Lauschen zwecklos!
oder
Wie aus einer seltsamen Erkenntnis über Zahlen die beste Geheimsprache aller Zeiten wurde*

U. Kirchgraber, Departement Mathematik ETH Zürich
J. Kramer, Institut für Mathematik der Humboldt-Universität Berlin

Stellen Sie sich folgende hypothetische Situation vor. Für einige Zeit, sagen wir drei Monate, können Sie und Ihre Freundin oder Ihr Freund nur über einen öffentlichen Kanal kommunizieren – zum Beispiel via Zeitung!
Das heisst, Sie können, wann immer Sie wollen, eine Botschaft für Ihre Freundin an die Zeitung schicken, diese druckt sie ab, Ihre Freundin erhält die Zeitung am nächsten Morgen wie alle übrigen Leserinnen und Leser. Und umgekehrt funktioniert es analog.
Aber irgend ein anderes Kommunikationsmittel gibt es nicht: Sie können einander nicht treffen, es gibt keine Post, kein Postillion d'Amour, kein Internet, weder Telefon noch Handy. Natürlich möchten Sie einander Dinge sagen, die niemanden sonst etwas angehen.
Ja – wenn Sie miteinander einen "Code" verabredet hätten, dann wäre die Sache ja noch ganz lustig: Sie könnten einander per Zeitung verschlüsselte Botschaften schicken. Dann müssten Freunde und Bekannte herumrätseln, was Sie sich so zu sagen haben. Nur – Sie haben keinerlei Absprachen getroffen.
Das Erstaunliche: Es ist trotzdem möglich, dass Sie und Ihre Freundin oder Ihr Freund via Zeitung miteinander kommunizieren, ohne dass irgend jemand die geringste Chance hat, Sie zu belauschen!
So etwas Verblüffendes leistet nur die Mathematik. Wie es funktioniert, können Sie in diesen Ausführungen selber entdecken. Überraschenderweise spielt ein 350 Jahre altes Resultat aus der sogenannten Zahlentheorie, einem Teilgebiet der Mathematik, eine wichtige Rolle. Aber erfunden wurde die sogenannte RSA-Methode erst 1977 von R. Rivest, A. Shamir und L. Adleman. Natürlich hat die RSA-Methode grosse zivile, wirtschaftliche und militärische Bedeutung.

Wie sollen Sie nun weiter vorgehen?

Das Material, das vor Ihnen liegt, ist in fünf Kapitel gegliedert. Jedes Kapitel enthält etwas Theorie und zahlreiche Aufgaben. Bitte lesen Sie die Theorieteile und versuchen Sie die dazwischen gestreuten Aufgaben zu lösen. Lesen Sie langsam. Die Lektüre eines mathematischen Textes verläuft ganz anders als das Lesen einer Novelle oder eines Romans: Viel langsamer! Meist muss man immer wieder zu einer Definition zurückkehren, bis man sie

*Dieses Material entstand im Zusammenhang mit dem Nachdiplomstudium Fachdidaktik Mathematik der Universität Bern 2003-2005 und der ETH-Studienwochen 2004 für Schülerinnen und Schüler. Die Autoren bedanken sich bei D. Stoffer und J. Waldvogel für die kritische Durchsicht des Manuskripts.

genau versteht. Eine Behauptung muss man immer wieder lesen, bis man ahnt, warum sie richtig sein könnte, bis man erste Schritte in Richtung eines Beweises machen kann. Die Aufgaben spielen in diesem Text eine wichtige Rolle. Man könnte sagen: Sie sind Wegweiser. Sie helfen Ihnen, die RSA-Methode "nachzuentdecken". Legen Sie Papier und Schreibzeug bereit: Sie brauchen es, um Rechnungen durchzuführen, um Überlegungen zu notieren. Es wäre gut, wenn Sie eine Art "Journal" führen würden, in dem Sie die Lösungen von Aufgaben, durchgerechnete Beispiele, Vermutungen, Fragen, usw. protokollieren.
Es folgen ein paar Angaben zu den Inhalten der fünf Kapitel. In *Kapitel 1* erinnern Sie sich ans Dividieren mit Rest, an den Begriff des grössten gemeinsamen Teilers (ggT) von zwei Zahlen. Sie erfahren, wie man den ggT durch "fortgesetzte Division" bequem und effizient berechnen kann, eine Methode, die man schon in den Büchern des griechischen Mathematikers Euklid (408?-325? v. Chr.) findet. Das erste Kapitel wird durch Überlegungen zu den Primzahlen abgeschlossen. Primzahlen sind – wie Sie sich wahrscheinlich erinnern – Zahlen, die nur durch sich selbst und die Zahl Eins teilbar sind. Sie bilden so etwas wie die Grundbausteine der Zahlen und spielen für die RSA-Verschlüsselung eine Schlüsselrolle.
In *Kapitel 2* lernen Sie das "Rechnen mit Resten" kennen. Eine noblere Bezeichnung dafür ist "Modulare Arithmetik". Das ist einfach, und – wie sich in den folgenden Kapiteln zeigt – folgenreich.
In *Kapitel 3* geht es um den sogenannten[1] "Kleinen Satz von Fermat". Sie werden eine gute Chance haben den "Kleinen Fermat" selber zu entdecken. Auch einen Beweis lassen wir Sie selber erarbeiten. Wir glauben, dass einige Hinweise genügen werden.
Leonhard Euler (1707-1783) hat den Kleinen Satz von Fermat verallgemeinert. Einem Spezialfall begegnen Sie im *Kapitel 4*.
In *Kapitel 5* lernen Sie schliesslich die RSA-Verschlüsselung von Rivest, Shamir und Adleman kennen und verstehen, warum sie funktioniert.
Für verwandte Darstellungen dieses Themenkreises konsultiere man die Referenzen am Ende dieses Artikels.

1 Divisionen, Reste, ggT und Primzahlen

Es bezeichnet $\mathbf{Z}$ die Menge der ganzen Zahlen $\mathbf{Z} = \{0, \pm 1, \pm 2, \pm 3, \pm 4, \ldots\}$ und $\mathbf{N}$ die Menge der natürlichen Zahlen $\mathbf{N} = \{1, 2, 3, \ldots\}$.
Zur Erinnerung: In $\mathbf{Z}$ kann man uneingeschränkt *addieren, subtrahieren* und *multiplizieren.* Divisionen hingegen gehen (meist) nicht auf. Beim Rechnen in $\mathbf{Z}$ oder $\mathbf{N}$ gelten die üblichen Rechenregeln, also die beiden kommutativen, die beiden assoziativen und das distributive Gesetz.

1.1 Division mit Rest

Die Zahl 21 ist durch die Zahl 7 teilbar: Die Division ergibt 3. Oder anders gesagt: Es gilt $21 = 3 \cdot 7$. Hingegen ist 17 nicht durch 5 teilbar: Es bleibt der Rest 2

$$17 = 3 \cdot 5 + 2$$

Mit Rest kann man immer dividieren, wobei der Rest immer kleiner ist als die Zahl, durch die man teilt. Division mit Rest ist für das Verschlüsseln nach der RSA-Methode so zentral, dass wir das, was gerade in Erinnerung gerufen wurde, als "mathematischen Satz" festhalten.

[1] Nach Pierre de Fermat (1601-1665).

Satz 1 *(Division mit Rest).*
Voraussetzung: Es seien $a, b \in \mathbf{Z}, b \neq 0$.
Behauptung: Es gibt (eindeutig bestimmte) Zahlen q, r *mit*

$$0 \leq r < |b|,$$

so dass a *in folgender Form geschrieben werden kann*

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

Aufgabe 1 *Bitte geben Sie einige Beispiele zur Illustration von Satz 1.*

Aufgabe 2 *Beweisen Sie Satz 1, zum Beispiel geometrisch, anhand der Zahlengeraden.*

Definition 1 *Es bezeichne* $\boxed{R_b(a)}$ *den Rest bei Division von* a *durch* b.
Geht die Division auf, das heisst, ist der Rest $R_b(a)$ *gleich 0, heisst* a durch b teilbar*, oder man sagt:* b teilt a *und schreibt*

$$b|a.$$

Beispielsweise gilt $R_5(17) = 2$ und $3|15$.

1.2 Grösster gemeinsamer Teiler

Seien $a, b \in \mathbf{Z}$. Die Zahlen a und b haben auf jeden Fall 1 als gemeinsamen Teiler. Vielleicht haben sie noch weitere gemeinsame Teiler. So haben zum Beispiel 12 und 30 auch 3 als gemeinsamen Teiler. Allgemein definiert man:

Definition 2 *Die Zahl* $c \in \mathbf{Z}$ *heisst (gemeinsamer) Teiler von* a *und* b*, falls* $c|a$ *und* $c|b$*, also wenn* c *sowohl* a *als auch* b *teilt.*

Definition 3 *Es seien* a*,* b *zwei ganze Zahlen. Die natürliche Zahl* d *heisst* grösster gemeinsamer Teiler von a und b*, wenn folgende zwei Bedingungen erfüllt sind:*

1. $d|a$ *und* $d|b$.
2. *Ist* c *gemeinsamer Teiler von* a *und* b*, dann teilt* c *die Zahl* d.

Man schreibt: $\boxed{(a, b) = d.}$
Eine Abkürzung für "grösster gemeinsamer Teiler" ist *ggT*, englisch *gcd*, für "greatest common divisor".

Frage 1 *i) Warum ist die Zahl* d *aus der Definition der* grösste *gemeinsame Teiler von* a *und* b*?*
ii) Warum haben zwei Zahlen immer *einen grössten gemeinsamen Teiler?*

Der grösste gemeinsame Teiler zweier Zahlen $a, b \in \mathbf{Z}$ lässt sich bequem mit Hilfe des sogenannten *Euklidschen Algorithmus* bestimmen, der im nächsten Abschnitt eingeführt wird.

1.3 Euklidscher Algorithmus

Der Euklidsche Algorithmus beruht auf dem Satz über die Division mit Rest, der wiederholt angewandt wird. Wir erklären Ihnen das Prinzip an einem Beispiel. Wir bestimmen den ggT von

$$a = 3182, \quad b = 711$$

durch fortgesetzte Division.

1. Schritt
Dividieren Sie $a = 3182$ durch $b = 711$. Das Resultat ist $q_1 = 4$ mit Rest $r_1 = 338$. Das heisst, es gilt

$$3182 = 4 \cdot 711 + 338 \quad \text{oder} \quad a = q_1 \cdot b + r_1.$$

2. Schritt
Dividieren Sie $b = 711$ durch $r_1 = 338$. Das Resultat ist $q_2 = 2$ mit Rest $r_2 = 35$. Das heisst, es gilt

$$711 = 2 \cdot 338 + 35 \quad \text{oder} \quad b = q_2 \cdot r_1 + r_2.$$

3. Schritt
Dividieren Sie $r_1 = 338$ durch $r_2 = 35$. Das Resultat ist $q_3 = 9$ mit Rest $r_3 = 23$. Das heisst, es gilt

$$338 = 9 \cdot 35 + 23 \quad \text{oder} \quad r_1 = q_3 \cdot r_2 + r_3.$$

4. Schritt
Dividieren Sie $r_2 = 35$ durch $r_3 = 23$. Das Resultat ist $q_4 = 1$ mit Rest $r_4 = 12$. Das heisst, es gilt

$$35 = 1 \cdot 23 + 12 \quad \text{oder} \quad r_2 = q_4 \cdot r_3 + r_4.$$

5. Schritt
Dividieren Sie $r_3 = 23$ durch $r_4 = 12$. Das Resultat ist $q_5 = 1$ mit Rest $r_5 = 11$. Das heisst, es gilt

$$23 = 1 \cdot 12 + 11 \quad \text{oder} \quad r_3 = q_5 \cdot r_4 + r_5.$$

6. Schritt
Dividieren Sie $r_4 = 12$ durch $r_5 = 11$. Das Resultat ist $q_6 = 1$ mit Rest $r_6 = 1$. Das heisst, es gilt

$$12 = 1 \cdot 11 + 1 \quad \text{oder} \quad r_4 = q_6 \cdot r_5 + r_6.$$

7. Schritt
Dividieren Sie $r_5 = 11$ durch $r_6 = 1$. Das Resultat ist $q_7 = 11$ mit Rest $r_7 = 0$. Das heisst, es gilt

$$11 = 11 \cdot 1 + 0 \quad \text{oder} \quad r_5 = q_7 \cdot r_6 + 0.$$

Es wird sich zeigen, dass gilt: *Der ggT von a und b ist gleich dem letzten nicht verschwindenden Rest bei der Durchführung des Euklidschen Algorithmus.*
Der ggT von $a = 3182$ und $b = 711$ ist daher gleich $r_6 = 1$. Man kann also schreiben $(3182, 711) = 1$.

Aufgabe 3 *Führen Sie den Euklidischen Algorithmus durch und bestimmen Sie damit den ggT von a und b.*

i) $a = 925, \quad b = 65.$

ii) $a = 5671, \quad b = 342.$

Definition 4 *Gilt $(a, b) = 1$, das heisst ist der ggT von a und b gleich 1, dann heissen a und b* teilerfremd.

Frage 2 *Warum bricht der Euklidische Algorithmus immer ab, d.h. warum gibt es* immer *einen* letzten *nicht verschwindenden Rest?*

Bis jetzt ist *nicht* klar, warum der Euklidische Algorithmus das Gewünschte leistet, das heisst, warum der Euklidsche Algorithmus den ggT (a, b) von zwei ganzen Zahlen a und b bestimmt. Diese Frage soll nun geklärt werden. Nehmen Sie an, der Euklidische Algorithmus breche zum Beispiel nach fünf Schritten ab:

$$\begin{array}{rcll} a & = & q_1 \cdot b + r_1 & \text{mit} \quad 0 < r_1 < |b| \quad (\Rightarrow b \neq 0), \\ b & = & q_2 \cdot r_1 + r_2 & \text{mit} \quad 0 < r_2 < r_1, \\ r_1 & = & q_3 \cdot r_2 + r_3 & \text{mit} \quad 0 < r_3 < r_2, \\ r_2 & = & q_4 \cdot r_3 + r_4 & \text{mit} \quad 0 < r_4 < r_3, \\ r_3 & = & q_5 \cdot r_4. & \end{array}$$

Aufgabe 4 *Zeigen Sie mit Hilfe der obigen Formeln, dass: $r_4|a$ und $r_4|b$.*

Aufgabe 5 *Zeigen Sie mit Hilfe der obigen Formeln, dass gilt: r_4 lässt sich als ganzzahlige Linearkombination von a und b darstellen. Das heisst, man kann zwei Zahlen $x, y \in \mathbf{Z}$ so finden, dass für r_4 die folgende Darstellung resultiert: $r_4 = x \cdot a + y \cdot b$.*

Aufgabe 6 *Zeigen Sie: $r_4 = (a, b)$.*

Was anhand des 5-schrittigen Euklidschen Algorithmus gezeigt wurde, gilt allgemein. Das Resultat wird als Satz zusammengefasst.

Satz 2 *(Euklischer Algorithmus).*
Seien $a, b \in \mathbf{Z}, b \neq 0$. Dann gibt es zwei Zahlen $x, y \in \mathbf{Z}$, so dass gilt:

$$(a, b) = x \cdot a + y \cdot b.$$

Das heisst, der ggT von a und b lässt sich immer als (ganzzahlige) Linearkombination *von a und b schreiben.*
Sind speziell a und b teilerfremd*, dann gibt es zwei ganze Zahlen x und y, so dass gilt:*

$$1 = x \cdot a + y \cdot b.$$

1.4 Primzahlen

Definition 5 *Eine natürliche Zahl $p > 1$ heisst* Primzahl*, wenn p nur durch ± 1 und $\pm p$ teilbar ist.*

Es sei $\mathbf{P}$ die Menge der Primzahlen:

$$\mathbf{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31 \ldots\}$$

Frage 3 *Können Sie beweisen, dass es* unendlich viele *verschiedene Primzahlen gibt?*

Aufgabe 7 *Benützen Sie den 2. Teil von Satz 2, um das sog. "Euklidische Lemma" zu beweisen.*

Satz 3 *(Euklidisches Lemma).*
Seien $a, b \in \mathbf{Z}$, $p \in \mathbf{P}$ und p teile das Produkt $a \cdot b$. Dann teilt p die Zahl a, oder die Zahl b, oder beide Zahlen.

Eine natürliche Zahl[2] ist entweder eine Primzahl oder aber eine *zusammengesetzte Zahl*, das heisst sie hat ausser 1 und sich selbst noch weitere Teiler. Indem man jeden Teiler wieder als Produkt schreibt, wenn er keine Primzahl ist, und ebenso verfährt mit allen Teilern der Teiler, usw. usw., erhält man schliesslich *die Zerlegung der gegebenen Zahl in Primfaktoren* (die sog. *Primfaktorzerlegung*). Hier ist ein Beispiel

$$1000 = 8 \cdot 125 = 2 \cdot 4 \cdot 5 \cdot 25 = 2 \cdot 2 \cdot 2 \cdot 5 \cdot 5 \cdot 5 = 2^3 \cdot 5^3.$$

Bemerkung 1 *Mit Hilfe des euklidischen Lemmas kann man beweisen, dass die* Primfaktorzerlegung *(bis auf die Reihenfolge)* eindeutig *ist. Das heisst, es ist unmöglich, dass je nach der Art und Weise, wie man die Primfaktorzerlegung gewinnt, in der einen Zerlegung zum Beispiel die Primzahl 5 vorkommt, in einer anderen Zerlegung hingegen nicht. Genau so ist es nicht möglich, dass der Faktor 3 in der einen Zerlegung 6 mal vorkommt und in einer anderen 7 oder 11 mal.*

Satz 4 *(Primfaktorzerlegung).*
Sei $a \in \mathbf{Z}$, $a \neq 0, \pm 1$. Dann gibt es eindeutig bestimmte Primzahlen $p_1, p_2 \ldots, p_r$ und natürliche Zahlen $\alpha_1, \alpha_2, \ldots, \alpha_r$, so dass gilt

$$a = \pm p_1^{\alpha_1} p_2^{\alpha_2} p_3^{\alpha_3} \ldots p_r^{\alpha_r}.$$

Bemerkung 2 *Kennt man die Primfaktorzerlegungen zweier Zahlen a, b, lässt sich daraus leicht der ggT bestimmen:*

$$a = 925 = 5^2 \cdot 37^1, \quad b = 65 = 5 \cdot 13 \quad \rightarrow \quad \text{ggT von } a \text{ und } b \text{ ist } 5.$$

Die Bestimmung des ggT mit Hilfe des Euklidschen Algrorithmus ist jedoch i.a. viel weniger aufwendig als via Primfaktorzerlegungen!

2 Rechnen mit Resten

Die ganzen Zahlen $\mathbf{Z}$, zusammen mit der Operation der Addition und der Operation der Multiplikation ist ein Beispiel für eine wichtige "mathematische Struktur": Man spricht von einem *Ring*.

[2] grösser 1.

Die rationalen Zahlen

$$\mathbf{Q} = \{\frac{p}{q} \,|\, p \in \mathbf{Z}, q \in \mathbf{N}\},$$

also die "Brüche", zusammen mit den Operationen Addition und Multiplikation ist ein Beispiel für eine andere wichtige "mathematische Struktur": Man spricht von einem *Körper*. Der Unterschied ist folgender: In $\mathbf{Q}$ kann man *jede* Gleichung der Form

$$a \cdot x = b, \qquad a \neq 0,$$

lösen[3], während das Gleiche in $\mathbf{Z}$ nicht gilt[4].

Sie werden sich jetzt mit einer Familie von Strukturen auseinandersetzen, die *manchmal* (!) Körperstruktur haben! Die Sache ist recht einfach – es geht um das *Rechnen mit Resten*.
Zur Erinnerung: $R_b(a)$ bezeichnet den Rest bei Division von a durch b. Beispielsweise ist: $R_5(31) = 1, \quad R_4(12) = 0, \quad R_3(17) = 2, \ldots$
Wählen Sie nun eine natürliche Zahl n *fest*, den sogenannten *Modul*, und betrachten Sie nur die n Zahlen

$$0, 1, 2, 3, \ldots, n-1.$$

Wir bezeichnen die Menge dieser n Zahlen bequemlichkeitshalber mit $\mathcal{R}_n$:

$$\mathcal{R}_n = \{0, 1, 2, 3, \ldots, n-1\}.$$

Für $n = 7$ beispielsweise ist $\mathcal{R}_7 = \{0, 1, 2, 3, 4, 5, 6\}$.
Wenn wir nun zwei Zahlen aus $\mathcal{R}_n$ nehmen, nennen wir sie a und b, dann ist ihre Summe $a + b$ manchmal wieder eine der Zahlen $0, 1, \ldots, n-1$, und manchmal nicht. Das gleiche gilt für das Produkt. Wieder für $n = 7$ erhält man zum Beispiel

$$\begin{aligned} 2 + 3 = 5, \quad 4 + 5 = 9; \\ 2 \cdot 3 = 6, \quad 4 \cdot 5 = 20. \end{aligned}$$

Um nicht aus der Menge $\mathcal{R}_n$ "herauszufallen", vereinbart man deshalb, dass man $a + b$ bzw. $a \cdot b$ *jeweils durch den Rest bei Division durch* n ersetzt, das heisst die *neue Addition* heisst:

$$a \oplus b = R_n(a + b),$$

und die *neue Multiplikation* lautet:

$$a \odot b = R_n(a \cdot b).$$

So erhält man mit dem Modul $n = 7$ etwa

$$\begin{aligned} 2 \oplus 3 = 5, \quad 4 \oplus 5 = R_7(9) = 2; \\ 2 \odot 3 = 6, \quad 4 \odot 5 = R_7(20) = 6. \end{aligned}$$

Aufgabe 8 *Stellen Sie eine Additions- und eine Multiplikationstabelle für den Modul* $n = 4$ *auf, das heisst, füllen Sie folgende Tabellen aus:*

[3]Sei $a = \frac{p}{q}, b = \frac{r}{s}$. Dann ist $x = \frac{q \cdot r}{p \cdot s}$ Lösung von $a \cdot x = b$.

[4]Die Gleichung $5 \cdot x = 30$ ist zwar in $\mathbf{Z}$ lösbar: die Lösung ist $x = 6$. Hingegen gibt es offensichtlich keine ganze Zahl x, für die $4 \cdot x = 30$ gilt.

$\oplus$	*0*	*1*	*2*	*3*
0				
1				
2				
3				

$\odot$	*1*	*2*	*3*
1			
2			
3			

Aufgabe 9 *Ebenso für* $n = 5$.

Aufgabe 10 *Ebenso für* $n = 6$.

Aufgabe 11 *Ebenso für* $n = 7$.

Aufgabe 12 *Betrachten Sie die Fälle* $n = 4, 5, 6, 7$. *Wie steht es mit der Lösbarkeit der Gleichungen*

$$a \oplus x = b\,?$$

Aufgabe 13 *Und wie steht es mit der Lösbarkeit der Gleichung*

$$a \odot x = b, \quad a \neq 0\,?$$

Aufgabe 14 *Es sei* n *(irgend) eine Primzahl und* $a \in \mathcal{R}_n, a \neq 0$. *Wir behaupten: Bildet man* $1 \odot a, 2 \odot a, \ldots, (n-1) \odot a$, *erhält man wieder die Zahlen* $1, 2, 3, \ldots, n-1$ *(allerdings in veränderter Reihenfolge wenn* $a \neq 1$*).*
a) Überprüfen Sie die Behauptung anhand der Tabellen in den Aufgaben 8 - 11.
b) Beweisen Sie die Behauptung!
Tipp: Zeigen Sie, dass folgendes gilt: Sind i *und* j *verschiedene Zahlen aus* $\mathcal{R}_n$, *dann sind auch* $i \odot a$ *und* $j \odot a$ *verschieden. Wieso reicht das, um die Behauptung zu beweisen?*

Bei den rationalen Zahlen (Brüchen) unterscheidet man gewisse nicht, man sagt "sie hätten den gleichen Wert" oder "stellten dieselbe Zahl dar". Hier ist ein Beispiel. Obwohl

$$\frac{1}{2}, \frac{2}{4}, \frac{3}{6}, \frac{4}{8}, \frac{5}{10}, \ldots$$

lauter verschiedene Objekte sind, *identifiziert* man sie, und schreibt (sogar)

$$\frac{1}{2} = \frac{2}{4} = \frac{3}{6} = \frac{4}{8} = \frac{5}{10} = \ldots$$

Allgemein indentifiziert man zwei Brüche $\frac{p}{q}$ und $\frac{p'}{q'}$ und schreibt

$$\frac{p}{q} = \frac{p'}{q'},$$

falls

$$p \cdot q' = q \cdot p'$$

gilt.

Wenn wir zum Rechnen mit Resten zurückkehren, dann ist die Einschränkung auf die Zahlen $0, 1, 2, , \ldots, n-1$ (wobei n der gewählte Modul ist) ungefähr vergleichbar mit der Forderung beim Bruchrechnen nur *gekürzte Brüche* zu verwenden.

Das ist zwar möglich, aber fürs Rechnen wäre es doch sehr unpraktisch. Analog ist es mit dem Rechnen mit Resten. Statt sich auf die Zahlen $0, 1, 2, \ldots, n-1$ zu beschränken, kann man ohne weiteres auch alle Zahlen in $\mathbf{Z}$ zulassen, aber man muss dann (wie beim Bruchrechnen) gewisse Zahlen *"identifizieren"*, also einander als *"gleichwertig"*, quasi "nicht der Unterscheidung würdig", betrachten.
Im Zusammenhang mit dem Rechnen mit Resten "unterscheidet man zwischen zwei Zahlen a und b nicht, wenn sie *um ein Vielfaches des Moduls n auseinander liegen.*
Anders formuliert: a und b werden für das Rechnen mit Resten "nicht unterschieden", wenn ihre Differenz, (also $a-b$, oder auch $b-a$, wie Sie mögen) *durch den Modul n teilbar ist.*
Hier ist ein Beispiel. Bei Verwendung des Moduls $n = 7$ unterscheidet man 21 und 35 nicht, weil $21 - 35 = -14 = (-2) \cdot 7$ ist. Hingegen sind 20 und 37 bezüglich des Moduls 7 "nicht gleich".
Im Hinblick auf eine *Kurznotation*[5] ist man nicht ganz so "salopp" wie in der Bruchrechnung! Statt

$$a = b$$

zu schreiben, *falls $a - b$ durch n teilbar ist*, schreibt man:

$$a \equiv b \mod n$$

und sagt:

a ist kongruent b modulo n

Aufgabe 15 *Welche der folgenden Behauptungen sind wahr?*

$$\begin{array}{lrcrl} i) & 1000 & \equiv & 4 & \mod 7. \\ ii) & 1000 & \equiv & 6 & \mod 7. \\ iii) & -1000 & \equiv & -6 & \mod 7. \\ iv) & -1000 & \equiv & 2 & \mod 7. \end{array}$$

Aufgabe 16 *Beweisen Sie folgende Behauptungen!*
a) Voraussetzung: $a \equiv b \mod n$ *und* $c \equiv d \mod n$.
Behauptung:

$$\begin{array}{lrcrl} i) & a \pm c & \equiv & b \pm d & \mod n. \\ ii) & a \cdot c & \equiv & b \cdot d & \mod n. \end{array}$$

b) Voraussetzung: $a \equiv b \mod n$ *und* $b \equiv c \mod n$.
Behauptung:

$$iii)\ a \equiv c \mod n.$$

Aufgabe 17 $R_7(123 \cdot 257 \cdot 425) = ?$ *Bitte wenden Sie die Erkenntnisse aus der vorigen Aufgabe an! Das Ziel ist, mit möglichst "kleinen" Zahlen zu rechnen.*

[5]Man möchte ja nicht immer die umständliche Formulierung "im Zusammenhang mit dem Rechnen mit Resten unterscheidet man zwischen den Zahlen ... und .... nicht" verwenden müssen!

Als Verallgemeinerung der letzten Aufgabe folgt unter Verwendung der Behauptungen in der vorletzten zum Beispiel für die Berechnung eines Restes eines Produktes von drei Zahlen:

$$\boxed{R_n(a \cdot b \cdot c) = R_n(R_n(R_n(a) \cdot R_n(b)) \cdot R_n(c))}$$

sowie analoge Formeln für mehr als drei Faktoren.
Die RSA-Verschlüsselung lebt davon, dass man

$$R_n(m^c)$$

für hohe Potenzen, also grosse Werte von c, *effizient berechnen* kann. Der Buchstabe m steht hier für "message", also "Nachricht".

Beispiel 1 *Bestimme* $R_{143}(2^{103})$.
Die Grunddee ist, den Exponenten 103 als Summe von "Zweierpotenzen" wie folgt darzustellen: 103=64+32+4+2+1. Daraus folgt für 2^{103} *die folgende Produktdarstellung*

$$2^{103} = 2^{64} \cdot 2^{32} \cdot 2^4 \cdot 2^2 \cdot 2.$$

Nun berechnet man der Reihe nach:
$R_{143}(2) = 2,\ R_{143}(2^2) = 4,\ R_{143}(2^4) = R_{143}(16) = 16,\ \ R_{143}(2^8) = R_{143}(256) = 113,$
$R_{143}(2^{16}) = R_{143}(2^8 \cdot 2^8) = R_{143}(113^2) = R_{143}(12769) = 42,$
$R_{143}(2^{32}) = R_{143}(2^{16} \cdot 2^{16}) = R_{143}(42^2) = R_{143}(1764) = 48,$
$R_{143}(2^{64}) = R_{143}(48^2) = R_{143}(2304) = 16.$
Und schliesslich:
$R_{143}(2^{103}) = R_{143}(16 \cdot 48 \cdot 16 \cdot 4 \cdot 2) = R_{143}(768 \cdot 128) = R_{143}(53 \cdot 128) = R_{143}(6784) = 63.$

Aufgabe 18 *Bestimmen Sie:*
i) $R_{89}(2^{44})$.
ii) $R_{79}(3^{100})$.

Frage 4 *Können Sie folgende Gleichung lösen?*

$$23x \equiv 1 \mod 56.$$

3 Der kleine Satz von Fermat

Pierre de Fermat (1601-1665) war eigentlich Jurist im französischen Toulouse. Mathematik betrieb er als Hobby. Doch er hat in der Mathematik Spuren hinterlassen. An seiner berühmtesten Vermutung[6] haben sich viele Mathematiker die Zähne ausgebissen. Aber seit 1995 ist die Fermatsche Vermutung bewiesen, also keine Vermutung mehr, sondern ein (mathematischer) Satz. Man nannte die Vermutung manchmal "Fermats Letzten, oder Grossen Satz". In Zukunft wird man wohl vom *Satz von Fermat-Wiles* sprechen, weil es Andrew Wiles war, der die Vermutung von Fermat nach 350 Jahren endlich beweisen konnte.

Der Schlüssel zur RSA-Verschlüsselung ist der sogenannte *kleine Satz von Fermat.*

	3	4	5	6	7	8	9	10	11	12	13
2	.	.	.	.	.	.	.	.	.	.	.
3		.	.	.	.	.	.	.	.	.	.
4			.	.	.	.	.	.	.	.	.
5				.	.	.	.	.	.	.	.
6					.	.	.	.	.	.	.
7						.	.	.	.	.	.
8							.	.	.	.	.
9								.	.	.	.
10									.	.	.
11										.	.
12											.

Tabelle 1: $a^b \mod b$. Linker Rand der Tabelle: Werte von a. Oberer Rand der Tabelle: Werte von b.

Aufgabe 19 *Füllen Sie die obere rechte Hälfte der folgenden Tabelle aus. Einzutragen ist $R_b(a^b)$ (für $a < b$). Die Werte für a stehen am linken Rand, diejenigen für b am oberen. Erkennen Sie etwas Bemerkenswertes? Notieren Sie Ihre Beobachtungen!*

Aufgabe 20 *a) Ist folgende Aussage richtig: "Aus $c \cdot a \equiv c \cdot b \mod n$ folgt $a \equiv b \mod n$"? Können Sie ein Beispiel angeben, für welches diese Behauptung nicht stimmt?*
b) Die in a) formulierte Aussage stimmt, wenn c und n teilerfremd sind. Erbringen Sie einen Beweis.

Aufgrund der Tabelle in Aufgabe 19 vermutet man die folgende, als *kleiner Satz von Fermat* bezeichnete Behauptung.

Satz 5 *(Kleiner Satz von Fermat, Version 1).*
Falls p eine Primzahl ist, gilt für $0 \leq a < p$:

$$R_p(a^p) = a.$$

Eine andere Formulierung des Satzes lautet:

Satz 6 *(Kleiner Satz von Fermat, Version 2).*
Falls p eine Primzahl ist, gilt für $a \in \mathbf{Z}$:

$$a^p \equiv a \mod p.$$

Frage 5 *Wie folgt aus der 2. Formulierung die erste?*

[6] Sie besagt, dass die Gleichung $x^n + y^n = z^n$ für $n > 2$ keine (nichttrivialen) ganzzahligen Lösungen x, y, z hat.

Eine weitere Formulierung lautet:

Satz 7 *(Kleiner Satz von Fermat, Version 3).*
Falls p eine Primzahl ist und $a \in \mathbf{Z}$ nicht Vielfaches von p ist, gilt:

$$a^{p-1} \equiv 1 \mod p.$$

Aufgabe 21 *Zeigen Sie, dass aus der zweiten Formulierung die dritte folgt (Tipp: Aufgabe 20, Teil b) benützen) und umgekehrt.*

3.1 Zum Beweis des Kleinen Satzes von Fermat

Aufgabe 22 *Beweisen Sie den Kleinen Satz von Fermat (in der 2. Formulierung) für $p = 2, 3, 5$, eventuell unter Verwendung von Identitäten wie:*

$$\begin{aligned} a^2 - a &= a \cdot (a+1), \\ a^3 - a &= (a-1) \cdot a \cdot (a+1), \\ a^5 - a &= (a-1) \cdot a \cdot (a+1) \cdot (a^2+1). \end{aligned}$$

In Aufgabe 22 angedeutete Beweismethode wird in der Durchführung offenbar sukzessive unbequemer.

Aufgabe 23 *Beweisen sie den Kleinen Fermat (in der 2. Formulierung) für $p = 7$ mit vollständiger Induktion, d.h. zeigen Sie:*

I) *Die Behauptung stimmt für $a = 1$ (Verankerung).*

II) *Falls die Behauptung für irgend eine natürliche Zahl $a \geq 1$ gilt, gilt sie auch für $a + 1$ anstelle von a (Induktionsschritt).*

Tipp: Aus dem "Pascalschen Dreieck" folgt

$$(a+1)^7 = a^7 + 7a^6 + 21a^5 + 35a^4 + 35a^3 + 21a^2 + 7a + 1.$$

Aufgabe 24 *Begründen Sie, warum die Beweismethode von Aufgabe 23 auch für $p = 11$ funktioniert.*

Aufgabe 25 *Welche Eigenschaft der "Entwicklung" von $(a+1)^n$ muss man kennen, um einzusehen, dass die Beweismethode der Aufgaben 23, 24 für* jede *Primzahl p funktioniert? Wieso gilt sie?*

Im folgenden erarbeiten Sie einen kurzen, eleganten Beweis des Kleinen Satzes von Fermat. Der Witz an der Sache ist ein Einfall, der nicht so offensichtlich ist.

Aufgabe 26 *Es sei p eine Primzahl und $a \in \mathbf{N}$, a kein Vielfaches von p. Es geht nun um die $p - 1$ Zahlen:*

$$a,\ 2a,\ 3a,\ \ldots, (p-1)a. \tag{1}$$

Die Behauptung ist: Bis auf die Reihenfolge lassen sie sich wie folgt darstellen

$$1 + k_1 p,\ 2 + k_2 p,\ 3 + k_3 p, \ldots, (p-1) + k_{p-1} p \tag{2}$$

mit nicht negativen ganzen Zahlen $k_1, k_2, \ldots, k_{p-1}$. Begründen Sie diese Behauptung. (Vergleichen Sie mit Aufgabe 14.)

Aufgabe 27 *Da es sich bei den Zahlen der Gruppen (1) und (2) um die gleichen Zahlen handelt (nur die Reihenfolge ist allenfalls eine andere), muss man dasselbe erhalten, wenn man jeweils das Produkt aller Zahlen bildet:*

$$a \cdot 2a \cdot 3a \cdot \ldots \cdot (p-1)a = (1 + k_1 p)(2 + k_2 p) \cdot \ldots \cdot (p - 1 + k_{p-1} p). \tag{3}$$

Machen Sie sich klar, dass man (3) in folgender Form schreiben kann

$$(p-1)!\, a^{p-1} = (p-1)! + lp. \tag{4}$$

Dabei ist l eine nicht negative ganze Zahl und $(p-1)!$ ist das Produkt der Zahlen 1, 2, 3, ..., $p-1$, das heisst:

$$(p-1)! = 1 \cdot 2 \cdot 3 \cdot 4 \cdot \ldots \cdot (p-1).$$

Aufgabe 28 *Begründen Sie, dass*

$$a^{p-1} \equiv 1 \mod p$$

folgt.
Tipp: Dividiert man die Beziehung (4) durch $(p-1)!$ erhält man

$$a^{p-1} = 1 + p\frac{l}{(p-1)!}.$$

$\frac{l}{(p-1)!}$ *muss eine nicht negative ganze Zahl sein. Warum?*

4 Euler und der Kleine Satz von Fermat

L. Euler[7] hat den Kleinen Satz von P. de Fermat verallgemeinert. Wir betrachten hier einen Spezialfall, der bei der RSA-Verschlüsselung zur Anwendung kommt. Statt einfach eine Primzahl, sei der Modul n jetzt das Produkt zweier verschiedener Primzahlen p, q. Also:

$$n = p \cdot q.$$

In Analogie zum Kleinen Satz von Fermat könnte man zunächst vielleicht vermuten, dass für beliebiges $a \in \mathbf{Z}$ gilt

$$a^n \equiv a \mod n.$$

Aufgabe 29 *Geben Sie ein Gegenbeispiel zu dieser Vermutung.*
Tipp: Konsultieren Sie die Tabelle in Aufgabe 19.

Wir erinnern an die 3. Formulierung des Kleinen Satzes von Fermat: Falls p Primzahl und $A \in \mathbf{Z}$ *nicht* Vielfaches von p ist, gilt: $A^{p-1} \equiv 1 \mod p$. Genau so gilt: Falls q Primzahl und $B \in \mathbf{Z}$ *nicht* Vielfaches von q ist, gilt: $B^{q-1} \equiv 1 \mod q$.
L. Euler behauptet:

[7]Der Schweizer Mathematiker Leonhard Euler (1707-1783) hat den überwiegenden Teil seines Lebens in Russland und Deutschland verbracht. Er ist einer der produktivsten Mathematiker aller Zeiten gewesen und hat zu allen damals bekannten Teilgebieten der Mathematik wichtige Beiträge geleistet.

Satz 8 *(Verallgemeinerung von Euler, Version 1).*
Seien p, q verschiedene Primzahlen und $n = p \cdot q$. Dann gilt für $a \in \mathbf{Z}$:

$$a^{(p-1)(q-1)+1} \equiv a \mod n.$$

Beweis Es muss gezeigt werden:

$$n = pq \text{ teilt } a^{(p-1)(q-1)+1} - a = a[a^{(p-1)(q-1)} - 1].$$

Da p und q verschiedene Primzahlen sind, muss gezeigt werden:

$$p \text{ teilt } a[a^{(p-1)(q-1)} - 1], \quad q \text{ teilt } a[a^{(p-1)(q-1)} - 1]. \tag{5}$$

Der Vorschlag ist, drei Fälle zu unterscheiden:
Fall 1: p teilt a, q teilt a.
Fall 2: p teilt a, q teilt a nicht.
Fall 3: a ist weder durch p noch durch q teilbar.
Im Fall 1 sind wir fertig (warum?).
Im Fall 2 ist die Richtigkeit der ersten Behauptung offensichtlich. Es bleibt die Richtigkeit der zweiten Behauptung von (5), und das heisst folgendes, zu zeigen:

$$q \text{ teilt } a^{(p-1)(q-1)} - 1.$$

Wegen $a^{(p-1)(q-1)} - 1 = (a^{p-1})^{q-1} - 1$ setzen wir $B = a^{p-1}$ und haben zu zeigen

$$q \text{ teilt } B^{q-1} - 1. \tag{6}$$

Nach Voraussetzung teilt die Primzahl q die Zahl a nicht, d.h. a ist *nicht* Vielfaches von q. Dann ist aber auch $B = a^{p-1}$ nicht Vielfaches von q (warum?). Somit folgt die Richtigkeit von (6) aus dem Kleinen Satz von Fermat.

Aufgabe 30 *Führen Sie den Beweis im Fall 3.*

Es gilt auch die folgende leicht verallgemeinerte Version des letzten Satzes.

Satz 9 *(Verallgemeinerung von Euler, Version 2).*
Seien p, q verschiedene Primzahlen und $n = p \cdot q$. Dann gilt für beliebiges $a \in \mathbf{Z}$ und $k \in \mathbf{N}$:

$$a^{k(p-1)(q-1)+1} \equiv a \mod n.$$

Aufgabe 31 *Machen Sie sich klar, dass diese 2. Version der Verallgemeinerung von Euler gilt, indem Sie überprüfen, was sich am vorhergehenden Beweis ändert.*

5 RSA-Verschlüsselung

Seien p, q zwei verschiedene, grosse Primzahlen. Ihr Produkt

$$n = p \cdot q$$

lässt sich leicht bilden. *Hingegen ist das Berechnen der beiden Faktoren p, q aus der Kenntnis von n eine aufwändige, ja praktisch unlösbare Aufgabe, wenn die Faktoren p und q genügend gross (sagen wir 200-300-stellig) sind.* Auf dieser *Erfahrung* beruht das RSA-Verfahren von Rivest, Shamir und Adleman. Wenn jemand ein Verfahren entdecken würde, mit dem auch riesige Zahlen schnell in ihre Faktoren zerlegt, faktorisiert - wie man sagt - werden könnten, dann würde das das Ende des RSA-Verfahrens bedeuten und die wirtschaftlichen, militärischen und rechtlichen Folgen wären aller Wahrscheinlichkeit nach unabsehbar. Im Folgenden gehen wir davon aus, dass jemand, der das benutzte n, jedoch *nicht* p und q kennt, p und q auch mit noch so viel Computereinsatz *nicht* bestimmen kann!
Das RSA-Verfahren benötigt des weiteren zwei natürliche Zahlen

$$c \text{ (für } \underline{c}\text{hiffrieren) und } d \text{ (für } \underline{d}\text{echiffrieren),}$$

die der Bedingung

$$c \cdot d \equiv 1 \qquad \text{mod} \quad (p-1)(q-1)$$

genügen. Genauer: *Man braucht natürliche Zahlen c, d und k, so dass gilt*:

$$\boxed{c \cdot d = 1 + k(p-1)(q-1). \qquad (7)}$$

Man kann c, d wie folgt konstruieren. Man wähle eine zu $r = (p-1)(q-1)$ teilerfremde, natürliche Zahl $c > 1$. Da daher $(c, r) = 1$ gilt, kann man mit Hilfe des Euklidschen Algorithmus, siehe Satz 2, ganze Zahlen u, v finden, so dass gilt:

$$1 = u \cdot c + v \cdot r. \qquad (8)$$

Falls $u > 0$ gilt, muss $v < 0$ sein, da $c > 1,\ r > 1$. Folglich kann man schreiben:

$$u \cdot c = 1 + (-v) \cdot r$$

und (7) ist mit $d = u$ und $k = -v$ erfüllt.
Falls $u < 0$ gilt, schreiben wir (8) in der Form

$$1 = (u + lr)c + (v - lc)r,$$

beziehungsweise

$$(u + lr)c = 1 + (lc - v)r.$$

Indem man $l \in \mathbf{N}$ genügend gross wählt, ist (7) mit $d = u + lr$ und $k = lc - v$ erfüllt.

Aufgabe 32 *Es sei $p = 11, q = 13, c = 103$. Wie würden Sie d wählen?*

An dieser Stelle tritt – sagen wir – Anna auf. Sie habe Primzahlen p und q gewählt, ihr Produkt $n = p \cdot q$ berechnet, und mit Hilfe des Euklidischen Algorithmus natürliche Zahlen c, d, k bestimmt, so dass (7) gilt, also:

$$c \cdot d = 1 + kr, \quad r = (p-1)(q-1).$$

Beachten Sie: Weil Anna nicht nur n kennt, sondern die beiden Faktoren p und q, kann sie leicht den Wert von r berechnen und zu einem beliebigen c ein d bestimmen, so dass (7) gilt.

Anna veröffentlicht nun die Zahlen

$$\boxed{c} \text{ und } \boxed{n}$$

und informiert, dass das ihr RSA-Schlüssel ist, mit dem man ihr geheime Botschaften übermitteln soll.

Alle RSA-Benützer wissen nun, dass man Anna wie folgt geheime Botschaften übermitteln kann.
1. Schritt: Zuerst wird die Botschaft mit ASCII in einen Block von Zahlen übersetzt; dann wird der Block in Portionen $m_1, m_2 \ldots$ aufgeteilt, wobei $m_j < n$ gelten muss. Sei m ein solcher Abschnitt, das heisst eine natürliche Zahl kleiner als n.
2. Schritt: m wird *verschlüsselt, chiffriert*, und zwar nach folgender Vorschrift

$$\overline{m} = R_n(m^c) \quad \text{(c)}$$

Zur Erinnerung: $R_n(m^c)$ bezeichnet den Rest von m^c bei Division durch n.

Aufgabe 33 *Es sei $p = 11, q = 13, c = 103$ und die Botschaft m an Anna laute: $m = 19$. Bestimmen Sie $\overline{m}$.*

$\overline{m}$ kann nun vom Verfasser der Botschaft m *ohne Schutzmassnahmen*, z.B. via Zeitungsinserat an Anna weitergegeben werden.
Obwohl öffentlich bekannt ist, wie man chiffriert, das heisst, wie man aus m die verschlüsselte Botschft $\overline{m}$ findet – nämlich nach der Vorschrift (c) – wobei n und c öffentlich bekannte Zahlen sind, erfordert (jedenfalls nach allem, was man bis heute weiss) die Berechnung von m aus $\overline{m}$ die Kenntnis der Zahl d. *Die Zahl d aber kennt nur Anna.*
(Natürlich – wenn es jemandem gelingt, aus der Kenntnis von n die Faktoren p, q zu ermitteln, kann diese Person – genau wie Anna – mit Hilfe des Euklidschen Algorithmus ein geeignetes d bestimmen. Aber wie gesagt: Wenn die Primzahlen p, q gross genug gewählt sind, dann ist nach heutigem Wissensstand die Aufgabe, aus $n = pq$ die Faktoren p, q zu bestimmen, de facto unlösbar.)
Was macht Anna nun mit der (zum Beispiel aus der Zeitung erhaltenen) chiffrierten Botschaft $\overline{m}$? Sie berechnet:

$$\tilde{m} = R_n(\overline{m}^d) \qquad \text{(d)}$$

Die *Behauptung* ist: Es gilt

$$\tilde{m} = m$$

Damit erfährt sie den nur für sie bestimmten Inhalt. Es bleibt einzusehen, dass $\tilde{m} = m$ gilt. Nach Definiton von $R_n(m^c) = \overline{m}$ gilt:

$$m^c = j_1 \cdot n + \overline{m}$$

wobei j_1 eine nichtnegative ganze Zahl bezeichnet. Also ist $\overline{m} = m^c - j_1 \cdot n$ und somit

$$\begin{aligned} \overline{m}^d &= (m^c - j_1 \cdot n)^d = (m^c)^d + j_2 \cdot n \\ &= m^{cd} + j_2 \cdot n. \end{aligned}$$

Dabei ist j_2 eine ganze Zahl. Im zweiten Schritt wurde benützt, dass aus den *binomischen Formeln* mit Hilfe des Pascalschen Dreiecks folgt:

$$(\alpha + \beta \cdot n)^d = \alpha^d + \gamma \cdot n.$$

Dabei sind d, n natürliche, α, β ganze Zahlen; γ ist ebenfalls eine ganze Zahl, die sich aus α, β, d, n ergibt.

Aufgabe 34 *Begründen Sie die obige Formel für $d = 1, 2, 3$.*

Aus $\overline{m}^d = m^{cd} + j_2 \cdot n$ folgt mit der Tatsache, dass

$$c \cdot d = 1 + k(p-1)(q-1)$$

gilt, k eine nichtnegative ganze Zahl,

$$\overline{m}^d = m^{1+k(p-1)(q-1)} + j_2 \cdot n.$$

Nun endlich kommt die *Eulersche Verallgemeinerung des Kleinen Satzes von Fermat* zum Zug. Gemäss Satz 9 gilt:

$$m^{1+k(p-1)(q-1)} = m + j_3 \cdot n$$

und daher

$$\overline{m}^d = m + j_4 \cdot n$$

mit $j_4 = j_2 + j_3$. Da nun $\overline{m}^d \geq 1$ gilt, und nach Voraussetzung $0 < m < n$ gilt, kann j_4 nicht negativ sein, und daher folgt:

$$\tilde{m} = R_n(\overline{m}^d) = m.$$

Das heisst: *Mit ihrer geheimen Zahl d ist Anna unter Verwendung der Vorschrift* (d) *tatsächlich in der Lage, an sie gerichtete, öffentlich übermittelte Botschaften zu entschlüsseln.*

Aufgabe 35 *Es sei weiterhin $p = 11, q = 13, c = 103$. In der vorletzten Aufgabe haben Sie d dazu bestimmt, und in der letzten Aufgabe haben Sie $\overline{m}$ zur Botschaft $m = 19$ berechnet. Dechiffrieren Sie nun $\overline{m}$ mittels d.*

Zum Schluss noch ein etwas grösseres Beispiel. Anna wähle als p Primzahl Nummer 1000000000 und als q Primzahl Nummer 1000005000. Der Befehl Prime[.] des Programms Mathematica liefert ihr

$$p = 22801763489, \quad q = 22801881559.$$

Daraus folgt

$$n = pq = 519923110412508599351.$$

Nun muss sie die Zahlen c und d so bestimmen, dass (7) gilt. Es ist $r = (p-1)(q-1) = 519923110366904954304$. Sie wählt

$$c = 4699873.$$

Mithilfe des Mathematica-Befehls GCD$[c, r]$, der den grössten gemeinsamen Teiler der beiden Zahlen c und r bestimmt, erhält man GCD$[c, r] = 1$, das heisst c und r sind teilerfremd. Der Mathematica-Befehl PowerMod[c,-1,r] liefert für d

$$d = \text{PowerMod}[c,-1,r] = 252883827627895253473.$$

Tatsächlich ergibt die Division

$$\frac{cd-1}{r} = k = 2285957.$$

Anna veröffentlicht nun in der Zeitung die beiden Zahlen

$$n = 519923110412508599351, \quad c = 4699873.$$

Ihr Freund Beat hat nur darauf gewartet und beschliesst, ihr die folgende Botschaft zu schicken

RSA IST EIN GENIESTREICH

Diesen Text übersetzt er zuerst nach ASCII in einen Block von Zahlen. Für die Grossbuchstaben A, B, C, ... verwendet ASCII der Reihe nach die Zahlen 65, 66, 67, ... Ein Leerschlag erhält die Zahl 32. Das ergibt folgenden Zahlenstring

82 83 65 32 73 83 84 32 69 73 78 32 71 69 78 73 69 83 84 82 69 73 67 72

Beat bildet daraus drei Zahlen m_1, m_2, m_3

$$m_1 = 82836532738384326973,\ m_2 = 78327169787369838482,\ m_3 = 69736772,$$

die alle kleiner als n sind. Weil

$$\text{PowerMod}[m,c,n] = R_n(m^c)$$

gilt, kann Beat mit Mathematica leicht

$$\overline{m}_1 = R_n(m_1^c) = 479529267290958755149$$

berechnen, und ebenso

$$\overline{m}_2 = R_n(m_2^c) = 428935216287316816132,$$

$$\overline{m}_3 = R_n(m_3^c) = 135766055009022893446.$$

Diese drei Zahlen veröffentlicht er in der Zeitung, in der sie Anna alsbald entdeckt. Sie berechnet nun, ebenfalls mit dem Mathematica-Befehl PowerMod sukzessive PowerMod[$\overline{m}_1$,d,n], PowerMod[$\overline{m}_2$,d,n], PowerMod[$\overline{m}_3$,d,n] und findet die drei Zahlen

8283653273838432697 3,

7832716978736983848 2,

69736772.

Indem sie den ASCII Code rückwärts übersetzt, findet sie Beats Mitteilung

RSA IST EIN GENIESTREICH

und ist enttäuscht: So eine Banalität hätte er nun wirklich nicht zu verschlüsseln brauchen!

Literatur

[1] A. Beutelspacher *Kryptografie*, Vieweg 1991[2].

[2] A. Beutelspacher *Geheimsprachen – Geschichte und Techniken*, Verlag C. H. Beck 1997.

[3] D. M. Davis *The Nature and Power of Mathematics*, Princeton University Press, 1993.

[4] J. Meyer *Einblick in die Kryptografie*, in: F. Förster, H.-W- Henn, J. Meyer (Hersg.): Materialien für einen Realitätsnahen Mathematikunterricht, Band 6 Computeranwendungen, divverlag franzbecker, 2000.

8.2.05/UK+JK