Kryptographie

Peter Lesky, Universität Stuttgart

Der vorliegende Text beschreibt einen Kurs über Kryptographie, der im Sommer 2006 im Schülersminar Mathematik für die Klassenstufen 8–10 abgehalten wurde. Der Kurs umfasst 6 dicht gepackte Doppelstunden, die Gliederung ist aus dem Text ersichtlich. Das Ziel des Kurses bestand darin, den Diffie-Hellman Schlüsseltausch und das RSA-Verfahren zu verstehen.

Die Aufgaben wurden von den Schülern in Dreier- oder Zweiergruppen gelöst. Oft habe ich verschiedene Aufgabenteile von verschiedenen Gruppen lösen lassen, und im Anschluss präsentierte dann aus jeder Gruppe eine Schülerin oder ein Schüler die Lösung an der Tafel oder gab das Ergebnis an.

Als Grundlage wurden die Bücher

- Einführung in die Kryptographie, Johannes Buchmann, Springer, 2004
- Zahlentheorie für Einsteiger, Andreas Bartholomé ; Josef Rung ; Hans Kern, Vieweg, 2001

verwendet. Das Buch von Buchmann ist für jüngere Schüler etwas zu trocken, man findet aber alles Nötige darin. Das andere Buch ist leichter zu lesen, dafür ist nicht der ganze Stoff unseres Seminars enthalten.

Bei meinen Vorbereitungen war mir wichtig, dass den Schülerinnen und Schülern Mathematik im eigentlichen Sinn nahegebracht wird: Viele konkrete Probleme können durch Ausprobieren gelöst werden. Aber danach müssen die Begriffe und die Problemstellung richtig definiert und die Lösungsmethoden in möglichst großer Allgemeinheit bewiesen werden. Erst dann ist das Problem als gelöst anzusehen:

$$\text{Probieren} \rightarrow \text{Vermuten} \rightarrow \text{Definieren} \rightarrow \text{Satz formulieren} \rightarrow \text{Beweisen}$$

Trotzdem wurden aus Zeitgründen nicht alle Sätze bewiesen. Falls mehr Zeit zur Verfügung steht, könnten folgende Themen noch ergänzt werden:

- Primzahlen,
- Teilen mit Rest,
- Eindeutigkeit der Primfaktorzerlegung.

Die zugehörigen Sätze werden alle benötigt.

21. Februar 2007 Peter Lesky

Universität Stuttgart
Schülerseminar Klasse 8–10

PD. Dr. P. Lesky
10. Mai 2006

Diophantische Gleichungen

Was ist eine diophantische Gleichung?

Gegeben:	$a, b, c \in \mathbb{N}$	$(\mathbb{N} = \{1, 2, 3, 4, \ldots\})$
Gesucht:	$x, y \in \mathbb{Z}$	$(\mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\})$
so dass	$ax + by = c$	

Aufgaben: Versuche, Lösungen zu finden. Falls du vermutest, dass es keine Lösung gibt, begründe deine Vermutung:

a) $3x + 7y = 1$

b) $5x + 5y = 1$

c) $5x + 15y = 50$

d) $18x + 12y = 3$

e) $18x + 12y = 66$

Hinweis: Es empfiehlt sich, verschiedene Schülergruppen mit verschiedenen Aufgabenteilen beginnen zu lassen. Dann müssen nicht alle Gruppen jeden Aufgabenteil gelöst haben, es reicht, wenn am Schluss alle Lösungen an der Tafel stehen. Z.B. kann eine Gruppe mit a), eine mit c) und eine mit d) beginnen und zyklisch wieder vorne anfangen, wenn d) erreicht ist. Dann sollten die Schüler ihre Vermutungen äußern, wann es eine Lösung gibt, und wann nicht.

Beobachtung: Es gibt nur Lösungen, wenn $\mathrm{ggT}(a, b)$ Teiler von c ist.

Größter gemeinsamer Teiler ist definiert durch

$$\mathrm{ggT}(a, b) \;:=\; \max\{k \in \mathbb{N} \mid k \text{ ist Teiler von } a \text{ und von } b\}$$

Aufgaben: Untersuche, ob $\mathrm{ggT}(a, b)$ Teiler von c ist, und rate gegebenenfalls ein Lösungspaar (x, y):

a) $5x + 15y = 5$

b) $18x + 12y = 6$

c) $300x + 468y = 12$
Hinweis: Du kannst die Gleichung vereinfachen, indem du durch $\mathrm{ggT}(a, b)$ teilst.

Um anzudeuten, dass zwei Zahlen eine Lösung bilden, schreiben wir diese zwei Zahlen in eine Klammer: (x, y) bezeichnet eine Lösung. Die Zahlen x, y sollen ganze Zahlen sein, daher schreibt man $(x, y) \in \mathbb{Z} \times \mathbb{Z}$. Das bedeutet, dass die erste Komponente x von (x, y) Element von $\mathbb{Z}$ sein soll, und die zweite Komponente y auch.

Satz: Seien $a, b, c \in \mathbb{N}$. Die Gleichung

$$ax + by \;=\; c$$

besitzt genau dann mindestens eine Lösung $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, wenn $\mathrm{ggT}(a, b)$ Teiler von c ist.

Wir wollen diesen Satz beweisen. Dazu brauchen wir ein paar Vorbereitungen:

Teilen mit Rest:
$$\begin{array}{rcl} 13:4 &=& 3 \text{ Rest } 1 \quad \Leftrightarrow \quad 13 = 3\cdot 4+1 \\ 223:25 &=& 8 \text{ Rest } 23 \quad \Leftrightarrow \quad 223 = 8\cdot 25+23 \end{array}$$

Allgemein: Teile a durch b mit Rest:

$$a = q\cdot b + r, \qquad 0 \le r < b$$

Wichtig ist, dass r echt kleiner als b ist, sonst könnte man q um 1 größer wählen (Alle Zahlen sind ganze Zahlen).

Witzig ist die Rechnung, wenn a negativ ist. Teile -13 durch 4 mit Rest:

$$-13 = (-4)\cdot 4 + 3$$

Hinweis: Der Beweis dieses Satzes wurde aus Zeitgründen weggelassen.

Hilfssatz: Es gibt Zahlen $x_0, y_0 \in \mathbb{Z}$, so dass $ax_0 + by_0 = \text{ggT}(a,b)$.

Beweis: Hier wird ein häufig verwendetes Prinzip verwendet. Es ist einfacher, zunächst die Menge **aller** Zahlen zu untersuchen, die durch $ax+by$ gebildet werden können:

$$R := \{ax + by \mid x,y \in \mathbb{Z} \ \wedge \ ax+by > 0\}$$

(R ist definiert als die Menge aller Zahlen $ax+by$, für die x,y ganze Zahlen sind und für die $ax+by>0$ gilt.)
Wir setzen nun $g := \min(R)$, d.h. g ist das kleinste Element von R. Wir vermuten, dass $g = \text{ggT}(a,b)$ gilt und beweisen dies nun.
Nach der Wahl von g gibt es Zahlen $x_0, y_0 \in \mathbb{Z}$, so dass $g = ax_0 + by_0$.

1) Wir zeigen: $\text{ggT}(a,b)$ teilt g:
$\text{ggT}(a,b)$ teilt a und b
$\Rightarrow$ $\text{ggT}(a,b)$ teilt ax_0 und by_0
$\Rightarrow$ $\text{ggT}(a,b)$ teilt $ax_0 + by_0 = g$

2) Wir zeigen: g teilt $\text{ggT}(a,b)$:
Teile a durch g mit Rest:

$$a = qg + r \text{ mit } 0 \le r < g$$

Diese Gleichung wird nach r aufgelöst und $g = ax_0 + by_0$ eingesetzt:

$$\begin{array}{rcl} r &=& a - qg \\ &=& a - q(ax_0 + by_0) \\ &=& a - qax_0 - qby_0 \\ &=& a(1-qx_0) + b(-qy_0) \end{array}$$

Du siehst, dass r in der Form $r = ax+by$ dargestellt werden kann. Es gibt jetzt zwei Möglichkeiten: $r \in R$ oder $r = 0$. $r \in R$ kann nicht sein, da $r < g$ gilt und g die kleinste Zahl aus R war. Also muss $r = 0$ sein:

$$a = qg + 0, \text{ das bedeutet: } g \text{ ist Teiler von } a$$

Dasselbe kann man nun mit b machen. Führe das selber durch. Dadurch beweist man, dass g Teiler von b ist.
Da g Teiler von a und von b ist, ist g Teiler von $\text{ggT}(a,b)$.

Aus 1) und 2) folgt nun $g = \text{ggT}(a, b)$, also $\text{ggT}(a, b) = g = ax_0 + by_0$.

Beweis des Satzes: 1) Sei (x, y) Lösung von $ax + by = c$. Dann ist $\text{ggT}(a, b)$ Teiler von a und von b, also auch von $ax + by = c$. Damit ist bewiesen:

Gibt es eine Lösung von $ax + by = c$, so ist $\text{ggT}(a, b)$ Teiler von c.

2) Sei $\text{ggT}(a, b)$ Teiler von c: $c = q\,\text{ggT}(a, b)$.
Aus dem Hilfssatz: $c = q(ax_0 + by_0) = a(qx_0) + b(qy_0)$.
Also ist eine Lösung durch $x = qx_0$, $y = qy_0$ gegeben. Dies beweist:

Ist $\text{ggT}(a, b)$ Teiler von c, so besitzt $ax + by = c$ mindestens eine Lösung.

Hausaufgaben oder Aufgaben (je nach Zeit) **oder für Beginn nächste Einheit:**
Suche möglichst viele verschiedene Lösungen. Kannst du ein Bildungsgesetz erkennen?

a) $3x + 2y = 1$

b) $3x + 9y = 3$

c) $7x + 11y = 1$

Universität Stuttgart
Schülerseminar Klasse 8–10

PD. Dr. P. Lesky
24. Mai 2006

Diophantische Gleichungen, Teil 2

Erinnerung: Seien $a, b, c \in \mathbb{Z}$ gegeben. Die Gleichung

$$ax + by \;=\; c$$

besitzt genau dann Lösungen $(x, y) \in \mathbb{Z} \times \mathbb{Z}$, wenn $\mathrm{ggT}(a, b)$ Teiler von c ist.

Aufgaben: Untersuche, ob es Lösungen gibt, und bestimme gegebenfalls möglichst alle Lösungen.

a) $45x + 75y = 25$,

b) $17x + 11y = 1$.

Hinweis: Es ist wichtig, dass jede Schülergruppe eine lösbare und eine unlösbare Gleichung durchprobiert hat. Danach kann man nach Vermutungen fragen, wie der Zusammenhang zwischen verschiedenen Lösungspaaren ist.

Beobachtung: Ist (x, y) eine Lösung, so ist (x_k, y_k) mit

$$\begin{array}{rcl} x_k & = & x + k \cdot \Delta x \\ y_k & = & y - k \cdot \Delta y \end{array} \qquad (k \in \mathbb{Z})$$

auch Lösung.

Betrachte

$$\begin{array}{rrrcl} & a(x+\Delta x) & + b(y-\Delta y) & = & c \\ -(& ax & + by & = & c\ ) \\ \hline & a\Delta x & - b\Delta y & = & 0 \\ \Leftrightarrow & & a\Delta x & = & b\Delta y \end{array}$$

Links steht ein Vielfaches von a, rechts ein Vielfaches von b. Das kleinstmögliche Δx ergibt sich somit aus $a\Delta x = \mathrm{kgV}(a, b)$.

Definition: $\mathrm{kgV}(a, b) := \min\{n \in \mathbb{N} : a \text{ ist Teiler von } n \ \wedge\ b \text{ ist Teiler von } n\}$.

Berechnung:

$$\begin{array}{rcl} \mathrm{kgV}(300, 468): \quad 300 & = & 2 \cdot 2 \cdot 3 \cdot 5 \cdot 5 \\ 468 & = & 2 \cdot 2 \cdot 3 \cdot 3 \cdot 13 \\ \mathrm{kgV}(300, 468) & = & 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 5 \cdot 13 \;=\; 300 \cdot 39 \;=\; 11700 \end{array}$$

Satz: $\mathrm{kgV}(a, b) \;=\; \dfrac{a \cdot b}{\mathrm{ggT}(a, b)}$.

Hinweis: Dieser Satz wurde aus Zeitgründen nicht bewiesen. Man sollte darauf hinweisen, dass er auf der eindeutigen Primfaktorzerlegung ganzer Zahlen beruht, die auch nicht bewiesen wurde.

Mögliche Lösungen: Ist (x, y) eine Lösung von $ax + by = c$, so ist die Lösung mit dem nächstgrößeren $x-$Wert $\left(x + \frac{\mathrm{kgV}(a,b)}{a}, y - \frac{\mathrm{kgV}(a,b)}{b}\right)$. Die Lösung mit dem nächstgrößeren x-Wert ist dann $\left(x + 2\frac{\mathrm{kgV}(a,b)}{a}, y - 2\frac{\mathrm{kgV}(a,b)}{b}\right)$. Lösungen mit $x-$Werten dazwischen kann es nicht geben, da der Mindestabstand der $x-$Werte $\frac{\mathrm{kgV}(a,b)}{a}$ beträgt.

Satz: Seien $a, b, c \in \mathbb{N}$, und sei (x, y) eine Lösung von

$$ax + by = c.$$

Dann sind alle Lösungen (x_k, y_k) gegeben durch

$$\begin{aligned} x_k &= x + k\,\frac{\text{kgV(a,b)}}{a} = x + k\,\frac{b}{\text{ggT}(a,b)} \\ y_k &= y - k\,\frac{\text{kgV(a,b)}}{b} = y - k\,\frac{a}{\text{ggT}(a,b)} \end{aligned} \qquad (k \in \mathbb{Z}).$$

Aufgaben: Bestimme alle Lösungen.

a) $7x + 11y = 123$,

b) $18x + 12y = 66$,

c) $144x + 400y = 48$.

Der Euklidische Algorithmus: Gesucht $\text{ggT}(468, 60)$.

Teilen mit Rest:

$$\begin{aligned} 468 &= 7 \cdot 60 + 48 \\ 60 &= 1 \cdot 48 + 12 \\ 48 &= 4 \cdot 12 + 0 \end{aligned} \quad \Rightarrow \quad \text{ggT}(468, 60) = 12$$

Probe:

$$\left.\begin{aligned} 468 &= 2^2 \cdot 3^2 \cdot 13 \\ 60 &= 2^2 \cdot 3 \cdot 5 \end{aligned}\right\} \quad \Rightarrow \quad \text{ggT}(468, 60) = 2^2 \cdot 3 = 12$$

Aufgaben: Berechne mit Euklidischem Algorithmus.

a) $\text{ggT}(150, 54)$,

b) $\text{ggT}(2717, 2431)$,

c) $\text{ggT}(4263, 4641)$.

Warum funktioniert das? Euklidischer Algorithmus allgemein für $a > b > 0$:

$$\begin{aligned} a &= q_1 \cdot b + r_1 \\ b &= q_2 \cdot r_1 + r_2 \\ r_1 &= q_3 \cdot r_2 + r_3 \\ &\vdots \\ r_{n-3} &= q_{n-1} \cdot r_{n-2} + r_{n-1} \\ r_{n-2} &= q_n \cdot r_{n-1} + 0 \end{aligned} \quad \Rightarrow \quad \text{ggT}(a, b) = r_{n-1}$$

Behauptung: Sei $a = q \cdot b + r$. Dann gilt $\text{ggT}(a, b) = \text{ggT}(b, r)$.

Beweis: **a)** $\text{ggT}(a, b)$ teilt $r = a - qb$ und $b \Rightarrow \text{ggT}(a, b) \leq \text{ggT}(b, r)$.

b) $\text{ggT}(b, r)$ teilt $a = qb + r$ und $b \Rightarrow \text{ggT}(b, r) \leq \text{ggT}(a, b)$.

$\Rightarrow \text{ggT}(b, r) = \text{ggT}(a, b)$.

Mehrfache Anwendung im Euklidischen Algorithmus:

$$\text{ggT}(a, b) = \text{ggT}(b, r_1) = \text{ggT}(r_1, r_2) = \ldots = \text{ggT}(r_{n-2}, r_{n-1}) = r_{n-1}.$$

Erweiterter Euklidischer Algorithmus: Bestimme (x, y), so dass $ax + by = \mathrm{ggT}(a, b)$.

Z.B. für $a = 66$, $b = 14$:

$$\begin{array}{rcl|rcll} 66 &=& 4 \cdot 14 + 10 & 10 &=& 66 - 4 \cdot 14 &= 1 \cdot 66 - 4 \cdot 14 \\ 14 &=& 1 \cdot 10 + 4 & 4 &=& 14 - 1 \cdot 10 &= (-1) \cdot \text{”} + 5 \cdot \text{”} \\ 10 &=& 2 \cdot 4 + 2 & 2 &=& 10 - 2 \cdot 4 &= 3 \cdot \text{”} - 14 \cdot \text{”} \\ 2 &=& 2 \cdot 2 & & & & \end{array}$$

$$\Rightarrow \quad \mathrm{ggT}(66, 14) \;=\; 2 \;=\; 3 \cdot 66 - 14 \cdot 14$$

Damit ist eine Lösung der Gleichung $66x + 14y = 6$ gegeben durch $(x, y) = (9, -42)$.

(Haus)Aufgaben: Bestimme alle Lösungen.

a) $119x + 143y = 4$,

b) $300x + 468y = 12$,

c) $924x + 1232y = 1848$.

Universität Stuttgart
Schülerseminar Klasse 8–10

PD. Dr. P. Lesky
14. Juni 2006

Kongruenzen und Restklassen

Ist 12345 durch 9 teilbar ? [Wie kann man das einfach feststellen?]
Quersummen $Q(12345) = 1+2+3+4+5 = 15$, $Q(15) = 6$ ist nicht durch 9 teilbar
$\Rightarrow$ 12345 ist nicht durch 9 teilbar.

Was bedeutet $Q(Q(12345)) = 6$? $12345 : 9 = 1371$ Rest 6.

Vermutung: Wiederholt gebildete Quersumme ergibt Rest beim Teilen durch 9.

Teste für: 34, 349, 6599

Kongruenz: Schreibe

$$a \equiv b \mod m \qquad (a \text{ ist kongruent zu } b \text{ modulo } m),$$

falls $a - b$ durch m teilbar ist.

Satz: $a \equiv b \mod m \;\Leftrightarrow\; a = b + km$ mit einem $k \in \mathbb{Z}$
$\Leftrightarrow$ Teilen mit Rest $a : m,\ b : m$ ergibt denselben Rest

Beweis der letzten Äquivalenz: Sei $a = k_1\, m + r_1,\ b = k_2\, m + r_2,\ 0 \le r_1, r_2 < m$.

$$\begin{aligned} r_1 = r_2 &\;\Rightarrow\; a - b = (k_1 - k_2)m \\ a - b = km &\;\Rightarrow\; a = km + b = (k + k_2)m + r_2 \overset{0\le r_1<m}{\Rightarrow} r_1 = r_2 \end{aligned}$$

Also: $12345 \equiv 6 \mod 9$, $\quad -34 \equiv 1 \mod 5$, $\quad m \equiv 0 \mod m$. Weitere Vorschläge?

Unsere Vermutung: $a \equiv Q(Q(\ldots Q(a))) \mod 9$.

Transitivität: Es gilt

$$a \equiv b \mod m \;\wedge\; b \equiv c \mod m \;\Rightarrow\; a \equiv c \mod m,$$

denn $a = b + km \;\wedge\; b = c + lm \;\Rightarrow\; a = c + (k + l)m$.

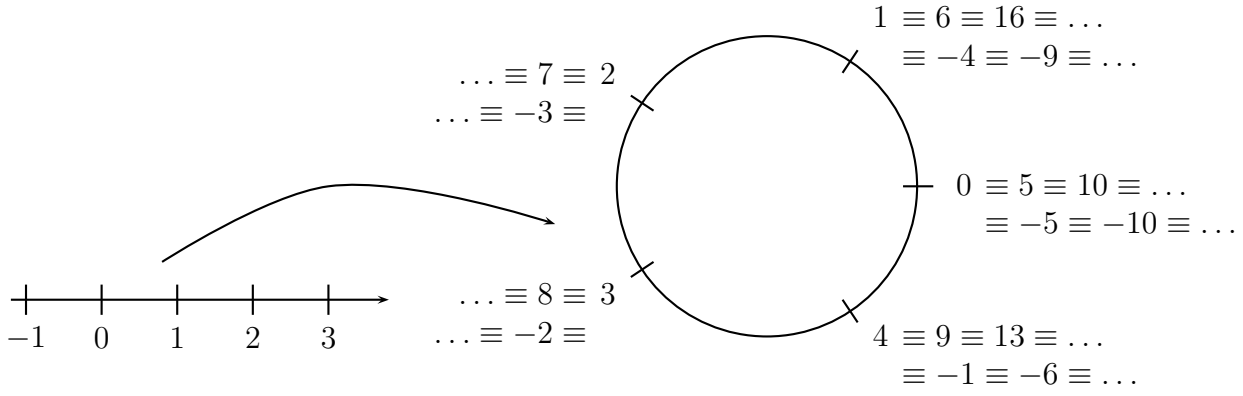
Für den Beweis unserer Vermutung reicht: $a \equiv Q(a) \mod 9$, denn

$$\begin{aligned} &a \equiv Q(a) \mod 9 \;\wedge\; Q(a) \equiv Q(Q(a)) \mod 9 \;\Rightarrow\; a \equiv Q(Q(a)) \mod 9 \\ &a \equiv Q(Q(a)) \mod 9 \;\wedge\; Q(Q(a)) \equiv Q(Q(Q(a))) \mod 9 \;\Rightarrow\; a \equiv Q(Q(Q(a))) \mod 9 \\ &\vdots \end{aligned}$$

Für den Beweis von $a \equiv Q(a) \mod 9$ benötigen wir noch etwas Vorbereitung.

Die Beziehung kongruent rollt die Zahlengerade zu einem Ring zusammen:

Z.B. $m = 5$:



$\{\ldots, -4, 1, 6, 11, \ldots\} = \{1 \pm 5k : k \in \mathbb{Z}\} =: [1]$
$\{\ldots, -3, 2, 7, 12, \ldots\} = \{2 \pm 5m : k \in \mathbb{Z}\} =: [2]$

Restklasse von a modulo 5: $[a] := \{b \in \mathbb{Z} : \quad b \equiv a \mod 5\}$

$\Rightarrow\ [1] = [6] = [-4] = \ldots$

Menge aller Restklassen: $\{[0], [1], [2], [3], [4]\} =: \mathbb{Z}/5\mathbb{Z}$.

Rechenregeln: Sei $a \equiv b \mod m$, $c \equiv d \mod m$. Dann gilt

a) $-a \equiv -b \mod m$,

b) $a + c \equiv b + d \mod m$,

c) $ac \equiv bd \mod m$,

d) $a^k \equiv b^k \mod m$.

Beweis von c): Sei $a - b = km,\ c - d = lm$.

$$\begin{aligned} \Rightarrow \quad ac - bd &= (b + km)(d + lm) - bd \\ &= bd + kmd + blm + kmlm - bd \\ &= m\underbrace{(kd + bl + klm)}_{\in\mathbb{Z}} \end{aligned}$$

Aufgabe: Beweise b) und d)

Beweis von $a \equiv Q(a) \mod 9$:

Sei a $(n+1)$-stellige Zahl:

$$a = a_n a_{n-1} \ldots a_0 = a_0 + 10a_1 + 10^2 a_2 + \ldots 10^n a_n.$$

$$\left.\begin{array}{r} 10 \equiv 1 \mod 9 \\ \Rightarrow 10^2 \equiv 1 \mod 9 \\ \vdots \\ \Rightarrow 10^n \equiv 1 \mod 9 \end{array}\right\} \Rightarrow \left.\begin{array}{l} 10a_1 \equiv a_1 \mod 9 \\ 10^2 a_2 \equiv a_2 \mod 9 \\ \vdots \\ 10^n a_n \equiv a_n \mod 9 \end{array}\right\} \Rightarrow \quad a \equiv \underbrace{a_0 + a_1 + \ldots + a_n}_{=Q(a)}$$

Hausaufgabe zur Wiederholung vom 24. Mai: Bestimme alle ganzzahligen Lösungen:

a) $119x + 143y = 4$,

b) $300x + 468y = 12$,

c) $924x + 1232y = 1848$.

Zusatzmaterial

Gehört zur Einheit, aber dafür reichte die Zeit nicht

Die Neunerprobe zur Kontrolle von Rechnungen:

$$\begin{aligned} a &\equiv Q(\ldots Q(a)) \\ b &\equiv Q(\ldots Q(b)) \\ \Rightarrow\ ab &\equiv Q(\ldots Q(ab)) \end{aligned}$$

Frage: $12345 \cdot 54321 \stackrel{?}{=} 671592745$

Probe: $12345 \equiv 6 \ \wedge \ 54321 \equiv 6 \quad \Rightarrow \quad 12345 \cdot 54321 \equiv 36 \equiv 9$

$671592745 \equiv 46 \equiv 10 \equiv 1$

Also ist das Ergebnis falsch.

Welche der folgenden Gleichungen sind falsch?

a) $12345 \cdot 54321 = 670592745$,

b) $6613598 \cdot 55500710 = 367359384654580$

c) $6613598 \cdot 55500710 = 367059384654580$

d) $6613598 \cdot 55500710 \cdot 432 = 158569654170778570$

e) $123456709 + 6789402 + 878787487 + 1232123 = 1010365721$

f) $123456709 + 6789402 + 878787487 + 1232123 = 1010265721$

Universität Stuttgart
Schülerseminar Klasse 8–10

PD. Dr. P. Lesky
5. Juli 2006

Rechnen auf dem Ring

Erinnerung:

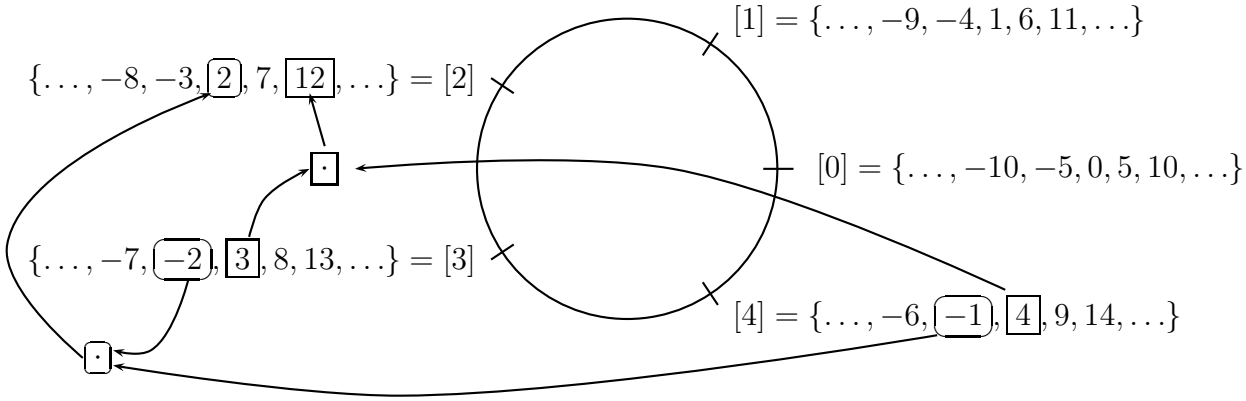
Kongruenz: $a \equiv b \mod m$ (a ist kongruent zu b modulo m), falls

- $a - b$ durch m teilbar ist,
- oder äquivalent: $a = b + km$ mit einem $k \in \mathbb{Z}$,

Restklassen: $[a] := \{b \in \mathbb{Z} : b \equiv a \mod m\} = \{a, a \pm m, a \pm 2m, a \pm 3m, \ldots\}$.

Menge aller Restklassen: $\big\{[0], [1], \ldots, [m-1]\big\} =: \mathbb{Z}/m\mathbb{Z}$.

Rechnen mit Restklassen aus $\mathbb{Z}/5\mathbb{Z}$:



Also definiere $[4] \cdot [3] := [12] = [2]$

Definiere Addition und Multiplikation: $\begin{array}{rcl} [a] + [b] & := & [a+b] \\ [a] \cdot [b] & := & [ab] \end{array}$

Dies geht, da gilt: $a \equiv c \ \wedge \ b \equiv d \ \Rightarrow \ \left\{ \begin{array}{c} a + c \equiv b + d \\ ac \equiv bd \end{array} \right.$ (Rechenregeln vom letzten Mal)

Verknüpfungstabelle für $\mathbb{Z}/4\mathbb{Z}$: Erste zwei Zeilen und Spalten zusammen, den Rest machen die Schüler alleine.

$\cdot$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

Klar ist: $[a] - [b] = [a - b]$, denn $[a - b] + [b] = [a - b + b] = [a]$.

Schüler fragen: Aber was ist $\dfrac{[a]}{[b]}$? Kann man das aus der Tabelle ablesen?

Aus Tabelle: $\dfrac{[1]}{[2]} = [3]$ denn $[2] \cdot [3] = [1]$; $\dfrac{[2]}{[3]} = [4]$ denn $[3] \cdot [4] = [12] = [2]$.

Übung: Bestimme

a) $[1]-[8]$ und $-[4]$ in $\mathbb{Z}/9\mathbb{Z}$,

b) $\dfrac{[1]}{[2]}$, $\dfrac{[1]}{[4]}$ und $\dfrac{[2]}{[4]}$ in $\mathbb{Z}/11\mathbb{Z}$,

c) $\dfrac{[1]}{[2]}$, $\dfrac{[2]}{[2]}$ in $\mathbb{Z}/4\mathbb{Z}$.

Existenz von Brüchen in $\mathbb{Z}/m\mathbb{Z}$:

$$\begin{aligned}\frac{[a]}{[b]} = [x] &\Leftrightarrow [a] = [b]\cdot[x] = [bx]\\ &\Leftrightarrow bx \equiv a \mod m\\ &\Leftrightarrow bx - a = km \text{ für ein } k\in\mathbb{Z}\\ &\Leftrightarrow b\underbrace{x}_{\text{gesucht}} + m\underbrace{(-k)}_{\text{unbekannt}} = a\end{aligned}$$

Dies ist eine diophantische Gleichung.
Wir wissen: Falls $\mathrm{ggT}(b,m)$ Teiler von a ist, gibt es eine Lösung x_0, und alle Lösungen erhält man durch $x = x_0 + l\dfrac{m}{\mathrm{ggT}(b,m)}$ $(l\in\mathbb{Z})$.
Falls m Primzahl: $\mathrm{ggT}(b,m)=1$, also existiert für jedes $a\in\mathbb{N}$ eine Lösung x_0. Alle Lösungen sind gegeben durch

$$x = x_0 + lm \ (l\in\mathbb{Z}).$$

Dies sind genau alle Elemente von $[x_0]$. Damit ist bewiesen:

Satz vom Dividieren: Ist p eine Primzahl und sind $a,b\in\mathbb{N}$, wobei b kein Vielfaches von p ist, so besitzt die Gleichung

$$[b]\cdot[x] = [a] \qquad \text{in } \mathbb{Z}/p\mathbb{Z}$$

genau eine Lösung $[x]$, d.h. $\dfrac{[a]}{[b]} := [x]$ ist definiert.

Hausaufgabe: Bestimme in $\mathbb{Z}/89\mathbb{Z}$ den Wert $\dfrac{[7]}{[20]}$ durch Lösung der Gleichung $20x-98k=7$.

Übung: Bestimme alle Potenzen:

a) von $[4]$ in $\mathbb{Z}/5\mathbb{Z}$,

b) von $[3]$ in $\mathbb{Z}/11\mathbb{Z}$,

c) von $[2],[3],[5]$ in $\mathbb{Z}/6\mathbb{Z}$.

Kleiner Satz von Fermat: Sei p Primzahl, $a\in\mathbb{N}$ kein Vielfaches von p. Dann gilt

$$[a]^{p-1} = [1] \text{ in } \mathbb{Z}/p\mathbb{Z} \qquad \text{bzw.} \qquad a^{p-1}\equiv 1 \mod p.$$

Beweis: Da a kein Vielfaches von p ist, gilt $[a]\neq[0]$.

Betrachte $[ja]$ für $j = 1,2,\ldots,p-1$.

Es gilt $[ja] = [j] \cdot [a] \neq [0]$, denn:

$$[0] = [j] \cdot [a] \;\Rightarrow\; [0] = [0] \cdot \frac{[1]}{[a]} = [j] \cdot [a] \cdot \frac{[1]}{[a]} = [j] \text{ Widerspruch}$$

Es gilt $[ja] = [j] \cdot [a] \neq [k] \cdot [a] = [ka]$ für $j \neq k$, denn:

$[j] \cdot [a] = [k] \cdot [a] \;\Rightarrow\; [j] = [j] \cdot [a] \cdot \frac{[1]}{[a]} = [k] \cdot [a] \cdot \frac{[1]}{[a]} = [k]$ Widerspruch, da $1 \leq j, k \leq q-1$

Da alle Elemente der Menge $\big\{[1a], [2a], \ldots, [(p-1)a]\big\}$ paarweise verschieden und ungleich $[0]$ sind, muss gelten:

$$\big\{[1a], [2a], \ldots, [(p-1)a]\big\} = \big\{[1], [2], \ldots, [p-1]\big\}.$$

Multipliziere alle Elemente der Menge:

$$\begin{array}{rrcl} & [1a \cdot 2a \cdot 3a \cdots (p-1)a] & = & [1 \cdot 2 \cdot 3 \cdots (p-1)] \\ \Leftrightarrow & [1 \cdot 2 \cdot 3 \cdots (p-1)] \cdot [a]^{p-1} & = & [1 \cdot 2 \cdot 3 \cdots (p-1)] \cdot [1] \;\neq\; [0] \\ & \Leftrightarrow \quad [a]^{p-1} & = & [1] \end{array}$$

Zusatzmaterial

Dafür reichte die Zeit nicht

Negativer Primzahltest: Für die Zahl $m \in \mathbb{N}$ soll gezeigt werden, dass sie keine Primzahl ist. Falls wir ein $a \in \mathbb{N}$ finden, so dass $a^{m-1} \not\equiv 1 \mod m$, ist m keine Primzahl. Man sagt, a ist Zeuge gegen die Primalität von m.

Beispiel: $m = 15$: $2^{14} = 16^3 \cdot 4 \equiv 1^3 \cdot 4 = 4 \mod 15$. Also ist 2 Zeuge gegen die Primalität von 15.

Übung: Finde einen Zeugen gegen die Primalität von

a) $m = 21$,

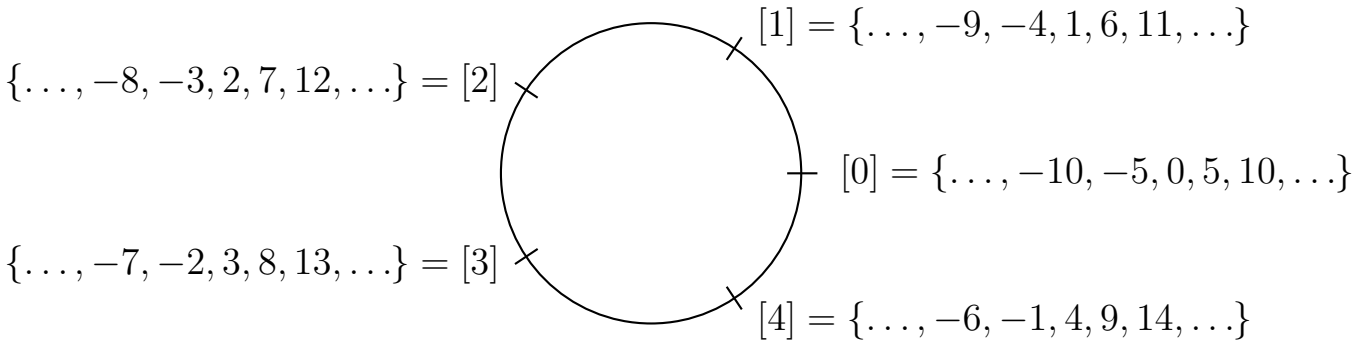
b) $m = 25$.

Universität Stuttgart
Schülerseminar Klasse 8–10

PD. Dr. P. Lesky
5. Juli 2006

Arbeitsblatt Rechnen auf dem Ring

Rechnen mit Restklassen aus $\mathbb{Z}/5\mathbb{Z}$:



Verknüpfungstabelle für die Multiplikation in $\mathbb{Z}/5\mathbb{Z}$:

$\cdot$	$[0]$	$[1]$	$[2]$	$[3]$	$[4]$
$[0]$	[ ]	[ ]	[ ]	[ ]	[ ]
$[1]$	[ ]	[ ]	[ ]	[ ]	[ ]
$[2]$	[ ]	[ ]	[ ]	[ ]	[ ]
$[3]$	[ ]	[ ]	[ ]	[ ]	[ ]
$[4]$	[ ]	[ ]	[ ]	[ ]	[ ]

Universität Stuttgart
Schülerseminar Klasse 8–10

PD. Dr. P. Lesky
12. Juli 2006

Kryptographie

Geheimbotschaft: xjsyw yatl wk khswlwj kmwkkaycwalwf

Cäsar-Chiffre: Das Alphabet wird verschoben:

unverschlüsselt:	A	B	C	D	E	F	G	...	X	Y	Z
	↓	↓	↓	↓	↓	↓	↓		↓	↓	↓
verschlüsselt:	x	y	z	a	b	c	d		u	v	w

Verschlüsselung knacken: Durchprobieren (25 Möglichkeiten)

Substitutionsverschlüsselung:

unverschlüsselt:	A	B	C	D	E	F	G	...	X	Y	Z
	↓	↓	↓	↓	↓	↓	↓		↓	↓	↓
verschlüsselt:	willkürlich vertauschte Reihenfolge										

Verschlüsselung knacken: Durch Häufigkeitsanalyse des Textes.

- Der häufigste Buchstabe in deutschen Texten ist „e“ mit 17,4%.
- Die beiden häufigsten Digramme (Buchstabenpaare) sind „er“ (4,1%) und „en“ (4,0%).
- Man kann noch die Häufigkeit der Trigramme (Dreierkombinationen von Buchstaben) zu Hilfe nehmen.

⟶ spätere Übung.

Man nennt diese Verschlüsselungen „Monoalphabetische Substitutionen“

Eine polyalphabetische Substitution: Vigenère Verschlüsselung:

Benötigt: Schlüsselwort
Vigenère-Quadrat → Übungsblatt

Verschlüsselung von „HEUTE IST ES SEHR HEISS“ mit dem Schlüsselwort „primzahl“:

Schreibe „primzahl“ unter den Text (ohne Leerzeichen):

Original:	H	E	U	T	E	I	S	T	E	S	S	E	H	R	H	E	I	S	S
	p	r	i	m	z	a	h	l	p	r	i	m	z	a	h	l	p	r	i
Verschlüsselt:	w	v	c	f	d	i	z	e	t	j	a	q	g	r	o	p	x	j	a

Unter „H“ steht „p“, dann wird „H“ mit der „p“-Zeile verschlüsselt: H→w.
Unter „E“ steht „r“, dann wird dieses „E„ mit der „r“-Zeile verschlüsselt: E→v.

Vorteil: Die Buchstabenhäufigkeit ist versteckt. Gleiche Buchstaben werden verschieden verschlüsselt

Nachteil: Nach l Buchstaben (l =Länge des Schlüsselwortes) wiederholt sich die Verschlüsselung, jeder Block aus l Buchstaben wird nach dem gleichen Prinzip verschlüsselt

Aufgabe: Entschlüssle mit dem Schlüsselwort „handy“ den Text „raaq gjh olrae rll nuzpgiaruaoea ecrozpcu“

Vigenère-Verschlüsselung knacken:

- Finde die Länge l des Passwortes
- Schreibe den verschlüsselten Text in l Spalten
- In jeder Spalte Häufigkeitsanalyse liefert die Codierung von „E“

Dann ist das Schlüsselwort bekannt, der Text kann entschlüsselt werden.

Für den Teil bis hierher benötigten wir ungefähr 45 Minuten. Dann gingen wir in den Computerraum und entschlüsselten zwei Texte, die mit Substitutionsverschlüsselung verschlüsselt waren, durch Häufigkeitsanalyse. Die Anleitung dazu ist auf den übernächsten Seiten. Die Texte können per Email bei mir angefordert werden: `lesky@mathematik.uni-stuttgart.de`
Für den zweiten Teil des Workshops wird das Programm `cryptool` benötigt. Auf den Emacs kann man verzichten, die Entschlüsselung kann auch in `cryptool` buchstabenweise eingetragen werden. Es gibt in `cryptool` sogar eine automatische Analyse eines deutschen Textes, die einige Buchstaben schafft, der Rest muss dann von Hand durchgeführt werden. Das Programm `cryptool` kann für Windows heruntergeladen werden von
`http://www.cryptool.de/`

Universität Stuttgart
Schülerseminar Klasse 8–10

PD. Dr. P. Lesky
12. Juli 2006

Arbeitsblatt Kryptographie

Vigenère-Quadrat:

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
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	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
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
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
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
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
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
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
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
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
l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	k
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
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
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
p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	l	l	m	n	o
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
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
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
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
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
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
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
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
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
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

Entschlüsselung geheimer Botschaften am Computer

12. Juli 2006

Falls nach dem Einloggen kein Arbeitsfenster erscheint, unten auf der Leiste auf das Bildschirm-Symbol klicken, dann wird ein Arbeitsfenster geöffnet. Falls beim Einloggen zwei Arbeitsfenster erscheinen, bitte eines wegklicken. Im Arbeitsfenster mit `cd crypt` (alles kleingeschrieben) in das Verzeichnis crypt wechseln. In diesem Verzeichnis gibt es die Dateien `nachricht1.txt` und `nachricht2.txt`. Zuerst soll `nachricht1.txt` entschlüsselt werden. Dazu benützen wir zwei Programme: Für die Analyse `CrypTool` und für die Entschlüsselung den Editor `emacs`.

Zuerst `crypt &` eingeben. Das Begrüßungs- und das Beispielfenster wegklicken. Mit `Datei`→`öffnen` die Datei `nachricht1.txt` aufmachen.

a) Dann mit `Analyse`→`Allgemein`→`N-Gramm` ein Histogramm (Häufigkeit der Buchstaben) erstellen und abspeichern. Jetzt sind zwei Fenster in `Cryptool` offen.

b) Auf das Fenster mit `nachricht1.txt` klicken, dann mit `Analyse`→`Allgemein`→`N-Gramm` die Häufigkeit der Digramme berechnen und speichern.

c) Auf das Fenster mit `nachricht1.txt` klicken, dann mit `Analyse`→`Allgemein`→`N-Gramm` die Häufigkeit der Trigramme berechnen und speichern.

Nun kann man mit den auf der Rückseite dieses Blattes angegebenen Häufigkeitsverteilungen anfangen, die Bedeutung der Buchstaben zu erraten.

Zum Entschlüsseln das CryptTool-Fenster verschieben, das Arbeitsfenster anklicken und dort `emacs nachricht1.txt &` eingeben. Dann ist der verschlüsselte Text im Editor. Nun die Tastenfolge Alt`-x decipher` gefolgt von der Zeilenende-Taste eingeben. Dann ist der Editor im Entschlüsselungsmodus. Die großgeschriebenen Buchstaben sind die des verschlüsselten Textes, die kleingeschriebenen die des entschlüsselten Textes. Nun können auf dem großgeschriebenen Alphabet Kleinbuchstaben eingegeben werden. Diese werden dann daruntergeschrieben und im Text entsprechend ersetzt.

Hinweise: Das Programm `cryptool` kann für Windows heruntergeladen werden von `http://www.cryptool.de/`

Den Editor `Emacs` gibts auch für Windows zum runterladen (selber suchen).

Eine sehr schöne Seite über Verschlüsselung findet sich unter `http://delphi.zsg-rottenburg.de/krypt.html`

Häufigkeitsverteilungen in deutschsprachigen Texten

Buchstaben

E	17,40 %	M	2,53 %
N	9,78 %	O	2,51 %
I	7,55 %	B	1,89 %
S	7,27 %	W	1,89 %
R	7,00 %	F	1,66 %
A	6,51 %	K	1,21 %
T	6,15 %	Z	1,13 %
D	5,08 %	P	0,79 %
H	4,76 %	V	0,67 %
U	4,35 %	J	0,27 %
L	3,44 %	Y	0,04 %
C	3,06 %	X	0,03 %
G	3,01 %	Q	0,02 %

Digramme

ER	4,09 %
EN	4,00 %
CH	2,42 %
DE	1,93 %
EI	1,87 %
ND	1,85 %
TE	1,68 %
IN	1,63 %
IE	1,47 %
GE	1,40 %
ES	1,22 %
NE	1,19 %
UN	1,16 %
ST	1,12 %
RE	1,02 %
HE	1,02 %
AN	1,02 %
BE	1,01 %

Trigramme

EIN	1,22 %
ICH	1,11 %
NDE	0,89 %
DIE	0,87 %
UND	0,87 %
DER	0,86 %
CHE	0,75 %

Universität Stuttgart
Schülerseminar Klasse 8–10

PD. Dr. P. Lesky
26. Juli 2006

Zahlentheorie und Verschlüsselung

Erinnerung: $\mathbb{Z}/7\mathbb{Z} = \{[0], [1], [2], \ldots, [6]\}$: Z.B. $[3] \cdot [4] = [12] = [5]$.

Potenzieren:

k	1	2	3	4	5	6
$[3]^k$	[3]	[2]	[6]	[4]	[5]	[1]
$[2]^k$	[2]	[4]	[1]			

Kleiner Fermat: $3^6 \equiv 1 \mod 7$

Durch $[3]^k$ können alle Elemente von $\mathbb{Z}/7\mathbb{Z}$ außer $[0]$ dargestellt werden.
Man nennt $[3]$ oder einfach 3 eine **Primitivwurzel** für $\mathbb{Z}/7\mathbb{Z}$.

Übung: Dasselbe für $[2], [3]$ in $\mathbb{Z}/11\mathbb{Z}$. Welche Zahl ist hier eine Primitivwurzel?

Problem: Anton und Bine treffen sich in einem Chatroom. Sie wollen Ihre Texte verschlüsseln, so dass niemand der anderen ihre Texte verstehen kann. Jede Person im Chatroom kann lesen, wie sie ihren Code vereinbaren. Ist so eine Verschlüsselung möglich? Auch wenn alle anderen im Chatroom Mathematiker sind?

Der Diffie-Hellman Schlüsseltausch: Beide Partner vereinbaren eine Primzahl p und eine Primitivwurzel g für $\mathbb{Z}/p\mathbb{Z}$.

Anton wählt $a \in \{1, 2, \ldots, p-2\}$ und berechnet: $A \equiv g^a \mod p$
Bine wählt $b \in \{1, 2, \ldots, p-2\}$ und berechnet: $B \equiv g^b \mod p$

Dann tauschen Sie A und B aus. Das bedeutet: (p, g, A, B) sind öffentlich bekannt,
a kennt nur Anton,
b kennt nur Bine.

Jeder von beiden berechnet nun den gemeinsamen Schlüssel $K \equiv g^{ab} \mod p$:

Anton berechnet: $K \equiv B^a \mod p$,
Bine berechnet: $K \equiv A^b \mod p$

Beispiel: Anton und Bine vereinbaren $p = 7$ und $g = 3$:

Anton wählt: $a = 3$, berechnet $6 = A \equiv 3^3 \mod 7$,
Bine wählt: $b = 4$, berechnet $4 = B \equiv 3^4 \mod 7$.

Anton berechnet den Schlüssel: $4^3 = 64 \equiv 1 \mod 7$, also $K = 1$,
Bine berechnet den Schlüssel: $6^4 = 36^2 \equiv 1^2 = 1 \mod 7$, also $K = 1$

Nun können beide *EINS* als Schlüsselwort für die Vigenère Verschlüsselung nehmen. Die Nachricht „Heute ist es heiß“ wird zu

Nachricht	H	E	U	T	E	I	S	T	E	S	H	E	I	S	S
Schlüssel	e	i	n	s	e	i	n	s	e	i	n	s	e	i	n
Verschlüsselt	l	m	h	l	i	q	f	l	i	a	u	w	m	a	f

Knack den Code: Anton und Bine vereinbaren $p = 11$ und $g = 2$. Anton schickt an Bine die Zahl $A = 5$, Bine meldet $B = 8$. Kurze Zeit später übermittelt Anton die Nachricht

w q x k z o y d h q f r z z g y z v

Bestimme a, b und den Schlüssel K, entschlüssle die Nachricht.

Hinweis: Man sollte eine Packung Gummibärchen bereit halten.

Sicherheit: Falls p, g, a groß sind, ist es schwierig, aus g und A die Zahl a zu berechnen. Und ohne a oder b kann man den Schlüssel nicht berechnen.

Problem: Frank schreibt auf seiner Homepage, dass er gerne Mails aus aller Welt bekommen möchte. Er hat Angst vor der CIA. Deshalb sollen die Mails gut verschlüsselt werden.

Das RSA-Verfahren:

Frank	wählt	zwei (große) Primzahlen p, q,
	berechnet	$m = pq$, $\widetilde{m} = (p-1)(q-1)$,
	wählt	Verschlüsselungsexponent v mit $1 < v < \widetilde{m}$ und $\mathrm{ggT}(v, \widetilde{m}) = 1$,
	veröffentlicht	m und v auf seiner Homepage,
	berechnet	Entschlüsselungsexponent e mit $1 < e < \widetilde{m}$ und $ev \equiv 1 \mod \widetilde{m}$.

Ein Leser der Homepage kann nun eine Mail mit Vigenère und einem Zahlwort verschlüsseln und das Zahlwort als Zahl N folgendermaßen übermitteln:

$$\text{Verschlüsselte Zahl } V \equiv N^v \mod m.$$

Frank bekommt die Zahl zurück durch

$$N \equiv V^e \mod m$$

und kann dann mit Vigenère entschlüsseln.

Beispiel:

Frank	wählt:	$p = 3$, $q = 11$,
	berechnet:	$m = 3 \cdot 11 = 33$, $\widetilde{m} = 2 \cdot 10 = 20$,
	wählt:	Verschlüsselungsexponent $v = 7$ ($1 < 7 < 20$ und $\mathrm{ggT}(7, 20) = 1$),
	veröffentlicht:	$m = 33$ und $v = 7$
	berechnet:	e mit $7e \equiv 1 \mod 20$, d.h. $7e + 20k = 1$ für ein $k \in \mathbb{Z}$.

Verallgemeinerter Euklidischer Algorithmus:

$$\begin{array}{rcl|l} 20 & = & 2 \cdot 7 + 6 & 6 = 1 \cdot 20 - 2 \cdot 7 \\ 7 & = & 1 \cdot 6 + 1 & 1 = 7 - 1 \cdot 6 = (-1) \cdot 20 + 3 \cdot 7 \end{array}$$

Also $e = 3$.

Jane liest die Homepage von Frank, verschlüsselt ihre Mail mit Vigenère und dem Schlüsselwort *drei*. Sie berechnet

$$3^7 = 3^4 \cdot 3^3 = 81 \cdot 27 \equiv 15 \cdot 27 = 5 \cdot 81 \equiv 5 \cdot 15 = 75 \equiv 9$$

und schickt Frank die verschlüsselte Mail und $V = 9$. Frank liest in Janes Mail $V = 9$ und berechnet

$$9^3 = 81 \cdot 9 \equiv 15 \cdot 9 = 3 \cdot 45 \equiv 3 \cdot 12 = 36 \equiv 3.$$

Nun kann er den Text entschlüsseln.

Warum klappt das? Es gilt $ve = 1 + k\widetilde{m}$ mit einem $k \in \mathbb{Z}$.

$$\Rightarrow \quad V^e = (N^v)^e = N^{ve} = N \cdot N^{k\widetilde{m}} \underset{(*)}{\equiv} \begin{cases} N \mod p \\ N \mod q \end{cases}$$

$$\Rightarrow \quad V^e - N = k_1 \cdot p = k_2 \cdot q$$

$$\overset{p \text{ Primzahl}}{\Rightarrow} \quad q \text{ teilt } k_1: \quad k_1 = k_3 \cdot q$$

$$\Rightarrow \quad V^e - N = k_3 \cdot q\, p, \text{ also } V^e \equiv N \mod p\, q$$

Zu $(*)$: Falls p Teiler von N: $N \equiv 0 \mod p \Rightarrow N \cdot N^{\cdots} \equiv 0 \equiv N \mod p$
Falls p kein Teiler von N: $N^{p-1} \equiv 1 \mod p$ (kleiner Satz von Fermat).

$$\Rightarrow \quad N \cdot N^{k\widetilde{m}} = N \cdot N^{k(p-1)(q-1)} = N \cdot \left(N^{p-1}\right)^{k(q-1)} \equiv N \cdot 1 = N \mod p.$$

Genauso für q.

Universität Stuttgart
Schülerseminar Klasse 8–10

PD. Dr. P. Lesky
26. Juli 2006

Arbeitsblatt Zahlentheorie und Verschlüsselung

Vigenère-Quadrat:

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
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	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
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
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
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
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
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
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
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
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
l	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	k	k
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
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
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
p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	l	l	m	n	o
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
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
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
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
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
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
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
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
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
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

Knack den Code 1: Anton und Bine vereinbaren $p = 11$ und $g = 2$. Anton schickt an Bine die Zahl $A = 5$, Bine meldet $B = 8$. Kurze Zeit später übermittelt Anton die Nachricht

w q x k z o y d h q f r z z g y z v

Bestimme a, b und den Schlüssel K, entschlüssle die Nachricht.

Knack den Code 2: Frank veröffentlicht auf seiner Homepage die Zahlen $m = 51$ und $v = 3$. Er erhält von Michael die Zahl $V = 8$.
Bestimme p, q, e und N.

Knack den Code 3 (schwer): Frank veröffentlicht auf seiner Homepage die Zahlen $m = 55$ und $v = 7$. Er erhält von Peter die Zahl $V = 25$.
Bestimme p, q, e und N.