Untersuchung der Gruppen $GL(s, Z_n)$ und $SL(s, Z_n)$ zur Nutzung in der Kryptographie

Inaugural-Dissertation
zur Erlangung des Grades eines
Doktors der Naturwissenschaftlichen Fachbereiche
(Fachbereich Mathematik)
der Justus-Liebig-Universität Gießen

vorgelegt von
Matthias Baumgart
aus Herborn/Hessen

Gießen, 2004

Inhaltsverzeichnis

Kapitel 1

Vorwort

Schon vor Jahrtausenden haben die Menschen versucht, Nachrichten so zu verfassen oder zu verändern, dass sie nur einem bestimmten Teilnehmerkreis zugänglich waren. Das erste überlieferte kryptographische Verfahren stammt von den Spartanern aus dem 5. Jh. v. Chr. Mittels der sogenannten Skytale konnten sie geheime Botschaften durch Transposition der Buchstaben verschlsseln. Die so verschüsselten Nachrichten wurden an die Staatsbeamten und Feldherrn im Ausland versandt. Zuvor hatten schon die Ägypter Geheimschriften verwendet. Diese dienten jedoch nicht dem Zweck, die Botschaft der Nachricht zu verschleiern, sondern sollten zum Verweilen an den Orten anregen, an denen sie angebracht wurden. In den spteren Jahrhunderten war insbesondere im militärischen Bereich die Verwendung von Kryptographie zur Verschlüsselung von Nachrichten von großer Bedeutung. Bis Mitte des 20. Jahrhunderts wurden dabei ausschließlich kryptographische Verfahren verwendet, die man heute der *klassischen Kryptographie* zuordnet. Dabei besitzen jeweils der Sender und der Empfänger der Nachricht den gleichen Schlüssel. Mit Hilfe dieses Schlüssels wandelt der Sender die Nachricht in einen Geheimtext um. Mit Hilfe des gleichen Schlüssels kann der Empfänger die Nachricht wieder aus dem Geheimtext rekonstruieren. Ein Nachteil der klassischen Kryptographie ist, dass Sender und Empfänger zunächst über einen sicheren Kanal den gemeinsamen Schlüssel austauschen müssen, bevor sie verschlüsselt kommunizieren können.

Die *asymmetrische Kryptographie* entstand aus der Frage, ob Sender und Empfänger immer den gleichen Schlüssel benötigen, und führte W. Diffie und M. Hellmann 1976 zu dem

Konzept der asymmetrischen Verschlüsselung (DH76). Dabei besitzt der Empfänger der Nachricht einen privaten Schlüssel und einen sogenannten öffentlichen Schlüssel, wobei nur der private Schlüssel geheimzuhalten ist. Der öffentliche Schlüssel hingegen wird möglichst vielen Personen zugänglich gemacht. Eine Nachricht an den Empfänger wird dann mit Hilfe des öffentlichen Schlüssels in den Geheimtext umgewandelt, den dann der Empfänger der Nachricht mit seinem privaten Schlüssel wieder entschlüsseln kann.

Das RSA-Verfahren gilt als das erste asymmetrische Verschlüsselungsverfahren. Es wurde 1979 von L.R. Rivest, A. Shamir und L. Adleman (RSA79) veröffentlicht. Das von den Autoren vorgestellte Verfahren basiert auf Operationen in der Gruppe Z_n^*, wobei n das Produkt zweier großer Primfaktoren p und q ist. Schon bald nach der Veröffentlichung wurde versucht, das Verfahren auf andere Gruppen zu übertragen. Bis heute jedoch wird das RSA-Verfahren in der Praxis fast ausschließlich in der Gruppe Z_n^* genutzt, da der Transfer auf andere Gruppen meist mit einer Verschlechterung der Effizienz einhergeht.

Einige Veröffentlichungen erweitern das RSA-Verfahren, indem sie es auf Matrizen aus der Gruppe $GL(s, Z_n)$ anwenden. Dazu gehören (VO85), (CD90) und (Fa96). Diese Verfahren verwenden jedoch zum Teil nur spezielle Matrizen aus $GL(s, Z_n)$ und operieren nicht auf der ganzen Gruppe $GL(s, Z_n)$. So werden zum Beispiel in (CD90) nur Dreiecksmatrizen verwendet und es wird aufgezeigt, dass dann die Sicherheit des Verfahrens äquivalent zu der Sicherheit des Verfahrens in Z_n^* ist. Der Grund für dieses Vorgehen liegt darin, dass es in $GL(s, Z_n)$ Matrizen gibt, für die das RSA-Verfahren leicht zu brechen ist. Es existieren zum Beispiel Matrizen, die die Ordnung n besitzen. Für diese Matrizen ist das Ziehen einer diskreten d-ten Wurzel leicht möglich. Eine umfassende Untersuchung der Gruppe $GL(s, Z_n)$ in Bezug auf die Sicherheit des RSA-Verfahrens erfolgt in keiner der Veröffentlichungen. Diese Aufgabe stellt sich desshalb die vorliegende Arbeit.

Da die Sicherheit des RSA-Verfahrens eng mit der Schwierigkeit des diskreten Logarithmusproblems in der jeweiligen Gruppe zusammenhängt, wird in dieser Arbeit auch das diskrete Logarithmusproblem in den Gruppen $GL(s, Z_p)\backslash SL(s, Z_p)$ und $SL(s, Z_p)$ betrachtet. Dazu erfolgt eine Klassifikation der Matrizen aus den Gruppen $GL(s, Z_p)\backslash SL(s, Z_p)$ und $SL(s, Z_p)$, so dass differenzierte Aussagen über die Schwierigkeit des diskreten Logarithmusproblems in den einzelnen Klassen getroffen werden können.

Darüber hinaus erfolgt eine Klassifikation der Matrizen der Gruppe $GL(s, Z_n)$, so

dass die Sicherheit des RSA-Verfahrens in den einzelnen Klassen differenziert beschreibbar wird. Da leicht gezeigt werden kann, dass das RSA-Verfahren, das auf Matrizen aus $GL(s, Z_n)\backslash SL(s, Z_n)$ basiert, immer mindestens so sicher ist wie das RSA-Verfahren in Z_n^*, erfolgt die Klassifikation für $SL(s, Z_n)$ und $GL(s, Z_n)\backslash SL(s, Z_n)$ getrennt. Es wird gezeigt werden, dass es Matrizen in $SL(s, Z_n)$ gibt, für die kein direkter Zusammenhang zwischen der Sicherheit des RSA-Verfahrens auf diesen Matrizen und der Sicherheit des Verfahrens in Z_n^* aufgezeigt werden kann. Mit anderen Worten: Wird das RSA-Verfahren basierend auf Z_n^* gebrochen, so geht damit nicht unbedingt zugleich ein Bruch des RSA-Verfahrens für diese Matrizen einher.

Durch die Untersuchung der Matrizeneigenschaften bestimmter Klassen konnten zwei neue Faktorisierungsverfahren entworfen werden. Die eine Faktorisierungsmethode zeigt auf, wie n mit Hilfe der Kenntnis zweier wesentlich verschiedener d-ter Wurzelmatrizen einer Matrix A faktorisiert werden kann. Eines der Hauptergebnisse dieser Arbeit ist die zweite Faktorisierungsmethode, die eine effiziente Faktorisierung von n mittels Matrizen aus $GL(s, Z_n)$ ermöglicht, wenn für genau eine der beiden Primzahlen p, q (oBdA p) gilt, dass $\sum_{i=0}^{s} p^i$ nur kleine Primfaktoren besitzt. Dies stellt eine Erweiterung der bisherigen Faktorisierungsmethoden dar, die ausnutzen, dass $p-1$ bzw. $p+1$ nur durch kleine Primzahlen geteilt werden. Eine Primzahl, die die Eigenschaft besitzt, dass p^2+p+1 nur durch kleine Primzahlen geteilt wird, ist z.B. 1451. In diesem Fall ist $1451^2+1451+1 = 7 \cdot 7 \cdot 19 \cdot 31 \cdot 73$. Eine Zusammengesetzte Zahl, die 1451 als Primteiler besitzt, könnte also mit dem neuen Verfahren faktorisiert werden. Im Anhang wird eine Zusammengesetzte Zahl, deren Binäre Darstellungslänge 80 Bit betägt angegeben, die mit neuen Verfahren effizient faktorisiert werden kann.

Die Arbeit gliedert sich wie folgt: Zunächst werden in Kapitel 2 das originale RSA-Verfahren sowie bekannte Angriffe und geeignete Gegenmaßnahmen vorgestellt. Dann werden die beiden Erweiterungen von (VO85) und (CD90) des RSA-Verfahrens auf Matrizen beschrieben. In Abschnitt 4 erfolgt dann zunächst eine Untersuchung des diskreten Logarithmusproblems und des RSA-Problems in den Gruppen $GL(2, Z_p)\backslash SL(2, Z_p)$ und $SL(2, Z_p)$ bzw. $GL(2, Z_n)\backslash SL(2, Z_n)$ und $SL(2, Z_n)$. Dies beinhaltet eine Klassifikation der Matrizen aus $GL(2, Z_p)\backslash SL(2, Z_p)$ und $SL(2, Z_p)$ bzw. $GL(2, Z_n)\backslash SL(2, Z_n)$ und $SL(2, Z_n)$. Diese Betrachtung wird dann in Abschnitt 5 auf die Gruppen $GL(s, Z_p)\backslash SL(s, Z_p)$

und $SL(s, Z_p)$ bzw. $GL(s, Z_n) \backslash SL(s, Z_n)$ und $SL(s, Z_n)$ erweitert. Abschnitt 5.7 beschreibt neue Faktorisierungsmethoden, die sich vor diesem Hintergrund ableiten lassen. In Abschnitt 5.8 erfolgt eine Zusammenfassung der Ergebnisse in Bezug auf die Sicherheit des RSA-Verfahrens in $GL(s, Z_n)$.

Im Anhang findet sich eine Auflistung der in dieser Arbeit verwendeten Notationen. Zum besseren Verständnis der Arbeit sollte der Leser über Grundkenntnisse in den Gebieten Algebra, lineare Algebra und Kryptographie verfügen.

Ich danke allen, die mich bei der Entstehung dieser Arbeit unterstützt haben. Insbesondere möchte ich mich bedanken bei Herrn Prof. Dr. Beutelspacher für die Vergabe des Themas und die Unterstützung bei dessen Bearbeitung. Herrn Prof Dr. Baumann danke ich für bereichernde Fachdisskussionen und Hinweise auf einschlägige Literatur. Besonders bedanken möchte ich mich ebenfalls bei allen, die diese Arbeit Korrektur gelesen haben und hilfreiche Anregungen geben konnten. Ein ganz besonderer Dank geht an meine Frau Stephanie Wodianka, die mich stets unterstützt und für ausreichenden Freiraum zur Erstellung dieser Arbeit gesorgt hat.

Kapitel 2

Grundlagen

2.1 Das RSA-Verfahren

1979 wurde von Rivest, Shamir und Adleman (RSA79) das sogenannte RSA-Verfahren entwickelt. Dabei handelt es sich um das erste veröffentlichte Public-Key-Verfahren. Im Folgenden wird dieses Verfahren kurz beschrieben, und heute bekannte Angriffe auf das Verfahren vorgestellt.

Das RSA-Verfahren kann sowohl zum Verschlüsseln von Nachrichten als auch zum Signieren von Nachrichten verwendet werden. Es besteht bei Verschlüsselung, als auch bei der Signaturerstellung jeweils aus drei Grundprotokollen: der Schlüsselgenerierung, der Verschlüsselung bzw. der Signaturerstellung und der Entschlüsselung bzw. der Signaturverifikation.

2.1.1 Die Schlüsselgenerierung

Die Schlüsselgenerierung ist bei dem RSA-Verschlüsselungsverfahren und dem RSA-Signaturerstellungsverfahren identisch. Dazu werden zwei ausreichend große (zur Zeit der Entstehung dieser Arbeit mindestens in einer Größe von 512 Bit) Primzahlen p und q zufällig gewählt und miteinander multipliziert. Das Ergebnis wird mit $n = pq$ bezeichnet.

Dann wird eine beliebige Zahl e gewählt, so dass $ggT(e, \varphi(n)) = 1$ gilt. Dabei wird häufig ein Wert für e verwendet, dessen Binärdarstellung wenige Eins-Einträge besitzt (wie z.B. $2^{16} + 1$), um eine effiziente Potenzierung zu ermöglichen. Das Zahlenpaar (e, n)

wird als öffentlicher Schlüssel bzw. auch als public key bezeichnet. Dieses Zahlenpaar wird veröffentlicht und dient zur Verschlüsselung bzw. zur Signaturverifikation.

Der geheime Schlüssel zur Entschlüsselung bzw. Signaturerstellung wird wie folgt berechnet: Mit Hilfe des erweiterten euklidischen Algorithmus bestimmt man ganze Zahlen d, v, so dass gilt: $ed + \varphi(n)v = 1$. Das Zahlenpaar (d, n) wird als geheimer Schlüssel bzw. auch als *private key* bezeichnet. Dieser Schlüssel ist nur dem Signaturersteller bzw. dem Empfänger einer verschlüsselten Nachricht bekannt und darf an keine andere Person weitergegeben werden.

2.1.2 Verschlüsselung und Signaturerstellung

Verschlüsselung:

Um eine Nachricht zu verschlüsseln, wird diese als eine Zahl $m \in Z_n^*$ dargestellt. Diese Nachricht wird vom Sender der Nachricht verschlüsselt, indem er $c := m^e \bmod n$ berechnet. c wird als der zu der Nachricht m gehörige Chiffretext bezeichnet.

Signaturerstellung:

Um eine Nachricht zu signieren, wird diese als eine Zahl $m \in Z_n^*$ dargestellt. Eine Nachricht m wird von dem Signierer signiert, indem der $Sig(m) := m^d \bmod n$ berechnet. Die Signatur $Sig(m)$ wird dann zusammen mit der Nachricht m versendet.

2.1.3 Entschlüsselung und Signaturverifikation

Entschlüsselung:

Der Empfänger der Nachricht erhält den Chiffretext c. Dieser Chiffretext kann von dem Inhaber des geheimen Schlüssels entschlüsselt werden, indem er $c^d \equiv_n m^{ed} \equiv_n m$ berechnet.

Signaturverifikation:

Der Empfänger der Nachricht erhält die Nachricht m zusammen mit der Signatur $Sig(m)$. Die Signatur der Nachricht kann mit Hilfe des öffentlichen Schlüssels (e, n) und der Nachricht m überprüft werden. Dazu berechnet man $m' := Sig(m)^e \bmod n$ und überprüft, ob $m = m'$ gilt.

2.2 Homomorphie-Eigenschaft des RSA-Verfahrens

Eine wesentliche Eigenschaft des RSA-Verfahrens aus (RSA79) ist, dass es bzgl. der Klartexte und Chriffretexte eine Homomorphie-Eigenschaft besitzt. Mit anderen Worten: Die multiplikative Verknüpfung zweier Klartexte resultiert in einer multiplikativen Verknüpfung der Chiffretexte:

$$\begin{aligned} c_1 &\equiv_n m_1^e \\ c_2 &\equiv_n m_2^e \\ \Rightarrow (m_1 * m_2)^e &\equiv_n m_1^e * m_2^e \equiv_n c_1 * c_2 \end{aligned}$$

Diese Eigenschaft wird von einigen kryptographischen Protokollen ausgenutzt, um unterschiedliche Chiffretexte miteinander zu verknüpfen. Es führt jedoch auch zu einer weiteren Möglichkeit, RSA-verschlüsselte bzw. RSA-signierte Nachrichten zu attackieren (siehe Abschnitt 2.3.8).

2.3 Sicherheit des RSA-Verfahrens

In diesem Abschnitt wird die Sicherheit des RSA-Verfahrens betrachtet. Dazu werden die bis zum Zeitpunkt der Erstellung dieser Arbeit bekannten Angriffe auf das RSA-Verfahren erläutert. Es werden nur Angriffe behandelt, die sich direkt auf den Algorithmus beziehen. Angriffe, die auf einer besonderen Implementation des RSA-Verfahrens basieren oder Angriffe, welche Hardwareeigenschaften ausnutzen, um den RSA zu brechen, werden in dieser Arbeit nicht betrachtet.

Die Erfolgswahrscheinlichkeit dieser Angriffe ist von den gewählten Parametern des Verfahrens abhängig, wie z.B. der Wahl der zugrundeliegenden Gruppe. Die aus den Angriffen resultierenden Anforderungen an die Gruppe bzw. an die Parameter des Verfahrens werden in Abschnitt 2.4 behandelt. Einige der Angriffe werden auch durch eine Abwandlung des RSA-Verfahrens verhindert. Eine dieser RSA-Varianten wird im Abschnitt 2.5 vorgestellt.

2.3.1 Eine Brute-Force-Attacke

Ein Angriff mittels Brute Force versucht, den geheimen Schlüssel durch Ausprobieren aller möglichen Schlüssel zu ermitteln. Brute-Force Angriffe werden häufig eingesetzt, um symmetrische Verschlüsselungsverfahren zu brechen, die eine zu kleine Schlüssellänge besitzen. Als Beispiel für eine solchen Angriff ist der erfolgreiche Angriff auf den Data Encryption Standard (FIPS64-2) zu nennen (vgl. http://www.distributed.net/des/). Im Januar 1999 wurde ein 56 Bit DES Schlüssel mit Hilfe von Computern im Internet innerhalb von 22 Stunden und 15 Minuten ermittelt. Dies ist einer der Gründe, warum an einem geeigneten Nachfolger für DES gearbeitet wurde, der 2002 als AES eingeführt worden ist. Der DES besitzt eine effektive Schlüssellänge von 56 Bit und wurde seit 1976 erfolgreich als Verschlüsselungsstandard in verschiedenen Bereichen eingesetzt. Neuere symmetrische Verschlüsselungsverfahren verwenden meist eine Schlüssellänge von 128 Bit, die nach heutigem Kenntnisstand als ausreichend sicher gegen Brute-Force Angriffe anzusehen ist.

Ein Brute-Force Angriff auf asymmetrische Verschlüsselungsverfahren ist genauso denkbar wie im symmetrischen Fall. Im Falle des oben beschriebenen RSA-Verfahrens würde das bedeuten, dass man versucht, den geheimen Schlüssel d durch Testen aller möglichen Werte zu ermitteln. Der Bitlänge von d entspricht der binären Darstellungslänge von $\varphi(n)$. Diese liegt in der gleichen Größenordnung wie die binäre Darstellungslänge von n. Die Bitlänge von n muss jedoch zum Schutz vor anderen Angriffen so groß gewählt werden, dass ein Brute-Force Angriff keine Erfolgsaussichten mehr hat.

2.3.2 Direkte Berechnung der diskreten Wurzel

Ein Angreifer, der eine RSA-verschlüsselte Nachricht abfängt, erhält $c := m^e \bmod n$. Der öffentliche Schlüssel (e, n) ist jedem, und somit auch dem Angreifer bekannt. Um den Wert m zu ermitteln, müsste er also die e-te Wurzel aus c modulo n berechnen. Dies ist möglich, wenn er die Ordnung von c oder ein zu e teilerfremdes, kleines Vielfaches der Ordnung bestimmen kann.

Ist die Ordnung $ord(c)$ von c gegeben, so berechnet er mit Hilfe des erweiterten euklidischen Algorithmus einen Wert d', für den gilt: $ed' \equiv_{ord(c)} 1$. Mit Hilfe dieses Wertes d', der nicht gleich dem Wert d sein muss, kann er dann den Chiffretext entschlüsseln, denn

es gilt: $c^{d'} \equiv_n m^{ed'} = m \bmod n$.

Die Berechnung von diskreten Wurzeln ist also immer dann leicht, wenn man die Ordnung des Elementes, aus dem die Wurzel gezogen werden soll, oder ein Vielfaches dieser Ordnung kennt. Kennt man also die Gruppenordnung der zugrundeliegenden Gruppe, so ist das RSA-Problem lösbar. Im Abschnitt 2.3.4 wird gezeigt, dass die Ermittlung der Gruppenordnung von Z_n^* äquivalent zur Faktorisierung von n ist.

2.3.3 Faktorisierung von n

Im Folgenden sei n immer das Produkt zweier Primzahlen p und q. Die Sicherheit des RSA-Verfahrens hängt eng mit dem Problem der Faktorisierung des Modul n zusammen. Ein Angreifer, der n faktorisieren kann, kann mit Hilfe der Faktoren $\varphi(n)$ und somit die Gruppenordnung von Z_n^* berechnen. Kennt man die Gruppenordnung von Z_n^*, so ist die Berechnung des geheimen Schlüssels und das Ziehen diskreter Wurzeln modulo n mit polynomiellem Zeit- und Speicheraufwand möglich (Siehe Abschnitt 2.3.2).

Es gibt eine große Anzahl verschiedener Faktorisierungsalgorithmen, so dass hier nicht näher auf alle eingegangen werden kann. Der derzeit effizienteste Algorithmus zum Faktorisieren großer allgemeiner Zahlen ist der sogenannte Number Field Sieve (LL93). Er hat eine erwartete Laufzeit von $O(e^{(ln(n)^{1/3}(lnln(n)^{2/3}(C+o(1))})$, wobei C ein Konstante ist, die im Bereich von $\frac{64}{9}^{1/3}$ liegt.

Es gibt Faktorisierungsalgorithmen, die effizient arbeiten, wenn die zu faktorisierende Zahl eine bestimmte Form besitzt. So lässt sich beispielsweise eine Zahl n, die das Produkt zweier Primzahlen p und q ist, mit polynomiellem Zeit- und Speicheraufwand faktorisieren, wenn für genau eine der beiden Primzahlen (z.B. p) gilt, dass $p-1$ nur durch kleine Primfaktoren teilbar ist.

Ebenso gibt es einen Faktorisierungsalgorithmus, der effizienter arbeitet, wenn $p+1$ nur durch kleine Primfaktoren teilbar ist. Im Folgenden sollen diese beiden Faktorisierungsalgorithmen kurz beschrieben werden.

Die $p-1$-Faktorisierungsmethode

In diesem Abschnitt wird gezeigt, dass eine Zahl $n = pq$ mit polynomiellem Zeit- und Speicheraufwand faktorisiert werden kann, wenn für genau eine der beiden Primfaktoren

p und q (im Folgenden oBdA p) von $n = pq$ gilt, dass $p-1$ nur durch Primzahlen teilbar ist, die kleiner als eine relativ kleine Schranke S sind. Die Schranke S wird dabei so klein gewählt, dass alle auf ihr beruhenden weiteren Berechnungen in polynomieller Laufzeit berechenbar sind. Diese Faktorisierungsmethode wurde von Pollard (Pol74) entwickelt.

Angenommen für eine der beiden Primzahlen p, q (oBdA p) gilt:

$$p - 1 = \prod_{p_i \in P; p_i < S} p_i^{e_i}$$

Zunächst wird nun eine Zahl k berechnet, für die gilt, dass sie von $p-1$ geteilt wird. Zum Beispiel kann $k := S!$ oder $k := \prod_{p_i \in P; p_i < S} p_i^{f_i}$ mit $f_i = \lfloor log_{p_i} S \rfloor$ gewählt werden. Dann wählt man eine zufällige Zahl $a \in Z_n^*$ und berechnet $b := a^k \bmod n$. Da $p-1|k$ gilt, folgt $b \equiv_p 1$. Mit einer hohen Wahrscheinlichkeit gilt aber $b \not\equiv_q 1$, da $q - 1 \not| k$ gilt. Dann ist $ggT(b-1, n)$ ein nichttrivialer Faktor von n.

Die Laufzeit des Algorithmus hängt neben der Größe der zu faktorisierenden Zahl auch von der Größe der Schranke S ab und liegt in der Größenordnung von $O(\frac{Sln(n)}{ln(S)})$.

Die $p+1$-Faktorisierungsmethode

Diese Methode zur Faktorisierung von Zahlen stammt von H.C.Williams (Wil82) und kann eine zusammengesetzte Zahl $n = pq$ faktorisieren, wenn für genau einen der beiden Faktoren p oder q gilt (im Folgenden oBdA p), dass $p+1$ nur durch Primzahlen teilbar ist, die kleiner als eine kleine Schranke S sind. Diese Faktorisierungsmethode nutzt eine besondere Eigenschaft von Lucas-Funktionen aus.

Zunächst sollen Lucas-Funktionen und einige ihrer besonderen Eigenschaften beschrieben werden.

Seien P, Q ganze Zahlen und seien α, β die Nullstellen des Polynoms $x - Px + Q$. Dann sind die zu dem Polynom gehörigen Lucas-Funktionen wie folgt für $k \in N$ definiert:

$$\begin{aligned} U_k(P,Q) &= \frac{\alpha^k - \beta^k}{\alpha - \beta} \\ V_k(P,Q) &= \alpha^k + \beta^k \end{aligned}$$

Diese Funktionenfolge hat unter anderem die folgenden Eigenschaften.

$$\begin{aligned} U_{k+1} &= PU_k - QU_{k-1} \quad \text{für } k \geq 1 \\ V_{k+1} &= PV_k - QV_{k-1} \quad \text{für } k \geq 1 \\ U_{2k} &= V_k U_k \quad \text{für } k \geq 0 \\ V_{2k} &= V_k^2 - 2Q^k \quad \text{für } k \geq 0 \end{aligned}$$

Aus den obigen Gleichungen kann ein effizienter Algorithmus zur Berechnung der Lucas-Funktionen U_ℓ, V_ℓ analog zum Square and Multiply-Algorithmus entworfen werden.

Die wichtigste Eigenschaft, um Lucas-Funktionen zur Faktorisierung nutzen zu können, steckt in dem folgenden Satz von Lehmer (Lem30):

2.3.3.0.1 Satz: Sei p eine ungerade Primzahl, $p \not| Q$ und sei das Legendre Symbol von $\left(\frac{P^2-4Q}{p}\right) = \epsilon$, dann gilt:

$$\begin{aligned} U_{(p-\epsilon)m}(P,Q) &\equiv_p 0 \\ V_{(p-\epsilon)m}(P,Q) &\equiv_p 2Q^{m(1-\epsilon)/2} \end{aligned}$$

Beweis:

Siehe (Lem30). □

2.3.3.0.2 Korollar: Sei p eine ungerade Primzahl, $p \not| Q$ und sei das Legendre Symbol von $\left(\frac{P^2-4Q}{p}\right) = -1$, dann gilt:

$$\begin{aligned} U_{(p+1)m}(P,Q) &\equiv_p 0 \\ V_{(p+1)m}(P,Q) &\equiv_p 2Q^m \end{aligned}$$

Beweis:

Die Behauptung folgt direkt aus dem obigen Satz mit $\epsilon = -1$. □

Der Algorithmus zur Faktorisierung von $n = pq$ erfolgt dann wie im Folgenden beschrieben: Angenommen, für eine der beiden Primzahlen (oBdA p) gilt $p+1 = \prod_{p_i \in P; p_i < S} p_i^{e_i}$. Zunächst wird nun eine Zahl k berechnet, für die gilt, dass sie von $p+1$ geteilt wird. Zum Beispiel kann $k := S!$ oder $k := \prod_{p_i \in P p_i < S} p_i^{f_i}$ mit $f_i = \lfloor log_{p_i} S \rfloor$ gewählt werden. Dann wählt

man zufällige Zahlen $P, Q \in Z_n^*$, so dass $\left(\frac{P^2-4Q}{p}\right) = -1$ gilt, und berechnet U_k und V_k. Dies ist effizient mit Hilfe der oben aufgeführten Gleichungen möglich.

Da $p+1|k$, also $k = r(p+1)$ für ein geeignetes r gilt, folgt nach dem obigen Korollar $U_k \equiv_p 0$. Mit einer hohen Wahrscheinlichkeit gilt aber $U_k \not\equiv_q 0$, da $q+1 \not| k$. Somit ist $ggT(U_k, n)$ ein nichttrivialer Faktor von n.

In Abschnitt 4.2.1 wird sich zeigen, dass die Lucas-Funktionen in engem Zusammenhang mit 2×2 Matrizen stehen, so dass auch mit Hilfe von 2×2 Matrizen ein äquivalenter $p+1$-Faktorisierungsalgorithmus erstellt werden kann.

2.3.4 RSA und Faktorisierung

Im Folgenden soll der Zusammenhang zwischen der Faktorisierung des Modul n und dem Lösen des RSA-Problems verdeutlicht werden.

2.3.4.1 Satz: Das Problem der Faktorisierung des Modul n ist bei gegebenem öffentlichem Schlüssel (e, n) mit $ggT(e, \varphi(n)) = 1$ äquivalent zu der Berechnung des geheimen RSA-Schlüssels d.

Beweis:

"$\Rightarrow$" Klar ist, dass mit der Faktorisierung von n auch $\varphi(n)$ berechnet werden kann. Damit ist die Berechnung von $d \equiv_{\varphi(n)} e^{-1}$ in polynomieller Zeit möglich.

"$\Leftarrow$" Nun soll der umgekehrte Weg gezeigt werden. Sei d gegeben. Dann ist $k := ed - 1$ nach der Definition von e und d ein Vielfaches von $\varphi(n)$. k kann dargestellt werden als $k = 2^t r$ für eine geeignete Zahl $t \geq 1$ und eine ungerade Zahl r. Da k ein Vielfaches von $\varphi(n)$ ist, gilt $g^k \equiv_n 1$ für alle $g \in Z_n^*$, und daher ist $g^{k/2}$ eine diskrete Einheitswurzel modulo n. Ist n das Produkt zweier Primzahlen p und q, so existieren genau 4 diskrete Einheitswurzeln modulo n. Diese sind 1, $n-1$, x_1, x_2, wobei x_1 die Kongruenzen $x_1 \equiv_p 1$ und $x_1 \equiv_q -1$ erfüllt. x_2 erfüllt die Kongruenzen $x_2 \equiv_p -1$ und $x_2 \equiv_q 1$. Besitzt man eine der beiden Quadratwurzeln x_1, x_2, so ist die Faktorisierung von n mit polynomiellem Zeit- und Speicheraufwand möglich, indem man $ggT(x_i - 1, n)$ berechnet. Denn es gilt $ggT(x_1 - 1, n) = p$ und $ggT(x_2 - 1, n) = q$.

Wählt man g zufällig aus Z_n^*, so ist ein Element der Folge $g^{k/2}, g^{k/4}, \ldots, g^{k/2^t}$ mit Wahrscheinlichkeit $\frac{1}{2}$ eine nichttriviale Einheitswurzel modulo n. Denn ein Wert k_i der Folge

$k/2, k/4, \ldots, k/2^t$ erfüllt eine der beiden folgenden Bedingungen:

1. k_i ist ein Vielfaches von genau einer der beiden Zahlen $p-1, q-1$ (z.B. $p-1$), aber nicht von beiden Zahlen. In diesem Fall wäre $g^{k_i} \equiv_p 1$ für alle $g \in Z_n^*$, aber für die Hälfte der möglichen Werte von g wäre $g \equiv_q -1$.

2. k_i ist weder ein Vielfaches von $p-1$ noch von $q-1$. In diesem Fall wäre $g^{k_i} \equiv_n 1$ für $\frac{1}{4}$ aller möglichen Werte von g (genau dann, wenn g ein quadratischer Rest ist), für $\frac{1}{4}$ aller möglichen Werte von g wäre $g^{k_i} \equiv_n -1$ (genau dann, wenn g ein quadratischer Nichtrest mit Jacobisymbol 1 ist) und für die Hälfte aller möglichen Werte von g wäre $g^{k_i} \equiv_p -1$ und $g^{k_i} \equiv_q +1$, also eine nichttriviale Wurzel von 1.

□

Das heißt also, dass die Kenntnis von geheimen und öffentlichen Schlüssel eines RSA-Schlüsselpaares äquivalent zu der Kenntnis der Faktoren des Modul n ist. Allerdings konnte bisher nicht bewiesen werden, dass das Brechen der RSA-Annahme, also das Berechnen von diskreten Wurzeln modulo n, ebenfalls äquivalent zur Berechnung der Faktoren von n ist.

2.3.4.2 Bemerkung: Offenes Problem:

> Es seien ein Modul n und eine Zahl e mit $ggT(e, n) = 1$ gegeben. Existiert ein polynomieller Algorithmus, der bei Eingabe von n die Zahl n faktorisieren kann, wenn er Zugriff auf ein Orakel hat, das e-te Wurzeln modulo n berechnen kann?

Bisher konnte keine endgültige Antwort auf diese Frage gefunden werden. Es gibt jedoch Indizien, die darauf hindeuten, dass die Frage zu verneinen ist. D. Boneh und R. Venkatesan haben in ihrem Artikel (BV98) bewiesen, dass das Lösen des RSA-Problems, also das Berechnen von diskreten e-ten Wurzeln modulo n, nicht äquivalent zur Faktorisierung ist, wenn dies nur für kleine Werte von e möglich ist.

2.3.5 Berechnen von diskreten Logarithmen modulo n

Fängt ein Angreifer eine signierte Nachricht ab, so muss er, um den geheimen Schlüssel zu berechnen, einen diskreten Logarithmus berechnen. In diesem Fall besitzt er die Nachricht m, die Signatur $Sig(m) := m^d \bmod n$ und den öffentlichen Schlüssel (e, n). Will er den geheimen Schlüssel d ermitteln, so muss er den diskreten Logarithmus von $Sig(m)$ zur Basis m berechnen.

Wie in Abschnitt 2.3.3 gezeigt wurde, ist die Kenntnis von e und d äquivalent zur Kenntnis der Faktoren von n. Daraus folgt, dass ein Algorithmus, der die Berechnung von diskreten Logarithmen modulo n ermöglicht, dazu verwendet werden kann, n zu faktorisieren.

2.3.6 Kleiner geheimer Exponent

Der Aufwand für die Entschlüsselung einer Nachricht bzw. für die Signaturerstellung einer Nachricht ist linear abhängig von der Bitlänge des geheimen Schlüssels d. Um eine möglichst effiziente Signaturerstellung zu ermöglichen, wäre also ein kleiner Wert für d nützlich. M. Wiener hat jedoch gezeigt (Wi90), dass es möglich ist, den geheimen Schlüssel d effizient zu berechnen, wenn d zu klein gewählt wurde.

2.3.6.1 Satz: M. Wiener,1990:

Es sei $n = pq$ mit $q < p < 2q$ und sei $d < \frac{1}{3}n^{1/4}$. Ist der öffentliche Schlüssel (e, n) bekannt, so ist es effizient möglich, d zu berechnen.

Beweis:

Da $ed \equiv_{\varphi(n)} 1$ gilt, existiert ein $k \in Z$, so dass gilt: $ed - k\varphi(n) = 1$. Somit gilt auch:

$$\left| \frac{e}{\varphi(n)} - \frac{k}{d} \right| = \frac{1}{d\varphi(n)}$$

Des Weiteren gilt: $p + q - 1 < 3q - 1 < 3q < 3\sqrt{n}$, und es folgt:

$$\mid n - \varphi(n) \mid = \mid n - (n - p - q + 1) \mid < 3\sqrt{n}$$

Man betrachtet nun $\frac{k}{d}$ als eine Näherung von $\frac{e}{\varphi(n)}$ und approximiert $\varphi(n)$ durch n. Es folgt:

$$\begin{aligned}\left|\frac{e}{n}-\frac{k}{d}\right| &= \left|\frac{ed-nk+k\varphi(n)-k\varphi(n)}{dn}\right| \\ &= \left|\frac{ed-k\varphi(n)-nk+k\varphi(n)}{dn}\right| = \left|\frac{1-k(n-\varphi(n))}{dn}\right| \leq \left|\frac{3k\sqrt{n}}{dn}\right| \\ &= \frac{3k}{d\sqrt{n}}\end{aligned}$$

Da $k\varphi(n) < ed$ ist, und somit $k < d < \frac{1}{3}n^{1/4}$ gilt, folgt für die obige Ungleichung:

$$\left|\frac{e}{n}-\frac{k}{d}\right| \leq \frac{n^{1/4}}{dn^{1/2}} = \frac{1}{dn^{1/4}} < \frac{1}{3d^2}$$

Der folgende Satz über Kettenbrüche aus der Zahlentheorie besagt, dass die Anzahl der Brüche $\frac{k}{d}$ mit $d < n$, die $\frac{e}{n}$ mit dieser Genauigkeit annähern, durch $log_2 n$ beschränkt ist.

2.3.6.2 Satz: Seien $x_1 = \frac{a_1}{b_1}, x_2 = \frac{a_2}{b_2}$ zwei rationale Zahlen. Gilt $\mid x_1 - \frac{a_2}{b_2} \mid < \frac{1}{2b_2^2}$, dann ist $\frac{a_2}{b_2}$ eine Konvergente der Kettenbruchentwicklung von x_1.

Beweis:

Siehe (HW75) Theorem 184. □

Das heißt in dem vorliegenden Fall, dass $\frac{k}{d}$ eine Konvergente der Kettenbruchentwicklung von $\frac{e}{n}$ ist. Die Kettenbruchdarstellung kann über einen Algorithmus, der dem euklidischen Algorithmus zur Bestimmung des ggT sehr ähnlich ist, berechnet werden. Näheres dazu siehe (HW75), Seite 143ff. Mit anderen Worten: Mit Hilfe der Kettenbruchentwicklung von $\frac{e}{n}$ lassen sich k und insbesondere d berechnen. □

2.3.7 Kleiner öffentlicher Exponent

Ebenso wie im oberen Abschnitt kann es nützlich sein, den öffentlichen Schlüssel möglichst klein zu wählen. Damit kann eine effizientere Verschlüsselung der Daten, oder eine effizientere Signaturverifizierung erreicht werden. Leider eröffnet ein zu klein gewählter öffentlicher Exponent aber auch neue Angriffsmöglichkeiten. Der kleinstmögliche öffentliche Exponent ist 3. Wird die 3 als öffentlicher Exponent gewählt, so können Nachrichten, die mit mindestens 3 verschiedenen RSA-Schlüsseln verschlüsselt wurden, wieder entschlüsselt werden, ohne dass die Kenntnis eines einzigen geheimen Schlüssels notwendig ist:

Angenommen, es werden 3 RSA-Schlüssel verwendet, bei denen jeweils der öffentliche Exponent gleich 3 ist, also $(3, n_1), (3, n_2), (3, n_3)$. Die Verschlüsselung einer Nachricht m unter den angegeben Schlüsseln würde die folgenden Werte annehmen:

$$c_1 := m^3 \bmod n_1$$
$$c_2 := m^3 \bmod n_2$$
$$c_3 := m^3 \bmod n_3$$

Unter der Annahme, dass die drei gewählten Moduli paarweise teilerfremd sind, existiert nach dem Chinesischen Restsatz ein eindeutiger Wert c in $Z^*_{n_1 n_2 n_3}$, der alle drei Kongruenzen erfüllt. Es folgt, dass $c = m^3 \bmod n$ sein muss, da dieser Wert alle obigen Kongruenzen erfüllt. Da aber auch $m < \min\{n_1, n_2, n_3\}b$ gilt, folgt $m^3 < n_1 n_2 n_3$ und somit $c = m^3$. Die Nachricht m kann also durch Ziehen der dritten Wurzel aus c berechnet werden. Dieser Angriff ist immer erfolgreich, wenn die gleiche Nachricht mit e verschiedenen Moduli verschlüsselt wird.

J. Hastad hat in (Ha88) eine Erweiterung dieses Angriffs beschrieben. Er zeigt, dass selbst dann, wenn nicht die gleiche Nachricht, sondern jeweils der Funktionswert eines Polynoms an der Stelle m unter verschiedenen Moduli verschlüsselt wird, die Nachricht ohne einen der geheimen Schlüssel rekonstruiert werden kann. D.h. es wird nicht jeweils die Nachricht m verschlüsselt, sondern $f_i(m)$, d.h. $c_i := f_i(m)^e \bmod n_i$.

2.3.8 Spezielle Angriffe auf das RSA-Signaturverfahren

Dieser Abschnitt beschäftigt sich mit speziellen Angriffen auf das RSA-Signaturverfahren. Diese Angriffe haben nicht zum Ziel, den geheimen Schlüssel zu berechnen, sondern versuchen aus gegebenen Informationen gültige Signaturen zu erzeugen. Man unterscheidet folgende Angriffskategorien nach (GMR88).

1. **Totaler Bruch:** Hierbei wird das Signaturverfahren komplett gebrochen. Dem Angreifer gelingt es, den geheimen Signaturschlüssel zu berechnen.

2. **Universelle Fälschung:** Dem Angreifer gelingt es zwar nicht, den geheimen Signaturschlüssel zu berechnen, aber es gelingt ihm, das System so zu brechen, dass er Signaturen zu jeder beliebigen Nachricht erzeugen kann.

3. **Existentielle Fälschung:** Dem Angreifer gelingt es ein Signatur-/Nachrichtenpaar zu erzeugen.

Die Erfolgsaussichten eines Angriffs hängen eng mit den dem Angreifer zur Verfügung stehenden Informationen zusammen. Man unterscheidet folgende Fälle (siehe ebenfalls (GMR88)):

1. **Angriff ohne Signaturen:** Der Angreifer besitzt lediglich den öffentlichen Schlüssel.

2. **Angriff mit bekannten Signaturen:** Der Angreifer besitzt außer dem öffentlichen Schlüssel ein oder mehrere Nachrichten-/Signaturpaare.

3. **Angriff mit gewählten Signaturen:** Der Angreifer besitzt außer dem öffentlichen Schlüssel Signaturen zu Nachrichten, die er zuvor selbst gewählt hat.

4. **Angriff mit adaptiv gewählten Signaturen:** Der Angreifer kann, während er den Angriff durchführt, Signaturen zu frei gewählten Nachrichten erstellen lassen.

Unter den oben beschriebenen Angriffszenarien können folgende Aussagen über das in Abschnitt 2.1 beschriebene RSA-Verfahren bewiesen werden.

2.3.8.1 Satz: Das RSA-Verfahren ist existentiell fälschbar unter einem Angriff ohne Signaturen.

Beweis:

Bei einem Angriff ohne Signaturen besitzt der Angreifer lediglich den öffentlichen Schlüssel (e, n) des RSA-Signaturschlüsselpaares. Damit ist es ihm möglich, ein gültiges Nachrichten-/Signaturpaar zu erzeugen. Dazu wählt er einen zufälligen Wert s und berechnet $m := s^e \bmod n$. Dann ist s eine gültige Signatur zu m. □

2.3.8.2 Satz: Das RSA-Verfahren ist universell fälschbar unter einem Angriff mit gewählten Signaturen.

Beweis:

Bei einem Angriff mit gewählten Signaturen besitzt der Angreifer außer dem öffentlichen Schlüssel (e, n) des RSA-Signaturschlüsselpaares die Möglichkeit, sich beliebige Nachrichten signieren zu lassen (natürlich darf die Nachricht, zu der er eine Signatur fälschen will, sich nicht unter diesen Nachrichten befinden). Um eine Signatur zu einer beliebigen Nachricht m zu fälschen, wählt er einen zufälligen Wert $s \in Z_n$. Er prüft, ob $ggT(s, n) > 1$ gilt. Falls dies der Fall ist, hat er einen nicht-trivialen Teiler von n gefunden und kann den geheimen Schlüssel d berechnen und beliebige Signaturen erzeugen. Gilt $ggT(s, n) = 1$, so berechnet er $m' := ms^e \bmod n$. Zu der Nachricht m' lässt er sich dann eine gültige Signatur erzeugen.

Es gilt:

$$Sig(m') \equiv_n (ms^e)^d = m^d s \bmod n$$

Somit ist $Sig(m')s^{-1} \equiv_n m^d$ eine gültige Signatur auf m. □

Diese Angriffsmöglichkeit nutzt die Homomorphieeigenschaft des RSA-Verfahrens aus Abschnitt 2.2 aus.

2.4 Anforderungen an die zugrundeliegende Gruppe Z_n^*

Damit das RSA-Verfahren sicher gegen die in Abschnitt 2.3 beschriebenen Angriffe ist, muss die zugrundeliegende Gruppe einige besondere Eigenschaften besitzen. In diesem Abschnitt sollen diese Eigenschaften behandelt werden. Die Sicherheit des RSA-Verfahrens ist abhängig von der Schwierigkeit, diskrete Wurzeln (siehe Abschnitt 2.3.2) berechnen zu können, d.h. es ist schwierig für ein gegebenes Gruppenelement c und einer natürlichen Zahl e, ein Element m zu finden, so dass $m^e = c$ gilt. Daraus ergeben sich folgende Anforderungen an die zugrundeliegende Gruppe:

2.4.1 Anforderung 1: Ordnung der Gruppe

Es muss schwierig sein, die Ordnung der zugrundeliegenden multiplikativen Gruppe zu bestimmen. Kennt man die Ordnung $|G|$ der multiplikativen Gruppe G (im Falle des in Abschnitt 2.1 beschriebenen RSA-Verfahrens ist $G = Z_n^*$), so ist das Ziehen von e-ten Wurzeln mit $ggT(e, |G|) = 1$ mit polynomiellem Zeit- und Speicheraufwand möglich. Man kann mit Hilfe des erweiterten euklidischen Algorithmus einen Wert d zu e berechnen, für den gilt: $d \equiv_{|G|} e^{-1}$. Um eine e-te Wurzel zu einem Element $g \in G$ zu bestimmen, berechnet man g^d innerhalb der Gruppe G.

2.4.2 Anforderung 2: Ordnung eines Elements

Es muss schwierig sein, innerhalb der Gruppe die Ordnung eines vorgegeben Elementes zu bestimmen. Ansonsten ist das Ziehen diskreter Wurzeln zu diesen Werten möglich: Um die e-te Wurzel des Elementes g zu bestimmen, bestimmt man zunächst die Ordnung von g ($ord(g)$). Gilt $ggT(e, ord(g)) = 1$, so existiert eine eindeutig bestimmte Wurzel c von g mit $ord(c) = ord(g)$. Diese kann bestimmt werden, indem man zunächst mit Hilfe des erweiterten euklidischen Algorithmus $d \equiv_{ord(g)} e^{-1}$ bestimmt und dann g^d berechnet.

2.4.3 Anforderung 3: Die Primzahlen p und q

Die Sicherheit des in Abschnitt 2.1 beschriebenen RSA-Verfahrens hängt eng mit dem Problem der Faktorisierung von Zahlen zusammen. Kennt man die Faktorisierung von n, so kann die Ordnung von Z_n^* berechnet werden, und das Problem der Berechnung von diskreten Wurzeln ist dann lösbar. Damit die Faktorisierung von $n = pq$ schwierig ist, sollten die Primzahlen p und q ausreichend groß gewählt werden. Nach heutigem Kenntnisstand gilt eine Wahl der Primzahlen in einer Größenordnung von 512 Bit als sicher. Somit ist das Faktorisieren von n weder mit dem Number-Field-Sieve noch mit einer Brute-Force-Attacke effizient möglich. Es sollte auch ausgeschlossen werden, dass für eine der beiden Primzahlen p gilt, dass $p-1$ nur durch kleine Primfaktoren geteilt wird, da sonst der Algorithmus aus Abschnitt 2.3.3 angewendet werden kann, um n zu faktorisieren. Ebenso sollte sichergestellt werden, dass nicht für eine der beiden Primzahlen p gilt, dass $p+1$ nur durch kleine Primzahlen geteilt wird, da sonst der Algorithmus aus Abschnitt 2.3.3 zur Berechnung der

Faktorisierung von n genutzt werden kann.

2.4.4 Anforderung 4: Der geheime Parameter d

In Abschnitt 2.3.6 wurde gezeigt, dass der Parameter d berechnet werden kann, wenn $d < \frac{1}{3}n^{1/4}$ gilt. Es sollte daher überprüft werden, dass auch der geheime Exponent d ausreichend groß ist. Eine weitere Möglichkeit den Angriff abzuwehren ist, den zugehörigen öffentlichen Schlüssel e groß genug zu wählen. Wählt man anstatt e einen Wert $e' := e + t\varphi(n)$ als öffentlichen Parameter, so kann e' so groß gewählt werden, dass $k < d < \frac{1}{3}n^{1/4}$ nicht mehr gilt und der Angriff nicht mehr erfolgreich sein kann.

2.4.5 Anforderung 5: Der öffentliche Parameter e

In Abschnitt 2.3.7 wurde gezeigt, dass ein zu klein gewählter Parameter e dazu führen kann, dass Nachrichten entschlüsselt werden können, wenn die gleiche Nachricht ausreichend oft mit verschiedenen Schlüsseln (die alle den gleichen öffentlichen Exponenten e verwenden) verschlüsselt wurde. Um dies zu verhindern, sollte der öffentliche Parameter e ausreichend groß gewählt werden. Häufig wird daher der Wert $2^{16} + 1 = 65537$ für e empfohlen, bei dem die beschriebenen Angriffe aus Abschnitt 2.3.7 wirkungslos bleiben.

2.5 Varianten des RSA-Signaturverfahrens

Die in Abschnitt 2.3.8 beschriebenen Angriffe auf das Signaturverfahren können nicht durch eine geeignete Wahl der Gruppenparameterwahl der Gruppe Z_n^* verhindert werden.

Aus diesem Grund wurde eine Variante des RSA-Signaturverfahrens entwickelt, für das sogar innerhalb eines bestimmten Modells, dem sogenannten Random-Oracle-Modell, ein Sicherheitsbeweis angegeben werden kann. Das Verfahren stammt von M. Bellare und P. Rogaway (BR96) und wird als *Full Domain Hash* (FDH-)RSA-Signaturverfahren bezeichnet. Dieser Name stammt von der Eigenschaft der Hashfunktion, die für den Sicherheitsbeweis benötigt wird. Eine Full-Domain-Hashfunktion $h_{FDH} : \{0,1\}^* \to Z_n^*$ hasht die Binärstrings zufällig gleichverteilt auf Z_n^*.
Das FDH-RSA-Verfahren erfolgt durch folgenden Schritte:

Der Signaturschlüssel wird genauso generiert wie in dem ursprünglichen RSA-Verfahren. Zusätzlich wird eine Full-Domain-Hashfunktion h gewählt und veröffentlicht. Eine Nachricht m wird von dem Signierer signiert, indem der die Full-Domain-Hashfunktion h auf die Nachricht anwendet: $Hash_m := h(m)$. Dann signiert er nur noch diesen Hashwert mittels $Sig(m) := Hash_m^d \bmod n$. Um die Signatur zu überprüfen, berechnet $m' := Sig(m)^e \bmod n$ und $Hash_m := h(m)$ und überprüft dann, ob $Hash_m = m'$ gilt.

Ein Nachteil dieses Verfahrens ist, dass die Sicherheit des Verfahrens nicht mehr nur von der Schwierigkeit der Berechnung von diskreten Wurzeln abhängig ist, sondern zusätzlich die Güte der verwendeten Hashfunktion ein erhebliche Rolle spielt. Eine Hashfunktion, deren Ausgaben in Relation zueinander stehen, kann die Angriffe aus Abschnitt 2.3.8 nicht verhindern.

Durch den Einsatz von Hashfunktionen geht eine weitere wichtige Eigenschaft des Signaturverfahrens verloren: Die Nichtabstreitbarkeit von Signaturen ist nicht mehr gewährleistet. Im ursprünglichen RSA-Verfahren gibt es zu jeder Signatur genau eine Nachricht $m \in Z_n^*$, zu der die Signatur gehören kann. In der RSA-Variante, die zunächst einen Hashwert der Nachricht bildet, der dann signiert wird, können mehrere Nachrichten auf denselben Hashwert abgebildet werden ($h(m_1) = h(m_2)$). Auch wenn die Hashfunktion gute kryptografische Eigenschaften besitzt und somit solche Kollisionen nur schwer gefunden werden können, kann nicht mehr bewiesen werden, dass die Signatur zu einer bestimmten Nachricht generiert wurde.

Kapitel 3

RSA-Verfahren auf Matrixgruppen

3.1 Verallgemeinerung des RSA-Verfahrens

Das in Abschnitt 2.1 beschriebene originale RSA-Verfahren basiert auf Operationen in dem Ring Z_n bzw. der multiplikativen Gruppe Z_n^*. Im ersten Abschnitt dieses Kapitels soll zunächst erläutert werden, welche Eigenschaften eine multiplikative Gruppe G haben muss, damit das RSA-Verfahren funktioniert. Im nächsten Abschnitt werden zwei veröffentlichte Verfahren vorgestellt, die das RSA-Verfahren auf Matrizengruppen erweitern. Dann werden die mathematischen Eigenschaften der Gruppen $SL(2, Z_n)$ und $GL(2, Z_n)$ in Bezug auf ihre kryptographische Nutzung untersucht.

3.1.1 Existenz einer Potenzfunktion

Auf der multiplikativen Gruppe G muss eine Potenzfunktion definiert sein. Das heißt, es muss eine Abbildung P geben, die als Eingabe einen Wert g aus G und eine Zahl $k \in Z$ aus der Menge der ganzen Zahlen besitzt und auf einen Wert $\ell \in G$ abbildet ($P(g, k) = \ell$). Des Weiteren muss es eine Verknüpfung $\oplus$ für zwei Zahlen $a, b \in Z$ geben mit $P(g, a \oplus b) = P(P(g, a), b)$.

Eine wichtige Eigenschaft der Gruppe, die Voraussetzung für das Funktionieren des RSA-Verfahrens ist, ist die Gültigkeit des Assoziativgesetzes. Das heißt, es gilt für $a, b, c \in$

G :

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

Diese Eigenschaft ist notwendig, damit für $e, d \in Z$ mit $ed \equiv_{|G|} 1$ und $g \in G$ gilt:

$$(g^e)^d = \underbrace{(g^e)(g^e)\cdots(g^e)}_{d-Mal} = g^{ed} = 1$$

Die Eigenschaft der Kommutativität, d.h. dass $g_1 g_2 = g_2 g_1$ gilt, ist jedoch eine für das RSA-Verfahren nicht notwendige Eigenschaft. Ist in der zugrundeliegenden Gruppe diese Eigenschaft nicht vorhanden, so gelingt der in Abschnitt 2.3.8 beschriebene Angriff nicht notwendigerweise, wie im folgenden Beispiel der Matrizengruppe $SL(2, Z_{77})$ gezeigt wird.

3.1.1.1 Beispiel: Sei $p = 7$ und sei $q = 11$, also $n = 77$ und seien $A := \begin{pmatrix} 20 & 3 \\ 15 & 10 \end{pmatrix}$,$B := \begin{pmatrix} 41 & 5 \\ 56 & 20 \end{pmatrix}$ Matrizen in $SL(2, Z_n)$.

Sei $e = 53$, dann gilt:

$$\begin{aligned}
A * B &\equiv_{77} \begin{pmatrix} 20 & 3 \\ 15 & 10 \end{pmatrix}\begin{pmatrix} 41 & 5 \\ 56 & 20 \end{pmatrix} \equiv_{77} \begin{pmatrix} 64 & 6 \\ 20 & 44 \end{pmatrix} \\
\begin{pmatrix} 20 & 3 \\ 15 & 10 \end{pmatrix}^{53} &\equiv_{77} \begin{pmatrix} 42 & 68 \\ 32 & 72 \end{pmatrix} \\
\begin{pmatrix} 41 & 5 \\ 56 & 20 \end{pmatrix}^{53} &\equiv_{77} \begin{pmatrix} 13 & 27 \\ 56 & 69 \end{pmatrix} \\
\begin{pmatrix} 64 & 6 \\ 20 & 44 \end{pmatrix}^{53} &\equiv_{77} \begin{pmatrix} 34 & 43 \\ 15 & 19 \end{pmatrix} \not\equiv_{77} \begin{pmatrix} 42 & 51 \\ 59 & 57 \end{pmatrix} \equiv_{77} \begin{pmatrix} 42 & 68 \\ 32 & 72 \end{pmatrix}\begin{pmatrix} 13 & 27 \\ 56 & 69 \end{pmatrix}
\end{aligned}$$

Aus diesem Ergebnis könnte man fälschlicherweise folgern, dass bestimmte Angriffe, welche die Homomorphie Eigenschaften des RSA-Verschlüsselungsfunktion in Z_n^* ausnutzen, nicht auf nicht-abelsche Gruppen übertragen werden können. So könnte man zum

Beispiel annehmen, dass RSA-Signaturen basierend auf nicht-abelschen Gruppen nicht universell fälschbar unter einem Angriff mit gewählten Signaturen sind.

In dieser Arbeit wird jedoch gezeigt werden, dass auch das RSA-Signaturverfahren, das auf nicht-abelschen Gruppen operiert, dennoch universell fälschbar unter einem Angriff mit gewählten Signaturen ist. Dies wird am Beispiel der RSA-Funktion in $GL(s, Z_n)$ erläutert und dann für den allgemeinen Fall der nicht-ableschen Gruppen bewiesen werden (siehe 5.8).

3.2 Verallgemeinerung des RSA-Verfahrens auf 2×2-Matrizen

In diesem Abschnitt wird gezeigt, wie das RSA-Verfahren auf 2×2- Matrizen erweitert werden kann. Diese Verallgemeinerung des RSA-Verfahrens ist zurückzuführen auf V. Varadharajan und R. Odoni (VO85), die als erste eine solche Erweiterung des Verfahrens vorgestellt haben. 1990 haben C. Chuang und J.G. Dunham (CD90) eine weitere Variante dieses Verfahrens vorgestellt, die zur Verschlüsselung zusätzlich eine Einwegfunktion verwendet.

Zunächst werden in Abschnitt 3.2.1 einige Eigenschaften der Matrixgruppen $SL(2, Z_n)$ und $GL(2, Z_n)$ behandelt, die zur Beschreibung der beiden Verfahren benötigt werden. Anschließend werden in den Abschnitten 3.2.2 und 3.2.3 die beiden aufgeführten Verfahren für den Fall der 2×2-Matrizen beschrieben. Eine weitergehende Untersuchung der Matrixgruppen $SL(2, Z_n)$ und $GL(2, Z_n)$ in Bezug auf die Verwendung und Sicherheit des RSA-Verfahrens erfolgt in Abschnitt 4. Es wird gezeigt werden, dass die Sicherheit des RSA-Verfahrens, das auf der Gruppe $GL(2, Z_n)$ operiert, mindestens so hoch ist wie die des RSA-Verfahrens, welches auf der Gruppe Z_n operiert.

Im Gegensatz zu den Sicherheitsuntersuchungen in (VO85) und (CD90), die im wesentlichen Dreiecksmatrizen betrachten, bei denen sich die Sicherheit direkt auf das RSA-Problem in der zugrundeliegenden Gruppe Z_n zurückführen lässt, wird in dieser Arbeit die Sicherheit der Verfahren bei Nutzung beliebiger nicht-singulärer Matrizen betrachtet.

In den Abschnitten 4.4.1 und 4.4.2 erfolgt eine Klassifizierung der Matrizen, für die unterschiedliche Sicherheitsaussagen getroffen werden können.

3.2.1 Grundlagen $GL(2, Z_n)$ und $SL(2, Z_n)$

In diesem Abschnitt werden die zur Beschreibung der von V. Varadharajan und R. Odoni (VO85), bzw. C. Chuang und J.G. Dunham (CD90) beschriebenen Erweiterungen des RSA-Verfahrens auf Matrixgruppen notwendigen Grundlagen von $SL(2, Z_n)$ und $GL(2, Z_n)$ beschrieben.

3.2.1.1 Definition: Die Menge der 2×2 Matrizen über Z_n mit Determinante 1 wird mit $SL(2, Z_n)$ bezeichnet.

3.2.1.2 Definition: Die Menge der 2×2 Matrizen über Z_n mit Determinante ungleich 0 wird mit $GL(2, Z_n)$ bezeichnet.

3.2.1.3 Satz: $SL(2, Z_n)$ bildet zusammen mit der üblichen Matrizenmultiplikation eine nicht abelsche endliche Gruppe.

Beweis:
Siehe (Ro96). □

3.2.1.4 Satz: $GL(2, Z_n)$ bildet zusammen mit der üblichen Matrizenmultiplikation eine nicht abelsche endliche Gruppe.

Beweis:
Siehe (Ro96). □

3.2.1.5 Satz: Sei p eine Primzahl, dann gilt: $|SL(2, Z_p)| = p(p-1)(p+1)$.

Beweis:
Siehe (Ro96). □

3.2.1.6 Satz: Sei p eine Primzahl, dann gilt: $|GL(2, Z_p)| = p(p-1)^2(p+1)$.

Beweis:
Siehe (Ro96). □

3.2.1.7 Satz: Chinesischer Restsatz für Matrizen:

Es sei $n = \prod_{i=1}^{k} p_i$ mit $ggT(p_i, p_j) = 1$ für $i \neq j$ und seien $A_1, A_2, \ldots, A_k$ Matrizen. Dann gibt es eine Matrix X, so dass $X = A_i \bmod p_i$ für $i = 1, 2, \ldots k$ gilt. Diese Matrix ist modulo n eindeutig bestimmt.

Beweis:

Zunächst wird die Behauptung für $k = 2$ gezeigt und dann per Induktion über k bewiesen. Sei $n = p_1 p_2$ mit $ggT(p_1, p_2) = 1$. Dann gibt es nach dem erweiterten Euklidischen Algorithmus zwei ganze Zahlen p_1', p_2' mit $p_1 p_1' + p_2 p_2' = 1$. Setzt man $X = A_1 p_2 p_2' + A_2 p_1 p_1'$, so folgt $X = A_1 \bmod p_1$ und $X = A_2 \bmod p_2$. Es bleibt zu zeigen, dass es nur eine Lösung modulo n gibt. Angenommen, es gibt ein weiteres X' mit $X' = A_1 \bmod p_1$ und $X' = A_2 \bmod p_2$. Dann gilt $p_1 | (X - X')$ und $p_2 | (X - X')$ (d.h. jeder Eintrag der Matrix $X - X'$ wird von p_1 und p_2 geteilt). Nach dem Chinesischen Restsatz wird dann auch jeder Eintrag der Matrix $X - X'$ von n geteilt. Somit gilt $X \equiv_n X'$, also $X = X'$.

Angenommen, die Behauptung gilt für $k = s$, d.h. es gibt eine eindeutige Matrix X modulo $\prod_{i=1}^{s} p_i$ mit $X = A_i \bmod p_i$ für $i = 1, 2, \ldots, s$ dann folgt für $k = s + 1$:

Sei $n^* = \prod_{i=1}^{s} p_i$, dann ist $n = n^* p_{s+1}$ mit $ggT(n^*, p_{s+1}) = 1$. Dann gibt es nach dem erweiterten Euklidischen Algorithmus zwei ganze Zahlen n', p_{s+1}' mit $n^* n' + p_{s+1} p_{s+1}' = 1$. Setzt man $X_{neu} = X p_{s+1} p_{s+1}' + A_{s+1} n^* n'$, so folgt $X = A_i \bmod p_i$ für $i = 1, 2, \ldots, s + 1$.

Es bleibt zu zeigen, dass es nur eine Lösung modulo $n = \prod_{i=1}^{s+1} p_i$ gibt. Angenommen, es gibt ein weiteres X' mit $X' = A_i \bmod p_i$ für $i + 1, 2, \ldots, s + 1$, dann gilt $p_i | (X - X')$ für $i = 1, 2, \ldots, s + 1$ (d.h. jeder Eintrag der Matrix $X - X'$ wird von p_i geteilt). Nach dem Chinesischen Restsatz wird dann auch jeder Eintrag der Matrix $X - X'$ von n geteilt. Somit gilt $X \equiv_n X'$, also $X = X'$. □

3.2.1.8 Korollar: Sei $n = pq$, p, q Primzahlen, dann gilt:

$$|SL(2, Z_n)| = n\varphi(n)(p + 1)(q + 1)$$

Beweis:

Aus Satz (3.2.1.7) folgt $SL(2, Z_n) \cong SL(2, Z_p) \times SL(2, Z_q)$ und somit $|SL(2, Z_n)| = |SL(2, Z_p)||SL(2, Z_q)|$. Nach Satz (3.2.1.5) gilt für eine Primzahl p:

$$|SL(2, Z_p)| = p(p-1)(p+1)$$

Also folgt:

$$\begin{aligned} |SL(2, Z_n)| &= |SL(2, Z_p)||SL(2, Z_q)| = p(p-1)(p+1)q(q-1)(q+1) \\ &= n\varphi(n)(p+1)(q+1) \end{aligned}$$

□

3.2.1.9 Korollar: Sei $n = pq$, p, q Primzahlen, dann gilt:

$$|GL(2, Z_n)| = n\varphi(n)^2(p+1)(q+1)$$

Beweis:

Aus Satz (3.2.1.7) folgt $GL(2, Z_n) \cong GL(2, Z_p) \times GL(2, Z_q)$ und somit $|GL(2, Z_n)| = |GL(2, Z_p)||GL(2, Z_q)|$. Nach Satz (3.2.1.6) gilt für eine Primzahl p:

$$|GL(2, Z_p)| = p(p-1)^2(p+1)$$

Also folgt:

$$\begin{aligned} |GL(2, Z_n)| &= |GL(2, Z_p)||GL(2, Z_q)| = p(p-1)^2(p+1)q(q-1)^2(q+1) \\ &= n\varphi(n)^2(p+1)(q+1) \end{aligned}$$

□

3.2.2 RSA-Erweiterung auf Matrixgruppen von V. Varadharajan und R. Odoni

In diesem Abschnitt wird die von V. Varadharajan und R. Odoni (VO85) entworfene Verallgemeinerung des RSA-Verfahrens auf Matrixgruppen beschrieben. Das Verfahren besteht wie das originale RSA-Verfahren aus drei Grundprotokollen: Der Schlüsselgenerierung, der Verschlüsselung bzw. der Signaturerstellung und der Entschlüsselung bzw. der Signaturverifikation.

Die Schlüsselgenerierung

Bei der Schlüsselgenerierung werden wie bei der Schlüsselgenerierung aus dem originalen RSA-Verfahren zwei ausreichend große Primzahlen p und q zufällig gewählt und miteinander multipliziert. Das Ergebnis wird mit $n = pq$ bezeichnet.

Dann wird eine beliebige Zahl e gewählt, so dass $ggT(e, |GL(2, Z_n)|) = 1$ gilt. Das Zahlenpaar (e, n) wird als öffentlicher Schlüssel bzw. auch als public key bezeichnet. Dieses Zahlenpaar wird veröffentlicht und dient zur Verschlüsselung, bzw. zur Signaturverifikation.

Der geheime Schlüssel zur Entschlüsselung bzw. Signaturerstellung wird wie folgt berechnet: Mit Hilfe des erweiterten euklidischen Algorithmus bestimmt man ganze Zahlen d, v, so dass gilt: $ed + |GL(2, Z_n)|v = 1$. Das Zahlenpaar (d, n) wird als geheimer Schlüssel bzw. auch als private key bezeichnet. Dieser Schlüssel ist nur dem Signaturersteller bzw. dem Empfänger einer verschlüsselten Nachricht bekannt und darf an keine andere Person weitergegeben werden.

Verschlüsselung und Signaturerstellung

Verschlüsselung und Signaturerstellung laufen im wesentlichen identisch zu der Verschlüsselung und Signaturerstellung im originalen RSA-Verfahren ab, jedoch erfolgen die Berechnungen nun nicht mehr in der Gruppe Z_n^*, sondern in der Gruppe $GL(2, Z_n)$.

Verschlüsselung:

Um eine Nachricht zu verschlüsseln, wird diese als eine Matrix $A \in GL(2, Z_n)$ dargestellt. Diese Nachricht wird vom Sender der Nachricht verschlüsselt, indem er $C := A^e \bmod n$ in $GL(2, Z_n)$ berechnet. Der Chiffretext C wird an den Empfänger gesendet, der den geheimen Schlüssel (d, n) besitzt.

Signaturerstellung:

Um eine Nachricht zu signieren, wird diese als eine Matrix $A \in GL(2, Z_n)$ dargestellt. Eine Nachricht A wird von dem Signierer signiert, indem der $Sig(A) := A^d \bmod n$ in $GL(2, Z_n)$ berechnet. Die Signatur $Sig(A)$ wird dann zusammen mit der Nachricht A versendet.

Entschlüsselung und Signaturverifikation

Entschlüsselung und Signaturverifikation laufen im wesentlichen identisch zu der Verschlüsselung und Signaturerstellung im originalen RSA-Verfahren ab, jedoch erfolgen die Berechnungen nun nicht mehr in der Gruppe Z_n^*, sondern in der Gruppe $GL(2, Z_n)$.

Entschlüsselung:

Der Empfänger der Nachricht erhält den Chiffretext als Matrix C. Dieser Chiffretext kann wieder von dem Inhaber des geheimen Schlüssels entschlüsselt werden, indem er $C^d \equiv_n A^{ed} = A \bmod n$ in $GL(2, Z_n)$ berechnet.

Signaturverifikation:

Der Empfänger der Nachricht erhält die Nachricht A zusammen mit der Signatur $Sig(A)$. Die Signatur der Nachricht kann mit Hilfe des öffentlichen Schlüssels (e, n) und der Nachricht A überprüft werden. Dazu berechnet man $A' := Sig(A)^e \bmod n$ in $GL(2, Z_n)$ und überprüft, ob $A = A'$ gilt.

3.2.2.0.3 Bemerkung: Die Autoren empfehlen in ihrer Veröffentlichung die Verwendung von Dreiecksmatrizen zur Verschlüsselung, um sicherzustellen, dass die Matrix A eine nicht-singuläre Matrix (also $\in GL(2, Z_n)$) ist.

3.2.3 RSA-Erweiterung auf Matrixgruppen von C. Chuan und J.G. Dunham

In diesem Abschnitt wird die Variante der RSA-Verschlüsselung auf Matrizen von C. Chuang und J.G. Dunham beschrieben. Diese Variante verwendet neben den RSA-Operationen in $GL(2, Z_n)$ noch eine Einwegfunktion F und operiert nur auf den Dreiecksmatrizen von $GL(2, Z_n)$.

Die Schlüsselgenerierung

Bei der Schlüsselgenerierung werden wie bei der Schlüsselgenerierung aus dem originalen RSA-Verfahren zwei ausreichend große Primzahlen p und q zufällig gewählt und miteinander multipliziert. Das Ergebnis wird mit $n = pq$ bezeichnet.

Dann wird eine beliebige Zahl e gewählt, so dass $ggT(e, \varphi(n)) = 1$ gilt. Das Zahlenpaar (e, n) wird als öffentlicher Schlüssel bzw. auch als public key bezeichnet. Dieses Zahlenpaar wird veröffentlicht und dient zur Verschlüsselung, bzw. zur Signaturverifikation.

Der geheime Schlüssel zur Entschlüsselung bzw. Signaturerstellung wird wie folgt berechnet: Mit Hilfe des erweiterten euklidischen Algorithmus bestimmt man ganze Zahlen d, v, so dass gilt: $ed + \varphi(n)v = 1$. Das Zahlenpaar (d, n) wird als geheimer Schlüssel bzw. auch als private key bezeichnet. Dieser Schlüssel ist nur dem Signaturersteller bzw. dem Empfänger einer verschlüsselten Nachricht bekannt und darf an keine andere Person weitergegeben werden.

Des Weiteren wird eine Einwegfunktion F benötigt, die allen Teilnehmern bekannt ist.

Verschlüsselung

Um eine Nachricht m zu verschlüsseln, wird eine Dreiecksmatrix $A \in GL(2, Z_n)$ wie folgt erstellt:

Die Einträge auf der Hauptdiagonalen a_{ii} $(i = 1, 2)$ werden zufällig aus Z_n^* gewählt, so dass gilt: $a_{11} \not\equiv_n a_{22}$ und $ggT(a_{ii}, n) = 1$ für $i = 1, 2$. a_{21} wird gleich 0 gesetzt.

Dann wird $r \equiv_n a_{11} + a_{22}$ berechnet. Die Nachricht wird dargestellt als eine Zahl $m \in Z_n^*$ und es wird $a_{12} := m \oplus F(r)$ gesetzt.

Dann wird $C = A^e \bmod n$ in $GL(2, Z_n)$ berechnet und an den Empfänger gesendet.

Entschlüsselung

Der Empfänger der Nachricht erhält den Chiffretext als Matrix C. Dieser Chiffretext kann wieder von dem Inhaber des geheimen Schlüssels entschlüsselt werden, indem er $C^d \equiv_n A^{ed} = A \bmod n$ in $GL(2, Z_n)$ berechnet. Dann berechnet der Empfänger $r := a_{11} + a_{22} \bmod n$ und $F(r)$. Die Nachricht m erhält er dann, indem er $F(r) \oplus a_{12} = m$ berechnet.

3.2.3.0.4 Bemerkung: Die Autoren nutzen bei ihrem Verfahren eine Eigenschaft aus, die aus dem Cayley-Hamilton Theorem folgt, um die Berechnung von Potenzen von Matrizen effizienter durchführen zu können. Auf diesen Algorithmus zur effizienten Berechnung der Potenzen wird an dieser Stelle nicht näher eingegangen.

Kapitel 4

Eigenschaften von $GL(2, Z_n)$ und $SL(2, Z_n)$

In diesem Anschnitt sollen besondere mathematische Eigenschaften der endlichen Gruppen $GL(2, Z_n)$ und $SL(2, Z_n)$ aufgezeigt werden, die für eine kryptografische Anwendung basierend auf dieser Gruppe eine Rolle spielen. Anschließend kann eine Bewertung der Sicherheit des RSA-Verfahrens basierend auf diesen Gruppen erfolgen.

Im ersten Teilabschnitt werden Eigenschaften von ähnlichen Matrizen aufgeführt. Im darauf folgenden Abschnitt wird die Gruppe $GL(2, Z_n)$, die Gruppe der 2×2-Matrizen, deren Determinante ungleich Null ist, betrachtet. Im zweiten Teilabschnitt ist die Gruppe $SL(2, Z_n)$, die Gruppe der Matrizen mit Determinante 1 Gegenstand der Betrachtung.

4.1 Ähnliche Matrizen

In diesem Abschnitt werden einige Eigenschaften von ähnlichen Matrizen behandelt, die in den folgenden Abschnitten benötigt werden.

4.1.1 Definition: Ähnliche Matrizen:

Zwei Matrizen A, B einer Matrixgruppe R heißen ähnlich, wenn ein $g \in R$ existiert, so dass $B = gAg^{-1}$ gilt.

4.1.2 Satz: Seien A und B ähnliche Matrizen, dann gelten folgende Aussagen:

1. $Det(A) = Det(B)$.
2. $Spur(A) = Spur(B)$.
3. Sind A und B Elemente einer endlichen Matrixgruppe, so gilt $ord(A) = ord(B)$.

Beweis:

1. Es gilt für alle Matrizen U, V:

$$Det(UV) = Det(U)Det(V)$$

Somit folgt:

$$\begin{aligned} Det(B) &= Det(gAg^{-1}) = Det(g)Det(A)Det(g^{-1}) \\ &= Det(g)Det(A)Det(g)^{-1} = Det(A) \end{aligned}$$

2. Sind A und B ähnliche Matrizen, dann gilt $B = gAg^{-1}$. Es folgt für das charakteristische Polynom: $Det(B - xI) = Det(gAg^{-1} - xI) = Det(gAg^{-1} - g(xI)g^{-1}) = Det(g(A - xI)g^{-1}) = Det(A - xI)$.

   Mit anderen Worten: A und B besitzen das gleiche charakteristische Polynom. Der zweithöchste Koeffizient des charakteristischen Polynoms einer Matrix A entspricht der negativen Spur der Matrix. Somit folgt $Spur(A) = Spur(B)$.

3. Sei d die Ordnung von B, dann gilt:
   $I = B^d = (gAg^{-1})^d = \underbrace{gAg^{-1}gAg^{-1} \cdot \ldots \cdot gAg^{-1}}_{d-Mal} = gA^dg^{-1}$.

   Es folgt: $g^{-1}Ig = I = A^d$ und somit $ord(A)|d$.

   Umgekehrt gilt aber auch $I = A^{ord(A)} = (g^{-1}Bg)^{ord(A)}$ und somit $d|ord(A)$. Zusammen folgt $d = ord(A)$.

□

4.2 Die Gruppe $GL(2, Z_n)$

4.2.1 Die Potenzfunktion in der Gruppe $GL(2, Z_n)$

In diesem Abschnitt werden besondere Potenzierungseigenschaften der Gruppe $GL(2, Z_n)$ behandelt. Es soll gezeigt werden, welche Ordnungen die Elemente der Gruppe $GL(2, Z_n)$ besitzen können.

Bemerkenswert ist, dass bei der Potenzierung einer Matrix aus der Gruppe $GL(2, Z_n)$ bestimmte Strukturen erhalten bleiben, wie der folgende Satz zeigt:

4.2.1.1 Satz: Sei n eine natürliche Zahl und sei $A := \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ eine Matrix aus $GL(2, Z_n)$, dann gilt für alle Matrizen $B := \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in GL(2, Z_n)$ mit $B \in < A >$:

$$b_{12}a_{21} \equiv_n a_{12}b_{21} \tag{4.1}$$

$$(a_{11} - a_{22})b_{12} \equiv_n (b_{11} - b_{22})a_{12} \tag{4.2}$$

Beweis:

Der Beweis erfolgt über Induktion über die Potenzen k von A. Für $k = 1$ ist $B := A^k \bmod n = A \bmod n$ und es gilt:

$$a_{12}a_{21} \equiv_n a_{12}a_{21}$$
$$(a_{11} - a_{22})a_{12} \equiv_n (a_{11} - a_{22})a_{12}$$

Angenommen, die Behauptung gilt für $B := A^k \bmod n = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$, dann gilt für A^{k+1}:

$$A^{k+1} := \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \equiv_n \begin{pmatrix} b_{11}a_{11} + b_{12}a_{21} & b_{11}a_{12} + b_{12}a_{22} \\ b_{21}a_{11} + b_{22}a_{21} & b_{21}a_{12} + b_{22}a_{22} \end{pmatrix}$$

Dann gilt:

$$\begin{aligned}
(b_{11}a_{12} + b_{12}a_{22})a_{21} &\equiv_n b_{11}a_{12}a_{21} + b_{12}a_{22}a_{21} \\
&\equiv_n b_{11}a_{12}a_{21} + (a_{11}b_{12} - (b_{11} - b_{22})a_{12})a_{21} \\
&\equiv_n b_{11}a_{12}a_{21} + a_{11}b_{12}a_{21} - b_{11}a_{12}a_{21} + b_{22}a_{12}a_{21} \\
&\equiv_n a_{11}b_{12}a_{21} + b_{22}a_{12}a_{21} \\
&\equiv_n a_{11}b_{21}a_{12} + b_{22}a_{12}a_{21} \\
&\equiv_n (b_{21}a_{11} + b_{22}a_{21})a_{12}
\end{aligned}$$

Somit ist Gleichung (4.1) bewiesen.

$$\begin{aligned}
(a_{11} - a_{22})(b_{11}a_{12} + b_{12}a_{22}) &\equiv_n a_{11}a_{12}b_{11} + a_{11}a_{22}b_{12} - a_{22}a_{12}b_{11} - a_{22}^2 b_{12} \\
&\equiv_n a_{11}a_{12}b_{11} + (a_{11} - a_{22})b_{12}a_{22} - a_{22}a_{12}b_{11} \\
&\equiv_n a_{11}a_{12}b_{11} + (b_{11} - b_{22})a_{12}a_{22} - a_{22}a_{12}b_{11} \\
&\equiv_n a_{11}a_{12}b_{11} - b_{22}a_{12}a_{22} \\
&\equiv_n a_{11}a_{12}b_{11} + a_{12}b_{12}a_{21} - a_{12}b_{12}a_{21} - b_{22}a_{12}a_{22} \\
&\equiv_n a_{11}a_{12}b_{11} + a_{12}b_{12}a_{21} - a_{12}b_{21}a_{12} - b_{22}a_{12}a_{22} \\
&\equiv_n (a_{11}b_{11} + b_{12}a_{21} - a_{12}b_{21} - b_{22}a_{22})a_{12}
\end{aligned}$$

Somit ist Gleichung (4.2) bewiesen. □

4.2.1.2 Korollar: Sei $A := \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ eine Matrix aus $GL(2, Z_n)$ mit $a_{12} \in Z_n^*$. Dann gilt für alle Matrizen $B := \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \in GL(2, Z_n)$ mit $B \in < A >$ und $b_{12} \in Z_n^*$:

$$\begin{aligned}
a_{12}^{-1}a_{21} &\equiv_n b_{12}^{-1}b_{21} \\
(a_{11} - a_{22})a_{12}^{-1} &\equiv_n (b_{11} - b_{22})b_{12}^{-1}
\end{aligned}$$

Mit anderen Worten: Für jede Matrix $B \in < A >$ sind die Werte $K_1 := b_{12}^{-1} b_{21} \bmod n$ und $K_2 := (b_{11} - b_{22}) b_{12}^{-1} \bmod n$ konstant.

Im Folgenden werden diese beiden Konstanten immer mit K_1 bzw. K_2 bezeichnet.

Beweis:

Der Beweis folgt direkt aus dem vorherigen Satz unter der Voraussetzung, dass b_{12}^{-1} und a_{12}^{-1} in Z_n^* existiert. □

Die beiden Konstanten sind jedoch kein hinreichendes Kriterium, um die von einer Matrix A erzeugten Matrizen zu identifizieren. Dies wird durch folgendes Beispiel verdeutlicht.

4.2.1.3 Beispiel: Seien $n = 23$, $A := \begin{pmatrix} 5 & 3 \\ 3 & 2 \end{pmatrix}$ und $B := \begin{pmatrix} 13 & 8 \\ 8 & 5 \end{pmatrix}$. Dann gilt:

$$\begin{aligned} K_1 &\equiv_n 3 \cdot 3^{-1} \equiv_n 8 \cdot 8^{-1} \equiv_n 1 \\ K_2 &\equiv_n (5-2) \cdot 3^{-1} \equiv_n 1 \equiv_n (13-5) \cdot 8^{-1} \end{aligned}$$

Aber es gilt weder $A \in < B >$ noch $B \in < A >$, denn es gilt $ord(A) = 12$ und $ord(B) = 8$. Wäre $A \in < B >$, so müsste nach dem Satz von Lagrange $ord(A) | ord(B)$ gelten, ebenso müsste $ord(B) | ord(A)$ gelten für $B \in < A >$.

Der folgende Satz zeigt, dass die Potenz einer Matrix durch eine Rekursionsformel berechnet werden kann.

4.2.1.4 Satz: Sei $A := \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ eine Matrix aus $GL(2, Z_n)$. Dann gilt für jede Matrix $B := A^k \bmod n$ mit $k \geq 2$:

$$B \equiv_n A^k \equiv_n Spur(A) A^{k-1} - Det(A) A^{k-2}$$

Beweis:

Der Beweis erfolgt über Induktion über k. Für $k = 1, 2, 3$ gilt:

$$A \equiv_n \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$$

$$
\begin{aligned}
A^2 &\equiv_n \begin{pmatrix} a_{11}^2 + a_{12}a_{21} & a_{12}(a_{11} + a_{22}) \\ a_{21}(a_{11} + a_{22}) & a_{22}^2 + a_{12}a_{21} \end{pmatrix} \\
&\equiv_n \begin{pmatrix} a_{11}^2 + a_{11}a_{22} - Det(A) & a_{12}(a_{11} + a_{22}) \\ a_{21}(a_{11} + a_{22}) & a_{22}^2 + a_{11}a_{22} - Det(A) \end{pmatrix} \\
A^3 &\equiv_n \begin{pmatrix} a_{11}^3 + 2a_{11}a_{12}a_{21} + a_{22}a_{12}a_{21} & a_{12}(a_{11}^2 + a_{11}a_{22} + a_{12}a_{21} + a_{22}^2) \\ a_{21}(a_{11}^2 + a_{11}a_{22} + a_{12}a_{21} + a_{22}^2) & a_{22}^3 + 2a_{22}a_{12}a_{21} + a_{11}a_{12}a_{21} \end{pmatrix} \\
&\equiv_n \begin{pmatrix} a_{11}^3 + (a_{11}a_{22} - Det(A))(2a_{11} + a_{22}) & a_{12}(a_{11}^2 + 2a_{11}a_{22} + a_{22}^2 - Det(A)) \\ a_{21}(a_{11}^2 + 2a_{11}a_{22} + a_{22}^2 - Det(A)) & a_{22}^3 + (a_{11}a_{22} - Det(A))(2a_{22} + a_{11}) \end{pmatrix}
\end{aligned}
$$

Bezeichne im Folgenden $a_{i,j}^{(k)}$ den Eintrag der $i-ten$ Zeile und $j-ten$ Spalte der Matrix A^k. Dann folgt:

$$
\begin{aligned}
a_{11}^{(3)} &\equiv_n a_{11}^3 + 2a_{11}a_{12}a_{21} + a_{22}a_{12}a_{21} \\
&\equiv_n a_{11}(a_{11}^2 + a_{12}a_{21}) + a_{22}(a_{11}^2 + a_{12}a_{21}) \\
&\quad -a_{22}(a_{11}^2 + a_{12}a_{21}) + a_{11}a_{12}a_{21} + a_{22}a_{12}a_{21} \\
&\equiv_n Spur(A)(a_{11}^2 + a_{12}a_{21}) - a_{22}a_{11}^2 + a_{11}a_{12}a_{21} \\
&\equiv_n Spur(A)(a_{11}^{(2)}) - a_{11}Det(A)
\end{aligned}
$$

$$
\begin{aligned}
a_{12}^{(3)} &\equiv_n a_{12}(a_{11}^2 + a_{11}a_{22} + a_{12}a_{21} + a_{22}^2) \\
&\equiv_n a_{12}(a_{11}^2 + 2a_{11}a_{22} + a_{22}^2 - Det(A)) \\
&\equiv_n (a_{11} + a_{22})^2 a_{12} - Det(A)a_{12} \\
&\equiv_n Spur(A)(a_{12}^{(2)}) - Det(A)a_{12}
\end{aligned}
$$

$$
\begin{aligned}
a_{21}^{(3)} &\equiv_n a_{21}(a_{11}^2 + a_{11}a_{22} + a_{12}a_{21} + a_{22}^2) \\
&\equiv_n a_{21}(a_{11}^2 + 2a_{11}a_{22} + a_{22}^2 - Det(A)) \\
&\equiv_n (a_{11} + a_{22})^2 a_{21} - Det(A)a_{21} \\
&\equiv_n Spur(A)(a_{21}^{(2)}) - Det(A)a_{21}
\end{aligned}
$$

$$\begin{aligned} a_{22}^{(3)} &\equiv_n a_{22}^3 + 2a_{22}a_{12}a_{21} + a_{11}a_{12}a_{21} \\ &\equiv_n a_{22}(a_{22}^2 + a_{12}a_{21}) + a_{11}(a_{22}^2 + a_{12}a_{21}) \\ &\quad -a_{11}(a_{22}^2 + a_{12}a_{21}) + a_{22}a_{12}a_{21} + a_{11}a_{12}a_{21} \\ &\equiv_n Spur(A)(a_{22}^2 + a_{12}a_{21}) - a_{11}a_{22}^2 + a_{22}a_{12}a_{21} \\ &\equiv_n Spur(A)(a_{22}^{(2)}) - a_{22}Det(A) \end{aligned}$$

Das heißt, die Behauptung gilt für $k = 3$.

Sei des Weiteren $B := A^{k-2} \bmod n = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$, dann gilt:

$$\begin{aligned} BA \equiv_n A^{k-1} &\equiv_n \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \equiv_n \begin{pmatrix} b_{11}a_{11} + b_{12}a_{21} & b_{11}a_{12} + b_{12}a_{22} \\ b_{21}a_{11} + b_{22}a_{21} & b_{21}a_{12} + b_{22}a_{22} \end{pmatrix} \\ BA^2 \equiv_n A^k &\equiv_n \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \begin{pmatrix} a_{11}^2 + a_{11}a_{22} - Det(A) & a_{12}(a_{11} + a_{22}) \\ a_{21}(a_{11} + a_{22}) & a_{22}^2 + a_{11}a_{22} - Det(A) \end{pmatrix} \\ &\equiv_n \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \end{aligned}$$

mit

$$\begin{aligned} c_{11} &\equiv_n b_{11}(a_{11}^2 + a_{11}a_{22} - Det(A)) + b_{12}(a_{21}(a_{11} + a_{22})) \\ c_{12} &\equiv_n b_{11}(a_{12}(a_{11} + a_{22})) + b_{12}(a_{22}^2 + a_{11}a_{22} - Det(A)) \\ c_{21} &\equiv_n b_{21}(a_{11}^2 + a_{11}a_{22} - Det(A)) + b_{22}(a_{21}(a_{11} + a_{22})) \\ c_{22} &\equiv_n b_{21}(a_{12}(a_{11} + a_{22})) + b_{22}(a_{22}^2 + a_{11}a_{22} - Det(A)) \end{aligned}$$

Angenommen, die Behauptung gilt für alle A^k bis zu einem $k \geq 3$, dann folgt für $k+1$:

$A^{k+1} \equiv_n BA^3 \equiv_n$

$$\begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \begin{pmatrix} a_{11}^3 + (a_{11}a_{22} - Det(A))(2a_{11} + a_{22}) & a_{12}(a_{11}^2 + 2a_{11}a_{22} + a_{22}^2 - Det(A)) \\ a_{21}(a_{11}^2 + 2a_{11}a_{22} + a_{22}^2 - Det(A)) & a_{22}^3 + (a_{11}a_{22} - Det(A))(2a_{22} + a_{11}) \end{pmatrix}$$

$$\equiv_n \begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix}$$

mit

$$d_{11} \equiv_n b_{11}(a_{11}^3 + (a_{11}a_{22} - Det(A))(2a_{11} + a_{22})) + b_{12}(a_{21}(a_{11}^2 + 2a_{11}a_{22} + a_{22}^2 - Det(A)))$$

$$d_{12} \equiv_n b_{11}(a_{12}(a_{11}^2 + 2a_{11}a_{22} + a_{22}^2 - Det(A))) + b_{12}(a_{22}^3 + (a_{11}a_{22} - Det(A))(2a_{22} + a_{11}))$$
$$d_{21} \equiv_n b_{21}(a_{11}^3 + (a_{11}a_{22} - Det(A))(2a_{11} + a_{22})) + b_{22}(a_{21}(a_{11}^2 + 2a_{11}a_{22} + a_{22}^2 - Det(A)))$$
$$d_{22} \equiv_n b_{21}(a_{12}(a_{11}^2 + 2a_{11}a_{22} + a_{22}^2 - Det(A))) + b_{22}(a_{22}^3 + (a_{11}a_{22} - Det(A))(2a_{22} + a_{11}))$$

Es folgt:

$$\begin{aligned}
a_{11}^{(k+1)} \equiv_n \; & d_{11} \equiv_n b_{11}(a_{11}^3 + (a_{11}a_{22} - Det(A))(2a_{11} + a_{22})) \\
& + b_{12}(a_{21}(a_{11}^2 + 2a_{11}a_{22} + a_{22}^2 - Det(A))) \\
\equiv_n \; & a_{11}(b_{11}(a_{11}^2 + a_{11}a_{22} - Det(A)) + (a_{11} + a_{22})(a_{11}a_{22} \\
& - Det(A))b_{11} + a_{11}(b_{12}(a_{21}(a_{11} + a_{22}))) + b_{12}a_{21}(a_{11}a_{22} \\
& + a_{22}^2 - Det(A)) \\
\equiv_n \; & a_{11}(b_{11}(a_{11}^2 + a_{11}a_{22} - Det(A)) + a_{22}(a_{11}a_{22} - Det(A))b_{11} \\
& + a_{22}b_{11}(a_{11}^2 - Det(A)b_{11}a_{11} + a_{11}(b_{12}(a_{21}(a_{11} + a_{22}))) \\
& + a_{22}(b_{12}(a_{21}(a_{11} + a_{22}))) - Det(A)(b_{12}a_{21}) \\
\equiv_n \; & Spur(A)((b_{11}(a_{11}^2 + a_{11}a_{22} - Det(A)) + b_{12}(a_{21}(a_{11} + a_{22}))) \\
& - Det(A)(b_{11}a_{11} + b_{12}a_{21}) \\
\equiv_n \; & Spur(A)a_{11}^{(k)} - Det(A)a_{11}^{(k-1)}
\end{aligned}$$

$$\begin{aligned}
a_{12}^{(k+1)} \equiv_n \; & d_{12} \equiv_n b_{11}(a_{12}(a_{11}^2 + 2a_{11}a_{22} + a_{22}^2 - Det(A))) \\
& + b_{12}(a_{22}^3 + (a_{11}a_{22} - Det(A))(2a_{22} + a_{11})) \\
\equiv_n \; & (a_{11} + a_{22})(b_{11}a_{12}(a_{11} + a_{12})) - Det(A)b_{11}a_{12} \\
& + b_{12}a_{22}^3 + 2b_{12}a_{11}a_{22}^2 + b_{12}a_{11}^2a_{22} \\
& - Det(A)(2b_{12}a_{22} + b_{12}a_{11}) \\
\equiv_n \; & (a_{11} + a_{22})(b_{11}a_{12}(a_{11} + a_{12}) + b_{12}a_{22}(a_{11} + a_{22})^2 \\
& - Det(A)(b_{11}a_{12} + 2b_{12}a_{22} \\
& + b_{12}a_{11}) \\
\equiv_n \; & (a_{11} + a_{22})^2(b_{11}a_{12} + b_{12}a_{22}) - Det(A)(b_{11}a_{12} \\
& + b_{12}a_{22}) - Det(A)(b_{12}a_{22} + b_{12}a_{11}) \\
\equiv_n \; & Spur(A)a_{12}^{(k-1)} - Det(A)a_{12}^{(k-2)}
\end{aligned}$$

$$
\begin{aligned}
a_{21}^{(k+1)} &\equiv_n d_{21} \equiv_n b_{22}(a_{21}(a_{22}^2 + 2a_{11}a_{22} + a_{11}^2 - Det(A))) \\
&\quad + b_{21}(a_{11}^3 + (a_{11}a_{22} - Det(A))(2a_{11} + a_{22})) \\
&\equiv_n (a_{11} + a_{22})(b_{22}a_{21}(a_{22} + a_{21})) - Det(A)b_{22}a_{21} + b_{21}a_{11}^3 \\
&\quad + 2b_{21}a_{22}a_{11}^2 + b_{21}a_{22}^2a_{11} - Det(A)(2b_{21}a_{11} + b_{21}a_{22}) \\
&\equiv_n (a_{11} + a_{22})(b_{22}a_{21}(a_{22} + a_{21}) + b_{21}a11(a_{11} + a_{22})^2 \\
&\quad - Det(A)(b_{22}a_{21} + 2b_{21}a_{11} + b_{21}a_{22}) \\
&\equiv_n (a_{11} + a_{22})^2(b_{22}a_{21} + b_{21}a11) - Det(A)(b_{22}a_{21} \\
&\quad + b_{21}a_{11}) - Det(A)(b_{21}a_{11} + b_{21}a_{22}) \\
&\equiv_n Spur(A)a_{21}^{(k-1)} - Det(A)a_{21}^{(k-2)}
\end{aligned}
$$

$$
\begin{aligned}
a_{22}^{(k+1)} &\equiv_n d_{22} \equiv_n b_{22}(a_{22}^3 + (a_{11}a_{22} - Det(A))(2a_{22} + a_{11})) \\
&\quad + b_{21}(a_{12}(a_{22}^2 + 2a_{11}a_{22} + a_{11}^2 - Det(A))) \\
&\equiv_n a_{22}(b_{22}(a_{22}^2 + a_{11}a_{22} - Det(A)) + (a_{11} + a_{22})(a_{11}a_{22} \\
&\quad - Det(A))b_{22} + a_{22}(b_{21}(a_{12}(a_{11} + a_{22}))) + b_{21}a_{12}(a_{11}a_{22} \\
&\quad + a_{11}^2 - Det(A)) \\
&\equiv_n a_{22}(b_{22}(a_{22}^2 + a_{11}a_{22} - Det(A)) + a_{11}(a_{11}a_{22} - Det(A))b_{22} \\
&\quad + a_{11}b_{22}(a_{22}^2 - Det(A)b_{22}a_{22} + a_{22}(b_{21}(a_{12}(a_{11} + a_{22}))) \\
&\quad + a_{11}(b_{21}(a_{12}(a_{11} + a_{22}))) - Det(A)(b_{21}a_{12}) \\
&\equiv_n Spur(A)((b_{22}(a_{22}^2 + a_{11}a_{22} - Det(A)) + b_{21}(a_{12}(a_{11} + a_{22}))) \\
&\quad - Det(A)(b_{22}a_{22} + b_{21}a_{12}) \\
&\equiv_n Spur(A)a_{22}^{(k)} - Det(A)a_{22}^{(k-1)}
\end{aligned}
$$

Also gilt: $A^k \equiv_n Spur(A)A^{k-1} - Det(A)A^{k-2}$ □

Aus diesem Satz kann der folgende Satz leicht gefolgert werden:

4.2.1.5 Satz: Sei $A := \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ eine Matrix aus $GL(2, Z_n)$. Dann gilt für jede Matrix $B := A^k \bmod n$ mit $k \geq 3$:

$$Spur(B) \equiv_n Spur(A^k) \equiv_n Spur(A)Spur(A^{k-1}) - Det(A)Spur(A^{k-2})$$

Beweis:
Nach Satz (4.2.1.4) gilt:
$a_{i,j}^{(k)} \equiv_n Spur(A)a_{i,j}^{(k-1)} - Det(A)a_{i,j}^{(k-2)}$. Es folgt:

$$\begin{aligned} Spur(A^k) &\equiv_n \sum_{s=1}^{2} a_{ss}^{(k)} \equiv_n \sum_{s=1}^{2}(Spur(A)a_{ss}^{(k-1)} - Det(A)a_{ss}^{(k-2)}) \\ &\equiv_n Spur(A)\sum_{s=1}^{2}(a_{ss}^{(k-1)}) - Det(A)\sum_{s=1}^{2}(a_{ss}^{(k-2)}) \\ &\equiv_n Spur(A)Spur(A^{k-1}) - Det(A)Spur(A^{k-2}) \end{aligned}$$

□

Die obige Rekursionsformel für die Potenzen einer Matrix lässt sich wie folgt auf eine Funktionenrekursionsformel verallgemeinern:

$$w(x)_k := p(x)w(x)_{k-1} + q(x)w(x)_{k-2}$$

mit $p(x) = Spur(A)$, $q(x) = -Det(A)$ und $w(x)_k = A^k$.

Funktionen, die einer solche Rekursionsformel genügen, werden in (Hora94) und (Hora96) eingehend behandelt. Setzt man $\alpha(x) = \frac{p(x)+\sqrt{p(x)^2+4q(x)}}{2}$ und $\beta(x) = \frac{p(x)-\sqrt{p(x)^2+4q(x)}}{2}$, so gibt es nach (Hora94) ein Paar von generalisierten Funktionen:

$$W_k(x) = \frac{\alpha(x)^k - \beta(x)^k}{\alpha(x) - \beta(x)} \quad (4.3)$$

$$w_k(x) = \alpha(x)^k + \beta(x)^k \quad (4.4)$$

Wie man leicht sieht, handelt es sich bei diesen generalisierten Funktionen um Lucas-Funktionen, die bereits in Abschnitt 2.3.3 verwendet wurden. Diese Funktionen genügen ebenfalls der Rekursionsformel. Setzt man $p(x) = Spur(A)$ und $q(x) = -Det(A)$ für eine beliebige Matrix $A \in GL(2, Z_n)$, so gilt der folgende Satz:

4.2.1.6 Satz: Sei A eine Matrix aus $GL(2, Z_n)$ mit $ggT(a_{12}, n) = 1$ und $ggT(a_{21}, n) = 1$.
Dann gilt für jede Matrix $B \equiv_n A^k$:

$$Spur(B) \equiv_n \alpha^k + \beta^k$$

$$\begin{aligned} b_{12}a_{12}^{-1} &\equiv_n a_{12}^{(k)}a_{12}^{-1} \equiv_n \frac{\alpha^k - \beta^k}{\alpha - \beta} \\ b_{21}a_{21}^{-1} &\equiv_n a_{21}^{(k)}a_{21}^{-1} \equiv_n \frac{\alpha^k - \beta^k}{\alpha - \beta} \end{aligned}$$

Dabei gilt:

$$\alpha := \frac{Spur(A) + \sqrt{(Spur(A))^2 - 4Det(A)}}{2} \bmod n$$
$$\beta := \frac{Spur(A) - \sqrt{(Spur(A))^2 - 4Det(A)}}{2} \bmod n$$

4.2.1.7 Bemerkung: Die beiden oben definierten Elemente α und β müssen nicht in der Gruppe Z_n liegen. Sie liegen genau dann in Z_n, wenn $(Spur(A))^2 - 4Det(A)$ ein quadratischer Rest modulo n ist, oder $(Spur(A))^2 - 4Det(A) \equiv_n 0$ gilt. Sind α und β Elemente aus Z_n, so ist das Berechnen von $\alpha^k + \beta^k$ in Z_n^* unproblematisch.

Sind α und β nicht in Z_n enthalten, ist also $(Spur(A))^2 - 4Det(A) \in Z_n^*$ ein quadratischer Nichtrest in Z_n^*, so geht man zur Berechnung von α^k und β^k in den Erweiterungsring von Z_n über, der die Nullstellen der Gleichung $X^2 \equiv_n (Spur(A))^2 - 4Det(A)$ enthält.

Um α^k bzw. β^k modulo n zu berechnen, geht man vor wie bei komplexen Zahlen: α hat die Form $u + \sqrt{v}$ mit $u, v \in Z_n$, so dass bei Potenzierung von α wieder ein Element in der Form $u'u + v'\sqrt{v}$ mit $u', v' \in Z_n$ entsteht.

Da $\beta \equiv_n u - \sqrt{(}v)$ gilt, folgt, dass für alle $k \in Z$ gilt: $(\alpha^k + \beta^k) \in Z_n$.

Beweis:
Es gilt:

$$\begin{aligned} W_0(x) &\equiv_n 0 \\ W_1(x) &\equiv_n 1 \\ W_2(x) &\equiv_n \frac{\alpha(x)^2 - \beta(x)^2}{\alpha(x) - \beta(x)} \equiv_n \alpha(x) + \beta(x) \equiv_n Spur(A) \\ w_0(x) &\equiv_n 2 \\ w_1(x) &\equiv_n \alpha(x) + \beta(x) \equiv_n Spur(A) \end{aligned}$$

$$\begin{aligned} w_2(x) &\equiv_n \alpha(x)^2 + \beta(x)^2 \\ &\equiv_n \frac{(Spur(A))^2 + 2Spur(A)\sqrt{(Spur(A))^2 - 4Det(A)}}{4} \\ &\quad + \frac{(Spur(A))^2 - 4Det(A) + (Spur(A))^2}{4} \\ &\quad + \frac{-2Spur(A)\sqrt{(Spur(A))^2 - 4Det(A)}}{4} \\ &\quad \frac{(Spur(A))^2 - 4Det(A)}{4} \\ &\equiv_n (Spur(A))^2 - 2Det(A) \end{aligned}$$

Wie leicht zu überprüfen ist, gilt $w_i(x) \equiv_n Spur(A^i)$ und $W_i(x) \equiv_n a_{12}^{(i)} a_{12}^{-1}$ (für $ggT(a_{12}, n) = 1$) für $i = 0, 1, 2$. Da die Funktionen die gleichen Rekursionsformeln erfüllen wie in Satz (4.2.1.4) und Satz (4.2.1.5), folgt, dass $w_i(x) \equiv_n Spur(A^i)$ und $W_i(x) \equiv_n a_{12}^{(i)} a_{12}^{-1}$ (für $ggT(a_{12}, n) = 1$) für alle $i \in Z$ gilt. □

4.2.2 Zyklische Untergruppen in $GL(2, Z_n)$

Im Folgenden werden die möglichen Ordnungen der von einem Element aus $GL(2, Z_n)$ erzeugten zyklischen Untergruppe behandelt. Dabei werden zunächst nur Matrizen über Z_p betrachtet, wobei p eine Primzahl ist. Die Aussagen können dann leicht mit Hilfe des Chinesischen Restsatzes auf Matrizen über Z_n erweitert werden.

4.2.2.1 Satz: Es sei p eine Primzahl. Jede diagonalisierbare Matrix $A \in GL(2, Z_p)$ besitzt eine Ordnung, die $p - 1$ teilt.

Beweis:

Sei $A \in GL(2, Z_p)$ eine diagonalisierbare Matrix, d.h. es gibt eine Matrix $B := \begin{pmatrix} b_{11} & 0 \\ 0 & b_{22} \end{pmatrix} \in GL(2, Z_n)$ mit $B \equiv_p gAg^{-1}$ für ein $g \in GL(2, Z_p)$.

Für B gilt:

$$B^k \equiv_p \begin{pmatrix} b_{11}^k & 0 \\ 0 & b_{22}^k \end{pmatrix}$$

Also gilt:

$$B^{p-1} \equiv_p \begin{pmatrix} b_{11}^{p-1} & 0 \\ 0 & b_{22}^{p-1} \end{pmatrix} \equiv_p \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

B und A haben nach Satz (4.1.2) die gleiche Ordnung, also gilt $ord(A)|(p-1)$. □

Der vorherige Satz sagt nur aus, dass es Matrizen gibt, deren Ordnung die Zahl $p-1$ teilt. Das folgende Korollar zeigt darüber hinaus, dass es Matrizen gibt, die genau die Ordnung $p-1$ besitzen.

4.2.2.2 Korollar: Es sei p eine Primzahl. Es gibt Matrizen $\in GL(2, Z_p)$, die die Ordnung $p-1$ besitzen.

Beweis:

Es seien a, b Elemente aus Z_p^* mit $ord(a) = ord(b) = p-1$. (Es existieren Elemente der Ordnung $p-1$ in Z_p^*, da Z_p^* eine zyklische Gruppe der Ordnung $p-1$ ist.) Dann ist $\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ eine Matrix aus $GL(2, Z_p)$, die die Ordnung $p-1$ besitzt. □

4.2.2.3 Korollar: Seien p, q Primzahlen und sei $n := pq$. Dann gilt: Jede diagonalisierbare Matrix $A \in GL(2, Z_n)$ besitzt eine Ordnung, die $\varphi(n)$ teilt.

Beweis:

Die Behauptung folgt direkt aus Satz (4.2.2.1) zusammen mit dem Chinesischen Restsatz für Matrizen (Satz (3.2.1.7)).

4.2.2.4 Satz: Jede Matrix $A \in GL(2, Z_p)$, deren Eigenwerte in Z_p^* liegen und verschieden sind, besitzt eine Ordnung, die $(p-1)$ teilt.

Beweis: Eine Matrix, deren Eigenwerte verschieden sind und in Z_p^* liegen, ist in $GL(2, Z_p)$ diagonalisierbar. Nach Satz (4.2.2.1) besitzt jede diagonalisierbare Matrix eine Ordnung, die $p-1$ teilt. □

4.2.2.5 Satz: Es sei p eine Primzahl. Jede Matrix $A \in GL(2, Z_p)$, die zwei gleiche Eigenwerte $\lambda \in Z_p^*$ besitzt, hat eine Ordnung, die $ord(\lambda)p$ teilt.

Beweis:

Da die Eigenwerte von $A \in GL(2, Z_p)$ in Z_p^* liegen, ist A eine triagonalisierbare Matrix. D.h. es gibt eine Matrix
$B := \begin{pmatrix} b_{11} & b_{12} \\ 0 & b_{22} \end{pmatrix} \in GL(2, Z_n)$ mit $B \equiv_p gAg^{-1}$ für ein $g \in GL(2, Z_p)$. B und A haben nach Satz (4.1.2) die gleiche Ordnung.

Es gibt ein $c \in Z_p$, so dass für B gilt: $B^k \equiv_p \begin{pmatrix} b_{11}^k & c \\ 0 & b_{22}^k \end{pmatrix}$

Da bei Dreiecksmatrizen die Eigenwerte auf der Hauptdiagonalen liegen, folgt $\lambda := b_{11} = b_{22} \bmod p$.

Dann ist also: $B \equiv_p \begin{pmatrix} \lambda & b_{12} \\ 0 & \lambda \end{pmatrix}$

Behauptung: Für eine solche Matrix gilt:

$$B^k \equiv_p \begin{pmatrix} \lambda^k & b_{12}(k\lambda^{k-1}) \\ 0 & \lambda^k \end{pmatrix}$$

Diese Behauptung lässt sich leicht durch Induktion beweisen:

Für $k = 1$ gilt:

$$B \equiv_p \begin{pmatrix} \lambda & b_{12} \\ 0 & \lambda \end{pmatrix} \equiv_p \begin{pmatrix} \lambda & b_{12}(1 \cdot \lambda^0) \\ 0 & \lambda \end{pmatrix}$$

Angenommen, die Behauptung gilt für alle $\ell \leq k$, dann folgt:

$$\begin{aligned} B^{k+1} \equiv_p BB^k &\equiv_p \begin{pmatrix} \lambda & b_{12} \\ 0 & \lambda \end{pmatrix} \begin{pmatrix} \lambda^k & b_{12}(k\lambda^{k-1}) \\ 0 & \lambda^k \end{pmatrix} \equiv_p \begin{pmatrix} \lambda^{k+1} & \lambda b_{12}(k\lambda^{k-1}) + b_{12}\lambda^k \\ 0 & \lambda^{k+1} \end{pmatrix} \\ &\equiv_p \begin{pmatrix} \lambda^{k+1} & b_{12}((k+1)\lambda^k) \\ 0 & \lambda^{k+1} \end{pmatrix} \end{aligned}$$

Somit folgt für $k = ord(\lambda)p$:

$$B^{ord(\lambda)p} \equiv_p \begin{pmatrix} \lambda^{ord(\lambda)p} & b_{12}((ord(\lambda)p)\lambda^{(pord(\lambda)-1)}) \\ 0 & \lambda^{ord(\lambda)p} \end{pmatrix} \equiv_p \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

□

4.2.2.6 Satz: Seien p, q Primzahlen und sei $n = pq$, dann gilt: Jede triagonalisierbare Matrix $A \in GL(2, Z_n)$ besitzt eine Ordnung, die $\varphi(n)n$ teilt.

Beweis:

Die Behauptung folgt direkt aus Satz (4.2.2.4) und Satz (4.2.2.5) mit Hilfe des Chinesischen Restsatzes für Matrizen (Satz (3.2.1.7)).

4.2.2.7 Satz: Es sei p eine Primzahl und $A \in GL(2, Z_p)$. A besitzt genau dann eine Ordnung, die $p-1$ teilt, wenn $(Spur(A))^2 - 4Det(A)$ ein quadratischer Rest in Z_p^* ist.

Beweis:

"$\Leftarrow$" Ist $(Spur(A))^2 - 4Det(A)$ ein quadratischer Rest, so ist A diagonalisierbar und nach Satz (4.2.2.1) gilt $ord(A)|p-1$.

"$\Rightarrow$" Angenommen, es gilt $ord(A)|p-1$. Dann gilt $A^p \equiv_p A$. Somit ist $Spur(A^p) \equiv_p Spur(A)$ und $a_{12}^{(p)} \equiv_p a_{12}$ sowie $a_{21}^{(p)} \equiv_p a_{21}$. Somit gilt nach Satz (4.2.1.6):

$$\begin{aligned} 1 &\equiv_p a_{12}^{(p)} a_{12}^{-1} \equiv_p \frac{\alpha^p - \beta^p}{\alpha - \beta} \\ &\equiv_p \frac{(\sqrt{(Spur(A))^2 - 4Det(A)})^p}{\sqrt{(Spur(A))^2 - 4Det(A)}} \\ &\equiv_p ((Spur(A))^2 - 4Det(A))^{\frac{p-1}{2}} \end{aligned}$$

Da $((Spur(A))^2 - 4Det(A))^{\frac{p-1}{2}} \equiv_p 1$ gilt, muss $(Spur(A))^2 - 4Det(A)$ ein quadratischer Rest in Z_p^* sein. □

4.2.2.8 Satz: Es sei p eine Primzahl und $A \in GL(2, Z_p) \backslash \{\pm I\}$. A besitzt genau dann eine Ordnung, die von p geteilt wird, wenn $(Spur(A))^2 - 4Det(A) \equiv_p 0$ gilt.

Beweis:

"$\Rightarrow$" Sei A eine Matrix aus $GL(2, Z_p)$, mit $p|ord(A)$. Dann gilt nach Satz (4.2.1.6) für A^p:

$$Spur(A^p) \equiv_p \alpha^p + \beta^p$$

$$\begin{aligned} a_{12}^{(p)} a_{12}^{-1} &\equiv_p \frac{\alpha^p - \beta^p}{\alpha - \beta} \\ a_{21}^{(p)} a_{21}^{-1} &\equiv_p \frac{\alpha^p - \beta^p}{\alpha - \beta} \end{aligned}$$

Dabei gilt $\alpha \equiv_p \frac{Spur(A)+\sqrt{(Spur(A))^2-4Det(A)}}{2}$ und $\beta \equiv_p \frac{Spur(A)-\sqrt{(Spur(A))^2-4Det(A)}}{2}$
Es folgt:

$$\begin{aligned} \alpha^p &\equiv_p \left(\frac{Spur(A) + \sqrt{(Spur(A))^2 - 4Det(A)}}{2}\right)^p \\ &\equiv_p \frac{(Spur(A))^p + (\sqrt{(Spur(A))^2 - 4Det(A)})^p}{2^p} \\ &\equiv_p \frac{Spur(A) + (\sqrt{(Spur(A))^2 - 4Det(A)})^p}{2} \end{aligned}$$

$$\begin{aligned} \beta^p &\equiv_p \left(\frac{Spur(A) - \sqrt{(Spur(A))^2 - 4Det(A)}}{2}\right)^p \\ &\equiv_p \frac{(Spur(A))^p - (\sqrt{(Spur(A))^2 - 4Det(A)})^p}{2^p} \\ &\equiv_p \frac{Spur(A) - (\sqrt{(Spur(A))^2 - 4Det(A)})^p}{2} \end{aligned}$$

Also gilt $Spur(A^p) \equiv_p \alpha^p + \beta^p \equiv_p Spur(A)$.
Des Weiteren gilt:

$$\begin{aligned} a_{12}^{(p)} a_{12}^{-1} &\equiv_p \frac{\alpha^p - \beta^p}{\alpha - \beta} \equiv_p \frac{(\sqrt{(Spur(A))^2 - 4Det(A)})^p}{\sqrt{(Spur(A))^2 - 4Det(A)}} \\ &\equiv_p ((Spur(A))^2 - 4)^{\frac{p-1}{2}} \end{aligned}$$

Angenommen, es gilt $(Spur(A))^2 \not\equiv_p 4Det(A)$, dann folgt:

$$((Spur(A))^2 - 4Det(A))^{\frac{p-1}{2}} \equiv_p \pm 1$$

Des Weiteren gilt: $Det(A^p) \equiv_p Det(A)^p \equiv_p Det(A)$
Mit anderen Worten:

$$a_{11}a_{22} - a_{12}a_{21} \equiv_p a_{11}^{(p)} a_{22}^{(p)} - a_{12}^{(p)} a_{21}^{(p)}$$

Zusammen folgt:

$$a_{11}a_{22} \equiv_p a_{11}^{(p)}a_{22}^{(p)}$$

Da $Spur(A^p) \equiv_p a_{11}^{(p)} + a_{22}^{(p)} \equiv_p a_{11} + a_{22} \equiv_p Spur(A)$ gilt, folgt:

$$\begin{aligned} a_{11}(a_{11}^{(p)} + a_{22}^{(p)} - a_{11}) \equiv_p a_{11}^{(p)}a_{22}^{(p)} &\Rightarrow a_{11}^2 - a_{11}(a_{11}^{(p)} + a_{22}^{(p)}) + a_{11}^{(p)}a_{22}^{(p)} \equiv_p 0 \\ &\Rightarrow (a_{11} - a_{11}^{(p)})(a_{11} - a_{22}^{(p)}) \equiv_p 0 \\ &\Rightarrow a_{11} \equiv_p a_{11}^{(p)} \vee a_{11} \equiv_p a_{22}^{(p)} \end{aligned}$$

Angenommen, es gilt $a_{11} \equiv_p a_{11}^{(p)}$, dann folgt $a_{22} \equiv_p a_{22}^{(p)}$, und zusammen mit Satz (4.2.1.1) folgt auch $a_{12} \equiv_p a_{12}^{(p)}$ und $a_{21} \equiv_p a_{21}^{(p)}$. Mit anderen Worten: $A^p \equiv_p A$, und somit wäre $ord(A) = p - 1$. Dies wäre aber ein Widerspruch zu $p|ord(A)$.

Angenommen, es gilt $a_{11} \equiv_p a_{22}^{(p)}$, dann folgt $a_{22} \equiv_p a_{11}^{(p)}$, und zusammen mit Satz (4.2.1.1) folgt auch $a_{12} \equiv_p -a_{12}^{(p)}$ und $a_{21} \equiv_p -a_{21}^{(p)}$. Dann wäre:

$$\begin{aligned} A^{p+1} \equiv_p AA^p &\equiv_p \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix} \\ &\equiv_p \begin{pmatrix} a_{11}a_{22} - a_{12}a_{21} & a_{12}(a_{11} - a_{11}) \\ a_{21}(a_{22} - a_{22} & -a_{12}a_{21} + a_{22}a_{11} \end{pmatrix} \equiv_p \begin{pmatrix} Det(A) & 0 \\ 0 & Det(A) \end{pmatrix} \end{aligned}$$

Es folgt $ord(A)|(p+1)(p-1)$. Dies ist aber ebenfalls ein Widerspruch zu $p|ord(A)$. Es folgt $p|ord(A) \Rightarrow (Spur(A))^2 \equiv_p 4Det(A)$

"$\Leftarrow$" Gilt $(Spur(A))^2 \equiv_p 4Det(A)$, so hat das charakteristische Polynom von A $X^2 - Spur(A)X + Det(A)$ eine zweifache Nullstelle. Mit anderen Worten A besitzt zwei gleiche Eigenwerte λ. Nach Satz (4.2.2.5) gilt dann $ord(A) = ord(\lambda p)$ und somit $p|ord(A)$. □

Da $GL(2, Z_p)$ keine zyklische Gruppe ist, gibt es kein erzeugendes Element. Da die Sicherheit des RSA-Verfahrens nicht nur von der Größe der Gruppenordnung, sondern von der Ordnung des zu verschlüsselnden Elementes abhängt, ist es interessant zu untersuchen, wie groß die Ordnung eine Elementes ausb $GL(2, Z_p)$ maximal werden kann, bzw. welche Ordnung die maximale zyklische Untergruppe von $GL(2, Z_p)$ besitzt.

4.2.2.9 Satz: Die maximale Ordnung eines Elementes $A \in GL(2, Z_p)$ beträgt $p^2 - 1$.

Beweis:

Zunächst wird gezeigt, dass die Ordnung einer Matrix $A \in GL(2, Z_p^*)$ durch p^2 beschränkt ist:

Ist A eine Diagonalmatrix, so gilt nach Satz (4.2.2.1) $ord(A)|p-1$ und somit $ord(A) \leq p-1 < p^2$.

Sei also A eine Matrix aus $GL(2, Z_p)$, die keine Diagonalmatrix ist, d.h. mindestens eine der Einträge a_{12}, a_{21} ist nicht Null. OBdA sei $a_{12} \not\equiv_p 0$. Nach Korollar (4.2.1.2) besitzen alle von A erzeugten Elemente $B \not\equiv_p \pm I$ zwei Konstanten $K_1, K_2 \in Z_n^*$:

$$\begin{aligned} K_1 &\equiv_p a_{12}^{-1} a_{21} \equiv_p b_{12}^{-1} b_{21} \\ K_2 &\equiv_p (a_{11} - a_{22}) a_{12}^{-1} \equiv_p (b_{11} - b_{22}) b_{12}^{-1} \end{aligned}$$

D.h. mit Festlegung des Elementes b_{12} ist auch der Eintrag b_{21} sowie die Differenz der Einträge b_{11} und b_{22} bestimmt. Durch Festlegung eines der beiden Elemente b_{11} oder b_{22} ist die Matrix B also vollständig bestimmt.

Mit anderen Worten: Eine beliebige in dem Erzeugnis von A liegende Matrix B ist durch Bestimmung zweier Einträge $b_{11}, b_{12} \in Z_p$ der Matrix eindeutig festgelegt. Es kann also maximal p^2 verschiedene Matrizen in dem Erzeugnis einer Matrix geben, somit gilt: $ord(A) \leq p^2$.

Die Ordnung einer Matrix A aus $GL(2, Z_p)$ kann also keinen Wert annehmen, der größer als p^2 ist. Da die maximale Ordnung eines Elementes die Gruppenordnung teilen muss und $|GL(2, Z_p)| = (p-1)^2 p(p+1)$ gilt, kann die maximale Ordnung eines Elements höchstens $(p-1)(p+1) = p^2 - 1$ betragen. □

4.2.2.10 Satz: Sei $n = pq$, p, q Primzahlen, dann gilt: Die maximale Ordnung eines Elementes $A \in GL(2, Z_n)$ beträgt $(p^2-1)(q^2-1)$.

Beweis:

Die Behauptung folgt direkt aus Satz (4.2.2.9) und dem Chinesischen Restsatz für Matrizen (Satz (3.2.1.7)).

4.3 Die Gruppe $SL(2, Z_n)$

4.3.1 Die Potenzfunktion in der Gruppe $SL(2, Z_n)$

In diesem Abschnitt werden besondere Potenzierungseigenschaften der Gruppe $SL(2, Z_n)$ behandelt.

Da $SL(2, Z_n)$ eine Untergruppe von $GL(2, Z_n)$ ist, gelten alle Sätze aus Abschnitt 4.2.1 auch für die Gruppe $SL(2, Z_n)$.

4.3.1.1 Satz: Sei A eine Matrix aus $SL(2, Z_p)$ mit $a_{12} \not\equiv_p 0$, dann gilt für alle $B \in < A >$: Entweder ist $b_{12} \not\equiv_p 0$, oder $B \equiv_p \pm I$.

Beweis:

Angenommen, für $B \in < A >$ gilt $b_{12} \equiv_p 0$. Nach Satz (4.2.1.1) gilt

$$\begin{aligned} b_{12}a_{21} &\equiv_p a_{12}b_{21} \\ (a_{11} - a_{22})b_{12} &\equiv_p (b_{11} - b_{22})a_{12} \end{aligned}$$

Es folgt $b_{21} \equiv_p 0$ und $b_{11} \equiv_p b_{22}$.

Da $B \in SL(2, Z_p)$ ist $Det(B) \equiv_p b_{11}b_{11} \equiv_p 1$. Es folgt $b_{11} \equiv_p 1$ oder $b_{11} \equiv_p -1$. Also gilt $B \equiv_p \pm I$ □

4.3.1.2 Korollar: Seien p, q Primzahlen und sei $n = pq$, dann gilt: Sei A eine Matrix aus $SL(2, Z_n)$ mit $a_{12} \in Z_n^*$, dann gilt für alle $B \in < A >$: Entweder ist $b_{12} \in Z_n^*$, oder es gilt für mindestens eine der beiden Primzahlen p und q: $B \equiv_p \pm I$.

Beweis:

Die Behauptung folgt direkt aus dem vorherigen Satz zusammen mit dem Chinesischen Restsatz für Matrizen (Satz (3.2.1.7)). □

4.3.2 Zyklische Untergruppen in $SL(2, Z_n)$

Im folgenden soll geklärt werden, welche zyklischen Untergruppen in $SL(2, Z_n)$ existieren und welche besonderen Eigenschaften diese besitzen. Zunächst werden wieder die Matrizen

über Z_p (wobei p eine Primzahl ist) betrachtet und dann mit Hilfe des Chinesischen Restsatzes für Matrizen auf Matrizen über Z_n zusammengesetzt. Wie in Abschnitt 3.2.1 bereits dargestellt, besteht $SL(2, Z_p)$ aus $(p-1)p(p+1)$ Elementen. Da $SL(2, Z_p)$ eine nicht abelsche, assoziative Gruppe und somit nicht zyklische Gruppe ist, kann es kein erzeugendes Element in der Gruppe geben.

Ebenso wie in $GL(2, Z_p)$ gibt es auch in $SL(2, Z_p)$ Matrizen, die genau die Ordnung $p-1$ besitzen.

4.3.2.1 Korollar: Es gibt Matrizen $\in SL(2, Z_p)$, die die Ordnung $p-1$ besitzen.

Beweis:

Es sei $a \in Z_p$ mit $ord(a) = p-1$. Dann ist $\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix}$ eine Matrix aus $SL(2, Z_p)$, die die Ordnung $p-1$ besitzt. □

4.3.2.2 Korollar: Es seien p, q zwei verschiedene Primzahlen und sei $n = pq$. Dann gibt es Matrizen $\in SL(2, Z_n)$, die die Ordnung $\varphi(n)$ besitzen.

Beweis:

Die Behauptung folgt direkt aus dem vorherigen Korollar zusammen mit dem Chinesischen Restsatz für Matrizen (Satz (3.2.1.7)). □

Im Gegensatz zu $GL(2, Z_p)$ ist die maximal zyklische Untergruppe in $SL(2, Z_p)$ wesentlich kleiner, wie der folgende Satz zeigt.

4.3.2.3 Korollar: Die maximale Ordnung eines Elementes $A \in SL(2, Z_p)$ beträgt $2p$.

Beweis:

Nach Satz (4.2.2.9) kann die Ordnung nicht größer als $p^2 - 1$ werden.

Sei $A := \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ eine Matrix aus $SL(2, Z_p)$, die nicht diagonalisierbar ist. OBdA sei $a_{12} \in Z_p^*$.

Nach Korollar (4.2.1.2) gibt es zwei Gleichungen mit den Konstanten K_1 und K_2, die alle Matrizen aus dem Erzeugnis von A erfüllen müssen:

$$\begin{aligned} K_1 &\equiv_p a_{12}^{-1} a_{21} \\ K_2 &\equiv_p (a_{11} - a_{22}) a_{12}^{-1} \end{aligned}$$

Des Weiteren gilt $a_{11}a_{22} - a_{12}a_{21} \equiv_p 1$. Setzt man die obigen Gleichungen in diese Gleichung ein, so erhält man:

$$1 \equiv_p a_{11}(a_{11} - K_2 a_{12}) - a_{12}(K_1 a_{12}) \equiv_p a_{11}^2 - K_2 a_{11}a_{12} - K_1 a_{12}^2$$

Da die Konstanten für alle Elemente $B \in < A >$, $B \not\equiv_p I$ gelten und mit $A \in SL(2, Z_p)$ auch $B \in SL(2, Z_p)$ ist, muss für jede Matrix $B := \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$ die folgende Gleichung gelten:

$$1 \equiv_p b_{11}^2 - K_2 b_{11}b_{12} - K_1 b_{12}^2$$

Dies bedeutet, dass es für jeden Wert von b_{11} maximal 2 Lösungen für b_{12} geben kann. Mit anderen Worten: Es gibt höchstens 2 Matrizen in $< A >$ für jeden möglichen Wert von b_{11}. Da b_{11} maximal p verschiedene Werte in Z_p annehmen kann, folgt $| < A > | \leq 2p$. Diese Schranke wird auch erreicht, z.B. durch die Matrix $\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$, denn es gilt:

$$\begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}^p \equiv_p \begin{pmatrix} -1 & -p \\ 0 & -1 \end{pmatrix} \equiv_p \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$$

□

4.3.2.4 Korollar: Es seien p, q zwei verschiedene Primzahlen und es sei $n = pq$. Die maximale Ordnung eines Elementes $A \in SL(2, Z_n)$ beträgt $4n$.

Beweis:

Die Behauptung folgt direkt aus dem vorherigen Korollar zusammen mit dem Chinesischen Restsatz für Matrizen (Satz (3.2.1.7)). □

4.3.2.5 Satz: Es existieren Matrizen in $SL(2, Z_p)$, die die Ordnung $p + 1$ besitzen.

Beweis:

Sei $A := \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ eine Matrix aus $SL(2, Z_p)$ und $B := A^k \bmod p$. Nach Satz (4.2.1.6) gilt:

$$\begin{aligned} Spur(B) &\equiv_p \alpha^k + \beta^k \\ b_{12}a_{12}^{-1} &\equiv_p a_{12}^{(k)}a_{12}^{-1} \equiv_p \frac{\alpha^k - \beta^k}{\alpha - \beta} \\ b_{21}a_{21}^{-1} &\equiv_p a_{21}^{(k)}a_{21}^{-1} \equiv_p \frac{\alpha^k - \beta^k}{\alpha - \beta} \end{aligned}$$

mit

$$\begin{aligned} \alpha &\equiv_p \frac{Spur(A) + \sqrt{(Spur(A))^2 - 4Det(A)}}{2} \\ &\equiv_p \frac{Spur(A) + \sqrt{(Spur(A))^2 - 4}}{2} \end{aligned}$$

$$\begin{aligned} \beta &\equiv_p \frac{Spur(A) - \sqrt{(Spur(A))^2 - 4Det(A)}}{2} \\ &\equiv_p \frac{Spur(A) - \sqrt{(Spur(A))^2 - 4}}{2} \end{aligned}$$

Es folgt:

$$\begin{aligned} \alpha^p &\equiv_p \left(\frac{Spur(A) + \sqrt{(Spur(A))^2 - 4}}{2}\right)^p \\ &\equiv_p \frac{(Spur(A))^p + (\sqrt{(Spur(A))^2 - 4})^p}{2^p} \\ &\equiv_p \frac{Spur(A) + (\sqrt{(Spur(A))^2 - 4})^p}{2} \end{aligned}$$

$$\begin{aligned} \beta^p &\equiv_p \left(\frac{Spur(A) - \sqrt{(Spur(A))^2 - 4}}{2}\right)^p \\ &\equiv_p \frac{(Spur(A))^p - (\sqrt{(Spur(A))^2 - 4})^p}{2^p} \\ &\equiv_p \frac{Spur(A) - (\sqrt{(Spur(A))^2 - 4})^p}{2} \end{aligned}$$

Es gilt:

$$\begin{aligned} a_{12}^{(p)} a_{12}^{-1} &\equiv_p \frac{\alpha^p - \beta^p}{\alpha - \beta} \equiv_p \frac{(\sqrt{(Spur(A))^2 - 4})^p}{\sqrt{(Spur(A))^2 - 4}} \\ &\equiv_p (\sqrt{(Spur(A))^2 - 4})^{p-1} \end{aligned}$$

Sei $(Spur(A))^2 - 4$ ein quadratischer Nichtrest modulo p maximaler Ordnung. Dann gilt:

$$ord((Spur(A))^2 - 4) = p - 1 \text{ und } ((Spur(A))^2 - 4)^{\frac{p-1}{2}} \equiv_p -1$$

Zusammen folgt:

$$\begin{aligned} a_{12}^{(p)} a_{12}^{-1} &\equiv_p \frac{\alpha^p - \beta^p}{\alpha - \beta} \equiv_p -1 \\ \Rightarrow a_{12}^{(p)} &\equiv_p -a_{12} \end{aligned}$$

Außerdem gilt:

$$Spur(A^p) \equiv_p \alpha^p + \beta^p \equiv_p \frac{2Spur(A)}{2} \equiv_p Spur(A)$$

Zusammen mit der zweiten Gleichung aus Satz (4.2.1.1) folgt:

$$\begin{aligned} (a_{11} - a_{22}) a_{12}^{-1} &\equiv_p (a_{11}^{(p)} - a_{22}^{(p)})(a_{12}^{(p)})^{-1} \\ \Rightarrow (a_{11} - a_{22})(-1) &\equiv_p (a_{11}^{(p)} - a_{22}^{(p)}) \end{aligned}$$

Aus der Gleichung

$$Spur(A) \equiv_p (a_{11} + a_{22}) \equiv_p (a_{11}^{(p)} + a_{22}^{(p)}) \equiv_p Spur(A^p)$$

folgt weiter:

$$\begin{aligned} 2a_{22} &\equiv_p 2a_{11}^{(p)} \\ \Rightarrow a_{22} &\equiv_p a_{11}^{(p)} \end{aligned}$$

und

$$\begin{aligned} 2a_{11} &\equiv_p 2a_{22}^{(p)} \\ \Rightarrow a_{11} &\equiv_p a_{22}^{(p)} \end{aligned}$$

Es folgt $A^p \equiv_p A^{-1}$, also $A^{p+1} \equiv_p I$. Somit gilt:

$$ord(A)|p+1$$

Es gilt sogar $ord(A) = p+1$. Angenommen, es wäre $ord(A) = t < p+1$. Dann gilt $A^{t-1} \equiv_p A^{-1}$, also gilt:

$$\begin{aligned} -1 &\equiv_p a_{12}^{(t-1)} a_{12}^{-1} \equiv_p \frac{\alpha^{t-1} - \beta^{t-1}}{\alpha - \beta} \\ &\equiv_p \frac{(\sqrt{(Spur(A))^2 - 4})^{t-1}}{\sqrt{(Spur(A))^2 - 4}} \\ &\equiv_p (\sqrt{(Spur(A))^2 - 4})^{t-2} \end{aligned}$$

Dann hätte $(Spur(A))^2 - 4$ eine Ordnung, die $t-2$ teilt. Da aber nach Voraussetzung $t - 2 < p - 1$ gilt, kann $(Spur(A))^2 - 4$ kein quadratischer Nichtrest maximaler Ordnung gewesen sein. □

4.3.2.6 Korollar: Es sei p eine Primzahl und $A \in SL(2, Z_p)$. A besitzt genau dann eine Ordnung, die $p+1$ teilt, wenn $(Spur(A))^2 - 4$ ein quadratischer Nichtrest in Z_p^* ist.

Beweis:

"⇒" Angenommen, es gilt $ord(A)|p+1$, dann folgt somit: $A^p \equiv_p A^{-1}$. Dann ist $Spur(A^p) \equiv_p Spur(A)$ und $a_{12}^{(p)} \equiv_p -a_{12}$, sowie $a_{21}^{(p)} \equiv_p -a_{21}$. Somit gilt nach Satz (4.2.1.6):

$$\begin{aligned} -1 &\equiv_p a_{12}^{(p)} a_{12}^{-1} \equiv_p \frac{\alpha^p - \beta^p}{\alpha - \beta} \\ &\equiv_p \frac{(\sqrt{(Spur(A))^2 - 4})^p}{\sqrt{(Spur(A))^2 - 4}} \\ &\equiv_p ((Spur(A))^2 - 4)^{\frac{p-1}{2}} \end{aligned}$$

Also ist $(Spur(A))^2 - 4$ ein quadratischer Nichtrest.

"⇐" Wird in dem Beweis des obigen Satzes (Satz (4.3.2.5)) gezeigt. □

4.3.2.7 Satz: Es sei p eine Primzahl und $A \in SL(2, Z_p)$. A besitzt genau dann eine Ordnung, die $p-1$ teilt, wenn $(Spur(A))^2 - 4$ ein quadratischer Rest in Z_p^* ist.

Beweis:

"$\Rightarrow$" Angenommen, es gilt $ord(A)|p-1$, dann gilt $A^p \equiv_p A$. Somit ist $Spur(A^p) \equiv_p Spur(A)$ und $a_{12}^{(p)} \equiv_p a_{12}$, sowie $a_{21}^{(p)} \equiv_p a_{21}$. Somit gilt nach Satz (4.2.1.6):

$$\begin{aligned} 1 &\equiv_p a_{12}^{(p)} a_{12}^{-1} \equiv_p \frac{\alpha^p - \beta^p}{\alpha - \beta} \\ &\equiv_p \frac{(\sqrt{(Spur(A))^2 - 4})^p}{\sqrt{(Spur(A))^2 - 4}} \\ &\equiv_p ((Spur(A))^2 - 4)^{\frac{p-1}{2}} \end{aligned}$$

Also ist $(Spur(A))^2 - 4$ ein quadratischer Rest.

"$\Leftarrow$" Ist $(Spur(A))^2 - 4$ ein quadratischer Rest, so ist A diagonalisierbar und nach Satz (4.2.2.1) gilt $ord(A)|p-1$. □

4.3.2.8 Korollar: Es sei p eine Primzahl und $A \in SL(2, Z_p)$. Dann gilt $ord(A)|p-1$ mit einer Wahrscheinlichkeit von $\frac{1}{2}$. Ebenso gilt $ord(A)|p+1$ mit einer Wahrscheinlichkeit von $\frac{1}{2}$.

Beweis:

Nach Satz (4.3.2.7) (bzw. Korollar (4.3.2.6)) gilt $ord(A)|p-1$ (bzw. $ord(A)|p+1$) genau dann, wenn $(Spur(A))^2 - 4$ ein quadratischer Rest (bzw. ein quadratischer Nichtrest) in Z_p^* ist.

Angenommen, die Wahrscheinlichkeit, dass $(Spur(A))^2 - 4$ ein quadratischer Rest modulo p ist, unterscheidet sich signifikant von $\frac{1}{2}$. Dann unterscheidet sich die Wahrscheinlichkeit, dass die auf einen quadratischen Rest vorangehende Zahl ein quadratischer Rest ist, ebenfalls signifikant von $\frac{1}{2}$. Also unterscheidet sich die Wahrscheinlichkeit, dass eine zufällig gewählte Zahl und die darauf folgende Zahl quadratische Reste sind, signifikant von $\frac{1}{4}$.

Dies widerspricht aber der Aussage von Theorem 1 aus (Pe92), in der bewiesen wird, dass die Wahrscheinlichkeit, dass zwei aufeinanderfolgende Zahlen quadratische Reste sind, sich nicht signifikant von $\frac{1}{4}$ unterscheidet. □

4.4 Das diskrete Logarithmusproblem in $SL(2, Z_n)$ und $GL(2, Z_n)$

In diesem Abschnitt wird das diskrete Logarithmusproblem in den Gruppen $SL(2, Z_n)$ und $GL(2, Z_n)$ betrachtet. Da sich das diskrete Logarithmusproblem in $SL(2, Z_n)$ bzw. $GL(2, Z_n)$ $(n = pq)$ mit Hilfe des Chinesischen Restsatzes für Matrizen auf das diskrete Logarithmusproblem in $SL(2, Z_p)$ und $SL(2, Z_q)$ bzw. $GL(2, Z_p)$ und $GL(2, Z_q)$ zurückführen lässt, wird im Folgenden das diskrete Logarithmusproblem lediglich in den Gruppen $SL(2, Z_p)$ und $GL(2, Z_p)$ betrachtet.

4.4.1 Das diskrete Logarithmusproblem in $SL(2, Z_p)$

Zunächst soll noch einmal die Definition des diskreten Logarithmusproblems gegeben werden.

4.4.1.1 Definition: Das Problem des diskreten Logarithmus:

Unter dem Problem des diskreten Logarithmus versteht man das Folgende: Sei eine multiplikative Gruppe G und ein Wertepaar $(x, y) \in G \times G$ mit $y \in < x >$. Bestimme eine Zahl k, so dass $y = x^k$ in G gilt.

Man kann leicht zeigen, dass das diskrete Logarithmusproblem in $SL(2, Z_p)$ mindestens so schwierig ist, wie das diskrete Logarithmusproblem in Z_p.

4.4.1.2 Satz: Das diskrete Logarithmusproblem in $SL(2, Z_p)$ ist mindestens so schwierig wie das diskrete Logarithmusproblem in Z_p.

Beweis:

Angenommen, das diskrete Logarithmusproblem in $SL(2, Z_p)$ wäre lösbar, d.h. es gibt einen effizienten Algorithmus Alg, der zu einem Wertepaar $(A, B) \in SL(2, Z_p) \times SL(2, Z_p)$ mit $B \in < A >$ und $p \in P$ ein k ermittelt, so dass $B \equiv_p A^k$ gilt, dann kann dieser Algorithmus dazu verwendet werden, das diskrete Logarithmusproblem in Z_p zu lösen.

Um das diskrete Logarithmusproblem für ein $(x, y) \in Z_p \times Z_p$ zu lösen, kann der Algorithmus Alg wie folgt verwendet werden:

Man setzt $A := \begin{pmatrix} x & 0 \\ 0 & x^{-1} \end{pmatrix} \bmod p$ und $B := \begin{pmatrix} y & 0 \\ 0 & y^{-1} \end{pmatrix} \bmod p$ und verwendet diese beiden Matrizen als Eingabe für den Algorithmus Alg. Dieser gibt ein k aus, so dass $B \equiv_p A^k$ gilt. Da $A^\ell \equiv_p \begin{pmatrix} x^\ell & 0 \\ 0 & x^{-\ell} \end{pmatrix}$ gilt, folgt, dass auch $x^k \equiv_p y$ in Z_p gilt. □

Aus diesem Satz kann man jedoch nicht folgern, dass das Problem des diskreten Logarithmus für alle Matrizen aus $SL(2, Z_p)$ schwierig ist, wie in diesem Abschnitt noch gezeigt werden soll.

4.4.1.3 Satz: Es sei p eine Primzahl. $A \in SL(2, Z_p) \backslash \{\pm I\}$ besitzt genau dann eine Ordnung, die von p geteilt wird, wenn $Spur(A) \equiv_p \pm 2$ gilt.

Beweis:

Gilt $Spur(A) \equiv_p \pm 2$, dann folgt $Spur(A)^2 - 4 \equiv_p 0$, und somit folgt die Behauptung aus Satz (4.2.2.8). □

4.4.1.4 Satz: Es gibt genau $2((p-1)^2 + 2(p-1))$ Matrizen aus $SL(2, Z_p)$, für die gilt $p | ord(A)$.

Beweis:

Nach Satz (4.4.1.3) gilt für alle A mit $p | ord(A)$, dass $Spur(A) \equiv_p \pm 2$ gilt. Des weitern gilt für jede Matrix $A \in SL(2, Z_p)$:

$$a_{11}a_{22} - a_{12}a_{21} \equiv_p 1$$

Es folgt also:

$$a_{11}(2 - a_{11}) - a_{12}a_{21} \equiv_p -a_{11}^2 + 2a_{11} - a_{12}a_{21} \equiv_p 1$$

Für $Spur(A) \equiv_p 2$ werden im Folgenden die beiden Fälle $a_{11} \equiv_p 1$ und $a_{11} \not\equiv_p 1$ unterschieden:

1. Sei $a_{11} \equiv_p 1$, dann folgt $a_{22} \equiv_p 2 - a_{11} \equiv_p 1$. In diesem Fall muss $a_{12}a_{21} \equiv_p 0$ gelten. Also entweder $a_{12} \equiv_p 0$ oder $a_{21} \equiv_p 0$. Es dürfen aber nicht beide Elemente a_{12} und a_{21} den Wert Null annehmen, da in diesem Fall $A \equiv_p I$ und $ord(A) = 1$ gilt.

   Dieser Fall kann genau $2(p-1)$ Mal auftreten.

2. Sei $a_{11} \not\equiv_p 1$, dann folgt $a_{22} \equiv_p 2 - a_{11} \not\equiv_p 1$ und es gilt $a_{11}a_{22} \equiv_p -a_{11}^2 + 2a_{11} \not\equiv_p 1$. In diesem Fall folgt $a_{12}a_{21} \not\equiv_p 0$. Also weder $a_{12} \equiv_p 0$ noch $a_{21} \equiv_p 0$. Aber für jeden sonstigen beliebigen Wert von $a_{12} \in Z_p^*$ gibt es genau einen Wert für $a_{21} \in Z_p^*$, so dass

$$-a_{11}^2 + 2a_{11} - a_{12}a_{21} \equiv_p 1$$

gilt. Dieser Fall kann genau $(p-1)(p-1)$ Mal auftreten.

Insgesamt gibt es also $(p-1)^2 + 2(p-1)$ Matrizen aus $SL(2, Z_p)$ mit $Spur(A) \equiv_p 2$, deren Ordnung von p geteilt wird. Für Matrizen mit $Spur(A) \equiv_p -2$ kann eine äquivalente Fallunterscheidung erfolgen, so dass also gilt:

Insgesamt gibt es $2((p-1)^2 + 2(p-1))$ Matrizen aus $SL(2, Z_p)$, deren Ordnung von p geteilt wird. □

Der folgende Satz zeigt, unter welchen Bedingungen eine Matrix aus $SL(2, Z_p)$ die Ordnung p besitzt.

4.4.1.5 Satz: Sei $A \in SL(2, Z_p)\backslash\{I\}$, dann gilt:

$$ord(A) = p \Leftrightarrow Spur(A) \equiv_p 2$$

Beweis:

"⇒" Sei $ord(A) = p$. Nach Satz (4.4.1.3) gilt $Spur(A) = \pm 2$. Nach Satz (4.2.1.6) gilt für jede Matrix $B \equiv_p A^k$:

$$\begin{aligned} Spur(B) &\equiv_p \alpha^k + \beta^k \\ b_{12}a_{12}^{-1} &\equiv_p a_{12}^{(k)}a_{12}^{-1} \equiv_p \frac{\alpha^k - \beta^k}{\alpha - \beta} \end{aligned}$$

Dabei ist $\alpha \equiv_p \frac{Spur(A)+\sqrt{(Spur(A))^2-4Det(A)}}{2} \equiv_p \frac{Spur(A)}{2}$ und $\beta \equiv_p \frac{Spur(A)-\sqrt{(Spur(A))^2-4Det(A)}}{2} \equiv_p \frac{Spur(A)}{2}$.

Es folgt für $k = p$:

$$Spur(A^p) \equiv_p \alpha^p + \beta^p \equiv_p Spur(A)$$

Wäre $Spur(A) \equiv_p -2$, so gilt $Spur(A^p) \equiv_p -2 \not\equiv_p 2 \equiv_p Spur(I)$, also $A^p \not\equiv_p I$. Dies wäre ein Widerspruch zu $ord(A) = p$.

"$\Leftarrow$" Sei $Spur(A) \equiv_p 2$ und $Det(A) \equiv_p 1$.

Dann gelten die folgenden Behauptungen für alle k:

$$\begin{aligned} Spur(A^k) &\equiv_p 2 \\ a_{12}^{(k)} a_{12}^{-1} &\equiv_p k \\ a_{21}^{(k)} a_{21}^{-1} &\equiv_p k \end{aligned}$$

Der Beweis der Behauptungen erfolgt durch Induktion über k, wobei die dritte Gleichung direkt aus der zweiten mit Hilfe von Korollar (4.2.1.2) gefolgert werden kann, weshalb auf eine explizite Aufführung im Folgenden verzichtet wird.

Nach Satz (4.2.1.4) gilt:

$$\begin{aligned} Spur(A^k) &\equiv_p Spur(A)Spur(A^{k-1}) - Det(A)Spur(A^{k-2}) \\ a_{12}^{(k)} a_{12}^{-1} &\equiv_p Spur(A) a_{12}^{(k-1)} a_{12}^{-1} - Det(A) a_{12}^{(k-2)} a_{12}^{-1} \\ &\equiv_p 2a_{12}^{(k-1)} a_{12}^{-1} - a_{12}^{(k-2)} a_{12}^{-1} \end{aligned}$$

Zunächst wird die erste Behauptung $Spur(A^k) \equiv_p 2$ bewiesen:

Es folgt für $k = 1, 2$:

$$\begin{aligned} 2 &\equiv_p Spur(A^1) \\ 2 &\equiv_p Spur(A^2) \equiv_p Spur(A)Spur(A^1) - Det(A)Spur(A^0) \equiv_p 4 - 2 \equiv_p 2 \end{aligned}$$

Also stimmt die Behauptung für $k = 1, 2$. Angenommen, die Behauptung gilt für alle natürlichen Zahlen bis zu einem $k - 1$, d.h. es gilt $Spur(A^{k-1}) \equiv_p 2$, dann folgt:

$$Spur(A^k) \equiv_p Spur(A)Spur(A^{k-1}) - Det(A)Spur(A^{k-2}) \equiv_p 4 - 2 \equiv_p 2$$

Nun soll die zweite Behauptung $a_{12}^{(k)} a_{12}^{-1} \equiv_p k$ bewiesen werden:

Es folgt für $k = 1, 2$:

$$\begin{aligned} 1 &\equiv_p a_{12}a_{12}^{-1} \\ 2 &\equiv_p a_{12}^{(2)}a_{12}^{-1} \equiv_p 2a_{12}^{(1)}a_{12}^{-1} - a_{12}^{(0)}a_{12}^{-1} \end{aligned}$$

Also stimmt die Behauptung für $k = 1, 2$. Angenommen, die Behauptung gilt für alle Zahlen bis zu einem $k-1$, d.h. es gilt $a_{12}^{(k-1)}a_{12}^{-1} \equiv_p k-1$. Dann folgt:

$$\begin{aligned} a_{12}^{(k)}a_{12}^{-1} &\equiv_p Spur(A)a_{12}^{(k-1)}a_{12}^{-1} \\ &\quad -Det(A)a_{12}^{(k-2)}a_{12}^{-1} \\ &\equiv_p 2a_{12}^{(k-1)}a_{12}^{-1} - a_{12}^{(k-2)}a_{12}^{-1} \\ &\equiv_p 2a_{12}^{(k-1)}a_{12}^{-1} - (a_{12}^{(k-1)}a_{12}^{-1} - 1) \\ &\equiv_p a_{12}^{(k-1)}a_{12}^{-1} + 1 \equiv_p k \end{aligned}$$

Es gilt also $Spur(A^p) \equiv_p 2$ und $a_{12}^{(p)} \equiv_p a_{12}p \equiv_p 0$ und somit $A^p \equiv_p I$ (da $A^p \in SL(2, Z_p)$ gilt). Da $A \not\equiv_p I$ gilt $ord(A) = p$. □

4.4.1.6 Satz: Sei $A \in SL(2, Z_p)$ und p eine Primzahl und sei $ord(A) = p$ und $B \in < A >$, dann kann das diskrete Logarithmusproblem von B bezüglich A mit polynomiellem Zeit- und Speicheraufwand gelöst werden.

Beweis:

Sei $B \equiv_p A^k$. Ist $B \equiv_p I$, so gilt $ord(A) = p|k$, und $k = p$ wäre eine Lösung des diskreten Logarithmusproblems. Sei also $B \not\equiv_p I$. Da $ggT(ord(A), p-1) = 1$ ist, ist A nicht diagonalisierbar, und somit gilt insbesondere entweder $a_{12} \not\equiv_p 0 \vee a_{21} \not\equiv_p 0$. OBdA sei $a_{12} \not\equiv_p 0$.

Wie im Beweis von Satz (4.4.1.5) dargestellt, gilt:

$$a_{12}^{(k)}a_{12}^{-1} \equiv_p k$$

Also gilt: $A^k \equiv_p \begin{pmatrix} a_{11}^{(k)} & a_{12}^{(k)} \\ a_{21}^{(k)} & a_{22}^{(k)} \end{pmatrix} \equiv_p \begin{pmatrix} a_{11}^{(k)} & ka_{12} \\ ka_{21} & a_{22}^{(k)} \end{pmatrix}$

D.h. der diskrete Logarithmus kann bei gegebenen A und $B \equiv_p A^k$ effizient berechnet werden. □

Klassifikation der Matrizen aus $SL(2, Z_p)$

In diesem Abschnitt soll geklärt werden, wie schwierig das diskrete Logarithmusproblem für Matrizen in $SL(2, Z_p)$ ist. Es wurde gezeigt, dass die Ordnung einer Matrix $A \in SL(2, Z_p)$ maximal den Wert $2p$ annehmen kann. Um Aussagen über die Komplexität des diskreten Logarithmusproblems für Matrizen aus $SL(2, Z_p)$ zu machen, werden die Matrizen in folgende Klassen eingeteilt:

4.4.1.0.5 Definition: Klassifizierung von Matrizen aus $SL(2, Z_p)$

Die Matrizen aus $SL(2, Z_p)$ werden in folgende Klassen eingeteilt:

- **Klasse 1:**
  Die Menge der Matrizen der Klasse 1 beinhaltet alle Matrizen $A \in SL(2, Z_p)$ mit $ord(A)|(p-1)$.
- **Klasse 2:**
  Die Menge der Matrizen der Klasse 2 beinhaltet alle Matrizen $A \in SL(2, Z_p)$ mit $ord(A)|2p$.
- **Klasse 3:**
  Die Menge der Matrizen der Klasse 3 beinhaltet alle Matrizen $A \in SL(2, Z_p)$ mit $ord(A)|p+1$.

4.4.1.0.6 Bemerkung: Die hier aufgeführte Klassifikation der Matrizen aus $SL(2, Z_p)$ entspricht den im Satz von Dickson ((Hu83) S. 213) aufgeführten möglichen zyklischen Untergruppen von $SL(2, Z_p)$.

4.4.1.0.7 Satz: Jede Matrix $A \in SL(2, Z_p)\backslash\{\pm I\}$ mit $ord(A) \neq 2$ liegt in genau einer der angegebenen Klassen.

Beweis:

Sei A eine Matrix aus $SL(2, Z_p)\backslash\{\pm I\}$ mit $ord(A) \neq 2$.

Zunächst wird gezeigt, dass A in mindestens einer der angegebenen Klassen enthalten ist. Ist A eine Diagonalmatrix, so gilt nach Satz (4.2.2.1) $ord(A)|p-1$ und somit wäre A eine Matrix der Klasse 1.

Ist A eine Dreiecksmatrix, so gilt nach Satz (4.2.2.4) und Satz (4.2.2.5) $ord(A)|(p-1)p$ und mit $ord(A) \leq 2p$ aus Korollar (4.3.2.3) folgt: Entweder gilt $ord(A)|p-1$ oder $ord(A)|2p$. Mit anderen Worten: Entweder ist dann A eine Matrix der Klasse 1 oder eine Matrix der Klasse 2.

Im folgenden soll nun der Fall betrachtet werden, dass A weder eine Diagonal- noch eine Dreiecksmatrix ist.

Gilt $Spur(A) \equiv_p 2$, so ist $ord(A) = p$ und somit eine Matrix der Klasse 2. Sei also im Folgenden auch $Spur(A) \not\equiv_p 2$.

Nach Satz (4.2.1.6) gilt für $B \equiv_p A^k$:

$$\begin{aligned} Spur(B) &\equiv_n \alpha^k + \beta^k \\ b_{12}a_{12}^{-1} &\equiv_p a_{12}^{(k)}a_{12}^{-1} \equiv_p \frac{\alpha^k - \beta^k}{\alpha - \beta} \\ b_{21}a_{21}^{-1} &\equiv_p a_{21}^{(k)}a_{21}^{-1} \equiv_p \frac{\alpha^k - \beta^k}{\alpha - \beta} \end{aligned}$$

Dabei ist $\alpha \equiv_p \frac{Spur(A)+\sqrt{(Spur(A))^2-4Det(A)}}{2}$ und $\beta \equiv_p \frac{Spur(A)-\sqrt{(Spur(A))^2-4Det(A)}}{2}$.
Somit folgt für $p = k$ und $Det(A) \equiv_p 1$:

$$\begin{aligned} Spur(B) &\equiv_p \alpha^p + \beta^p \\ b_{12}a_{12}^{-1} &\equiv_p a_{12}^{(k)}a_{12}^{-1} \equiv_p \frac{\alpha^p - \beta^p}{\alpha - \beta} \\ b_{21}a_{21}^{-1} &\equiv_p a_{21}^{(k)}a_{21}^{-1} \equiv_p \frac{\alpha^p - \beta^p}{\alpha - \beta} \end{aligned}$$

Wie in dem Beweis von Satz (4.3.2.5) folgt:

$$\begin{aligned} Spur(B) &\equiv_p Spur(A) \\ a_{12}^{(p)}a_{12}^{-1} &\equiv_p \frac{\alpha^p - \beta^p}{\alpha - \beta} \equiv_p \pm 1 \end{aligned}$$

für $Spur(A) \not\equiv_p 2$ und

$$Spur(A^p) \equiv_p \alpha^p + \beta^p \equiv_p \frac{2Spur(A)}{2} \equiv_p Spur(A)$$

Gilt $a_{12}^{(p)} a_{12}^{-1} \equiv_p ((Spur(A))^2 - 4)^{\frac{p-1}{2}} \equiv_p -1$, dann ist $(Spur(A))^2 - 4$ ein quadratischer Nichtrest. Nach Korollar (4.3.2.6) gilt dann $ord(A)|p+1$, also $A^p \equiv_p A^{-1}$

Gilt $a_{12}^{(p)} a_{12}^{-1} \equiv_p 1$, dann gilt $a_{12}^{(p)} \equiv_p a_{12}$. Nach Satz (4.2.1.1) folgt $a_{21}^{(p)} \equiv_p a_{21}$ und

$$\begin{aligned} (a_{11} - a_{22}) a_{12}^{-1} &\equiv_p (a_{11}^{(p)} - a_{22}^{(p)})(a_{12}^{(p)})^{-1} \\ \Rightarrow a_{11} - a_{22} &\equiv_p a_{11}^{(p)} - a_{22}^{(p)} \end{aligned}$$

Zusammen mit

$$Spur(A) \equiv_p a_{11} + a_{22} \equiv_p a_{11}^{(p)} + a_{22}^{(p)} \equiv_p Spur(A^p)$$

folgt $a_{11} \equiv_p a_{11}^{(p)} \wedge a_{22} \equiv_p a_{22}^{(p)}$.

Mit anderen Worten: Es gilt:

$$A^p \equiv_p A \quad \vee \quad A^p \equiv_p A^{-1}$$

Also gilt entweder $A^{p-1} \equiv_p I$, dann ist A eine Matrix der Klasse 1, oder $A^{p+1} \equiv_p I$, dann ist A eine Matrix der Klasse 3. Also ist jede Matrix in mindestens einer der Klassen enthalten.

Nun wird gezeigt, dass A in genau einer der obigen Klassen liegt, falls $ord(A) \neq 2$ gilt. Es existiert eine Primzahl $t > 2$ mit $t|ord(A)$ (da $A \not\equiv_p \pm I$). Würde A in mehreren Klassen liegen, so müsste t mindestens zwei der Zahlen $p-1, p, p+1$ teilen. Wenn t zwei Zahlen teilt, so teilt t auch die Differenz der beiden Zahlen. Da die möglichen Differenzen von $p-1, p, p+1$ jedoch $1, 2$ sind müsste $t \in \{1, 2\}$ gelten. Dies ist aber ein Widerspruch zu $t > 2$. □

Je nach Klasse, in der eine Matrix liegt, können unterschiedliche Aussagen über die Schwierigkeit des diskreten Logarithmusproblems getroffen werden.

4.4.1.0.8 Satz: Sei A eine Matrix der Klasse 1, dann ist das diskrete Logarithmusproblem in $< A >$ äquivalent zum diskreten Logarithmusproblem in Z_p.

Beweis:

Wenn es einen Algorithmus Alg gibt, der das diskrete Logarithmusproblem für Matrizen der Klasse 1 lösen kann, kann dieser dazu verwendet werden, das diskrete Logarithmusproblem in Z_p^* zu lösen. Dies geschieht wie folgt:

Um das diskrete Logarithmusproblem (x, y) mit $y \equiv_p x^k$ zu lösen, gibt man als Eingabeparameter für Alg die Matrizen $\begin{pmatrix} a_{11} & 0 \\ 0 & a_{11}^{-1} \end{pmatrix}$ und $\begin{pmatrix} a_{11}^k & 0 \\ 0 & a_{11}^{-k} \end{pmatrix}$ ein.

Nun soll der umgekehrte Fall betrachtet werden. Angenommen, es gibt einen Algorithmus Alg, der das diskrete Logarithmusproblem in Z_p^* lösen kann, dann kann dieser Algorithmus dazu verwendet werden, das diskrete Logarithmusproblem für Matrizen der Klasse 1 zu lösen.

Sei A eine Matrix der Klasse 1, also $ord(A)|p-1$. Ist A eine Diagonalmatrix, so folgt die Behauptung sofort, da dann gilt:

$$A^k \equiv_p \begin{pmatrix} a_{11} & 0 \\ 0 & a_{11}^{-1} \end{pmatrix}^k \equiv_p \begin{pmatrix} a_{11}^k & 0 \\ 0 & a_{11}^{-k} \end{pmatrix}$$

Also sei im Folgenden A keine Diagonalmatrix, oBdA sei $a_{12} \not\equiv_p 0$, dann gilt $A^p \equiv_p A$ und somit:

$$a_{12}^{(p)} a_{12}^{-1} \equiv_p 1 \equiv_p \frac{\alpha^p - \beta^p}{\alpha - \beta} \equiv_p \sqrt{(Spur(A))^2 - 4Det(A)}^{p-1}$$

Also muss $(Spur(A))^2 - 4Det(A)$ ein quadratischer Rest in Z_p^* sein. D.h. man kann die diskreten quadratischen Wurzeln von $(Spur(A))^2 - 4Det(A)$ in Z_p^* berechnen. D.h. $\sqrt{(Spur(A))^2 - 4Det(A)} \in Z_p^*$, und somit gilt auch:

$$\begin{aligned} \alpha &\equiv_p Spur(A) + \sqrt{(Spur(A))^2 - 4Det(A)} \in Z_p^* \\ &\text{und} \\ \beta &\equiv_p Spur(A) - \sqrt{(Spur(A))^2 - 4Det(A)} \in Z_p^* \\ (\text{Es gilt } \alpha, \beta &\not\equiv_p 0, \text{da } \sqrt{Spur(A^2) - 4Det(A)} \not\equiv_p \pm Spur(A)) \end{aligned}$$

Nach Satz (4.2.1.6) gilt für $B \equiv_p A^k$:

$$\begin{aligned} Spur(B) &\equiv_p \alpha^k + \beta^k \\ b_{12}a_{12}^{-1}(\alpha - \beta) &\equiv_p b_{12}a_{12}^{-1}\sqrt{(Spur(A))^2 - 4Det(A)} \\ &\equiv_p \alpha^k - \beta^k \end{aligned}$$

Es folgt also für eine Matrix $B \equiv_p A^k$:

$$2^{-1}(Spur(B) + b_{12}a_{12}^{-1}(\alpha - \beta)) \equiv_p \alpha^k$$

Mit anderen Worten: Um das diskrete Logarithmusproblem (A, B) mit $B \equiv_p A^k$ für die Matrizen der Klasse 1 mit Hilfe des Algorithmus Alg zu lösen, gibt man als Eingabeparameter für Alg α und $2^{-1}(Spur(B) + b_{12}a_{12}^{-1}(\alpha - \beta)) \equiv_p \alpha^k$ ein. □

4.4.1.0.9 Satz: Sei A eine Matrix der Klasse 2, dann ist das diskrete Logarithmusproblem in $< A >$ mit polynomiellem Zeit- und Speicheraufwand lösbar.

Beweis:

Gilt $ord(A) = p$, so ist das diskrete Logarithmusproblem nach Satz (4.4.1.6) mit polynomiellem Zeit- und Speicheraufwand lösbar. Gilt $ord(A) = 2p$, und man möchte das diskrete Logarithmusproblem von einer Matrix $B \in < A >$ bezüglich A lösen, so löst man zunächst das diskrete Logarithmusproblem von B^2 bezüglich A^2. Sei k diese Lösung. Dann ist entweder k oder $k + p$ die Lösung des diskreten Logarithmusproblems von B bezüglich A. □

4.4.1.0.10 Bemerkung: Für Matrizen der Klasse 3 lässt sich keine direkte Beziehung zwischen dem Berechnen von diskreten Logarithmen in der Gruppe Matrizen der Klasse 3 und dem Berechnen von diskreten Logarithmen in der Gruppe Z_p^* beweisen.

Da Matrizen der Klasse 3 nicht diagonalisierbar sind, kann auch keine Aussage darüber getroffen werden, ob das Berechnen von diskreten Logarithmen in der Gruppe Matrizen der Klasse 3 mindestens so schwierig ist wie in der Gruppe Z_p^*.

4.4.2 Das diskrete Logarithmusproblem in $GL(2, Z_p)$

In diesem Abschnitt soll gezeigt werden, dass das diskrete Logarithmusproblem in $GL(2, Z_p)$ in engem Zusammenhang mit dem diskreten Logarithmusproblem in Z_p^* steht.

Betrachtet man die Gruppe $GL(2, Z_p)\backslash SL(2, Z_p)$, so wird sofort deutlich, dass das diskrete Logarithmusproblem in $GL(2, Z_p)$ mindestens so schwierig ist wie das diskrete Logarithmusproblem in Z_p^*.

4.4.2.1 Satz: Das diskrete Logarithmusproblem in $GL(2, Z_p)\backslash SL(2, Z_p)$ ist mindestens so schwierig wie das diskrete Logarithmusproblem in Z_p^*.

Beweis:

Angenommen, das diskrete Logarithmusproblem in $GL(2, Z_p)\backslash SL(2, Z_p)$ wäre lösbar, d.h. es gibt einen Algorithmus Alg, der zu einem Wertepaar $(A, B) \in GL(2, Z_p)\backslash SL(2, Z_p) \times GL(2, Z_p)\backslash SL(2, Z_p)$ mit $B \in < A >$ und $p \in P$ ein k ermittelt, so dass $B \equiv_p A^k$ gilt, dann kann dieser Algorithmus dazu verwendet werden, das diskrete Logarithmusproblem in Z_p^* zu lösen.

Um das diskrete Logarithmusproblem für ein $(x, y) \in Z_p^* \times Z_p^*$ zu lösen, kann der Algorithmus Alg wie folgt verwendet werden: Man setzt $A := \begin{pmatrix} x & 0 \\ 0 & 1 \end{pmatrix} \bmod p$ und $B := \begin{pmatrix} y & 0 \\ 0 & 1 \end{pmatrix} \bmod p$ und verwendet diese beiden Matrizen als Eingabe für den Algorithmus Alg. Dieser gibt ein k aus, so dass $B \equiv_p A^k$ gilt. Da $A^\ell \equiv_p \begin{pmatrix} x^\ell & 0 \\ 0 & 1^\ell \end{pmatrix}$ gilt, folgt, dass auch $x^k \equiv_p y$ in Z_p^* gelten muss. □

Es stellt sich die Frage, ob das diskrete Logarithmusproblem in Z_p^* äquivalent zu dem diskreten Logarithmusproblem in $GL(2, Z_p)$ ist. Diese Frage soll im nächsten Abschnitt eingehender behandelt werden.

Klassifikation der Matrizen aus $GL(2, Z_p)$

In diesem Abschnitt soll geklärt werden, wie schwierig das diskrete Logarithmusproblem für Matrizen in $GL(2, Z_p)$ ist. Es wurde gezeigt, dass die Ordnung einer Matrix $A \in GL(2, Z_p)$

maximal den Wert $(p^2 - 1)$ annehmen kann. Die in dem vorherigen Abschnitt eingeführte Einteilung der Matrizen in Klassen kann für den Fall $A \in GL(2, Z_p)$ erweitert werden.

4.4.2.0.11 Definition: Klassifizierung von Matrizen aus $GL(2, Z_p)\backslash SL(2, Z_p)$

Die Matrizen aus $GL(2, Z_p)\backslash SL(2, Z_p)$ werden in folgende Klassen eingeteilt:

- **Klasse 4:**

  Die Menge der Matrizen der Klasse 4 beinhaltet alle Matrizen $A \in GL(2, Z_p)\backslash SL(2, Z_p)$ mit $ord(A)|(p-1)$.

- **Klasse 5:**

  Die Menge der Matrizen der Klasse 5 beinhaltet alle Matrizen $A \in GL(2, Z_p)\backslash SL(2, Z_p)$ mit $ord(A)|(p-1)p$.

- **Klasse 6:**

  Die Menge der Matrizen der Klasse 6 beinhaltet alle Matrizen $A \in GL(2, Z_p)\backslash SL(2, Z_p)$ mit $ord(A)|(p-1)(p+1)$.

Zunächst soll gezeigt werden, dass in dieser Klassifizierung alle Matrizen aus $GL(2, Z_p)$ enthalten sind.

4.4.2.0.12 Satz: Jede Matrix $A \in GL(2, Z_p)\backslash SL(2, Z_p)$ liegt in mindestens einer der Klassen 4, 5 oder 6.

Beweis: Sei $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ eine beliebige Matrix aus $GL(2, Z_p)\backslash SL(2, Z_p)$. Dann gilt $B :\equiv_p A^{p-1} \in SL(2, Z_p)$.

Des Weiteren gilt nach Satz (4.2.1.6) für $B \equiv_p A^{p-1}$:

$$Spur(B) \equiv_p \alpha^{p-1} + \beta^{p-1}$$

mit $\alpha \equiv_p \frac{Spur(A)+\sqrt{(Spur(A))^2-4Det(A)}}{2}$ und $\beta \equiv_p \frac{Spur(A)-\sqrt{(Spur(A))^2-4Det(A)}}{2}$.

Man unterscheidet die folgenden zwei Fälle:

1. Fall: $(Spur(A))^2 - 4Det(A)$ ist ein quadratischer Rest in Z_p^*.

   In diesem Fall gilt $\alpha \in Z_p^*$ und $\beta \in Z_p^*$ und somit:

   $$Spur(B) \equiv_p \alpha^{p-1} + \beta^{p-1} \equiv_p 2$$

   Dann gilt nach Satz (4.4.1.5) entweder $B \equiv_p I$, oder $ord(B) = p$. Gilt $B \equiv_p I$, so ist A eine Matrix der Klasse 4. Gilt $ord(B) = p$, so ist A eine Matrix der Klasse 5.

2. Fall: $(Spur(A))^2 - 4Det(A)$ ist kein quadratischer Rest in Z_p^*.

   In diesem Fall gilt $\alpha \notin Z_p^*$ und $\beta \notin Z_p^*$, und somit gilt für $C := A^p \bmod p$:

   $$\begin{aligned} Spur(C) &\equiv_p \alpha^p + \beta^p \\ &\equiv_p \frac{(Spur(A) + \sqrt{(Spur(A))^2 - 4Det(A)})^p}{2^p} \\ &\quad + \frac{(Spur(A) - \sqrt{(Spur(A))^2 - 4Det(A)})^p}{2^p} \\ &\equiv_p \frac{2Spur(A) + \sqrt{(Spur(A))^2 - 4Det(A)} - \sqrt{(Spur(A))^2 - 4Det(A)}}{2} \\ &\equiv_p Spur(A) \end{aligned}$$

   Falls A eine Diagonalmatrix ist, gilt nach Satz (4.2.2.1) $ord(A)|p-1$, und somit wäre A eine Matrix der Klasse 4. Ist A eine Dreiecksmatrix, so ist nach Satz (4.2.2.4) und Satz (4.2.2.5) A entweder eine Matrix der Klasse 4 oder eine Matrix der Klasse 5.

   Also sei A weder eine Diagonalmatrix noch eine Dreiecksmatrix, dann gilt:

   $$\begin{aligned} c_{12}a_{12}^{-1} &\equiv_p \frac{\alpha^p - \beta^p}{\alpha - \beta} \equiv_p \frac{(\sqrt{(Spur(A))^2 - 4})^p}{\sqrt{(Spur(A))^2 - 4}} \\ &\equiv_p (\sqrt{(Spur(A))^2 - 4})^{p-1} \end{aligned}$$

Ebenso folgt:

$$c_{21}a_{21}^{-1} \equiv_p (\sqrt{(Spur(A))^2 - 4})^{p-1}$$

Da $(Spur(A))^2 - 4$ ein quadratische Nichtrest ist, gilt:

$$(\sqrt{(Spur(A))^2 - 4})^{p-1} \equiv_p -1$$

Mit Hilfe der Konstanten aus Satz (4.2.1.1) können auch c_{11} und c_{22} bestimmt werden. Dass heißt, für $C \equiv_p A^p$ gilt:

$$C \equiv_p \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix}$$

Dann gilt für A^{p+1}:

$$CA \equiv_p \begin{pmatrix} a_{22} & -a_{12} \\ -a_{21} & a_{11} \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \equiv_p \begin{pmatrix} a_{11}a_{22} - a_{12}a_{21} & 0 \\ 0 & a_{11}a_{22} - a_{12}a_{21} \end{pmatrix}$$

Mit anderen Worten: A^{p+1} ist eine Diagonalmatrix und besitzt nach Satz (4.2.2.1) eine Ordnung, die $p - 1$ teilt. Daraus folgt, dass A eine Matrix der Klasse 6 ist.

□

Klar ist, dass nach der obigen Definition jede Matrix aus der Klasse 4 auch in den Klassen 5 und 6 enthalten ist. Daher kann Satz (4.4.1.0.7) nur auf die Klassen 5 und 6 erweitert werden.

4.4.2.0.13 Satz: Jede Matrix $A \in GL(2, Z_p)\backslash SL(2, Z_p)$, die nicht in der Klasse 4 liegt, liegt in genau einer der Klassen 5 oder 6.

Beweis:

Nach Satz (4.4.2.0.13) ist jede Matrix aus $GL(2, Z_p)\backslash SL(2, Z_p)$, die keine Matrix der Klasse 4 ist, in mindestens einer der beiden Klassen 5 oder 6 enthalten.

Angenommen A wäre eine Matrix aus $GL(2, Z_p)\backslash SL(2, Z_p)$, die sowohl in der Klasse 5 als auch in der Klasse 6 enthalten ist. Wenn A in Klasse 5 enthalten ist, gilt $p|ord(A)$. Ist A eine Matrix der Klasse 6, so folgt $ord(A)|(p-1)(p+1)$, und somit müsste auch $p|(p-1)(p+1)$ gelten. Dies ist aber ein Widerspruch, da keine Primzahl existiert, die entweder die vorangegangene Zahl oder die nachfolgende Zahl teilt. □

Je nachdem, in welcher Klasse eine Matrix liegt, können unterschiedliche Aussage über die Schwierigkeit des diskreten Logarithmusproblems getroffen werden.

4.4.2.0.14 Satz: Sei A eine Matrix der Klasse 4, dann ist das diskrete Logarithmusproblem in $< A >$ äquivalent zum diskreten Logarithmusproblem in Z_p^*.

Beweis:

Klar ist, dass ein Algorithmus Alg, der das diskrete Logarithmusproblem für Matrizen der Klasse 4 zu lösen vermag, dazu verwendet werden kann, das diskrete Logarithmusproblem in Z_p^* zu lösen. Dies geschieht wie folgt:

Um das diskrete Logarithmusproblem (x, y) mit $y \equiv_p x^k$ zu lösen, gibt man als Eingabeparameter für Alg einfach die Matrizen $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ und $\begin{pmatrix} y & 0 \\ 0 & y \end{pmatrix}$ ein.

Nun soll der umgekehrte Fall betrachtet werden. Angenommen, es gibt einen Algorithmus Alg, der das diskrete Logarithmusproblem in Z_p^* lösen kann, dann kann dieser Algorithmus dazu verwendet werden, das diskrete Logarithmusproblem für Matrizen der Klasse 4 zu lösen.

Sei A eine Matrix der Klasse 4, also $ord(A)|p-1$. Ist A eine Diagonalmatrix, so folgt die Behauptung sofort, da dann gilt:

$$A^k \equiv_p \begin{pmatrix} a_{11} & 0 \\ 0 & a_{22} \end{pmatrix}^k \equiv_p \begin{pmatrix} a_{11}^k & 0 \\ 0 & a_{22}^k \end{pmatrix}$$

Also sei im Folgenden A keine Diagonalmatrix, oBdA sei $a_{12} \not\equiv_p 0$, dann gilt $A^p \equiv_p A$ und somit:

$$a_{12}^{(p)} a_{12}^{-1} \equiv_p 1 \equiv_p \frac{\alpha^p - \beta^p}{\alpha - \beta} \equiv_p \sqrt{(Spur(A))^2 - 4Det(A)}^{p-1}$$

Also muss $(Spur(A))^2 - 4Det(A)$ ein quadratischer Rest in Z_p^* sein. D.h. man kann die diskreten quadratischen Wurzeln von $(Spur(A))^2 - 4Det(A)$ in Z_p^* berechnen und es gilt: $\sqrt{(Spur(A))^2 - 4Det(A)} \in Z_p^*$. Da Z_p ein Körper ist, gilt somit auch $\alpha, \beta \in Z_p$. Des Weiteren gilt $\alpha, \beta \not\equiv_p 0$, da $\sqrt{(Spur(A))^2 - 4Det(A)} \not\equiv_p \pm Spur(A)$ für $Det(A) \not\equiv_p 0$. Das heißt, es gilt:

$$\alpha \equiv_p Spur(A) + \sqrt{(Spur(A))^2 - 4Det(A)} \in Z_p^*$$
$$\beta \equiv_p Spur(A) - \sqrt{(Spur(A))^2 - 4Det(A)} \in Z_p^*$$

Nach Satz (4.2.1.6) gilt für $B \equiv_p A^k$:

$$\begin{aligned} Spur(B) &\equiv_p \alpha^k + \beta^k \\ b_{12}a_{12}^{-1}(\alpha - \beta) &\equiv_p b_{12}a_{12}^{-1}\sqrt{(Spur(A))^2 - 4Det(A)} \\ &\equiv_p \alpha^k - \beta^k \end{aligned}$$

Es folgt also für eine Matrix $B \equiv_p A^k$:

$$2^{-1}(Spur(B) + b_{12}a_{12}^{-1}(\alpha - \beta)) \equiv_p \alpha^k$$

Mit anderen Worten: Um das diskrete Logarithmusproblem (A, B) mit $B \equiv_p A^k$ für die Matrizen der Klasse 4 mit Hilfe des Algorithmus Alg zu lösen, gibt man als Eingabeparameter für Alg α und $2^{-1}(Spur(B) + b_{12}a_{12}^{-1}(\alpha - \beta)) \equiv_p \alpha^k$ ein. □

4.4.2.0.15 Satz: Sei A eine Matrix der Klasse 5, die nicht in der Klasse 4 enthalten ist, dann ist das diskrete Logarithmusproblem in $< A >$ höchstens so schwierig wie das diskrete Logarithmusproblem in Z_p^*.

Beweis:

Gibt es einen Algorithmus Alg, der das diskrete Logarithmusproblem in Z_p^* löst, dann kann dieser dazu verwendet werden, um das diskrete Logarithmusproblem für Matrizen der Klasse 5 zu lösen. Sei A eine Matrix der Klasse 5 und sei $B := A^k \bmod p$ gegeben. Um das diskrete Logarithmusproblem (A, B) zu lösen, löst man die beiden folgenden Logarithmusprobleme:

Zunächst löst man das diskrete Logarithmusproblem von (A^{p-1}, B^{p-1}). A^{p-1} ist eine Matrix der Klasse 2, und somit ist dieses Logarithmusproblem nach Satz (4.4.1.6) mit polynomiellem Zeit- und Speicheraufwand lösbar. Man erhält ein k' mit $k' \equiv_p k$.

Des Weiteren löst man das diskrete Logarithmusproblem von (A^p, B^p). A^p ist eine Matrix der Klasse 4 und somit ist das Lösen dieses diskreten Logarithmusproblems äquivalent zum diskreten Logarithmusproblem in Z_p^*. Mit anderen Worten: Man kann den Algorithmus Alg verwenden, um dieses Logarithmusproblem zu lösen. Man erhält ein k'' mit $k'' \equiv_{p-1} k$. Aus k' und k'' kann k mit Hilfe des Chinesischen Restsatzes berechnet werden. □

4.4.2.0.16 Bemerkung: Für Matrizen der Klasse 6 kann nicht gezeigt werden, ob das Berechnen von diskreten Logarithmen in der Gruppe der Klasse 6 Matrizen genauso schwierig oder sogar schwieriger ist als das Berechnen von diskreten Logarithmen in der Gruppe Z_p^*. Aber es kann gezeigt werden, dass das diskrete Logarithmusproblem in der Gruppe der Klasse 6 Matrizen ebenfalls mindestens so schwierig ist, wie das diskrete Logarithmusproblem in Z_p^*:

Es seien A, B Matrizen der Klasse 6, dann gilt:$Det(A) \not\equiv_p \pm 1$ und $Det(B) \not\equiv_p \pm 1$. Wenn es einen Algorithmus gäbe, der das diskrete Logarithmusproblem (A, B) lösen könnte, dann könnte dieser auch dazu verwendet werden, das diskrete Logarithmusproblem $(Det(A), Det(B))$ in der Gruppe Z_p^* zu lösen.

4.5 Das diskrete Wurzelproblem in $GL(2, Z_n)$ und $SL(2, Z_n)$

In diesem Abschnitt wird das Problem des Ziehens diskreter Wurzeln in $GL(2, Z_n)$ und $SL(2, Z_n)$ behandelt, wobei $n = pq$ das Produkt zweier Primzahlen darstellt. Generell muss man beim Ziehen diskreter Wurzeln in einer Gruppe G mit Ordnung $|G|$ zwei Fälle unterscheiden. Betrachtet man die $d-te$ Wurzel eines Elements aus G und es gilt $ggT(d, |G|) = 1$, so existiert eine eindeutige diskrete $d - te$ Wurzel zu jedem Element $g \in G$, denn dann existiert ein $t \in Z$ mit $dt \equiv_{|G|} 1$ und g^t ist die $d - te$ Wurzel von g.

Gilt $ggT(d, |G|) = \ell > 1$, so kann es für ein $g \in G$ keine, eine oder mehrere $d - te$ Wurzeln geben. Zunächst soll der erste Fall betrachtet werden, also $ggT(d, |G|) = 1$ mit $G =$

$GL(2, Z_n)$. Dieser Fall entspricht der RSA-Verschlüsselung, da bei der RSA-Verschlüsselung immer eine eindeutige Entschlüsselung des Chiffretextes möglich sein muss.

4.5.1 Satz: Ist die Ordnung $ord(A)$ einer Matrix A oder ein Vielfaches dieser Ordnung, wie z.B. $|GL(2, Z_n)|$, bekannt, so ist das Ziehen diskreter $d-ter$ Wurzeln mit $ggT(d, ord(A)k) = 1$ mit polynomiellem Zeit- und Speicheraufwand möglich.

Beweis: Sei A eine beliebige Matrix aus $GL(2, Z_n)$ und ein Vielfaches der Ordnung von A ($ord(A)k$) bekannt, so dass $ggT(d, ord(A)k) = 1$ gilt. Dann gibt es eine Zahl t mit $dt \equiv_{ord(A)k} 1$. Dann ist A^t eine $d-te$ Wurzel von A, denn es gilt $(A^t)^d \equiv_n A^{td} \equiv_n A$. □

4.5.2 Korollar: Für jede Matrix $A \in SL(2, Z_n)$ mit $Spur(A) \equiv_p 2$ ist das Berechnen einer diskreten $d-ten$ Wurzel mit $ggT(d, n) = 1$ mit polynomiellem Zeit- und Speicheraufwand möglich.

Beweis:

Nach Satz (4.4.1.5) gilt $ord(A) = p$ in $SL(2, Z_p)$ und $ord(A) = q$ in $SL(2, Z_q)$ und somit $ord(A) = n$ in $SL(2, Z_n)$. □

Im folgenden soll das RSA-Problem für die Matrixgruppe $GL(2, Z_n)$ formuliert werden.

RSA-Problem in $GL(2, Z_n)$:

Sei eine Matrix $A \in GL(2, Z_n)$ und eine Zahl d mit $ggT(d, |GL(2, Z_n)|) = 1$ gegeben. Finde eine Matrix $B \in GL(2, Z_n)$, so dass $B^d \equiv_n A$ gilt.

4.5.3 Satz: Das RSA-Problem in $GL(2, Z_n)\backslash SL(2, Z_n)$ ist mindestens so schwierig wie das RSA-Problem in Z_n^*.

Beweis:

Angenommen, das RSA-Problem in $GL(2, Z_n)\backslash SL(2, Z_n)$ wäre lösbar, d.h. es gibt einen Algorithmus Alg, der zu einer beliebigen Matrix $A \in GL(2, Z_n)\backslash SL(2, Z_n)$ und einer Zahl d mit $ggT(d, |GL(2, Z_n)|) = 1$ eine Matrix B ermittelt, so dass $B^d \equiv_n A$ gilt, dann kann dieser Algorithmus dazu verwendet werden, diskrete $d-te$ Wurzeln in Z_n^* zu berechnen.

Um eine diskrete $d-te$ Wurzel für ein Element $g \in Z_n^*$ zu lösen, kann der Algorithmus Alg wie folgt verwendet werden: Man wählt $A \in GL(2, Z_n)\backslash SL(2, Z_n)$ mit $Det(A) \equiv_n g$

und verwendet diese Matrix sowie d als Eingabe für den Algorithmus Alg. Dieser gibt eine Matrix B aus, so dass $B^d \equiv_n A$ gilt. Dann folgt: $Det(B)^d \equiv_n Det(B^d) \equiv_n Det(A) \equiv_n g$. Also ist $Det(B)$ eine $d-te$ Wurzel von g in Z_n^*. □

Auch in der Gruppe $SL(2, Z_n)$ ist das RSA-Problem mindestens so schwierig wie in Z_n^*:

4.5.4 Satz: Das RSA-Problem in $SL(2, Z_n)$ ist mindestens so schwierig wie das RSA-Problem in Z_n^*.

Beweis:

Angenommen, das RSA-Problem in $SL(2, Z_n)$ wäre lösbar, d.h. es gibt einen Algorithmus Alg, der zu einer Matrix $A \in SL(2, Z_n)$ und einer Zahl d mit $ggT(d, |SL(2, Z_n)|) = 1$ eine Matrix B ermittelt, so dass $B^d \equiv_n A$ gilt, dann kann dieser Algorithmus dazu verwendet werden, diskrete $d-te$ Wurzeln in Z_n zu berechnen.

Um eine diskrete $d-te$ Wurzel für ein Element $g \in Z_n$ zu lösen, kann der Algorithmus Alg wie folgt verwendet werden: Man setzt $A :\equiv_n \begin{pmatrix} g & 0 \\ 0 & g^{-1} \end{pmatrix}$ und verwendet diese Matrix sowie d als Eingabe für den Algorithmus Alg. Dieser gibt eine Matrix B aus, so dass $B^d \equiv_n A$ gilt. Da $A^\ell \equiv_n \begin{pmatrix} g^\ell & 0 \\ 0 & g^{-\ell} \end{pmatrix}$ gilt, folgt, dass auch $B \equiv_n \begin{pmatrix} u & 0 \\ 0 & u^{-1} \end{pmatrix}$ mit $u^d \equiv_n g$ in Z_n gelten muss. □

4.5.1 Klassifikation der Matrizen aus $SL(2, Z_n)$

Um differenzierte Aussagen über die Beziehung des RSA-Problems in $SL(2, Z_n)$ bzw. $GL(2, Z_n)$ machen zu können, werden die Matrizen wieder in Klassen unterteilt. Zuerst werden Matrizen aus $SL(2, Z_n)$ betrachtet.

4.5.1.1 Definition: Klassifizierung von Matrizen aus $SL(2, Z_n)$

Sei $n = pq$, p, q Primzahlen. Die Matrizen aus $SL(2, Z_n)$ werden in folgende Klassen eingeteilt:

- **Klasse A:**

  Die Menge der Matrizen der Klasse A beinhaltet alle Matrizen $A \in SL(2, Z_n)$, so dass $A \bmod p$ eine Matrix der Klasse 1 ist und $A \bmod q$ eine Matrix der Klasse 1 ist. Es gilt also $ord(A) | \varphi(n)$.

- **Klasse B:**

  Die Menge der Matrizen der Klasse B beinhaltet alle Matrizen $A \in SL(2, Z_n)$, so dass entweder genau $A \bmod p$ eine Matrix der Klasse 2 ist oder genau $A \bmod q$ eine Matrix der Klasse 2 ist, aber nicht beide Matrizen in der Klasse 2 enthalten sind.

- **Klasse C:**

  Die Menge der Matrizen der Klasse C beinhaltet alle Matrizen $A \in SL(2, Z_n)$, so dass $A \bmod p$ eine Matrix der Klasse 1 ist und $A \bmod q$ eine Matrix der Klasse 3 ist, oder umgekehrt $A \bmod p$ eine Matrix der Klasse 3 ist und $A \bmod q$ eine Matrix der Klasse 1 ist.

- **Klasse D**

  Die Menge der Matrizen der Klasse D beinhaltet alle Matrizen $A \in SL(2, Z_n)$, so dass $A \bmod p$ eine Matrix der Klasse 2 ist und $A \bmod q$ eine Matrix der Klasse 2 ist.

- **Klasse E:**

  Die Menge der Matrizen der Klasse E Matrizen beinhaltet alle Matrizen $A \in SL(2, Z_n)$, so dass $A \bmod p$ eine Matrix der Klasse 3 ist und $A \bmod q$ eine Matrix der Klasse 3 ist.

4.5.1.2 Satz: Sei $A \in SL(2, Z_n)$ eine Matrix, für die gilt: $A \not\equiv_p I$, $A \not\equiv_q I$ und $ggT(ord(A), 2) = 1$. Dann liegt A in genau einer der angegebenen Klassen.

Beweis:

Nach Satz (4.4.1.0.7) liegt $A \bmod p$ in genau einer der Klassen aus Definition (4.4.1.0.5). Ebenso liegt $A \bmod q$ in genau einer der Klassen aus Definition (4.4.1.0.5). Durch den Chinesischen Restsatz für Matrizen (Satz (3.2.1.7)) folgt, dass A in genau einer der oben aufgeführten Klassen liegen muss. □

4.5.1.3 Satz: Das RSA-Problem ist für Matrizen der Klasse D mit polynomiellem Zeit- und Speicheraufwand lösbar.

Beweis:

Sei A eine Matrix der Klasse D, dann hat $A \bmod p$ eine Ordnung, die $2p$ teilt und $A \bmod q$ eine Ordnung, die $2q$ teilt. Es folgt, dass die Ordnung von A $4pq = 4n$ teilen muss. Nach Satz (4.5.1) ist dann die Berechnung diskreter $d - ter$ Wurzeln möglich. □

Es zeigt sich sogar, dass das Ziehen diskreter Wurzeln möglich ist, wenn die betrachtete Matrix modulo einer der beiden Primzahlen eine Matrix der Klasse 2 ist.

4.5.1.4 Satz: Das RSA-Problem ist für Matrizen der Klasse B mit polynomiellem Zeit- und Speicheraufwand lösbar.

Beweis:

Sei A eine Matrix der Klasse B, dann ist A modulo genau eine der beiden Primzahlen (oBdA p) eine Matrix der Klasse 2. D.h. es gilt dann $A \bmod p$ hat eine Ordnung, die $2p$ teilt. Dann gilt für $A^{2n} \bmod p$:

$$A^{2n} \equiv_p A^{2pq} \equiv_p (A^{2p})^q \equiv_p I^q \equiv_p I$$

Da $A \bmod q$ keine Matrix der Klasse 2 ist, folgt, dass für $a_{11}^{(2n)}$ gilt:

$$\begin{aligned} a_{11}^{(2n)} - 1 &\equiv_p 0 \\ a_{11}^{(2n)} - 1 &\not\equiv_q 0 \end{aligned}$$

Mit anderen Worten: $ggT(a_{11}^{(2n)} - 1, n)$ ist ein nicht trivialer Faktor von n. Kennt man die Faktorisierung von n, so kann man die Ordnung der Gruppe $SL(2, Z_n)$ bestimmen. Nach Satz (4.5.1) ist dann die Berechnung diskreter $d - ter$ Wurzeln von $A \in SL(2, Z_n)$ möglich. □

4.5.1.5 Satz: Das RSA-Problem für Diagonalmatrizen aus $SL(2, Z_n)$ ist äquivalent zum RSA-Problem in Z_n^*.

Beweis:

Eine Diagonalmatrix $A \in S(2, Z_n)$ hat die folgende Form:

$$A = \begin{pmatrix} g & 0 \\ 0 & g^{-1} \end{pmatrix}$$

Dabei ist $g \in Z_n^*$.

Es gilt:

$$x^d \equiv_n g \quad \Leftrightarrow \quad \begin{pmatrix} x^d & 0 \\ 0 & x^{-d} \end{pmatrix} \equiv_n \begin{pmatrix} g & 0 \\ 0 & g^{-1} \end{pmatrix}$$

Angenommen es gibt einen Algorithmus Alg, der das RSA-Problem in Z_n^* lösen kann, d.h. also in der Lage ist $d - te$ Wurzeln modulo n zu berechnen. Dann kann dieser zur Berechnung einer $d - te$ Wurzel aus der obigen Matrix verwendet werden.

Umgekehrt kann ein Algorithmus, der das RSA-Problem für Diagonalmatrizen lösen kann, dazu verwendet werden, das RSA-Problem in Z_n^* zu lösen. □

4.5.1.6 Korollar: Das RSA-Problem ist für Diagonalmatrizen der Klasse A ist mindestens so schwierig, wie das RSA-Problem in Z_n^*.

Beweis:

Diagonalmatrizen sind Matrizen der Klasse A, damit folgt die Behauptung aus Satz (4.5.1.5). □

4.5.1.7 Bemerkung: Der obige Satz lässt sich nicht auf alle Matrizen der Klasse A erweitern. Um den Satz anwenden zu können, müsste man die Matrizen der Klasse A zuerst diagonalisieren. Um die Eigenwerte zu bestimmen, muss eine quadratische Gleichung in Z_n^* gelöst werden. Dies ist aber äquivalent zur Faktorisierung von n.

Daher ist nicht klar, ob das RSA-Problem für Matrizen der Klasse A äquivalent zu dem RSA-Problem in Z_n^* ist. Es könnte daher sein, dass das RSA-Problem für Matrizen der Klasse A schwieriger zu lösen ist als das RSA-Problem in Z_n^*.

Ebenso ist nicht bekannt, ob das RSA-Problem in den Klassen C und E in einer Relation zu dem RSA-Problem in Z_n^* steht. Das RSA-Problem könnte in den einzelnen Klassen sowohl schwieriger als auch leichter als in Z_n^* sein. Die beiden folgenden Sätze zeigen, dass es von der Zahl d abhängt, wie sich das diskrete Wurzelproblem in diesen Klassen zu dem RSA-Problem in Z_n^* verhält.

4.5.1.8 Satz: Sei d eine Zahl, die genau eine der beiden Zahlen $p - 1$ und $p + 1$ teilt. Dann ist das Ziehen einer $d - ten$ Wurzel in den Klassen C und E mindestens so schwierig wie in Z_n^*.

Beweis:

Angenommen es gibt einen Algorithmus Alg, der eine d-te Wurzel aus einer Matrix A mit $d|ord(A)$ bestimmen kann, die aus einer der Klassen C oder E stammt. Da $d|ord(A)$ gilt, gibt es mehrere (verschiedene) d-te Wurzeln. In Abschnitt 4.5.3 wird gezeigt werden, wie mittels eines solchen Algorithmus der Modulus n faktorisiert werden kann. D.h. das Berechnen d-ter Wurzeln in den Klassen C und E ist äquivalent zur Faktorisierung von n und somit mindestens so schwierig wie das Berechnen d-ter Wurzeln in Z_n^*. □

4.5.1.9 Satz: Seien p, q zwei große Primzahlen und sei $n = pq$. Das Ziehen einer $n - ten$ Wurzel für eine beliebige Matrix $A \in GL(2, Z_p)$ mit $ggT(ord(A), n) = 1$ ist genauso schwierig wie das Berechnen von diskreten $n - ten$ Wurzeln in Z_n^*.

Beweis:

Nach Satz (4.2.1.6) gilt für $A \equiv_n B^n$:

$$Spur(A) \equiv_n \alpha^n + \beta^n$$

mit $\alpha \equiv_n \frac{Spur(B)+\sqrt{(Spur(B))^2-4Det(B)}}{2}$ und $\beta \equiv_n \frac{Spur(B)-\sqrt{(Spur(B))^2-4Det(B)}}{2}$.
Somit folgt:

$$\begin{aligned} Spur(A) &\equiv_n \left(\frac{Spur(B) + \sqrt{(Spur(B))^2 - 4Det(B)}}{2}\right)^n \\ &\quad + \left(\frac{Spur(B) - \sqrt{(Spur(B))^2 - 4Det(B)}}{2}\right)^n \\ &\equiv_n \frac{Spur(B)^n + (\sqrt{(Spur(B))^2 - 4Det(B)})^n}{2^n} \\ &\quad + \frac{Spur(B)^n - (\sqrt{(Spur(B))^2 - 4Det(B)})^n}{2^n} \\ &\equiv_n \frac{Spur(B)^n}{2^{n-1}} \end{aligned}$$

Außerdem gilt $Det(A) \equiv_n Det(B^n) \equiv_n (Det(B))^n$.

Mit anderen Worten: Ein Algorithmus, der die $n-te$ Wurzel aus A berechnen kann, berechnet immer auch gleichzeitig die beiden $n-ten$ Wurzeln von $Det(A)$ und $Spur(A)2^{-(n-1)}$. Er kann also dazu verwendet werden, diskrete $n-te$ Wurzeln in Z_n^* zu berechnen.

Ebenso ist es möglich, einen Algorithmus, der $n-te$ Wurzeln in Z_n^* lösen kann, dazu zu verwenden zu einer Matrix $A \equiv_n B^n$ die Werte $Spur(B)$ und $Det(B)$ zu bestimmen. In Abschnitt 4.5.3 wird gezeigt werden, dass diese beiden Werte zusammen mit der Kenntnis von A ausreichen, um B vollständig aus A zu bestimmen, wenn $ggT(ord(A), n) = 1$ gilt. □

4.5.2 Klassifikation der Matrizen aus $GL(2, Z_n)$

Die erfolgte Klassifizierung für Matrizen aus $SL(2, Z_n)$ soll nun wie im vorherigen Abschnitt auf Matrizen aus $GL(2, Z_n)\backslash SL(2, Z_n)$ erweitert werden.

4.5.2.1 Definition: Klassifizierung von Matrizen aus $GL(2, Z_n)\backslash SL(2, Z_n)$

Seien p, q Primzahlen und sei $n = pq$. Die Matrizen aus $GL(2, Z_n)\backslash SL(2, Z_n)$ werden in folgende Klassen eingeteilt:

- **Klasse G:**

  Die Menge der Matrizen der Klasse G beinhaltet alle Matrizen $A \in SL(2, Z_n)$, so dass für eine der beiden Primzahlen (oBdA p) $A \bmod p \in SL(2, Z_p)$ sowie $A \bmod q \in GL(2, Z_q)\backslash SL(2, Z_q)$ gilt.

- **Klasse H:**

  Die Menge der Matrizen der Klasse H beinhaltet alle Matrizen $A \in GL(2, Z_n)\backslash SL(2, Z_n)$, so dass $A \bmod p$ eine Matrix der Klasse 4 und $A \bmod q$ eine Matrix der Klasse 4 ist.

- **Klasse I:**

  Die Menge der Matrizen der Klasse I beinhaltet alle Matrizen $A \in GL(2, Z_n)\backslash SL(2, Z_n)$, so dass entweder genau $A \bmod p$ eine Matrix der Klasse 5 oder genau $A \bmod q$ eine Matrix der Klasse 5 ist, aber nicht beide Matrizen der Klasse 5 angehören.

- **Klasse J:**

  Die Menge der Matrizen der Klasse J beinhaltet alle Matrizen $A \in GL(2, Z_n) \backslash SL(2, Z_n)$, so dass A mod p eine Matrix der Klasse 4 und A mod q eine Matrix der Klasse 6 ist, oder umgekehrt A mod p eine Matrix der Klasse 6 und A mod q eine Matrix der Klasse 4 ist.

- **Klasse K**

  Die Menge der Matrizen der Klasse K beinhaltet alle Matrizen $A \in GL(2, Z_n) \backslash SL(2, Z_n)$, so dass A mod p eine Matrix der Klasse 5 ist und A mod q eine Matrix der Klasse 5 ist.

- **Klasse L:**

  Die Menge der Matrizen der Klasse L beinhaltet alle Matrizen $A \in GL(2, Z_n) \backslash SL(2, Z_n)$, so dass A mod p eine Matrix der Klasse 6 und A mod q eine Matrix der Klasse 6 ist.

4.5.2.2 Satz: Jede Matrix $A \in GL(2, Z_n) \backslash SL(2, Z_n)$ liegt in genau einer der angegebenen Klassen.

Beweis:

Sei A eine Matrix aus $GL(2, Z_n) \backslash SL(2, Z_n)$. Gilt für eine der beiden Primzahlen p oder q (oBdA p), dass A mod $p \in SL(2, Z_p)$ liegt, so ist A eine Matrix der Klasse G.

Also sei A keine Matrix der Klasse G. Nach Satz (4.4.2.0.13) liegt A mod p in genau einer der Klassen aus Definition (4.4.2.0.11), falls A mod $p \notin SL(2, Z_p)$. Ebenso liegt A mod q in genau einer der Klassen aus Definition (4.4.2.0.11), falls A mod $q \notin SL(2, Z_q)$. Durch den Chinesischen Restsatz für Matrizen (Satz (3.2.1.7)) folgt, dass A in genau einer der oben aufgeführten Klassen liegen muss. □

Nach Satz (4.5.3) ist das RSA-Problem in $GL(2, Z_n) \backslash SL(2, Z_n)$ mindestens so schwierig wie in Z_n^*. Nach der obigen Klasseneinteilung kann nun eine Aussage getroffen werden, für welche Klassen das RSA-Problem in $GL(2, Z_n) \backslash SL(2, Z_n)$ mit polynomiellem Zeit- und Speicheraufwand lösbar ist.

4.5.2.3 Satz: Das RSA-Problem ist für Matrizen der Klassen G und I mit polynomiellem Zeit- und Speicheraufwand lösbar.

Beweis:

Das RSA-Problem ist mit polynomiellem Zeit- und Speicheraufwand lösbar, wenn die Ordnung der Gruppe $GL(2, Z_n)$ bekannt ist. Die Ordnung von $GL(2, Z_n)$ kann berechnet werden, wenn man die Primfaktoren p und q der Zahl n kennt.

Sei A eine Matrix der Klasse G, dann gilt entweder $A \in SL(2, Z_p)$ oder $A \in SL(2, Z_q)$, aber $A \notin SL(2, Z_n)$. OBdA sei $A \in SL(2, Z_p)$ und $A \notin SL(2, Z_q)$. Dann gilt $Det(A) \equiv_p 1$ und $Det(A) \not\equiv_q 1$. Es folgt, dass $ggT(Det(A) - 1, n) = p$ gilt. Somit erhält man einen nichttrivialen Faktor von n und kann n faktorisieren. Dann ist auch das RSA-Problem mit polynomiellem Zeit- und Speicheraufwand lösbar.

Sei A eine Matrix aus einer der Klassen I, dann gilt für genau eine der beiden Primzahlen p und q (oBdA p), dass $A \bmod p$ eine Matrix der Klasse 5 in $GL(2, Z_p)$ ist. Nach Satz (4.2.2.8) gilt dann, dass $Spur(A) \equiv_p 4Det(A)$ gilt. Es folgt, dass $ggT(Spur(A) - 4Det(A), n) = p$ ein nichttrivialer Faktor von n ist. Dann ist auch das RSA-Problem mit polynomiellem Zeit- und Speicheraufwand lösbar. □

4.5.2.4 Bemerkung: Für Matrizen der Klasse K und der Klasse L kann keine konkretere Aussage über den Zusammenhang des RSA-Problems in den einzelnen Klassen mit dem RSA-Problem in Z_p^* getroffen werden. Es gilt aber wie für alle Matrizen aus $GL(2, Z_p) \backslash SL(2, Z_p)$, dass das RSA-Problem für Matrizen mindestens so schwierig ist wie das RSA-Problem in Z_p^* (siehe Satz (4.5.3)).

4.5.3 Diskrete Wurzeln in $GL(2, Z_n)$ und Faktorisierung

In diesem Abschnitt soll der Zusammenhang zwischen diskreten Wurzeln in $GL(2, Z_n)$ und der Faktorisierung von n erläutert werden. In diesem Zusammenhang sind vor allen Dingen $d - te$ diskrete Wurzeln zu betrachten wobei $ggT(d, |GL(2, Z_n)|) = \ell > 1$ gilt.

Zunächst wird kurz der Zusammenhang zwischen der Faktorisierung von n und Quadratwurzeln *modulo* n erläutert.

Es soll gezeigt werden, dass sowohl das Berechnen von wesentlich verschiedenen Quadratwurzeln in $GL(2, Z_n)$, als auch das Berechnen von wesentlich verschiedenen kubischen Wurzeln in $GL(2, Z_n)$ äquivalent zur Faktorisierung von n ist.

4.5.3.1 Satz: Sei $n = pq$ (p, q prim mit $p \neq q$) und $y \equiv_n x^2$ ein quadratischer Rest

modulo n. Dann existieren vier diskrete quadratische Wurzeln $x_i, i = 1, 2, 3, 4$ mit $x_i^2 \equiv_n y$ und es gilt:

$$\begin{aligned} &x_2 \equiv_p x_1 \quad && x_2 \equiv_q -x_1 && \\ &x_3 \equiv_p -x_1 \quad && x_3 \equiv_q x_1 \quad && x_3 \equiv_n -x_2 \\ &x_4 \equiv_p -x_1 \quad && x_4 \equiv_q -x_1 \quad && x_4 \equiv_n -x_1 \end{aligned}$$

Beweis:

Es reicht zu zeigen, dass es vier genau quadratische Wurzeln $z_i, i = 1, 2, 3, 4$ von 1 gibt (also $z_i^2 \equiv_n 1$), dann folgt für $x^2 \equiv_n y$:

$$(xz_i)^2 \equiv_n x^2 z_i^2 \equiv_n y \tag{4.5}$$

Nach dem Chinesischen Restsatz gilt $Z_n \cong Z_p \times Z_q$. Es gibt mindestens vier Quadratwurzeln von 1, denn $1, n-1, x_1, x_2$ mit

$$\begin{aligned} x_1 &\equiv_p 1 \quad && x_1 \equiv_q -1 \\ x_2 &\equiv_p -1 \quad && x_2 \equiv_q 1 \end{aligned}$$

sind Quadratwurzeln von 1. Sei umgekehrt z eine Quadratwurzel von 1 in Z_n, also $z^2 \equiv_n 1$, dann muss nach dem Chinesischen Restsatz auch $z^2 \equiv_p 1$ und $z^2 \equiv_q 1$ gelten, also $z \equiv_p \pm 1$ und $z \equiv_q \pm 1$. □

Da im allgemeinen in nicht-abelschen Gruppen, wie den Matrizengruppen $GL(2, Z_p)$ und $SL(2, Z_p)$, nicht $(AB)^2 = A^2B^2$ für $A, B \in GL(2, Z_p)$ gilt, soll im Folgenden geklärt werden, wann für zwei Matrizen $A, B \in GL(2, Z_p)$ $AB \equiv_p BA$ und somit auch $(AB)^2 \equiv_p A^2B^2$ gilt.

4.5.3.2 Satz: Seien $A := \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ und $B := \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}$ Matrizen aus $GL(2, Z_n)$, dann gilt $AB \equiv_n BA$ genau dann, wenn:

$$\begin{aligned} b_{12}a_{21} &\equiv_n a_{12}b_{21} \\ (a_{11} - a_{22})b_{12} &\equiv_n (b_{11} - b_{22})a_{12} \end{aligned}$$

Beweis:

Es gilt:

$$AB \equiv_n \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \equiv_n \begin{pmatrix} a_{11}b_{11} + a_{12}b_{21} & a_{11}b_{12} + a_{12}b_{22} \\ a_{21}b_{11} + a_{22}b_{21} & a_{21}b_{12} + a_{22}b_{22} \end{pmatrix}$$

$$BA \equiv_n \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix} \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \equiv_n \begin{pmatrix} b_{11}a_{11} + b_{12}a_{21} & b_{11}a_{12} + b_{12}a_{22} \\ b_{21}a_{11} + b_{22}a_{21} & b_{21}a_{12} + b_{22}a_{22} \end{pmatrix}$$

Dann folgt, dass $AB \equiv_n BA$ genau dann erfüllt ist, wenn die folgenden Gleichungen gelten:

$$\begin{aligned} a_{11}b_{11} + a_{12}b_{21} &\equiv_n b_{11}a_{11} + b_{12}a_{21} \\ a_{11}b_{12} + a_{12}b_{22} &\equiv_n b_{11}a_{12} + b_{12}a_{22} \\ a_{21}b_{11} + a_{22}b_{21} &\equiv_n b_{21}a_{11} + b_{22}a_{21} \\ a_{21}b_{12} + a_{22}b_{22} &\equiv_n b_{21}a_{12} + b_{22}a_{22} \end{aligned}$$

Diese Gleichungen können in die beiden folgenden Gleichungen überführt werden:

$$\begin{aligned} a_{12}b_{21} &\equiv_n b_{12}a_{21} \\ (a_{11} - a_{22})b_{12} &\equiv_n (b_{11} - b_{22})a_{12} \end{aligned}$$

□

Bemerkung:

Die beiden Gleichungen entsprechen den Gleichungen aus Satz (4.2.1.1).

4.5.3.3 Korollar: Seien $A := \begin{pmatrix} a_{11} & 0 \\ 0 & a_{22} \end{pmatrix}$ und $B := \begin{pmatrix} b_{11} & 0 \\ 0 & b_{22} \end{pmatrix}$ Diagonalmatrizen aus $GL(2, Z_n)$, dann gilt $AB \equiv_n BA$.

Beweis:

Die Behauptung folgt direkt aus der Kommutativität von Z_n^*. □

4.5.3.4 Satz: Seien A, B Matrizen aus $GL(2, Z_p)$ mit $B \equiv_p A^k$, wobei B keine Diagonalmatrix der Form $\begin{pmatrix} b_{11} & 0 \\ 0 & b_{11} \end{pmatrix}$ ist. Dann gilt: Sind B, k, $Spur(A)$ und $Det(A)$ bekannt, so ist damit A eindeutig bestimmt.

Beweis:

Ist A eine Diagonalmatrix, so ist $Spur(A)^2 - 4Det(A)$ ein quadratischer Rest, und auf der Hauptdiagonalen stehen die beiden Werte $\frac{Spur(A)+\sqrt{(Spur(A))^2-4Det(A)}}{2}$ und $\frac{Spur(A)-\sqrt{(Spur(A))^2-4Det(A)}}{2}$. Da $Spur(A)^2-4Det(A)$ ein quadratischer Rest in Z_p^* ist, können die Quadratwurzeln in Z_p^* berechnet und somit die beiden Einträge auf der Hauptdiagonalen bestimmt werden. Welcher Eintrag an die Stelle a_{11} gehört, kann durch Ausprobieren und Berechnen von A^k bestimmt werden.

Sei A keine Diagonalmatrix, d.h. einer der Einträge $a_{12}, a_{21} \not\equiv_p 0$ (oBdA sei $a_{12} \not\equiv_p 0$). Da B in dem Erzeugnis von A liegt, müssen A und B die gleichen Konstanten aus Korollar (4.2.1.2) besitzen. Wäre B eine Diagonalmatrix, so folgt aus der zweiten Gleichung aus Satz (4.2.1.1) ($(a_{11} - a_{22})b_{12} \equiv_p (b_{11} - b_{22})a_{12}$), dass $b_{11} \equiv_p b_{22}$ gilt. Somit wäre $B \equiv_p \begin{pmatrix} b_{11} & 0 \\ 0 & b_{11} \end{pmatrix}$. Dies ist ein Widerspruch zur Satzvoraussetzung.

Sei also B keine Diagonalmatrix (oBdA sei $b_{12} \not\equiv_p 0$). Dann gilt:

$$\begin{aligned} K_1 &\equiv_p a_{12}^{-1}a_{21} \equiv_p b_{12}^{-1}b_{21} \\ K_2 &\equiv_p (a_{11} - a_{22})a_{12}^{-1} \equiv_p (b_{11} - b_{22})b_{12}^{-1} \end{aligned}$$

Nach Satz (4.2.1.6) gilt für $B \equiv_p A^k$:

$$\begin{aligned} Spur(B) &\equiv_p \alpha^k + \beta^k \\ b_{12}a_{12}^{-1} &\equiv_p a_{12}^{(k)}a_{12}^{-1} \equiv_p \frac{\alpha^k - \beta^k}{\alpha - \beta} \\ b_{21}a_{21}^{-1} &\equiv_p a_{21}^{(k)}a_{21}^{-1} \equiv_p \frac{\alpha^k - \beta^k}{\alpha - \beta} \end{aligned}$$

mit $\alpha \equiv_p \frac{Spur(A)+\sqrt{(Spur(A))^2-4Det(A)}}{2}$ und $\beta \equiv_p \frac{Spur(A)-\sqrt{(Spur(A))^2-4Det(A)}}{2}$.

Ist $Spur(A)$ und $Det(A)$ bekannt, so können $\alpha, \beta, \alpha^k, \beta^k$ in dem Zerfällungskörper von $P_A(X)$ berechnet werden. Somit ist auch die Bestimmung der Elemente $a_{12} \equiv_p b_{12}\frac{\alpha-\beta}{\alpha^k-\beta^k}$ und $a_{21} \equiv_p b_{21}\frac{\alpha-\beta}{\alpha^k-\beta^k}$ möglich. Zusammen mit K_2 und a_{12} kann $a_{11} - a_{22} \equiv_p K_2 a_{12}$ berechnet werden.

Da die $Spur(A) \equiv_p a_{11} + a_{22}$ bekannt ist, können auch a_{11} und a_{22} bestimmt werden:

$$\begin{aligned} a_{11} &\equiv_p K_2 a_{12} + a_{22} \equiv_p K_2 a_{12} + Spur(A) - a_{11} \\ \Rightarrow a_{11} &\equiv_p 2^{-1}(K_2 a_{12} + Spur(A)) \\ a_{22} &\equiv_p Spur(A) - a_{11} \end{aligned}$$

Somit ist A vollständig bestimmt. □

4.5.3.5 Korollar: Sei A eine Matrix aus $GL(2, Z_p)$, die keine Diagonalmatrix ist. Dann gilt: Sind $Spur(A)$, $Det(A)$ und die Konstanten K_1, K_2 aus Korollar (4.2.1.2) bekannt, ist damit A eindeutig bis auf Vertauschung der Einträge auf der Hauptdiagonalen bestimmt.

Beweis:

Es gilt nach dem Beweis von Satz (4.5.3.4):

$$\begin{aligned} K_1 &\equiv_p a_{12}^{-1} a_{21} \equiv_p b_{12}^{-1} b_{21} \\ K_2 &\equiv_p (a_{11} - a_{22}) a_{12}^{-1} \equiv_p (b_{11} - b_{22}) b_{12}^{-1} \\ Spur(A) &\equiv_p a_{11} + a_{22} \\ Det(A) &\equiv_p a_{11} a_{22} - a_{12} a_{21} \end{aligned}$$

Es folgt:

$$\begin{aligned} a_{11} &\equiv_p 2^{-1}(Spur(A) + a_{12} K_2) \\ a_{22} &\equiv_p 2^{-1}(Spur(A) - a_{12} K_2) \\ \Rightarrow Det(A) &\equiv_p \frac{(Spur(A) + a_{12} K_2)(Spur(A) - a_{12} K_2)}{4} - a_{12}^2 K_1 \\ &\equiv_p \frac{((Spur(A))^2 - a_{12}^2 K_2^2) - 4 a_{12}^2 K_1}{4} \\ \Rightarrow a_{12} &\equiv_p \sqrt{\frac{((Spur(A))^2 - 4 Det(A)}{K_2^2 + 4 K_1}} \end{aligned}$$

Da Z_p ein Körper ist, kann es in Z_p für vorgegebene K_1, K_2 maximal zwei mögliche Lösungen für a_{12} geben. Wie aus dem Beweis von Satz (4.5.3.4) bereits hervorgeht, sind bei gegebenem $a_{12}, K_1, K_2, Spur(A), Det(A)$ die restlichen Einträge der Matrix A eindeutig

bestimmbar. Es gibt also höchstens 2 Matrizen $\in GL(2, Z_p)$, die die gleiche Spur, die gleiche Determinante und die gleichen Konstanten K_1, K_2 besitzen.

Da mit $A := \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$ auch $A' := \begin{pmatrix} a_{22} & -a_{12} \\ a_{21} & a_{11} \end{pmatrix}$ alle obigen Vorgaben erfüllt, ist A bis auf Vertauschung der Einträge auf der Hauptdiagonalen eindeutig bestimmt. □

4.5.3.6 Satz: Es seien p, q Primzahlen und sei $n = pq$. Seien A, B Matrizen aus $GL(2, Z_n)$ mit $B \equiv_n A^k$, wobei B mod p und B mod q jeweils keine Diagonalmatrix der Form $\begin{pmatrix} b_{11} & 0 \\ 0 & b_{11} \end{pmatrix}$ ist. Dann gilt: Sind B, k, $Spur(A)$ und $Det(A)$ bekannt, so ist A damit eindeutig bestimmt.

Beweis:

Die Behauptung folgt aus Satz (4.5.3.4) und dem Chinesischen Restsatz für Matrizen (Satz (3.2.1.7)). □

4.5.3.7 Korollar: Sei A eine Matrix aus $GL(2, Z_n)$, die keine Diagonalmatrix ist. Es gelte $ggT(a_{12}, n) = ggT(a_{21}, n) = 1$, dann folgt: Sind $Spur(A)$, $Det(A)$ und die Konstanten K_1, K_2 aus Korollar (4.2.1.2) bekannt, so ist damit A eindeutig bis auf Vertauschung der Einträge auf der Hauptdiagonalen bestimmt.

Beweis:

Folgt aus Korollar (4.5.3.5) zusammen mit dem Chinesischen Restsatz für Matrizen (Satz (3.2.1.7)). □

Quadratwurzeln in $SL(2, Z_n)$

Der folgende Abschnitt beschäftigt sich mit Quadratwurzeln in der Gruppe $SL(2, Z_n)$, wobei $n = pq$ das Produkt der beiden Primzahlen p und q ist. Dabei werden die Aussagen zunächst für die Gruppe $SL(2, Z_p)$ bewiesen und dann auf zusammengesetzte Zahlen $n = pq$ erweitert. Am Ende des Abschnitts wird ein Verfahren angegeben, wie ein Algorithmus, der Quadratwurzeln in $SL(2, Z_n)$ berechnet, zur Faktorisierung von n verwendet werden kann.

Zunächst wird gezeigt, dass für zwei Quadratwurzeln A, B einer Matrix gilt, dass das Produkt $(A - B)(A + B)$ immer die Nullmatrix ergibt.

4.5.3.0.17 Satz: Seien A und B Matrizen aus $SL(2, Z_p)$ mit $A^2 \equiv_p B^2 \equiv_p C$ mit $C^2 \not\equiv_p \pm I$. Dann folgt $(A - B)(A + B) \equiv_p \overline{0}$.

Beweis:

Es gilt $A^2 - B^2 \equiv_p \overline{0}$. In diesem Beweis werden zwei Fälle unterschieden, je nachdem, ob C eine Diagonalmatrix ist oder nicht.

Sei zunächst C keine Diagonalmatrix. Da C keine Diagonalmatrix ist, ist weder A noch B eine Diagonalmatrix. OBdA sei $a_{12} \not\equiv_p 0$. Nach Korollar (4.2.1.2) müssen alle Matrizen aus $< A >$ die gleichen Konstanten aus Korollar (4.2.1.2) besitzen. Ebenso müssen alle Matrizen aus $< B >$ die gleichen Konstanten besitzen. Aus $A^2 \equiv_p B^2$ folgt, dass auch A und B die gleichen Konstanten besitzen. Aus Satz (4.5.3.2) folgt, dass Matrizen, die die gleichen Konstanten besitzen, bezüglich Matrizenmultiplikation vertauschbar sind. Es folgt:

$$\begin{aligned} \overline{0} &\equiv_p A^2 - B^2 \equiv_p AA - BB \equiv_p AA + AB - BA - BB \\ &\equiv_p (A - B)(A + B) \end{aligned}$$

Sei nun C eine Diagonalmatrix. Sind A und B ebenfalls Diagonalmatrizen, so gilt nach Korollar (4.5.3.3) $AB \equiv_p BA$ und somit

$$\begin{aligned} \overline{0} &\equiv_p A^2 - B^2 \equiv_p AA - BB \equiv_p AA + AB - BA - BB \\ &\equiv_p (A - B)(A + B) \end{aligned}$$

Sei also eine der beiden Matrizen A, B (oBdA A) keine Diagonalmatrix (oBdA sei A keine Diagonalmatrix und $a_{12} \not\equiv_p 0$). Es gilt:

$$C \equiv_p \begin{pmatrix} c_{11} & c_{12} \\ c_{21} & c_{22} \end{pmatrix} \equiv_p A^2 \equiv_p \begin{pmatrix} a_{11}^2 + a_{12}a_{21} & a_{12}(a_{11} + a_{22}) \\ a_{21}(a_{11} + a_{22}) & a_{22}^2 + a_{12}a_{21} \end{pmatrix}$$

Da $a_{12} \not\equiv_p 0$ gilt, folgt $a_{11} + a_{22} \equiv_p 0$, also $a_{11} \equiv_p -a_{22}$. Es folgt: $c_{11} \equiv_p a_{11}^2 + a_{12}a_{21} \equiv_p a_{22}^2 + a_{12}a_{21} \equiv_p c_{22}$ und $Det(C) \equiv_p 1 \equiv_p c_{11}c_{22} \equiv_p c_{11}^2$. Somit wäre $c_{11} \equiv_p c_{22} \pm 1$, also $C \equiv_p \pm I$, was ein Widerspruch zur Voraussetzung $C \not\equiv_p \pm I$ ist. □

4.5.3.0.18 Bemerkung: Aus der Tatsache, dass $(A - B)(A + B) \equiv_p \overline{0}$ gilt, folgt nicht $A \equiv_p \pm B$, da der Matrizenring über dem Körper Z_p Nullteiler enthält. Aber es gilt $Det(A - B) \equiv_p 0$ oder $Det(A + B) \equiv_p 0$.

4.5.3.0.19 Korollar: Seien A und B Matrizen aus $SL(2, Z_n)$ mit $n = pq$ und $A^2 \equiv_n B^2 \equiv_n C$ mit $C^2 \not\equiv_p \pm I$ und $C^2 \not\equiv_q \pm I$. Dann folgt $(A - B)(A + B) \equiv_n \overline{0}$ in $SL(2, Z_n)$.

Beweis:

Die Behauptung folgt direkt aus dem vorherigen Satz zusammen mit dem Chinesischen Restsatz für Matrizen (Satz (3.2.1.7)). □

4.5.3.0.20 Satz: Es gibt genau zwei Quadratwurzeln von I, die in $SL(2, Z_p)$ liegen. Diese sind I und $-I$.

Beweis:

Sei A eine Matrix in $SL(2, Z_p)$ mit $A^2 \equiv_p I$. Es werden zwei Fälle unterschieden, je nachdem, ob A eine Diagonalmatrix ist oder nicht.

Sei zunächst A eine Diagonalmatrix. Ist A eine Diagonalmatrix, so folgt $Det(A) \equiv_p a_{11}a_{22} \equiv_p 1$, und somit $a_{11} \equiv_p a_{22}^{-1}$. Des weiteren folgt aus $A^2 \equiv_p I$:

$$a_{11}^2 \equiv_p 1 \equiv_p a_{22}^2$$

Zusammen folgt $a_{11} \equiv_p a_{22} \equiv_p \pm 1$ und somit $A \equiv_p \pm I$.

Angenommen, A ist keine Diagonalmatrix, dann ist eines der beiden Elemente a_{12}, a_{21} auf der Nebendiagonalen ungleich 0.

Es gilt:

$$I \equiv_p A^2 \equiv_p \begin{pmatrix} a_{11}^2 + a_{12}a_{21} & a_{12}(a_{11} + a_{22}) \\ a_{21}(a_{11} + a_{22}) & a_{22}^2 + a_{12}a_{21} \end{pmatrix}$$

Somit folgt, dass $Spur(A) \equiv_p 0$ gelten muss, also $a_{11} \equiv_p -a_{22}$. Es folgt für Det(A): $Det(A) \equiv_p a_{11}a_{22} - a_{12}a_{21} \equiv_p -a_{11}^2 - a_{12}a_{21} \equiv_p -(a_{11}^2 + a_{12}a_{21}) \equiv_p -1$. Dies wäre aber ein Widerspruch zu $A \in SL(2, Z_p)$. □

4.5.3.0.21 Satz: Seien A, B Matrizen aus $SL(2, Z_p)\backslash\{\pm I\}$ mit $A \equiv_p B^2$, dann gibt es genau eine weitere Matrix C aus $SL(2, Z_p)$ mit $C^2 \equiv_p A$ und es gilt $C \equiv_p -B$.

Beweis:

Mit $B \in SL(2, Z_p)$ gilt auch $-B \in SL(2, Z_p)$, also gibt es mindestens zwei quadratische Wurzeln von A. Sei C eine quadratische Wurzel von A mit $C^2 \equiv_p A$.

Wieder werden zwei Fälle unterschieden. Sei zunächst A keine Diagonalmatrix. Ist A keine Diagonalmatrix, so kann auch weder B noch C eine Diagonalmatrix sein. D.h. mindestens einer der Elemente b_{12}, b_{21} (bzw. $c_{12}, c21$) ist ungleich $0 \bmod p$. Seien oBdA $b_{12}, c_{12} \not\equiv_p 0$. Nach Satz (4.2.1.1) gilt:

$$\begin{aligned} b_{12}a_{21} &\equiv_p a_{12}b_{21} \\ (a_{11} - a_{22})b_{12} &\equiv_p (b_{11} - b_{22})a_{12} \\ c_{12}a_{21} &\equiv_p a_{12}c_{21} \\ (a_{11} - a_{22})c_{12} &\equiv_p (c_{11} - c_{22})a_{12} \end{aligned}$$

und somit:

$$\begin{aligned} b_{12}c_{21} &\equiv_p c_{12}b_{21} \\ (c_{11} - c_{22})b_{12} &\equiv_p (b_{11} - b_{22})c_{12} \end{aligned}$$

Nach Satz (4.5.3.2) gilt somit $BC \equiv_p CB$ und $C^{-1}B \equiv_p BC^{-1} \in SL(2, Z_p)$. Es folgt:

$$(BC^{-1})^2 \equiv_p BC^{-1}BC^{-1} \equiv_p BBC^{-1}C^{-1} \equiv_p AA^{-1} \equiv_p I$$

Also ist BC^{-1} eine Quadratwurzel von I und somit nach Satz (4.5.3.0.20) gleich $\pm I$. Es folgt $C \equiv_p \pm B$.

Sei nun A eine Diagonalmatrix. Sind B und C ebenfalls Diagonalmatrizen, so gilt $BC \equiv_p CB$ und die Behauptung folgt wie oben. Sei also mindestens eine der beiden Matrizen B, C keine Diagonalmatrix. oBdA sei $b_{12} \not\equiv_p 0$. Da $a_{12} \equiv_p b_{12}(b_{11} + b_{22}) \equiv_p 0$ gilt, folgt $b_{11} \equiv_p -b_{22}$. Es gilt $1 \equiv_p Det(B) \equiv_p -b_{11}^2 - b_{12}b_{21}$. Des Weiteren gilt $a_{11} \equiv_p b_{11}^2 + b_{12}b_{21}$ und $a_{22} \equiv_p b_{11}^2 + b_{12}b_{21}$. Da A eine Diagonalmatrix ist, folgt zusammen:

$$A \equiv_p \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \equiv_p -I$$

Dies ist aber ein Widerspruch zur Voraussetzung $A \in SL(2, Z_p) \backslash \{\pm I\}$. □

4.5.3.0.22 Korollar: Seien p, q Primzahlen und seien A, B Matrizen aus $SL(2, Z_n)$ mit $A \equiv_n B^2$ und $n = pq$, so dass $A \not\equiv_p \pm I$ und $A \not\equiv_q \pm I$. Dann gibt es genau 4 Matrizen C_i aus $SL(2, Z_n)$ mit $C_i^2 \equiv_n A$.

Beweis:

Der Beweis folgt aus Satz (4.5.3.0.20) und Satz (4.5.3.0.21) zusammen mit dem Chinesischen Restsatz für Matrizen (Satz (3.2.1.7)). □

Die Frage, wann überhaupt eine Matrix $A \in SL(2, Z_p)$ ein quadratischer Rest ist, wird durch den folgenden Satz beantwortet:

4.5.3.0.23 Satz: Sei A eine Matrix aus $SL(2, Z_p)$. Genau dann ist A ein quadratischer Rest in $SL(2, Z_p)$, wenn gilt: $Spur(A) + 2$ ist ein quadratischer Rest in Z_p^*.

Beweis:

"$\Rightarrow$" Ist A ein quadratischer Rest in $SL(2, Z_p)$, dann gibt es eine Matrix $B \in SL(2, Z_p)$ mit $B^2 \equiv_p A$. Nach Satz (4.2.1.5) gilt $Spur(A) \equiv_p Spur(B)Spur(B^1) - Det(B)Spur(B^0) \equiv_p (Spur(B))^2 - 2$. Also ist $Spur(A) + 2$ ein quadratischer Rest in Z_p^*.

"$\Leftarrow$" Angenommen, $Spur(A) + 2$ ist ein quadratischer Rest in Z_p^*, dann gibt es ein $g \in Z_p^*$ mit $g^2 \equiv_p Spur(A) + 2$. Setzt man $g \equiv_p Spur(B)$, dann gibt es nach Satz (4.5.3.4) eine Matrix $B \in < A >$, die sich eindeutig bis auf die Reihenfolge der Einträge auf der Hauptdiagonalen bestimmen lässt und die gleichen Konstanten wie A besitzt. Für den nicht durch Satz (4.5.3.4) abgedeckten Fall, dass B die Form $\begin{pmatrix} b_{11} & 0 \\ 0 & b_{11} \end{pmatrix}$ besitzt, folgt $B \equiv_p \pm I$ und $A \equiv_p I$.

Ist B^2 eine Matrix, welche die gleichen Konstanten, die gleiche Spur und die gleiche Determinante wie A besitzt, so existieren nach Korollar (4.5.3.5) nur zwei Matrizen, die diese Vorgaben erfüllen können. Diese unterscheiden sich in der Reihenfolge der Einträge auf der Hauptdiagonalen und der Multiplikation der Nebendiagonalen mit -1. Für eine Matrix $A \in SL(2, Z_p)$ ist die von A verschiedene Matrix, die die gleichen Konstanten und die gleiche Spur besitzt, also gleich A^{-1}. Gilt also $B^2 \not\equiv_p A$, so folgt $(B^{-1})^2 \equiv_p A$. Dann ist A ein quadratischer Rest in $SL(2, Z_p)$. □

4.5.3.0.24 Korollar: Sei A eine Matrix aus $SL(2, Z_p)$. Kennt man eine Quadratwurzel $B \in SL(2, Z_p)$ von A, so kennt man auch eine Quadratwurzel von $Spur(A) + 2$ in Z_p^*.

Beweis:

Aus dem ersten Teil des Beweises von Satz (4.5.3.0.23) folgt $(Spur(B))^2 \equiv_p Spur(A)+2$. Also ist $Spur(B)$ eine Quadratwurzel von $Spur(A) + 2$. □

4.5.3.0.25 Korollar: Es seien p, q Primzahlen und $n = pq$. Sei A eine Matrix aus $SL(2, Z_n)$. Genau dann ist A ein quadratischer Rest in $SL(2, Z_n)$, wenn gilt: $Spur(A) + 2$ ist ein quadratischer Rest in Z_n^*.

Beweis:

Die Behauptung folgt direkt aus Satz (4.5.3.0.23) zusammen mit dem Chinesischen Restsatz für Matrizen (Satz (3.2.1.7)).

4.5.3.0.26 Korollar: Es seien p, q Primzahlen und $n = pq$. Sei A eine Matrix aus $SL(2, Z_n)$. Kennt man eine Quadratwurzel $B \in SL(2, Z_n)$ von A, so kennt man auch eine Quadratwurzel von $Spur(A) + 2$ in Z_n^*.

Beweis:

Die Behauptung folgt direkt aus Korollar (4.5.3.0.24) zusammen mit dem Chinesischen Restsatz für Matrizen (Satz (3.2.1.7)).

4.5.3.0.27 Satz: Es seien p, q Primzahlen und $n = pq$. Ein Algorithmus, der in $SL(2, Z_n)$ Quadratwurzeln berechnen kann, kann dazu verwendet werden, n zu faktorisieren.

Beweis:

Ein Algorithmus, der für einen quadratischen Rest $A \in SL(2, Z_n)$ eine Wurzel berechnen kann, berechnet nach Korollar (4.5.3.0.26) eine Quadratwurzel aus $Spur(A) + 2$.

Um n zu faktorisieren, wählt man eine zufällige Matrix $B \in SL(2, Z_n)$ und berechnet $A \equiv_n B^2$. A gibt man als Eingabe in den Algorithmus, der Wurzeln in $SL(2, Z_n)$ berechnen kann. Erhält man als Rückgabewert von A eine Matrix C, für die gilt $C \not\equiv_n \pm B$, so erhält man auch eine wesentlich verschiedene Wurzel von $Spur(A) + 2$. Mit Hilfe von zwei wesentlich verschiedenen Wurzeln kann n faktorisiert werden. □

Kubische Wurzeln in $SL(2, Z_n)$

Der folgende Abschnitt beschäftigt sich mit kubischen Wurzeln in der Gruppe $SL(2, Z_n)$ ($n = pq$). Die gesonderte Betrachtung kubischer Wurzeln in $SL(2, Z_p)$ resultiert aus der Tatsache, dass in der Gruppe $SL(2, Z_p)$ immer Matrizen existieren, die mehrere (verschiedene) dritte Wurzeln besitzen. Daher wird durch Kenntnis zweier wesentlich verschiedener dritter Wurzeln einer Matrix aus $SL(2, Z_n)$ immer auch die Faktorisierung von n ermöglicht.

Wie im vorherigen Abschnitt werden die Aussagen zunächst für die Gruppe $SL(2, Z_p)$ bewiesen und dann auf zusammengesetzte Zahlen $n = pq$ erweitert. Am Ende des Abschnitts wird ein Verfahren angegeben, wie ein Algorithmus, der Kubische Wurzeln in $SL(2, Z_n)$ berechnet, zur Faktorisierung von n verwendet werden kann.

Zu einer Matrix aus $SL(2, Z_p)$ kann es sowohl eine eindeutige dritte Wurzel aus $SL(2, Z_p)$ geben also auch mehrere dritte Wurzeln. Der folgende Satz zeigt auf, wie viele Wurzeln es zu einer Matrix in $SL(2, Z_p)$ geben kann.

4.5.3.0.28 Satz: Seien A, B Matrizen aus $SL(2, Z_p)\backslash\{\pm I\}$ mit $A \equiv_p B^3$, dann gibt es entweder keine weitere dritte Wurzel von A, oder genau zwei weitere Matrizen C_1, C_2 aus $SL(2, Z_p)$ mit $C_i^3 \equiv_p A$.

Beweis:

Zunächst soll gezeigt werden, dass sowohl Matrizen in $SL(2, Z_p)$ existieren, die eine eindeutige dritte Wurzel besitzen, als auch Matrizen, die drei verschiedene dritte Wurzeln in $SL(2, Z_p)$ besitzen.

Es gilt nach Satz (3.2.1.5) $|SL(2, Z_p)| = (p-1)p(p+1)$, somit teilt die Zahl 3 genau eine der Zahlen $p-1, p, p+1$. Nach Korollar (4.3.2.3) beträgt die maximale Ordnung einer Matrix aus $SL(2, Z_p)$ genau $2p$.

Nach Satz (4.3.2.5) existieren Matrizen aus $SL(2, Z_p)$, deren Ordnung $p+1$ beträgt.

Diagonalisierbare Matrizen in $SL(2, Z_p)$ besitzen eine Ordnung, die $p-1$ teilt.

Es werden nun die folgenden drei Fälle unterschieden:

1. $3|p-1$:

   Somit gilt $3 \not| p+1$. Nach Satz (4.3.2.5) existieren Matrizen, die die Ordnung $p+1$ besitzen. Wählt man eine solche Matrix A, so gibt es

nur eine Matrix $B \in SL(2, Z_p)$ mit $B^3 \equiv_p A$ und $ord(B) = p+1$. Gäbe es eine weitere Matrix $C \in SL(2, Z_p)$ mit $C^3 \equiv_p A$, so hätte diese die Ordnung $3(p+1) = 3p+3 > 2p$, was einen Widerspruch zu Korollar (4.3.2.3) darstellt.

2. $3 = p$:

   Somit gilt $3 \not| p+1$. Dieser Fall kann wie Fall 1 behandelt werden.

3. $3|p+1$:

   Somit gilt $3 \not| p-1$. Nach Korollar (4.3.2.1) existieren Matrizen, die die Ordnung $p-1$ besitzen. Wählt man eine solche Matrix A, so gibt es nur eine Matrix $B \in SL(2, Z_p)$ mit $B^3 \equiv_p A$ und $ord(B) = p-1$. Gäbe es eine weitere Matrix $C \in SL(2, Z_p)$ mit $C^3 \equiv_p A$, so hätte diese die Ordnung $3(p-1) = 3p-3 > 2p$ für $p > 3$, was einen Widerspruch zu Korollar (4.3.2.3) darstellt.

Nun wird gezeigt, dass es, wenn mehrere dritte Wurzeln einer Matrix $A \in SL(2, Z_p)$ existieren, mindestens 3 unterschiedliche dritte Wurzeln geben muss. Angenommen, es gäbe Matrizen $B, C \in SL(2, Z_p)$ mit $B^3 \equiv_p C^3 \equiv_p A$ und $B \not\equiv_p C$, so sind wieder die beiden folgenden Fälle zu unterscheiden:

1. Sei A keine Diagonalmatrix. Ist A keine Diagonalmatrix, so kann weder B noch C eine Diagonalmatrix sein. D.h. mindestens eines der beiden Elemente b_{12}, b_{21} (bzw. c_{12}, c_{21}) ist ungleich 0 mod p. Seien oBdA $b_{12}, c_{12} \not\equiv_p 0$. Nach Satz (4.2.1.1) gilt:

$$\begin{aligned} b_{12}a_{21} &\equiv_p a_{12}b_{21} \\ (a_{11}-a_{22})b_{12} &\equiv_p (b_{11}-b_{22})a_{12} \\ c_{12}a_{21} &\equiv_p a_{12}c_{21} \\ (a_{11}-a_{22})c_{12} &\equiv_p (c_{11}-c_{22})a_{12} \end{aligned}$$

und somit:

$$\begin{aligned} b_{12}c_{21} &\equiv_p c_{12}b_{21} \\ (c_{11} - c_{22})b_{12} &\equiv_p (b_{11} - b_{22})c_{12} \end{aligned}$$

Nach Satz (4.5.3.2) gilt dann $BC \equiv_p CB$ und somit auch $C^{-1}B \equiv_p BC^{-1} \in SL(2, Z_p)$. Es folgt:

$$(BC^{-1})^3 \equiv_p BC^{-1}BC^{-1}BC^{-1} \equiv_p BBBC^{-1}C^{-1}C^{-1} \equiv_p AA^{-1} \equiv_p I$$

Also ist BC^{-1} eine dritte Wurzel von I.

Es folgt, dass $(BC^{-1})^2 \equiv_p (BC^{-1})^{-1}$ ebenfalls eine dritte Wurzel von I und somit CCB^{-1} ebenfalls eine dritte Wurzel von A ist. Also gibt es mindestens drei verschiedene Wurzeln von A.

2. Sei A eine Diagonalmatrix. Sind B und C ebenfalls Diagonalmatrizen, so gilt $BC \equiv_p CB$, und die Behauptung folgt wie oben.

   Sei also mindestens eine der beiden Matrizen B, C keine Diagonalmatrix. OBdA sei $b_{12} \not\equiv_p 0$.

   Da

   $$a_{12} \equiv_p b_{12}(b_{11}^2 + b_{11}b_{22} + b_{22}^2 + b_{12}b_{21}) \equiv_p b_{12}((b_{11} + b_{22})^2 - Det(B)) \equiv_p 0$$

   gilt, folgt

   $$(b_{11} + b_{22})^2 \equiv_p Det(B) \equiv_p 1 \text{und somit } b_{22} \equiv_p 1 - b_{11} \vee b_{22} \equiv_p -1 - b_{11}$$

   Dann gilt für a_{11}:

   $$\begin{aligned} a_{11} &\equiv_p b_{11}^3 + 2b_{11}b_{12}b_{21} + b_{22}b_{12}b_{21} \\ &\equiv_p b_{11}^3 + (b_{11}b_{22} - Det(B))(2b_{11} - b_{22}) \\ &\equiv_p b_{11}^3 + 2b_{11}^2b_{22} + b_{11}b_{22}^2 - Det(B)(2b_{11} + b_{22}) \\ &\equiv_p b_{11}^3 - 2b_{11}^3 \pm 2b_{11}^2 + b_{11}^3 \mp 2b_{11}^2 + b_{11} - Det(B)(2b_{11} - b_{11} \pm 1) \\ &\equiv_p b_{11} - Det(B)(b_{11} \pm 1) \equiv_p \pm 1 \end{aligned}$$

Ebenso gilt für a_{22}:

$$\begin{aligned} a_{22} &\equiv_p b_{22}^3 + 2b_{22}b_{12}b_{21} + b_{11}b_{12}b_{21} \\ &\equiv_p b_{22}^3 + 2b_{22}^2 b_{11} + b_{22}b_{11}^2 - Det(B)(2b_{22} + b_{11}) \\ &\equiv_p b_{22}^3 - 2b_{22}^3 \pm 2b_{22}^2 + b_{22}^3 \mp 2b_{22}^2 + b_{22} - Det(B)(2b_{22} - b_{22} \pm 1) \\ &\equiv_p b_{22} - Det(B)(b_{22} \pm 1) \equiv_p \pm 1 \end{aligned}$$

Zusammen folgt $A \equiv_p \pm I$. Dies ist aber ein Widerspruch zur Voraussetzung $A \in SL(2, Z_p)\backslash\{\pm I\}$. Also gilt auch in dem Fall, dass A eine Diagonalmatrix ist, dass A entweder genau eine oder mindestens 3 diskrete Wurzeln besitzt.

Es kann aber auch höchstens 3 Wurzeln $C_i \in SL(2, Z_p)$ von einer Matrix $A \in SL(2, Z_p)\backslash\{\pm I\}$ geben, da nach Satz (4.2.1.5) für jede kubische Wurzel $C_i \in SL(2, Z_p)$ von A gilt:

$$\begin{aligned} Spur(A) &\equiv_p Spur(C_i)Spur(C_i^2) - 1Spur(C_i) \\ &\equiv_p Spur(C_i)(Spur(C_i)Spur(C_i) - 2) - 1Spur(C_i) \\ &\equiv_p (Spur(C_i))^3 - 3Spur(C_i) \end{aligned}$$

Also sind die Elemente $Spur(C_i)$ die Nullstellen der kubischen Gleichung $X^3 - 3X \equiv_p Spur(A)$. Es kann höchstens 3 verschiedene Elemente $Spur(C_i)$ geben, die diese Gleichung erfüllen, da Z_p ein Körper ist. Zusammen mit $Det(C_i) \equiv_p 1$ gibt es nach Satz (4.5.3.4) höchstens 3 verschiedene Matrizen C_i mit $C_i^3 \equiv_p A$. □

4.5.3.0.29 Korollar: Seien p und q Primzahlen und $n = pq$. Seien A, B Matrizen aus $SL(2, Z_n)\backslash\{\pm I\}$ mit $A \equiv_n B^3$, dann gibt es entweder keine weitere dritte Wurzel von A, genau 2 oder genau 8 weitere Matrizen $C_i \in SL(2, Z_p)$ mit $C_i^3 \equiv_p A$.

Beweis:

Die Behauptung folgt direkt aus Satz (4.5.3.0.28) zusammen mit dem Chinesischen Restsatz für Matrizen (Satz (3.2.1.7)). □

4.5.3.0.30 Satz: Es seien p, q Primzahlen und $n = pq$. Ein Algorithmus, der in $SL(2, Z_n)$ kubische Wurzeln berechnen kann, kann dazu verwendet werden, n zu faktorisieren.

Beweis:

Ein Algorithmus, der für einen kubischen Rest $A \in SL(2, Z_n)$ eine kubische Wurzel C_i berechnen kann, berechnet nach Korollar (4.5.3.0.29) eine von höchstens 9 kubischen Wurzeln modulo n.

Um n zu faktorisieren, wählt man eine zufällige Matrix $B \in SL(2, Z_n)$ und berechnet $A \equiv_n B^3$. A gibt man als Eingabe in den Algorithmus, der kubische Wurzeln $C_i \in SL(2, Z_p)$ berechnen kann. Erhält man als Rückgabewert von A eine Matrix C, für die $C \not\equiv_n B$ gilt, so gilt mit Wahrscheinlichkeit $\frac{1}{3}$, dass $C \equiv_p B$ oder $C \equiv_q B$ gilt. In diesem Fall gilt, dass für mindestens eine der Matrizenstellen gilt: $ggT(c_{i,j} - b_{i,j}, n)$ ist ein nichttrivialer Faktor von n. □

Ein Faktorisierungsalgorithmus mittels Matrizen aus $SL(2, Z_n)$

Neben den bereits aufgeführten Verfahren, die beschreiben, wie ein Algorithmus, der quadratische oder kubische Wurzeln in $SL(2, Z_n)$ zu berechnen vermag, dazu genutzt werden kann, n zu faktorisieren, wird im Folgenden ein weiteres Verfahren beschrieben, wie man mit Hilfe von Matrizen aus $SL(2, Z_n)$ die Zahl n faktorisieren kann, wenn für eine der beiden Primfaktoren p bzw. q gilt, dass $p-1$ (oder $p+1$) bzw. $q-1$ (oder $p+1$) nur durch kleine Primfaktoren teilbar ist.

Im folgenden sei angenommen, dass oBdA $p-1$ (oder $p+1$) nur durch Primfaktoren geteilt wird, die kleiner als eine kleine Schranke S sind.

Zunächst wird nun eine Zahl k berechnet, für die gilt, dass sie von $p-1$ ($p+1$) geteilt wird. Zum Beispiel kann $k := S!$ oder $k := \prod_{p_i \in P; p_i < S} p_i^{f_i}$ mit $f_i = \lfloor log_{p_i} S \rfloor$ gewählt werden. Dann wählt man eine zufällige Matrix $A \in SL(2, Z_n)$ und berechnet $B := A^k \bmod n$.

Nach Definition (4.4.1.0.5) und Satz (4.4.1.0.7) gilt für A:

$$ord(A)|p-1 \quad \vee \quad ord(A)|2p \quad \vee \quad ord(A)|p+1$$

Da $p-1|k$ (oder $p+1$) gilt, folgt $B \equiv_p I$ mit Wahrscheinlichkeit $\frac{1}{2}+\epsilon$ (Korollar (4.3.2.8)). Mit einer hohen Wahrscheinlichkeit gilt aber $B \not\equiv_q I$, da $q-1 \not| k$ (oder $q+1 \not| k$) gilt. Somit ist $ggT(b_{11}-1, n)$ ein nichttrivialer Faktor von n.

Kapitel 5

Eigenschaften von $GL(s, Z_n)$ und $SL(s, Z_n)$

In diesem Kapitel sollen die in dem vorherigen Kapitel dargestellten Erkenntnisse für 2×2 Matrizen auf allgemeine $s \times s$ Matrizen erweitert werden.

5.1 Grundlagen

In diesem Abschnitt werden einige grundlegende Sätze vorgestellt, die für die Untersuchung der Gruppen $GL(s, Z_p)$ und $SL(s, Z_p)$ notwendig sind. Für diese Sätze werden keine vollständigen Beweise aufgeführt, sondern es wird lediglich auf die entsprechenden Beweise in der Literatur verwiesen.

5.1.1 Satz: Satz von Cayley-Hamilton

Sei A eine $s \times s$ Matrix und $P_A(X) = Det(A - xI)$ das charakteristische Polynom von A. Dann gilt $P_A(X) = 0$.

Beweis:
Siehe (Beu94). □

5.1.2 Satz: Sei p eine Primzahl, dann gilt: $|SL(s, Z_p)| = \frac{1}{p-1} \prod_{i=0}^{s-1} (p^s - p^i)$.

Beweis:
Siehe (Ro96). □

5.1.3 Korollar: Es seien p, q zwei verschiedene Primzahlen und sei $n = pq$. Dann hat die Gruppe $SL(s, Z_n)$ genau $\frac{1}{p-1}\prod_{i=0}^{s-1}(p^s - p^i)\frac{1}{q-1}\prod_{j=0}^{s-1}(q^s - q^j)$ Elemente.

Beweis: Folgt aus Satz (5.1.2) zusammen mit dem Chinesischen Restsatz für Matrizen (Satz (3.2.1.7)). □

5.1.4 Satz: Sei p eine Primzahl, dann gilt: $|GL(s, Z_p)| = \prod_{i=0}^{s-1}(p^s - p^i)$

Beweis:
Siehe (Ro96). □

5.1.5 Korollar: Es seien p, q zwei verschiedene Primzahlen und es sei $n = pq$. Dann hat die Gruppe $GL(s, Z_n)$ genau $\prod_{i=0}^{s-1}(p^s - p^i)(q^s - q^i)$ Elemente.

Beweis:
Folgt aus Satz (5.1.4) zusammen mit dem Chinesischen Restsatz für Matrizen (Satz (3.2.1.7)). □

5.1.6 Satz: Sei $A := \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1s} \\ a_{21} & a_{22} & \cdots & a_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{ss} \end{pmatrix}$ eine Matrix aus $GL(s, Z_p)$ und sei $P_A(X) := \sum_{i=0}^{s} c_i X^i \bmod p$ das charakteristische Polynom von A. Dann gilt für jede Matrix $B := A^k \bmod p$ mit $k \geq s$:

$$Spur(B) \equiv_p Spur(A^k) \equiv_p \sum_{i=k-s}^{k-1} -c_{i-(k-s)} Spur(A^i)$$

Dabei sind die $c_{i-(k-s)}$ die Koeffizienten des charakteristischen Polynoms von A sind.

Beweis:

Der Beweis erfolgt durch Induktion über k.

Nach Satz (5.1.1) gilt $P_A(A) = A^s + c_{s-1}A^{s-1} + \cdots + c_1A + c_0I = 0$ und somit $A^s \equiv_p -\sum_{i=0}^{s-1} c_iA^i$. Es folgt $Spur(A^s) \equiv_p -\sum_{i=0}^{s-1} c_iSpur(A^i)$. D.h. die Behauptung gilt für $k = s$. Angenommen, die Behauptung gilt für alle $\ell \leq k$, dann folgt für A^{k+1}:

$$\begin{aligned} Spur(A^{k+1}) \equiv_p Spur(AA^k) &\equiv_p Spur(A(-\sum_{i=k-s}^{k-1} -c_{i-(k-s)}A^i)) \\ &\equiv_p Spur(-\sum_{i=k-s}^{k-1} -c_{i-(k-s)}A^{i+1}) \\ &\equiv_p Spur(-\sum_{i=k+1-s}^{k} -c_{i-(k-s)-1}A^i) \\ &\equiv_p -\sum_{i=k+1-s}^{k} -c_{i-(k+1-s)}Spur(A^i) \end{aligned}$$

□

Der folgende Satz zeigt auf, wann zwei Matrizen $A, B \in GL(s, Z_p)$ zueinander kommutativ sind, d.h. wann $AB \equiv_p BA$ gilt.

5.1.7 Satz: Seien $A := \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1s} \\ a_{21} & a_{22} & \cdots & a_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{ss} \end{pmatrix}$ und $B := \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1s} \\ b_{21} & b_{22} & \cdots & b_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ b_{s1} & b_{s2} & \cdots & b_{ss} \end{pmatrix}$ Matrizen aus $GL(s, Z_p)$. Genau dann gilt $AB \equiv_p BA$, wenn die folgenden Gleichungen erfüllt sind:

$$\sum_{k=1}^{s} a_{ik}b_{kj} \equiv_p \sum_{k=1}^{s} a_{kj}b_{ik} \quad \forall i, j = 1, 2, \ldots, s$$

Beweis:

Der Beweis folgt direkt, wenn man die Produkte AB und BA bildet und die Komponenten vergleicht. □

5.1.8 Korollar: Seien $A := \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & a_{ss} \end{pmatrix}$ und $B := \begin{pmatrix} b_{11} & 0 & \dots & 0 \\ 0 & b_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & b_{ss} \end{pmatrix}$ Diagonalmatrizen aus $GL(s, Z_n)$, dann gilt $AB \equiv_n BA$.

Beweis:
Die Behauptung folgt direkt aus der Kommutativität von Z_n^*. □

5.1.9 Korollar: Seien $A := \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & a_{sbs} \end{pmatrix}$ eine Diagonalmatrix aus $GL(s, K)$ mit $a_{ii} \neq a_{jj}$ für $i \neq j$ und B eine beliebige Matrix aus $GL(s, K)$, wobei K ein Körper ist. Dann gilt:

$$AB = BA \Rightarrow B \text{ ist eine Diagonalmatrix}$$

.

Beweis:
Da $AB = BA$ in $GL(s, K)$ gilt, folgt für $i, j \in \{1, 2, \dots, s\}$ in dem Körper K :

$$\begin{aligned} \sum_{t=1}^{s} a_{it} b_{tj} &= \sum_{t=1}^{s} a_{tj} b_{it} \\ \Rightarrow \quad a_{ii} b_{ij} &= a_{jj} b_{ij} \\ \Leftrightarrow \quad 0 &= a_{ii} b_{ij} - a_{jj} b_{ij} = b_{ij}(a_{ii} - a_{jj}) \end{aligned}$$

Da $a_{ii} \neq a_{jj}$ für $i \neq j$ gilt und K ein Körper ist, folgt dann $b_{ij} = 0$ für $i \neq j$. Somit folgt die Behauptung. □

5.1.10 Satz: Seien A und B zwei zueinander ähnliche Matrizen aus $GL(s, Z_p)$, dann ist es in polynomieller Zeit möglich, eine Matrix $C \in GL(s, Z_p)$ zu bestimmen, so dass $A \equiv_p CBC^{-1}$ gilt.

Beweis:

Jede Matrix kann als Darstellungsmatrix $M_{\mathfrak{B}}^{\mathfrak{B}}(f)$ einer linearen Abbildung $f : V \to V$ des s-dimensionalen Vektorraumes V über Z_p auf sich selbst zu einer Basis $\mathfrak{B}$ des Vektorraums interpretiert werden. Für zwei Darstellungsmatrizen $M_{\mathfrak{B}}^{\mathfrak{B}}(f)$ und $M_{\mathfrak{C}}^{\mathfrak{C}}(f)$ der gleichen linearen Abbildung f gilt:

$$M_{\mathfrak{B}}^{\mathfrak{B}}(f) = M_{\mathfrak{B}}^{\mathfrak{C}}(id) M_{\mathfrak{C}}^{\mathfrak{C}}(f) M_{\mathfrak{C}}^{\mathfrak{B}}(id)$$

Dabei sei id die identische Abbildung, und es gilt $M_{\mathfrak{B}}^{\mathfrak{C}}(id) = (M_{\mathfrak{C}}^{\mathfrak{B}}(id))^{-1}$.

Um zu zwei ähnlichen Matrizen $A, B \in GL(s, Z_p)$ eine Matrix $C \in GL(s, Z_p)$ zu konstruieren, so dass $A \equiv_p CBC^{-1}$ gilt, geht man wie folgt vor:

Seien $A := \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1s} \\ a_{21} & a_{22} & \cdots & a_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{ss} \end{pmatrix}$ und $B := \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1s} \\ b_{21} & b_{22} & \cdots & b_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ b_{s1} & b_{s2} & \cdots & b_{ss} \end{pmatrix}$ zueinander ähnliche Matrizen aus $GL(s, Z_p)$. Wähle eine Basis $\mathfrak{B} := \{\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_s\}$ des s-dimensionalen Vektorraums V über Z_p und definiere die Abbildung $f : V \to V$ durch $f_{\mathfrak{b}_j} :\equiv_p \sum_{i=1}^{s} a_{ij}\mathfrak{b}_i$. Dann ist $A = M_{\mathfrak{B}}^{\mathfrak{B}}(f)$ die Darstellungsmatrix von f zur Basis $\mathfrak{B}$. Kennt man eine Basis $\mathfrak{C}$, so dass $B = M_{\mathfrak{C}}^{\mathfrak{C}}(f)$ gilt, so kann man leicht die Matrizen $C := M_{\mathfrak{B}}^{\mathfrak{C}}(id)$ und $C^{-1} := M_{\mathfrak{C}}^{\mathfrak{B}}(id)$ erzeugen, so dass $A \equiv_p CBC^{-1}$ gilt.

Im folgenden wird nun gezeigt, wie eine solche Basis erzeugt werden kann: Sei $\mathfrak{C} := \{\mathfrak{c}_1, \mathfrak{c}_2, \ldots \mathfrak{c}_i\}$ eine Basis, so dass $M_{\mathfrak{C}}^{\mathfrak{C}}(f) = B$ gilt. Dann gilt: $f(\mathfrak{c}_j) \equiv_p \sum_{i=1}^{s} b_{ij}\mathfrak{c}_i$. Da $\mathfrak{B}$ eine Basis von V ist, gibt es Elemente $r_{k\ell} \in Z_p$, $k, \ell \in \{1, 2, \ldots, s\}$, so dass $\mathfrak{c}_j \equiv_p \sum_{k=1}^{s} r_{kj}\mathfrak{b}_k$ gilt. Es folgt für $j = 1, 2, \ldots, s$:

$$f(\mathfrak{c}_j) \equiv_p \sum_{i=1}^{s} b_{ij}\mathfrak{c}_i \equiv_p \sum_{i=1}^{s} b_{ij}\Big(\sum_{k=1}^{s} r_{kj}\mathfrak{b}_k\Big)$$

Da f eine lineare Abbildung ist, gilt $f(\mathfrak{c}_j) \equiv_p \sum_{\ell=1}^{s} r_{\ell j} f(\mathfrak{b}_\ell)$. Zusammen folgt für $j = 1, 2, \ldots, s$:

$$\sum_{\ell=1}^{s} r_{\ell j} f(\mathfrak{b}_\ell) \equiv_p \sum_{i=1}^{s} b_{ij} (\sum_{k=1}^{s} r_{kj} \mathfrak{b}_k)$$

Dies ist ein Gleichungssystem von s Gleichung in den s^2 Unbekannten r_{ij}. Wählt man nun $s(s-1)$ zufällige Werte für $r_{i,j} \in Z_p$ für $i = 1, 2, \ldots, s-1$ und $j = 1, 2, \ldots s$, so sind die übrigen $r_{i,s}$ für $i = 1, 2, \ldots, s$ eindeutig bestimmt. Die r_{ij} definieren dann eine Basis $\mathfrak{C}$ durch $\mathfrak{c}_j \equiv_p \sum_{k=1}^{s} r_{kj} \mathfrak{b}_k$, so dass $B = M_{\mathfrak{C}}^{\mathfrak{C}}(f)$ gilt. Da das Lösen des Gleichungssystems in polynomieller Zeit möglich ist, folgt die Behauptung des Satzes. □

5.1.11 Satz: Seien p und q zwei große Primzahlen und sei $n := pq$. Seien A und B zwei zueinander ähnliche Matrizen aus $GL(s, Z_n)$, dann ist es in polynomieller Zeit möglich, eine Matrix $C \in GL(s, Z_n)$ zu bestimmen, so dass $A \equiv_n CBC^{-1}$ gilt.

Beweis:

Man geht einfach vor wie im Beweis von Satz (5.1.10) und erhält mit hoher Wahrscheinlichkeit eine Matrix $C \in GL(s, Z_n)$, so dass $A \equiv_p CBC^{-1}$ und $A \equiv_q CBC^{-1}$ gilt. Nach dem Chinesischen Restsatz für Matrizen (Satz (3.2.1.7)) folgt dann $A \equiv_n CBC^{-1}$.

5.2 Die Gruppe $GL(s, Z_n)$

5.2.1 Die Potenzfunktion in der Gruppe $GL(s, Z_n)$

In diesem Abschnitt werden besondere Potenzierungseigenschaften der Gruppe $GL(s, Z_n)$ behandelt.

Ebenso wie im Fall $s = 2$ bleiben bei der Potenzierung einer Matrix aus der Gruppe $GL(s, Z_n)$ bestimmte Strukturen erhalten:

5.2.1.1 Satz: Sei $A := \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1s} \\ a_{21} & a_{22} & \cdots & a_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ a_{s1} & a_{s2} & \cdots & a_{ss} \end{pmatrix}$ eine Matrix aus $GL(s, Z_n)$ und sei

$$B := \begin{pmatrix} b_{11} & b_{12} & \cdots & b_{1s} \\ b_{21} & b_{22} & \cdots & b_{2s} \\ \vdots & \vdots & \ddots & \vdots \\ b_{s1} & b_{s2} & \cdots & b_{ss} \end{pmatrix} \in < A >.$$

Dann gilt:

$$\sum_{t=1}^{s} a_{it} b_{tj} \equiv_p \sum_{t=1}^{s} a_{tj} b_{it} \quad \forall i, j \in \{1, 2, \ldots, s\}$$

Beweis:

Der Beweis erfolgt durch Induktion über die Potenz von A. Im folgenden sei $a_{ij}^{(k)}$ der Eintrag in der $i-ten$ Zeile und $j-ten$ Spalte der Matrix A^k.

Die Behauptung gilt für $k = 1$, denn :

$$\sum_{t=1}^{s} a_{it}^{(1)} a_{tj}^{(1)} \equiv_p \sum_{t=1}^{s} a_{tj}^{(1)} a_{it}^{(1)} \quad \forall i, j = 1, 2, \ldots, s$$

Angenommen, die Behauptung gilt für alle $\ell \leq k$, dann folgt für $k+1$:

$$\begin{aligned} \sum_{t=1}^{s} a_{it}^{(1)} a_{tj}^{(k+1)} &\equiv_p \sum_{t=1}^{s} a_{it}^{(1)} \sum_{u=1}^{s} a_{tu}^{(k)} a_{uj}^{(1)} \\ &\equiv_p \sum_{t=1}^{s} \sum_{u=1}^{s} a_{it}^{(1)} a_{tu}^{(k)} a_{uj}^{(1)} \\ &\equiv_p \sum_{u=1}^{s} a_{iu}^{(k+1)} a_{uj}^{(1)} \\ &\equiv_p \sum_{t=1}^{s} a_{tj}^{(1)} a_{it}^{(k+1)} \quad \forall i, j = 1, 2, \ldots, s \end{aligned}$$

□

5.2.2 Zyklische Untergruppen in $GL(s, Z_n)$

Im folgenden werden die möglichen Ordnungen der von einem Element aus $GL(s, Z_n)$ erzeugten zyklischen Untergruppe behandelt. Dabei werden besonders große zyklische Untergruppen betrachtet. Diese Betrachtung ist sinnvoll, da Verschlüsselungsfunktionen, die

auf dem diskreten Logarithmusproblem oder dem RSA-Problem basieren, immer nur auf einer zyklischen Untergruppe operieren. Die Wahl der zyklischen Untergruppe, auf der operiert wird, hängt dabei beim RSA-Verschlüsselungsverfahren direkt von der Matrix ab, die verschlüsselt werden soll.

Zunächst werden nur Matrizen über Z_p betrachtet, wobei p eine Primzahl ist. Die bewiesenen Aussagen können dann leicht mit Hilfe des Chinesischen Restsatzes auf Matrizen über Z_n zusammengesetzt werden.

5.2.2.1 Satz: Es sei p eine Primzahl. Jede diagonalisierbare Matrix $A \in GL(s, Z_p)$ besitzt eine Ordnung, die $p-1$ teilt.

Beweis:

Sei $A \in GL(s, Z_p)$ eine diagonalisierbare Matrix, d.h. es gibt eine Diagonalmatrix $B \in GL(s, Z_n)$ mit $B \equiv_p gAg^{-1}$ für ein geeignetes $g \in GL(s, Z_p)$.

Für B gilt:

$$B^k \equiv_p \begin{pmatrix} b_{11}^k & 0 & \cdots & 0 \\ 0 & b_{22}^k & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & b_{ss}^k \end{pmatrix}$$

Also gilt:

$$B^{p-1} \equiv_p \begin{pmatrix} b_{11}^{p-1} & 0 & \cdots & 0 \\ 0 & b_{22}^{p-1} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & b_{ss}^{p-1} \end{pmatrix} \equiv_p I$$

B und A haben nach Satz (4.1.2) die gleiche Ordnung, also gilt $ord(A)|(p-1)$. □

Klar ist, dass es auch Matrizen in $GL(s, Z_p)$ gibt, die genau die Ordnung $p-1$ besitzen, da dies schon für Matrizen aus $GL(2, Z_p)$ gezeigt wurde. Für jede Matrix $A \in GL(2, Z_p)$ gilt, dass $B := \begin{pmatrix} \boxed{A} & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 1 \end{pmatrix}$ eine Matrix aus $GL(s, Z_p)$ mit $ord(A) = ord(B)$ ist. Dabei stellt die rechte untere Teilmatrix die $(s-2) \times (s-2)$ Einheitsmatrix dar.

5.2.2.2 Korollar: Seien p, q Primzahlen und sei $n := pq$. Dann gilt: Jede diagonalisierbare Matrix $A \in GL(s, Z_n)$ besitzt eine Ordnung, die $\varphi(n)$ teilt.

Beweis:

Die Behauptung folgt direkt aus Satz (5.2.2.1) zusammen mit dem Chinesischen Restsatz für Matrizen (Satz (3.2.1.7)).

5.2.2.3 Satz: Jede Matrix $A \in GL(s, Z_p)$, deren Eigenwerte in Z_p^* liegen und verschieden sind, besitzt eine Ordnung, die $(p-1)$ teilt.

Beweis:

Eine Matrix, deren Eigenwerte verschieden sind und in Z_p^* liegen, ist in $GL(s, Z_p)$ diagonalisierbar. Nach Satz (5.2.2.1) besitzt jede diagonalisierbare Matrix eine Ordnung, die $p-1$ teilt. □

5.2.2.4 Satz: Es sei p eine Primzahl. Jede Matrix $A \in GL(s, Z_p)$, die mindestens zwei gleiche Eigenwerte $\lambda \in Z_p^*$ besitzt und deren Eigenwerte alle in Z_p^* liegen, hat eine Ordnung, die $(p-1)p$ teilt.

Beweis:

Da die Eigenwerte α_i von $A \in GL(s, Z_p)$ in Z_p^* liegen, existiert eine zu A ähnliche Matrix $B \in GL(s, Z_p)$, die die Jordansche Normalform besitzt. Mit anderen Worten: Es gibt eine Matrix B der Form:

$$B := \begin{pmatrix} \boxed{J_1} & 0 & \cdots & 0 \\ 0 & \boxed{J_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \boxed{J_l} \end{pmatrix}$$

$$\text{mit } J_i := \begin{pmatrix} \alpha_i & 1 & 0 \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 0 & \cdots & 0 & \alpha_i \end{pmatrix}$$

B und A haben nach Satz (4.1.2) die gleiche Ordnung.

Es folgt, dass B^p eine Diagonalmatrix ist, da für jede Teilmatrix J_i gilt:

$$J_i^p := \begin{pmatrix} \alpha_i^p & p\alpha^{p-1} & 0\cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & p\alpha^{p-1} \\ 0 & \cdots & 0 & \alpha_i^p \end{pmatrix} \equiv_p \begin{pmatrix} \alpha_i^p & 0 & 0\cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 0 \\ 0 & \cdots & 0 & \alpha_i^p \end{pmatrix}$$

Nach Satz (5.2.2.1) folgt, dass $ord(B^p)|p-1$ gilt. Somit gilt auch $ord(B)|p(p-1)$. □

5.2.2.5 Satz: Seien p, q Primzahlen und sei $n = pq$, dann gilt: Jede triagonalisierbare Matrix $A \in GL(s, Z_n)$ besitzt eine Ordnung, die $\varphi(n)n$ teilt.

Beweis:

Die Behauptung folgt direkt aus Satz (5.2.2.3) und Satz (5.2.2.4) mit Hilfe des Chinesischen Restsatzes für Matrizen (Satz (3.2.1.7)). □

5.2.2.6 Satz: Es sei p eine Primzahl und $A \in GL(s, Z_p)\backslash\{\pm I\}$. Es gilt genau dann $p|ord(A)$, wenn $P_A(X)$ mindestens zwei gleiche Nullstellen in dem Zerfällungskörper $K_{P_A(X)}$ von $P_A(X)$ besitzt und A in $GL(s, K_{P_A(X)})$ nicht diagonalisierbar ist.

Beweis:

"⇒" Sei A eine Matrix aus $GL(s, Z_p)$ mit $p|ord(A)$. Sei $P_A(X)$ das charakteristische Polynom von A und sei $P_A(X) = \prod_{j\in J} f_j$ mit $f_j \in Z_p[x]$ irreduzibel. Seien weiterhin α_i $i = 1, 2, \ldots, s$ die Nullstellen von $P_A(X)$ in dem Zerfällungskörper von $P_A(X)$ über Z_p. Dann ist jedes α_i eine Nullstelle von mindestens einem f_j mit $Grad(f_j) < s$. Da f_j irreduzibel ist, folgt $\alpha_i^{p^{Grad(f_j)}-1} = 1$ in dem Zerfällungskörper. Angenommen alle Nullstellen α_i sind verschieden, dann existiert eine zu A ähnliche Matrix $B \in GL(s, K_{P_A(X)})$, so dass B eine Diagonalmatrix ist. Mit anderen Worten: A ist in $GL(s, K_{P_A(X)})$ diagonalisierbar. Dann gilt $B^{\prod_{j\in J}(p^{Grad(f_j)}-1)} \equiv_p I$, da $\alpha_i^{\prod_{j\in J}(p^{Grad(f_j)}-1)} = 1$ in $K_{P_A(X)}$ gilt. Es folgt $ord(B)|\prod_{j\in J}(p^{Grad(f_j)} - 1)$, und da $ord(A) = ord(B)$ gilt, folgt $p|\prod_{j\in J}(p^{Grad(f_j)} - 1)$. Dies ist aber nicht möglich, da $\prod_{j\in J}(p^{Grad(f_j)} - 1) \equiv_p \pm 1$ gilt. Also muss $P_A(X)$ mindestens zwei gleiche Nullstellen besitzen. Ist A in $GL(s, K_{P_A(X)})$ diagonalisierbar, so folgt wie im obigen Fall $p|\prod_{j\in J}(p^{Grad(f_j)} - 1)$, was einen Widerspruch darstellt.

"$\Leftarrow$" Hat das charakteristische Polynom $P_A(X)$ von A in dem Zerfällungskörper $K_{P_A(X)}$ eine mehrfache Nullstelle, existiert eine zu A ähnliche Matrix $B \in GL(s, K_{P_A(X)})$, die die Jordansche Normalform besitzt. Ist A in $GL(s, Z_{K_{P_A(X)}})$ nicht diagonalisierbar, dann ist auch B keine Diagonalmatrix.

Mit anderen Worten: Es gibt eine Matrix B der Form:

$$B := \begin{pmatrix} \boxed{J_1} & 0 & \cdots & 0 \\ 0 & \boxed{J_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \boxed{J_l} \end{pmatrix}$$

$$\text{mit } J_i := \begin{pmatrix} \alpha_i & 1 & 0 \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 0 & \cdots & 0 & \alpha_i \end{pmatrix}$$

Dabei besitzt mindestens eine der Jordanmatrizen J_i eine Dimension ≥ 2. Es ist leicht zu sehen, dass für jede t_i-dimensionale Jordanmatrix $J_i \in GL(t_i, K_{P_A(X)})$ gilt: $ord(J_i) = ord(\alpha_i)p$, denn es gilt

$$(J_i)^k := \begin{pmatrix} \alpha_i^k & k\alpha^{k-1} & 0 \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & k\alpha^{k-1} \\ 0 & \cdots & 0 & \alpha_i^k \end{pmatrix}$$

Daraus folgt, dass $p|ord(B)$ und somit auch $p|ord(A)$ gilt. □

5.2.2.7 Satz: Die maximale Ordnung eines Elements $A \in GL(s, Z_p)$ beträgt $p^s - 1$

Beweis:

Sei A eine Matrix aus $GL(s, Z_p)$ und sei $P_A(X) := \sum_{i=0}^{s} c_i X^i$ mit $c_i \in Z_p$ und $c_s \equiv_p (-1)^s$ das charakteristische Polynom von A. Seien α_i $(i = 1, 2, \ldots, s)$ die Nullstellen des charakteristischen Polynoms. Da die α_i nicht in Z_p liegen müssen, wird im folgenden der

Zerfällungskörper $K_{P_A(X)}$ des charakteristischen Polynoms betrachtet, in dem alle Nullstellen α_i von $P_A(X)$ liegen. $K_{P_A(X)}$ ist ein Erweiterungskörper von Z_p, und der Grad der Körpererweiterung ist maximal $s!$.

Da $P_A(X)$ in dem Zerfällungskörper $K_{P_A(X)}$ in Linearfaktoren zerfällt, existiert eine zu A ähnliche Matrix $B \in GL(s, K_{P_A(X)})$, die die Jordansche Normalform besitzt. Mit anderen Worten: Es gibt eine Matrix B der Form:

$$B := \begin{pmatrix} \boxed{J_1} & 0 & \cdots & 0 \\ 0 & \boxed{J_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \boxed{J_l} \end{pmatrix}$$

$$\text{mit } J_i := \begin{pmatrix} \alpha_i & 1 & 0 \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 0 & \cdots & 0 & \alpha_i \end{pmatrix}$$

Es ist leicht zu sehen, dass für jede t_i-dimensionale Jordanmatrix $J_i \in GL(t_i, K_{P_A(X)})$ gilt: $ord(J_i) = ord(\alpha_i)p$, denn es gilt

$$(J_i)^k := \begin{pmatrix} \alpha_i^k & k\alpha^{k-1} & 0 \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & k\alpha^{k-1} \\ 0 & \cdots & 0 & \alpha_i^k \end{pmatrix}$$

Somit gilt für B^k:

$$B^k := \begin{pmatrix} \boxed{(J_1)^k} & 0 & \cdots & 0 \\ 0 & \boxed{(J_2)^k} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \boxed{(J_l)^k} \end{pmatrix}$$

Ist $P_A(X)$ irreduzibel, so kann $P_A(X)$ in $K_{P_A(X)}$ keine mehrfachen Nullstellen besitzen, da $K_{P_A(X)}$ ein endlicher und somit vollkommener Körper ist. Hat $P_A(X)$ keine mehrfachen

Nullstellen, so ist A in $GL(s, K_{P_A(X)})$ diagonalisierbar. Im folgenden sei $B \in GL(s, K_{P_A(X)})$ die zu A ähnliche Diagonalmatrix. Es wird nun gezeigt, dass die Ordnung von B und somit auch die Ordnung von A maximal p^s-1 betragen kann. Für jedes $\alpha_i \in K_{P_A(X)} \backslash \{0\}$ gilt, dass α_i in dem Teilkörper $Z_p(\alpha_i)$ (also dem Körper Z_p adjungiert der Nullstelle α_i) von $K_{P_A(X)}$ liegt. Diese Körpererweiterung hat den Grad s, da α_i eine Nullstelle von $P_A(X) \in Z_p[x]$ ist, $P_A(X)$ irreduzibel ist und $Grad(P_A(X)) = s$ gilt. Die multiplikative Gruppe von $Z_p(\alpha_i)$ besitzt somit maximal $p^s - 1$ Elemente und es gilt in dieser Gruppe $ord(\alpha_i) \mid p^s - 1$. Da die multiplikative Gruppe von $Z_p(\alpha_i)$ eine Untergruppe der multiplikativen Gruppe von $K_{P_A(X)}$ ist, folgt auch, dass $ord(\alpha_i) \mid p^s - 1$ in der multiplikativen Gruppe von $K_{P_A(X)}$ gilt. Mit anderen Worten: Es gilt $ord(B) \mid p^s - 1$ und somit auch $ord(A) \mid p^s - 1$. Insbesondere gilt somit auch $ord(A) \leq p^s - 1$.

Ist $P_A(X)$ reduzibel, so gibt es irreduzible Polynome $f_j \in Z_p[x]$, so dass $P_A(X) = \prod_{j=1}^{m} f_j$ und $0 < Grad(f_j) < s \quad \forall j = 1, 2, \ldots, m$ gilt. Jede Nullstelle α_i von $P_A(X)$ ist eine Nullstelle von mindestens einem f_j. Somit hat das Minimalpolynom von α_i einen Grad $a_i < s$. Ist α_i eine Nullstelle von f_j, dann besitzt f_j den gleichen Grad a_i wie das Minimalpolynom von α_i. Es gilt $a_i < s$. Die Teilkörper $Z_p(\alpha_i)$ des Zerfällungskörpers $K_{P_A(X)}$ haben somit auch jeweils den Grad $a_i < s$. Die multiplikative Gruppe des Teilkörpers $K(\alpha_i)$ hat dann genau $p^{a_i} - 1$ Elemente. Es gilt also für jede der obigen Jordanmatrizen J_i: $J_i^{p(p^{a_i}-1)} = I$ über dem jeweiligen Erweiterungskörper $Z_p(\alpha_i)$ von Z_p. Es folgt für die Matrix B:

$$\begin{aligned} ord(B) &= kgV\{p(p^{a_i} - 1), i = 1, 2, \ldots, m\} \\ &\leq p(p-1)kgV\left\{\left(\sum_{\ell=0}^{a_i-1} p^\ell\right), i = 1, 2, \ldots, m\right\} \\ &\leq p(p-1)\prod_{i=1}^{m}\left(\sum_{\ell=0}^{a_i-1} p^\ell\right) \leq p(p-1)F(p) \end{aligned}$$

Dabei ist $F(x)$ ein Polynom vom Grad $s - m$. Es folgt:

$$ord(B) \leq p(p-1)F(p) < p(p-1)p^{s-m+1} < p^{s-m+3} - 1$$

Das heißt, die Behauptung des Satzes gilt für den Fall, dass $P_A(X)$ mindestens drei irreduzible Faktoren (vom Grad größer 0) besitzt. Um den Satz vollständig zu beweisen, muss nur noch der Fall betrachtet werden, dass $P_A(X)$ genau zwei irreduzibel Faktoren mit einem Grad ≥ 1 besitzt.

Besitzt $P_A(X)$ keine mehrfachen Nullstellen in dem Zerfällungskörper $K_{P_A(X)}$, so ist A diagonalisierbar und die Behauptung folgt wie oben. Sei also α eine mehrfache Nullstelle von $P_A(X)$ und seien $g(x), h(x)$ die beiden irreduziblen Faktoren von $P_A(X)$. Da $g(x)$ und $h(x)$ irreduzibel sind, können sie in dem endlichen Zerfällungskörper $K_{P_A(X)}$ von $P_A(X)$ keine mehrfachen Nullstellen besitzen. Somit muss α eine Nullstelle sowohl von $g(x)$ als auch von $h(x)$ sein. Da beide Polynome irreduzibel sind, müssen sie den gleichen Grad haben wie das Minimalpolynom von α. Insbesondere müssen $g(x)$ und $h(x)$ den gleichen Grad besitzen. Es gilt also $Grad(g(x)) = Grad(h(x)) = \frac{s}{2}$.

Dann ist jeder Teilkörper $Z_p(\alpha_i)$ von $K_{P_A(X)}$ eine Körpererweiterung vom Grad $\frac{s}{2}$ über dem Körper Z_p. Die multiplikative Gruppe von $Z_p(\alpha_i)$ besitzt somit maximal $p^{\frac{s}{2}}-1$ Elemente und es gilt $ord(\alpha_i) \mid p^{\frac{s}{2}} - 1$. Da die multiplikative Gruppe von $Z_p(\alpha_i)$ eine Untergruppe der multiplikativen Gruppe von $K_{P_A(X)}$ ist, folgt auch, dass $ord(\alpha_i) \mid p^{\frac{s}{2}} - 1$ in der multiplikativen Gruppe von $K_{P_A(X)}$ gilt. Es folgt $ord(B) \mid p^{\frac{s}{2}} - 1$ und somit auch $ord(A) \mid p^{\frac{s}{2}} - 1$. Insbesondere gilt somit auch $ord(A) < p^s - 1$. □

5.2.2.8 Korollar: Gilt für eine Matrix $A \in GL(s, Z_p)$ $ord(A) = p^s - 1$, so ist $P_A(X)$ irreduzibel.

Beweis:

Die Behauptung folgt direkt aus dem Beweis von Satz (5.2.2.7). Dort wird gezeigt, dass eine Matrix, deren charakteristisches Polynom reduzibel ist, eine kleinere Ordnung als $p^s - 1$ besitzt. □

5.2.2.9 Korollar: Sei $n = pq$, p, q Primzahlen, dann gilt: Die maximale Ordnung eines Elementes $A \in GL(s, Z_n)$ beträgt $(p^s - 1)(q^s - 1)$.

Beweis:

Die Behauptung folgt direkt aus Satz (5.2.2.7) und dem Chinesischen Restsatz für Matrizen (Satz (3.2.1.7)).

5.3 Die Gruppe $SL(s, Z_n)$

5.3.1 Die Potenzfunktion in der Gruppe $SL(s, Z_n)$

In diesem Abschnitt werden besondere Potenzierungseigenschaften der Gruppe $SL(s, Z_n)$ behandelt.

Da $SL(s, Z_n)$ eine Untergruppe von $GL(s, Z_n)$ ist, gelten alle Sätze aus Abschnitt 5.2.1 auch für die Gruppe $SL(s, Z_n)$.

5.3.2 Zyklische Untergruppen in $SL(s, Z_n)$

Im folgenden soll geklärt werden, welche zyklischen Untergruppen in $SL(s, Z_n)$ existieren und welche besonderen Eigenschaften diese besitzen. Zunächst werden wieder nur die Matrizen über Z_p (wobei p eine Primzahl ist) betrachtet, und dann mit Hilfe des Chinesischen Restsatzes für Matrizen auf Matrizen über Z_n zusammengesetzt. Wie in Abschnitt 5.1 bereits dargestellt, besteht $SL(s, Z_p)$ aus $\frac{1}{p-1}\prod_{i=0}^{s-1}(p^s - p^i)$ Elementen. Da $SL(s, Z_p)$ eine nicht abelsche, assoziative Gruppe und somit eine nicht zyklische Gruppe ist, kann es kein erzeugendes Element der Gruppe geben.

Ebenso wie in $GL(s, Z_p)$ gibt es auch in $SL(s, Z_p)$ Matrizen, die genau die Ordnung $p - 1$ besitzen.

5.3.2.1 Korollar: Es gibt Matrizen $\in SL(s, Z_p)$, die die Ordnung $p - 1$ besitzen.

Beweis:

Es sei $a \in Z_p$ mit $ord(a) = p - 1$. Dann ist $\begin{pmatrix} a & 0 & \ddots & 0 & 0 \\ 0 & a^{-1} & 0 & \ddots & \vdots \\ \vdots & \ddots & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \cdots & \cdots & \cdots & 1 \end{pmatrix}$ eine Matrix aus $SL(s, Z_p)$, die die Ordnung $p - 1$ besitzt. □

Wie der folgende Satz zeigt, ist die Ordnung einer zyklischen Untergruppe von $SL(s, Z_p)$ durch $\sum_{i=0}^{s-1} p^i$ beschränkt.

5.3.2.2 Satz: Sei p eine Primzahl. Die maximale Ordnung eines Elements $A \in SL(s, Z_p)$ beträgt $\frac{p^s-1}{p-1} = \sum_{i=0}^{s-1} p^i$.

Beweis:

Klar ist, dass die maximale Ordnung eines Elements mindestens $\frac{p^s-1}{p-1}$ beträgt. Denn sei $B \in GL(s, Z_p)$ ein Element maximaler Ordnung, also $ord(B) = p^s - 1$, dann ist B^{p-1} eine Matrix, die in $SL(s, Z_p)$ liegt und die Ordnung $\frac{p^s-1}{p-1}$ besitzt.

Im folgenden wird zunächst gezeigt, dass die Ordnung einer Matrix $A \in SL(s, Z_p)$ kleiner als $\frac{p^s-1}{p-1}$ ist, wenn das charakteristische Polynom $P_A(X)$ von A reduzibel ist.

Ebenso wie im Beweis von Satz (5.2.2.7) gilt: Da $P_A(X)$ in dem Zerfällungskörper $K_{P_A(X)}$ in Linearfaktoren zerfällt, existiert eine zu A ähnliche Matrix $B \in SL(s, K_{P_A(X)})$, die die Jordansche Normalform besitzt. Mit anderen Worten: Es gibt eine Matrix B der Form:

$$B := \begin{pmatrix} \boxed{J_1} & 0 & \cdots & 0 \\ 0 & \boxed{J_2} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \boxed{J_l} \end{pmatrix}$$

mit

$$J_i := \begin{pmatrix} \alpha_i & 1 & 0 \cdots & 0 \\ 0 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & 1 \\ 0 & \cdots & 0 & \alpha_i \end{pmatrix}$$

Ist $P_A(X)$ reduzibel, so gibt es irreduzible Polynome $f_j \in Z_p[x]$, so dass $P_A(X) = \prod_{j=1}^{m} f_j$ und $0 < Grad(f_j) < s \quad \forall j = 1, 2, \ldots, m$. Jede Nullstelle α_i von $P_A(X)$ ist eine Nullstelle von mindestens einem f_j. Somit hat das Minimalpolynom von α_i einen Grad $a_i < s$. Ist α_i eine Nullstelle von f_j, dann hat f_j den gleichen Grad wie das Minimalpolynom von α_i. Die Teilkörper $Z_p(\alpha_i)$ des Zerfällungskörpers $K_{P_A(X)}$ haben somit auch jeweils den Grad $a_i < s$. Die multiplikative Gruppe des Teilkörpers $Z_p(\alpha_i)$ hat dann genau $p^{a_i} - 1$ Elemente. Es gilt also für jede der obigen Jordanmatrizen J_i: $J_i^{p(p^{a_i}-1)} = I$ in dem Erweiterungskörper

$Z_p(\alpha_i)$ von Z_p, der α_i enthält. Es folgt für die Matrix B:

$$\begin{aligned} ord(B) &= kgV\{p(p^{a_i}-1), i=1,2,\ldots,m\} \\ &\leq p(p-1)kgV\left\{\left(\sum_{\ell=0}^{a_i-1} p^\ell\right), i=1,2,\ldots,m\right\} \\ &\leq p(p-1)\prod_{i=1}^{m}\left(\sum_{\ell=0}^{a_i-1} p^\ell\right) \leq p(p-1)F(p) \end{aligned}$$

Dabei ist $F(x)$ ein Polynom vom Grad $s-m$. Es folgt $ord(B) \leq p(p-1)F(p) < p(p-1)p^{s-m+1} < p^{s-m+3}-1$.

Das heißt, die Behauptung, dass die Ordnung von Matrizen aus $SL(s, Z_p)$ mit reduziblen charakteristischem Polynom kleiner als $\frac{p^s-1}{p-1}$ ist, gilt für den Fall, dass $P_A(X)$ mindestens vier irreduzible Faktoren (vom Grad größer 0) besitzt. Um die Behauptung vollständig zu beweisen, müssen nur noch die Fälle betrachtet werden, in denen $P_A(X)$ genau zwei oder genau drei irreduzibel Faktoren mit einem Grad ≥ 1 besitzt.

Angenommen, $P_A(X)$ zerfällt in genau zwei irreduzible Polynome. Besitzt $P_A(X)$ keine mehrfachen Nullstellen in dem Zerfällungskörper $K_{P_A(X)}$, so ist A diagonalisierbar und es gilt:

$$\begin{aligned} ord(A) &\leq kgV(p^{Grad(f_1)}-1, p^{Grad(f_2)}-1) \\ &\leq (p^{Grad(f_1)-1}+p^{Grad(f_1)-2}+\ldots+1)(p^{Grad(f_2)}-1) \\ &= p^{s-1}+p^{s-2}+\ldots+p^{Grad(f_2)}-p^{Grad(f_1)-1} \\ &\quad -p^{Grad(f_1)-2}-\ldots-1 \\ &< p^{s-1}+p^{s-2}+\ldots+1 = \frac{p^s-1}{p-1} \end{aligned}$$

Angenommen, $P_A(X)$ besitzt eine mehrfache Nullstelle α. Es seien im folgenden $g(x), h(x)$ die beiden irreduziblen Faktoren von $P_A(X)$. Da $g(x)$ und $h(x)$ irreduzibel sind, können sie in dem endlichen Zerfällungskörper $K_{P_A(X)}$ von $P_A(X)$ keine mehrfachen Nullstellen besitzen. Somit muss α eine Nullstellen sowohl von $g(x)$ als auch von $h(x)$ sein. Da beide Polynome irreduzibel sind, müssen sie den gleichen Grad haben wie das Minimalpolynom von α. Insbesondere müssen $g(x)$ und $h(x)$ den gleichen Grad besitzen. Es gilt also $Grad(g(x)) = Grad(h(x)) = \frac{s}{2} < s-1$.

Dann ist jeder Teilkörper $Z_p(\alpha_i)$ von $K_{P_A(X)}$ eine Körpererweiterung vom Grad $\frac{s}{2}$ über dem Körper Z_p. Die multiplikative Gruppe von $Z_p(\alpha_i)$ besitzt somit maximal $p^{\frac{s}{2}}-1$ Elemente und es gilt $ord(\alpha_i) \mid p^{\frac{s}{2}} - 1$. Da die multiplikative Gruppe von $Z_p(\alpha_i)$ eine Untergruppe der multiplikativen Gruppe von $K_{P_A(X)}$ ist, folgt auch, dass $ord(\alpha_i) \mid p^{\frac{s}{2}} - 1$ in der multiplikativen Gruppe von $K_{P_A(X)}$ gilt. Es folgt $ord(B) \mid p^{\frac{s}{2}} - 1$ und somit auch $ord(A) \mid p^{\frac{s}{2}} - 1$. Insbesondere gilt somit auch $ord(A) < p^{s-1}$.

Angenommen, $P_A(X)$ zerfällt in genau drei irreduzible Polynome. Besitzt $P_A(X)$ keine mehrfachen Nullstellen in dem Zerfällungskörper $K_{P_A(X)}$, so ist A diagonalisierbar und es gilt:

$$\begin{aligned}
ord(A) &\leq kgV(p^{Grad(f_1)} - 1, p^{Grad(f_2)} - 1, p^{Grad(f_3)} - 1) \\
&\leq (p^{Grad(f_1)-1} + p^{Grad(f_1)-2} + \ldots + 1)(p^{Grad(f_2)} - 1)(p^{Grad(f_3)} - 1) \\
&< (p^{Grad(f_1)-1} + p^{Grad(f_1)-2} + \ldots + 1)(p^{Grad(f_2)+Grad(f_3)} - 1) \\
&= p^{s-1} + p^{s-2} + \ldots + p^{Grad(f_2)+Grad(f_3)} - p^{Grad(f_1)-1} - p^{Grad(f_1)-2} - \ldots - 1 \\
&< p^{s-1} + p^{s-2} + \ldots + 1 = \frac{p^s - 1}{p - 1}
\end{aligned}$$

Angenommen $P_A(X)$ besitzt eine mehrfache Nullstelle α. Seien $f_1(x), f_2(x), f_3(x)$ die drei irreduziblen Faktoren von $P_A(X)$. Da diese Faktoren irreduzibel sind, können sie in dem endlichen Zerfällungskörper $K_{P_A(X)}$ von $P_A(X)$ keine mehrfachen Nullstellen besitzen. Somit muss α eine Nullstelle von mindestens zwei Polynomfaktoren sein. OBdA sei α eine Nullstelle von $f_1(x)$ und $f_2(x)$. Da beide Polynome irreduzibel sind, müssen sie den gleichen Grad haben wie das Minimalpolynom von α. Insbesondere müssen $f_1(x)$ und $f_2(x)$ den gleichen Grad besitzen. Es gilt also $Grad(f_1(x)) = Grad(f_2(x))$.

Seien im Folgenden α_i die Nullstellen von $f_1(x)$ und $f_2(x)$ und β_i die Nullstellen von $f_3(x)$. Dann ist jeder Teilkörper $Z_p(\alpha_i)$ von $K_{P_A(X)}$ eine Körpererweiterung vom Grad $Grad(f_1(x))$ über dem Körper Z_p. Die multiplikative Gruppe von $Z_p(\alpha_i)$ besitzt somit maximal $p^{Grad(f_1(x))}-1$ Elemente und es gilt $ord(\alpha_i) \mid p^{Grad(f_1(x))} - 1$. Da die multiplikative Gruppe von $Z_p(\alpha_i)$ eine Untergruppe der multiplikativen Gruppe von $K_{P_A(X)}$ ist, folgt auch, dass $ord(\alpha_i) \mid p^{Grad(f_1(x))} - 1$ in der multiplikativen Gruppe von $K_{P_A(X)}$ gilt. Ebenso folgt für alle Nullstellen β_i von $f_3(x)$, dass $ord(\beta_i) \mid p^{Grad(f_3(x))} - 1$ gilt. Es folgt

$$ord(B) \quad | \quad kgV(p^{Grad(f_1(x)} - 1, p^{Grad(f_3(x)} - 1)$$

$$\begin{aligned} &< p^{Grad(f_1(x))+Grad(f_3)(x)} \\ &= p^{s-Grad(f_1(x))} < p^{s-1} + p^{s-2} + \ldots + 1 \end{aligned}$$

Somit folgt auch $ord(A) < p^{s-1} + p^{s-2} + \ldots + 1 = \frac{p^s-1}{p-1}$.

Es bleibt zu zeigen, dass die maximale Ordnung von Matrizen in $SL(s, Z_p)$, deren charakteristisches Polynom irreduzibel in Z_p ist, kleiner als $p^{s-1} + p^{s-2} + \ldots + 1$ ist.

Sei $A \in SL(s, Z_p)$ eine Matrix, deren charakteristisches Polynom $P_A(X)$ irreduzibel ist. Dann gilt für jede Nullstelle α_i von $P_A(X)$, dass in dem Erweiterungskörper $Z_p(\alpha_i)$ gilt: $\alpha_i^{p^s-1} = 1$. Somit gilt auch für alle $\alpha_i; \quad i = 1, 2, \ldots, s$ in dem Zerfällungskörper $K_{P_A(X)}$ von $P_A(X)$: $\alpha_i^{p^s-1} = 1$. Es folgt also $ord(A)|p^s - 1$.

Seien die $\alpha_i; \quad i = 1, 2, \ldots s$ die Nullstellen des charakteristischen Polynoms in dem Zerfällungskörper von $P_A(X)$. Da $P_A(X)$ irreduzibel ist und $K_{P_A(X)}$ ein endlicher und somit vollkommener Körper ist, gilt $\alpha_i \neq \alpha_j$ für $i \neq j$. Dann existiert eine zu A ähnliche Matrix $B \in SL(s, K_{P_A(X)})$ der Form:

$$B := \begin{pmatrix} \alpha_1 & 0 & \cdots & 0 \\ 0 & \alpha_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \alpha_s \end{pmatrix}$$

Dann gilt für B^p:

$$B^p := \begin{pmatrix} \alpha_1^p & 0 & \cdots & 0 \\ 0 & \alpha_2^p & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \alpha_s^p \end{pmatrix}$$

Sei $P_A(X) = \sum_{\ell=0}^{s} c_\ell x^\ell$ mit

$$\begin{aligned} c_s &\equiv_p (-1)^s \\ c_i &\equiv_p (-1)^i \sum_{\substack{\text{alle } s-i \text{ elementigen} \\ \text{Teilmengen J}}} \prod_{j \in J} \alpha_j \end{aligned}$$

Dann gilt für c_i^p:

$$\begin{aligned} c_i^p &\equiv_p ((-1)^i \sum_{\substack{\text{alle } s-i \text{ elementigen} \\ \text{Teilmengen J}}} \prod_{j\in J} \alpha_j)^p \\ &\equiv_p (-1)^i \sum \sum_{\substack{\text{alle } s-i \text{ elementigen} \\ \text{Teilmengen J}}} (\prod_{j\in J} \alpha_j)^p \\ &\equiv_p (-1)^i \sum \sum_{\substack{\text{alle } s-i \text{ elementigen} \\ \text{Teilmengen J}}} \prod_{j\in J} \alpha_j^p \end{aligned}$$

Es gilt aber auch $P_B(X) = \sum_{\ell=0}^{s} d_\ell x^\ell$ mit

$$\begin{aligned} d_s &\equiv_p (-1)^s \\ d_i &\equiv_p (-1)^i \sum_{\substack{\text{alle } s-i \text{ elementigen} \\ \text{Teilmengen J}}} \prod_{j\in J} \alpha_j^p \end{aligned}$$

Also gilt $d_j \equiv_p c_j^p$. Da $d_j, c_j \in Z_p \quad \forall j \in \{1, 2, \ldots, s\}$ und $ggT(p, p-1) = 1$ gilt, folgt $d_j \equiv_p c_j \quad \forall j \in \{1, 2, \ldots, s\}$. Mit anderen Worten: Es gilt $P_A(X) \equiv_p P_B(X) \equiv_p P_{A^p}(X)$. Somit gilt für die Nullstellen $\alpha_i \quad i = 1, 2, \ldots, s$ von $P_A(X)$, dass $\alpha_i^p = \alpha_j$ für ein geeignetes j gilt. Da dies für alle Nullstellen gilt, folgt, dass es eine Zahl $k \in Z$ mit $\alpha_i = \alpha_i^{p^k}$ in $K_{P_A(X)}$ geben muss.

Es wird nun gezeigt, dass $k = s$ gilt. Angenommen, es gilt $k < s$, dann gibt es Nullstellen $\alpha_i \in K_{P_A(X)} \quad i = 1, 2, \ldots, k$, die so angeordnet werden können, dass $\alpha_i^p = \alpha_{i+1}$ für $i = 1, 2, \ldots, k-1$ und $\alpha_k^p = \alpha_1$ gilt. Dann gilt für $j = 1, 2, \ldots, k$:

$$\begin{aligned} e_j^p &\equiv_p (\sum_{\substack{\text{alle } s-i \text{ elementigen} \\ \text{Teilmengen J}}} \prod_{j\in J} \alpha_j)^p \\ &\equiv_p \sum_{\substack{\text{alle } s-i \text{ elementigen} \\ \text{Teilmengen J}}} \prod_{j\in J} \alpha_j^p \\ &\equiv_p \sum_{\substack{\text{alle } s-i \text{ elementigen} \\ \text{Teilmengen J}}} \prod_{j\in J} \alpha_j \equiv_p e_j \end{aligned}$$

Damit folgt für alle $e_j \quad j = 1, 2, \ldots, k$: $e_j^{p-1} = 1$ für alle $e_j \neq 0$ in dem Zerfällungskörper $K_{P_A(X)}$ und somit $e_j \in Z_p$ für alle e_j. Dann wäre aber $\sum_{j=0}^{s} (-1)^j e_j x^j$ ein Polynom $\in Z_p[x]$,

das $P_A(X)$ teilt (da alle Nullstellen auch Nullstellen von $P_A(X)$ sind) und einen kleineren Grad hat als $P_A(X)$. Dies ist aber ein Widerspruch zur Irreduziblität von $P_A(X)$. Also gilt $k = s$.

Mit anderen Worten: Die Nullstellen $\alpha_i \in K_{P_A(X)} \quad i = 1, 2, \ldots, s$ lassen sich so anordnen, dass $\alpha_i^p = \alpha_{i+1}$ für $i = 1, 2, \ldots, s-1$ und $\alpha_s^p = \alpha_1$ gilt.

Dann gilt für die Matrix B:

$$
\begin{aligned}
B^{p^{s-1}+p^{s-2}+\ldots+p+1} &:= \begin{pmatrix} \alpha_1^{p^{s-1}+p^{s-2}+\ldots+p+1} & 0 & \cdots & 0 \\ 0 & \alpha_2^{p^{s-1}+p^{s-2}+\ldots+p+1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \alpha_s^{p^{s-1}+p^{s-2}+\ldots+p+1} \end{pmatrix} \\
&= \begin{pmatrix} \prod_{i=1}^{s} \alpha_i & 0 & \cdots & 0 \\ 0 & \prod_{i=1}^{s} \alpha_i & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \prod_{i=1}^{s} \alpha_i \end{pmatrix} \\
&= \begin{pmatrix} Det(B) & 0 & \cdots & 0 \\ 0 & Det(B) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & Det(B) \end{pmatrix} = I
\end{aligned}
$$

Es gilt also $ord(B) | p^{s-1} + p^{s-2} + \ldots + p + 1$ und somit $ord(A) | p^{s-1} + p^{s-2} + \ldots + p + 1$. Insbesondere gilt somit $ord(A) \leq \frac{p^s - 1}{p-1}$ □

5.3.2.3 Korollar: Sei p eine Primzahl und sei A eine Matrix aus $SL(s, Z_p)$. Ist $P_A(X)$ irreduzibel, dann gilt $ord(A) | \sum_{i=0}^{s-1} p^i$.

Beweis:

Folgt aus dem Beweis von Satz (5.3.2.2). □

5.3.2.4 Korollar: Sei p eine Primzahl und sei A eine Matrix aus $GL(s, Z_p)$ mit $ord(A) = p^s - 1$, dann ist $Det(A)$ ein erzeugendes Element von Z_p^*.

Beweis:

Sei A eine Matrix der Ordnung $p^s - 1$. Nach Korollar (5.2.2.8) muss dann $P_A(X)$ irreduzibel sein. Ebenso wie im Beweis von Satz (5.3.2.2) folgt dann, dass Nullstellen $\alpha_i \in K_{P_A(X)} \quad i = 1, 2, \ldots, s$ von $P_A(X)$ sich so anordnen lassen, dass $\alpha_i^p = \alpha_{i+1}$ für $i = 1, 2, \ldots, s-1$ und $\alpha_s^p = \alpha_1$ gilt.

Dann gilt für die zu A ähnliche Diagonalmatrix $B \in GL(s, Z_p)$:

$$
\begin{aligned}
B^{p^{s-1}+p^{s-1}+\ldots+p+1} &:= \begin{pmatrix} \alpha_1^{p^{s-1}+p^{s-1}+\ldots+p+1} & 0 & \cdots & 0 \\ 0 & \alpha_2^{p^{s-1}+p^{s-1}+\ldots+p+1} & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \alpha_s^{p^{s-1}+p^{s-1}+\ldots+p+1} \end{pmatrix} \\
&= \begin{pmatrix} \prod_{i=1}^{s} \alpha_i & 0 & \cdots & 0 \\ 0 & \prod_{i=1}^{s} \alpha_i & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \prod_{i=1}^{s} \alpha_i \end{pmatrix} \\
&= \begin{pmatrix} Det(B) & 0 & \cdots & 0 \\ 0 & Det(B) & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & Det(B) \end{pmatrix}
\end{aligned}
$$

Also gilt in diesem Fall $ord(B)|(p^{s-1} + p^{s-1} + \ldots + p + 1)(ord(Det(B)))$ und somit auch $ord(A)|(p^{s-1} + p^{s-1} + \ldots + p + 1)(ord(Det(A)))$. Insbesondere folgt aus $ord(A) = p^s - 1$, dass $ord(Det(A)) = p - 1$ gelten muss. □

5.3.2.5 Bemerkung: Die Aussage aus Korollar (5.3.2.4) beantwortet eine Frage aus (De90). Das dort erläuterte Problem wurde nach Angaben der Autoren kurz nach dessen Veröffentlichung bereits auf anderem Wege gelöst. Der obige Beweis geht aber noch einen Schritt weiter. Er zeigt auf, wie sich die Ordnung von Matrizen verhält, deren charakteristisches Polynom irreduzibel ist: Ist $P_A(X)$ irreduzibel und existiert eine Zahl $t \in Z$ mit $t|ord(A)$ und $ggT(t, \prod_{i=0}^{s-1} p^i) = 1$, so gilt $t|ord(Det(A))$.

5.3.2.6 Satz: Es sei p eine Primzahl und $A \in SL(s, Z_p)$. A besitzt genau dann eine Ordnung, die $p-1$ teilt, wenn A diagonalisierbar ist.

Beweis:

"$\Rightarrow$" Angenommen, es gilt $ord(A)|p-1$. Dann gibt es eine zu A ähnliche Matrix $B \in SL(s, K_{P_A(X)})$ der Form:

$$B := \begin{pmatrix} \alpha_1 & 0 & \cdots & 0 \\ 0 & \alpha_2 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & \alpha_s \end{pmatrix}$$

Dabei sind die α_i die Nullstellen des charakteristischen Polynoms $P_A(X)$ von A. Da B eine Diagonalmatrix ist, gilt: $ord(B) = kgV(ord(\alpha_i); i = 1, 2, \ldots, s)$. Da $ord(A) = ord(B)$ gilt, folgt: $\alpha_i^{p-1} = 1$ in dem Zerfällungskörper $K_{P_A(X)}$ des charakteristischen Polynoms $P_A(X)$ von A. $K_{P_A(X)}$ ist ein Erweiterungskörper von Z_p. Die Elemente des Erweiterungskörpers, deren Ordnung $p-1$ teilt, sind genau die Elemente, die in Z_p^* liegen, denn es gilt: Da $K_{P_A(X)}$ ein endlicher Körper ist, ist die multiplikative Gruppe des Körpers zyklisch. Es gibt also ein Element $\theta \in K_{P_A(X)}$, welches die multiplikative Gruppe von $K_{P_A(X)}$ erzeugt. Für alle Elemente $\beta_i \in K_{P_A(X)}$, deren Ordnung $p-1$ teilt, existiert also eine Zahl $a_i < |K_{P_A(X)}| - 1$, so dass $\beta_i = \theta^{a_i}$ gilt. Es folgt, dass ein Element der multiplikativen Gruppe genau dann eine Ordnung besitzt, die $p-1$ teilt, wenn $|K_{P_A(X)}| \mid a_i(p-1)$ mit $a_i < |K_{P_A(X)}|$ gilt. Also genau dann, wenn $a_i = \frac{|K_{P_A(X)}|}{p-1} i$ für $i = 1, 2, \ldots, p-1$. Mit anderen Worten es gibt in dem Erweiterungskörper von Z_p genau $p-1$ Elemente, deren Ordnung $p-1$ teilt. Dieses sind genau die Elemente aus Z_p^*

"$\Leftarrow$" Ist A diagonalisierbar, so gilt nach Satz (5.2.2.1): $ord(A)|p-1$. □

5.4 Das diskrete Logarithmusproblem in $SL(s, Z_n)$

In diesem Abschnitt wird das diskrete Logarithmusproblem in der Gruppe $SL(s, Z_n)$ betrachtet. Da sich das diskrete Logarithmusproblem in $SL(s, Z_n)$ $(n = pq)$ mit Hilfe des Chinesischen Restsatzes für Matrizen auf das diskrete Logarithmusproblem in $SL(s, Z_p)$

und $SL(s, Z_q)$ zurückführen lässt, wird im Folgenden nur das diskrete Logarithmusproblem in $SL(s, Z_p)$ betrachtet.

Man kann leicht zeigen, dass das diskrete Logarithmusproblem in $SL(s, Z_p)$ mindestens so schwierig ist wie das diskrete Logarithmusproblem in Z_p.

5.4.1 Satz: Das diskrete Logarithmusproblem in $SL(s, Z_p)$ ist mindestens so schwierig wie das diskrete Logarithmusproblem in Z_p.

Beweis:

Angenommen, das diskrete Logarithmusproblem in $SL(s, Z_p)$ wäre lösbar, d.h. es gibt einen effizienten Algorithmus Alg, der zu einem Wertepaar $(A, B) \in SL(s, Z_p) \times SL(s, Z_p)$ mit $B \in < A >$ und $p \in P$ ein k ermittelt, so dass $B \equiv_p A^k$ gilt, dann kann dieser Algorithmus dazu verwendet werden, das diskrete Logarithmusproblem in Z_p zu lösen.

Um das diskrete Logarithmusproblem für ein $(x, y) \in Z_p \times Z_p$ zu lösen, kann der Algorithmus Alg wie folgt verwendet werden:

Man setzt $A \equiv_p \begin{pmatrix} x & 0 & \dots & 0 \\ 0 & 1 & 0 & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & x^{-1} \end{pmatrix}$ und $B \equiv_p \begin{pmatrix} y & 0 & \dots & 0 \\ 0 & 1 & 0 & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & y^{-1} \end{pmatrix}$ und verwendet diese beiden Matrizen als Eingabe für den Algorithmus Alg. Dieser gibt ein k aus, so dass $B \equiv_p A^k$ gilt. Da $A^\ell \equiv_p \begin{pmatrix} x^\ell & 0 & \dots & 0 \\ 0 & 1 & 0 & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & x^{-\ell} \end{pmatrix}$ gilt, folgt $x^k \equiv_p y$ in Z_p. Damit ist das diskrete Logarithmusproblem für $(x, y) \in Z_p \times Z_p$ gelöst. □

Der folgende Satz zeigt, unter welchen Bedingungen eine Matrix aus $SL(s, Z_p)$ die Ordnung p besitzt.

5.4.2 Satz: Sei $A \in SL(s, Z_p) \backslash \{I\}$ Dann gilt:

$$ord(A) = p \quad \Leftrightarrow \quad P_A(X) \equiv_p \sum_{i=0}^{s} (-1)^i \binom{s}{i} x^i$$

Beweis:

"$\Rightarrow$" Sei A eine Matrix der Ordnung p und seien α_i die Nullstellen des charakteristischen Polynoms von A in dem Zerfällungskörper von $P_A(X)$.

Dann existiert eine zu A ähnliche Dreiecksmatrix $B \in SL(s, K_{P_A(X)})$, die auf der Hauptdiagonalen die Elemente α_i besitzt. Es gilt für die Koeffizienten c_i von $P_B(X)$:

$$\begin{aligned}
c_s &\equiv_p (-1)^s \\
c_i &\equiv_p (-1)^i \sum_{\substack{\text{alle } s-i \text{ elementigen} \\ \text{Teilmengen J}}} \prod_{j \in J} \alpha_j \\
c_i^p &\equiv_p \left((-1)^i \sum_{\substack{\text{alle } s-i \text{ elementigen} \\ \text{Teilmengen J}}} \prod_{j \in J} \alpha_j \right)^p \\
&\equiv_p (-1)^i \sum_{\substack{\text{alle } s-i \text{ elementigen} \\ \text{Teilmengen J}}} \left(\prod_{j \in J} \alpha_j \right)^p \\
&\equiv_p (-1)^i \sum_{\substack{\text{alle } s-i \text{ elementigen} \\ \text{Teilmengen J}}} \prod_{j \in J} \alpha_j^p \\
&\equiv_p (-1)^i \sum_{\substack{\text{alle } s-i \text{ elementigen} \\ \text{Teilmengen J}}} \prod_{j \in J} 1 \equiv_p (-1)^i \binom{s}{i}
\end{aligned}$$

"$\Leftarrow$" Sei $P_A(X) \equiv_p \sum_{i=0}^{s} (-1)^i \binom{s}{i} x^i$. Dann gilt $P_A(X) \equiv_p (1-x)^s$.

Dann gibt es eine zu A ähnliche Matrix B der Form

$$B := \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

Es folgt $ord(A) = ord(B) = p$. □

5.4.3 Satz: Sei $A \in SL(s, Z_p)$ und p eine Primzahl und sei $ord(A) = p$ und $B \in < A >$,

dann kann das diskrete Logarithmusproblem von B bezüglich A mit polynomiellem Zeit- und Speicheraufwand gelöst werden.

Beweis:

Sei $B \equiv_p A^k$. Ist $B \equiv_p I$, so gilt $ord(A) = p|k$, und $k = p$ wäre eine Lösung des diskreten Logarithmusproblems. Sei also $B \not\equiv_p I$.

Nach Satz (5.4.2) gibt es eine zu A ähnliche Matrix C der Form:

$$C := \begin{pmatrix} 1 & 1 & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & 1 \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

Es gilt für $ggT(k, p) = 1$:

$$C^k \equiv_p \begin{pmatrix} 1 & k & 0 & \cdots & 0 \\ 0 & 1 & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & k \\ 0 & \cdots & \cdots & 0 & 1 \end{pmatrix}$$

Es ist in polynomieller Zeit möglich, Matrizen $U, U^{-1} \in GL(s, Z_p)$ zu bestimmen, so dass $UAU^{-1} \equiv_p C$ gilt. Dann folgt: $UBU^{-1} \equiv_p UA^kU^{-1} \equiv_p (UAU^{-1})^k \equiv_p C^k$. Dann ist der diskrete Logarithmus von B zur Basis A direkt in den Einträgen von C zu finden. □

5.4.1 Klassifikation der Matrizen aus $SL(s, Z_p)$

In diesem Abschnitt soll geklärt werden, wie schwierig das diskrete Logarithmusproblem für Matrizen in $SL(s, Z_p)$ ist. Dazu werden die Matrizen aus $SL(s, Z_p)$ ebenso wie die Matrizen aus $SL(2, Z_p)$ in Klassen unterteilt:

5.4.1.1 Definition: Klassifizierung von Matrizen aus $SL(s, Z_p)$

Die Matrizen aus $SL(s, Z_p)$ werden in folgende Klassen eingeteilt:

- **Klasse 1:**

  Die Menge der Matrizen der Klasse 1 beinhaltet alle Matrizen $A \in SL(s, Z_p)$ mit $ord(A)|(p-1)$.

- **Klasse 2:**

  Die Menge der Matrizen der Klasse 2 beinhaltet alle Matrizen $A \in SL(s, Z_p)$ mit $ord(A) = 2p$ oder $ord(A) = p$.

- **Klasse 3:**

  Die Menge der Matrizen der Klasse 3 beinhaltet alle Matrizen $A \in SL(s, Z_p)$ die weder in Klasse 1 sind noch in Klasse 2 mit $ord(A)|(p-1)p$.

- **Klasse 4:**

  Die Menge der Matrizen der Klasse 4 beinhaltet alle Matrizen $A \in SL(s, Z_p)$, die nicht in Klasse 1 oder Klasse 3 liegen mit $ggT(ord(A), p^i - 1) > 1$ für ein $i \in \{2, 3, \ldots, s-1\}$.

- **Klasse 5:**

  Die Menge der Matrizen der Klasse 5 beinhaltet alle Matrizen $A \in SL(s, Z_p)$ mit $ggT(ord(A), \sum_{j=0}^{s-1} p^j) > 1$, die nicht in den Klassen 1, 3 oder 4 enthalten. sind.

5.4.1.2 Satz: Jede Matrix $A \in SL(s, Z_p)\backslash\{\pm I\}$ mit $ord(A) \neq 2$ liegt in genau einer der angegebenen Klassen.

Beweis:

Sei A eine Matrix aus $SL(s, Z_p)\backslash\{\pm I\}$ mit $ord(A) \neq 2$.

Zunächst wird gezeigt, dass A in mindestens einer der angegebenen Klassen ist. Ist A eine Diagonalmatrix, so gilt nach Satz (5.2.2.1) $ord(A)|p-1$, und somit wäre A eine Matrix der Klasse 1.

Ist A triagonalisierbar, so existiert eine zu A ähnliche Matrix B, die die Jordansche Normalform besitzt. Diese ist entweder eine Diagonalmatrix und ist somit eine Matrix der Klasse 1, oder eine Matrix der Klasse 2 oder der Klasse 3.

Im Folgenden soll nun der Fall betrachtet werden, dass A nicht triagonalisierbar ist. Ist A nicht triagonalisierbar, so besitzt das charakteristische Polynom $P_A(X)$ von A mindestens eine Nullstelle α, die nicht in Z_p^* liegt. Es gilt $\alpha \not\equiv_p 0$, da sonst $Det(A) \equiv_p 0$ und somit $A \notin SL(s, Z_p)$ gelten würde. Ist $P_A(X)$ reduzibel, so sei $F(x)$ der irreduzible Faktor von $P_A(X)$, der die Nullstelle α enthält. Dann gilt $\alpha^{p^{Grad(F(x))}-1} = 1$ in dem Zerfällungskörper von $P_A(X)$ über Z_p. Somit gilt $ggT(ord(A), p^{Grad(F(x))} - 1) > 1$, und A ist eine Matrix der Klasse 4. Ist $P_A(X)$ irreduzibel, so gilt nach Korollar (5.3.2.3): $ord(A) | \sum_{i=0}^{s-1} p^i$. Dann ist A mindestens in Klasse 5 enthalten.

Nun wird gezeigt, dass A in genau einer der obigen Klassen liegt, falls $ord(A) \neq 2$ gilt. Angenommen, A würde in Klasse 1 und einer weiteren Klasse liegen (nach Definition kann sie nicht gleichzeitig in Klasse 3 liegen). A kann nicht in Klasse 2 liegen, denn dann existiert eine Primzahl $t > 2$ mit $t | ord(A)$ (da $A \not\equiv_p \pm I$), die auch die $2p$ teilen müsste. Da $t > 2$ gilt, folgt $t | p$, also $t = p$. Dies ist aber ein Widerspruch zur Voraussetzung $t | p - 1$.

Die charakteristischen Polynome der Matrizen der Klassen 4 und 5 besitzen mindestens eine Nullstelle, die nicht in Z_p^* liegt, und somit sind diese Matrizen nicht triagonalisierbar in $SL(s, Z_p)$. Somit können sie auch in keiner der Klassen 1, 2 oder 3 liegen. Folglich können Matrizen, die in einer der Klassen 1, 2 oder 3 liegen, in keiner weiteren Klasse sein. Nach Definition sind auch die Klasse 4 und 5 disjunkt. □

Abhängig von der Klasse in der eine Matrix liegt, können unterschiedliche Aussagen über die Schwierigkeit des diskreten Logarithmusproblems getroffen werden.

5.4.1.3 Satz: Sei A eine Matrix der Klasse 1, dann ist das diskrete Logarithmusproblem in $< A >$ äquivalent zum diskreten Logarithmusproblem in Z_p.

Beweis:

Dass das diskrete Logarithmusproblem in Z_p gelöst werden kann, falls ein Algorithmus zur Berechnung des diskreten Logarithmus für Matrizen der Klasse 1 existiert, folgt direkt aus dem gleichen Satz für Matrizen aus $SL(2, Z_p)$ (Satz (4.4.1.0.8)), da die Matrizen der

Klasse 1 aus $SL(2, Z_p)$ in den Matrizen der Klasse 1 aus $SL(s, Z_p)$ eingebettet werden können.

Nun soll der umgekehrte Fall betrachtet werden. Angenommen, es gibt einen Algorithmus Alg, der das diskrete Logarithmusproblem in Z_p^* lösen kann, dann kann dieser Algorithmus dazu verwendet werden, das diskrete Logarithmusproblem für Matrizen der Klasse 1 zu lösen.

Sei A eine Matrix der Klasse 1, also $ord(A)|p-1$. Ist A eine Diagonalmatrix, so folgt die Behauptung sofort, da in diesem Fall für $B \equiv_p A^k$ gilt:

$$A^k \equiv_p \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & \prod_{i=1}^{s-1} a_{ii}^{-1} \end{pmatrix}^k \equiv_p \begin{pmatrix} a_{11}^k & 0 & \dots & 0 \\ 0 & a_{22}^k & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & \prod_{i=1}^{s-1} a_{ii}^{-k} \end{pmatrix}$$

Es ist leicht zu sehen, dass der Algorithmus zur Berechnung von diskreten Logarithmen in Z_p^* dazu verwendet werden kann, das diskrete Logarithmusproblem für Diagonalmatrizen zu lösen.

Also sei im Folgenden A keine Diagonalmatrix. Da A eine Matrix der Klasse 1 ist, ist A nach Satz (5.3.2.6) diagonalisierbar. Mit anderen Worten: Das charakteristische Polynom $P_A(X)$ von A zerfällt in Z_p in Linearfaktoren. Mit Hilfe des Algorithmus von E. Berlekamp (Be67) können die Nullstellen von $P_A(X)$ bestimmt werden. Somit kann auch eine zu A ähnliche Diagonalmatrix C bestimmt werden. Es gibt also Matrizen $U, U^{-1} \in SL(s, Z_p)$, so dass $UAU^{-1} \equiv_p C$ gilt. Dann ist $UBU^{-1} \equiv_p C^k$ ebenfalls eine Diagonalmatrix, mit deren Hilfe der diskrete Logarithmus von B zur Basis A auf das diskrete Logarithmusproblem der Nullstellen der charakteristischen Polynome in Z_p zurückgeführt werden kann. Daraus folgt die Behauptung des Satzes. □

5.4.1.4 Satz: Sei A eine Matrix der Klasse 2, dann ist das diskrete Logarithmusproblem in $< A >$ mit polynomiellem Zeit- und Speicheraufwand lösbar.

Beweis:

Gilt $ord(A) = p$, so ist das diskrete Logarithmusproblem nach Satz (5.4.3) mit polynomiellem Zeit- und Speicheraufwand lösbar. Gilt $ord(A) = 2p$, und man möchte das diskrete Logarithmusproblem von einer Matrix $B \in < A >$ bezüglich A lösen, so löst man zunächst das diskrete Logarithmusproblem von B^2 bezüglich A^2. Sei k diese Lösung. Dann ist entweder k oder $k + p$ die Lösung des diskreten Logarithmusproblems von B bezüglich A. □

5.4.1.5 Satz: Sei A eine Matrix der Klasse 3, dann ist das diskrete Logarithmusproblem in $< A >$ äquivalent zum diskreten Logarithmusproblem in Z_p.

Beweis:

Sei A eine Matrix der Klasse 3. Dann gilt $ord(A)|p(p-1)$. Um das diskrete Logarithmusproblem (A, B) mit $B \in < A >$ zu lösen, geht man wie folgt vor:

Zunächst berechnet man den diskreten Logarithmus k_1 zu (A^{p-1}, B^{p-1}), was nach Satz (5.4.1.4) mit polynomiellem Zeit- und Speicheraufwand möglich ist. Dann berechnet man den diskreten Logarithmus k_2 zu (A^p, B^p), welcher nach Satz (5.4.1.3) äquivalent zum Lösen des diskreten Logarithmusproblems in Z_p ist. Der diskrete Logarithmus zu (A, B) ist dann die eindeutig bestimmbare Zahl $k \in Z_{p(p-1)}$ mit $k \equiv_p k_1$ und $k \equiv_{p-1} k_2$. Also ist das Berechnen von diskreten Logarithmen in der Klasse 3 äquivalent zu dem Berechnen von diskreten Logarithmen in Z_p. □

5.4.1.6 Bemerkung: Für Matrizen der Klassen 4 und 5 lässt sich keine direkte Beziehung zwischen dem Berechnen von diskreten Logarithmen in der Gruppe der Matrizen der beiden Klassen und dem Berechnen von diskreten Logarithmen in der Gruppe Z_p^* beweisen.

Besitzt das charakteristische Polynom einer Matrix der Klasse 4 eine Nullstelle $\alpha \in Z_p^*$, so ist das diskrete Logarithmusproblem für diese Matrix mindestens so schwierig zu lösen wie das diskrete Logarithmusproblem zur Basis α in Z_p^*

Da das charakteristische Polynom von Matrizen der Klasse 5 keine Nullstellen in Z_p besitzt, kann auch keine Aussage darüber getroffen werden, ob das Berechnen von diskreten Logarithmen in der Gruppe der Klasse 5 Matrizen mindestens so schwierig ist wie in der Gruppe Z_p^*.

5.5 Das diskrete Logarithmusproblem in $GL(s, Z_n)$

Da sich das diskrete Logarithmusproblem in $GL(s, Z_n)$ $(n = pq)$ mit Hilfe des Chinesischen Restsatzes für Matrizen auf das diskrete Logarithmusproblem in $GL(s, Z_p)$ und $GL(s, Z_q)$ zurückführen lässt, wird im Folgenden nur das diskrete Logarithmusproblem in $GL(s, Z_p)$ betrachtet.

5.5.1 Klassifikation der Matrizen aus $GL(s, Z_p)$

In diesem Abschnitt wird gezeigt werden, dass das diskrete Logarithmusproblem in $GL(s, Z_p)$ in engem Zusammenhang mit dem diskreten Logarithmusproblem in Z_p steht.

Betrachtet man die Gruppe $GL(s, Z_p)\backslash SL(s, Z_p)$, so wird sofort deutlich, dass das diskrete Logarithmusproblem in $GL(s, Z_p)$ mindestens so schwierig ist wie das diskrete Logarithmusproblem in Z_p.

5.5.1.1 Satz: Das diskrete Logarithmusproblem in $GL(s, Z_p)\backslash SL(s, Z_p)$ ist mindestens so schwierig wie das diskrete Logarithmusproblem in Z_p.

Beweis:

Die Behauptung folgt direkt aus Satz (4.4.2.1), da die Gruppe $GL(2, Z_p)\backslash SL(2, Z_p)$ in eine Untergruppe der Gruppe $GL(s, Z_p)\backslash SL(s, Z_p)$ eingebettet werden kann. □

Ebenso wie in $SL(s, Z_p)$ besteht ein enger Zusammenhang zwischen der Diagonalisierbarkeit einer Matrix und deren Ordnung:

5.5.1.2 Satz: Es sei p eine Primzahl und $A \in GL(s, Z_p)$. A besitzt genau dann eine Ordnung, die $p - 1$ teilt, wenn A diagonalisierbar ist.

Beweis:

Der Beweis erfolgt genauso wie in Satz (5.3.2.6) mit $A \in GL(s, Z_p)$ und $B \in GL(s, K_{P_A(X)})$. □

Es wurde bereits gezeigt, dass die Ordnung einer Matrix $A \in GL(s, Z_p)$ maximal den Wert $(p^s - 1)$ annehmen kann. Die in dem vorherigen Abschnitt eingeführte Einteilung der Matrizen in Klassen kann für den Fall $A \in GL(s, Z_p)\backslash SL(s, Z_p)$ erweitert werden.

5.5.1.3 Definition: Klassifizierung von Matrizen aus $GL(s, Z_p)\backslash SL(s, Z_p)$

Die Matrizen aus $GL(s, Z_p)\backslash SL(s, Z_p)$ werden in folgende Klassen eingeteilt:

- **Klasse 6:**

  Die Menge der Matrizen der Klasse 6 beinhaltet alle Matrizen $A \in GL(s, Z_p)\backslash SL(s, Z_p)$ mit $ord(A)|(p-1)$.

- **Klasse 7:**

  Die Menge der Matrizen der Klasse 7 beinhaltet alle Matrizen $A \in GL(s, Z_p)\backslash SL(s, Z_p)$ mit $p|ord(A)$.

- **Klasse 8:**

  Die Menge der Matrizen der Klasse 8 beinhaltet alle Matrizen $A \in GL(s, Z_p)\backslash SL(s, Z_p)$ mit $ggT(ord(A), p^i + p^{i-1} + \cdots + p + 1) > 1$ für ein $i \in \{1, 2, 3, \ldots, s-1\}$, die nicht in der Klasse 6 enthalten sind.

- **Klasse 9:**

  Die Menge der Matrizen der Klasse 9 beinhaltet alle Matrizen $A \in GL(s, Z_p)\backslash SL(s, Z_p)$ mit $ord(A)|(p^s - 1)$, die nicht in Klasse 6 oder Klasse 8 enthalten sind.

Zunächst soll gezeigt werden, dass in dieser Klassifizierung alle Matrizen aus $GL(s, Z_p)$ enthalten sind.

5.5.1.4 Satz: Jede Matrix $A \in GL(s, Z_p)\backslash SL(s, Z_p)$ liegt in mindestens einer der angegebenen Klassen 6-9.

Beweis: Sei $A \in GL(s, Z_p)\backslash SL(s, Z_p)$ eine beliebige Matrix, dann können die folgenden Fälle unterschieden werden:

Ist A diagonalisierbar, so ist A eine Matrix der Klasse 6.

Ist A triagonalisierbar, aber nicht diagonalisierbar, dann ist A eine Matrix der Klasse 7.

Ist A nicht triagonalisierbar, dann besitzt A mindestens eine Nullstelle $\alpha \notin Z_p^*$, und es gilt für das Minimalpolynom $\mu \in Z_p[x]$ von α: $\mu | P_A(X)$ und $\alpha^{p^{Grad(\mu)}-1} = 1$ in dem

Erweiterungskörper $K_{P_A(X)}$ von Z_p. Somit gilt $ord(\alpha)|p^{Grad(\mu)} - 1$. Da $\alpha \notin Z_p^*$ gilt, folgt, dass es eine Primzahl t geben muss mit $t|ord(\alpha)$ und $t|p^{Grad(\mu)-1} + p^{Grad(\mu-2)} + \ldots + 1$.

Gilt $\mu \neq P_A(X)$, dann ist $Grad(\mu) < Grad(P_A(X)) = s$, und es folgt $ggT(ord(A), p^{Grad(\mu)-1} + p^{Grad(\mu-2)} + \ldots + 1) > 1$, also ist in diesem Fall A eine Matrix der Klasse 8.

Gilt für alle Nullstellen α_i von $P_A(X)$: $\alpha_i \notin Z_p^*$, so ist $P_A(X)$ irreduzibel. Dann ist $P_A(X)$ das Minimalpolynom von allen α_i, und es gilt $\alpha_i^{p^s-1} = 1$ in dem Zerfällungskörper von $P_A(X)$. Dann gilt auch $ord(A)|p^s - 1$. Dann ist A eine Matrix der Klasse 9. □

Nach der obigen Definition ist klar, dass eine Matrix A nur in genau einer der Klassen enthalten ist.

Abhängig von der Klasse, in der eine Matrix liegt, können unterschiedliche Aussagen über die Schwierigkeit des diskreten Logarithmusproblems getroffen werden.

5.5.1.5 Satz: Sei A eine Matrix der Klasse 6, dann ist das diskrete Logarithmusproblem in $< A >$ äquivalent zum diskreten Logarithmusproblem in Z_p.

Beweis:

Dass das diskrete Logarithmusproblem in Z_p gelöst werden kann, falls ein Algorithmus zur Berechnung des diskreten Logarithmus für Matrizen der Klasse 6 existiert, folgt direkt aus dem gleichen Satz für Matrizen aus $SL(2, Z_p)$ Satz (4.4.2.0.14), da die Matrizen der Klasse 6 aus $SL(2, Z_p)$ in die Matrizen der Klasse 6 aus $SL(s, Z_p)$ eingebettet werden können.

Nun soll der umgekehrte Fall betrachtet werden. Angenommen, es gibt eine Algorithmus Alg, der das diskrete Logarithmusproblem in Z_p^* lösen kann, dann kann dieser Algorithmus dazu verwendet werden, das diskrete Logarithmusproblem für Matrizen der Klasse 6 zu lösen.

Sei A eine Matrix der Klasse 6, also $ord(A)|p - 1$. Ist A eine Diagonalmatrix, so folgt die Behauptung sofort, da für $B \equiv_p A^k$ gilt:

$$A^k \equiv_p \begin{pmatrix} a_{11} & 0 & \dots & 0 \\ 0 & a_{22} & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & \prod_{i=1}^{s-1} a_{ii}^{-1} \end{pmatrix}^k \equiv_p \begin{pmatrix} a_{11}^k & 0 & \dots & 0 \\ 0 & a_{22}^k & \ddots & \vdots \\ \vdots & \ddots & \ddots & \vdots \\ 0 & \cdots & \cdots & \prod_{i=1}^{s-1} a_{ii}^{-k} \end{pmatrix}$$

Es ist leicht zu sehen, dass der Algorithmus zur Berechnung von diskreten Logarithmen in Z_p^* dazu verwendet werden kann, das diskrete Logarithmusproblem für Diagonalmatrizen zu lösen.

Also sei im Folgenden A keine Diagonalmatrix. Da A eine Matrix der Klasse 6 ist, ist A nach Satz (5.5.1.2) diagonalisierbar. Mit anderen Worten: Das charakteristische Polynom $P_A(X)$ von A zerfällt in Z_p in paarweise verschiedene Linearfaktoren. Mit Hilfe des Algorithmus von E. Berlekamp (Be67) können die Nullstellen von $P_A(X)$ bestimmt werden. Somit kann auch eine zu A ähnliche Diagonalmatrix bestimmt werden, mit deren Hilfe der diskrete Logarithmus von B zur Basis A bestimmt werden kann. Also gilt die Behauptung des Satzes. □

5.5.1.6 Bemerkung: Für Matrizen der Klassen 7, 8 und 9 kann nicht gezeigt werden, ob das Berechnen von diskreten Logarithmen für Matrizen dieser Klassen genauso schwierig oder sogar schwieriger ist als das Berechnen von diskreten Logarithmen in der Gruppe Z_p^*.

Es kann auch nicht gezeigt werden, dass das diskrete Logarithmusproblem in diesen Gruppen mindestens so schwierig ist wie das diskrete Logarithmusproblem in Z_p^*:

Es gilt zwar, dass für Matrizen A, B der Klassen 7, 8 oder 9 ein Algorithmus, der das diskrete Logarithmusproblem (A, B) löst, immer auch das diskrete Logarithmusproblem $(Det(A), Det(B))$ in der Gruppe Z_p^* löst. Dies reicht aber nicht aus, um zu zeigen, dass das diskrete Logarithmusproblem in diesen Klassen mindestens so schwierig ist wie in Z_p^*. Um dies zu zeigen, müsste man zu zwei vorgegebenen Zahlen $(x, y) \in Z_p^* \times Z_p^*$ mit $y \equiv_p x^k$ zwei Matrizen A, B aus einer der Klassen 7,8 oder 9 finden, so dass $B \in < A >$; $Det(A) \equiv_p x$ und $Det(B) \equiv_p y$ gilt. Zu diesem Problem ist aber bis heute kein effizienter Algorithmus bekannt, der nicht die Kenntnis von k voraussetzt.

Die folgenden Sätze zeigen, mit welcher Wahrscheinlichkeit eine zufällig gewählte Matrix in den einzelnen Klassen enthalten ist.

5.5.1.7 Satz: Sei p eine große Primzahl und sei A eine zufällige Matrix aus $GL(s, Z_p)$, dann lässt sich die Wahrscheinlichkeit, dass A eine Matrix aus der Klasse 1 oder Klasse 6 ist, durch $\frac{1}{s!}$ abschätzen.

Beweis:

Die Matrizen der Klasse 1 und der Klasse 6 sind genau die Matrizen, für die $ord(A)|p-1$ gilt. Nach Satz (5.5.1.2) ist dann A diagonalisierbar, und $P_A(X)$ zerfällt in Z_p in paarweise verschiedene Linearfaktoren. Ist A eine zufällige Matrix aus $GL(s, Z_p)$, dann ist auch das charakteristische Polynom von A ein zufälliges normiertes Polynom aus $Z_p[x]$ vom Grad s. Die Wahrscheinlichkeit, dass ein zufälliges normiertes Polynom aus $Z_p[x]$ komplett in paarweise verschiedene Linearfaktoren zerfällt, beträgt $\frac{\binom{p}{s}}{p^s}$.

Es gilt:

$$\begin{aligned}
\frac{\binom{p}{s}}{p^s} &= \frac{p(p-1)\cdots(p-s+1)}{s!p^s} < \frac{1}{s!} \\
\frac{\binom{p}{s}}{p^s} &= \frac{p(p-1)\cdots(p-s+1)}{s!p^s} > \frac{p^s - s(s-1)p^{s-1}}{s!p^s} \\
&= \frac{1}{s!} - \frac{1}{(s-2)!p}
\end{aligned}$$

Es gilt also:

$$\frac{1}{s!} - \frac{1}{(s-2)!p} < \frac{\binom{p}{s}}{p^s} < \frac{1}{s!}$$

Da p im Vergleich zu s sehr groß ist, ist der letzte Term sehr klein. Somit gilt die Behauptung des Satzes. □

5.5.1.8 Satz: Sei p eine große Primzahl und sei A eine zufällige Matrix aus $GL(s, Z_p)$, dann liegt die Wahrscheinlichkeit, dass A eine Matrix aus der Klasse 2, der Klasse 3 oder der Klasse 7 ist, in der Größenordnung von $\frac{1}{p}$.

Beweis:

Die Matrizen der Klasse 2, der Klasse 3 und der Klasse 7 sind genau die Matrizen, für die $p|ord(A)$ gilt. Nach Satz (5.2.2.6) besitzt $P_A(X)$ in dem Zerfällungskörper $K_{P_A(X)}$ mindestens eine mehrfache Nullstelle. Mit anderen Worten: $P(A)$ besitzt keine quadratfreie Faktorzerlegung. Ist A eine zufällig gewählte Matrix aus $GL(s, Z_p)$, dann ist auch das charakteristische Polynom von A ein zufälliges normiertes Polynom aus $Z_p[x]$ vom Grad s. Die Wahrscheinlichkeit, dass ein zufällig gewähltes normiertes Polynom aus $Z_p[x]$ eine quadratfreie Faktorzerlegung besitzt, beträgt nach (FGP96) $1 - \frac{1}{p}$. Also beträgt die Wahrscheinlichkeit, dass ein zufälliges Polynom keine quadratfreie Faktorzerlegung besitzt, $\frac{1}{p}$. □

5.5.1.9 Satz: Sei p eine große Primzahl und sei A eine zufällig gewählte Matrix aus $GL(s, Z_p)$, dann kann die Wahrscheinlichkeit, dass A eine Matrix aus der Klasse 4 oder der Klasse 8 ist, durch $1 - \frac{(s-1)!+1}{s!}$ abgeschätzt werden.

Beweis:

Die Matrizen der Klasse 4 und der Klasse 8 sind genau die Matrizen, für die $ggT(ord(A), p^i + p^{i-1} + \cdots + p + 1) > 1$ für ein $i \in \{1, 2, 3, \ldots, s-1\}$ gilt. Dann ist $P_A(X)$ nicht irreduzibel über Z_p und besitzt mindestens einen irreduziblen Faktor vom Grad ≥ 2. Mit anderen Worten: Die Matrizen der Klasse 4 und Klasse 8 sind genau die Matrizen, deren charakteristisches Polynom weder irreduzibel ist, noch komplett in Linearfaktoren zerfällt. Ist A eine zufällig gewählte Matrix aus $GL(s, Z_p)$, dann ist auch das charakteristische Polynom von A ein zufälliges normiertes Polynom aus $Z_p[x]$ vom Grad s.

Die Wahrscheinlichkeit, dass ein zufällig gewähltes normiertes Polynom aus $Z_p[x]$ irreduzibel ist, lässt sich nach (FGP96) durch $\frac{1}{s}$ abschätzen. Die Wahrscheinlichkeit, dass einzufällig gewähltes normiertes Polynom aus $Z_p[x]$ in Linearfaktoren zerfällt, lässt sich nach Satz (5.5.1.7)und Satz (5.5.1.8)durch $\frac{1}{s!}$ abschätzen.

Dann lässt sich die Wahrscheinlichkeit, dass A eine Matrix der Klasse 4 oder der Klasse 8 ist, mit $1 - \frac{1}{s} - \frac{1}{s!} = 1 - \frac{(s-1)!+1}{s!}$ abschätzen. Damit folgt die Behauptung. □

5.5.1.10 Satz: Sei p eine große Primzahl und sei A eine zufällig gewählte Matrix aus $GL(s, Z_p)$, dann lässt sich die Wahrscheinlichkeit, dass A eine Matrix aus der Klasse 5 oder der Klasse 9 ist, durch $\frac{1}{s}$ abschätzen.

Beweis:

Die Matrizen der Klasse 5 und der Klasse 9 sind genau die Matrizen, für die $ord(A)|(p^s - 1)$ gilt. Nach Korollar (5.2.2.8) und Korollar (5.3.2.3) ist dann $P_A(X)$ irreduzibel über Z_p. Ist A eine zufällige Matrix aus $GL(s, Z_p)$, dann ist auch das charakteristische Polynom von A ein zufälliges normiertes Polynom aus $Z_p[x]$ vom Grad s. Die Wahrscheinlichkeit, dass ein zufälliges normiertes Polynom aus $Z_p[x]$ irreduzibel ist, lässt sich nach (FGP96) durch $\frac{1}{s}$ abschätzen. □

5.6 Das diskrete Wurzelproblem in $GL(s, Z_n)$ und $SL(s, Z_n)$

In diesem Abschnitt wird das Problem des Ziehens diskreter Wurzeln in $GL(s, Z_n)$ und $SL(s, Z_n)$ behandelt, wobei $n = pq$ das Produkt zweier Primzahlen darstellt. Wie bereits in Abschnitt 4.5 beschrieben, muss man beim Ziehen diskreter Wurzeln in einer Gruppe G mit Ordnung $|G|$ zwei Fälle unterscheiden. Betrachtet man die $d-te$ Wurzel eines Elements aus G, und es gilt $ggT(d, |G|) = 1$, so existiert eine eindeutige diskrete $d - te$ Wurzel zu jedem Element $g \in G$, denn dann existiert ein $t \in Z$ mit $dt \equiv_{|G|} 1$ und g^t ist eine $d - te$ Wurzel von g.

Gilt $ggT(d, |G|) = \ell > 1$, so kann es für ein $g \in G$ keine, eine oder mehrere $d - te$ Wurzeln geben. Zunächst soll der RSA-Fall betrachtet werden, also $ggT(d, |G|) = 1$ mit $G = GL(s, Z_n)$.

RSA-Problem in $GL(s, Z_n)$:

Sei eine Matrix $A \in GL(s, Z_n)$ und eine Zahl d mit $ggT(d, |GL(s, Z_n)|) = 1$ gegeben. Finde eine Matrix $B \in GL(s, Z_n)$, so dass $B^d \equiv_n A$ gilt.

5.6.1 Satz: Ist die Ordnung $ord(A)$ einer Matrix A oder ein Vielfaches $ord(A)k$ dieser Ordnung, wie z.B. $|GL(s, Z_n)|$ bekannt, so ist das Ziehen diskreter $d - ter$ Wurzeln mit $ggT(d, ord(A)k) = 1$ mit polynomiellem Zeit- und Speicheraufwand möglich.

Beweis:

Der Beweis erfolgt ebenso wie der Beweis von Satz (4.5.1) mit $A \in GL(s, Z_n)$: Sei A eine beliebige Matrix aus $GL(s, Z_n)$ und $ord(A)k$ bekannt, so dass $ggT(d, ord(A)k) = 1$

gilt. Dann gibt es eine Zahl t mit $dt \equiv_{ord(A)k} 1$. Dann ist A^t eine $d-te$ Wurzel von A, denn es gilt $(A^t)^d \equiv_n A^{td} \equiv_n A$. □

5.6.2 Korollar: Für jede Matrix $A \in SL(s, Z_n)$ mit $P_A(X) \equiv_p \sum_{i=0}^{s}(-1)^i\binom{s}{i}x^i$ ist das Berechnen einer diskreten $d-ten$ Wurzel mit $ggT(d, n) = 1$ mit polynomiellem Zeit- und Speicheraufwand möglich.

Beweis:

Nach Satz (5.4.2) gilt $ord(A) = p$ in $SL(s, Z_p)$ und $ord(A) = q$ in $SL(s, Z_q)$ und somit $ord(A) = n$ in $SL(s, Z_n)$. Dann folgt die Behauptung aus Satz (5.6.1). □

5.6.3 Satz: Das RSA-Problem in $GL(s, Z_n)\backslash SL(s, Z_n)$ ist mindestens so schwierig wie das RSA-Problem in Z_n^*.

Beweis:

Folgt aus Satz (4.5.3), da $GL(2, Z_n)\backslash SL(2, Z_n)$ in $GL(s, Z_n)\backslash SL(s, Z_n)$ eigebettet werden kann. □

Ebenso gilt auch:

5.6.4 Satz: Das RSA-Problem in $SL(s, Z_n)$ ist mindestens so schwierig wie das RSA-Problem in Z_n^*.

Beweis:

Folgt aus Satz (4.5.4), da $SL(2, Z_n)$ in $SL(s, Z_n)$ enthalten ist. □

5.6.1 Klassifikation der Matrizen aus $SL(s, Z_n)$

Um differenzierte Aussagen über die Beziehung des RSA-Problems in $SL(s, Z_n)$ machen zu können, werden die Matrizen wieder in verschiedene Klassen unterteilt.

5.6.1.1 Definition: Klassifizierung von Matrizen aus $SL(s, Z_n)$

Sei $n = pq$, p, q Primzahlen. Die Matrizen aus $SL(s, Z_n)$ werden in folgende Klassen eingeteilt:

- **Klasse A:**

  Die Menge der Matrizen der Klasse A beinhaltet alle Matrizen $A \in SL(s, Z_n)$, so dass A mod p eine Matrix der Klasse 1 und A mod q eine Matrix der Klasse 1 ist. Es gilt also $ord(A)|\varphi(n)$.

- **Klasse B:**

  Die Menge der Matrizen der Klasse B beinhaltet alle Matrizen $A \in SL(s, Z_n)$, so dass A mod p eine Matrix der Klasse 2 und A mod q eine Matrix der Klasse 2 ist. Es gilt also $ord(A) \in \{n, 2n, 4n\}$.

- **Klasse C:**

  Die Menge der Matrizen der Klasse C beinhaltet alle Matrizen $A \in SL(s, Z_n)$, so dass genau eine der beiden Matrizen A mod p und A mod q eine Matrix der Klasse 2 oder eine Matrix der Klasse 3 ist und die andere Matrix aus keiner der beiden Klassen stammt. Es gilt also für genau eine der beiden Primzahlen p, q (oBdA p): $p|ord(A)$.

- **Klasse D**

  Die Menge der Matrizen der Klasse D beinhaltet alle Matrizen $A \in SL(s, Z_n)$, so dass mindestens eine der beiden Matrizen A mod p und A mod q eine Matrix der Klasse 3 ist.

- **Klasse E**

  Die Menge der Matrizen der Klasse E beinhaltet alle Matrizen $A \in SL(s, Z_n)$, so dass mindestens eine der beiden Matrizen A mod p und A mod q eine Matrix der Klasse 4 oder der Klasse 5 ist.

5.6.1.2 Satz: Sei $A \in SL(s, Z_n)$ eine Matrix für die gilt: $A \not\equiv_p I$, $A \not\equiv_q I$ und $ggT(ord(A), 2) = 1$. Dann liegt A in mindestens einer der angegebenen Klassen.

Beweis:

Nach Satz (5.4.1.2) liegt A mod p in genau einer der Klassen aus Definition (5.4.1.1). Ebenso liegt A mod q in genau einer der Klassen aus Definition (5.4.1.1). Durch den Chinesischen Restsatz für Matrizen (Satz (3.2.1.7)) folgt, dass A in mindestens einer der oben aufgeführten Klassen liegen muss. □

Im folgenden wird gezeigt werden, in welcher Relation das RSA-Problem in Z_n^* zu dem RSA-Problem in den einzelnen Klassen steht.

5.6.1.3 Satz: Das RSA-Problem ist für Diagonalmatrizen aus $SL(s, Z_n)$ äquivalent zum RSA-Problem in Z_n^*.

Beweis:

Folgt aus Satz (4.5.1.5), da die Diagonalmatrizen aus $SL(2, Z_n)$ eine Untergruppe der Diagonalmatrizen aus $SL(s, Z_n)$ sind. □

5.6.1.4 Korollar: Das RSA-Problem für Matrizen der Klasse A ist mindestens so schwierig wie das RSA-Problem in Z_n^*.

Beweis:

Diagonalmatrizen sind Matrizen der Klasse A, damit folgt die Behauptung aus Satz (5.6.1.3). □

5.6.1.5 Bemerkung: Der obige Satz lässt sich nicht auf alle Matrizen der Klasse A erweitern. Um den Satz anwenden zu können, müsste man die Matrizen der Klasse A zuerst diagonalisieren. Um die Eigenwerte zu bestimmen, muss man die Nullstellen eines Polynoms vom Grad s in Z_n^* lösen. Dies ist aber äquivalent zur Faktorisierung von n.

Daher ist nicht klar, ob das RSA-Problem für Matrizen der Klasse A äquivalent zu dem RSA-Problem in Z_n^* ist. Es könnte daher sein, dass das RSA-Problem für Matrizen der Klasse A schwieriger zu lösen ist, als das RSA-Problem in Z_n^*.

5.6.1.6 Satz: Das RSA-Problem ist für Matrizen der Klasse B mit polynomiellem Zeit- und Speicheraufwand lösbar.

Beweis:

Sei A eine Matrix der Klasse B, dann hat $A \bmod p$ eine Ordnung, die $2p$ teilt und $A \bmod q$ eine Ordnung, die $2q$ teilt. Es folgt, dass die Ordnung von A $4pq = 4n$ teilen muss. Nach Satz (5.6.1) ist dann die Berechnung diskreter $d - ter$ Wurzeln in polynomieller Zeit möglich. □

Es zeigt sich sogar, dass das Ziehen diskreter Wurzeln möglich ist, wenn die betrachtete Matrix modulo einer der beiden Primzahlen eine Matrix der Klasse 2 oder der Klasse 3 ist.

5.6.1.7 Satz: Das RSA-Problem ist für Matrizen der Klasse C mit polynomiellem Zeit- und Speicheraufwand lösbar.

Beweis:

Sei A eine Matrix aus einer der Klasse C, dann ist A modulo genau einer der beiden Primzahlen (oBdA p) eine Matrix der Klasse 2 oder der Klasse 3. D.h. es gilt dann A mod p hat eine Ordnung, die von p geteilt wird.

Nach Satz (5.2.2.6) gilt dann, dass $P_A(X)$ mindestens eine mehrfache Nullstelle in dem Zerfällungskörper von $P_A(X)$ über Z_p besitzt, aber in dem Zerfällungskörper von $P_A(X)$ über Z_q nur einfache Nullstellen besitzt.

Es folgt, dass $ggT(P_A(X), P'_A(X)) = 1$ in dem Zerfällungskörper über Z_q und $ggT(P_A(X), P'_A(X)) > 1$ in dem Zerfällungskörper über Z_p gilt. Dass $ggT(P_A(X), P'_A(X)) > 1$ gilt, ist klar, falls die mehrfache Nullstelle in Z_p liegt, aber auch, wenn alle mehrfache Nullstellen im Zerfällungskörper liegen, gilt $ggT(P_A(X), P'_A(X)) > 1$:

Sei $\alpha \in K_{P_A(X)} \backslash \{Z_p\}$ eine mehrfache Nullstelle von $P_A(X)$. Da Z_p ein endlicher und somit vollkommener Körper ist, ist $P_A(X) \in Z_p[x]$ reduzibel und es gibt zwei irreduzible Polynome $f_1(x); f_2(x) \in Z_p[x]$ mit $f_1(x)|P_A(X)$ und $f_2(x)|P_A(X)$ und $f_1(\alpha) \equiv_p 0 \equiv_p f_2(\alpha)$. Da $f_1(x)$ und $f_2(x)$ irreduzibel sind und α als Nullstelle besitzen, folgt $Grad(f_1(x)) = Grad(f_2(x))$. Da das Minimalpolynom von α eindeutig bestimmt ist, folgt $f_1(x) \equiv_p z \times f_2(x)$ mit $z \in Z_p$. Es folgt also $P_A(X) \equiv_p f_1(x)f_2(x)g(x) \equiv_p z \times f_2(x)^2 g(x)$ für ein geeignetes $g(x) \in Z_p[x]$. Es folgt $P'_A(X) = 2z \times f(x)f'(x)g(x) + z \times f(x)^2 g'(x)$ und somit: $z \times f(x)|ggT(P_A(X), P'_A(X))$.

Berechnet man $P'_A(X)$ mod n, so gilt $ggT(P_A(X), P'_A(X)) = 1$ in $Z_n[x]$. Da aber $ggT(P_A(X), P'_A(X)) > 1$ in $Z_p[x]$ gilt, folgt, dass für das bei der Anwendung des euklidischen Algorithmus im letzten Schritt entstandene Polynom $f(x)$ gilt: $f(x) \equiv_p 0$. In diesem Fall kann somit n faktorisiert werden, und das Berechnen diskreter Wurzeln für eine der oben aufgeführten Klassen ist mit polynomiellem Zeitaufwand möglich. □

Es ist nicht bekannt, ob das RSA-Problem in der Klasse E in einer Relation zu dem RSA-Problem in Z_n^* steht. Das RSA-Problem könnte in der Klasse sowohl schwieriger als auch leichter sein als in Z_n^*.

Es ist klar, dass nicht für alle möglichen Werte von d das RSA-Problem in Z_n^* äquivalent zum RSA-Problem in $SL(s, Z_n)$ sein kann. Dies wird auch durch den folgenden Satz noch

einmal verdeutlicht.

5.6.1.8 Satz: Seien p und q Primzahlen und sei $n = pq$. Sei A eine Matrix aus $SL(s, Z_n)$ mit $ggT(ord(A), n) = 1$. Sei d eine Zahl, die genau eine der beiden Zahlen $ord(A)$ mod p und $ord(A)$ mod q teilt. Dann ist das Ziehen einer $d-ten$ Wurzel von A äquivalent zum Faktorisieren von n.

Beweis:

Gilt $d|ord(A)$ mod p, so gibt es mehrere d-te Wurzeln. Ist das Ziehen einer $d-ten$ Wurzel aus A in polynomieller Zeit möglich, so erhält man verschiedene Wurzeln C, C' mit $C^d \equiv_n C'^n \equiv_n A$. Da $d \not| ord(A)$ mod q gilt, folgt $C \equiv_q C'$. Dann gibt es mindestens einen Eintrag in C und C', so dass $ggT(c_{ij} - c'_{ij}, n)$ ein nichttrivialer Faktor von n ist. □

Interessanterweise gibt es einen Wert für d, für den das RSA-Problem in Z_n^* äquivalent zu dem RSA-Problem in $GL(s, Z_p)$ ist.

5.6.1.9 Satz: Seien p, q zwei große Primzahlen und sei $n = pq$. Das Ziehen einer $n-ten$ Wurzel für eine beliebige Matrix $A \in GL(s, Z_p)$ mit $ggT(ord(A), n) = 1$ ist genauso schwierig wie das Berechnen von diskreten $n-ten$ Wurzeln in Z_n^*.

Beweis:

Es gilt für $A \equiv_n B^n$:

$Det(A) \equiv_n Det(B^n) \equiv_n (Det(B))^n$.

Mit anderen Worten: Ein Algorithmus, der die $n-te$ Wurzel aus A (also B) berechnen kann, berechnet immer auch gleichzeitig eine $n-te$ Wurzel von $Det(A)$. Er kann also dazu verwendet werden, diskrete $n-te$ Wurzeln in Z_n^* zu berechnen.

Ebenso kann ein Algorithmus, der $n-te$ Wurzeln in Z_n^* lösen kann, dazu verwendet werden, zu einer Matrix $A \equiv_n B^n$ die Koeffizienten von $P_B(X)$ zu berechnen.

Es gilt für jeden Koeffizienten c_j von $P_B(X)$, dass c_j^n mod n die Koeffizienten von $P_A(X)$ sind:

Seien α_i $i = 1, 2, \ldots, s$ die Nullstellen des charakteristischen Polynoms $P_B(X)$ in dem Zerfällungskörper von $P_B(X)$ über Z_p und β_i $i = 1, 2, \ldots, s$ die Nullstellen von $P_B(X)$ in dem Zerfällungskörper über Z_q. Des Weiteren seien γ_i die nach dem Chinesischen Restsatz eindeutigen Elemente in dem Ring, der durch das kartesische Produkt der beiden

Zerfällungskörper entsteht, so dass $\gamma_i \equiv_p \alpha_i$ und $\gamma_i \equiv_q \beta_i$ gilt. Dann sind α_i^n die Nullstellen von $P_A(X)$ in dem Zerfällungskörper über Z_p und β_i^n die Nullstellen von $P_A(X)$ in dem Zerfällungskörper über Z_q.

Dann gilt $c_j \equiv_n \sum_{\substack{\text{alle } s-j \text{ elementigen} \\ \text{Teilmengen J}}} \prod_{u \in J} \gamma_u$. Es folgt:

$$\begin{aligned} c_j^n &\equiv_n \left(\sum_{\substack{\text{alle } s-j \text{ elementigen} \\ \text{Teilmengen J}}} \prod_{u \in J} \gamma_u \right)^n \\ &\equiv_n \sum_{\substack{\text{alle } s-j \text{ elementigen} \\ \text{Teilmengen J}}} \left(\prod_{u \in J} \gamma_u \right)^n \\ &\equiv_n \sum_{\substack{\text{alle } s-j \text{ elementigen} \\ \text{Teilmengen J}}} \prod_{u \in J} (\gamma_u)^n \end{aligned}$$

Dies ist gleich dem $j-ten$ Koeffizienten von $P_A(X)$, da $\gamma_i^n \equiv_p \alpha_i^n$ und $\gamma_i^n \equiv_q \beta_i^n$ für $i = 1, 2, \ldots, s$ gilt.

Mit anderen Worten: Man erhält das charakteristische Polynom von B. Um daraus B zu bestimmen, kann man wie folgt vorgehen:

Zunächst konstruiert man eine Matrix $C \in GL(s, Z_n)$, die das gleiche charakteristische Polynom besitzt wie B. Dies ist nach (SM96) in polynomieller Zeit möglich. C ist mit hoher Wahrscheinlichkeit eine zu B ähnliche Matrix. Die Matrix C^d ist dann eine Matrix, die das gleiche charakteristische Polynom wie A besitzt. Diese ist mit hoher Wahrscheinlichkeit ähnlich zu A. Ist A ähnlich zu C^d, so ist es nach Satz (5.1.11) in polynomieller Zeit möglich, Matrizen $U, U^{-1} \in GL(s, Z_n)$ zu bestimmen, so dass $A \equiv_n UC^dU^{-1}$ gilt. Dann ist $B \equiv_n UCU^{-1}$. Mit anderen Worten: B ist in polynomieller Zeit aus der Kenntnis des charakteristischen Polynoms von B und d berechenbar. □

Die erfolgte Klassifizierung für Matrizen aus $SL(s, Z_n)$ soll nun wie im vorherigen Abschnitt auf Matrizen aus $GL(s, Z_n) \backslash SL(s, Z_n)$ erweitert werden.

5.6.1.10 Definition: Klassifizierung von Matrizen aus $GL(s, Z_n)\backslash SL(s, Z_n)$ Sei $n = pq$, p, q Primzahlen. Die Matrizen aus $GL(s, Z_n)\backslash SL(s, Z_n)$ werden in folgende Klassen eingeteilt:

- **Klasse F:**

  Die Menge der Matrizen der Klasse F beinhaltet alle Matrizen $A \in GL(s, Z_n)\backslash SL(s, Z_n)$, so dass für eine der beiden Primzahlen (oBdA p) $A \bmod p \in SL(s, Z_p)$ gilt und $A \bmod q \in GL(s, Z_q)\backslash SL(s, Z_q)$ gilt.

- **Klasse G:**

  Die Menge der Matrizen der Klasse G beinhaltet alle Matrizen $A \in GL(s, Z_n)\backslash SL(s, Z_n)$, so dass $A \bmod p$ eine Matrix der Klasse 6 und $A \bmod q$ eine Matrix der Klasse 6 ist. Es gilt also $ord(A)|p - 1$.

- **Klasse H:**

  Die Menge der Matrizen der Klasse H beinhaltet alle Matrizen $A \in GL(s, Z_n)\backslash SL(s, Z_n)$, so dass für eine der beiden Primzahlen p, q (oBdA p) $p|ord(A)$ gilt.

- **Klasse I:**

  Die Menge der Matrizen der Klasse I beinhaltet alle Matrizen $A \in GL(s, Z_n)\backslash SL(s, Z_n)$, so dass $n|ord(A)$ gilt.

- **Klasse J:**

  Die Menge der Matrizen der Klasse J Matrizen beinhaltet alle Matrizen $A \in GL(s, Z_n)\backslash SL(s, Z_n)$, so dass mindestens eine der beiden Matrizen $A \bmod p$ und $A \bmod q$ eine Matrix der Klasse 8 oder der Klasse 9 ist.

5.6.1.11 Satz: Jede Matrix $A \in GL(s, Z_n)\backslash SL(s, Z_n)$ liegt in mindestens einer der angegebenen Klassen.

Beweis:

Sei A eine Matrix aus $GL(s, Z_n)\backslash SL(s, Z_n)$. Gilt für eine der beiden Primzahlen p oder q (oBdA p), dass $A \bmod p \in SL(s, Z_p)$ liegt, so ist A eine Matrix der Klasse F.

Also sei A keine Matrix der Klasse F. Nach Satz (5.5.1.4) liegt $A \bmod p$ in mindestens einer der Klassen aus Definition (5.5.1.3), falls $A \bmod p \notin SL(s, Z_p)$. Ebenso liegt $A \bmod q$

in mindestens einer der Klassen aus Definition (5.5.1.3), falls $A \bmod q \notin SL(s, Z_q)$. Durch den Chinesischen Restsatz für Matrizen (Satz (3.2.1.7)) folgt, dass A in mindestens einer der oben aufgeführten Klassen liegen muss, denn ist A modulo einer der beiden Primzahlen eine Matrix der Klasse 7, dann liegt $A \bmod n$ in der Klasse H oder I. Liegt A modulo einer der beiden Primzahlen in einer der Klassen 8 oder 9, so ist $A \bmod n$ eine Matrix der Klasse J. □

Nach Satz (5.6.3) ist das RSA-Problem in $GL(s, Z_n) \backslash SL(s, Z_n)$ mindestens so schwierig wie in Z_n^*. Nach der obigen Klasseneinteilung kann nun eine Aussage getroffen werden, für welche Klassen das RSA-Problem in $GL(s, Z_n) \backslash SL(s, Z_n)$ mit polynomiellem Zeit- und Speicheraufwand zu lösen ist.

5.6.1.12 Satz: Das RSA-Problem ist für Matrizen der Klassen F und H mit polynomiellem Zeit- und Speicheraufwand lösbar.

Beweis:

Das RSA-Problem ist mit polynomiellem Zeit- und Speicheraufwand zu lösen, wenn die Ordnung der Gruppe $GL(s, Z_n)$ oder die Ordnung der Matrix, zu der die diskrete Wurzel berechnet werden soll, bekannt ist. Die Ordnung von $GL(s, Z_n)$ kann berechnet werden, wenn man die Primfaktoren p und q der Zahl n kennt.

Sei A eine Matrix der Klasse F, dann gilt entweder $A \in SL(s, Z_p)$ oder $A \in SL(s, Z_q)$, aber $A \notin SL(s, Z_n)$. OBdA sei $A \in SL(s, Z_p)$ und $A \notin SL(s, Z_q)$. Dann gilt $Det(A) \equiv_p 1$ und $Det(A) \not\equiv_q 1$. Es folgt, dass $ggT(Det(A) - 1, n) = p$ gilt. Somit erhält man einen nichttrivialen Faktor von n und kann n faktorisieren. Dann ist auch das RSA-Problem mit polynomiellem Zeit- und Speicheraufwand lösbar.

Sei A eine Matrix der Klasse H. Dann gilt für genau eine der beiden Primzahlen p und q (oBdA p), dass $A \bmod p$ eine Matrix der Klasse 7 in $GL(s, Z_p)$ ist. Nach Satz (5.2.2.6) gilt dann, dass $P_A(X)$ mindestens eine mehrfache Nullstelle in dem Zerfällungskörper von $P_A(X)$ über Z_p besitzt, aber in dem Zerfällungskörper von $P_A(X)$ über Z_q nur einfache Nullstellen besitzt.

Es folgt, dass $ggT(P_A(X), P'_A(X)) = 1$ in dem Zerfällungskörper über Z_q und $ggT(P_A(X), P'_A(X)) > 1$ in dem Zerfällungskörper über Z_p gilt. Das $ggT(P_A(X), P'_A(X)) > 1$ gilt, ist klar, falls die mehrfache Nullstelle in Z_p liegt, aber auch dann, wenn alle mehrfachen Nullstellen im Zerfällungskörper liegen, gilt $ggT(P_A(X), P'_A(X)) > 1$:

Sei $\alpha \in K_{P_A(X)} \backslash \{Z_p\}$ eine mehrfache Nullstelle von $P_A(X)$. Da Z_p ein endlicher und somit vollkommener Körper ist, ist $P_A(X) \in Z_p[x]$ reduzibel und es gibt zwei irreduzible Polynome $f_1(x); f_2(x) \in Z_p[x]$ mit $f_1(x)|P_A(X)$ und $f_2(x)|P_A(X)$ und $f_1(\alpha) \equiv_p 0 \equiv_p f_2(\alpha)$. Da $f_1(x)$ und $f_2(x)$ irreduzibel sind und α als Nullstelle besitzen, folgt $Grad(f_1(x)) = Grad(f_2(x))$. Da das Minimalpolynom von α eindeutig bestimmt ist, folgt $f_1(x) \equiv_p z \cdot f_2(x)$ mit $z \in Z_p$. Es folgt also $P_A(X) \equiv_p f_1(x)f_2(x)g(x) \equiv_p z \cdot f_2(x)^2 g(x)$ für ein geeignetes $g(x) \in Z_p[x]$. Es folgt $P'_A(X) = 2z \cdot f(x)f'(x)g(x) + z \cdot f(x)^2 g'(x)$ und somit $z \cdot f(x)|ggT(P_A(X), P'_A(X))$.

Berechnet man $P'_A(X)$ mod n, so gilt $ggT(P_A(X), P'_A(X)) = 1$ in $Z_n[x]$. Da aber $ggT(P_A(X), P'_A(X) > 1$ in $Z_p[x]$ gilt, folgt, dass für das bei der Anwendung des euklidischen Algorithmus im letzten Schritt entstandene Polynom $f(x)$ gilt: $f(x) \equiv_p 0$. In diesem Fall kann somit n faktorisiert werden, und das Berechnen diskreter Wurzeln für eine der oben aufgeführten Klassen ist mit polynomiellem Zeitaufwand möglich. □

5.7 Diskrete Wurzeln in $SL(s, Z_n)$ bzw. $GL(s, Z_n)$ und Faktorisierung

In diesem Abschnitt wird der Zusammenhang zwischen diskreten Wurzeln von Matrizen über Z_n und der Faktorisierung von n erläutert. Dabei sind insbesondere $d - te$ diskrete Wurzeln zu betrachten, wobei $ggT(d, |SL(s, Z_n)|) = \ell > 1$ gilt.

5.7.1 $d - te$ Wurzeln in $SL(s, Z_n)$ und $GL(s, Z_n)$

Der folgende Abschnitt beschäftigt sich mit d-ten Wurzeln in den Gruppen $SL(s, Z_n)$ und $GL(s, Z_n)$ ($n = pq$, p, q Primzahlen). Aus den Abschnitten 4.5.3 und 4.5.3 ist bereits bekannt, dass ein Algorithmus, der Quadratwurzeln oder kubische Wurzeln in $SL(2, Z_n)$ berechnet, zur Faktorisierung von n verwendet werden kann. Da $SL(2, Z_n)$ eine Untergruppe von $SL(s, Z_n)$ ist, gilt die Aussage auch für Algorithmen, die Quadratwurzeln in $SL(s, Z_n)$ berechnen können. Hier wird diese Aussage dahingehend erweitert, dass ein Algorithmus, der k-te Wurzeln (wobei $k|ord(A)$ gilt) aus einer Matrix $A^k \in GL(s, Z_n)$ zu berechnen vermag, dazu verwendet werden kann, n zu faktorisieren.

5.7.1.1 Satz: Es seien p, q Primzahlen, so dass $n = pq$ gilt. Seien k und s natürliche Zahlen logarithmischer Länge von n, mit $k| \, |GL(s, Z_n)|$ und $k \neq n$. Sei B eine Matrix aus $GL(s, Z_n)$ mit $k|ord(B)$, dann gilt: Ein Algorithmus, der zu der Matrix $A := B^k \bmod n$ eine k-te Wurzeln $C \not\equiv_n B$ in polynomieller Zeit zu berechnen vermag, kann dazu verwendet werden, n in polynomieller Zeit zu faktorisieren.

Beweis:

OBdA kann angenommen werden, dass $n \not| ord(B)$ gilt. Dies kann sichergestellt werden, indem man eine zufällige Matrix $D \in GL(s, Z_n)$ wählt und $B := D^n \bmod n$ berechnet.

Ebenso kann oBdA angenommen werden, dass für die beiden Primzahlen p, q gilt $p \not| ord(B)$ und $q \not| ord(B)$. Wäre dies nicht der Fall, so wäre nach Satz (5.6.1.12) die Faktorisierung von n in polynomieller Zeit möglich.

Angenommen, B und C besitzen das gleiche charakteristische Polynom, so haben $P_B(X)$ und $P_C(X)$ in den Zerfällungskörpern über Z_p und Z_q die gleichen Nullstellen.

Im folgenden werden die Matrizen $B \bmod p$ und $C \bmod p$ betrachtet. Da $P_C(X) \equiv_p P_B(X)$ gilt, haben die Polynome in dem Zerfällungskörper von $P_C(X)$ die gleichen Nullstellen $\alpha_i \quad i = 1, 2, \ldots, s$.

Da $p \not| ord(B)$ gilt, hat $P_B(X)$ paarweise verschiedene Nullstellen im Zerfällungskörper $K_{P_B(X)}$. Dann ist B in der Gruppe $GL(s, K_{P_B(X)})$ diagonalisierbar. Sei $B' := gBg^{-1}$ die zu B ähnliche Diagonalmatrix. Dann ist gAg^{-1} ebenfalls eine Diagonalmatrix, und nach Korollar (5.1.9) folgt, dass dann gCg^{-1} ebenfalls eine Diagonalmatrix ist. Da $P_B(X)$ paarweise verschiedene Nullstellen besitzt, gilt für alle Nullstellen α_i von $P_B(X)$ bzw. $P_C(X)$: $\alpha_i^k \not\equiv_p \alpha_j$ für $\forall i, j \in \{1, 2, \ldots, s\}$. Somit folgt auch $gBg^{-1} \equiv_p gCg^{-1}$ und somit $B \equiv_p C$. Da die gleiche Argumentation auch für die Zerfällungskörper über Z_q gilt, folgt $B \equiv_q C$. Dies ist aber ein Widerspruch zu der obigen Voraussetzung, dass $B \not\equiv_n C$ gilt.

Im Folgenden wird gezeigt, wie hoch die Wahrscheinlichkeit ist, dass $ggT(P_B(X), P_C(X)) \equiv_p 1$ gilt. Zunächst werden die Nullstellen der beiden Polynome über dem jeweiligen Zerfällungskörper über Z_p betrachtet.

Seien $\beta_i \quad i = 1, 2, \ldots, s$ die Nullstellen von $P_B(X)$ in dem Zerfällungskörper von $P_B(X)$ über Z_p und seien $\gamma_i \quad i = 1, 2, \ldots, s$ die Nullstellen von $P_C(X)$ in dem Zerfällungskörper von $P_C(X)$ über Z_p. Da $B^k \equiv_n C^k$ gilt, folgt mit einer geeigneten Indizierung in dem Erweiterungskörper von Z_p, der alle Nullstellen von $P_B(X)$ und $P_C(X)$ enthält:

$\beta_i^k = \gamma_i^k \quad i = 1, 2, \ldots, s$

Da es in jedem Körper maximal k verschiedene k-te Wurzeln gibt, gilt $\beta_i \neq \gamma_i$ mit einer Wahrscheinlichkeit von jeweils $\frac{k-1}{k}$. Mit einer Wahrscheinlichkeit von $\left(\frac{k-1}{k}\right)^s$ haben $P_B(X)$ und $P_C(X)$ keine gemeinsamen Nullstellen.

Es folgt: $\exists i \in \{1, 2, \ldots, s\} : \beta_i = \gamma_i$ mit einer Wahrscheinlichkeit:

$$P \geq 1 - \left(\frac{k-1}{k}\right)^s \geq \frac{1}{k}$$

In diesem Fall gilt $ggT(P_B(X), P_C(X)) \not\equiv_p 1$.

Die gleichen Wahrscheinlichkeiten gelten für die Polynome über den Zerfällungskörpern über Z_q. Daher gilt für die Wahrscheinlichkeit, dass $ggT(P_B(X), P_C(X)) \equiv_p 1$ und $ggT(P_B(X), P_C(X)) \not\equiv_q 1$ gilt:

$$P \geq \frac{1}{k}\left(\frac{k-1}{k}\right)^s$$

In diesem Fall ist $ggT(ggT(P_B(X), P_C(X)) - 1, n)$ ein irreduzibler Faktor von n. Da k und s logarithmisch in der Länge von p sind, ist der Algorithmus in polynomieller Zeit erfolgreich. □

5.7.2 Faktorisierung von n mittels Matrizen aus $SL(s, Z_n)$

Wie im Falle der 2×2 Matrizen kann ein weiteres Verfahren beschrieben werden, wie man mit Hilfe von Matrizen aus $SL(s, Z_n)$ die Zahl n faktorisieren kann, wenn für eine der beiden Primfaktoren p bzw. q (im folgenden oBdA p) gilt, dass $\sum_{i=0}^{s-1} p^i$ nur durch kleine Primfaktoren teilbar ist. Dabei ist s logarithmisch im Vergleich zu n.

Im folgenden sei angenommen, dass oBdA $\sum_{i=0}^{s-1} p^i$ nur durch Primfaktoren geteilt wird, die kleiner als eine kleine Schranke S sind.

Zunächst wird nun eine Zahl k berechnet, für die gilt, dass sie von $\sum_{i=0}^{s-1} p^i$ geteilt wird. Zum Beispiel kann $k := S!$ oder $k := \prod_{p_i \in P; p_i < S} p_i^{f_i}$ mit $f_i = \lfloor log_{p_i} S \rfloor$ gewählt werden. Dann wählt man zufällig eine Matrix $A \in SL(s, Z_n)$ und berechnet $B := A^k \bmod n$.

Da A zufällig gewählt wurde, ist auch $P_A(X)$ ein zufälliges Polynom aus $Z_n[x]$ vom Grad s. Die Wahrscheinlichkeit, dass ein Polynom vom Grad s in dem Polynomring eines

endlichen Körpers irreduzibel ist, kann nach (FGP96) mit $\frac{1}{s}$ abgeschätzt werden. Mit anderen Worten: Mit einer Wahrscheinlichkeit von ca. $\frac{1}{s}$ ist $P_A(X)$ mod p irreduzibel. Dann gilt nach Korollar (5.3.2.3) $ord(A \bmod p) | \sum_{i=0}^{s-1} p^i$ in $SL(s, Z_p)$.

Da $\sum_{i=0}^{s-1} p^i | k$ gilt, folgt $B \equiv_p I$ mit Wahrscheinlichkeit ca. $\frac{1}{s}$. Mit einer hohen Wahrscheinlichkeit gilt $ord(A \bmod q) \not| k$, und somit $B \not\equiv_q I$. Dann ist $ggT(b_{11} - 1, n)$ ein nichttrivialer Faktor von n. □

5.8 Sicherheit des RSA-Verfahrens auf der Gruppe $GL(s, Z_n)$

Ebenso wie bei dem originären RSA-Verfahren steht die Sicherheit des Verfahrens in engem Zusammenhang mit der Wahl der Parameter. Alle in Abschnitt 2.3 beschriebenen Angriffe sind auf die beiden oben beschriebenen Erweiterungen des RSA direkt übertragbar, wenn (wie es der Vorschlag der Autoren vorsieht) nur Dreiecksmatrizen verwendet werden.

Lediglich die Aussage aus Abschnitt 2.3.8, dass RSA-Signaturen universell fälschbar unter einem Angriff mit gewählten Signaturen sind, lässt sich nicht direkt auf Dreiecksmatrizen übertragen. Im Allgemeinen gilt auch für Dreiecksmatrizen $A, B \in GL(s, Z_n)$ nicht $AB \equiv_n BA$.

Dennoch ist es auch bei dem RSA-Verfahren, das auf $GL(s, Z_n)$ operiert, möglich, Signaturen universell zu fälschen. Die universelle Fälschbarkeit von RSA-Signaturen lässt sich sogar durch die Verwendung von nicht-abelschen Gruppen gar nicht verhindern, wie der folgenden Satz beweist.

5.8.1 Satz: Sei G eine beliebige nicht abelsche Gruppe, auf der das RSA-Verfahren operiert. Dann gilt: Das RSA-Verfahren ist universell fälschbar unter einem Angriff mit gewählten Signaturen.

Beweis:

Bei einem Angriff mit gewählten Signaturen besitzt der Angreifer außer dem öffentlichen Schlüssel (e, n) des RSA-Signaturschlüsselpaares die Möglichkeit, sich beliebige Nachrichten signieren zu lassen (natürlich darf sich die Nachricht, zu der er eine Signatur fälschen will,

nicht unter diesen Nachrichten befinden). Um eine Signatur zu einer beliebigen Nachricht m zu fälschen, wählt er zufällig ein $g \in G$. Dann berechnet er in G: $m' := gmg^{-1}$. Zu der Nachricht m' lässt er sich dann eine gültige Signatur erzeugen.

Es gilt in G:

$$Sig(m') = (gmg^{-1})^d = gm^d g^{-1}$$

Somit ist $g^{-1}Sig(m')g = m^d$ eine gültige Signatur auf m. □

Aus den gewonnenen Erkenntnissen können die folgenden Schlüsse für das RSA-Verfahren auf der Gruppe $GL(s, Z_n)$ gezogen werden:

1. Damit die Sicherheit des RSA-Verfahrens auf $GL(s, Z_n)$ gewährleistet ist, müssen die Sicherheitsanforderungen an die Parameter aus Abschnitt 2.4 erfüllt sein.

2. Es gibt Matrizen in $GL(s, Z_n)$, für die das RSA-Problem effizient lösbar ist.

3. Wählt man die zu verschlüsselnde Matrix zufällig aus der Gruppe $GL(s, Z_n)$, dann ist die Wahrscheinlichkeit, dass das RSA-Problem für diese Matrix in polynomieller Zeit lösbar ist, vernachlässigbar.

4. Es gibt Matrizen in $SL(s, Z_p)$, für die nicht entschieden werden kann, ob das RSA-Problem schwieriger oder leichter ist, als in der Gruppe Z_n^*.

5. Wählt man die zu verschlüsselnde Matrix zufällig aus der Gruppe $GL(s, Z_n)$, so ist das RSA-Problem für diese Matrix mit hoher Wahrscheinlichkeit mindestens so schwierig wie das RSA-Problem in der Gruppe Z_n^*.

6. Es ergibt sich eine neue Sicherheitsanforderung an die Primzahlen, die in einem RSA-basierten Verfahren eingesetzt werden sollen:

   Neue Anforderung an die Primzahlen p und q:

> Damit die Zahl $n = pq$ nicht in polynomieller Zeit mit dem oben beschriebenen Verfahren faktorisiert werden kann, müssen die beiden Primzahlen p und q die folgende Eigenschaft besitzen: Für kleine Werte von s ($s < log_2 p$) sollten die Zahlen $\sum_{i=0}^{s-1} p^i$ und $\sum_{i=0}^{s-1} q^i$ nicht ausschließlich kleine Primteiler besitzen.

Mit anderen Worten: Wendet man das RSA-Verfahren auf zufällige Matrizen aus $GL(s, Z_n)$ an, so ist die Sicherheit des Verfahrens mindestens so hoch wie das RSA-Verfahren in der Gruppe Z_n^*. Es ist sogar möglich, dass das RSA-Verfahren auf der Gruppe $GL(s, Z_n)$ eine höhere Sicherheit bietet: Es wurde keine Möglichkeit gefunden, wie ein Algorithmus, der das RSA-Verfahren in Z_p^* bricht, genutzt werden könnte, um das allgemeine RSA-Verfahren in $GL(s, Z_p)$ zu lösen.

Kapitel 6

Zusammenfassung und Ausblick

In dieser Arbeit wurde die Sicherheit des RSA-Verfahrens analysiert, das auf der Gruppe $GL(s, Z_n)$ operiert. Dazu wurde zunächst das diskrete Logarithmusproblem in den Gruppen $SL(s, Z_p)$ und $GL(s, Z_p)\backslash SL(s, Z_p)$ untersucht.

Ein wesentlicher Bestandteil dieser Untersuchung ist die Unterteilung der Matrizen aus $GL(s, Z_p)$ in verschiedene Klassen, für die differenzierte Aussagen über die Schwierigkeit des diskreten Logarithmusproblems getroffen werden konnten. Es konnte gezeigt werden, dass für einen Großteil der Matrizen das diskrete Logarithmusproblem mindestens so schwierig ist wie in der Gruppe Z_p^*. Eine genaue Aussage darüber, für welche Klassen das Problem äquivalent zu dem Problem in Z_p^* ist, konnte ebenfalls getroffen werden. Darüber hinaus wurde gezeigt, dass es sowohl Klassen von Matrizen gibt, für die das diskrete Logarithmusproblem in polynomieller Zeit lösbar ist, als auch Klassen von Matrizen, für die das diskrete Logarithmusproblem in keinem direktem Zusammenhang mit dem diskreten Logarithmusproblem zu stehen scheint.

Zur Untersuchung des RSA-Verfahrens in der Gruppe $SL(s, Z_n)$ und der Gruppe $GL(s, Z_n)\backslash SL(s, Z_n)$ wurde die Klassifikation der Matrizen auf den Fall $n = pq$ erweitert. Auch in diesem Fall konnte gezeigt werden, dass für den Großteil der Matrizen das RSA-Verfahren mindestens so sicher ist wie das RSA-Verfahren in Z_n^*. Ebenso konnte auch hier gezeigt werden, dass Klassen von Matrizen existieren, für die das RSA-Problem in polynomieller Zeit lösbar ist. Diese Klassen besitzen jedoch eine kleine Mächtigkeit, so dass die Wahrscheinlichkeit, dass das RSA-Problem für eine zufällig gewählte Matrix in polynomi-

eller Zeit lösbar ist, vernachlässigbar klein ist. Wie bei dem diskreten Logarithmusproblem gibt es auch bei dem RSA-Problem Klassen von Matrizen, für die das RSA-Problem in keinem direktem Zusammenhang mit dem RSA-Problem in Z_n^* zu stehen scheint. Lediglich für den Exponenten n selbst konnte gezeigt werden, dass die Probleme für Matrizen und in Z_n^* äquivalent sind. Im Gegensatz dazu gibt es auch Exponenten, für die gezeigt werden konnte, dass das RSA-Problem zu diesem Exponenten für bestimmte Matrizen äquivalent zur Faktorisierung des Moduls ist. Dies legt die Vermutung nahe, dass das RSA-Problem in $GL(s, Z_n)$ genau dann äquivalent zu dem RSA-Problem in Z_n^* ist, wenn für den Exponenten e gilt: $ggT(e, \varphi(n)) = ggT(e, |GL(s, Z_n)|) = 1$

Aus der Analyse der Gruppen $SL(s, Z_n)$ und $GL(s, Z_n) \backslash SL(s, Z_n)$ konnte eine neue Forderung an Primzahlen abgeleitet werden, die in einem RSA-Verfahren eingesetzt werden sollen. Diese resultiert aus einer Verallgemeinerung der Faktorisierungsalgorithmen, die ausnutzen, dass für genau eine der beiden Primzahlen p, q (oBdA p) gilt, dass $p-1$ oder $p+1$ nur kleine Primteiler besitzt. Diese beiden bisher bekannten Algorithmen konnten dahingehend erweitert werden, dass für die Primzahl p gilt, dass $\sum_{i=0}^{s} p^i$ nur kleine Primteiler besitzt. Dabei ist s eine natürliche Zahl, deren Größe logarithmisch zu p ist.

Diese Arbeit kann als Ausgangspunkt für weitergehende Forschungsarbeiten dienen. Interessante Fragestellungen, die zum Beispiel die Effizienz der kryptographischen Verfahren betreffen, wurden in dieser Arbeit nicht betrachtet, da sie den Rahmen der Untersuchung gesprengt hätten. So ist z.B. denkbar, dass in einigen Klassen von Matrizen effizientere Algorithmen zur Potenzierung der Matrizen existieren als in anderen Klassen. Dies wird umso relevanter, je größer die Dimension s gewählt wird. Ebenso sollte der neu entwickelte Faktorisierungsalgorithmus näher untersucht werden. Es ist der Frage nachzugehen, für welche Werte s der Algorithmus praktikabel ist. Die Laufzeit des Faktorisierungsalgorithmus steigt mit der Größe von s, gleichzeitig sinkt die Wahrscheinlichkeit, dass die Zahl $\sum_{i=0}^{s} p^i$ nur kleine Primteiler besitzt. Bisher wurde der entworfene Algorithmus noch nicht implementiert. Interessant wird nicht zuletzt auch die Antwort auf die Frage sein, welche derzeit verwendeten RSA-Schlüssel durch den neuen Algorithmus gebrochen werden können.

Anhang

Notationen

p, q	p und q bezeichnen jeweils eine ungerade Primzahl.
n	Zusammengesetzte natürliche Zahl. Im Allgemeinen gilt innerhalb dieser Arbeit $n = pq$.
Z_n	Menge der Restklassen modulo n.
Z_n^*	Menge der Zahlen $a \in Z_n$ mit $ggT(a, n) = 1$. Diese bildet zusammen mit der modularen Multiplikation eine Gruppe.
$\varphi(n)$	Ordnung der multiplikativen Gruppe Z_n^*.
$\equiv_n$	Es gilt $a \equiv_n b$ genau dann, wenn $n \mid a - b$ gilt.
e	Natürliche Zahl, die als öffentlicher RSA-Exponent verwendet wird.
d	Natürliche Zahl, die als geheimer RSA-Exponent verwendet wird. Es gilt $ed \equiv_{\varphi(n)} 1$.
m	Natürliche Zahl, die als Nachricht bezeichnet wird.
c	Natürliche Zahl, die als der Chiffretext bezeichnet wird.
r	Zufällig gewählte natürliche Zahl.
i, j, k	Natürliche Zahlen, die als Indizes verwendet werden.
$\alpha_i, \beta_i, \gamma_i$	Nullstellen eines Polynoms.
$h(m)$	Hashwert der Nachricht m.

$GL(s, Z_n)$	Generalisierte Lineare Gruppe der Dimension s über Z_n. Diese besteht aus allen $s \times s$-Matrizen mit Einträgen aus Z_n, deren Determinante teilerfremd zu n ist.
$SL(s, Z_n)$	Spezielle Lineare Gruppe der Dimension s über Z_n. Diese besteht aus allen $s \times s$-Matrizen mit Einträgen aus Z_n, deren Determinante modulo n den Wert 1 annimmt.
A, B, C	Matrizen aus der Menge $GL(s, Z_n)$ oder $SL(s, Z_n)$.
I	Einheitsmatrix.
$< A >$	Menge aller Matrizen, die in dem Erzeugnis von A liegen, also Potenzen von A sind.
$Det(A)$	Determinante der Matrix A.
$Spur(A)$	Spur der Matrix A.
a_{ij}	Eintrag in der i-ten Zeile und j-ten Spalte der Matrix A.
$a_{ij}^{(k)}$	Eintrag in der i-ten Zeile und j-ten Spalte der Matrix A^k.
$\square$	Kennzeichnet das Ende eines Beweises.

Beispiel einer großen faktorisierbaren Zahl

Im Folgenden soll eine Zahl mit Binärlänge 80 angegeben werden, die mit dem neuen Verfahren zur Faktorisierung faktorisiert werden kann. Es gilt:

$$1093027772825687045118713 \quad = \quad 1054578991787 \cdot 1036458891499$$

Dabei ist 1036458891499 eine Primzahl, für die gilt:

$$1036458891499^2 + 1036458891499 + 1 \quad = \quad 3 \cdot 43 \cdot 607 \cdot 4051 \cdot 27901 \cdot 174829$$

Literaturverzeichnis

[BR96] M. Bellare, P. Rogaway, *The exact security of digital signatures. How to sign with RSA and Rabin*, in: Eurocrypt 96, Springer-Verlag, 1996, S. 399-416.

[Be67] E.R. Berlekamp, *Factoring polynomials over finite fields*, in: Bell System Technical Journal, Bell Laboratories, 1967, S. 1853-1859.

[Beu94] A. Beutelspacher, *Lineare Algebra*, Vieweg-Verlag, 1994.

[BSW95] A. Beutelspacher, J. Schwenk, K.-D. Wolfenstetter, *Moderne Verfahren der Kryptographie*, Vieweg-Verlag, 1995.

[BV98] D. Boneh, R. Venkatesan *Breaking RSA may not be equivalent to factoring*, in: Eurocrypt '98, Springer-Verlag, 1998, S. 59-71.

[CD90] C-C.Chuang, J.G. Dunham, *Matrix Extension of the RSA Algorithm*, in: Crypto '90 , Springer-Verlag, 1990, S. 140-151.

[Co97] D. Coppersmith, *Small sollutions to polynomial equations and low exponent RSA vulnerabilities*, in: Journal of Cryptology, Springer-Verlag, 1997, S. 233-260.

[De90] L.Y. Deng, *Elements of maximum order in a matrix group*, in: Problems and Solutions of SIAM Review, Vol. 32, No. 3, SIAM-Verlag, 1990, S. 479.

[DH76] W. Diffie, M. Hellman, *New Directions in Cryptography*, in: IEEE Transactions on Information Theory, Vol. 6, IEEE Computer Society, 1976, S. 644-654.

[Fa96] H. Farroukh, *Entwicklung und Untersuchung von Public-Key-Algorithmen auf der Basis der Potenzfunktion in algebraischen Strukturen*, Dissertation Gießen, 1996.

[FIPS64-2] U.S. Department of Commerce, *Data Encryption Standard (DES)*, FIPS PUB 46-1, 1988.

[FGP96] P. Flajolet, X. Gourdon, D. Panario, *Random Polynomials and Polynomial Factorization*, in: Proc. of the 23rd International Colloquium on Automata, Languages and Programming, Springer-Verlag, 1996, S. 1-9.

[GMR88] S. Goldwasser, S. Micali, R. Rivest, *A digital signature scheme secure against adaptive chosen message attack*, in: SIAM Journal of Computung, Vol.17, SIAM-Verlag, 1988, S. 281-308.

[HW75] G.H. Hardy, E.M. Wright, *An Introduction to the Theory of numbers*, in: Oxford Clarendon Press 1975 Theory, Oxford Clarendon Press, 1975, S. 469-472.

[Ha88] J. Hastad, *Solving simultaneous modular equations of low degree*, in: SIAM Journal of Computing, Vol. 17, SIAM-Verlag, 1988, S. 336-341.

[Hora94] A.F. Horadam, *Extension of a synthesis for a class of polynomial sequences*, in: Fibonacci Quarterly, Fibonacci Association, 1994, S. 68-74.

[Hora96] A.F. Horadam, *A Synthesis of Certain Polynomial Sequences*, in: Applications of Fibonacci Numbers, Vol. 6, Kluwer Academic Publishers, 1996, S. 74-75.

[Hu83] B. Huppert, *Endliche Gruppen I*, Springer Verlag, 1983.

[Ku91] E. Kunz, *Algebra*, Vieweg-Verlag, 1991.

[Lem30] D.H. Lehmer, *An extended theory of Lucas Functions*, in: Annals of Mathematics, Princeton University, 1930, S. 419-448.

[LL93] A. Lenstra, H.W. Lenstra, *The Development of the Number Field Sieve*, in: Lecture Notes of Mathematics, Vol. 1554, Springer-Verlag, 1993, S. 4-10.

[Pe92] R. Peralta,*On the distribution of quadratic residues and non-residues modulo a prime number*, in: Mathematics of Computations, Vol. 58, American Mathematical Society, 1992, S. 433-440.

[Pol74] J.M. Pollard, *Theorems on factorization and primality testing*, in: Proceedings of the Cambridge Philosophical Society, Vol. 76, Springer-Verlag, 1974, S. 521-528.

[RSA79] L.R. Rivest, A. Shamir, L. Adleman, *A method for obtaining digital signatures and public key cryptosystems*, in: Communications of the ACM, Association for Computing Machinery, 1978, S. 120-126.

[Ro96] D.J.S. Robinson, *A course in the theory of groups*, Springer-Verlag, 1996.

[SM96] B. De Schutter, B. De Moor, *A method to find all solutions of a system of multivariate polynomial equalities and inequalities in the max algebra*, in: Discrete Event Dynamic Systems Theory and Applications, Vol. 6, Springer-Verlag, 1996, S. 115-138.

[VO85] V.Varadharajan, R. Odoni, *Extension of RSA cryptosystems to matrix rings*, in: Cryptologia, Vol. 9, Springer-Verlag, 1985, S. 140-153,.

[Wi90] M.Wiener, *Cryptanalysis of short RSA secret exponents*, in: IEEE Transactions on Information Theory, Vol. 36, IEEE Information Theory Society, 1990, S.553-558.

[Wil82] H.C. Williams, *A p+1 Method of Factoring*, in: Mathematics of Computations, Vol. 39, American Mathematical Society, 1982, S. 225-234.