Elementare Zahlentheorie (Version 1)

(Winter Semester, 2005-6)

1 Zur Notation

- $\mathbb{N}$ ist die Menge der *natürlichen* Zahlen: $1, 2, 3, 4, 5, \ldots$ und so weiter.
- $\mathbb{Z}$ ist die Menge aller ganzen Zahlen: $\ldots, -4, -3, -2, -1, 0, 1, 2, 3, 4, \ldots$ und so weiter.
- $\mathbb{Q}$ ist die Menge der rationalen Zahlen. D.h. Bruchzahlen wie $\frac{1}{2}$, $\frac{22}{7}$, u.s.w. Auch $0,25 = \frac{1}{4}$ ist eine rationale Zahl.

  Selbstverständlich sind alle Zahlen in $\mathbb{Z}$ auch in $\mathbb{Q}$.
- $a \in X$ heißt: X ist eine Menge und a ist ein Element in X.

  $a \notin X$ heißt: a ist *nicht* in X.

  Z.B. $2 \in \mathbb{N}$. Jedoch $0,5 \notin \mathbb{Z}$.
- Für n eine Zahl und $k \in \mathbb{N}$ eine natürliche Zahl, schreibt man

$$n^k = \underbrace{n \cdot n \cdots n}_{\text{k-mal}}.$$

  Z.B. $2^3 = 8$ und $3^3 = 27$.
- Für $n \in \mathbb{N}$ ist

$$n! = 1 \cdot 2 \cdot 3 \cdots (n-1) \cdot n.$$

  Z.B. $3! = 6$ und $5! = 120$. Man sagt "n-fakultät". Es wird auch vereinbart, daß $0! = 1$, obwohl diese Vereinbarung eigentlich nicht in das übrige Schema passt.
- Seien $a_1, \ldots, a_n$ Zahlen. Um die Summe darzustellen, wird

$$\sum_{k=1}^{n} a_k = a_1 + a_2 + \cdots + a_n$$

  geschrieben. Daher, $\sum_{n=1}^{100} n = 5050$. Man schreibt auch z.B.

$$\sum_{k=m}^{n} a_k = a_m + a_{m+1} + \cdots + a_n.$$

2 Vollständige Induktion

Sei $A(n)$ eine Aussage, wobei eine Zahl $n \in \mathbb{N}$ vorkommt.
Z.B. die Aussage: "Das 'Turm-von-Hanoi' Puzzel mit n Scheiben kann in $2^n - 1$ Zügen gelöst werden".

Um eine Aussage dieser Art zu bestätigen für alle $n \in \mathbb{N}$, genügt es:

1. Die Aussage für den Fall $n = 1$ zu bestätigen.
2. Unter der *Annahme*, daß die Aussage $A(n)$ wahr ist, wird bestätigt, daß dann auch $A(n+1)$ wahr ist.

Beispiel (1).
Es gilt

$$\sum_{n=1}^{N} (2n - 1) = N^2.$$

Beweis. Durch vollständige Induktion.

1. Der Fall $n = 1$ ist klar: $\sum_{n=1}^{1}(2n-1) = 1 = 1^2$.
2. Sei nun angenommen, daß unsere Formel wahr ist für den Fall N. Wir müssen zeigen, daß die Formel dann auch wahr ist im Falle $N+1$. Aber es gilt

$$\begin{aligned}(N+1)^2 &= N^2 + 2N + 1 \\ &= \left(\sum_{n=1}^{N}(2n-1)\right) + (2(N+1)-1) \\ &= \sum_{n=1}^{N+1}(2n-1)\end{aligned}$$

□

Beispiel (2). *Die Wahrscheinlichkeit, beim Lotto (6 aus 45) zu gewinnen, ist 1 zu 8145060.*

Beweis. Allgemeiner gilt: Sei $n \in \mathbb{N}$, und k eine Integerzahl zwischen 0 und n. Wir bezeichnen mit $\binom{n}{k}$ die Anzahl der *verschiedenen* Möglichkeiten, k verschiedene Zahlen aus der Menge $\{1, 2, \ldots, n\}$ zu ziehen. Nach einer einfachen Idee (die in der Vorlesung beschrieben wird) gilt

$$\binom{n}{k} = \binom{n-1}{k-1} + \binom{n-1}{k},$$

(wobei $n \geq 2$ und $k \geq 1$).

Behauptung: Es gilt immer

$$\binom{n}{k} = \frac{n!}{(n-k)!k!}.$$

Diese Formel wird mittels vollständiger Induktion über die Zahl n bestätigt.

1. Falls $n = 1$, dann gilt offensichtlich

$$\binom{1}{0} = 1, \text{ und } \binom{1}{1} = 1.$$

2. Falls $n > 1$, sei angenommen, daß die Formel wahr ist für $n-1$. Dann gilt

$$\begin{aligned}\binom{n}{k} &= \binom{n-1}{k-1} + \binom{n-1}{k} \\ &= \frac{(n-1)!}{((n-1)-(k-1))!(k-1)!} + \frac{(n-1)!}{((n-1)-k)!k!} \\ &= \frac{(n-1)!}{(n-k)!(k-1)!} + \frac{(n-1)!}{((n-k)-1)!k!} \\ &= \frac{k\cdot(n-1)!}{(n-k)!k!} + \frac{(n-k)\cdot(n-1)!}{(n-k)!k!} \\ &= k\cdot\frac{(n-1)!}{(n-k)!k!} + n\cdot\frac{(n-1)!}{(n-k)!k!} - k\cdot\frac{(n-1)!}{(n-k)!k!} \\ &= \frac{n!}{(n-k)!k!}\end{aligned}$$

□

Dies wird anhand von Pascal's Dreieck nachvollziehbar.

$$
\begin{array}{ccccccccccccc}
 & & & & & & 1 & & & & & & \\
 & & & & & 1 & & 1 & & & & & \\
 & & & & 1 & & 2 & & 1 & & & & \\
 & & & 1 & & 3 & & 3 & & 1 & & & \\
 & & 1 & & 4 & & 6 & & 4 & & 1 & & \\
 & 1 & & 5 & & 10 & & 10 & & 5 & & 1 & \\
1 & & 6 & & 15 & & 20 & & 15 & & 6 & & 1
\end{array}
$$

u.s.w.

Bemerkung. *Durch Kürzungen gilt:*

$$\binom{n}{k} = \frac{n!}{(n-k)!k!} = \frac{n \cdot (n-1) \cdots (n-k+1)}{k \cdot (k-1) \cdots 2 \cdot 1}.$$

Daher, um die Wahrscheinlichkeit beim Lotto auszurechnen, brauchen wir nur sechs Zahlen im Zähler und sechs Zahlen im Nenner zu multiplizieren.

3 Die Teilbarkeit in $\mathbb{N}$

Zum Beispiel, $6 = 2 \cdot 3$. Daher ist 6 *teilbar* durch 2 und auch durch 3. Folglich ist 6 *keine* Primzahl. Man schreibt $a|b$, um zu sagen, "a ist ein Teiler von b". D.h. eine Zahl c existiert, mit $b = a \cdot c$. Daher ist etwa $3|6$ und $2|6$. Im allgemeinen werden wir uns hier auf Integerzahlen beschränken, und zwar die natürlichen Zahlen $\mathbb{N}$. Aber wenn auch die besondere Zahl 0 zugelassen wird, dann gilt: a ist *immer* ein Teiler von 0, egal welches a gewählt wird. Denn es gilt immer $0 = 0 \cdot a$.

Auf jeden Fall gilt: für alle $n \in \mathbb{N}$ sind sowohl 1 als auch n Teiler von n.

3.1 Die Primzahlen

Die Primzahlen sind $2, 3, 5, 7, 11, 13, 17, \ldots$ Es gibt viele Leute, für die die Folge der Primzahlen extrem faszinierend ist. Die größte noch ungelöste Frage in der Mathematik — die Riemann'sche Vermutung — hat etwas mit der Folge der Primzahlen zu tun.

Wir in der Mathematik verwenden die folgende Definition für den Begriff "Primzahl":

Definition 3.1. Eine Zahl $p \in \mathbb{N}$ (mit $p \geq 2$) heißt *prim*, falls wann immer p ein Produkt von zwei weiteren Zahlen $a \cdot b$ in $\mathbb{N}$ teilt, dann teilt p entweder a oder b (oder beide).

Nun, nehmen wir an, wir haben zwei Zahlen $a, b \in \mathbb{N}$ mit $a|b$. Dann ist sicherlich $a \leq b$. Der *kleinste* Teiler von b ist einfach die 1. Der *größte* Teiler ist dann b selbst.

Definition 3.2. Seien $a, b \in \mathbb{N}$ zwei Zahlen. Eine weitere Zahl d heißt ein *gemeinsamer Teiler* von a und b, falls $d|a$ und auch $d|b$. Der *großte gemeinsame Teiler* wird mit $\mathrm{ggt}(a, b)$ bezeichnet.

Sei $d = \mathrm{ggt}(a, b)$. Dann gilt sicherlich sowohl $d \leq a$ als auch $d \leq b$.

Satz 1. *Angenommen,* $p \in \mathbb{N}$ *ist eine Primzahl und* $a \in \mathbb{N}$ *ist gegeben, wobei* $1 \leq a < p$*. Dann gilt* $\mathrm{ggt}(p, a) = 1$*.*

Beweis. Sei $d = \mathrm{ggt}(p, a)$. Angenommen doch, $d > 1$. Dann ist $d|p$ und auch $d \leq a < p$. D.h. wir können schreiben $p = d \cdot b$, wobei auch $1 < b < p$. Aber nach der Definition von Primzahlen, *muß* entweder $p|b$ oder $p|d$ gelten. Dies ist unmöglich, da beide Zahlen b und d kleiner als p sind. □

Folglich ist eine Primzahl nur durch die 1 und durch sich selbst teilbar. Andererseits, falls eine Zahl n einen Teiler a besitzt, mit $1 < a < n$, dann ist sicherlich n *keine* Primzahl.

Satz 2. *Jede natürliche Zahl* $n \geq 2$ *hat eine eindeutige Primfaktorzerlegung.*

Beweis. Wenn dieser Satz doch falsch wäre, dann gäbe es eine Zahl n ohne eindeutige Primfaktorzerlegung. Unter der Voraussetzung, daß solche Zahlen existieren, sei n die *kleinste* solche Zahl.

Kann es sein, daß n überhaupt keine Primfaktorzerlegung besitzt? D.h. es wäre nicht möglich, n als Produkt: $n = p_1 \cdots p_r$ zu schreiben, wobei $p_1, p_2, \ldots, p_r$ alle Primzahlen sind. Insbesondere wäre dann n selbst *keine* Primzahl, und daher muß eine kleinere Zahl a existieren, mit $1 < a < n$ und $n = a \cdot b$ etwa, wobei $a, b \in \mathbb{N}$. Aber dann ist auch b kleiner als n, und folglich haben beide Zahlen, a und b Primfaktorzerlegungen. Daher auch n selbst.

Kann es sein, daß n zwar eine Primfaktorzerlegung besitzt, aber diese ist nicht eindeutig? D.h. seien etwa

$$n = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s$$

zwei verschiedene Primfaktorzerlegungen von n. Kann es sein, daß eine Primzahl auf beiden Seiten vorkommt? D.h. $p_i = q_j$, für irgendwelche i und j? Aber dann ist n/p_i auch eine natürliche Zahl und n/p_i hat auch eine zweideutige Primfaktorzerlegung. Und n/p_i ist kleiner als n. Dies widerspricht unserer Annahme, daß n die kleinste solche Zahl sein soll. Daher müssen alle $p_i's$ und $q_j's$ verschieden sein.

Nun, wir wissen zumindest, daß $p_1 | n = q_1 q_2 \cdots q_s$. D.h.

$$p_1 | q_1 \cdot (q_2 q_3 \cdot q_s).$$

Nach unserer Definition des Begriffs "Primzahl" muß dann entweder $p_1 | q_1$ oder $p_1 | q_2 q_3 \cdot q_s$. Aber q_1 ist prim. Daher muß gelten $p_1 | q_2 q_3 \cdot q_s$. Ebenso ist q_2 prim. Daher muß gelten $p_1 | q_3 \cdot q_s$. U.s.w. Letztendes muß gelten $p_1 | q_s$. Dies ist unmöglich, da auch q_s prim ist. Die einzige Folgerung ist, daß ein solches n nicht existieren kann, und daher muß unser Satz doch wahr sein. □

3.2 Division mit Rest; Der Euklidsche Algorithmus

Gegeben $a, b \in \mathbb{N}$, dann ist entweder a ein Teiler von b, oder eben nicht. Falls $a | b$, dann ist $b = ca$, wobei $c \in \mathbb{N}$. Man schreibt einfach

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

Falls dies nicht geht, dann schreibt man $a \not| b$. Zumindest ist das, was wir mit $\frac{b}{a}$ bezeichnen, keine natürliche Zahl. Immerhin ist es immer möglich, zu sagen, daß zwei Integerzahlen c und r existieren, wobei $b = ca + r$ und $0 \leq r < a$. Dazu schreibt man oft b 'div' a für die Zahl c und b 'mod' c für die Zahl r. Man sagt auch, daß r der 'Rest' ist nach der Division b/a.

Satz 3. *Für* $a, b \in \mathbb{N}$ *gilt* $\mathrm{ggt}(a, b) = \mathrm{ggt}(r, a)$, *wobei* $r = b \pmod{a}$.

Beweis. Sei $d = \mathrm{ggt}(a, b)$. Dann ist $d | a$, aber auch $d | r$, denn $r = b - ca$ und $d | b$. Folglich ist d ein gemeinsamer Teiler von r und a. Kann es sein, daß ein noch größerer gemeinsamer Teiler d' von r und a existiert? Aber dann gilt $d' | a$, aber auch $d' | b = ca + r$. Daher ist d' auch ein gemeinsamer Teiler von a und b. Dies ist ein Widerspruch, da d doch der größter gemeinsame Teiler von a und b ist. □

Seien zwei Zahlen $a, b \in \mathbb{N}$ vorgegeben. Wie finden wir $\mathrm{ggt}(a, b)$? Der *Euklidsche Algorithmus* ist eine Methode, dies zu finden.

1. Falls $a = b$, dann ist offensichtlich $\mathrm{ggt}(a, b) = a = b$. Fertig.
2. Sonst ist $a \neq b$; sei etwa $b > a$, und wir setzen $r = b \pmod{a}$.
   (a) Falls $r = 0$, dann ist $a | b$ und daher $\mathrm{ggt}(a, b) = a$. Wieder sind wir fertig.
   (b) Sonst ist $\mathrm{ggt}(a, b) = \mathrm{ggt}(r, a)$. Daher setze die Rechnung bei Schritt 2 fort, wobei a anstelle von b und r anstelle von a eingesetzt wird. Da stets die Beziehung $b > a > r \geq 0$ gilt, wird nach endlich vielen weiteren Schritten das Ergebnis entstehen.

4 Die rationalen Zahlen

4.1 Die Bruchzahlen

Die rationalen Zahlen $\mathbb{Q}$ sind die Zahlen, die als Bruchzahlen geschrieben werden können. D.h.

$$\mathbb{Q} = \left\{ \frac{a}{b} : a \in \mathbb{Z}, b \in \mathbb{N} \right\}.$$

Zum Beispiel ist $1/2$ eine Bruchzahl. Man könnte auch $7/14$ schreiben, oder so etwas. Aber jeder wird sofort sagen, daß $1/2$ die bessere Darstellung ist, weil $1/2$ eine *gekürzte* Bruchzahl ist. Eine Bruchzahl a/b heißt gekürzt, falls $\mathrm{ggt}(a,b) = 1$.

Falls $b = 1$, dann ist a/b einfach eine Integerzahl, nämlich die Zahl a.

In der Grundschule lernen wir, wie man Bruchzahlen addiert und multipliziert, und zwar:

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + cb}{bd}$$

und

$$\frac{a}{b} \times \frac{c}{d} = \frac{ac}{bd}.$$

Wenn wir eine Zahl wie etwa $\frac{22}{7}$ betrachten, dann werden viele sagen, es ist doch besser, $3\frac{1}{7}$ zu schreiben. D.h. im allgemeinen, gegeben eine Bruchzahl wie a/b, dann kann die Zahl als

$$(a \text{ div } b)\ \frac{a \bmod b}{b} = c\ \frac{d}{e}$$

dargestellt werden, wobei $c \in \mathbb{Z}$, $\mathrm{ggt}(d,e) = 1$ und $0 \le d < e$.

- D.h. $c = a$ div b und $d = a \bmod b$ (aber dann gekürzt bzgl. b).
- Falls $d = 0$ (d.h. falls a teilbar ist durch b), dann wird natürlich nur c alleine geschrieben.

4.2 Die Dezimalzahlen

Die übliche Dezimaldarstellung von Zahlen ist eine Verallgemeinerung dieser Idee. Zum Beispiel

$$123.45 = \frac{12345}{100} = 123\frac{45}{100} = 1 \cdot 100 + 2 \cdot 10 + 3 \cdot 1 + 4 \cdot \frac{1}{10} + 5 \cdot \frac{1}{100}.$$

Ebenso ist

$$\frac{22}{7} = 3 + 1 \cdot \frac{1}{7}.$$

U.s.w. Aber wenn wir versuchen, $22/7$ in der Dezimaldarstellung zu schreiben, dann gibt es Schwierigkeiten!

$$\frac{22}{7} = 3.142857142857142857142857142857142857142857\ldots$$

Die Zahl $22/7$ hat also eine schöne, kurze Darstellung, wenn 7 als die Basis unseres Zahlensystems gewählt wird, aber eine unendlich lange, unangenehme Darstellung im Dezimalsystem zur Basis 10.

Man könnte als Basis irgendein $n \in \mathbb{N}$ nehmen. Zum Beispiel wieder die (glückliche) Zahl 7. Dann wäre etwa die Zahl 10 als $1 \cdot 7 + 3 \cdot 1$, d.h. als '13' dargestellt. Wie man sieht: die Integerzahlen bleiben immer ziemlich problemlos.

Aber wie ist etwa die Darstellung von $11,1 = \frac{111}{10}$ in unserem System zur Basis 7?

$$\begin{aligned} \frac{111}{10} &= 1 \cdot 7 + 3 \cdot 1 + 0 \cdot \frac{1}{7} + 4 \cdot \frac{1}{49} + 2 \cdot \frac{1}{343} + \cdots \\ &= 1 \cdot 7 + 3 \cdot 1 + 0 \cdot \frac{1}{7} + 4 \cdot \frac{1}{7^2} + 2 \cdot \frac{1}{7^3} + \cdots \\ &= \text{'}13,042\ldots\text{'} \quad \text{u.s.w.} \end{aligned}$$

Zur Basis 2 (das "binäre" System) haben wir

$$\frac{11}{10} = 1 \cdot 1 + 0 \cdot \frac{1}{2} + 0 \cdot \frac{1}{4} + 0 \cdot \frac{1}{8} + 1 \cdot \frac{1}{16} + 1 \cdot \frac{1}{32} + \cdots = 1,00011\ldots$$

Im allgemeinen gilt: Für eine vorgegebene Basiszahl $n \in \mathbb{N}$ (wobei $n \geq 2$) und eine beliebige rationale Zahl a/b gibt es immer eine Darstellung der Art

$$\frac{a}{b} = \sum_{k=m}^{\infty} \frac{a_k}{n^k},$$

für ein $m \in \mathbb{Z}$, wobei $0 \leq a_k < n$ für alle k.

4.3 Vorteile und Nachteile

Zunächst scheint die Darstellung von rationalen Zahlen als einfache Bruchzahlen besser als das komplizierte Dezimalsystem. Wir benutzen zwar das Dezimalsystem für die Darstellung von Integerzahlen. Aber was übrig bleibt — die 'Rest' Zahlen, die Werte zwischen 0 und 1 haben — ist vielleicht zu kompliziert für das Dezimalsystem. Dies ist der Grund, warum es nötig ist, komplizierte 'Rechenregeln' in der Schule zu lernen.

Trotzdem hat das Dezimalsystem einen Vorteil gegenüber dem Rechnen mit Bruchzahlen. Es ist nämlich immer einfach, zu entscheiden, ob eine vorgegebene Zahl größer oder kleiner ist als eine andere Zahl.

Nehmen wir zum Beispiel

$$x = \frac{5}{7}, \text{ und } y = \frac{31}{43}.$$

Welche Zahl ist größer? Wenn wir die Dezimaldarstellung anschauen, dann ist klar:

$$x = 0,7142857142\ldots \quad < \quad y = 0,7209302326\ldots$$

4.4 Die Kettenbruchzahlen

haben — in gewisser Weise — die Vorteile von *beiden* Systemen. Im Kettenbruchsystem schreiben wir wieder

$$11,1 = \frac{111}{10} = 11 + \frac{1}{10} \quad \text{und} \quad \frac{22}{7} = 3 + \frac{1}{7}.$$

Aber z.B.

$$\frac{26}{7} = 3 + \frac{1}{1 + \frac{1}{2 + \frac{1}{2}}}.$$

Oder

$$\frac{33}{30} = 1 + \frac{1}{2 + \frac{1}{3 + \frac{1}{4}}}.$$

Diese Schreibweise ist natürlich ziemlich umständlich. Es wäre einfacher etwa

$$\frac{26}{7} = [3; 1, 2, 2]$$

oder

$$\frac{33}{30} = [1; 2, 3, 4]$$

zu schreiben.

Die Idee ist, immer eine 1 im 'Zähler' in der 'partiellen' Bruchzahl zu haben. Es ist möglich, daß das Rechnen mit Kettenbruchzahlen die Basis für die Zahlentheorie bei den alten Griechen war.

Können Sie die Rechenregeln für die Addition und Multiplikation von Kettenbruchzahlen selber (durch Ausprobieren) herausfinden?

4.5 Die Kettenbruchdarstellung einer rationalen Zahl ist endlich

Sei $\frac{a}{b} \in \mathbb{Q}$ vorgegeben. Durch Kürzen können wir annehmen, daß $\mathrm{ggt}(a,b) = 1$. Wir schreiben zunächst

$$\frac{a}{b} = a_0 + \frac{r_0}{b}.$$

Hier ist a_0 der Quotient, a div b. Und r_0 ist der Rest, a mod b. Es gilt immer $0 \le r_0 < b$. Falls $r_0 = 0$, dann sind wir fertig. Sonst ist $0 < \frac{r_0}{b} < 1$. D.h. $1 < \frac{b}{r_0}$. Wir schreiben dann

$$\frac{a}{b} = a_0 + \frac{r_0}{b} = a_0 + \frac{1}{\frac{b}{r_0}} = a_0 + \frac{1}{a_1 + \frac{r_1}{r_0}}.$$

Hier ist $a_1 = b$ div r_0 und $r_1 = b$ mod r_0. Insbesondere gilt $0 \le r_1 < r_0$. Der nächste Schritt ist zu schreiben

$$\frac{a}{b} = a_0 + \frac{r_0}{b} = a_0 + \frac{1}{\frac{b}{r_0}} = a_0 + \frac{1}{a_1 + \frac{r_1}{r_0}} = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \frac{r_2}{r_1}}},$$

wobei $r_2 = r_0$ mod r_1. D.h. $0 \le r_2 < r_1$. Und so weiter. Es gilt immer

$$r_0 > r_1 > r_2 > \cdots \ge 0.$$

D.h. irgendwann muß ein $r_n = 0$ sein, und dann sind wir fertig. Der Kettenbruchzahl ist endlich.

5 Die irrationalen Zahlen

Das Rechnen mit Kettenbruchzahlen gibt uns eine Methode, irrationale Zahlen zu finden, und zwar ist eine Zahl, die eine *unendliche* Kettenbruchdarstellung hat, dann ist sie sicherlich nicht rational. Zum Beispiel, die Kettenbruchzahl

$$g = 1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1 + \cdots}}}}$$

ist irrational. Dies ist “Der goldener Schnitt”.

Auch die Zahl

$$\sqrt{2} = 1 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \frac{1}{2 + \cdots}}}}$$

ist irrational.

5.1 Die Zahl $\sqrt{2}$

Ist $\sqrt{2}$ tatsächlich diese Kettenbruchzahl? Wenn wir die Darstellung anschauen, dann wird uns bald klar, daß die folgende Beziehung gilt:

$$\sqrt{2} = 1 + \frac{1}{1 + \sqrt{2}}.$$

D.h.

$$\sqrt{2} - 1 = \frac{1}{1 + \sqrt{2}},$$

oder

$$1 = (\sqrt{2} - 1)(\sqrt{2} + 1) = (\sqrt{2})^2 - 1^2,$$

oder

$$2 = (\sqrt{2})^2.$$

Es stimmt!

Es ist vielleicht üblicher, die Irrationalität von $\sqrt{2}$ nach dem folgenden Verfahren zu beweisen.

5.2 Noch ein Beweis

Satz 4. $\sqrt{2} \notin \mathbb{Q}$.

Beweis. Angenommen, $\sqrt{2}$ sei doch eine rationale Zahl, etwa $\sqrt{2} = \frac{a}{b}$. Wir können annehmen, daß sowohl a als auch b positive ganze Zahlen sind. Vielleicht gibt es verschiedene Möglichkeiten, $\sqrt{2}$ durch solche Bruchzahlen darzustellen. Unter allen Möglichkeiten sei die Bruchzahl $\frac{a}{b}$ gewählt, wobei die Zahl b so *klein* wie möglich ist.

Nun, da $(\sqrt{2})^2 = 2$, gilt

$$\left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2} = 2,$$

oder

$$a^2 = 2b^2.$$

Dies geht nur, wenn a eine gerade Zahl ist[1]. Sei dann $a = 2c$, wobei auch c eine positive ganze Zahl ist. Dann gilt wiederum

$$a^2 = (2c)^2 = 4c^2 = 2b^2,$$

oder

$$b^2 = 2a^2.$$

Folglich ist auch b eine gerade Zahl, etwa $b = 2d$ mit d eine positive ganze Zahl. Dann ist

$$\sqrt{2} = \frac{a}{b} = \frac{2c}{2d} = \frac{c}{d}.$$

Somit haben wir einen Widerspruch, da $d < b$. □

5.3 Andere Methoden, irrationale Zahlen zu finden

In der Vorlesung ist gezeigt worden, daß jede rationale Zahl eine Dezimaldarstellung hat, die entweder endlich, oder unendlich aber periodisch ist. Daher ist jede Zahl, die eine *nicht* periodische, unendliche Darstellung hat, sicherlich irrational. Zum Beispiel die Zahl

$$1,101001000100001000001000000001\ldots$$

ist irrational.

6 Folgen von Zahlen

Eine Folge ist einfach eine unendliche, geordnete Liste. Z.B. die Liste

$$1, 3, 2, 2, 5, 8, 3, \ldots$$

Oder auch eine mehr "ordentliche" Folge:

$$\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \frac{1}{5}, \frac{1}{6}, \frac{1}{7}, \ldots$$

Man schreibt $(a_k)_{k\in\mathbb{N}}$. Daher ist a_k die k-te Zahl in der Folge. Wir interessieren uns insbesondere für *konvergente* Folgen. Eine Folge $(a_k)_{k\in\mathbb{N}}$ heißt konvergent, falls eine Zahl a existiert, so daß der Abstand von a_k zu a kleiner wird, wenn k grosser wird.

Aber eigentlich ist diese Beschreibung doch etwas zu locker.

Definition 6.1. Sei x eine (reelle) Zahl. Der *Absolutbetrag* von x ist die Zahl

$$|x| = \begin{cases} x, & \text{falls } x \geq 0, \\ -x, & \text{falls } x < 0. \end{cases}$$

Falls auch y noch eine Zahl ist, dann ist der *Abstand* zwischen x und y die Zahl $|x - y|$.

[1] Zur Erinnerung: ungerade mal ungerade ist stets ungerade!

Es ist klar, daß der Abstand zwischen x und y positiv ist, falls $x \neq y$. Nur wenn $x = y$, ist der Abstand auch null.

Wichtig ist die *Dreiecksungleichung*:

$$|x + y| \leq |x| + |y|.$$

Warum gilt diese Ungleichung? Man braucht nur die verschiedenen Fälle, wobei x und y entweder positiv oder negativ (oder null) sind zu untersuchen. Falls beide gleichzeitig positiv oder negativ sind, dann gilt $|x + y| = |x| + |y|$. Andernfalls, wenn etwa $x < 0$ und $y > 0$, dann ist $|x + y| < |x| + |y|$. Eine triviale Folgerung ist

$$|x - y| \leq |x| + |y|.$$

Es folgt dann, daß auch

$$|a_1 + a_2 + \cdots + a_n| \leq |a_1| + |a_2| + \cdots + |a_n|.$$

Nun, seien wieder x und y Zahlen. Dann gilt

$$|x| = |(x - y) + y| \leq |x - y| + |y|.$$

Daher

$$|x| - |y| \leq |x - y|.$$

Allgemeiner,

$$|x| - \sum_{k=1}^{n} |y_k| \leq \left| x - \sum_{k=1}^{n} y_k \right|.$$

6.1 Konvergenz bei Folgen

Definition 6.2. Die Folge $(a_n)_{n\in\mathbb{N}}$ *konvergiert*, mit Limes a, falls für alle vorgegebenen positiven Zahlen $\epsilon > 0$, eine hinreichend große Zahl N existiert (im allgemeinen abhängig von der Zahl ϵ), so daß

$$|a - a_k| < \epsilon,$$

für alle $k \geq N$.

Zum Beispiel, die Folge $(1/n)_{n\in\mathbb{N}}$ konvergiert gegen 0. Denn, sei $\epsilon > 0$ vorgegeben. Wir nehmen N so groß[2], daß $N > \frac{1}{\epsilon}$. Dann ist sicherlich

$$\left| 0 - \frac{1}{k} \right| = \frac{1}{k} \leq \frac{1}{N} < \epsilon,$$

für alle $k \geq N$.

Bemerkung (Eine Schwierigkeit). *Was passiert, wenn die Folge gegen einen Limes konvergiert, der gar nicht im vorgesehenen System liegt?*

Betrachten Sie zum Beispiel die Kettenbruchdarstellung von $\sqrt{2}$. Dies ist eine Folge von *rationalen* Zahlen, die aber gegen einer nicht rationalen Zahl, nämlich $\sqrt{2}$ konvergiert. Daher, logischerweise, wenn wir nur die rationalen Zahlen als System haben, dann müssen wir einfach sagen, daß die Folge *im System der rationalen Zahlen* gar nicht konvergiert.

Aber so eine Feststellung ist doch unbefriedigend. Es ist klar, daß die Folge *an sich* konvergiert. D.h. die Folge ist eine *Cauchy-Folge*.

Definition 6.3. Die Folge $(a_n)_{n\in\mathbb{N}}$ heißt *Cauchy-Folge*, falls für alle $\epsilon > 0$ eine hinreichend große Zahl N existiert (im allgemeinen abhängig von der Zahl ϵ), wobei

$$|a_k - a_l| < \epsilon,$$

für alle $k, l \geq N$.

[2]Zum Beispiel, für $\epsilon = \frac{1}{1000000}$, könnten wir etwa die Zahl $N = 1000001$ nehmen.

Um das System der reellen Zahlen zu definieren, brauchen wir eigentlich einige weitere Begriffe (Äquivalenzrelation, u.s.w.), aber hier möchte ich einfach locker sagen, daß die Menge der reellen Zahlen $\mathbb{R}$ die Menge aller möglichen Konvergenzpunkten von Cauchy-Folgen ist (sowohl in $\mathbb{Q}$ als auch in $\mathbb{R}$ selbst). Somit ist insbesondere $\mathbb{Q} \subset \mathbb{R}$.

Satz 5. *Jede konvergente Folge ist auch eine Cauchy-Folge.*

Beweis. Sei $(a_n)_{n\in\mathbb{N}}$ eine Folge, die gegen die Zahl a konvergiert. Wir können dazu auch

$$a_n \underset{n\to\infty}{\longrightarrow} a$$

schreiben. Sei nun $\epsilon > 0$ vorgegeben. Dann ist auch $\epsilon/2$ eine positive Zahl. Da die Folge gegen a konvergiert, existiert eine Zahl N, die so groß ist, daß $|a_n - a| < \epsilon/2$, für alle $n \geq N$. Seien nun k, $l \geq N$ zwei solche Zahlen. Dann gilt

$$|a_k - a_l| = |(a_k - a) + (a - a_l)| \leq |a_k - a| + |a - a_l| < \frac{\epsilon}{2} + \frac{\epsilon}{2} = \epsilon.$$

Die erste Ungleichung hier ist unsere Dreiecksungleichung für die Absolutbetragfunktion. □

Daher gilt (im System der reellen Zahlne $\mathbb{R}$): eine Folge ist genau dann konvergent, wenn sie eine Cauchy-Folge ist.

6.2 Reihen

Definition 6.4. Eine Reihe ist eine unendliche Summe

$$\sum_{n=1}^{\infty} a_n.$$

Die Zahlen a_n sind vorgegeben. Man kann daher sagen, daß eine Reihe die Summe einer Folge $(a_n)_{n\in\mathbb{N}}$ ist.

Gegeben eine Reihe $\sum_{k=1}^{\infty} a_k$, dann ist die n-te *partielle Summe* die endliche Summe

$$S_n = \sum_{k=1}^{n} a_k.$$

Die Reihe $\sum_{k=1}^{\infty} a_k$ konvergiert also genau dann, wenn die Folge der partiellen Summen konvergiert.

6.2.1 Die geometrische Reihe

Sei $|x| < 1$ vorgegeben. Dann können wir die Reihe, bestehend aus den Potenzen, betrachten.

$$\sum_{n=0}^{\infty} x^n.$$

(Bemerken Sie, daß diese Reihe mit $n = 0$, statt mit $n = 1$ anfängt.)

Satz 6. *Sei $x \neq 1$. Dann gilt*

$$\sum_{k=0}^{n} x^n = \frac{1 - x^{n+1}}{1 - x}.$$

Beweis.

$$(1 - x)\left(\sum_{k=0}^{n} x^n\right) = 1 + x + \cdots + x^n - x - \cdots - x^n - x^{n+1} = 1 - x^{n+1}.$$

□

Aber Sie haben schon in einer Übung gesehen, daß

$$x^n \underset{n\to\infty}{\longrightarrow} 0,$$

falls $|x| < 1$. Daher gilt

$$\sum_{n=0}^{\infty} x^n = \frac{1}{1-x}.$$

6.3 Absolute Konvergenz

Definition 6.5. Die Reihe

$$\sum_{n=1}^{\infty} a_n$$

heißt *absolut konvergent*, falls die entsprechende Reihe, bestehend aus den Absolutbeträgen der einzelnen Terme, nämlich

$$\sum_{n=1}^{\infty} |a_n|,$$

konvergiert.

Satz 7. *Eine absolut konvergente Reihe konvergiert.*

Beweis. Sei die Reihe $\sum_{n=1}^{\infty} a_n$ absolut konvergent. D.h. $\sum_{n=1}^{\infty} |a_n| <$ konvergiert. Wir haben etwa

$$\sum_{n=1}^{\infty} |a_n| = A.$$

D.h. wenn wir die partiellen Summen $A_n = \sum_{k=1}^{n} |a_k|$ betrachten, dann stellen wir fest, daß $A^n \underset{n\to\infty}{\longrightarrow} A$. Aber da $A_n \geq 0$ für alle n, gilt $A \geq 0$. Es gilt sogar

$$0 \leq A_1 \leq A_2 \leq \cdots \leq A_n \leq \cdots \longrightarrow A.$$

Sei nun $\epsilon > 0$ vorgegeben. Da $A_n \longrightarrow A$, gibt es ein N so gross, daß $|A - A_k| = A - A_k < \epsilon$, für alle $k \geq N$. Insbesondere ist

$$|A_m - A_n| = A_m - A_n = \sum_{k=n+1}^{m} |a_k| < \epsilon,$$

wenn $m \geq n$.

Sei nun S_n die n-te partielle Summe der ursprünglichen Reihe. D.h.

$$S_n = \sum_{k=1}^{n} a_k.$$

Dann, für $m \geq n \geq N$ gilt

$$|S_m - S_n| = \left| \sum_{k=n+1}^{m} a_k \right| \leq \sum_{k=n+1}^{m} |a_m| < \epsilon.$$

Die erste Ungleichung hier ist wiederum unsere Dreiecksungleichung. □

6.4 Der Majorantenkriterium

Satz 8. *Angenommen, eine Folge $(c_n)_{n\in\mathbb{N}}$ sei vorgegeben, wobei alle $c_n \geq 0$. Sei weiter angenommen, daß die Reihe*

$$C = \sum_{n=1}^{\infty} c_n$$

konvergiert. Falls eine weitere Reihe $\sum_{n=1}^{\infty} a_n$ gegeben ist mit $|a_n| \leq c_n$ für alle n, dann ist diese Reihe auch konvergent — sogar absolut konvergent.

Beweis. Sei $\epsilon > 0$ gegeben, und sei $N \in \mathbb{N}$ so groß, daß

$$\left| C - \sum_{k=1}^{n} c_k \right| < \epsilon, \quad \text{für } n \geq N.$$

Dann ist

$$\begin{aligned} |S_m - S_n| &= \left| \sum_{k=n+1}^{m} a_k \right| \\ &\leq \sum_{k=n+1}^{m} |a_k| \\ &\leq \sum_{k=n+1}^{\infty} c_n \\ &= \left| C - \sum_{k=1}^{n} c_k \right| < \epsilon \end{aligned}$$

für $m \geq n \geq N$. Daher bilden die partiellen Summen eine Cauchy-Folge. □

7 Äquivalenzrelationen

Definition 7.1. Sei M eine Menge. Eine Äquivalenzrelation auf M wird folgenderweise definiert. Falls x zu y äquivalent ist (wobei $x, y \in M$), dann schreiben wir $x \sim y$. Anderenfalls ist $x \not\sim y$. Eine Äquivalenzrelation unterliegt der folgenden Regel:

1. $x \sim x$, für alle $x \in M$.
2. Falls $x \sim y$ dann gilt auch $y \sim x$.
3. Falls $x \sim y$ und $y \sim z$ dann gilt $x \sim z$.

Eine Menge M versehen mit einer vorgegebenen Äquivalenzrelation $\sim$ wird oft als Paar $(M, \sim)$ geschrieben.

Beispiele

Für diese Beispiele werden wir einfach die Menge $M = \mathbb{Z}$ (die ganzen Zahlen) nehmen.

- Die einfachste Äquivalenzrelation ist die Gleichheitsrelation "=". Es it eine triviale Sache, die drei Regeln dann zu bestätigen.
- Andererseits ist die Relation "$\leq$" (d.h. "kleiner oder gleich") *keine* Äquivalenzrelation, denn unsere Regel 2 gilt nicht für "$\leq$".
- Die Relation "$<$" ("kleiner als") ist auch *keine* Äquivalenzrelation. Sowohl Regel 1 als auch Regel 2 wird hier verletzt.

Sei nun $x \in M$ irgendein Element in M, d.h. in einer Menge mit einer Äquivalenzrelation $(M, \sim)$. Die *Äquivalenzklasse*, die x enthält, ist die Teilmenge

$$[x] = \{y \in M : y \sim x\}.$$

Satz 9. *Sei $(M, \sim)$ eine Menge, versehen mit einer Äquivalenzrelation. Seien $x, y \in M$. Dann gilt*

$$[x] \cap [y] \neq \emptyset \quad \Longrightarrow \quad [x] = [y].$$

Mit anderen Worten: Falls ein $z \in M$ existiert, wobei sowohl $z \in [x]$ als auch $z \in [y]$, dann folgt $[x] = [y]$.

Beweis. Um zu zeigen, daß $[x] = [y]$, genügt es zu zeigen daß sowohl $[x] \subseteq [y]$ als auch $[y] \subseteq [x]$. Sei dann $w \in [x]$. D.h. $w \sim x$. Aber $x \sim y$. Daher, nach unser Regel 3 muß gelten $w \sim y$ und folglich $w \in [y]$. Da $w \in [x]$ beliebig war, gilt $[x] \subseteq [y]$. Durch Symmetrie folgt auch $[y] \subseteq [x]$. □

Dieser kleine Satz zeigt uns zweierlei. Zum Ersten ist klar, daß es egal ist, welcher "Vertreter" einer Äquivalenzklasse genommen wird, um die Äquivalenzklasse zu beschreiben. D.h. falls $x \sim y$, dann ist es egal, ob man $[x]$ oder auch $[y]$ schreibt. Es handelt sich um ein und dieselbe Äquivalenzklasse. Zum Zweiten folgt, daß die gesamte Menge M in *disjunkte* Äquivalenzklassen zerfällt.

Beispiel. *Das* eigentliche *Beispiel für uns ist die folgende Äquivalenzrelation. Wieder sei* $M = \mathbb{Z}$. *Wir nehmen nun eine feste positive ganze Zahl* $n \in \mathbb{N}$. *Dann gilt* $a \sim b$ *für beliebige Zahlen* $a, b \in \mathbb{Z}$ *genau dann, wenn* $n|a - b$. *(D.h.* n *teilt* $a - b$.*)*

Es ist eine kleine Übung, zu zeigen daß dies eine Äquivalenzrelation ist. Was sind die Äquivalenzklassen? Es ist eine weitere kleine Übung zu sehen, daß genau n verschiedene Äquivalenzklassen existieren, und zwar

$$[0], [1], \ldots, [n-1].$$

Die Menge dieser Äquivalenzklassen wird (etwas umständlich) mit $\mathbb{Z}/n\mathbb{Z}$ bezeichnet. D.h.[3]

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

Für $a, b \in \mathbb{Z}$ zwei beliebige ganze Zahlen gilt $a \sim b$ genau dann, wenn $a \bmod n = b \bmod n$. Es ist üblich in dieser Theorie,

$$a \equiv b \bmod n$$

statt $a \sim b$ zu schreiben. Man sagt auch, daß $[a]$ die *Restklasse* von a modulo n sei.

8 Arithmetik in $\mathbb{Z}/n\mathbb{Z}$

Die Operationen "$+$" und "$\cdot$" (Addition und Multiplikation) werden in $\mathbb{Z}/n\mathbb{Z}$ wie folgt definiert.

$$[a] + [b] = [a + b],$$

$$[a] \cdot [b] = [a \cdot b],$$

wobei $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$ beliebig sind.

Sind diese Operationen "wohl definiert"? D.h. seien $c \equiv a \bmod n$ und $d \equiv b \bmod n$. (Und daher $[c] = [a]$ und $[d] = [b]$.) Ist es dann wahr, daß auch $c + d \equiv a + b \bmod n$? (D.h. $[c + d] = [a + b]$.)

Nun, da $c \equiv a \bmod n$, gilt $c - a = kn$, für ein $k \in \mathbb{Z}$. Auch gibt es ein $l \in \mathbb{Z}$ mit $d - b = ln$. Wir haben

$$(c + d) - (a + b) = (c - a) + (d - b) = kn + ln = (k + l)n.$$

Folglich ist $(c + d) - (a + b)$ teilbar durch n, und es gilt $c + d \equiv a + b \bmod n$.

Auch für die Multiplikation gilt

$$\begin{aligned} c \cdot d - a \cdot b &= c \cdot d - a \cdot d + a \cdot d - a \cdot b \\ &= (c - a) \cdot d + a \cdot (d - b) \\ &= knd + aln = (kd + al)n. \end{aligned}$$

Daher ist $c \cdot d - a \cdot b$ teilbar durch n, und folglich $c \cdot d \equiv a \cdot b \bmod n$.

[3] Manche schreiben auch $\overline{0}, \overline{1}, \ldots, \overline{n-1}$ statt $[0], [1], \ldots, [n-1]$. Wenn es von vornherein klar ist, daß wir es mit dem System $\mathbb{Z}/n\mathbb{Z}$ zu tun haben, dann könnten wir auch einfach $0, 1, \ldots, n-1$ schreiben — aber immer daran denken, daß wir Äquivalenzklassen, *nicht* Zahlen allein haben.

8.1 Division in $\mathbb{Z}/n\mathbb{Z}$

Wenn wir die Arithmetik im Rahmen der rationalen Zahlen betrachten, dann sehen wir, daß die Divisionsoperation eigentlich eine Multiplikation ist. D.h. sei $a \in \mathbb{Q}$ mit $a \neq 0$. Dann ist für jedes $b \in \mathbb{Q}$ b/a eine rationale Zahl, und zwar die Zahl

$$\frac{b}{a} = b \cdot \frac{1}{a} = b \cdot a^{-1}.$$

Hier ist a^{-1} eine bestimmte Zahl in $\mathbb{Q}$, nämlich die eindeutige Zahl, die die Gleichung

$$a \cdot a^{-1} = 1$$

erfüllt. Es ist ganz klar, daß $0 \cdot x \neq 1$ für alle mögliche $x \in \mathbb{Q}$. Daher ist die Division mit 0 nicht möglich. Aber für alle anderen Zahlen $a \neq 0$ in $\mathbb{Q}$ gibt es ein a^{-1}.

Wie ist die Situation in $\mathbb{Z}/n\mathbb{Z}$? Ist es auch wahr, daß ein $[a]^{-1}$ existiert, für alle $[a] \neq [0]$? Die Antwort: nicht immer. Es gilt nur dann, wenn n eine Primzahl ist.

Satz 10. *Sei $a \in \mathbb{Z}$ und $n \in \mathbb{N}$. Dann existiert ein $c \in \mathbb{Z}$ mit $ac \equiv 1 \bmod n$ genau dann, wenn*

$$ggt(a, n) = 1.$$

Beweis. Falls $ac \equiv 1 \bmod n$ dann heißt dies $ac - 1 = kn$, für ein $k \in \mathbb{Z}$. Oder $1 = ac - kn$. Aber dann ist jeder gemeinsame Teiler von a und n auch ein Teiler von 1. Die einzige Möglichkeit ist, daß $ggt(a, n) = 1$.

Umgekehrt, sei $ggt(a, n) = 1$. Dann (nach Übung 3.5) gibt es ganze Zahlen c,$d \in \mathbb{Z}$ mit

$$ca + dn = ggt(a, n) = 1.$$

Oder $ca - 1 = -dn$, oder $ca \equiv 1 \bmod n$. □

Wenn n eine Primzahl ist, dann ist $ggt(a, n) = 1$ für alle mögliche a zwischen 1 und $n - 1$. Daher existiert $[a]^{-1}$ in $\mathbb{Z}/n\mathbb{Z}$ für alle $[a] \neq [0]$.

Umgekehrt, falls n *keine* Primzahl ist, dann gibt es ein $a \in \{2, \ldots, n-1\}$ mit $a|n$. D.h. $n = ab$, für ein $b \in \{2, \ldots, n-1\}$. Gibt es dann ein c mit

$$ac \overset{??}{\equiv} 1 \bmod n?$$

D.h. $ac - 1 = kn$, für ein $k \in \mathbb{Z}$. Oder $1 = ac - kn = ac - kab$. Aber dann wäre a auch Teiler von 1; Unmöglich!

Daher haben wir:

Satz 11. *In $\mathbb{Z}/n\mathbb{Z}$ gibt es für* jedes $[a] \neq [0]$ *ein multiplikatives Inverses $[a]^{-1}$ dann und nur dann, wenn n eine Primzahl ist.*

Man sagt auch: $\mathbb{Z}/n\mathbb{Z}$ ist ein *Körper* genau dann, wenn n prim ist. Auch $\mathbb{Q}$ ist ein Körper.

9 Körper

Definition 9.1. Ein Körper ist eine Menge K (von "Zahlen") versehen mit zwei Operationen: '+' und '$\cdot$', d.h. Addition und Multiplikation, wobei die folgenden Bedingungen gelten.

Für die Addition:

- $a + b = b + a$, für alle a, $b \in K$.
- $a + (b + c) = (a + b) + c$, für alle a, b, und $c \in K$.
- Ein besonderes Element, genannt 0, existiert in K mit $0 + a = a$, für alle $a \in K$.
- Für jedes $a \in K$, existiert ein Element, genannt $-a$ in K, mit der Eigenschaft, daß $a + (-a) = 0$.

(Man sagt dazu, K sei eine *abelsche Gruppe* unter der Operation '+'.)

Für die Multiplikation:

- $a \cdot b = b \cdot a$, für alle a, $b \in K$.
- $a \cdot (b \cdot c) = (a \cdot b) \cdot c$, für alle a, b, und $c \in K$.
- Ein besonderes Element, genannt 1, wobei $1 \neq 0$, existiert in K mit $1 \cdot a = a$, für alle $a \in K$.
- Für jedes $a \neq 0$, existiert ein Element, genannt a^{-1} in K, mit der Eigenschaft, daß $a \cdot a^{-1} = 1$.

(Daher ist K (aber ohne das Element 0) auch eine abelsche Gruppe unter Multiplikation.)

Schließlich gibt es das Distributivgesetz:

- $a \cdot (b + c) = a \cdot b + a \cdot c$, für alle a, b, und $c \in K$.

Man könnte dann sagen, daß ein Körper ein arithmetisches System ist, wobei die "üblichen" arithmetischen Operationen vorhanden sind.

Z.B. die Menge der rationalen Zahlen $\mathbb{Q}$ ist ein Körper. Auch $\mathbb{Z}/n\mathbb{Z}$ ist ein Körper, *vorausgesetzt* n ist eine Primzahl. Andererseits ist $\mathbb{N}$ *kein* Körper. Auch $\mathbb{Z}$ ist kein Körper.

10 Die Gleichung $ax \equiv b \bmod n$

Betrachten wir nun die Gleichung $ax \equiv b \bmod n$. Hier sind sowohl $n \in \mathbb{N}$ als auch $a, b \in \mathbb{Z}/n\mathbb{Z}$ vorgegeben. Gibt es dann eine Lösung $x \in \mathbb{Z}/n\mathbb{Z}$?

Satz 12. *Sei* $d = ggt(a, n)$. *Die Gleichung* $ax \equiv b(n)$ *ist lösbar genau dann, wenn* $d|b$.

Beweis. Zunächst sei x_0 eine Lösung mit $ax_0 \equiv b \bmod n$. Da $ax_0 - b = mn$, für ein $m \in \mathbb{Z}$, gilt $b = ax_0 - mn$. Aber $d|a$ und $d|n$, daher gilt $d|b$.

Umgekehrt, sei $d|b$. Da $d = \mathrm{ggt}(a, n)$, gibt es zwei Zahlen, u, $v \in \mathbb{Z}$ mit $au + nv = d$. Sei $c = \frac{b}{d} \in \mathbb{N}$. Dann ist $a(cu) \equiv b \bmod n$, denn

$$a(cu) + ncv = \frac{aub}{d} + \frac{nvb}{d} = b\left(\frac{au + nv}{d}\right) = b\frac{d}{d} = b.$$

D.h. eine Lösung (nämlich cu) existiert. □

Eigentlich können wir noch mehr über die Menge der möglichen Lösungen sagen. Falls nämlich $d|b$, dann gibt es genau d verschiedene Lösungen, und zwar die (Äquivalenzklassen der) Zahlen

$$x_0 + k \cdot \left(\frac{n}{d}\right), \quad k = 0, \ldots, d-1$$

wobei x_0 irgendeine bestimmte Lösung ist.

Denn sei x_0 eine Lösung mit $ax_0 \equiv b \bmod n$. Aber dann ist

$$a(x_0 + k \cdot \left(\frac{n}{d}\right)) = ax_0 + k \cdot \left(\frac{a}{d}\right) n \equiv ax_0 \equiv b \bmod n$$

auch eine Lösung für alle $k \in \mathbb{Z}$. (Dies gilt, da $\frac{a}{d} \in \mathbb{N}$.)

Seien jetzt $k_1 \neq k_2$ in $\{1, \ldots, d-1\}$. Dann ist

$$\left|\left(x_0 + k_1 \cdot \left(\frac{n}{d}\right)\right) - \left(x_0 + k_2 \cdot \left(\frac{n}{d}\right)\right)\right| = \left|(k_1 - k_2)\left(\frac{n}{d}\right)\right| < n,$$

da $0 \leq k_i \leq d-1$. Folglich ist

$$x_0 + k_1 \cdot \left(\frac{n}{d}\right) \not\equiv x_0 + k_2 \cdot \left(\frac{n}{d}\right) \bmod n.$$

Daher sind die Lösungen mit k_1 bzw. k_2 echt verschieden.

Allgemein, sei x_1 irgendeine beliebige Lösung (mit $ax_1 \equiv b \bmod n$). Dann ist

$$0 = b - b \equiv a(x_0 - x_1) \bmod n$$

$$\Rightarrow n | a(x_0 - x_1) \Rightarrow \frac{n}{d} \Big| \frac{a}{d}(x_0 - x_1) \ .$$

Die Zahlen $\frac{n}{d}$ und $\frac{a}{d}$ haben keinen gemeinsamen Teiler (d ist doch der größte). Folglich ist $\frac{n}{d} | x_0 - x_1$. D.h. $x_0 - x_1 = k \cdot \frac{n}{d}$ für ein $k \in \mathbb{Z}$. Oder

$$x_1 = x_0 - k\left(\frac{n}{d}\right).$$

Aber dann gibt es ein $0 \leq k' \leq d-1$ mit

$$x_0 - k\left(\frac{n}{d}\right) \equiv x_0 - k'\left(\frac{n}{d}\right) \bmod n.$$

D.h. $(x_0 - k\frac{n}{d}) - (x_0 - k'\frac{n}{d}) = (k - k')\frac{n}{d} = mn$, für ein $m \in \mathbb{Z}$, oder $k - k' = md$. Wähle nun m so, daß $k' = k - md \in \{0, \ldots, d-1\}$.

11 Der Chinesische Restklassensatz

Sun Tsu Suan-Ching (4. Jahrhundred) hat das folgende Problem gestellt.

> *Es gibt Dinge, dessen Zahl unbekannt ist.*
> *Geteilt durch drei ist der Rest zwei.*
> *Geteilt durch fünf ist der Rest drei.*
> *Geteilt durch sieben ist der Rest zwei.*
> *Welche Zahl ist es?*

Mehr allgemein:

Satz 13. *Seien $n_1, n_2, \ldots, n_k \in \mathbb{N}$ verschiedene Zahlen, wobei $ggt(n_i, n_j) = 1$ für alle i, j mit $i \neq j$. Wähle nun k beliebige weitere Zahlen $b_1, b_2, \ldots, b_k \in \mathbb{Z}$. Dann gibt es genau eine Lösung $x \in \mathbb{Z}$ mit $0 \leq x < n_1 n_2 \cdots n_k$ zu den Gleichungen*

$$x \equiv b_i \bmod n_i$$

für alle i.

Beweis. Für jedes $i \in \{1, \ldots, k\}$ sei

$$m_i = n_1 \cdots n_{i-1} \cdot n_{i+1} \cdots n_k.$$

Dann ist für jedes i, $ggt(m_i, n_i) = 1$. (Dies folgt aus unserem Satz 2.) Nun, wegen $ggt(m_i, n_i) = 1$ folgt, daß jeweils zwei Zahlen $r_i, s_i \in \mathbb{Z}$ existieren, mit

$$r_i m_i + s_i n_i = 1.$$

Wir bezeichnen mit $l_i \in \mathbb{Z}$, für jedes i, jeweils das Produkt $l_i = r_i m_i$. Dann ist $l_i \equiv 1 \bmod n_i$, aber auch $l_i \equiv 0 \bmod n_j$ für $j \neq i$, da doch m_i die Zahl n_j als Faktor enthält. Die Zahl

$$x_0 = b_1 l_1 + \cdots + b_t l_t$$

ist dann offensichtlich eine Lösung, da $x_0 \equiv b_i \bmod n_i$ für alle i.

Sei nun $r \in \mathbb{Z}$ beliebig und sei $n = n_1 n_2 \cdots n_k$. Dann ist auch $rn \equiv 0 \bmod n_i$ für alle i, da jeweils $n_i | n$. D.h. $x_0 + rn$ ist auch eine Lösung, für alle $r \in \mathbb{Z}$. Wir können daher r so wählen, daß die Lösung $x = x_0 + rn$ in $\{0, 1, \ldots, n-1\}$ liegt.

Gegeben eine beliebige Lösung $y \in \mathbb{Z}$, dann gilt $y - x \equiv b_i - b_i \equiv 0 \bmod n_i$ für alle i. D.h. $n_i | y - x$. Da die verschiedenen n_i keine gemeinsamen Teiler haben, muß (nach dem Fundamentalsatz der Arithmetik) auch

$$n = n_1 \cdots n_k | y - x.$$

Folglich ist $y = x + rm$, für ein $r \in \mathbb{Z}$. □

11.1 Die Lösung zum Problem des Sun Tsu Suan-Ching

Es gilt

$$\begin{aligned} n_1 &= 3, \\ n_2 &= 5, \\ n_3 &= 7. \end{aligned}$$

Daher ist $n = 3 \cdot 5 \cdot 7 = 105$. Es gilt weiterhin

$$\begin{aligned} b_1 &= 2, \\ b_2 &= 3, \\ b_3 &= 2. \end{aligned}$$

Gesucht wird eine Lösung x mit $0 \leq x < 105$, wobei

$$\begin{aligned} x &\equiv 2 \bmod 3, \\ x &\equiv 3 \bmod 5, \\ x &\equiv 2 \bmod 7. \end{aligned}$$

Nun,

$$\begin{aligned} m_1 &= 35, \\ m_2 &= 21, \\ m_3 &= 15. \end{aligned}$$

Es gilt

$$\begin{aligned} 12 \cdot n_1 + (-1) \cdot m_1 &= 12 \cdot 3 + (-1) \cdot 35 = 1, \\ (-4) \cdot n_2 + 1 \cdot m_2 &= (-4) \cdot 5 + 1 \cdot 21 = 1, \\ (-2) \cdot n_3 + 1 \cdot m_3 &= (-2) \cdot 7 + 1 \cdot 15 = 1. \end{aligned}$$

Daher

$$\begin{aligned} l_1 &= -35, \\ l_2 &= 21, \\ l_3 &= 15. \end{aligned}$$

Folglich ist

$$x_0 = 2 \cdot (-35) + 3 \cdot 21 + 2 \cdot 15 = 23,$$

und hier ist $x = x_0$ schon die Lösung.

12 Die Zahl $\phi(n)$

Sei $n \in \mathbb{N}$ vorgegeben. Wir bezeichnen mit $\phi(n)$ die Anzahl der Zahlen a, wobei $1 \leq a \leq n$ und $\mathrm{ggt}(a, n) = 1$. Offensichtlich ist *immer* die 1 dabei. Folglich ist immer $\phi(n) \geq 1$. Man sagt, daß eine Zahl a mit $\mathrm{ggt}(a, n) = 1$ *relativ prim* zu n ist.

Hier ist eine Tabelle für $n = 1, \ldots, 10$, wobei die Zahlen, die zu n relativ prim sind, aufgelistet werden.

$$\begin{aligned}
1 &: 1\\
2 &: 1\\
3 &: 1,2\\
4 &: 1,3\\
5 &: 1,2,3,4\\
6 &: 1,5\\
7 &: 1,2,3,4,5,6\\
8 &: 1,3,5,7\\
9 &: 1,2,4,5,7,8\\
10 &: 1,3,7,9
\end{aligned}$$

Man beobachtet:

- Es gilt $\mathrm{ggt}(1, n) = 1$ immer.
- Es gilt $\mathrm{ggt}(n-1, n) = 1$, falls $n > 1$. D.h. $\phi(n) \geq 2$, falls $n \geq 3$.
- $\mathrm{ggt}(a, n) = 1$, für alle $1 \leq a \leq n-1$, falls n eine Primzahl ist. D.h. $\phi(n) = n-1$ für Primzahlen.

Definition 12.1. Für jedes $n \in \mathbb{N}$, sei $U(n) \subset \{1, \ldots, n\}$ die Menge der Zahlen zwischen 1 und n, die zu n relativ prim sind. Es sind also genau $\phi(n)$ Elemente in $U(n)$, für jedes n.

Satz 14. *Seien* $a, b \in U(n)$. *Dann ist* $\mathrm{ggt}(ab, n) = 1$.

Beweis. Wir brauchen nur die Primzahlfaktorisierung von ab und von n zu betrachten. Da $\mathrm{ggt}(a, n) = 1$, kommt kein Primfaktor von a in n vor. Ebenfalls ist kein Primfaktor von b ein Faktor von n. Daher gibt es keine gemeinsame Primfaktoren von ab und n. D.h. $\mathrm{ggt}(ab, n) = 1$. □

Es gilt auch:

Satz 15. *Seien* $a, b, c \in U(n)$. *Angenommen,* $a \neq b$. *Dann ist auch* $ac \not\equiv bc \bmod n$.

Beweis. Nach unserem Satz 10 gibt es ein $d \in \mathbb{Z}/n\mathbb{Z}$ mit $cd \equiv 1 \bmod n$. Falls $ac \equiv bc \bmod n$, dann gilt auch $(ac)d \equiv (bc)d \bmod n$; oder $a(cd) \equiv b(cd) \bmod n$; oder $a \equiv b \bmod n$, ein Widerspruch. □

13 Fermat's kleiner Satz

Satz 16 (Fermat). *Sei* $a \in U(n)$. *Dann gilt* $a^{\phi(n)} \equiv 1 \bmod n$.

Beweis. Seien $u_1, u_2, \ldots, u_{\phi(n)}$ die Elemente von $U(n)$. Für $a \in U(n)$ ist dann (nach Satz 14) $\mathrm{ggt}(au_i, n) = 1$, für alle $i = 1, \ldots, \phi(n)$. Nach Satz 15 sind die Äquivalenzklassen für die verschiedenen au_i alle verschieden. Für jedes i, sei etwa $v_i \equiv au_i \bmod n$, mit $1 \leq v_i < n$. Dann ist die Menge

$$\{v_1, \ldots, v_{\phi(n)}\}$$

identisch mit der Menge

$$\{u_1, \ldots, u_{\phi(n)}\},$$

nur vielleicht in einer anderen Reihenfolge aufgelistet.

Daher ist

$$\prod_{i=1}^{\phi(n)} u_i = \prod_{i=1}^{\phi(n)} v_i \equiv \prod_{i=1}^{\phi(n)} au_i = a^{\phi(n)} \left(\prod_{i=1}^{\phi(n)} u_i \right) \bmod n.$$

Sei $x = \prod_{i=1}^{\phi(n)} u_i$. Dann ist unsere Gleichung einfach

$$x \equiv a^{\phi(n)} x \bmod n.$$

Nach Satz 14 ist $ggt(x, n) = 1$. Daher (nach Satz 10) gibt es ein y mit $xy \equiv 1 \bmod n$, und wir haben

$$a^{\phi(n)} \equiv a^{\phi(n)}(xy) \equiv (a^{\phi(n)}x)y \equiv (x)y \equiv 1 \bmod n.$$

□

Falls n eine Primzahl ist, dann ist $\phi(n) = n - 1$. Folglich ist

$$2^{n-1} \equiv 1 \bmod n,$$

für alle *Primzahlen* $n > 2$. Aber was ist $2^{n-1} \bmod n$, wenn n *nicht* notwendigerweise eine Primzahl ist?

Hier ist eine kleine Tabelle

n	2^{n-1}	$2^{n-1} \bmod n$
2	2	0
3	4	1
4	8	0
5	16	1
6	32	2
7	64	1
8	128	0
9	256	4
10	512	2
11	1024	1
12	2048	8

Bisher gilt: falls n *nicht* prim, dann ist $2^{n-1} \not\equiv 1 \bmod n$. Leider ist diese Regel nicht immer gültig. Z.B. ist

$$2^{560} \equiv 1 \bmod 561.$$

Aber 561 ist *keine* Primzahl. Es gilt

$$561 = 3 \times 11 \times 17.$$

Tatsächlich ist 561 eine "Carmichaelzahl". D.h. $a^{560} \equiv 1 \bmod 561$ für alle $a \in \mathbb{N}$ mit $ggt(a, 561) = 1$.

Aber

$$\begin{aligned} 2^{560} = \; & 377396242482154135224155458098826889091692 \\ & 122041644042837620630024562416239214885208 \\ & 612672517765876754146837503076384489977058 \\ & 462992479263256143425143269604364939532697 6. \end{aligned}$$

Eine ziemlich große Zahl! Und, wie wir sehen werden, rechnet man heutzutage üblicherweise mit Zahlen von der Art

$$a^b \bmod c,$$

wobei die drei Zahlen a, b und c in der Größenordnung von 100 bis 200 Stellen sind! Wie geht das überhaupt?

14 Wie berechnet man eine Zahl wie $a^{\phi(n)} \bmod n$?

Allgemeiner, wie berechnet man $a^b \bmod c$, wobei a, b und $c \in \mathbb{N}$. Es gibt drei Fälle:

- Falls $b = 1$, dann ist $a^b \bmod c = a \bmod c$.
- Falls b ungerade, dann ist $a^b \bmod c = a \times (a^{b-1} \bmod c) \bmod c$.
- Falls b gerade, dann ist $a^b \bmod c = (a^{b/2} \bmod c) \times (a^{b/2} \bmod c) \bmod c$.

Hier ist eine rekursive C-Funktion, die diese Schritte problemlos durchführt.

```
int potenzen (int a, int b, int c)
{
    int x;
    if (b == 1) { return a % c; }
    else
    if (b % 2 == 0)
        {
            x = potenzen (a, b/2, c);
            return x * x % c;
        }
    else
    {
        x = potenzen (a, b-1,c);
        return a * x % c;
    };
};
```

Der Computer rechnet stets mit relativ kleinen Zahlen und die Anzahl der Rechenschritte ist vergleichbar mit der Anzahl der Ziffern in der Zahl b.

15 Über die Kryptographie I

Die Kryptographie ist nicht nur für Spione relevant. Jedesmal, wenn Sie etwas mit der EC-Karte (und PIN) bezahlen, werden die Informationen verschlüsselt an die Bank gesendet. Ein Dieb könnte dabei, mittels "wiretapping", die übermittelten Informationen mitlesen. Ist das ein Problem?

Stellen wir uns vor, wir wollen eine besondere Nachricht verschlüsselt übermitteln. Der Empfänger sollte diese verschlüsselte Nachricht dann entschlüssen können. Unsere Nachricht lautet

"Hallo Welt!"

Nun, es gibt viele Analphabeten in der Welt. Für solche Leute ist diese geschriebene Nachricht schon unlesbar und daher hinriechend verschlüsselt.[4] Aber leider können wir nicht immer davon ausgehen, daß die Diebe Analphabeten sind!

Eine Idee wäre, den Buchstaben Zahlen zuzuordnen. Etwa die Buchstaben $a \ldots z$ und die Zahlen $1 \ldots 26$, in dieser Reihenfolge. Unsere Nachricht würde dann lauten

"8 1 12 12 15 _ 23 5 12 20"

Diese verschlüsselte Nachricht ist schon schwierig zu lesen. Für einen Menschen mit genügend "krimineller Energie" ist die Entschlüsselung jedoch kein großes Problem.

Eine weitere Idee wäre, die einzelnen Zahlen n in unserer Nachricht zu ersetzen, etwa mit Zahlen der Art $n + a \bmod 26$, wobei a eine weitere Zahl ist. Z.B. wenn $a = 11$ ist, dann lautet die Nachricht

"19 12 23 23 0 _ 8 16 23 5"

[4] Ich befürchte, daß auch dieses Skript manchen Teilnehmern wie eine verschlüsselte Nachricht vorkommt. Es ist sehr unwahrscheinlich, daß der Nachbar, mit dem gerade geplaudert wird, einen geeigneten Entschlüsselungsalgorithmus hat!

Leider ist diese Methode auch allgemein bekannt. Man braucht nur alle 26 Möglichkeiten für die Zahl a zu probieren, um zu sehen, ob etwas Vernünftiges herauskommt.

Schließlich gibt es die Idee, die Zahl a laufend zu verändern mit einer Kette von verschiedenen a's. Aber welche Kette von a's sollte man nehmen? Eine Möglichkeit wäre, einen allgemein bekannten Text aussuchen, um die darin enthaltenen Buchstaben als Zahlenkette zu benutzen. Zum Beispiel fängt Goethe's "Die Leiden des jungen Werther" wie folgt an:

Wie froh bin ich, dass ich weg bin!

Dadurch haben wir die Zahlenkette

"23 9 5 6 18 15 8 2 9 14 9 3 8 4 1 19 19 9 3 8 23 5 7 2 9 14"

Unsere Nachricht würde dann lauten

"5 10 17 18 7 _ 12 13 14 3"

D.h. die erste Zahl ist $8 + 23 \equiv 5 \bmod 26$. Die zweite Zahl ist $1 + 9 \equiv 10 \bmod 26$. Und so weiter.
Diese verschlüsselte Nachricht ist fast vollständig unlesbar!

Trotzdem ist diese Methode ungeeignet für die Übermittlung von EC-Karten Informationen bei elektronischen Geldüberweisungen. Warum?

- Vielleicht wird ein "Hacker" herausfinden, daß Goethe's "Die Leiden des jungen Werther" hinter allen Geldüberweisungen steckt!
- Jedes EC-Kartenlesegerät enthält die Information, die für die Verschlüsselung nötig ist. Aber diese Information kann auch für die Entschlüsselung benutzt werden.
- Falls ein neuer Schlüsseltext — anstelle von Goethe's "Die Leiden des jungen Werther" — eingeführt wird, muß dieser an alle EC-Kartenlesegeräte übermittelt werden, wodurch auch der neue Text wieder allgemein bekannt werden könnte.

16 Über die Kryptographie II

Die moderne Kryptographie benutzt einige Ideen aus der elementaren Zahlentheorie. Dadurch wird ein praktisches, absolut sicheres System aufgebaut.

Zuerst stellt Folgendes man fest:

- Es gibt sehr viele Primzahlen. Es ist auch relativ leicht (für einen Computer), Primzahlen in der Größenordnung von circa 100 Ziffern zu finden.
- Es ist dagegen sehr schwierig — in der Praxis eigentlich unmöglich — große Zahlen mit circa 200 Ziffern, die *nicht* prim sind, zu faktorisieren.

16.1 Ein öffentlicher Schlüssel wird erzeugt

1. Zuerst werden zwei verschiedene große Primzahlen p und q mit $p \neq q$ gefunden. Die Zahl n ist das Produkt $n = pq$.
2. Nach unserer Übung wissen wir, daß $\phi(n) = (p-1)(q-1)$.
3. Sei e irgendeine (relativ große) Zahl mit $1 \leq e < \phi(n)$, wobei $\mathrm{ggt}(e, \phi(n)) = 1$. (Hier gibt es *sehr* viele verschiedene Möglichkeiten!)
4. Sei $1 \leq d < \phi(n)$ die Zahl mit $ed \equiv 1 \bmod \phi(n)$. (Siehe wieder unser Satz 10.)
5. Nun haben wir alle nötigen Informationen. Die Zahlen n und e werden veröffentlicht. (Auch jeder EC-Kartendieb darf diese Zahlen sehen!) Die Zahl d wird geheim gehalten. Die Primzahlen p und q werden nicht mehr benötigt.

16.2 Der Verschlüsselungsalgorithmus

1. Unser Text lautet “Hallo Welt!”. Zahlenmäßig heißt dies: “8 1 12 12 15 _ 23 5 12 20”. Wir können diese Zahlen in Blöcke zusammenfassen, um größere Zahlen zu haben, etwa:

$$8 \quad 1 \quad 12 \quad 12 \quad 15 \quad \_ \quad 23 \quad 5 \quad 12 \quad 20 \quad \longrightarrow \quad 0801121215, \quad 23051220 \; = \; K_1, \; K_2$$

   (Es ist zu beachten, daß stets $0 \leq K_i < n$ gelten soll für die Blöcke K_i.)

2. Nun wird Block für Block verschlüsselt. Sei K ein Block. Die verschlüsselte Version ist einfach die Zahl

$$V = K^e \bmod n.$$

16.3 Der Entschlüsselungsalgorithmus

- Um die verschlüsselte Zahl V zu entschlüsseln; d.h. um die Zahl K wieder zu gewinnen, braucht man die “geheime” Zahl d. Es gilt nämlich

$$K = V^d \bmod n.$$

16.4 Warum funktioniert es?

D.h. ist es wirklich wahr, daß

$$K = V^d \bmod n$$

immer?

Nun, da $ed \equiv 1 \bmod \phi(n)$, gilt

$$ed - 1 = u\phi(n), \quad \text{oder} \quad ed = 1 + u\phi(n),$$

für irgendein $u \in \mathbb{Z}$.

Es gibt zwei Fälle.

1. Falls $ggt(K, n) = 1$, dann ist

$$V^d = (K^e)^d = K^{ed} = K^{1+u\phi(n)} = K \cdot K^{u\phi(n)} = K \cdot \left(K^{\phi(n)}\right)^u.$$

   Aber nach Fermat's kleinem Satz (unser Satz 16) gilt $K^{\phi(n)} \equiv 1 \bmod n$. Daher

$$V^d = K \cdot \left(K^{\phi(n)}\right)^u \equiv K \cdot 1^u = K \bmod n.$$

2. Falls $ggt(K, n) \neq 1$, dann benutzen wir den Chinesischen Restwertsatz. Es gilt, entweder $p|K$ oder $q|K$. Sagen wir $p|K$. (Unser Block K ist eine Zahl nicht größer als n. Daher ist $q \not| K$. D.h. $ggt(K, q) = 1$.) Nun, einerseits gilt $K \equiv 0 \bmod p$, d.h.

$$V^d = K^{ed} \equiv 0^{ed} = 0 \equiv K \bmod p.$$

   Andererseits gilt

$$V^d = K^{ed} = K^{1+u\phi(n)} = K \cdot K^{u\phi(n)} = K \cdot K^{u(p-1)(q-1)} = K \cdot \left(K^{q-1}\right)^{u(p-1)} \equiv K \cdot 1^{u(p-1)} = K \bmod q.$$

   Da $n = pq$ gilt nach dem Chinesischen Restwertsatz

$$V^d \equiv K \bmod n.$$