Zahlentheorie und Kryptologie

für Einsteiger von
Gerhard Schallenkamp

6.12.2016

Inhalt Seite

Hinweis: Eilige können die Lektüre mit dem 2. Kapitel beginnen.

1. Extremalprinzip und Primfaktorzerlegung

Für die Zahlentheorie sind die folgenden Erkenntnisse fundamental.
Eine nach oben beschränkte Teilmenge der natürlichen Zahlen ist endlich. Endlich heißt eine Menge, wenn die Anzahl ihrer Elemente endlich ist. Folglich: Eine nach oben und unten beschränkte Teilmenge der ganzen Zahlen ist endlich.
Auf sie ist das Extremalprinzip anwendbar:

> Satz 1.1. Eine nichtleere endliche Menge von reellen Zahlen hat ein kleinstes und größtes Element.

Der Satz ist trivial für Mengen, die genau eine Zahl enthalten, weil dann diese Zahl zugleich größtes und kleinstes Element. Das Extremalprinzip folgt daraus mittels vollständiger Induktion. Dazu genügt es zu zeigen: Gilt eine Eigenschaft (ein Satz) für eine Anfangszahl k und bleibt sie beim Schritt von n nach n+1 erhalten, dann gilt sie für alle Zahlen $n \geq k$. Für $k = 1$ gilt das Extremalprinzip. Was folgt also für n+1, wenn es für die Zahl n richtig ist?
M_n bezeichne eine Menge mit n Elementen, M_{n+1} eine mit n+1 Elementen.
Die Menge M_{n+1} mit n+1 Elementen zerlegen wir beliebig in eine Menge M_n von n Elementen und eine Menge M_1 mit einem Element, das wir mit e_1 bezeichnen. M_n hat nach Voraussetzung ein kleinstes Element k_n. Ist $k_n \leq e_1$ ist k_n ein kleinstes Element von M_{n+1}, andernfalls ist es e_1; eine dritte Möglichkeit gibt es nicht. Analog folgt, dass M_{n+1} ein größtes Element hat. Das bedeutet: Die durch das Extremalprinzip beschriebene Eigenschaft der Menge M_n „vererbt" sich auf die größere Menge M_{n+1}.
Allgemeiner formuliert: Die Regel für die Zahl n „vererbt" die Eigenschaft der Wahrheit auf die Regel für die Zahl n+1.
Anmerkung: Dieser Satz gilt nicht für Mengen von unendlich vielen Zahlen. Die Menge der natürlichen Zahlen hat ja kein größtes Element. Aber aus dem Extremalprinzip folgt:

Satz 1.2a. Jede nichtleere, nach unten beschränkte Teilmenge der ganzen Zahlen hat ein kleinstes Element.

Analog:

Satz 1.2b. Jede nichtleere, nach oben beschränkte Teilmenge der ganzen Zahlen hat ein größtes Element.

Begründung für Satz 2a: Die Zahlen größer als ein Element der Teilmenge sind für die Eigenschaft irrelevant und die übrige Zahlenmenge ist endlich.

Folgerung aus Satz 2a: Jede nichtleere Teilmenge der natürlichen Zahlen hat ein kleinstes Element.

Die Eindeutigkeit der Primfaktorzerlegung

Eine Primzahl ist eine natürliche Zahl > 1, die sich nur durch sich selbst und 1 (ganzzahlig ohne Rest) teilen lässt, also 2, 3, 5, 7, 11, 13, 17, 19, 23 etc. sind Primzahlen. Alle anderen natürlichen Zahlen lassen sich in Produkte von Primzahlen zerlegen: $18 = 2 \cdot 3 \cdot 3$ oder $60 = 2 \cdot 2 \cdot 3 \cdot 5$. Primzahlen können in der Faktorzerlegung mehrfach auftreten, man spricht von Potenzen.

Wegen des Kommutativgesetzes spielt die Reihenfolge der Primzahlen keine Rolle, d.h. es ist $7 \cdot 11 \cdot 13 = 7 \cdot 13 \cdot 11 = 11 \cdot 7 \cdot 13 = 13 \cdot 11 \cdot 7 = 1001$.

Woher wissen wir, dass $7 \cdot 11 \cdot 13 \neq 3^3 \cdot 37$ ist oder allgemein ein unterschiedliches Produkt von Primfaktoren immer zu einem unterschiedlichen Resultat führt?

Als Erster erkannte Carl Friedrich Gauß (1777 – 1855) hier ein Beweisproblem und bewies den *Fundamentalsatz der elementaren Zahlentheorie*:

Satz 1.3. Jede natürliche Zahl größer als 1 besitzt eine Zerlegung in Primfaktoren, die bis auf die Reihenfolge eindeutig ist.

Für Primzahlen ist der Satz trivial, da eine Primzahl per Definition nur einen einzigen Primfaktor hat, nämlich sich selbst; eine Multiplikation entfällt.

Der Beweis für die anderen Zahlen ist hier indirekt, d.h. er nimmt das Gegenteil an und widerlegt es, indem er zeigt, dass daraus ein logischer Widerspruch folgt. Er benutzt eine Idee des Mathematikers Ernst Zermelo (1871 – 1953), die auf dem Extremalprinzip basiert: Eine *endliche* nichtleere Menge von reellen Zahlen hat ein kleinstes und größtes Element. (Endlich heißt: die Anzahl der Elemente ist endlich.) Daraus folgt: Jede nichtleere Teilmenge der natürlichen Zahlen hat ein kleinstes Element, weil die Zahlen größer als ein Element der Teilmenge für die Eigenschaft irrelevant sind und die übrige Zahlenmenge endlich ist.

1) Beweis der Existenz:
Das Gegenteil sei angenommen: Gibt es eine natürliche Zahl ohne Primfaktorzerlegung, dann gibt es eine kleinste Zahl mit dieser Eigenschaft, kurz n genannt. Da n keine Primzahl ist, hat n einen Teiler a zwischen 1 und n (d.h. $1 < a < n$), so dass wir $n = a \cdot b$ mit natürlichen Zahlen schreiben können. Weil a und b kleiner als n sind, gibt es für a und b eine Primfaktorzerlegung, also auch für das Produkt $n = a \cdot b$, also Widerspruch zur Annahme! Also gibt es keine Zahl ohne Zerlegung in Primfaktoren.

2) Beweis der Eindeutigkeit:
Wieder Annahme des Gegenteils: Sei nun n die kleinste natürliche Zahl mit zwei wesentlich verschiedenen Primfaktorzerlegungen. Sei q der kleinste Teiler von n, so dass wir $n = q \cdot Q$ schreiben können mit natürlicher Zahl Q. Da Q eine Primfaktorzerlegung hat, gibt es eine Primfaktorzerlegung für n, die die Primzahl q enthält.

Nun sei p die kleinste Primzahl der zweiten, verschiedenen Primfaktorzerlegung, so dass wir notieren können:

(1) $\quad n = q \cdot Q = p \cdot P$

Nun muss $q \neq p$ sein, sonst haben wir für die kleinere Zahl $Q = P$ ebenfalls eine mehrfache Primfaktorzerlegung und n wäre nicht die kleinste Zahl mit dieser Eigenschaft. Folglich ist $p > q$.

Die Subtraktion des Produktes $q \cdot P$ auf jeder Seite der Gleichungen (1) ergibt:

(2) $\quad k = n - q \cdot P = q \cdot (Q - P) = (p - q) \cdot P$

Das führt zum logischen Widerspruch. Wegen $p > q$ und $P \geq 2$ gilt $2 \leq k < n$. Weil k und P eindeutige Primfaktorzerlegungen haben, müssen beide Produkte in (2) zur gleichen Zerlegung führen. Wegen $k = q \cdot (Q - P)$ hat k hat den Primteiler q. Wo aber steckt der Primteiler q im Produkt $(p - q) \cdot P$? Alle Primfaktoren von P sind nicht kleiner als p, also größer als q. Da er nicht in der Zahl P stecken kann, muss $(p - q)$ durch q teilbar sein, d.h. $p - q = q \cdot r$. Daraus folgt $p = q \cdot r + q = q \cdot (r + 1)$, d.h. p ist keine Primzahl, d.h. Widerspruch!

2. Der größte gemeinsame Teiler (ggT)

Das Folgende handelt nur von der Menge **Z** der ganzen Zahlen.

Die Vielfachen einer gegebenen Zahl $b \neq 0$ bilden eine Menge $B = \{z \mid z = q \cdot b, q \in \mathbf{Z}\}$, die sich über den gesamten Zahlenstrahl ins Unendliche ausdehnt. Da der Abstand zweier benachbarter Zahlen von B gleich $|b|$ ist, ist der kleinste Abstand einer beliebigen Zahl a zu den Zahlen von B kleiner als $|b|$. Aus diesen elementaren Überlegungen folgt:

Satz 2.1. Division mit Rest. Seien a und b ganze Zahlen und $b \neq 0$, dann gibt es eindeutige ganze Zahlen q und r mit $0 \leq r < |b|$, so dass gilt:

$$a = q \cdot b + r$$

Die Berechnung von q und r heißt ganzzahlige Division a durch b mit Rest und $r = a \bmod b$ (sprich a modulo b) bezeichnet den Funktionswert von $f:(a,b) \rightarrow r$.

Zu gegebenen Zahlen a und b definieren wir die Zahlenmenge L(a,b), die entsteht, wenn zu a und b beliebig oft die Werte a und b addiert oder subtrahiert werden:

$$L(a,b) = \{z \mid z = a \cdot x + b \cdot y,\ x, y \in \mathbf{Z}\}$$

In dieser Menge können wir beliebig addieren, subtrahieren und mit ganzen Zahlen multiplizieren. Denn für beliebige $z_1, z_2 \in L(a,b)$ gilt:

$z_3 = z_1 - z_2 = (a \cdot x_1 + b \cdot y_1) - (a \cdot x_2 + b \cdot y_2) = a \cdot (x_1 - x_2) + b \cdot (y_1 - y_2) \in L(a,b)$.

Für beliebige $c, d \in L(a,b)$ ist auch der Rest der ganzzahligen Division c/d in L(a,b) enthalten, und zwar wegen $r = c - q \cdot d$. Hilfreich ist der Satz:

Die kleinste positive Zahl k von L(a,b) ist ein Teiler von a und auch von b.

Beweis: Wegen $a = q \cdot k + r$ (d. h. $r = a - q \cdot k$) gehört der nicht negative Rest $r < k$ ebenfalls zu L(a,b) und muss Null sein, weil sonst k nicht die kleinste positive Zahl wäre. Damit ist $a = q \cdot k$ und analog folgt $b = p \cdot k$. Daraus folgt:

$$L(a,b) = \{z \mid z = x \cdot ggT(a,b),\ x \in \mathbf{Z}\}$$

Da alle gemeinsamen Teiler von a und b die Zahl $k = a \cdot x + b \cdot y$ teilen, ist k zugleich der größte gemeinsame Teiler (= ggT) von a und b. Er wird gern durch fortgesetzte Division mit Rest berechnet, d.h. mit dem euklidischen Algorithmus: Sei $a > b > 0$, $r_0 = a$ und $r_1 = b$. q_k und r_k werden mit Satz 3.1 rekursiv berechnet:

$$\begin{aligned} r_2 &= r_0 - q_1 \cdot r_1 = r_0 \bmod r_1, \\ r_3 &= r_1 - q_2 \cdot r_2 = r_1 \bmod r_2, \\ r_4 &= r_2 - q_3 \cdot r_3 = r_2 \bmod r_3, \ldots \\ &\ldots \end{aligned}$$

(eA) $\quad r_{k+1} = r_{k-1} - q_k \cdot r_k, = r_{k-1} \bmod r_k \ldots$

Wegen $r_1 > r_2 > r_3 > \ldots > 0$ endet er, und zwar mit dem letzten Rest > 0, dem $ggT(a,b) = ggT(r_{k-1}, r_k) = d$, weil sowohl der ggT die Zahl d teilt als auch d den ggT. Alle Reste r_k gehören zu L(a,b).
$ggT(a,b) = \max \{z \in \mathbf{Z} \mid z \text{ teilt a und b}\} = \min \{z \in \mathbf{N} \mid z > 0, z \in L(a,b)\}$.

Daraus folgt $L(a,b) = \{z \mid z = x \cdot ggT(a,b),\ x \in \mathbf{Z}\}$ und das Lemma von Bézout:

Satz 2.2. Die Gleichung $a \cdot x + b \cdot y = ggT(a,b)$ ist ganzzahlig lösbar;
mit der Lösung $(x_0; y_0)$ sind alle $(x_0 + k \cdot b\ ;\ y_0 - k \cdot a)$ Lösungen $(k \in \mathbf{Z})$.

Die zweite Zeile folgt aus $a \cdot (x_0 + k \cdot b) + b \cdot (y_0 - k \cdot a) = a \cdot x_0 + b \cdot y_0$.

Anmerkungen: Eine Gleichung in ganzen Zahlen heißt diophantisch.

Die Zahlen a und b heißen (zueinander) teilerfremd, wenn ggT(a,b) = 1.

Erweiterter Euklidischer Algorithmus

ggT-Aufgabe: Löse die Gleichung $a\cdot x + b\cdot y = d = ggT(a,b)$ in ganzen Zahlen.

Lösung:

Ersetze im euklidischen Algorithmus (eA) $r_{k+1} = r_{k-1} - q_k\cdot r_k$ alle Folgenglieder r_k durch $a\cdot x_k + b\cdot y_k$, d. h. durch Vielfache von a und b, bis $r_{k+1} = ggT(a,b)$.

Beginne mit $r_0 = a = a\cdot x_0 + b\cdot y_0$, d. h. $x_0 = 1$ und $y_0 = 0$,
$r_1 = b = a\cdot x_1 + b\cdot y_1$, d. h. $x_1 = 0$ und $y_1 = 1$,
und $r_2 = a - q_1\cdot b = a\cdot x_2 + b\cdot y_2$, d. h. $x_2 = 1$ und $y_2 = - q_1$.
Dann folgt $r_3 = r_1 - q_2\cdot r_2$

$$= a\cdot x_1 + b\cdot y_1 - q_2\cdot(a\cdot x_2 + b\cdot y_2)$$
$$= a\cdot(x_1 - q_2\cdot x_2) + b\cdot(y_1 - q_2\cdot y_2)$$
$$= a\cdot x_3 + b\cdot y_3.$$

$x_3 = x_1 - q_2\cdot x_2$ und $y_3 = y_1 - q_2\cdot y_2$.

Der erweiterte euklidische Algorithmus liefert mittels
$r_{k+1} = r_{k-1} - q_k\cdot r_k$ (berechne und merke q_k und r_{k+1}),
$x_{k+1} = x_{k-1} - q_k\cdot x_k$ und
$y_{k+1} = y_{k-1} - q_k\cdot y_k$ die Gleichungen
$r_k = a\cdot x_k + b\cdot y_k$, bis $r_k = ggT(a,b)$ erreicht ist.

Beispiel. Löse die Gleichung $17\cdot x + 15\cdot y = z = 1$ in ganzen Zahlen.
Startwerte z = 15, 17 und 2 = 17-15. Ziel: z = 1.

Lösungsweg	a·x + b·y	= z	Gleichungs-Tupel (x;y;z)
(G1)	17·1 + 15·0	= 17	(1;0;17)
(G2)	17·0 + 15·1	= 15	(0;1;15)
(G3) = (G1)-(G2)	17·1 – 15·1	= 2	(1;-1;2)
(G4)=(G2)-7·(G3)	17·(-7) + 15·8	= 1	(-7;8;1) = Lösungsvektor

Weitere Lösungen ergeben sich aus der Gleichung $17\cdot x + 15\cdot y = 0$ mit dem Lösungsvektor (-15;17;0) und deren Vielfache $(-15\cdot t;17\cdot t;0)$ ($t \in \mathbf{Z}$), die vektoriell auf den Lösungsvektor (-7;8;1) addiert werden können.
Lösungen sind also $x = -7 - 15\cdot t$ und $y = 8 + 17\cdot t$ ($t = 0, \pm1, \pm2, \ldots$).

Computer realisieren solche Rekursionen durch Kreisläufe (Schleifen). Startend mit den Anfangswerten $a > b > 0$, rechnen sie in diesem Fall mit Speichern ganzzahligen Inhalts: R1, R2, R3 für die Reste, die gleich $a\cdot x + b\cdot y$ sind, Q1 für den Quotienten, X1, X2, X3 für die Faktoren von a, Y1, Y2, Y3 für die Faktoren von b. Die Speicher werden immer wieder neu berechnet. Beispiel Programmiersprache COBOL.

```
     MOVE   a  TO  R1, MOVE  b  TO  R2.
     MOVE   1  TO  X1, Y2.
     MOVE   0  TO  X2, Y1.
LOOP-BEGIN.
     DIVIDE R1 BY R2 GIVING Q1 REMAINDER R3.
* Kommentar: Jetzt ist Q1 = R1/R2 und Rest  R3 = R1 – R2*Q1
     IF  R3 = 0     THEN GO TO END-ALGORITHMUS.
     COMPUTE  X3 = X1 - X2*Q1.
     COMPUTE  Y3 = Y1 - Y2*Q1.
     MOVE  R2  TO  R1, MOVE  R3  TO  R2.
     MOVE  X2  TO  X1, MOVE  X3  TO  X2.
     MOVE  Y2  TO  Y1, MOVE  Y3  TO  Y2.
     GO TO LOOP-BEGIN.
END-ALGORITHMUS.
*  Es folgt die Auswertung R2 = ggT(a,b), (X2,Y2) = Lösung der Gleichung
```

3. Die Kongruenzmethode und Modularrechnung

Seit C. F. Gauß heißen zwei Zahlen a und b „kongruent nach dem Modul m“, wenn sie bei der Division durch eine natürliche Zahl m > 0, die man in dieser Funktion Modul nennt, denselben Rest r ($0 \le r < m$) lassen, und schreibt:

$$a \equiv b \ (\text{môd } m)$$ (sprich: a ist kongruent b modulo m)

Aufgrund des Satzes über die Division mit Rest ist ja der Rest immer eindeutig. Die Kongruenz zweier Zahlen bedeutet „Restgleichheit“ und gilt immer nur für einen bestimmten Modul (Divisor). a ist kongruent b modulo m, wenn m Teiler der Differenz a – b ist:

Definition 3.1. $a \equiv b \ (\text{môd } m) \ \Leftrightarrow \ a - b = q \cdot m \quad (q \in \mathbf{Z})$

Die Kongruenz ist eine *Äquivalenzrelation*, d.h. es gelten

- Reflexivität: $a \equiv a \ (\text{môd } m)$,
- Symmetrie: $a \equiv b \ (\text{môd } m) \ \Leftrightarrow \ b \equiv a \ (\text{môd } m)$ und
- Transitivität: $a \equiv b \ (\text{môd } m)$ und $b \equiv c \ (\text{môd } m) \ \Rightarrow \ a \equiv c \ (\text{môd } m)$.

In der Literatur bezeichnet mod m oft keine Relation, sondern eine Funktion, die jeder ganzen Zahl ihren Rest bei der Division durch m zuordnet:

Definition 3.2. $a \bmod m = r_{/m}(a) = r$, wobei $m > r \ge 0$, $r = a - q \cdot m$, $q \in \mathbf{Z}\}$.

Beide Definitionen sind gleichwertig:

Satz 3.1. $a \bmod m = b \bmod m \ \Leftrightarrow a \equiv b \ (\text{môd } m) \ \Leftrightarrow \ a - b = q \cdot m \quad (q \in \mathbf{Z})$ $\Rightarrow ggT(a,m) = ggT(b,m)$

„$\Rightarrow$“ gilt, weil ein gemeinsamer Teiler von a und m wegen $b = a - q \cdot m$ auch b teilt.

Wichtig ist nun, dass die Addition, Subtraktion und Multiplikation in **Z** die Kongruenz erhalten (man sagt auch, die Kongruenzrelation oder $r_{/m}$ sei mit den Operationen verträglich):

Satz 3.2. Aus $r_{/m}(a) = r_{/m}(b)$ und $r_{/m}(a') = r_{/m}(b')$ folgen: $r_{/m}(a+a') = r_{/m}(b+b')$, $r_{/m}(a - a') = r_{/m}(b - b')$, $r_{/m}(a \cdot a') = r_{/m}(b \cdot b')$

Nach Voraussetzung ist $a - b = q \cdot m$ und $a' - b' = q' \cdot m$. Beiderseitige Addition oder Subtraktion ergibt: $(a \pm a') - (b \pm b') = (q \pm q') \cdot m$.

Wir subtrahieren $0 = a \cdot b' - b' \cdot a$ von der multiplikativen Analogie:
$a \cdot a' - b \cdot b' = a \cdot a' - (a \cdot b' - b' \cdot a) - b \cdot b' = a \cdot (a' - b') + b' \cdot (a - b) = (a \cdot q' + b' \cdot q) \cdot m$,
d.h. die Differenz der Produkte ist durch m teilbar weil $(a \cdot q' + b' \cdot q) \in \mathbf{Z}$.

Aufgabe: Elementares Rechnen beweist den

Satz 3.3. $(a + b) \bmod m = ((a \bmod m) + (b \bmod m)) \bmod m$ $(a \cdot b) \bmod m = ((a \bmod m) \cdot (b \bmod m)) \bmod m$

Ob man mit ganzen Zahlen oder ihren modulo-Resten rechnet, das Ergebnis mod m ist das gleiche.

Definitionen: $\mathbf{Z}_m = \{0, 1, 2, \ldots, m-1\}$ ist die Menge der Reste im Modul m,
f(A) die Menge der Bildpunkte einer Funktion $f:A \to B$ und
|A| bzw. |f(A)| die Anzahl der Elemente der Menge A bzw. f(A), sofern endlich.
Eine Funktion $f:A \to B$ ist **injektiv**, wenn aus $x \ne y$ folgt $f(x) \ne f(y)$ bzw. aus $f(x) = f(y)$ folgt $x = y$. Man kann dann von dem Funktionswert $z = f(x)$ eindeutig auf das Argument x schließen. Anders gesagt, es gibt die Umkehrfunktion $f^{-1}:f(A) \to A$.

Was ist aber mit der Kürzungsregel? Aus $3\cdot9 \equiv 5\cdot9 \equiv 3$ (môd 6) folgt ja nicht die Kongruenz von 3 und 5 zum Modul 6. Wenn aber a und m teilerfremd sind, d. h. der größte gemeinsame Teiler ggT(a,m) = 1, gilt die Kürzungsregel und mehr:

Satz 3.4. Sei ggT(a,m) = 1 und T Teilmenge von $\mathbf{Z}_m$, $f:T\rightarrow \mathbf{Z}_m$, $x\rightarrow(a\cdot x) \bmod m$; Φ_m die Menge der zu m teilerfremden Zahlen in $\mathbf{Z}_m$; dann gilt:

(I) a hat einen modularen **Kehrwert** $\mathbf{a_m^{-1}} \in \mathbf{Z}_m$ mit $(a\cdot a_m^{-1}) \bmod m = 1$.

(II) $(a\cdot b) \bmod m = (a\cdot b') \bmod m \Leftrightarrow b \bmod m = b' \bmod m$.

(III) Die Funktion f ist injektiv, also $|f(T)| = |T|$.

(IV) $f(\Phi_m) = \Phi_m$. $f: \Phi_m \rightarrow \Phi_m$ ist eine Permutation auf Φ_m.

(V) Sei $\varphi(m) = |\Phi_m|$; dann gilt $a^{\varphi(m)} \bmod m = 1$.

Beweis (I): x_0 löse laut Satz 2.2 die Gleichung $a\cdot x + m\cdot y = 1$. Daraus folgt $(a\cdot x_0 + m\cdot y) \bmod m = (a\cdot x_0) \bmod m = 1$. Also $a_m^{-1} = x_0 \bmod m$.

Beweis (II): Die Richtung $\Leftarrow$ folgt direkt aus Satz 3.2. Für die Richtung $\Rightarrow$ folgt wegen (I) aus der Voraussetzung $(a_m^{-1}\cdot a\cdot b) \bmod m = (a_m^{-1}\cdot a\cdot b') \bmod m$ und daraus die Behauptung.

Beweis (III): Sei f(x), f(y) $\in$ f(T) und f(x) = f(y), d.h. $(a\cdot x) \bmod m = (a\cdot y) \bmod m$. Wegen (II) folgt daraus $x \bmod m = y \bmod m$ und, weil $x, y \in \mathbf{Z}_m$, x = y.

Beweis (IV): Wenn $x\in \Phi_m$, dann ist auch $f(x) = (a\cdot x) \bmod m$ teilerfremd zu m, folglich ist $f(\Phi_m)$ Teilmenge von Φ_m und wegen (III) $|f(\Phi_m)| = |\Phi_m|$.

Beweis (V): Wegen (IV) ist das Produkt aller $f(x_i) = r_{/m}(a\cdot x_i)$ mit $x_i\in \Phi_m$ gleich dem Produkt aller $x_i\in \Phi_m$, d. h. $r_{/m}(a\cdot x_1)\cdot r_{/m}(a\cdot x_2) \cdots r_{/m}(a\cdot x_{\varphi(m)}) = x_1\cdot x_2 \cdots x_{\varphi(m)}$. Folglich $(a^{\varphi(m)}\cdot x_1\cdot x_2 \cdots x_{\varphi(m)}) \bmod m = (x_1\cdot x_2 \cdots x_{\varphi(m)}) \bmod m$. Weil alle Faktoren x_i teilerfremd zu m sind, folgt durch Kürzen gemäß (II) die Behauptung (V).

Definition: Euler'sche φ-Funktion $\varphi(m) = |\Phi_m|$ = Anzahl zu m teilerfremden Reste.

Satz 3.5. Seien $p \neq q$ Primzahlen; dann ist $\varphi(p) = p-1$ und $\varphi(p\cdot q) = (p-1)\cdot(q-1)$.

Beweis: $\varphi(p) = p-1$ ist für Primzahlen klar und für $n = p\cdot q$ hat $\mathbf{Z}_n$ als nicht teilerfremde Zahlen q Vielfache von p und q Vielfache von p, d. h. $\varphi(p\cdot q) = p\cdot q - p - q + 1$. Plus 1, weil die Null zu beiden Vielfachen gehört und nicht doppelt gezählt werden darf. Daraus folgt $\varphi(p\cdot q) = p\cdot q - p - q + 1 = (p-1)\cdot(q-1)$.

Aus den Sätzen 3.4(V) und 3.5 folgt unmittelbar

Satz 3.6. Kleiner Satz von Fermat: p ist Primzahl und $a \neq k\cdot p \Rightarrow a^{p-1} \bmod p = 1$.
Satz 3.6a. p ist Primzahl, $n \geq 0$ und a, $n\in \mathbf{Z} \Rightarrow a^{1+n(p-1)} \bmod p = a \bmod p$.

Denn aus Satz 3.6 folgt Satz 3.6a, der auch für $a = k\cdot p$, d. h. für $a \bmod p = 0$ gilt.

Satz 3.7. Chinesischer Restsatz. Sind a und b teilerfremd und $m = a\cdot b$, dann sind die Gleichungen $r = x \bmod a$ und $s = x \bmod b$ eindeutig für $x\in \mathbf{Z}_m$ lösbar. Die Abbildung $c_r: \mathbf{Z}_m \leftrightarrow \mathbf{Z}_a \times \mathbf{Z}_b$, $x\leftrightarrow(r;s)$ ist umkehrbar eindeutig (= bijektiv).

Beweis: Wegen ggT(a,b) = 1 gibt es Kehrwerte b_a^{-1} und a_b^{-1} laut Satz 3.4(I). Damit erfüllt $x = r\cdot b_a^{-1}\cdot b + s\cdot a_b^{-1}\cdot a$ die geforderten modulo-Gleichungen. Erfüllt auch $y\in \mathbf{Z}_m$ die Gleichungen, dann ist $(y - x) \bmod a = (y - x) \bmod b = 0$, d. h. durch $(a\cdot b)$ teilbar. Daraus folgt x = y.

Rechts für a = 5 und b = 7 die Zahlen 0 bis $34 < m = a\cdot b$. Je Zeile r die Zahlen r (mod 5), je Spalte s die Zahlen s (mod 7). Jede Zahl von 0 bis 34 erscheint genau einmal.
Beispiel: $(4;1) = c_r(29)$.

	0	1	2	3	4	5	6
0	0	15	30	10	25	5	20
1	21	1	16	31	11	26	6
2	7	22	2	17	32	12	27
3	28	8	23	3	18	33	13
4	14	29	9	24	4	19	34

Satz 3.7 ist erweiterbar auf mehrere paarweise teilerfremde Zahlen.

Satz 3.8. Chinesischer Restsatz. Sind a_i paarweise teilerfremd $1 \le i \le n$, dann sind die Gleichungen $r_i = x \bmod a_i$ eindeutig in $0 \le x < a_1 \cdot a_2 \cdot a_3 \ldots \cdot a_n$ lösbar.

Der Beweis geht rekursiv: Man löst die Aufgabe für zwei a_i und dann für deren Produkt und ein drittes a_i usw.

Die in Satz 3.7 definierte Bijektion c_r ist verträglich mit dem modularen Rechnen in den verwendeten Mengen $\mathbf{Z}_k$. Statt in $\mathbf{Z}_m$ kann man in $\mathbf{Z}_a$ und $\mathbf{Z}_b$ rechnen und umgekehrt. Der Beweis benötigt dafür den elementaren

Hilfssatz. Sei $k > 0$. $(x \bmod (k \cdot m)) \bmod m = x \bmod m$.

Satz 3.9. Die Bijektion c_r sei wie in Satz 3.7 definiert: $c_r(x) = [r;s]$, $c_r(y) = [t;u]$ und $m = a \cdot b$ (a und b teilerfremd). Dann gelten:
$c_r((x \pm y) \bmod m) = [(r \pm t) \bmod a; (s \pm u) \bmod b]$
und $c_r((x \cdot y) \bmod m) = [(r \cdot t) \bmod a; (s \cdot u) \bmod b]$.

Beweis: Man bilde wie im Beweis von Satz 3.7 mit
$x = r \cdot b_a^{-1} \cdot b + s \cdot a_b^{-1} \cdot a$
und $y = t \cdot b_a^{-1} \cdot b + u \cdot a_b^{-1} \cdot a$
die Summe oder Differenz $x \pm y$ bzw. das Produkt $x \cdot y$. Das Produkt ergibt
$((x \cdot y) \bmod m) \bmod a = (x \cdot y) \bmod a = (r \cdot t) \bmod a$ und
$((x \cdot y) \bmod m) \bmod b = (x \cdot y) \bmod b = (s \cdot u) \bmod b$. Der Beweis des letzten Satzes gelingt mit dem Hilfssatz und $m = k \cdot a$ bzw. $m = k \cdot b$.

Über modulare Quadratwurzeln

Im Folgenden bezeichnen p und q Primzahlen > 2.

Satz 3.10. Sei $0 < a < p$, $p > 2$. $x^2 \bmod p = a$ hat keine oder genau 2 Lösungen.

Beweis: Aus $x^2 \bmod p = y^2 \bmod p$ folgt $0 = (x^2 - y^2) \bmod p = (x-y) \cdot (x+y) \bmod p$, d. h. $x-y$ ist durch p teilbar oder $x+y$. Ersteres bedeutet $x = y$ und letzteres $x+y = p$, d. h. $y = p - x \neq x$. Folgerung:

Satz 3.10a. Sei $0 < a < p$, $p > 2$, $u = (p-1)/2$. Dann ist $a^u \bmod p$ gleich 1 oder $p-1$.

Beweis: Nach Satz 3.6 ist $a^{p-1} \bmod p = 1$. Der Rest folgt aus Satz 3.10.

Satz 3.11. Sei $0 <$ a Quadratzahl modulo p und $u = (p+1)/4 \in \mathbf{Z}$.
Dann ist a^u eine Lösung der Gleichung $x^2 \bmod p = a$.

Beweis: Sei $w \neq 0$ eine Wurzel von a, d. h. $w^2 \bmod p = a$. Dann gilt
$(a^u)^2 \bmod p = w^{4 \cdot u} \bmod p = w^{p+1} \bmod p = w^{p-1} \cdot w^2 \bmod p = a$ (wegen Satz 3.6).
Folglich: a^u ist Quadratwurzel von a im Modul p. Anmerkung: $u \in \mathbf{Z} \Leftrightarrow p \bmod 4 = 3$.

Satz 3.12. Seien p, q Primzahlen >2, $n = p \cdot q$. $x^2 \bmod n = a$ hat höchstens vier Lösungen.

Beweis: Aus $c_r(x) = (r,s)$ folgt nach Satz 3.9 $c_r(x^2 \bmod n) = (r^2 \bmod p; s^2 \bmod q)$. Maximal je 2 Lösungen für $r^2 \bmod p$ und $s^2 \bmod q$ (laut Satz 3.10) kombiniert ergeben maximal vier Tupel für (r;s) und damit laut Satz 3.7 maximal vier Lösungen für $x^2 \bmod n$.

4. Anwendungen in der Kryptologie

Die Kryptologie untersucht, wie ein Sender A (Alice) öffentlich eine verschlüsselte Nachricht (Text m) an einen Empfänger B (Bob)schickt. Die Öffentlichkeit soll den Text m nicht entschlüsseln können. Die Kommunikation zwischen Alice und Bob benötigt ein Protokoll.

Definition: Ein (Kommunikations-)Protokoll legt für beide Partner die Reihenfolge der Nachrichten fest, die sie austauschen (senden bzw. empfangen).

Die Texte liegen in digitaler Form vor, als Folge von Bits, zusammengefasst zu einer Folge binärer Zahlen. Ein zufällig gewählter binärer Schlüssel kann einen Text verschlüsseln und ebenso wieder entschlüsseln, muss aber zuerst zwischen Alice und Bob ausgetauscht werden. Verschlüsselungsfunktionen $f_k(w) = c$ müssen injektiv sein, damit die Entschlüsselung $f_k^{-1}(c) = w$ gelingt. Nur in Ausnahmefällen sind wenige Umkehrlösungen zu vergleichen.

Die Zahlentheorie bietet nützliche Einwegfunktionen, auch Falltürfunktionen genannt.

Definition: Eine Einwegfunktion ist eine effizient berechenbare Funktion f, deren Umkehrung f^{-1} nicht effizient berechenbar ist, also höchst aufwändig ist.

Der heute bekannte Rechenaufwand wächst schneller als jede Potenz n^k mit der Größe n der gewählten Zahlen, dessen Notwendigkeit aber nicht bewiesen ist.

Beispiel 4.1: Exponentialfunktion oder Problem des diskreten Logarithmus
Sei p Primzahl. $y = f(x) = b^x \bmod p$
Modulare Potenzen sind schnell berechenbar. Es ist sehr aufwändig, aus dem y-Wert den x-Wert bei gegebenem b und p zu berechnen. Da f nicht injektiv ist, sind mehrere x-Werte möglich.

Beispiel 4.2.: Faktorisierung und Wurzeln. Seien p, q Primzahlen und $n = p \cdot q$. Es ist sehr aufwändig, die Zahl n zu faktorisieren, also p und q zu berechnen.
$n = f(p,q) = p \cdot q$. $f:(p,q) \rightarrow n$ (Problem der Faktorisierung),
$y = f(x) = x^2 \bmod n \qquad (x^2 > n)$,
$y = f(x) = x^e \bmod n$.

Die folgenden Protokolle setzen die Unumkehrbarkeit von Einwegfunktionen voraus.

Protokoll 1: Diffie-Hellman-Schlüsselaustausch
Vereinbarung über Primzahl p und Zahl g ist öffentlich.

Alice (wählt a zufällig)		Bob (wählt b zufällig)
sendet $g^a \bmod p = \alpha$	$\rightarrow \alpha$	
berechnet	$\beta \leftarrow$	sendet $\beta = g^b \bmod p$
$k = \beta^a \bmod p = g^{a \cdot b} \bmod p$		berechnet $k = \alpha^b \bmod p = g^{a \cdot b} \bmod p$.

Erläuterung: Die Exponentialfunktion g^x fungiert als Einwegfunktion, a und b bleiben geheim. Am Ende verfügen beide über den gleichen geheimen Schlüssel k.

Protokoll 2: El-Gamal-Verschlüsselung
Vereinbarung über Primzahl p und Zahl g ist öffentlich. Text w wird verschlüsselt.

Alice (wählt a zufällig)		Bob (wählt b zufällig, $\beta = g^b \bmod p$)
berechnet den Schlüssel $k = \beta^a \bmod p$	$\beta \leftarrow$	β
verschlüsselt w:	$f_k(w) = c \rightarrow c$	
schickt auch:	$g^a \bmod p = \alpha \rightarrow \alpha$	berechnet $k = \alpha^b \bmod p = g^{a \cdot b} \bmod p$, entschlüsselt $w = f_k^{-1}(c)$.

Hauptakteur der Protokolle 3 und 4 ist der Empfänger, der Sender benutzt nur das vom Empfänger veröffentlichte Verschlüsselungsverfahren. Mit einem geheimen Trick kann der Empfänger die Einwegfunktion effizient umkehren. RSA ist das Kürzel der Namen seiner Autoren Ronald Rivest, Adi Shamir und Leonard Adleman.

Protokoll 3: Public-Key-Kryptosystem RSA

Alice	Bob
kennt n und e.	wählt $n = p \cdot q$ und $(d \cdot e) \bmod \varphi(n) = 1$,
Digitaler Klartext ist $w < n$.	p und q sind Primzahlen.
.	B. veröffentlicht nur n und e.
A. verschlüsselt: $w^e \bmod n = c$ $\rightarrow c$	
	B. entschlüsselt: $w = c^d \bmod n$.

Erläuterung: Bedingung ist, dass p, q, d und w dank Einwegfunktion geheim bleiben. $\varphi(n) = (p-1)\cdot(q-1)$ ist die Euler'sche φ-Funktion. Warum ist $w^{e\cdot d} \bmod n = w$?
Wegen $(e\cdot d) \bmod \varphi(n) = 1$ ist $e\cdot d = 1 + k\cdot(p-1)\cdot(q-1)$ und es gilt nach Satz 3.6a

$$w^{e\cdot d} \bmod p = w^{1+k\cdot\varphi(n)} \bmod p = w \bmod p.$$

Analoges gilt für w mod q. Die Bijektion c_r von Satz 3.7 vollendet den Beweis:

$$w^{e\cdot d} \bmod n = c_r^{-1}(w^{e\cdot d} \bmod p; w^{e\cdot d} \bmod q) = c_r^{-1}(w \bmod p; w \bmod q) = w.$$

(Das Argument von Satz 3.4(V) ist nur für den Fall ggT(w,n) = 1 gültig.)
Wenn der zu übertragende Text w größer als n ist, wird er in passende Textblöcke zerlegt und die verschlüsselten Blöcke werden nacheinander gesendet.

Das Kryptosystem RABIN stammt vom Informatiker Michael O. Rabin.

Protokoll 4: Public-Key-Kryptosystem RABIN

Alice	Bob
kennt n.	wählt $n = p\cdot q$, p, q Primzahlen und
Digitaler Klartext ist w.	$p \bmod 4 = q \bmod 4 = 3$
$\sqrt{n} < w < n$	B. veröffentlicht nur n,
A. verschlüsselt: $w^2 \bmod n = c$ $\rightarrow c$	rechnet $u = (p+1)/4$, $v = (q+1)/4$,
	rechnet weiter: $w_p = c^u \bmod p$
	$w_q = c^v \bmod q$.
	Die vier Kombinationen $(\pm w_p; \pm w_q)$ ergeben nach dem chines. Restsatz 3.7 vier Lösungen x mod n. Nur eine ist korrekt.

Erläuterung: w_p und w_q werden laut Satz 3.11 berechnet. Da Satz 3.11 nur je eine Lösung liefert, sind die Lösungen $p - w_p$ und $q - w_q$ zu ergänzen. Satz 3.12 verbindet sie zur Lösung mod n. Die Umrechnung in die Formen x mod n erfolgt über die Gleichungen im Beweis von Satz 3.7 und 3.9. Die dabei benutzten modularen Kehrwerte hängen nur von p und q ab, sind also für mehrere w-Texte verwendbar. Nur eine sinnvolle Lösung ergibt wieder den ursprünglichen Text w.

Ein Problem gibt es, wenn derselbe Text w nochmals mit einer zu n teilerfremden Zahl m verschlüsselt wird. Dann ist $w^2 \bmod (m\cdot n)$ mit dem chinesischen Restsatz berechenbar und damit die Wurzel wegen $w^2 < m\cdot n$.

5. Anhang – Der kleine Satz von Fermat

Das Folgende handelt nur von nicht negativen ganzen Zahlen und benötigt den binomischen Lehrsatz, der hier vorausgesetzt wird:

$(a + b)^n = \sum_{k=0}^{n} \binom{n}{k} \cdot a^{n-k} \cdot b^k$ mit den Binomialkoeffizienten $\binom{n}{k} = \frac{n!}{k!(n-k)!}$

Beachte: 0! = 1 und k! = (k-1)!·k für k>0. Binomialkoeffizienten sind natürliche Zahlen.

Hilfssatz. Wenn $0 < k < n$ und n eine Primzahl ist, ist $\binom{n}{k}$ durch n teilbar.

Beweis: Bei der Primfaktorzerlegung erscheint der Primfaktor n nur im Zähler.

Satz 5.1. Wenn p Primzahl ist, ist p ein Teiler von $(n^p – n)$.

Beweis mittels vollständiger Induktion. Der Satz ist richtig für n = 0. Die Frage ist: Wenn er für $n^p – n$ gilt, ist er dann auch für

(T1) $(n+1)^p – (n+1)$

richtig? Der binomischen Lehrsatz wird auf $(n+1)^p$ angewandt und laut Hilfssatz sind alle Koeffizienten $\binom{p}{k}$ außer die vor n^p und 1 durch p teilbar. Daher folgt

(T2) $(n+1)^p = n^p + 1 + p \cdot x$

mit ganzer Zahl x. Die rechte Seite von (T2) in (T1) eingesetzt, ergibt:

(T3) $n^p - n + p\,x = (n+1)^p – (n+1)$ (x ganzzahlig)

Aus der Voraussetzung: p ist Teiler von $n^p – n$, folgt somit: p teilt (T1).

Warum folgt aus Satz 5.1 der kleine Satz von Fermat (Satz 3.6)? Weil p kein Teiler von n ist, teilt p in der Faktorisierung $n^p – n = n \cdot (n^{p-1} – 1)$ den rechten Faktor.

Kombinatorischer Beweis von Satz 5.1:
Wie viele unterscheidbare Schnüre aus genau p Perlen mit n verschiedenen Farben sind möglich? In der Kombinatorik ist das eine Variation mit Wiederholung, und die Anzahl ist n^p, weil je Perle n Farben möglich sind. Die Anzahl der einfarbigen Schnüre ist n, die Anzahl der Farben. Die Anzahl der mehrfarbigen Perlenschnüre ist daher $n^p – n$.
Eine zyklische Permutationen (kurz **Zyklip** genannt) entsteht, wenn jede Perle einen Platz weiterrückt und die Perle auf Platz p-1 auf Platz 0. Wenn die Perlen auf einem Kreis angeordnet sind, entspricht das einer Drehung von einem Platz zum nächsten. Zur Unterscheidung der Zyklips gibt es Platznummern 0 bis p-1. Wir fragen nun: Sind alle Zyklips unterschiedliche Variationen? Darauf antwortet der

Hilfssatz. Ist p Primzahl, sind alle p Zyklips von mehrfarbigen Ketten von p Perlen auf den Plätzen 0 bis p-1 unterscheidbar.

Um das Problem zu verdeutlichen, betrachten wir die Zyklips zweier schwarzweißer Ketten der Länge 6:

Anzahl Zyklips	0	1	2	3	4	5
Kette 1	○○○●●○	→ ○○○○●●	→ ●○○○○●	→ ●●○○○○	→ ○●●○○○	→ ○○●●○○
Kette 2	●●○●●○	→ ○●●○●●	→ ●○●●○●	→ ●●○●●○	→ ○●●○●●	→ ●○●●○●

Die Zyklips der Kette 1 unterscheiden sich alle, die von Kette 2 nicht, weil nach 3 Zyklips wieder dasselbe Farbschema erscheint. Das liegt daran, dass sich das auf Platz 0 beginnende Farbschema ab Platz 3 wiederholt. Bezogen auf die Anzahl der Variationen heißt das, alle Zyklips der Kette 1 sind darin enthalten, von denen der Kette 2 aber nur drei. Der Hilfssatz sagt nun, dass bei jedem Farbschema alle Zyklips unterschiedliche Variationen bilden, wenn die Länge p der Kette eine Primzahl ist.

Um den Hilfssatz zu beweisen, sei k die *kleinste* Anzahl von Zyklips, ab der sich das Farbschema wiederholt und die Schnur auf den Plätzen 0 bis p-1 farblich identisch ist. k = 1 hieße, die Schur wäre einfarbig. Nach Satz 2.1 (Division mit Rest) gibt es Zahlen s und r, so dass

$$p = s \cdot k + r \qquad (0 < r < k,\ 1 < k < p)$$

wobei 0< r < k. Weil p prim ist, kann r = 0 nicht sein. Nun wiederholt sich das Farbschema ab s·k und (s·k + r) mod p = 0, d. h. es gibt eine Wiederholung bereits nach r Zyklips. Aber r < k widerspricht der Annahme, dass k die kleinste Anzahl von Zyklips ist. Damit ist der Hilfssatz bewiesen.

Entfallen die nummerierten Plätze weg und liegen die Ketten kreisförmig geschlossen, dann sind zyklisch vertauschte Ketten nicht mehr unterscheidbar und $(n^p - n)/p$ ist die Anzahl der möglichen mehrfarbigen ringförmigen Ketten mit p Perlen und n Farben. Weil das eine ganze Zahl ist, ist Satz 5.1 damit kombinatorisch bewiesen.

Literatur, für Oberstufenschüler geeignet:

George E. Andrews, Number Theory, W. B. Saunders Co. Philadelphia 1971.
Andreas Bartholomé, Josef Rung, Hans Kern, Zahlentheorie für Einsteiger, Vieweg+Teubner Verlag 2010. Hieraus stammt die Tabelle auf S. 7.
Albrecht Beutelspacher, Kryptologie, Verlag Springer Spectrum Wiesbaden 2015.
Karin Freiermuth, Juraj Hromkovič, Lucia Keller, Björn Steffen, Einführung in die Kryptologie, Lehrbuch für Schulen, Verlag Springer Vieweg Wiesbaden 2014.
Arnold Scholz, Bruno Schoeneberg, Einführung in die Zahlentheorie, Verlag Walter de Gruyter & Co. Berlin 1955.