Anhang A

Anhang

Die Inhalte des Anhangs sind zwar nicht klausurrelevant, können aber zum Verständnis des Stoffes bzw. seiner Tragweite beitragen, da sie eine ganz wichtige Anwendung der modernen Algebra, die Kryptologie, kurz anreissen.

A.1 Eulersche ϕ-Funktion

In diesem Anhang werden wir nicht so weit in die Tiefe gehen, wie in den Kapiteln des Skripts, jedoch möchte ich gerade für die Hörer des Moduls mat200 die Chance nicht verstreichen lassen, eine Anwendung der Algebra zu besprechen: die Verschlüsselung von Daten mittels RSA-Verfahren. Dazu sind allerdings einige Grundlagen aus der Theorie der Gruppen notwendig, die eigentlich erst in der Algebra II behandelt werden.

Satz A.1.1 *(Lagrange – kommutativer Fall) Sei G eine endliche abelsche Gruppe mit $|G| = n$ Elementen und sei $U \subseteq G$ eine Untergruppe. Dann gilt*

$$|G/U| \cdot |U| = n.$$

Beweis: Wir betrachten den Restklassenhomomorphismus

$$\pi : G \longrightarrow G/U,$$

dessen Kern gerade $\ker(\pi) = U$ ist. Sei nun $\mathcal{O}$ ein Repräsentantensystem von G/U, so ist die Anzahl der Restklassen $|G/U|$ gleich der Anzahl der Elemente von $\mathcal{O}$. Jede Äquivalenzklasse $[a]_U = a + U$ für ein $a \in \mathcal{O}$ hat andererseits genau $|U|$ Elemente. Damit gilt:

$$n = |G| = |G/U| \cdot |U|.$$

□

Korollar A.1.2 *Sei $(G, \cdot)$ eine endliche abelsche Gruppe mit $|G| = n$ Elementen. Dann gilt:*

$$\forall g \in G : \quad g^n = e_G.$$

Beweis: Betrachte zu einem beliebigen gegebenen $g \in G$ die Menge $U = \{g^i \mid i \in \mathbb{Z}\}$. Da $1_G = g^0 \in U$ und $g^i \cdot g^{-j} = g^{i-j} \in U$ für beliebige $i, j \in \mathbb{Z}$, erfüllt U das Untergruppenkriterium. Ausserdem muss es wegen der Endlichkeit von G und damit auch U ein kleinstes nicht-negatives r geben mit $g^r = g^0 = 1_G$. Nach den Rechenregeln für Gruppen impliziert das auch $g^i = g^{i \bmod r}$ für alle $i \in \mathbb{Z}$ und somit ist $|U| = r$. Nach Satz A.1.1 ist dann r Teiler von n und damit $g^n = g^0 = 1_G$.

□

Betrachten wir nun eine spezielle Klasse von Gruppen, die Einheitengruppen $(\mathbb{Z}/m\mathbb{Z})^*$ der Ringe $\mathbb{Z}/m\mathbb{Z}$:

Definition A.1.3 *Sei $m \in \mathbb{N}$. Dann ist die Eulersche ϕ-Funktion definiert als*

$$\begin{array}{rcl} \phi : \mathbb{N} & \longrightarrow & \mathbb{N} \\ m & \longmapsto & |\,(\mathbb{Z}/m\mathbb{Z})^*\,| = |\{1 \leq a \leq m \mid \mathrm{ggT}(a, m) = 1\}| \end{array}$$

Satz A.1.4 *(Euler) Sei $m \in \mathbb{N}$. Dann gilt*

$$a^{\phi(m)} \equiv 1 \bmod m \quad \forall a \in \mathbb{Z} \text{ mit } \mathrm{ggT}(a, m) = 1.$$

Beweis: Da $\phi(m)$ genau die Anzahl der Elemente in $(\mathbb{Z}/m\mathbb{Z})^*$ ist, ist dieser Satz ein direktes Korollar zu der Aussage direkt davor.

□

Satz A.1.5 *(Kleiner Satz von Fermat) Sei p eine Primzahl und $a \in \mathbb{Z}$. Dann gilt:*

$$a^p \equiv a \bmod p.$$

Ist $a \in \mathbb{Z}$ und p kein Teiler von a, so gilt insbesondere

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

Beweis: Die zweite Aussage ist gerade der Satz von Euler, da jedes nicht durch p teilbare Element eine Restklasse aus $(\mathbb{Z}/p\mathbb{Z})^*$ repräsentiert.
Multipliziert man die zweite Aussage mit a, was nach Voraussetzung der zweiten Aussage nicht Null ist, so erhält man die erste Aussage für alle $a \in \mathbb{Z} \setminus p\mathbb{Z}$. Für Vielfache von p ist die Aussage trivial erfüllt.

□

Satz A.1.6 *Die Eulersche ϕ-Funktion besitzt folgende Eigenschaften:*

a) Für eine Primzahl p und ein $a \in \mathbb{N}$ gilt:

$$\phi(p^a) = p^a - p^{a-1} = p^a \cdot (1 - \frac{1}{p}).$$

b) Sind $n, m \in \mathbb{Z}$ teilerfremd, so gilt

$$\phi(mn) = \phi(m)\phi(n).$$

Beweis:

a) Es gibt genau p^a ganze Zahlen $0 \leq z < p^a$. Davon sind genau die Zahlen der Form $z = p \cdot m$ mit $0 \leq (p \cdot m) < (p \cdot p^{a-1})$ durch die Primzahl p teilbar, wobei dann für m offensichtlich $0 \leq m < p^{a-1}$ gilt. Also gibt es

$$p^a - p^{a-1} = p^a \cdot (1 - \frac{1}{p})$$

zu p teilerfremde Zahlen zwischen 0 und p^a ,was zu zeigen war.

b) Nach dem Chinesischen Restsatz wissen wir, dass

$$\mathbb{Z}/\langle mn\rangle \cong \mathbb{Z}/\langle m\rangle \times \mathbb{Z}/\langle n\rangle$$

und damit auch Isomorphie der zugehörigen Einheitengruppen gilt. Ein Element $([v]_m, [w]_n) \in \mathbb{Z}/\langle m\rangle \times \mathbb{Z}/\langle n\rangle$ ist somit genau dann Einheit, wenn $[v]_m \in (\mathbb{Z}/\langle m\rangle)^*$ und $[w]_n \in (\mathbb{Z}/\langle n\rangle)^*$. Damit ist die Anzahl der Elemente von $(\mathbb{Z}/\langle m\rangle \times \mathbb{Z}/\langle n\rangle)^*$ gerade $\phi(m) \cdot \phi(n)$.

□

Korollar A.1.7 *Ist* $m = \prod_{i=1}^{n} p_i^{e_i}$ *eine Primfaktorzerlegung der natürlichen Zahl* m *mit* $p_i \neq p_j$ *für* $i \neq j$*, so gilt:*

$$\phi(m) = m \prod_{i=1}^{n} (1 - \frac{1}{p_i}).$$

Der Beweis dieses Korollars ist eine direkte Anwendung des vorstehenden Satze und bleibt dem interessierten Leser überlassen.

A.2 Ver- und Entschlüsseln mit RSA

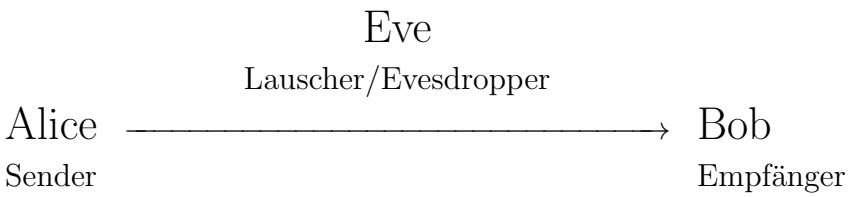
Möchten Alice und Bob miteinander auf einem öffentlichen Kanal (z.B. Internet) kommunizieren, ohne dass jemand anderes die Informationen abhören kann, so müssen sie diese verschlüsseln. Hier stellen wir ein recht grundlegendes Asymmetrisches Verschlüsselungsverfahren nach Rivest-Shamir-Adleman vor, das sogenannte RSA-Verfahren, das lange Zeit state-of-the-art war, bis die Weiterentwicklung der Computer und insbesondere Fortschritte auf dem Weg zum Quantencomputing es zumindest für viele praktische Anwendungen obsolet machten. Da es hier vorrangig um das Prinzip eines asymmetrischen Kryptoverfahrens geht und nicht um eine detaillierte Beleuchtung aller theoretischen und praktischen Aspekte, erhebt dieser Abschnitt auch keinerlei Anspruch, eine vollständige Einführung zu sein.

Sprechen wir hier von einem Asymmetrischen Kryptoverfahren, so ist damit gemeint, dass Alice und Bob nicht gegenseitig über dieselben Informationen zur Ver- und Entschlüsselung verfügen, sondern jeder einen öffentlichen Schlüssel besitzt, der allen zur Verfügung gestellt wird, sowie einen privaten Schlüssel, der aus dem öffentlichen Schlüssel nicht (bzw. hinreichend nicht leicht) errechnet werden kann und geheim gehalten wird.

Eine Nachricht ist für uns in diesem Kontext einfach eine Zahl $M \in \mathbb{Z}/N\mathbb{Z}$ für eine geeignete (und hinreichend große) zusammengesetzte Zahl N. Denken Sie etwa an recht offensichtliche Minibeispiele wie das Abzählen der Buchstaben des Alphabets oder den ASCII-Code zur Umsetzung der Buchstaben sowie Sonder- und Steuerzeichen in Zahlen.

Das Kommunikationsproblem

Alice möchte eine Nachricht an Bob schicken, die Eve als Lauscher an der Leitung nicht entschlüsseln kann.



Die Erzeugung der Schlüssel

Da Bob der Empfänger der Nachricht sein wird, muss das Geheimnis zur Entschlüsselung auf seiner Seite liegen. Es ist also an Bob, ein Schlüsselpaar zu erzeugen, von dem er den öffentlichen Schlüssel Alice zur Verfügung stellt.

RSA-Schlüsselerzeugung (Bob):

- Wähle/Erzeuge zwei Primzahlen p und q der Größenordnung von 2048 Bit ($=2^{2048}$) (die nicht zu dicht beieinander liegen und unabhängig erzeugt wurden – für Deutschland genauer spezifiziert in Bekanntmachung der Bundesnetzagentur vom 14.1.2014)

- $N = p \cdot q$ und damit $\phi(N) = (p-1) \cdot (q-1)$

- Wähle $e \in \mathbb{Z}$ mit $1 < e < \phi(N)$ und $\mathrm{ggT}(e, \phi(N)) = 1$, d.h. $[e]_{\phi(N)}$ ist Einheit in $\mathbb{Z}/\phi(N)\mathbb{Z}$.

- Berechne die Inversen $[d]_{\phi(N)}$ zu $[e]_{\phi(N)} \in (\mathbb{Z}/\phi(N)\mathbb{Z})^*$ und nenne den Repräsentanten mit $1 < d < \phi(N)$ nun d.
  Es gilt also:
  $$1 = ed - k\phi(N)$$
  für ein geeignetes $k \in \mathbb{Z}$.

- Publiziere (e, N) und halte $(d, p, q, \phi(N))$ geheim.

RSA-Verschlüsselung

Alice hat nun Bob's öffentlichen Schlüssel (N, e) erhalten und möchte ihre Nachricht m, die bereits als ganze Zahl $0 \leq M < N$ dargestellt ist, damit verschlüsseln. Dazu bedient sie sich der Multiplikation auf $\mathbb{Z}/N\mathbb{Z}$ und des erhaltenen Exponenten e.

Verschlüsselung (Alice):

- Suche Bob's Schlüssel (N, e) heraus
- Berechne $C = M^e \bmod N$
- Sende C an Bob

RSA-Entschlüsselung

Bob hat nun Alices Nachricht erhalten und verwendet seinen privaten Schlüssel sowie Gruppentheorie aus dem Abschnitt A.1, um die Nachricht zu entschlüsseln.

Entschlüsselung (Bob):

- Erhalte $C < N$ von Alice
- Rechne
$$C^d = M^{ed} = M^{1+k\phi(N)} \equiv M \bmod N.$$
(Denn $M^{\phi(N)} = 1$ nach dem Satz von Euler angewandt modulo N, falls $\mathrm{ggT}(M, N) = 1$.Im Fall $\mathrm{ggT}(M, N) = p$ (bzw. q) verwendet man unter Ausnutzung des Chinesischen Restsatzes dasselbe Argument oder den kleinen Satz von Fermat.)

RSA-Trapdoor-Einwegfunktion

Dieses Verschlüsselungsverfahren beruht im Grunde genommen darauf, dass es schwer ist zu C den Wert $C^{\frac{1}{e}}$ zu bestimmen, wenn man nur e und N kennt, nicht aber $p, q, d, \phi(N)$. Es gibt aber eine "Falltür", nämlich die Kenntnis von d, die das Unterfangen ganz einfach macht.

Gegeben: e, N wie oben mit $\mathrm{ggT}(e, N) = 1$

RSA-Trapdoor-Funktion:

$$f_{N,e}(M) := M^e \bmod N \text{ für } M \in \mathbb{Z}/N\mathbb{Z}$$

Es ist einfach $f_{N,e}$ zu evaluieren. Es sollte schwierig sein, $f_{N,e}$ zu invertieren (Einwegfunktion), aber durch die Falltür kann Bob trotzdem leicht M aus $f_{N,e}(M)$ bestimmen.

Einige Kommentare zum Brechen von RSA

- Mit 'Brechen von RSA' ist das Berechnen von $C^{\frac{1}{e}}$ zu gegebenem C gemeint.
- Das 'spezielle ganzzahlige Faktorisierungsproblem' ist das Problem der Ermittlung der beiden Primzahlen p und q aus $N = pq$.
- Ist es möglich das spezielle ganzzahlige Faktorisierungsproblem zu lösen, so kann man RSA leicht brechen, da aus der Kenntnis von p und q direkt die Kenntnis von $\phi(N) = (p-1)(q-1)$ folgt, womit dann mittels der Bézout-Identität modulo $\phi(N)$ direkt d bestimmt werden kann.
- Es ist nicht klar, ob das spezielle ganzzahlige Faktorisierungsproblem ebenfalls gelöst ist, sobald eine effektive Methode zum Brechen von RSA zur Verfügung steht.

Weiter werden wir an dieser Stelle nicht in die Tiefe oder in die Breite gehen, sondern überlassen dies z.B. einer Veranstaltung zur Kryptographie oder dem Selbststudium in einem Buch.
Es sei nur soviel gesagt, dass sie gerade mal einen ersten Eindruck von Kryptographie erhalten haben, aber nicht weiter in das Gebiet eingetaucht sind, als sie es z.B. mit dem Lösen linearer Gleichungssysteme in zwei Variablen in der Schule in die Lineare Algebra waren.
Für modernere Schlagworte zur Kryptographie möchte ich gerade noch die Stichworte "elliptische Kurven Kryptographie" sowie "Post-Quantum-Kryptographie" nennen, ohne jedoch auf deren Inhalt einzugehen.