo 17 ist. Aus Aussage (iv) der Proposition 1.5.7 wissen wir, daß sämtliche Elemente, welche $\mathbf{Z}/16\mathbf{Z}$ erzeugen, von der Form $a + 16\mathbf{Z}$ mit $\operatorname{ggT}(a, 16) = 1$ sind. Derer gibt es $\varphi(16)$ Stück und und ihre Bilder unter e sind gerade die Primitivwurzeln in $\mathbf{F}_{17}$. Die Teilerfremdheits $\operatorname{ggT}(a, 16) = 1$ ist nun äquivalent zu $2 \nmid a$, sodaß wir jeweils für $a = 1, 3, 5, 7, 9, 11, 13, 15$ eine Primtivwurzel $3^a + 17\mathbf{Z}$ in $\mathbf{F}_{17}$ erhalten. Dies sind alle Primitivwurzeln modulo 17.

Proposition 1.5.31 (Kriterium zur Bestimmung der Ordnung eines Elementes)**.** *Es sei $g \in G$ ein Element einer Gruppe $(G, \cdot)$ mit Neutralelement e. Für $n \geq 1$ sind dann äquivalent:*

(i) $\operatorname{ord} g = n$

(ii) $g^n = e$ *und für jede Primzahl* $p \mid n$ *gilt* $g^{n/p} \neq e$.

Beweis. Sei zunächst $\operatorname{ord} g = n$. Dann gilt $g^n = e$ und da $n \geq 1$ minimal mit dieser Eigenschaft ist, muß $g^{n/p} \neq e$ für alle Primteiler $p \mid n$ gelten. Das zeigt (i) $\Rightarrow$ (ii).

Sei nun umgekehrt $g^n = e$ und für jede Primzahl $p \mid n$ sei weiterhin $g^{n/p} \neq e$. Wegen $g^n = e$ ist n ein Vielfaches der Ordnung: Die Abbildung

$$\mathbf{Z}/m\mathbf{Z} \to \langle g \rangle, \quad k + m\mathbf{Z} \mapsto g^k$$

ist für $m = \operatorname{ord} g$ wohldefiniert und ein Isomorphismus von Gruppen. Dann ist $g^n = e$ äquivalent zu $n + m\mathbf{Z} = 0$, was wiederum zu $m \mid n$ äquivalent ist. Das zeigt, daß $\operatorname{ord} g \mid n$. Sei nun explizit $n = k \cdot \operatorname{ord} g$. Wenn $k > 1$, so existiert ein Primteiler $p \mid k$ (Lemma 1.4.28) und wir erhalten

$$g^{n/p} \;=\; g^{(\operatorname{ord} g)\cdot(k/p)} \;=\; \left(g^{\operatorname{ord} g}\right)^{k/p} \;=\; e^{k/p} \;=\; e,$$

im Widerspruch zur Annahme, daß $g^{n/p} \neq e$. Damit kann der Fall $k > 1$ nicht eintreten, womit $n = \operatorname{ord} g$, was zu zeigen war. □

Beispiel 1.5.32 (Primitivwurzeln modulo 109)**.** Im Fall $p = 109$ erhalten wir $p - 1 = 2^2 \cdot 3^3$. Dann repräsentiert ein $a \in \mathbf{Z}$ genau dann eine Primtivwurzel modulo 109, wenn $109 \nmid a$ und wenn zusätzlich:

$$\begin{aligned} a^{\frac{108}{2}} &\not\equiv 1 \pmod{109} \\ a^{\frac{108}{3}} &\not\equiv 1 \pmod{109} \end{aligned}$$

Man rechnet nach, daß

$$2^{36} \;\equiv\; 1 \pmod{109},$$

sodaß 2 keine Primitivwurzel modulo 109 ist. Weiterhin gilt

$$3^{36} \;\equiv\; 1 \pmod{109},$$

sodaß auch 3 keine Primitivwurzel repräsentiert. 4 scheidet als Quadrat von 2 ohnehin aus. Der nächste Kandidat scheidet wegen

$$5^{54} \;\equiv\; 1 \pmod{109},$$

aus, womit wir 6 testen:

$$\begin{aligned} 6^{\frac{108}{2}} &\equiv -1 \not\equiv 1 \pmod{109} \\ 6^{\frac{108}{3}} &\equiv 63 \not\equiv 1 \pmod{109}. \end{aligned}$$

Mithin ist 6 eine Primitivwurzel modulo 109. Die alle weiteren Primitivwurzeln erhalten wir durch Betrachtung von

$$6^k \pmod{109}, \quad 1 \leq k < 108,\ \operatorname{ggT}(k, 6) = 1,$$

denn k ist genau dann zu 108 teilerfremd, wenn es zu seinen beiden Primteilern 2 und 3 teilerfremd ist.

Bemerkung 1.5.33 (Diskretes Logarithmusproblem)**.** Es ist im Allgemeinen ein schwieriges Problem, zu einer gegebenen Primitivwurzel $a \in \mathbf{F}_p^\times$ und einem gegebenen $b \in \mathbf{F}_p^\times$ den eindeutig bestimmten Exponenten $1 \leq k < p - 1$ mit $a^k = b$ zu bestimmen. Diese Fragestellung wird als *diskretes Logarithmusproblem* bezeichnet. Algebraisch formuliert ist dies die Frage, das Inverse des Isomorphismus

$$e :\ \mathbf{Z}/(p-1)\mathbf{Z} \;\to\; \mathbf{F}_p^\times, \quad k + (p-1)\mathbf{Z} \;\mapsto\; a^k$$

zu bestimmen. Das Paradoxon besteht hier darin, daß $e(k)$ einfach zu berechnen ist, wohingegen sich die Berechnung von $e^{-1}(b)$ aufwendig gestaltet, wenn p nur groß genug ist.

1.5.5 Kryptographische Anwendungen

Die Tatsache, daß a^k in einem endlichen Körper $\mathbf{F}$ einfach zu berechnen, aber aus der Kenntnis von a und a^k der Exponent k schwer zu rekonstruieren ist, läßt sich in mehrerlei Hinsicht nutzen. Dies erlaubt es beispielsweise, daß sich zwei Parteien auf einen gemeinsamen geheimen Schlüssel einige und gleichzeitig garantiert werden kann, daß keine der beiden Parteien die Schlüsselwahl zu seinen Gunsten beeinflussen kann. Dies wird durch folgendes Verfahren realisiert.

Beispiel 1.5.34 (Diffie-Hellman-Schlüsselaustausch)**.** *Alice* und *Bob* wollen sich auf einen gemeinsamen Schlüssel einigen, um geheime Botschaften auszutauschen. Das Problem ist, daß sie sich erstens gegenseitig wenig vertrauen, d. h. beide Beanspruchen den gleichen Einfluß auf die Schlüsselwahl, und zweitens können Alice und Bob nur über einen öffentlichen Kanal kommunizieren[27]. Zunächst einigen sich Alice und Bob auf eine große Primzahl p, welche mindestens 300 Stellen im Dezimalsystem, sowie auf eine Primitivwurzel a modulo p, welche Sie beispielsweise durch Ausprobieren mittels Proposition 1.5.31 bestimmen. Das Paar (a, p) darf öffentlich bekannt sein. Daraufhin bestimmt Alice eine Zufallszahl $k \in \mathbf{Z}/(p-1)\mathbf{Z}$ und berechnet $\alpha := a^k$ modulo p. Bob wählt ebenfalls zufällig $\ell \in \mathbf{Z}/(p-1)\mathbf{Z}$ und berechnet $\beta := a^\ell$ modulo p. Daraufhin tauschen Alice und Bob auf dem öffentlichen Kanal α und β aus. Bob berechnet nun $\gamma := \alpha^\ell$ und Alice berechnet $\gamma' := \beta^k$. Wegen

$$\gamma \;=\; \alpha^\ell \;=\; (a^k)^\ell \;=\; a^{k\cdot\ell} \;=\; a^{\ell\cdot k} \;=\; (a^\ell)^k \;=\; \beta^k \;=\; \gamma'$$

kennen Alice und Bob nun beide die selbe Restklasse $\gamma \in (\mathbf{Z}/p\mathbf{Z})^\times$, aber Bob kennt weder k noch kennt Alice ℓ, ohne das entsprechende diskrete Logarithmusproblem zu lösen.

Anstatt in $\mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ zu rechnen, können Alice und Bob auch in einem ausreichend großen Körper $\mathbf{F}_q$ mit $q = p^d$ Elementen arbeiten. Aus technischen Gründen bieten sich hier insbesondere endliche Körper mit $q = 2^d$ Elementen an.

Obwohl dieses Verfahren nach *Whitfield Diffie* und *Martin Hellman* benannt ist, welche es 1976 publizierten, war es zuvor von *Ralph Merkle* entdeckt worden.

Bemerkung 1.5.35. Modulo einer 240-stelligen Zahl wurde 2019 ein diskreter Logarithmus erfolgreich berechnet. Dabei wurden 3100 CPU-Kern-Jahre auf Intel Xenon Gold 6130-Prozessoren aufgewandt. Daher sollte man heutzutage mindestens eine 1000-stellige Primzahl im Dezimalsystem wählen, wenn man auf der sicheren Seite sein möchte.

Bemerkung 1.5.36. Das Diffie-Hellman-Verfahren schützt nicht gegen *Man-in-the-middle-Angriffe*. D. h. wenn die Kommunikation zwischen Alice und Bob von Mallory abgefangen und verändert werden kann, dann kann sich Mallory ohne das Wissen von Alice und Bob sich jeweils mit Alice und Bob auf einen geheimen Schlüssel einigen und damit dann sämtliche Kommunikation, welche mit diesen geheimen Schlüsseln von Alice und Bob ausgetauscht wird, mitlesen und sogar modifizieren. Daher bedarf es weiterer Methoden, um die *Authentizität* sicherzustellen, d. h. es sollte ebenfalls ein Mechanismus zur Authentifizierung implementiert werden.

Bemerkung 1.5.37 (Public-Key-Verfahren)**.** Das Diffie-Hellman-Verfahren basiert auf der Schwierigkeit, diskrete Logarithmen zu bestimmen und erlaubt es, Schlüssel auszutauschen. Das Problem der Authentifizierung als auch der Verschlüsselung wird von einem

[27] Das bedeutet, daß Dritte die Kommunikation mithören können!

Public-Key-Verfahren gelöst. Das Prinzip besteht darin, daß Alice ein Geheimnis kennt, dessen Besitz sie Bob nachweisen kann, ohne das Geheimnis dabei zu verraten. Dieses Geheimnis wird als *privater Schlüssel* oder *private key* von Alice bezeichnet. Bob wird hingegen Zugriff auf einen *öffentlichen Schlüssel* oder *public key* von Alice erlaubt, mit dessen Hilfe er verifizieren kann, ob eine Nachricht von Alice kommt und den er wahlweise auch dafür nutzen kann, um Alice verschlüsselte Nachrichten zu senden, welche nur Alice entschlüsseln kann, da nur sie ihren *private key* kennt.

Beispiel 1.5.38 (ElGamal-Verschlüsselungs-Verfahren)**.** Sei $\mathbf{F}$ ein endlicher Körper mit q Elementen. Als Variante des Verfahrens von Diffie-Hellman-Merkle könnte Alice eine Primitivwurzel $a \in \mathbf{F}^\times$ wählen, sowie einen zufälligen Exponenten $1 \leq k < q-1$. Dann veröffentlicht Alice (a, a^k) als ihren öffentlichen Schlüssel. Das Geheimnis, das Alice für sich bewahrt ist k, d. h. ihr privater Schlüssel ist in diesem Fall k. Da die Extraktion von k aus dem Paar (a, a^k) eine Instanz des diskreten Logarithmus-Problems ist, ist es für Mallory schwierig, hieraus k zu rekonstruieren.

Sei (a, b) der öffentliche Schlüssel von Alice, d. h. in nach obiger Konstruktion gilt $b = a^k$. Wenn Bob Alice nun eine geheime Nachricht $x \in \mathbf{F}^\times$ zukommen lassen möchte, wählt er ein zufälliges $1 \leq \ell < q-1$ und berechnet $m := x \cdot b^\ell$, sowie $n := a^\ell$ und übermittelt diese beide an Alice.

Alice entschlüsselt die Nachricht (m, n) von Bob nun wie folgt: Sie rekonstruiert zunächst b^ℓ, indem sie $n^k = (a^\ell)^k$ berechnet, denn es gilt $n^k = a^{k \cdot \ell} = b^\ell$. Damit ergibt sich:

$$m \cdot (n^k)^{-1} \;=\; m \cdot (b^\ell)^{-1} \;=\; x \cdot b^\ell \cdot b^{-\ell} \;=\; x.$$

Die Sicherheit des Verfahrens beruht darauf, daß die Kenntnis von x äquivalent zur Kenntnis von $x^{-1} \cdot m = b^\ell = (a^k)^\ell$ ist, was ohne Kenntnis des Geheimnisses k oder des Geheimnisses ℓ nicht aus den gegebenen Daten rekonstruierbar ist, wenn das diskrete Logarithmusproblem für a, a^k schwierig ist bzw. ℓ nicht aus b, xb^ℓ rekonstruiert werden kann[28].

Beispiel 1.5.39 (ElGamal-Verschlüsselung in $\mathbf{F}_{109}^\times$)**.** Alice und Bob einigen sich auf $p = 109$, d. h. konkret $\mathbf{F} = \mathbf{F}_{109} = \mathbf{Z}/109\mathbf{Z}$. Weiterhin einigen sich Alice und Bob auf die Primitivwurzel $a = 6$ (vgl. Beispiel 1.5.32). Weiterhin teilt Alice Bob ihren öffentlichen Schlüssel mit: $(a, b) = (6, 95)$. Nun möchte Bob Alice mitteilen, daß er 100 Seiten des Elementare-Zahlentheorie-Skriptums gelesen hat. Daher möchte er Alice die Zahl $x = 100$ als verschlüsselte Nachricht m übermitteln. Er wählt also ein zufälliges $1 \leq \ell < 108$. Konkret wählt er $\ell = 57$ und berechnet damit

$$b^\ell \;\equiv\; 95^\ell \;\equiv\; 19 \pmod{109}$$

Er erhält er

$$m \;\equiv\; x \cdot b^\ell \;\equiv\; 100 \cdot 95^{57} \;\equiv\; 47 \pmod{109}$$

Damit Alice x rekonstruieren kann, muß Bob noch

$$n \;\equiv\; a^\ell \;\equiv\; 6^{57} \;\equiv\; 2 \pmod{109}$$

[28] Das Verfahren ist anfällig für *Chosen-Ciphertext-Angriffe*, d. h. wenn Mallory z. B. Alice dazu bringen kann, für ein $f \neq 0$ die Nachricht $f \cdot m$ zu entschlüsseln, dann erhält sie $f \cdot x$ als Ergebnis, woraus sich x rekonstruieren läßt.

bestimmen. Nun übermittelt Bob Alice die Nachricht $(m, n) = (47, 2)$.

Alice packt nun ihren geheimen Schlüssel $k = 43$ aus und berechnet zunächst

$$n^k \equiv 2^{43} \equiv 19 \pmod{109}$$

Dies gilt es modulo 19 zu invertieren[29]. Hier könnte Alice nun den erweiterten Euklidischen Algorithmus anwerfen, entschließt sich jedoch stattdessen, folgenden Trick anzuwenden: Da für $c \in \mathbf{F}_{109}^{\times}$ stets $c^{108} = 1$ gilt, muß

$$2^{43} \cdot 2^{108-43} \equiv 2^{43+(108-43)} \equiv 2^{108} \equiv 1 \pmod{109}$$

gelten, womit

$$2^{108-43} \equiv 2^{65} \equiv 23 \pmod{109}$$

das multiplikative Inverse zu 2^{43} modulo 109 ist, womit sich Alice obige Berechnung von 2^{43} modulo 109 hätte sparen können!

Mit diesem Inversen an der Hand, entschlüsselt Alice schlußendlich die Nachricht:

$$m \cdot (2^{43})^{-1} \equiv 47 \cdot 23 \equiv 100 \pmod{109}.$$

Beispiel 1.5.40 (ElGamal-Signatur-Verfahren)**.** Als wie zuvor veröffentlicht Alice das Paar (a, a^k) und behält k für sich. Im Unterschied zum Verschlüsselungsverfahren, arbeitet Alice zur Erstellung einer Unterschrift nicht in einem allgemeinen endlichen Körper $\mathbf{F}$, sondern konkret in einem Primkörper $\mathbf{F} = \mathbf{F}_p = \mathbf{Z}/p\mathbf{Z}$ und sie betrachtet nicht Nachrichten direkt in $\mathbf{F}_p^{\times}$, sondern in $\mathbf{Z}/(p-1)\mathbf{Z}$, was via

$$\ell + (p-1)\mathbf{Z} \mapsto a^{\ell}$$

jedoch zu $\mathbf{F}_p^{\times}$ isomorph ist[30].

Wenn Alice nun eine Nachricht $1 \leq x \leq p-1$ unterschreiben möchte, dann wählt sie ein zufälliges $1 < \ell < p-1$, welches zu $p-1$ teilerfremd ist, d. h. sie wählt ℓ derart, daß $\ell + (p-1)\mathbf{Z}$ in $\mathbf{Z}/(p-1)\mathbf{Z}$ multiplikativ invertierbar ist. Das bedeutet, daß Alice die Inverse der Abbildung $\mathbf{F}_p \to \mathbf{F}_p$, $y \mapsto y^{\ell}$ effizient als $z \mapsto z^r$ berechnen kann, wenn $r \cdot \ell \equiv 1 \pmod{()p-1}$, denn es gilt dann:

$$(y^{\ell})^r = y^{\ell \cdot r} = y^1.$$

Damit ausgestattet berechnet Alice nun ihre Unterschrift als $t + p\mathbf{Z} := g^{\ell}$, sowie

$$s := (x - k \cdot t) \cdot r \pmod{(p-1)},$$

wobei sie den Repräsentanten $0 \leq t < p$ wählt. Im unwahrscheinlichen Fall, daß $s = 0$, wählt Alice ein anderes zufälliges ℓ. Sie übersendet Bob schlußendlich x zusammen mit dem Paar (s, t)

Wenn Bob nun die Nachricht x zusammen mit obiger Signatur (s, t) erhält, berechnet er

$$b^t \cdot t^s = (a^k)^t \cdot t^{(x-kt)r} = a^{kt} \cdot a^{\ell \cdot (x-kt)r} = a^{kt} \cdot a^{x-kt} = a^x,$$

[29] Zur Verifikation: Es gilt tatsächlich $19 \equiv 95^{57}$!

[30] Das Problem besteht darin, daß auch Alice keine diskreten Logarithmen effizient berechnen kann, weswegen sie im Folgenden nicht direkt von einem $x \in \mathbf{F}_p^{\times}$ ausgehen kann.

d. h. wenn a^x mit $b^t \cdot t^s$ übereinstimmt, ist die Signatur von Alice gültig. Andernfalls ist sie ungültig.

In der Praxis ist es wichtig, nicht unmittelbar die Nachricht x zu verwenden, sondern das Bild von x unter einer kryptographischen *Hash-Funktion* zu verwenden. Andernfalls ist obiges Verfahren anfällig für Fälschungen der Signatur. Auch aus Effiziengründen ist die Verwendung einer Hash-Funktion angeraten.

Beispiel 1.5.41 (RSA-Verfahren)**.** Eine weitere Variation des Diffie-Hellman-Verfahrens ist das RSA-Verfahren von Ron Rivest, Adi Shamir und Leonard Adleman aus dem Jahr 1977. Hier wählt Alice zwei zufällige große Primzahlen p und q und berechnet $N := p \cdot q$. Sie behält p und q für sich, diese sind Teil ihres Geheimnisses, d. h. ihres privaten Schlüssels. Die Sicherheit dieses Verfahrens beruht auf der Schwierigkeit, p und q aus N zu rekonstruieren. Weiterhin wählt Alice ein zufälliges $2 \leq e < \varphi(N) - 1$, welches zu $\varphi(N) = (p-1) \cdot (q-1)$ teilerfremd ist. Schließlich veröffentlicht sie (N, e) als ihren öffentlichen Schlüssel. Ihr privater Schlüssel besteht letztendlich aus demjenigen $2 \leq d < \varphi(N) - 1$ mit $d \cdot e \equiv 1 \pmod{\varphi(N)}$, welches sie problemlos mithilfe des erweiterten Euklidischen Algorithmus bestimmen kann. Da Mallory $\varphi(N)$ nicht kennt (er kennt weder p noch q, er kennt nur e und N), kann er sich d nicht so einfach beschaffen.

Nachrichten werden nun als Elemente in $(\mathbf{Z}/N\mathbf{Z})^\times$ kodiert. Wenn Bob Alice eine geheime Nachricht $x \in (\mathbf{Z}/N\mathbf{Z})^\times$ übermitteln möchte, berechnet er $m := x^e \in \mathbf{Z}/N\mathbf{Z}$ und übermittelt dieses. Alice berechnet daraufhin[31]

$$m^d \;=\; (x^e)^d \;=\; x^{ed} \;=\; x^{1+k\varphi(N)} \;=\; x \cdot \underbrace{x^{\varphi(N)}}_{=1}.$$

Weiterhin kann Alice Nachrichten mithilfe von d unterschreiben: Will sie die Nachricht $x \in (\mathbf{Z}/N\mathbf{Z})^\times$ unterzeichnen, dann berechnet sie die Signatur als $s := x^d$ und veröffentlicht (x, s). Bob kann die Signatur verifizieren, indem er analog zu Alice Entschlüsselungsverfahren s^e mit x vergleicht. Gilt $s^e = x$ in $\mathbf{Z}/N\mathbf{Z}$, so ist die Signatur gültig, andernfalls nicht.

Beispiel 1.5.42 (Eine konkrete RSA-Signatur)**.** Alice wählt $p = 17$ und $q = 23$ als Primzahlen und erhält $N = 17 \cdot 23 = 391$, sowie

$$\varphi(N) \;=\; \varphi(17) \cdot \varphi(23) \;=\; 16 \cdot 22 \;=\; 352.$$

Schlußendlich wählt sie $d = 125$ zufällig und prüft, daß $\mathrm{ggT}(d, \varphi(N)) = 1$. Weiterhin bestimmt sie nebenbei mithilfe des erweiterten Euklidischen Algorithmus den Repräsentanten $e = 245$ des Inversen von d modulo $\varphi(N)$. Sie veröffentlicht $(N, e) = (391, 245)$ als ihren öffentlichen Schlüssel.

Nun will Alice Bob eine Nachricht zukommen lassen, zusammen mit ihrer digitalen Unterschrift. Die Nachricht lautet $x = 200$, interpretiert als Element von $\mathbf{Z}/391\mathbf{Z}$, denn sie hat inzwischen ganze 200 Seiten des Skriptums zur Elementaren Zahlentheorie verinnerlicht. Ihre Unterschrift s berechnet sie als

$$s \;\equiv\; x^d \;\equiv\; 200^{125} \;\equiv\; 285 \pmod{391}.$$

[31] Wenn $ed = 1 + k\varphi(N)$ mit einem $k \in \mathbf{Z}$.

Konkret übermittelt sie Bob die Nachricht x zusammen mit der Signatur $s = 285$ als Paar $(200, 285)$.

Bob weiß mit Sicherheit, daß der Schlüssel $(391, 245)$ zu Alice gehört und verifiziert ihre Unterschrift, indem er

$$s^e \equiv 285^{245} \equiv 200 \pmod{391}$$

berechnet und mit der Nachricht $x = 200$ vergleicht. Bob würde gerne glauben, daß dies ein Scherz von Mallory war, denn 200 Seiten sind ein großer Batzen — so weit ist Bob noch nicht. Da s^e und $x = 200$ übereinstimmen, kann Bob jedoch sicher sein, daß diese Nachricht tatsächlich von Alice kommt, d. h. Alice hat wirklich 200 Seiten gelesen, oder behauptet dies zumindest.

Bemerkung 1.5.43. Bei diesen kryptographischen Anwendungen der Zahlentheorie hat man es mit großen Zahlen zu tun. Um diese einzuordnen, anbei eine Tabelle zur Einordnung:

	Absolut	Dezimalstellen	Binärstellen
Jahre bis Erholung der Korallenriffe	2 000 000	7	21
Jahre bis Erholung der Ökodiversität	10 000 000	8	23
Jahre bis Bildung eines Superkontinents	250 000 000	9	28
Jahre bis vollständige Mondfinsternis unmögl.	600 000 000	9	30
Jahre bis Leuchtkraft Sonne 10% größer	1 100 000 000	10	31
Jahre bis Kollision Milchstraße & Andromeda-Galaxie	4 000 000 000	10	32
Jahre bis Erde in Sonne fällt	7 590 000 000	10	33
Weltbevölkerung Menschen (2020)	7 800 000 000	10	33
Jahre bis Galaxien außerh. der lokalen Gruppe hinter den kosmischen Lichthorizont fallen	125 000 000 000	12	37
Jahre bis Brennstoff aller Sterne verbraucht	105 000 000 000 000	14	47
Fläche der Erde in m^2	510 000 000 000 000	15	49
Weltbevölkerung Ameisen	1 000 000 000 000 000	15	50
Volumen der Erde in m^3	1 083 206 916 846 000 000 000	21	70
Sterne im Universum	$2 \cdot 10^{23}$	23	76
Durchmesser des Universums in m	$9 \cdot 10^{26}$	26	90
Jahre bis Zerfall aller Nukleonen (frühe Schätzung)	$2 \cdot 10^{36}$	37	121
Jahre bis Zerfall aller Nukleonen (späte Schätzung)	$3 \cdot 10^{43}$	44	144
Masse des Universums in kg	$1,5 \cdot 10^{53}$	54	177
Atome im Universum	10^{80}	80	266
Volumen des Universums in m^3	$4 \cdot 10^{80}$	81	268
Jahre bis Zerfall aller Nukleonen (späteste Schätzung)	10^{200}	200	665

1.5.6 Faktorisierungsverfahren

In diesem Abschnitt beschäftigen wir uns mit dem *Faktorisierungsproblem*: Wie zerlegen wir ein gegebenes $n \in \mathbf{N}$ in Primfaktoren?

Zunächst beobachten wir, daß es keine Schwierigkeit darstellt, Potenzen von 2 abzuspalten, sodaß wir im Folgenden getrost annehmen dürfen, daß n ungerade ist, sofern die konkrete Situation dies erfordert.

Das Faktorisierungsverfahren von Fermat hatten wir bereits auf dem Übungsblatt 3 besprochen. Ein weiteres elementares Verfahren ist

Pollards $p-1$-Methode. Die Idee dieses Verfahrens besteht darin, daß wenn $n = n_1 \cdot n_2$ mit teilerfremden n_1, n_2, uns der Chinesische Restsatz einen kanonischen Isomorphismus

$$(\mathbf{Z}/n\mathbf{Z})^\times \;\cong\; (\mathbf{Z}/n_1\mathbf{Z})^\times \times (\mathbf{Z}/n_2\mathbf{Z})^\times$$

beschert. Dabei ist die erste Gruppe rechterhand von Ordnung $\varphi(n_1)$ und die zweite von Ordnung $\varphi(n_2)$. Wir wählen nun ein $a + n\mathbf{Z} \in (\mathbf{Z}/n\mathbf{Z})^\times$ zufällig und versuchen ein k zu erraten, für welches

$$a^k \equiv 1 \pmod{n_1} \quad \text{und} \quad a^k \not\equiv 1 \pmod{n_2},$$

oder

$$a^k \not\equiv 1 \pmod{n_1} \quad \text{und} \quad a^k \equiv 1 \pmod{n_2}.$$

Tritt einer dieser beiden Fälle ein, dann erhalten wir

$$n_1 \mid \mathrm{ggT}(a^k - 1, n) \neq n \text{ (erster Fall)} \quad \text{bzw.} \quad n_2 \mid \mathrm{ggT}(a^k - 1, n) \neq n \text{(zweiter Fall)},$$

d. h. wir hätten mit $d = \mathrm{ggT}(a^k - 1, n)$ einen nichttrivialen Teiler von n gefunden.

Um dies zu bewerkstelligen, hoffen wir, daß konkret $\varphi(n_1)$ nur Primteiler $\leq B$ für eine nicht allzu große Schranke B besitzt. Dann wählen wir k als Produkt aller Primzahlen $\leq B$ (ggf. erlauben wir kleine Primzahlen wie 2, 3 mit größerem Exponenten als 1 in k), womit hoffentlich $\varphi(n_1) \mid k$ gilt. Dann ist die Relation

$$a^k \equiv 1 \pmod{n_1}$$

für alle zu n_1 teilerfremden $a \in \mathbf{Z}$ automatisch erfüllt und sofern $\varphi(n_2)$ einen Primteiler $> B$ besitzt, gilt mit großer Wahrscheinlichkeit

$$a^k \not\equiv 1 \pmod{n_2}.$$

Beispiel 1.5.44 (Pollards $p-1$-Methode)**.** Konkret ist der öffentliche Schlüssel $(391, 245)$ von Alice aus Beispiel 1.5.42 auf diese Weise angreifbar. Für die Primfaktor 17 und 23 von 391 gilt

$$\varphi(17) = 16 = 2^4 \quad \text{und} \quad \varphi(23) = 22 = 2 \cdot 11.$$

Hier tut es also $B = 2$, sofern wir den Exponenten von 2 in k ausreichend groß, d. h. ≥ 4 wählen.

Konkret ergibt sich im Fall $B := 3$ beispielsweise für $k = 2^4 \cdot 3^2 = 144$ (a priori wissen wir nicht, daß nur der Primteiler 2 in $\varphi(17)$ auftritt!) und $a = 3$:

$$a^k \equiv 3^{144} \equiv ((((3^2)^2)^{\cdots})^3)^3 \equiv 256 \pmod{391}$$

und damit

$$\mathrm{ggT}(a^k - 1, 391) \;=\; \mathrm{ggT}(256 - 1, 391) \;=\; \mathrm{ggT}(255, 391) \;=\; 17,$$

womit wir einen nichttrivialen Teiler von 391 und damit im vorliegenden Fall sogar bereits die Primfaktorzerlegung

$$391 \;=\; 17 \cdot (391/17) \;=\; 17 \cdot 23$$

erhalten.

Bemerkung 1.5.45. Das Verfahren von Pollard ist der Grund dafür, daß man in der Praxis bei der Schlüsselwahl im RSA-Verfahren prüft, ob die Primzahlen, p und q, aus welchen man $N = p \cdot q$ konstruieren möchte die Eigenschaft besitzen, daß jeweils $\varphi(p) = p-1$ und $\varphi(q) = q-1$ mindestens einen großen Primteiler besitzen. Ansonsten könnte N mithilfe von Pollards $p-1$-Methode faktorisiert werden.

Bemerkung 1.5.46 (Gruppenbasierte Faktorisierungsverfahren)**.** Die Gruppe $(\mathbf{Z}/n\mathbf{Z})^\times$ läßt sich durch andere endliche Gruppen $G(\mathbf{Z}/n\mathbf{Z}) \cong G(\mathbf{Z}/p\mathbf{Z}) \times G(\mathbf{Z}/q\mathbf{Z})$ ersetzen, deren Ordnung variiert, sodaß selbst im Fall, daß $p-1$ und $q-1$ große Primteiler besitzen, welche Pollards Methode inpraktikabel machen, eine Chance besteht, auf analoge Weise n zu faktorisieren. Hierzu bieten sich insbesondere *elliptische Kurven* an.

In Aufgabe 4 von Übungsblatt 3 haben wir gesehen, daß das Problem, n zu faktorisieren äquivalent dazu ist, n in nichttrivialer Weise als Differenz zweier Quadrate zu schreiben: $n = x^2 - y^2$, da sich dann wegen $x^2 - y^2 = (x+y) \cdot (x-y)$ die beiden Zahlen $x+y$ und $x-y$ als nichttriviale Teiler von n erweisen.

Mit dem Verfahren von Fermat haben wir auf selbigem Übungsblatt eine Methode kennengelernt, die dies ausnutze, jedoch im Allgemeinen trotzdem nicht effizient ist. Fermats Methode wollen wir verbessern.

Die erste Beobachtung besteht darin, daß es ausreichend ist, anstatt für $x, y \in \mathbf{Z}$ die Bedingung $n = x^2 - y^2$ zu fordern, abgeschwächt $x^2 - y^2 \equiv 0 \pmod{n}$, d. h. äquivalent

$$x^2 \;\equiv\; y^2 \pmod{n} \tag{1.31}$$

erreichen möchten. Dabei stellt sich die Frage, wann dies eine Faktorisierung von n liefert. Sei hierzu konkret $n = p \cdot q$ mit paarweise verschiedenen Primzahlen $p, q \geq 3$. Dann ist (1.31) dank des Chinesischen Restsatzes äquivalent zu den beiden simultanen Kongruenzen

$$\begin{aligned} x^2 \;&\equiv\; y^2 \pmod{p} \\ x^2 \;&\equiv\; y^2 \pmod{q} \end{aligned}$$

Wir dürfen dabei annehmen, daß $p, q \nmid x, y$ (ansonsten hätten wir einen Teiler erraten!).

Die erste Kongruenz ist äquivalent zu $y \equiv \pm x \pmod{p}$, da $x^2 + p\mathbf{Z}$ in $\mathbf{F}_p$ genau zwei quadratwurzeln besitzt, denn $\mathbf{Z}/p\mathbf{Z}$ ist ein Körper der Charakteristik $p \neq 2$. Analog ist die zweite Kongruenz äquivalent zu $y \equiv \pm x \pmod{q}$. Wir schließen damit, daß insgesamt vier Fälle möglich sind.

In zwei Fällen, nämlich wenn $y \equiv \pm x \pmod{n}$, dann beschert uns (1.31) keine Faktorisierung. Dies sind die trivialen Fällen. In den anderen beiden Fällen gilt $y \equiv \pm x \pmod{p}$ und zugleich $y \equiv \mp x \pmod{q}$, was zeigt, daß in diesem Fall stets

$$1 < \mathrm{ggT}(x - y, n) < n.$$

Mit anderen Worten: In der Hälfte aller möglichen Fälle führt die Kongruenz (1.31) zu einer Faktorisierung von n (unter der Voraussetzung, daß $n = p \cdot q$).

Wir schließen hieraus ebenfalls, daß die Bestimmung aller Quadratwurzeln einer Restklasse modulo n das Faktorisierungsproblem löst. Mithin: Quadratwurzeln modulo n bestimmen ist mindestens so schwer wie n zu faktorisieren.

Beispiel 1.5.47. Sei $n = 3 \cdot 5 = 15$. Wir wählen $x = 7$ und erhalten

$$x^2 \equiv 49 \equiv 4 \pmod{15}.$$

Dann genügt offensichtlich $y = 2$ der Bedingung

$$x^2 \equiv y^2 \pmod{15}.$$

Wegen

$$\mathrm{ggT}(x - y, n) = \mathrm{ggT}(7 - 2, 15) = \mathrm{ggT}(5, 15) = 5$$

erhalten wir tatsächlich eine Faktorisierung von 15. Der zweite nichttriviale Fall ist $y \equiv -2 \pmod{15}$, die beiden trivialen Fälle sind $y \equiv \pm 7 \pmod{15}$.

Es stellt sich die Frage, wie wir uns x und y beschaffen können, welche der Kongruenz (1.31) genügen. In obigem Beispiel hatten wir Gück: Wir haben dem Rest 4 modulo 15 angesehen, daß er ein Quadrat war und dies führte zufälligerweise zu einem nichttrivialen Fall.

Aus der Perspektive des Chinesischen Restsatzes, sollten wir zuerst verstehen, wie sich Quadrate modulo p, d. h. in $\mathbf{F}_p$, verhalten. Wieviele gibt es? Trägt die Menge der Quadrate eine besondere Struktur?

1.5.7 Quadrate in $\mathbf{F}_p$

Die letzte Frage ist einfach zu beantworten: In jedem Körper K ist die Menge der von Null verschiedenen Quadrate

$$Q(K) := \{x^2 \mid x \in K^\times\}$$

eine abelsche Gruppe bezüglich der Multiplikation: $1 = 1^2$ ist ein Quadrat, weswegen $Q(K) \neq \emptyset$. Weiterhin ist für $x, y \in K^\times$ stets

$$(x^2)^{-1} \cdot y^2 = \left(x^{-1}\right)^2 \cdot y^2 = (x^{-1}y)^2 \in Q(K)$$

wieder ein Element in $Q(K)$, was zeigt, daß $Q(K)$ eine Untergruppe von $K^\times$ ist (Untergruppenkriterium).

Damit wissen wir, daß $Q(\mathbf{F}_p)$ eine Untergruppe von $\mathbf{F}_p^\times$ ist. Letztere Gruppe hat Kardinalität $p - 1$, mithin gilt $\#Q(\mathbf{F}_p) \mid p - 1$. Die Anzahl der von Null verschiedenen Quadrate in $\mathbf{F}_p$ ist also ein Teiler von $p - 1$. Wir können jedoch mehr sagen:

Satz 1.5.48 (Quadrate in $\mathbf{F}_p$)**.** *Sei $p \geq 3$ prim. In $\mathbf{F}_p$ existieren $\frac{p+1}{2}$ Quadrate. Die Gruppe $Q(\mathbf{F}_p)$ der von Null verschiedenen Quadrate in $\mathbf{F}_p$ ist zyklisch von Ordnung $\frac{p-1}{2}$. Eine Einheit $a \in \mathbf{F}_p^\times$ ist genau dann ein Quadrat, wenn*

$$a^{\frac{p-1}{2}} = 1. \tag{1.32}$$

Andernfalls gilt

$$a^{\frac{p-1}{2}} = -1. \tag{1.33}$$

Beweis. Es ist klar, daß $0 = 0^2$ ein Quadrat in $\mathbf{F}_p$ ist. Daher genügt es im Folgenden, die von Null verschiedenen Quadrate in $\mathbf{F}_p^\times$ zu studieren. Hierzu bemerken wir zunächst, daß die Einheitengruppe $\mathbf{F}_p^\times$ zyklisch ist (vgl. Satz 1.5.23). Ist $w \in \mathbf{F}_p^\times$ eine Primitivwurzel, erhalten wir einen Isomorphismus

$$e:\ \mathbf{Z}/(p-1)\mathbf{Z} \to \mathbf{F}_p^\times, \quad k + (p-1)\mathbf{Z} \mapsto w^k.$$

Das Urbild $e^{-1}(Q(\mathbf{F}_p))$ ist eine zu $Q(\mathbf{F}_p)$ isomorphe Untergruppe von $\mathbf{Z}/(p-1)\mathbf{Z}$ und damit zyklisch (vgl. Proposition 1.5.7 (v)). Insbesondere ist $Q(\mathbf{F}_p)$ zyklisch (Moral: Untergruppen zyklischer Gruppen sind stets zyklisch).

Sei nun $a \in Q(\mathbf{F}_p)$ ein Quadrat. Dann finden wir ein $x \in \mathbf{F}_p^\times$ mit $x^2 = a$ und wir erhalten

$$a^{\frac{p-1}{2}} \ = \ (x^2)^{\frac{p-1}{2}} \ = \ x^{2\frac{p-1}{2}} \ = \ x^{p-1} \ = \ 1,$$

da $p-1$ die Gruppenordnung ist.

Sei umgekehrt $a \in \mathbf{F}_p^\times$ mit

$$a^{\frac{p-1}{2}} \ = \ 1.$$

Da w eine Primitivwurzel ist, finden wir einen Exponenten k mit $a = w^k$. Damit ergibt sich

$$w^{k\cdot\frac{p-1}{2}} \ = \ (w^k)^{\frac{p-1}{2}} \ = \ a^{\frac{p-1}{2}} \ = \ 1,$$

was zeigt, daß die Ordnung $p-1$ von w den Exponenten $k \cdot \frac{p-1}{2}$ teilen muß. Aus der Relation

$$(p-1) \mid \frac{k\cdot(p-1)}{2}$$

schließen wir, daß k gerade sein muß. Dann haben wir mit $x := w^{k/2}$ eine Quadratwurzel von a gefunden, mithin ist a ein Quadrat. Das zeigt, daß die Bedingung (1.32) tatsächlich (von Null verschiedene) Quadrate charakterisiert.

Für allgemeines $a \in \mathbf{F}_p^\times$ schließen wir aus

$$\left(a^{\frac{p-1}{2}}\right)^2 \ = \ a^{2\frac{p-1}{2}} \ = \ a^{p-1} \ = \ 1,$$

daß $a^{\frac{p-1}{2}}$ stets eine Quadratwurzel von 1 ist, was zeigt, daß ± 1 die einzigen Werte sind, welche dieser Ausdruck annehmen kann. Das zeigt, daß Bedingung (1.33) die Nichtquadrate in $\mathbf{F}_p$ charakterisiert.

Zuguterletzt müssen wir zählen, wieviele Quadrate es gibt. Hierzu beobachten wir, daß die Quadrate in $\mathbf{F}_p^\times$ unter obigem Isomorphismus e denjenigen Exponenten $k + (p-1)\mathbf{Z}$ entsprechen, für welche k gerade ist ($p-1$ ist ebenfalls gerade!). Da es hiervon genau $\frac{p-1}{2}$ gibt, schließt dies den Beweis ab. □

Korollar 1.5.49. *Das Produkt zweier Nichtquadrate in $\mathbf{F}_p$ ist ein Quadrat in $\mathbf{F}_p^\times$.*

Beweis. Zunächst beobachten wir, daß Nichtquadrate stets von 0 verschieden sind (0 ist ein Quadrat). Sind $a, b \in \mathbf{F}_p^\times$ keine Quadrate, so zeigt Bedingung (1.33) aus Satz 1.5.48, daß

$$(a\cdot b)^{\frac{p-1}{2}} \ = \ \underbrace{a^{\frac{p-1}{2}}}_{=-1} \cdot \underbrace{b^{\frac{p-1}{2}}}_{=-1} \ = \ (-1)^2 \ = \ 1,$$

womit das Kriterium (1.32) aus Satz 1.5.48, zeigt, daß $a\cdot b \in Q(\mathbf{F}_p)$, was zu zeigen war. □

Wir fassen zusammen: Das Produkt zweier Quadrate ist ein Quadrat und das Produkt zweier Nichtquadrate ist wieder ein Quadrat. Beides ergibt sich letztendlich aus der Charakterisierung aus Satz 1.5.48 zusammen mit der Tatsache, daß $a \mapsto a^{\frac{p-1}{2}}$ ein Gruppenhomomorphismus ist (genau dies haben wir soeben ausgenutzt!). Weil dieser so nützlich ist, formulieren wir

Definition 1.5.50 (Legendre-Symbol)**.** Für jede Primzahl $p \geq 3$ definieren wir das *Legendre-Symbol* als den Gruppenhomomorphismus

$$\left(\frac{\cdot}{p}\right) : (\mathbf{Z}/p\mathbf{Z})^\times \to \{\pm 1\}, \quad a \mapsto a^{\frac{p-1}{2}}.$$

Bemerkung 1.5.51. Die Menge $Q(\mathbf{F}_p)$ der von Null verschiedenen Quadrate ist gemäß Satz 1.5.48 der Kern des Legendre-Symbols $\left(\frac{\cdot}{p}\right)$.

Beispiel 1.5.52 (Eine Quadratische Gleichung in $\mathbf{F}_{17}$)**.** Wir möchten entscheiden, ob die quadratische Gleichung

$$X^2 + X + 1 \;=\; 0$$

in $\mathbf{F}_{17}$ lösbar ist. Hierzu reduzieren wir die Lösbarkeit zunächst auf die Frage, ob die äquivalente Gleichung

$$\left(X + \frac{1}{2}\right)^2 - \frac{1}{4} + 1 \;=\; 0$$

in $\mathbf{F}_{17}$ lösbar ist. Hierbei stehen $1/2$ und $1/4$ jeweils als Platzhalter für die multiplikativen Inversen zu 2 und4 modulo 17. Es stellt sich also die Frage, ob

$$\frac{1}{4} - 1 \;=\; -\frac{3}{4}$$

ein Quadrat in $\mathbf{F}_{17}$ ist. Nun ist $1/4 = (1/2)^2$ stets ein Quadrat, was uns auf die Frage reduziert, ob -3 ein Quadrat modulo 17 ist. Hierzu berechnen wir

$$(-3)^{\frac{17-1}{2}} \;=\; (-3)^8 \;=\; (((-3)^2)^2)^2 \;\equiv\; -1 \pmod{17}.$$

Das zeigt, daß -3 kein Quadrat in $\mathbf{F}_{17}$ ist, womit das Polynom $X^2 + X + 1$ in $\mathbf{Z}/17\mathbf{Z}$ *keine* Nullstellen besitzt. Mithin ist es irreduzibel in $\mathbf{F}_{17}[X]$.

Als Konsequenz erhalten wir, daß $X^2 + X + 1$ auch keine Nullstelle in $\mathbf{Z}$ besitzt[32]. Mit Bemerkung 1.4.35 sehen wir, daß $X^2 + X + 1$ sogar in $\mathbf{Q}$ keine Nullstelle besitzt.

Bemerkung 1.5.53. Wie in obigem Beispiel die Unlösbarkeit einer Gleichung zu zeigen, ist im Allgemeinen Schwieriger als die Lösbarkeit nachzuweisen: Für letzteres genügt es, eine Lösung anzugeben, für ersteres müssen *alle* in Frage kommenden Elemente als Lösungen ausgeschlossen werden, in obigem Beispiel alle Elemente aus $\mathbf{F}_{17}$. hier leistet uns das Kriterium aus Satz 1.5.48 sehr nützliche Dienste. Zusammen mit Bemerkung 1.4.35 erhalten wir einen Ansatz, um Existenz von Nullstellen sogar in $\mathbf{Q}$ auszuschließen.

Bemerkung 1.5.54. Eine wichtige weitere Erkenntnis aus Satz 1.5.48 ist, daß *die Hälfte* der Elemenge in $\mathbf{F}_p^\times$ Quadrate sind. Wenn wir also ein Element $a \in \mathbf{F}_p^\times$ zufällig[33] wählen, ist a mit Wahrscheinlichkeit $1/2$ ein Quadrat und mit Wahrscheinlichkeit $1/2$ kein Quadrat.

[32] Andernfalls wäre diese Nullstelle modulo 17 auch eine Nullstelle in $\mathbf{F}_{17}$.

[33] Bzgl. der Gleichverteilung.

Bemerkung 1.5.55. Die Relevanz von Satz 1.5.48 für das Faktorisierungsproblem besteht darin, daß der Satz es uns erlaubt, Quadratwurzeln in $\mathbf{F}_p$ zu bestimmen. In der Anwendung ist p dabei kein Primteiler der zu Faktorisierenden Zahl n, sondern kommt auf andere Weise ins Spiel.

Es bleibt die Frage, wie wir Quadratwurzeln in $\mathbf{F}_p$ bestimmen können. Sei allgemeiner

$$f \;=\; X^2 + aX + b \;\in\; \mathbf{F}_p[X] \tag{1.34}$$

ein quadratisches Polynom mit zwei verschiedene Nullstellen $\alpha, \beta \in \mathbf{F}_p$. Dann gilt $f = (X-\alpha)\cdot(X-\beta)$ und diese Faktorisierung ist eindeutig (vgl. Aufgabe 3 von Übungsblatt 6). Da $\alpha \neq \beta$ sind die beiden Polynome $X-\alpha$ und $X-\beta$ teilerfremd, weswegen wir dank des erweiterten Euklidischen Algorithmus zwei Polynome $g, h \in \mathbf{F}_p[X]$ finden, mit

$$g\cdot(X-\alpha) \;+\; h\cdot(X-\beta) \;=\; 1.$$

Dies nutzen wir wie im Fall von $\mathbf{Z}$ aus, um nachzuweisen, daß der Chinesische Restsatz gilt:

$$\begin{gathered}\mathbf{F}_p[X]/f\mathbf{F}_p[X] \;\to\; \mathbf{F}_p[X]/(X-\alpha)\mathbf{F}_p[X] \;\times\; \mathbf{F}_p[X]/(X-\beta)\mathbf{F}_p[X], \\ a + f\mathbf{F}_p[X] \;\mapsto\; (a+(X-\alpha)\mathbf{F}_p[X], a+(X-\beta)\mathbf{F}_p[X])\end{gathered} \tag{1.35}$$

ist ein Isomorphismus. Hierzu beobachten wir, daß beide seiten endlich von Kardinalität p^2 sind: Jede Restklasse in $\mathbf{F}_p[X]/f\mathbf{F}_p[X]$ besitzt dank Polynomdivision (Aufgabe 1 von Übungsblatt 6) einen eindeutig bestimmten Repräsentanten vom Grad < 2. Derer gibt es genau p^2 Stück. Analog gibt es rechterhand modulo $X-\alpha$ und modulo $X-\beta$ jeweils genau p Repräsentanten vom Grad < 1, letzteres sind gerade die Elemente in $\mathbf{F}_p$. Mit anderen Worten: Wir Rechnen auf der rechten Seite tatsächlich in $\mathbf{F}_p \times \mathbf{F}_p$:

Sei $a = q\cdot(X-\alpha) + r$ mit einem Rest $r \in \mathbf{F}_p$. Dann ergibt Auswerten beider Seiten bei α:

$$a(\alpha) \;=\; \underbrace{q(\alpha)\cdot(\alpha-\alpha)}_{=0} + \underbrace{r(\alpha)}_{=r} \;=\; r.$$

D. h. obiger Ringhomomorphismus läßt sich auch äquivalent in den Ringhomomorphismus

$$R:\; \mathbf{F}_p[X]/f\mathbf{F}_p[X] \;\to\; \mathbf{F}_p \times \mathbf{F}_p, \quad a + f\mathbf{F}_p[X] \;\mapsto\; (a(\alpha), a(\beta)) \tag{1.36}$$

umformulieren. Dabei ist $(a(\alpha), a(\beta))$ unabhängig von der Wahl des Repräsentanten a einer Restklasse, weil $f(\alpha) = 0$ und $f(\beta) = 0$. In dieser Form läßt sich die Isomorphie einfacher direkt nachweisen, ohne auf den erweierten Euklidischen Algorithmus zurückzugreifen: Weil beide Seiten die selbe Kardinalität haben, genügt es, zu zeigen, daß obiger Ringhomomorphismus injektiv ist.

Sei also $a + f\mathbf{F}_p[X]$ ein Element im Kern, mit anderen Worten: $a \in \mathbf{F}_p[X]$ ist ein Polynom, für welches $a(\alpha) = 0$ und $a(\beta) = 0$ gilt. Laut Aufgabe 4 von Übungsblatt 6 sind letztere Bedingungen äquivalent zu

$$(X-\alpha) \mid a \quad \text{und} \quad (X-\beta) \mid a,$$

was aufgrund der Teilerfremdheit von $(X-\alpha)$ und $(X-\beta)$ zur Folge hat (vgl. Aufgabe 3 selbigen Übungsblattes), daß

$$f \;=\; (X-\alpha)\cdot(X-\beta) \mid a.$$

Mithin ist a ein Vielfaches von f, womit a die 0 repräsentiert, was zu zeigen war.

Wir haben soeben gesehen, daß (1.35) bzw. (1.36) ein Isomorphismus ist. Dies können wir ausnutzen, um das quadratische Polynom f aus (1.34) wie folgt zu faktorisieren.

Algorithmus zur Faktorisierung quadratischer Polynome über $\mathbf{F}_p$. Es sei p eine ungerade Primzahl und $f \in \mathbf{F}_p[X]$ sei ein reduzibles quadratisches Polynom der Gestalt (1.34) mit zwei verschiedenen Nullstellen α und β in $\mathbf{F}_p$.

(i) Wähle $a = a_1X + a_0 \in \mathbf{F}_p[X]$ zufällig mit $a_1 \neq 0$, d. h. wähle zufällige Koeffizienten $a_0 \in \mathbf{F}_p$ und $a_1 \in \mathbf{F}_p^\times$ im Sinne der Gleichverteilung.

(ii) Prüfe, ob $a \mid f$. Falls ja, so ist $f = (X + a_0/a_1) \cdot f/(X + a_0/a_1)$ eine Faktorisierung von f. Andernfalls

(iii) Berechne $b \in \mathbf{F}_p[X]$ mit $b \equiv a^{\frac{p-1}{2}} \pmod f$.

(iv) Berechne den normierten $d := \mathrm{ggT}(b-1, f)$.

(v) Wenn $d = X - d_0$ mit $d_0 \in \mathbf{F}_p$, so ist $f/(X-d_0)$ ebenfalls normiert von Grad 1 und es gilt $f = (X-d_0) \cdot f/(X-d_0)$. Andernfalls springe zurück zu (i) und wiederhole den Prozeß.

Proposition 1.5.56. *Eine Iteration obigen Verfahrens bestimmt mit Wahrscheinlichkeit $\geq 1/2$ eine Faktorisierung von f.*

Beweis. Sei a wie in (i) zufällig gewählt. Dies entspricht gemäß Polynomdivision der zufälligen Wahl einer Restklasse $a + f\mathbf{F}_p[X]$ in $\mathbf{F}_p[X]/f\mathbf{F}_p[X]$.

In Schritt (ii) sind wir genau dann erfolgreich, wenn a ein Vielfaches von $X - \alpha$ oder $X - \beta$ im Polynomring $\mathbf{F}_p[X]$ ist. Da sich diese beiden Fälle gegenseitig ausschließen da $a \neq 0$ kein Vielfaches von f sein kann, genügt es aus Symmetriegründen, die Wahrscheinlichkeit zu bestimmen, daß a ein Vielfaches von $X - \alpha$ ist.

Hierzu beobachten wir, daß a genau dann ein Vielfaches von $X - \alpha$ ist, wenn $a_1 \neq 0$ und $\alpha = a_0/a_1$, d. h. $a_0 = \alpha a_1$. Damit ist a_0 durch α und a_1 eindeutig bestimmt und da es für $a_1 \neq 0$ genau $\#\mathbf{F}_p^\times = p - 1$ Fälle gibt, ist die Wahrscheinlichkeit, daß a ein Vielfaches von $X - \alpha$ ist, durch

$$\mathbf{P}(a \text{ ist Vielfaches von } \alpha) \;=\; \frac{p-1}{(p-1)\cdot p} \;=\; \frac{1}{p}$$

Insgesamt ergibt sich also

$$\mathbf{P}(a \text{ ist Vielfaches von } X-\alpha \text{ oder } X-\beta) \;=\; \frac{2}{p}$$

Wir sehen also, daß für großes p dieser Fall selten eintritt.

Wir nehmen nun an, daß a eine Einheit ist. Dann gilt für b aus Schritt (iii) im Sinne des Isomorphismus (1.36), daß

$$R(a) \;=\; (a(\alpha), a(\beta)) \;\in\; \mathbf{F}_p \times \mathbf{F}_p$$

Da a ein zufälliges Element aus $(\mathbf{F}_p[X]/f\mathbf{F}_p[X])^\times$ ist, sind $a(\alpha)$ und $a(\beta)$ zufällige unabhängige Elemente aus $\mathbf{F}_p^\times$. Gemäß Satz 1.5.48 gilt dann $a(\alpha)^{\frac{p-1}{2}} = \pm 1$ und jeder dieser

beiden Fälle besitzt die selbe Wahrscheinlichkeit $\frac{1}{2}$. Da entsprechendes für $a(\beta)$ gilt, welches unabhängig von $a(\alpha)$ variiert, erhalten wir wegen

$$R(b) \;=\; R(a^{\frac{p-1}{2}}) \;=\; R(a)^{\frac{p-1}{2}} \;=\; (a(\alpha)^{\frac{p-1}{2}}, a(\beta)^{\frac{p-1}{2}})$$

insgesamt mit $d = \mathrm{ggT}(b-1, f)$

$$\begin{aligned}\mathbf{P}(1 \neq d \neq f) &= \mathbf{P}\left(\left(a(\alpha)^{\frac{p-1}{2}} = 1 \wedge a(\beta)^{\frac{p-1}{2}} = -1\right) \vee \left(a(\alpha)^{\frac{p-1}{2}} = 1 \wedge a(\beta)^{\frac{p-1}{2}} = -1\right)\right) \\ &= \mathbf{P}(a(\alpha)^{\frac{p-1}{2}} = -a(\beta)^{\frac{p-1}{2}}) \\ &= \frac{1}{2}.\end{aligned}$$

Dies ist die Bedingte Erfolgswahrscheinlichkeit unter der Prämisse, daß wir in Schritt (ii) bzw. (i) noch keine Faktorisierung erraten haben.

Insgesamt erhalten wir also mit Wahrscheinlichkeit

$$\frac{2}{p} + (1 - \frac{2}{p}) \cdot \frac{1}{2} \;=\; \frac{2}{p} + \frac{p-1}{2p} \;=\; \frac{p+3}{2p} \;\geq\; \frac{1}{2},$$

eine Faktorisierung von f, was den Beweis abschließt. □

Bemerkung 1.5.57. Dieser Faktorisierungsalgorithmus läßt sich als Variante der Pollard'schen $p-1$-Methode in einem anderen Kontext interpretieren: Wir produzieren wie bei Pollards Algorithmus ein Element, welches 1 modulo einem Teiler und $\neq 1$ modulo einem anderen Teiler ist. Hierzu kommt uns zugute, daß die die Ordnung der Einheitengruppen modulo der irreduziblen Teiler bereits kennen: Sie ist $p-1$. Bei Pollards Methode müssen wir hier raten, da uns dort $\varphi(p) = p-1$ und $\varphi(q) = q-1$ unbekannt sind. Weiterhin nutzen wir im Vorliegenden Fall aus, daß die Einheitengruppe von $\mathbf{F}_p^\times$ zyklisch ist, was obiges Vorgehen letztendlich erst ermöglicht (vgl. Beweis von Satz 1.5.48).

Beispiel 1.5.58. Wir möchten $f = X^2 + X + 1 \in \mathbf{F}_7[X]$ faktorisieren.

Schritt (i): Wir wählen $a = 2X + 2$ zufällig.

Schritt (ii): Wir prüfen, daß $2X + 2 \nmid f$, z. B. weil $2X + 2 = 2(X + 1)$ und -1 damit Nullstelle von a, aber nicht von f ist. Das schließt Schritt (ii) ab.

Schritt (iii): Wir beobachten $\frac{p-1}{2} = 3$ und bestimmen einen Repäsentanten $b \in \mathbf{F}_7[X]$ mit

$$b \;\equiv\; a^3 \pmod{f}.$$

Zunächst berechnen wir hierzu mittels Polynomdivision in $\mathbf{F}_7[X]$:

$$a^2 \;=\; (2X+2)^2 \;=\; 4X^2 + X + 4 \;=\; 4f + (-3X),$$

sowie analog

$$a \cdot a^2 \;=\; (2X+2) \cdot (-3X) \;=\; X^2 + X \;=\; -1.$$

Damit schließen wir, daß $b = -1$ der Bedingung

$$b \;\equiv\; a^3 \pmod{f}$$

genügt.

Schritt (iv): Zuguterletzt erhalten wir in

$$\mathrm{ggT}(b-1, f) \;=\; \mathrm{ggT}(-2, f) \;=\; 1.$$

Schritt (v): Wir waren nicht erfolgreich und müssen einen weiteren Versuch starten.

Diesmal wählen wir $a = 5X + 3$ zufällig und prüfen, daß $5X + 3 \nmid f$, z. B. weil uns Division mit Rest

$$f \;=\; X^2 + X + 1 \;=\; (3X + 4)(5X + 3) + 3$$

beschert (wegen $3 \cdot 5 = 15 \equiv 1 \pmod 7$ ist 3 in $\mathbf{F}_7$ multiplikativ invers zu 5).

Nun bestimmen wir wie in der ersten Iteration

$$\begin{aligned}(5X+3)^2 &= 5^2(X+2)^2\\ &= 4(X^2+4X+4)\\ &= 4X^2+2X+2\\ &= 4f-2(X+1)\\ &\equiv -2(X+1) \pmod f.\end{aligned}$$

denn $5X + 3 = 5(X + 2)$. Weiterhin ergibt sich

$$\begin{aligned}(5X+3)\cdot(-2)(X+1) &= 4X^2+5X+1\\ &= 4(X^2+X+1)+(X-3)\\ &= 4f+(X-3)\\ &\equiv X-3 \pmod f.\end{aligned}$$

Wir erhalten $b = X - 3$.

Zur Bestimmgung von $\mathrm{ggT}(b - 1, f)$, berechnen wir

$$d \;=\; \mathrm{ggT}((X-3)-1, f) \;=\; \mathrm{ggT}(X-4, f) \;=\; X-2,$$

da

$$f \;=\; (X-4)\cdot(X-2),$$

womit wir eine Faktorisierung gefunden haben.

Bemerkung 1.5.59. Eine Erfolgswahrscheinlichkeit von $\geq \frac{1}{2}$ bedeutet nicht, daß im Allgemeinen zwei Iterationen ausreichen. Es bedeutet vielmehr, daß nach k Iterationen mit Wahrscheinlichkeit mindestens $1 - \frac{1}{2^k}$ eine Faktorisierung gefunden wurde. Da $\frac{1}{2^k} \to 0$ für $k \to \infty$, konvertiert die Erfolgswahrscheinlichkeit entsprechend gegen 1. Bereits nach $k = 10$ versuchen gilt $1 - \frac{1}{2^k} = 1 - \frac{1}{1024} = \frac{1023}{1024}$, d. h. die Wahrscheinlichkeit nach 10 versuchen *nicht* erfolgreich zu sein, ist kleiner als $\frac{1}{1024} < \frac{1}{1000}$. *Im Schnitt* müssen wir also in weniger als einem von 1000 Anwendungen des Verfahrens damit rechnen, nach 10 Iterationen noch keine Faktorisierung gefunden zu haben.

Bemerkung 1.5.60 (Erwartete Laufzeit)**.** Die zu erwartende Laufzeit kann wie folgt abgeschätzt werden. Wir schätzen die Erfolgswahrscheinlichkeit pro Iteration nach unten durch 1/2 ab und erhalten damit als untere Schranke für die zu erwartende Laufzeit

$$\begin{aligned}
&\sum_{k=1}^{\infty} \mathbf{P}(\text{Algorithmus terminiert in der } k\text{-ten Iteration}) \cdot k \\
= &\sum_{k=1}^{\infty} \mathbf{P}(\text{Nichterfolg nach } k-1 \text{ Iterationen}) \cdot \mathbf{P}(\text{Erfolg in der } k\text{-ten Iteration}) \cdot k \\
= &\sum_{k=1}^{\infty} \frac{1}{2^{k-1}} \cdot \frac{1}{2} \cdot k \\
= &\sum_{k=1}^{\infty} \frac{k}{2^k} \cdot k \\
= &\lim_{\ell \to \infty} \frac{2^{\ell+1} - (\ell+2)}{2^\ell} \\
= &\ 2,
\end{aligned}$$

denn induktiv verifiziert man leicht, daß

$$\sum_{k=1}^{\ell} \frac{k}{2^k} \ = \ \frac{2^{\ell+1} - (\ell+2)}{2^\ell}.$$

Wir halten fest:

Proposition 1.5.61 (Durchschnittliche Laufzeit)**.** *Die Durchschnittliche Anzahl an Iterationen, welche notwendig sind, um mit obigem Algorithmus ein quadratisches Polynom über* $\mathbf{F}_p$ *zu faktorisieren, ist* ≤ 2*.*

Bemerkung 1.5.62. Durch Betrachtung von $f = X^2 - a$ kann obiges Verfahren dazu benutzt werden, Quadratwurzeln in $\mathbf{F}_p$ zu bestimmen.

Bemerkung 1.5.63. Obiges Verfahren kann grundsätzlich dazu benutzt werden, die Nullstellen eines beliebigen *separablen* Polynoms $f \in \mathbf{F}_p[X]$ zu bestimmen. Dabei heißt f *separabel*, wenn $\mathrm{ggT}(f, f') = 1$ wobei

$$f' \ = \ n \cdot a_n X^{n-1} + (n-1) a_{n-1} X^{n-2} + \cdots + 1 \cdot a_1$$

die *formale Ableitung* von

$$f \ = \ a_n X^n + a_{n-1} X^{n-1} + \cdots + a_1 X + a_0$$

bezeichnet. Hierzu ist es zweckmäßig, jedoch genau genommen nicht notwendig, f durch $\mathrm{ggT}(f, X^p - X)$ zu ersetzen. Letzterer ggT kann als separables Substitut für ein beliebiges $f \in \mathbf{F}_p[X]$ genutzt werden, vgl. hierzu Aufgabe 4 von Übungsblatt 6 sowie Übungsblatt 9.

1.5.8 Quadratische Reziprozität

Wir haben in Satz 1.5.48 ein nützliches Kriterium gesehen, um Quadrate in $\mathbf{F}_p$ zu reduzieren, was wiederum Anwendungen auf die Existenz von Nullstellen von Polynomen hatte:

In der Notation mithilfe des Legendre-Symbols gilt für jede ungerade Primzahl p und $a \in \mathbf{Z}$, zu p teilerfremd:

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$$

und dieser Wert ist genau dann 1 (modulo p), wenn a ein Quadrat modulo p ist, andernfalls ist es -1.

Das Quadratische Reziprozitätsgesetz stellt eine explizite Beziehung zwischen $\left(\frac{q}{p}\right)$ und $\left(\frac{p}{q}\right)$ für zwei verschiedene Primzahlen her und erlaubt es uns deshalb, mithilfe der Multiplikativität des Legendre-Symbols, $\left(\frac{a}{p}\right)$ mithilfe einer Primfaktorzerlegung von a effizient zu bestimmen.

Satz 1.5.64 (Quadratisches Reziprozitätsgesetz)**.** *Es seien p, q ungerade Primzahlen. Dann gilt*

$$\left(\frac{q}{p}\right) \cdot \left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \tag{1.37}$$

Weiterhin gelten die beiden Zusätze:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & \textit{falls } p \equiv \pm 1 \pmod 8 \\ -1 & \textit{falls } p \equiv \pm 3 \pmod 8 \end{cases} \tag{1.38}$$

sowie

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & \textit{falls } p \equiv 1 \pmod 4 \\ -1 & \textit{falls } p \equiv 3 \pmod 4 \end{cases} \tag{1.39}$$

Gauß war der erste, dem ein Beweis gelang und wie bereits eingangs im kurzen Abriß über die Geschichte der Zahlentheorie erwähnt, nannte Gauß diesen Satz *Aureum Theorema*, d. h. *goldener Satz*. Es war zuvor bereits von Euler vermutet worden.

Bemerkung 1.5.65. Relation (1.37) besagt, daß $\left(\frac{p}{q}\right)$ den Wert von $\left(\frac{q}{p}\right)$ bestimmt und umgekehrt.

Dabei ist $\frac{p-1}{2}$ genau dann gerade, wenn $p \equiv 1 \pmod 4$. Im Fall $p \equiv 3 \pmod 4$ ist es ungerade. Damit nimmt $(-1)^{\frac{p-1}{2}\frac{q-1}{2}}$ genau dann den Wert -1 an, wenn $p \equiv q \equiv 3 \pmod 4$. In allen anderen Fällen nimmt dieser Ausdruck den Wert 1 an.

Bemerkung 1.5.66. Eine weitere Darstellung der Identität (1.37) ist

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{p}{q}\right).$$

Der Zusatz 1.39 beschert uns zusammen mit der Multiplikativität des Legendre-Symbols

$$\left(\frac{q}{p}\right) = \left(\frac{(-1)^{\frac{p-1}{2}}}{q}\right)\left(\frac{p}{q}\right),$$

was uns die äquivalente Formulierung

$$\left(\frac{q}{p}\right) \;=\; \left(\frac{p^*}{q}\right),$$

mit

$$p^* \;:=\; (-1)^{\frac{p-1}{2}} \cdot p$$

beschert.

Beispiel 1.5.67. Wir möchten entscheiden, ob $a = 35$ ein Quadrat modulo $p = 257$ ist.

Zunächst beobachten wir, daß $a = 35 = 5 \cdot 7$. Damit ergibt sich:

$$\begin{aligned}
\left(\frac{35}{257}\right) &= \left(\frac{5\cdot 7}{257}\right) \\
&= \left(\frac{5}{257}\right)\cdot\left(\frac{7}{257}\right) && \text{(Multiplikativität)} \\
&= (-1)^{\frac{5-1}{2}\frac{257-1}{2}}\left(\frac{257}{5}\right)\cdot(-1)^{\frac{7-1}{2}\frac{257-1}{2}}\left(\frac{257}{7}\right) && \text{(Quadratische Reziprozität)} \\
&= (-1)^{4\cdot 128}\left(\frac{257}{5}\right)\cdot(-1)^{3\cdot 128}\left(\frac{257}{7}\right) \\
&= \left(\frac{257}{5}\right)\cdot\left(\frac{257}{7}\right).
\end{aligned}$$

Die Werte dieser beiden Legendre-Symbole hängen nur von der Restklasse modulo 257 ab, womit wir wegen $257 \equiv 2 \pmod 5$ und $257 \equiv 5 \pmod 7$ wie folgt fortfahren:

$$\begin{aligned}
\left(\frac{35}{257}\right) &= \left(\frac{257}{5}\right)\cdot\left(\frac{257}{7}\right) \\
&= \left(\frac{2}{5}\right)\cdot\left(\frac{5}{7}\right) \\
&= (-1)^{\frac{5^2-1}{2}}\cdot\left(\frac{5}{7}\right) && \text{(Zusatz (1.38))} \\
&= (-1)\cdot(-1)^{\frac{5-1}{2}\frac{7-1}{2}}\left(\frac{7}{5}\right) && \text{(Quadratische Reziprozität)} \\
&= (-1)\cdot\left(\frac{2}{5}\right) && \text{(da } 7 \equiv 2 \pmod 5\text{)} \\
&= (-1)\cdot(-1) && \text{(wieder Zusatz (1.38))} \\
&= 1.
\end{aligned}$$

Wir schließen also, daß 35 ein Quadrat in $\mathbf{F}_{257}$ ist.

Wir schicken dem Beweis von Satz 1.5.64 folgendes Lemma voraus, wofür wir zunächst etwas Terminologie benötigen. Für eine ungerade Primzahl p nennen wir eine Teilmenge $U = \{u_1, \ldots, u_r\} \subseteq \mathbf{Z}$ eine *Gauß'sche Menge*, wenn U ein Repräsentantensystem für die Elemente in $\mathbf{F}_p^\times/\{\pm 1\}$ ist. Mit anderen Worten: Wir betrachten auf $\mathbf{F}_p^\times$ die Äquivalenzrelation $x \sim y \;\Leftrightarrow\; x = \pm y$. Bezüglich dieser zerfällt $\mathbf{F}_p^\times$ in zweielementige Äquivalenzklassen

der Gestalt $\{x, -x\}$ auf und U ist ein Repräsentantensystem für diese Partition von $\mathbf{F}_p^\times$: Jedes $x \in \mathbf{F}_p^\times$ besitzt dann einen eindeutigen Repräsentanten der Form $\pm u_i$ für ein eindeutig bestimmtes $1 \leq i \leq r$. Mit anderen Worten: es gilt $x = u_i + p\mathbf{Z}$ oder $x = -u_i + p\mathbf{Z}$ für genau ein $1 \leq i \leq r$. Da es in $\mathbf{F}_p^\times$ bezüglich dieser Relation in genau $\frac{p-1}{2}$ Äquivalenzklassen zerfällt (jede Äquivalenzklasse enthält genau zwei Elemente!), gilt $r = \frac{p-1}{2}$.

Beispiel 1.5.68. Im Fall $p = 3$ gibt es wegen $\mathbf{F}_3^\times = \{\pm 1\}$ genau zwei Gaußsche Mengen: $U = \{1\}$ aund $U = \{-1\}$ sind beides Gaußsche Mengen.

Im Fall $p = 7$ ist beispielsweise $U = \{1, 3, 5\}$ eine Gaußsche Menge. Hier gelten exemplarisch $4 \equiv -3 \pmod 7$ und $6 \equiv -1 \pmod 7$.

Bemerkung 1.5.69. Die Menge $U = \{1, 2, \ldots, \frac{p-1}{2}\}$ ist für jede ungerade Primzahl p eine Gaußsche Menge.

Gauß' Schlüssel zum Beweis des Quadratischen Reziprozitätsgesetzes ist folgende Verallgemeinerung der Formel (1.39):

Lemma 1.5.70 (Gauß)**.** *Es sei p eine ungerade Primzahl und $U = \{u_1, \ldots, u_r\} \subseteq \mathbf{Z}$ sei eine Gaußsche Menge. Dann gilt für jedes zu p teilerfremde $a \in \mathbf{Z}$: Wenn $\varepsilon_1, \ldots, \varepsilon_r \in \{\pm 1\}$ die eindeutigen Vorzeichen mit jeweils*

$$a \cdot u_i \equiv \varepsilon_i u_j \pmod p \tag{1.40}$$

für alle $1 \leq i \leq r$ und das entsprechende $1 \leq j \leq r$ sind[34]*, dann gilt*

$$\left(\frac{a}{p}\right) = \varepsilon_1 \cdot \varepsilon_2 \cdots \varepsilon_r. \tag{1.41}$$

Beweis. Wir beobachten zunächst, daß für jedes $1 \leq i \leq r$ der Index j ist durch die Relation (1.40) eindeutig bestimmt und Anwendung von $(-)^{-1}$ auf die äquivalente Formulierung

$$a \equiv \varepsilon_i u_i^{-1} u_j \pmod p, \tag{1.42}$$

zeigt, daß

$$a^{-1} \equiv \varepsilon_i u_i u_j^{-1} \pmod p,$$

womit sich

$$u_j a^{-1} \equiv \varepsilon_i u_i \pmod p,$$

ergibt. Letztere Relation zeigt, daß umgekehrt zu jedem $1 \leq j \leq r$ ein eindeutiger Index i existiert[35]

Das zeigt, daß die durch die Relation (1.40) induzierte Zuordnung $i \mapsto j$ eine Bijektion $\{1, 2, \ldots, r\} \to \{1, 2, \ldots, r\}$ ist.

Das Produkt sämtlicher Relationen (1.42) für $1 \leq i \leq r$ beschert uns daher einerseits die Kongruenz

$$\begin{aligned} a^{\frac{p-1}{2}} &\equiv \varepsilon_1\varepsilon_2 \cdots \varepsilon_r \cdot u_1 \cdot u_2 \cdots u_r \cdot u_1^{-1} \cdot u_2^{-1} \cdots u_r^{-1} \\ &\equiv \varepsilon_1\varepsilon_2 \cdots \varepsilon_r \pmod p. \end{aligned}$$

[34]Wir wenden hier die Eigenschaft von U, eine Gaußsche Menge zu sein an, um $a \cdot u_i$ als $\pm x$ mit $x \in U$ darzustellen. Das Vorzeichen $\pm$ bestimmt ε_i und x bestimmt den Index j.

[35]Hier wenden wir die Eigenschaft von U, eine Gaußsche Menge zu sein darauf an, um $u_j a^{-1}$ als $\pm x$ mit $x \in U$ darzustellen.

Andererseits gilt per Definitionem

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p},$$

womit die Behauptung folgt[36]. □

Beweis der Zusätze in Satz 1.5.64. Relation (1.39) ist eine unmittelbare Konsequenz der Definition des Legendre-Symbols und bedarf keiner weiteren Diskussion.

Um (1.38) einzusehen, wählen wir $U = \{1, 2, \ldots, \frac{p-1}{2}\}$ als Gaußsche Menge und betrachten den Fall $a = 2$ in Lemma 1.5.70. Hier ergibt sich für $1 \leq i \leq \frac{p-1}{2}$, daß $u_i = i$ und damit

$$a \cdot u_i = 2 \cdot i \quad \begin{cases} \leq \frac{p-1}{2}, & \text{wenn } i \leq \frac{p-1}{4} \\ > \frac{p-1}{2}, & \text{wenn } i \geq \frac{p+1}{4}. \end{cases}$$

Das zeigt,

$$\varepsilon_i = -1 \quad \Leftrightarrow \quad i \geq \frac{p+1}{4},$$

und $\varepsilon_i = 1$ sonst. Zusammenfassend ergibt sich damit mit Lemma 1.5.70, daß

$$\left(\frac{2}{p}\right) = (-1)^{\#\{1 \leq i \leq r | i \geq \frac{p-1}{4}\}} = \begin{cases} 1, & \text{wenn } \#\{\frac{p+1}{4} \leq i \leq \frac{p-1}{2}\} \text{ gerade,} \\ -1, & \text{wenn } \#\{\frac{p+1}{4} \leq i \leq \frac{p-1}{2}\} \text{ ungerade.} \end{cases}$$

Eine genaue Inspektion zeigt, daß die Kardinalität $\#\{\frac{p+1}{4} \leq i \leq \frac{p-1}{2}\}$ genau dann gerade ist, wenn $p \equiv \pm 1 \pmod 8$, was die Behauptung zeigt (vgl. Übungsblatt). □

Beweis von Satz 1.5.64. Um schlußendlich Relation (1.37) zu beweisen, gehen wir ähnlich vor wie im Beweis von (1.38). Seien p, q zwei verschiedene ungerade Primzahlen. Wir wählen $U_p := \{1, 2, \ldots, \frac{p-1}{2}\}$ und analog $U_q = \{1, 2, \ldots, \frac{q-1}{2}\}$ als Gaußsche Mengen.

Im Fall $a = q$ erhalten wir hier

$$a \cdot u_i = q \cdot i \equiv \varepsilon_i u \pmod{p}$$

mit $\varepsilon_i = \pm 1$ und $1 \leq u \leq \frac{p-1}{2}$, denn letztere Bedingung ist äquivalent zu $u \in U_p$. Diese Relation übersetzt sich wiederum zu

$$q \cdot i = \varepsilon_i u + y \cdot p$$

für ein geeignetes $y \in \mathbf{Z}$. Dabei sind ε_i, y_i und u sämtlich durch i eindeutig bestimmt.

Insbesondere ist die Bedingung $\varepsilon_i = -1$ äquivalent zu

$$q \cdot i = -u + y \cdot p$$

beziehungsweise

$$q \cdot i + u = y \cdot p$$

[36] Wichtig: $\varepsilon_1, \ldots, \varepsilon_r$ nehmen nur Werte in ± 1 an, weswegen (1.41) einer Gleichheit und nicht nur eine Kongruenz modulo p ist!

für ein $y \in \mathbf{Z}$. Da die linke Seite stets positiv ist, gilt $y > 0$ und Einsetzen von $i = \frac{p-1}{2}$ und $u = \frac{p-1}{2}$ beschert uns die obere Schranke

$$py \;\leq\; q \cdot \frac{p-1}{2} \;+\; \frac{p-1}{2} \;=\; \frac{(q+1)\cdot(p-1)}{2},$$

beziehungsweise

$$y \;\leq\; \frac{(q+1)\cdot(p-1)}{2p} \;<\; \frac{q+1}{2}.$$

Die Anzahl der Indizes $1 \leq i \leq \frac{p-1}{2}$ mit $\varepsilon_i = -1$ ist also die Anzahl N_p der Paare (i, y), welche den drei Bedingungen

$$1 \leq i \leq \frac{p-1}{2}, \quad 1 \leq y \leq \frac{q-1}{2}, \quad 1 \leq py - qi \leq \frac{p-1}{2},$$

genügt, denn $u = py - qi$.

Gemäß Lemma 1.5.70 gilt dann

$$\left(\frac{q}{p}\right) \;=\; (-1)^{N_p}.$$

Aus Symmetriegründen ergibt sich analog

$$\left(\frac{p}{q}\right) \;=\; (-1)^{N_q}$$

mit N_q die Anzahl der Paare (i, y), für welche

$$1 \leq i \leq \frac{q-1}{2}, \quad 1 \leq y \leq \frac{p-1}{2}, \quad 1 \leq qy - pi \leq \frac{q-1}{2}.$$

Zusammenfassend gilt damit

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) \;=\; (-1)^{N_p+N_q}.$$

Es bleibt also zu zeigen, daß $N_p + N_q \equiv \frac{p-1}{2}\frac{q-1}{2} \pmod 2$ gilt.

Hierzu bemerken wir zunächst, daß $N_p + N_q$ die Anzahl der Paare $(x, y) \in \mathbf{Z}^2$ mit

$$1 \leq x \leq \frac{p-1}{2}, \quad 1 \leq y \leq \frac{q-1}{2}, \quad -\frac{p-1}{2} \leq qy - px \leq \frac{q-1}{2}$$

ist, denn $px - qy$ nimmt aufgrund der ersten beiden Ungleichungen und der Teilerfremdheit von p und q niemals den Wert 0 an.

Bezeichne nun $R_p \subseteq \mathbf{Z}^2$ bzw. $R_q \subseteq \mathbf{Z}^2$ jeweils die Mengen derjenigen Paare (x, y), für welche

$$1 \leq x \leq \frac{p-1}{2}, \quad 1 \leq y \leq \frac{q-1}{2}, \quad -\frac{p-1}{2} > qy - px,$$

bzw.

$$1 \leq x \leq \frac{p-1}{2}, \quad 1 \leq y \leq \frac{q-1}{2}, \quad qy - px > \frac{q-1}{2},$$

gelten. Die Abbildung

$$R_p \to R_q, \quad (x,y) \mapsto \left(\frac{p+1}{2} - x,\ \frac{q+1}{2} - y\right)$$

ist eine Bijektion (die selbe Rechenvorschrift rechterhand definiert die inverse Abbildung), sodaß ihre Kardinalitäten

$$M_p \ := \ \#R_p, \quad M_q \ := \ \#R_q$$

übereinstimmen. Mithin ist $M_p + M_q = 2M_p$ einerseits eine gerade Zahl.

Andererseits ist $N_p + N_q + M_p + M_q$ die Anzahl der Paare (x,y), welche den beiden Bedingungen

$$1 \leq x \leq \frac{p-1}{2}, \quad 1 \leq y \leq \frac{q-1}{2},$$

genügen, sodaß

$$N_p + N_q + M_p + M_q \ = \ \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Zusammenfassend ergibt sich damit die gesuchte Kongruenz

$$N_p + N_q \ \equiv \ N_p + N_q + M_p + M_q \ \equiv \ \frac{p-1}{2} \cdot \frac{q-1}{2} \pmod 2,$$

was zu zeigen war. □

Beispiel 1.5.71. Es sei $0 \neq d \in \mathbf{Z}$ gegeben. Wir betrachten das Problem, welche Zahlen $n \in \mathbf{Z}$ von der Form

$$n \ = \ x^2 + dy^2, \quad x,y \in \mathbf{Z}, \tag{1.43}$$

sind. Hier wird sich das quadratische Reziprozitätsgesetz als sehr hilfreich (bzw. sogar äquivalent) zur Beantwortung dieses Problems herausstellen.

Hierzu beobachten wir zunächst, daß wenn

$$n_1 \ = \ x_1^2 + dy_1^2, \quad \text{und} \quad n_2 \ = \ x_2^2 + dy_2^2,$$

dann gilt wegen

$$n_i \ = \ \det \begin{pmatrix} x_1 & -dy_1 \\ y_1 & x_1 \end{pmatrix},$$

daß

$$\begin{aligned} n_1 \cdot n_2 \ &= \ \det \begin{pmatrix} x_1 & -dy_1 \\ y_1 & x_1 \end{pmatrix} \cdot \det \begin{pmatrix} x_2 & -dy_2 \\ y_2 & x_2 \end{pmatrix} \\ &= \ \det \begin{pmatrix} x_1 & -dy_1 \\ y_1 & x_1 \end{pmatrix} \cdot \begin{pmatrix} x_2 & -dy_2 \\ y_2 & x_2 \end{pmatrix} \\ &= \ \det \begin{pmatrix} x_1x_2 - dy_1x_7 & -d(x_1y_2 + y_1x_2) \\ x_1y_2 + y_1x_2 & x_1x_2 - dy_1y_2 \end{pmatrix} \\ &= \ (x_1x_2 - dy_1x_7)^2 \ + \ d(x_1y_2 + y_1x_2)^2. \end{aligned}$$

Insbesondere ist also das Produkt $n_1 \cdot n_2$ ebenfalls von der Form (1.43). Wir schließen, daß die Menge

$$\mathscr{L}_d \;:=\; \{0 \neq n \in \mathbf{Z} \mid \exists x, y \in \mathbf{Z} : n = x^2 + dy^2\}$$

der von Null verschiedenen ganzen Zahlen der Form (1.43) multiplikativ abgeschlossen ist. Wegegen $1 = 1^2 + d \cdot 0^2$ gilt $1 \in \mathscr{L}_d$, womit $\mathscr{L}_d$ ein Monoid[37] ist.

Allgemeiner ist wegen $n^2 = n^2 + d \cdot 0^2$ jedes von Null verschiedene Quadrat in $\mathscr{L}_d$ enthalten, womit sich mit Blick auf die Primfaktorzerlegung die Frage stellt, welche *Primzahlen* p von der Form (1.43) sind. Wenn $p = x^2 + dy^2$, dann ist p gewiß ein Teiler von $x^2 + dy^2$, d. h. wir erhalten die zunächst schwächere Fragestellung, wann

$$x^2 + dy^2 \;=\; 0 \tag{1.44}$$

in $\mathbf{F}_p$ nicht-trivial lösbar[38] ist. Da es im Fall $p \mid d$ offensichtliche nicht-triviale Lösungen gibt, z. B. $x = 0$ und $y = 1$, gehen wir im Folgenden von $p \nmid d$ aus. Dann impliziert $x \neq 0$ auch $y \neq 0$ und umgekehrt, weswegen (1.44) (unter der Hypothese $p \nmid d$!) äquivalent ist

$$\left(\frac{x}{y}\right)^2 \;=\; -d$$

in $\mathbf{F}_p$. Mit anderen Worten: Wenn $p \nmid d$, dann ist (1.44) genau dann nicht-trivial Lösbar, wenn $-d$ ein Quadrat in $\mathbf{F}_p^\times$ ist. Mithilfe des Quadratischen Reziprozitätsgesetzes läßt sich

$$\left(\frac{-d}{p}\right) \;=\; \left(\frac{-1}{p}\right) \cdot \left(\frac{d}{p}\right) \;=\; (-1)^{\frac{p-1}{2}} \cdot \left(\frac{d}{p}\right)$$

auswerten, wobei wir in dieser Rechnung bereits den Zusatz (1.39) des Reziprozitätsgesetz angewandt haben.

Im Fall $d = 1$ gilt stets $\left(\frac{d}{p}\right) = \left(\frac{1}{p}\right) = 1$, sodaß wir hier das Kongruenzkriterium

$$\left(\frac{-d}{p}\right) \;=\; (-1)^{\frac{p-1}{2}} \;=\; \begin{cases} 1, & \text{wenn } p \equiv 1 \pmod 4 \\ -1, & \text{wenn } p \equiv 3 \pmod 4 \end{cases}$$

erhalten. In diesem Fall ging lediglich der zweite Zusatz (1.39) des Reziprozitätsgesetzes ein.

Konkrete Interpretation: Für eine ungerade Primzahl p existieren genau dann zu p teilerfremde $x, y \in \mathbf{Z}$ mit $p \mid x^2 + y^2$, wenn $p \equiv 1 \pmod 4$ ist.

---

[37] D. h. eine Halbgruppe mit Neutralelement.

[38] D. h. daß wir Lösungen $(x, y) \neq (0, 0)$ suchen.

Exemplarisch führen wir dies im Fall $d = 3$ aus, womit wir für $p > 3$

$$\begin{aligned}\left(\frac{-3}{p}\right) &= (-1)^{\frac{p-1}{2}} \cdot \left(\frac{3}{p}\right) \\ &= (-1)^{\frac{p-1}{2}} \cdot \left(\frac{d}{p}\right) \\ &= (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}\frac{3-1}{2}} \left(\frac{p}{3}\right) \\ &= (-1)^{\frac{p-1}{2}} \cdot (-1)^{\frac{p-1}{2}} \left(\frac{p}{3}\right) \\ &= \left(\frac{p}{3}\right) \\ &= \begin{cases} 1, & \text{wenn } p \equiv 1 \pmod 3 \\ -1, & \text{wenn } p \equiv -1 \pmod 3 \end{cases}\end{aligned}$$

Hier war tatsächlich eine Anwendung von (1.37) erforderlich.

Konkrete Interpretation: Für eine Primzahl $p \geq 5$ existieren genau dann zu p teilerfremde $x, y \in \mathbf{Z}$ mit $p \mid x^2 + 3y^2$, wenn $p \equiv 1 \pmod 3$ ist.

Beispiel 1.5.72. Eine nützliche Anwendung des vorigen Beispiels (1.5.71) und damit der quadratischen Reziprozität ist die Existenz unendlich vieler Primzahlen, welche gewissen Kongruenzbedingungen genügen.

Wollen wir die Existenz unendlich viele Primzahlen $p \equiv 1 \pmod 3$ finden, so müssen wir dank obiger konkreter Interpretation lediglich zeigen, daß die Menge der Primteiler, welche in einen ganzen Zahlen n der Form $n = x^2 + 3y^2$ auftreten unendlich ist. Dies ist nicht allzu schwer: Wir halten $x = 1$ fest und varrieren y über die Menge aller natürlichen Zahlen. Seien $p_1, \ldots, p_r$ endlich viele Primteiler von Zahlen $n_1, n_2, \ldots, n_r$ jeweils der Gestalt $n_i = 1 + 3y_i^2$. Wenn q ein Teiler von $n := 1 + 3(p_1 \cdot p_2 \cdots p_r)^2$ ist, dann ist n wegen

$$n \equiv 1 \pmod{p_i}$$

für alle $1 \leq i \leq r$ zu jedem p_i teilerfremd, weswegen wir dank $n > 1$ in n einen weiteren Primteiler q finden (vgl. Lemma 1.4.28), welcher von $p_1, \ldots, p_r$ verschieden ist.

Wir halten fest: Es existieren unendlich viele Primzahlen p mit $p \equiv 1 \pmod 3$. Analog ergibt sich, daß unendlich viele Primzahlen p mit $p \equiv 1 \pmod 4$ existieren.

Bemerkung 1.5.73. Der *Dirichletsche Primzahlsatz* besagt, daß für jedes gegebene $n \geq 1$ und jedes zu n teilerfremdes $a \in \mathbf{Z}$ unendlich viele Primzahlen p existieren, welche der Kongruenz $p \equiv a \pmod n$ genügen. Der Beweis dieses Satzes benötigt jedoch analytische Hilfsmittel, auf die wir hier nicht zurückgreifen werden. Mithilfe des quadratischen Reziprozitätsgesetzes lassen sich mit der Methode aus den Beispielen 1.5.71 und 1.5.72 unendlich viele Fälle des Dirichletschen Primzahlsatzes algebraisch beweisen, jedoch nicht alle.

1.5.9 Faktorisierungsverfahren II: Das quadratische Sieb

Mit unserem Wissen über quadratische Reste kehren wir zum Faktorisierungsproblem zurück. Wir hatten gelernt, daß die Faktorisierung einer natürlichen Zahl $n = p \cdot q$ äqui-

valent zum Produzieren einer nicht-trivialen Kongruenz

$$x^2 \equiv y^2 \pmod{n} \tag{1.45}$$

zweier Quadrate modulo n ist. Letztere Kongruenz hatten wir mit (1.31) bezeichnet und die möglichen Konsequenzen diskutiert. Offen ist weiterhin, wie wir derartige x und y möglichst effizient bestimmen können.

Dabei hat sich folgender Ansatz als nützlich erwiesen. Wir wählen $x_1, \ldots, x_s \in \mathbf{Z}$ derart, daß wir die Reste $r_1, \ldots, r_s$ mit

$$x_i^2 \equiv r_i \pmod{n}$$

in Primfaktoren zerlegen können und die auftretenden Primfaktoren durch eine Schranke B beschränkt sind. Sind nun $p_1, \ldots, p_u$ sämtliche Primzahlen $\leq B$ und schreiben wir

$$r_i = (-1)^{e_{0i}} \cdot p_1^{e_{1i}} \cdot p_2^{e_{2i}} \cdots p_u^{e_{ui}},$$

so hoffen wir, daß wir genügend Reste $r_1, \ldots, r_s$ an der Hand haben, daß das lineare Gleichungssystem

$$E \cdot y = 0 \tag{1.46}$$

mit

$$E = \big(e_{ki} \pmod 2 \big)_{ki} \in \mathbf{F}_2^{u+1 \times s}$$

in $\mathbf{F}_2^s$ nicht-trivial lösbar ist. Gemäß Linearer Algebra ist das immer der Fall, wenn es mehr Unbestimmte als Gleichungen gibt, d. h. wenn $s > u + 1$.

Ist $y = (y_1, \ldots, y_s)^t \in \mathbf{F}_2^s$ eine nicht-triviale Lösung, dann gilt (wenn wir die Einträge $y_1 \ldots, y_s$ als Elemente $0, 1 \in \mathbf{N}$ auffassen):

$$\begin{aligned} r_1^{y_1} \cdot r_2^{y_2} \cdots r_s^{y_s} &= \prod_{i=1}^{s} (-1)^{e_{0i} y_i} \cdot p_1^{e_{1i} y_i} \cdot p_2^{e_{2i} y_i} \cdots p_u^{e_{ui} y_i} \\ &= (-1)^{\sum_{i=1}^s e_{0i} y_i} \cdot p_1^{\sum_{i=1}^s e_{1i} y_i} \cdot p_2^{\sum_{i=1}^s e_{2i} y_i} \cdots p_u^{\sum_{i=1}^s e_{ui} y_i}. \end{aligned}$$

Da y eine Lösung von (1.46) ist, gilt für jeden Exponenten in der letzten Gleichung

$$\sum_{i=1}^{s} e_{ki} y_i \equiv 0 \pmod 2,$$

was dank äquivalent dazu ist, daß die ganze Zahl

$$z := r_1^{y_1} \cdot r_2^{y_2} \cdots r_s^{y_s}$$

ein Quadrat in $\mathbf{Z}$ ist (vgl. Korollar 1.4.33). Halbieren wir die diese Exponenten, erhalten wir mit

$$y := (-1)^{\frac{1}{2}\sum_{i=1}^s e_{0i} y_i} \cdot p_1^{\frac{1}{2}\sum_{i=1}^s e_{1i} y_i} \cdot p_2^{\frac{1}{2}\sum_{i=1}^s e_{2i} y_i} \cdots p_u^{\frac{1}{2}\sum_{i=1}^s e_{ui} y_i}$$

einerseits eine Quadratwurzel von z.

Andererseits gilt

$$\begin{aligned} \left(x_1^{y_1} \cdot x_2^{y_2} \cdots x_s^{y_s}\right)^2 &= x_1^{2y_1} \cdot x_2^{2y_2} \cdots x_s^{2y_s} \\ &\equiv r_1^{y_1} \cdot r_2^{y_2} \cdots r_s^{y_s} \\ &\equiv z \pmod{n}. \end{aligned}$$

Damit ist

$$x \;:=\; x_1^{y_1} \cdot x_2^{y_2} \cdots x_s^{y_s}$$

ebenfalls eine Quadratwurzel von z modulo n, womit wir ein Paar x und y gefunden haben, welches der Kongruenz (1.45) genügt.

Wir wissen bereits, daß in der Hälfte der Fälle, eine nicht-triviale Kongruenz vorliegt, in welchen wir eine Faktorisierung von n erhalten. Sofern der Lösungsraum des linearen Gleichungssystems (1.46) Dimension > 1 hat, erhalten wir für jedes Element einer Basis dieses Lösungsraumes ein weiteres Paar und damit einen weiteren Versuch. Ist der Lösungsraum konkret von Dimension d und gehen wir davon aus, daß die resultierenden x und y als Quadrate zufällig verteilt sind (was sie real jedoch nicht sind!), dann erhalten wir d unabhängige zufällige Paare, was uns eine Erfolgswahrscheinlichkeit von $1 - \frac{1}{2^d}$ beschert.

Wir haben in obigem Ansatz das Faktorisierungsproblem in zwei Probleme geteilt:

(i) Bestimme ausreichend viele *Relationen* der Form

$$x_i^2 \;\equiv\; (-1)^{e_{0i}} \cdot p_1^{e_{1i}} \cdot p_2^{e_{2i}} \cdots p_u^{e_{ui}} \pmod{n}. \tag{1.47}$$

(ii) Löse das lineare Gleichungssystem (1.46).

Aufgrund der Relationen und dem Zusammenhang zur Linearen Algebra in Schritt (ii) wird die konkret verwandte Menge $\{-1, p_1, \ldots, p_u\}$ von Primzahlen zusammen mit $p_0 = -1$ als *Faktorbasis* bezeichnet.

Anpassen der Faktorbasis

Relationen der Art lassen sich probabilistisch finden, was für große Moduli n jedoch noch Verbesserungsbedarf erlaubt: Anstatt ein zufälliges x_i modulo n zu quadrieren und zu hoffen, daß der resultierende quadratische Rest in kleine Primfaktoren zerfällt und die entsprechende Primfaktorzerlegung zu bestimmen, stellen wir das Problem auf den Kopf und fragen: Welche x_i führen zu durch p_j teilbare quadratische Reste?

Hierzu fixieren wir zunächst[39] $d := \lfloor \sqrt{n} \rfloor$ und betrachten das quadratische Polynom

$$f \;:=\; (X - d)^2 - n \;=\; X^2 - 2dX + d^2 - n.$$

Da d^2 die größte Quadratzahl $\leq n$ ist, gilt $|d^2 - n| < 2d + 1$, sodaß $|d^2 - n|$ im Vergleich zu n klein ist. Insbesondere ist der Absolutbetrag von $f(x)$ für x nah bei 0 durch $2d \leq 2\sqrt{n}$ beschränkt ($d^2 - n$ ist negativ!).

Nun gilt einerseits für $x \in \mathbf{Z}$

$$f(x) \;=\; (x - d)^2 - n \;\equiv\; (x - d)^2 \pmod{n}$$

sodaß wir mit $x - d + n\mathbf{Z}$ eine Quadratwurzel von $f(x) \pmod{n}$ an der Hand haben. Andererseits dürfen wir hoffen, daß $f(x)$ in kleine Primfaktoren zerfällt, da sein Absolutbetrag durch $2\sqrt{n}$ beschränkt ist, sodaß wir auf diese Weise letztendlich Relationen der Form (1.47) erhalten. Wir möchten jedoch nicht alle möglichen kleinen x in f einsetzen und

[39] d. h. d ist die größte natürliche Zahl $\leq \sqrt{n}$.

danach $f(x)$ faktorisieren. Umgekehrt streben wir an, diejenigen x, welche zu Relationen führen, im Vorfeld zu identifizieren.

Für eine beliebige ungerade Primzahl p gilt

$$p \mid f(x) \quad \Leftrightarrow \quad f(x) \equiv 0 \pmod{p}.$$

Daher gehen wir wie folgt vor: Wir bestimmen einen Repräsentanten $x_j \pmod{p_j}$ einer Nullstellen f in $\mathbf{F}_{p_j}$ für sämtliche ungerade Primzahlen $p_2, \ldots, p_u$ welche kleiner als unsere Schranke B sind. Dies bewerkstelligen wir mit dem Algorithmus zur Faktorisierung quadratischer Polynome über $\mathbf{F}_p$ aus Abschnitt 1.5.7.

Damit wissen wir: Jedes $x \in \mathbf{Z}$ für welches p_j in der Relation (1.47) auftritt, genügt einer der beiden Kongruenzen

$$x \equiv x_j \pmod{p_j} \quad \text{oder} \quad x \equiv 2d - x_j \pmod{p_j}, \tag{1.48}$$

denn f besitzt in $\mathbf{F}_p$ nur die beiden durch x_j bzw. $2d - x_j$ repräsentierten Nullstellen[40].

Wir halten fest: Besitzt f keine Nullstelle in $\mathbf{F}_{p_j}$, d. h. ist n kein quadratischer Rest modulo p_j, so tritt p_j in *keiner* Relation (1.47) auf. Daher streichen wir im ersten Schritt sämtliche (ungerade) p_j aus unserer Faktorbasis, für welche die notwendige und hinreichende Bedingung

$$\left(\frac{n}{p_j}\right) = 1$$

verletzt ist. Formal betrachten wir also die Faktorbasis

$$F(B) := \{\pm 1\} \cup \{2\} \cup \{3 \leq p \leq B \mid p \text{ prim und } \left(\frac{n}{p}\right) = 1\}.$$

Diese nummerieren wir wieder durchgehend von p_0 bis p_u.

Bei der Bestimmung von $F(B)$ hilft uns das Sieb des Eratosthenes zusammen mit dem Quadratischen Reziprozitätsgesetz: n besitzt modulo p einen Rest mit Betrag $< p$, sodaß wir hier effizient mittels Faktorisierung dieses Restes zum Ziel kommen. Alternativ kann selbstverständlich $\left(\frac{n}{p}\right) \equiv n^{\frac{p-1}{2}} \pmod{p}$ ausgenutzt werden.

Sieben von Relationen

Wir gehen nun wie folgt vor. Wir fixieren eine weitere Schranke C für den Siebprozeß, üblicherweise um $\sqrt[4]{n}$ herum und betrachten die Menge sämtlicher ganzer Zahlen $-C \leq x \leq C$. Dies ist unser *Siebintervall*. Analog zum Sieb des Eratosthenes legen wir eine Tabelle bzw. Liste an, in welcher jedes x einem Eintrag a_x entspricht.

Zu Beginn des Verfahrens ist jeder Eintrag $a_x = f(x)$. Nun betrachten wir nacheinander jede ungerade Primzahl p_j aus unserer Faktorbasis und dividieren sämtliche a_x durch p_j, für welche eine der beiden Kongruenzen (1.48) zutrifft. Konkret läßt sich dies wie folgt bewerkstelligen: Ausgehend vom kleinstmöglichen Repräsentanten $x_j \geq 0$ einer Nullstelle von f modulo p_j betrachten wir sämtliche x der Form

$$x = x_j + kp_j \quad \text{für} \quad \left\lceil \frac{C}{p_j} \right\rceil \leq k \leq \left\lfloor \frac{C}{p_j} \right\rfloor,$$

[40] f besitzt modulo p_j keine doppelte Nullstelle, da ansonsten $p_j \mid n$ gilt, was wir ausschließen dürfen.

und analog für die zweite, zu $2d - x_j$ kongruente Nullstelle.

Nachdem sämtliche $p_j \geq 3$ für $2 \leq j \leq u$ abgehandelt wurden, gehen wir unsere Tabelle durch, und identifizieren diejenigen x, für welche a_x von der Form

$$a_x \;=\; \pm 2^e \quad \text{für geeignetes } e \in \mathbf{N}$$

ist. Jedes derartige x führt dann zu einer Relation der Form (1.47) bezüglich unserer Faktorbasis $F(B)$.

Haben wir auf diese Weise $s > u+1$ Relationen gefunden, so ist das Gleichungssystem in Schritt (ii) nicht-trivial lösbar und wir dürfen auf eine Faktorisierung von n hoffen. Liegen nicht genügend Relationen vor oder führen alle nicht-triviale Lösungen des LGS zu trivialen Faktorisierungen von n, so vergrößern wir B und/oder C und sieben weiter.

Alternativ können wir ebensogut f durch ein Polynom der Form

$$f_k \;=\; (X + d_k)^2 - k \cdot n \;=\; X^2 + 2d_k X + d_k^2 - kn.$$

ersetzen, wobei $d_k = \lfloor \sqrt{kn} \rfloor$ für ein fest gewähltes $k \geq 1$ und erneut sieben.

Die Faktorbasis $F(B)$ bleibt hiervon unberührt und es lassen sich die zuvor bestimmten Nullstellen umrechnen und es gibt auch Varianten des Verfahrens, welche von Vornherein mit mehreren Polynomen der Art f_k arbeitet, um die Schranke C zu drücken. Das heuristische Argument für diesen Ansatz besteht darin, daß wir bei der Verwendung von K verschiedenen Polynomen $f_1, \ldots, f_K$ einerseits pro Polynom im Schnitt nur $1/K$-tel der Relationen sammeln müsseln, als wenn wir mit einem einzigen Polynom arbeiten würden. Andererseits finden wir $1/K$-tel Relationen bereit in einem deutlich kleineren Siebintervall, d. h. für ein neues C, welches signifikant kleiner als $1/K$-tel des alten C's ist. Dies ergibt sich daraus, daß kleinere Zahlen mit größerer Wahrscheinlichkeit über unserer Faktorbasis $F(B)$ zerfallen als größere, sodaß die hieraus resultierende Verkleinerung des Siebintervalles überproportional im Vergleich zur Anzahl K der Polynome ausfällt. Letztendlich führt dies auch zu einer reduktion der Schranke B, wenn man die Laufzeit optimiert. Diese Variante eignet sich besonders für parallele Implementierungen.

Beispiel 1.5.74 (Quadratisches Sieb)**.** Wir betrachten das Faktorisierungsproblem für $n = 12707$. Wir wählen $B = 70$ und $C = 79$. Dann ergibt sich zunächst als Faktorbasis die Menge

$$F(B) \;=\; \{-1, 2, 7, 17, 29, 31, 37, 47, 53, 59, 61\}.$$

Dies sind die möglichen Faktoren -1 und 2, zusammen mit allen ungeraden Primzahlen $p \leq B = 70$ sodaß

$$\left(\frac{12707}{p}\right) \;=\; 1.$$

Diese Faktorbasis enthält $u + 1 = 11$ Elemente.

Weiterhin gilt $d = \lfloor \sqrt{12707} \rfloor = 112$, sodaß hier explizit

$$f \;=\; X^2 - 224X - 163.$$

Für den Siebschritt sammeln wir zunächst die Nullstellen (1.48) von f modulo der 9 ungeraden Primzahlen $7, 17, \ldots, 61$ aus der Faktorbasis $F(B)$:

j	p_j	$x_j \pmod{p_j}$	$2d - x_j \pmod{p_j}$
2	7	4	3
3	17	15	5
4	29	14	7
5	31	30	8
6	37	34	5
7	47	26	10
8	53	33	32
9	59	44	3
10	61	33	8

Unser Siebintervall ist von Länge $2C + 1 = 159$ und entspricht dem Tupel

$$I \;=\; (-C, -C+1, \ldots, C-1, C) \;=\; (-79, -78, -77, \ldots, 77, 78, 79),$$

und die entsprechenden Werte von f führen zu dem Tupel

$$S \;=\; (f(-C), f(-C+1), \ldots, f(C-1), f(C)) \;=\; (23774, 23393, \ldots, -11551, -11618).$$

Beim Sieben werden die Einträge von S sukzessive durch die Primzahlen p_j geteilt.

Das Sieben für die Primzahl $p_2 = 7$ verläuft wie folgt. Ausgehend von $x_j = 4$ als das $C + 4$-te Element von S (wenn wir die Zählung der Einträge von S bei 0 beginnen) teilen wir den $C + 4$-ten Eintrag $f(4) = -1043$ in S durch 7, erhalten als Ergebnis -149, und ersetzen den $C + 4$-ten Eintrtag von S durch -149.

Daraufhin gehen wir jeweils sieben Schritte nach rechts und links und widmen uns dem $C + 4 - 7 = C - 3$-ten bzw. $C + 4 + 7 = C + 11$-ten Eintrag $f(-3) = 518$ bzw. $f(11) = -2506$ von S, teilen diese jeweils durch 7 und ersetzen diese Einträge durch die beiden Ergebnisse $518/7 = 74$ und $-2506/7 = -358$. Wir fahren weiter so fort, bis wir sämtliche zu $x_j = 4$ kongruenten Einträge von I abgearbeitet haben. Danach fahren wir analog fort für die zweite Nullstelle $3 + 7\mathbf{Z}$ von f: Wir teilen $f(3) = 826$ durch 7 und ersetzen den $C + 3$-ten Eintrag von S durch $826/7 = 118$ und setzen unsere Reise nach links und rechts fort.

Alternativ können wir auch jeweils beim kleinsten Eintrag von I beginnen, welcher kongruent 4 bzw. kongruent 3 modulo 7 ist und dann jeweils immer sieben Schritte weiter nach rechts wandern.

Dieses Verfahren wiederholen wir mit allen anderen ungeraden Primzahlen $p_3 = 17$, $p_4 = 29$, $\ldots$, $p_{10} = 61$ aus unserer Faktorbasis. Letztendlich erhalten wir am Ende des Siebens die folgenden Einträge des Tupels S:

23774	23393	622	22637	22262	1	2	21149	20782	1201
542	419	2762	2711	18622	18269	34	17569	17222	2411
2362	16193	15854	263	15182	479	2	2027	478	13537
13214	12893	12574	103	1706	401	11318	11009	10702	281
1442	1399	202	541	8902	8609	8318	1	1106	7457
422	113	6614	6337	866	827	178	181	2	89
262	599	562	3677	2	3169	2918	157	346	311
1934	1693	1454	1217	982	107	2	17	2	-163
-386	-607	-118	-149	-2	-1471	-58	-61	-2098	-7
-358	-2707	-2906	-107	-194	-3491	-526	-553	-4058	-4243
-4426	-271	-4786	-709	-734	-113	-5482	-5651	-5818	-193
-878	-1	-122	-179	-6778	-239	-7082	-1033	-2	-7523
-7666	-7807	-274	-8083	-1174	-1193	-8482	-8611	-514	-8863
-8986	-1301	-1318	-9343	-9458	-563	-9682	-9791	-1414	-1429
-326	-10207	-10306	-10403	-10498	-89	-1526	-10771	-10858	-10943
-11026	-11107	-11186	-11263	-11338	-11411	-11482	-11551	-11618	

Im nächsten Schritt behandeln wir die Primzahl $p_2 = 2$. Wir teilen sämtliche Einträge von S jeweils so lange durch 2, bis alle ungerade sind. Wir erhalten schließlich:

11887	23393	311	22637	11131	1	1	21149	10391	1201
271	419	1381	2711	9311	18269	17	17569	8611	2411
1181	16193	7927	263	7591	479	1	2027	239	13537
6607	12893	6287	103	853	401	5659	11009	5351	281
721	1399	101	541	4451	8609	4159	1	553	7457
211	113	3307	6337	433	827	89	181	1	89
131	599	281	3677	1	3169	1459	157	173	311
967	1693	727	1217	491	107	1	17	1	-163
-193	-607	-59	-149	-1	-1471	-29	-61	-1049	-7
-179	-2707	-1453	-107	-97	-3491	-263	-553	-2029	-4243
-2213	-271	-2393	-709	-367	-113	-2741	-5651	-2909	-193
-439	-1	-61	-179	-3389	-239	-3541	-1033	-1	-7523
-3833	-7807	-137	-8083	-587	-1193	-4241	-8611	-257	-8863
-4493	-1301	-659	-9343	-4729	-563	-4841	-9791	-707	-1429
-163	-10207	-5153	-10403	-5249	-89	-763	-10771	-5429	-10943
-5513	-11107	-5593	-11263	-5669	-11411	-5741	-11551	-5809	

Jeder Eintrag mit Absolutbetrag 1 entspricht einem Wert von $f(x)$, welcher als Produkt von Elementen der Faktorbasis geschrieben werden kann, wobei jeder Faktor höchstens einmalig auftritt. D. h. daß wir auf diese Weise im konkreten Fall 11 Relationen erhalten.

Um unsere Chancen zu erhöhen, betrachten wir diejenigen Einträge, von S, deren Absolutbetrag $\leq B$ ist. Denn diese zerfallen ebenfalls sämtlich in ein Produkt von Faktoren aus der Faktorbasis $F(B)$, wobei hier Faktoren nun mehrfach auftreten können.

Konkret erhalten wir auf diese Weise folgende 14 mit i indizierte Kandidaten für Relationen:

i	x	$f(x)$	Faktorisierung von $f(x)$	$x_i = \lvert x - d \rvert$
1	-74	21889	$7 \cdot 53 \cdot 59$	186
2	-73	21518	$2 \cdot 7 \cdot 29 \cdot 53$	185
3	-63	17918	$2 \cdot 17^2 \cdot 31$	175
4	-53	14518	$2 \cdot 7 \cdot 17 \cdot 61$	165
5	-32	8029	$7 \cdot 31 \cdot 37$	144
6	-21	4982	$2 \cdot 47 \cdot 53$	133
7	-15	3422	$2 \cdot 29 \cdot 59$	127
8	-3	518	$2 \cdot 7 \cdot 37$	115
9	-2	289	17^2	114
10	-1	62	$2 \cdot 31$	113
11	5	-1258	$-1 \cdot 2 \cdot 17 \cdot 37$	107
12	10	-2303	$-1 \cdot 7^2 \cdot 47$	102
13	32	-6307	$-1 \cdot 7 \cdot 17 \cdot 53$	80
14	39	-7378	$-1 \cdot 2 \cdot 7 \cdot 17 \cdot 31$	73

Konkret gilt hier stets

$$x_i^2 \equiv f(x)$$

mit dem korrespondierenden x aus der zweiten Spalte. Beispielsweise entspricht die erste Zeile der Relation

$$186^2 \equiv 7 \cdot 53 \cdot 59 \pmod{12707}.$$

Jeder dieser Relationen ordnen wir einen Exponentenvektor e_i modulo 2 zu, wobei wir an

$$F(B) = \{-1, 2, 7, 17, 29, 31, 37, 47, 53, 59, 61\}.$$

erinnern:

i	x_i	e_i
1	186	$\begin{pmatrix}0&0&1&0&0&0&0&0&1&1&0\end{pmatrix}$
2	185	$\begin{pmatrix}0&1&1&0&1&0&0&0&1&0&0\end{pmatrix}$
3	175	$\begin{pmatrix}0&1&0&0&0&1&0&0&0&0&0\end{pmatrix}$
4	165	$\begin{pmatrix}0&1&1&1&0&0&0&0&0&0&1\end{pmatrix}$
5	144	$\begin{pmatrix}0&0&1&0&0&1&1&0&0&0&0\end{pmatrix}$
6	133	$\begin{pmatrix}0&1&0&0&0&0&0&1&1&0&0\end{pmatrix}$
7	127	$\begin{pmatrix}0&1&0&0&1&0&0&0&0&1&0\end{pmatrix}$
8	115	$\begin{pmatrix}0&1&1&0&0&0&1&0&0&0&0\end{pmatrix}$
9	114	$\begin{pmatrix}0&0&0&0&0&0&0&0&0&0&0\end{pmatrix}$
10	113	$\begin{pmatrix}0&1&0&0&0&1&0&0&0&0&0\end{pmatrix}$
11	107	$\begin{pmatrix}1&1&0&1&0&0&1&0&0&0&0\end{pmatrix}$
12	102	$\begin{pmatrix}1&0&0&0&0&0&0&1&0&0&0\end{pmatrix}$
13	80	$\begin{pmatrix}1&0&1&1&0&0&0&0&1&0&0\end{pmatrix}$
14	73	$\begin{pmatrix}1&1&1&1&0&1&0&0&0&0&0\end{pmatrix}$

Tragen wir diese Zeilenvektoren jeweils als Spalten in eine 14×11-Matrix $E \in \mathbf{F}_2^{14\times 11}$ ein, so erhalten wir das überbestimmte homogene lineare Gleichungssystem (1.46) in folgender konkreter Gestalt:

$$\begin{pmatrix}
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 1 & 1 & 1 \\
0 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \\
1 & 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 \\
0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 \\
1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 \\
1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0
\end{pmatrix} \cdot y \;=\; 0$$

für $y = (y_1, \ldots, y_{14})^t \in \mathbf{F}_2^{14}$. Der Lösungsraum dieses Gleichungssystems ist von Dimension 5 und besitzt die Basis

$$\begin{aligned}
b_1 &= \begin{pmatrix} 1 & 1 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}^t \\
b_2 &= \begin{pmatrix} 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 \end{pmatrix}^t \\
b_3 &= \begin{pmatrix} 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 1 \end{pmatrix}^t \\
b_4 &= \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 1 & 1 & 0 & 0 & 1 \end{pmatrix}^t \\
b_5 &= \begin{pmatrix} 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}^t
\end{aligned}$$

Wir prüfen nun, ob der erste Basis-Vektor zu einer Faktorisierung führt, indem wir seine Einträge einerseits als Exponenten von $x_1, \ldots, x_{14}$ interpretieren und andererseits die korrepondierenden Werte von $f(x)$ die Faktorisierungen substituieren, was uns einerseits

$$x \;\equiv\; x_1 \cdot x_2 \cdot x_7 \;\equiv\; 186 \cdot 185 \cdot 127 \;\equiv\; -1138 \pmod{12707},$$

und andererseits

$$y^2 \;\equiv\; (7 \cdot 53 \cdot 59) \cdot (2 \cdot 7 \cdot 29 \cdot 53) \cdot (2 \cdot 29 \cdot 59) \;\equiv\; 2^2 \cdot 7^2 \cdot 29^2 \cdot 53^2 \cdot 59^2 \pmod{12707},$$

was uns

$$y \;\equiv\; -1138 \;\equiv\; 2 \cdot 7 \cdot 29 \cdot 53 \cdot 59 \pmod{12707}$$

beschert. Da x und y modulo n übereinstimmen, haben wir Pech gehabt.

Wir widmen uns daher dem zweiten Basisvektor, welcher uns analog

$$x \;\equiv\; 175 \cdot 113 \;\equiv\; -5639 \pmod{12707},$$

sowie

$$y^2 \;\equiv\; (2 \cdot 17^2 \cdot 31) \cdot (2 \cdot 31) \;\equiv\; 2^2 \cdot 17^2 \cdot 31^2 \pmod{12707},$$

ergo

$$y \equiv 2 \cdot 17 \cdot 31 \equiv 1054 \pmod{12707}.$$

In diesem Fall erhalten wir mit

$$d = \mathrm{ggT}(x - y, n) = \mathrm{ggT}(-5639 - 1054, 12707) = \mathrm{ggT}(-6693, 12707) = 97$$

tatsächlich einen nicht-trivialen Teiler von $n = 12707$ und mit $n/d = 131$ die Faktorisierung

$$12707 = 97 \cdot 131.$$

Wir merken an, daß b_5 nur einen Eintrag besitzt, da die neunte Relation ($i = 9$) bereits der Relation $f(x) \equiv 17^2 \pmod{n}$ entspricht, was ebenfalls eine Faktorisierung von n beschert:

$$\mathrm{ggT}(x_9 - 17, n) = \mathrm{ggT}(114 - 17, 12707) = \mathrm{ggT}(97, 12707) = 97.$$

Für große n ist es jedoch extrem unwahrscheinlich, daß der Fall, daß die Faktorisierung von $f(x)$ modulo n bereits ein Quadrat beschert.

Wie obiges Beispiel illustriert, ist das Quadratische Sieb für kleine Zahlen wie $n = 12707$ sehr aufwendig. Erst bei der Faktorisierung großer n ab etwa 50 Dezimalstellen, spielt es seinen asymptotischen Vorteil aus und ist schneller als das bis dahin schnellste Verfahren, welches auf elliptischen Kurven basiert.

Parameterwahl und Laufzeit des Quadratischen Siebs

Die Laufzeit eines Algorithmus wie dem Quadratischen Sieb hängt von der Parameterwahl ab, hier konkret B und C. Wir wollen die Laufzeit minimieren, d h. wir müssen uns zunächst überlegen, welche Werte von B und C überhaupt in Frage kommen.

Da wir mindestens $u + 1$ Relationen suchen, wobei $u + 1 = \#F(B)$ die Anzahl der Elemente in unserer Faktorbasis sind, stellt sich die Frage, wieviele Elemente unseres Siebintervalls $-C \le x \le C$ zu Relationen führen. Mit anderen Worten: Wieviele x mit $-C \le x \le C$ existieren, sodaß $f(x)$ eine *B-glatte Zahl* ist? Dabei nennen wir $f(x)$ B-glatt, wenn in seiner Primfaktorzerlegung nur Primteiler $\le B$ auftreten.

Wenn x zwischen $-C$ und C variiert, so ist der Betrag von $f(x)$ durch

$$C^2 + 2C\lfloor\sqrt{n}\rfloor + \lfloor\sqrt{n}\rfloor^2 - n \sim C^2 + 2C\sqrt{n} =: C_0$$

beschränkt.

Wir interessieren uns daher für die Wahrscheinlichkeit, daß eine zufällig gewählte natürliche Zahl $1 \le x \le C_0$ B-glatt ist:

$$P(C_0, B) := \mathbf{P}(x \le C_0 \wedge x \text{ ist } B\text{-glatt}) = \frac{\#\{1 \le x \le C_0 \mid x \ B\text{-glatt}\}}{C_0}.$$

Diese Wahrscheinlichkeit exakt zu bestimmen ist im Wesentlich nur in Einzelfällen durch Bestimmung aller B-glatten Zahlen bis C_0 möglich. Das ist jedoch kein Hindernis: Für ausreichend große C_0 und B stellt sich hier eine Regelmäßigkeit ein, welche wiederum nur in Einzelfällen tatsächlich beweisen wurde. *Asymptotisch* erwarten wir, daß

$$P(C_0, B) \sim \left(\frac{\ln C_0}{\ln B}\right)^{\frac{\ln C_0}{\ln B}},$$

dabei bedeutet *asymptotisch*, daß wir B als Funktion von C_0 (oder umgekehrt) ausdrücken und diesen Parameter dann gegen Unendlich laufen lassen.

Eine zweite Frage lautet, wie groß ist $F(B)$ asymptotisch? Dies wird durch den Primzahlsatz (Satz 1.4.49) zusammen mit quadratischer Reziprozität beantwortet: Im Schnitt sind die Hälte der Primzahlen bis $\leq B$ in $F(B)$ enthalten, da n jeweils ein Quadrat modulo der Elemente der Faktorbasis sein muß[41]. Es ergibt sich also

$$\#F(B) \;=\; \frac{1}{2}\pi(B)+1 \;\sim\; \frac{1}{2}\pi(B) \;\sim\; \frac{B}{2\ln B}.$$

Setzen wir in obige Formeln für B den expliziten Wert

$$B \;=\; e^{\frac{1}{2}\sqrt{\ln n \ln\ln n}} \tag{1.49}$$

ein, so erhalten wir

$$\#F(B) \;\sim\; \frac{e^{\frac{1}{2}\sqrt{\ln n \ln\ln n}}}{\sqrt{\ln n \ln\ln n}}.$$

Dies ist die Mindestanzahl an Relationen, welche wir asymptotisch finden müssen, um garantieren zu können, daß das resultierende lineare Gleichungssystem nicht-trivial lösbar ist, weswegen wir aus obiger heuritischen Formel für $P(C_0, B)$ die Schranke

$$2C \cdot P(C_0, B) \;>\; \#F(B),$$

also

$$2C \cdot \left(\frac{\ln C_0}{\ln B}\right)^{\frac{\ln C_0}{\ln B}} \;>\; \frac{B}{2\ln B}$$

erhalten.

Wir schätzen nun C_0 durch $2C\sqrt{n}$ ab, was sinnvoll ist, so lange C^2 klein im Vergleich zu $\sqrt{n}$ ist. Damit ergibt sich die Ungleichung

$$2C \cdot \left(\frac{\ln 2C\sqrt{n}}{\ln B}\right)^{\frac{\ln 2C\sqrt{n}}{\ln B}} \;>\; \frac{B}{2\ln B}.$$

Diese ist jedoch nicht nach C auflösbar, weswegen wir für einen Moment $2C\sqrt{n} = n$ wählen, mit dem Hintergedanken, daß wir das Sieben abbrechen, sobald wir ausreichend viele Relationen gefunden haben.

Damit ergibt sich dann, daß wir im Durchschnitt

$$\frac{1}{2}\frac{\pi(B)}{P(n,B)} \;\sim\; \frac{B}{2\ln B} \cdot \left(\frac{\ln n}{\ln B}\right)^{\frac{\ln n}{\ln B}}$$

Zahlen sieben müssen, um mindestens $\#F(B)$ Relationen zu finden.

Damit läßt sich dann C abschätzen, indem wir diesen Ausdruck halbieren[42]:

$$C \;:=\; \frac{B}{4\ln B} \cdot \left(\frac{\ln n}{\ln B}\right)^{\frac{\ln n}{\ln B}}. \tag{1.50}$$

[41] vgl. Aufgabe 2 von Übungsblatt 10.

[42] denn unser Siebintervall hat länge $2C$.

Optimiert man diese Schranke und stöpselt das Resultat zusammen mit Abschätzungen für die notwendigen Operationen im Siebverfahren, so erhält man eine asymptotische obere Laufzeitschranke für das quadratische Siebverfahren von

$$O\left(e^{\sqrt{\ln n \ln\ln n}}\right).$$

Diese Notation bedeutet: Es existiert eine positive Konstante $c > 0$ derart, daß die Laufzeit des Verfahrens für ausreichend große Werte von n stets $\leq c \cdot \exp(\sqrt{\ln n \ln\ln n})$ ist. Wir merken an, daß bei obiger Wahl von B damit die Laufzeit $O(B^2)$ ist.

In einer praktischen Implementierung ist obige pessimistische Wahl (1.50) für C sehr ineffizient und führt zu einem deutlich zu langen Siebintervall. Obige Laufzeit besagt im Wesentlichen, daß wir $C \in O(B^2)$ wählen sollten, d. h.

$$C \;:=\; c_0 \cdot B^2$$

mit einer Konstanten c_0.

Da wir a priori n als Grenze des Siebintervalles ansetzen, um die Anzahl der B-glatten Zahlen zu bestimmen, unterschätzen wir die Wahrscheinlichkeit, eine B-glatte Zahl zu finden. In der Realität ist C deutlich kleiner als $\frac{1}{2}\sqrt{n}$, weswegen wir $2C\sqrt{n}$ in obiger Abschätzung durch eine kleinere Zahl als n ersetzen sollten. Die Frage lautet, wie wir hier am Besten vorgehen: Sollen wir n durch eine Konstante teilen? Das wäre möglich, aber auch nicht effizient, da wir es mit einem *multiplikativen Problem* zu tun haben. Ein besserer Ansatz besteht daher darin, n durch n^δ für ein geeignetes $0 < \delta < 1$ zu ersetzen. Experimentell stellt man fest, daß $\delta = 0.7$ eine vernünftige Wahl für n ab 10^{20} ist und $\delta = 0.6$ eine gute Wahl für n ab 10^{40} darstellt, d. h. wir ählen in diesem Fall:

$$C \;:=\; \frac{B}{4\ln B} \cdot \left(\frac{0.6 \cdot \ln n}{\ln B}\right)^{\frac{0.6\cdot\ln n}{\ln B}}. \tag{1.51}$$

Eine optimale Parameterwahl für eine Implementierung optimiert ebenfalls die Wahl von B aus (1.49), was wiederum C beeinflußt.

Für die ersten 10-er-Potenzen für n ergeben sich aus (1.49) und (1.50) folgende Parameter-Werte:

n	B gem. (1.49)	C gem. (1.50)	$e^{\sqrt{\ln n \ln\ln n}}$
10^{10}	70	39 082	4 907
10^{20}	765	$1.9 \cdot 10^7$	585 565
10^{30}	5 178	$3.2 \cdot 10^9$	$2.6 \cdot 10^7$
10^{40}	27 041	$2.8 \cdot 10^{11}$	$7.3 \cdot 10^8$
10^{50}	119 098	$1.6 \cdot 10^{13}$	$1.4 \cdot 10^{10}$
10^{60}	463 630	$6.3 \cdot 10^{14}$	$2.1 \cdot 10^{11}$
10^{70}	1 641 126	$2.0 \cdot 10^{16}$	$2.7 \cdot 10^{12}$
10^{80}	5 382 470	$5.2 \cdot 10^{17}$	$2.9 \cdot 10^{13}$
10^{90}	16 574 472	$1.1 \cdot 10^{19}$	$2.7 \cdot 10^{14}$
10^{100}	48 389 444	$2.2 \cdot 10^{20}$	$2.3 \cdot 10^{15}$
10^{110}	134 940 810	$3.6 \cdot 10^{21}$	$1.8 \cdot 10^{16}$
10^{120}	361 533 574	$5.5 \cdot 10^{22}$	$1.3 \cdot 10^{17}$
10^{130}	934 964 947	$7.6 \cdot 10^{23}$	$8.7 \cdot 10^{17}$
10^{140}	2 342 826 584	$9.6 \cdot 10^{24}$	$5.5 \cdot 10^{18}$
10^{150}	5 706 337 341	$1.1 \cdot 10^{26}$	$3.3 \cdot 10^{19}$
10^{200}	$3.5 \cdot 10^{11}$	$9.6 \cdot 10^{30}$	$1.2 \cdot 10^{23}$
10^{250}	$1.4 \cdot 10^{13}$	$2.5 \cdot 10^{35}$	$1.9 \cdot 10^{26}$
10^{300}	$3.9 \cdot 10^{14}$	$2.9 \cdot 10^{39}$	$1.5 \cdot 10^{29}$

Die Laufzeit ist in etwa ein konstantes Vielfaches der letzten Spalte, d. h. daß z. B. das Faktorisieren erin 100-stelligen Dezimalzahl etwa

$$\frac{2.3 \cdot 10^{15}}{1.4 \cdot 10^{10}} \sim 1.6 \cdot 10^5$$

mal länger dauern sollte, als die Faktorisierung einer 50-stelligen Dezimalzahl.

Das Faktorisieren einer 20-stelligen Dezimalzahl mithilfe des Quadratischen Siebes sollte im Gegenzug etwa

$$\frac{7.3 \cdot 10^8}{585\,565} \sim 1.6 \cdot 10^5 = 1\,247$$

mal schneller sein, als die Faktorisierung einer 40-stelligen Dezimalzahl.

Vergleich der vorletzten Spalte mit der letzten zeigt, daß die Wahl (1.50) für C zu pessimistisch ist. Kompensation via (1.51) ist ein sinnvoller Ansatz. In der Praxis kann man das Siebintervall gut schätzen, indem man für das gegebene große n zunächst kleine Intervalle an verschiedenen Stellen des angedachten Siebintervalles siebt und prüft, wie gut der Ertrag ist. Diese Zahlen werden dann extrapoliert, um C realistisch abzuschätzen.

Bis etwa $n = 10^{110}$ ist das Quadratische Sieb bzw. seine Variante mit mehreren Polynomen das schnellste bekannte Verfahren. Danach ist das *Zahlkörpersieb* schneller. Bis etwa 10^{40} ist Faktorisieren mit elliptischen Kurven effizienter als das Quadratische Sieb.

Zum Abschluß seien noch folgende Optimierungsmöglichkeiten erwähnt:

Additionen statt Divisionen: Anstatt in einer Liste die Werte $f(x)$ zu tabellieren und in jedem Siebschritt durch p zu teilen, können wir stattdessen $\log f(x)$ tabellieren und $\log p$ subtrahieren. Damit tauschen wir teure Divisionen gegen billigere Sutraktionen (von Gleitkommazahlen) aus. In der Praxis wird dies stets so gemacht.

Faktorisierungen merken: Anstatt im Siebschritt nur zu subtrahieren, können (insbesondere größere) die Primteiler von $f(x)$ mit tabelliert werden, sodaß die Faktorisierung

der B-glatten Werte $f(x)$ am Ende des Siebschrittes bereits vorliegt und nicht erneut berechnet werden muß.
Große Primfaktoren: Es kann pro x ein Primteiler p von $f(x)$ größer als B zugelassen werden, welche separat tabelliert wird, in der Hoffnung, so B drücken zu können und zugleich Relationen mit bis zu einem Primteiler $> B$ zu erhalten. Am Ende des Siebschrittes wird jeder aufgetretene Primteiler $> B$ in einer Glattheitsrelation zu $F(B)$ hinzugefügt, sodaß der Rest des Verfahrens unverändert abläuft.
Mehrere Polynome: Diese Variante haben wir bereits oben angedeutet. Durch die Nutzung von mehreren Polynomen der allgemeineren Form $f = aX^2 + bX + c$ kann das Siebintervall deutlich verkleinert werden, wobei im Grunde mehrere kleinere Siebintervalle entstehen (für jedes Polynom eines), welche nacheinander abgearbeitet werden müssen. Die Nullstellenbestimmung modulo der Primzahlen muß genau genommen nur einmal durchgeführt werden, da sich die Nullstellen für verschiedene Polynome ineinander umrechnen lassen. Diese Optimierung führt zu einem drastischen Geschwindigkeitsgewinn in der Praxis.

1.6 Die ganzen Gauß'schen Zahlen

In Beispiel 1.5.71 hatten wir uns mit der Frage beschäftigt, wann die Gleichung (1.44)

$$x^2 + dy^2 \;=\; 0 \tag{1.52}$$

nicht-triviale Lösungen modulo p besitzt und gesehen, daß ein notwendiges und hinreichendes Kriterium durch

$$\left(\frac{-d}{p}\right) \;=\; 1 \tag{1.53}$$

gegeben ist, sofern p ungerade und $p \nmid d$. Dabei entspricht eine nicht-triviale Lösung der Gleichung (1.52) modulo p einem Paar (x, y) ganzer Zahlen, für welche

$$p \mid x^2 + dy^2 =: n$$

und zugleich $p \nmid x$ oder $p \nmid y$.

Ausgangspunkt unserer Betrachtungen war die Frage gewesen, welche $n \in\in \mathbf{Z}$ zu gegebenem d der Gestalt

$$n \;=\; x^2 + dy^2, \quad x, y \in \mathbf{Z}, \tag{1.54}$$

sind (vgl. (1.43)). Dabei ist für $n = p$ (1.53) stets eine notwendige Bedingung, sofern wir auf die *Primitivitätsbedingung*

$$\mathrm{ggT}(n, x, y) \;=\; 1 \tag{1.55}$$

bestehen. Die Reduktion auf Primzahlen $n = p$ war dadurch gerechtfertigt, daß die Menge $\mathscr{L}_d \subseteq \mathbf{Z}$ derjenigen n, welche von der Gestalt (1.54) sind, multiplikativ abgeschlossen ist (vgl. Beispiel 1.5.71).

In diesem Abschnitt werden wir uns dem Fall $d = 1$ annehnmen und einsehen, daß hier die Bedingung (1.53) nicht nur notwendig, sondern auch hinreichend für (1.54) ist. In diesem Fall beschäftigen wir uns also mit der Frage, wann eine Primzahl p von der Gestalt

$$p \;=\; x^2 + y^2 \tag{1.56}$$

mit $x, y \in \mathbf{Z}$ ist. Primzahlen dieser Gestalt werden *Pythagoreische Primzahlen* genannt, da sie aufgrund des Satzes von Pythagoras als Hypothenusen rechtwinkler Dreiecke mit ganzzahligen Seitenlängen auftreten. Erste Beispiele sind

$$5 \;=\; 1^2 + 2^2, \quad 13 = 13^2 + 3^2, \quad 17 \;=\; 1^2 + 4^2, \quad 29 = 2^2 + 5^2, \ldots$$

Die Beobachtung, daß Bedingung (1.53) im vorliegenden Fall nicht nur notwendig sondern auch hinreichend ist, geht auf Pierre der Fermat zurück, welcher den Beweis hierfür jedoch schuldig blieb. Leonhard Euler gelang als erster ein Beweis dieser Aussage, gefolgt von Beweisen von Joseph-Louis Lagrange, Gauß und Dedekind.

Wir wissen bereits, daß für $p \equiv 3 \pmod 4$ stets (1.53) wegen

$$\left(\frac{-d}{p}\right) \;=\; \left(\frac{-1}{p}\right) \;=\; (-1)^{\frac{p-1}{2}} \;=\; -1$$

verletzt ist, sodaß eine derartige Primzahl nicht von der Form (1.56) sein kann. Umgekehrt gilt für $p \equiv 1 \pmod 4$ stets

$$\left(\frac{-1}{p}\right) \;=\; (-1)^{\frac{p-1}{2}} \;=\; 1,$$

sodaß wir bereits wissen, daß es $x, y \in \mathbf{Z}$ mit $\mathrm{ggT}(p, x, y) = 1$ gibt und

$$p \mid x^2 + y^2.$$

Es stellt sich also die Frage, wie es uns gelingen kann, diese Teilbarkeitsrelation zu einer Gleichheit verschärfen.

Der kürzeste bekannte Beweis geht auf die beiden zeitgenössischen Zahlentheoretiker David Rodney „Roger“ Heath-Brown und Don Bernard Zagier zurück. Diesen werden wir auf dem Übungsblatt aufgreifen.

Unser Ansatz ist arithmetisch inspiriert. Wir betrachten zunächst den Ring

$$\mathbf{Z}[i] \;:=\; \mathbf{Z} + i\mathbf{Z} \;=\; \{x + iy \mid x, y \in \mathbf{Z}\}$$

der *ganzen Gaußschen Zahlen*, welchen wir als Teilring des Körpers der komplexen Zahlen $\mathbf{C}$ auffassen. Wegen $i^2 = -1$ sind Addition und Multiplikation explizit gegeben durch

$$\begin{aligned}(x_1 + iy_1) \;+\; (x_2 + iy_2) \;&=\; (x_1 + x_2) \;+\; i(y_1 + y_2),\\ (x_1 + iy_1) \cdot (x_2 + iy_2) \;&=\; (x_1x_2 - y_1y_2) \;+\; i(x_1y_2 + x_2y_1).\end{aligned}$$

Analog zu unserer Rechnung in Beispiel 1.5.71 lassen sich die Elemente aus $\mathbf{Z}[i]$ mit 2×2-Matrizen der Form

$$A(x, y) \;:=\; \begin{pmatrix} x & -y \\ y & x \end{pmatrix}$$

identifizieren. Eine kleine Rechnung zeigt, daß die Abbildung

$$\phi : \; \mathbf{Z}[i] \to \{A(x, y) \mid x, y \in \mathbf{Z}\}, \quad x + iy \;\mapsto\; A(x, y) \tag{1.57}$$

ein Ringisomorphismus ist.

Der Bezug zu unserem Ursprungsproblem (1.56) besteht darin, daß

$$N(x+iy) \;:=\; \det A(x,y) \;=\; \det \begin{pmatrix} x & -y \\ y & x \end{pmatrix} \;=\; x^2+y^2.$$

Diese Abbildung bezeichnen wir als *Norm*. Wir beobachten, daß die Norm nur Werte in den natürlichen Zahlen annimmt, d. h. es handelt sich um eine Abbildung $N : \mathbf{Z}[i] \to \mathbf{N}$. Die Multiplikativität der Determinante zeigt die Multiplikativität

$$N(\alpha \cdot \beta) \;=\; N(\alpha) \cdot N(\beta)$$

der Norm für beliebige $\alpha, \beta \in \mathbf{Z}[i]$.

Unsere ursprüngliche Fragestellung (1.56) ist also äquivalent dazu, für $p \equiv 1 \pmod 4$ ein Element $x + iy \in \mathbf{Z}[i]$ zu finden mit

$$N(x+iy) \;=\; p. \tag{1.58}$$

Die Darstellung

$$N(x+iy) \;=\; (x+iy)\cdot(x-iy), \tag{1.59}$$

welche sich aus der dritten binomischen Formel ergibt, zeigt, daß (1.58) äquivalent zu

$$p \;=\; (x+iy)\cdot(x-iy) \tag{1.60}$$

ist. Mit anderen Worten: Es stellt sich die Frage, wie eine Primzahl $p \in \mathbf{Z}$ in $\mathbf{Z}[i]$ zerfällt, womit wir unsere ursprüngliche Frage in eine arithmetische Fragestellung im Ring $\mathbf{Z}[i]$ übersetzt haben.

Proposition 1.6.1 (Einheiten in $\mathbf{Z}[i]$)**.** *Für ein Element $\alpha = x+iy \in \mathbf{Z}[i]$ sind äquivalent:*

(a) $\alpha \in \mathbf{Z}[i]^\times$, d. h. α ist eine Einheit in $\mathbf{Z}[i]$,

(b) $N(\alpha) = 1$.

Insbesondere gilt

$$\mathbf{Z}[i]^\times \;=\; \{\pm 1, \pm i\}.$$

Beweis. Wenn $\alpha \in \mathbf{Z}[i]^\times$, so finden wir $\beta \in \mathbf{Z}[i]$ mit $\alpha \cdot \beta = 1$. Aufgrund der Multiplikativität der Norm

$$N(\alpha)\cdot N(\beta) \;=\; N(\alpha\cdot\beta) \;=\; N(1) \;=\; 1$$

zur Folge hat. Da $N(\alpha)$ und $N(\beta)$ natürliche Zahlen sind, folgt hieraus $N(\alpha) = 1$, was (a) $\Rightarrow$ (b) beweist.

Umgekehrt zeigt die Darstellung (1.59), daß wenn $\alpha = x + iy$ und $N(\alpha) = 1$, daß durch $\beta := x - iy \in \mathbf{Z}[i]$ ein Inverses zu α gegeben ist. Mithin folgt $\alpha \in \mathbf{Z}[i]^\times$, womit (b) $\Rightarrow$ (a) nachgewiesen ist.

Die Gleichung

$$x^2 + y^2 \;=\; 1$$

besitzt für $x, y \in \mathbf{Z}$ nur die vier Lösungen $x = \pm 1$ und $y = 0$ bzw. $x = 0$ und $y = \pm 1$, was mithilfe der Äquivalenz von (a) und (b) zeigt, daß $\mathbf{Z}[i]^\times = \{\pm 1, \pm i\}$. □

Proposition 1.6.2 (Division mit Rest in $\mathbf{Z}[i]$)**.** *Der Ring* $\mathbf{Z}[i]$ *ist zusammen mit der Abbildung* $\mathbf{Z}[i] \to \mathbf{N}$, $x + iy \mapsto N(x + iy)$ *ein* euklidischer Ring*, d. h. es gilt: Für alle* $\alpha, \beta \in \mathbf{Z}[i]$ *mit* $\beta \neq 0$ *existieren* $\gamma, \delta \in \mathbf{Z}[i]$ *mit:*

$$\alpha \;=\; \gamma \cdot \beta \;+\; \delta, \quad \textit{und} \quad N(\delta) < N(\beta). \tag{1.61}$$

Wir merken an, daß $\mathbf{Z}[i]$ als Teilring von $\mathbf{C}$ nullteilerfrei ist.

Beweis. Seien explizit $\alpha = a + ib$ und $\beta = c + id$ und $a, b, c, d \in \mathbf{Z}$. Wir betrachten die komplexe Zahl[43]

$$\frac{a+bi}{c+di} \;=\; \frac{ac+bd}{c^2+d^2} \;+\; i\frac{bc-ad}{c^2+d^2} \;=:\; x + iy.$$

Seien nun $u, v \in \mathbf{Z}$ mit

$$|u - x| \;\leq\; \frac{1}{2} \quad \text{und} \quad |v - y| \leq \frac{1}{2}.$$

Dann gilt bezüglich der komplexen Norm

$$|(x + iy) - (u + iv)|^2 \;=\; (x-u)^2 \;+\; (y-v)^2 \;\leq\; \left(\frac{1}{2}\right)^2 \;+\; \left(\frac{1}{2}\right)^2 \;=\; \frac{1}{2} \;<\; 1.$$

Multiplikation dieser Ungleichung mit $N(\beta) = c^2 + d^2 = |\beta|^2$ beschert uns

$$N(\alpha - (u + iv)\beta) \;=\; |(a + ib) - (u + iv)(c + id)|^2 \;<\; N(\beta),$$

womit die Wahl

$$\gamma \;:=\; u + iv \quad \text{und} \quad \delta \;:=\; (a + ib) - (u + iv)(c + id)$$

die Existenz von γ und δ nachweist. □

Wir haben nun genug Werkzeuge an der Hand, um unsere ursprüngliche Fragestellung zu beantworten.

Satz 1.6.3 (Satz über Pythagoreische Primzahlen)**.** *Eine Primzahl* $p \in \mathbf{N}$ *ist genau dann als Summe*

$$p \;=\; x^2 + y^2 \tag{1.62}$$

zweier Quadrate mit $x, y \in \mathbf{Z}$ *darstellbar, wenn entweder* $p = 2$ *oder* $p \equiv 1 \pmod 4$.

Bemerkung 1.6.4 (Geometrische Interpretation)**.** Die Aussage aus Satz 1.6.3 hat folgende geometrische Interpretation: Wir betrachten $\mathbf{Z}^2 \subseteq \mathbf{R}^2$ als Gitterpunkte in der reellen Ebene. Dann ist (1.62) äquivalent dazu, daß auf dem Kreis mit Radius $r = \sqrt{p}$ um den Ursprung ein Gitterpunkt $(x, y) \in \mathbf{Z}^2$ liegt. Damit besagt Satz 1.6.3, daß für eine Primzahl p genau dann ein ganzahliger Gitterpunkt $(x, y) \in \mathbf{Z}^2$ auf Kreis mit Radius $r = \sqrt{p}$ liegt, wenn $p = 2$ oder $p \equiv 1 \pmod 4$.

[43] Wegen $N(\beta) = c^2 + d^2 = (c+id)(c-id)$ folgen die Formeln für Real- und Imaginärteil nach Erweitern des Bruches mit $\overline{\beta} = (c - id)$.

Beweis von Satz 1.6.3. Die Darstellbarkeit im Fall $p = 2$ ist wegen $2 = 1^2 + 1^2$ offensichtlich.

Wir haben bereits gesehen, daß für $p > 2$ die Bedinung $p \equiv 1 \pmod 4$ notwendig ist (vgl. Beispiel 1.5.71). Um einzusehen, daß diese Bedingung hinreichend ist, fixieren wir eine Primzahl p mit $p \equiv 1 \pmod 4$ und zeigen die Existenz eines Elementes $\pi \in \mathbf{Z}[i]$ mit $N(\pi) = p$. Hierzu gehen wir wie folgt vor:

Die Teiler $\beta \mid p$ im Ring $\mathbf{Z}[i]$ sind geeignete Kandidaten für π, denn aufgrund der Multiplikativität der Norm gilt für jeden Teiler $\beta \mid p$ stets $N(\beta) \mid N(p) = p^2$. Wir müssen also die Existenz eines *nicht-trivialen* Teilers $\pi \mid p^2$ nachweisen[44], d. h. $\pi \notin \mathbf{Z}[i]^\times$ und $p/\pi \notin \mathbf{Z}[i]^\times$.

Hierzu erinnern wir daran, daß wir bereits wissen, daß wegen $p \equiv 1 \pmod 4$ Elemente $x, y \in \mathbf{Z}$ existieren mit $p \nmid x$ und $p \nmid y$ und

$$p \mid x^2 + y^2 \;=\; N(x + iy) \;=\; (x + iy) \cdot (x - iy).$$

Es existiert also ein Element $\zeta := x + iy \in \mathbf{Z}[i]$, welches *kein* $\mathbf{Z}[i]$-Vielfaches von p ist[45].

Die Idee besteht nun darin, π als größten gemeinsamen Teiler von ζ und p zu identifizieren.

Um dies zu bewerkstelligen, betrachten wir die Menge

$$P \;:=\; \{\mu \cdot \zeta + \nu \cdot p \mid \mu, \nu \in \mathbf{Z}[i]\} \;\subseteq\; \mathbf{Z}[i]$$

aller $\mathbf{Z}[i]$-Linearkombinationen von ζ und p. Diese ist eine additive Untergruppe von $\mathbf{Z}[i]$ und unter Multiplikation mit beliebigen Elementen aus $\mathbf{Z}[i]$ abgeschlossen. Insbesondere liegt für zwei Elemente $\alpha, \beta \in P$ mit $\beta \neq 0$ auch stets der Rest δ der Division von α durch β wieder in P. Mit anderen Worten: Wenn wir den euklidischen Algorithmus auf ζ und p anwenden, dann erhalten wir als Ergebnis einen Teiler π in P von p, welcher p teilt, aber kein Vielfaches von p ist, da π ebenfalls ζ teilt und letzteres *kein* Vielfaches von p ist.

Es ist denkbar, daß der Fall $\pi = 1$ bzw. $\pi \in \mathbf{Z}[i]^\times$ eintritt, d. h. daß ζ und p teilerfremd sind. Um diesen Fall auszuschließen, werden wir zeigen, daß $N(\pi) \neq 1$ gilt, aber der Reihe nach.

Obwohl der Euklidische Algorithmus in $\mathbf{Z}[i]$ anwendbar ist und wir dies in Beispielen auch anwenden werden, kürzen hier ab und wählen kurzerhand $\pi = c + id \in P$ als ein Element mit minimaler positiver Norm in P, d. h. $\pi \in P$ und $N(\pi) > 0$ sei minimal. Ein solches Element existiert, dank des Wohlordnungsprinzips da $N(P) \subseteq \mathbf{N}$ und $P \setminus \{0\} \neq \emptyset$.

Wir behaupten, daß jedes Element $\alpha \in P$ von der Form

$$\alpha \;=\; \gamma \cdot \pi$$

mit $\gamma \in \mathbf{Z}[i]$ ist. Mit anderen Worten: Die Elemente in P sind sämtlich Vielfache des „minimalen“ Elementes π.

In der Tat: Sei $\alpha \in P$ beliebig gegeben. Dann zeigt die Division mit Rest in $\mathbf{Z}[i]$ aus Proposition 1.6.2, daß wir $\gamma, \delta \in \mathbf{Z}[i]$ finden mit

$$\alpha \;=\; \gamma \cdot \pi \;+\; \delta, \quad N(\delta) < N(\pi).$$

[44] vgl. Proposition 1.6.2.

[45] Denn sämtliche Vielfache von p sind von der Form $k \cdot p + ik \cdot p$, sodaß sowohl Real- als auch Imaginärteil stets durch p teilbar sind.

Wegen

$$\delta \;=\; \alpha - \gamma \cdot \pi \;\in\; P$$

impliziert die Minimalität von $N(\pi)$, daß $N(\delta) = 0$ gelten muß. Mithin gilt $\delta = u + iv = 0$ (da $u^2 + v^2 = N(\delta) = 0$). Das Element α ist also ein Vielfaches von π.

Wir behaupten nun, daß

$$N(\pi) \;=\; p.$$

Um dies einzusehen, beobachten wir, daß uns die Multiplikativität der Norm zusammen mit $p = \gamma \cdot \pi$ für geeignetes $\gamma \in \mathbf{Z}[i]$

$$N(\gamma) \cdot N(\pi) \;=\; N(\gamma \cdot \pi) \;=\; N(p) \;=\; p^2$$

beschert. Die Norm von π ist also ein Teiler von p^2, womit die beiden Fälle $N(\pi) = 1$ und $N(\pi) = p^2$ auszuschließen sind.

Angenommen, $N(\pi) = p^2$. Dann gilt aufgrund obiger Gleichung zwangsläufig $N(\gamma) = 1$, womit γ laut Proposition 1.6.1 eine Einheit ist, d. h. $\gamma^{-1} \in \mathbf{Z}[i]$, sodaß

$$\pi \;=\; \gamma^{-1} \cdot p$$

ein Vielfaches von p ist. Damit teilt p das Element ζ, welches per Konstruktion nicht durch p teilbar war, Widerspruch. Dieser Fall kann also nicht eintreten.

Um den Fall $N(\pi) = 1$ auszuschließen, beobachten wir, daß die Normen *aller* Elemente $\alpha \in P$ durch p teilbar sind. Hierzu sei explizit

$$\alpha \;=\; \mu \cdot \zeta \;+\; \nu \cdot p$$

mit $\mu, \nu \in \mathbf{Z}[i]$ ein beliebiges Element aus P. Wir wissen, daß $p \mid N(\zeta)$ und $N(p) = p^2$, aber da die Normabbildung nicht additiv ist, müssen wir etwas genauer hinsehen: Seien $\mu = m_1 + im_2$ und $\nu = n_1 + in_2$ mit $m_1, m_2, n_1, n_2 \in \mathbf{Z}$ und $\zeta = x + iy$ mit $x, y \in \mathbf{Z}$ als wie zuvor. Dann erhalten wir

$$\begin{aligned}
\alpha \;&=\; (m_1 + im_2) \cdot (x + iy) \;+\; (n_1 + in_2) \cdot p \\
&=\; (m_1 x - m_2 y) + (m_1 y + m_2 x) \cdot i \;+\; n_1 p + n_2 p i \\
&=\; (m_1 x - m_2 y + n_1 p) \;+\; (m_1 y + m_2 x + n_2 p) \cdot i,
\end{aligned}$$

und somit

$$\begin{aligned}
N(\alpha) \;&=\; (m_1 x - m_2 y + n_1 p)^2 \;+\; (m_1 y + m_2 x + n_2 p)^2 \\
&\equiv\; (m_1 x - m_2 y)^2 \;+\; (m_1 y + m_2 x)^2 \\
&\equiv\; N((m_1 + im_2) \cdot (x + iy)) \\
&\equiv\; N(\mu \cdot \zeta) \\
&\equiv\; N(\mu) \cdot N(\zeta) \\
&\equiv\; N(\mu) \cdot 0 \\
&\equiv\; 0 \pmod{p},
\end{aligned}$$

denn $p \mid N(\zeta)$. Das zeigt, daß $p \mid N(\alpha)$, also insbesondere $p \mid N(\pi)$ (wegen $\pi \in P$), sodaß $N(\pi) = 1$ ebenfalls unmöglich ist.

Zusammenfassend sehen wir, daß $N(\pi) = p$ gilt[46], was zu zeigen war. □

[46] Im Übrigen ergibt sich ebenfalls $N(\gamma) = p$.

Bemerkung 1.6.5. Im Beweis von Satz 1.6.3 nutzen wir geschickt Teilbarkeitsrelationen im Ring $\mathbf{Z}[i]$ aus. Es stellt sich heraus, daß in $\mathbf{Z}[i]$ aufgrund von Proposition 1.6.2 der Satz der eindeutigen Primfaktorzerlegung gilt, letztendlich weil wir den (erweiterten) Euklidischen Algorithmus in $\mathbf{Z}[i]$ anwenden können. Aus dieser Perspektive betrachtet haben wir in obigem Beweis die Primfaktorzerlegung von p in $\mathbf{Z}[i]$ bestimmt, unter der Voraussetzung daß $p \equiv 1 \pmod 4$: p ist das Produkt der beiden Primelemente π und γ. Es stellt sich heraus, daß im Fall $p \equiv 3 \pmod 4$ die Primzahl p im Ring $\mathbf{Z}[i]$ selbst ein Primelement ist, womit p seine eigene Primfaktorzerlegung in $\mathbf{Z}[i]$ ist. Letzteres liefert eine alternative Erklärung dafür, daß p in diesem Fall *nicht* von der Form $p = x^2 + y^2$ ist.

Bemerkung 1.6.6. Der Beweis des Satzes läßt sich zu folgendem Verfahren zur Bestimmung von x, y mit $p = x^2 + y^2$ im Fall $p \equiv 1 \pmod 4$ verfeinern:

(i) Bestimme zunächst eine nicht-triviale Lösung von $x^2 + y^2 = 0$ in $\mathbf{F}_p$, d. h. konkret: Bestimme eine Quadratwurzel $\xi \in \mathbf{F}_p$ von -1 mithilfe des Algorithmus zur Faktorisierung quadratischer Polynome über $\mathbf{F}_p$: Zerlege das Polynom $f = X^2 + 1$ in Linearfaktoren bzw. bestimme eine Nullstelle ξ desselbigen Polynoms in $\mathbf{F}_p$. Dann gilt $1^2 + \xi^2 = 1 + (-1) = 0$, womit für einen beliebigen Repräsentanten $z \in \mathbf{Z}$ der Restklasse $\xi = z + p\mathbf{Z}$ automatisch $p \mid 1^2 + z^2$ gilt.

(ii) Nutze den euklidischen Algorithmus in $\mathbf{Z}[i]$ mit der Polynomdivision aus Proposition 1.6.2 (vgl. den dortigen Beweis für eine algorithmische Realisierung der Polynomdivision), um einen größten gemeinsamen Teiler $\pi = x + iy$ von p und $\zeta = 1 + iz$ in $\mathbf{Z}[i]$ zu bestimmen.

(iii) Wegen $N(\pi) = p$ gilt $x^2 + y^2 = p$.

Beispiel 1.6.7. Wir wollen $p = 41$ als Summe zweier Quadrate schreiben, was wegen $p \equiv 1 \pmod 4$ auch möglich ist. Zunächst bestimmen wir eine Quadratwurzel von -1 in $\mathbf{F}_{41}$, allerdings mit folgender Vereinfachung des Algorithmus zur Nullstellenbestimmung von $f = X^2 + 1$. Wir wählen $a = 7 + 41\mathbf{Z}$ zufällig[47] und berechnen

$$a^{\frac{41-1}{2}} \;=\; 7^{20} \;\equiv\; -1 \pmod{41}.$$

Damit gilt

$$(7^{10})^2 \;\equiv\; -1 \pmod{41},$$

sodaß

$$z \;\equiv\; 7^{10} \;\equiv\; 9 \pmod{41}$$

wählen können.

Wir müssen also einen größten gemeinsamen Teiler von $p = 41$ und $\zeta = 1 + iz = 1 + 9i$ bestimmen. Hierzu berechnen wir zunächst die Norm

$$N(1 + 9i) \;=\; 1^2 + 9^2 \;=\; 1 + 81 \;=\; 82 \;=\; 2 \cdot 41,$$

sodaß wir erwarten können, daß bereits eine Iteration des Euklidischen Algorithmus ausreichen wird[48]. Wir teilen also $p = 41 + 0i$ durch $1 + 9i$, denn die Norm von p ist mit

[47] Da nur die Hälfte der Elemente in $\mathbf{F}_p^\times$ Quadrate sind, sind wir in der Hälfte der Fälle erfolgreich.

[48] Begründung: Teilen wir $p = 41$ durch $1+9i$, so wird der Rest r eine Norm $0 < N(r) < N(1+9i) = 2 \cdot 41$ haben. Da die Norm von r ein Vielfaches von 41 ist, muß also $N(r) = 41$ gelten.

41^2 größer als $N(1+9i) = 82$. Hierzu müssen wir laut Beweis von Proposition 1.6.2 die Koeffizienten

$$x \;=\; \frac{p \cdot 1}{N(1+9i)} \;=\; \frac{41}{82} \;=\; \frac{1}{2}$$

und

$$y \;=\; \frac{p \cdot 9}{N(1+9i)} \;=\; \frac{-41 \cdot 9}{82} \;=\; -\frac{9}{2}$$

durch ganze Zahlen $u, v \in \mathbf{Z}$ approximieren. Hier kommen $u = 0$ und $v = -4$ infrage, womit wir als Rest

$$\begin{aligned} r \;&=\; 41 - (u+iv)\cdot(1+9i) \\ &=\; 41 - (0-i4)\cdot(1+9i) \\ &=\; 41 + 4i\cdot(1+9i) \\ &=\; 41 + 4i - 36 \\ &=\; 5 - 4i \end{aligned}$$

erhalten. In der Tat gilt

$$N(r) \;=\; 5^2 + 4^2 \;=\; 41,$$

was wir erzielen wollten.

Satz 1.6.8 (Zweiquadrate-Satz)**.** *Es sei $n \neq 0$ eine ganze Zahl. Dann ist n genau dann als Summe zweier Quadrate*

$$n \;=\; x^2 + y^2, \quad x, y \in \mathbf{Z},$$

darstellbar, wenn $n > 0$ und wenn jede Primzahl p in der Primfaktorzerlegung von n mit $p \equiv 3 \mod 4$ in gerader Potenz in n aufgeht[49]*.*

Beweis. Daß das genannte Kriterium hinreichend ist, ergibt sich aus Satz 1.6.3 zusammen mit der Beobachtung, daß für $p \equiv 3 \pmod 4$ stets $p^2 = p^2 + 0^2$ eine Summe zweier Quadrate ist, denn wir haben bereits gesehen, daß das Produkt von zwei Summen zweier Quadrate wieder eine Summe von zwei Quadrate ist.

Wir zeigen nun, daß die genannte Bedingung an n ebenfalls *notwendig* ist. Sei hierzu $n \neq 0$ von der Form $n = x^2 + y^2$. Die Forderung $n > 0$ ist klar, da eine Summe von Quadraten stets nicht-negativ ist und $n \neq 0$ vorausgesetzt wurde. Sei nun p eine Primzahl mit $p \equiv 3 \pmod 4$, welche n teilt und sei e der Exponent von p in der Primfaktorzerlegung von n.

Dann gilt

$$x^2 + y^2 \;=\; n \;\equiv\; 0 \pmod{p^e}.$$

Insbesondere gilt

$$x^2 + y^2 \;\equiv\; 0 \pmod{p}.$$

Wir wissen bereits, daß wegen $p \equiv 3 \pmod 4$ stets $x \equiv 0 \pmod p$ und $y \equiv 0 \pmod p$ gelten muß. Mit anderen Worten, es gilt $p \mid x$ und $p \mid y$. Das zeigt, daß

$$p^2 \mid x^2 \quad \text{und} \quad p^2 \mid y^2.$$

[49] Das bedeutet, daß der Exponent e von p in der Primfaktorzerlegung von n gerade ist für alle $p \equiv 3 \pmod 4$.

Insbesondere teilt p^2 die Zahl n. Damit gilt ebenfalls

$$(x/p)^2 + (y/p)^2 = n/p^2,$$

wobei $\widetilde{x} := x/p$, $\widetilde{y} := y/p$ und $\widetilde{n} := n/p^2$ jeweils ganze Zahlen sind mit

$$\widetilde{x}^2 + \widetilde{y}^2 = \widetilde{n}^2.$$

Wenn $p \nmid \widetilde{n}$, so ist p^2 die größte Potenz von p, welche $n = p^2 \cdot \widetilde{n}$ teilt, sodaß insbesondere $e = 2$ gerade ist.

Wenn $p \mid \widetilde{n}$, mit anderen Worten, wenn $e > 2$, so können wir obiges Argument auf $\widetilde{n}$, $\widetilde{x}$ und $\widetilde{y}$ anwenden und folglich $\widetilde{n}$ erneut durch p^2 teilen.

Wiederholen wir diesen Prozeß, so sehen wir induktiv, daß e gerade sein muß, denn per Induktionshypothese dürfen wir annehmen, daß der Exponent $\widetilde{e}$ von p in $\widetilde{n}$ gerade ist, womit $e = \widetilde{e} + 2$ ebenfalls gerade ist, was zu zeigen war. □

Bemerkung 1.6.9 (Geometrische Interpretation)**.** Analog zu Bemerkung 1.6.4 besitzt Satz 1.6.8 folgende geometrische Interpretation: Zu gegebenem ganzzahligen $n > 0$ liegt genau dann ein ganzahliger Gitterpunkt $(x, y) \in \mathbf{Z}^2$ auf Kreis mit Radius $r = \sqrt{n}$, wenn jede Primzahl $p \mid n$ mit $p \equiv 3 \pmod 4$, in gerader Potenz in n aufgeht.

Bemerkung 1.6.10 (Algebraische Interpretation)**.** Satz 1.6.8 besagt, daß das Bild der Normabbildung $N : \mathbf{Z}[i] \to \mathbf{Z}$ aus 0 und denjenigen natürlichen Zahlen besteht, in welchen Primzahlen p mit $p \equiv 3 \pmod 4$ jeweils in gerader Potenz aufgehen.

Bemerkung 1.6.11 (Algorithmische Interpretation)**.** Satz 1.6.8 zusammen mit der algorithmischen Konstruktion für Primzahlen $p \equiv 1 \pmod 4$ beschert uns folgenden Algorithmus, um ein n, welches den Voraussetzungen des Satzes genügt, als Summe von zwei Quadraten zu schreiben:

(i) Bestimme die Primfaktorisierung $n = p_1^{e_1} \cdots p_r^{e_r}$ von n.

(ii) Bestimme für jede Primzahl p_i mit $p_i = 2$ oder $p_i \equiv 1 \pmod 4$ jeweils $x_i, y_i \in \mathbf{Z}$ mit $x_i^2 + y_i^2 = p_i$.

(iii) Bestimme analog zu Beispiel 1.5.71 mithilfe dieser Darstellungen eine Darstellung

$$\prod_{\substack{i=1 \\ p_i \equiv 1 \pmod 4 \\ \text{oder} \\ p_i = 2}}^{r} p_i^{e_i} = \widetilde{x}^2 + \widetilde{y}^2, \quad \text{mit} \quad \widetilde{x}, \widetilde{y} \in \mathbf{Z}.$$

(iv) Setze

$$z := \prod_{\substack{j=1 \\ p_j \equiv 3 \pmod 4}}^{r} p_j^{e_j/2}.$$

(v) Setze $x := \widetilde{x} \cdot z$ und $y := \widetilde{y} \cdot z$. Dann gilt

$$n = x^2 + y^2.$$

Stichwortverzeichnis