**DIPLOMARBEIT**

# Zahlentheorie im Schulunterricht
# Möglichkeiten und Grenzen

ausgeführt am Institut für
Diskrete Mathematik und Geoinformation
der technischen Universität Wien

unter der Anleitung von: Ao.Univ.Prof. Dipl.-Ing. Dr.techn.
**Johann Wiesenbauer**

durch
**Katharina Czakler**
Adlergasse 23
2120 Wolkersdorf im Weinviertel

21. Mai 2007

# Vorwort

Mathematik ist eine Wissenschaft, die sich über Jahrtausende hin aufgebaut hat und sich noch immer ständig weiterentwickelt. Heutzutage sind alle Gebiete dieser Wissenschaft kaum mehr von einem zu überblicken. Wenn man ein bisschen in der Geschichte der Mathematik blättert, sieht man wie diese Wissenschaft Schritt für Schritt immer neue Erkenntnisse hervorgebracht hat. Oft lag der Nutzen der Forschung auf den verschiedenen Gebieten der Mathematik nicht unmittelbar auf der Hand: Ein Ingenieur der heute einen Elektromotor berechnet, bedient sich mit der größten Selbstverständlichkeit der komplexen Zahlen. Davon konnten Gauß, Euler und alle anderen nichts ahnen, als sie ab Mitte des 18. Jahrhunderts an der Entwicklung dieser Zahlen mitgeholfen haben. Ohne die binäre Zahlendarstellung, die Leibniz entwickelt hat, wären unsere Computer undenkbar. Einstein hätte seine Relativitätstheorie ohne Riemanns Vorarbeiten nicht formulieren können. Die Erforschung der Primzahlen war seit Euklid und Eratosthenes eine Beschäftigung für exzentrische Mathematiker von der niemand hätte angeben können, wozu sie gut sei - bis man in unserer Zeit die Wichtigkeit dieser Zahlen beim Übermitteln geheimer Botschaften erkannte. Es ist also geradezu verblüffend wie "reine" mathematische Modelle, die zunächst als ziemlich weltfremd angesehen wurden, später plötzlich einen gesellschaftlichen Nutzen bringen.

Leider sind für einen großen Teil der Bevölkerung diese Verbindungen nicht durchschaubar, sie sehen nicht, wie sehr unser Alltag von der Mathematik geprägt und durchdrungen ist. Man begegenet dem allgmeinen Vorurteil "Mathematik ist eine Qual, ich bin froh dass ich die Matura geschafft habe", und keiner macht sich die Mühe, sich für mathematische Inhalte und Zusammnenhänge zu interessieren. Hans Magnus Enzensberger stellt vollkommen zu Recht fest: "Wir leben in einer Kultur, die sich durch profundes mathematisches Nichtwissen auszeichnet. Das allgemeine Bewußtsein ist hinter der Forschung um Jahrhunderte zurückgeblieben, ja man kann feststellen, dass große Teile der Bevölkerung über den Stand der griechischen Mathematik nicht hinausgekommen sind" [9]

Sucht man dafür eine Erklärung, so wird man sicher auch auf den Mathematikunterricht in unseren Schulen stoßen, denn dieser Unterricht prägt maßgebend das Bild vieler von dieser Wissenschaft. Je mehr es hier den Lehrern gelingt, Mathematik als lebendiges, modernes, praxisbezogenens Fach zu präsentieren, umso mehr wird sich auch das Bild von der Mathematik als starrer Wissenschaft ändern. Moderne Entwicklungen wie Algorithmen, Codierung, Graphentheorie, Optimierung, RSA, usw. müssen neben den klassischen Gebieten wie die Analysis und die analytische Geometrie, Einzug in den Schulunterricht halten. Die Anwendungs- und Problemorientierung muss anhand moderner Themen wesentlich verstärkt werden. Die Schüler sollen die Fähigkeit erwerben, Fragestellungen aus unterschiedlichen Bereichen sachgerecht zu bearbeiten. Ihnen soll bewußt werden, dass mathematische Denkweisen Anwendung in den meisten Wissenschaften, den unterschiedlichsten Berufen und nicht zuletzt im täglichen Leben finden. Der Unterricht soll Freude an der Beschäftigung mit mathematischen Themen wecken und die Neugier der Schüler erhalten. Die im Mathematikunterricht oft gestellte Frage "Wozu brauchen wir das eigentlich" soll nicht unbeantwortet bleiben. Die Schüler haben ein Recht auf eine Antwort und sollen nicht im Unklaren gelas-

sen werden. Dies rechtfertigt auch das Arbeiten mit vielleicht etwas schwierigeren Aufgaben als es die Schüler gewöhnt sind. Natürlich ist es notwendig mathematische Routinen wie Bruchrechnen, Differenzieren usw. gut mit den Schülern einzüben, aber genau so wichtig ist es, auch immer wieder das mathematische Denken zu trainieren und zu fördern.

Um den Unterricht für die Schüler interessant zu gestalten, ist es auch wichtig die Aktualität der Mathematik nicht außer Acht zu lassen. Die Schüler sollen über die aktuellen Forschungen informiert werden, da besonders diese faszinierend und spannend sein können. Neueste Erkenntnisse der einzelnen Fachgebiete können die Schüler dazu bewegen, sich mehr für Mathematik zu interessieren und sich damit auch mehr auseinanderzusetzen. Nur so wird sich eine aufgeschlossenere, informiertere Haltung zur Mathematik in der Bevölkerung einstellen. In diesem Sinne ist auch meine Arbeit zu verstehen. Ich habe mich entschieden, die Zahlentheorie für den Schüler zugänglich zu machen und den sonst sehr komplizierten Stoff verständlicher und einfacher zu gestalten. Mit dem Ziel in jeder Klasse einen Einblick in die Zahlentheorie zu ermöglichen, behandle ich in dieser Arbeit einige interessante Themen.

Nun möchte ich mich an dieser Stelle bei den Menschen bedanken, die mich ermutigt haben, diese Arbeit zu schreiben und die bei der Fertigstellung beteiligt waren. Zuerst möchte ich mich vor allem bei meinem Vater Mag. Karl Czakler bedanken, der mich in dieser Zeit sehr unterstützt hat. Da er selbst Mathematikprofessor an einem Gymnasium ist, konnte er immer wieder darauf hinweisen, welche Themen und welche Anwendungen in einer Schulklasse überhaupt möglich sind. Mit ihm hatte ich interessante Diskussionen, die das Schreiben an der Arbeit angeregt haben.

Ich bedanke mich auch besonders bei meinem Bruder Johannes Czakler, der mir das Programm Latex beigebracht hat und sich immer wieder Zeit genommen hat, technische Fragen zu beantworten.

Weiters danke ich meiner Familie, die mir den Freiraum gegeben hat mein Studium zu verwirklichen und diese Arbeit zu verfassen. Unentbehrlich war auch die Durchsicht der Fehler der Diplomarbeit von Maria Mechtler.

Abschließend bedanke ich mich bei meinem Betreuer der Diplomarbeit, Ao.Univ.Prof. Dipl.-Ing. Dr.techn. Johann Wiesenbauer, der mir ermöglichte meine Vorstellungen der Diplomarbeit zu verwirklichen und der mir immer wieder mit vielen Informationen und Hinweisen zur Seite gestanden ist.

Wolkersdorf im Weinviertel, im Mai 2007 Katharina Czakler

# Inhaltsverzeichnis

# Kapitel 1

# Einleitung

Durchforstet man den Lehrplan für Mathematik nach zahlentheoretischen Inhalten, so findet man im Lehrplan (Kernbereich) für die Unterstufe:

- Vertiefung der Kenntnisse und Fähigkeiten im Umgang mit natürlichen Zahlen (1. Klasse)
- Anhand von Teilern und Vielfachen Einblicke in Zusammenhänge zwischen natürlicher Zahlen gewinnen (1. Klasse)
- Wichtige Teilbarkeitsregeln kennen und anwenden können (2. Klasse)
- und immer wieder: Vertiefung des Zahlenverständnisses

In der Oberstufe ist nur mehr in der 5. Klasse, wenn mehr als drei Wochenstunden Mathematik angeboten werden, das Arbeiten mit Primzahlen, Teilern und Untersuchungen von Teilbarkeitsfragen obligatorisch.

Zusammenfassend kann man also festhalten: Neben der Förderung des Zahlenverständnisses sind nur Grundbegriffe und Beziehungen der Teilbarkeit als verbindliche Inhalte angeführt. Im Zusammenhang mit dem Bruchrechnen müssen ja die Schüler die Berechnung des $ggT$ und des $kgV$ durchführen können. Ansonsten findet die Zahlentheorie, die Gauß als die "Königin der Mathematik" bezeichnete, kaum Berücksichtigung im Mathematikunterricht. Interessantes gibt es zu entdecken, wenn man ein bisschen zurückblickt: Im Lehrplan für Mathematik aus dem Jahr 1976 ist das Rechnen mit Kongruenzen und Restklassen für das Realgymnasium noch verbindlich vorgeschrieben und auch ausführlich in den entsprechenden Schulbüchern behandelt. In den folgenden Jahren wurden aber diese Kapitel schrittweise immer mehr gekürzt und heute sind sämtliche Ansätze von Algebra und Zahlentheorie praktisch aus dem Schulunterricht wieder verschwunden.

Das ist eigentlich schade, denn ein großer Vorteil der elementaren Zahlentheorie besteht auch darin, dass viele Fragestellungen sehr allgemein verständlich formuliert werden können und somit bei den Schülern sofort auf Interesse stoßen. Außerdem ist etwa zur selben Zeit, als man daran ging das

bisschen Zahlentheorie wieder aus dem Unterricht zu verbannen, das RSA-Verfahren entwickelt worden, welches zum Großteil auf Sätzen der Zahlentheorie beruht, die in der Schule durchaus gebracht werden könnten. Wenn Schüler daher oft den Mathematiklehrer mit der Frage quälen "Wozu braucht man das eigentlich später im Leben", so hätte man gerade hier eine Anwendung des abstrakten Stoffes, welche sie so oft vermissen: Das Verschlüsseln von Nachrichten zum Beispiel mit RSA ist heute aus dem Alltagsleben nicht mehr wegzudenken.

Wenn man nun nach Ausbaumöglichkeiten der Zahlentheorie im Schulunterricht sucht, stellt sich zunächst das zeitliche Problem: Wann habe ich überhaupt die Möglichkeit Zahlentheorie zu betreiben? Im Regelunterricht wird es nur gelingen, wenn ich das ab und zu in einer Stunde "Erweiterungsstoff" mache und altersadäquate zahlentheoretische Fragestellungen behandle. Die ägyptische Multiplikation vorzustellen und ihren Hintergrund zu beleuchten füllt mühelos eine Stunde und ist sicher eine derjenigen Mathematikstunden, die den Schülern in Erinnerung bleiben. Auch ist es durchaus denkbar, einen Teil der einen oder anderen Unterrichtseinheit mit einem zahlentheoretischen Problem aufzulockern und damit das Interesse der Schüler zu wecken. Die motivierenden Beispiele im nächsten Kapitel sind in diesem Sinn gedacht.

Die in dieser Arbeit vorgestellten komplexeren Themen (zum Beispiel: RSA, Primzahltests, usw.) können nur im Rahmen eines Projektunterrichtes, eventuell fächerübergreifend mit Informatik oder Physik oder in einem vertiefenden Wahlpflichtfach Mahematik durchgenommen werden. Sie eignen sich natürlich auch dazu, als Spezialgebiet für die Matura oder im Rahmen einer Fachbereichsarbeit von Schülern mit entsprechender Lehrerunterstützung behandelt zu werden. Damit die Schüler den mathematischen Hintergrund dieser Themen verstehen, ist es dabei sicher notwendig zunächst elementare Grundlagen wie Kongruenzen, oder den Euklidischen Algorithmus bereitzustellen. Um diese Fundamente zu legen muss dem Lehrer klar sein, dass er viel Zeit braucht. Das Versäumnis des Mathematikunterrichts sich überhaupt nicht, beziehungsweise nur marginal der Zahlentheorie zu widmen ist schwer in einem Wahlpflichtfach oder im Rahmen eines Projektes aufzuholen.

Damit haben wir aber auch schon ein inhaltliches Problem angesprochen: Um "ernsthaft" Zahlentheorie zu betreiben, ist es unbedingt notwendig, dass die Schüler über Teilbarkeit, den Euklidischen Algorithmus und über Kongruenzen Bescheid wissen und dass diese Grundlagen auch gut eingeübt sind. Während man bei der Teilbarkeit ein wenig "Starthilfe" aus dem Schulunterricht hat, so wird man bei den beiden anderen Themen praktisch von Null beginnen und alle wesentlichen Begriffe und Sätze zunächst herleiten müssen. Es ist hier sicher ratsam behutsam und langsam vorzugehen. Hat man diese Grundlagen erarbeitet, dann kann man sich den Themen "lineare Kongruenzen", den diophantischen Gleichungen, der RSA-Verschlüsselung usw. widmen und auch immer die entsprechenden mathematischen Grundlagen herleiten.

Mit Rücksicht auf den Umfang der Arbeit wurden die elementaren Sätze und Definitionen in Bezug auf Teilbarkeit und Kongruenzen nur zusammengestellt, auf Beweise wurde verzichtet. Da auch viele Begriffe aus der Algebra, wie Gruppe, Ring, usw. im Regelunterricht nicht mehr vorkommen, wurden diese algebraischen Themen, obwohl sie sich im Zuammenhang mit Restklassen anbieten,

in dieser Arbeit nicht behandelt. Auch habe ich darauf Wert gelegt, bei Formulierungen und Beweisen immer auf Begriffe zurückzugreifen, die Schüler bereits aus dem Regelunterricht kennen.

Zum Abschluss noch ein Wort zum Computereinsatz: Manche Kapitel wie etwa das RSA-Verfahren oder Primzahltests lassen sich ohne Einsatz eines CAS-Systems nicht realistisch behandeln. Aber genau dieser Umstand macht das Thema ja so faszinierend. In Österreichs AHS ist das CAS-System DERIVE aufgrund einer Generallizenz allgemein zugänglich, daher habe ich es auch in dieser Arbeit verwendet. Einfache DERIVE-Befehle wurden selbst erstellt, für komplexere Befehle verweise ich immer auf das Number Theory Utility File (Autor: Johann Wiesenbauer, TU-Wien) von DERIVE das praktisch alle gängigen zahlentheoretischen Funktionen beinhaltet. Das setzt natürlich gewisse Kenntnisse über DERIVE voraus, die man vorher entweder im Mathematik- oder im Informatikunterricht vermittlen muss.

Bevor wir jetzt mit Zahlentheorie loslegen, seien einige Bezeichnungen noch klargestellt:

| | |
|---|---|
| $\mathbb{N} = \{0, 1, 2, 3, 4, \ldots\}$ | Menge der natürlichen Zahlen |
| $\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}$ | Menge der ganzen Zahlen |
| $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ | Menge der Primzahlen |

In dieser Arbeit wird aus Gründen der einfacheren Lesbarkeit auf die sprachliche Differenzierung männlich/weiblich verzichtet. Die in dieser Arbeit gewählte männliche Form steht sinngemäß auch für die weibliche Form.

# Kapitel 2

# Motivation durch Zahlentheorie

Man erweckt immer das Interesse von Schülern wenn man den normalen Regelunterricht unterbricht und irgendein anderes Problem der Mathematik vorstellt. Mit diesen Aufgaben kann man die Freude an der Beschäftigung mit Mathematik wieder neu wecken und unterstützen. Wohlgemerkt diese Aufgaben sollen in keinerlei Weise abgeprüft werden, sondern einfach motivierend wirken. Mit solchen Inhalten erfüllt man sicherlich den im Lehrplan angesprochenen kreativen und gestalterischen Aspekt: "Mathematik besitzt neben der deduktiven auch eine induktive Seite; vor allem das Experimentieren an neuen Aufgabenstellungen und Problemen macht diese Seite sichtbar, bei der Kreativität und Einfallsreichtum gefördert werden." [14]

Hier hat sich gerade auch im Mathematikunterricht in unseren Schulen in den letzten Jahren einiges getan: Am Wettbewerb "Känguru der Mathematik" nehmen immer mehr Schulen teil und auf der TU-Wien finden alljährlich der Denksportwettbewerb für die vierten Klassen, die Jagd auf Zahlen und Figuren und "Yo-Einstein" statt. Bei all diesen Veranstaltungen wird das Verständnis für Mathematik gefördert, die Kinder und Jugendlichen haben Spaß bei der Beschäftigung mit Mathematik und es gelingt auf diese Weise das "verstaubte" Image dieses Faches ein wenig abzubauen.

Kaum ein Kapitel der Mathematik eignet sich besser dafür solche Aufgaben zu finden als die Zahlentheorie. Es sollen hier jetzt einige Aufgaben der Zahlentheorie vorgestellt werden, die man im Unterricht entsprechend der Schulstufe einstreuen kann. Alle diese Aufgaben verlangen kein tieferes Wissen der Zahlentheorie, es genügen die den Schülern bekannten Grundkenntnisse aus dem Unterricht. Die Aufgabenstellungen können in allen Fällen von den Schülern sofort erfasst werden. Die Lösung wird dagegen von den Lernenden eine Auseinandersetzung mit den mathematischen Inhalten, Kreativität, Selbständigkeit und Gewissenhaftigkeit erfordern.

Ich stelle zunächst einige Aufgaben für die Unterstufe (5. - 8. Schulstufe) vor:

## 2.1 Beispiele für die Unterstufe

Zunächst eine Aufgabe, bei der man Schüler der ersten Klasse, vielleicht gleich am Beginn des Jahres, begeistern kann. Da die Schüler in diesem Alter nur die vier Grundrechnungsarten aus der Volksschule kennen und noch nicht mit den Gegebenheiten des Gymnasiums vertraut sind, sind besonders die ersten Mathematikstunden wichtig. Dabei sollte der Lehrer darauf achten, dass er nicht die Motivation für das Lernen zerstört, sondern fördert. Bei dieser Aufgabe lässt man zwei Schüler gegeneinander antreten:

**Beispiel 2.1.1.** Jener Schüler, der beginnt, nennt eine Zahl $a$ mit $1 \leq a \leq 10$. Zu dieser Zahl wird nun abwechselnd eine Zahl größer gleich 1 und kleiner gleich 10 addiert. Wer als erster die Zahl 100 erreicht gewinnt.

Diese Aufgabe (Spiel) erweckt sofort Interesse. Nach ein bis zwei Durchgängen erkennen einige, dass es ausreicht die Zahl 89 zu erreichen und bald hat man die Menge der "Gewinnzahlen"

$$M = \{1, 12, 23, 34, 45, 56, 67, 78, 89, 100\}$$

erarbeitet, also alle Zahlen $x \leq 100$ mit $x \equiv 1 \bmod 11$. Diese Schreibweise verwendet man natürlich nicht in einer ersten Klasse. Sieger ist also jener Schüler, der mit 1 beginnt.

Auch das folgende bekannte Beispiel kann in einer ersten Klasse schon vorgestellt werden:

**Beispiel 2.1.2.** Um die Seitenzahlen eines Buches zu drucken (das Buch beginnt mit der Seite 1), werden insgesamt 3337 Ziffern benötigt. Wie viele Seiten hat das Buch?

Eine Aufgabe, die das Verständnis des Unterschieds zwischen Zahl und Ziffer fördert und die Kenntnisse der Schüler über die natürlichen Zahlen vertieft.

**Lösung:**

| | | |
|---|---|---|
| Seiten 1-9: | 9 Zahlen | 9 Ziffern |
| Seiten 10-99: | 90 Zahlen | 180 Ziffern |
| Seiten 100- 999: | 900 Zahlen | 2700 Ziffern |

Für die ersten 999 Seiten braucht man daher 2889 Ziffern. Alle folgenden Zahlen sind vierstellig, daher liefert die Rechnung $999 + (3337 - 2889) : 4 = 1111$ die gesuchte Seitenanzahl.

□

Ein weiteres motivierendes Beispiel für die Unterstufe verwendet die Primfaktorzerlegung von Zahlen.

**Beispiel 2.1.3.** "How many children have you, and how old are they?" asked the guest, a mathematics teacher. "I have three boys," said Mr. Smith, "The product of their ages is 72 and the sum of their ages is the street number."
The guest went to look at the entrance, came back and said: "The problem is indeterminate."

"Yes, that is so," said Mr. Smith, "but I still hope that the oldest boy will some day win the Stanford competition."
Tell the ages of the boys, stating your reasons.

**Lösung:** Es ist zunächst nicht schwer, für das Alter x,y,z der Knaben folgende Gleichungen herzuleiten

$$x \cdot y \cdot z = 72 \quad \text{und} \quad x + y + z = h,$$

wenn $h$ die Hausnummer bezeichnet. Das Problem besteht darin, nur zwei, eigentlich nur eine Gleichung zu haben mit 3 Unbekannten. Was kann man tun? Man weist sicher darauf hin, dass alle Altersangaben ganzzahlig sind, das heißt $x$, $y$, $z$ natürliche Zahlen sind. Sicher kommt ein Schüler auf die Idee die Primfaktorzerlegung von $72 = 2^3 \cdot 3^2$ zu bestimmen. Jetzt kann man mit den Schülern gemeinsam eine Tabelle mit dem Alter der Knaben und der daraus resultierenden Hausnummer anlegen:

| $x$ | $y$ | $z$ | $h$ |
|---|---|---|---|
| 1 | 2 | 36 | 39 |
| 1 | 3 | 24 | 28 |
| 1 | 6 | 12 | 19 |
| 1 | 8 | 9 | 18 |
| 1 | 4 | 18 | 23 |
| 1 | 1 | 72 | 74 |
| 2 | 2 | 18 | 22 |
| 2 | 4 | 9 | 15 |
| 2 | 3 | 12 | 17 |
| 2 | 6 | 6 | 14 |
| 3 | 3 | 8 | 14 |
| 3 | 4 | 6 | 13 |

Was fällt auf? Man bemerkt, dass nur zwei Zeilen dieselbe Hausnummer liefern und aus der Antwort des Gastgebers auf die letzte Feststellung schließt man auf das Alter der Kinder: 8, 3 und 3 Jahre. Das Beispiel kann beginnend mit der zweiten Klasse (vielleicht dann nicht mit Originaltext) im Unterricht verwendet werden und ist eine nette Anwendung für die Primfaktorzerlegung und für das Lösen von diophantischen Gleichungen.

□

Ein ideales Beispiel um den Unterricht in einer dritten Klasse AHS mit ein bisschen Zahlentheorie aufzulockern und um gleichzeitig auch die Äquivalenzumformungen von Gleichungen zu trainieren ist folgende Aufgabe:

**Beispiel 2.1.4.** 286 Gäste sollen mit Autobussen zu 17 bzw. 19 Plätzen transportiert werden. Wie viele von welchem Typ soll man bestellen, dass alle Plätze in den Bussen besetzt werden?

**Lösung:** Natürlich kommt man bei dieser Aufgabe durch Probieren ans Ziel. Schneller und zielführender ist es aber die lineare diophantische Gleichung $17x + 19y = 286$ zu betrachten. Durch Äquivalenzumformungen kann man sie auf die Form

$$x = 16 - y + \frac{2(7-y)}{17}$$

bringen. Daraus ergibt sich sofort die Lösung $x = 9$ und $y = 7$. Bei dieser Gelegenheit kann man den Schülern ein wenig über lineare diophantische Gleichungen erzählen und vielleicht die Frage diskutieren ob solche Gleichungen immer lösbar sein müssen. Interessierte Schüler kann man mit zusätzlichen einfachen Beispielen versorgen.

□

Beim Einüben der binomischen Formeln kann man folgendes Beispiel an die Tafel schreiben:

**Beispiel 2.1.5.** Betrachte folgende Gleichungen:

$$6^2 - 5^2 = 11$$

$$56^2 - 45^2 = 1111$$

$$556^2 - 445^2 = 111111$$

$$5556^2 - 4445^2 = 11111111$$

Stelle eine allgemeine Vermutung auf und beweise sie.

**Lösung:** Zunächst wird man fragen, wie man die angeschriebenen Gleichungen einfach beweist. Hier wird man auf die binomische Formel $(a-b)(a+b) = a^2 - b^2$ hinweisen und obige Beispiele mit dieser Formel nachrechnen. Die Verallgemeinerung ist dann:

$$(\overbrace{55\cdots5}^{n}6)^2 - (\overbrace{44\cdots4}^{n}5)^2 = (\overbrace{11\cdots1}^{2n+2})$$

Mit Hilfe der binomischen Formel erhält man:

$$(\overbrace{11\cdots1}^{n+1})(1\overbrace{00\cdots0}^{n}1) = (\overbrace{11\cdots1}^{2n+2})$$

Diese Aufgabe ist eine wunderbar zum Schulstoff passende Aufgabe, die das Zahlenverständnis fördert. Außerdem kann man hier den Schülern die sogenannten "Repunits" (repeated units) vorstellen, also Zahlen die nur die Ziffer eins in ihrer Darstellung aufweisen. Wann sind solche Zahlen Primzahlen? Im Falle einer geraden Anzahl von Einsern zeigt uns das Beispiel, dass hier nur 11 eine Primzahl sein kann. Bei der Gelegenheit kann man die Frage "Welche Repunits sind sicher auch keine Primzahlen?" stellen und die Teilbarkeitsregel durch 3 wiederholen. Die Repunits bestehend aus 19 und 23 Ziffern sind ebenfalls Primzahlen.

□

## 2.2 Beispiele für die Oberstufe

Beweise spielen in der Mathematik eine wichtige Rolle, sie verdeutlichen die Exaktheit dieser Wissenschaft. Ein klassisches Beispiel für einen indirekten Beweis, der viele Elemente der Zahlentheorie beinhaltet, darf meines Erachtens im Mathematikunterricht nicht fehlen. Er kann in der 5. Klasse Oberstufe im Zusammenhang mit der Einführung der reellen Zahlen gebracht werden:

**Beispiel 2.2.1.** Zeige: $\sqrt{2}$ ist eine irrationale Zahl.

Wenn man bis zu diesem Zeitpunkt den Schülern noch nicht die Idee des indirekten Beweises vorgestellt hat, so ist diese Aufgabe bestens dazu geeignet. Der Beweis verwendet die Primfaktorzerlegung (von Quadratzahlen) und die Teilbarkeit:

**Beweis:** Annahme: $\sqrt{2}$ ist rational. Dann kann man $\sqrt{2}$ so darstellen:

$$\sqrt{2} = \frac{p}{q} \qquad \text{mit } p, q \in \mathbb{N} \text{ und } ggT(p,q) = 1 \text{ (gekürzter Bruch).}$$

Es folgt nun:

$$\sqrt{2} = \frac{p}{q} \Longleftrightarrow 2 = \frac{p^2}{q^2} \Longleftrightarrow 2q^2 = p^2.$$

Daraus folgt:

$$2 \mid p^2 \Longrightarrow 2 \mid p \Longrightarrow 2k = p \text{ mit } k \in \mathbb{N}$$

Setzt man diese Beziehung in obige Gleichung ein, so erhält man:

$$2q^2 = 4k^2 \text{ also } q^2 = 2k^2$$

Mit derselben Argumentation wie vorher erhält man: $2 \mid q$. Das ist aber ein Widerspruch zur Annahme $ggT(p,q) = 1$.

□

Im Zusammenhang mit dem binomischen Lehrsatz kann man folgendes Beispiel bringen:

**Beispiel 2.2.2.** Zeige, dass 25 die größte Zahl ist, die alle Zahlen der Menge

$$A = \{16^n + 10n - 1 \text{ mit } n = 1, 2, 3, ...\}$$

teilt.

**Lösung:** Die ersten Zahlen der Menge $A$ lauten $25, 275, 4125, \ldots$ was die aufgestellte Behauptung bestätigt. Es gilt nun:

$$16^n = (1+15)^n = \binom{n}{0}1^n + \binom{n}{1}1^{n-1}15 + \binom{n}{2}1^{n-2}15^2 + \binom{n}{3}1^{n-3}15^3 + \cdots = 1 + 15n + 15^2 \cdot k \text{ mit } k \in \mathbb{N}$$

Daraus folgt

$$16^n + 10n - 1 = 1 + 15n + 15^2 \cdot k + 10n - 1 = 25(n + 9 \cdot k)$$

und damit ist alles gezeigt.

□

Ist den Schülern der Begriff Fakultät vertraut, etwa in der 7. Klasse, so kann man folgendes zahlentheoretische Beispiel bringen:

**Beispiel 2.2.3.** Auf wie viele Nullen endet die Zahl 100!?

**Lösung:** Man wird zunächst gezielt folgende Frage stellen: "Wann hat das Produkt zweier natürlicher Zahlen als Einerziffer eine Null?". Mit den Schülern erarbeitet man, dass das genau dann der Fall ist, wenn zumindest einer der beiden Faktoren durch 5 und einer durch 2 teilbar ist. Da in 100! nun aber mehr gerade Zahlen als durch 5 teilbare Zahlen vorkommen, muss man nur die Anzahl der durch 5 teilbaren Zahlen kleiner gleich 100 ermitteln, man hat also sicher bereits $100 : 5 = 20$ Nullen. Hinzu kommen noch Zahlen in denen der Primfaktor 5 zweimal auftritt: 25, 50, 75 und 100. Sie liefern alle eine weitere Null am Ende von 100! und damit endet diese Zahl auf insgesamt 24 Nullen. Man wird mit dem Hinweis schließen, dass 24 der größte Exponent $r$ von 5 ist, sodass $5^r$ ein Teiler von 100! ist.

□

Ausgehend davon kann man folgende Fragen stellen:

"Auf wie viele Nullen endet 1000!, 10000!, 100000!, ..., usw.?"

Hier ergibt sich ein guter Einstieg in das Programmieren von DERIVE. Um die Lösungen zu den Fragen zu finden, gibt es mehrere Möglichkeiten das Problem zu programmieren. Eine einfache Implementierung lautet:

```
Anzahl(n):=MAX(SELECT(MOD(n!,10^i) = 0, i, 1, n))
```

Eine weitere Lösung, welche wesentlich schneller das Ergebnis liefert, ist:

```
Anzahl(n):=
  If n < 5
   0
   FLOOR(n, 5) + Anzahl(FLOOR(n, 5))
```

Nun ist es einfach die Fragen nach der Anzahl der Nullstellen von 100!, 1000! und 10000! zu beantworten.

## 2.2 Beispiele für die Oberstufe

```
Anzahl(100)=24
Anzahl(1000)=249
Anzahl(10000)=2499
```

Sei $n$ irgendeine natürliche Zahl. Gibt es eine Formel für den größten Exponenten $r$ einer Primzahl $p$, so dass $p^r$ teilt $n$? Oder anders ausgedrückt: Wie oft kommt ein Primfaktor $p$ in der Primfaktorzerlegung von $n$ vor?

Es hängt natürlich vom Interesse und von der Leistungsbereitschaft ab, ob es noch einen Sinn ergibt die Formel

$$r = \sum_{k=1}^{n} \left[ \frac{n}{p^k} \right] \qquad ([x]...\text{Gaußklammer})$$

vorzutragen beziehungsweise zu beweisen. Außerdem treten hier mit dem Summenzeichen und der Gaußklammer zwei Notationen auf, die nicht zum alltäglichen Repertoire eines Schülers gehören.

# Kapitel 3

# Verschiedene Algorithmen

## 3.1 “Gelosia” - Methode

Der hier angeführte Algorithmus geht auf eine indische Erfindung aus dem 12. nachchristlichen Jahrhundert zurück und wurde in weiterer Folge im Laufe des 14. und 15. Jahrhunderts nach China und in die arabische Welt exportiert, bis er schließlich im 15. Jahrhundert in Italien angelangt war, wo man ihm wegen der Ähnlichkeit der Rechenfenster mit den Fensterläden in Venedig fortan die Bezeichnung “Gelosia” - Methode gab. Es soll jetzt kurz vorgestellt werden, wie diese Methode funtkioniert: Es seien $z_1 = 10a + b$ und $z_2 = 100c + 10d + e$ zwei Zahlen die ich miteinander multiplizieren will. Ich ordne die Ziffern jetzt folgendermaßen an:

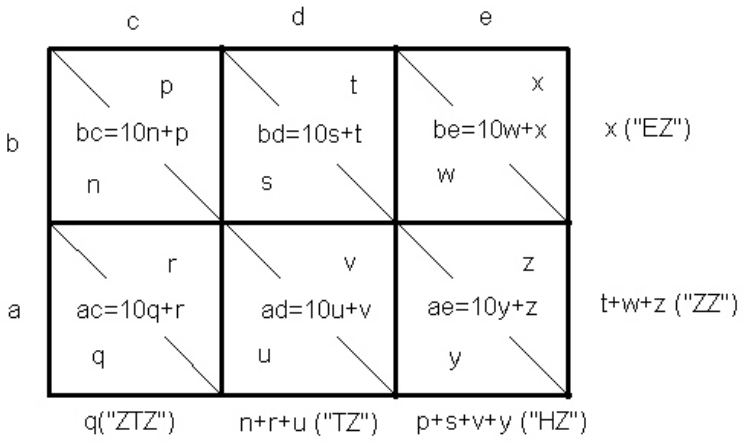


Abbildung 3.1: “Gelosia” - Methode

Also vertikal die Ziffern von $z_1$ und oben horizontal die Ziffern von $z_2$. Die Multiplikation in den sechs Kästchen ergibt zeilenweise von links nach rechts

$$bc = 10n + p, \quad bd = 10s + t, \quad be = 10w + x, \quad ac = 10q + r, \quad ad = 10u + v, \quad ae = 10y + z$$

Trägt man wie in der Abbildung die entsprechende Zehner- bzw. Einerziffer der insgesamt sechs Produkte jeweils links unten bzw. rechts oben ein und addiert dann jeweils die zwischen den Diagonalen liegenden zusammengehörigen Ziffern, so erhält man nacheinander von rechts oben bis links unten im Uhrzeigersinn die Einerziffer $x$, die "Zehnerziffer" $t+w+z$, (noch ohne Übertrag, deshalb die Anführungszeichen vor und nach dem Wort Zehnerziffer), die "Hunderterziffer" $p+s+v+y$, die "Tausenderziffer" $n+r+v$ sowie die "Zehntausenderziffer" $q$, also das Ergebnis

$$z_1 \cdot z_2 = 10000q + 1000(n+r+u) + 100(p+s+v+y) + 10(t+w+z) + x.$$

Der Beweis der Richtigkeit dieser Methode ist nicht schwierig und erfordert nur eine einfache sinnvolle Termumformung:

$$z_1 \cdot z_2 = (10a+b)(100c+10d+e) = 1000ac+100(bc+ad)+10(bd+ac)+be =$$

$$= 1000(10q+r) + 1000(10n+p+10u+v) + 100(10s+t+10y+z) + 10w + x =$$

$$= 10000q + 1000(n+r+u) + 100(p+s+v+y) + 10(t+w+z) + x$$

In der dritten und vierten Klasse kann man die allgemeine dekadische Darstellung einsetzen, in der ersten und zweiten Klasse ist es sicher besser gewählte Beispiele zu verwenden. Auf alle Fälle ist dieser Algorithmus eine willkommene Abwechslung im Mathematikunterricht.

## 3.2 Der Karatsuba - Algorithmus

Diese Methode zur Multiplikation zweier Zahlen wurde 1962 von A. Karatsuba und Y. Ofman veröffentlicht und hat in der Informatik eine große Bedeutung. Bevor man diesen Algorithmus den Schülern erklärt, wird man die Darstellung einer natürlichen Zahl mit Zehnerpotenzen

$$a = a_n 10^n + a_{n-1}10^{n-1} + \cdots + a_2 10^2 + a_1 10^1 + a_0 \qquad 0 \le a_i \le 9,\ a_n \neq 0,\ i = 1,2,\ldots,n$$

wiederholen. In der Schule ist es sicher besser den Algorithmus zunächst für zweistellige Zahlen durchzunehmen, wir wollen jedoch hier gleich die Methode für beliebig lange Zahlen vorstellen:

Wir gehen aus von zwei $2n$-stelligen Zahlen $a$ und $b$ im Dezimalsystem. Durch Voranstellen von ausreichend vielen Nullen kann man immer erreichen, dass $a$ und $b$ genau $2n$ Ziffern haben, wobei $2n$ die kleinste gerade Zahl größer als $a$ und $b$ ist. Wir können nun diese $2n$-stelligen Zahlen $a$ bzw. $b$ in zwei Hälften $p$ und $q$ bzw. $r$ und $s$ teilen und sie daher so anschreiben:

$$a = p \cdot 10^n + q \quad \text{und} \quad b = r \cdot 10^n + s.$$

Als Produkt von $a$ und $b$ erhalten wir

$$ab = pr \cdot 10^{2n} + (ps+qr) \cdot 10^n + qs = pr \cdot 10^{2n} + [pr + qs - (q-p)(s-r)] \cdot 10^n + qs,$$

da $ps + qr = pr + qs - (q-p) \cdot (s-r)$ ist. Es reicht also aus, die drei Produkte

- $u = pr$
- $v = (q - p) \cdot (s - r)$
- $w = qs$

zu berechnen, um das Produkt $ab$ zu erhalten, denn es gilt:

$$ab = u \cdot 10^{2n} + (u + w - v) \cdot 10^n + w \tag{3.1}$$

Man sieht, dass man das Produkt der zwei $2n$-stelligen Zahlen $a$ und $b$ ausrechnen kann, indem man drei Multiplikationen $n$-stelliger Zahlen sowie einige Additionen und Subtraktionen durchführt. Das ist aber auch schon die entscheidende Idee, die hinter dem Karatsuba - Algorithmus steht: Die vorgelegte Aufgabe, zwei $2n$-stellige Zahlen miteinander zu multiplizieren, wird zurückgeführt auf drei Aufgaben der gleichen Art, aber von kleinerer Größe, nämlich, zwei $n$-stellige Zahlen miteinander zu multiplizieren. Auf diese Art kann man das Problem so lange verkleinern, bis es einfach geworden ist. Dieses Prinzip ist in der Informatik sehr wichtig und nennt sich "divide and conquer" (teile und herrsche): Man teilt ein grosses Problem in kleinere Teilprobleme auf. Man führt dieses Verfahren solange rekursiv durch, bis man sehr kleine Zahlen miteinander zu multiplizieren hat, und erhält so eine wesentlich günstigere Laufzeit bei entsprechenden Computerprogrammen als nach der Schulmethode.

Der Algorithmus wird den Schülern rasch klar, wenn man ein Beispiel durchführt.

**Beispiel 3.2.1.** Multipliziere die Zahlen $a = 8823409$ und $b = 234235$ mit dem Karatsuba - Algorithmus.

**Lösung:** Da die Länge der Zahl $a$ nicht gerade ist, wird eine Null vorangestellt. Also: $a = 08823409$. Damit $b$ die selbe Länge hat, werden zwei Nullen vorangestellt: $b = 00234235$. Jetzt werden die Zahlen getrennt:

$$a = 0882 \cdot 10^4 + 3409 \qquad \text{und} \qquad b = 0023 \cdot 10^4 + 4235$$

Man erhält:

$$p = 0882, \;\; q = 3409, \;\; r = 0023 \;\text{ und }\; s = 4235$$

Nun berechnet man die einzelnen Produkte:

- $u = pr = 0882 \cdot 0023 = 00020286$
- $v = (q - p) \cdot (s - r) = 2527 \cdot 4212 = 10643724$
- $w = qs = 14437115$

Zum Abschluss werden die errechneten Produkte noch in die obige “Formel” 3.1 eingesetzt:

$a{\cdot}b = 8823409{\cdot}234235$

$= 00020286 \cdot 10^8 + (00020286 + 14437115 - 10643724) \cdot 10^4 + 14437115 = 2066751207115$

□

## 3.3 Zahlensysteme

Eine interessante Stunde kann es auch sein, wenn man Zahlendarstellungen in anderen Zahlensystemen behandelt. Die Schüler kennen das Stellenwertsystem mit der Basis 10, in dem man mit der Hilfe von nur 10 Ziffern jede Zahl anschreiben kann. Eine natürliche Zahl $a$ kann man infolge des Stellenwertsystems etwa so anschreiben:

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 10^2 + a_1 10^1 + a_0 10^0 \qquad 0 \le a_i \le 9,\ i = 0, 1, 2, \ldots, n$$

Hier wird man noch einmal den Unterschied zwischen Ziffer und Zahl herausarbeiten.

Das lässt sich nun verallgemeinern, indem man statt 10 eine beliebige natürliche Zahl $p > 1$ wählt. Man spricht dann statt von einem Dezimalsystem von einem $p$-adischen System. Jedes solche System besteht aus $p$ Ziffern;

$$\{0, 1, 2, 3, \ldots, p-1\}$$

Die natürliche Zahl $a$ kann man dann so anschreiben:

$$a = c_n p^n + c_{n-1} p^{n-1} + \cdots + c_2 p^2 + c_1 p^1 + c_0 p^0 \qquad 0 \le c_i \le p-1,\ i = 0, 1, 2, \ldots, n$$

Um zu erkennen, welches Zahlenssystem gemeint ist, klammert man die Zahl ein und schreibt rechts tiefgestellt die Basis des Zahlensystems an, also

$$a = (c_n c_{n-1} c_{n-2} \ldots c_1 c_0)_p$$

Zahlen ohne diese Angaben sind stets Dezimalzahlen.

Aus

$$a = p(\cdots p(p(p(c_n p + c_{n-1}) + c_{n-2}) + c_{n-3}) + \cdots + c_1) + c_0$$

folgt sofort der Algorithmus zum Umrechnen der Zahl $a$ vom Dezimalsystem ins $p$-adische System: Man dividiert $a$ durch $p$ und der Rest $c_0$ mit $0 \le c_0 \le p-1$ ist die erste Ziffer in der $p$-adischen Darstellung. Dividiert man den erhaltenen Quotienten wiederum durch $p$, so erhält man mit dem Rest $c_1$ mit $0 \le c_1 \le p-1$ die zweite Ziffer in der $p$-adischen Darstellung. Dieses Verfahren setzt

man fort, bis der erhaltene Quotient kleiner als $p$ ist und somit die letzte Ziffer in der $p$-adischen Entwicklung darstellt. Mit

$$43 : 3 = 14 \text{ Rest: } 1, \quad 14 : 3 = 4 \text{ Rest: } 2, \quad 4 : 3 = 1 \text{ Rest: } 1,$$

erhält man

$$43 = (1121)_3$$

In der Praxis bedeutsam sind vor allem zwei andere Systeme, nämlich das auf G.W. Leibniz (1646 - 1716) zurückgehende Dualsystem mit der Basis $p = 2$ und das Hexadezimalsystem mit der Basis $p = 16$. Beide werden heute in der Informatik benützt. Da man für das Hexadezimalsystem 16 Ziffern benötigt, verwendet man die Buchstaben $A$, $B$, $C$, $D$, $E$, $F$ als Ziffern für "10" bis "15".

Vom Dualsystem lässt sich sehr schnell (ohne Umweg über das Dezimalsystem) ins Hexadezimalsystem umrechnen und umgekehrt:

Wegen $16 = (10000)_2$, $A = 10 = (1010)_2$ und $B = 11 = (1011)_2$ gilt zum Beispiel:

$$(AB3)_{16} = A \cdot 16^2 + B \cdot 16^1 + 3 \cdot 16^0 = A \cdot 100000000 + B \cdot 10000 + 3 = (\overbrace{1011}^{A}\,\overbrace{1011}^{B}\,\overbrace{0011}^{3})_2.$$

Man braucht also nur auf die entsprechende Unterteilung in "Vierergruppen" achten und gegebenenfalls mit Nullen ergänzen.

In den anderen Zahlensystemen kann man wie im Dezimalsystem rechnen, wenn man das "Kleine 1 und 1" sowie das "Kleine 1 mal 1" kennt. Man kann die Schüler diese Tabellen für das Dualsystem und etwa für das System zur Basis 3 und 4 aufschreiben lassen. Mit vielen Beispielen kann man dann das Rechnen in anderen Zahlensystemen einüben und die Ergebnisse durch Übergang zum Dezimalsystem kontrollieren.

Mit DERIVE lassen sich die Zahlen in eine beliebige Zahlendarstellungen folgendermaßen umrechnen (Autor: J. Wiesenbauer):

```
convert(n, b:=2, k:=0, s_:="", t_) :=
  Loop
   If k ≤ 0 ∧ n = 0
    RETURN s_
   t_ := MOD(n, b) + 48
   s_ := ADJOIN(CODES_TO_NAME(t_ + 7·IF(t_ > 57)), s_)
   n := FLOOR(n, b)
   k :- 1
```

Um das Ergebnis von der gewählten Zahlendarstellung wieder in die Dezimaldarstellung umzurechnen, wendet man folgenden Befehl an:

```
todec(h, b:=2, s_:=0, t_) :=
  Loop
   If h = ""
    RETURN s_
   t_ := FIRST(NAME_TO_CODES(FIRST(h)))
   t_ := IF(t_ < 65, t_ - 48, MOD(t_, 32) + 9)
   s_ := b·s_ + t_
   h := REST(h)
```

Anhand eines Beispiels werden sich die Schüler schnell an den Umgang mit den Zahlendarstellungen gewöhnen.

```
convert(234523, 7)=1664512
convert(28345, 20)=3AH5

todec("1664512", 7) = 234523
todec("3AH5", 20) = 28345
```

Schließlich kann man den Schülern auch noch die NAF- Darstellung (non-adjacent-form) einer Zahl vorstellen, die erst im Jahr 1960 von Reitwiesner entwickelt wurde. Das ist eine binäre Darstellung einer Zahl $n$, wobei man die Ziffern $1, 0$ und $-1$ verwendet und festsetzt, dass zwei benachbarte Ziffern niemals beide verschieden von 0 sind.

Das kann man auch so anschreiben:

Sei $n$ eine natürliche Zahl. Ist

$$n = \sum_{i=0}^{m} d_i 2^i \text{ mit } d_i \in \{-1, 0, 1\} \text{ und } d_1 \cdot d_{i+1} = 0, \ \forall i$$

dann heißt

$$(d_m d_{m-1} \dots d_2 d_1 d_0)$$

die NAF-Darstellung der Zahl $n$, wobei $d_m = 1$ und $d_{m-1} = 0$ sein muss.

Reitwiesner bewies, dass die NAF-Darstellung einer natürlichen Zahl eindeutig ist. Diese Darstellung hat den Vorteil, dass durchschnittlich mehr als zwei Drittel der Ziffern gleich 0 sind, was zum Beispiel ein schnelleres Multiplizieren ermöglicht. Ein weiterer Vorteil ist die Anwendung der NAF-Darstellung in der Kryptographie, da sie gegenüber einer "Power monitoring attack" resistenter ist. Diese Attacke benutzt den Unterschied eines Stromverbrauchs einer Festplatte während

eines Rechenvorgangs. Man kann nämlich bei einer Strommessung nicht zwischen einer 1 und einer $-1$ unterscheiden, jedoch zwischen einer 1 und einer 0 schon.

Wie kommt man nun zu einer NAF-Darstellung einer Zahl $n$? Hier kann man die Schüler sicher selbst ein wenig forschen lassen und sie werden bald erkennen, dass man sie am besten aus der Binärdarstellung dieser Zahl berechnet. Vielleicht kann man mit ihnen folgende Methode zum Umwandeln erarbeiten:

Zunächst stellt man folgendes fest:

- $3 = (11)_2 = (10 - 1)$
- $7 = (111)_2 = (100 - 1)$
- $\cdots\cdots\cdots$
- $2^n - 1 = (\overbrace{111\cdots1}^{n})_2 = (\overbrace{100\cdots00}^{n+1} - 1)$

Mit Hilfe dieser Umwandlungen kann man nun schrittweise eine Zahl vom Binärsystem in eine NAF-Form verwandeln. Dabei beginnt man immer von "hinten" und wandelt zunächst die erste Kette aufeinanderfolgender Einsern in die entsprechende NAF-Form um. Wir demonstrieren es anhand der Zahl 87:

$$87 = (1010111)_2 = (101100 - 1), \text{ denn } (111)_2 = (100 - 1)$$

Damit haben wir natürlich noch nicht die NAF-Darstellung von 87 gewonnen, denn es stehen zwei Einsern nebeneinander. Wir verwenden nun zweimal $3 = (11)_2 = (10 - 1)$ und erhalten

$$87 = (1010111)_2 = (101100 - 1) = (110 - 100 - 1) = (10 - 10 - 100 - 1)$$

und haben damit die NAF-Form von $87 = (10 - 10 - 100 - 1) = 2^7 - 2^5 - 2^3 - 2^0$ gewonnen.

Einige weitere Beispiele:

$$23 = (10111)_2 = (10 - 1001)$$

$$59 = (111011)_2 = (1000 - 10 - 1)$$

$$234 = (11101010)_2 = (100 - 101010)$$

Mit den NAF-Formen kann man wie mit den Zahlen in anderen Zahlensystemen rechnen. Das "Kleine 1 und 1" und das "Kleine 1 mal 1" sind dabei sehr kurz:

| + | −1 | 0 | 1 |
|---|---|---|---|
| −1 | −10 | −1 | 0 |
| 0 | −1 | 0 | 1 |
| 1 | 0 | 1 | 10 |

| · | −1 | 0 | 1 |
|---|---|---|---|
| −1 | 1 | 0 | −1 |
| 0 | 0 | 0 | 0 |
| 1 | −1 | 0 | 1 |

Tabelle 3.1: Rechnen in der NAF-Darstellung

Mit dem DERIVE Programm NAF($n$) (Autor: Johann Wiesenbauer) kann man die NAF-Form einer Zahl $n$ berechnen:

```
NAF(n, s_:=[ ]) :=
  Loop
   If n = 0
    RETURN s_
   Loop
    If ODD?(n) exit
    n :/ 2
    s_:=ADJOIN(0, s_)
   If MOD(n, 4) = 1
    Prog
     n:=FLOOR(n, 2)
     s_:=ADJOIN(1, s_)
   If MOD(n, 4) = 3
    Prog
     s_:=ADJOIN(-1, s_)
     n:=FLOOR(n, 2)
     Loop
      s_:=ADJOIN(0, s_)
      n:=FLOOR(n, 2)
      If EVEN?(n) exit
     n :+ 1
```

## 3.4 Die Ägyptische Multiplikation

Die ägyptische Multiplikation ist einer der ältesten Algorithmen und wird verwendet zum Multiplizieren zweier natürlicher Zahlen. Dokumentiert wurde dieser Algorithmus im Papyrus Rhind ca. 1650 - 1850 vor Christus. Der Papyrus Rhind ist eine der wichtigsten Quellen für unser Wissen über die Mathematik der Ägypter. Der Papyrus wurde benannt nach dem Schotten Alexander Henry Rhind, der ihn 1858 in Luxor entdeckte.

Die Vorschrift lautet: Der Multiplikand wird ständig verdoppelt, der Multipliklator wird - unter Vernachlässigung des eventuell auftretenden Restes 1 - ständig halbiert und zwar solange, bis in der rechten Spalte 1 steht. Aufsummiert werden alle diejenigen Vielfachen des Multiplikanden in der linken Spalte, bei denen in der rechten Spalte eine ungerade Zahl steht, also alle jene, bei denen der Rest 1 vernachlässigt wurde. Sinnvollerweise streicht man vorher alle jene Zeilen, wo rechts eine gerade Zahl steht.

Gleich hier bringt man das Beispiel einer ägyptischen Multiplikation:

| | | |
|---|---|---|
| 11 | 23 | |
| 5 | 46 | |
| ~~2~~ | ~~92~~ | gestrichen |
| 1 | 184 | |
| | 253 | Ergebnis |

Tabelle 3.2: Die ägyptische Multiplikation anhand eines Beispiels

Will man einen Beweis (Begründung) dafür angeben, so wird man je nach Schulstufe verschieden vorgehen. Stellt man die ägyptische Multiplikation in einer ersten oder zweiten Klasse vor, so wird man unter Verwendung des Distributivgesetzes das Beispiel einfach nachrechnen:

$$23 \cdot 11 = 23 \cdot (10+1) = 23 \cdot 10 + 23 = 46 \cdot 5 + 23 = 46 \cdot (4+1) + 23 = 46 \cdot 4 + 46 + 23 =$$

$$= 92 \cdot (2) + 46 + 23 = 184 \cdot 1 + 46 + 23 = 253$$

Führt man so einige Beispiele aus, wird das Prinzip den Schülern hier rasch klar und man hat außerdem eine sinnvolle Anwendung zum Einüben der Rechengesetze. Es genügt aber durchaus in diesen Klassen den Algorithmus vorzustellen und einige Multiplikationen “ägyptisch” und zur Probe “normal” durchzuführen - ein gutes Training der Grundrechnungsarten.

Ist man ab der vierten Klasse mit der Algebra schon mehr vertraut, so kann man folgende Beziehungen anschreiben:

### 3.4 Die Ägyptische Multiplikation

$a \cdot 1 = a$

$a \cdot b = 2a \cdot \frac{b}{2}$, wenn b gerade ist.

$a \cdot b = a + 2a \cdot \left(\frac{b-1}{2}\right)$, wenn b ungerade ist und b ungleich 1

In der letzten Zeile steht eigentlich das Geheimnis dieser ägyptischen Multiplikation: Wenn $b$ ungerade ist, muss man $a$ zum Produkt der in der nächsten Zeile stehenden Faktoren addieren um das Produkt $a \cdot b$ der vorhergehenden Zeile zu erhalten. Umgekehrt, wenn $b$ gerade ist, ändert sich der Wert des Produktes von einer Zeile auf die nächste nicht. In einer höheren Klasse kann man hier, wenn man sich ausführlich mit diesem Algorithmus beschäftigt, einen strengen Induktionsbeweis angeben. Überraschend für die Schüler ist, dass man bei diesem Thema den Zusammenhang mit der Informatik herstellen kann. Hat man die Binärdarstellung der natürlichen Zahlen zur Verfügung, so kann man die ägyptische Multiplikation auch so anschreiben:

| 1011 | 10111 | |
|---|---|---|
| 101 | 101110 | |
| ~~10~~ | ~~1011100~~ | gestrichen |
| 1 | 10111000 | |
| | 1111101 | Ergebnis |

Tabelle 3.3: ägyptischen Multiplikation mit binären Zahlen

Die ganzahlige Division durch 2, also die Vernachlässigung eines eventuell auftretenden Restes, bedeutet die letzte Stelle (das letzte Bit) einfach wegzunehmen, die Multiplikation mit 2 bedeutet 0 anzuhängen. Daraus resultiert auch ihre Bedeutung für die Informatik. Streicht man nun wieder jene Zeilen, wo in der Binärdarstellung in der linken Spalte die Ziffer 0 steht (gerade Zahlen), so hat man in der rechten Spalte nichts anderes als die ausgeführte Multiplikation von $10111 \cdot 1011$. Dies kann man leicht vergleichen:

| 10111 | $\cdot$ 1011 |
|---|---|
| 10111000 | |
| 00000000 | |
| 00101110 | |
| 00010111 | |
| 11111101 | |

Tabelle 3.4: Multiplikation von binären Zahlen

## 3.5 Teilbarkeit und Euklidischer Algorithmus

Die Teilbarkeit ist der erste Schritt zur Zahlentheorie. In der zweiten Klasse Unterstufe werden den Schülern wichtige Teilbarkeitsregeln mitgeteilt und anhand von Beispielen begründet. Die Summen- und Produktregel, die Teilbarkeitsregeln für das Teilen durch besondere Zahlen aber auch der $ggT$ und das $kgV$ werden im Schulunterricht mittels Primfaktorzerlegung ermittelt. Hier werden also zumindest einige Grundbegriffe erklärt, auf die man bei der Beschäftigung mit Zahlentheorie zurückgreifen kann. Da man eine ohnehin sicher knapp bemessenen Zeit für Zahlentheorie in der Schule zur Verfügung hat, wird man sicher nicht langwierig zunächst das Kapitel Teilbarkeit behandeln. Die entsprechenden Definition und Regeln wird man immer nur dann bringen und begründen, wenn man sie braucht. Noch dazu, wo viele dieser Regeln den Schülern unmittelbar einsichtig erscheinen. Es sei jetzt hier ganz kurz das Wichtigste über Teilbarkeit ohne Beweise zusammengestellt:

**Definition 3.5.1.** Es seien $a$ und $b$ ganze Zahlen. Man sagt: $a$ teilt $b$, wenn es eine ganze Zahl $q$ gibt, sodass $a \cdot q = b$ und schreibt dafür $a \mid b$.

**Satz 3.1.**
Für alle ganzen Zahlen $a, b, c, d \in \mathbb{Z}$ gilt:

- $\pm 1, \pm a$ sind stets Teiler von a (die sog. unechten oder trivialen Teiler von a)
- $a \mid 0$
- $a \mid b$ und $b \mid c \Longrightarrow a \mid c$
- $a \mid b \Longleftrightarrow ac \mid bc$ mit $c \neq 0$
- $a \mid b$ und $a \mid c \Longrightarrow a \mid (xb + yc)$ für $x, y \in \mathbb{Z}$
- $a \mid b$ und $c \mid d \Longrightarrow ac \mid bd$
- $a \mid b$ und $b \neq 0 \Longrightarrow \mid a \mid \leq \mid b \mid$
- $a \mid b$ und $b \mid a \Longrightarrow a = \pm b$

**Satz 3.2.**
Sei $a$ eine ganze Zahl und $b$ eine positive ganze Zahl. Dann existiert genau ein Paar von ganzen Zahlen $(q, r)$, sodass $0 \leq r < b$ und $a = b \cdot q + r$ gilt.

Dieser Satz erscheint den Schülern unmittelbar einsichtig, obwohl er nicht ganz so trivial ist. Es genügt aber sicher, wenn man im Zusammenhang mit dem Euklidischen Algorithmus nur auf diesen Satz hinweist.

**Definition 3.5.2.** Es seien $a$ und $b$ ganze Zahlen. Die Zahl $c$ heißt gemeinsamer Teiler von $a$ und $b$ wenn $c \mid a$ und $c \mid b$.

**Definition 3.5.3.** Die größte ganze Zahl, die gemeinsamer Teiler von $a$ und $b$ ist, nennt man größter gemeinsamer Teiler von $a$ und $b$ und schreibt ggT(a,b).

**Definition 3.5.4.** Ganze Zahlen $a$ und $b$, für die $ggT(a, b) = 1$ gilt, heißen teilerfremd oder relativ prim.

In der Schule wird der größte gemeinsame Teiler über die Primfaktorzerlegung der beiden Zahlen $a$ und $b$ berechnet. In der Zahlentheorie erweist sich aber eine andere Methode als zweckmäßig um den $ggT$ zweier ganzer Zahlen $a$ und $b$ zu berechnen: Der Euklidische Algorithmus, den Euklid bereits in seinen "Elementen" als Möglichkeit zur Berechnung des $ggT$ beschreibt. Hat man in einem Wahlpflichtfach vor, mehr Zahlentheorie zu machen, dann ist es unbedingt notwendig, diesen Algorithmus eingehender zu behandeln.
Zunächst kann man folgendes festhalten: Wegen

$$\text{ggT(a,b)} = \text{ggT(b,a)},\ ggT(a, 0) = \mid a \mid \text{ und } ggT(a, b) = ggT(\mid a \mid, \mid b \mid)$$

genügt es im Folgenden den Fall $a \geq b > 0$ zu betrachten.

Um nun den größten gemeinsamen Teiler von $a \geq b > 0$ zu berechnen, gehen wir folgendermaßen vor:

$$\begin{array}{ll} a = bq_1 + r_1 & 0 < r_1 < b \\ b = r_1q_2 + r_2 & 0 < r_2 < r_1 \\ r_1 = r_2q_3 + r_3 & 0 < r_3 < r_2 \\ \ldots\ldots & \ldots \end{array}$$

Wir erhalten dadurch eine monotone abnehmende Folge positiver Zahlen:

$$b > r_1 > r_2 > r_3 > \ldots$$

Diese kann also nur endlich viele Glieder enthalten. Das Verfahren bricht also nach endlich vielen Schritten ab. Dies kann aber nur dann der Fall sein, wenn der Rest 0 auftritt, denn sonst ergibt sich stets ein neuer Schritt in diesem Verfahren. Die drei letzten Zeilen sehen so aus:

$$\begin{aligned} r_{n-3} &= r_{n-2}q_{n-1} + r_{n-1} & 0 < r_{n-1} < r_{n-2} \\ r_{n-2} &= r_{n-1}q_n + r_n & 0 < r_n < r_{n-1} \\ r_{n-1} &= r_n q_{n+1} \end{aligned}$$

Wir setzen nun $d = r_n$, dann gilt:

$$d > 0, \qquad d \mid r_{n-1} \Rightarrow d \mid r_{n-2} \Rightarrow d \mid r_{n-3} \Rightarrow \ldots \Rightarrow d \mid b \Rightarrow d \mid a \Rightarrow d \mid a \text{ und } d \mid b$$

Es sei $t$ eine weiterer Teiler von $a$ und $b$. Aus $t \mid a$ und $t \mid b$ folgt

$$t \mid r_1 \Rightarrow t \mid r_2 \Rightarrow t \mid r_3 \Rightarrow \ldots \Rightarrow t \mid r_n \Rightarrow t \mid d.$$

Die Zahl $d$ ist also die größte natürliche Zahl, die a und b teilt, also $d = ggT(a, b)$.

Dieses Verfahren ist zugleich Existenzbeweis, Eindeutigkeitsbeweis und Berechnungsmethode.

Ein Beispiel dazu:

**Beispiel 3.5.1.** Berechne den $ggT$ von 8991 und 3293:

**Lösung:**

$$\begin{aligned} 8991 &= 3293 \cdot 2 + 2405 \\ 3293 &= 2405 \cdot 1 + 888 \\ 2405 &= 888 \cdot 2 + 629 \\ 888 &= 629 \cdot 1 + 259 \\ 629 &= 259 \cdot 2 + 111 \\ 259 &= 111 \cdot 2 + 37 \\ 111 &= 37 \cdot 3 \end{aligned}$$

Also: $ggT(8991, 3293) = 37$

□

Man kann bei der Durchführung des Euklidischen Algorithmus einfach zusätzliche Informationen herausholen, die sich später als sehr nützlich erweisen werden. Wir demonstrieren das gleich anhand dieses Beispiels. Wir schreiben den Euklidischen Algorithmus etwas anders an:

| $r_i$ | | $x_i$ | | | $y_i$ | | | $q_i$ |
|---|---|---|---|---|---|---|---|---|
| 8991 | = | 1 | ·8991 | + | 0 | ·3293 | | |
| 3293 | = | 0 | ·8991 | + | 1 | ·3293 | \| | ·2 |
| 2405 | = | 1 | ·8991 | − | 2 | ·3293 | \| | ·1 |
| 888 | = | −1 | ·8991 | + | 3 | ·3293 | \| | ·2 |
| 629 | = | 3 | ·8991 | − | 8 | ·3293 | \| | ·1 |
| 259 | = | −4 | ·8991 | + | 11 | ·3293 | \| | ·2 |
| 111 | = | 11 | ·8991 | − | 30 | ·3293 | \| | ·2 |
| 37 | = | −26 | ·8991 | + | 71 | ·3293 | \| | ·3 |
| 0 | | | | | | | | |

Man multipliziert immer mit dem entsprechenden $q_i$ (vergleiche oben mit dem Euklidischen Algorithmus) und subtrahiert die entstehende Gleichung von der vorhergehenden. Man führt also auf der linken Seite den Euklidischen Algorithmus aus, während rechts immer eine Linearkombination von $a$ (8991) und $b$ (3293) steht. Das kommt den Schülern vom Lösen zweier linearer Gleichungen bekannt vor, sie müssen sich nur den etwas trickreichen Ansatz der ersten und der zweiten Zeile merken. Welche zusätzliche Information hat man nun mit diesem "erweiterten Euklidischen Algorithmus" gewonnen? Wir haben $37 = ggT(8991, 3293)$ als Linearkombination von 8991 und 3293 dargestellt, denn es gilt:

$$37 = -26 \cdot 8991 + 71 \cdot 3293$$

Allgmein kann man das so interpretieren: In der Spalte $r_i$ steht genau die monoton abnehmende Folge positiver Zahlen

$$a > b > r_1 > r_2 > r_3 > \dots$$

des Euklidischen Algorithmus von oben. Der Vollständigkeit halber setzt man $r_{-1} = a$ und $r_0 = b$. Die Folge muss igendwann abrechen, das heißt es tritt der Rest 0 auf. Jede diese Zahlen $r_i$ lässt sich als Linearkombination von $a$ und $b$ darstellen, wobei die Zahlen in den Spalten $x_i$ und $y_i$ die jeweiligen Koeffizienten angeben. Hier ist sicher der Hinweis notwendig, dass die Summe zweier Linearkombinationen von $a$ und $b$ wieder eine Linearkombination von $a$ und $b$ ergibt. Daher gibt es auch für die letzte Zeile $d = r_n$, das ist nach dem oben Bewiesenen der $ggT$ von $a$ und $b$, so eine Darstellung. Wir können daher folgenden Satz aussprechen:

**Satz 3.3.**
Gilt $d = ggT(a, b)$, so gibt es zwei ganze Zahlen $x$ und $y$, sodass gilt:

$$d = ax + by \tag{3.2}$$

Bemerkung: Auf die rekursive Definition der Folgen $r_i$, $x_i$ und $y_i$ wird man im Unterricht nicht eingehen. Es ist vollkommen ausreichend, wenn die Schüler mit diesem Algorithmus rechnen können, ihn verstehen und wissen, was er leistet.

Dieses Verfahren, das auch auch unter den Namen Berlekamp - Algorithmus bekannt ist, kann man noch weiter formalisieren, wie in der folgenden Tabelle zu sehen ist:

| $r_i$ | $x_i$ | $y_i$ | $q_i$ |
|---|---|---|---|
| 8991 | 1 | 0 | |
| 3293 | 0 | 1 | 2 |
| 2405 | 1 | −2 | 1 |
| 888 | −1 | 3 | 2 |
| 629 | 3 | −8 | 1 |
| 259 | −4 | 11 | 2 |
| 111 | 11 | −30 | 2 |
| 37 | −26 | 71 | 3 |
| 0 | | | |

Tabelle 3.5: Der Berlekamp - Algortihmus

Wie kann man den $ggT$ von zwei Zahlen mit DERIVE berechnen?

Bevor man daran geht hier einen Befehl zu schreiben, wird man noch folgenden Satz bringen:

**Satz 3.4.**
Es seien $a$ und $b$ ganze Zahlen. Für alle ganzen Zahlen gilt:

$$ggT(a,b) = ggT(b, a - bk)$$

**Beweis:** Es sei $r = a - bk$, $d_1 = ggT(a,b)$ und $d_2 = ggT(b,r)$.

Da $d_1 \mid a$ und $d_1 \mid bk$, gilt $d_1 \mid r = a - bk$. Da $d_1$ gemeinsamer Teiler von $b$ und $r$ ist, aber $d_2$ der größte gemeinsame Teiler von $b$ und $r$ ist, gilt:

$$d_2 \geq d_1$$

Umgekehrt folgt aber aus $a = bk + r$ analog zu oben $d_2 \mid a$ und daher ist $d_2$ gemeinsamer Teiler von $a$ und $b$. Da aber $d_1$ der größte gemeinsame Teiler von $a$ und $b$ ist, gilt folglich:

$$d_2 \leq d_1$$

Zusammenfassend haben wir $d_1 = d_2$ und damit ist der Satz bewiesen.

□

Diesen Satz kann man nun verwenden um einen DERIVE Befehl für den $ggT(a,b)$ zu schreiben:

```
GGT1(a, b) := IF(b = 0, a, GGT1(b, ABS(a - b)))
```

oder besser:

```
GGT2(a, b) := IF(b = 0, a, GGT2(b, MOD(a, b)))
```

Die vorprogrammierte Funktion GCD($a_1, a_2, \ldots, a_n$) berechnet ebenfalls den größten gemeinsamen Teiler der Zahlen $a_1, a_2, \ldots, a_n$.

Der Euklidische Algorithmus ist durch ein Programm von J. Wiesenbauer gut ersichtlich, da jeder Schritt des Algorithmus gezeigt wird.

```
euclid(a, b, q_, r_, s_:=[ ], t_) :=
  Loop
   If b = 0
    RETURN REVERSE(s_)
   q_ := FLOOR(a, b)
   r_ := MOD(a, b)
   If r_ = 0
    t_ := [a, "=", q_, "·", b, "", ""]
    t_ := [a, "=", q_, "·", b, "+", r_]
   s_ := ADJOIN(t_, s_)
   a := b
   b := r_
```

Um es an einem einfachen Beispiel zu zeigen, wollen wir den größten gemeinsamen Teiler von 12345 und 6543 berechnen.

```
euclid(12345,6543)
```

$$\begin{bmatrix} 12345 = 1 \cdot 6543 + 5802 \\ 6543 = 1 \cdot 5802 + 741 \\ 5802 = 7 \cdot 741 + 615 \\ 741 = 1 \cdot 615 + 126 \\ 615 = 4 \cdot 126 + 111 \\ 126 = 1 \cdot 111 + 15 \\ 111 = 7 \cdot 15 + 6 \\ 15 = 2 \cdot 6 + 3 \\ 6 = 2 \cdot 3 \end{bmatrix}$$

Um den erweiterten Euklidischen Algorithmus in DERIVE zu berechnen, kann man auch folgenden Befehl eingeben. Dieser ermöglicht eine genaue Auflistung der einzelnen Linearkombinationen.

```
eea(a, b, q_, r_, s_:=[ ]) :=
  Prog
   a := [a, [1, 0]]
   b := [b, [0, 1]]
   Loop
    If FIRST(b) = 0
     RETURN REVERSE(s_)
    s_ := ADJOIN([FIRST(a), FIRST(b), FIRST(REST(a)), FIRST(REST(b))], s_)
    q_ := FLOOR(FIRST(a), FIRST(b))
    r_ := a - q_·b
    a := b
    b := r_
```

An einem Beispiel ist nun für die Schüler gut ersichtlich, wie der erweiterte Euklidische Algorithmus funktioniert.

```
eea(2345234,6455243)
```

| | | | |
|---|---|---|---|
| 2345234 | 6455243 | [1, 0] | [0, 1] |
| 6455243 | 2345234 | [0, 1] | [1, 0] |
| 2345234 | 1764775 | [1, 0] | [-2, 1] |
| 1764775 | 580459 | [-2, 1] | [3, -1] |
| 580459 | 23398 | [3, -1] | [-11, 4] |
| 23398 | 18907 | [-11, 4] | [267, -97] |
| 18907 | 4491 | [267, -97] | [-278, 101] |
| 4491 | 943 | [-278, 101] | [1379, -501] |
| 943 | 719 | [1379, -501] | [-5794, 2105] |
| 719 | 224 | [-5794, 2105] | [7173, -2606] |
| 224 | 47 | [7173, -2606] | [-27313, 9923] |
| 47 | 36 | [-27313, 9923] | [116425, -42298] |
| 36 | 11 | [116425, -42298] | [-143738, 52221] |
| 11 | 3 | [-143738, 52221] | [547639, -198961] |
| 3 | 2 | [547639, -198961] | [-1786655, 649104] |
| 2 | 1 | [-1786655, 649104] | [2334294, -848065] |

In unserem Beispiel ergeben sich in der 5. Zeile also folgende Linearkombinationen:

$$3 \cdot 2345234 - 1 \cdot 6455243 = 580459$$

$$-11 \cdot 2345234 + 4 \cdot 6455243 = 23398$$

# Kapitel 4

# Primzahlen

## 4.1 Grundlegendes

Die Primzahlen und ihre faszinierenden Eigenschaften haben zu allen Zeiten Mathematiker in ihren Bann gezogen. Namen wie Fermat, Euler, Lagrange, Legendre, Gauß, usw. lassen sich hier als Beispiel anführen. Das Studium der Primzahlen ist, wenn man so will, das Kernstück der Zahlentheorie. Eine Fülle von Gesetzmäßigkeiten wurde im Laufe der Jahrhunderte entdeckt und der Themenkomplex Primzahlen bietet genug Material um die eine oder andere interessante Unterrichtseinheit zu gestalten. Die Begriffe Primzahl, Sieb des Eratosthenes und der Fundamentalsatz der Zahlentheorie findet man noch in jedem besseren Lehrbuch für Mathematik.

Der Fundamentalsatz der Zahlentheorie lautet:

**Satz 4.1.**
Jede natürliche Zahl $a > 0$ ist als Produkt endlich vieler Primzahlen darstellbar. Diese Darstellung ist eindeutig, wenn man die in ihr vorkommenden Primzahlen der Größe nach ordnet.

In einem Wahlpflichtfach mit Schwerpunkt "Primzahlen" kann man durchaus den exakten Beweis dafür bringen. Jedoch kann man auf einen Beweis des Fundamentalsatzes im Normalunterricht verzichten, da der Inhalt dieses Satzes den Schülern sowieso evident erscheint und man mit einem strengen Beweis die Schüler eher demotiviert. Hingegen sollte man in diesem Zusammenhang unbedingt auf drei Dinge hinweisen:

- Die Primzahlen sind die multiplikativen Bausteine der natürlichen Zahlen.
- Würde man 1 zu den Primfaktoren zählen, so wäre der obige Satz falsch, da man zur Primfaktorzerlegung einer natürlichen Zahl stets beliebig viele Faktoren 1 dazuschreiben könnte und die Darstellung somit nicht eindeutig wäre. Das ist der Grund, warum bei der Definition der Primzahlen 1 ausgeschlossen wird. Vielleicht merken sich so die Schüler, dass 2 die kleinste Primzahl ist.

- Gemäß mathematischer Konvention hat das sogenannte leere Produkt aus null Faktoren den Wert 1 und stellt damit die Primfaktorzerlegung der 1 dar.

Nicht auslassen darf man hier den Beweis des Satzes von Euklid, denn die Schüler einer AHS sollten diesen einfachen Beweis kennen. Es ist ein Muss in der Schule diesen Beweis durchzunehmen, da der Satz einen ähnlichen Stellenwert wie der Satz des Pythagoras besitzt. Der Beweis kann durchaus schon in einer fünften Klasse Oberstufe gebracht werden:

**Satz 4.2. "Satz von Euklid"**
Es gibt unendlich viele Primzahlen.

**Beweis:** Man erklärt zunächst die einfache Teilbarkeitsregel:

$$t \mid a \text{ und } t \nmid b \Longrightarrow t \nmid a + b$$

Wir multiplizieren jetzt die ersten zwei, drei, ... Primzahlen, addieren jeweils den Wert 1 und ermitteln das Ergebnis:

$$2 \cdot 3 + 1 = 7$$

$$2 \cdot 3 \cdot 5 + 1 = 31$$

$$2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$$

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2311$$

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 = 30031$$

Die Werte auf der rechten Seite können alle nicht durch die Primzahlen, die auf der linken Seite im Produkt auftreten, teilbar sein. Daher steht rechts entweder eine neue Primzahl (7, 31, 211, 2311) oder eine Zahl, die einen Primteiler besitzt, der größer als die links auftretenden ist ($30031 = 59 \cdot 509$). Aus der entsprechenden Verallgemeinerung folgt sogleich, dass es nicht endlich viele Primzahlen geben kann. Vielleicht führt man aber hier auch einen strengeren indirekten Beweis, der in einem Wahlpflichtfach durchaus gezeigt werden kann:

Annahme: Es gibt nur endlich viele Primzahlen $p_1, p_2, p_3, \ldots, p_r$.

Wir bilden nun wie oben die Zahl $n = p_1 p_2 p_3 \cdots p_r + 1$. Da bei der Division von $n$ durch eine der Primzahlen $p_1, p_2, p_3, \ldots, p_r$ stets der Rest 1 bleibt und jede natürliche Zahl $> 1$ mindestens eine Primzahl als Teiler besitzt, muss $n$ entweder selbst eine neue Primzahl sein oder einen Primteiler verschieden von $p_1, p_2, p_3, \ldots, p_r$ besitzen. Beide Fälle stehen aber im Widerspruch zur Annahme.

□

Aus dem Beweis folgt auch, dass es keine größte Primzahl gibt.

## 4.2 Primzahlverteilung

Wie sind nun die Primzahlen verteilt? Gibt es hier Regelmäßigkeiten und gehorchen sie gewissen Gesetzen oder bestimmt nur der Zufall ihr Auftreten in der Folge der natürlichen Zahlen? Euler verzweifelte noch in Hinblick auf die Komplexität dieses Problems:

"Die Mathematiker haben sich bis jetzt vergeblich bemüht, irgendeine Ordnung in der Folge der Primzahlen zu entdecken, und man ist geneigt zu glauben, dies sei ein Geheimnis, das der menschliche Geist niemals durchdringen wird. Um sich davon zu überzeugen, braucht man nur einen Blick auf die Primzahltabellen zu werfen und man wird bemerken, dass dort weder eine Ordnung herrscht noch eine Regel zu beobachten ist" [1] (S.82)

Dieses Zitat kann man sicher als Einstieg verwenden um in der Oberstufe, etwa in der sechsten Klasse, wenn der Logarithmus schon zur Verfügung steht, einmal eine Stunde "Erweiterungsstoff" zu machen, und das Thema "Primzahlverteilung" anzuschneiden. Zweckmäßig ist es dabei in den Informatikraum zu übersiedeln und dort mit DERIVE zu arbeiten.

Man führt zwei Funktionen ein:

- Die Primzahlfunktion $\pi(x)$, welche für eine positive natürliche Zahl $x$ die Anzahl der Primzahlen $\leq x$ angibt.
- Die Funktion $\frac{x}{\pi(x)}$, welche einen Wert für die durchschnittlichen "Lücke" zwischen zwei Primzahlen kleiner oder gleich $x$ darstellt.

Dann lässt man die Schüler folgende Tabelle für die Funktionen $\pi(x)$ und $\frac{x}{\pi(x)}$ anlegen.

| $x$ | $\pi(x)$ | $x/\pi(x)$ |
|---|---|---|
| $10^1$ | 4 | 2.5 |
| $10^2$ | 25 | 4.0 |
| $10^3$ | 168 | 6.0 |
| $10^4$ | 1229 | 8.1 |
| $10^5$ | 9592 | 10.4 |
| $10^6$ | 78498 | 12.7 |
| $10^7$ | 664579 | 15.0 |
| $10^8$ | 5761455 | 17.4 |
| $10^9$ | 50847534 | 19.7 |

Tabelle 4.1: Primzahlverteilung

## 4.2 Primzahlverteilung

Der DERIVE Befehl

```
PRIMEPI(x)
```

liefert die Elemente der zweiten Spalte. Damit die Rechenzeiten nicht allzu groß werden, wird man die Ergebenisse der letzten Zeilen bekanntgeben. Wie wächst die dritte Spalte dieser Tabelle? Man sieht, dass die Funktion $x/\pi(x)$ als Funktion des Exponenten von $x$ annähernd linear ist mit der Steigung $\approx 2,3$. Da $2,3 \approx ln10$ ist, kommt man zu der Abschätzung

$$\frac{x}{\pi(x)} \approx lnx \text{ also } \pi(x) \approx \frac{x}{lnx}.$$

Diese Abschätzung war schon dem jungen Gauß bekannt, obwohl er viel weniger Werte für $\pi(x)$ zur Verfügung hatte. Die Werte der Funktion $\pi(x)$ waren damals etwa nur bis 300 000 bekannt. Schon er vermutete, dass für $x \longrightarrow \infty$ die Differenz $\pi(x) - x/lnx$ gegen Null geht, das heisst es gilt in etwa:

$$\lim_{x\to\infty}(\pi(x) - \frac{x}{lnx}) = 0$$

Das ist der Inhalt des berühmten Primzahlsatzes, der allerdings erst von J. Hadamard (1865 - 1963) und C. de la Vallée Poussin (1866 - 1962) unabhängig voneinander bewiesen wurde. Die Schüler haben hiermit einen großartigen Satz der Zahlentheorie kennen gelernt: Eine Approximation für $\pi(x)$. Es gibt bessere Näherungen für $\pi(x)$, aber hier hat man sicher die Grenze des Möglichen im Mathematikunterricht in der Schule erreicht.

Mit DERIVE kann man sich in dieser Stunde "Primzahlverteilung" auch noch einem anderen Problem widmen: Man erklärt (oder wiederholt) den Begriff Primzahlzwilling. Diese Primzahlzwillinge werden mit größer werdenden Zahlen immer seltener, es ist aber nicht bekannt, ob die Folge der Zwillinge nicht ganz aufhört. Dies würde die Existenz eines größten Primzahlzwillings bedeuten.

Folgende DERIVE-Routine ermittelt Primzahlzwillinge $(a, b)$:

```
next_twin(x) :=
  Loop
   x := NEXT_PRIME(x)
   If NEXT_PRIME(x) = x + 2
    RETURN [x, NEXT_PRIME(x)]
```

Damit ist es möglich zu jedem Wert $x$, den nächstliegenden Primzahlzwilling $(p, p + 2)$ mit $p \geq x$ zu berechnen.

```
next_twin(123)=[137, 139]
```

## 4.2 Primzahlverteilung

Der Befehl

```
nth_twin(n) := ITERATE(next_twin(AVERAGE(x)), x, [3, 5], n - 1)
```

ermöglicht die Berechnung des $n$-ten Primzahlzwillings. Wie schon erwähnt gehört es zu einem ungelösten Problem der Zahlentheorie, ob es unendlich viele Primzahlzwillinge gibt. Wie wir gesehen haben beträgt die Wahrscheinlichkeit, dass eine natürliche Zahl der Größenordnung $x$, eine Primzahl ist, ungefähr $\frac{1}{lnx}$, das heißt in einem Intervall um $x$ der Länge $a$ liegen etwa $\frac{a}{lnx}$ Primzahlen. Entsprechend ist die Wahrscheinlichkeit dafür, dass zwei zufällig (in der Umgebung von x) gewählte Zahlen beide Primzahlen sind, etwa $\frac{1}{lnx^2}$. Bezogen auf Primzahlzwillinge bedeutet dies, dass in den genannten Intervallen $\frac{a}{lnx^2}$ Primzahlzwillinge zu erwarten sind. Heuristische Überlegungen führen zu folgender Formel:

$$C \cdot \frac{a}{lnx^2} \qquad \text{mit } C = 1,320323632,$$

welche die Anzahl der Primzahlzwillinge im Intervall $[x, x + a]$ angibt.

Numerische Rechnungen führen zu überraschenden Übereinstimmungen mit der Theorie, wie die Tabelle 4.2 zeigt.

| Intervall | Primzahlzwilllinge erwartet | Primzahlzwillinge gefunden |
|---|---|---|
| $[10^8, 10^8 + 150.000]$ | 584 | 601 |
| $[10^{10}, 10^{10} + 150.000]$ | 461 | 466 |
| $[10^{11}, 10^{11} + 150.000]$ | 309 | 276 |
| $[10^{12}, 10^{12} + 150.000]$ | 259 | 276 |
| $[10^{13}, 10^{13} + 150.000]$ | 221 | 208 |
| $[10^{14}, 10^{14} + 150.000]$ | 191 | 186 |
| $[10^{15}, 10^{15} + 150.000]$ | 166 | 161 |

Tabelle 4.2: Primzahlzwillinge

Mit einem Programm von DERIVE (Autor: J. Wiesenbauer) kann man die ungefähre Anzahl der auftretenden Primzahlzwillinge unter den ersten $s$ Zahlen berechnen:

```
twinpi(s, exact := true, c_ := 1, p_ := 3, t_) :=
 If exact
  Prog
   If s < 5
    RETURN 0
   Loop
    t_ := next_twin(p_)
```

```
  p_ := FIRST(REST(t_))
  If p_ > s
   RETURN c_
  c_ :+ 1
APPROX(STRING(∫(1.320323632/LN(t)^2, t, 2, s)))
```

In Zusammenhang mit der Primzahlverteilung kann man weiters den Satz über die Primzahllücken bringen:

**Satz 4.3.**
Es gibt beliebig große Lücken in der Primzahlfolge. Oder anders ausgedrückt: Ist $k$ eine natürliche Zahl, dann gibt es mindestens $k$ aufeinanderfolgende zusammengesetzte Zahlen.

**Beweis:** Wir betrachten die Zahlen

$$(k+1)!+2 \qquad (k+3)!+3 \qquad \cdots \qquad (k+1)!+k \qquad (k+1)!+k+1$$

Der Begriff "Fakulät" sollte in einer sechsten Klasse schon zur Verfügung stehen. Jede dieser Zahlen ist zusammengesetzt, denn es gilt :

$$j \mid \Big((k+1)!+j\Big) \quad \text{für} \quad 2 \le j \le k+1$$

□

Die Mathematiker haben immer nach Primzahlformeln gesucht. Auch dieses Thema kann man anschneiden. Das "Euler'sche Primzahlpolynom" $n^2+n+41$ etwa liefert der Reihe nach Primzahlen für die Werte $1, 2, \ldots, 39$ (Übung mit DERIVE). Wenn man den Binomischen Lehrsatz zur Verfügung hat, so kann man folgendes zeigen:

**Satz 4.4.**
Es gibt kein nichtkonstantes Polynom

$$f(x) = a_n x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_o$$

mit natürlichen Koeffizienten ($a_n \neq 0$), so dass $f(x)$ eine Primzahl ist für alle $x \in \mathbb{N}$.

**Beweis:** Den Beweis führt man indirekt.

Angenommen es gibt so ein Polynom, dann ist $f(1) = a_n + \cdots + a_1 + a_0$ eine Primzahl $p$. Wir berechnen nun $f(1+p)$:

$$f(1+p) = a_n(1+p)^n + a_{n-1}(1+p)^{n-1} + \cdots + a_1(1+p) + a_0 =$$

$$= a_n(1+p)^n - a_n + a_{n-1}(1+p)^{n-1} - a_{n-1} + \cdots + a_1(1+p) - a_1 + a_0 + a_1 + \cdots + a_n =$$

$$= a_n(1+p)^n - a_n + a_{n-1}(1+p)^{n-1} - a_{n-1} + \cdots + a_1(1+p) - a_1 + p$$

Man erkennt nun mit Hilfe der binomischen Formel, dass

$$a_k(1+p)^k - a_k = a_k\Big(1 + kp + \binom{k}{2}p^2 + \binom{k}{3}p^3 + \cdots + p^k\Big) - a_k$$

durch $p$ teilbar ist. Es gilt aber sicher auch $f(1+p) > f(1) = p$, da alle $a_i$ natürliche Zahlen sind und das Polynom nicht konstant ist. Daher gilt

$$p \mid f(1+p)$$

und das steht im Widerspruch zur Annahme, dass $f(x)$ eine Primzahl ist für alle $x \in \mathbb{N}$.

□

Im Falle des oben erwähnten "Euler'schen Polynoms" gilt:

$$(1 + 1 + 41) = 43 \mid (44^2 + 44 + 41) = 2021 = 43 \cdot 47$$

Allgemein gilt obiger Satz auch für ganzzahlige Koeffizienten $a_i$. Der Beweis verläuft ähnlich, im Unterricht kann man sich aber auf die vereinfachte Form mit natürlichen Zahlen als Koeffizienten beschränken.

## 4.3 Besondere Primzahlen

### 4.3.1 Mersenne'sche Primzahlen

Bei der Jagd auf große Primzahlen spielen die Zahlen der Bauart $M_p : 2^p - 1$ eine zentrale Rolle. Eine Zahl dieser Bauart $M_p := 2^p - 1$ heißt die $p$-te Mersenne'sche Zahl, die Primzahlen unter diesen Zahlen heißen Mersenne'sche Primzahlen. Beispielsweise ist $M_3 := 3 = 2^2 - 1$ eine Mersenne'sche Primzahl, genau wie $M_7 = 2^3 - 1$. Der kleinste prime Exponent, der auf keine Mersenne'sche Primzahl führt, ist $M_{11} : 2^{11} - 1 = 2047$ ist faktorisierbar als $2047 = 23 \cdot 89$.

Den Namen haben diese Primzahlen von dem französischen Mönch und Priester Marin Mersenne (1588 Ű 1648), der behauptete, dass für $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ und $257$ $M_p$ eine Primzahl ist. Dabei irrte er aber bei den Zahlen 67 und 257 und übersah die Zahlen 61, 89 und 107.

Die größten bekannten Primzahlen sind vom Mersenne Typus. GIMPS (**G**reat **I**nternet **M**ersenne **P**rime **S**earch) erlaubt eine weltweite Beteiligung an den Berechnungen von Primzahlen. Die notwendige Software wird einfach heruntergeladen und installiert. Von GIMPS lässt man sich die Zahl zuschicken, die untersucht werden soll. Nach mehreren Wochen oder auch Monaten, wird das Ergebnis zurückgeschickt. Da die Primzahlen mittlerweile sehr groß sind, brauchen die Computer lange Programmlaufzeiten. Der Rekordhalter ist derzeit die 44. Mersenne'sche Primzahl

$2^{32.582.657} - 1$ mit 9808358 Stellen (Stand: 21. Mai 2007).

Ob eine Mersenne'sche Zahl nun tatsächlich eine Primzahl ist, wird durch einige Tests gelöst. Der folgende Satz ermöglicht eine Eingrenzung der Untersuchungen um festzustellen, welche Mersenne'sche Zahlen auch tatsächlich Primzahlen sind:

**Satz 4.5.**
Wenn $M_p = 2^p - 1$ eine Primzahl ist, dann muss auch $p$ eine Primzahl sein.

Diese Eigenschaft grenzt die Suche nach großen Mersenne'sche Primzahlen ein, da nur noch Mersenne'sche Zahlen untersucht werden müssen, deren Exponent eine Primzahl ist. Die Umkehrung ist falsch, wie wir schon oben etwa bei $M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$ gesehen haben.

**Beweis:** Es sei $M_p = 2^{p-1}$ und $p = m \cdot n$, wobei $m$ und $n$ natürliche Zahlen größer als 1 sind. Wir beginnen mit der Summenformel für eine endliche geometrische Reihe:

$$1 + q + q^2 + \cdots + q^{n-1} = \frac{q^n - 1}{q - 1}$$

Daraus folgt:

$$\left(1 + q + q^2 + \cdots + q^{n-1}\right)(q - 1) = q^n - 1$$

Ersetzt man nun $q$ durch $2^m$ so erhält man

$$\left(1 + 2^m + (2^m)^2 + \cdots + (2^m)^{n-1}\right)(2^m - 1) = (2^m)^n - 1,$$

also:

$$\left(1 + 2^m + 2^{2m} + \cdots + 2^{(n-1)m}\right)(2^m - 1) = 2^{mn} - 1 = 2^p - 1$$

$M_p$ lässt sich daher als Produkt von zwei Faktoren darstellen, die beide sicher größer als 1 sind. $M_p$ ist daher keine Primzahl.

□

Jede Mersenne'sche Zahl hat eine Binärdarstellung, die nur aus Einsern besteht. Mit dem folgenden DERIVE-Befehl kann man die Frage beantworten, für welche Primzahlen kleiner als 1000 $M_p$ eine Primzahl ist.

```
MERSENNE(n) := SELECT(PRIME(2^p - 1), p, SELECT(PRIME(p), p, n))
```

[2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607]

Die Mersenne'schen Primzahlen erhält man dann mit dem Befehl:

$M_p$(n) := VECTOR($2^p$ - 1, p,[2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127, 521, 607] ))

[3, 7, 31, 127, 8191, 131071, 524287, 2147483647, 2305843009213693951,
618970019642690137449562111,
162259276829213363391578010288127,
170141183460469231731687303715884105727]

($2^{521}$ und $2^{607}$ wurden weggelassen.)

### 4.3.2 Der Lucas-Lehmer-Test

Zum Abschluss der Mersenne'schen Zahlen kann man noch einen deterministischen Primzahltest vorstellen, den Lucas-Lehmer-Test. Der Lucas-Lehmer-Test ist einer der schnellsten und der am häufigsten verwendeten Tests, um festzustellen, ob eine Mersenne'sche Zahl tatsächlich eine Primzahl ist. Da für diese Mersenne'schen Zahlen ein einfacher Primzahltest existiert, eignen sich diese Zahlen auch für die Suche nach Primzahlrekorden. Der Lucas-Lehmer-Test funktioniert wie folgt:

**Satz 4.6.** Gegeben sei die durch

$$s_{n+1} = s_n^2 - 2 \qquad \text{und} \quad s_1 = 4$$

definierte rekursive Folge $< s_n >$ . Weiters sei $p$ eine ungerade Primzahl.

Dann ist die Mersennne'sche Zahl $M_p = 2^p 1$ genau dann eine Primzahl, wenn $s_{p-1}$ durch $M_p$ teilbar ist, also

$$M_p \text{ ist prim} \iff M_p \mid s_{p-1}.$$

Auf den Beweis wird man in der Schule nicht eingehen, da er Grundlagen der Gruppentheorie beinhaltet. Mit dem DERIVE Befehl

s(n) := ITERATES($i^2$ - 2, i, 4, n)

macht man sich rasch klar, dass die Glieder der Folge rasch größer werden. Das 12-te Glied dieser Folge hat bereits 2343 Dezimalstellen.

**Beispiel 4.3.1.** Ist die Mersenne'sche Zahl $M_7$ eine Primzahl?

Man rechnet nach:

$$\frac{s_6}{M_7} = \frac{20059565468227461 14}{127} = 15794933439549182$$

also $M_7$ ist eine Primzahl.

Die Schüler sehen anhand dieses Beispiels, wie groß die Zahlen werden. Daher wird man auch hier mit Kongruenzen rechnen. Es genügt die Folge $< s_n >$ modulo $M_p$ zu betrachten. Damit verringert sich der Rechnenaufwand enorm, wie folgendes Beispiel zeigt:

**Beispiel 4.3.2.** Ist die Mersenne'sche Zahl $M_{13} = 8191$ eine Primzahl?

**Lösung:** $s_1 = 4 \equiv 4 \bmod 8191$
$s_2 = 14 \equiv 14 \bmod 8191$
$s_3 = 194 \equiv 194 \bmod 8191$
$s_4 = 194^2 - 2 = 37643 \equiv -3321 \bmod 8191$
$s_5 = (-3321)^2 - 2 = 11029039 \equiv 3953 \bmod 8191$
$s_6 = 3953^2 - 2 = 15626207 \equiv -2221 \bmod 8191$
$s_7 = (-2221)^2 - 2 = 4932839 \equiv 1857 \bmod 8191$
$s_8 = (1857)^2 - 2 = 3448447 \equiv 36 \bmod 8191$
$s_9 = (36)^2 - 2 = 1294 \equiv 1294 \bmod 8191$
$s_{10} = (1294)^2 - 2 = 1674434 \equiv 3470 \bmod 8191$
$s_{11} = (3470)^2 - 2 = 12040898 \equiv 128 \bmod 8191$
$s_{12} = (128)^2 - 2 = 16382 \equiv 0 \bmod 8191$

Da $M_{13} = 8191$ das Folgeglied $s_{12}$ ohne Rest teilt, folgt daraus, dass $M_{13}$ eine Primzahl ist. Es sind hier 9 Divisionen zu berechnen.

□

Als Gegenbeispiel kann man mit dem Test zeigen, dass $M_{11} = 2^{11} - 1$ keine Primzahl ist. Das Prinzip des Lucas-Lehmer-Tests für große Mersenne'sche Zahlen ist damit klar.

Mit dem `LUCAS_LEHMER` - Befehl aus dem Number Theory Utility File von DERIVE kann man überprüfen, ob eine Mersenne'sche Zahl eine Primzahl ist oder nicht.

Zum Beispiel ergeben sich für $M_7$ und $M_{13}$ folgende Ergebnisse:

```
LUCAS_LEHMER(2^13-1)=false
```

```
LUCAS_LEHMER(2^7-1)=true
```

### 4.3.3 Fermat'sche Zahlen

Eine Fermat'sche Zahl, benannt nach dem französischen Mathematiker Pierre de Fermat, ist eine natürliche Zahl der Form

$$F_n := 2^{2^n} + 1 \qquad \text{mit} \qquad n \in \mathbb{N}$$

Eine Fermat'sche Zahl, die gleichzeitig Primzahl ist, wird Fermat'sche Primzahl genannt. Fermat zeigte, dass die ersten fünf Fermat'schen Zahlen $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ und $F_4 = 65537$ Primzahlen sind und vermutete 1637, dass dies auf alle Fermat'sche Zahlen zutrifft. Diese Vermutung wurde von Leonhard Euler 1732 widerlegt, indem er mit 641 einen echten Teiler von $F_5 = 4294967297$ berechnete. Man vermutet inzwischen, dass alle Fermat'sche Zahlen außer den ersten fünf keine Primzahlen sind. Das Faszinierende an diesen Zahlen ist, dass sie mit wachsenden $n$ schnell ungeheuer groß werden. Schon die Fermat'sche Zahl $F_{10}$ besitzt 309 Dezimalstellen und $F_{73}$ besitzt so viele Stellen, dass sie in den Büchern aller Bibliotheken der ganzen Welt nicht mehr Platz hätte. Das kann man mit den Schülern auch nachrechnen. Erstens übt man dabei das Potenzrechnen und zweitens das Abschätzen großer Werte. Man wird zunächst gemeinsam großzügig die Anzahl der Bibliotheken und ihren Umfang abschätzen: Es gibt eine Million Bibliotheken mit je einer Million Büchern, jedes davon mit 1000 Seiten, wovon jede Seite 100 Zeilen mit je 100 Zeichen hat. Diese Annahme bedeutet, dass in allen Bibliotheken zusammen

$$100 \cdot 1000 \cdot 1000 \cdot 1000000 \cdot 1000000 = 10^{19}$$

Ziffern stehen können.

Jetzt müssen wir uns einen Überblick über die Stellenanzahl von $F_{73}$ verschaffen. Es gilt:

$$2^{10} = 1024 > 10^3 \qquad \text{daher} \qquad 2^{73} = 8 \cdot 2^{70} > 8 \cdot 10^{21}$$

Jetzt folgt für die Stellenanzahl von $F_{73}$ :

$$2^{2^{73}} > 2^{8 \cdot 10^{21}} = (2^{80})^{10^{20}} = \left((2^{10})^8\right)^{10^{20}} > 10^{24 \cdot 10^{20}} = 10^{240 \cdot 10^{19}}$$

Man müsste also mehr als 240 Millionen Bibliotheken mit obigem (großzügigem) Umfang zur Verfügung haben, um alle Ziffern von $F_{73}$ anschreiben zu können. Trotzdem konnte bewiesen werden, dass es sich um eine zusammengesetzte Zahl handelt. Auch bei der gigantischen Zahl $F_{23471}$ konnte der Primteiler $10 \cdot 2^{23472} + 1$ gefunden werden. Man kann den Schülern jetzt zeigen, dass eine Primzahl der Form $2^n + 1$ eine Fermat'sche Primzahl sein muss. Es gilt nämlich folgender Satz:

**Satz 4.7.**
Wenn $2^n + 1$ eine Primzahl ist, dann ist $n$ eine Zweierpotenz.

**Beweis:** Es sei $n = a \cdot b$ wobei $a$ und $b$ natürliche Zahlen größer als 1 und kleiner als $n$ sind und weiters sei $b$ ungerade. Dann ist $2^n + 1 = (2^a)^b + 1$. Wir beginnen wieder mit der umgeformten Summenformel für eine endliche geometrische Reihe:

$$\left(1 + q + q^2 + \cdots + q^{n-1}\right)(q - 1) = q^n - 1$$

Setzt man $q = -2^a$ und $n = b$ so ergibt sich:

$$\left(1 + (-2^a) + (-2^a)^2 - \cdots + (-2^a)^{b-1}\right)(-2^a - 1) = (-2^a)^b - 1$$

also

$$\left(1 - (2^a) + (2^a)^2 - \cdots + (2^a)^{b-1}\right)(2^a + 1) = (2^a)^b + 1.$$

Wenn also $n$ einen ungeraden Teiler hat, dann ist $2^n + 1$ zusammengesetzt (beide Faktoren auf der linken Seite sind größer als 1). Mit anderen Worten: Für jede Primzahl der Form $2^n + 1$ ist n eine Zweierpotenz, also eine Fermat'sche Primzahl. Eleganter lässt sich das mit Kongruenzen durch

$$(2^a)^b + 1 \equiv (-1)^b + 1 \equiv 0 \mod (2^a + 1)$$

beweisen, doch wurde hier absichtlich ein Beweis angegeben, der auf eine den Schülern bekannte Formel zurückgreift.

□

Wenn man noch mehr über die Fermat'schen Zahlen erzählen will, dann kann man noch folgenden Satz bringen:

**Satz 4.8.**
Zwei verschiedene Fermat'sche Zahlen sind stets teilerfremd.

**Beweis:** Man zeigt zunächst, dass die Fermat'sche Zahlen die Rekursionsbeziehung

$$F_n = F_0 \cdot F_1 \cdot F_3 \cdots F_{n-1} + 2$$

erfüllen. Diese Beziehung kann man mit vollständiger Induktion beweisen. Unsere Beweismethode stützt sich auf die den Schülern geläufige binomische Formel $(a - b)(a + b) = a^2 - b^2$. Die Fermat'sche Zahl $F_r$ kann mit Hilfe dieser Formel als Bruch dargestellt werden:

$$F_r = 2^{2^r} + 1 = \frac{(2^{2^r} + 1) \cdot (2^{2^r} - 1)}{2^{2^r} - 1} = \frac{\left(2^{2^r}\right)^2 - 1}{2^{2^r} - 1} = \frac{2^{2^{r+1}} - 1}{2^{2^r} - 1}$$

Dies ergibt für das Produkt der Fermat'schen Zahlen $F_0$ bis $F_{n-1}$ folgenden Ausdruck

$$F_0 F_1 F_2 \cdots F_{n-2} F_{n-1} = \frac{2^{2^1} - 1}{2^{2^0} - 1} \frac{2^{2^2} - 1}{2^{2^1} - 1} \frac{2^{2^3} - 1}{2^{2^2} - 1} \cdots \frac{2^{2^{n-1}} - 1}{2^{2^{n-2}} - 1} \frac{2^{2^n} - 1}{2^{2^{n-1}} - 1} = 2^{2^n} - 1 = F_n - 2 \qquad (4.1)$$

Ausgehend von dieser Rekursionsformel kann man nun leicht zeigen, dass je zwei Fermat'sche

Zahlen zueinander teilerfremd sind. Denn haben $F_m$ unf $F_n$ mit $m < n$ einen gemeinsamen Teiler, dann muss dieser wegen

$$F_n = F_0 \cdot F_1 \cdot F_3 \cdots F_m \cdots F_{n-1} + 2$$

auch 2 teilen, kann also nur 1 oder 2 sein. Da alle Fermat'sche Zahlen ungerade sind, kann der Teiler nur 1 sein und damit ist der Satz bewiesen.

□

Folgerung: Wegen $F_n > 1$ hat jede Fermat'sche Zahl einen Primteiler, der keine andere Fermat'sche Zahl teilt. Da es unendlich viele Fermat'sche Zahlen gibt und jede Zahl $\in \mathbb{N}$ einen Primfaktor $> 1$ besitzt, erhält man hiermit einen weiteren Beweis dafür, dass es unendlich viele Primzahlen gibt.

Carl Friedrich Gauß zeigte, dass es einen Zusammenhang zwischen der Konstruktion von regelmäßigen Vielecken und den Fermat'schen Primzahlen gibt: Ein regelmäßiges Vieleck mit $n$ Seiten kann nur dann mit Zirkel und Lineal konstruiert werden, wenn $n$ eine Potenz von 2 oder das Produkt einer Potenz von 2 und verschiedenen Fermat'schen Primzahlen ist.

### 4.3.4 Vollkommene Zahlen

Abschließend kann man noch ein wenig über die vollkommenene Zahlen erzählen. Sie scheinen bei einer ersten Betrachtung sehr wenig mit den Primzahlen gemeinsam zu haben.

Eine natürliche Zahl $n$ heißt vollkommen, wenn sie gleich der Summe ihrer Teiler $< n$ ist. Dieser Begriff geht auf Pythagoras und die pythagoräische Schule (ca. 500 vor Christus) zurück. Als Einstieg zu diesem Kapitel kann man die Schüler solche vollkommenen Zahlen suchen lassen. Die Zahlen $6 = 1 + 2 + 3$ und $28 = 1 + 2 + 4 + 7 + 14$ werden sie noch leicht finden, dann werden sie aber merken, dass die Suche nicht ganz so einfach ist. Schon Euklid (300 vor Christus) bewies in seinen Elementen, dass Zahlen der Bauart

$$n = 2^{p-1}(2^p - 1)$$

vollkommen sind, wenn $2^p - 1$ eine Primzahl ist. Wie wir bereits wissen, wird eine Primzahl dieser Gestalt Mersenne'sche Primzahl genannt, und ebenfalls wissen wir, dass dann $p$ selbst eine Primzahl ist. Fast 2000 Jahre später bewies Euler, dass sich jede gerade vollkommene Zahl so darstellen lässt. Wir können daher folgenden Satz über gerade vollkommenen Zahlen formulieren:

**Satz 4.9. Euklid-Euler**
Die geraden vollkommenen Zahlen sind genau die Zahlen der Gestalt

$$n = 2^{p-1}(2^p - 1)$$

wobei $p$ eine Primzahl ist, sodass auch $2^p - 1$ eine Primzahl ist, das heißt der zweite Faktor eine Mersenne'sche Primzahl ist.

**Beweis:** Wir zeigen zunächst jenen Teil des Satzes, den schon Euklid in seinen Elementen angegeben hatte:
Es sei also $n = 2^{p-1}(2^p - 1)$ wobei $p$ eine Primzahl ist für die auch $2^p - 1$ eine Primzahl ist. Die Summe aller Teiler von der Zahl $n$ ergibt sich dann durch

$$(1 + 2 + 2^2 + \cdots + 2^{p-1}) \cdot \Big((2^p - 1) + 1\Big),$$

denn multipliziert man diese beiden Klammern aus, so tritt sicher jeder Teiler von n (einschließlich $n$) als Summand auf. Mit Hilfe der Summenformel für eine geometrische Reihe erhält man daraus für die Summe aller Teiler

$$\frac{2^p - 1}{2 - 1} \cdot 2^p = 2 \cdot (2^p - 1)2^{p-1} = 2n.$$

Damit haben wir aber gezeigt, dass die Summe aller Teiler $< n$ gleich der Zahl ist.

Die Umkehrung dieses Satzes beruht auf dem Beweis von Euler, der hier angeführt wird. Hier erreicht man aber sicher eine Grenze des Möglichen im Schulunterricht. Dieser Beweis kann eventuell in einem Wahlpflichtfach vorgetragen oder im Rahmen einer Fachbereichsarbeit von einem interessierten Schüler verlangt werden. Es ist aber nicht möglich, den Beweis im Normalunterricht zu zeigen.

Für den Beweis braucht man die zahlentheoretische Funktion $\sigma(n)$. Mit $\sigma(n)$ bezeichnet man die Summe aller positiven Teiler einer natürlichen Zahl $n$. Diese Funktion könnte man natürlich auch schon im ersten Teil des Beweises verwenden, dort ist sie aber, wie wir gesehen haben, nicht unbedingt notwendig. Eine Zahl $n$ ist nun genau dann vollkommen, wenn

$$\sigma(n) = 2n$$

gilt. Weiters brauchen wir noch die folgenden beiden leicht herleitbaren Eigenschaften diese Funktion:

- Sei $p$ eine Primzahl und $\alpha \geq 1$. Dann gilt:

$$\sigma(p^\alpha) = \frac{p^{\alpha+1} - 1}{p - 1}$$

- Allgemein kann man zeigen, dass die $\sigma(n)$ - Funktion multiplikativ ist. Vielleicht wird man aber hier nur einen für diesen Beweis notwendigen Sonderfall dieses Satzes zeigen: Sind $a$ und $b$ teilerfremde natürliche Zahlen, dann gilt:

$$\sigma(a) \cdot \sigma(b) = \sigma(a \cdot b)$$

Die erste Eigenschaft folgt unmittelbar aus der Summenformel für eine endliche geometrische Reihe. Die zweite Eigenschaft überlegt man sich so:

Jeder Teiler von $d = a \cdot b$ hat, da $a$ und $b$ teilerfremd sind, eine Darstellung in der Gestalt $d = d_1 \cdot d_2$, wobei $d_1$ ein Teiler von $a$ und $d_2$ ein Teiler von $b$ ($1 \leq d_1 \leq a, 1 \leq d_2 \leq b$) ist. Daher gilt:

$$\sigma(a \cdot b) = \sum_{d|a \cdot b} d = \sum_{d_1|a} d_1 \cdot \sum_{d_2|b} d_2 = \sigma(a) \cdot \sigma(b)$$

Jetzt erst kann man den Satz von Euler beweisen:

Es sei also $n$ eine gerade vollkommene Zahl. Wir schreiben:

$$n = 2^{p-1} \cdot u \qquad \text{mit} \qquad p \geq 2 \text{ und u ungerade}$$

Dann ist:

$$\sigma(n) = \sigma(2^{p-1} \cdot u) = \sigma(2^{p-1}) \cdot \sigma(u) = (2^p - 1) \cdot \sigma(u)$$

Da $n$ vollkommen sein soll, gilt

$$(2^p - 1) \cdot \sigma(u) = \sigma(n) = 2n = 2 \cdot 2^{p-1} \cdot u = 2^p \cdot u.$$

Da $2^p - 1$ ungerade ist, folgt

$$2^p - 1 \mid u, \qquad \text{das heißt} \qquad u = (2^p - 1) \cdot v,$$

wobei $v$ eine natürliche Zahl ist.

Die bisherigen Ergebnisse zusammenfassend haben wir:

$$n = 2^{p-1}(2^p - 1)v \qquad \text{und} \qquad \sigma(n) = (2^p - 1)\sigma((2^p - 1)v)$$

Da $n$ vollkommen ist folgt:

$$\sigma((2^p - 1)v) = 2^p v$$

Wäre nun $v > 1$, so hätte $(2^p - 1)v$ wegen $2^p - 1 \geq 3$ mindestens die verschiedenen Teiler 1, $v$ und $(2^p - 1)v$, also wäre

$$\sigma((2^p - 1)v) \geq (2^p - 1)v + v + 1 = 2^p v + 1 > 2^p v.$$

Dieses Ergebnis steht aber im Widerspruch zu $\sigma((2^p - 1)v) = 2^p v$. Daher bleibt nur die Möglichkeit, dass $v = 1$ gilt und damit erhält man

$$\sigma(2^p - 1) = 2^p.$$

Da $\sigma(2^p - 1) \geq (2^p - 1) + 1 = 2^p$ gilt, kann $2^p - 1$ nur die unechten Teiler 1 und $2^p - 1$ besitzen. Darum ist $2^p - 1$ eine Primzahl und wie wir bereits wissen, ist diese Zahl nur dann auch wirklich eine Primzahl, wenn $p$ ebenfalls prim ist. Damit ist alles gezeigt.

□

Folgerung: Es gibt also genauso so viele gerade vollkommenen Zahlen, wie es Mersenne'sche Primzahlen gibt. Wir wissen nicht, ob es unendlich viele Mersenne'sche Primzahlen gibt, daher auch nicht ob es unendlich viele gerade vollkommene Zahlen gibt.

Mit den Schülern ist es auch interessant die ersten 12 vollkommenen Zahlen zu betrachten:

6

28

496

8128

33550336

8589869056

137438691328

2305843008139952128

2658455991569831744654692615953842176

191561942608236107294793378084303638130997321548169216

13164036458569648337239753460458722910223472318386943117783728128

1447401115466452442794637312608598848157367749147483588906635434913119915212 8

Dabei fällt den Schülern sicher schnell auf, dass die ersten 12 vollkommenen Zahlen als letzte Ziffer 6 oder 8 besitzen.

Als Abschluss zu den vollkommenen Zahlen sollten die Schüler noch auf ein weiteres ungelöstes Problem der Zahlentheorie aufmerksam gemacht werden. Denn es ist noch die Frage offen, ob es auch ungerade vollkommene Zahlen gibt. Bis heute wurden noch keine gefunden und wenn es welche geben sollte, dann müssten sie mindestens 300 Dezimalstellen und viele Faktoren besitzen.

# Kapitel 5

# Kongruenzen

## 5.1 Grundlegendes

Will man Zahlentheorie eingehender betreiben, braucht man unbedingt Kenntnisse über Kongeruenzen und Restklassen. Viele Aufgaben und Probleme lassen sich einfacher oder überhaupt nur lösen, wenn man das Rechnen mit Kongruenzen beherrscht. Leider wird heute im Regelunterricht verabsäumt dieses grundlegende Wissen zu vermitteln. Interessant ist, wenn man in diesem Zusammenhang den Lehrplan für Mathematik für die 5. Klasse Realgymnasium einer AHS verfolgt: Im Jahr 1978 ist das Rechnen mit Kongruenzen und Restklassen für das Realgymnasium noch verbindlich vorgeschrieben und auch ausführlich in den entsprechenden Schulbüchern behandelt (vgl. [16]). In den folgenden Jahren wurden aber diese Kapitel schrittweise immer mehr gekürzt und heute ist das Rechnen mit Kongruenzen im Regelunterricht praktisch nicht mehr vorgesehen. Nimmt man sich daher vor, im Rahmen eines Projektes oder im Wahlpflichtfach Mathematik Zahlentheorie eingehender zu vermitteln, so wird man zunächst diese Grundlagen behandeln müssen. In der Schule sollte auch klar gemacht werden, dass man im Alltag durchaus mit Kongruenzen rechnet, ohne dass man sich dessen bewusst ist. Wenn es zum Beispiel 15 Uhr am Nachmittag ist, sagen viele, dass es 3 Uhr ist. Dabei haben sie $15 \equiv 3 \bmod 12$ gerechnet. Es seien im folgenden kurz die wichtigsten Begriffe und Rechenregeln zusammengestellt, die man im Zusammenhang mit den Kongruenzen bringen sollte. Auf die Beweise wurde hier verzichtet, im Unterricht muss aber durchaus der eine oder andere gebracht werden.

**Definition 5.1.1.**

**Restklassen modulo m:** Es sei $m > 1$ eine natürliche Zahl und $i = 0, 1, 2, \ldots, m-1$. Die Restklasse $\bar{i} \bmod m$ ist die Menge der ganzen Zahlen der Form $m \cdot k + i$ wobei $k$ eine ganze Zahl ist:

$$\bar{i} = \{x \mid (x = m \cdot k + i), k \in \mathbb{Z}\} \tag{5.1}$$

**Definition 5.1.2.**

**Kongruenz:** Es sei $m > 1$ eine natürliche Zahl und $a$, $b$ ganze Zahlen. Man sagt $a$ und $b$ sind zueinander "kongruent modulo $m$", genau dann, wenn $a$ und $b$ in derselben Restklasse modulo $m$ liegen. Man schreibt:

$$a \equiv b \bmod m$$

Man zeigt die Äquivalenz zu folgender Definition von Kongruenz:

Zwei ganze Zahlen $a$ und $b$ sind genau dann kongruent modulo $m$, wenn

$$m \mid (a - b) \tag{5.2}$$

gilt.

**Definition 5.1.3.**

**Der mod-Operator:** Für eine positive ganze Zahl m mit $m \neq 1$ versteht man unter

$$i = a \mod m \tag{5.3}$$

den kleinsten nichtnegativen Rest i bei der Division von a durch m.

Hier muss man natürlich näher darauf eingehen, was der Rest einer negativen Zahl bei der Division durch m bedeutet. In diesem Zusammenhang ist es wichtig die unterschiedliche Bedeutung von $x = a \bmod m$ und $x \equiv a \bmod m$ klarzustellen.

### 5.1.1 Rechenregeln für Kongruenzen

Es seien im Folgenden $a, b, c, d$ ganze Zahlen und $m, n, k$ natürliche Zahlen größer als 1.

$$a \equiv b \bmod m \quad \text{und} \quad c \equiv d \bmod m \implies a + c \equiv b + d \bmod m \tag{5.4}$$

$$a \equiv b \bmod m \quad \text{und} \quad c \equiv d \bmod m \implies a - c \equiv b - d \bmod m \tag{5.5}$$

$$a \equiv b \bmod m \quad \text{und} \quad c \equiv d \bmod m \implies a \cdot c \equiv b \cdot d \bmod m \tag{5.6}$$

$$a \equiv b \bmod m \implies a^k \equiv b^k \bmod m \tag{5.7}$$

$$a \equiv b \bmod m \quad \text{und} \quad a \equiv b \bmod n \quad \text{und} \quad ggT(m,n) = 1 \implies a \equiv b \bmod kgV(m,n) \tag{5.8}$$

$$a \cdot k \equiv b \cdot k \bmod m \quad \text{und} \quad ggT(m,k) = 1 \implies a \equiv b \bmod m \tag{5.9}$$

$$a \equiv b \bmod m \implies k \cdot a \equiv k \cdot b \bmod (k \cdot m) \tag{5.10}$$

Mit diesen Begriffen und Regeln wird man die Schüler natürlich nicht erschlagen, sondern man wird sie langsam und behutsam vorstellen und mit vielen Beispielen einüben. Dazu kann man durchaus

die alten Lehrbücher heranziehen. Auch die eine oder andere Rechenregel sollte man beweisen, das fördert sicher ein tieferes Verstehen des Kongruenzrechnens. Welches mächtige Werkzeug man sich damit geschaffen hat, kann man den Schülern anhand vieler Beispiele demonstrieren, eines sei hier ausgeführt:

**Beispiel 5.1.1.** Zeige: Die Zahl $2^{12066} - 1$ ist durch 7 teilbar.

**Lösung:** Es gilt: $2^6 = 64$ , $64 \equiv 1 \bmod 7$ und $12066 = 2011 \cdot 6$. Daher folgt:

$$2^6 \equiv 1 \bmod 7 \Longrightarrow \text{(vgl.5.6)} \ \left(2^6\right)^{2011} \equiv 1^{2011} \bmod 7 \ \text{ also: } \ 2^{12066} \equiv 1 \bmod 7.$$

Daher ist $2^{12066} - 1$ durch 7 teilbar.

□

# 5.2 Anwendungen

Alle folgenden Anwendungen lassen sich mit dem Wissen über Kongruenzen sehr schnell ableiten beziehungsweise beweisen. Es ist aber auch durchaus möglich, die eine oder andere Anwendung im Unterricht zu bringen, wenn die Schüler diese Begriffe nicht kennen. Man hilft sich dann mit Teilbarkeitsregeln oder man arbeitet nur mit dem mod-Operator, den man bei dieser Gelegenheit erklärt (vgl. [24] und 5.3).

## 5.2.1 Beweis der Teilbarkeitsregeln

Schon in der zweiten Klasse Unterstufe haben die Schüler Teilbarkeitsregeln kennengelernt und angewandt. Jedoch wurden diese nicht im exakten Sinne der Mathematik bewiesen, sondern nur anhand von Beispielen bestätigt. Mit Hilfe der Kongruenzen kann man jetzt diese Regeln beweisen. Man wird zunächst die verschiedenen Regeln in Erinnerung rufen und die Darstellung einer natürlichen Zahl mit Zehnerpotenzen

$$a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 10^2 + a_1 10^1 + a_0 \qquad 0 \leq a_i \leq 9,\ a_n \neq 0,\ i = 1, 2, \ldots, n$$

wiederholen oder in dieser allgemeinen Form vielleicht zum ersten Mal anschreiben. Wir wollen uns hier auf den Beweis von zwei Teilbarkeitsregeln beschränken: Zunächst die den Schülern bekannte Teilbarkeitsregel durch 3 bzw. 9:

**Satz 5.1.**
Eine natürliche Zahl $z$ ist genau dann durch 3 bzw. 9 teilbar, wenn ihre Ziffernsumme (=Quersumme) durch 3 bzw. 9 teilbar ist.

**Beweis:** Wegen $10 \equiv 1 \bmod 3$ bzw. 9 gilt $10^k \equiv 1^k = 1$ bzw. 9 für alle $k \geq 1$. Daher gilt:

$$a = a_n 10^n + \cdots + a_1 10^1 + a_0 \equiv a_n + a_{n-1} + \cdots + a_2 + a_1 + a_0 \bmod 3 \text{ bzw.} 9$$

□

Die wenigsten werden die Teilbarkeitsregel durch 11 kennen. Verschiedene durch 11 teilbare Zahlen - Schüler beobachten lassen - führen vielleicht zu dem folgenden Satz:

**Satz 5.2.**
Eine natürliche Zahl $z$ ist genau dann durch 11 teilbar, wenn ihre alternierende Ziffernsumme (Wechselquersumme) durch 11 teilbar ist.

Mit Hilfe der Kongruenzen ist diese Regel analog zu obenstehenden Beweis sofort gezeigt:

**Beweis:** Wegen $10 \equiv -1 \bmod 11$ gilt $10^k \equiv (-1)^k \bmod 11$ für alle $k \geq 1$. Daher gilt:

$$a = a_0 + a_1 10^1 + \cdots + a_n 10^n \equiv a_0 - a_1 + a_2 - + \cdots \pm a_n \bmod 11$$

□

Zum Abschluss sei eine Teilbarkeitsregel durch 7 vorgestellt. Dazu brauchen wir folgenden Begriff: Es sei $a = a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 10^2 + a_1 10^1 + a_0$. Streicht man bei dieser Zahl die Einerziffer $a_0$, so entsteht eine neue Zahl $\overline{a} = a_1 + a_2 10^1 \cdots + a_n 10^{n-1}$. Diese bezeichnen wir im Folgenden als Testzahl. Jetzt können wir die Teilbarkeitsregel durch 7 aufstellen.

**Satz 5.3.** Eine Zahl $a$ ist genau dann durch 7 teilbar, wenn die um das Doppelte der Einerziffer von $a$ verminderte Testzahl $\overline{a}$ durch 7 teilbar ist.

Der Beweis zu diesem Satz ist nicht schwer:

**Beweis:**

$$\begin{aligned}
& a_n 10^n + a_{n-1} 10^{n-1} + \cdots + a_2 10^2 + a_1 10^1 + a_0 \equiv 0 \bmod 7 \\
\iff & 10 \cdot (a_n 10^{n-1} + a_{n-1} 10^{n-2} + \cdots + a_2 10^1 + a_1) + a_0 \equiv 0 \bmod 7 \\
\iff & 10 \cdot (a_n 10^{n-1} + a_{n-1} 10^{n-2} + \cdots + a_2 10^1 + a_1) - 20 a_0 \equiv 0 \bmod 7 \\
\iff & a_n 10^{n-1} + a_{n-1} 10^{n-2} + \cdots + a_2 10^1 + a_1 - 2 a_0 \equiv 0 \bmod 7
\end{aligned}$$

□

### 5.2.2 Die Wochentags- und Osterformel von Gauß

Für beide Formeln benötigt man den Begriff der Gauß-Klammer:

**Definition 5.2.1.** Mit der Gauß-Klammer $[x]$ bezeichnet man die größte ganze Zahl $\leq x$.

Dieser Begriff ist wahrscheinlich bis zu diesem Zeitpunkt im Unterricht nicht vorgekommen und man wird ihn zunächst ein wenig üben.

Die Wochentagsformel von Gauß erlaubt die Berechnung des Wochentages anhand eines gegebenen Datums. Sie wird auch im Lehrbuch der 5. Klasse AHS von Götz-Reichel (vgl. [24]) vorgestellt und ist ein einfaches Beispiel für die Anwendung des mod-Operators. Die Wochentagsformel von Gauß lautet:

**Satz 5.4.**

$$A = d + [2,6 \cdot m - 0,2] + y + \left[\frac{y}{4}\right] + \left[\frac{c}{4}\right] - 2c$$

$$w = A \bmod 7$$

Die auftretenden Variablen haben folgende Bedeutung

$A$ ..... Hilfsgröße
$d$ ..... Tagesdatum
$y$ ..... ist die aus den beiden letzten Ziffern der Jahreszahl gebildete Zahl
$c$ ..... ist die aus den beiden ersten Stellen der Jahreszahl gebildete Zahl
$m$ ..... Monat (wobei das Monat aus der Tabelle 5.1 abzulesen ist)

| Monat | März | April | Mai | Juni | Juli | Aug. | Sept. | Okt. | Nov. | Dez. | Jän. | Feb. |
|---|---|---|---|---|---|---|---|---|---|---|---|---|
| $m$ | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 |

Tabelle 5.1: Monatstabelle

Jänner und Februar sind also stets zu dem vorhergehenden Jahr zu zählen. Der Jänner 1990 entspricht dem Jänner 1989. Hat man $w$ mit der Hilfsvariabeln $A$ berechnet, so liest man aus der Tabelle 5.2 den Wochentag ab.

| Tag | So | Mo | Di | Mi | Do | Fr | Sa |
|---|---|---|---|---|---|---|---|
| $w$ | 0 | 1 | 2 | 3 | 4 | 5 | 6 |

Tabelle 5.2: Ergebnis: Wochentag

Es macht den Schülern sicher Spaß, jenen Wochentag zu berechnen, an dem sie auf die Welt gekommen sind.

Ostern ist ein beweglicher Feiertag. Seit dem Konzil von Nizäa im Jahre 325 nach Christus, wird das Osterfest am ersten Sonntag nach dem ersten Frühlingsvollmond gefeiert. Damit ist der 22. März der früheste Termin, der 25. April der letzte, auf den Ostern fallen kann. Vom Ostertermin hängen auch alle anderen beweglichen christlichen Feiertage ab.

Gauß gab eine Formel zur Berechnung des Osterdatums (=Datum des Ostersonntags) an. Sie lautet:

$A = \left[\frac{\text{Jahr}}{100}\right], \quad B = \left[\frac{\text{Jahr}}{400}\right]$
$M = 15 + A - B - \left[\frac{8 \cdot A + 13}{25}\right]$
$N = 4 + A - B$
$a = \ Jahr \bmod 19$
$b = \ Jahr \bmod 4$
$c = \ Jahr \bmod 7$
$d = (19 \cdot a + M) \bmod 30$
$e = (2 \cdot b + 4 \cdot c + 6 \cdot d + N) \bmod 7$
$\text{Ostern} \ = \ 22 + d + e$

Das Osterdatum wird als Märzdatum dargestellt. Zwei Ausnahmen sind zu beachten:
Stößt man bei der Berechnung auf Ostern $= 57$, so gilt Ostern $= 50$. Wenn $d = 28$ und $e = 6$ und $a > 10$ ist, dann gilt Ostern $= 49$.

Zum Nachrechnen: Ostern 1818 fiel auf den 22. März und Ostern 1886 auf den 25. April.

### 5.2.3 ISB-Nummern

Eine Reihe schöner Anwendungen für Kongruenzen bilden auch die internationalen Buchnummern, abgekürzt ISBN (**I**nternational **S**tandard **B**ook **N**umber). Das sind eindeutige 10- beziehungsweise seit 1. Januar 2007, 13-stellige Nummern zur Kennzeichnung von Büchern. An den ISB-Nummern erkennt man die Sprache, den Verlag und die Verlagsnummer eines Buches. Mit der ISBN wird eine nichtperiodische Veröffentlichung eines Verlags eindeutig identifiziert, eine bereits verwendete ISBN kann nicht noch einmal verwendet werden. Da bei der Ermittlung einer Bestellung oder beim Einlesen einer Artikelnummer oft Fehler passieren, ist die letzte Ziffer eine Kontrollnummer, die sich nach einfachen Regeln berechnet. Bei den bisherigen 10 stelligen ISB-Nummern ($a_1 a_2 \cdots a_9 a_0$) berechnete sich die Kontrollnummer $0 \leq a_0 \leq 9$ aus den vorhergehenden neun wie folgt:

$$a_0 = 1a_1 + 2a_2 + \cdots + 9a_9 \bmod 11 \qquad \left(a_0 \equiv \sum_{i=1}^{9} a_i \cdot i \bmod 11\right)$$

Also man multipliziert von links nach rechts die erste Ziffer mit eins, die zweite mit zwei, usw., summiert die entstehenden Produkte auf und der Rest dieser Summe bei der Division durch 11 ergibt dann die Kontrollnummer $a_0$. Man setzt $a_0 = X$, wenn der Rest 10 ist.

Mit DERIVE werden ISB-Nummern mit folgendem Programm (Autor: J. Wiesenbauer) auf Korrektheit überprüft:

```
ISBN(n, g_:=1, s_:=0) :=
  Loop
   If n = 0
    RETURN SOLVE(MOD(s_, 11) = 0)
   s_:+ g_·MOD(n, 10)
   g_:+ 1
   n := FLOOR(n, 10)
```

Eine weitere interessante Überlegung zu den ISB-Nummern stellt sich durch folgendes Problem: Man weiß, dass eine Nummer an einer bestimmten Stelle falsch ist. Kann man die richtige Ziffer an dieser Stelle berechnen? Diese Aufgabe führt auf eine lineare Kongruenz, welche mit DERIVE einfach zu lösen ist. Hat man zu diesem Zeitpunkt noch nicht mit den linearen Kongruenzen in der Klasse gearbeitet, so ergibt sich hier ein guter Einstieg in diesen Bereich der Zahlentheorie. Ein Beispiel:

Wir wissen, dass die dritte Ziffer der ISB-Nummer 3-87640-001-2 falsch ist. Man erhält folgende lineare Kongruenz

$$1 \cdot 3 + 2 \cdot 8 + 3 \cdot x + 4 \cdot 6 + 5 \cdot 4 + 6 \cdot 0 + 7 \cdot 0 + 8 \cdot 0 + 9 \cdot 1 = 3 \cdot x + 72 \equiv 2 \bmod 11,$$

also

$$3 \cdot x + 4 \equiv 0 \bmod 11.$$

Mit DERIVE ergibt sich $x = 6$:

```
SOLVE_MOD(3·x+4,x,11)=[6]
```

Ab 1. Jänner 2007 wird den bisherigen ISB-Nummern die Ziffernfolge “978” vorangestellt, die innerhalb der EAN (**E**uropäische **A**rtikel **N**ummerierung) für diese Verlagsprodukte vorgesehen ist. Die letzte Ziffer ändert sich dadurch auch, denn jetzt wird die Prüfziffer mit dem EAN-Verfahren aus allen vorangehenden Ziffern berechnet. Die Prüfziffer $0 \leq a_0 \leq 9$ einer solchen 13-stelligen Kontrollnummer $(978 - a_9 a_8 \cdots a_1 a_0)$ berechnet sich nun wie folgt:

$$10 - a_0 \equiv 3a_1 + 1a_2 + 3a_3 + \cdots + 3a_9 + 1 \cdot 8 + 3 \cdot 7 + 1 \cdot 9 \bmod 10$$

Bei der Berechnung werden also die Ziffern von links nach rechts abwechselnd mit 1 und 3 multipliziert, diese Produkte aufsummiert und aus dem Rest dieser Summe bei der Division durch 10

folgert man dann die Kontrollnummer $a_0$. So wird aus der ISBN-10 “3-86640-001-2” die ISBN-13 “978-3-86640-001-6”. Die Prüfziffer einer ISBN-13 ist stets eine arabische Ziffer.

Die Sozialversicherungsnummern folgen einem ähnlichen Prinzip wie die ISB-Nummern. Die folgende Summe der Ziffern hat modulo 11 gerechnet keinen Rest.

$$8a_1 + 4a_2 + 2a_3 + a_4 + 6a_5 + 3a_6 + 7a_7 + 9a_8 + 10a_9 + 5a_{10}$$

Bei einer Eingabe von ISBN, EAN oder Sozialversicherungsnummern können Fehler auftreten. Mögliche auftretende Fehler sind in der Tabelle 5.3 eingetragen.

| Fehlertyp | symbolisch | Rel. Häufigkeit in % |
|---|---|---|
| Einzel- oder Transkriptionsfehler | a → b | 79.1 |
| Transpositionsfehler | ab → ba | 10.2 |
| Übersprungener Vertauschungsfehler | acb → bca | 0.8 |
| Zwillingsfehler | aa → bb | 0.5 |
| Phonetischer Fehler | a0 → 1a (a = 2,...,9) | 0.5 |
| Übersprungener Zwillingsfehler | aca → bcb | 0.3 |

Tabelle 5.3: Fehlertypen

Wir wollen nun die einzelnen Fehler betrachten und herausfinden, ob diese in einem der beschriebenen Codes entdeckt werden. Kommt es zum Beispiel bei einer Sozialversicherungsnummer zu einem Einzelfehler oder zu einer Vertauschung von zwei Ziffern, so werden diese Fehler sofort erkannt:

Betrachten wir den Fall eines Einzelfehlers: An der i-ten Stelle steht statt einem $a_i$ ein $b_i$, dann gilt

$$\cdots + ga_i + \cdots = \cdots + gb_i + \cdots \equiv 0 \bmod 11,$$

wobei $g \in \{1, 2, \ldots, 10\}$ ist. Daraus folgt:

$$g(a_i - b_i) \equiv 0 \bmod 11$$

also $a - i = b_i$, da $g$ nicht durch 11 teilbar ist. Ein Einzelfehler würde also einer solchen Überprüfung nicht standhalten.

Nun betrachten wir den Fall, dass zwei Ziffern $a$ und $b$ in der Sozialversicherungsnummer vertauscht wurden:

$$\cdots + ga + \cdots + hb + \cdots = \cdots + gb + \cdots + ha + \cdots \equiv 0 \bmod 11,$$

wobei $g, h \in \{1, 2, \ldots, 10\}$. Man erhält

$$(g - h)(a - b) \equiv 0 \bmod 11,$$

also $a = b$, und daher würde auch so ein Fehler entdeckt werden.
Ein phonetischer Fehler kann bei einem EAN-Code ebenfalls aufgedeckt werden. Folgende beiden Möglichkeiten sind denkbar:

$$\cdots + a + 3 \cdot 0 + \cdots = \cdots + 1 + 3a + \cdots \equiv 0 \bmod 10$$

beziehungsweise

$$\cdots + 3a + 0 + \cdots = \cdots + 3 \cdot 1 + a + \cdots \equiv 0 \bmod 10$$

Durch Umformen erhält man

$$2a + 1 \equiv 0 \bmod 10$$

beziehungsweise

$$2a - 3 \equiv 0 \bmod 10,$$

und das ist unmöglich, da links jeweils eine ungerade Zahl steht.

Der ISBN-Code würde einen phonetischen Fehler nicht entdecken, da

$$\cdots + ga + (g - 1) \cdot 0 + \cdots = \cdots + g + (g - 1)a + \cdots \equiv 0 \bmod 11$$

vereinfacht

$$a \equiv g \bmod 11$$

ergibt. Wenn also die Ziffer $a$ mit der Stelle $g$ übereinstimmt, so kann der ISBN-Code den phonetischen Fehler nicht entdecken.

Alle weiteren Fehler können nachgerechnet werden. Hier ergeben sich viele Möglichkeiten die Schüler selbstständig arbeiten zu lassen.

### 5.2.4 Cäsar-Verschlüsselung

Julius Cäsar war nachweislich der erste, der seine Nachrichten verschlüsselte. In seinem Briefwechsel mit Cicero ersetzte er jeden Buchstaben seiner Nachricht durch den im Alphabet nach drei Stellen folgenden Buchstaben. Daher wird ein Verschlüsselungsverfahren durch Buchstabenverschiebung in der Kryptographie auch Cäsar-Verschlüsselung genannt. Mit Hilfe des Kongruenzbegriffes kann man sie leicht beschreiben:

Vor der Verschlüsselung des Textes werden die auftretenden Zeichen in Zahlen verwandelt. Dies kann durch die Stellung im Alphabet erfolgen:

| $A$ | $B$ | $C$ | ... | Z | Leerzeichen |
|---|---|---|---|---|---|
| 01 | 02 | 03 | ... | 26 | 00 |

Ersetzt man jeden Buchstaben durch den im Alphabet nach $e$ Stellen folgenden, so lautet die Verschlüsselungsvorschrift:

$$y = (x + e) \; mod \; 27$$

Die Zahl $e$ nennt man den "Schlüssel".

Wir wollen die Nachricht "MORGEN" mit $e = 11$ verschlüsseln. Wir schreiben die Nachricht zunächst als Zahlenfolge auf: 13, 15, 18, 07, 05, 14

Dann lautet die Vorschrift für die Verschlüsselung:

| $x$ | 13 | 15 | 18 | 07 | 05 | 14 |
|---|---|---|---|---|---|---|
| $y = (x + 11) \; mod \; 27$ | 24 | 26 | 02 | 18 | 16 | 25 |

Man erhält den Geheimtext: 24, 26, 02, 18, 16, 25 oder wieder in Buchstaben: "XZBRPY". Ist der Schlüssel $e$ bekannt, so kann ein verschlüsselter Text sofort entschlüsselt werden. Ist der Schlüssel nicht bekannt, so ist dies bei diesem Verfahren natürlich auch kein Problem, da nur höchstens 26 verschiedene Schlüssel durchprobiert werden müssen.

Auch die Entschlüsselung des verschlüsselten Textes ist in der Schule durchaus möglich. Beachtet man die Buchstabenhäufigkeit des deutschen Alphabets, dann ist die Entschlüsselung noch einfacher.

### 5.2.5 Zahlentrick

Ein schöner Zahlentrick geht auf Michael Stifel zurück, den der Mathematikhistoriker Moritz Cantor als den ersten großen Zahlentheoretiker bezeichnet. Michael Stifel (1487(?) - 1567) war ein Anhänger Luthers und bekleidete lange Zeit eine Pfarrstelle in der Nähe von Wittenberg, wo auch sein Hauptwerk "Artihmetica integra" (Die gesamte Arithmetik) entstand. Ganz interessant ist auch, dass Stifel sich mit der sogenannten Wortrechnung befasste. Damit versuchte er, Texte und Buchstaben der Bibel mathematisch zu deuten und kam so zu dem Ergebnis, dass die Welt am 8. Oktober 1533 um 8 Uhr morgens untergehen werde. Als der Untergang nicht eintraf, wurde er festgenommen und erst nach vierwöchiger Haft wieder freigelassen. Die Redewendung "einen Stiefel rechnen" geht auf diese Affäre zurück. Aber jetzt zu dem Zahlentrick, der in der "Arithmetica integra" zu finden ist:

Die Person A bildet das Produkt zweier aufeinanderfolgender natürlicher Zahlen, also $a(a+1)$.

Jetzt bittet man eine Person B sich eine beliebige natürliche Zahl $n < a(a+1)$ auszudenken und die Reste $r_1, r_2$ bei der Division durch $a$ und $a+1$ festzustellen und bekanntzugeben.
Die Person A rechnet nun $(a+1)r_1 + a^2 r_2 = s$ aus. Die von B ausgedachte Zahl $n$ ist dann der Rest von $s$ bei der Division durch $a(a+1)$ also $n = (a+1)r_1 + a^2 r_2 \bmod a(a+1)$.

**Beweis:** Es gilt:

$$n \equiv r_1 \bmod a \qquad \text{und} \qquad n \equiv r_2 \bmod a+1 \qquad \text{mit } 0 \le r_1 < a \text{ und } 0 \le r_2 < a+1$$

Daraus folgt (vgl. 5.9)

$$(a+1)n \equiv (a+1)r_1 \bmod a(a+1) \qquad \text{und} \qquad a^2 n \equiv a^2 r_2 \bmod a(a+1).$$

Addiert man diese beiden Kongruenzen, so erhält man:

$$(a+1)n + a^2 n \equiv (a+1)r_1 + a^2 r_2 \bmod a(a+1)$$

Beachtet man ferner, dass $(a+1)n + a^2 n = a(a+1)n + n$ ist, so folgt:

$$n \equiv (a+1)r_1 + a^2 r_2 \bmod a(a+1)$$

□

Bemerkung: $r_1 = 0$ und $r_2 = 0$ ist unmöglich, da $n < a(a+1)$ und $n$ bei der Division durch $a$ und $a+1$ nicht beide Male den Rest 0 haben kann.

In einer einfachen Form kann man den Zahlentrick jetzt etwa so formulieren:

Denk dir eine Zahl $n$ kleiner als 10000. Dividiere sie durch 101 und 102 ($101 \cdot 102 > 10000$) und nenne mir die beiden Reste $r_1$ und $r_2$. Ich kann dir dann deine gedachte Zahl sagen.

**Beispiel 5.2.1.** $n = 5647$, $r_1 = 92$, $r_2 = 37$,

$$(a+1)r_1 + a^2 r_2 = 386821 \equiv 5647 \bmod (101 \cdot 102)$$

# Kapitel 6

# Lösen von Kongruenzen

## 6.1 Lineare Kongruenzen

Hier begeben wir uns auf ein Gebiet der Zahlentheorie, das nur mehr in einem Wahlpflichtfach oder im Rahmen eines Spezialgebietes zur Matura gegeben werden kann. Hat man den Kongruenzbegriff bereits durchgenommen, so kann man die Schüler mit folgender Frage konfrontieren: Für welche Zahlen $x$ gilt die Kongruenz

$$2x \equiv 4 \bmod 6?$$

Die Ähnlichkeit mit einer linearen Gleichung fällt sofort auf. Die Bezeichnung "lineare Kongruenz" ist daher auch für Schüler naheliegend. Weiters erkennen sie unschwer, dass mit jeder Lösung $x$ auch jedes Element der Restklasse $\overline{x}$ eine Lösung ist. Durch Probieren findet man, dass alle Zahlen der Restklassen $\overline{2}$ modulo 6 und $\overline{5}$ modulo 6 Lösungen dieser Kongruenz sind. Es gibt also im Gegensatz zur linearen Gleichung $2x = 4$ zwei inkongruente Lösungen $x$ modulo 6. Hier wird man auch noch einmal daran erinnern, dass man nicht wie bei einer linearen Gleichung durchkürzen kann (vgl. 5.9).

Weitere Beispiele - Schüler können selbst solche linearen Kongruenzen aufschreiben - zeigen, dass so eine lineare Kongruenz keine, eine oder mehrere Lösungen haben kann. Vielleicht gelingt es mit geeigneten Beispielen folgenden Satz gemeinsam mit den Schülern zu finden:

**Satz 6.1.**
Die lineare Kongruenz

$$ax \equiv b \mod \mathrm{m} \tag{6.1}$$

ist genau dann lösbar, wenn $ggT(a, m) \mid b$. In diesem Fall gibt es genau $ggT(a, m)$ inkongruente Lösungen modulo $m$.

Man muss diesen Satz nicht unbedingt beweisen. Es ist schon viel gewonnen, wenn man ihn gemeinsam mit den Schülern erarbeitet hat. Der Beweis setzt neben einem sicheren Umgehen mit den

Teilbarkeitsregeln auch die Kenntnis des erweiterten Euklidischen Algorithmus voraus und erfordert große Genauigkeit:

**Beweis:**
Wir nehmen zunächst an, dass die lineare Kongruenz $ax \equiv b \bmod m$ eine Lösung hat und setzen $d = ggT(a, m)$. Da $d \mid a$ und $d \mid m$ und $m \mid ax - b$ folgt, dass $d \mid b$. Notwendig für die Lösbarkeit der Kongruenz ist also die Bedingung $d \mid b$.

Ist sie auch ein hinreichende Bedingung, das heißt gibt es eine Lösung wenn $d \mid b$? Um das zu zeigen müssen wir eine Lösung dieser Kongruenz konstruieren: Nach dem erweiterten Euklidischen Algorithmus gibt es zwei ganze Zahlen $u$ und $v$, sodass

$$d = ggT(a, m) = au + mv.$$

Multipliziert man diese Gleichung mit $r = \frac{b}{d}$, was ja nach Voraussetzung eine ganze Zahl ist, so erhält man

$$b = d \cdot r = aur + mvr,$$

und daraus ergibt sich

$$aur \equiv b \bmod m.$$

Wir haben also mit $x = ur$ eine Lösung dieser Kongruenz gefunden.

Die Bedingung $d \mid b$ ist also auch hinreichend für die Lösbarkeit dieser Kongruenz. Damit ist der erste Teil des Satzes gezeigt.

Es sei nun $x_0$ eine fixe Lösung (etwa die durch den erweiterten Euklidischen Algorithmus gefundene) und $x$ eine weitere Lösung dieser Kongruenz. Dann gilt:

$$ax \equiv ax_0 \bmod m \quad \text{also} \quad m \mid a(x - x_0)$$

Jetzt setzen wir $\frac{m}{d} = r$ und $\frac{a}{d} = s$. Da $d$ der größte gemeinsame Teiler von $a$ und $m$ ist, sind $r$ und $s$ teilerfremd, also $ggT(r, s) = 1$. Es gilt nun

$$m \mid a(x - x_0) \Longleftrightarrow r \mid s(x - x_0) \Longleftrightarrow r \mid x - x_0 \Longleftrightarrow x \equiv x_0 \bmod (r = \frac{m}{d}).$$

Alle Lösungen der linearen Kongruenz haben daher die Form

$$x = x_0 + k \cdot \frac{m}{d}$$

und jedes so gebildete $x$ ist auch tatsächlich Lösung der Kongruenz:

$$ax = ax_0 + ak \cdot \frac{m}{d} = ax_0 + \frac{a}{d} \cdot km = ax_0 + skm \equiv b \bmod m$$

Jetzt bleibt nur mehr die Anzahl der Lösungen festzustellen. Es seien $x_1 = x_0 + k_1 \cdot \frac{m}{d}$ und $x_2 = x_0 + k_2 \cdot \frac{m}{d}$ zwei Lösungen mit $x_1 \equiv x_2 \bmod m$. Dann folgt:

$$x_1 \equiv x_2 \bmod m \Longleftrightarrow x_0 + k_1 \cdot \frac{m}{d} \equiv x_0 + k_2 \cdot \frac{m}{d} \bmod m \Longleftrightarrow k_1 \equiv k_2 \bmod d$$

Es gibt also genau $x_0, x_1, \ldots, x_{d-1}$ inkongruente Lösungen modulo $d$.

□

Ein wichtiger Spezialfall ist der Fall $b = 1$. Der größte gemeinsame Teiler von $a$ und $m$ teilt nun $b$ genau dann, wenn $ggT(m, a) = 1$. Für diesen Spezialfall können wir obigen Satz daher so formulieren:

**Satz 6.2.**
Sind $a$ und $m > 1$ zwei teilerfremde positive ganze Zahlen, so gibt es (genau) eine natürliche Zahl $x < m$, die Lösung der linearen Kongruenz

$$ax \equiv 1 \bmod m \tag{6.2}$$

ist.

Diese eindeutige Lösung $x$ wird manchmal auch als das zu $a$ inverse Element $a^{-1} \bmod m$ bezeichnet.

**Beispiel 6.1.1.** Man bestimme alle Lösungen der Kongruenz $15x \equiv 6 \bmod 33$.

**Lösung:** Wegen $ggT(15, 33) = 3$ und $3 \mid 6$ hat diese lineare Kongruenz 3 inkongruente Lösungen modulo 33. Mit dem erweiterten Euklidischen Algorithmus sucht man jetzt ganze Zahlen $x$ und $y$, sodass $33x + 15y = 3$ ist. Bei dieser Aufgabe braucht man aber nicht viel zu rechnen, man sieht unmittelbar:

$$33 \cdot 1 + 15 \cdot (-2) = 3 \quad \text{also} \quad 33 \cdot 2 + 15 \cdot (-4) = 6$$

Daraus folgt

$$15 \cdot (-4) \equiv 6 \bmod 33 \quad \text{also} \quad 15 \cdot 29 \equiv 6 \bmod 33.$$

Damit haben wir mit $x_1 = 29$ eine Lösung modulo 33 gefunden. Die beiden anderen Lösungen modulo 33 sind dann $x_2 = 29 + 1 \cdot \frac{33}{3} = 40 \equiv 7 \bmod 33$ und $x_3 = 29 + 2 \cdot \frac{33}{3} = 51 \equiv 18 \bmod 33$.

□

Lineare Kongruenzen können auch mit DERIVE einfach gelöst werden. Dazu verwendet man den Befehl:

```
SOLVE_MOD(u, x, m)
```

Nun lösen wir das vorherige Beispiel mit DERIVE:

```
SOLVE_MOD(15x-6,x,33)=[7,18,29]
```

## 6.2 Chinesischer Restsatz

Hier kann ein kleiner Kartentrick als Einstieg dienen.

Man hat zu Hause 42 verschiedene Karten vorbereitet, deren Reihenfolge man sich auf einem Zettel notiert hat, etwa 1 (oberste Karte) = Pik 10, 2 (darunterliegende Karte) = Karo Dame usw., das heißt jeder Zahl von 1- 42 ist ein eindeutiges Kartenmotiv zugeordnet. Jetzt legt man der Reihe nach die 42 Karten in Form eines Rechtecks mit sieben Zeilen und sechs Spalten auf, das heißt in der ersten Zeile liegen der Reihe nach die Karten 1-6, in der zweiten Zeile die Karten 7-12 usw. Man bittet einen Schüler sich eine Karte zu denken und bekanntzugeben, in welcher Spalte sie sich befindet. Jetzt sammelt man die Karten ein und zwar so, dass sie in der gleichen Reihenfolge zu liegen kommen, wie zu Beginn des Spieles, das heißt oben die Karte 1 (Pik 10), dann 2 (Karo Dame) usw. Jetzt werden die Karten aufs neue ausgelegt, diesmal in Form eines Rechtecks mit sechs Zeilen und sieben Spalten, das heißt in der ersten Zeile liegen die Karten 1-7, in der zweiten Zeile die Karten 8-14, usw. Der Schüler wird nocheinmal gefragt in welcher Spalte die Karte nun liegt und man kann dann nach einer kurzen Rechnung mitteilen, welche Karte er sich zu Beginn gedacht hat: Hat man etwa als erste Antwort Spalte 3 und als zweite Antwort Spalte 5 bekommen, so kann man den Schülern folgendermaßen erklären, wie der Kartentrick funktioniert:

Es gilt

$$x \equiv 3 \bmod 6 \quad \text{und} \quad x \equiv 5 \bmod 7,$$

also

$$x = 3 + 6r \quad \text{und} \quad x = 5 + 7s.$$

Daraus folgt

$$3 + 6r = 5 + 7s \iff 6r = 2 + 7s \iff 6r \equiv 2 \bmod 7 \iff r \equiv 5 \bmod 7 \iff r = 5 + 7t,$$

und somit

$$x = 3 + 6r = 3 + 6(5 + 7t) = 33 + 42t.$$

Der Schüler hat sich also die 33-ste Karte gedacht, man muss nur mehr am "Motivzettel" nachsehen und das entsprechende Ergebnis bekanntgeben.

Bemerkung: Als Lehrer wird man sich vorher die einfache Formel $x = 7a - 6b + 42k$, wobei $a$ und $b$ die entsprechenden Spaltenwerte sind, zurechtlegen. Damit kann man sehr rasch das entsprechende Ergebnis ermitteln.

Funktioniert dieser Kartentrick nun immer? Erstaunlicher Weise ja, wenn die Zerlegung der Anzahl $n$ der Karten in ein Produkt $n = p \cdot q$ zweier teilerfremder Faktoren $p$ und $q$ größer 1 möglich ist.

Darüber gibt uns der Chinesische Restsatz Auskunft, den man im Anschluss daran vorstellen kann. Man betrachtet das System linearer Kongruenzen

$$x \equiv a_1 \bmod m_1$$

$$x \equiv a_2 \bmod m_2$$

$$\ldots\ldots$$

$$x \equiv a_n \bmod m_n,$$

für die man alle Lösungen $x \in \mathbb{Z}$ bestimmen soll. Also man sucht Zahlen, die sämtliche lineare Kongruenzen gleichzeitig lösen. Ein solches System muss aber keine Lösungen haben. Beispielsweise gibt es für das System

$$x \equiv 3 \bmod 4$$

$$x \equiv 1 \bmod 8$$

keine Lösung, da aus $x \equiv 1 \bmod 8$ auch $x \equiv 1 \bmod 4$ folgt. Daher müsste $x$ bei der Division durch 4 den Rest 3 und den Rest 1 lassen, was unmöglich ist. Daher ist es sinnvoll nur paarweise teilerfremde Modulen zuzulassen. Jetzt kann man den Chinesischen Restsatz formulieren:

**Satz 6.3. Der Chinesische Restsatz**

Es seien $m_1, m_2, \ldots, m_n$ paarweise teilerfremde natürliche Zahlen größer als 1 und $a_1, a_2, \ldots, a_n$ ganze Zahlen, dann gibt es genau ein $x$ modulo $m_1 m_2 m_3 \cdots m_n$, sodass

$$x \equiv a_i \bmod m_i \quad \text{für } i = 1, 2, \ldots, n.$$

**Beweis:** Wir beweisen die Existenz einer solchen Lösung durch vollständige Induktion. Für $n = 1$ ist nichts zu zeigen.

Wir zeigen nun den Schritt von $n$ auf $n + 1$:

Es sei $M = m_1 m_2 \cdots m_n$. Die Induktionsvoraussetzung lautet nun: Es gibt ein $a \in \mathbb{Z}$ mit

$$a \equiv a_i \bmod m_i \quad \text{für } i = 1, 2, \ldots, n.$$

Wir setzen nun $x = a + y \cdot m$ mit einem unbekannten $y \in \mathbb{Z}$. Dieses $x$ erfüllt wegen der Wahl von $a$ jedenfalls die Kongruenzen

$$x \equiv a + y \cdot m \equiv a \equiv a_i \bmod m_i \quad \text{für } i = 1, 2, \ldots, n.$$

Wir müssen jetzt nur mehr das $y$ so wählen, dass auch die letzte Kongruenz

$$x \equiv a + y \cdot m \equiv a \equiv a_{n+1} \bmod m_{n+1}$$

erfüllt ist. Diese Kongruenz ist aber äquivalent zu

$$y \cdot m \equiv a_{n+1} - a \bmod m_{n+1}$$

und diese ist nach Satz 6.2 lösbar, weil laut Voraussetzung $ggT(m, m_{n+1}) = 1$ gilt. Damit haben wir die Existenz einer Lösung gezeigt, es bleibt nur mehr die Eindeutigkeit zu beweisen: Sind $a$ und $a'$ ($a, a' \in \mathbb{Z}$) zwei Zahlen, die alle Kongruenzen

$$x \equiv a_i \bmod m_i \quad \text{für } i = 1, 2, \ldots, n$$

erfüllen, dann gilt:

$$m_i \mid (a - a') \quad \text{für } i = 1, 2, \ldots, n$$

Da aber $m_1, m_2, \ldots, m_n$ paarweise teilerfremde natürliche Zahlen sind, folgt

$$m_1 m_2 m_3 \cdots m_n \mid (a - a'),$$

die Zahlen $a$ und $a'$ sind also kongruent modulo $m_1 m_2 m_3 \cdots m_n$.

□

Der Beweis der Existenz einer Lösung durch vollständige Induktion ist deswegen naheliegend, weil man beim praktischen Durchrechnen eines solchen Systems analog vorgeht.

**Beispiel 6.2.1.** Ein Vater hat fünf Söhne und will eine (zweistellige) Anzahl Schafe vererben. Er sagt: Wenn ich zweien meiner Söhne die gleiche Anzahl gebe, bleibt ein Schaf übrig; gebe ich dreien die gleiche Anzahl, bleiben zwei Schafe übrig; gebe ich vieren die gleiche Anzahl, bleiben drei übrig; gebe ich schließlich allen fünfen die gleiche Anzahl, sind noch vier übrig. Wie viele Schafe ($x$) hatte der Mann mindestens?

**Lösung:** Es muss zunächst gelten:

1. $x \equiv 1 \bmod 2$
2. $x \equiv 2 \bmod 3$
3. $x \equiv 3 \bmod 4$
4. $x \equiv 4 \bmod 5$

Aus der ersten und der zweiten Kongruenz folgt

$$x = 2t_1 + 1 \equiv 2 \bmod 3 \iff 2t_1 \equiv 1 \bmod 3 \iff t_1 \equiv 2 \bmod 3.$$

Daraus folgt $t_1 = 3t_2 + 2$ und daher $x = 2t_1 + 1 = 2(3t_2 + 2) + 1 = 6t_2 + 5$.

Mit der dritten Kongruenz folgt

$$6t_2 + 5 \equiv 3 \bmod 4 \iff 6t_2 \equiv 2 \bmod \iff 3t_2 \equiv 1 \bmod 2 \iff t_2 \equiv 1 \bmod 2.$$

Daher gilt $t_2 = 2t_3 + 1$ also $x = 6t_2 + 5 = 6(2t_3 + 1) + 5 = 12t_3 + 11$.

Daraus folgt mit der vierten und letzten Bedingung

$$12t_3 + 11 \equiv 4 \bmod 5 \Longleftrightarrow 12t_3 \equiv 3 \bmod 5 \Longleftrightarrow t_3 \equiv 4 \bmod 5.$$

Daher ist $t_3 = 5t_4 + 4$ und wir erhalten $x = 12t_3 + 11 = 12(5t_4 + 4) + 11 = 60t_4 + 59$.

Die minimale Anzahl von Schafen ist daher 59.

□

Zu diesem Chinesischen Restsatz gibt es eine Unzahl von interessanten Aufgaben. Schriftlich überliefert sind uns solche Problemstellungen erstmals im Suan-ching (Handbuch der Arithmetik) des Chinesen Sun-Tsu. Er stellt dort unter anderem folgende Aufgabe:

"Wir haben eine gewisse Anzahl von Pferden, wissen aber nicht genau wie viele. Wenn wir sie zu je drei zählen, bleiben zwei übrig. Wenn wir sie zu je fünf zählen, bleiben drei übrig. Wenn wir sie zu je sieben zählen bleiben zwei übrig. Wie viele Pferde sind es? Die kleinste mögliche Zahl ist gesucht."

Hinzuweisen ist hier noch auf den DERIVE-Befehl

CRT([$a_1$,$a_2$,...,$a_n$],[$m_1$,$m_2$,...,$m_n$]),

mit dem ein System von linearen Kongruenzen unmittelbar lösbar ist.

# Kapitel 7

# Diophantische Gleichungen

## 7.1 Lineare diophantische Gleichungen

Als Einstieg zu diesem Kapitel wählt man ein klassisches Beispiel: Ein Bauer bekommt die Aufgabe, auf dem Markt für 1000 Taler Ferkel, Enten und Tauben zu kaufen; und zwar genau 1000 Tiere und von jedem mindestens eines. Ein Ferkel kostet 10 Taler, eine Ente 3 Taler und eine Taube einen halben Taler. Bestimme alle Möglichkeiten, natürlich sollen dabei die Tiere lebendig und vollständig sein.

Mit Einführung der Variablen $x$ (Anzahl der Ferkels), $y$ (Anzahl der Enten) und $z$ (Anzahl der Tauben) schreibt man die entsprechenden Gleichungen auf und erhält:

$$10x + 3y + 0,5z = 1000 \text{ und } x + y + z = 1000 \Longrightarrow 19x + 5y = 1000$$

Wir suchen nun alle ganzzahligen positiven Lösungen dieser Gleichung. Gleichungen, deren Lösungen man nur in der Menge der ganzen Zahlen $\mathbb{Z}$ sucht, heißen nach dem griechischen Mathematiker Diophantus von Alexandrien (3. Jahrhundert nach Christus) "diophantische Gleichungen". Hier hat man es im Speziellen mit einer linearen diophantischen Gleichung in zwei Variablen zu tun. Obige Gleichung kann man auch so anschreiben:

$$y = 200 - 4x + \frac{x}{5}$$

Daraus folgt sofort, dass die Anzahl der Ferkel ein Vielfaches von 5 sein muss und man folgert unschwer die zehn richtigen Lösungstripel:

$$(5,\ 181,\ 814),\ (10,\ 162,\ 828),\ \ldots,\ (50,\ 10,\ 910)$$

Diese Aufgabe ist sicher eine diophantische Gleichung, die man ohne viel zahlentheorisches Wissen lösen kann und die Schüler werden wahrscheinlich selbständig die Lösungen finden. Diese Aufgabe

eignet sich durchaus als “Auflockerung” im Regelunterricht, etwa ab der achten Schulstufe.

Man kann hier noch einige Fragen anschließen:

Gibt es diophantische Gleichungen in zwei Variablen, die keine Lösung haben?
Was stellen die Lösungen einer solchen Gleichung dar, wenn man sie geometrisch betrachtet?
Werden die Gleichungen immer so einfach zu lösen sein, wie die hier angegebene? usw.

Fragen, die sicher das Interesse der Schüler wecken, aber auch die im Unterricht erlernten Methoden und Begriffe (Geradengleichung, Äquivalenzumformungen) festigen.

Behandelt man dieses Thema in einem Wahlpflichtfach, wird man ansschließend daran diesen Satz bringen:

**Satz 7.1.**
Die lineare diophantische Gleichung

$$ax + by = c \tag{7.1}$$

ist genau dann lösbar, wenn der

$$ggt(a, b) \mid c.$$

**Beweis:** Gibt es eine Lösung, dann gilt klarerweise $ggT(a, b) \mid c$.

Es gilt also $d = ggT(a, b)$ und $d \mid c$. Wir müssen zeigen, dass die diophantische Gleichung eine Lösung hat. Nach dem erweiterten Euklidischen Algorithmus gibt es Zahlen $x'$ und $y'$ mit

$$ax' + by' = d.$$

Multipliziert man diese Gleichung mit der ganzen Zahl $\frac{c}{d}$, so erhält man

$$a\frac{cx'}{d} + b\frac{cy'}{d} = d\frac{c}{d} = c,$$

und mit $(x_0 = \frac{cx'}{d}, y_0 = \frac{cy'}{d})$ hat man eine Lösung der diophantischen Gleichung gefunden.

□

Bemerkungen:

- Analog gilt dieser Satz auch für eine lineare Gleichung in drei, vier, …, n Variablen. Auf einen Beweis (etwa durch vollständige Induktion) wird man verzichten.

- Alle Lösungen der linearen diophantischen Gleichung 7.1 sind gegeben durch $x = x_0 + \frac{bk}{d}$ und $y = y_0 - \frac{ak}{d}$, wobei $k$ eine beliebige ganze Zahl ist. Danach wird man von den Schülern sicherlich gefragt.

  Das überlegt man sich wie folgt: Es sei $x$ neben $x_0$ eine weitere Lösung von 7.1. Dann gilt:

  $$ax + by = c \text{ und } ax_0 + by_0 = c \Longrightarrow a(x - x_0) + b(y - y_0) = 0 \Longrightarrow \frac{a}{d}(x - x_0) + \frac{b}{d}(y - y_0) = 0.$$

  Daraus folgt, da $\text{ggt}(\frac{a}{d}, \frac{b}{d}) = 1$

  $$\frac{a}{d} \mid (y - y_0) \text{ und } \frac{b}{d} \mid (x - x_0).$$

  Also gilt

  $$x - x_0 = \frac{bk}{d} \text{ und } y - y_0 = \frac{ak}{d} \text{ mit } k \in \mathbb{Z}.$$

  Man überlegt sich umgekehrt leicht, dass die so gewonnenen Lösungen $(x, y)$ tatsächlich der Gleichung 7.1 genügen.

- Wissen die Schüler schon über lineare Kongruenzen Bescheid, dann wird man auch auf den Zusammenhang von $ax + by = c$ (vgl. 7.1) mit der linearen Kongruenz $ax \equiv c \bmod b$ (vgl. 6.1) hinweisen.

## 7.2 Pythagoräische Tripel, Indische Formeln

Es geschieht nicht häufig, dass ein mathematisches Problem auf ein breiteres Interesse stößt. Meistens ist schon die aufgestellte Behauptung so unverständlich, dass man an die Beweisführung erst gar nicht denken mag. Ganz anders verhält es sich bei der Fermat'schen Vermutung, denn mehr als etwas Schulmathematik bedarf es nicht, um sie zu begreifen. Diese Vermutung besagt, dass es keine von Null verschiedenen ganzen Zahlen $a$, $b$, $c$ gibt, welche der Gleichung $a^n + b^n = c^n$ genügen, sobald der Exponent $n$ größer als zwei ist. Fermat stellte seine Vermutung um das Jahr 1637 herum, also vor fast genau 370 Jahren, auf. Zur Popularisierung hat sicherlich auch die Behauptung Fermats beigetragen, er habe einen wahrhaft wunderbaren Beweis gefunden, doch sei der Buchrand zu schmal, um ihn zu fassen. [1]

[1] *Cubum autem in duos cubos aut quadrato quadratum in duos quadrato quadratos et generaliter nullam in infinitum quadratum potestatem in duos eiusdem nominis fas est dividere. Cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.*
Die deutsche Übersetzung dieser lateinischen Randnotiz lautet: *Es ist nicht möglich, einen Kubus in zwei Kuben oder ein Biquadrat in zwei Biquadrate und allgemein eine Potenz, höher als die zweite, in zwei Potenzen mit demselben Exponenten zu zerlegen. Ich habe hierfür einen wahrhaft wunderbaren Beweis, doch ist der Rand hier zu schmal, um ihn zu fassen.* [15]

Unzählige Lösungsversuche wurden unternommen, doch erst 1995 gelang es dem britischen, in Princeton (New Jersey, USA) lehrenden Mathematiker Andrew Wiles gemeinsam mit Richard Taylor diese Vermutung von Fermat zu beweisen.

Diesen Satz kann man nun zum Einstieg verwenden um eine Unterrichtseinheit über pythagoräische Zahlentripel zu gestalten.

Man motiviert die Schüler mit der Frage: Wie stieß Fermat auf seine Vermutung? Bevor man diese Frage beantwortet, erinnert man an den Lehrsatz des Pythagoras: Ist ein rechtwinkliges Dreieck mit den beiden Katheten $a$, $b$ und der Hypothenuse $c$ gegeben, so besteht nach Pythagoras die Beziehung

$$a^2 + b^2 = c^2. \tag{7.2}$$

Es stellt sich dann sogleich die Frage, ob es positive natürliche Zahlen $a$, $b$, $c$ gibt, welche die Gleichung erfüllen. Das wohl bekannteste Beispiel dazu ist das Tripel $(a, b, c) = (3, 4, 5)$.

Nun macht man sich mit den Schülern auf die Suche nach weiteren pythagoräischen Tripeln. Es wird den Schülern keine großen Schwierigkeiten bereiten einige weitere pythagoräische Zahlentripel zu finden: (3, 4, 5), (6, 8, 10), (5, 12, 13), (10, 24, 48), (20, 24, 24), (15, 8, 17), ...

Hier kann man die Geschichte der Mathematik einfließen lassen. Bei den Pythagoräern wurden solche ganzzahligen Tripel $(a, b, c)$ besonders verehrt, da sie harmonischen Verhältnissen entsprechen. Diese pythagoräischen Zahlentripel waren zum Teil aber auch schon den Babyloniern etwa 1600 vor Christus bekannt. Man entdeckte eine Tontafel ("Plimpton 322") von den Babyloniern, die eine Liste mit 15 Dreiecken dieser Eigenschaft aufweist. Damit konnten sie nämlich leicht rechte Winkel mit Seilen konstruieren, was ihnen bei der Landvermessung zu Gute kam. Diophantes stellte dann die Frage nach einer systematischen Berechnung pythagoräischer Zahlentripel. Damit hängt insbesondere auch die Frage zusammen, ob es endlich viele oder gar unendlich viele solcher Zahlentripel gibt. Seine Formeln findet man jedoch schon in den indischen Texten der Sulvasutras, die ca. 500 - 200 vor Christus lebten. Deshalb heißen die Formeln zur Berechnung der pythagoräischen Tripel auch Indische Formeln.

Fermat hat sich nun sicher damit beschäftigt und sich die Frage gestellt, wie viele Lösungstripel $(a, b, c)$, bestehend aus positiven natürlichen Zahlen, es gibt, wenn in der Gleichung 7.2 der Exponent 2 durch den Exponenten $n > 2$ ersetzt wird. Aufgrund seiner Untersuchungen kam er zum Schluss, dass es unter diesen Umständen - im Gegensatz zum Fall pythagoräischer Zahlentripel - kein einziges solches Zahlentripel $(a, b, c)$ gibt und stellte seine berühmte Vermutung auf.

Der Beweis der Indischen Formeln ist erst in einer siebenten oder achten Klasse Oberstufe möglich. Es gehört aber in jeden Mathematikunterricht, über Fermats Behauptung zu reden, über die Geschichte des Satzes zu erzählen, pythagoräische Zahlentripel zusammenzustellen und eventuell die Indischen Formeln ohne Beweis anzugeben. Das Thema fasziniert die Schüler und ermöglicht einen wunderbaren Einblick in die Welt der Mathematik.

## 7.2 Pythagoräische Tripel, Indische Formeln

Bevor man mit der Herleitung der Indischen Formeln beginnt, sollte intensiv mit Kongruenzen und Teilbarkeit gearbeitet worden sein.

Folgende einfache Überlegungen werden vorangestellt:

- Mit jedem Tripel $(a, b, c)$ ist auch das Tripel $(ta, tb, tc)$ mit positivem ganzen $t$ ein pythagoraisches Zahlentripel und umgekehrt. Es reicht daher nur Tripel mit $ggT(a, b, c) = 1$ zu suchen.
- Aus $ggT(a, b, c) = 1$ folgt unmittelbar unter der Verwendung von $a^2 + b^2 = c^2$, dass alle Glieder paarweise teilerfremd sind:

$$ggT(a, b) = 1 \qquad ggT(b, c) = 1 \qquad ggT(a, c) = 1 \tag{7.3}$$

- Ist $(a, b, c)$ ein pythagoräisches Tripel mit $ggT(a, b, c) = 1$, dann ist auch $(b, a, c)$ ein pythagoräisches Tripel mit $ggT(b, a, c) = 1$. Es genügt daher alle Tripel $(a, b, c)$ mit $ggT(a, b, c) = 1$ und ungeradem $a$ zu ermitteln.

Darüber gibt nun folgender Satz Auskunft:

**Satz 7.2.**
Das Tripel $(a, b, c)$ ist genau dann ein pythagoräisches Tripel mit ungeradet'm $a$ und $ggT(a, b, c) = 1$, wenn es natürliche Zahlen $u$, $v$ gibt mit $ggT(u, v) = 1$, $u > v$, von denen eine gerade und eine ungerade ist, sodass folgende Beziehungen gelten:

$$a = u^2 - v^2, \qquad b = 2uv, \qquad c = u^2 + v^2 \qquad \text{“Indische Formeln”} \tag{7.4}$$

Bemerkung: Aus diesen Tripeln kann man durch Multiplizieren mit einer natürlichen Zahl $t$ und eventuelles Vertauschen der ersten beiden Glieder nun jedes pythagoräisches Tripel gewinnen.

**Beweis:** “⇒” Wir wollen also alle pythagoräischen Zahlentripel mit $ggT(a, b, c) = 1$ und ungeradem $a$ ermitteln.
Zunächst folgende Überlegung: Sind sowohl $a$ als auch $b$ ungerade Zahlen, dann gilt:

$$a^2 \equiv 1 \bmod 4 \qquad \text{und} \qquad b^2 \equiv 1 \bmod 4 \qquad \text{und daher} \qquad c^2 \equiv 2 \bmod 4.$$

Das ist aber unmöglich, da jede Quadratzahl bei der Division durch 4 den Rest 1 oder 0 lässt. Hier sollten Beispiele zur Erklärung berechnet oder der Beweis selbst gezeigt werden. Es ist daher $b$ gerade und $c$ ungerade.

Die Gleichung 7.2 können wir daher so schreiben:

$$b^2 = c^2 - a^2 = (c + a)(c - a)$$

und daraus folgt, da $b$, $(c + a)$ und $(c - a)$ gerade sein müssen:

$$\left(\frac{b}{2}\right)^2 = \frac{c + a}{2} \cdot \frac{c - a}{2}.$$

Weil $a$ und $c$ keinen gemeinsamen Teiler (vgl. 7.3) haben können, haben auch $(c + a) / 2$ und $(c - a) / 2$ keinen gemeinsamen Teiler. Auch dieser Schritt gehört in der Schule genau ausgeführt: Hätten $(c + a) / 2$ und $(c - a) / 2$ einen gemeinsamen Teiler größer als 1, dann würde er auch die Summe und die Differenz dieser beiden Zahlen, also $c$ beziehungsweise $a$, teilen. Das steht aber im Widerspruch zu $ggT(a, c) = 1$ (vgl. 7.3).

Das Produkt dieser beiden Zahlen kann daher nur dann eine Quadratzahl ergeben, wenn die beiden Faktoren selbst Quadratzahlen sind. Das folgt aus der eindeutigen Primfaktorzerlegung. Wir setzen daher

$$\frac{c+a}{2} = u^2 \qquad \frac{c-a}{2} = v^2$$

für gewisse $u$ und $v$. Daraus sind nun $a$, $b$ und $c$ berechenbar und es ergeben sich die Indischen Formeln:

$$a = u^2 - v^2, \qquad b = 2uv, \qquad c = u^2 + v^2$$

- Aus $a = u^2 - v^2$ folgt $u > v$.
- Aus $c \equiv 1 \bmod 2$ folgt, dass von $u$ und $v$ eine Zahl ungerade und eine gerade ist.
- Aus $a = u^2 - v^2$, $c = u^2 + v^2$ und $ggT(a, c) = 1$ folgt $ggT(u, v) = 1$.

"⇐" Es seien nun umgekehrt $u$ und $v$ zwei natürliche Zahlen mit den oben angeführten Eigenschaften und $(a, b, c)$ das entsprechend den Indischen Formeln gebildete Zahlentripel. Man rechnet leicht nach, dass es auch tatsächlich ein pythagoräisches Zahlentripel darstellt:

$$\begin{aligned}(u^2 - v^2)^2 + (2uv)^2 &= (u^2 + v^2)^2 \\ u^4 - 2u^2v^2 + v^4 + 4u^2v^2 &= u^4 + 2u^2v^2 + v^4 \\ u^4 + 2u^2v^2 + v^4 &= u^4 + 2u^2v^2 + v^4\end{aligned}$$

Nun stellt sich noch die Frage, ob $a$ auch wirklich ungerade, $b$ gerade und der $ggT(a, b, c) = 1$ ist.

- $b$ ist gerade, da $b = 2uv$ gilt.
- $a$ ist ungerade, da die Differenz von einer ungeraden und einer geraden Zahl immer ungerade ist.
- Es gilt $ggT(u, v) = 1$, $u > v$, $u$ ungerade und $v$ gerade. Annahme: Es gibt einen $ggT(a, b, c) = t > 0$. Dann gibt es aber auch eine Primzahl $p$, die $a$, $b$ und $c$ teilt. Daraus folgt:

$$p \mid u^2 - v^2 \wedge p \mid u^2 + v^2$$

Also teilt $p$ auch die Summe und die Differenz von $a$ und $c$, also $p \mid 2u^2$ und $p \mid 2v^2$. Da weiters $p$ nicht 2 ist ($a$ ungerade), folgt:

$$p \mid u^2 \wedge p \mid v^2 \Rightarrow p \mid u \wedge p \mid v.$$

Das ist aber ein Widerspruch, da $ggT(u, v) = 1$ ist, also gilt $ggT(a, b, c) = 1$.

□

Man braucht nicht viele zahlentheoretische Begriffe (Kongruenzen, größter gemeinsamer Teiler, Eindeutigkeit der Primfaktorzerlegung) um diesen Beweis zu führen, trotzdem stellt er hohe Anforderungen an die Schüler. Erstens sind wahrscheinlich die Grundlagen nicht genügend eingeübt und zweitens sind viele Schüler aus dem Regelunterricht gar nicht daran gewöhnt einen derart exakten Beweis durchzuführen. Innerhalb einer Klasse mit normalem Leistungsnieveau ist von diesem Beweis abzuraten. In einem Wahlpflichtfach, als Spezialgebiet bei der Matura oder als Projekt mit interessierten Schülern ist er aber durchaus möglich.

Nach der Berechnung der Indischen Formeln können wir in einer Liste auch $u$ und $v$ eintragen, um daraus die pythagoräischen Zahlentripel zu berechnen.

| $u$ | $v$ | $a$ | $b$ | $c$ | abgeleitete Zahlentripel | | |
|---|---|---|---|---|---|---|---|
| 2 | 1 | 3 | 4 | 5 | 9 | 12 | 15 |
| 3 | 2 | 5 | 12 | 13 | 20 | 48 | 52 |
| 4 | 1 | 15 | 8 | 17 | 45 | 24 | 51 |
| 4 | 3 | 7 | 24 | 27 | 14 | 48 | 54 |
| 5 | 2 | 21 | 20 | 29 | 42 | 40 | 58 |
| 5 | 4 | 9 | 40 | 41 | 27 | 120 | 123 |
| 6 | 1 | 35 | 12 | 37 | 70 | 24 | 74 |
| 6 | 3 | 27 | 36 | 45 | 54 | 72 | 90 |
| 6 | 5 | 11 | 60 | 61 | 33 | 180 | 183 |

Tabelle 7.1: Pythagoräische Zahlentripel

Eine nette Anwendung zu diesem Kapitel ist folgender

**Satz 7.3.**
Ein rechtwinkeliges Dreieck, dessen Seitenlängen ganzzahlig sind, besitzt immer einen ganzzahligen Inkreisradius.

**Beweis:** Die ganzzahligen Seitenlängen eines rechtwinkeligen Dreiecks bilden nach Vorausset-

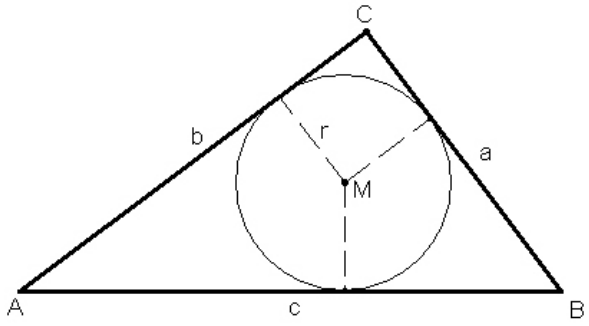


Abbildung 7.1: Ein rechtwinkeliges Dreieck

zung ein pythagoräisches Tripel $(ta, tb, tc)$, wobei $a, b, c, t \in \mathbb{N} \setminus \{0\}$ sind und $\text{ggT}(a, b, c) = 1$ ist. Den Inkreisradius berechnet man mit der Formel:

$$r = \frac{A}{S} = \frac{\frac{ab}{2}}{\frac{a+b+c}{2}} = \frac{ab}{a+b+c}$$

Für den Inkreisradius $r$ des Dreiecks folgt daher:

$$r = \frac{t^2 ab}{t(a+b+c)} = t \cdot \frac{ab}{a+b+c}$$

Es reicht also zu zeigen, dass

$$\frac{ab}{a+b+c}$$

ganzzahlig ist.

Mit Hilfe der Indischen Formeln erhält man

$$\frac{(u^2-v^2)2uv}{u^2-v^2+2uv+u^2+v^2} = \frac{(u^2-v^2)2uv}{2u^2+2uv} = \frac{(u+v)(u-v)v}{u+v} = (u-v)v,$$

und damit ist alles gezeigt.

□

# Kapitel 8

# Die Fibonacci-Zahlen

## 8.1 Allgemeines

Die Fibonacci-Zahlen können den Schülern in der sechsten Klasse Oberstufe bereits beigebracht werden. Leonardo Fibonacci wurde um 1170 geboren und und lebte bis ca. 1240. Der italienische Mathematiker fasste das mathematische Wissen der klassischen, indischen, europäischen und arabischen Kultur zusammen und ergänzte es durch seine eigenen Beiträge zur Zahlentheorie und Algebra. Er formulierte das Kaninchenproblem, welches den Schülern als Beispiel für eine rekursiv definierte Folge vorgestellt wird.

Das Bildungsgesetz zu diesem Problem lautet:

- Am Anfang gibt es nur ein Kaninchenpaar.
- Ein neugeborenes Kaninchenpaar braucht ein Monat, bis es geschlechtsreif ist.
- Jedes geschlechtsreife Kaninchenpaar bringt jeden Monat genau ein neues Kaninchenpaar zur Welt.
- Die Kaninchen leben ewig.

Diese Zahlenfolge soll dann von den Schülern in einer Liste nach Monaten geordnet eingetragen werden.

| Monat | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| Anzahl der Kaninchenpaare | 1 | 1 | 2 | 3 | 5 | 8 | 13 | 21 | 34 | 55 | 89 | ... | ... | ... |

Mit diesen Unterlagen werden die Schüler manche Eigenschaften der Zahlenfolge selbst entdecken. Die rekursive Definition der Folge $a_n$ der Fibonacci-Zahlen lautet:

$$a_1 = 1, a_2 = 1, \text{ und } a_{n+2} = a_n + a_{n+1} \qquad \forall n \in \mathbb{N}, n > 0 \tag{8.1}$$

## 8.1 Allgemeines

Man hat vielleicht im Rahmen des Regelunterrichts die Möglichkeit auf das vielfältige Vorkommen dieser Zahlen in der Mathematik, Biologie, Physik, usw. hinzuweisen, zu mehr wird aber im normalen Schulunterricht die Zeit nicht reichen. Das Wahlplichtfach Mathematik eröffnet die Möglichkeit hier einzuhaken, und diese Zahlen den interessierten Schülern genauer vorzustellen. Es gibt eine Vielzahl von Querbezügen zu anderen Gebieten der Mathematik: Eine explizite Formel setzen die Fibonacci-Zahlen beispielsweise in Verbindung mit dem goldenen Schnitt. Sie tauchen im Pascalschen Dreieck als Summen von Diagonalen auf.

Uns interessieren hier nur die zahlentheoretischen Eigenschaften der Fibonacci-Zahlen. Hier kann man DERIVE einsetzen, um sich diesen Zahlen zu nähern. Voraussetzung ist natürlich wieder, dass die Schüler die wichtigen Befehle bereits kennen, und selbständig einfache DERIVE Befehle schreiben können.

Um die ersten 11 Fibonacci-Zahlen zu erzeugen, verwendet man folgenden Befehl von DERIVE:

```
VECTOR(FIBONACCI(n), n, 0, 10)
```

```
VECTOR(FIBONACCI(n), n, 0, 30)= [1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233,
377, 610, 987, 1597, 2584, 4181, 6765, 10946, 17711, 28657, 46368, 75025, 121393,
196418, 317811, 514229, 832040]
```

Wie viele Primzahlen sind unter den ersten tausend Gliedern der Fibonacci-Folge?

```
Anzahl(n) := DIM(SELECT(PRIME(i), i, VECTOR(FIBONACCI(i), i, 0, n)))
```

```
Anzahl(1000)= 21
```

Auch den Teilbarkeitskriterien kann man sich mit DERIVE nähern:

Welche Indizes haben die durch 7 teilbaren Fibonacci-Zahlen?

```
Teilbar7(n) := SELECT(U_MOD(i, 1, -1, 7) = 0, i, n)
```

```
Teilbar7(200)= [8, 16, 24, 32, 40, 48, 56, 64, 72, 80, 88, 96, 104, 112, 120,
128, 136, 144, 152, 160, 168, 176, 184, 192, 200]
```

Hier werden die Schüler sicher auf die richtige Vermutung kommen, dass nur jene Fibonacci-Zahlen durch 7 teilbar sind, deren Indizes durch 8 teilbar sind. Es sind hier sehr viele Fragestellungen möglich, wo die Schüler selbstständig arbeiten und Probleme lösen können. Hier können die durch Rechnereinsatz gewonnenen Ergebnisse von den Schülern festgehalten und allgemeine Vermutungen aufgestellt werden.

Das Arbeiten mit DERIVE ist sicher ein guter Einstieg, um jetzt einige zahlentheoretische Eigenschaften dieser Zahlen herzuleiten.

## 8.2 Einfache zahlentheoretische Eigenschaften

Für die folgenden Sätze setzen wir voraus, dass $a_n$ die Folge der Fibonacci-Zahlen ist, wie sie unter 8.1 definiert werden.

**Satz 8.1.**
Je zwei benachbarte Fibonacci-Zahlen sind teilerfremd, das heißt:

$$ggT(a_n, a_{n+1}) = 1 \qquad \forall n \in \mathbb{N}, n > 0 \tag{8.2}$$

**Beweis:** Es sei

$$d = ggT(a_n, a_{n+1}) \text{ mit } d > 0.$$

Dann ist aber auch die Differenz $a_{n+1} - a_n = a_{n-1}$ durch $d$ teilbar, das heißt $d \mid a_{n-1}$. Analog zeigt man durch Induktion, dass $d \mid a_{n-2}$, $d \mid a_{n-3}$, ... gilt und schließlich $d \mid a_1 = 1$. Also ist $d = 1$ und wir haben geziegt, dass $a_n$ und $a_{n+1}$ teilerfremd sind.

□

Um weitere zahlentheoretische Folgerungen anzustellen, beweisen wir nun den folgenden wichtigen Satz durch Induktion. Es wird dabei vorausgesetzt, dass die Schüler mit diesem Beweisverfahren sehr vertraut sind, da es sich hier sogar um einen "zweistufigen" Induktionsbeweis handelt.

**Satz 8.2. "Additionsformel"**
Für $n \geq 2, m \geq 1$ gilt:

$$a_{n+m} = a_{n-1}a_m + a_n a_{m+1} \tag{8.3}$$

**Beweis:** Wir führen den Beweis durch vollständige Induktion nach $m$:

Für $m = 1$ hat 8.3 folgende Gestalt: $a_{n+1} = a_{n-1}a_1 + a_n a_2$ mit $a_1 = a_2 = 1$, was klarerweise richtig ist. Auch für $m = 2$ ist die Behauptung richtig:

$$a_{n+2} = a_{n-1}a_2 + a_n a_3 = a_{n-1} + a_n + a_n = a_{n+1} + a_n$$

Damit ist der Induktionsanfang gezeigt.

Induktionsschluss:

Wir dürfen daher annehmen, dass die Aussage 8.3 für $m$ und $m + 1$ richtig ist, also:

$a_{n+m} = a_{n-1}a_m + a_n a_{m+1}$
$a_{n+m+1} = a_{n-1}a_{m+1} + a_n a_{m+2}$ (Induktionsvoraussetzungen)

Zu zeigen ist: $a_{n+m+2} = a_{n-1}a_{m+2} + a_n a_{m+3}$ (Induktionsbehauptung)

Diese folgt aber sofort aus der Addition der beiden Zeilen von oben:

$a_{n+m} = a_{n-1}a_m + a_n a_{m+1}$
$\underline{a_{n+m+1} = a_{n-1}a_{m+1} + a_n a_{m+2}}$

Auf der linken Seite ergibt die Addition:

$$a_{n+m} + a_{n+m+1} = a_{n+m+2}$$

Auf der rechten Seite ergibt die Addition:

$$a_{n-1}a_m + a_{n-1}a_{m+1} + a_n a_{m+1} + a_n a_{m+2} = a_{n-1}(a_m + a_{m+1}) + a_n(a_{m+1} + a_{m+2}) = a_{n-1}a_{m+2} + a_n a_{m+3}$$

Damit ist die Induktionsbehauptung gezeigt und 8.3 bewiesen.

□

Setzt man in obiger "Formel" $m = n - 1$, so erhält man:

$$a_{2n-1} = a_{n-1}^2 + a_n^2 \qquad \forall n \in \mathbb{N}, n \geq 2$$

Es gilt also folgender Satz:

**Satz 8.3.**
Die Summe der Quadrate aufeinanderfolgender Glieder der Fibonaccifolge ist ebenfalls eine Fibonacci-Zahl.

Wir wollen nun noch einige Teilbarkeitseigenschaften der Fibonacci-Zahlen herleiten.

**Satz 8.4.**
Ist $n$ durch $m$ teilbar, so ist auch $a_n$ durch $a_m$ teilbar, also:

$$m \mid n \Rightarrow a_m \mid a_n \tag{8.4}$$

**Beweis:** Es sei $n$ durch $m$ teilbar, das heißt $n = km$, mit $k \in \mathbb{N}$.

Wir führen den Beweis durch Induktion nach $k$:

Für $k = 1$ gilt: $a_n \mid a_n$ und das ist klarerweise richtig.

Induktionsvoraussetzung: wir nehmen nun an, dass $a_n = a_{m \cdot k}$ durch $a_m$ teilbar ist. Wir betrachten nun $a_{(k+1)\cdot m}$. Es gilt nach 8.3:

$$a_{(k+1)\cdot m} = a_{km+m} = a_{km-1}a_m + a_{km}a_{m+1}$$

Der erste Summand der rechten Seite dieser Gleichung ist durch $a_n$ teilbar, der zweite Summand enthält $a_{km}$, ist also nach Induktionsvoraussetzung ebenfalls durch $a_m$ teilbar. Daher teilt $a_m$ auch $a_{(k+1)\cdot m}$. Und damit ist alles gezeigt.

□

## 8.3 Ein zentraler Satz und seine Folgerungen

Hat man jetzt auch noch den Euklidischen Algorithmus zur Verfügung und sind die Schüler eingehend mit dem Begriff der Teilbarkeit vertraut, dann kann man vielleicht auch folgenden Satz bringen:

**Satz 8.5.**
Ist $d$ der größte gemeinsame Teiler von $n$ und $m$, dann ist $a_d$ der größte gemeinsame Teiler von $a_n$ und $a_m$, also:

$$ggT(a_n, a_m) = a_{ggT(n,m)} = a_d \qquad \forall m, n \in \mathbb{N}$$

**Beweis:** Wir nehmen ohne Beschränkung der Allgemeinheit an, dass $m > n$. Zur Berechnung des größten gemeinsamen Teilers von $n$ und $m$ verwenden wir den Euklidischen Algorithmus:

$$m = q_1 n + r_1 \text{ mit } 0 < r_1 < n$$

$$n = q_2 r_1 + r_2 \text{ mit } 0 < r_2 < r_1$$

$$r_1 = q_3 r_2 + r_3 \text{ mit } 0 < r_3 < r_2$$

$$r_2 = q_4 r_3 + r_4 \text{ mit } 0 < r_4 < r_3$$

$$\ldots\ldots$$

$$r_{k-1} = q_{k+1} r_k$$

$r_k$ ist dann der größte gemeinsame Teiler von $m$ und $n$. Es gilt nun:

$$ggT(n, m) = ggT(n, r_1) = ggT(r_1, r_2) = ggT(r_2, r_3) = \ldots = ggT(r_{k-1}, r_k) = r_k \tag{8.5}$$

Wir berechnen nun den größten gemeinsamen Teiler von $a_n$ und $a_m$:

$$ggT(a_m, a_n) = ggT(a_{q_1 n + r_1}, a_n)$$

Mit der Additionsformel (vgl. 8.3) folgt daraus:

$$ggT(a_{q_1 n + r_1}, a_n) = ggT(a_{q_1 n - 1} a_{r_1} + a_{q_1 n} a_{r_1 + 1}, a_n)$$

Da weiters $a_n$ ein Teiler von $a_{q_1 n}$ ist (vgl. 8.4), folgern wir

$$ggT(a_{q_1 n - 1} a_{r_1} + a_{q_1 n} a_{r_1 + 1}, a_n) = ggT(a_n, a_{q_1 n - 1} a_{r_1}),$$

und da $a_n$ und $a_{q_1 n - 1}$ teilerfremd sind, haben wir schließlich

$$ggT(a_n, a_{q_1 n - 1} a_{r_1}) = ggT(a_n, a_{r_1}).$$

Der Sachverhalt, dass $a_n$ und $a_{q_1 n-1}$ teilerfremd sind, gehört für Schüler sicher genauer ausgeführt: Ist $d$ ein Teiler von $a_n$ und $a_{kn-1}$, dann ist $d$ auch ein Teiler von $a_{kn}$ und $a_{kn-1}$ (nach 8.4). Nach 8.2 sind aber $a_{kn}$ und $a_{kn-1}$ teilerfremd und daher muss $d$ gleich 1 sein.

Unter Verwendung von 8.5 kann man weiters folgern:

$$ggT(a_m, a_n) = ggT(a_n, a_{r_1}) = ggT(a_{r_1}, a_{r_2}) = \cdots = a_{r_k}$$

Am Ende erhält man

$$ggT(a_m, a_n) = a_{r_k} = a_{ggT(m,n)},$$

und damit ist der Satz bewiesen.

□

Man verwendet also bei diesem Beweis nicht nur die Aussagen der vorhergehenden Sätze, sondern auch den Euklidischen Algorithmus und einige Regeln über den größten gemeinsamen Teiler zweier Zahlen. Alle diese Voraussetzungen müssen gut vorbereitet sein, damit es überhaupt sinnvoll ist diesen Beweis zu bringen.

Abschließend können wir jetzt leicht die Umkehrung von 8.4 beweisen:

**Satz 8.6.**
Ist $a_n$ durch $a_m$ teilbar, so ist auch $n$ durch $m$ teilbar, also:

$$a_m \mid a_n \Rightarrow m \mid n$$

**Beweis:** Unter Verwendung des vorhergehenden Satzes folgt:

$$a_m \mid a_n \Rightarrow ggT(a_m, a_n) = a_m = a_{ggT(n,m)}$$

Daher gilt $m = ggT(n, m)$, also $m$ teilt $n$.

□

Zusammenfassend kann man daher festhalten:

**Satz 8.7.**
Es ist $a_n$ dann und nur dann durch $a_m$ teilbar, wenn $n$ durch $m$ teilbar ist.

$$a_m \mid a_n \Leftrightarrow m \mid n$$

Man kann nun einige Teilbarkeitskriterien für Fibonacci-Zahlen angeben:

- Eine Fibonacci-Zahl ist dann und nur dann gerade, wenn ihr Index durch 3 teilbar ist.

$$(a_3 = 2) \mid a_n \Leftrightarrow 3 \mid n$$

- Eine Fibonacci-Zahl ist dann und nur dann durch 3 teilbar, wenn ihr Index durch 4 teilbar ist.

$$(a_4 = 3) \mid a_n \Leftrightarrow 4 \mid n$$

- Eine Fibonacci-Zahl ist dann und nur dann durch 4 teilbar, wenn ihr Index durch 6 teilbar ist.

$$4 \mid a_n \Leftrightarrow 6 \mid n$$

- Eine Fibonacci-Zahl ist dann und nur dann durch 5 teilbar, wenn ihr Index durch 5 teilbar ist.

$$5 \mid a_n \Leftrightarrow 5 \mid n$$

- Eine Fibonacci-Zahl ist dann und nur dann durch 7 teilbar, wenn ihr Index durch 8 teilbar ist.

$$7 \mid a_n \Leftrightarrow 8 \mid n$$

Eine weitere Folgerung:

Ist $a_n$ eine Primzahl, so ist $n = 4$, oder $n$ selbst eine Primzahl.

Das überlegt man sich folgendermaßen:

Wegen $a_m \mid a_n \Leftrightarrow m \mid n$ und da $a_n$ eine Primzahl ist, muss $a_m$ gleich 1 sein, also $m$ gleich 1 oder 2 sein. Daher ist $n$ entweder eine Primzahl oder $n = 2^k$ mit $k \in \mathbb{N}, k \geq 2$. Da aber nach der Teilbarkeitsregel alle Fibonacci-Zahlen mit einem durch 4 teilbaren Index durch 3 teilbar sind, kann $n$ entweder nur 4 oder selbst eine Primzahl sein.

Die Umkehrung davon gilt jedoch nicht: $a_{19} = 4181 = 37 \cdot 113$. Ob es unter den Fibonacci-Zahlen unendlich viele Primzahlen gibt, ist bis heute ungelöst.

# Kapitel 9

# Das RSA-Verfahren

Im Mathematikunterricht wird man von den Schülern manchmal mit der Frage: "Wozu braucht man das eigentlich?" konfrontiert und es ist nicht immer ganz so leicht eine passende Antwort zu finden. Wahrscheinlich eignet sich aber kein Gebiet besser um den Schülern vor Augen zu führen, wie zunächst abstrakt scheinende Sätze und Theorien eine ungeheurer wichtige Bedeutung gewinnen können, als das RSA-Verfahren. Die algebraischen und zahlentheoretischen Grundlagen sind den Schülern durchaus zugänglich und resultieren in einem der ersten und wichtigsten Public Key Kryptosysteme, dem RSA Verfahren, benannt nach den Erfindern R. L. Rivest, A. Shamir und L. Adleman, welches 1978 veröffentlicht wurde. Dieses Verfahren wird heute in wichtigen Bereichen, wie im Bankenwesen (z.B. bei der Verschlüsselung von Geheimzahlen), bei der Verschlüsselung von Mobilfunknetzen oder bei Geheimdiensten, verwendet. Daher ist es sicher für Schüler interessant zu wissen, wie dieses Verfahren funktioniert. Das RSA-System sollte aus diesem Grund in einer Oberstufe unbedingt vorgestellt werden, vielleicht nur der Algorithmus mit sehr einfachen Zahlen im Rahmen einer Supplierstunde, vielleicht gelingt es ein fächerübegreifendes Projekt Mathematik-Informatik zu initiieren oder man hat die Gelegenheit im Rahmen eines Wahlpflichtfaches ausführlich alle mathematischen Grundlagen des RSA-Verfahrens aufzubereiten. Im folgenden Kapitel werden zunächst alle Begriffe und Sätze - soweit sie in dieser Arbeit noch nicht behandelt wurden - zusammengestellt, die für das Verständnis des RSA-Verfahrens notwendig sind.

## 9.1 Die Mathematik des RSA-Verfahrens

Viele der mathematischen Grundlagen, auf denen das Verfahren der RSA-Verschlüsselung beruht, wurden in dieser Arbeit schon zusammengestellt. Wir setzen hier voraus, dass die Schüler bereits mit dem Kongruenzbegriff vertraut sind und die Rechenregeln für Kongruenzen kennen. Auch der Begriff der Primzahl und der Euklidische Algorithmus seien hier schon als bekannt vorausgesetzt. In dem Kapitel über lineare Kongruenzen wurde weiters folgender Satz gezeigt:

Sind $a$ und $m$ zwei teilerfremde positive ganze Zahlen, so gibt es (genau) eine positive ganze Zahl

$x < m$, die Lösung der linearen Kongruenz

$$ax \equiv 1 \bmod m$$

ist (vgl. 6.2). Dieses inverse Element $a^{-1}$ kann mit Hilfe des "erweiterten" Euklidischen Algorithmus berechnet werden. Hat man die linearen Kongruenzen nicht durchgenommen, so kann man den Satz folgendermaßen beweisen:

**Beweis:** Da der $ggT(a, m) = 1$ ist, gibt es nun durch den Euklidischen Algorithmus zwei Zahlen $x$ und $y$ mit

$$ax + my = 1.$$

Daher ist $x$ eine Lösung der linearen Kongruenz

$$ax \equiv 1 \bmod m.$$

Sei nun $x'$ eine weitere Lösung. Dann gilt

$$ax' \equiv 1 \bmod m$$

$$ax \equiv 1 \bmod m,$$

daraus folgt

$$ax - ax' \equiv 0 \bmod m \quad \text{also} \quad a(x - x') \equiv 1 \bmod m.$$

Da $ggT(a, m) = 1$ gilt daher

$$x \equiv x' \bmod m$$

und damit hat man gezeigt, dass es nur eine einzige Lösung der Kongruenz $ax \equiv 1 \bmod m$ geben kann.

□

Die Grundlage des RSA-Verfahrens liegt aber im Satz von Fermat. Dieser Satz lautet:

**Satz 9.1.**
Ist $p$ eine Primzahl und $a$ eine ganze Zahl, so gilt:

$$a^p \equiv a \bmod p \tag{9.1}$$

Wir wollen zwei Möglichkeiten angeben diesen grundlegenden Satz zu beweisen. Beide Möglichkeiten sind für Schüler durchaus zugänglich, wenn die entsprechenden Grundlagen vorbereitet sind. Der erste Beweis verlangt ein sicheres Umgehen mit den Rechenregeln für Kongruenzen:

**Beweis:** Ist $a$ durch $p$ teilbar, dann ist der Satz klarerweise richtig. Im Folgenden sei jetzt $a \not\equiv 0 \bmod p$. Es seien $x_1, x_2, \ldots, x_{p-1}$ Zahlen, die wie folgt definiert sind:

$$x_1 = 1 \cdot a$$

$$x_2 = 2 \cdot a$$

$$\ldots\ldots$$

$$x_{p-1} = (p-1) \cdot a$$

Es gilt nun: Je zwei $x_r$ und $x_s$ mit $1 \leq r, s \leq p-1$ und $r \neq s$ sind nicht kongruent modulo $p$. Das zeigt man durch einen indirekten Beweis.
Annahme:

$$x_r \equiv x_s \bmod p$$

also

$$r \cdot a \equiv s \cdot a \bmod p.$$

Da $a$ kein Vielfaches von $p$ und somit zu $p$ teilerfremd ist ($p$ ist Primzahl), folgt

$$r \equiv s \bmod p,$$

was allerdings ein Widerspruch zu $r \neq s$ ist, da $1 \leq r, s \leq p-1$.

Da nun alle $x_i$ paarweise inkongruent modulo $p$ sind und keine der Zahlen $x_1, x_2, \ldots, x_{p-1}$ durch $p$ teilbar ist, durchlaufen die $(p-1)$ Zahlen $x_1, x_2, \cdots, x_{p-1}$ genau die $(p-1)$ primen Restklassen modulo $p$. Jede dieser Zahlen stellt also einen Vertreter genau einer dieser Restklassen dar. Es gilt daher:

$$x_1 \cdot x_2 \cdot x_3 \cdots x_{p-1} \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \bmod p$$

also

$$1a \cdot 2a \cdot 3a \cdots (p-1)a \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \bmod p$$

und

$$a^{p-1} \cdot 1 \cdot 2 \cdot 3 \cdots (p-1) \equiv 1 \cdot 2 \cdot 3 \cdots (p-1) \bmod p$$

Da aber die Faktoren $1, 2, 3, \ldots, (p-1)$ alle nicht durch $p$ teilbar und somit zu $p$ teilerfremd sind, folgt

$$a^{p-1} \equiv 1 \bmod p$$

und somit

$$a^p \equiv a \bmod p.$$

□

Diesen Satz kann man aber auch sehr schön mit vollständiger Induktion beweisen:

**Beweis:**

Wir führen einen Induktionsbeweis nach $a$.

Der Induktionsanfang mit $a = 0$ ist sicher richtig. Nun nimmt man an, dass es auch für $a$ gilt. Der Induktionsschluss von $a$ auf $a + 1$ wird nun mit dem binomischen Lehrsatz gezeigt.

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a + 1$$

Wir betrachten nun die Koeffizienten dieser Entwicklung:

$$\binom{p}{k} = \frac{p \cdot (p-1) \cdot \cdots \cdot (p-k+1)}{1 \cdot 2 \cdot \cdots \cdot k}, \quad k = 1, \ldots, p-1$$

Ein solcher Koeffizient kann nur dann durch $p$ teilbar sein, wenn $p$ eine Primzahl ist. Denn es gilt:

$$\binom{p}{k} \cdot 1 \cdot 2 \cdot \cdots \cdot k = p \cdot (p-1) \cdot (p-2) \cdots (p-k+1), \qquad k = 1, \ldots, p-1$$

Da $p$ zu $1, 2, \ldots, k$ teilerfremd ist, kann nur $p$ den Koeffizienten $\binom{p}{k}$ teilen. Es sind also alle Koeffizienten von $(a+1)^p$ durch $p$ teilbar, außer der erste und der letzte Koeffizient der Entwicklung. Es gilt daher:

$$(a+1)^p = a^p + \binom{p}{1}a^{p-1} + \cdots + \binom{p}{p-1}a + 1 \equiv a^p + 1 \bmod p$$

Mit der Induktionsvoraussetzung $a^p \equiv a \bmod p$ folgt:

$$(a+1)^p \equiv a^p + 1 \equiv (a+1) \bmod p$$

Und damit wurde der Induktionsschluss gezeigt.

□

Für das RSA-Verfahren benötigt man eine Erweiterung dieses Satzes von Fermat, welche aber leicht herzuleiten ist.

Es seien nun $p$ und $q$ zwei verschiedene Primzahlen und $a$ zunächst eine zu $p$ und $q$ teilerfremde ganze Zahl. Nach dem Satz von Fermat gilt:

$$a^{p-1} \equiv 1 \mod p \qquad \text{und} \qquad a^{q-1} \equiv 1 \mod q$$

und daher

$$\left(a^{p-1}\right)^k = a^{(p-1)k} \equiv 1 \mod p \qquad \text{und} \qquad \left(a^{q-1}\right)^r = a^{(q-1)r} \equiv 1 \mod q \quad \text{mit } k, r \in \mathbb{N}.$$

Bezeichnet man mit kgV$(p-1, q-1)$ das kleinste gemeinsame Vielfache der Zahlen $(p-1)$ und $(q-1)$ so folgt, da $p$ und $q$ teilerfremd sind (verschiedene Primzahlen)

$$a^{kgV(p-1,q-1)} \equiv 1 \mod p \cdot q,$$

und daher

$$a^{1+kgV(p-1,q-1)} \equiv a \bmod p \cdot q.$$

Aus $p \mid a$ und $q \nmid a$ folgt mit dem Satz von Fermat und den Rechenregeln für Kongruenzen:

$$a^{kgV(p-1,q-1)} \equiv 1 \bmod q$$

also

$$a^{1+kgV(p-1,q-1)} \equiv a \bmod q.$$

Da $p$ aber $a$ teilt und $p$ und $q$ verschiedene Primzahlen sind, gilt

$$a^{1+kgV(p-1,q-1)} \equiv a \bmod (n = pq).$$

Der andere Fall $p \nmid a$ und $q \mid a$ geht analog.

Man kann daher folgende Erweiterung des Satzes von Fermat formulieren:

**Satz 9.2.**
Sind $p$ und $q$ Primzahlen und $a$ eine zu $p$ und $q$ teilerfremde ganze Zahl, dann gilt:

$$a^{1+kgV(p-1,q-1)} \equiv a \bmod p \cdot q \tag{9.2}$$

In diesem Zusammenhang kann man den Schülern vielleicht auch noch die Verallgemeinerung des Satzes von Fermat, den Satz von Euler mitteilen:

**Satz 9.3.**
Ist $m$ eine positive ganze Zahl und $a$ eine zu $m$ teilerfremde ganze Zahl, so gilt

$$a^{\varphi(m)} \equiv 1 \bmod m,$$

wobei $\varphi(m)$ die sogenannte "Eulersche-$\varphi$-Funktion" ist, welche die Anzahl der ganzen Zahlen $x$ mit $1 \leq x \leq m-1$ liefert, die zu $m$ teilerfremd sind.

Für das Verstehen der RSA-Verschlüsselung ist dieser Satz, der sich im Grunde genau so beweisen lässt wie der Satz von Fermat, aber nicht notwendig.

Damit hat man alle zahlentheoretischen Grundlagen zusammengestellt um das RSA-Verfahren zu verstehen.

## 9.2 RSA-Verschlüsselung

Ein wichtiger Bereich der Zahlentheorie ist die Kryptologie. Diese wird in zwei Gebiete eingeteilt, die Kryptographie und die Kryptoanalyse. Die Zahlentheoretiker des ersten Bereiches beschäftigen sich hauptsächlich mit der Verschlüsselung von Nachrichten, der zweite Bereich wird genutzt, um zu prüfen, wie leicht man die Verfahren knacken kann.

Verschlüsselung nennt man den Vorgang, bei dem ein klar lesbarer Text (M ... Message ) mit Hilfe eines Verschlüsselungsverfahrens (Kryptosystem) in eine “unleserliche”, das heißt nicht einfach interpretierbare Zeichenfolge, eine Geheimschrift (C ... Cipher) umgewandelt wird. Alle Verfahren verwendeten bis in die ausgehenden 70-er Jahre denselben Schlüssel bei der Verschlüsselung wie bei der Entschlüsselung: Man spricht von symmetrischen Verschlüsselungen (siehe Abbildung 9.1).

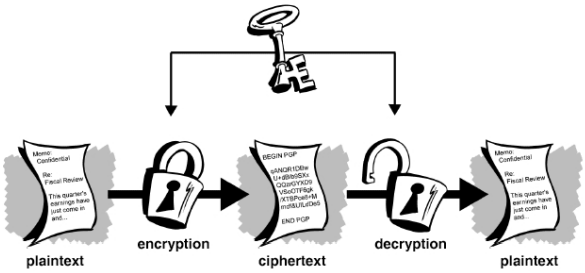


Abbildung 9.1: Prinzip der symmetrischen Verschlüsselung [32]

Als Beispiel für die Verschlüsselung eines Klartextes in einen Geheimtext haben die Schüler vielleicht schon die Cäsar-Verschlüsselung kennengelernt (vgl. Kapitel 5.2.4). Wenn nicht, soll sie in diesem Zusammenhang zum Einstieg kurz vorgestellt werden.

Bei symmetrischen Verschlüsselungsmethoden werden also stets identische geheime Schlüssel zur Verschlüsselung und Entschlüsselung benutzt und dieser Schlüssel muss geheim bleiben. Die Schlüsselverteilung wurde aber immer mehr zu einem Sicherheitsproblem. Deshalb suchte man nach

Methoden mit unterschiedlichen Schlüsseln zur Ver- und Entschlüsselung, sie werden als asymmetrische Verfahren (engl.: Public key methods) bezeichnet (siehe Abbildung 9.2).

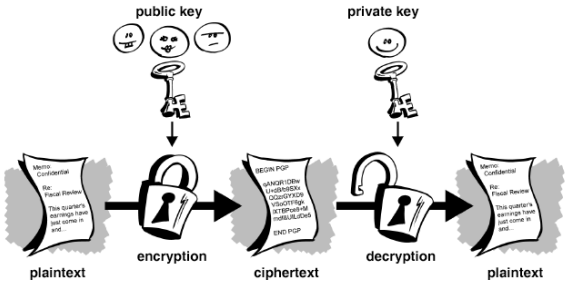


Abbildung 9.2: Prinzip der asymmetrischen Verschlüsselung [32]

Es muss also nur der öffentliche Schlüssel ausgetauscht werden. Jeder besitzt eine Art Telephonbuch, indem die öffentlichen Schlüssel der Kommunikationspartner stehen. Das macht aber nichts, denn mit diesem lässt sich eine verschlüsselte Nachricht ja nicht lesen, das geht nur mit dem privaten, geheim zu haltenden Schlüssel. Natürlich hängen die beiden Schlüssel voneinander ab: sie müssen gemeinsam von demselben Algorithmus erzeugt werden. Einen Teil, den öffentlichen, lässt man all jene wissen, von denen man verschlüsselte Nachrichten bekommen möchte, den anderen Teil, mit dem die Entschlüsselung möglich ist, hält man geheim. Nie muss ein geheimer Schlüssel ausgetauscht werden, jeder kann mit jedem verschlüsselte Botschaften tauschen, ohne denjenigen je getroffen zu haben.

Eines der bekanntesten und heute das am weitesten verbreitete asymmetrische Verschlüsselungsverfahren ist das RSA-Verfahren.

Wie funktioniert nun dieses Verfahren?

Für die Erzeugung der Schlüssel wählt man zunächst zwei große Primzahlen **p** und **q** und bildet ihr Produkt $\mathbf{n} := \mathbf{p} \cdot \mathbf{q}$.

**e** sei eine ganze Zahl ($> 1$), die zum kleinsten gemeinsamen Vielfachen von $(p-1)$ und $(q-1)$ teilerfremd ist. Die Zahlen **e** (**e**ncipher = verschlüsseln) und **n** bilden den “Public Key”.

Da e und kgV(p-1, q-1) teilerfremd sind, ist die lineare Kongruenz $e \cdot x \equiv 1 \mod \text{kgV}(p-1, q-1)$ eindeutig lösbar. Die Lösung **d** (**d**ecipher = entschlüsseln) heißt der ”Private Key”. Es gilt also:

$$e \cdot d \equiv 1 \mod kgV(p-1, q-1)$$

Bemerkung: Statt des $kgV(p-1, q-1)$ kann auch das Produkt $(p-1)(q-1)$ genommen werden. Die

Entschlüsselung funktioniert dann auch mit dem so gewonnenen $d$ (aus $e \cdot d \equiv 1 \bmod (p-1)(q-1)$ folgt ja $e \cdot d \equiv 1 \bmod kgV(p-1, q-1)$ ), doch ist das so erhaltene $d$ dann im allgemeinen größer als jenes, welches mit dem $kgV$ berechnet wurde.

Es sei nun **M** (= **M**essage) die zu verschlüsselnde Nachricht, wobei folgende Bedingung für M gelten muss: **M** ist eine ganze Zahl mit $0 \leq \mathbf{M} \leq n-1$. **C** (= **C**ipher) sei die verschlüsselte Nachricht.
Das **RSA-Verfahren** funktioniert nun so:

**Verschlüsseln:** $\mathbf{C} = \mathbf{M}^e \bmod n$

**Entschlüsseln:** $\mathbf{M} = \mathbf{C}^d \bmod n$

Bevor wir dieses Verfahren beweisen, wird man es anhand eines Beispiels einüben:
Person B möchte Person A eine geheime Nachricht schicken:

**Geheimer Bereich von A**:
A wählt zwei verschiedene Primzahlen

$$p = 97$$
$$q = 131$$

und bildet ihr Produkt
$\mathbf{n} = p \cdot q = 12707$
und das kleinste gemeinsame Vielfache
$kgV(p-1, q-1) = 6240$.
Weiters wählt A eine zu $kgV(p-1, q-1)$ teilerfremde Zahl $\mathbf{e} = 331$.
A ermittelt aus $e$ und $kgV(p-1, q-1)$ die Zahl
$d = 5731$
und entschlüsselt die Nachricht von B:

$$\mathbf{M} = C^d \bmod n$$

$\mathbf{M} = 11453^{5731} = 9865 \bmod n$

**Öffentlicher Bereich**

A gibt die beiden Zahlen **n**und **e** als den "öffentlichen Schlüssel "bekannt.
**n = 12707**
**e= 331**

Die Person B übermittelt an die Person A:
**C** = 11453

**Geheimer Bereich von B**:
Die Nachricht von B an A ist eine Zahl, die kleiner als n ist:
**M** =9865
Er verschlüsselt sie gemäß obiger Formel
$C = M^e \bmod (n)$
also

$\mathbf{C} = 11453 = 9865^{331} \bmod 12707$.

Zur Berechnung der entsprechenden Werte wird man natürlich DERIVE einsetzen. Zur Ermittlung von $a^r \bmod n$ wird man die in DERIVE programmierte Funktion `MOD(x,y)` verwenden. Für die Berechnung des inversen Elementes kann man sich mit dem einfachen Befehl

`INVERSE_MOD(a,m)`,

welcher im Utility-File "NUMBER.MTH" im DERIVE Paket mitgeliefert wird, behelfen.

Möglich ist in diesem Zusammenhang für den Schulunterricht auch die interaktive Flash-Animation zur RSA-Verschlüsselung von Franz Embacher, die unter der Adresse

http://www.mathe-online.at/materialien/Franz.Embacher/files/RSA/

abrufbar ist. Aber hier dürfen die Primzahlen $p$ und $q$ nur maximal drei Stellen aufweisen. Ein weiterer Nachteil dieser Internetseite ist, dass mit dem Produkt $(p-1)(q-1)$ und nicht mit dem $kgV(p-1, q-1)$ gerechnet wird.

Der Beweis dieses Verfahrens ist mit den oben bereitgestellten Grundlagen nicht mehr sehr schwer:

**Beweis:** Wir wollen zeigen, dass $C^d \bmod n$ wieder die ursprüngliche Nachricht M ergibt. Beachtet man, dass

$$e \cdot d \equiv 1 \bmod kgV(p-1, q-1)$$

gilt, so folgt:

$$\left(M^e\right)^d = M^{ed} = M^{s \cdot kgV(p-1,q-1)+1} \equiv M \bmod n$$

Der letzte Schritt folgt aus den Rechenregeln für Kongruenzen und dem Satz 9.2.

□

Als Abschluss betrachten wir ein Beispiel für eine realistische RSA-Verschlüsselung:

Zuerst brauchen wir zwei große Primzahlen $p$ und $q$:

`NEXT_ PRIME (RANDOM(`$10^{103}$`))`

```
4431972011918778119439465595235419351198091374460 56
2778338602692680389897083751099045929780710375989 53
```

```
p:= 4431972011918778119439465595235419351198091374460 5
6277833860269268038989707837510990459297807103759895 3
```

`NEXT_ PRIME(RANDOM(`$10^{93}$`))`

```
71760099006195520986075975207070101098042057581
13591353102136596042664363468872484900390233 79

q := 7176009900619552098607597520707010109804 2057
581135913531021365960426643634688724849003902 3379
```

Wir bilden das Produkt $n := p \cdot q$

```
31803875036797907341955402757898686633973548542123617874631459458307315
63184222486120861780605489152378828053191214918151942983992910117249956
07644138173917812380876938175555376627962011719292 2187
```

$n = 3.180387503 \cdot 10^{195}$. Die Zahl hat also 196 Dezimalstellen.

Jetzt sucht man eine zu ($kgV(p-1, q-1) =$) $LCM(p-1, q-1)$ teilerfremde Zahl $e$:

```
RANDOM(10^10)
4862380054

GCD(4862380054, (p - 1)·(q - 1))=2
```

$\frac{4862380054}{2} = 2431190027$

```
GCD(2431190027, LCM(p - 1)·(q - 1))=1

e := 2431190027
```

Die Zahlen $n$ und $e$ bilden den öffentlichen Schlüssel. Wir ermitteln den privaten Schlüssel $d$ unter Verwendung der Funktion "EXTENDED_ GCD":

```
EXTENDED_ GCD(e, LCM(p - 1)·(q - 1))
[1, [85610630167983639409674829301060662218318282236213389591284305731 65
64621441669910929989092639391858981850525676792350525531756923003673650 8
85312363130872155473822989662619038437820241018888299283, -654435065]]
```

also:

```
d := 85610630167983639409674829301060662218318282236213389591284305731 65
64621441669910929989092639391858981850525676792350525531756923003673650 8
85312363130872155473822989662619038437820241018888299283
```

Die Nachricht sei $M < n$:

```
M := 12345678901234567890123456789012345678890
```

Wir verschlüsseln sie: $C := MOD(m^e, n)$

```
C:= 486759604000427540634481958849591852139435079476744052201835531987
829836793661792871503877787205659711684208797477441049568944349103117 5
5409621444047611405196525166888201832003431228274378752 5489
```

Entschlüsselt wird die Nachricht mit dem privatem Schlüssel $d$: $M := MOD(c^d, n)$

```
M:= 12345678901234567890123456789012345678890
```

## 9.3 Die Sicherheit von RSA

Abschließend wird man die Frage "Wie sicher ist die RSA-Verschlüsselung?" aufwerfen. Hier kann zunächst ein Schüler in Form eines Referates die wichtigsten Punkte ansprechen und nachher wird man manches noch ergänzen oder vertiefen.

Das RSA-Verfahren stützt seine gesamte Sicherheit darauf, dass aus dem öffentlichen Schlüssel, bestehend aus $n$ und $e$, keine Rückschlüsse auf den geheimen privaten Schlüssel $d$ gezogen werden können. Die einzige Möglichkeit, $d$ zu berechnen, besteht darin, dass die Faktorisierung von $n$ in $p \cdot q$ gelingt. Dann kann mit $e$ der geheime Schlüssel $d$ leicht berechnet werden. Diese Primfaktorzerlegung ist für große Zahlen mit den heute bekannten Verfahren praktisch nicht durchführbar. Die wachsende Rechenleistung der Computer stellt dabei kein Problem dar, da diese Entwicklung vorauszusehen ist: Der Nutzer kann bei der Wahl seiner Schlüssel darauf achten, dass sein $n$ groß genug ist, sodass es während der Zeit der beabsichtigten Verwendung nicht faktorisierbar ist. Dabei ist nicht einmal bewiesen, dass es sich bei der Faktorisierung von großen Zahlen um ein prinzipiell schwieriges Problem handelt. Im Gegenteil, es wurden schon verschiedene Algorithmen zum Faktorisieren großer Zahlen entwickelt und mit dem derzeit besten Verfahren, mit der Methode des Zahlkörpersiebes wurde von 2003 bis 2005 die bislang größte aus zwei großen Primfaktoren zusammengesetzte Zahl ohne spezielle Struktur faktorisiert. Dabei handelt es sich um eine 200-stellige Dezimalzahl. Damit das Faktorisieren von $n$ in einer realistischen Zeit unmöglich wird, muss man bei der Auswahl von $p$ und $q$ einiges beachten. Ein wichtiges Kriterium ist, das $p$ und $q$ nicht zu nahe beieinander liegen. "Nahe" ist hier in Bezug auf die Größe von $p$ und $q$ zu verstehen. Stimmen zum Beispiel die Hälfte der führenden Stellen von $p$ und $q$ überein, so kann ihre Absolutdifferenz noch immer sehr groß sein, relativ gesehen sind sie aber bereits viel zu nahe. Ein $n$, welches aus zwei nahe beieinander liegenden Primzahlen gebildet wird, läßt sich mit einer ganz einfachen Faktorisierungsmethode, dem Fermat'schen Algorithmus, leicht zerlegen. Diesen Algorithmus kann man an dieser Stelle als eine einfache Möglichkeit zum Faktorisieren großer Zahlen vorstellen:

Ist $n = p \cdot q$ mit $p$, $q$ Primzahlen größer als 2, dann gilt mit $u = \frac{p+q}{2}, v = \frac{p-q}{2}$:

$$n = u^2 - v^2 = \left(\frac{p+q}{2}\right)^2 - \left(\frac{p-q}{2}\right)^2 = pq$$

Man geht daher folgendermaßen vor: Man formt die obige Gleichung auf $u^2 - n = v^2$ um und testet für verschiedene Werte $u > \sqrt{n}$, ob $u^2 - n$ eine Quadratzahl ist. Man beginnt am besten bei $[\sqrt{n}] + 1$ und erhöht jeweils um 1. Hat man ein $u$ gefunden, so dass $u^2 - n$ eine Quadratzahl ist, dann ist mit $n = (u + v)(u - v) = p \cdot q$ die Faktorisierung von $n$ gegeben.

Hier kann man auch von dem inzwischen freiwillig in der Haft aus dem Leben geschiedenen Verbrecher erzählen, der 1996 in einem mit RSA verschlüsselten Brief an ein österreichisches Nachrichtenmagazin eine Serie von Briefbomben ankündigte. Er verwendete zum Verschlüsseln zwei Primzahlen $p$ und $q$ mit je 122 Stellen, welche sich jedoch nur in den 13 letzten Stellen unterschieden. Dieses daraus 243 - stellige $n$ ist dann leicht mit dem Fermat-Algorithmus zu zerlegen.

Die Primzahlen, die man also für eine RSA-Verschlüsselung braucht, sind riesengroße Zahlen, die nicht nahe beieinander liegen: Für ein n mit 1024 bits müssen die beiden Primfaktoren $p$ und $q$ etwa halb so viele Stellen haben, also ca. je 512 bits, was etwa 155 Dezimalstellen entspricht. Doch wie findet man solche Primzahlen? Hier geht man natürlich nicht so vor, dass man versucht die Zahl zu faktorisieren - das würde, wie schon erwähnt, viel zu lange dauern. Mit Hilfe von Primzahltests kann man feststellen ob eine Zahl mit großer Wahrscheinlichkeit prim ist oder nicht. Die Frage "Ist die Zahl $n$ mit sehr hoher Wahrscheinlichkeit prim?" ist wesentlich leichter zu beantworten, als "Welche Faktoren hat $n$?". Und genau darauf beruht das RSA-Verfahren: Man kann schnell große Primzahlen finden und deren Produkt bilden, viel schwerer beziehungsweise unmöglich ist es dagegen, anhand des Produktes herauszufinden, wie die Faktoren dieser Zahl lauten.

Man findet etwa 10 Primzahlen obiger Größenordnung mit DERIVE durch die Eingabe

`VECTOR(NEXT_Prime(RANDOM(2^512)),k_,1,10)`

in wenigen Sekunden. Man muss allerdings sagen, dass man nicht mit 100%iger Sicherheit annehmen kann, dass die Zahlen wirklich prim sind. Es gibt ungefähr $10^{131}$ Primzahlen mit 512 bits und es ist unmöglich, eine Datenbank mit all diesen Primzahlen anzulegen.

Natürlich kommt in diesem Zusammenhang die interessante Frage: "Kann die RSA-Verschlüsselung auch funktionieren, wenn die ausgewählten Zahlen nicht prim sind?"

Die etwas überraschende Antwort lautet: Ja, es kann funktionieren und diese Frage ist gleichzeitig der Einstieg in das nächste Kapitel.

# Kapitel 10

# Verschiedene Primzahltests

Schon in der zweiten Klasse Unterstufe wird den Schülern ein einfacher Algorithmus vorgestellt um Primzahlen zu finden: Das Sieb des Eratosthenes. Hierbei streicht man aus einer Liste der natürlichen Zahlen von 2 bis $n$ zunächst alle Vielfachen von 2, die 2 selbst aber nicht, dananch alle Vielfachen von 3, aber nicht die 3 selbst, danach alle Vielfachen des kleinsten nichtgestrichenen Elements, also 5, aber 5 selbst nicht, usw. Ist die kleinste nichtgestrichene Zahl größer als $\sqrt{n}$, so beendet man das Verfahren und alle nicht gestrichenen Elemente der Liste sind Primzahlen $\leq n$. Das ist der einfachste Primzahltest, aber für große Zahlen ist er nicht geeignet. Für asymmetrische Verschlüsselungen werden aber, wie wir gesehen haben, große Primzahlen benötigt. Man braucht Tests, Algorithmen, um festzustellen, ob eine vorgegebene Zahl eine Primzahl ist oder nicht. Die grundsätzliche Idee beim Herstellen eines Primzahltests ist es nun, Eigenschaften von Primzahlen zu finden, die leicht zu überprüfen sind und die die (meisten) zusammengesetzten Zahlen nicht besitzen. Der Satz von Fermat bietet so eine Möglichkeit:

## 10.1 Fermat-Test, Pseudoprimzahlen, Carmichaelzahlen

Wir beginnen wieder mit dem Satz von Fermat:

**Satz 10.1.**
Ist $p$ eine Primzahl und $a$ eine zu $p$ teilerfremde ganze Zahl (das heisst $p \nmid a$), so gilt:

$$a^{p-1} \equiv 1 \bmod p \tag{10.1}$$

Diese Erkenntnis lässt sich für Primzahltests verwenden: Sei $n$ eine Zahl, von der getestet werden soll, ob sie prim ist. Dann wähle ein $a$ mit $ggT(a, n) = 1$ und wenn nun $a^{n-1}$ nicht kongruent 1 modulo $a$ ist, dann ist $n$ sicher keine Primzahl. Dieser Test heißt Fermat-Test. Wir testen, ob 15 eine Primzahl ist. Es gilt:

$$2^{14} = 16384 \equiv 4 \bmod 15$$

und daher kann nach dem Satz von Fermat 15 keine Primzahl sein.

Mit DERIVE lässt sich der Fermat-Test wie folgt durchführen:

```
Fermat(n, a := 2) :=
  Prog
   If NUMBER?(a)
    If a > 0
     a := [a]
     a := SELECT(PRIME(q_), q_, -a)
   Loop
    If a = [] exit
    If MOD(FIRST(a)^(n - 1), n) ≠ 1
     RETURN false
    a := REST(a)
```

Die Frage stellt sich nun, ob aus der Gültigkeit von 10.1 auch darauf geschlossen werden kann, dass $p$ eine Primzahl ist. Leider ist das nicht der Fall, es gibt auch zusammengesetzte Zahlen, die den Test bestehen. Die Bedingung 10.1 ist nur notwendig aber nicht hinreichend dafür, dass eine Zahl $n$ Primzahl ist, man spricht von einem sogenannten probabilistischen Primzahltest. So ist $91 = 13 \cdot 7$ eine zusammengesetzte Zahl, aber $3^{90}$ kongruent 1 modulo 91. Eine solche Zahl heißt Pseudoprimzahl zur Basis 3, kurz PSP(3). Wir geben daher folgende Definition:

**Definition 10.1.1.**
Eine ungerade zusammengesetzte Zahl $n$, für die

$$a^{n-1} \equiv 1 \bmod n$$

gilt, heißt Pseudoprimzahl zur Basis $a$, kurz PSP(a).

Der Fermat-Test liefert für die Zahl 341 folgende Ergebnisse:

```
Fermat(341,2)=true
```

```
Fermat(341,[2,3])=false
```

Daher ist 341 eine PSP(2), aber keine Primzahl ($341 = 11 \cdot 13$).

Wir bestimmen mit DERIVE die PSP(a) $\leq n$:

```
PSP(n, a) := SELECT(¬ PRIME(x) ∧ MOD(a^(x-1) , x) = 1, x, n)
```

Die Pseudoprimzahlen zur Basis 2 kleiner als 2000 sind: 341, 561, 645, 1105, 1387, 1729 und 1905. Es gibt also immerhin 7 Pseudoprimzahlen zur Basis 2 kleiner als 2000. Leibniz und Euler vermuteten noch, dass alle Zahlen $n$ die $2^{n-1} - 1$ teilen, Primzahlen sind.

Man kann zeigen, dass es zu jeder Basis $a$ unendlich viele Pseudoprimzahlen gibt. Wir wollen den Beweis für $a = 2$ führen:

**Satz 10.2.**
Ist $n$ eine PSP(2), dann ist auch $2^n - 1$ eine PSP(2).

Daraus folgt natürlich sofort, dass es unendlich viele PSP(2) gibt.

**Beweis:** Wir setzen $r = 2^n - 1$. Dann gilt, da $n$ eine PSP(2) ist:

$$n \mid 2^{n-1} - 1 \Longrightarrow n \mid 2^n - 2 \Longrightarrow n \mid r - 1 \Longrightarrow n \cdot k = r - 1 \text{ mit } k \in \mathbb{N}$$

also gilt:

$$2^{r-1} - 1 = 2^{kn} - 1 = (2^n - 1)s = r \cdot s \text{ mit } s \in \mathbb{N}$$

Damit hat man aber

$$2^{r-1} \equiv 1 \bmod r$$

gezeigt und $r = 2^n - 1$ ist wieder eine PSP(2).

□

Es liegt nahe, beim Testen, ob eine Zahl Primzahl ist, den Fermattest für verschiedene Werte von $a$ durchzuführen und so die "Störenfriede" auszusondern. Wenn wir etwa beim Test von 91 für $a$ den Wert 2 wählen, so erhalten wir $2^{90} \equiv 64 \bmod 91$, also ist 91 keine PSP(2) und daher keine Primzahl. Hingegen gilt $3^{1728} \equiv 1 \bmod 1729$, das heißt 1729 ist auch eine PSP(3). Ist nun 1729 auch eine PSP(4), PSP(5), ... ? Hier kann man die Schüler ein wenig forschen lassen, vorausgesetzt sie haben DERIVE zur Verfügung.

Es wäre schön, wenn man alle Pseudoprimzahlen erkennen ("entlarven") könnte, wenn man genügend viele Werte für $a$ ausprobiert. Es gibt aber Zahlen, die für alle Werte von $a$ Pseudoprimzahlen sind, die man also mit keiner Basis kleiner $a$ "erwischen" kann. Wir geben folgende Definition:

**Definition 10.1.2.**
Eine zusammengesetzte Zahl $n$, welche für alle Basen $a$ mit $ggT(a, n) = 1$ den Fermattest erfüllt, heißt Carmichaelzahl.

Eine Carmichaelzahl ist also eine Pseudoprimzahl für alle $a$ mit $ggT(a, n) = 1$.

Die schon oben erwähnte Zahl $561 = 3 \cdot 11 \cdot 17$ ist keine Primzahl, aber für alle $a$ mit $1 < a < 561$ und $ggT(a, 561) = 1$ gilt:

$$a^{560} \equiv 1 \bmod 561$$

561 ist die kleinste Carmichaelzahl. Alle Carmichaelzahlen kleiner als 100.000 sind in der Tabelle 10.1 aufgelistet.

| | | | | | |
|---|---|---|---|---|---|
| 561 | = | $3 \cdot 11 \cdot 17$ | 1105 | = | $5 \cdot 13 \cdot 17$ |
| 1729 | = | $7 \cdot 13 \cdot 19$ | 2465 | = | $5 \cdot 17 \cdot 29$ |
| 2821 | = | $7 \cdot 13 \cdot 31$ | 6601 | = | $7 \cdot 23 \cdot 41$ |
| 8911 | = | $7 \cdot 19 \cdot 67$ | 10585 | = | $5 \cdot 29 \cdot 73$ |
| 15841 | = | $7 \cdot 31 \cdot 73$ | 29341 | = | $13 \cdot 37 \cdot 61$ |
| 41041 | = | $7 \cdot 11 \cdot 13 \cdot 41$ | 46657 | = | $13 \cdot 37 \cdot 97$ |
| 52633 | = | $7 \cdot 73 \cdot 103$ | 62745 | = | $3 \cdot 5 \cdot 47 \cdot 89$ |
| 63973 | = | $7 \cdot 13 \cdot 19 \cdot 37$ | 75361 | = | $11 \cdot 17 \cdot 31$ |

Tabelle 10.1: Carmichealzahlen bis 100.000

Es gibt, wie 1994 gezeigt wurde, unendlich viele Carmichaelzahlen.

Jetzt kann man auch die Frage beantworten, ob die RSA-Verschlüsselung auch funktioniert, wenn $p$ oder $q$ nicht prim sind. Wenn man sich die grundlegenden mathematischen Gleichungen zu RSA ansieht, stellt man fest, dass nur zwei Tatsachen über $p$ und $q$ wirklich benötigt werden:

- $p$ und $q$ sind teilerfremd
- Es muss für alle $a \in \mathbb{N}$ mit $1 < a < pq$ gelten:

$$a^p \equiv a \bmod p \quad \text{und} \quad a^q \equiv a \bmod q$$

Daraus folgt aber, dass $p$ und $q$ nicht notwendigerweise prim sein müssen, sondern auch Carmichaelzahlen sein können. Daher ist das RSA-Verfahren kein Primzahltest.

DERIVE ermöglicht auch einen Test von Carmichaelzahlen. Mit folgendem Befehl kann man überprüfen, ob es sich um eine Carmichaelzahl handelt oder nicht:

```
Carmichael?(n, f_) :=
  Prog
   If n = 1 ∨ MOD(n, 2) = 0 ∨ PRIME?(n)
    RETURN false
```

```
f_ := FACTORS(n)
If SOME(e_ > 1, e_, f_ COL 2)
 RETURN false
EVERY(MOD(n - 1, p_ - 1) = 0, p_, f_ COL 1)
```

## 10.2 Der Rabin-Miller-Test

Ein Ziel ist es nun den Fermattest soweit zu verschärfen, dass es ein Pendant zu den Carmichaelzahlen dann nicht mehr gibt. Ein effektiveres Testverfahren fanden Rabin und Miller 1976. Es liefert zwar nicht mit absoluter Sicherheit Primzahlen, denn es handelt sich um ein probabilistisches Verfahren, doch die Fehlerwahrscheinlichkeit ist sehr gering.

Der Test beruht auf der einfachen Tatsache, dass die quadratische Kongruenz

$$x^2 \equiv 1 \bmod p$$

für eine Primzahl $p$ nur die Lösungen $\pm 1 \bmod p$ besitzt. Denn ist etwa $x$ eine Lösung dieser Kongruenz, so gilt, da $p$ eine Primzahl ist,

$$p \mid (x+1)(x-1) \Longleftrightarrow p \mid (x+1) \vee p \mid (x-1), \tag{10.2}$$

also $x \equiv \pm 1 \bmod p$.

Betrachten wir nun die kleinste Carmichaelzahl 561: Sie ist klarerweise auch eine PSP(2), also gilt:

$$2^{560} \equiv 1 \bmod 561$$

Weiters berechnet man:

$$2^{280} \equiv 1 \bmod 561$$

$$2^{140} \equiv 67 \bmod 561$$

Aber hier hat man schon 561 als nicht prim entlarvt: Denn nach 10.2 müsste $2^{140} \equiv \pm 1 \bmod 561$ gelten, wenn 561 eine Primzahl wäre.
Betrachten wir nun ein Beispiel mit einer Primzahl, etwa $p = 97$, und nehmen als Basis 3: Nach dem Satz von Fermat gilt:

$$3^{96} \equiv 1 \bmod 97$$

Weiters berechnet man:

$$3^{48} \equiv 1 \bmod 97$$

$$2^{24} \equiv -1 \bmod 97$$

Die Zahl $p = 97$ hat den Test bestanden (für eine Primzahl natürlich eine Selbstverständlichkeit).

## 10.2 Der Rabin-Miller-Test

Die Frage ob $n$ eine Primzahl ist oder nicht, darüber kann man ausgehend von der Gleichung

$$a^{n-1} \equiv 1 \bmod n$$

folgende Überlegungen anstellen:

- Wenn
$$a^{\frac{n-1}{2}} \not\equiv \pm 1 \bmod n$$
dann ist $n$ sicher keine Primzahl.

- Wenn
$$a^{\frac{n-1}{2}} \equiv -1 \bmod n$$
oder
$$a^{\frac{n-1}{2}} \equiv 1 \bmod n \quad \text{und} \quad \frac{n-1}{2} \quad \text{ist ungerade,}$$
dann ist der Test bestanden und $n$ kann eine Primzahl sein.

- Wenn
$$a^{\frac{n-1}{2}} \equiv 1 \bmod n \quad \text{und} \quad \frac{n-1}{2} \quad \text{ist gerade,}$$
dann wiederholt man den Test mit $\frac{n-1}{2}$ statt $n-1$.

In der Praxis geht man umgekehrt vor:

**Satz 10.3. Rabin-Miller-Test**
Es sei $n$ eine ungerade natürliche Zahl $n$ mit $n = 2^s \cdot t + 1$ mit $t \in \mathbb{N}$ ungerade und $s > 1, s \in \mathbb{N}$. (Diese Darstellung ist eindeutig.)

Die Zahl $n$ kann nur dann eine Primzahl sein, wenn für alle $a$ mit $0 < a < n$ entweder $a^t \equiv \pm 1 \bmod n$ oder wenn man durch (s-1)-maliges Quadrieren dieses Wertes auf $-1$ modulo $n$ kommt.

Betrachten wir dazu wieder das Beispiel $n = 561$ und die Basis $a = 2$: Es gilt :

$$561 = 2^4 \cdot 35 + 1$$

Man berechnet:

$$2^{35} \equiv 263 \bmod 561$$

$$2^{2 \cdot 35} \equiv 166 \bmod 561$$

$$2^{4\cdot 35} \equiv 67 \bmod 561$$
$$2^{8\cdot 35} \equiv 1 \bmod 561$$

Also gilt:
$2^{35} \not\equiv \pm 1 \bmod 561$ und der Wert $-1$ tritt nicht beim Quadrieren auf, das heißt 561 kann keine Primzahl sein.

Vielleicht bringt man hier auch noch den Begriff der starken Pseudoprimzahl zur Basis $a$:

**Definition 10.2.1.**
Eine zusammengesetzte Zahl, die den Rabin-Miller Test zur Basis $a$ besteht, das heißt nicht als zusammengesetzt erkannt wird, heißt starke Pseudoprimzahl zur Basis $a$, kurz SPSA(a).

Wir wählen $n = 3277$ (=PSP(2)) und $a = 2$, dann gilt:

$$3277 = 4 \cdot 819 + 1$$
$$2^{819} \equiv 128 \bmod 3277$$
$$2^{2\cdot 819} \equiv -1 \bmod 3277$$

Die Zahl $3277 = 29 \cdot 113$ ist also sogar eine SPSP(2). Führt man man hingegen den Test für die Basis 3 aus, so zeigt sich, dass 3277 nicht prim ist.

Die kleinste zusammengesetzte Zahl, die den Rabin-Miller-Test für die Basen 2 und 3 besteht ist $1373653 = 829 \cdot 1657$. Indem man zum Beispiel nur drei Rabin-Miller-Tests durchführt, und zwar für die Basen 2, 3 und 5, wird jede zusammengesetzte Zahl $n < 25 \cdot 10^9$ sicher erkannt.

Der Rabin-Miller-Test ist ein relativ schneller und einfach zu programmierender probabilistischer Test. Ist bei k-maliger unabhängiger Durchführung nicht die Zusammengesetztheit bewiesen worden, dann kann man mit einer Irrtumswahrscheinlichkeit von $(\frac{1}{4})^k$ davon ausgehen, dass $n$ eine Primzahl ist.

Bei den hier zu bearbeitenden Aufgaben geht es um das Potenzieren von Zahlen mit großen Exponenten. Daher soll jetzt hier ein schneller Potenzieralgorithmus vorgestellt werden, die “Square and Multiply”-Methode, welche sehr schnell ist. Die Idee dahinter ist rasch erklärt: Will man zum Beispiel $3^{21}$ berechnen, so kann man das so tun:

$$3^{21} = 3^1 \cdot 3^4 \cdot 3^{16}$$

Dabei gehen die Faktoren durch Quadrieren auseinander hervor, es wird aber nicht jedes Quadrat benötigt. Sieht man sich die Binärdarstellung von 21 an, $21 = 10101_2$, so erkennt man, dass der Faktor genau dann berücksichtigt werden muss, wenn in der Binärdarstellung eine 1 steht.

Also kann man $a^r$ folgendermßen rasch berechnen: Wenn

$$r = \sum_{i=0}^{s} e_i 2^i \qquad \text{mit } e_i \in \{0, 1\}$$

die eindeutige Binärdarstellung des Exponenten $e$ von $a$ ist, dann gilt:

$$a^r = (a^{2^s})^{e_s} \cdots (a^2)^{e_1} \cdot a^{e_0}$$

und damit kann man den Rechenaufwand erheblich einschränken: Hat man einen Exponenten von 10000, so müssen höchstens 14 Quadrierungen und höchstens 14 Produktbildungen durchgeführt werden.

Das Programm vom Rabin-Miller-Test in DERIVE sieht folgendermaßen aus:

```
Rabin_Miller(n, a := 2, a_, s_, t_) :=
  Prog
   If n = 1
    RETURN false
   If EVEN?(n)
    RETURN SOLVE(n = 2)
   If NUMBER?(a)
    If a > 0
     a := [a]
     a := SELECT(PRIME(q_), q_, -a)
   t_ := n - 1
   Loop
    t_ :/ 2
    If ODD?(t_) exit
   Loop
    If a = [] exit
    s_ := t_
    a_ := - ABS(MODS(FIRST(a)^s_, n))
    Loop
     If a_ = -1
      [a := REST(a), exit]
     s_ :* 2
     If s_ = n - 1
      RETURN false
     a_ := MODS(a_^2, n)
```

Mit diesem Programm können wir nocheinmal unsere Überlegungen für die Zahl 3277 durchführen:

```
Rabin_Miller(3277) = true
```

```
Rabin_Miller(3277, [2, 3]) = false
```

Das bestätigt unsere vorhergehenden Ergebnisse.

# Kapitel 11

# Die Zufälligkeit von Zahlen

Um die Sicherheit des RSA-Verfahren zu garantieren, ist es unbedingt notwendig darauf zu achten, wirklich zufällige Primzahlen zu verwenden. Lässt man sich von DERIVE einige Primzahlen berechnen, so ist nicht erwiesen, dass diese auch tatsächlich zufällig gewählte Zahlen sind. In diesem abschließenden Kapitel beschäftigen wir uns daher mit der "Zufälligkeit von Zahlen" und stellen ein paar schöne Querverbindungen zur Statistik beziehungsweise Wahrscheinlichkeitsrechnung her.

Mit einem Experiment werden wir den Schülern zunächst vor Augen führen, dass "Zufallszahlen" gewissen Gesetzmäßigkeiten gehorchen, nämlich den Gesetzen der Statistik.

## 11.1 Run-Test

Man lässt jeden Schüler eine Zahlenfolge aufschreiben, die einen 50 mal durchgeführten Münzwurf (Kopf 0, Adler 1) simulieren soll. Anschließend soll jeder das Experiment tatsächlich durchführen. Jeder Schüler erhält so zwei Serien von je 50 0/1-Folgen:

$r_1 := [1,0,1,0,1,1,1,0,0,0,1,1,1,0,1,0,1,0,1,1,0,0,1,1,1,0,1,0,0,1,0,0,1,1,0,0,0,1,0,0,$

$1,0,0,1,0,1,1,0,1,0]$

$r_2 := [0,0,1,1,1,0,0,0,1,0,1,1,1,1,1,1,0,1,0,0,1,0,0,0,0,1,0,1,0,1,1,1,0,0,0,0,0,1,0,1,$

$0,1,1,0,0,1,1,1,0,0]$

Man zählt nun die Runs (= Blöcke) gleicher Ziffern (der erste Run der zweiten Serie ist (00), dann folgt der Run (111) usw.), welches zu folgendem Ergebnis führt:

1. Folge: 32 Runs
2. Folge: 25 Runs

Mit Hilfe der Wahrscheinlichkeitsrechnung (Binomialverteilung) kann man berechnen, dass bei 50 Würfen der Erwartungswert $\mu$ für die Anzahl der Runs $25,5$ beträgt und die Wahrscheinlichkeit für mehr als 32 Runs ungefähr $7,62\%$ beträgt. Mit diesem Wissen kann man daher ziemlich sicher annehmen, dass die 1. Folge von den Schülern konstruiert wurde: Bei dem Versuch den Zufall nachzubilden, haben sie mehr Wechsel zwischen 0 und 1 produziert, als es den Regeln der Statistik entspricht. Berechnet man den Mittelwert der Runs, der von den Schülern gedachten Zufallszahlenfolgen und der tatsächlichen Zufallsfolgen, dann wird der Erste um einiges größer sein als der Zweite. Die Schüler erkennen, dass in den tatsächlichen Zufallsfolgen oft längere Runs als vorausgesehen auftreten (zum Beispiel: 5-mal hintereinander Kopf), während in den gedachten Folgen Runs mit 5 aufeinanderfolgenden Ziffern selten sind. Man wird also in sehr vielen Fällen die vom Schüler "gedachten" Zufallsfolgen erraten können.

Hat man in der siebenten Klasse die Binomialverteilung schon zur Verfügung, dann empfiehlt es sich die oben angegebenen Berechnungen auch durchzuführen:

Es sei $R_n$ die Anzahl der Runs in der Zahlenfolge $x_1 x_2 \cdots x_n$, wobei $x_i \in \{0, 1\}$.

Es gilt: $1 \leq R_n \leq n$. (Mindestens ein Run findet immer statt, z.B.: $1111 \cdots 11$.) Wir betrachten nun die Anzahl der Runs $R_n - 1$, die der ersten Ziffer folgen. Die Anzahl der Möglichkeiten für $k$ Runs innerhalb der Zahlenfolge $x_2 x_3 \cdots x_n$ ist dann gegeben durch

$$2 \cdot \binom{n-1}{k},$$

denn man hat $\binom{n-1}{k}$ Möglichkeiten einen Anfangspunkt unter den $n-1$ Zahlen für einen Run zu wählen und die Multiplikation mit 2 ist notwendig, weil die Zufallszahlenfolge entweder mit $x_1 = 0$ oder mit $x_1 = 1$ gestartet werden kann.

Wir berechnen nun die Wahrscheinlichkeit, dass genau $k$ Runs innerhalb der $n-1$ Zufallszahlen stattfinden:

$$P(R_n - 1 = k) = \frac{2 \cdot \binom{n-1}{k}}{2^n} = \binom{n-1}{k} \cdot \left(\frac{1}{2}\right)^k \cdot \left(\frac{1}{2}\right)^{n-1-k}$$

Dabei wurde die Laplace'sche Wahrscheinlichkeitsregel verwendet und die Tatsache, dass eine Menge von $n$ Elementen $2^n$ Teilmengen besitzt. Das Ergebnis zeigt, dass $R_n - 1$ binomialverteilt ist mit den Parametern $n$ und $p = \frac{1}{2}$. Daher können wir den Erwartungswert $\mu$ berechnen:

$$\mu = E(R_n) = 1 + E(R_n - 1) = 1 + \frac{n-1}{2} = \frac{n+1}{2}.$$

Für die Standardabweichung $\sigma$ gilt:

$$\sigma = \sqrt{(n-1)\frac{1}{2}\frac{1}{2}} = \sqrt{\frac{n-1}{4}}$$

Für $n = 50$ ergibt sich $\mu = 25,5$ und $\sigma = 3,5$. Weiters berechnet sich:

$$P(R_n > 31) = P(R_n - 1 > 30) = 1 - P(R_n - 1 \leq 29) \approx 1 - 0,9237 = 7,62\%$$

## 11.2 Erzeugung von Pseudozufallszahlen

Das menschliche Gehirn kann also einen Zufallsprozess nur sehr unvollkommen nachahmen. Es stellt sich daher die Frage, wie man zufällige Zahlen erzeugen kann. Computer sind Maschinen, die nichts dem Zufall überlassen, sie berechnen beliebig oft aus denselben Rohdaten genau die gleichen Resultate. Deshalb bezeichnet man Computer als deterministische Maschinen. Wie kann man eine solche deterministische Maschine dazu bringen, zufällige Resultate zu erzeugen? Man wird die Schüler mit der Frage konfrontieren, ob ein Computer zum Beispiel als Würfel herhalten und in dieser Eigenschaft eine völlig zufällige Folge von Zahlen zwischen eins und sechs produzieren kann. Die vorweggenommene Antwort lautet, er kann es streng genommen nicht. Das Erzeugen von zufälligen Folgen von Zahlen ist aber eine derart wichtige Aufgabe, dass Lösungen gesucht wurden, Folgen von Zahlen zu erzeugen, die möglichst viele Eigenschaften einer zufälligen Folge aufweisen. Dazu gibt es einfache Algorithmen, die man in der Schule vorstellen kann. Solche Zahlen entstehen also nicht "zufällig", sondern sind streng determiniert. Deshalb spricht man von Pseudozufallszahlen. Diese Zahlen sind zunächst ganzzahlig. Sie lassen sich durch Skalierung auf jedes beliebige Intervall beschränken, allerdings sind sie dann nicht mehr ganzzahlig. Häufig benötigt man Zufallszahlen $x_i$ im Intervall $[0; 1]$, die als Realisierungen von unabhängigen und gleichverteilten Zufallsvariablen $X_i$ aufgefasst werden können. Diese Zufallszahlen $x_i$ heißen dann Standard-Psesudozufallszahlen.

### 11.2.1 Quadratmittenmethode

Das älteste bekannte Verfahren und Grundlage der ersten Zufallsgeneratoren ist die Quadratmittenmethode nach Neumann (1946): Man wählt eine $n$-stellige Zahl als Startwert. Dann nimmt man diese zum Quadrat und holt aus der Mitte des Ergebnisses wieder eine $n$-stellige Zahl heraus.

Wir berechnen Zufallszahlen mit der Quadratmittenmethode mit dem Startwert 3546:

$3546 \longrightarrow 3546^2 = 12574116 \longrightarrow 5741$
$5741 \longrightarrow 5741^2 = 32959081 \longrightarrow 9590$
$9590 \longrightarrow 9590^2 = 91968100 \longrightarrow 9681$
$9681 \longrightarrow 9681^2 = 93721761 \longrightarrow 7217$
$7217 \longrightarrow 7217^2 = 52085089 \longrightarrow 850$
$850 \longrightarrow 850^2 = 722500 \longrightarrow 2250$, usw.

Es entsteht die Zufallsfolge 5741, 9590, 9681, 7217, 0850, 2250, ... und da man $n = 4$ gewählt hat, liegen alle Zufallszahlen im Intervall $[0, 9999]$. Die Standard-Pseudozufallszahlen entstehen, indem man diese Zahlen durch 10000 dividiert. Sie liegen im Intervall $[0; 1]$.

Unter Umständen entstehen hier aber sehr kurze "Zufallsfolgen" (etwa mit dem Startwert 3792). Das ist auch ein Grund, weshalb diese Methode nicht mehr verwendet wird.

### 11.2.2 Lineare Kongruenzmethode

In seinem Buch "The Art of Computer Programming" hat Donald E. Knuth viele Grundlagen zusammengetragen, auf denen die Berechnungsmethoden der heutigen Computerprogramme aufbauen. Er behandelt darin auch mehrere Vorschläge, wie pseudo-zufällige Zahlenfolgen erzeugt werden können. Auf diesen Vorschlägen basieren die Zufallszahlen-Generatoren, die in Programmiersprachen, Tabellenkalkulations-Programmen und anderer Software eingesetzt werden. Am besten hat Knuth die Methode der linearen Kongruenz untersucht, die er von D. H. Lehmer übernimmt. Viele Zufallsgeneratoren arbeiten nach dieser Methode, die auf der Rekursion

$$z_n = (a \cdot z_{n-1} + c) \mod m \quad \text{mit } n \geq 1 \tag{11.1}$$

beruht. Dazu muss man die drei Parameter $a \in \{0, 1, \ldots, m-1\}$, $c \in \{0, 1, \ldots, m-1\}$ und $m \in \mathbb{N}$ und $m > 1$ vorgeben und den Startwert $z_0 \in \{0, 1, \ldots, m-1\}$ selbst wählen. Hieraus ergeben sich durch $x_i = \frac{z_i}{m}$ die Standard-Pseudozufallszahlen $x_i$.

- Es ist klar, dass mit dem in 11.1 definierten linearen Kongruenzgenerator höchstens $m$ verschiedene Zahlen $z_1, z_2, \ldots, z_n$ erzeugt werden können.
- Sobald sich eine Zahl $z_k$ zum ersten Mal wiederholt, das heißt es gibt ein $r > 0$ mit $z_k = z_{k-r}$, beginnt erneut die gleiche Periode der Länge $r$, die bereits einmal vollständig erzeugt worden ist. Das folgt leicht mittels vollständiger Induktion:

$$z_{k+1} = a \cdot z_k + c = a \cdot z_{k-r} + c = z_{k-r+1} \mod m$$

- Bei einer ungünstigen Wahl der Parameter $a, c, m$ bzw $z_0$ kann die Länge der Periode sehr klein sein. Beispielsweise ist $r = 2$ für $a = c = z_0 = 5$ und $m = 10$. In diesem Fall werden nur die Zahlen $5, 0, 5, 0, \ldots$ erzeugt.

Ein wünschenswertes Qualitätskriterium von linearen Kongruenzgeneratoren ist jedoch, dass die Länge der Periode $r$ möglichst nahe bei der Maximallänge $m$ liegt. Offensichtlich müssen die Parameter in der Rekursion einigen Bedingungen genügen, um eine möglichst lange Periode zu erreichen.

Man kann den Schülern nun folgenden Satz von D.E. Knuth mitteilen:

**Satz 11.1.**
Lineare Kongruenzgeneratoren erreichen für $c > 0$ genau dann ihre maximal mögliche Periodenlänge $m$, wenn die folgenden Voraussetzungen erfüllt sind:

- Der Parameter $c$ ist zum Modul $m$ teilerfremd.
- Jeder Primfaktor von $m$ teilt $a - 1$.
- Wenn $m$ durch 4 teilbar ist, dann auch $a - 1$.

In diesem Fall erzeugt der in 11.1 definierte Generator für jedes $z_0 \in \{0, 1, \ldots, m-1\}$ eine Zahlenfolge $z_1, z_2, \ldots, z_n$ mit der maximalen Periodenlänge $m$.

Die Zahlen $a = 49, c = 35$ und $m = 96 = 2^5 3$ erfüllen obige Bedingungen. Mit dem DERIVE-Befehl

```
ITERATES(mod(49i+35,96),i,1,96)
```

erhält man

```
[1, 84, 23, 10, 45, 32, 67, 54, 89, 76, 15, 2, 37, 24, 59, 46, 81, 68, 7, 90,
29, 16, 51, 38, 73, 60, 95, 82, 21, 8, 43, 30, 65, 52, 87, 74, 13, 0, 35, 22,
57, 44, 79, 66, 5, 88, 27, 14, 49, 36, 71, 58, 93, 80, 19, 6, 41, 28, 63, 50,
85, 72, 11, 94, 33, 20, 55, 42, 77, 64, 3, 86, 25, 12, 47, 34, 69, 56, 91, 78,
17, 4, 39, 26, 61, 48, 83, 70, 9, 92, 31, 18, 53, 40, 75, 62, 1]
```

also genau eine Zahlenfolge mit der maximalen Periodenlänge 96. (Hier wurde 1 als $z_0$ gewählt, ein analoges Ergebnis erhält man für jeden anderen Startwert.)

Wenn $c = 0$ ist, spricht man von einem multiplikativen Kongruenzgenerator. Für die maximale Periodenlänge gilt: $r \leq m - 1$. Von weiteren Regeln in Zusammenhang mit der Periodenlänge wollen wir in diesem Fall absehen.

### 11.2.3 Erzeugung von Zufallszahlen mit DERIVE

Ein weiterer Vorschlag zur Erzeugung von Zufallszahlen stammt von J. Wiesenbauer für das Programm DERIVE. Dabei wird zuerst eine 4-bit Zahl festgesetzt mit

```
r:=RANDOM(8) + 8.
```

Dann wird folgende Zeile in die Eingabezeile von DERIVE kopiert, ohne dass Enter gedrückt wird.

```
0ů(r:= 16ůr + MOD(RANDOM(0), 16)) + FLOOR(LOG(r, 2) + 1)
```

Nun drückt man solange mit der Maus auf die Taste "=", welche sich links von der Eingabezeile befindet, bis am Bildschirm jene Zahl erscheint, die die Anzahl der Bits der gewünschten Zufallszahl angibt (zum Beispiel 160 Bits). Während dieses Vorgangs darf man weder die "Enter"-Taste noch die Taste "Vereinfachen" in der Menüleiste oben drücken. Dann fehlt nur noch die Eingabe `r =` und man erhält eine mögliche Zufallszahl.

Es gibt noch viele andere Generatoren zur Erzeugung von Pseudozufallszahlen, wie beispielsweise nichtlineare Kongruenzgeneratoren, Schieberegister-Generatoren, Fibonacci-Generatoren usw.

Es gibt aber keine ganz zuverlässige Methode zum Herstellen von Zufallszahlen. Daher müssen die Ziffern nach ihrer Herstellung geprüft werden. Es genügt nicht nur, dass die Häufigkeiten der einzelnen Ziffern stimmen, es müssen auch die Häufigkeiten aller Ziffernblöcke stimmen.

## 11.3 Tests von Zufallszahlen- Pokertest

Wir wollen im Folgenden nach dem Run-Test zwei weitere Tests für eine binäre Zufallsfolge $r = [r_0, r_1, r_2, \ldots, r_{n-1}]$ mit $r_i \in \{0, 1\}$ vorstellen. Dazu brauchen wir den Chi-Quadrattest aus der Stochastik, den man den Schülern an dieser Stelle wahrscheinlich zunächst vorstellen muss, da er im Regelunterricht nicht vorgesehen ist. Es sei hier nur kurz darauf eingegangen, da er nicht zum eigentlichen Thema dieser Arbeit gehört. Voraussetzung ist natürlich auch, dass die Schüler einiges an Wissen aus der Wahrscheinlichkeitsrechnung und Statistik mitbringen.

Mit dem Chi-Quadrattest ($\chi^2$-Test) kann man eine Hypothese über die Form der Verteilung prüfen.

Es wird zunächst bei einer gegebenen Datenmenge von $n$ Daten eine Klasseneinteilung getroffen. Nehmen wir an, es seien $k$ Klassen (Intervalle) gewählt worden. Dann bezeichnen wir mit $h_i$ die absolute Häufigkeit, also die Anzahl von Daten in der $i$-ten Klasse und mit $e_i$ die aus der Hypothese theoretisch berechnete Häufigkeit, also die erwartete Häufigkeit. Die Statistik verwendet nun die quadratischen Abweichungen, genauer die Testfunktion

$$X = \sum_{i=1}^{k} \frac{(h_i - e_i)^2}{e_i}. \tag{11.2}$$

Dieses $X$ ist nun annähernd $\chi^2$-verteilt mit $k - 1$ Freiheitsgraden. Mit Hilfe dieser (tabellierten) Verteilung entscheidet man schließlich über die jeweilige Hypothese: Wählt man eine Irrtumswahrscheinlichkeit $\alpha$ und ist $f$ die Anzahl der Freiheitsgrade, dann wird die Hypothese abgelehnt, wenn

$$X > \chi^2(f; \alpha).$$

Gilt hingegen

$$X \leq \chi^2(f; \alpha),$$

so wird die Hypothese angenommen .

Da die $\chi^2$-Verteilung eine Näherung ist, ist der $\chi^2$-Test nur aussagekräftig, wenn die Anzahl der betrachteten Zahlen groß genug ist. Für die Größe von $n$ gibt Knuth folgende Faustregel an: Die Anzahl der Zahlen $n$ muss mindestens so groß sein, dass für jede Klasse der Erwartungswert der Beobachtungen mindestens fünf oder mehr betrage.

Wir behandeln zunächst den Gleichverteilungstest. Dieser Test untersucht, ob die Anzahl der “0” und “1” annähernd gleich ist. Es ist leicht einzusehen, dass dies eine erste wichtige Forderung für eine Zufallszahl ist. Bezeichnet man mit $n_0$ und $n_1$ die Anzahl der Ziffern “0” und “1”, dann berechnet man mit $n = n_0 + n_1$

$$X = \sum_{i=0}^{1} \frac{(n_i - \frac{n}{2})^2}{\frac{n}{2}} = \frac{(n_0 - n_1)^2}{n}.$$

Dieser Wert lässt eine Ausssage zu, ob die Verteilung der Zahlen zufällig sein kann: Die Hypothese, dass $r$ eine Zufallszahl ist, wird mit einer Irrtumswahrscheinlichkeit $\alpha$ abgelehnt oder angenommen, wobei der Freiheitsgrad hier 1 ist. Um die Forderung, dass der Erwartungswert für $n_0$ und $n_1$ mindestens fünf oder mehr betrage, zu erfüllen, muss $n \geq 10$ sein.

Ein Verallgemeinerung dieses Tests ist der Pokertest:

Um die Voraussetzungen für den Chi-Quadrattest zu erfüllen, bestimmen wir eine positive ganze Zahl $m$ so, dass

$$[\frac{n}{m}] \geq 5 \cdot 2^m \quad \text{und setzen } \; k = [\frac{n}{m}].$$

Jetzt unterteilen wir die Folge $r$ in $k$ sich nicht überdeckende Blöcke (Teilfolgen) der Länge $m$. Wir zählen nun, wie oft der $i$-te Typ einer dieser Blöcke der Länge $m$ vorkommt, wobei $1 \leq i \leq 2^m$. Bezeichnet man mit $n_i$ $(1 \leq i \leq 2^m)$ die Anzahl des Auftretens der einzelnen Blöcke, dann berechnet man mit $n = n_0 + n_1 + \cdots + n_{2^m}$

$$X = \sum_{i=1}^{2^m} \frac{(n_i - \frac{k}{2^m})^2}{\frac{k}{2^m}} = \frac{2^m}{k}\Big(\sum_{i=1}^{2^m} n_i^2\Big) - k.$$

Aufgrund der Wahl von $m$ beträgt der Erwartungswert für die $n_i$ mindestens fünf. Dieses $X$ ist nun annähernd $\chi^2$-verteilt mit $2^m - 1$ Freiheitsgraden. Der Wert $X$ lässt daher eine Ausssage zu, ob die Verteilung der Zahlen zufällig sein kann: Die Hypothese, dass $r$ eine Zufallszahl ist, wird mit einer Irrtumswahrscheinlichkeit $\alpha$ abgelehnt oder angenommen.

Als Beispiele untersuchen wir mit dem Pokertest die beiden beim Run-Test angeführten Folgen:

$r_1 := [1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 1, 1, 1, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 1, 1, 0, 0, 0, 1, 0, 0,$

$1, 0, 0, 1, 0, 1, 1, 0, 1, 0]$

Hier ist $m = 2$ und $k = 25$. Die Blöcke 00, 01, 10 und 11 kommen 5, 4, 11 und 5 mal vor. Als Wert für $X$ ergibt sich $4,92$. Laut Tabelle oder Berechnung ergibt sich mit dem Freiheitsgrad $3 = 2^2 - 1$ für den "Schwellenwert" der Irrtumswahrscheinlichkeit $\alpha$ der Wert $17,77\%$, denn es gilt:

$$\chi^2(0,1777; 3) \approx 4,92$$

Die Hypothese $r_1$ ist eine Zufallsfolge, sie wird daher mit einer Irrtumswahrscheinlichkeit größer als $17,77\%$ abgelehnt, mit einer Irrtumswahrscheinlichkeit kleiner als $17,77\%$ angenommen.

$r_2 := [0, 0, 1, 1, 1, 0, 0, 0, 1, 0, 1, 1, 1, 1, 1, 1, 0, 1, 0, 0, 1, 0, 0, 0, 0, 1, 0, 1, 0, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1,$

$0, 1, 1, 0, 0, 1, 1, 1, 0, 0]$

Hier ist $m = 2$ und $k = 25$. Die Blöcke 00, 01, 10 und 11 kommen 7, 8, 4 und 6 mal vor. Als Wert für $X$ ergibt sich $1,4$. Hier gilt:

$$\chi^2(0,7055; 3) \approx 1,4$$

Die Hypothese $r_2$ ist eine Zufallsfolge, sie wird daher hier mit einer Irrtumswahrscheinlichkeit $\alpha$ größer als 70, 55% abgelehnt, mit einer Irrtumswahrscheinlichkeit kleiner als 70, 55% angenommen.

Auch der Pokertest zeigt, dass die zweite Folge eher einer echten Zufallsfolge entspricht als die erste.

Der Pokertest kann auch mit DERIVE durchgeführt werden. Das entsprechende Programm stammt von J. Wiesenbauer.

```
pokertest(s, m:=0, α:=5, info:=false, m_, n_, s_:=[ ], t_):=
 Prog
  If STRING?(s)
   s:=VECTOR(IF(s↓k_="1 "), k_, 1, DIM(s))
  If NUMBER?(s)
   Prog
    t_:=s
    s:=[ ]
    Loop
     If t_=0 exit
     s:=ADJOIN(MOD(t_, 2), s)
     t_:=FLOOR(t_, 2)
  If info
   DISPLAY(s)
  n_:=DIM(s)
  If n_<10
   RETURN "Binary string s is too short!  "
  m_:=m
  If m=0
   m:=FLOOR(LOG(n_/5, 2))
  If n_/m<5·2^m
   Prog
    Loop
     m:-1
     If n_/m=5·2^m exit
    If m_>0
     RETURN APPEND("Maximal block length m is ", m)
  Loop
   If DIM(s)<m exit
   m_:=m
   t_:=0
   Loop
```

```
   t_:* 2
   t_:+ FIRST(s)
   s:=REST(s)
   m_:-1
   If m_=0 exit
 s_:=ADJOIN(t_, s_)
s:=VECTOR(0, k_, 2^m)
Loop
 s↓(FIRST(s_) + 1) :+ 1
 s_:=REST(s_)
 If s_=[] exit
n_:=FLOOR(n_, m)
If info
  DISPLAY(s)
t_:=2^m/n_· s^2-n_
If info
  DISPLAY(APPEND "Test statistics X= ", APPROX(STRING(t_), 5)))
t_:=(1-CHI_SQUARE(t_, 2^m-1))·100
If info
  DISPLAY(APPEND("P-value for m ", m, "is ", APPROX(STRING(t_), 4), "%")
t_>α
```

Die Zahl $r$ kann in Dezimalform oder als "binärer Vektor" eingegeben werden. Ist $m$ die maximale Blocklänge, so erhält man mit der Eingabe

`pokertest(r,m,5,true)`

zusätzliche Informationen über den ausgeführten Pokertest:

- Die binäre Darstellung der Zahl, wenn man sie in Dezimalschreibweise eingegeben hat.
- Die Häufigkeiten der einzelnen Blöcke.
- Den Funktionswert $X$ (vgl. 11.2).
- Den "Schwellenwert" für die Irrtumswahrscheinlichkeit $\alpha$.
- Mit der Eingabe

  `pokertest(r,1,5,true)`

  führt man den Gleichverteilungstest durch.

Als Abschluss wollen wir mit DERIVE eine Zufallszahl erzeugen und anschließend diese auf ihre

"Zufallstauglichkeit" mit dem Pokertest überprüfen. Zuerst wird

```
r:=RANDOM(8) + 8
```

eingegeben. Weiters wird bis zur Zahl 160 mit

```
0·(r:=16·r + MOD(RANDOM(0), 16)) + FLOOR(LOG(r, 2) + 1)
```

gezählt. Nun erhalten wir für $r$ folgenden Wert

```
r = 2459419282570819411142400564995631099440251126554 99.
```

Mit dem Pokertest überprüfen wir nun, ob die Zahl tatsächlich zufällig entstanden ist. Für den Wert $m$ ergibt sich hier 3, für $k$ der Wert 53 und die entsprechende $\chi^2$-Verteilung hat $7 = 2^3 - 1$ Freiheitsgrade.

```
pokertest(r, 3, 5, true)
[1, 0, 1, 0, 1, 0, 0, 0, 0, 1, 0, 0, 0, 1, 1, 1, 1, 1, 0, 0, 0, 0, 0, 1, 0, 1,
1, 1, 1, 0, 1, 1, 1, 1, 1, 1, 0, 0, 0, 1, 0, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 1,
0, 0, 0, 1, 0, 1, 0, 0, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 0, 1, 1, 0, 1,
0, 1, 1, 0, 1, 1, 1, 1, 0, 1, 1, 1, 0, 0, 1, 1, 0, 0, 1, 0, 1, 1, 1, 0, 0, 1,
0, 1, 1, 1, 0, 0, 1, 1, 0, 1, 0, 1, 0, 1, 1, 1, 1, 0, 0, 0, 1, 1, 0, 1, 0, 0,
0, 0, 0, 0, 1, 1, 0, 1, 1, 0, 1, 1, 0, 0, 1, 1, 0, 1, 0, 0, 0, 0, 0, 0, 1, 1,
0, 1, 1, 0, 1, 0, 0, 0, 1, 0, 1, 1]
[5, 8, 7, 10, 8, 8, 4, 6]
Test statistics X = 3.7142
P-value for m = 3 is 81.20%
```

Es gibt auch den Pokertest für Dezimalzahlen. Die Idee dahinter ist der Vergleich der Häufigkeiten der verschiedenen Arten von 5-er Blöcken von Pseudozufallszahlen mit den theoretischen Wahrscheinlichkeiten. Die dabei betrachteten Möglichkeiten von 5-er Blöcken entsprechen im Prinzip möglichen Ausgängen beim Pokern, daher auch der Name. Man wird das Spiel aber etwas vereinfachen, indem man nur fünf Klassen $E_1, \ldots, E_5$ bildet: 5 verschiedene, 4 verschiedene (1 Paar), 3 verschiedene (2 Paare oder 3 von einer Sorte), 2 verschiedene (4 von einer Sorte oder ein Tripel und ein Paar) und alle von einer Sorte bildet. Die entsprechenden theoretischen Wahrscheinlichkeiten sind: $P(E_1) = 0,3024$, $P(E_2) = 0,5040$, $P(E_3) = 0,1800$, $P(E_4) = 0,0135$ und $P(E_5) = 0,0001$. Zum Berechnen dieser Werte braucht man im Wesentlichen nichts anderes als die Laplace'sche Wahrscheinlichkeitsregel. Sei $r$ nun eine $n$-stellige Dezimalzahl, dann gibt es $[\frac{n}{5}]$ 5-er Tupel. Die theoretische Häufigkeit $e_i$ (vgl. 11.2) für das Aufreten eines Tupels der Klasse $E_i$ ist dann gegeben durch

$$e_i = P(E_i) \cdot \frac{n}{5}.$$

Da mit den erhaltenen Werten wieder ein $\chi^2$-Test durchgeführt wird, sollte $r$ eine mindestens 250000-stellige Dezimalzahl sein, damit in die letzte und kleinste Klasse mindestens 5 der 50000 5-er Tupel fallen. Wir bestimmen wieder den Wert der Testfunktion $X$ für die Zahl $r$ und mit Hilfe der $\chi^2$-

Verteilung (Freiheitsgrad 4, Irrtumswahrscheinlichkeit $\alpha$) entscheiden wir wieder, ob die Hypothese angenommen oder abgelehnt wird.

# Kapitel 12

# Beispiele

Im folgenden sind einige Beispiele zu den einzelnen Kapiteln angeführt, die man im Unterricht einsetzen kann.

## Motivierende Beispiele

1. Herbert las auf einer alten Rechnung:

   $$72 \text{ Fußbälle} \ldots\ldots Y59X \text{ Schilling.}$$

   Die erste und die letzte Ziffer des Betrages (X und Y) konnte er leider nicht mehr entziffern.

   Wie viel Schilling kostete damals ein Fußball?

2. Zeige, dass jede sechsstellige Zahl $n$ der Form

   $$n = \overline{abcabc}$$

   durch 7, 11 und 13 teilbar ist.

   Zeige entsprechend, dass jede achtstellige Zahl $n$ der Form

   $$n = \overline{abcdabcd}$$

   durch 73 und 137 teilbar ist.

3. Beweise: Setzt man vor eine beliebige dreistellige natürliche Zahl ihr Doppeltes, so ist die entstehende sechs- oder siebenstellige Zahl durch 23 und 29 teilbar.

4. Vier Personen $A$, $B$, $C$, $D$ legen gemeinsam eine natürliche Zahl fest. Jede der vier Personen gibt über diese Zahl drei Auskünfte, von denen jeweils mindestens eine wahr und mindestens eine falsch ist.

   A:

   - Die Zahl ist durch 4 teilbar.
   - Die Zahl ist durch 9 teilbar.
   - Das 11-fache der Zahl ist kleiner als 1000.

   B:

   - Die Zahl ist durch 10 teilbar.
   - Die Zahl ist größer als 100.
   - Das 12-fache der Zahl ist größer als 1000.

   C:

   - Die Zahl ist eine Primzahl.
   - Die Zahl ist durch 7 teilbar.
   - Die Zahl ist kleiner als 20.

   D:

   - Die Zahl ist nicht durch 7 teilbar.
   - Die Zahl ist kleiner als 12.
   - Das 5-fache der Zahl ist kleiner als 70.

   Wie lautet die Zahl?

5. Beweise: Ist $n$ ungerade und $n > 2$, so gilt $24 \mid n^3 - n$.

6. Zwei Brüder verkaufen $n$ Schafe zu je $n$ Dollar. Dann teilen sie das Geld wie folgt: Der ältere Bruder nimmt als erster 10 Dollar, anschließend der jüngere 10 Dollar usw. Am Ende zeigte sich, dass die Summe des jüngeren Bruders um 10 Dollar geringer war. Er nimmt den Zehner-Rest und das Messer des Bruders. Diese Aufteilung hat auch der ältere Bruder als korrekt anerkannt. Was kostet das Messer?

# Algorithmen

1. Gib das “Kleine 1 und 1” und das “Kleine 1 mal 1” für das Zahlensystem mit der Basis 3 und der Basis 5 an.

2. Gib die NAF-Form der Zahl 77 an.

3. Führe folgende Addition mit den NAF-Formen aus und überprüfe sie durch Übergang zum Dezimalsystem.

$$\begin{array}{cccccccc} & & & 1 & 0 & -1 & 0 \\ & & 1 & 0 & -1 & 0 & 1 \\ & 1 & 0 & 0 & -1 & 0 & 0 \\ \hline 1 & 0 & -1 & 0 & 0 & 0 & 1 \end{array}$$

4. Bestimme die NAF-Formen der Zahlen 19 und 26 , multipliziere diese beiden Zahlen miteinander und überprüfe das Ergebnis durch Nachrechnen im Dezimalsystem.

5. Für welche Zahlen kleiner gleich 64 stimmt die NAF-Form mit der binären Form dieser Zahl überein?

6. Man suche alle natürlichen Zahlen $p$ ($p > 1$) mit der Eigenschaft, dass die Zahl 307 im $p$-adischen System mit lauter gleichen Ziffern geschrieben wird.

   **Lösung:**

   Triviallösungen sind zunächst alle natürlichen Zahlen $p > 307$, da in diesen Systemen die Zahl 307 mit einem Symbol (einer “Ziffer”) dargestellt wird. Eine weitere Lösung ist $p = 306$, denn es gilt klarerweise:

   $$307 = (11)_{306}$$

   Da 307 eine Primzahl ist, kann die gesuchte $p$-adische Darstellung für $p < 306$ nur aus lauter Einsern bestehen, also

   $$307 = 1 + p + p^2 + p^3 + \cdots .$$

   Daher muss 306 durch $p$ teilbar sein und $\frac{306}{p} - 1$ ebenfalls durch $p$ teilbar sein. Der einzige Teiler von $306 = 2 \cdot 3 \cdot 3 \cdot 17$, der beide Bedingungen erfüllt, ist 17.

   Es gilt

   $$307 = 17^2 + 17^1 + 17^0$$

   also

   $$307 = (111)_{17}.$$

Alle Lösungen sind daher gegeben durch 17, 306 und alle Zahlen größer als 307.

□

7. Führe die Multiplikation $67 \cdot 45$ im dekadischen und im binären System "ägyptisch" aus.
8. Berechne mit dem erweiterten Euklidischen Algorithmus (Berlekamp- Algorithmus) den $ggT(a, b)$ und stelle ihn jeweils als Linearkombination von $a$ und $b$ dar.
   - $a = 124, b = 48$
   - $a = 391, b = 153$
   - $a = 522, b = 47$

# Primzahlen

1. Welche Zahl, die sich als Produkt von genau zwei Primzahlen schreiben lässt, liegt am nächsten bei 100?
2. Es sei $p$ eine ungerade Primzahl. Zeige:
$$24 \mid p^2 - 1$$
3. Die Formel
$$n^2 - 79n + 1601$$
liefert für $n = 0, 1, 2, \ldots, 79$ Primzahlen. Überprüfe diese Aussage mit DERIVE.
4. Sind $p$ und $p + 2$ mit $p \geq 6$ Primzahlzwillinge, so ist $p + 1$ durch 6 teilbar.
5. Jede Primzahl $p > 2$ lässt sich eindeutig als Differenz zweier Quadratzahlen darstellen.
6. Die bis heute ungelöste GOLDBACH'sche Vermutung besagt, dass jede gerade Zahl größer als 4 als Summe von zwei ungeraden Primzahlen geschrieben werden kann (Christian Goldbach (1690 - 1764)). Warum äußerte Goldbach seine Vermutung nicht für ungerade Zahlen? Gib alle "Goldbach-Zerlegungen" von 26 an! Schreib einen DERIVE Befehl um alle GOLDBACH-Zerlegungen einer vorgegebenen natürlichen Zahl zu finden.
7. Bestimme alle Primzahlen $p$, für die $4p + 1$ Quadratzahl ist.

8. Berechne $x$, $y$ und $z$ in:
$$2^x \cdot 3^{y-1} \cdot 10 \cdot 11^z = 2540$$
$$24 \cdot 3^{x-1} 5^y 7^{z+2} = 9000$$

9. Das Produkt von drei Primzahlen ist gleich dem Siebenfachen ihrer Summe. Um welche Primzahlen handelt es sich?

10. Berechne $\sigma(220)$ und $\sigma(284)$.
Zwei verschiedene natürliche Zahlen $a$ und $b$, für die gilt $\sigma(a) = \sigma(b)$, bilden ein Paar befreundeter Zahlen.
Zeige, dass auch 1184 und 1210 ein Paar befreundete Zahlen sind.

11. Es gibt keinen Term der Form
$$x^2 + ax + b \text{ mit } a, b \in \mathbb{Z},$$
der für alle $x \in \mathbb{N}$ eine Primzahl ist.

12. Überprüfe anhand der Zahl 496: Die Summe der Kehrwerte aller Teiler einer vollkommenen Zahl ist 2.

13. Zeige, dass das Produkt $n = p \cdot q$ zweier verschiedener ungerader Primzahlen $p$ und $q$ keine vollkommene Zahl sein kann.

14. Zeige: Eine Fermat'sche Zahl kann nie eine Quadratzahl sein!

15. Beweise: Ist $p$ prim, so ist $\binom{2^p}{2}$ vollkommen, wenn $2^p - 1$ eine Mersenne'sche Primzahl ist.

# Kongruenzen

1. Überprüfe die Rechnung
$$443^3 + 209^4 - 66^5 = 742635492$$
mit der Neunerprobe, das heißt stelle den Rest der linken Seite bei der Division durch 9 und den Rest der rechten Seite bei der Division durch 9 fest.

2. Überprüfe die Rechnung
$$12^3 + 45^6 + (7 + 8)^5 = 46747137728$$
mit der Elferprobe, das heißt stelle den Rest der linken Seite bei der Division durch 11 und den Rest der rechten Seite bei der Division durch 11 fest.

3. Die Zahlen 151, 175, 295, 439 und 3487 sind bei der Wahl eines geeigneten Moduls zueinander kongruent. Bestimme alle möglichen Modulen $m$.

4. Zeige, dass eine Quadratzahl bei der Division durch 4 nur den Rest 0 oder 1 lassen kann.

5. Berechne die Einerziffer der Zahlen $3^{125}$ und $7^{200}$.

6. Wir betrachten die ISBN des Buches "Fermats letzter Satzt't': ISBN 3 – 446 – 19313 – 8 Kann diese ISBN korrekt sein?

7. Kann man zwei Ziffern der ISBN von Fermats letztem Satz so abändern, dass sich trotzdem die Kontrollnummer 8 ergibt?

8. Welche Prüfziffer hat der 13-stellige ISBN-Code 978349913599 – [?] für das Buch "Fräulein Smillas Gespür für Schnee"?

# Lineare Kongruenzen

1. Ersetze die Kongruenzen $x \equiv 1 \bmod 7$ und $x \equiv 2 \bmod 11$ durch eine einzige Kongruenz.

2. Löse die folgenden linearen Kongruenzen:

$$23x \equiv 47 \bmod 253$$

$$67x \equiv 1 \bmod 127$$

3. Finde eine Zahl, die beim Teilen durch 6, 5, 4, 3 die Reste 5, 4, 3, 2 hat. (Bramagupta 598-665)

4. Jemand denkt sich eine Zahl zwischen 0 und 999. Wenn er sie durch 8 teilt, so erhält er den Rest $a$, wenn er sie durch 1254 teilt, den Rest $b$. Gib eine Formel an, wie man die gedachte Zahl aus $a$ und $b$ berechnen kann und überprüfe die Formel für $a = 7$ und $b = 5$.

5. Wenn sich die Schüler einer Klasse in Zweier- Dreier- und Viererreihen aufstellen, so bleibt jedesmal ein Schüler übrig. Erst wenn sie sich in Fünferreihen gruppieren, hat jeder seinen Platz. Wie viele Schüler hat die Klasse?

# Diophantische Gleichungen

1. Jemand kauft Lose zum Stückpreis von 40 Euro, 10 Euro und 1 Euro. Er bezahlt insgesamt 259 Euro für 100 Lose. Wie viele Lose um 1 Euro hat er gekauft?

2. Ein Betrieb kauft in unterschiedlicher Stückzahl drei verschiedene Einzelteile, die 52 Euro, 29 Euro beziehungsweise 3 Euro kosten. Es wurden insgesamt 100 Einzelteile gekauft, die Gesamtkosten betrugen 2500 Euro. Wie viele Stücke wurden von jedem Teil gekauft?

3. Löse die folgenden diophantischen Gleichungen. Gib jeweils 3 Lösungen an:

   - $17x - 21y = 22$
   - $55x + 91y = 100$
   - $100x - 99y = 81$

4. Gilt $x^2 + y^2 = z^2$ für natürliche Zahlen $x$, $y$ und $z$, dann ist entweder $x$ oder $y$ durch 3 teilbar.

5. Wie muss man vorgehen, um ganzzahlige Lösungen der Gleichung

   $$5x + 7y + 17z = 1$$

   zu finden?

6. Bergbauer Loisl stellt fest: Ein Fünftel meiner Tiere sind Schafe, einige Siebentel meiner Tiere sind Kühe und 3 meiner Tiere sind Ziegen. Wieviele Tiere hat er insgesamt?

# Fibonacci-Zahlen

1. Es sei $a_n$ die Folge der Fibonacci-Zahlen, wie sie unter 8.1 definiert werden. Beweise:

   $$a_1 + a_2 + \cdots + a_n = a_{n+2} - 1$$

2. Zeige: Wenn $a_n$ und $a_m$ teilerfremde Fibonacci-Zahlen sind, dann gilt:

   $$a_n \cdot a_m \mid a_{mn}$$

3. Zeige, dass es keine ungerade Fibonacci-Zahl gibt, die durch 17 teilbar ist.

4. Wann ist eine Fibonacci-Zahl durch 11 teilbar?

5. Der Mathematiker Zeckendorf konnte zeigen, dass mit den Fibonacci-Zahlen jede natürliche Zahl auf folgende Weise eindeutig dargestellt werden kann:

   $$n = \sum_{k \geq 1} c_k \cdot a_{k+1}, \quad \text{wobei} \quad c_k \in \{0, 1\} \quad \text{und} \quad c_k \cdot c_{k+1} = 0, \ \forall k$$

Eine Zahl wird also im "Fibonacci-Zahlensystem" wie im Binärsystem als Folge von Einsern und Nullen dargestellt, jedoch folgen niemals zwei Einser aufeinander. Die Zahl 42 hat beispielsweise die Darstellung

$$42 = 34 + 8 = a_9 + a_6 = (10010000)_F.$$

Stelle die Zahl 157 im "Fibonacci-Zahlensystem" dar.

# RSA-Verschlüsselung

1. An einen Teilnehmer mit dem öffentlichen Schlüssel $e = 65$ und $N = 263713$ soll der Text "MATHEMATIK" chiffriert geschickt werden. Dabei wird jeder Buchstabe entsprechend seiner Stellung im Alphabet kodiert (Leerzeichen=00, A=01, B=02, ..., Z=26) und die entsprechende Ziffernfolge in Blöcke der Länge drei geteilt. Wie lautet die chiffrierte Nachricht? Entschlüssle wieder die Nachricht, wenn die Zerlegung von $N = 307 \cdot 859$ bekannt ist.

2. Neben dem öffentlichen $N = 14803$ hat man aus Versehen verraten, dass $(p-1)(q-1) = 14560$ ist. Kann man daraus $p$ und $q$ berechnen?

3. Warum geht das RSA-Verfahren nicht, wenn $M \geq N$ ist? Warum funktioniert in diesem Fall das Entschlüsseln nicht?

# Primzahltests

1. Zeige mit dem Rabin-Miller-Test: Die $PSP(7) = 6697$ ist keine Primzahl. Nimm als "Zeugen" 3 (das heißt führe den Test bezüglich der Basis 3 durch).

2. Zeige, die $PSP(2) = 8321$ ist sogar eine $SPSP(2)$.

3. Zeige mit dem Rabin-Miller-Test: Die $PSP(3) = 3367$ ist keine Primzahl. Nimm als "Zeugen" 2 (das heißt führe den Test bezüglich der Basis 2 durch).

4. Zeige mit dem Lucas-Lehmer-Test, das $M_{31}$ prim ist.

5. Gegeben sei die durch
$$s_{n+1} = s_n^2 - 2 \qquad \text{und} \qquad s_1 = 4$$
definierte rekursive Folge $< s_n >$. Weiters sei $w = 2 + \sqrt{3}$ und $\overline{w} = 2 + \sqrt{3}$. Beweise die explizite Darstellung
$$s_n = w^{2^{m-1}} + \overline{w}^{2^{m-1}}$$
dieser Folge durch vollständige Induktion.

# Die Zufälligkeit von Zahlen

1. Gegeben ist die Rekursion

$$z_n = (a \cdot z_{n-1} + c) \mod m \quad \text{mit } n \geq 1$$

mit entsprechend gewählten Parametern $a, c, m$ und einem gewissen Startwert $z_0$ (vgl. 11.1, lineare Kongruenzmethode). Beweise mit vollständiger Induktion, dass für jedes $k \in \{1, 2, \ldots, n\}$ gilt:

$$z_k = \left(a^k z_0 + c\frac{a^k - 1}{a - 1}\right) \mod m$$

# Literaturverzeichnis


[1] Bartholomé A., J. Rung. und H. Kern: *Zahlentheorie für Einstieger - Eine Einführung für Schüler, Lehrer, Studierende und andere Interessierte*. Braunschweig/Wiesbaden: Verlag Vieweg, vierte Auflage, 2003.

[2] Bauer, F. L.: *Entzifferte Geheimnisse . Methoden und Maximen der Kryptologie*. Berlin: Springer, zweite Auflage, 1997.

[3] Böhm, J.: *DUG - Derive User Group*. Newsletter, Derive, Würmla, April 2007. http://www.austromath.at/dug/.

[4] Brünner, A.: *Prüfzifferberechnung*. Schulmathematik, Lichtenberg-Oberstufengymnasium, Dezember 2006. http://www.arndt-bruenner.de/mathe/scripts/pruefziffern.htm.

[5] Bundschuh, P.: *Einführung in die Zahlentheorie*. Berlin; Heidelberg; New York; London; Paris; Tokyo: Springer, 1988.

[6] Conway, J. H. und R. K. Guy: *Zahlenzauber - Von natürlichen, imaginären und anderen Zahlen*. Basel; Boston; Berlin: Birkhäuser, 1997.

[7] Dorner, M.: *Zahlentheorie in der Schule*. Unterrichtsmaterial, Schiller-Schule Bochum, Zentrale für Unterrichtsmedien, Februar 2007. http://www.zum.de/Faecher/Materialien/dorner/manuskripthtml/index.html.

[8] Engel, W. und U. Pirl (Hrsg.): *Mathematische Olympiade-Aufgaben*. Köln: Aulis Verlag Deubner & Co KG, 1979.

[9] Enzensberger, H. M.: *Zugbrücke außer Betrieb*. Artikel, Frankfurter Allgemeine Zeitung, Bergische Universität Wuppertal, April 2007. http://www.math.uni-wuppertal.de/guide/StInfo/Zugbruecke.html.

[10] Freund, H.: *Elemente der Zahlentheorie : mit 17 Beispielen und 56 Aufgaben*. Stuttgart: Teubner, 1979.

[11] Gut, J.: *Einiges über Dreiecke*. Newsletter, bfi Wien, Dezember 2006. http://members.chello.at/gut.jutta.gerhard/newsletter/newsletter9.htm.

[12] HONSBERGER, R.: *Gitter - Reste - Würfel : 91 mathematische Probleme mit Lösungen*. Braunschweig; Wiesbaden: Vieweg, 1984.

[13] KEMPERMANN, T.: *Zahlentheoretische Kostproben*, Band 86. Frankfurt am Main; Thun: Verlag Harri Deutsch, erste Auflage, 1995.

[14] KERN, A.: *Mathematik*. Lehrplan, Bundesministerium für Unterricht, Kunst und Kultur, AHS-Abteilung des BMUKK, November 2006. http://www.bmukk.gv.at/schulen/unterricht/lp/Lehrplaene_der_Allgemein2102.xml.

[15] KRAMER, J.: *Der große Satz von Fermat - die Lösung eines 300 Jahre alten Problems*. Vortrag, Humboldt Universität Berlin, Institut für Mathematik, Dezember 2006. www.mathematik.huberlin.de/~kramer/fermat.ps.

[16] LAUB, J. und ANDERE: *Lehrbuch der Mathematik - Arbeitsbuch für die fünfte Klasse*, Band 1. Wien: Hölder-Pichler-Tempsky, 1978.

[17] MATTHES, R.: *Kryptologie und Kodierungstheorie: mathematische Methoden der Datensicherheit*. München; Wien: Fachbuchverl. Leipzig im Carl Hanser Verlag, 2003.

[18] NIVEN, I. und H. ZUCKERMANN: *Einführung in die Zahlentheorie I*, Band 46. Mannheim: Bibliographisches Institut - Wissenschaftsverlag, 1976.

[19] NIVEN, I. und H. ZUCKERMANN: *Einführung in die Zahlentheorie II*, Band 47. Mannheim: Bibliographisches Institut - Wissenschaftsverlag, 1976.

[20] NÖBAUER, W. und J. WIESENBAUER: *Zahlentheorie*. Eisenstadt: Prugg, 1981.

[21] PIEPER, H.: *Heureka - Ich hab's gefunden*, Band 62. Frankfurt am Main; Thun: Verlag Harri Deutsch, zweite Auflage, 1996.

[22] POLYA, G. and J. KILPATRICK: *The Stanford Mathematics Problem Book*. New York; London: Teachers College Press - Columbia University, 1974.

[23] POMMERENING, K.: *Kryptologie*. Material zu vorlesungen, Johannes-Gutenberg-Universität Mainz, Fachbereiche Physik/Mathematik/Informatik und Medizin, Jänner 2007. http://www.staff.uni-mainz.de/pommeren/Kryptologie.

[24] REICHEL, H-C. und ANDERE: *Mathematik Lehrbuch 5 - 8*. Würzburg; Wien: öbv & hpt Verlagsgesellschaft, erste Auflage, 2004.

[25] ROHM, W.: *Testen von Folgen von Zufallszahlen*. Unterrichtsmaterial, HTBL Saalfelden, Arbeitsgruppe Moderner MathematikUnterricht, März 2007. http://www.ammu.at/archiv/4/4_4.htm.

[26] WIESENBAUER, J.: *Number Theory with Derive - Some Suggestions for Classroom Teaching*. Technische Universität Wien.

[27] WIESENBAUER, J.: *Primality Testing and Factoring Large Numbers with Derive*. Technische Universität Wien, 2002.

[28] WIESENBAUER, J.: *Public Key Kryptosysteme in Theorie und Programmierung*. Technische Universität Wien.

[29] WIESENBAUER, J.: *Zahlentheorie und Anwendungen*. Unterlagen zur Vorlesung "AKDIS Zahlentheorie und Anwendungen", Technische Universität Wien, Institut für Diskrete Mathematik und Geometrie, SS 2007. http://www.algebra.tuwien.ac.at/institut/zthanw/index.html.

[30] WINKLER, R.: *Kongruenzen*. Unterrichtsmaterial, Humboldt Universität Berlin, Institut für Mathematik, März 2007. http://www.mathematik.hu-berlin.de/~winkler/msg/msgKo2.pdf.

[31] WOBST, R.: *Abenteuer Kryptologie : Methoden, Risiken und Nutzen der Datenverschlüsselung*. Bonn: Addison-Wesley, zweite Auflage, 1998.

[32] ZIMMERMANN, P.: *An Introduction to Cryptography*. Kurzeinführung, PGP Corporation, New Jersey, Jänner 2007. http://www.pgpi.org/doc/pgpintro/.