Euler's digitale Unterschriften

Kurzvorlesung im Schnupperstudium Mathematik 2001

von Wiland Schmale

Inhalt

Vorwort	S. 1
Literaturangaben	S. 1
Teil I: Potenzreste	S. 2
Teil II: Digitale Unterschriften mit dem RSA-Verfahren	S. 7
Übungsaufgaben	S. 9
Anhang 1: Beweis von Satz 1	S. 10
Anhang 2: Ein Beweis des Euler'schen Satzes	S. 11
Anhang 3: Einige Informationen zu Leonhard Euler	S. 12

Vorwort

Die Präsenz von Mathematik im Alltag und ihr Vordringen in immer weitere Wissensbereiche wird meist nur unzureichend wahrgenommen. Ganz bestimmt ist das so beim sogenannten E-Kommerz und bei der Digitalisierung von Verwaltungsvorgängen. Wie kann man ein vertrauliches Dokument (z. B. Scheckkartennummer, Verwaltungsunterlagen, etc.) im Internet versenden ohne zu riskieren, dass es von Unbefugten gelesen wird und wie kann der Empfänger zweifelsfrei erkennen, von wem das Dokument abgesandt wurde?

Bisher hat nur die Mathematik brauchbare Verfahren anzubieten. Ohne diese Verfahren ist E-Kommerz nicht möglich. Am häufigsten benutzt wird z. Zt. das sogenannte RSA-Verfahren, benannt nach den Autoren Ron Rivest, Adi Shamir und Len Adlman (1978).

Im folgenden Teil I werden zahlentheoretische Grundlagen erarbeitet, wie sie zum Verstehen des RSA-Verfahrens unerlässlich sind. Im Teil II wird dieses Verfahren und seine Anwendung beim Verschlüsseln und digitalen Unterschreiben erläutert.

Ein paar Bücher zu unserem Thema, in die man sich ohne Hochschulwissen hineinlesen kann:

Literatur

[1] Albrecht Beutelspacher: *Geheimsprachen*, Geschichten und Techniken, Beck (2000)

[2] Johannes Buchmann: *Einführung in die Kryptographie*, Springer (1999)

[3] Reinhold Remmert, Peter Ulrich: *Elementare Zahlentheorie*, Birkhäuser (1995)

I Potenzreste

Später in Teil II werden wir Buchstaben als Zahlen darstellen und diese als Potenzreste "verstecken". Jetzt geht es zuerst einmal darum, die mathematischen Voraussetzungen für dieses "Versteckspiel" zu erarbeiten.

Nehmen Sie sich einen ganz primitiven dezimalen Taschenrechner vor, bei dem nur mit ganzen Zahlen gerechnet wird und außerdem die Anzeige bis auf die letzte Stelle zugeklebt ist.

Berechnen Sie die k-ten Potenzen

$$0^k, 1^k, 2^k, 3^k, 4^k, 5^k, 6^k, 7^k, 8^k, 9^k, \ldots$$

Die allein sichtbaren letzten Stellen sind dann in derselben Reihenfolge für $k = 2$:

$$0, 1, 4, 9, 6, 5, 6, 9, 4, 1$$

und für $k = 3$:

$$0, 1, 8, 7, 4, 5, 6, 3, 2, 9$$

Verfolgen wir diese beiden Fälle ($k = 2$, $k = 3$) weiter und setzen der Reihe nach $10, 11, \ldots, 19$ ein, so erhalten wir genau die gleiche Ergebnisfolge. Dies kann man sich wie folgt klar machen

$$(10 + r)^2 = (\cdots)10 + r^2$$

Für die Anzeige an der letzten Stelle kann also nur r^2 einen Beitrag leisten. Ähnlich für $k = 3$, denn es ist

$$(10 + r)^3 = (\cdots)10 + r^3$$

Da jede ganze positive Dezimalzahl z in der Form $z = s \cdot 10 + r$ mit r aus $\{0, \ldots, 9\}$ geschrieben werden kann, gilt ganz allgemein: $z^2 = (\cdots)10 + r^2$ und $z^3 = (\cdots)10 + r^3$. Durch die Beschränkung auf die letzte Ziffer wird die Folge der k-ten Potenzen periodisch mit (nicht unbedingt minimaler) Periodenlänge 10.

Wer m-adische Zahldarstellungen wie etwa Dualzahlen ($m = 2$) oder Hexadezimalzahlen ($m = 16$) kennt, sieht sicher sofort, wie das Potenzieren "modulo 10" verallgemeinert werden könnte. Im Folgenden interessiert uns aber immer nur die letzte Ziffer solcher Zahldarstellungen: der Rest bei Division mit m. Wir gehen daher einen anderen und direkteren Weg mit Hilfe der sogenannten **Division mit Rest** und des **Kongruenz**begriffs. Beides sind fundamentale Bausteine der Zahlentheorie und entsprechend auch für alles was jetzt folgt. Dabei ist stets m eine natürliche Zahl und $m \geq 2$.

Satz 1 (Division mit Rest): *Zu jeder ganzen Zahl z gibt es eine ganze Zahl s und eine Zahl $r \in \{0, \ldots, m-1\}$ derart, dass gilt:*

$$z = sm + r$$

s und r sind eindeutig bestimmt. r heißt **Rest von z bei Division mit m.** *Für den Rest r schreiben wir auch $\varrho_m(z)$. Die zulässige Reste- oder Ziffernmenge beim Divisor m oder bei der Grundzahl m bezeichnen wir mit*

$$\mathbb{Z}_m := \{0, \ldots, m-1\}$$

Ein Beweis von Satz 1 mit vollständiger Induktion ist für Kennerinnen dieser Beweistechnik im Anhang 1 wiedergegeben.

Beispiele: $\varrho_{10}(4^3) = 4 = \varrho_{10}(16 \cdot 4) = \varrho_{10}(6 \cdot 4)$, $\varrho_{10}(8^3) = 2 = \varrho_{10}(64 \cdot 8) = \varrho_{10}(4 \cdot 8)$, $\varrho_{10}(7) = 7$, $\varrho_7(4) = 4$ und allgemein: $\varrho_m(r) = r$ für $r \in \mathbb{Z}_m$.

Veranschaulichungen (siehe Vorlesung):

(a) $\boldsymbol{m = 10}$: Taschenrechnermodell (s.o.)

(b) $\boldsymbol{m = 12}$: Wasserkistenmodell
($m = 6, 20, 24$ kommen bei Flaschen auch vor)

(c) **beliebige** $\boldsymbol{m}$: Wickelmodell

(d) " : Streifenmodell

Definition 2 (Kongruenz): *Zwei ganze Zahlen a und b heißen* **kongruent modulo** $\boldsymbol{m}$*, in Zeichen* $\boldsymbol{a \equiv_m b}$ *oder* $\boldsymbol{a \equiv b \mod m}$*, wenn $a - b$ und natürlich dann auch $b - a$ ein ganzzahliges Vielfaches von m ist, kurz, wenn mit einer ganzen Zahl u gilt:*

$$a - b = um \quad \textit{bzw.} \quad (b - a) = (-u)m$$

Beispiele: $z + um \equiv_m z$, $(z + um)^2 \equiv_m z^2$, $-1 \equiv_{10} 9$, $-6 \equiv_{12} 6$, $7^2 \equiv_8 1$, $7^3 \equiv_8 7$, $12^2 \equiv_{15} 11$ etc.

Kongruenz von Zahlen hat etwas mit "Abstand" zu tun. a und b sind kongruent, wenn ihr Abstand $|a - b|$ sich in der "Einheit m" ganzzahlig messen lässt. Da der maximale Abstand zweier Zahlen r, r' aus $\mathbb{Z}_m$ stets kleiner als m ist, erhalten wir

Beobachtung 3: *Für $r, r' \in \mathbb{Z}_m$ gilt:*

$$r \equiv_m r' \iff r = r'$$

Der Divisionsrest $\varrho_m(z)$ und z selbst sind nach Satz 1 stets kongruent modulo m. Darüber hinaus stellen wir fest:

Beobachtung 4: *Für ganze Zahlen a, b gilt:*

$$a \equiv_m b \iff \varrho_m(a) = \varrho_m(b)$$

Beweis. '$\Rightarrow$' Wir führen die Division mit Rest nach Satz 1 bei a und b durch und erhalten: $a = sm + r$ und $b = s'm + r'$. Wenn dann außerdem $a \equiv_m b$ bzw. $a - b = um$ mit einer ganzen Zahl u, dann folgt:

$$um = a - b = (s - s')m + r - r'$$

und daraus

$$r - r' = (u - s + s')m \quad \text{bzw.} \quad r \equiv_m r'$$

Da $r, r' \in \mathbb{Z}_m$, folgt mit Beobachtung 3: $r = r'$ und das besagt ja gerade $\varrho_m(a) = \varrho_m(b)$.

'$\Leftarrow$:' Trauen Sie sich diese Richtung selbst zu? □

Beispiele: $\varrho_m(z + um) = \varrho_m(z)$; $\varrho_6(5^7) = \varrho_6(25^3 \cdot 5) = \varrho_6((4 \cdot 6 + 1)^3 \cdot 5) = \varrho_6(5) = 5$

Wenn man nur an den Divisionsresten interessiert ist, kann man wegen Beobachtung 4 unterwegs Vielfache von m weglassen und dadurch bei Bedarf mit kleineren Zahlen weiterrechnen. Man entdeckt beim Rechnen folgende leicht zu beweisende Regeln:

Beobachtung 5: *Für ganze Zahlen a, b, u, k mit $k \geq 1$ gilt:*

$$(a + um)b \equiv_m ab$$

und

$$(a + um)^k \equiv_m a^k$$

Wir benutzen jetzt die Division mit Rest zur Einführung der **Potenzrestefolgen** für beliebige m:

$$0^k, 1^k, \varrho_m(2^k), \varrho_m(3^k), \ldots, \varrho_m(z^k), \ldots \tag{1}$$

Beispiele:

											10	11	12	13	14
z	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E
$\varrho_6(z^2)$	0	1	4	3	4	1									
$\varrho_6(z^3)$	0	1	2	3	4	5									
$\varrho_{15}(z^2)$	0	1	4	9	1	A	6	4	4	6	A	1	9	4	1
$\varrho_{15}(z^3)$	0	1	8	C	4	5	6	D	2	9	A	B	3	7	E
$\varrho_{15}(z^9)$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E
$\varrho_{14}(z^2)$	0	1	4	9	2	B	8	7	8	B	2	9	4	1	
$\varrho_{14}(z^3)$	0	1	8	D	8	D	6	7	8	1	6	1	6	D	
$\varrho_{14}(z^5)$	0	1	4	5	2	3	6	7	8	B	C	9	A	D	
$\varrho_{14}(z^7)$	0	1	2	3	4	5	6	7	8	9	A	B	C	D	

Wegen der Beobachtungen 4 und 5 genügt es, die Potenzreste $\varrho_m(z^k)$ für $z \in \mathbb{Z}_m$ zu berechnen, denn es ist ja

$$\varrho_m((z + um)^k) = \varrho_m(z^k)$$

für alle ganzen Zahlen z. m ist also stets eine natürliche Periode für die Potenzrestefolge (1).

An Beispielen kann man sehen, dass es u. U. noch kürzere Perioden geben kann (z. B. $m = 8$, $k = 4$). Als nächstes wollen wir versuchen zu klären, wann eine Potenzrestefolge genau m verschiedene Zahlen liefert ("**optimale Resteverwertung**"). Mehr ist wegen der m-Periodizität nicht möglich.

Der folgende Satz von Euler wird uns helfen, dies zu klären. Einige Informationen zu Leonard Euler (1707-1783) sind im Anhang 3 wiedergegeben.

Satz von Euler: *Seien $E_m := \{z \in \mathbb{Z}_m : \mathrm{ggT}(z, m) = 1\}$ und $\varphi(m) :=$ Anzahl der Elemente in E_m. Für alle ganzen Zahlen z gilt:*

$$\boxed{\mathrm{ggT}(z, m) = 1 \quad \Longrightarrow \quad z^{\varphi(m)} \equiv_m 1}$$

φ heißt **Euler'sche $\boldsymbol{\varphi}$-Funktion**.

Dabei ist mit $\mathrm{ggT}(z, m)$ der größte gemeinsame und positive Teiler der beiden ganzen Zahlen z und m gemeint. Falls $z = 0$, ist $\mathrm{ggT}(0, m) = m$. Im Anhang 2 zu diesem Skript ist ein elementarer Beweis wiedergegeben. Wir setzen diesen Satz von Euler im Folgenden voraus. Nur in zwei Spezialfällen werden wir ihn wirklich benutzen und zwar, wenn

$$m = p \quad \text{eine Primzahl}$$

und wenn

$$m = p \cdot q \quad \text{Produkt zweier verschiedener Primzahlen}$$

Die entsprechenden Werte der Euler'schen φ-Funktion lassen sich leicht bestimmen.

Beobachtung 6:

(a) Ist $m = p$ eine Primzahl, dann ist $\varphi(p) = p - 1$.

(b) Ist $m = pq$ Produkt zweier verschiedener Primzahlen, dann ist $\varphi(p \cdot q) = (p-1)(q-1)$.

Der Nachweis ist Gegenstand der Aufgabe (3).

Beispiele: Berechnen Sie $\varrho_{10}(3^4)$, $\varrho_{14}(11^6)$, $\varrho_{15}(7^8)$.

Nun können wir Situationen beschreiben, in denen die Potenzreste alle möglichen Reste in $\mathbb{Z}_m$ ausschöpfen. Die Folge ist, dass dann jedem Potenzrest genau ein Rest entspricht (umgekehrt ist das ohnehin immer der Fall). Teil (b) des folgenden Satzes besagt zusätzlich, dass man einfach ausreichend oft "weiterpotenzieren" muss, um den Ausgangsrest wiederzuerhalten.

Satz 7: *Seien p, q zwei verschiedene Primzahlen. Wir setzen $m := pq$. Seien weiter $d, e \in \mathbb{Z}_{\varphi(m)}$ derart gewählt, dass gilt:*

$$\boxed{d \cdot e \equiv_{\varphi(m)} 1}$$

Behauptung:

(a) $\varrho_m(0^d), \varrho_m(1^d), \ldots, \varrho_m((m-1)^d)$ sind paarweise verschieden.

(b) Für alle $z \in \mathbb{Z}_m$ gilt:

$$(z^d)^e \equiv_m z \quad \textit{bzw.} \quad \varrho_m((z^d)^e) = z$$

M. a. W.: Man kann durch geeignetes Potenzieren und Dividieren mit Rest die "Eingabe" z aus dem Potenzrest $\varrho_m(z^d)$ wiedergewinnen, sofern man e kennt.

Beachte: Bei Satz 7 kommt es auf die Reihenfolge von d, e nicht an!

Beispiele sind in der Tabelle auf Seite 4 enthalten:

$$m = 15,\ d = 3,\ e = 3 \quad \text{und} \quad m = 14,\ d = 5 = e$$

Erst bei großen p und q gibt es auch eine größere Auswahl für das Paar d, e. Insbesondere gibt es dann auch zunehmend viele Paare d, e mit $d \neq e$. So gibt es etwa schon mit $p = 41$ und $q = 43$ reichlich Auswahl. Ein paar Beispiele sind:

d	11	19	229	257	457
e	611	41	353	317	583

Wenn man solch ein Paar vorgesetzt bekommt, ist es nicht so schwierig zu überprüfen, ob $d \cdot e \equiv_{\varphi(m)} 1$. Es ist aber auch nicht schwer, alle solchen Paare bei bekannten p, q und $m = pq$ zu bestimmen, nur haben wir dafür jetzt keine Zeit.

(Das hierhergehörige Ergebnis wäre: Für jedes $d \in \mathbb{Z}_{\varphi(m)}$ mit $\mathrm{ggT}(d, \varphi(m)) = 1$ gibt es genau ein passendes e und man kann es mit dem euklidischen Algorithmus bestimmen. Für $m = 41 \cdot 43$ gibt es also bereits $\varphi(\varphi(m)) = 384$ Paare.)

Beweis von Satz 7. Zuerst machen wir uns klar, dass (a) aus (b) folgt. Denn falls für $z, z' \in \mathbb{Z}_m$ die d-ten Potenzreste übereinstimmen, wenn also $\varrho_m(z^d) = \varrho_m(z'^d)$, dann ist nach Beobachtung 4: $z^d \equiv_m z'^d$ bzw. $z^d + um = z'^d$ mit einer ganzen Zahl u. Mit Beobachtung 5 folgt daraus $(z^d)^e \equiv_m (z'^d)^e$ und mit (b) dann $z \equiv_m z'$. Beobachtung 3 besagt dann $z = z'$.

Wir brauchen also jetzt nur noch (b) zu beweisen. Davon beweisen wir vorerst nur einen Teil, der aber in den Anwendungen, die wir vorhaben in der Regel ausreicht:

Sei $0 \leq z < \min(p, q) =: n$, dann sind

(a′) $\varrho_m(0^d), \ldots, \varrho_m((n-1)^d)$ paarweise verschieden und es gilt

(b′) $(z^d)^e \equiv_m z$

Aus (b′) folgt (a′), wie wir es oben schon für beliebige $z \in \mathbb{Z}_m$ gesehen haben. Wir beweisen jetzt (b′):

Auf Grund der zusätzlichen Voraussetzungen ist $\mathrm{ggT}(z, m) = 1$. Der Satz von Euler sagt dann: $z^{\varphi(m)} \equiv_m 1$. Die Voraussetzung über d und e besagt: $d \cdot e = 1 + u \cdot \varphi(m)$ mit einer ganzen Zahl u. Nun rechnen wir:

$$(z^d)^e = z^{de} = z^{1+u\varphi(m)} = z \cdot (z^{\varphi(m)})^u \equiv_m z$$

Sie sollten zunächst nur versuchen, den Beweis **bis hierher** zu verstehen. Wie schon bemerkt, reicht das in den Anwendungen, die wir vorhaben, in der Regel aus.

Trotzdem soll natürlich auch die vollständige Behauptung bewiesen werden: Der bisherige Beweisteil funktioniert immer dann, wenn $\mathrm{ggT}(z, m) = 1$. Da $z \in \mathbb{Z}_m$, gibt es ansonsten nur noch die beiden Fälle $\mathrm{ggT}(z, m) = p$ und $\mathrm{ggT}(z, m) = q$.

1. Fall $\mathrm{ggT}(z, m) = p$: Dann ist $(z^d)^e - z$ durch p teilbar und es ist demnach

$$(z^d)^e \equiv_p z\,. \tag{2}$$

Genau wie oben können wir herleiten, dass $(z^d)^e = z^{de} = z^{1+u\varphi(m)}$. Nun ist aber $\varphi(q) = q-1$ nach Beobachtung 6 und $(q-1)$ ein Teiler von $\varphi(m) = (q-1)(p-1)$ und wir erhalten

$$(z^d)^e = z^{1+v\cdot\varphi(q)} = z \cdot (z^{\varphi(q)})^v \quad \text{mit } v = u(p-1)$$

Da zwangsläufig $\mathrm{ggT}(z, q) = 1$, folgt daraus mit Hilfe des Satzes von Euler:

$$(z^d)^e \equiv_q z \tag{3}$$

(2) besagt: p teilt $z^{d^e} - z$. (3) besagt: q teilt $z^{d^e} - z$.

Da p und q verschiedene Primzahlen sind, folgt:

$$m = p \cdot q \quad \text{teilt} \quad (z^d)^e - z$$

und das bedeutet ja grade $(z^d)^e \equiv_m z$.

Der Nachweis für den 2. Fall: $\mathrm{ggT}(z, m) = q$ verläuft genauso. □

II Digitale Unterschrift mit dem RSA-Verfahren

Das RSA-Verfahren gehört zur Klasse der unsymmetrischen Verschlüsselungsverfahren, bei dem derjenige der einen Text verschlüsselt ihn hinterher trotzdem nicht ohne Zusatzinformation entschlüsseln kann. Das Verschlüsselungsverfahren wird sogar veröffentlicht, damit es jeder anwenden kann.

Zuallererst muss aber ein Alphabet vereinbart sein:

$$\mathcal{A} = \{a, b, \ldots, A, B, \ldots, \} \cup \{\text{Sonderzeichen}\} \cup \{\text{Leerstelle}\}$$

Wir gehen davon aus, dass $\mathcal{A}$ weniger als 100 Zeichen enthält. Dann wird jedem Zeichen aus $\mathcal{A}$ eine zweistellige Dezimalzahl zugeordnet. Wir schreiben stets 01 für 1, 02 für 2 etc. Etwa so

leer	a	b	$\cdots$	$\cdots$	z	ä	ö	ü	A	B	$\cdots$	$\cdots$	Z	Ä	Ö	Ü	,	.
00	01	02			26	27	28	29	30	31			55	56	57	58	59	60 $\cdots$

Aus einem Text wird dadurch eine Ziffernreihe: Z. B. wird aus

I c h h o f f e, d i e Z e i t r e i c h t.

380308000|815060605|590004090|500550509|201805090|3082060

Danach wird die Ziffernreihe in Blöcke unterteilt, im Beispiel in 9-er Blöcke $B_1, \ldots, B_6$. In der Praxis ist die Blocklänge L sehr viel größer. Jeder Block wird als Dezimalzahl interpretiert.

Beim RSA-Verfahren wählt z. B. Alice[1] zwei ungefähr gleich große und "sehr große" Primzahlen p, q ($p \neq q$) und ein Paar d, e mit $de \equiv_{\varphi(m)} 1$ mit $m = pq$. Auf jeden Fall wird gewährleistet sein, dass $10^L < \min(p, q)$. Nun veröffentlicht Alice den **öffentlichen Schlüssel (m, d)** und behält den **geheimen Schlüssel (m, e)** für sich. Bob kann ihr jetzt wie folgt eine verschlüsselte Nachricht schicken:

Seien $B_1, B_2, \ldots$ die Blöcke der digitalisierten Nachricht. Bob berechnet $V_1 = \varrho_m(B_1^d)$, $V_2 = \varrho_m(B_2^d), \ldots$ und verschickt diese Zahlenfolge an Alice. Alice berechnet $\varrho_m(V_1^e), \varrho_m(V_2^e), \ldots,$. Von Teil I her weiß Alice, dass folgendes gilt für $i \geq 1$: $V_1 \equiv_m B_i^d$ und daher $V_i^e \equiv_m B_i^{de}$. Mit Satz 7 folgt $V_i^e \equiv_m B_i$ und damit $\varrho_m(V_i^e) = B_i$, denn $B_i < \min(p, q) < m$.

Jeder, der in der Lage ist die Zahl e zu finden, kann das genau so machen. Der springende Punkt beim RSA-Verfahren ist nun, dass man riesige Primzahlen noch relativ leicht erzeugen und ihr Produkt m berechnen kann. Die Zerlegung von m in seine beiden Primzahlen ist aber ungleich schwerer (Falltürprinzip). Nach dem heutigen Stand der Wissenschaft gibt es kein schnelleres Verfahren, um $\varphi(m)$ zu berechnen, als das mit der Formel $(p-1)(q-1)$. Ohne $\varphi(m)$ kann e aber nicht berechnet werden.

Je nach Sicherheitsanspruch werden die Primzahlen p, q so groß gewählt, dass die Faktorzerlegung vom m nach den schnellsten Verfahren Monate oder Jahrhunderte dauert. Zur Zeit müssen dafür 50- bis 600-stellige Primzahlen benutzt werden.

Selbst einfache Beispiele sind nur mit Hilfe eines Computers zu bewältigen. Ich hoffe, die Zeit reicht auch noch dafür. Ansonsten verweise ich auf den Abschnitt "Ein berühmtes Beispiel..." im Dokument

`http://www.uni-oldenburg.de/~schmale/dateien/Oeffentlich/Leitdatei-RSA.html`

[1] Alice und ihr Freund Bob sind international bekannt. Ständig versuchen eifersüchtige und bösartige Wesen ihre E-Mails abzufangen. Sie sind gerade dabei eine gute Strategie zu finden, um sich gegen ungebetene Mitleser zu schützen.

Zurück zu Bob and Alice. Nicht nur Bob, sondern jeder könnte mit dem Schlüssel (m, d) eine verschlüsselte Nachricht an Alice schicken. Wenn alles richtig gemacht wird, kann nur Alice die Botschaft wieder entschlüsseln. Aber wie soll Alice wissen, von wem die Nachricht stammt? Das ist ohne weitere Maßnahmen schlichtweg unmöglich. Es fehlt eine unfälschbare Unterschrift in digitaler Form: die digitale Signatur. Digitale Signaturen sind das A und O beim E-Kommerz oder ganz allgemein bei digitalen Verwaltungsvorgängen.

Das RSA-Verfahren liefert eine ganz einfache Lösung: Auch Bob konstruiert sich Primzahlen p', q' und ein Paar d', e' mit $d'e' \equiv_{\varphi(m')} 1$ und setzt $m' = p'q'$. Er veröffentlicht den Schlüssel: (m', d'). Da er den Schlüssel von Alice kennt (so wie jeder andere), prüft er zuerst, ob $m \leq m'$. Wenn ja, verfährt er nach folgendem Rezept um Alice die Nachricht $B_1, B_2, \ldots$ zu senden.

Berechne $W_i := \varrho_{m'}\Big(\varrho_m\big(B_i^d\big)^{e'}\Big)$. Beachte: e' statt d'
(e' kennt nur Bob.)

Versende W_i

Was fängt Alice damit an? Sie kennt ebenfalls beide öffentlichen Schlüssel (m, d) und (m', d') und stellt fest $m \leq m'$. Dann berechnet Sie:

$$\varrho_m\Big(\varrho_{m'}\big(W_i^{d'}\big)^e\Big) \quad i = 1, 2, \ldots$$

Nur wenn die Nachricht von Bob stammt, kann ein vernünftiger Text dabei entstehen, denn nur dann gilt nach unserer Mathematik aus Teil I mit $V_i = \varrho_m(B_i^d)$:

$$\varrho_{m'}\Big(\varrho_{m'}\big(V_i^{e'}\big)^{d'}\Big) = \varrho_{m'}\big(V_i^{d'e'}\big) = \varrho_{m'}(V_i) = V_i$$

letzteres, weil $m \leq m'$ und somit $V_i \in \mathbb{Z}_{m'}$

Mit V_i erhält man wie oben:

$$\varrho_m\big(V_i^e\big) = B_i$$

Alice kann nun mit dem Alphabet A den digitalisierten Text lesen und sich sicher sein,

- dass niemand außer dem Sender den Text gelesen hat,
- dass der Text nur von Bob stammen kann.

Wenn $m' \leq m$ müssen sowohl Alice, als auch Bob lediglich die Reihenfolge der Potenzierungen ändern.

Die Rechnungen beim RSA-Verfahren lassen sich recht leicht programmieren. Die Potenzberechnungen darf man allerdings nicht einfach ausführen und danach den Potenzrest bestimmen. Dies würde rasch zu Zahlen führen, die die Kapazität eines Computers überfordern: Der von den Erfindern zum "knacken" veröffentlichte legendäre RSA-129-Schlüssel benutzte 129-stellige Dezimalzahlen. Wie groß ist $B^{10^{129}}$ für einen Ziffernblock B , der ja selbst u.U. mindestens so groß sein kann wie der Exponent? In Aufgabe (4) können Sie lernen, wie tatsächlich gerechnet wird.

Viele Feinheiten zur Erhöhung der Sicherheit des RSA-Verfahrens sind bei der praktischen Anwendung zu beachten. Hierfür gibt es reichlich Spezialliteratur, die allerdings auch reichlich mehr Mathematik voraussetzt.

Übungsaufgaben

(1) Überprüfen Sie einige Einträge in der Tabelle auf Seite 4 des Skripts.

(2) Zeigen Sie:

$$\forall a, b, c, m, r, s, t \in \mathbb{Z}:$$
$$(a + rm)(b + sm)(c + tm) \equiv_m abc$$

Sie können dabei wie gewohnt "$m \geq 2$" voraussetzen. Darauf kommt es aber nicht an. Bemerkung: Eine allgemeinere Regel wäre:

$$\forall k \in \mathbb{N}_+ \; \forall a_1, \ldots, a_k, r_1, \ldots, r_k \in \mathbb{Z}:$$
$$\prod_{j=1}^{k} (a_j + r_j m) \equiv_m \prod_{j=1}^{k} a_j$$

Man kann sie durch vollständige Induktion beweisen.

(3) (a) Für eine Primzahl p ist $\varphi(p) = p - 1$.

(b) Für ein Produkt $m = p \cdot q$ zweier verschiedener Primzahlen p, q ist $\varphi(m) = (p-1)(q-1)$

Anleitung zu (b): Es ist leichter, die Zahlen aus $\mathbb{Z}_m$ abzuzählen, die durch p oder q teilbar sind.

(4) (a) Wie kann man mit einem Taschenrechner, der nur die Grundrechenarten für Dezimalzahlen bietet, dennoch ganzzahlige Division mit Rest mit beliebigem Divisor m betreiben?

(b) Jede natürliche Zahl lässt sich als Dualzahl darstellen in der Form $d = c_r 2^r + c_{r-1} 2^{r-1} + \cdots + c_1 \cdot 2 + c_0$ mit $c_0, \ldots, c_r$ aus $\{0, 1\}$. Zur Berechnung von $\varrho_m(z^d)$ genügt es daher, die folgenden Potenzreste zu berechnen: $Q_0 := z$, $Q_1 = \varrho_m(z^2)$, $Q_2 = \varrho_m(Q_1^2), \ldots Q_r = \varrho_m(Q_{r-1}^2)$. Es ist dann $\varrho_m(z^d) = \varrho_m(Q_0^{c_0} \cdots Q_r^{c_r})$. Wenden Sie dieses Verfahren an bei $m = 77$, $d = 23$ und $z = 37$.

(c) Digitalisiert man wie im Skript die kurze Nachricht "Hi", so erhält man "3708". Daraus bildet Bob zwei Zweierblöcke $B_1 = 37$, $B_2 = 08 = 8$. Alice und Bob haben vereinbart, dieselben Primzahlen $p = 7$, $q = 11$ zu benutzen. Die folgende Liste enthält die in Frage kommenden Paare (e, d) mit $ed \equiv_{\varphi(m)} 1$ und $e \neq d$. Wählen Sie für Alice und Bob jeweils ein Paar aus und versenden Sie für Bob die Nachricht "Hi" digital signiert. Überprüfen Sie, ob Alice die Botschaft wirklich lesen kann. Bei geeigneter Wahl kann die Rechnung aus (b) mit benutzt werden.

d	7	13	17	23	37	43	47	53
e	43	37	53	47	13	7	23	17

(5) Beweisen Sie die im Anhang 2 beim Beweis des Euler'schen Satzes vorausgesetzten Aussagen (a) und (b).

Anleitung zu (b): Der Satz über die eindeutige Primzerlegung ganzer Zahlen (bis auf das Vorziehen und die Anordnung der Primteiler) kann benutzt werden.

Anhang 1

Ein **Beweis von Satz 1** mit vollständiger Induktion kopiert aus dem Buch "Algebraische Strukturen" von Serge Lang (Vandehoek & Rupprecht, 1979), S. 11/12.

Beweis. Wir beweisen zuerst die Existenz durch Induktion nach n.

(1) Für $n = 0$ sind mit $q = r = 0$ die Bedingungen erfüllt.

(2) Es sei nun $n > 0$. Im Falle $n < m$ nehmen wir $q = 0$ und $r = n$. Im Falle $n \geqq m$ haben wir $0 \leqq n - m < n$. Nach Induktionsvoraussetzung gibt es q_1, $r \geqq 0$ mit

$$n - m = q_1 m + r \text{ und } r < m.$$

Dann ist

$$n = m + q_1 m + r = (1+q_1)\, m + r.$$

Damit ist die Existenz von $q = 1 + q_1$ und r wie gewünscht bewiesen.

Nun zur Eindeutigkeit. Angenommen es ist

$$n = qm + r \text{ mit } 0 \leqq r < m$$
$$n = pm + s \text{ mit } 0 \leqq s < m$$

Es sei etwa $r \geqq s$. Durch Subtraktion erhalten wir

$$(p-q)m = r - s \text{ mit } 0 \leqq r - s < m.$$

Da $r - s$ ein ganzzahliges Vielfaches von m ist, bleibt nur $r - s = 0$, also $r = s$ und dann auch $q = p$. Damit ist die Eindeutigkeit gesichert und unser Satz bewiesen.

Die beim Beweis benutzte Induktionsvoraussetzung lautet:

"für alle Zahlen $n' < n$ gilt Satz 1"

Anhang 2

Ein Beweis des Euler'schen Satzes: Wir benutzen bei diesem Beweis

(a) Wenn $z_1, z_2 \in E_m$, dann auch $\varrho_m(z_1 z_2)$.

(b) Wenn m ein Produkt uv ganzer Zahlen teilt und wenn außerdem $\mathrm{ggT}(m, u) = 1$, dann ist m ein Teiler von v.

Zum Beweis des Euler'schen Satzes zeigen wir zuerst für ein beliebiges $a \in E_m$:

Mit $M = \{\varrho_m(az) : z \in E_m\}$ gilt:

$$M = E_m$$

Wegen (a) gilt jedenfalls $M \subseteq E_m$. Da E_m endlich ist, genügt es jetzt für $z_1, z_2 \in E_m$ zu zeigen:

$$\varrho_m(az) = \varrho_m(az_2) \quad \Longrightarrow \quad z_1 = z_2$$

denn dann gibt es genauso viele Reste $\varrho_m(az)$, wie es Elemente in E_m gibt und es muss $M = E_m$ sein.

Gelte nun also $\varrho_m(az_1) = \varrho_m(az_2)$, dann folgt $az_1 \equiv_m az_2$ bzw. $a(z_1 - z_2) = um$ mit einer geeigneten ganzen Zahl u. Insbesondere ist m demnach ein Teiler des Produkts $a(z_1 - z_2)$. Da $\mathrm{ggT}(a, m) = 1$, muss m wegen (b) ein Teiler von $z_1 - z_2$ sein. Nach Definition 2 gilt also: $z_1 \equiv_m z_2$. Mit Beobachtung 3 folgt schließlich $z_1 = z_2$.

Mit folgendem Trick erhalten wir jetzt den Satz von Euler:

Da $E_m = M$, müssen auch die Produkte aller Zahlen aus E_m und aus M übereinstimmen: $\prod_{z \in E_m} z = \prod_{z \in E_m} \varrho_m(az)$. Übergang zu Kongruenzen ergibt:

$$\prod_{z \in E_m} z \equiv_m \prod_{z \in E_m} az$$

Mit einer geeigneten ganzen Zahl v gilt daher

$$vm = \prod_{z \in E_m} z - \prod_{z \in E_m} az = \Big(1 - \prod_{z \in E_m} a\Big) \prod_{z \in E_m} z = \Big(1 - a^{\varphi(m)}\Big) \prod_{z \in E_m} z$$

Da $\mathrm{ggT}(m, \prod_{z \in E_m} z) = 1$, muss m ein Teiler von $1 - a^{\varphi(m)}$ sein und das bedeutet:

$$a^{\varphi(m)} \equiv_m 1\,.$$

$\square$

Man kann den Satz von Euler auch völlig anders beweisen, siehe etwa [3, S. 167] für einen völlig verschiedenen Beweiskontext. Euler's Beweis wird dort auf S. 186 wiedergegeben. Unser obiger Beweis wird dort James Ivory (1765-1842) zugeschrieben und in etwas anderer Form auf S. 188 entwickelt. Elegantere, abstraktere und allgemeingültigere Versionen des Satzes sind dort auch noch ab S. 219 zu finden. Das Buch [3] ist ohne universitäre Kenntnisse lesbar.

Anhang 3

Einige Informationen zu Leonhard Euler kopiert aus dem Buch "Abriß der Geschichte der Mathematik" von Dirk Struik, (Deutscher Verlag der Wissenschaften, 1976)

7.4. Das Werk L. Eulers

Aus Basel stammte auch der produktivste Mathematiker des achtzehnten Jahrhunderts — wenn nicht aller Zeiten —, Leonhard Euler. Sein Vater studierte Mathematik bei Jakob Bernoulli und Leonhard bei Johann. Als Johanns Sohn Nikolaus 1725 nach Petersburg reiste, folgte ihm der junge Euler und blieb bis 1741 an der dortigen Akademie. Von 1741 bis 1766 arbeitete Euler an der Berliner Akademie, die unter der besonderen Schirmherrschaft Friedrichs II. stand; von 1766 bis 1783 war er wieder in Petersburg, nunmehr unter der Ägide der Kaiserin Katharina. Er heiratete zweimal und hatte dreizehn Kinder. Das Leben dieses Akademikers des achtzehnten Jahrhunderts war fast ausschließlich den verschiedenen Gebieten der reinen und der angewandten Mathematik gewidmet. Obwohl er 1735 das eine und 1766 das zweite Auge verlor, konnte nichts seine enorme Produktivität unterbrechen. Der erblindete Euler, der über ein phänomenales Gedächtnis verfügte, fuhr fort, seine Entdeckungen zu diktieren. Während seines Lebens erschienen 530 Bücher und Arbeiten; bei seinem Tode hinterließ er viele Manuskripte, die während der nächsten siebenundvierzig Jahre von der Petersburger Akademie veröffentlicht wurden. (Damit erhöhte sich die Anzahl seiner Werke auf 771, aber durch Nachforschungen von Gustav Eneström wurde die Liste auf 886 ergänzt.)
Euler lieferte in allen Gebieten der Mathematik, die zu seiner Zeit existierten, maßgebliche Beiträge. Er veröffentlichte seine Ergebnisse nicht nur in Einzelarbeiten von verschiedener Länge, sondern auch in einer eindrucksvollen Zahl von großen Lehrbüchern, die das während der früheren Zeiten gesammelte Material ordneten und geschlossen darstellten. Auf einigen Gebieten war die Eulersche Darstellung so gut wie endgültig. Ein Beispiel dafür ist unsere heutige Trigonometrie mit ihrer Auffassung der trigonometrischen Werte als Verhältniszahlen und ihrer üblichen Schreibweise, die aus Eulers „Introductio in analysin infinitorum" (1748) stammt. Das überragende Ansehen seiner Lehrbücher bereinigte viele strittige Bezeichnungsfragen der Algebra und Infinitesimalrechnung für immer; Lagrange, Laplace und Gauß kannten Euler und übernahmen seine Bezeichnungen in allen ihren Werken.

Die „Introductio" von 1748 enthält in ihren zwei Bänden eine Vielzahl von verschiedenen Gegenständen. Sie gibt eine Darstellung der unendlichen Reihen einschließlich derjenigen für e^x, $\sin x$ und $\cos x$ und die Relation $e^{ix} = \cos x + i \sin x$ (die schon von Johann Bernoulli und anderen in verschiedenen Formen entdeckt worden war). Kurven und Flächen werden mit Hilfe ihrer Gleichungen so gewandt untersucht, daß man die „Introductio" als die erste lehrbuchmäßige Darstellung der analytischen Geometrie betrachten kann. Auch eine algebraische Eliminationstheorie ist darin enthalten. Zu den reizvollsten Teilen dieses Buches gehören das Kapitel über die Zetafunktion und ihre Beziehung zur Theorie der Primzahlen ebenso wie das Kapitel über die „partitio numerorum".[1])

Ein anderes großes und reichhaltiges Lehrbuch war Eulers Werk „Institutiones calculi differentialis" (1755), dem weitere drei Bände der „Institutiones calculi integralis" (1768—1774) folgten. Hier findet man nicht nur unsere elementare Differential- und Integralrechnung, sondern auch eine Theorie der Differentialgleichungen, den Satz von Taylor mit zahlreichen Anwendungen, die Eulersche Summenformel und die Eulerschen Γ- und B-Integrale. Der Abschnitt über Differentialgleichungen mit seiner Unterscheidung zwischen „linearen", „exakten" und „homogenen" Gleichungen dient noch heute als Muster unserer elementaren Lehrbücher.

Eulers „Mechanica, sive motus scientia analytice exposita" (1736) war das erste Lehrbuch, in dem die Newtonsche Dynamik des Massenpunktes mit analytischen Methoden entwickelt wurde. Ein Lehrbuch von 1765 enthält die Eulersche Gleichung für einen um einen Punkt rotierenden Körper. Die „Vollständige Anleitung zur Algebra" (1770), die deutsch geschrieben und einem Diener diktiert wurde, ist zum Vorbild für viele spätere Lehrbücher der Algebra geworden. Sie führt bis zur Theorie der kubischen und biquadratischen Gleichungen und zu unbestimmten Gleichungen.

Im Jahre 1744 erschien Eulers „Methodus inveniendi lineas curvas maximi minimive proprietate gaudentes". Das war die erste Darstellung der Variationsrechnung; sie enthielt die Eulersche Differentialgleichung mit vielen Anwendungen einschließlich der Entdeckung, daß das Katenoid und die Schraubenfläche Minimalflächen sind. Viele andere Resultate von Euler finden sich in seinen kleineren Arbeiten, die manchen sogar heute wenig bekannten Edelstein enthalten. Zu den wohlbekannten Entdeckungen gehören der Eulersche Polyedersatz, der die Anzahl der Ecken (E), Kanten (K) und Flächen (F) eines geschlossenen Polyeders verknüpft ($E + F - K = 2$)[2]), die Eulersche Gerade im Dreieck, die Kurven konstanter Breite (Euler nannte sie orbiforme Kurven) und die Eulersche Konstante C:

$$\lim_{n\to\infty}\left(1 + \frac{1}{2} + \cdots + \frac{1}{n} - \log n\right) = 0{,}5772156\ldots$$

Einige Arbeiten sind mathematischen Unterhaltungen gewidmet (das Königsberger Brückenproblem, Rösselsprünge). Eulers Beiträge zur Zahlentheorie würden allein hinreichen, um ihm eine Nische in der Ruhmeshalle zu sichern; zu seinen Entdeckungen auf diesem Gebiet gehört das quadratische Reziprozitätsgesetz.

[1]) Siehe A. Speisers Vorrede zur *Introductio* in: Euler, *Opera* I, 9 (1945).

[2]) Er war schon Descartes bekannt: *Œuvres* (C. Adam et P. Tannery) X, S. 257—276.

Ein großer Teil der Tätigkeit von Euler war der Astronomie gewidmet, wo die Mondtheorie, ein wichtiger Sonderfall des Dreikörperproblems und auch für die Lösung der uralten Frage der Längenbestimmung von Bedeutung, seine besondere Aufmerksamkeit auf sich zog. Die „Theoria motus planetarum et cometarum" (1774) ist eine Abhandlung über Himmelsmechanik. Verwandt mit dieser Arbeit war Eulers Studium der Anziehung von Ellipsoiden (1738).
Euler hat Bücher über Hydraulik, Schiffbau und Artillerie geschrieben. 1769—1771 erschienen drei Bände einer „Dioptrica" mit einer Theorie des Strahlenverlaufs beim Durchgang durch ein Linsensystem. Im Jahre 1739 erschien seine neue Theorie der Musik, von der man gesagt hat, daß sie zu musikalisch für Mathematiker und zu mathematisch für Musiker sei. Eulers philosophische Darlegung der wichtigsten Probleme der Naturwissenschaft in seinen „Briefen an eine deutsche Prinzessin" (1760/61 geschrieben) sind ein Musterbeispiel einer populären Darstellung geblieben.
Die enorme Fruchtbarkeit Eulers bildet eine ständige Quelle der Überraschung und Bewunderung für jeden, der versucht hat, sein Werk zu studieren, übrigens eine Aufgabe, die nicht so schwierig ist, wie sie scheint, denn Eulers Latein ist sehr einfach, und seine Bezeichnungen sind fast modern — oder vielleicht sollte man besser sagen, daß die heutigen Bezeichnungen fast die gleichen wie bei Euler sind! Man kann eine lange Liste der bekannten Entdeckungen aufstellen, bei denen Euler die Priorität besitzt, und eine weitere Liste von Ideen, die es noch verdienen, bearbeitet zu werden. Große Mathematiker haben stets ihre Schuld gegenüber Euler betont. Laplace pflegte zu jüngeren Mathematikern zu sagen: „Lisez Euler, c'est notre maître à tous." (Lest Euler, er ist unser aller Meister.) Und Gauß drückte sich etwas gewichtiger so aus: „Das Studium der Werke Eulers bleibt die beste Schule in den verschiedenen Gebieten der Mathematik und kann durch nichts anderes ersetzt werden." Riemann kannte Eulers Werke sehr gut, und einige seiner tiefschürfenden Werke haben einen Eulerschen Zug. Verleger könnten wohl Schlimmeres tun, als Übersetzungen von einigen Werken Eulers unter Beifügung moderner Kommentare herauszubringen.