Universität Regensburg
Fakultät für Mathematik

Schnupperstudium 2019
4. September 2019

Kryptographie, Rechnen modulo n und wie findet man eigentlich grosse Primzahlen?

Stefan Friedl

1. Rechnen modulo n

Natürliche und ganze Zahlen kann man addieren und multiplizieren, und hierbei gelten gewisse Regeln, die uns jetzt nach vielen Schuljahren völlig selbstverständlich sind. Beispielsweise gilt immer

$$\begin{array}{rcll} a+b & = & b+a & \text{Kommutativgesetz} \\ (a+b)+c & = & a+(b+c) & \text{Assoziativgesetz} \\ a(b+c) & = & ab+ac & \text{Distributivgesetz.} \end{array}$$

Manchmal kann es aber sinnvoll sein, auch mit anderen Zahlensystemen zu arbeiten. Beispielsweise möchten wir gerne folgende Frage möglichst schnell beantworten

Frage: *Heute ist Mittwoch. Was für ein Wochentag ist in 33 Tagen?*

Bei den Wochentagen kommt es natürlich auf 7 Tage hin- oder her nicht drauf an. Also ist

$$\begin{array}{rcl} \text{Wochentag in 33 Tagen} & = & \text{Wochentag } \underbrace{4\cdot 7+5}_{=33} \text{ Tage nach Mittwoch} \\ & = & \text{Wochentag 5 Tage nach Mittwoch} \\ & = & \text{Montag.} \end{array}$$

Wir können die Lösung der Aufgabenstellung nun formalisieren. Es sei n im Folgenden eine beliebige Zahl, z.B. $n=7$. Für eine beliebige andere natürliche Zahl k schreiben wir nun

$$k \,\text{modulo}\, n \;:=\; \text{der Rest von } k \text{ geteilt durch } n.$$

Beispielsweise ist

$$\begin{array}{ccccc} 33 \text{ modulo } 7 & = & 5 & \text{und} & 35 \text{ modulo } 7 \;=\; 0. \\ & \uparrow & & & \uparrow \\ & \text{denn } 33 = 4\cdot 7+5 & & & \text{denn } 35 = 5\cdot 7+0 \end{array}$$

Das Schöne am Rechnen modulo n ist, dass die gleichen Regeln wie zuvor gelten. Beispielsweise ist

$$\begin{array}{ccccc} 19\cdot 3+19\cdot 4 \text{ modulo } 7 & = & 19\cdot(3+4) \text{ modulo } 7 & = & 19\cdot 0 \text{ modulo } 7 = 0 \text{ modulo } 7. \\ & \uparrow & & \uparrow & \\ & \text{Distributivgesetz} & & \text{denn } 3+4=0 \text{ modulo } 7 & \end{array}$$

Wir können nun unsere ursprüngliche Aufgabe in dieser Sprache formulieren. Wir weisen dazu den Wochentagen die Zahlen $0, \ldots, 6$ wie folgt zu:

Montag	0	Freitag	4
Dienstag	1	Samstag	5
Mittwoch	2	Sonntag	6
Donnerstag	3.		

Mit dieser Übersetzung ist die ursprüngliche Frage also:

Frage: *Was ist* $2 + 33$ *modulo* 7*?*

Diese Frage kann man nun leicht lösen, denn

$$2 + 33 \text{ modulo } 7 \;=\; 35 \text{ modulo } 7 \;=\; 0.$$

Die 0 entspricht gerade Montag, also erhalten wir, dass in 33 Tagen ein Montag ist.

2. Kryptographie

Die Kryptographie beschäftigt sich mit der Frage, wie man einen Text verschlüsseln und dann auch wieder entschlüsseln kann.

Die einfachste und wohl bekannteste Verschlüsselungsmethode geht angeblich auf Cäsar zurück: man verschiebt einfach jeden Buchstaben im Alphabet um "eins nach rechts". Die Verschlüsselung ist also gegeben durch

```
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
 ↘ ↘ ↘ ↘ ↘ ↘ ↘ ↘ ↘ ↘ ↘ ↘ ↘ ↘ ↘ ↘ ↘ ↘ ↘ ↘ ↘ ↘ ↘ ↘ ↘ ↘
A B C D E F G H I J K L M N O P Q R S T U V W X Y Z
```

Den letzten Buchstaben Z schickt man dann natürlich auf A. Hier ist ein Beispiel:

ursprünglicher Text	`DIES IST EIN SEHR EINFACHER SCHLUESSEL`
verschlüsselter Text	`EJFT JTU FJO TFIS FJOGBDIFS TDIMVFTTFM`

Die Entschlüsselung ist dann dadurch gegeben, dass wir jeden Buchstaben im Alphabet um "eins nach links" verrutschen.

Wir können diesen Verschlüsselungsalgorithmus wieder in die Sprache von "modulo n" übersetzen. Im vorherigen Beispiel hatten wir den Wochentagen die Zahlen 0 bis 6 zugeordnet. Jetzt ordnen wir den 26 Buchstaben die Zahlen 0 bis 25 auf die offensichtliche Weise zu:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

Der Verschlüsselungsalgorithmus ist dann gegeben durch die Funktion[1]

$$n \quad \mapsto \quad n + 1 \;\text{ modulo } 26.$$

[1] An der Universität verwendet man hier lieber das Wort Abbildung als das Wort Funktion, aber das kann uns jetzt egal sein.

Der Entschlüsselungsalgorithmus ist dann natürlich gegeben durch die Funktion

$$n \quad \mapsto \quad n-1 \ \text{ modulo } 26.$$

Man kann dieses Spiel natürlich auch leicht abändern, beispielsweise könnte man genauso gut um 5 Buchstaben nach links verschieben.

Es gibt aber auch noch andere Verschlüsselungsmethoden. Wir können ja nicht nur "modulo 26" addieren, sondern auch multiplizieren. Betrachten wir beispielsweise die Funktion

$$n \quad \mapsto \quad 3 \cdot n \ \text{ modulo } 26.$$

Ausgeschrieben erhalten wir also die Funktion

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
0	3	6	9	12	15	18	21	24	1	4	7	10	13	16	19	22	25	2	5	8	11	14	17	20	23

In Buchstaben übersetzt ergibt uns das

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
A	D	G	J	M	P	S	V	Y	B	E	H	K	N	Q	T	W	Z	C	F	I	L	O	R	U	X

Wir erhalten beispielsweise folgende Verschlüsselung:

ursprünglicher Text	DIESER SCHLUESSEL IST KOMPLIZIERTER ALS DER VORHERIGE
verschlüsselter Text	JYMCMZ CGVHIMCCMH YCF EQKTHYXYMZFMZ AHC JMZ LQZVMZYSM

Es stellt sich hierbei die Frage, wie man denn die Entschlüsselung am einfachsten beschreiben kann. Wir werden dieser Frage in den Übungsaufgaben nachgehen.

Wir haben also gerade jeden Buchstaben mit drei multipliziert. Wie schaut's aus, wenn wir anstattdessen mit zwei multipliziert hätten? Betrachten wir also die Funktion

$$n \quad \mapsto \quad 2 \cdot n \text{ modulo } 26.$$

Ausgeschrieben erhalten wir also die Funktion

0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
0	2	4	6	8	10	12	14	16	18	20	22	24	0	2	4	6	8	10	12	14	16	18	20	22	24

In Buchstaben übersetzt ergibt uns das

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓	↓
A	C	E	G	I	K	M	O	Q	S	U	W	Y	A	C	E	G	I	K	M	O	Q	S	U	W	Y

Wir erhalten beispielsweise folgende Verschlüsselung:

ursprünglicher Text	DIESER SCHLUESSEL TAUGT NIX
verschlüsselter Text	GQIKII KEOWOIKKIW MAOMM AQU

Diese "Verschlüsselung" ist allerdings ziemlich nutzlos, denn man kann aus dem verschlüsselten Text den ursprünglichen Text nicht mehr herleiten, nachdem in diesem Fall sowohl dem Buchstaben `E` als auch dem Buchstaben `R` der Buchstabe `I` zugewiesen wird.

Es stellt sich also folgende Frage.

Frage 2.1. *Für welche k ist die Funktion*

$$n \mapsto k \cdot n \quad \textit{modulo } 26$$

eine brauchbare Verschlüsselung? Mit anderen Worten, für welche k folgt aus $a \neq b$ auch $k \cdot a \neq k \cdot b \,\text{modulo}\, 26$?

Bevor wir die Frage genauer betrachten führen wir erst einmal noch eine Definition ein.

Definition. Eine Funktion $f\colon A \to B$ von einer Menge A zu einer Menge B heißt *injektiv*, wenn für $a \neq a'$ aus A auch folgt, dass $f(a) \neq f(a')$.

Beispiele.

(1) Die Funktion
$$\begin{array}{rcl} f\colon A = \{0,\ldots,25\} & \to & B = \{0,\ldots,25\} \\ n & \mapsto & 3 \cdot n \mod 26 \end{array}$$
ist injektiv. Dies sieht man sofort anhand der obigen Tabelle, denn zwei verschiedenen Zahlen aus $\{0,\ldots,25\}$ werden durch diese Funktion immer auch zwei verschiedene Zahlen aus $\{0,\ldots,25\}$ zugeordnet.

(2) Die Funktion
$$\begin{array}{rcl} f\colon A = \{0,\ldots,25\} & \to & B = \{0,\ldots,25\} \\ n & \mapsto & 2 \cdot n \mod 26 \end{array}$$
ist nicht injektiv, denn $f(13) = f(0) = 0$.

(3) Die Funktion
$$\begin{array}{rcl} f\colon A = \mathbb{R} & \to & B = \mathbb{R} \\ x & \mapsto & x^2 \end{array}$$
ist nicht injektiv, denn $f(-2) = 4 = f(2)$.

Manchmal läßt sich eine Frage wie Frage 2.1 einfacher beantworten, wenn man gleich versucht eine allgemeinere Frage zu beantworten. Dies klingt vielleicht eigenartig, aber der Grund ist, dass man sich bei einer allgemeineren Frage auf das Wesentliche konzentriert und nicht auf das Unwesentliche.

Folgende Frage ist nun eine Verallgemeinerung von Frage 2.1.

Frage 2.2. *Es sei $m \in \mathbb{N}$. Für welche $k \in \{0,\ldots,m-1\}$ ist die Funktion*

$$\begin{array}{rcl} A = \{0,\ldots,m-1\} & \to & B = \{0,\ldots,m-1\} \\ n & \mapsto & k \cdot n \mod m \end{array}$$

injektiv?

Wenn man etwas mit dem Beispiel "modulo 26" oder auch mit anderen Beispielen umherspielt, dann kommt irgendwann der Verdacht auf, dass die Antwort davon abhängt, ob k und m einen gemeinsamen Teiler haben, oder nicht. Der folgende Satz besagt, dass dies in der Tat der Fall ist.

Satz 2.3. *Es sei $m \in \mathbb{N}$ und es sei $k \in \{0, \dots, m-1\}$. Dann sind die folgenden beiden Aussagen äquivalent:*

(1) *k ist teilerfremd zu m,*
(2) *die Funktion*

$$\begin{array}{rcl} A = \{0, \dots, m-1\} & \to & B = \{0, \dots, m-1\} \\ n & \mapsto & k \cdot n \ \text{ modulo } \ m \end{array}$$

ist injektiv.

Für den Beweis von Satz 2.3 benötigen wir folgendes Lemma.

Lemma 2.4. *Es seien $m, k, r \in \mathbb{N}$. Wir nehmen an, dass $m | k \cdot r$. Wenn m und k teilerfremd sind, dann gilt schon $m | r$.*

Beweis von Lemma 2.4. Es sei $m = p_1^{n_1} \cdot \dots \cdot p_r^{n_r}$ die Primfaktorzerlegung von m. Der Faktor $p_i^{n_i}$ kann nicht k teilen, denn m und k sind nach Voraussetzung teilerfremd. Also muss der Faktor $p_i^{n_i}$ den zweiten Faktor r teilen. Nachdem dies für alle Faktoren der Fall ist folgt, dass $m | r$. $\square$

Beweis von Satz 2.3. Wir zeigen zuerst "(1) $\Rightarrow$ (2)". Wir nehmen also an, dass k teilerfremd zu m ist. Es seien $a, b \in \{0, \dots, m-1\}$. Wir müssen zeigen, dass gilt

$$a \neq b \ \text{ modulo } \ m \quad \Longrightarrow \quad k \cdot a \neq k \cdot b \ \text{ modulo } \ m.$$

Diese Aussage ist äquivalent zur Aussage

$$k \cdot a = k \cdot b \ \text{ modulo } \ m \quad \Longrightarrow \quad a = b \ \text{ modulo } \ m.$$

Diese zweite Aussage beweisen wir nun wie folgt:

$$\begin{array}{l} k \cdot a = k \cdot b \ \text{ modulo } \ m \implies k \cdot a - k \cdot b = 0 \ \text{ modulo } \ m \implies k \cdot (a-b) = 0 \ \text{ modulo } \ m \\ \qquad \implies m | k \cdot (a-b) \underset{\uparrow}{\implies} m | (a-b) \implies a = b \ \text{ modulo } \ m. \end{array}$$

folgt aus Lemma 2.4, und der Voraussetzung, dass m and k teilerfremd sind

Wir zeigen nun "(2) $\Rightarrow$ (1)". Wir führen einen indirekten Beweis durch. D.h. wir zeigen, dass wenn k nicht teilerfremd zu m ist, dann ist die Funktion nicht injektiv.

Wir nehmen nun also an, dass k nicht teilerfremd zu m ist. Es sei $x = \mathrm{ggT}(m, k)$. Nach Voraussetzung ist $x > 1$. Wir schreiben nun $k = xy$ und $m = xz$ mit $y, z \in \mathbb{N}$. Nachdem $x > 1$ gilt $z \in \{1, \dots, m-1\}$, d.h. es ist

$$z \ \neq \ 0 \ \text{ modulo } \ m.$$

Andererseits gilt

$$k \cdot z \ = \ \underbrace{xy}_{=k} z \ = \ y \cdot \underbrace{xz}_{=m} \ = 0 \ \text{modulo}\, m \ = \ k \cdot 0 \ \text{modulo}\, m.$$

Also ist Multiplikation mit k nicht injektiv. □

3. Injektive und surjektive Funktionen

Wenn wir modulo m rechnen, dann können wir problemlos addieren, subtrahieren und multiplizieren. Man kann sich nun fragen, wann es bezüglich der Multiplikation ein inverses Element gibt.

Frage 3.1. *Es sei $m \in \mathbb{N}$. Für welche $k \in \{1, \ldots, m-1\}$ gibt es ein $l \in \{0, \ldots, m-1\}$ mit*

$$k \cdot l \;=\; 1 \;\text{ modulo }\; m?$$

Beispiele. Es sei wiederum $m = 26$.

(1) Wir haben im vorherigen Kapitel gesehen, dass es zu $k = 3$ solch ein l gibt, nämlich $l = 9$.
(2) Andererseits hatten wir im vorherien Kapitel auch gesehen, dass es für $k = 2$ kein solches l gibt.

Es drängt sich also etwas der Verdacht auf, dass die Antwort zu Frage 3.1 vielleicht die Gleiche ist wie zu Frage 2.2. Bevor wir Frage 3.1 beantworten können, müssen wir noch einen weiteren Begriff einführen.

Definition. Es sei $f\colon A \to B$ eine Funktion von einer Menge A zu einer Menge B.

(1) Wir hatten gerade eingeführt, dass f *injektiv* heißt, wenn für $a \neq a'$ aus A folgt, dass auch $f(a) \neq f(a')$.
(2) Wir sagen nun, dass f *surjektiv* ist, wenn es zu jedem $b \in B$ ein $a \in A$ mit $f(a) = b$ gibt.

Bemerkung. Eine Funktion, welche sowohl injektiv als auch surjektiv ist, wird normalerweise *bijektiv* genannt.

Beispiele.

(1) Die Tabelle aus dem vorherigen Kapitel zeigt, dass die Funktion

$$\begin{array}{rcl} f\colon A = \{0, \ldots, 25\} & \to & B = \{0, \ldots, 25\} \\ n & \mapsto & 3 \cdot n \;\text{ modulo }\; 26 \end{array}$$

injektiv und surjektiv ist.
(2) Die Funktion

$$\begin{array}{rcl} g\colon A = \{0, \ldots, 25\} & \to & B = \{0, \ldots, 25\} \\ n & \mapsto & 2 \cdot n \;\text{ modulo }\; 26 \end{array}$$

ist weder injektiv noch surjektiv. Wir hatten oben schon gesehen, dass die Funktion nicht injektiv ist. Zudem folgt aus der Tabelle aus Kapitel 2, dass es zu $b = 1$ keine Zahl a mit $2 \cdot a = 1 \,\text{modulo}\, 26$ gibt, d.h. die Funktion g ist nicht surjektiv.

(3) Die Funktion

$$\begin{array}{rcl} A = \mathbb{N}_0 & \to & B = \mathbb{N}_0 \\ n & \mapsto & n+1 \end{array}$$

ist injektiv aber nicht surjektiv, denn für $b = 0$ gibt es kein $a \in \mathbb{N}_0$ mit $f(a) = 0$.

(4) Die Funktion

$$\begin{array}{rcl} A = \mathbb{R} & \to & B = [-1, 1] \\ x & \mapsto & \sin(x) \end{array}$$

ist surjektiv[2] aber nicht injektiv, denn es ist $\sin(\pi) = \sin(0)$.

Wir sehen also in den Beispielen, dass injektiv und surjektiv unabhängige Begriffe sind. Andererseits drängt sich der Verdacht auf, dass die Funktion $n \mapsto k \cdot n \operatorname{modulo} m$ injektiv ist, genau dann, wenn die Funktion surjektiv ist.

Dies ist in der Tat der Fall. Für die Formulierung des nächsten Satzes benötigen wir noch die Notation, dass wir für eine endliche Menge A mit $\#A$ die Anzahl der Elemente bezeichnen. Beispielsweise gilt

$$\#\{0, \ldots, m-1\} \;=\; \#\{1, \ldots, m\} \;=\; m.$$

Satz 3.2. *Es sei $f\colon A \to B$ eine Funktion zwischen zwei endlichen Mengen A und B. Wenn $\#A = \#B$, dann gilt:*

$$f \text{ ist injektiv} \quad \Longleftrightarrow \quad f \text{ ist surjektiv.}$$

Bemerkung. Eigentlich ist die Aussage von Satz 3.2 ganz logisch. Nehmen wir an, sie organisieren ein Essen mit n Gästen und besitzen einen Tisch mit n Stühlen. Wir bezeichnen mit A die Menge der Gäste und mit B die Menge der Stühle. Eine Funktion $f\colon A \to B$ ist dann nichts anderes als ein Sitzplan. Die Funktion f ist injektiv, wenn verschiedene Gäste auf verschiedenen Stühlen sitzen, und die Funktion f ist surjektiv, wenn jeder Stuhl belegt ist. In diesem Fall ist es klar, dass f "injektiv" ist, genau dann, wenn f surjektiv ist.

Beweis. Wir beweisen nur die Richtung "$\Rightarrow$" des Satzes. Der Beweis der Rückrichtung ist fast wort-wörtlich der Gleiche: wir müssen im Folgenden nur die Wörter "injektiv" und "surjektiv" vertauschen.

Wir beweisen nun die Richtung "$\Rightarrow$" per Induktion nach $\#A = \#B$. Wenn $\#A = \#B = 1$, dann besitzen sowohl A als auch B jeweils nur ein Element a und ein Element b. Es gibt dann nur eine Funktion von A nach B, nämlich $f(a) = b$. Diese Funktion ist natürlich surjektiv.

Nehmen wir nun an, dass die Aussage für alle Mengen mit $\#A = \#B = k$ gilt. Es sei nun $f\colon A \to B$ eine injektive Funktion zwischen zwei Mengen A und B mit $\#A = \#B = k+1$. Es sei $a \in A$. Wir setzen $b = f(a)$. Dann ist die Einschränkung von f auf $f\colon A\backslash\{a\} \to B\backslash\{b\}$ weiterhin injektiv. Nachdem wir aus A und B jeweils ein Element rausgenommen haben, besitzen die

[2]Hier ist es natürlich wichtig, dass $B = [-1, 1]$. Die Funktion

$$\begin{array}{rcl} A = \mathbb{R} & \to & B = \mathbb{R} \\ x & \mapsto & \sin(x) \end{array}$$

ist *nicht surjektiv*, denn für $b = 2 \in \mathbb{R}$ gibt es kein $a \in \mathbb{R}$ mit $\sin(a) = 2$.

Mengen $A \setminus \{a\}$ und $B \setminus \{b\}$ jeweils k Elemente. Also ist die Funktion $f\colon A \setminus \{a\} \to B \setminus \{b\}$ nach Induktionsvoraussetzung surjektiv. Aber dann ist auch $f\colon A \to B$ surjektiv.[3] □

Wir können nun Frage 3.1 beantworten.

Satz 3.3. *Es sei $m \in \mathbb{N}$ und es sei $k \in \{0, \dots, m-1\}$. Dann sind die folgenden drei Aussagen äquivalent:*

(1) *k ist teilerfremd zu m,*
(2) *die Funktion*

$$\begin{array}{rcl} A = \{0, \dots, m-1\} & \to & B = \{0, \dots, m-1\} \\ n & \mapsto & k \cdot n \mod m \end{array}$$

ist surjektiv,
(3) *es gibt eine Zahl $l \in \{1, \dots, m-1\}$ mit*

$$k \cdot l \;=\; 1 \mod m.$$

Beweis. Es sei $m \in \mathbb{N}$ und es sei $k \in \{0, \dots, m-1\}$. Die Äquivalenz von (1) und (2) folgt sofort aus Satz 2.3 und aus Satz 3.2. Es ist klar, dass (2) $\Rightarrow$ (3).[4] Zudem folgt aus (3) auch (2), denn nehmen wir an es gibt ein $l \in \{1, \dots, m-1\}$ mit $k \cdot l = 1 \operatorname{modulo} m$. Dann gilt für jedes $b \in \{0, \dots, m-1\}$, dass $k \cdot (lb) = b \operatorname{modulo} m$. □

Wenn k und m teilerfremd sind, dann besagt also Satz 3.3, dass es ein l mit $k \cdot l = 1 \operatorname{modulo} m$ gibt. Allerdings gibt der Satz, und auch der Beweis, keinen Hinweis darauf, wie man den nun solch ein l finden kann. Es stellt sich also folgende Frage:

Frage 3.4. *Es seien k und m teilerfremde Zahlen. Wie kann man aus k und m ein l bestimmen, so dass*

$$k \cdot l \;=\; 1 \mod m?$$

4. Primzahlen

Verschlüsselungsalgorithmen spielen im Internet eine wichtige Rolle. Beispielsweise will man mit Kreditkarten zahlen können, ohne dass beim Verschicken der Kreditkartennummer jemand diese abfangen kann. Die verwendeten Algorithmen sind natürlich weniger naiv als die im Kapitel 1 genannten, aber sie basieren auch auf den Tricks der "elementaren Zahlentheorie". Einer der sichersten Algorithmen nennt sich RSA-Algorithmus. Dieser ist zu lange um ihn in dieser kurzen Vorlesung zu erläutern, er ist aber im Prinzip so einfach, dass man ihn mit Schulkenntnissen verstehen kann. Details kann man, wie üblich, auf Wikipedia finden

`https://de.wikipedia.org/wiki/RSA-Kryptosystem`

Um den RSA-Algorithmus zu verwenden benötigt man sehr große Primzahlen, mit etwa 100 Stellen. Es stellt sich also folgende Frage:

[3] In der Tat, denn sei $b' \in B$. Wenn $b' = b$, dann ist $f(a) = b'$. Wenn $b \neq b'$, dann gibt es ein $a' \in A \setminus \{a\}$ mit $f(a') = b'$.

[4] In der Tat, denn "surjektiv" bedeutet, dass es zu jedem $b \in \{0, \dots, m-1\}$ ein a mit $k \cdot a = b \operatorname{modulo} m$ gibt. Für $b = 1$ erhalten wir gerade die gewünschte Aussage.

Frage 4.1. *Wie kann man* schnell *feststellen, ob eine beliebige 100-stellige Zahl eine Primzahl ist?*

Der übliche Schulalgorithmus ist wie folgt: man überprüft, ob die gegebene Zahl n durch 2 teilbar ist, dann durch 3, dann durch 5, dann durch 7 usw. Dieser Algorithmus ist allerdings unglaublich langsam. Wenn n eine Primzahl ist mit 100 Stellen, dann würde der Schulalgorithmus länger als die Lebensdauer des Universums brauchen, um zu zeigen, dass n in der Tat eine Primzahl ist.

Zum Glück gibt's in der Praxis einen deutlich schnelleren Algorithmus. Der Mathematiker Fermat hat im 17. Jahrhundert folgendes Theorem bewiesen.

Kleiner Fermatscher Satz. *Es sei p eine Primzahl und es sei $a \in \{1, \ldots, p-1\}$. Dann gilt*

$$a^{p-1} \;=\; 1 \mod p.$$

Betrachten wir beispielsweise die Primzahl $p = 7$ und $a = 2$, dann ist in der Tat

$$2^{p-1} \;=\; 2^6 \;=\; 64 \;=\; 7 \cdot 9 + 1 \;=\; 1 \mod 7.$$

Andererseits ist für $n = 6$ und $a = 2$

$$2^{n-1} \;=\; 2^5 \;=\; 32 \;=\; 2 \;\neq\; 1 \mod 6.$$

Nach dem kleinen Fermatschen Satz ist also $n = 6$ keine Primzahl. Das war uns natürlich auch so klar, aber mithilfe vom kleinen Fermatschen Satz kann man in der Praxis innerhalb von Sekunden mit an Sicherheit grenzender Wahrscheinlichkeit bestimmen, ob eine 100-stellige Zahl eine Primzahl ist oder nicht.

Genauer gesagt, wenn n eine beliebige Zahl ist, dann kann man erstaunlich schnell 2^{n-1} modulo n ausrechnen. Wenn das Ergebnis ungleich 1 ist, dann ist n keine Primzahl. Wenn jedoch das Ergebnis gleich 1 ist, dann ist n zwar nicht notwendigerweise eine Primzahl[5], aber dennoch mit sehr großer Wahrscheinlichkeit eine Primzahl.

Zum Beispiel, wenn n eine 100-stellige Zahl ist mit $2^{n-1} = 1 \bmod n$, dann ist die Wahrscheinlichkeit, dass n *keine Primzahl* höchstens 10^{-12}. D.h. die Fehlerwahrscheinlichkeit liegt bei höchstens einem Billionstel.

Beweis. Es sei also p eine Primzahl und und es sei $a \in \{1, \ldots, p-1\}$. Nachdem p eine Primzahl ist, und nachdem $a \in \{1, \ldots, p-1\}$ folgt, dass a und p teilerfremd ist. Also folgt aus Satz 2.3 und aus Satz 3.3, dass die Funktion

$$\begin{array}{rcl} A = \{1, \ldots, p-1\} & \to & B = \{1, \ldots, p-1\} \\ n & \mapsto & a \cdot n \mod p \end{array}$$

injektiv und surjektiv ist. Mit anderen Worten gilt folgende Aussage:

[5]Beispielsweise ist $2^{561} = 2 \mod 561$, obwohl $561 = 3 \cdot 11 \cdot 17$ keine Primzahl ist. Mehr Details dazu kann man auf

`https://de.wikipedia.org/wiki/Carmichael-Zahl`

finden.

(∗) Jede Zahl $b \in \{1, \ldots, p-1\}$ ist von der Form $a \cdot n$ modulo p für genau ein einziges $a \in \{1, \ldots, p-1\}$.

Wir führen nun folgende einfache Rechnung modulo p aus:

$$a^{p-1} \cdot (1 \cdot 2 \cdot \cdots \cdot (p-1)) \overset{\text{Ausklammern und Umsortieren}}{\downarrow} = \underbrace{(a \cdot 1) \cdot (a \cdot 2) \cdot \cdots \cdot (a \cdot (p-1))}_{\substack{\text{nach } (*) \text{ tauchen hier, modulo } p, \text{ alle Zahlen} \\ 1, \ldots, p-1 \text{ genau einmal als Faktor auf}}} = \text{Produkt der Zahlen zwischen 1 und } p-1 \text{ modulo } p.$$

Zusammengefasst gilt also

$$a^{p-1} \cdot (1 \cdot 2 \cdot \cdots \cdot (p-1)) = 1 \cdot (1 \cdot 2 \cdot \cdots \cdot (p-1)) \text{ modulo } p$$

Die Zahl $1 \cdot 2 \cdot \cdots \cdot (p-1)$ ist teilerfremd zu p. Es folgt nun aus Satz 2.3, dass

$$a^{p-1} = 1 \text{ modulo } p.$$

Wenn m eine Primzahl ist dann können wir nun eine Antwort zu Frage 3.4 geben. □

Korollar 4.2. *Es sei p eine Primzahl und $k \in \{1, \ldots, p-1\}$. Wir setzen $l := k^{p-2}$. Dann ist*

$$k \cdot l = 1 \text{ modulo } p.$$

Beweis. Es ist

$$k \cdot l = k \cdot k^{p-2} = k^{p-1} \overset{\text{der kleine Fermatsche Satz}}{\uparrow} = 1 \text{ modulo } p.$$

□

Für beliebiges m gibt es ebenfalls verschiedene Algorithmen um k zu bestimmen. Man kann dies mit einer Abwandlung von Korollar 4.2 bewerkstelligen oder mit einer geschickten Anwendung des euklidischen Algorithmus.