# 01321 Mathematische Grundlagen der Kryptografie
# Vorbereitung auf die mündliche Prüfung
# Bei Prof. Unger

# Kryptografie im Allgemeinen

**Was ist Kryptographie?**
Kryptografie ist der sichere Nachrichtentransfer über einen unsicheren Kanal.

**Wie lässt sich die Kryptografie mathematisch beschreiben?**
Ein Kryptosystem ist ein 5-Tupel $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, so dass die folgenden Regeln gelten:

1. $\mathcal{P}$ ist eine *endliche* Menge von Klartexten (englisch: $\mathcal{P}$lain texts).
2. $\mathcal{C}$ ist eine *endliche* Menge von Geheimtexten (englisch: $\mathcal{C}$ipher texts).
3. $\mathcal{K}$ ist eine *endliche* Menge von Schlüsseln (englisch: $\mathcal{K}$eys).
4. Für jedes $K \in \mathcal{K}$ gibt es eine Chiffrierungsregel $e_K \in \mathcal{E}$ (englisch: $\mathcal{E}$ncryption rule) und eine Dechiffrierungsregel $d_K \in \mathcal{D}$ (englisch: $\mathcal{D}$ecryption rule). Dabei sind $e_K : \mathcal{P} \to \mathcal{C}$ und $d_K : \mathcal{C} \to \mathcal{P}$ Abbildungen, so dass für alle $x \in P$ gilt: $d_K(e_K(x)) = x$.

**Was gilt für die Chiffrierungsregel $e_K$ und Dechiffrierungsregel $d_K$ eines Kryptosystems?**
Die Chiffrierungsregel $e_K$ muss injektiv sein, und da $P$ endlich ist, folgt, dass $e_K$ surjektiv, also bijektiv ist. Die Dechiffrierungsregel $d_K$ ist die Umkehrfunktion von $e$.

**Wofür braucht man die Kryptografie?**
Während bis vor Kurzem der Kryptografie die Romantik und Komik des *Spion gegen Spion* anhaftete, hat sich dies in den letzten Jahren dramatisch verändert. Mit der Verbreitung der elektronischen Datenverarbeitung, insbesondere der elektronischen Kommunikation bieten sich der Kryptografie völlig neue Aufgabenfelder. Einige Beispiele:

- Telefongespräche über Satellit kann im Prinzip jeder mithören.
- Geldüberweisungen und andere Bankgeschäfte werden zunehmend elektronisch getätigt.
- Viele komplexe Multiuser Systeme wie Rechner, Telefonnetze und Banken arbeiten mit Passworten oder PINs, mit denen sich ein Benutzer gegenüber dem System identifiziert. Diese müssen sicher verwaltet werden.

**Zu den klassischen Aufgaben der Kryptografie, der sicheren Nachrichtenübermittlung, kommen noch andere Aufgaben dazu. Welche sind das?**

- Authentifikation (stelle sicher, dass eine Nachricht von X wirklich von X ist)
- Integrität (stelle sicher, dass eine Nachricht im Zuge der Übermittlung nicht verändert wurde).

**Wie gehen Alice und Bob vor, wenn sie Nachrichten übermitteln wollen?**
Zu einem Zeitpunkt, an dem sie vor Oscar sicher sind, vereinbaren sie ein Kryptosystem $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$ **und** einen Schlüssel $K \in \mathcal{K}$.

**Was ist das Prinzip Kerckhoff?**
Die Sicherheit eines Kryptosystems darf nicht von der Geheimhaltung der *Chiffrierungsregel* abhängen, sondern darf nur auf der Geheimhaltung des *Schlüssels* beruhen. Mit anderen Worten: Selbst wenn Oscar weiß, wie du verschlüsselst, soll er deine Nachrichten nicht entschlüsseln können, solange er den Schlüssel nicht kennt.

# Mono- und polyalphabetische Kryptosysteme

**Was ist der Unterschied zwischen monoalphabetischen und polyalphabetischen Kryptosystemen?**

- In monoalphabetischen Kryptosystemen werden einzelne Buchstaben auf einzelne Buchstaben verschlüsselt.
- In polyalphabetischen Kryptosystemen werden einzelne Buchstaben nicht immer auf denselben Buchstaben verschlüsselt.

**Was sind die Chiffrierungsregeln monoalphabetischer Kryptosysteme im Grunde?**
Permutationen.

**Was ist ein Nachteil von monoalphabetischen Kryptosystemen?**
Sie lassen sich durch Häufigkeitsanalysen knacken.

**Was ist der Vorteil eines polyalphabetischen Kryptosystems gegenüber einem monoalphabetischen?**
Die Anwendung einer polyalphabetischen Kryptosystem verschleiert die Buchstabenfrequenzen, damit das Knacken des Systems schwieriger wird.

**Welche monoalphabetischen Kryptosysteme kennen Sie?**

- Atbasch (A wird Z, B wird Y, etc.)
- Verschiebe-Kryptosystem (Cäsar)
- affines Kryptosystem
- Permutations-Kryptosystem

**Welche polyalphabetischen Kryptosysteme kennen Sie?**

- Viginère-Kryptosystem
- One-time Pad
- Hill-Kryptosystem
- Selbstschlüssel-Kryptosystem

**Was sind Blockchiffren?**
Kryptosysteme, bei denen der Klartext in Blöcke einer festen Länge $m$ unterteilt wird, und jeder Block unter der Verwendung des gleichen Schlüssels chiffriert wird.

**Nennen Sie ein Beispiel für eine Blockchiffre!**
Das Viginère-Kryptosystem.

**Was sind Stromchiffren?**
Bei Stromchiffren wählt man für jedes Klartextsymbol einen eigenen Schlüssel.

**Nennen Sie ein Beispiel für eine Stromchiffre!**
Das Selbstschlüssel-Kryptosystem.

**Was bedeutet das Wort *synchron* in der Kryptografie?**
Eine Stromchiffre heißt **synchron**, wenn der Schlüsselstrom *unabhängig vom Klartext* ist.

**Nennen Sie ein Beispiel für eine synchrone Stromchiffre!**
Das One-time-Pad.

**Nennen Sie ein Beispiel für eine asynchrone Stromchiffre!**
Das Selbstschlüssel-Kryptosystem.

# Symmetrische und asymmetrische Kryptosysteme

**Worauf bezieht sich das Wort symmetrisch?**
Auf die Tatsache, dass aus der Chiffrierungsregel $e_K$ die Dechiffrierungsregel $d_K$ leicht berechnet werden kann, und umgekehrt auch. Jeder, der chiffrieren kann, also $e_K$ kennt, kann auch dechiffrieren.

**Worin unterscheiden sich symmetrische und asymmetrische Verschlüsselung?**

- symmetrisch: Die Dechiffrierungsregel ($d_K$) lässt sich leicht aus der Chiffrierungsregel($e_K$) ableiten
- asymmetrisch: Die zwei Schlüssel - der öffentliche und der geheime - können nicht leicht von einander abgeleitet werden. Eine Nachricht kann nicht ohne die Zusatzinformation des geheimen Schlüssels leicht geknackt werden.

**Was sind die Vor- und Nachteile der symmetrischen Kryptosysteme?**

- Vorteile
  - Symmetrische Systeme brauchen nur wenig Rechenaufwand.
- Nachteile
  - Sie sind leicht zu knacken
  - Ein Schlüssel muss irgendwie vereinbart werden.

**Was sind die Vor- und Nachteile der asymmetrischen Kryptosysteme?**

- Vorteile
  - Sicherheit; sie erfüllen die Forderung, dass man den Algorithmus nicht geheim halten muss, weil selbst in Kenntnis von Algorithmus und öffentlichem Schlüssel die Entschlüsselung nur mit unangemessenem Rechenaufwand möglich ist.
- Nachteile
  - Der deutlich höhere Rechenaufwand für Ver- und Entschlüsselung.

**Verwendet man überhaupt symmetrischen Verfahren noch?**
Nur noch dann, wenn die Möglichkeit besteht, den Schlüssel sehr häufig zu wechseln.

# Symmetrische Kryptosysteme

**Was sind Beispiele für symmetrische Kryptosysteme? Wie viele mögliche Schlüssel gibt es jeweils?**

- Monoalphabetische Kryptosysteme
  - Atbasch (A wird Z, B wird Y, etc.), 1 Schlüssel
  - Verschiebe-Kryptosystem (Cäsar), 26 Schlüssel
  - affines Kryptosystem, $\varphi(26) \cdot 26$ Schlüssel
  - Permutations-Kryptosystem, 26! Schlüssel
- Polyalphabetische Kryptosyteme
  - Selbstschlüssel-Kryptosystem, 26 Schlüssel
  - Viginère-Kryptosystem, $26^m$ Schlüssel, wobei $m$ die Länge des Schlüsselworts darstellt.
  - One-time Pad, $2^m$ Schlüssel, wobei $m$ die Länge der binären Nachricht darstellt.
  - Hill-Kryptosystem. Bei Schlüsselworten der Länge $m$ gibt es $26^m < |\operatorname{Gl}_m(\mathbb{Z}/26\mathbb{Z})| < 26^{m^2}$ Schlüssel für $m > 1$.

**Was ist ein Nachteil des Permutations-Kryptosystems? Was kann man dagegen machen?**
Eine Permutation lässt sich schwer merken. Darum verwendet man oft ein Schlüsselwort und einen Schlüsselbuchstaben.

**Erklären Sie das One-time-Pad-Kryptosystem!**
Es handelt sich im Wesentlichen um eine Vigenère-Verschlüsselung, bei der die Schlüsselwortlänge gleich der Länge des Klartextes ist.

**Was ist das Besondere an dem One-time Pad?**
Das One-time Pad ist eines der wenigen Kryptosysteme, von denen man beweisen kann, dass sie sicher sind. Dabei bedeutet Sicherheit, dass Oscar keine Chance hat, seine Kenntnisse über das Kryptosystem zu vergrößern, selbst wenn ihm alle Rechenkapazität der Welt zur Verfügung steht. Das One-time Pad wurde auch als „heißer Draht“ zwischen dem amerikanischen Präsidenten und dem sowjetischen Generalsekretär verwendet.

**Was ist die Schwäche des Viginère-Kryptosystems?**
Kennt man die Blocklänge, ist das Vigenère-Kryptosystem genauso sicher wie das Verschiebekryptosystem.

**Was ist die Klartext- und Geheimtextmenge im Viginère-Kryptosystem?**
$\mathcal{P} = \mathcal{C} = (\mathbb{Z}/\ 26\mathbb{Z})^m$, wobei $m$ die Blocklänge ist.

**Was ist die Schlüsselmenge im Viginère-Kryptosystem?**
$\mathcal{K} = (\mathbb{Z}/\ 26\mathbb{Z})^m$, wobei $m$ die Blocklänge ist.

**Was ist die Schlüsselmenge im Hill-Kryptosystem?**
$\mathcal{K} = \mathrm{Gl_m}(\mathbb{Z}/\ 26\mathbb{Z})$, wobei $m$ die Blocklänge ist.

# Symmetrische Kryptosysteme: Analyse

**Was sind drei Attacken auf Kryptosysteme?**

- Known-ciphertext-attack
- Known-plaintext-attack
- Chosen-plaintext-attack

**Was ist ein Known-ciphertext-attack?**
Oscar kennt ein relativ großes Stück des Geheimtextes.

**Was ist ein Known-plaintext-attack?**
Oscar kennt ein vergleichsweise kleines Stück von zusammengehörigem Klartext und Geheimtext. Dies könnten beispielsweise Standardgrußformeln zu Beginn oder Ende der abgefangenen Nachricht sein.

**Was ist ein Chosen-plaintext-attack?**
Oscar hat Zugang zu einem Chiffrieralgorithmus und möchte die sich dahinter verbergende Chiffrierungsregel und den Schlüssel erkennen. Zum Beispiel gibt es Mailsysteme, bei denen die Möglichkeit zum Chiffrieren von Mails voreingestellt ist. Oscar kann einen Klartext, etwa die Buchstabenfolge e e e e e e .... e e an sich selbst, verschlüsselt, schicken und so versuchen, hinter den Schlüssel zu kommen. Gelingt ihm dies, kann er später chiffrierte Nachrichten versenden, und vorgeben, ein autorisierter Benutzer des Kryptosystems zu sein.

**Wodurch lassen sich manche symmetrischen Kryptosysteme knacken?**
Durch Häufigkeitsanalysen.

**Was sind die zwei häufigsten Buchstaben im Deutschen? Wie oft kommen sie jeweils vor?**
$E$ (etwa 18%) und $N$ (etwa 9%).

**Was sind die zwei häufigsten Bigramme im Deutschen?**
*EN* und *ER*.

**Was ist das häufigste Trigramm im Deutschen?**
*ICH*.

**Wie kann man feststellen, ob ein [deutscher] Text vermutlich polyalphabetisch oder monoalphabetisch verschlüsselt wurde?**
Wir berechnen den Friedmansche Koinzidenzindex. Weicht dieser Wert deutlich von $0,0762$ ab, wurde der Klartext vermutlich polyalphabetisch verschlüsselt.

**Was ist der Friedmansche Koinzidenzindex?**

$I(x) = \frac{\sum_{i=0}^{25} n_i(n_i - 1)}{n(n-1)}$, wobei $n_0$ die Anzahl der a's, $n_1$ die Anzahl der b's, $\ldots n_{25}$ die Anzahl der z's in $x$, einer $n$-elementigen Menge.

**Was ist der Friedemann-Test?**

Man berechnet

$$l \approx \frac{0,0377n}{(n-1)I(x) - 0,0385n + 0,0762}$$

wobei $n$ die Länge des Textes ist. Dann liefert $l$ einen ungefähren Wert für die Blocklänge.

**Was ist der Kasiski-Test**

Häufige Buchstabenkombinationen suchen und Abstände zählen, um die Blocklänge herauszubekommen.

**Wie kann man das Hill-Kryptosystem brechen?**

*Das Hill-Kryptosystem ist mit einem Known-Ciphertext-Angriff allein nicht leicht zu brechen.* Anders ist es dagegen mit einem Known-Plaintext-Angriff. Hier kennt Oscar ein vergleichsweise kleines Stück von zusammengehörigem Klartext und Geheimtext. Dies könnten beispielsweise Standardgrußformeln zu Beginn oder Ende der abgefangenen Nachricht sein. Wenn Oscar die Blocklänge kennt, dann ergibt sich ein großes lineares Gleichungssystem, das man mit Glück lösen kann.

**Das Hill-Kryptosystem hat ja mit invertierbaren Matrizen über kommutativen Ringen zu tun. Welcher Satz ermöglicht es uns, Matrizen über kommutativen Ringen zu invertieren (sofern die Matrizen invertierbar sind)?**

Der Adjunktensatz.

**Wie lautet der Adjunktensatz?**

Sei $R$ ein kommutativer Ring, und sei $A \in M_{nn}(R)$. Dann gilt $AA^{Ad} = A^{Ad}A = \det(A)I_n$.

**Wie rechnet man anhand des Adjunktensatzes die inverse zu einer Matrix $A$ aus?**

$A^{-1} = \det(A)^{-1}A^{Ad}$.

**Wie berechnet man den Adjunkten einer Matrix $A$?**

Sei $A = (a_{ij}) \in M_{mm}(R)$. Dann ist $A^{Ad} = (a'_{ij}) \in M_{mm}(R)$, wobei für alle $1 \leq i, j \leq m$ gilt: $a'_{ij} = (-1)^{i+j} \det A_{ji}$ und $A_{ji} \in M_{m-1,m-1}(R)$ ist die Matrix, die aus $A$ entsteht, indem wir die $j$-te Zeile und die $i$-te Spalte aus $A$ streichen.

## Asymmetrische Kryptosysteme: *Public-Key-Kryptosysteme*

**Nennen Sie Beispiele für asymmetrische Kryptosysteme! Wann wurden Sie jeweils erfunden?**

- Diffie-Hellman (1976)
- Rivest-Shamir-Adleman *RSA* (1978)
- Merkle-Hellman *Knapsack* (1978, gebrochen 1984)
- Massey-Omura (1983)
- ElGamal (1985)

**Kennen Sie ein Schlüsselaustauschverfahren?**
Diffie-Hellman.

**Was ist das heute noch am häufigsten eingesetzte Public-Key-Kryptosystem?**
RSA.

**Was war das erste Public-Key-Kryptosystem?**
Diffie-Hellman.

**Wird eine Nachricht bei Diffie-Hellman geschickt?**
Nein, es wird keine Nachricht geschickt, sondern ein Schlüssel für ein anderes [symmetrisches] Kryptosystem vereinbart.

**Was für eine Rolle spielt die Reihenfolge der Kommunikationen in Diffie-Hellman?**
Die Reihenfolge der Kommunikationen spielt keine Rolle.

**Welcher Teilnehmer ist verantwortlich für die Erfindung des Schlüssels in Diffie-Hellman?**
Der Schlüssel, der vereinbart wird, wird nicht von einem Teilnehmer erfunden, sondern hängt von den Zahlen ab, die beide Teilnehmer wählen.

**Auf welchen mathematischen Problemen basieren Public-Key-Kryptosysteme? Welche Kryptosysteme basieren auf welchen Problemen?**

- Auf der Faktorisierung großer Primzahlen (*RSA*)
- Auf dem Diskreter-Logarithmus-Problem
  - Diffie-Hellman
  - Massey-Omura
  - ElGamal

- Auf dem Teilmengen-Summen-Problem (*Knapsack*)

**Wofür steht DLP?**
*D*iskreter-*L*ogarithmus-*P*roblem.

**Es gibt Gruppen, für die das Diskreter-Logarithmus-Problem ganz einfach zu lösen ist, z.B. $\mathbb{Z}$. Bei welchen Gruppen ist das Problem schwer?**
Für endliche Körper und elliptische Kurven (bzw. deren Untergruppen).

**Auf was für Gruppen haben wir die Kryptosysteme angewendet, die auf dem Diskreter-Logarithmus-Problem basieren?**
Auf elliptische Kurven und auf die Einheitengruppen endlicher Körper (insbesondere auf $\mathbb{F}_{p^n}, p \in \mathbb{P}, n \in \mathbb{N}$, nicht nur auf $\mathbb{F}_p$, schließlich ist $\mathbb{F}_{p^n}$ auch eine zyklische Gruppe, da endlich).

**Was ist das Diskreter-Logarithmus-Problem für endliche Körper?**
Sei $\mathbb{K}$ ein endlicher Körper, und sei $g \in \mathbb{K}^\times$ ein primitives Element von $\mathbb{K}^\times$. Gegeben sei $a \in \mathbb{K}^\times$. Bestimme $x \in \mathbb{Z}$ mit $a = g^x$.

**Was ist das Diskreter-Logarithmus-Problem für elliptische Kurven?**
Sei $E(a, b, \mathbb{K})$ eine elliptische Kurve, und sei $P \in E(a, b, \mathbb{K})$ ein Punkt auf der elliptischen Kurve. Gegeben sei $A \in \langle P \rangle \subseteq E(a, b, \mathbb{K})$. Bestimme $x \in \mathbb{Z}$ mit $A = Px$.

**Was vermutet man über das Diskreter-Logarithmus-Problem?**
Man vermutet, dass es keinen effizienten Algorithmus gibt, um das DLP über endlichen Körpern oder elliptischen Kurven zu lösen.

**Was vermutet man über das Diskreter-Logarithmus-Problem auf elliptschen Kurven?**
Dass das DLP über elliptischen Kurven „schwerer“ ist als über endlichen Körpern. Das heißt, selbst, wenn es einmal einen effizienten oder fast effizienten Algorithmus für das DLP für endliche Körper geben sollte, dann heißt das wahrscheinlich noch nicht, dass es auch einen für elliptische Kurven gibt.

**Es stellt sich heraus, dass das diskreter-Logarithmus-Problem für die elliptischen Kurven scheinbar schwerer zu lösen ist als das über den endlichen Körpern. Was hat das für praktische Konsequenzen?**
Das heißt, dass man die Größe des endlichen Körpers für Kryptoverfahren über endlichen Körpern sehr viel größer wählen muss als bei den elliptischen Kurven, um die gleiche Sicherheitsstufe zu erreichen. Das ist der große Vorteil der Kryptoverfahren über elliptischen Kurven, dass die Körpergröße relativ klein gewählt werden kann und damit wenig Speicherplatz verbraucht wird und auch schneller gerechnet werden kann. Dies führt dazu, dass die elliptischen Kurven immer öfter verwendet werden.

# RSA

**Auf welchem Problem basiert RSA und warum gilt es als sicher?**
Es wird vermutet, dass man $m$ faktorisieren muss ($m = pq$), um RSA zu brechen. Weiter wird vermutet, dass Faktorisierung nicht effizient möglich ist.

**Wie findet man die zwei Primzahlen $p$ und $q$, die man für das RSA-Verfahren braucht?**
Durch probabilistische Primzahltests. Es wird zufällig eine ungerade Zahl $n$ ermittelt, und dann wird ein Primzahltest auf diese Zahl losgelassen. Entweder besteht die Zahl den Test und ist selbst [höchstwahrscheinlich] eine Primzahl oder der Test wird für $n+2$ wiederholt. Das wird so lange fortgesetzt bis eine Primzahl gefunden ist.

**Wie findet man die Zahl $e$ im RSA-Verfahren?**
Ein Zufallszahlengenerator schlägt eine Zahl $e$ vor. Mit Hilfe des *Euklidischen Algorithmus* berechnet man $\mathrm{ggT}(e, \varphi(m))$. Ist das Ergebnis $\neq 1$, so setzt man $e$ auf $e+1$ und versucht es erneut. Nach wenigen Schritten wird man eine passende Zahl $e$ gefunden haben. ERGÄNZUNG: Das ist die Erklärung im Skript (S. 170), aber mir scheint, es wäre besser, wieder eine *ungerade* Zahl für $e$ zu wählen, und dann $e$ auf $e+2$ zu setzen, denn $\varphi(m)$ wird unweigerlich eine *gerade* Zahl sein.

**Wie findet man die Zahl $d$ im RSA-Verfahren?**
Mit dem erweiterten Euklidischen Algorithmus.

**Was berechnet der erweiterte Euklidische Algorithmus allgemein?**
Seien $a, b \in \mathbb{Z}$. Der erweiterte Euklidische Algorithmus berechnet Koeffizienten $r, s \in \mathbb{Z}$, sodass $\mathrm{ggT}(a, b) = r \cdot a + s \cdot b$.

**Wie berechnet man $N^e$ in dem RSA-Verfahren?**
Durch wiederholtes Quadrieren, bei dem nicht jede Potenz berechnet wird, nur $N^2, N^4, N^8$ usw. Der Exponent wird dann als Summe von 2-er Potenzen dargestellt und die berechneten Potenzen eingesetzt.

**Welche Menge stellt $\mathcal{P}$ bei RSA dar?**
Diese Menge ist $\mathcal{P} = \mathbb{Z}/m\mathbb{Z}$ mit $m = pq$. *Insbesondere müssen $a$ und $m$ nicht teilerfremd sein.* Wir haben im Kurs eine Verallgemeinerung des kleinen Satzes von Fermat bewiesen, sodass wir wissen, dass alle Zahlen in $\mathbb{Z}/m\mathbb{Z}$ ver- und entschlüsselt werden können.

**Welche Verallgemeinerung des kleinen Satzes von Fermat braucht man bei RSA?**
Seien $p$ und $q$ **verschiedene** Primzahlen. Sei $c$ eine natürliche Zahl mit $c \equiv 1 \pmod{\varphi(pq)}$. Dann gilt $a^c \equiv a \pmod{pq}$ für alle $a \in \mathbb{Z}$.

**Können Sie die Verallgemeinerung des kleinen Satzes von Fermat, die man beim RSA-Verfahren braucht, beweisen?**
Wir werden zeigen, dass $p|(a^c - a)$ und $q|(a^c - a)$ gelten. Da $p$ und $q$ verschiedene Primzahlen sind, folgt dann $pq|(a^c - a)$ und damit $a^c \equiv a \pmod{pq}$.
Fall 1: Wenn $p$ ein Teiler von $a$ ist, so folgt $p|(a^c - a)$.
Fall 2: Angenommen, $p$ teilt nicht $a$. Dann gilt

$$\begin{aligned}
a^c &\equiv a^{k\varphi(pq)+1} && \text{für ein } k \in \mathbb{Z} \\
&\equiv a^{k(p-1)(q-1)+1} && \text{denn } \varphi(pq) = (p-1)(q-1) \\
&\equiv (a^{p-1})^{k(q-1)} a \\
&\equiv 1^{k(q-1)} a && \text{mit dem kleinen Satz von Fermat} \\
&\equiv a && \pmod{p}
\end{aligned}$$

Aus $a^c \equiv a \pmod{p}$ folgt dann $p|(a^c - a)$. In beiden Fällen gilt also $p|(a^c - a)$. Nun lassen wir $p$ und $q$ die Rollen tauschen und erhalten $q|(a^c - a)$.

**Beschreiben Sie das RSA-Kryptosystem!**
Schlüsselerstellung

- Zwei große, verschiedene Primzahlen $p$ und $q$ wählen
- Zwei Produkte berechnen

$$\begin{aligned} m &= pq \text{ und} \\ \varphi(m) &= (p-1)(q-1) \end{aligned}$$

- Eine Zahl $e$ mit $\mathrm{ggT}(e, \varphi(m)) = 1$ wählen
- Eine Zahl $d$ mit $ed \equiv 1 \mod \varphi(m)$ berechnen

Geheimer Schlüssel $(p, q, d)$
Öffentlicher Schlüssel: $(m, e)$

Ziel: Alice möchte die Nachricht $N \in \mathbb{Z}/m\mathbb{Z}$ an Bob schicken.

Kommunikationen: Alice schickt $N^e$.

Nacharbeit: Bob berechnet

$$\begin{aligned} (N^e)^d &= N^{ed} \\ &= N^{\varphi(m)v+1} && v \in \mathbb{Z} \\ &= N \in \mathbb{Z}/m\mathbb{Z} \end{aligned}$$

**Geben Sie ein Beispiel dafür, wie das RSA-Verfahren läuft!**
Schlüsselerstellung

- $p := 7$ und $q := 11$
- $m = pq = 77$ und $\varphi(m) = (p-1)(q-1) = 60$
- $e := 7$ und $d := 43$

Geheimer Schlüssel $(7, 11, 43)$
Öffentlicher Schlüssel $(77, 7)$

Ziel: Alice möchte die Nachricht $N := 3$ an Bob schicken.

Kommunikationen: Alice schickt $N^e = 3^7 = 31$.

Nacharbeit: Bob berechnet $(N^e)^d = 31^{43} = 3 = N \in \mathbb{Z}/m\mathbb{Z}$.

# endliche Körper

**Was sind endliche Körper**
Das sind Körper mit endlich vielen Elementen.

**Welche Eigenschaften haben endliche Körper?**

- Die Charakteristik eines endlichen Körpers ist immer eine Primzahl $p$.
- Es gibt zu jeder Primzahl $p$ und jedem $n \in \mathbb{N}$ bis auf Isomorphie genau einen Körper mit $p^n$ Elementen.
- Der Primkörper eines endlichen Körpers ist ein Körper der Form $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, wobei $p$ eine Primzahl ist.
- Jeder endliche Körper ist eine endliche Erweiterung seines Primkörpers.
- Ist $\mathbb{K}$ ein endlicher Körper, dann ist $(\mathbb{K}^\times, \cdot)$ zyklisch. Daraus folgt direkt, dass $\mathbb{K}$ eine einfache algebraische Erweiterung seines Primkörpers $\mathbb{P}$ ist, nämlich $\mathbb{P}(a)$, wobei $a$ ein primitives Element von $\mathbb{K}^\times$ ist.
- Wenn $\mathrm{char}(\mathbb{K}) = p$ gilt, dann ist $(a+b)^p = a^p + b^p$ für alle $a, b \in \mathbb{K}$.
- Ist $\mathbb{K}$ ein endlicher Körper mit $\mathrm{char}(\mathbb{K}) = p$, dann ist die Abbildung $a \mapsto a^p$ für alle $a \in \mathbb{K}$ ein Automorphismus.
- Die Anzahl der Elemente eines endlichen Körpers $\mathbb{K}$ ist $p^n$, wobei $p$ die Charakteristik von $\mathbb{K}$ und $n$ der Grad der Körpererweiterung von $\mathbb{K}$ über seinem Primkörper ist.

**Was ist ein Primkörper?**
Ein Körper $\mathbb{K}$, der keine Unterkörper enthält, die eine echte Teilmenge von $\mathbb{K}$ sind.

**Enthält jeder Körper einen Primkörper als kleinsten Unterkörper?**
Ja.

**Was sind die einzigen Körper (bis auf Isomorphie), die Primkörper sein können?**
$\mathbb{Q}$ und $\mathbb{F}_p, p \in \mathbb{P}$.

**Was sind die einzigen Körper (bis auf Isomorphie), die Primkörper in endlichen Körpern sein können?**
$\mathbb{F}_p, p \in \mathbb{P}$.

**Wie sehen die Elemente eines endlichen Körpers $\mathbb{F}_p$ aus?**
Das sind die Elemente vom Ring $\mathbb{Z}/p\mathbb{Z}$. Mit anderen Worten sind das die Zahlen zwischen einschließlich 0 und $p-1$.

**Warum gibt es denn genau $p^n$ Elemente in $\mathbb{F}_{p^n}$?**
Ist $\mathbb{K} = \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$, $p$ eine Primzahl, ein Körper mit $p$ Elementen, so gibt es $p^n$ Polynome

$$a_0 + a_1 T + \ldots + a_{n-1} T^{n-1}$$

vom Grad $< n$, denn für jeden Koeffizienten $a_i$ haben wir $p$ Möglichkeiten.

**Wie sehen die Elemente des Körpers $\mathbb{F}_{2^3}$ aus?**
Jedes Element wird repräsentiert von einem Polynom vom Grad $< 3$ und steht für eine Restklasse modulo einem Ideal eines irreduziblen Polynoms, z.B. $T^3 + T + 1$.

**Was wissen wir über Hauptidealringe, das uns dabei hilft, endliche Körper zu konstruieren?**
Wir kennen Satz 5.6.10: Wenn $R$ ein Hauptidealring ist, so ist $R/(c)$ genau dann ein Körper, wenn $c$ ein Primelement in $R$ ist.

**Gibt es zu jedem $p^n$ einen endlichen Körper?**
Ja, und zwar gibt es bis auf Isomorphie genau einen.

**Gibt es einen endlichen Körper mit 6 Elementen? Begründen Sie ihre Antwort!**
Nein, denn 6 ist keine Primzahlpotenz.

**Was ist denn ein primitives Element?**
Wenn $\mathbb{F}$ ein endlicher Körper ist, dann wird ein erzeugendes Element von $\mathbb{F}^\times$ ein primitives Element in $\mathbb{F}$ genannt.

**Konstruieren Sie mal einen Körper mit 8 Elementen!**
Wir betrachten den Ring $\mathbb{F}_2[T]$. Das ist ein Hauptidealring. Nun brauchen wir ein irreduzibles Element dritten Grades, z.B. $T^3+T+1$. Dann ist der Faktorring $\mathbb{F}_2[T]/(T^3+T+1)$ ein Körper. Die Elemente der Körper werden repräsentiert durch Polynome vom Grad $< 3$ und stehen für Restklassen modulo $(T^3 + T + 1)$.

**Sei $f \in \mathbb{F}_2[T]$ irreduzibel. Was ist die Beziehung zwischen $\mathbb{F}_2[T]/(f)$ und $\mathbb{F}_2$?**
Der Körper $\mathbb{F}_2[T]/(f)$ ist ein Erweiterungskörper von $\mathbb{F}_2$, also $\mathbb{F}_2[T]/(f) : \mathbb{F}_2$. Dazu muss man allerdings die Restklasse $[0]$ beziehungsweise $[1]$ in $\mathbb{F}_2[T]/(f)$ mit den Körperelementen 0 beziehungsweise 1 identifizieren.

**Wie multipliziert bzw. addiert man zwei Elemente in dem Körper $\mathbb{F}_{2^3}$?**
In dem wir die Verknüpfung ausführen, und dann anschließend durch das irreduzible Polynom $f$ dividieren, das wir verwendet haben, um den Körper zu konstruieren. Wir können dann auch Verknüpfungstabellen für Addition und Multiplikation erstellen, indem wir die Elemente des Körpers in eine Tabelle schreiben, und dann wieder das Resultat in die Tabelle eintragen, nachdem wir gegebenenfalls durch $f$ dividiert und den

Rest genommen haben.

**Welchen Trick kann man einsetzen, um festzustellen, welche Polynome irreduzibel sind?**
Man kann Proposition 5.7.22 einsetzen: Ein Polynom $f$ in $\mathbb{K}[T]$ vom Grad 2 oder 3 ist genau dann irreduzibel, wenn es keine Nullstelle in $\mathbb{K}$ hat.

**Erklären Sie die Begriffe Unterkörper und Körpererweiterung!**
Eine nichtleere Teilmenge $\mathbb{K}$ eines Körpers $\mathbb{L}$ heißt Unterkörper von $\mathbb{L}$, wenn $\mathbb{K}$ mit den Verknüpfungen $+$ und $\cdot$ in $\mathbb{L}$ ein Körper ist. In diesem Fall heißt $\mathbb{L}$ Körpererweiterung oder Erweiterungskörper von $\mathbb{K}$. Ein solcher Körper $\mathbb{L}$ von $\mathbb{K}$ wird mit $\mathbb{L} : \mathbb{K}$ notiert.

**Wie ist der Grad einer Körpererweiterung definiert?**
Sei $\mathbb{L} : \mathbb{K}$ eine Körpererweiterung. Der Grad der Körpererweiterung ist

$$[\mathbb{L} : \mathbb{K}] = \dim_{\mathbb{K}} \mathbb{L}.$$

Die Körpererweiterung $\mathbb{L} : \mathbb{K}$ heißt endlich oder unendlich, je nachdem, ob $[\mathbb{L} : \mathbb{K}]$ endlich oder unendlich ist.

**Wie lautet der Gradsatz?**
Seien $\mathbb{M} : \mathbb{L}$ und $\mathbb{L} : \mathbb{K}$ **endliche** Körpererweiterungen. Dann ist $\mathbb{M} : \mathbb{K}$ ebenfalls endlich, und es gilt

$$[\mathbb{M} : \mathbb{K}] = [\mathbb{M} : \mathbb{L}][\mathbb{L} : \mathbb{K}].$$

**Was lässt sich mit dem Gradsatz zeigen, was $\mathbb{R}$ und $\mathbb{C}$ angeht?**
Mit dem Gradsatz lässt sich zum Beispiel zeigen, dass es keinen Körper gibt, der zwischen den Körpern $\mathbb{R}$ und $\mathbb{C}$ liegt, das heißt, es gibt keinen Körper, der $\mathbb{R}$ als echte Teilmenge enthält und der andererseits eine echte Teilmenge von $\mathbb{C}$ ist.

**Was bedeutet das Wort *algebraisch*?**
Sei $\mathbb{L} : \mathbb{K}$ eine Körpererweiterung, und sei $a \in \mathbb{L}$. Ist $a$ Nullstelle eines Polynoms $f \in \mathbb{K}[T], f \neq 0$, dann heißt $a$ algebraisch über $\mathbb{K}$.

**Was ist ein Zerfällungskörper?**
Sei $\mathbb{L} : \mathbb{K}$ eine Körpererweiterung, und sei $f \in \mathbb{K}[T]$ nicht konstant. Wir sagen, dass $f$ über $\mathbb{L}$ zerfällt, wenn $f$ über $\mathbb{L}$ als Produkt von Linearfaktoren geschrieben werden kann, also

$$f = a(T - a_1)(T - a_2) \dots (T - a_n) \text{ mit } a, a_1, \dots, a_n \in \mathbb{L}.$$

Der Körper $\mathbb{L}$ heißt Zerfällungskörper von $f$, wenn $f$ über $\mathbb{L}$ zerfällt, und wenn $\mathbb{L} = \mathbb{K}(a_1, \dots, a_n)$ gilt.

**Wozu haben wir in diesem Kurs Zerfällungskörper gebraucht?**
Um die Existenz von Körpern mit $p^n$ Elementen für jede Primzahl $p$ und jedes $n \in \mathbb{N}$

zu zeigen.

**Was ist ein Minimalpolynom?**
Sei $a \in \mathbb{L}$ algebraisch über $\mathbb{K}$. Das eindeutig bestimmte normierte Polynom $g \in \mathbb{K}[T]$ mit $(g) = \{f \in \mathbb{K}[T] | f(a) = 0\}$ heißt Minimalpolynom von $a$. Der Grad von $g$ wird auch als Grad von $a$ über $\mathbb{K}$ bezeichnet.

**Beschreiben Sie das Diffie-Hellman-Verfahren in endlichen Körpern!**
Schlüsselerstellung

- ein großer endlicher Körper $\mathbb{K}$ wählen
- ein primitives Element $g \in \mathbb{K}^\times$ wählen
- Alice wählt $a \in \mathbb{N}$ mit $1 \leq a \leq |\mathbb{K}^\times|$.
- Bob wählt $b \in \mathbb{N}$ mit $1 \leq b \leq |\mathbb{K}^\times|$.

Geheimer Schlüssel

- Alice: $a$
- Bob: $b$

Öffentlicher Schlüssel $(\mathbb{K}, g)$

Ziel: Alice und Bob möchten einen Schlüssel $K \in \mathbb{K}^\times$ vereinbaren.

Kommunikationen (2)

- Alice schickt $g^a$.
- Bob schickt $g^b$.

Nacharbeit

- Alice berechnet $K := (g^b)^a = g^{ab} \in \mathbb{K}^\times$.
- Bob berechnet $K := (g^a)^b = g^{ab} \in \mathbb{K}^\times$.

Merke: $K$ ist der neu vereinbarte Schlüssel, den man sonst wie weiter verwenden kann, und ist nicht mit den geheimen und öffentlichen Schlüsseln des Diffie-Hellman-Verfahrens zu verwechseln.

**Geben Sie ein Beispiel für das Diffie-Hellman-Verfahren über endlichen Körpern!**

Schlüsselerstellung

- $\mathbb{K} := \mathbb{F}_{19}$
- $g := 2$
- Alice wählt $a := 3$.
- Bob wählt $b := 4$.

Geheimer Schlüssel

- Alice: 3.
- Bob: 4.

Öffentlicher Schlüssel $(\mathbb{F}_{19}, 2)$

Ziel: Alice und Bob möchten einen Schlüssel $K \in \mathbb{F}_{19}^{\times}$ vereinbaren.

Kommunikationen

- Alice schickt $g^a = 2^3 = 8$.
- Bob schickt $g^b = 2^4 = 16$.

Nacharbeit

- Alice berechnet $K := (g^b)^a = 16^3 = 11 \in \mathbb{F}_{19}^{\times}$.
- Bob berechnet $K := (g^a)^b = 8^4 = 11 \in \mathbb{F}_{19}^{\times}$.

**Beschreiben Sie das Massey-Omura-Verfahren in endlichen Körpern!**

Schlüsselerstellung

- ein großer endlicher Körper $\mathbb{K}$
- Alice
  - wählt $e_A \in \mathbb{N}$ mit $1 \leq e_A \leq |\mathbb{K}^\times|$ und $\mathrm{ggT}(e_A, |\mathbb{K}^\times|) = 1$, und
  - berechnet $d_A$ mit dem Euklidischen Algorithmus, sodass $e_A d_A \equiv 1 \pmod{|\mathbb{K}^\times|}$.
- Bob
  - wählt $e_B \in \mathbb{N}$ mit $1 \leq e_B \leq |\mathbb{K}^\times|$ und $\mathrm{ggT}(e_B, |\mathbb{K}^\times|) = 1$, und
  - berechnet $d_B$ mit dem Euklidischen Algorithmus, sodass $e_B d_B \equiv 1 \pmod{|\mathbb{K}^\times|}$.

Geheimer Schlüssel

- Alice: $(e_A, d_A)$
- Bob: $(e_B, d_B)$

Öffentlicher Schlüssel ($\mathbb{K}$)

Ziel: Alice möchte die Nachricht $N \in \mathbb{K}^\times$ an Bob schicken.

Kommunikationen (3)

- Alice schickt $N^{e_A}$.
- Bob schickt $(N^{e_A})^{e_B}$.
- Alice schickt $(N^{e_A e_B})^{d_A}$.

Nacharbeit: Bob berechnet

$$\begin{aligned}
(N^{e_A e_B d_A})^{d_B} &= (N^{e_A d_A})^{e_B d_B} \\
&= (N^{|\mathbb{K}^\times| v+1})^{e_B d_B} && v \in \mathbb{Z} \\
&= N^{e_B d_B} \\
&= N^{|\mathbb{K}^\times| w+1} && w \in \mathbb{Z} \\
&= N \in \mathbb{K}^\times
\end{aligned}$$

**Geben Sie ein Beispiel für Massey-Omura über endlichen Körpern!**

Schlüsselerstellung

- $\mathbb{K} = \mathbb{F}_{31}$
- Alice
  - wählt $e_A := 7$ und
  - berechnet $d_A := 13$.
- Bob
  - wählt $e_B := 11$ und
  - berechnet $d_B := 11$.

Geheimer Schlüssel

- Alice: $(7, 13)$
- Bob: $(11, 11)$

Öffentlicher Schlüssel ($\mathbb{F}_{31}$)

Ziel: Alice möchte die Nachricht $N := 3 \in \mathbb{F}_{31}$ an Bob schicken.

Kommunikationen (3)

- Alice schickt $N^{e_A} = 3^7 = 17$.
- Bob schickt $(N^{e_A})^{e_B} = 17^{11} = 22$.
- Alice schickt $(N^{e_A e_B})^{d_A} = 22^{13} = 13$.

Nacharbeit

- Bob berechnet $(N^{e_A e_B d_A})^{d_B} = 13^{11} = 3 = N \in \mathbb{F}_{31}$.

**Beschreiben Sie das ElGamal-Verfahren in endlichen Körpern!**

Schlüsselerstellung

- ein großer endlicher Körper $\mathbb{K}$ und
- ein primitives Element $g \in \mathbb{K}^\times$
- Alice wählt $a \in \mathbb{N}$ mit $1 \leq a \leq |\mathbb{K}^\times|$.
- Bob wählt $b \in \mathbb{N}$ mit $1 \leq b \leq |\mathbb{K}^\times|$.

Geheimerschlüssel

- Alice: $a$
- Bob: $b$

Öffentlicher Schlüssel: $(\mathbb{K}, g)$

Ziel: Alice möchte die Nachricht $N \in \mathbb{K}^\times$ an Bob schicken.

Kommunikationen (2)

- Bob schickt $g^b$.
- Alice schickt $(g^a, N(g^b)^a)$.

Nacharbeit: Bob berechnet die Nachricht $N(g^b)^a \cdot (g^a)^{|\mathbb{K}^\times|-b} = Ng^{ab} \cdot g^{-ab} = N \in \mathbb{K}^\times$.

**Geben Sie ein Beispiel für ElGamal über endlichen Körpern!**
Schlüsselerstellung

- $\mathbb{K} := \mathbb{F}_{19}$
- $g := 2$
- Alice wählt $a := 3$.
- Bob wählt $b := 4$.

Geheimer Schlüssel

- Alice: 3
- Bob: 4

Öffentlicher Schlüssel $(\mathbb{F}_{19}, 2)$

Ziel: Alice möchte die Nachricht $N := 5 \in \mathbb{F}_{19}^{\times}$ an Bob schicken.

Kommunikationen (2)

- Bob schickt $g^b = 2^4 = 16$.
- Alice schickt $(g^a = 2^3 = 8, N(g^b)^a = 5(16)^3 = 5 \cdot 11 = 17)$.

Nacharbeit: Bob berechnet die Nachricht $(g^a)^{|\mathbb{K}^{\times}|-b} \cdot N(g^b)^a = 8^{18-4} \cdot 17 = 7 \cdot 17 = 5 = N \in \mathbb{F}_{19}^{\times}$.

# Elliptische Kurven

**Gibt es neben den endlichen Körpern eine weitere Grundmenge, für die Kryptosysteme eingeführt wurden?**
Elliptische Kurven.

**Was ist eine elliptische Kurve?**
Wie der Name schon sagt, sind elliptische Kurven Kurven, das heißt, eine Menge von Punkten im zweidimensionalen Raum über dem betrachteten Körper. Darüber hinaus sind sie grafisch schön vorstellbar. Ich kann Ihnen gerne ein Beispiel zeichnen.

**Was ist das Interessante an elliptischen Kurven?**
Dass man die Punkte der Kurve nach bestimmten Vorschriften addieren kann und auf diese Art und Weise eine abelsche Gruppe erhält. Ist darüber hinaus der zugrunde liegende Körper ein *endlicher* Körper, dann erhält man so eine *endliche* abelsche Gruppe, in der man *effizient* rechnen kann.

**Welche Art von elliptischen Kurven spielen in der Kryptografie eine Rolle?**
Klassischerweise werden eher elliptische Kurven über den reellen und komplexen Zahlen studiert. Bei den elliptischen Kurven über einem endlichen Körper $\mathbb{K}$ werden in der Regel drei Fälle getrennt betrachtet:

- $\mathrm{char}(\mathbb{K}) = 2$
- $\mathrm{char}(\mathbb{K}) = 3$
- $\mathrm{char}(\mathbb{K}) > 3$.

Anwendung in der Kryptografie finden entweder elliptische Kurven über $\mathbb{F}_p$, wobei $p$ eine große Primzahl ist, oder elliptische Kurven über $\mathbb{F}_{2^n}$ für großes $n \in \mathbb{N}$.

**Wie wird der Punkt $\mathcal{O}$, der zu jeder elliptischen Kurve gehört, genannt?**
Der *Punkt bei Unendlich*.

**Wie kann man die Addition zweier Punkte $P$ und $Q$ auf einer elliptischen Kurve vorstellen?**
Sind zwei Punkte $P = (x_1, y_1)$ und $Q = (x_2, y_2)$ in $E(a, b, \mathbb{R})$ gegeben, dann verbindet man diese beiden Punkte durch eine Gerade. Diese Gerade schneidet die elliptische Kurve in einem weiteren Punkt $R' = (x_3', y_3')$. Die Summe $P+Q$ ist dann der an der $x$-Achse gespiegelte Punkt $R = (x_3, y_3)$, also $x_3 = x_3'$ und $y_3 = -y_3'$.

**Wie kann man die Addition zweier Punkte $P$ und $Q$ auf einer elliptischen Kurve vorstellen, wenn beide Punkte gleich sind?**
Gilt $P = Q$, so geht man vor wie oben, nimmt aber die Tangente in $P$ an der Kurve (anschaulich ist das die Gerade, die die Kurve in $P$ *berührt*). Diese schneidet dann wieder in einem weiteren Punkt $R'$ die Kurve, und $P + P = 2P = R$, wobei $R$ der an der

$x$-Achse gespiegelte Punkt $R'$ ist.

**Was ist das neutrale Element der Gruppenstruktur auf einer elliptischen Kurve?**
Der *Punkt bei Unendlich*, $\mathcal{O}$.

**Wie findet man das inverse Element zu einem Punkt $P$ auf einer elliptischen Kurve für den Fall** char $> 3$**?**
Um zu einem Punkt $P$ das Inverse, also $-P$, zu bekommen, spiegelt man den Punkt an der $x$-Achse. Ist also $P = (x, y) \in E(a, b, \mathbb{K})$, dann ist $-P = (x, -y) \in E(a, b, \mathbb{K})$.

**Wie findet man das inverse Element zu einem Punkt $P$ auf einer elliptischen Kurve für den Fall** char $= 2$**?**
Ist $P = (x, y) \in E(a, b, \mathbb{K})$, dann ist $-P = (x, x + y) \in E(a, b, \mathbb{K})$.

**Warum gilt die Bedingung $4a^3 + 27b^2 \neq 0$ bei elliptischen Kurven?**
Diese Bedingung stellt sicher, dass es keine sogenannten *Singularitäten* auf der Kurve gibt. Das sind zum Beispiel Spitzen oder Punkte, an denen sich die Kurve selbst schneidet.

**Wie lautet die Merkregel für drei Punkte auf einer Geraden bei einer elliptischen Kurve?**
Liegen drei Punkte $P, Q, R \in E(a, b, \mathbb{R})$ auf einer Geraden, dann gilt $P + Q + R = \mathcal{O}$.

**Wie sind elliptische Kurven der Charakteristik $> 3$ definiert?**
$E(a, b, \mathbb{K}) = \{(x, y) \in \mathbb{K}^2 | y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\}$ mit $a, b \in \mathbb{K}$ und $4a^3 + 27b^2 \neq 0$.

**Wie sind elliptische Kurven der Charakteristik $= 2$ definiert?**
$E(a, b, \mathbb{K}) = \{(x, y) \in \mathbb{K}^2 | y^2 + xy = x^3 + ax^2 + b\} \cup \{\mathcal{O}\}$ mit $a, b \in \mathbb{K}$ und $b \neq 0$.

**Wie kann man verstehen, dass bei einer elliptischen Kurve der Charakteristik $= 2$ die Bedingung $b \neq 0$ eingehalten werden muss?**
Wenn man es genau betrachtet, ist das die gleiche Bedingung als bei elliptischen Kurven der Charakteristik $> 3$, wo die Bedingung $4a^3 + 27b^2 \neq 0$ herrscht. Durch die Charakteristik 2 gilt $4a^3 + 27b^2 \neq 0 \iff b^2 \neq 0$ und durch die Nullteilerfreithit gilt $b^2 \neq 0 \iff b \neq 0$.

**Sind die Gruppen, die auf elliptischen Kurven definiert werden, immer zyklisch? Welcher Satz sagt etwas darüber aus?**
Nein, sie sind nicht immer zyklisch. Es gilt nämlich folgender Satz: Sei $E(a, b, \mathbb{K})$ eine elliptische Kurve. Dann ist

$$E(a, b, \mathbb{K}) \simeq (\mathbb{Z}/d_1\mathbb{Z}) \times (\mathbb{Z}/d_2\mathbb{Z}),$$

wobei $d_1 | d_2$.

**Was liefert der Satz von Hasse?**
Eine Abschätzung der Anzahl der Punkte einer elliptischen Kurve.

**Wie lautet der Satz von Hasse?**
Sei $N$ die Anzahl der Punkte einer elliptischen Kurve $E(a, b, \mathbb{K})$ mit $\mathbb{K} = \mathbb{F}_q$. Dann gilt:

$$|N - (q + 1)| \leq 2\sqrt{q}.$$

**Ist es effizient möglich, die Anzahl der Punkte einer elliptischen Kurve exakt zu bestimmen? Begründen Sie Ihre Antwort!**
Ja, es ist mit dem Algorithmus von Schoof effizient möglich, die Anzahl der Punkte einer elliptischen Kurve zu bestimmen. Allerdings sind die Berechnungen trotzdem recht aufwändig.

**Beschreiben Sie das Diffie-Hellman-Verfahren auf elliptischen Kurven!**
Schlüsselerstellung

- ein großer endlicher Körper $\mathbb{K}$ mit $\mathrm{char}(\mathbb{K}) > 3$ oder $\mathrm{char}(\mathbb{K}) = 2$
- eine entsprechende elliptische Kurve $E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})$ über $\mathbb{K}$
- ein zufällig gewählter Punkt $P \in E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})$. Der Punkt $P$ sollte so gewählt sein, dass die von $P$ erzeugte Untergruppe in $E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})$ möglichst groß ist, also ungefähr so groß wie $E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})$ selbst.
- Alice wählt $a \in \mathbb{N}$ mit $1 \leq a \leq |\langle P \rangle|$.
- Bob wählt $b \in \mathbb{N}$ mit $1 \leq b \leq |\langle P \rangle|$.

Geheimer Schlüssel

- Alice: $a$.
- Bob: $b$.

Öffentlicher Schlüssel: $(\mathbb{K}, E(\mathfrak{a}, \mathfrak{b}, \mathbb{K}), P)$

Ziel: Alice und Bob möchten einen zufällig gewählten Punkt $K \in E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})$ – oder genauer $K \in \langle P \rangle$: in der von $P$ erzeugten Untergruppe von $E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})$ – als Schlüssel für ihr Kryptosystem vereinbaren.

Kommunikationen (2)

- Alice schickt $Pa$.
- Bob schickt $Pb$.

Nacharbeit

- Alice berechnet $K := (Pb)a = Pab \in \langle P \rangle \subseteq E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})$.
- Bob berechnet $K := (Pa)b = Pab \in \langle P \rangle \subseteq E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})$.

**Beschreiben Sie das Massey-Omura-Verfahren auf elliptischen Kurven!**
Schlüsselerstellung

- ein großer endlicher Körper $\mathbb{K}$ mit $\mathrm{char}(\mathbb{K}) > 3$ oder $\mathrm{char}(\mathbb{K}) = 2$
- eine entsprechende elliptische Kurve $E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})$ über $\mathbb{K}$
- $|E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})|$
- Alice
  - wählt $e_A \in \mathbb{N}$ mit $1 \leq e_A \leq |E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})|$ und $\mathrm{ggT}(e_A, |E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})|) = 1$, und
  - berechnet $d_A$ mit dem Euklidischen Algorithmus, sodass $e_A d_A \equiv 1 \pmod{|E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})|}$.
- Bob
  - wählt $e_B \in \mathbb{N}$ mit $1 \leq e_B \leq |E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})|$ und $\mathrm{ggT}(e_B, |E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})|) = 1$, und
  - berechnet $d_B$ mit dem Euklidischen Algorithmus, sodass $e_B d_B \equiv 1 \pmod{|E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})|}$.

Geheimer Schlüssel

- Alice: $(e_A, d_A)$
- Bob: $(e_B, d_B)$

Öffentlicher Schlüssel: $(\mathbb{K}, E(\mathfrak{a}, \mathfrak{b}, \mathbb{K}), |E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})|)$

Ziel: Alice möchte als Nachricht den Punkt $N \in E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})$ an Bob schicken.

Kommunikationen (3)

- Alice schickt $Ne_A$.
- Bob schickt $(Ne_A)e_B$.
- Alice schickt $(Ne_A e_B)d_A$.

Nacharbeit: Bob berechnet

$$\begin{aligned}
(Ne_A e_B d_A)d_B &= N(e_A d_A)(e_B d_B) \\
&= N(|E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})|v + 1)(e_B d_B) && v \in \mathbb{Z} \\
&= N(e_B d_B) \\
&= N(|E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})|w + 1) && w \in \mathbb{Z} \\
&= N \in E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})
\end{aligned}$$

Merke: Im Kurs wird es so beschrieben wie oben, und ich denke das ist richtig. Man könnten denken, dass das, was man eigentlich wissen müsste, nicht $|E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})|$, sondern $|\langle P \rangle| \leq E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})|$ für ein $P \in E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})$ wäre, aber wir haben hier mit keinem primitiven Element zu tun, also haben wir die Idee $\langle P \rangle$ gar nicht nötig.

**Beschreiben Sie das ElGamal-Verfahren auf elliptischen Kurven!**
Schlüsselerstellung

- ein großer endlicher Körper $\mathbb{K}$ mit $\mathrm{char}(\mathbb{K}) > 3$ oder $\mathrm{char}(\mathbb{K}) = 2$
- eine entsprechende elliptische Kurve $E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})$ über $\mathbb{K}$
- ein zufällig gewählter Punkt $P \in E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})$. Der Punkt $P$ sollte so gewählt sein, dass die von $P$ erzeugte Untergruppe in $E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})$ möglichst groß ist, also ungefähr so groß wie $E(\mathfrak{a}, \mathfrak{b}, \mathbb{K})$ selbst.
- Alice wählt $a \in \mathbb{N}$ mit $1 \leq a \leq |\langle P \rangle|$.
- Bob wählt $b \in \mathbb{N}$ mit $1 \leq b \leq |\langle P \rangle|$.

Geheimerschlüssel

- Alice: $a$
- Bob: $b$

Öffentlicher Schlüssel $(\mathbb{K}, E(\mathfrak{a}, \mathfrak{b}, \mathbb{K}), P)$

Ziel: Alice möchte die Nachricht $N \in \langle P \rangle$ an Bob schicken.

Kommunikationen (2)

- Bob schickt $Pb$.
- Alice schickt $(Pa, N + (Pb)a)$.

Nacharbeit: Bob berechnet die Nachricht $N + (Pb)a - b(Pa) = N + Pab - Pab = N \in \langle P \rangle$.

# Effiziente Algorithmen

**Was ist ein effizienter Algorithmus?**
Ein Algorithmus heißt effizient, wenn er polynomial ist.

**Wie ist die $\mathcal{O}$-Notation definiert?**
Seien $f, g : \mathbb{N}_0^r \longrightarrow \mathbb{R}$. Gibt es $B, C \in \mathbb{N}_0$, so dass für alle $(n_1, \ldots n_r) \in \mathbb{N}_0^r$ mit $n_i \geq B$ für alle $1 \leq i \leq r$ gilt:

- $f(n_1, \ldots, n_r) > 0$ und $g(n_1, \ldots n_r) > 0$, und
- $f(n_1, \ldots, n_r) < C \cdot g(n_1, \ldots, n_r)$,

dann sagen wir, dass $f$ durch $g$ beschränkt ist und schreiben $f = \mathcal{O}(g)$. (Man sagt: *$f$ ist gleich Groß-O von $g$.*)

**Welche effizienten Algorithmen kennen Sie?**

- Addition
- Subtraktion
- Multiplikation
- Division mit Rest
- wiederholtes Quadrieren
- [erweiterter] Euklidischer Algorithmus
- probabilistische Primzahltests
- probabilistiche Algorithmen für das Lösen von quadratischen Gleichungen auf elliptischen Kurven
  - Um Punkte auf einer vorgegebenen elliptischen Kurve zu finden, muss man quadratische Gleichungen über dem Grundkörper $\mathbb{K}$ lösen können.

**Welche effiziente Algorithmen kommen in RSA vor? Wo?**

- probabilistische Primzahltests: $p$ und $q$ finden
- Multiplikation: $N^e$.
- Division mit Rest: $N^e \mod pq$.
- wiederholtes Quadrieren: $N^e$.
- Euklidischer Algorithmus: $\mathrm{ggT}(e, \varphi(pq)) = 1$.
- erweiterter Euklidischer Algorithmus: $de \equiv 1 \pmod{\varphi(pq)}$.

**Welche effiziente Krypto-Verfahren kennen Sie?**

- Diffie-Hellman.
- Massey-Omura.
- ElGamal.
- RSA
- LLL-Algorithmus

# Primzahltests

**Nennen Sie Beispiele für probabilistische Primzahltests! Was ist an jedem besonders?**

- der Fermat-Test (der offensichtlichste)
- der Rabin-Miller-Test (einer der am häufigsten benutzten)
- der Solovay-Strassen-Test (einer der ersten probabilistischen Algorithmen überhaupt)

**Welchen Primzahltest gibt es sonst noch, der nicht probabilistisch ist?**
Der AKS. Er ist ein neuerer effizienter Test, der *beweist*, dass eine Zahl prim oder zusammengesetzt ist.

**Worauf basiert der AKS-Test?**
Der AKS-Test basiert auf folgendem Satz: Eine ganze Zahl $n \geq 2$ ist eine Primzahl genau dann, wenn $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$ und

$$(X + a)^n \equiv (X^n + a) \pmod{n}.$$

**Welcher Primzahltest wird in der Praxis verwendet?**
Rabin-Miller.

**Erklären Sie den Fermat-Test!**
Sei $n \in \mathbb{N}$. Wähle zufällig $b \in \mathbb{N}$ mit $0 < b < n$. Ist $\mathrm{ggT}(b, n) \neq 1$, dann ist dieser ggT ein Teiler von $n$, und $n$ ist zusammengesetzt. Ist $\mathrm{ggT}(b, n) = 1$, dann berechne $b^{n-1} \bmod n$. Gilt $b^{n-1} \bmod n \neq 1$, dann ist $n$ zusammengesetzt. Gilt $b^{n-1} \bmod n = 1$, dann ist $n$ entweder prim oder eine Carmichael-Zahl, oder $n$ ist zusammengesetzt, und die Wahrscheinlichkeit ein solches $b$ zu wählen, ist höchstens $\frac{1}{2}$.

**Bei der Verwendung des Fermat-Tests würde man mehrere Basen testen. Wie viele Basen testet man normalerweise?**
Zwischen $k = 20$ und $k = 50$. Dann ist die Wahrscheinlichkeit ein falsches Ergebnis zu bekommen (gesetzt den Fall, dass wir mit keiner Carmichael-Zahl zu tun haben) etwa $\frac{1}{2^k}$, denn die Wahrscheinlichkeit eines falschen Ergebnisses beträgt für jede Basis $\leq \frac{1}{2}$. Wenn man $k$ so wählt, ist die Irrtumswahrscheinlichkeit schon sehr klein - wohl kleiner als die Wahrscheinlichkeit, dass bei der Berechnung ein Hardwarefehler, ein Blitzeinschlag oder Ähnliches auftritt.

**In der Tat ist $3^{90} \bmod 91 = 1$, obwohl $91$ keine Primzahl ist. Wie nennt man eine solche Zahl?**
Eine [Fermatsche] Pseudoprimzahl zur Basis 3.

**Was ist eine [Fermatsche] Pseudoprimzahl?**
Sei $n \in \mathbb{N}$ eine zusammengesetzte Zahl, und sei $b \in (\mathbb{Z}/n\mathbb{Z})^\times$. Wir nennen $n$ eine [Fermatsche] Pseudoprimzahl zur Basis $b$, falls $b^{n-1} \bmod n = 1$ gilt.

**Was sind Carmichael-Zahlen und was ist so gemein an denen?**
Das sind *zusammengesetzte* Zahlen, die trotzdem den Fermat-Test für alle Basen erfüllen. Das gemeine ist, dass sonst nur Primzahlen die Eigenschaft haben, und dass es unendlich viele davon gibt.

**Wie sieht die Primfaktorisierung von Carmichael-Zahlen aus?**
Ihre Primfaktorisierung enthält mindestens 3 Primzahlen und ist quadratfrei.

**Wie viele Carmichael Zahlen gibt es denn?**
Unendlich viele, ein Resultat aus dem Jahr 1994.

**Was ist die kleinste Carmichael-Zahl?**
561.

**Kennen Sie eine andere Carmichael-Zahl?**
Die berühmte Ramanujan-Zahl (Taxi-Cab-Zahl) 1729 ist übrigens auch eine Carmichael-Zahl.

**Auf welchem Satz basiert der Fermat-Test?**
Auf dem kleinen Satz von Fermat.

**Wie lautet der kleine Satz von Fermat?**
Sei $a \in \mathbb{N}, p \in \mathbb{P}$ mit $\mathrm{ggT}(a,p) = 1$. Dann gilt $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$.

**Erklären Sie den Rabin-Miller-Test!**
Sei $n \in \mathbb{N}$ ungerade. Wähle zufällig $b \in \mathbb{N}$ mit $0 < b < n$. Ist $\mathrm{ggT}(b,n) \neq 1$, dann ist dieser ggT ein Teiler von $n$, und $n$ ist zusammengesetzt. Ist $\mathrm{ggT}(b,n) = 1$, berechne $r, s \in \mathbb{N}$, so dass $n - 1 = 2^r s$ gilt, wobei $s$ ungerade ist. Berechne die Folge

$$(x_0 = b^{2^0 s} \bmod n, x_1 = b^{2^1 s} \bmod n, \ldots, x_r = b^{2^r s} \bmod n = b^{n-1} \bmod n).$$

Gilt $(x_0, \ldots, x_r) \in \{(*, \ldots, *), (*, \ldots, *, 1, \ldots, 1), (*, \ldots, *, n-1)\}$, wobei $* \notin \{1, n-1\}$ gilt, dann ist $n$ zusammengesetzt. Gilt $(x_0, \ldots, x_r) \in \{(1, \ldots, 1), (*, \ldots, *, n-1, 1, \ldots, 1)\}$, dann ist $n$ entweder prim, oder $n$ ist zusammengesetzt, und die Wahrscheinlichkeit eine solche Zahl $b$ zu wählen, ist höchstens $\frac{1}{2}$.

**Welche Fälle können beim Rabin-Miller-Test vorkommen?**

$$
\begin{aligned}
&(*,\ldots,*)\\
&(*,\ldots,*,-1)\\
&\qquad\quad(-1)\\
&(*,\ldots,*,-1,1,\ldots,1)\\
&\qquad\quad(-1,1,\ldots,1)\\
&(*,\ldots,*,1,\ldots,1)\\
&\qquad\quad(1,\ldots,1)
\end{aligned}
$$

**Wie kann man sich merken, welche Folgen den Rabin-Miller-Test bestehen?**
Eine Zahl $n$ besteht den Test, nur wenn eine 1 am Ende steht, und neben einer 1 nur $\pm 1$ steht. Das sieht dann folgendermaßen aus:

$$
\begin{aligned}
&(*,\ldots,*) && \\
&(*,\ldots,*,-1) && \\
&\qquad\quad(-1) && \\
&(*,\ldots,*,-1,1,\ldots,1) && \checkmark\\
&\qquad\quad(-1,1,\ldots,1) && \checkmark\\
&(*,\ldots,*,1,\ldots,1) && \\
&\qquad\quad(1,\ldots,1) && \checkmark
\end{aligned}
$$

**Welche Art von Pseudoprimzahlen sind mit dem Rabin-Miller-Test assoziiert?**
Starke Pseudoprimzahlen.

**Was ist eine starke Pseudoprimzahl?**
Eine zusammengesetzte, ungerade Zahl $n$ heißt starke Pseudoprimzahl zur Basis $b \in (\mathbb{Z}/n\mathbb{Z})^\times$, falls $n-1 = 2^r s$ ist mit $s$ ungerade, und falls entweder $b^{2^0 s} \equiv 1 (\bmod n)$ gilt, oder falls es ein $i$ mit $0 \leq i < r$ gibt, so dass $b^{2^i s} \equiv -1 (\bmod n)$.

**Gibt es beim Rabin-Miller-Test äquivalente Zahlen zu den Carmichael-Zahlen?**
Nein.

**Im Grunde ist der Rabin-Miller-Test lediglich eine Verbesserung von welchem anderen Test?**
Er ist eine Verbesserung des Fermat-Tests.

**Erklären Sie den Solovay-Strassen-Test!**
Sei $n \in \mathbb{N}, n > 2$, ungerade. Wähle zufällig $b \in \mathbb{N}$ mit $0 < b < n$. Gilt $\mathrm{ggT}(b,n) \neq 1$,

dann ist dieser ggT ein Teiler von $n$, und $n$ ist zusammengesetzt. Ist $\mathrm{ggT}(b,n)=1$, dann berechne $b^{\frac{n-1}{2}} \bmod n$ und $(\frac{b}{n})$. Gilt $b^{\frac{n-1}{2}} \not\equiv (\frac{b}{n}) \bmod n$, dann ist $n$ zusammengesetzt. Gilt $b^{\frac{n-1}{2}} \equiv (\frac{b}{n}) (\bmod n)$, dann ist entweder $n$ eine Primzahl, oder $n$ ist zusammengesetzt, und die Wahrscheinlichkeit, ein solches $b$ zu wählen, ist höchstens $\frac{1}{2}$.

**Auf welcher Proposition basiert der Solovay-Strassen-Test? Von wem ist die Proposition?**
Er basiert auf folgender Proposition von Euler: Sei $a \in \mathbb{Z}$ und $p > 2$ eine Primzahl. Dann gilt:

$$(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} (\bmod p).$$

**Welche Art von Pseudoprimzahlen sind mit dem Solovay-Strassen-Test assoziiert?**
Eulersche Pseudoprimzahlen.

**Was ist eine Eulersche Pseudoprimzahl?**
Sei $n > 2$ ungerade und zusammengesetzt. Sei $b \in (\mathbb{Z}/n\mathbb{Z})^\times$. Die Zahl $n$ heißt Eulersche Pseudoprimzahl zur Basis $b$, wenn $b^{\frac{n-1}{2}} \equiv (\frac{b}{n}) (\bmod n)$ gilt.

**Was bedeutet *quadratischer Rest*?**
Sei $p > 2$ eine Primzahl. Eine Quadratzahl in $(\mathbb{Z}/p\mathbb{Z})^\times$ wird quadratischer Rest modulo $p$ genannt. Eine Zahl, die keine Quadratzahl ist, wird quadratischer Nichtrest modulo $p$ genannt.

**Wie ist das Legendre-Symbol definiert?**
Sei $a \in \mathbb{Z}$ und $p > 2$ eine Primzahl. Das Legendre-Symbol $(\frac{a}{p})$ ist definiert als

$$(\frac{a}{p}) = \begin{cases} 0, & \text{falls } p|a \text{ gilt.} \\ 1, & \text{falls } a \mod p \text{ quadratischer Rest modulo } p \text{ ist.} \\ -1, & \text{falls } a \mod p \text{ quadratischer Nichtrest modulo } p \text{ ist.} \end{cases}$$

**Wie ist das Jacobi-Symbol definiert?**
Sei $n > 2$ eine *ungerade* Zahl und sei $a \in \mathbb{Z}$. Sei $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$ die Primzahlzerlegung von $n$. Das Jacobi-Symbol $(\frac{a}{n})$ ist definiert als

$$(\frac{a}{n}) = (\frac{a}{p_1})^{\alpha_1} \dots (\frac{a}{p_r})^{\alpha_r}.$$

**Was sind 4 Eigenschaften des Jacobi-Symbols?**
Sei $n > 2$ eine ungerade Zahl, und seien $a, b \in \mathbb{Z}$.

1. Gilt $a \equiv b(\mod n)$, dann ist $(\frac{a}{n}) = (\frac{b}{n})$
2. $(\frac{ab}{n}) = (\frac{a}{n})(\frac{b}{n})$

3. $(\frac{1}{n}) = 1$

4. $(\frac{2}{n}) = (-1)^{\frac{n^2-1}{8}}$

**Was ist das quadratische Reziprozitätsgesetz?**
Seien $p$ und $q$ verschiedene, ungerade Primzahlen. Dann gilt

$$(\frac{p}{q})(\frac{q}{p}) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} 1, & \text{falls } p \mod 4 = 1 \text{ oder } q \mod 4 = 1, \\ -1, & \text{falls } p \mod 4 = 3 \text{ und } q \mod 4 = 3. \end{cases}$$

# Gruppen

**Was ist eine Verknüpfung?**
Eine Verknüpfung auf einer Menge $S$ ist eine Abbildung $f : S \times S \to S$.

**Was ist eine Gruppe?**
Eine Gruppe ist eine Menge $G$ mit einer Verknüpfung *, so dass die folgenden drei Bedingungen gelten:

- * ist assoziativ.
- Es gibt ein neutrales Element $e$ in $G$.
- Für jedes $a$ in $G$ gibt es ein inverses Element.

**Wie wird eine Gruppe genannt, wenn ihre Verknüpfung kommutativ ist?**
Abelsch.

**Was ist ein Gruppenhomomorphismus?**
Seien $(G, *), (H, \times)$ Gruppen. Eine Abbildung $\varphi : G \to H$ ist ein Gruppenhomomorphismus, wenn

$$\varphi(g_1 * g_2) = \varphi(g_1) \times \varphi(g_2) \text{ für alle } g_1, g_2 \in G \text{ gilt.}$$

**Was ist die Homomorphiesatz für Gruppen?**
Sei $\phi : G \to H$ ein Gruppenhomomorphismus. Dann ist $G/\operatorname{Kern}(\phi)$ isomorph zu $\operatorname{Bild}(\phi)$. Genauer, es ist

$$\Phi : G/\operatorname{Kern}(\phi) \to \operatorname{Bild}(\phi), \quad g\operatorname{Kern}(\phi) \mapsto \phi(g)$$

ein Isomorphismus von Gruppen.

**Wie lautet das Untergruppenkriterium für Gruppen?**
Sei $(G, \cdot)$ eine Gruppe und $\emptyset \neq H \subseteq G$. Dann gilt

$$H < G \Leftrightarrow ab^{-1} \in H \text{ für alle } a, b \in H.$$

**Was ist ein Normalteiler?**
Sei $G$ eine Gruppe und $H < G$. Wenn $aH = Ha$ für alle $a \in G$ gilt, dann wird $H$ ein Normalteiler von $G$ genannt.

**Wie notieren wir, dass $H$ eine Untergruppe von $G$ ist?**
Ist $H$ eine Untergruppe von $G$, so schreiben wir $H < G$.

**Wie notieren wir, dass $H$ ein Normalteiler von $G$ ist?**
Ist $H$ ein Normalteiler von $G$, so schreiben wir $H \triangleleft G$.

**Was ist eine Linksnebenklasse?**
Sei $(G, \cdot)$ eine Gruppe, $H < G$ und $a \in G$. Dann ist $aH = \{ah | h \in H\}$ die Linksnebenklasse von $a$ modulo $H$.

**Was bedeutet $[G : H]$?**
Sei $G$ eine Gruppe, und sei $H < G$. Die Anzahl der Linksnebenklassen modulo $H$ (der Index von $H$ in $G$) wird mit $[G : H]$ darstellt.

**Was ist der *Index* einer Untergruppe $H < G$?**
Das ist die Anzahl der Linksnebenklassen modulo $H$.

**Wie lautet der Satz von Lagrange?**
Sei $G$ eine *endliche* Gruppe, und sei $H < G$. Dann gilt

$$|G| = [G : H]|H|,$$

wobei $[G : H]$ die Anzahl der Linksnebenklassen modulo H (der Index von $H$ in $G$) darstellt.

**Nennen Sie drei Korollare zum Satz von Lagrange!**
Sei $G$ eine *endliche* Gruppe, $H < G, a \in G$, und $e$ das neutrale Element in $G$. Dann gilt:

- $|H|$ ist ein Teiler von $|G|$.
- $\mathrm{ord}(a)$ ist ein Teiler von $|G|$.
- $a^{|G|} = e$.

**Welcher Satz von Euler kann auch als Korollar zum Satz von Lagrange gesehen werden?**
Eulers Verallgemeinerung von Fermats kleinem Satz.

**Wie lautet Eulers Verallgemeinerung von Fermats kleinem Satz?**
Seien $a, n \in \mathbb{N}$ mit $\mathrm{ggT}(a, n) = 1$. Dann gilt $a^{\varphi(n)} \equiv 1 (\mathrm{mod}\ n)$.

**Wie ist die Ordnung eines Elements $a$ in einer Gruppe definiert?**
Sei $(G, \cdot)$ eine Gruppe und $a \in G$. Dann ist

$$\langle a \rangle = \{a^i | i \in Z\}$$

die von $a$ erzeugte Untergruppe in $G$. Ist $\langle a \rangle$ endlich, dann ist die Ordnung von $a$ definiert als $\mathrm{ord}(a) = |\langle a \rangle|$. Ist $\langle a \rangle$ unendlich, dann ist die Ordnung von $a$ definiert als $\mathrm{ord}(a) = \infty$.

**Was ist eine Faktorgruppe?**
Sei $G$ eine Gruppe, $N \triangleleft G$. Dann ist $G/N = \{aN | a \in G\}$ die Faktorgruppe oder Quotientengruppe von $G$ nach $N$.

# Ringe

**Was ist ein Ring?**
Ein Ring $(R, +, \cdot)$ ist eine Menge $R$ mit zwei Verknüpfungen $+$ und $\cdot$, so dass folgende Bedingungen erfüllt sind:

(i) $(R, +)$ ist eine abelsche Gruppe.

(ii) $\cdot$ ist assoziativ, und es gibt ein neutrales Element der Multiplikation $e \in R$.

(iii) Es gelten die Distributivgesetze.

**Wie heißt ein Ring, wobei $\cdot$ auch kommutativ ist?**
Wenn $\cdot$ auch kommutativ ist, so wird $R$ ein kommutativer Ring genannt.

**Wird ein *Ring* überall gleich definiert?**
Es gibt in der Tat konkurrierende Definitionen von Ringen. Oft wird die Bedingung (ii) dahingehend abgeschwächt, dass die Existenz eines neutralen Elementes der Multiplikation nicht gefordert wird.

**Was ist ein Ideal?**
Sei $(R, +, \cdot)$ ein Ring. Ein Ideal $I$ in $R$ ist eine Untergruppe von $(R, +)$, so dass für alle $a \in I$ und alle $b \in R$ die Elemente $ab$ und $ba$ in $I$ liegen.

**Wie notieren wir, dass $I$ ein Ideal von $R$ ist?**
Ist $I$ ein Ideal in $R$, so schreiben wir $I \triangleleft R$.

**Was ist ein Hauptideal?**
Ein Ideal $I$ in einem Ring $R$ heißt Hauptideal, wenn es ein $a \in I$ gibt, so dass $I = (a) = \{ar | r \in R\}$ ist.

**Was ist ein Hauptidealring?**
Ein Ring $R$ heißt Hauptidealring, wenn $R$ ein *Integritätsbereich* ist, und wenn alle Ideale in $R$ Hauptideale sind.

**Was ist ein Primideal?**
Sei $R$ ein kommutativer Ring. Ein Ideal $P \neq R$ in R heißt Primideal, wenn für alle $a, b \in R$ mit $ab \in P$ folgt, dass $a$ oder $b$ in $P$ liegen.

**Was ist ein maximales Ideal?**
Sei $R$ ein kommutativer Ring. Ein Ideal $M \neq R$ in $R$ heißt maximales Ideal, wenn für jedes Ideal $I$ mit $M \subseteq I \subseteq R$ folgt, dass $M = I$ oder $I = R$ ist.

**Was ist ein Primring?**
Sei $R$ ein Ring, und sei $e$ das neutrale Element der Multiplikation in $R$. Der Unterring

$\mathbb{Z}e$ von $R$ wird der Primring von $R$ genannt.

**Wie wird der Primring von einem Ring $R$ bezeichnet?**
$P(R)$.

**Wie ist die Charakteristik?**
Sei $R$ ein Ring mit Primring $P(R)$.

1. Wenn $P(R) \simeq \mathbb{Z}$ ist, dann sagen wir, dass $R$ die Charakteristik 0 hat und schreiben $\mathrm{char}(R) = 0$.

2. Wenn $P(R) \simeq \mathbb{Z}/m\mathbb{Z}$ für ein $m > 1$ ist, dann sagen wir, dass $R$ die Charakteristik $m$ hat, beziehungsweise, dass $R$ **positiv** Charakteristik hat, und schreiben $\mathrm{char}(R) = m$.

Für den Ring $R = \{0\}$ ist keine Charakteristik definiert.

**Welcher Satz gibt Antwort auf die Frage, wie gewisse Kongruenzen simultan gelöst werden können?**
Der Chinesische Restsatz.

**Was ist die Aussage des Chinesischen Restsatzes?**
Dass $\mathbb{Z}/n\mathbb{Z}$ und $\prod_{i=1}^{r} \mathbb{Z}/p_i^{s_i}\mathbb{Z}$ als Ringe isomorph sind.

**Wieso hat der Chinesische Restsatz so wichtige Folgerungen in der Computeralgebra?**
Wenn wir mit dem Rechner $x + y$ oder $xy$ mit $x, y \in \mathbb{Z}$ berechnen wollen, dann ist es völlig egal, ob wir diese Rechnung in $\mathbb{Z}$ durchführen oder in $\mathbb{Z}/n\mathbb{Z}$, so lange das Ergebnis kleiner als $n$ ist. Wenn $x$ und $y$, und damit $n$ nun riesig groß sind, so kann es Zeit und Speicher sparender sein, die Rechnung auszulagern und viele kleinere Rechnungen zu machen. Mit anderen Worten, wir können ein großes $n$, dessen Primfaktorzerlegung $n = \prod_{i=1}^{r} p_i^{s_i}$ wir kennen, wählen, und an Stelle von $x + y$ oder $xy$ berechnen wir einfach $((x+y) \mod p_1^{s_1}, \ldots, (x+y) \mod p_r^{s_r})$ beziehungsweise $(xy \mod p_1^{s_1}, \ldots, xy \mod p_r^{s_r})$. Die einzelnen Einträge können sogar parallel berechnet werden. Der Chinesische Restsatz garantiert, dass wir das Ergebnis mit der im Satz angegebenen Formel wieder zusammensetzen können und das Ergebnis in $\mathbb{Z}/n\mathbb{Z}$ erhalten.

**Was ist ein Ringhomomorphismus?**
Seien $R$ und $R'$ Ringe. Eine Abbildung $\phi : R \to R'$ heißt ein Ringhomomorphismus, wenn für alle $r_1, r_2 \in R$ gilt:

1. $\phi(r_1 + r_2) = \phi(r_1) + \phi(r_2)$

2. $\phi(r_1 r_2) = \phi(r_1)\phi(r_2)$

3. $\phi(1) = 1$.

**Was ist die Homomorphiesatz für Ringe?**
Sei $\phi : R \to R'$ ein Ringhomomorphismus. Dann ist $R/\operatorname{Kern}(\phi)$ isomorph zu $\operatorname{Bild}(\phi)$. Genauer, es ist

$$\Phi : R/\operatorname{Kern}(\phi) \to \operatorname{Bild}(\phi), \quad [r] \mapsto \phi(r)$$

ein Isomorphismus von Ringen.

**Was ist ein Restklassenring?**
Sei $R$ ein Ring, $I \triangleleft R$. Der Ring

$$R/I = \{[r] | r \in R\} = \{r + I | r \in R\}$$

mit $[r][s] = [rs]$ und $[r] + [s] = [r + s]$ für alle $r, s \in R$ wird Restklassenring von $R$ modulo $I$ genannt.

# Das Teilmengen-Summen-Problem

**Wir haben ein Kryptosystem kennengelernt, das sich dann als Flop herausgestellt hat. Wie heißt das?**
Das Knapsack-Kryptosystem.

**Worauf basiert das Knapsack-Kryptosystem?**
Auf dem Teilmengen-Summen-Problem.

**Was ist das Teilmengen-Summen-Problem?**
Seien $a_1, \ldots, a_n, s \in \mathbb{N}$ gegeben. Gibt es $x_1, \ldots, x_n \in \{0, 1\}$ mit

$$\sum_{i=0}^{n} a_i x_i = s?$$

**Wie schwer ist es, ein Teilmengen-Summen-Problem zu lösen?**
Es ist bekannt, dass das Problem NP-hart ist. Allerdings ist ein Teilmengen-Summen-Problem mit superaufsteigender Zahlenfolge leicht zu lösen.

**Was bedeutet es, dass ein Problem NP-hart ist?**
Das bedeutet, dass es vermutlich keine effizienten Algorithmen zur Lösung gibt – und wenn es einen gibt, dann auch für viele andere, sehr schwere Probleme.

**Was ist eine *superaufsteigende* Zahlenfolge?**
Wir nennen eine Folge von natürlichen Zahlen superaufsteigend, wenn jedes Element größer ist, als die Summe der vorhergehenden Elemente.

**Ist eine Lösung des Teilmengen-Summen-Problems eindeutig?**
Wenn es eine Lösung eines Teilmengen-Summen-Problems gibt, so ist diese Lösung in der Regel *nicht* eindeutig. Andererseits ist ein Teilmengen-Summen-Problem mit *superaufsteigender* Zahlenfolge immer eindeutig bestimmt.

**Was haben superaufsteigende Folgen mit dem Knapsack-Verfahren zu tun?**
Die Idee der Knapsack-Verschlüsselung besteht darin, eine superaufsteigende Folge (den geheimen Schlüssel) als eine gewöhnliche Folge (den öffentlichen Schlüssel) zu verschleiern.

**Worin liegt die vermeintliche Sicherheit des Knapsack-Kryptosystems begründet?**
Darin, dass Oscar mit einem Teilmengen-Summen-Problem konfrontiert ist, das auf einer Zahlenfolge basiert, die nicht superaufsteigend ist. Auf den ersten Blick sieht es also so aus, als müsse er ein Problem in der Klasse $NP$ knacken. Es geht aber anders: mit dem $LLL - Algorithmus$.

**Was ist der LLL-Algorithmus?**
Vereinfacht gesagt ist der LLL-Algorithmus der Versuch, das Gram-Schmidt Orthogonalisierungsverfahren für ganzzahlige Linearkombinationen von Vektoren zu kopieren. Er ist ein effizienter Algorithmus, der zwar nicht immer einen kürzesten Vektor in Gittern, aber immerhin einen *relativ kurzen* Vektor in Gittern mit Basen in $\mathbb{Q}^n$ berechnet.

**Was liefert letztendlich der LLL-Algorithmus?**
Eine reduzierte Basis eines Gitters.

**Was ist ein Gitter?**
Sei $(a_1, \ldots, a_n)$ eine Basis von $\mathbb{R}^n$. Die Menge

$$L(a_1, \ldots, a_n) = \left\{ \sum_{i=1}^{n} \lambda_i a_i | \lambda_i \in \mathbb{Z} \right\}$$

aller ganzzahligen Linearkombinationen der Vektoren $a_1, \ldots, a_n$ wird ein Gitter mit Basis $(a_1, \ldots, a_n)$ genannt.

**Wie ist die Determinante eines Gitters definiert?**
Sei $L = L(a_1, \ldots, a_n)$ ein Gitter in $\mathbb{R}^n$. Die Determinante $\det L$ von $L$ ist definiert als $\det L = |\det(a_1| \cdots |a_n)|$.

**Was ist ein schwieriges Problem in Verbindung mit einem Gitter $L$?**
Ein schwieriges Problem, von dem man erst seit wenigen Jahren weiß, dass es NP-hart ist, ist, einen Algorithmus anzugeben, der einen kürzesten Vektor $\neq 0$ in $L$ findet. Diese Tatsache macht Gitter für kryptografische Zwecke hochinteressant. Kryptosysteme, deren Sicherheit darauf beruht, dass kürzeste Vektoren in Gittern gefunden werden müssen, scheinen gegen Angriffe resistent zu sein.

**Erklären Sie das Knapsack-Kryptosystem!**
Schlüsselerstellung

- ein superaufsteigendes $n-$Tupel natürlicher Zahlen $(a_1, \ldots, a_n)$
- eine natürliche Zahl $m > \sum_{i=1}^{n} a_i$ als Modul
- eine zu $m$ teilerfremde Zahl $a$
- $b \in \mathbb{Z}/m\mathbb{Z}$ mit $ab \equiv 1 \pmod{m}$
- $(w_1, \ldots w_n) = (aa_1 \mod m, \ldots, aa_n \mod m)$ - Diese Folge ist in der Regel nicht mehr superaufsteigend - sonst müssen neue Parameter gewählt werden.)

Geheimschlüssel: $((a_1, \ldots, a_n), m, a, b)$
Öffentlicher Schlüssel: $(w_1, \ldots w_n)$

Ziel: Alice möchte ein $n$-Bit Zahl $(x_1, \ldots, x_n)$ an Bob schicken. Für alle $1 \leq i \leq n$ gilt also $x_i \in \{0, 1\}$.

Kommunikationen (1)

- Alice schickt Bob $s = \sum_{i=1}^{n} x_i w_i$.

Nacharbeit: Bob bildet in $\mathbb{Z}/m\mathbb{Z}$

$$bs = b \sum_{i=1}^{n} x_i w_i = b \sum_{i=1}^{n} x_i a a_i = \sum_{i=1}^{n} x_i b a a_i = \sum_{i=1}^{n} x_i a_i.$$

Er ist jetzt gefordert, ein Teilmengen-Summen-Problem mit superaufsteigender Folge zu berechnen. Dies kann er leicht lösen.

# Das Knacken des Knapsacks

**Muss ein Teilmengen-Summen-Problem gelöst werden, um das Knapsack-Kryptosystem zu knacken?**
Um das Knapsack-Kryptosystem zu knacken, muss *kein* Teilmengen-Summen-Problem gelöst werden, wie Adi Shamir 1984 feststellte.

**Wie wird das Knapsack-Kryptosystem geknackt?**
Stellen wir uns vor, wir sind Oscar, und suchen $x_1, \ldots, x_n \in \{0, 1\}$, für die die Gleichung

$$s = \sum_{i=1}^{n} w_i x_i \text{ mit } w_i \in \mathbb{N} \text{ für alle } 1 \leq i \leq n$$

erfüllt ist. Dabei ist $(w_1, \ldots, w_n)$ der öffentliche Schlüssel des Knapsack-Kryptosystems. Wir können annehmen, dass die $w_i$ sehr große Zahlen sind, denn wären die $w_i$ klein, dann könnte man das Kryptosystem auch durch Ausprobieren brechen. Wir bilden das Gitter $L(b_1, \ldots, b_{n+1})$, dessen Basis $b_1, \ldots, b_{n+1}$ die Spalten der folgenden Matrix sind:

$$\begin{pmatrix} 1 & 0 & \cdots & 0 & 0 \\ 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & \ddots & 0 & 0 \\ 0 & 0 & \cdots & 1 & 0 \\ -w_1 & -w_2 & \cdots & -w_n & s \end{pmatrix}.$$

Angenommen, wir haben $x_1, \ldots, x_n \in \{0, 1\}$ gefunden, für die $\sum_{i=1}^{n} w_i x_i + s = 0$ gilt. Dann ist

$$\sum_{i=1}^{n} x_i b_i + b_{n+1} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \\ 0 \end{pmatrix}$$

ein Vektor in $L(b_1, \ldots, b_{n+1})$, der sehr kurz ist, denn seine Länge ist maximal $\sqrt{n}$. *Um das Knapsack-Kryptosystem zu brechen, berechnen wir mit dem LLL-Algorithmus eine reduzierte Basis von $L(b_1, \ldots, b_{n+1})$ und hoffen, dass der erste Vektor der reduzierten Basis der Vektor* $\begin{pmatrix} x_1 \\ \vdots \\ x_n \\ 0 \end{pmatrix}$, *ist.* Und das ist so oft der Fall, dass das Knapsack-Kryptosystem als nicht sicher verworfen wurde.

**Was ist die für das Knacken von Knapsack entscheidende Eigenschaft von dem LLL-Algorithmus?**
Der kurze 1. Vektor der reduzierten Basis, der häufig die Lösung des Knapsack-Problems liefert.