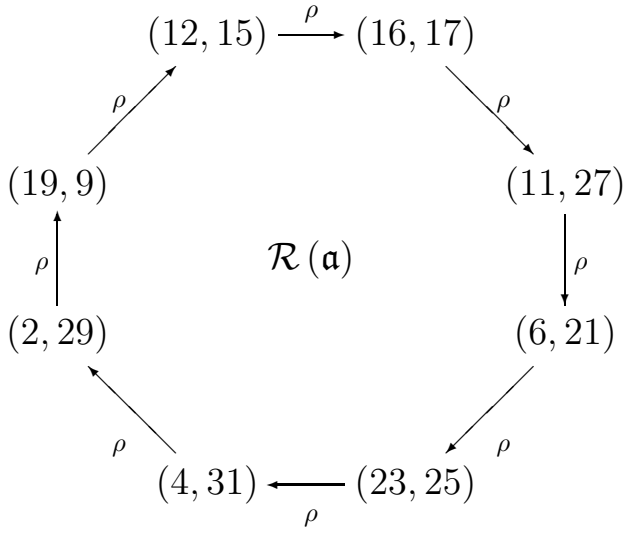
Realisierung der ElGamal-Verschlüsselung in quadratischen Zahlkörpern

Diplomarbeit von
Daniel Schielzeth



Angefertigt am Institut für Mathematik der
Technischen Universität Berlin
April 2003

Danksagung

Ich möchte mich an dieser Stelle bei Prof. Pohst für seine Hilfe bei der Auswahl des Themas und seine Betreuung bedanken. Weiterhin danke ich Detlef Hühnlein für seine hilfreichen Tips und Anregungen und Claus Fieker für seine Hilfe beim Umgang mit KASH. Ich danke Andreas Schöpp und Sebastian Freundt für das Korrekturlesen und deren Hinweise und Vorschläge zur Gestaltung der Arbeit. Vor allem aber möchte ich mich bei meinen Eltern bedanken, die mich immer bedingungslos unterstützt und gefördert haben.

Inhaltsverzeichnis

Symbolverzeichnis

Grundlagen

$\mathbb{N}$	Menge der natürlichen Zahlen $= \{1, 2, 3, \ldots\}$
$\mathbb{P}$	Menge der Primzahlen
$\mathbb{Z}$	Menge der ganzen Zahlen
$\mathbb{Q}$	Menge der gebrochenen Zahlen
$\mathbb{R}$	Menge der reellen Zahlen
$\mathbb{M}^+$	$\{m \in \mathbb{M} \mid m > 0\} \quad \forall\, \mathbb{M} \in \{\mathbb{Z}, \mathbb{Q}, \mathbb{R}\}$
$\sharp M$	Anzahl der Elemente der Menge M
sign	Vorzeichenfunktion
$\dot{\exists}\, x \in M$	Es existiert ein eindeutiges $x \in M$
n, k	Natürliche Zahlen
$\exp(x)$	Exponentialfunktion ($\exp(x) = e^x$)
$\ln(x)$	Natürlicher Logarithmus
$\log_b(x)$	$= \frac{\ln(x)}{\ln(b)}$ (Logarithmus zur Basis b)
$\mathcal{O}(f)$	Größenordnung von f ($\mathcal{O}$-Notation) 2
$o(f)$	o-Notation 2
$L_x[u, v]$	$= \exp\left((v + o(1))(\ln x)^u (\ln \ln x)^{1-u}\right)$ 2
size (g)	Speicherplatz eines Objektes g 4
Ascii(z)	Ascii-Code eines Ascii-Zeichens z 44
Char(k)	Ascii-Zeichen eines Ascii-Codes k 44

Elementare Zahlentheorie

$\mathbb{Z}_n$	Die Faktorgruppe $\mathbb{Z}/n\mathbb{Z}$
C_n	Zyklische Gruppe mit n Elementen
$\operatorname{rank} G$	$= k$ falls $G \cong C_{p^k}$ mit $p \in \mathbb{P}$, sonst $\operatorname{rank} G = 0$
α, β, γ	Elemente einer Gruppe
$\operatorname{ord} \alpha$	$= \min\{n \in \mathbb{N} \mid \alpha^n = 1_G\}$ Ordnung eines Gruppenelementes α

$\langle\gamma\rangle$	$= \{\gamma, \gamma^2, \gamma^3, \ldots\} \subseteq G$ Erzeugnis eines Gruppenelementes γ
(α)	Das von α erzeugte Ideal
$\mathbb{Z}[x, y]$	Polynomring in zwei Variablen über $\mathbb{Z}$
$\mathrm{SL}(n, \mathbb{Z})$	Gruppe der Matrizen $M \in \mathbb{Z}^{n\times n}$ mit $\det M = 1$
$a \mid b$	$\Leftrightarrow\ \exists\ c \in \mathbb{Z} : c \cdot a = b$ (a teilt b)
$a \parallel b$	$\Leftrightarrow a \mid b$ und $a^2 \nmid b$ (a teilt b genau)
$(p)_\alpha$	$\prod_{k=1}^{\alpha} \left(1 - p^{-k}\right)\ \ \forall\ p \in \mathbb{N}, p \geq 2$ und $\alpha \in \mathbb{N} \cup \{\infty\}$
$\zeta(s)$	Riemannsche Zeta-Funktion
$\varphi(n)$	$= \sharp\mathbb{Z}_n^\times$ (Eulersche φ-Funktion)
$\left(\frac{a}{p}\right)$	$= \begin{cases} 0 & \Leftrightarrow p \mid a \\ 1 & \Leftrightarrow\ \exists\ b \in \mathbb{Z}_p : b^2 \equiv a \bmod p \\ -1 & \Leftrightarrow \forall\ b \in \mathbb{Z}_p : b^2 \not\equiv a \bmod p \end{cases}$ (Legendre Symbol)
$\lfloor r \rfloor$	$= z \in \mathbb{Z}$ mit $r \leq z < r + 1$ (Floor-Funktion)

Formen

Zahlkörper

$\mathfrak{a}, \mathfrak{b}, \mathfrak{c}$	Ideale einer Maximalordnung $\mathcal{O}_\Delta$
σ	Nichttrivialer Automorphismus von $\mathbb{Q}\left(\sqrt{D}\right)/\mathbb{Q}$ 20
$\mathrm{N}(\alpha)$	Norm eines Elementes 20
$\mathrm{N}(\mathfrak{a})$	Norm eines Ideals 20
$\mathfrak{a}^*$	Konjugiertes Ideal 34
$\mathcal{R}(\mathfrak{a})$	Zyklus reduzierter Ideale 35
(a, b)	Standardrepräsentation eines Ideals 22
$\mathrm{Cl}(\Delta)$	Klassengruppe von $\mathcal{O}_\Delta$ 23
$\mathrm{h}(\Delta)$	Klassenzahl von $\mathcal{O}_\Delta$ 23
$\mathrm{Cl}_2(\Delta)$	Klassen der Ordnung ≤ 2 aus $\mathrm{Cl}(\Delta)$ 61
$\mathrm{h}_2(\Delta)$	Anzahl der Klassen der Ordnung ≤ 2 aus $\mathrm{Cl}(\Delta)$ 61
$\mathrm{Cl}_{\mathrm{odd}}(\Delta)$	Klassen aus $\mathrm{Cl}(\Delta)$ mit ungerader Ordnung 61
$\mathrm{h}_{\mathrm{odd}}(\Delta)$	Anzahl der Klassen aus $\mathrm{Cl}(\Delta)$ mit ungerader Ordnung 61
$\mathrm{h}_{\mathrm{cycl}}(\Delta)$	Größe der größten zyklischen Untergruppe von $\mathrm{Cl}(\Delta)$ 81
$\mathcal{O}_\Delta^\times$	Einheitengruppe von $\mathcal{O}_\Delta$ 23
ε_Δ	Grundeinheit von $\mathcal{O}_\Delta$ 24
$\mathrm{Reg}(\Delta)$	Regulator von $\mathcal{O}_\Delta$ 24
P_Δ	Menge der primitiven Ideale in $\mathcal{O}_\Delta$ 26
$\psi((a, b))$	$= ax^2 + bxy + \frac{b^2-\Delta}{4a}y^2$ (Funktion zwischen P_Δ und $\mathrm{Form}(\Delta)$) 26
$\eta(\mathfrak{a})$	Normalisierungsoperator 35
$\rho(\mathfrak{a})$	Reduktionsoperator 35
$\mathfrak{a} \sim \mathfrak{b}$	Äquivalenz von Idealen 23
$\mathfrak{a} \simeq \mathfrak{b}$	Äquivalenz im engeren Sinne von Idealen 28
$\mathrm{Cl}(\Delta)^+$	Klassengruppe von Idealen bezüglich der engeren Äquivalenz 28
$[\mathfrak{a}]$	Klasse eines Ideals 23
$[\mathfrak{a}]^+$	Klasse eines Ideals bezüglich der engeren Äquivalenz 28
$\psi_{\mathrm{Cl}}([\mathfrak{a}])$	$= [\psi(\mathfrak{a})]$ Bijektion zwischen $\mathrm{Cl}_{\mathrm{F}}(\Delta)$ und $\mathrm{Cl}(\Delta)^+$ 31

Tabellen

$\tau(x)$	Anzahl der Primzahlen $\leq x$ 75
$M(x)$	Anzahl der Primzahlen der Form $n^2 + 1 \leq x$ 75
$\overline{X}$	Der Durchschnitt einer Zufallsvariablen X
$\delta(n)$	Produkt aller Primzahlen $\leq n$ 80
$\mu(N)$	$= (\mathrm{Reg}(\Delta)\,\mathrm{h}(\Delta))/\sqrt{\Delta}$ mit $\Delta = \Delta\left(\mathbb{Q}\left(\sqrt{N^2+1}\right)\right)$ 79
$\lambda(N)$	$= (\mathrm{Reg}(\Delta)\,\mathrm{h}_{\mathrm{cycl}}(\Delta))/\sqrt{\Delta}$ mit $\Delta = \Delta\left(\mathbb{Q}\left(\sqrt{N^2+1}\right)\right)$ 81
$\mathfrak{h}(N, p)$	Das Ideal $(p, 1) \in \mathrm{P}_\Delta$ mit $2 \cdot p \mid N$, $\Delta = \Delta\left(\mathbb{Q}\left(\sqrt{N^2+1}\right)\right)$ ... 82

Kapitel 1

Einleitung

Im Zeitalter des Computers und des Internets nimmt die Bedeutung der Kryptographie auch für den Normalbürger immer mehr zu. Sie ermöglicht zum Beispiel den sicheren Gebrauch von Kreditkarten und vertrauliche Kommunikation über das Internet. Die Sicherheit heute gebräuchlicher Kryptosysteme basiert auf mathematischen Problemen, die zur Zeit als schwer lösbar gelten, zum Beispiel die Berechnung des Logarithmus in endlichen Gruppen (DLP) oder die Zerlegung einer großen natürlichen Zahl in ihre Primfaktoren (IFP). Problematisch dabei ist, daß man bis jetzt noch nicht beweisen konnte, daß diese Probleme tatsächlich schwierig sind. Die letzten Jahrzehnte zeigen, daß immer wieder Durchbrüche auf der Suche nach schnelleren Algorithmen möglich sind, so zum Beispiel das Zahlkörpersieb. Neben Versuchen, die Schwierigkeit von mathematischen Problemen zu beweisen oder zu widerlegen, sucht man auch nach neuen Problemen und untersucht deren Verwendbarkeit für Kryptosysteme. Diese könnten dann unsicher gewordene Ansätze ersetzen. Im Zuge dieser Forschungen wurden Ende der siebziger Jahre Elliptische Kurven als mögliche Alternative entdeckt und inzwischen auch zunehmend verwendet. Seit Ende der achtziger Jahre wird auch die Idee untersucht, Klassengruppen quadratischer Zahlkörper für die Verschlüsselung zu verwenden.
In dieser Arbeit wollen wir am Beispiel der ElGamal-Verschlüsselung zeigen, wie man Klassengruppen in der Kryptographie einsetzen kann und wovon die Sicherheit des Verfahrens abhängt. Wir betrachten dabei Klassengruppen imaginärquadratischer und reellquadratischer Zahlkörper und vergleichen diese untereinander und mit dem gängigen RSA-Verfahren. Es werden Algorithmen angegeben, die eine Implementation dieses Verfahrens in einem Computeralgebrasystem erlauben.

1.1 Gliederung

In den Kapiteln 2 und 3 werden wir uns mit Formen und Zahlkörpern beschäftigen. Dort untersuchen wir auch den Zusammenhang zwischen Formen und Idealen, sowie deren Reduktion und Arithmetik. Nach diesen zahlentheoretischen Grundlagen geht es in Kapitel 4 um die Grundlagen der Kryptographie. Wir stellen dort unter

anderem auch die ElGamal-Verschlüsselung vor. In den Kapiteln 5 und 6 zeigen wir dann, wie das ElGamal-Verfahren in der Klassengruppe imaginärquadratischer bzw. reellquadratischer Zahlkörper realisiert werden kann, wovon dessen Sicherheit abhängt. In Kapitel 7 werden wir die praktische Seite etwas näher beleuchten und die vorgestellten Verfahren miteinander vergleichen. Das letzte Kapitel faßt die Ergebnisse dieser Arbeit zusammen und zeigt Perspektiven für das weitere Studium oder die weitere Forschung auf diesem Gebiet.

1.2 Komplexität von Algorithmen

1.2.1 Definition Eine Funktion $f : \mathbb{N} \to \mathbb{N}$ heißt von der **Größenordnung** von $g : \mathbb{N} \to \mathbb{N} :\Leftrightarrow$

$$\exists\, c \in \mathbb{R}^+ : f(n) \leq c \cdot g(n) \text{ für fast alle } n \in \mathbb{N}.$$

Schreibweise:

$$f = \mathcal{O}(g).$$

1.2.2 Definition Es seien $f, g : \mathbb{R}^+ \to \mathbb{R}^+$ Funktionen. Wir schreiben

$$f = o(g),$$

falls

$$\lim_{x \to \infty} \frac{f(x)}{g(x)} = 0.$$

1.2.3 Definition Für $x, u, v \in \mathbb{R}, x > \exp(1), u > 0, 0 \leq v \leq 1$ definieren wir

$$L_x[u, v] := \exp\left((v + o(1)) (\ln x)^u (\ln \ln x)^{1-u}\right).$$

1.2.4 Definition Ein Algorithmus heißt

(i) **polynomial** oder auch **effizient**, wenn er einen Aufwand in der Größenordnung eines Polynoms in den Bitlängen der Eingabedaten hat, zum Beispiel $L_n[0, v]$.

(ii) **exponentiell**, wenn er einen Aufwand in der Größenordnung einer Exponentialfunktion in den Bitlängen der Eingabedaten hat, zum Beispiel $L_n[1, v]$.

(iii) **subexponentiell**, wenn er einen Aufwand in der Größenordnung einer Funktion zwischen den beiden obigen hat, also $L_n[u, v]$ mit $0 < u < 1$.

(iv) **probabilistisch**, wenn sein Verlauf von Zufallsgrößen abhängt. Es besteht mit einer minimalen Wahrscheinlichkeit die Möglichkeit, daß er nicht terminiert, d. h. der Name Algorithmus ist eigentlich nicht gerechtfertigt. In der Praxis sind solche Verfahren allerdings meist schneller als **deterministische** Versionen, oft gibt es zu einem Problem nur vernünftige probabilistische Lösungen. Bei ihnen spricht man dann von einem **erwarteten Aufwand**.

1.2.5 Definition Ein **MIPS-Jahr** entspricht dem Arbeitsaufwand eines Rechners, der eine Million Operationen pro Sekunde verarbeiten kann und ein Jahr arbeitet. Das sind also

$$10^6 \cdot 60^2 \cdot 24 \cdot 365 = 31536 \cdot 10^9 \approx 10^{13,5}$$

Operationen.
Für einen guten PC werden wir hier 1000 MIPS veranschlagen, d. h. ein solcher Rechner würde für ein MIPS-Jahr knapp 9 Stunden arbeiten.
Die Benutzung dieser Einheit ist nicht unumstritten, aber wegen ihrer Anschaulichkeit oft gebraucht. Für eine genauere Untersuchung empfehlen wir [Sil99].

1.2.6 Bemerkung Bezüglich des Angriffs auf Verschlüsselungssysteme werden in dieser Arbeit sehr große Zahlen auftreten. Zum Beispiel schätzt man den Aufwand zur Faktorisierung einer 2048-Bit-Zahl auf ca. $6{,}98 \cdot 10^{19}$ MIPS-Jahre, das heißt unser Computer würde dafür $6{,}98 \cdot 10^{16}$ Jahre benötigen. Geht man von einem geschlossenen Universum aus, so haben wir allerdings nur ca. 10^{11} Jahre Zeit, dieses Problem zu lösen. Von solchen Zahlen sollte man sich nicht zu sehr beeindrucken lassen, da es nicht sicher ist, ob sich in den verbleibenden 10^{11} Jahren nicht noch ein schnellerer Algorithmus zur Lösung des Problems findet. Geht man weiterhin davon aus, daß man sich hin und wieder einen neuen Computer kauft, so kann man das Problem letztendlich wieder in Polynomialzeit lösen, da sich die Leistung von Computern momentan ebenfalls exponentiell entwickelt. Nimmt man zum Beispiel die gängige Zeit von 1,5 Jahren zur Verdopplung der Rechenleistung, so entwickelt sich der geleistete Arbeitsaufwand $A(t)$ wie folgt:

$$A(t) = \int_0^t 1000 \cdot 2^{\frac{2}{3}x} dx = \frac{3 \cdot 1000}{2 \cdot \ln 2} \cdot \left(\exp\left(\frac{2 \cdot \ln 2}{3} \cdot t \right) - 1 \right).$$

Also ergibt sich aus $A(t) = 6{,}98 \cdot 10^{19}$ als benötigt Zeit:

$$t \approx \left(\ln\left(6{,}98 \cdot 10^{16} \cdot (1,5 \cdot \ln 2) \right) + 1 \right) \cdot \frac{2}{3 \cdot \ln 2} \approx 38{,}3 \text{ Jahre.}$$

Den meisten Geheimnissen genügt es allerdings, wenige Jahre geheim zu bleiben.

1.2.7 Definition Es sei $0 \neq a \in \mathbb{Z}$. Die **Bitlänge** von a (inklusive Vorzeichen) wird dann mit

$$\operatorname{size}(a) := \lfloor \log_2 |a| \rfloor + 2$$

bezeichnet. Wir setzen weiterhin $\operatorname{size}(0) = 1$.

1.2.8 Primzahltests Der zur Zeit beste Algorithmus um zu testen, ob eine natürliche Zahl n eine Primzahl ist, ist Morains ECPP aus [AM93], ein probabilistischer Algorithmus der Elliptische Kurven benutzt. Es konnte bewiesen werden, daß dieser Algorithmus polynomial für fast alle Eingaben ist. Heuristisch wurde in [LL90] ein erwarteter Aufwand von $\mathcal{O}\left(\operatorname{size}(n)^{6+\varepsilon}\right)$ mit $\varepsilon > 0$ ermittelt.
Nach dem Primzahlsatz ist die Wahrscheinlichkeit, daß eine zufällige Zahl n eine Primzahl ist gerade $\ln n$. Daher liegt der Aufwand, eine Primzahl mit einer bestimmten Bitlänge k zu finden, also bei $\mathcal{O}(k^{7+\varepsilon})$.
Nachdem in diesem Jahr in [AKS02] ein neuer Ansatz für einen deterministischen Primzahltest gefunden wurde, hat Daniel Bernstein in [Ber03] einen entsprechenden Primzahltest mit einem Aufwand von $\mathcal{O}\left(\operatorname{size}(n)^{4+o(1)}\right)$ vorgestellt. Dieser ist aber praktisch noch viel langsamer als ECPP, und daher keine Alternative. Es bleibt zu hoffen, daß die neuen Ideen in diesem Test zu verbesserten deterministische Tests führen.

1.2.9 Zufallszahlen Für die Erzeugung von kryptographisch sicheren Zufallszahlen $n \leq M \in \mathbb{N}$ werden wir den *Monster*-Algorithmus von G. Marsaglia ([Mar00]) verwenden, er hat einen Aufwand von $\mathcal{O}(\operatorname{size}(M))$.

Mit Hilfe der letzten beiden Aussagen und den Angaben in [MvOV97, Kap.3] haben wir in Tabelle 1.1 den Aufwand einiger Standardoperationen für ganze Zahlen zusammengetragen. Diese Erkenntnisse bilden die Grundlage für Aufwandsaussagen der meisten von uns entwickelten Algorithmen.

Name	Formel	Aufwand
Addition	$a \pm b$	$\mathcal{O}\left(\max\{\text{size}\left(a\right), \text{size}\left(b\right)\}\right)$
Multiplikation	ab	$\mathcal{O}\left(\text{size}\left(a\right) \text{size}\left(b\right)\right)$
Division mit Rest	$a = qb + r$	$\mathcal{O}\left(\text{size}\left(q\right) \text{size}\left(b\right)\right)$
Euklidischer Algorithmus	$\text{ggT}\left(a, b\right)$	$\mathcal{O}\left(\text{size}\left(a\right) \text{size}\left(b\right)\right)$
Erweiterter Euklid. Algorithmus	$\text{ggT}\left(a, b\right) = ua + vb$	$\mathcal{O}\left(\text{size}\left(a\right) \text{size}\left(b\right)\right)$
Potenzieren modulo n	$a^b \bmod n$	$\mathcal{O}\left(\text{size}\left(b\right) \left(\text{size}\left(n\right)\right)^2\right)$
Invertieren modulo n	$a^{-1} \bmod n$	$\mathcal{O}\left(\text{size}\left(n\right)^2\right)$
Quadratwurzel modulo n falls		
Faktorisierung von n bekannt	$\sqrt{a} \bmod n$	$\mathcal{O}\left(\text{size}\left(n\right)^3\right)$
Legendre Symbol	$\left(\frac{a}{n}\right)$	$\mathcal{O}\left(\text{size}\left(n\right)^2\right)$
Primzahltest (ECPP)	`IsPrime`(n)	$\mathcal{O}\left(\text{size}\left(n\right)^{6+\varepsilon}\right)$
Nächstgrößere Primzahl (ECPP)	`NextPrime`(n)	$\mathcal{O}\left(\text{size}\left(n\right)^{7+\varepsilon}\right)$
Zufallszahl $\leq n$	`RandomInt(`n`)`	$\mathcal{O}\left(\text{size}\left(n\right)\right)$

Tabelle 1.1: Aufwand einiger Standardoperationen für ganze Zahlen a, b, n.

Kapitel 2

Formen

Die Theorie der Formen geht im wesentlichen auf Carl Friedrich Gauß (1777-1855) zurück und war eines der wichtigsten Werkzeuge der Zahlentheorie. Sie wurde aber bald von Eisensteins und Dedekinds idealtheoretischem Zugang zur Zahlentheorie, wie wir ihn heute kennen, verdrängt. Da moderne Literatur über Formen im Hinblick auf unsere Zwecke heute schwer zu finden ist, wollen wir hier eine etwas ausführlichere Einführung in diese Theorie geben. Sie wird uns helfen, effiziente Algorithmen für das Rechnen in der Klassengruppe zu finden.

2.1 Formen und deren Klassen

2.1.1 Definition Ein homogenes Polynom zweiten Grades

$$f = f(x, y) = ax^2 + bxy + cy^2 \in \mathbb{Z}[x, y], ac \neq 0$$

heißt ganze binäre quadratische Form oder einfach **Form**. Sie wird durch (a, b, c) dargestellt. Eine Form heißt **primitiv** $:\Leftrightarrow \mathrm{ggT}(a, b, c) = 1$. Die Zahl

$$\Delta := \Delta(f) := b^2 - 4ac$$

heißt **Diskriminante** der Form f.

$$\mathrm{sign}(f) := \mathrm{sign}(a)$$

heißt **Vorzeichen** von f. Dementsprechend nennen wir Formen **positiv** oder **negativ**. Im Folgenden heißen primitive ganze binäre quadratischen Formen einfach Formen.

2.1.2 Definition Es sei $f = (a, b, c)$ eine Form. Dann ist

$$\mathrm{size}(f) := \mathrm{size}(a) + \mathrm{size}(b) + \mathrm{size}(c).$$

2.1.3 Bemerkung Es sei $f = (a, b, c)$ eine Form. Dann gilt:

$$\begin{aligned} 4af(x,y) &= 4a^2x^2 + 4abxy + 4acy^2 \\ &= (2ax + by)^2 - b^2y^2 + 4acy^2 \\ &= (2ax + by)^2 - y^2\Delta(f). \end{aligned}$$

Dies zeigt, daß f für $\Delta(f) > 0$ positive und negative Werte annimmt. Für $\Delta(f) < 0$ nimmt f entweder nur positive oder nur negative Werte an, abhängig davon, welches Vorzeichen a hat. Dies motiviert die folgende

2.1.4 Definition Eine Form $f = (a, b, c)$ heißt

(i) **indefinit**, falls $\Delta(f) > 0$

(ii) **definit**, falls $\Delta(f) < 0$

(iii) **positiv definit**, falls $\Delta(f) < 0$ und $\operatorname{sign} f > 0$

(iv) **negativ definit**, falls $\Delta(f) < 0$ und $\operatorname{sign} f < 0$.

2.1.5 Definition Es seien $f(x, y)$ und $g(x, y)$ Formen und

$$T = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z}).$$

f heißt mittels T in g **transformiert**, falls

$$f(rx + sy, tx + uy) = g(x, y). \tag{2.1}$$

Schreibweise: $f \cdot T = g$. In diesem Fall heißen f und g **äquivalent** ($f \sim g$).

2.1.6 Bemerkung Die Äquivalenz von Formen ist eine Äquivalenzrelation, da $\mathrm{SL}(2, \mathbb{Z})$ eine Gruppe ist.

2.1.7 Bemerkung Für äquivalente Formen $f = (a, b, c)$ und $g = \left(\tilde{a}, \tilde{b}, \tilde{c}\right)$ wie in (2.1) gilt:

$$\begin{aligned} \tilde{a} &= ar^2 + brt + ct^2 &&= f(r,t) \\ \tilde{b} &= 2ars + b(ru + st) + 2ctu \\ \tilde{c} &= as^2 + bsu + cu^2 &&= f(s,u). \end{aligned}$$

Damit ergibt sich $\Delta(f) = \Delta(g)$. Auch alle weiteren bisher genannten Eigenschaften einer Form wie Primitivität, Indefinitheit, positive und negative Definitheit bleiben unter Operationen aus $\mathrm{SL}(2, \mathbb{Z})$ unverändert.

2.1.8 Beispiel Es sei $f = (a, b, c)$ eine Form.

(i) Für $M(s) := \begin{pmatrix} 1 & s \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$ gilt: $f \cdot M(s) = (a, b + 2as, as^2 + bs + c)$

(ii) Für $P := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \in \mathrm{SL}(2, \mathbb{Z})$ gilt: $f \cdot P = (c, -b, a)$

2.1.9 Bemerkung Nach Bemerkung 2.1.7 zerfällt die Menge aller definiten Formen zu einer gegebenen Diskriminante in die zwei disjunkten Teilmengen der positiv und negativ definiten Formen. Diese Mengen verhalten sich wegen

$$f \text{ ist positiv definit } \iff -f \text{ ist negativ definit}$$

völlig symmetrisch und werden durch Operationen aus $\mathrm{SL}(2, \mathbb{Z})$ fest gelassen.

Da für uns in dieser Arbeit nur indefinite und positive definite Formen wichtig sind, werden wir im Folgenden negative definite Formen nicht mehr betrachten.

2.1.10 Definition Es sei Δ die Diskriminante einer Form. Wir definieren

$$\mathrm{Form}(\Delta) := \begin{cases} \{f \text{ Form mit } \Delta(f) = \Delta \text{ und } \operatorname{sign} f > 0\} & \text{für } \Delta < 0 \\ \{f \text{ Form mit } \Delta(f) = \Delta\} & \text{für } \Delta > 0 \end{cases}.$$

Es heißen

$$\begin{aligned} \mathrm{Cl}_{\mathrm{F}}(\Delta) &:= \mathrm{Form}(\Delta) / \mathrm{SL}(2, \mathbb{Z}) \\ \mathrm{h}_{\mathrm{F}}(\Delta) &:= \sharp\, \mathrm{Cl}_{\mathrm{F}}(\Delta) \end{aligned}$$

Klassengruppe bzw. **Klassenzahl** von $\mathrm{Form}(\Delta)$.

2.2 Reduzierte Formen

2.2.1 Definition $f = (a, b, c) \in \mathrm{Form}(\Delta)$ heißt **normal**, falls eine der folgenden Aussagen gilt:

(i) f ist positiv definit und $-a < b \leq a$

(ii) f ist indefinit, $|a| \geq \sqrt{\Delta}$ und $-|a| < b \leq |a|$

(iii) f ist indefinit, $|a| < \sqrt{\Delta}$ und $\sqrt{\Delta} - 2|a| < b < \sqrt{\Delta}$.

Das **Normalisieren** einer Form $f = (a, b, c) \in \mathrm{Form}\,(\Delta)$, d. h. das Ersetzen von f durch eine äquivalente normale Form, ist denkbar einfach: Wir berechnen das eindeutige $s\,(f) \in \mathbb{Z}$, für das

$$-|a| < b + 2a \cdot s\,(f) \leq |a| \text{ bzw. } \sqrt{\Delta} - 2|a| < b + 2a \cdot s\,(f) < \sqrt{\Delta}$$

gilt.

(i) Es ist

$$\begin{aligned}
& -|a| < b + 2a \cdot s\,(f) \leq |a| \\
\iff\ & -|a| \leq -b - 2a \cdot s\,(f) < |a| \\
\iff\ & 2a \cdot s\,(f) \leq -b + |a| < 2a \cdot s\,(f) + 2|a| \\
\iff\ & \operatorname{sign} a \cdot s\,(f) \leq \frac{|a| - b}{2|a|} < \operatorname{sign} a \cdot s\,(f) + 1 \\
\iff\ & \operatorname{sign} a \cdot s\,(f) = \left\lfloor \frac{|a| - b}{2|a|} \right\rfloor \\
\iff\ & s\,(f) = \operatorname{sign} a \cdot \left\lfloor \frac{|a| - b}{2|a|} \right\rfloor
\end{aligned}$$

(ii) Es ist

$$\begin{aligned}
& \sqrt{\Delta} - 2|a| < b + 2a \cdot s\,(f) \leq \sqrt{\Delta} \\
\iff\ & -\sqrt{\Delta} \leq -b - 2a \cdot s\,(f) < -\sqrt{\Delta} + 2|a| \\
\iff\ & 2a \cdot s\,(f) \leq -b + \sqrt{\Delta} < 2a \cdot s\,(f) + 2|a| \\
\iff\ & \operatorname{sign} a \cdot s\,(f) \leq \frac{\sqrt{\Delta} - b}{2|a|} < \operatorname{sign} a \cdot s\,(f) + 1 \\
\iff\ & \operatorname{sign} a \cdot s\,(f) = \left\lfloor \frac{\sqrt{\Delta} - b}{2|a|} \right\rfloor \\
\iff\ & s\,(f) = \operatorname{sign} a \cdot \left\lfloor \frac{\sqrt{\Delta} - b}{2|a|} \right\rfloor
\end{aligned}$$

Wir wählen also folgende

2.2.2 Definition Es sei $f = (a, b, c) \in \mathrm{Form}\,(\Delta)$. Dann sei

$$s\,(f) := \begin{cases} \left\lfloor \frac{a-b}{2a} \right\rfloor & \text{für } f \text{ positiv definit} \\ \mathrm{sign}\,(a) \left\lfloor \frac{|a|-b}{2|a|} \right\rfloor & \text{für } f \text{ indefinit und } |a| \geq \sqrt{\Delta} \\ \mathrm{sign}\,(a) \left\lfloor \frac{\sqrt{\Delta}-b}{2|a|} \right\rfloor & \text{für } f \text{ indefinit und } |a| < \sqrt{\Delta} \end{cases} .$$

Nun kommt uns die schon oben betrachtete Matrix $M\,(s)$ zugute, denn sie transformiert f in eine äquivalente normale Form. Dies zeigt gleichzeitig auch, daß jede Form normalisiert werden kann. Wir definieren

$$\eta\,(f) := f \cdot M\,(s\,(f))\,.$$

2.2.3 Definition Eine normale Form $f = (a, b, c) \in \mathrm{Form}\,(\Delta)$ heißt **reduziert**, falls eine der folgenden Aussagen gilt:

(i) f ist positiv definit und $(a < c)$ oder $(a = c$ und $b \geq 0)$

(ii) f ist indefinit und $\left|\sqrt{\Delta} - 2|a|\right| < b$.

2.2.4 Bemerkung Eine sei $f = (a, b, c)$ eine indefinite Form Dann gilt:

$$f \text{ ist reduziert } \iff \left|\sqrt{\Delta} - 2|a|\right| < b < \sqrt{\Delta}.$$

2.2.5 Lemma *Wenn $f = (a, b, c)$ normal ist und $|a| < \frac{\sqrt{|\Delta|}}{2}$ gilt, so ist f reduziert.*

Beweis: Es sei f normal und $|a| < \frac{\sqrt{|\Delta|}}{2}$, also $4a^2 < |\Delta|$.

(i) f positiv definit:

$$\Delta < 0 \Longrightarrow c = \frac{b^2 + |\Delta|}{4a} \geq \frac{|\Delta|}{4a} > \frac{4a^2}{4a} = a.$$

(ii) f indefinit: Es gilt $\sqrt{\Delta} - 2|a| < b$ da f normal ist. Wegen $|a| < \frac{\sqrt{|\Delta|}}{2}$ gilt $\left|\sqrt{\Delta} - 2|a|\right| > 0$ also auch $\left|\sqrt{\Delta} - 2|a|\right| < b$.

Daher ist f in beiden Fällen reduziert. □

2.2.6 Lemma *Es sei $f = (a, b, c)$ reduziert. Dann gilt:*

(i) *f positiv definit* $\Longrightarrow |a|, |b| \leq \sqrt{\frac{|\Delta|}{3}}$

(ii) *f indefinit* $\Longrightarrow |a|, |b| \leq \sqrt{\Delta}$

Beweis:

(i) Es sei $f = (a, b, c)$ positiv definit und reduziert. Dann gilt nach Definition $|b| \leq |a| \leq c$, also

$$|\Delta| = 4ac - b^2 \geq 4a^2 - a^2 \Longrightarrow |a| \leq \sqrt{\frac{|\Delta|}{3}}.$$

(ii) Es sei $f = (a, b, c)$ indefinit und reduziert. Dann gilt $\left|\sqrt{\Delta} - 2|a|\right| < \sqrt{\Delta}$, also muß $|a| < \sqrt{\Delta}$ gelten. Es ist $0 < b < \sqrt{\Delta}$, da f reduziert ist.

□

2.2.7 Definition Die Abbildung

$$\rho : \mathrm{Form}\,(\Delta) \longrightarrow \mathrm{Form}\,(\Delta) : (a, b, c) \longmapsto \eta\,((c, -b, a))$$

heißt **Reduktionsoperator**.

2.2.8 Bemerkung Es ist

$$\rho\,(f) \sim f \quad \forall\ f \in \mathrm{Form}\,(\Delta)\,,$$

da $\rho\,(f) = \eta\,(f \cdot P) = (f \cdot P) \cdot M\,(s\,(f \cdot P))$

Das **Reduzieren** einer Form $f = (a, b, c)$, also das Ersetzen von f durch eine äquivalente reduzierte Form, wird durch den folgenden Algorithmus aus [BB97] erreicht:

Algorithmus `FormReduce`

Eingabe : Eine Form $f = (a, b, c)$
Ausgabe: Eine äquivalente reduzierte Form

`1:` $f := \eta\,(f)$
`2:` **while** f `is not reduced` **do**
`3:` $f := \rho\,(f)$
`4:` **end while**
`5:` **return** f

Aufwand: $\mathcal{O}\left(\mathrm{size}\,(f)^2\right)$

Zum Aufwand siehe [BB97].

2.2.9 Lemma *Für $f = (a, b, c) \in \mathrm{Form}\,(\Delta)$ normal gilt:*

(i) $|a| \geq \sqrt{\Delta} \Longrightarrow |c| \leq \frac{|a|}{2}$

(ii) $|a| < \sqrt{\Delta} \Longrightarrow f$ *oder* $\rho\,(f)$ *ist reduziert .*

Beweis: [BB97, Lemma 4.2, S. 5-6] □

2.2.10 Korollar `FormReduce` *terminiert nach maximal* $\log_2\left(\frac{|a|}{\sqrt{\Delta}}\right) + 2$ *Schritten und ist korrekt.*

Beweis: [BB97, Theorem 4.3, S. 6] □

In den folgenden beiden Sätzen werden erste grundlegende Unterschiede zwischen definiten und indefiniten Formen sichtbar. Diese übertragen sich später auf Ideale in imaginärquadratischen und reellquadratischen Zahlkörpern.

2.2.11 Satz *Jede positiv definite Form ist äquivalent zu einer eindeutig bestimmten reduzierten Form.*

Beweis: [Coh95, Prop. 5.3.3, S. 226] □

2.2.12 Satz *Für indefinite Formen f gilt:*

(i) Ist f reduziert, dann ist auch $\rho\,(f)$ reduziert.

(ii) Alle reduzierten Formen äquivalent zu f lassen sich durch wiederholte Anwendung von ρ auf eine reduzierte Form $f_1 \sim f$ berechnen und deren Anzahl ist endlich.

Beweis: [Coh95, Prop. 5.6.6, S. 259] □

2.3 Der Zyklus einer Formenklasse

2.3.1 Definition Es sei $\Delta > 0$ und $f \in \mathrm{Form}\,(\Delta)$. Dann heißt die Menge $\{f_1, \ldots, f_k\}$ der reduzierten Formen in $[f]$ mit ihrer Struktur

$$f_1 \xrightarrow{\rho} f_2 \xrightarrow{\rho} \ldots \xrightarrow{\rho} f_k \xrightarrow{\rho} f_1$$

Zyklus von reduzierten Formen von f bzw. $[f]$. Dieser Zyklus ist eindeutig bis auf zyklische Vertauschungen der f_i. Schreibweise:

$$\mathcal{R}\,(f) = (f_1, \ldots, f_k)\,.$$

2.3.2 Lemma *Es sei $\Delta > 0$. Dann gilt:*

(i) *Ist $f \in \mathrm{Form}(\Delta)$ reduziert, so alterniert deren Vorzeichen unter der Anwendung von ρ.*

(ii) $\forall\ f \in \mathrm{Form}(\Delta)\ \exists\ h \sim f : \mathrm{sign}(h) = 1$.

(iii) $2 \mid \sharp\mathcal{R}(f) \quad \forall\ f \in \mathrm{Form}(\Delta)$.

Beweis:

(i) Es sei $f = (a, b, c)$ reduziert. Dann gilt:

$$\begin{aligned} 0 \leq \left|\sqrt{\Delta} - 2|a|\right| < b < \sqrt{\Delta} \quad &\Longrightarrow \quad \Delta > b^2 \\ &\Longrightarrow \quad \Delta - b^2 = -4ac > 0 \\ &\Longrightarrow \quad ac < 0. \end{aligned}$$

Wegen

$$\rho(f) = \eta((c, -b, a)) = \left(c, \tilde{b}, \tilde{a}\right)$$

wechselt das Vorzeichen von f mit jeder Anwendung von ρ.

(ii) f ist äquivalent zu einer reduzierten Form g. Wegen (i) ist entweder $\mathrm{sign}(g) = 1$ oder $\mathrm{sign}(\rho(g)) = 1$.

(iii) Es sei $f \in \mathrm{Form}(\Delta)$ und $g \sim f$ reduziert. Aus Satz 2.2.12 folgt: $\exists\ k \in \mathbb{N} : g = \rho^k(g)$. Wegen Teil (i) ist aber $\mathrm{sign}(g) = \mathrm{sign}\left(\rho^k(g)\right)$ nur falls k gerade ist.

□

2.3.3 Definition Es sei $\Delta > 0$ und $f = (a, b, c) \in \mathrm{Form}(\Delta)$. Dann heißt

$$f^* := (-a, b, -c) \in \mathrm{Form}(\Delta)$$

konjugierte Form zu f.

2.3.4 Lemma *Es sei $\Delta > 0$. Dann gilt:*

(i) *$f \in \mathrm{Form}(\Delta)$ ist reduziert (normal) $\Longleftrightarrow$ f^* ist reduziert (normal).*

(ii) $s(f^*) = -s(f) \quad \forall\ f \in \mathrm{Form}(\Delta)$

(iii) $\eta(f^*) = \eta(f)^* \quad \forall\ f \in \mathrm{Form}(\Delta)$

(iv) $\rho(f^*) = \rho(f)^* \quad \forall\ f \in \mathrm{Form}(\Delta)$

(v) `FormReduce(`f^*`)` $=$ `FormReduce(`f`)`* $\forall\ f \in \mathrm{Form}(\Delta)$.

Beweis:

(i) f unterscheidet sich von f^* nur in den Vorzeichen von a und c. Da diese aber in der Definition von normalen und reduzierten Formen keine Rolle spielen, folgt die Behauptung.

(ii) Es sei $f = (a,b,c) \in \mathrm{Form}\,(\Delta)$. Dann gilt:

$$\begin{aligned} s\,(f^*) &= s\,((-a,b,-c)) \\ &= \begin{cases} \operatorname{sign}(-a)\left\lfloor \frac{|-a|-b}{2|-a|} \right\rfloor & \text{für } |-a| \geq \sqrt{\Delta} \\ \operatorname{sign}(-a)\left\lfloor \frac{\sqrt{\Delta}-b}{2|-a|} \right\rfloor & \text{für } |-a| < \sqrt{\Delta} \end{cases} \\ &= \begin{cases} -\operatorname{sign}(a)\left\lfloor \frac{|a|-b}{2|a|} \right\rfloor & \text{für } |a| \geq \sqrt{\Delta} \\ -\operatorname{sign}(a)\left\lfloor \frac{\sqrt{\Delta}-b}{2|a|} \right\rfloor & \text{für } |a| < \sqrt{\Delta} \end{cases} \\ &= -s\,((a,b,c)) \\ &= -s\,(f)\,. \end{aligned}$$

(iii) Es sei $f = (a,b,c) \in \mathrm{Form}\,(\Delta)$. Dann gilt:

$$\begin{aligned} \eta\,(f^*) &= \eta\,((-a,b,-c)) \\ &= \left(-a, b - 2as\,(f^*), -as\,(f^*)^2 + bs\,(f^*) - c\right) \\ &= \left(-a, b + 2as\,(f), -as\,(f)^2 - bs\,(f) - c\right) \\ &= \left(a, b + 2as\,(f), as\,(f)^2 bs\,(f)\,c\right)^* \\ &= \eta\,((a,b,c))^* \\ &= \eta\,(f)^*\,. \end{aligned}$$

(iv) Es sei $f = (a,b,c) \in \mathrm{Form}\,(\Delta)$. Dann gilt:

$$\begin{aligned} \rho\,(f^*) &= \rho\,((-a,b,-c)) \\ &= \eta\,((-c,-b,-a)) \\ &= \eta\,((c,-b,a)^*) \\ &= \eta\,((c,-b,a))^* \\ &= \rho\,(f)^*\,. \end{aligned}$$

(v) Folgt aus Teil (iii) und (iv)

□

2.3.5 Lemma *Es sei $\Delta > 0$. Dann gilt:*

(i) Ist $\mathcal{R}\,(f) = (f_1, \ldots, f_k)$, so ist $\mathcal{R}\,(f^*) = (f_1^*, \ldots, f_k^*)$.

(ii) Ist $\mathcal{R}\,(f) = \mathcal{R}\,(f^*)$, also $g \sim g^* \;\; \forall\; g \in [f]$, so hat $\mathcal{R}\,(f)$ die Form

$$f_1 \xrightarrow{\rho} f_2 \xrightarrow{\rho} \ldots \xrightarrow{\rho} f_{\frac{k}{2}} \xrightarrow{\rho} f_1^* \xrightarrow{\rho} f_2^* \xrightarrow{\rho} \ldots \xrightarrow{\rho} f_{\frac{k}{2}}^* \xrightarrow{\rho} f_1.$$

In diesem Fall gilt $2 \parallel k = \sharp\mathcal{R}\,(f)$.

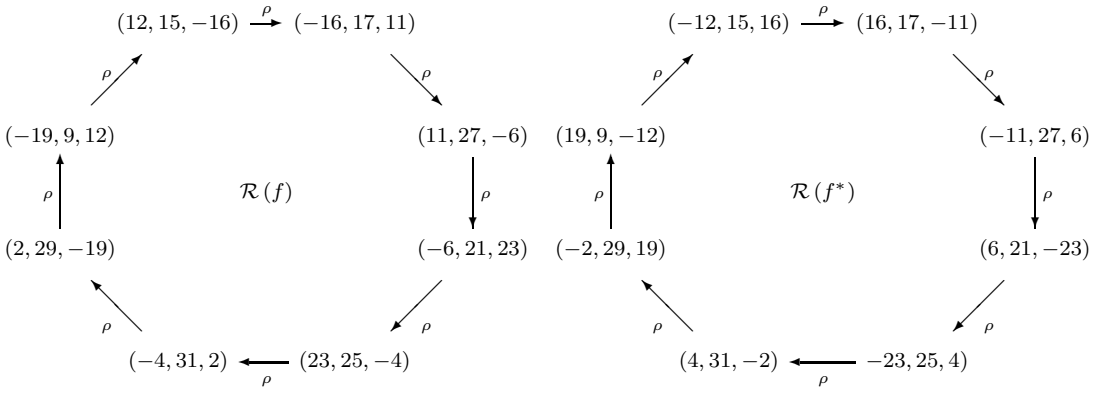
Beweis:

(i) Folgt aus Lemma 2.3.4.

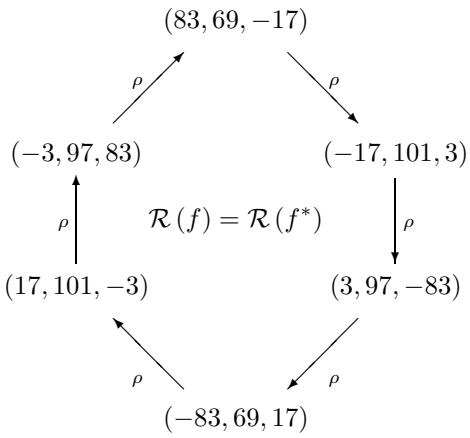
(ii) Ist ebenfalls klar nach Lemma 2.3.4. Wäre $\frac{k}{2}$ gerade, so wäre nach Teil (i) von Lemma 2.3.2 $\operatorname{sign}(f_1) = \operatorname{sign}\left(\rho^{\frac{k}{2}}(f_1)\right) = \operatorname{sign}(f_1^*)$, was ein Widerspruch ist.

□

2.3.6 Beispiel Wir wollen die beiden Möglichkeiten für konjugierte Zyklen an einem Beispiel veranschaulichen. $f = (12, 15, -16) \in \operatorname{Form}(993)$:



$f = (83, 69, -17) \in \operatorname{Form}(10405)$:



2.3.7 Definition Es sei $\Delta > 0$. Die letzten beiden Lemmata 2.3.4 und 2.3.5 zeigen, daß sich f und f^* völlig symmetrisch verhalten. Wir definieren daher:

$$f \sim_* g :\Longleftrightarrow g \in \{f, f^*\}.$$

Da $\sim_*$ eine Äquivalenzrelation ist, definieren wir

$$\operatorname{Form}_*(\Delta) := \operatorname{Form}(\Delta) / \sim_*$$

und erhalten die Projektion auf die Klassen:

$$\pi : \mathrm{Form}\,(\Delta) \longrightarrow \mathrm{Form}_*\,(\Delta) : f \longmapsto \pi(f).$$

Wir weichen hier von der üblichen Schreibweise für Klassen ab, um Verwechslungen mit $[f]$ zu vermeiden.

2.3.8 Definition Wegen Lemma 2.3.4 und 2.3.5 sind die Eigenschaften „normal“ und „reduziert“, der Zyklus $\mathcal{R}$ sowie die Abbildungen η und ρ nur von der Klasse bezüglich $\sim_*$ abhängig. Wir können diese Begriffe und Abbildungen also sinnvoll auf $\mathrm{Form}_*\,(\Delta)$ fortsetzen.

2.3.9 Definition Wir setzen ebenfalls $\sim$ auf $\mathrm{Form}_*\,(\Delta)$ fort:

$$\pi(f) \sim \pi(g) \Longleftrightarrow f \sim g \text{ oder } f^* \sim g$$

$\forall\ f, g \in \mathrm{Form}\,(\Delta)$.

2.3.10 Korollar *Es sei $\Delta > 0$ und $\pi(f) \in \mathrm{Form}_*\,(\Delta)$. Dann gilt:*

(i) Ist $\pi(f)$ reduziert, dann ist auch $\rho\,(\pi(f))$ reduziert.

(ii) Alle reduzierten Formen äquivalent zu $\pi(f)$ lassen sich durch wiederholte Anwendung von ρ auf eine reduzierte Form $\pi(f_1) \sim \pi(f)$ berechnen und deren Anzahl ist endlich.

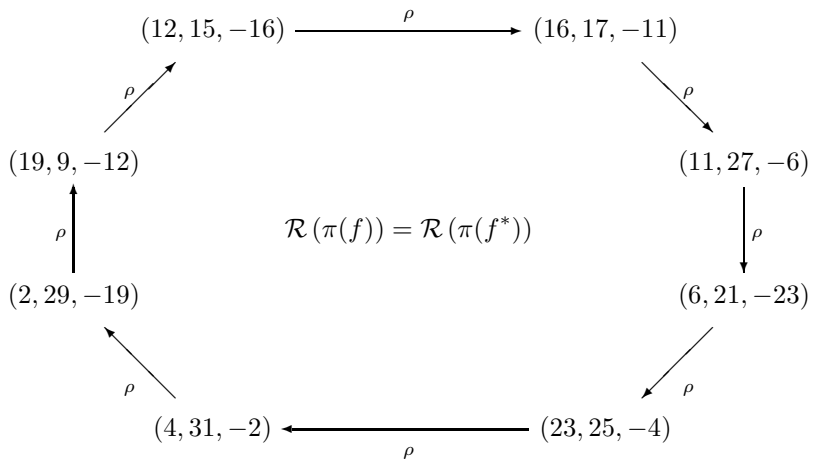
Beweis: Folgt aus Satz 2.3.10. □

2.3.11 Bemerkung Es sei $f \in \mathrm{Form}\,(\Delta)$. Die Zyklen reduzierter Formen vereinfachen sich wie folgt:

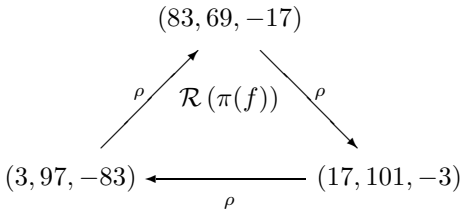
(i) Für
$$\mathcal{R}\,(f^*) \neq \mathcal{R}\,(f) = (f_1, \ldots, f_k)$$
werden beide Zyklen zu einem:
$$\mathcal{R}\,(\pi(f)) = \mathcal{R}\,(\pi(f^*)) = (\pi(f_1), \ldots, \pi(f_k)).$$

(ii) Für
$$\mathcal{R}\,(f^*) = \mathcal{R}\,(f) = (f_1, \ldots, f_k, f_1^*, \ldots, f_k^*)$$
halbiert sich der Zyklus:
$$\mathcal{R}\,(\pi(f)) = (\pi(f_1), \ldots, \pi(f_k)).$$

2.3.12 Beispiel Dieses Beispiel zeigt, wie sich die Zyklen aus Beispiel 2.3.6 in $\mathrm{Form}_*(\Delta)$ vereinfachen. Wir schreiben dabei statt $\pi(f)$ immer den positiven Vertreter aus $\pi(f)$.
$f = (12, 15, -16) \in \mathrm{Form}(993)$:



$f = (83, 69, -17) \in \mathrm{Form}(10405)$:



Kapitel 3

Zahlkörper

Dieses Kapitel wiederholt zunächst die Grundlagen über Zahlkörper und deren Ordnungen, Ideale und Klassengruppen. In Abschnitt 3.3 betrachten wir den Zusammenhang zwischen Idealen und Formen, um die Theorie der Reduktion auch für Ideale zu nutzen. In Abschnitt 3.4 zeigen wir, wie man effizient mit Idealen bzw. deren Klassen rechnen kann.

3.1 Zahlkörper und Ordnungen

3.1.1 Definition Es sei $D \in \mathbb{Z}, D \neq 1$ quadratfrei, das $p^2 \nmid D \ \ \forall\ p \in \mathbb{P}$. Dann heißt

$$K := \mathbb{Q}\left(\sqrt{D}\right) := \left\{a + b\sqrt{D} \mid a, b \in \mathbb{Q}\right\}$$

quadratischer Zahlkörper.

$$\Delta := \Delta(K) := \begin{cases} D & \text{für } D \equiv 1 \bmod 4, \\ 4D & \text{für } D \equiv 2, 3 \bmod 4. \end{cases}$$

heißt **Diskriminante** von K. Im Folgenden ist stets $D \in \mathbb{Z}$ eine quadratfreie Zahl und Δ die Diskriminante von $\mathbb{Q}\left(\sqrt{D}\right)$. Statt $\mathbb{Q}\left(\sqrt{D}\right)$ werden wir nun auch $\mathbb{Q}\left(\sqrt{\Delta}\right)$ schreiben, da Δ den Zahlkörper eindeutig definiert.

3.1.2 Definition Es sei K ein quadratischer Zahlkörper mit Diskriminante Δ. Dann heißt der Ring

$$\mathcal{O}_K := \mathcal{O}_\Delta := \left\{ a + b\frac{\Delta + \sqrt{\Delta}}{2} \;\middle|\; a, b \in \mathbb{Z} \right\} \subseteq \mathbb{Q}\left(\sqrt{\Delta}\right)$$

Maximalordnung von K bzw. Δ.

3.1.3 Bemerkung Es sind 1 und $\frac{\Delta+\sqrt{\Delta}}{2}$ linear unabhängig über $\mathbb{Q}$, die obige Darstellung von Elementen aus $\mathcal{O}_\Delta$ ist also eindeutig.

3.1.4 Definition Ein quadratischer Zahlkörper $\mathbb{Q}\left(\sqrt{\Delta}\right)$, seine Maximalordnung $\mathcal{O}_\Delta$ und seine Diskriminante Δ heißen

1. **reellquadratisch**, falls $\Delta > 0$.
2. **imaginärquadratisch**, falls $\Delta < 0$.

Bevor wir einen wichtigen Satz über die Darstellung von Idealen in $\mathcal{O}_\Delta$ beweisen, führen wir eine wichtige Funktion ein:

3.1.5 Definition Es sei $\sigma : \mathbb{Q}\left(\sqrt{D}\right) \to \mathbb{Q}\left(\sqrt{D}\right) : x + y\sqrt{D} \mapsto x - y\sqrt{D}$ das nichttriviale Element der Automorphismengruppe von $\mathbb{Q}\left(\sqrt{D}\right)/\mathbb{Q}$. Es sei $\alpha = x + y\sqrt{D} \in \mathbb{Q}\left(\sqrt{D}\right)$ mit $x, y \in \mathbb{Q}$. Dann heißt

$$\mathrm{N}(\alpha) := \alpha\sigma(\alpha) = \left(x + y\sqrt{D}\right)\left(x - y\sqrt{D}\right) = x^2 - y^2 D.$$

Norm von α. Diese Abbildung ist wegen Bemerkung 3.1.3 wohldefiniert.

3.1.6 Lemma *Es sei $\mathfrak{a}$ ein Ideal von $\mathcal{O}_\Delta$. Dann ist der Faktorring $\mathcal{O}_\Delta/\mathfrak{a}$ endlich.*

Beweis: [Nar74, Satz 16.9.1, S. 437] □

3.1.7 Definition Es sei $\mathfrak{a}$ ein Ideal von $\mathcal{O}_\Delta$.

$$\mathrm{N}(\mathfrak{a}) := [\mathcal{O}_\Delta : \mathfrak{a}] = \sharp(\mathcal{O}_\Delta/\mathfrak{a})$$

heißt **Norm** von $\mathfrak{a}$.

3.1.8 Lemma *Es seien $\alpha, \beta \in \mathbb{Q}\left(\sqrt{\Delta}\right)$ und $\mathfrak{a}, \mathfrak{b}$ Ideale in $\mathcal{O}_\Delta$. Dann gilt:*

(i) $\mathrm{N}(\alpha \cdot \beta) = \mathrm{N}(\alpha) \cdot \mathrm{N}(\beta)$

(ii) $\mathrm{N}(\mathfrak{a} \cdot \mathfrak{b}) = \mathrm{N}(\mathfrak{a}) \cdot \mathrm{N}(\mathfrak{b})$

(iii) $\mathrm{N}(\alpha \cdot \mathfrak{a}) = |\mathrm{N}(\alpha)| \cdot \mathrm{N}(\mathfrak{a})$

(iv) $\mathrm{N}((\alpha)) = |\mathrm{N}(\alpha)|$.

Beweis: [Nar74, Satz 16.9.3, 16.9.4, S. 437] □

3.1.9 Satz *Es sei* $\{0\} \neq \mathfrak{a} \subseteq \mathcal{O}_\Delta$. *Dann gilt:* $\mathfrak{a}$ *ist ein Ideal* $\Longleftrightarrow \dot{\exists}\, a, m \in \mathbb{N}, b \in \mathbb{Z}$ *mit*

$$\mathfrak{a} = m\left(a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}\right),$$

$\frac{b^2-\Delta}{4a} \in \mathbb{Z}$ *und* $s\left(\left(a, b, \frac{b^2-\Delta}{4a}\right)\right) = 0$ *(s wie in Definition 2.2.2). Es gilt weiterhin*

$$\mathrm{N}(\mathfrak{a}) = m^2 a.$$

Beweis:

„⇒“ Es sei $\mathfrak{a}$ ein Ideal. Nach Proposition 5.2.1 in [Coh95] kann $\mathfrak{a}$ durch eine Matrix

$$A := \begin{pmatrix} x & y \\ 0 & z \end{pmatrix} \text{ mit } x, y, z \in \mathbb{Z}, z \mid x, y \text{ und } x, z > 0$$

in Hermite-Normalform bezüglich einer Basis $\{1, \omega\}$ dargestellt werden, das heißt

$$x\mathbb{Z} + (y + z\omega)\,\mathbb{Z}.$$

Dabei sind x, z eindeutig, y ist eindeutig modulo x. Für

$$\omega = \frac{\Delta + \sqrt{\Delta}}{2}$$

folgt damit

$$\begin{aligned} \mathfrak{a} &= x\mathbb{Z} + (y + z\omega)\,\mathbb{Z} \\ &= x\mathbb{Z} + \left(y + z\frac{\Delta+\sqrt{\Delta}}{2}\right)\mathbb{Z} \\ &= z \cdot \left(\frac{x}{z}\mathbb{Z} + \frac{\left(\frac{2y}{z} + \Delta\right) + \sqrt{\Delta}}{2}\mathbb{Z}\right). \end{aligned}$$

Es sei nun $a := \frac{x}{z}$, $b := \frac{2y}{z} + \Delta$ und $m := z$. Nach Satz 16.9.1 in [Nar74] gilt

$$\mathrm{N}(\mathfrak{a}) = |\det A|,$$

also

$$\mathrm{N}\left(m\left(a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}\right)\right) = xz = a \cdot m^2.$$

Wir haben bis jetzt: $a, m > 0$ und $b \in \mathbb{Z}$. a und m sind dabei eindeutig, da x und y eindeutig waren, b ist eindeutig modulo $2a$, es gibt also genau ein b,

welches $s\left(\left(a, b, \frac{b^2-\Delta}{4a}\right)\right) = 0$ erfüllt. Dazu bleibt zu zeigen, daß $\frac{b^2-\Delta}{4a} \in \mathbb{Z}$. Da $\mathfrak{a}$ ein Ideal ist, gilt

$$\omega \cdot \frac{b+\sqrt{\Delta}}{2} \in \mathfrak{a}.$$

Es existieren also eindeutige $u, v \in \mathbb{Z}$ mit

$$\begin{aligned} ua + v\frac{b+\sqrt{\Delta}}{2} &= \omega \cdot \frac{b+\sqrt{\Delta}}{2} && (3.1)\\ &= \frac{\Delta+\sqrt{\Delta}}{2} \cdot \frac{b+\sqrt{\Delta}}{2} && (3.2)\\ &= \frac{1}{4}\left(\Delta b + \Delta + (b+\Delta)\sqrt{\Delta}\right) && (3.3)\\ &= \frac{b+\Delta}{2} \cdot \frac{b+\sqrt{\Delta}}{2} + \frac{\Delta-b^2}{4} && (3.4) \end{aligned}$$

Damit ist $\frac{\Delta-b^2}{4a} = u \in \mathbb{Z}$.

„⇐“ Es sei $\mathfrak{a} = m\left(a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}\right)$ eine wie in der Voraussetzung beschriebene Menge. Um einzusehen, daß $\mathfrak{a}$ ein Ideal ist, genügt es zu zeigen, daß ωa und $\omega\frac{b+\sqrt{\Delta}}{2} \in \mathfrak{a}$. Es ist

$$\omega a = \frac{a\Delta + a\sqrt{\Delta}}{2} = \left(\frac{\Delta-b}{2}\right) \cdot a + a \cdot \frac{b+\sqrt{\Delta}}{2} \in \mathfrak{a},$$

da $4 \mid \Delta - b^2$ also $2 \mid \Delta - b$ und damit $a, \frac{\Delta-b}{2} \in \mathbb{Z}$.
Wie in Gleichung (3.1) gesehen, gilt weiterhin:

$$\omega \cdot \frac{b+\sqrt{\Delta}}{2} = \frac{\Delta-b^2}{4a} \cdot a + \frac{b+\Delta}{2} \cdot \frac{b+\sqrt{\Delta}}{2} \in \mathfrak{a}$$

wegen $\frac{\Delta-b^2}{4a}$ und $\frac{b+\Delta}{2} \in \mathbb{Z}$.

□

3.1.10 Definition Es sei $\{0\} \neq \mathfrak{a} \subseteq \mathcal{O}_\Delta$ ein Ideal, $0 \neq \alpha \in K$. Dann heißt $\alpha \cdot \mathfrak{a}$ **gebrochenes Ideal** von $\mathcal{O}_\Delta$. Für

$$\mathfrak{b} = \alpha\left(a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}\right)$$

gemäß Satz 3.1.9 heißt $\alpha\,(a, b)$ **Standardrepräsentation** von $\mathfrak{b}$. $\mathfrak{b}$ heißt **primitiv**, falls $\alpha = 1$. Die Menge der primitiven Ideale wollen wir mit P_Δ bezeichnen. Im Folgenden wird mit

$$\mathfrak{a} = a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z} = (a, b)$$

immer die eindeutige Darstellung eines primitiven Ideals $\mathfrak{a}$ gemäß Satz 3.1.9 gemeint.

3.1.11 Beispiel Für $\Delta < 0$ ist $\mathcal{O}_\Delta = (1, \Delta \bmod 2)$.

Ideale werden später nur noch als Vertreter ihrer Klassengruppe angesehen (siehe Abschnitt 3.2). Daher spielen Faktoren aus $K \setminus \{0\}$ keine Rolle, es reicht also eine Darstellung (a, b) für primitive Ideale. Auch in den späteren Algorithmen (z. B. `IdealProduct`, `IdealInverse`) werden wir aus Gründen der Effizienz mögliche auftretende Faktoren vernachlässigen, die Algorithmen müssen also für reine Idealarithmetik leicht modifiziert werden. Wenn nicht anders angegeben, sind im Folgenden alle Ideale primitiv.
Ein Ideal gehört natürlich immer zu einer Ordnung, es ist also immer mit einer Diskriminante verbunden. Da diese aber für unsere späteren Algorithmen immer die gleiche ist, können wir sie fest in diese einbauen, oder zentral irgendwo speichern. Dann gilt:

$$\operatorname{size}(\mathfrak{a}) = \operatorname{size}(a) + \operatorname{size}(b).$$

3.2 Klassengruppe und Regulator

3.2.1 Satz *Die Menge der gebrochenen Ideale* I_Δ *bildet bezüglich der Idealmultiplikation eine abelsche Gruppe mit Einselement* $\mathcal{O}_\Delta$*. Die Menge der gebrochenen Hauptideale* $\mathrm{H}_\Delta = \{(\alpha) \mid 0 \neq \alpha \in K\}$ *ist darin eine Untergruppe.*

Beweis: [PZ89, S. 287] □

3.2.2 Definition Die Faktorgruppe

$$\mathrm{Cl}(\Delta) := \mathrm{I}_\Delta / \mathrm{H}_\Delta = \{[\mathfrak{a}] \mid \mathfrak{a} \in \mathrm{I}_\Delta\}$$

heißt **Klassengruppe** und deren Ordnung **Klassenzahl**:

$$\mathrm{h}(\Delta) := \sharp \mathrm{Cl}(\Delta).$$

Zwei Ideale der gleichen Nebenklasse heißen **äquivalent**.

3.2.3 Satz *Die Klassenzahl eines Zahlkörpers ist endlich.*

Beweis: [Mar77, Theorem 35, S.130] □

3.2.4 Definition Die Menge

$$\mathcal{O}_\Delta^\times := \{\alpha \in \mathcal{O}_\Delta \mid \exists\, \beta \in \mathcal{O}_\Delta : \alpha \cdot \beta = 1\}$$

ist eine multiplikative Gruppe, die sogenannte **Einheitengruppe** von $\mathcal{O}_\Delta$.

3.2.5 Lemma *In imaginärquadratischen Zahlkörpern sehen die Einheitengruppen wie folgt aus:*

(i) $\mathcal{O}_\Delta{}^\times = \{\pm 1, \frac{\pm 1 \pm i\sqrt{3}}{2}\}$ *für* $\Delta = -3$.

(ii) $\mathcal{O}_\Delta{}^\times = \{\pm 1, \pm i\}$ *für* $\Delta = -4$.

(iii) $\mathcal{O}_\Delta{}^\times = \{\pm 1\}$ *für* $\Delta < -4$.

Der Fall $\Delta \in \{-1, -2\}$ *kann nicht auftreten, da* $\Delta \equiv 0, 1 \bmod 4$.

Beweis: [Has64, 16.4.VIIIa] □

3.2.6 Satz *In reellquadratischen Zahlkörpern gilt für die Einheitengruppe der Maximalordnung:*

$$\mathcal{O}_\Delta{}^\times \cong \{\pm 1\} \times \mathbb{Z} \cong \{\pm 1\} \times \langle \varepsilon_\Delta \rangle.$$

Beweis: [Has64, 16.4.VIIIb] □

3.2.7 Definition Ein Erzeuger $\varepsilon_\Delta > 1$ des freien Anteils von $\mathcal{O}_\Delta^\times$ ist eindeutig und heißt **Grundeinheit**. $\operatorname{Reg}(\Delta) := \ln \varepsilon_\Delta$ heißt **Regulator** von $\mathcal{O}_\Delta$.
Im imaginärquadratischen Fall definiert man $\operatorname{Reg}(\Delta) := 1$.

3.2.8 Satz von Brauer-Siegel *Für eine unendliche Familie quadratischer Zahlkörper mit zugehörigen Diskriminanten* Δ *gilt:*

$$\lim_{|\Delta| \to \infty} \frac{\ln\left(\sqrt{|\Delta|}\right)}{\ln\left(\mathrm{h}(\Delta) \operatorname{Reg}(\Delta)\right)} = 1.$$

Schreibweise:

$$\ln\left(\sqrt{|\Delta|}\right) \sim \ln\left(\mathrm{h}(\Delta) \operatorname{Reg}(\Delta)\right).$$

Das heißt, $\forall\, \varepsilon > 0\ \exists\, \Delta_0 > 0$*:*

$$\sqrt{|\Delta|}^{1-\varepsilon} \leq \mathrm{h}(\Delta) \operatorname{Reg}(\Delta) \leq \sqrt{|\Delta|}^{1+\varepsilon} \quad \forall\, |\Delta| > \Delta_0. \tag{3.5}$$

Beweis: [Lan91] □

3.2.9 Korollar *Im Falle imaginärquadratischer Zahlkörper gilt*

$$\ln\left(\mathrm{h}(\Delta)\right) \sim \ln\left(\sqrt{|\Delta|}\right).$$

3.2.10 Satz *Für $\Delta < 0$ gilt für den Durchschnitt τ von $\frac{\mathrm{h}(\Delta)}{\sqrt{|\Delta|}}$: $\tau \approx 0{,}461559$.*

Beweis: [Coh95, Abschnitt 5.10.1] □

3.2.11 Satz *Für $-2^{4600} < \Delta < 0$ gilt unter Annahme der verallgemeinerten Riemannschen Vermutung (siehe z. B. [KV92])*

$$\mathrm{h}(\Delta) > \frac{\sqrt{|\Delta|}}{2^6}.$$

Beweis: [Ham02, Satz 5.1.4, Seite 57] □

3.2.12 Satz *Es sei $\Delta > 0$. Unter Annahme der verallgemeinerten Riemannschen Vermutung existiert ein $\Delta_0 \in \mathbb{N}$:*

$$\frac{\sqrt{\Delta}}{6 \ln \Delta} \leq \mathrm{h}(\Delta) \operatorname{Reg}(\Delta) \leq \sqrt{\Delta} \ln \Delta \quad \forall\ \Delta > \Delta_0.$$

Beweis: Folgt aus Lemma 3.3 und 3.5 in [BTW95]. □

Es gibt leider noch nicht sehr viele bewiesene Aussagen über $\mathrm{h}(\Delta)$. In der weiteren Arbeit müssen wir uns deshalb zunehmend auf Vermutungen stützen, die durch zahlreiche Beispiele begründet sind.

3.3 Reduzierte Ideale

In diesem Abschnitt wollen wir erklären, wie man den Reduktionsalgorithmus für Formen auf Ideale übertragen kann. Dazu wollen wir uns als erstes ansehen, wie Ideale bzw. Idealklassen und Formen zusammenhängen. Dazu benötigen wir zunächst ein

3.3.1 Lemma *Es sei $\{0\} \neq \left(a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}\right) \subseteq \mathcal{O}_\Delta$ ein Ideal. Dann gilt für $c := \frac{b^2-\Delta}{4a}$:*

$$g := \mathrm{ggT}(a, b, c) = 1.$$

Beweis: Es gilt:

$$g^2 \mid b^2 - 4ac = \Delta.$$

Daher kommt neben $g = 1$ nur $g = 2$ im Fall $D = \frac{\Delta}{4} \equiv 2, 3 \bmod 4$ in Frage. Es sei also $D \equiv 2, 3 \bmod 4$ und $g = 2$. Damit sind $a \equiv b \equiv c \equiv 0 \bmod 2$ und

$$2 \mid c = \frac{b^2 - \Delta}{4a} \Longrightarrow b^2 \equiv \Delta \bmod 16.$$

Wegen $D \equiv 2, 3 \bmod 4$, folgt $\Delta = 4D \equiv 8, 12 \bmod 16$, also auch

$$b^2 = 4\left(\frac{b}{2}\right)^2 \equiv 8, 12 \bmod 16$$

und damit

$$\left(\frac{b}{2}\right)^2 \equiv 2, 3 \bmod 4,$$

was ein Widerspruch ist, da $z^2 \equiv 0, 1 \bmod 4 \ \ \forall\ z \in \mathbb{Z}$. □

3.3.2 Satz *Es ist*

$$\psi : \mathrm{P}_\Delta \to \{ f \in \mathrm{Form}\,(\Delta) \mid f \ \textit{normal} \} : \left(a\mathbb{Z} + \frac{b + \sqrt{\Delta}}{2}\mathbb{Z} \right) \mapsto ax^2 + bxy + \frac{b^2 - \Delta}{4a} y^2$$

eine injektive Abbildung.

Beweis: Die Wohldefiniertheit ist klar wegen Satz 3.1.9 und Lemma 3.3.1. Die Injektivität folgt ebenfalls aus Satz 3.1.9. □

3.3.3 Bemerkung Aus Satz 3.1.9 folgt weiterhin:

(i) Für $\Delta < 0$ ist ψ bijektiv.

(ii) Für $\Delta > 0$ ist $\psi\,(\mathrm{P}_\Delta)$ die Menge der normalen indefiniten Formen f mit $\operatorname{sign} f > 0$, also gerade die Hälfte aller indefiniten Formen. Das Bild von $\psi\,(\mathrm{P}_\Delta)$ unter $\mathrm{SL}\,(2, \mathbb{Z})$ ist wegen Lemma 2.3.2 die Menge aller indefiniten Formen.

3.3.4 Lemma *Es sei* $\mathfrak{a} = a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}$. *Dann gilt*

$$\psi\,(\mathfrak{a}) = \frac{\mathrm{N}\left(ax + \frac{b+\sqrt{\Delta}}{2} y\right)}{\mathrm{N}\,(\mathfrak{a})}.$$

Beweis: Nach Satz 3.1.9 ist $\mathrm{N}(\mathfrak{a}) = a$ und man erhält:

$$\begin{aligned}
\frac{\mathrm{N}\left(ax + \frac{b+\sqrt{\Delta}}{2}y\right)}{\mathrm{N}(\mathfrak{a})} &= \frac{\mathrm{N}\left(\left(ax + \frac{b}{2}y\right) + \frac{\sqrt{\Delta}}{2}y\right)}{a} \\
&= \frac{\left(ax + \frac{b}{2}y\right)^2 - \frac{\Delta}{4}y^2}{a} \\
&= \frac{a^2x^2 + \frac{b^2}{4}y^2 + abxy - \frac{\Delta}{4}y^2}{a} \\
&= ax^2 + bxy + \frac{b^2 - \Delta}{4a}y^2 \\
&= \psi\left(a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}\right) \\
&= \psi(\mathfrak{a}).
\end{aligned}$$

□

3.3.5 Lemma *Es sei* $\mathfrak{a} = a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}$ *ein Ideal in* $\mathcal{O}_\Delta$ *und* $\alpha, \beta \in \mathcal{O}_\Delta$ *mit* $\mathfrak{a} = \alpha\mathbb{Z} + \beta\mathbb{Z}$. *Es sei weiterhin* $M = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathbb{Z}^{2\times 2}$ *die unimodulare Matrix mit*

$$\begin{pmatrix} \alpha \\ \beta \end{pmatrix} = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \begin{pmatrix} a \\ \frac{b+\sqrt{\Delta}}{2} \end{pmatrix}.$$

Dann sind äquivalent:

(i) $\det M = 1$

(ii) $\psi(\mathfrak{a}) \sim \frac{\mathrm{N}(\alpha x+\beta y)}{\mathrm{N}(\mathfrak{a})}$

(iii) $\frac{\alpha\sigma(\beta)-\beta\sigma(\alpha)}{\sqrt{\Delta}} < 0$

Beweis: Die Behauptungen ergeben sich aus folgenden zwei Beobachtungen:

(i) $\Leftrightarrow$ (ii) Es gilt:

$$\begin{aligned}
\frac{\mathrm{N}(\alpha x + \beta y)}{\mathrm{N}(\mathfrak{a})} &= \frac{\mathrm{N}\left(\left(ra + s\frac{b+\sqrt{\Delta}}{2}\right)x + \left(ta + u\frac{b+\sqrt{\Delta}}{2}\right)y\right)}{\mathrm{N}(\mathfrak{a})} \\
&= \frac{\mathrm{N}\left(a(rx+ty) + \frac{b+\sqrt{\Delta}}{2}(sx+uy)\right)}{\mathrm{N}(\mathfrak{a})}
\end{aligned}$$

$$= \psi(\mathfrak{a})(rx+ty, sx+uy).$$

Dabei ist die letzte Zeile als Transformation der Form $\psi(\mathfrak{a})$ mittels $\begin{pmatrix} r & t \\ s & u \end{pmatrix}$ gemäß Definition 2.1.5 zu verstehen.

(i) $\Leftrightarrow$ (iii) Es gilt:

$$\begin{aligned}
\alpha\sigma(\beta) - \beta\sigma(\alpha) &= \left(ra + s\frac{b+\sqrt{\Delta}}{2}\right)\left(ta + u\frac{b-\sqrt{\Delta}}{2}\right) \\
&\quad - \left(ta + u\frac{b+\sqrt{\Delta}}{2}\right)\left(ra + s\frac{b-\sqrt{\Delta}}{2}\right) \\
&= rua\frac{b-\sqrt{\Delta}}{2} + sta\frac{b+\sqrt{\Delta}}{2} - sta\frac{b-\sqrt{\Delta}}{2} - rua\frac{b+\sqrt{\Delta}}{2} \\
&= a\frac{b-\sqrt{\Delta}}{2}(ru-st) - a\frac{b+\sqrt{\Delta}}{2}(ru-st) \\
&= \det Ma\left(\frac{b-\sqrt{\Delta}}{2} - \frac{b+\sqrt{\Delta}}{2}\right) \\
&= \det Ma\left(-\sqrt{\Delta}\right).
\end{aligned}$$

□

Als erstes wollen wir untersuchen, wie die Äquivalenz von Formen mit der von Idealen zusammenhängt. Dazu benötigen wir die folgende

3.3.6 Definition Es seien $\mathfrak{a}, \mathfrak{b} \neq \{0\}$ Ideale in $\mathcal{O}_\Delta$. Dann heißen $\mathfrak{a}$ und $\mathfrak{b}$ **äquivalent im engeren Sinne** ($\mathfrak{a} \simeq \mathfrak{b}$), wenn es ein $\gamma \in K$ gibt mit $\mathfrak{b} = (\gamma)\mathfrak{a}$ und $\mathrm{N}(\gamma) > 0$. Dies ist eine Äquivalenzrelation. Die entsprechende Faktorgruppe wollen wir mit $\mathrm{Cl}^+(\Delta)$ bezeichnen, deren Elemente mit $[\mathfrak{a}]^+$.

3.3.7 Bemerkung Es ist klar, daß $\mathfrak{a} \simeq \mathfrak{b} \Longrightarrow \mathfrak{a} \sim \mathfrak{b}$.

3.3.8 Satz *Es seien* $\mathfrak{a}, \mathfrak{b} \in P_\Delta$. *Dann gilt:*

$$\mathfrak{a} \simeq \mathfrak{b} \Longleftrightarrow \psi(\mathfrak{a}) \sim \psi(\mathfrak{b}).$$

Beweis:

„⇒ “ Es seien $\mathfrak{a} = a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}, \mathfrak{b} \in P_\Delta$ mit $\mathfrak{a} \simeq \mathfrak{b}$. Das heißt,

$$\exists\, \gamma \in K : \mathfrak{b} = (\gamma)\,\mathfrak{a} = \left(\gamma a\mathbb{Z} + \gamma\frac{b+\sqrt{\Delta}}{2}\mathbb{Z}\right) \text{ und } \mathrm{N}(\gamma) > 0.$$

Um Lemma 3.3.5 anwenden zu können, betrachten wir:

$$\begin{aligned}
\frac{(\gamma a)\,\sigma\left(\gamma\frac{b+\sqrt{\Delta}}{2}\right) - \left(\gamma\frac{b+\sqrt{\Delta}}{2}\right)\sigma(\gamma a)}{\sqrt{\Delta}} &= \frac{\gamma\sigma(\gamma)\left(a\sigma\left(\frac{b+\sqrt{\Delta}}{2}\right) - \left(\frac{b+\sqrt{\Delta}}{2}\right)\sigma(a)\right)}{\sqrt{\Delta}} \\
&= \frac{\mathrm{N}(\gamma)\,a\left(\sigma\left(\frac{b+\sqrt{\Delta}}{2}\right) - \left(\frac{b+\sqrt{\Delta}}{2}\right)\right)}{\sqrt{\Delta}} \\
&= \frac{\mathrm{N}(\gamma)\,a\left(-\sqrt{\Delta}\right)}{\sqrt{\Delta}} \\
&= -\mathrm{N}(\gamma)\,a \\
&< 0,
\end{aligned}$$

da $\mathrm{N}(\gamma) > 0$. Daher ist nach Lemma 3.3.4 und 3.3.5:

$$\begin{aligned}
\psi(\mathfrak{b}) &\sim \frac{\mathrm{N}\left(\gamma a x + \gamma\frac{b+\sqrt{\Delta}}{2}y\right)}{\mathrm{N}((\gamma)\,\mathfrak{a})} \\
&= \frac{\mathrm{N}(\gamma)}{\mathrm{N}((\gamma))} \cdot \frac{\mathrm{N}\left(ax + \frac{b+\sqrt{\Delta}}{2}y\right)}{\mathrm{N}(\mathfrak{a})} \\
&= \frac{\mathrm{N}(\gamma)}{|\,\mathrm{N}(\gamma)\,|} \cdot \frac{\mathrm{N}\left(ax + \frac{b+\sqrt{\Delta}}{2}y\right)}{\mathrm{N}(\mathfrak{a})} \\
&= \psi(\mathfrak{a}),
\end{aligned}$$

da $\mathrm{N}(\gamma) > 0$.

„⇐ “ Es seien $\mathfrak{a} = \left(a\mathbb{Z} + \frac{b+\sqrt{\Delta}}{2}\mathbb{Z}\right)$ und $\mathfrak{b} = \left(\tilde{a}\mathbb{Z} + \frac{\tilde{b}+\sqrt{\Delta}}{2}\mathbb{Z}\right) \in P_\Delta$ mit $\psi(\mathfrak{a}) \sim \psi(\mathfrak{b})$. Das heißt:

$$\exists\, M = \begin{pmatrix} r & s \\ t & u \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) : \psi(\mathfrak{b})\,M = \psi(\mathfrak{a}).$$

Also

$$\tilde{a} = ar^2 + brt + ct^2$$

$$\tilde{b} \;=\; 2ars + b\,(ru+st) + 2ctu.$$

Wegen $ru - st = \det M = 1$ ist dann

$$\begin{aligned}
\mathfrak{b} &= \tilde{a}\mathbb{Z} + \frac{\tilde{b}+\sqrt{\Delta}}{2}\mathbb{Z} \\
&= \left(ar^2+brt+ct^2\right)\mathbb{Z} + \frac{(2ars+b\,(ru+st)+2ctu)+\sqrt{\Delta}}{2}\mathbb{Z} \\
&= \frac{4a^2r^2+4abrt+(b^2-\Delta)\,t^2}{4a}\mathbb{Z} \\
&\quad + \frac{2ars+2tuc+b\,(ru+st)+(ru-st)\sqrt{\Delta}}{2}\mathbb{Z} \\
&= \frac{(2ar+tb)^2-t^2\Delta}{4a}\mathbb{Z} \\
&\quad + \frac{2ars+tu\frac{b^2-\Delta}{2a}+ru\left(b+\sqrt{\Delta}\right)+st\left(b-\sqrt{\Delta}\right)}{2}\mathbb{Z} \\
&= \frac{(2ar+tb)^2-t^2\Delta}{4a}\mathbb{Z} \\
&\quad + \frac{4a^2rs+tu\,(b^2-\Delta)+2aru\left(b+\sqrt{\Delta}\right)+2ast\left(b-\sqrt{\Delta}\right)}{4a}\mathbb{Z} \\
&= \frac{(2ar+tb)^2-t^2\Delta}{4a}\mathbb{Z} + \frac{\left(2ar+t\left(b-\sqrt{\Delta}\right)\right)\left(2as+u\left(b+\sqrt{\Delta}\right)\right)}{4a}\mathbb{Z} \\
&= \frac{(2ar+tb)-t\sqrt{\Delta}}{2a}\left(\frac{(2ar+tb)+t\sqrt{\Delta}}{2}\mathbb{Z} + \frac{2as+u\left(b+\sqrt{\Delta}\right)}{2}\mathbb{Z}\right) \\
&= \left(r+t\frac{b-\sqrt{\Delta}}{2a}\right)\left(\left(ra+t\frac{b+\sqrt{\Delta}}{2}\right)\mathbb{Z} + \left(sa+u\frac{b+\sqrt{\Delta}}{2}\right)\mathbb{Z}\right) \\
&= \left(r+t\frac{b-\sqrt{\Delta}}{2a}\right)\cdot\mathfrak{a},
\end{aligned}$$

denn

$$\begin{pmatrix} ra+t\frac{b+\sqrt{\Delta}}{2} \\ sa+u\frac{b+\sqrt{\Delta}}{2} \end{pmatrix} = \begin{pmatrix} r & t \\ s & u \end{pmatrix}\begin{pmatrix} a \\ \frac{b+\sqrt{\Delta}}{2} \end{pmatrix}$$

und

$$\det\begin{pmatrix} r & t \\ s & u \end{pmatrix} = ru - st = \det M = 1.$$

Mit

$$\begin{aligned}
\mathrm{N}\left(r+t\frac{b-\sqrt{\Delta}}{2a}\right) &= \mathrm{N}\left(\left(r+\frac{tb}{2a}\right)-\frac{t\sqrt{\Delta}}{2a}\right)\\
&= \left(r+\frac{tb}{2a}\right)^2-\frac{t^2\Delta}{4a^2}\\
&= r^2+\frac{t^2b^2}{4a^2}+\frac{rtb}{a}-\frac{t^2\Delta}{4a^2}\\
&= \left(ar^2+brt+\frac{b^2-\Delta}{4a}t^2\right)a^{-1}\\
&= \left(ar^2+brt+ct^2\right)a^{-1}\\
&= \tilde{a}a^{-1}\\
&> 0,
\end{aligned}$$

da $\tilde{a}, a > 0$ nach Voraussetzung, folgt schließlich

$$\mathfrak{b} = \left(r+t\frac{b-\sqrt{\Delta}}{2a}\right)\cdot\mathfrak{a} \simeq \mathfrak{a}.$$

□

3.3.9 Korollar *ψ induziert eine Bijektion*

$$\psi_{\mathrm{Cl}} : \mathrm{Cl}^+(\Delta) \longrightarrow \mathrm{Cl}_{\mathrm{F}}(\Delta) : [\mathfrak{a}]^+ \longmapsto [\psi(\mathfrak{a})].$$

Beweis: Die Wohldefiniertheit und Injektivität folgt aus Satz 3.3.8. Die Surjektivität folgt aus Bemerkung 3.3.3. □

3.3.10 Satz *Es gilt*

$$\mathrm{Cl}(\Delta) \cong \begin{cases} \mathrm{Cl}^+(\Delta) & \text{für } \Delta < 0 \\ \mathrm{Cl}^+(\Delta) & \text{für } \Delta > 0 \text{ und } \mathrm{N}(\varepsilon_\Delta) = -1 \\ \mathrm{Cl}^+(\Delta)\,/\left(\left[\sqrt{\Delta}\right]\right) & \text{für } \Delta > 0 \text{ und } \mathrm{N}(\varepsilon_\Delta) = +1 \end{cases}$$

wobei $\cong$ als Isomorphie von Mengen zu verstehen ist. ε_Δ ist die Grundeinheit für den reellquadratischen Fall.

Beweis:

(i) Für $\Delta < 0$ ist $\mathrm{N}(\gamma) \geq 0 \ \ \forall\, \gamma \in \mathbb{Q}\left(\sqrt{\Delta}\right)$, also gilt $\mathfrak{a} \simeq \mathfrak{b} \Longleftrightarrow \mathfrak{a} \sim \mathfrak{b}$.

(ii) Für $\Delta > 0$ und $\mathrm{N}(\varepsilon_\Delta) = -1$ gilt: $\mathfrak{a} \sim \mathfrak{b} \Longrightarrow \ \exists\, \gamma \in \mathbb{Q}\left(\sqrt{\Delta}\right) : \mathfrak{a} = (\gamma)\,\mathfrak{b} = (\varepsilon_\Delta \gamma)\,\mathfrak{b}$ mit entweder $\mathrm{N}(\gamma) > 0$ oder $\mathrm{N}(\varepsilon_\Delta \gamma) > 0$, also folgt $\mathfrak{a} \simeq \mathfrak{b}$.

(iii) Es sei $\Delta > 0$ und $\mathrm{N}(\varepsilon_\Delta) = +1$. Ist $\varepsilon \in \mathcal{O}_\Delta^\times$, so gilt: $\exists\, k \in \mathbb{Z} : \varepsilon = \pm\varepsilon_\Delta^k$, also $\mathrm{N}(\varepsilon) = \mathrm{N}(\varepsilon_\Delta)^k = 1$. Es sei $\mathfrak{a} \sim \mathfrak{b}$. Wegen $\mathrm{N}\left(\sqrt{\Delta}\right) < 0$ ist damit $\mathfrak{b} \not\simeq \left(\sqrt{\Delta}\right)\mathfrak{b}$ also entweder $\mathfrak{a} \simeq \mathfrak{b}$ oder $\mathfrak{a} \simeq \left(\sqrt{\Delta}\right)\mathfrak{b}$ $\left(\text{d. h. } [\mathfrak{a}] = [\mathfrak{a}]^+ \,\dot\cup\, \left[\left(\sqrt{\Delta}\right)\mathfrak{a}\right]^+\right)$.

□

3.3.11 Definition Ein Ideal $\mathfrak{a} \in \mathrm{P}_\Delta$ heißt **reduziert**, wenn die Form $\psi(\mathfrak{a})$ reduziert ist.

3.3.12 Korollar *Jede Idealklasse* $[\mathfrak{a}]$ *eines imaginärquadratischen Zahlkörpers enthält ein eindeutig bestimmtes reduziertes Ideal* $\psi^{-1}(\texttt{FormReduce}(\psi(\mathfrak{a})))$. *Dieses ist effizient berechenbar.*

Beweis: Folgt aus Satz 2.2.11 und 3.3.8. □

Damit haben wir für $\Delta < 0$ die Reduktion von $\mathrm{Form}(\Delta)$ auf P_Δ übertragen, da ψ bijektiv ist und die Äquivalenzen respektiert. Für $\Delta > 0$ ist es ein wenig komplizierter, da ψ nicht surjektiv ist. Es liegen genau die Formen f mit $\operatorname{sign} f < 0$ nicht im Bild von ψ, aber deren Konjugierte. Wie wir in Abschnitt 2.2 gesehen haben, können wir f und f^* miteinander identifizieren. Dies ist sinnvoll wie folgendes Lemma zeigt.

3.3.13 Lemma *Es sei* $\Delta > 0$. *Die Abbildung*

$$\pi \circ \psi : \mathrm{P}_\Delta \longrightarrow \{\pi(f) \in \mathrm{Form}_*(\Delta) \mid f \textit{ normal}\}$$

ist bijektiv.

Beweis:

(i) $\pi \circ \psi$ ist injektiv: Es seien $\mathfrak{a} = (a_1, a_2), \mathfrak{b} = (b_1, b_2) \in \mathrm{P}_\Delta$. Dann gilt:

$$\begin{aligned}(\pi\circ\psi)(\mathfrak{a}) = (\pi\circ\psi)(\mathfrak{b}) &\Longleftrightarrow \psi(\mathfrak{a}) = \psi(\mathfrak{b}) \text{ oder } \psi(\mathfrak{a}) = \psi(\mathfrak{b})^* \\ &\Longleftrightarrow (a_1 = b_1 \text{ oder } a_1 = -b_1) \text{ und } (a_2 = b_2) \\ &\Longleftrightarrow \mathfrak{a} = \mathfrak{b},\end{aligned}$$

denn $a_1, b_1 > 0$.

(ii) $\pi \circ \psi$ ist surjektiv: Es sei $\pi(f) \in \mathrm{Form}_*(\Delta)$ normal, $f = (a,b,c) \in \mathrm{Form}(\Delta)$. Für $a > 0$ ist $(a,b) \in \mathrm{P}_\Delta$ und

$$(\pi \circ \psi)((a,b)) = \pi(f).$$

Für $a < 0$ ist $(-a,b) \in \mathrm{P}_\Delta$ und

$$(\pi \circ \psi)((-a,b)) = \pi(f^*) = \pi(f).$$

□

Wir wollen weiterhin zeigen, daß $\pi \circ \psi$ auch Äquivalenzen respektiert. Dazu schauen wir uns die Struktur von $\mathrm{Cl}^+(\Delta)$ noch einmal genauer an.

3.3.14 Lemma *Es sei $\Delta > 0$ und $\mathfrak{a} \in \mathrm{P}_\Delta$ reduziert. Dann gilt:*

$$\left(\sqrt{\Delta}\right) \cdot \mathfrak{a} \simeq \psi^{-1}\left(\rho\left(\psi\left(\mathfrak{a}\right)^*\right)\right).$$

Beweis: Es sei $\mathfrak{a} = (a,b)$ reduziert, $c = \frac{b^2-\Delta}{4a} < 0$ und $s = s((-c,-b,-a))$. Es folgt:

$$\begin{aligned}
\psi^{-1}\left(\rho\left(\psi\left(\mathfrak{a}\right)^*\right)\right) &= \psi^{-1}\left(\rho\left((-a,b,-c)\right)\right) \\
&= \psi^{-1}\left(\eta\left((-c,-b,-a)\right)\right) \\
&= \psi^{-1}\left(\left(-c,-b-2cs,-cs^2-bs-a\right)\right) \\
&= (-c)\,\mathbb{Z} + \frac{-b-2cs+\sqrt{\Delta}}{2}\mathbb{Z} \\
&= (-c)\,\mathbb{Z} + \left((-cs) + \frac{-b+\sqrt{\Delta}}{2}\right)\mathbb{Z} \\
&= (-c)\,\mathbb{Z} + \left(\frac{-b+\sqrt{\Delta}}{2}\right)\mathbb{Z} \\
&= \frac{\sqrt{\Delta}-b}{2a} \cdot \left(\frac{b+\sqrt{\Delta}}{2}\mathbb{Z} + a\mathbb{Z}\right) \\
&= \frac{\sqrt{\Delta}-b}{2a} \cdot \mathfrak{a} \\
&\simeq \left(\sqrt{\Delta}\right) \cdot \mathfrak{a},
\end{aligned}$$

da $\mathrm{N}\left(\sqrt{\Delta}\right), \mathrm{N}\left(\frac{\sqrt{\Delta}-b}{2a}\right) < 0$ □

3.3.15 Definition Es sei $\Delta > 0$, $\mathfrak{a} \in \mathrm{P}_\Delta$ reduziert. Dann heißt

$$\mathfrak{a}^* := \psi^{-1}\left(\rho\left(\psi\left(\mathfrak{a}\right)^*\right)\right)$$

konjugiertes Ideal zu $\mathfrak{a}$.

3.3.16 Korollar *Es sei $\Delta > 0$ und $\mathfrak{a} \in \mathrm{P}_\Delta$ reduziert. Dann gilt $\mathfrak{a} \sim \mathfrak{a}^*$ und*

$$\mathrm{N}(\varepsilon_\Delta) = 1 \Longleftrightarrow \mathfrak{a} \not\simeq \mathfrak{a}^* \Longleftrightarrow [\mathfrak{a}] = [\mathfrak{a}]^+ \dot\cup\, [\mathfrak{a}^*]^+.$$

Beweis: Folgt aus Lemma 3.3.14 und Satz 3.3.10. □

3.3.17 Beispiel In Beispiel 2.3.6 ist $\mathrm{N}(\varepsilon_{993}) = 1$ und $\mathrm{N}(\varepsilon_{10405}) = -1$.

3.3.18 Lemma *Es sei $\Delta > 0$. Die Abbildung $\pi \circ \psi$ respektiert Äquivalenzen.*

Beweis: Es seien $\mathfrak{a}, \mathfrak{b} \in \mathrm{P}_\Delta$. Wegen Lemma 2.3.2 existiert eine reduzierte Form $\psi(\mathfrak{c}) \sim \psi(\mathfrak{b})$ und damit $(\pi \circ \psi)(\mathfrak{c}) \sim (\pi \circ \psi)(\mathfrak{b})$. Es gilt weiterhin $\mathfrak{c} \sim \mathfrak{b}$ wegen Satz 3.3.8. Wir stellen zunächst fest, daß

$$\begin{aligned} \psi(\mathfrak{c})^* &\sim \rho\left(\psi(\mathfrak{c})^*\right) \\ &= \psi\left(\psi^{-1}\left(\rho\left(\psi(\mathfrak{c})^*\right)\right)\right) \\ &= \psi\left(\mathfrak{c}^*\right). \end{aligned}$$

Es folgt weiter wegen Satz 3.3.8:

$$\begin{aligned} \mathfrak{a} \sim \mathfrak{b} &\Longleftrightarrow \mathfrak{a} \in [\mathfrak{b}] = [\mathfrak{c}] = [\mathfrak{c}]^+ \cup [\mathfrak{c}^*]^+ \\ &\Longleftrightarrow \mathfrak{a} \simeq \mathfrak{c} \text{ oder } \mathfrak{a} \simeq \mathfrak{c}^* \\ &\Longleftrightarrow \psi(\mathfrak{a}) \sim \psi(\mathfrak{c}) \text{ oder } \psi(\mathfrak{a}) \sim \psi(\mathfrak{c})^* \\ &\Longleftrightarrow \pi(\psi(\mathfrak{a})) \sim \pi(\psi(\mathfrak{c})) \\ &\Longleftrightarrow (\pi \circ \psi)(\mathfrak{a}) \sim (\pi \circ \psi)(\mathfrak{b}). \end{aligned}$$

□

Nun definieren wir die entsprechenden Algorithmen, die die Bijektionen ψ bzw. $\pi \circ \psi$ realisieren. Aus Gründen der Übersichtlichkeit werden wir für $\Delta > 0$ von nun an statt $\pi(f) \in \mathrm{Form}_*\left(\Delta\right)$ nur noch f schreiben, wobei f der positive Vertreter von $\pi(f)$ ist.

Algorithmus `Ideal2Form`

Eingabe : Ein Ideal $\mathfrak{a} = (a, b)$ in Standardrepräsentation
Ausgabe: $\psi(\mathfrak{a}) \in \mathrm{Form}(\Delta)$ bzw. $(\pi \circ \psi)(\mathfrak{a}) \in \mathrm{Form}_*(\Delta)$

1: **return** $\left(a, b, \frac{b^2-\Delta}{4a}\right)$

Aufwand: $\mathcal{O}(\mathrm{size}(\mathfrak{a}))$

Algorithmus `Form2Ideal`

Eingabe : Eine normale primitive Form $f = (a, b, c) \in \mathrm{Form}(\Delta)$
Ausgabe: $\psi^{-1}(f) \in \mathrm{P}_\Delta$

1: **return** $(|a|, b)$

Aufwand: $\mathcal{O}(1)$

Mit diesen beiden Algorithmen läßt sich insbesondere der Reduktionsalgorithmus von Formen auf Ideale übertragen. Wir definieren für $\mathfrak{a} \in \mathrm{P}_\Delta$:

$$\eta(\mathfrak{a}) := \begin{cases} (\psi^{-1} \circ \eta \circ \psi)(\mathfrak{a}) & \text{für } \Delta < 0 \\ ((\pi \circ \psi)^{-1} \circ \eta \circ (\pi \circ \psi))(\mathfrak{a}) & \text{für } \Delta > 0 \end{cases}$$

und

$$\rho(\mathfrak{a}) := \begin{cases} (\psi^{-1} \circ \rho \circ \psi)(\mathfrak{a}) & \text{für } \Delta < 0 \\ ((\pi \circ \psi)^{-1} \circ \rho \circ (\pi \circ \psi))(\mathfrak{a}) & \text{für } \Delta > 0 \end{cases}.$$

Dementsprechend definieren wir:

$$\texttt{IdealReduce}(\mathfrak{a}) := \texttt{Form2Ideal}(\texttt{FormReduce}(\texttt{Ideal2Form}(\mathfrak{a}))).$$

3.3.19 Korollar *Es sei $\Delta > 0$ und $\mathfrak{a} \in \mathrm{P}_\Delta$. Dann gilt:*

(i) Ist $\mathfrak{a}$ reduziert, dann ist auch $\rho(\mathfrak{a})$ reduziert.

(ii) Alle reduzierten Formen äquivalent zu $\mathfrak{a}$ lassen sich durch wiederholte Anwendung von ρ auf eine reduzierte Form $\mathfrak{b} \sim \mathfrak{a}$ berechnen und deren Anzahl ist endlich.

Beweis: Folgt aus Satz 2.3.10 und Lemma 3.3.13 und 3.3.18. □

3.3.20 Definition Es sei $\Delta > 0$ und $\mathfrak{a} \in \mathrm{P}_\Delta$. Die Menge der reduzierten Ideale in $[\mathfrak{a}]$ wird durch ρ zu einem **Zyklus reduzierter Ideale** $\mathcal{R}(\mathfrak{a})$.

3.3.21 Beispiel Siehe Beispiel 2.3.12.

3.3.22 Lemma *Es sei k die Anzahl reduzierter Ideale einer Idealklasse. Dann gilt:*

$$\frac{2\mathrm{Reg}\,(\Delta)}{\ln \Delta} \leq k \leq \frac{2\mathrm{Reg}\,(\Delta)}{\ln 2}.$$

Beweis: Siehe [BTW95, Lemma 2.33]. □

Folgender Algorithmus berechnet $\mathcal{R}(\mathfrak{a})$:

Algorithmus `IdealCycle`

Eingabe: Ein reduziertes Ideal $\mathfrak{a}$
Ausgabe: $\mathcal{R}(\mathfrak{a})$

```
1: b := a
2: R := []
3: i := 0
4: repeat
5:     i := i + 1
6:     R[i] := a
7:     a := ρ(a)
8: until a = b
9: return R
```

Aufwand: $\mathcal{O}\left(\mathrm{Reg}\,(\Delta) \cdot \mathrm{size}\,(\Delta)^2\right)$

3.4 Idealarithmetik

3.4.1 Satz *Es seien $\mathfrak{a} = (a_1, a_2)$ und $\mathfrak{b} = (b_1, b_2) \in \mathrm{P}_\Delta$. Dann ist $\mathfrak{a}\cdot\mathfrak{b} = g\cdot\eta((c_1, c_2))$ mit*

$$g = \mathrm{ggT}\left(a_1, b_1, \frac{a_2 + b_2}{2}\right) = ua_1 + vb_1 + w\frac{a_2 + b_2}{2}$$

und

$$c_1 = \frac{a_1 b_1}{g^2} \text{ und } c_2 = \left(ua_1b_2 + vb_1a_2 + w \cdot \frac{(a_2b_2 + \Delta)}{2}\right) g^{-1}.$$

Beweis: Es gilt:

$$\begin{aligned}\frac{a_2^2-\Delta}{4a_1}, \frac{b_2^2-\Delta}{4b_1} \in \mathbb{Z} &\implies a_2^2 \equiv b_2^2 \equiv \Delta \bmod 4\\ &\implies a_2 \equiv b_2 \equiv \Delta \bmod 2\\ &\implies \frac{a_2+b_2}{2} \in \mathbb{Z}.\end{aligned}$$

Es sei also

$$g = \mathrm{ggT}\left(a_1, b_1, \frac{a_2+b_2}{2}\right) = ua_1 + vb_1 + w\frac{a_2+b_2}{2}.$$

Es gilt:

$$\begin{aligned}\mathfrak{a}\cdot\mathfrak{b} &= \left(a_1\mathbb{Z} + \frac{a_2+\sqrt{\Delta}}{2}\mathbb{Z}\right)\cdot\left(b_1\mathbb{Z} + \frac{b_2+\sqrt{\Delta}}{2}\mathbb{Z}\right)\\ &= a_1b_1\mathbb{Z} + a_1\left(\frac{b_2+\sqrt{\Delta}}{2}\right)\mathbb{Z} + b_1\left(\frac{a_2+\sqrt{\Delta}}{2}\right)\mathbb{Z}\\ &\quad + \frac{a_2b_2+\Delta+(a_2+b_2)\sqrt{\Delta}}{4}\mathbb{Z}. \qquad (3.6)\end{aligned}$$

Dabei ist g der kleinste Faktor vor $\frac{\sqrt{\Delta}}{2}$, also existieren $c_1, c_2 \in \mathbb{Z}$ mit $\mathfrak{a}\cdot\mathfrak{b} = g\,(c_1, c_2)$. Es gilt nach Satz 3.1.9:

$$g^2c_1 = \mathrm{N}\,(\mathfrak{a}\cdot\mathfrak{b}) = \mathrm{N}\,(\mathfrak{a})\cdot\mathrm{N}\,(\mathfrak{b}) = a_1b_1, \text{ also } c_1 = \frac{a_1b_1}{g^2}.$$

Setzt man in die Gleichung (3.6) nacheinander $0, u, v, w \in \mathbb{Z}$ ein, so erhält man:

$$\begin{aligned}\mathfrak{a}\cdot\mathfrak{b} &\ni a_1\left(\frac{b_2+\sqrt{\Delta}}{2}\right)u + b_1\left(\frac{a_2+\sqrt{\Delta}}{2}\right)v + \frac{a_2b_2+\Delta+(a_2+b_2)\sqrt{\Delta}}{4}w\\ &= \frac{1}{2}\left(a_1b_2u + b_1a_2v + \frac{w}{2}\left(\Delta + a_2b_2\right)\right) + \frac{\sqrt{\Delta}}{2}\left(a_1u + b_1v + \frac{a_2+b_2}{2}w\right)\\ &= \frac{a_1b_2u + b_1a_2v + \frac{w}{2}\left(\Delta + a_2b_2\right) + g\sqrt{\Delta}}{2}\\ &= g\cdot\frac{\left(a_1b_2u + b_1a_2v + \frac{w}{2}\left(\Delta + a_2b_2\right)\right)g^{-1} + \sqrt{\Delta}}{2}.\end{aligned}$$

Damit folgt

$$c_2 \equiv \left(a_1b_2u + b_1a_2v + \frac{w}{2}\left(\Delta + a_2b_2\right)\right)g^{-1} \bmod 2c_1.$$

□

In der Praxis berechnet man die Darstellung von $\mathrm{ggT}\left(a_1, b_1, \frac{a_2+b_2}{2}\right)$ in 2 Schritten mit Hilfe des erweiterten Euklidischen Algorithmus, denn es gilt:

$$g = \mathrm{ggT}\left(a_1, b_1, \frac{a_2+b_2}{2}\right) = \mathrm{ggT}\left(\mathrm{ggT}\left(a_1, b_1\right), \frac{a_2+b_2}{2}\right).$$

Für

$$h := \mathrm{ggT}\left(a_1, b_1\right) = u_1 a_1 + v_1 b_1$$

und

$$\mathrm{ggT}\left(h, \frac{a_2+b_2}{2}\right) = u_2 h + v_2 \frac{a_2+b_2}{2}$$

ist also

$$\begin{aligned} g &= \mathrm{ggT}\left(h, \frac{a_2+b_2}{2}\right) \\ &= u_2 \cdot (u_1 a_1 + v_1 b_1) + v_2 \cdot \frac{a_2+b_2}{2} \\ &= (u_2 u_1) \cdot a_1 + (u_2 v_1) \cdot b_1 + v_2 \cdot \frac{a_2+b_2}{2}. \end{aligned}$$

Es ist dann in Satz 3.4.1:

$$\begin{aligned} c_2 &\equiv \left((u_2 u_1) \cdot a_1 b_2 + (u_2 v_1) \cdot b_1 a_2 + v_2 \cdot \frac{a_2 b_2 + \Delta}{2}\right) \cdot g^{-1} \\ &\equiv \left(u_1 u_2 a_1 b_2 + \left(g - (u_2 u_1) \cdot a_1 + v_2 \frac{a_2+b_2}{2}\right) a_2 + v_2 \cdot \frac{a_2 b_2 + \Delta}{2}\right) \cdot g^{-1} \\ &\equiv \left(u_1 u_2 a_1 b_2 + a_2 g - u_1 u_2 a_1 a_2 - v_2 \frac{a_2^2 + b_2 a_2}{2} + v_2 \cdot \frac{a_2 b_2 + \Delta}{2}\right) \cdot g^{-1} \\ &\equiv a_2 + \left(u_2 \cdot (u_1 a_1 (b_2 - a_2)) + v_2 \cdot \frac{\Delta - a_2^2}{2}\right) \cdot g^{-1} \mod \left(2 \cdot \frac{a_1 b_1}{g^2}\right). \end{aligned}$$

Für $h = 1$ ist dabei $u_2 = 1$, $v_2 = 0$ und $g = 1$.

Für den Fall

$$\mathfrak{a} = \mathfrak{b} = (a_1, a_2)$$

ist mit

$$h = \mathrm{ggT}(a_1, a_1) = a_1 = 0 \cdot a_1 + 1 \cdot a_1$$

und

$$g = \mathrm{ggT}\left(h, a_2\right) = \mathrm{ggT}\left(a_1, a_2\right) = u_2 a_1 + v_2 a_2,$$

und somit

$$c_2 \equiv a_2 + v_2 \cdot \frac{\Delta - a_2^2}{2g} \mod \left(2 \cdot \frac{a_1^2}{g^2}\right).$$

Wir erhalten damit die beiden folgenden (optimierten) Algorithmen zum Multiplizieren und Quadrieren von Idealen:

Algorithmus `IdealProduct`

Eingabe: Zwei Ideale $\mathfrak{a} = (a_1, a_2)$ und $\mathfrak{b} = (b_1, b_2) \in \mathrm{P}_\Delta$
Ausgabe: $\mathfrak{c} = (c_1, c_2) \in \mathrm{P}_\Delta$ mit $q \cdot \mathfrak{c} = \mathfrak{a} \cdot \mathfrak{b}$ für ein $q \in \mathbb{Q}^\times$

`1:` `Berechne` $u_1, v_1 \in \mathbb{Z}$ `mit` $h = \mathrm{ggT}(a_1, b_1) = u_1 a_1 + v_1 b_1$
`2:` $c_1 := a_1 b_1$
`3:` $c_2 := u_1 a_1 (b_2 - a_2)$
`4:` **if** $h \neq 1$ **then**
`5:` `Berechne` $u_2, v_2 \in \mathbb{Z}$ `mit` $g = \mathrm{ggT}\left(h, \frac{a_2+b_2}{2}\right) = u_2 h + v_2 \cdot \frac{a_2+b_2}{2}$
`6:` $c_1 := \frac{c_1}{g^2}$
`7:` $c_2 := \left(u_2 c_2 + v_2 \cdot \frac{\Delta - a_2^2}{2}\right) g^{-1}$
`8:` **end**
`9:` $c_2 := a_2 + c_2$
`10:` **return** $\eta((c_1, c_2))$

Aufwand: $\mathcal{O}(\max\{\mathrm{size}(\mathfrak{a}), \mathrm{size}(\mathfrak{b})\}^2) = \mathcal{O}\left(\mathrm{size}\left(\sqrt{\Delta}\right)\right)$

Algorithmus `IdealSquare`

Eingabe: Ein Ideal $\mathfrak{a} = (a_1, a_2) \in \mathrm{P}_\Delta$
Ausgabe: $\mathfrak{c} = (c_1, c_2) \in \mathrm{P}_\Delta$ mit $q \cdot \mathfrak{c} = \mathfrak{a}^2$ für ein $q \in \mathbb{Q}^\times$

`1:` `Berechne` $u, v \in \mathbb{Z}$ `mit` $g = \mathrm{ggT}(a_1, a_2) = u a_1 + v a_2$
`2:` $c_1 := \frac{a_1^2}{g^2}$
`3:` $c_2 := a_2 + v \frac{\Delta - a_2^2}{2g}$
`4:` **return** $\eta((c_1, c_2))$

Aufwand: $\mathcal{O}\left(\mathrm{size}(\mathfrak{a})^2\right) = \mathcal{O}\left(\mathrm{size}\left(\sqrt{\Delta}\right)^2\right)$

3.4.2 Satz *Es sei* $\mathfrak{a} = (a, b)$ *ein Ideal in* $\mathcal{O}_\Delta$. *Dann ist*

$$\mathfrak{a}^{-1} = \frac{1}{a} \cdot \eta((a, -b)).$$

Beweis: Es ist

$$\eta((a,-b)) = \begin{cases} (a,-b) & \text{für } a \neq b \\ (a,b) & \text{für } a = b \end{cases}.$$

In jedem Fall existieren nach Satz 3.4.1 $c_1, c_2, g \in \mathbb{Z}$ mit

$$\frac{1}{a} \cdot \eta((a,-b)) \cdot (a,b) = \frac{g}{a} \cdot (c_1, c_2) = \mathfrak{c}$$

und

$$g = \mathrm{ggT}\,(a,a,0) = a \text{ und } c_1 = \frac{a^2}{g^2} = 1.$$

Daher ist $1 \in \mathfrak{c}$, also $\mathfrak{c} = \mathcal{O}$. □

Wir erhalten damit folgenden Algorithmus:

Algorithmus `IdealInverse`

Eingabe: Ein Ideal $\mathfrak{a} = (a,b) \in \mathrm{P}_\Delta$
Ausgabe: $\mathfrak{b} \in \mathrm{P}_\Delta$ mit $q \cdot \mathfrak{b} = \mathfrak{a}^{-1}$ für ein $q \in \mathbb{Q}^\times$

```
1: if a ≠ b then
2:     return (a, −b)
3: else
4:     return (a, b)
5: end if
```

Aufwand: $\mathcal{O}(1)$

Zum Rechnen in der Klassengruppe können nun diese Algorithmen mit anschließender Reduktion verwendet werden, etwa zur Multiplikation zweier Klassen:

$$[\mathfrak{a}] \cdot [\mathfrak{b}] := [\texttt{IdealReduce}\,(\mathfrak{a} \cdot \mathfrak{b})].$$

Im Folgenden stellen wir Idealklassen nur noch durch reduzierte Vertreter dar, das heißt in der Schreibweise $[\mathfrak{a}] \in \mathrm{Cl}\,(\Delta)$ ist $\mathfrak{a}$ reduziert. Wegen Lemma 2.2.6 ist sichergestellt, daß für reduzierte Ideale $\mathfrak{a}$

$$\mathrm{size}\,(\mathfrak{a}) \leq 2\,\mathrm{size}\left(\sqrt{|\Delta|}\right)$$

gilt. Sind die Eingaben für `IdealProduct` und `IdealInverse` reduzierte Ideale, so ist gilt für das Ergebnis $\mathfrak{c}$:

$$\mathrm{size}\,(\mathfrak{c}) \leq 2\Delta,$$

also hat der anschließende Aufruf von `IdealReduce` eine Laufzeit in $\mathcal{O}\left(\mathrm{size}\,(\Delta)^2\right)$, und damit auch die entsprechenden Algorithmen für die Klassen.

Mit Hilfe des Multiply-and-Square-Verfahrens und ständiger Reduktion kann man nun einen effizienten Algorithmus angeben, der beliebige ganze Potenzen einer Idealklasse berechnet.

Algorithmus `IdealClassPower`

Eingabe : Eine Idealklasse $[\mathfrak{a}]$ und ein $n \in \mathbb{Z}$
Ausgabe: Die Idealklasse $[\mathfrak{a}]^n \in \mathrm{Cl}\,(\Delta)$

1: `Berechne die binäre Darstellung von` $|n| = \sum_{i=0}^{k} n_i 2^i$
2: $[\mathfrak{b}] := [\mathcal{O}]$
3: **for** $i \in \{1, \ldots, k\}$ **do**
4: **if** $n_i = 1$ **then**
5: $[\mathfrak{b}] := [\mathfrak{a}] \cdot [\mathfrak{b}]$
6: **end if**
7: $[\mathfrak{a}] := [\mathfrak{a}]^2$
8: **end for**
9: **if** $n < 0$ **then**
10: $[\mathfrak{b}] := [\mathfrak{b}]^{-1}$
11: **end if**
12: **return** $[\mathfrak{b}]$

Aufwand: $\mathcal{O}\left(\mathrm{size}\,(\Delta)^2 \,\mathrm{size}\,(n)\right)$

Kapitel 4

Kryptographische Grundlagen

Die Kryptographie entstand aus dem Bedürfnis, Informationen vor fremden Personen zu verstecken. Dies ist insbesondere wichtig bei schriftlicher Kommunikation über unsichere Kanäle. Um eine Nachricht vor Angreifern geheim zu halten, wird diese verschlüsselt, d. h. durch etwas ersetzt, aus dem sich die eigentliche Information nur durch Kenntnis eines geheimen Schlüssels zurückgewinnen läßt (Entschlüsselung). In den letzten Jahrzehnten sind weitere Aufgaben wie digitale Unterschriften hinzugekommen. Darauf wollen wir hier aber nicht weiter eingehen.
Die Verschlüsselungsverfahren teilen sich grob in symmetrische und asymmetrische auf. Symmetrische Verfahren sind dabei die wesentlich älteren und finden sich zum Beispiel auch im ältesten bekannten Verschlüsselungsverfahren, dem nach seinem Erfinder Julius Cäsar benannten Cäsar-Code wieder. Er funktioniert wie folgt:

(i) **Initialisierung** Sender und Empfänger (im Folgenden Alice und Bob genannt) einigen sich auf einen geheimen Schlüssel $\kappa \in \mathbb{Z}_{26}$.

(ii) **Verschlüsselung** Die zu versendende Nachricht besteht ausschließlich aus einer Kette $B_1 B_2 \dots B_n$ von Buchstaben B_i. Zuerst ordnet Alice jedem Buchstaben aus $\{A, \dots, Z\}$ einen Zahlenwert zu:

$$A = 0, B = 1, \dots, Z = 25.$$

Dann übersetzt sie die Buchstaben B_i in ihre entsprechenden Zahlenwerte b_i und versendet den Buchstaben C_i, der zu der Zahl

$$b_i + \kappa \bmod 26$$

gehört.

(iii) **Entschlüsselung** Bob berechnet jeweils den Buchstaben, der zu

$$c_i - \kappa \bmod 26$$

gehört, wobei c_i ein zu einem empfangenen Buchstaben C_i gehöriger Zahlenwert ist.

Solche Verfahren, in denen Alice und Bob den gleichen Schlüssel κ benutzen, nennt man symmetrisch. Der Cäsarcode bietet heutzutage natürlich praktisch überhaupt keine Sicherheit mehr, ganz im Gegensatz zu seinen Nachfolgern wie zum Beispiel DES. Trotzdem haben symmetrische Verschlüsselungsverfahren ein grundlegendes Problem. Für die Kommunikation mit einer dritten Person, Claire, müßte sich Alice wieder einen neuen Schlüssel ausdenken, damit Bob die Nachrichten an Claire nicht lesen kann. Alle Parteien, die vertraulich miteinander kommunizieren wollen, müssen dazu ihre Schlüssel auf sicherem Wege austauschen. Das führt zu einem riesigen Aufwand wenn man in heutigen Dimensionen von einigen hundert Millionen Internetbenutzern denkt; jedes Paar von Benutzern müßte einen eigenen Schlüssel vereinbaren.
Die Lösung dieses Problems bieten asymmetrische Verfahren, sie leisten das, was man von einer komfortablen Kommunikation erwartet. Jeder Teilnehmer besitzt einen öffentlichen und einen privaten Schlüssel. So ist zum Beispiel der öffentliche Schlüssel von Bob jedem bekannt und jeder kann damit Nachrichten verschlüsseln und an Bob senden. Die Entschlüsselung ist nur mit Hilfe des privaten Schlüssels möglich, den nur Bob alleine kennt. Damit funktioniert die Kommunikation wie ein Briefkasten - jeder kann Bob einen Brief schicken, aber nur er kann den Briefkasten aufmachen und den Brief lesen.
Realisiert wird diese Idee durch sogenannte **Einweg-Funktionen**, dies sind bijektive Funktionen, die sich leicht berechnen lassen, deren Umkehrfunktionen aber praktisch extrem schwer zu finden ist. Eine solche Einweg-Funktion ist zum Beispiel das Potenzieren in endlichen Gruppen, was wir in dieser Arbeit etwas genauer beleuchten wollen.

4.1 Darstellung von Nachrichten

Die meisten Verschlüsselungsalgorithmen sind mathematische Funktionen, die mit Zahlen, Polynomen, Idealen oder ähnlichem rechnen. Daher muß eine Nachricht als erstes durch etwas ersetzt werden, womit ein solcher Algorithmus etwas anfangen kann.
Eine Nachricht in eindeutiger Weise durch eine Zahl darzustellen, ist recht einfach und Voraussetzung für fast jeden Verschlüsselungsalgorithmus. Zuerst einigt man sich auf das Alphabet, aus dessen Zeichen die Nachrichten bestehen sollen, und numeriert dieses dann durch. Standardmäßig wird der ASCII-Code verwendet, das sind 256 Zeichen, die durch die Zahlen $0, \ldots, 255$ codiert sind, zum Beispiel Ascii(`A`)=65, Ascii(`B`)=66, ..., Ascii(`Z`)=90, entsprechend ist zum Beispiel Char(65) = `A`. Normalerweise kann ein Verschlüsselungsalgorithmus nur Zahlen verschlüsseln, die kleiner als eine Zahl M sind (siehe Beispiele). Dabei sollte $M \geq 256$ gelten, wenn man den ASCII-Code verwenden will. Wir müssen unsere Nachricht nun in kleine Stücke $s \leq M$ zerteilen, damit diese verschlüsselt werden können. Dazu bestimmen wir

$$k = \lfloor \log_{256} M \rfloor .$$

Dieses k, genannt **Blocklänge**, ist die Anzahl von Zeichen, die man in einem Schritt verschlüsseln kann. Daher teilt man die Nachricht in Blöcke von je k Zeichen ein und füllt dabei eine mögliche Lücke am Ende auf (Null-Padding). Ist $b_1, \ldots, b_k$ solch ein Block von Buchstaben b_i, so wird dieser dann in die Zahl

$$n = \sum_{i=1}^{k} \text{Ascii}\,(b_i) \cdot 265^{k-i}$$

übersetzt, also praktisch die Dezimaldarstellung einer 256-adischen Zahl $b_1 \ldots b_k$. Diese kann dann verschlüsselt werden und nach dem Entschlüsseln wieder in die eigentliche Nachricht umgerechnet werden. Die Übersetzung kann zum Beispiel durch die folgenden zwei Algorithmen realisiert werden.

Algorithmus `Message2Number`

Eingabe : Eine $k \in \mathbb{N}$ und $s = s_1 s_2 \ldots s_n$ aus maximal k ASCII-Zeichen
Ausgabe: Die zu s gehörige Dezimalzahl

`1:` $m := 0$
`2:` **for** $i \in \{0, \ldots, n-1\}$ **do**
`3:` $\quad m := 256 \cdot m + \texttt{Ascii}\,(s_i)$
`4:` **end for**
`5:` $m := m \cdot 256^{k-n}$
`6:` **return** m

Aufwand: $\mathcal{O}\,(k \cdot \text{size}\,(m)) = \mathcal{O}\,(k^2)$

Algorithmus `Number2Message`

Eingabe : Eine Blocklänge k und eine natürliche Zahl $m < 256^k$
Ausgabe: Die zu m gehörige Nachricht

`1:` $s := []$
`2:` **for** $i \in \{1, \ldots, k\}$ **do**
`3:` $\quad s[k-i] := \texttt{Char}\,(m \bmod 256)$
`4:` $\quad m := \lfloor m/256 \rfloor$
`5:` **end for**
`6:` **return** s

Aufwand: $\mathcal{O}\,(k^2)$

Als nächstes wollen wir uns überlegen, wie man eine Nachricht durch eine Idealklasse repräsentieren können. Nach Lemma 2.2.5 ist jedes Ideal $\mathfrak{a} = (a, b)$ mit $|a| < \frac{\sqrt{|\Delta|}}{2}$

reduziert. Im imaginärquadratischen Fall heißt das, daß dieses Ideal der eindeutige reduzierte Vertreter einer Idealklasse ist (siehe Corollar 3.3.12). Im reellquadratischen Fall haben wir einen Zyklus von reduzierten Idealen (siehe Corollar 3.3.19). Wie wir aus diesem Zyklus das reduzierte Ideal wiederfinden, das wir verschlüsselt haben, wird in Abschnitt 6.2 besprochen.

Zur Darstellung einer Nachricht durch Ideale wird sie als erstes wieder durch Zahlen $a_1, \ldots, a_n$ mit $0 \leq a_i < \frac{\sqrt{|\Delta|}}{2} \;\; \forall\, 1 \leq i \leq n$ dargestellt. Die Blocklänge ist hier also

$$k = \left\lfloor \log_{256} \frac{\sqrt{|\Delta|}}{2} \right\rfloor .$$

Als zweiten Schritt müssen wir die Zahlen a_i in Ideale (a_i, b_i) umwandeln. Dazu berechnen wir b_i als Quadratwurzel von Δ modulo $4a_i \;\; \forall\, 1 \leq i \leq n$.

Für den Fall, daß $a \notin \mathbb{P}$ ist das Wurzelziehen modulo $4a$ für große a bereits ein praktisch unlösbares Problem, was selbst für Kryptosysteme verwendet werden kann. Gilt $a \in \mathbb{P}$, so gibt es modulo a genau $\frac{a-1}{2}$ Quadrate und ebenso viele Nichtquadrate, es kann also sein, daß gar keine Quadratwurzel von Δ modulo a existiert. Man muß sich hier damit behelfen, statt a einfach eine zufällige oder die nächstliegende Primzahl mit $\left(\frac{p}{\Delta}\right) = 1$ zu nehmen. Das Wurzelziehen modulo einer Primzahl p ist in $\mathcal{O}\left(\text{size}\,(a)^4\right)$ möglich (siehe [MvOV97]). Für $a \equiv 3, 5, 7 \bmod 8$ der Aufwand sogar nur $\mathcal{O}\left(\text{size}\,(a)^3\right)$ (siehe [MvOV97] und [Mey97]).

Wir wollen nun einen entsprechenden Algorithmus angeben, der natürliche Zahlen n in Ideale (a, b) übersetzt. Die einfachste Möglichkeit dafür ist, statt n einfach eine Primzahl $a > 2$ mit obigen Eigenschaften zu nehmen und sich dann zusätzlich $n - a$ zu merken. Dieses Verfahren nennt man **Abstandseinbettung**. Für weitere Möglichkeiten und genauere Betrachtungen empfehlen wir [Sch99]. Wir können dann effizient eine Wurzel von Δ modulo a berechnen (siehe [MvOV97]). Um nun eine Wurzel von Δ modulo $4a$ zu finden, stellen wir wegen $\Delta \equiv 0, 1 \bmod 4$ und $b \equiv 0, 1 \bmod 4$ fest:

$$\begin{aligned} \Delta \not\equiv b^2 \bmod 4 &\iff \Delta \not\equiv b \bmod 2 \\ &\iff \Delta \equiv a - b \bmod 2 \text{ da } a \equiv 1 \bmod 2 \\ &\iff \Delta \equiv (a-b)^2 \bmod 4 \end{aligned}$$

Wegen $(a-b)^2 \equiv b^2 \bmod a$ und $\text{ggT}\,(a, 4) = 1$ ist also entweder b oder $a - b$ eine Quadratwurzel von von Δ modulo $4a$.

Wir erhalten also folgenden Algorithmus, um Zahlen in Ideale zu übersetzen:

Algorithmus `Number2Ideal`

Eingabe : Eine Diskriminante Δ und eine natürliche Zahl $n \leq P \leq \frac{\sqrt{|\Delta|}}{2}$
Ausgabe: Ein zu n gehöriges reduziertes Ideal $\mathfrak{a}$ mit Abstand d

1: $a := \max\{2, n-1\}$
2: **repeat**
3: $\quad a := \texttt{NextPrime}\,(a)$
4: **until** $\left(\frac{\Delta}{a}\right) = 1$ **and** $a \equiv 3, 5, 7 \bmod 8$
5: **if** $a \equiv 3 \bmod 4$ **then**
6: $\quad b := \Delta^{\frac{a+1}{4}} \bmod a$
7: **else**
8: $\quad$ **if** $\Delta^{\frac{a-1}{4}} \equiv 1 \bmod a$ **then**
9: $\quad\quad b := \Delta^{\frac{a+3}{8}} \bmod a$
10: $\quad$ **else**
11: $\quad\quad b := 2\Delta \cdot (4\Delta)^{\frac{a-5}{8}} \bmod a$
12: $\quad$ **end if**
13: **end if**
14: **if** $\Delta \not\equiv b \bmod 2$ **then**
15: $\quad b := a - b$
16: **end if**
17: **return** $\eta\,((a, b)), (n - a)$

Aufwand: $\mathcal{O}\left(\text{size}\left(\frac{\sqrt{|\Delta|}}{2}\right)^{7+\varepsilon}\right)$

Bei der Implementierung dieses Algorithmus sollte man natürlich in den Schritten 2 – 4 den Primzahltest als letztes durchführen, da er am längsten dauert. Unter Umständen muß man die maximale Größe von n anpassen, damit $a < \frac{\sqrt{|\Delta|}}{2}$ garantiert bleibt. Dazu berechnet man (effizient) die größte Primzahl $P \leq \frac{\sqrt{|\Delta|}}{2}$ mit $\left(\frac{\Delta}{P}\right) = 1$ und $P \equiv 3, 5, 7 \bmod 8$ und beschränkt n durch diese Zahl.
Nach dem Primzahlsatz verhält sich $\tau\,(n)$, die Anzahl der Primzahlen $\leq n$, asymptotisch wie $\frac{n}{\ln n}$. Von diesen Primzahlen sind etwa $\frac{3}{4}$ kongruent $3, 5$ oder 7 modulo 8. Weiterhin ist die Chance $\frac{1}{2}$, daß Δ ein Quadrat modulo einer Primzahl ist. Dadurch verringert sich also die Anzahl der verschlüsselbaren Zahlen von

$$n := \frac{\sqrt{|\Delta|}}{2}$$

auf

$$\frac{1}{2} \cdot \frac{3}{4} \cdot \frac{n}{\ln\,(n)} = \frac{3n}{8 \ln\,(n)}.$$

Die Idee, nicht die eigentliche Nachricht m zu verschlüsseln, sondern eine andere Zahl a, wobei man sich $m-a$ merkt, darf nicht dazu verleiten, beliebig große Zahlen zu verschlüsseln, indem man sie durch eine kleine verschlüsselbare Zahl a ersetzt. Ist nämlich $m-a>a$, so sind die ersten überschüssigen Bits von $m-a$ ein unverschlüsselter Teil der Nachricht m.
Der Inverse Algorithmus, der aus einem Ideal $\mathfrak{a}$ und dem Abstand wieder die ursprüngliche Zahl berechnet, ergibt sich kanonisch:

Algorithmus `Ideal2Number`

Eingabe : Eine Ideal $\mathfrak{a}=(a,b)\in \mathrm{P}_\Delta$ und ein Abstand c
Ausgabe: Die mit $\mathfrak{a}$ und c verschlüsselte Zahl

`1:` **return** $a+c$

Aufwand: $\mathcal{O}(\mathrm{size}(\Delta))$

Um uns auf das Wesentliche zu beschränken, werden wir das Problem, Zahlen in Ideale zu übersetzen, vorerst in den Verschlüsselungsalgorithmen nicht mehr beachten und davon ausgehen, nur noch ein gegebenes Ideal verschlüsseln zu wollen. In den Beispielen und in Kapitel 7 werden wir dann noch mal auf dieses Problem zurückkommen.

4.2 Verschlüsselungsprotokolle

4.2.1 Definition Es sei G eine endliche multiplikative Gruppe, $\alpha,\beta\in G$ und $a\in\mathbb{N}$ minimal mit $\alpha^a=\beta$. Dann heißt a **diskreter Logarithmus** von β zur Basis α. Die Berechnung von a aus α und β wird als (verallgemeinertes) **diskretes Logarithmus Problem** (**DLP**) bezeichnet.

Name und evtl. Voraussetzungen	Aufwand
Naives Nachzählen	$\mathcal{O}(\mathrm{ord}\,\alpha)=\mathcal{O}(n)$
Babystep-Giantstep-Algorithmus	$\mathcal{O}\left(\sqrt{\mathrm{ord}\,\alpha}\right)=\mathcal{O}(\sqrt{n})$
Pollard-ρ-Algorithmus ($n\in\mathbb{P}$)	$\mathcal{O}\left(\sqrt{\mathrm{ord}\,\alpha}\right)=\mathcal{O}(\sqrt{n})$
Pohlig-Hellman-Alg. ($n=\prod_{i=1}^k p_i^{e_i}$ bekannt)	$\mathcal{O}\left(\sum_{i=1}^k e_i\left(\mathrm{size}(n)+\sqrt{p_i}\right)\right)$
Index-Calculus-Alg. (Faktorbasis wählbar)	mindestens $L_n\left[\frac{1}{3},\sqrt[3]{\frac{64}{9}}\right]$

Tabelle 4.1: Aufwand der gängigen Algorithmen zur Lösung des DLP.

Tabelle 4.1 aus [MvOV97, Kap. 3] zeigt den Aufwand der bekanntesten Algorithmen

zur Lösung des DLP zur Basis α in einer zyklischen Gruppe G mit Ordnung n. Auf der Grundlage dieses Laufzeitverhaltens und empirischer Messungen wird zum Beispiel in [Hüh00b] vorausgesagt, daß die Lösung des DLP in $\mathbb{Z}_n^\times$ mit $n \approx 2^{823}$ im Durchschnitt einen Aufwand von $3{,}55 \cdot 10^{10}$ MIPS-Jahren hat. Das entspricht ungefähr der Arbeit, eine natürliche Zahl n der Form $n = pq \approx 2^{1024}$ mit $p, q \in \mathbb{P}$, wie sie für das RSA-Verfahren verwendet wird, zu faktorisieren. Das heißt, ein besserer PC wäre über 35 Millionen Jahre mit der Lösung dieses Problems beschäftigt.
Das sind sehr große Zahlen. Sie zeigen aber auch, daß Verschlüsselungssysteme auf der Basis dieses Problems angreifbar sind. Es gibt hingegen Verschlüsselungsverfahren, von denen man beweisen kann, daß sie nicht angreifbar sind, auch wenn man alle Zeit der Welt hat (z. B. das One-time-pad). Man benutzt solche Systeme trotzdem, weil sie viel komfortabler als die bekannten total sicheren Verfahren sind. Wie sicher das System letztendlich ist, kann man durch die Wahl kryptographischer Parameter festlegen, im Falle von RSA oder dem ElGamal-Verfahren in $\mathbb{Z}_n$ wäre das in erster Linie die Größe von n. Man braucht meistens gar keine absolute Sicherheit, es reicht oft aus, die Sicherheit einfach so groß zu wählen, daß der Aufwand eines erfolgreichen Angriffs höher ist, als der Nutzen. Der Aufwand für den Angreifer eine verschlüsselte Information zu bekommen, muß also um Größenordnungen höher sein als der Nutzen den er aus dieser Information ziehen kann. Das Verhältnis von der Schwierigkeit und der Gefährlichkeit eines erfolgreichen Angriffs kann man oft gut abschätzen und sich dann auf das benötigte Maß an Sicherheit festlegen. Dieses sollte man andererseits auch nicht zu hoch ansetzen, da eine erhöhte Sicherheit natürlich immer an mindestens einer Stelle auf Kosten der Effizienz geht.
Wir werden nun drei für die Kryptographie wichtige Verfahren vorstellen.

4.2.1 Das RSA-Verfahren

Der Klassiker unter den asymmetrischen Verschlüsselungsverfahren und das noch heute am meisten benutzte Verfahren ist das nach Ron Rivest, Adi Shamir und Leonard Adleman benannte **RSA-Verfahren** aus dem Jahre 1977 ([RSA78]). Es wird wegen seiner Popularität oft als Referenz für Sicherheits- und Laufzeitvergleiche benutzt. Wir wollen es deshalb kurz beschreiben. Für weitere Ausführungen empfehlen wir [MvOV97].
Die Sicherheit des RSA-Verfahrens basiert auf der Schwierigkeit, große Zahlen zu faktorisieren.

(i) **Initialisierung** Alice und Bob wählen zwei große Primzahlen $p, q \in \mathbb{P}$ und berechnen

$$n = p \cdot q.$$

Bob wählt dann $e \in \mathbb{N}$ mit $\mathrm{ggT}\,(e, (p-1)\,(q-1)) = 1$ und bestimmt mit dem euklidischen Algorithmus Zahlen $f, s \in \mathbb{Z}$ mit

$$1 = e \cdot f + s \cdot (p-1)\,(q-1)\,.$$

Dann ist (n, e) der öffentliche und (n, f) der geheime Schlüssel.

(ii) **Verschlüsselung** Die Nachricht $m \in \mathbb{Z}_n^\times$ von Alice wird durch

$$\tilde{m} := m^e \bmod n$$

verschlüsselt und gesendet.

(iii) **Entschlüsselung** Bob empfängt $\tilde{m} \in \mathbb{Z}_n^\times$ und berechnet m durch

$$\tilde{m}^f \equiv m^{ef} \equiv m \cdot \left(m^{(p-1)(q-1)}\right)^{-s} \equiv m \cdot \left(m^{\sharp \mathbb{Z}_n^\times}\right)^{-s} \equiv m \bmod n.$$

Ver- und Entschlüsselung haben damit nach Tabelle 1.1 einen Aufwand in $\mathcal{O}\left(\text{size}\,(n)^3\right)$. Eine realistische Größe von n sind 1024 Bit. Wenn ein Angreifer n faktorisieren kann, also p und q kennt, so kann er aus dem öffentlichen Schlüssel e mit Hilfe des erweiterten euklidischen Algorithmus f berechnen und alle Nachrichten entschlüsseln. Das direkte Entschlüsseln, also das e-te Wurzel ziehen modulo n, ist im wesentlichen auch wieder die Faktorisierung von n (siehe [MvOV97]).
Da e der öffentliche Schlüssel ist und an vielen Orten gespeichert werden muß, wählt man e oft relativ klein. Dies macht das Verschlüsseln effizienter. Es gibt dazu ein paar Details, die zu beachten sind (siehe [MvOV97]), ansonsten stellt diese Wahl kein Sicherheitsrisiko dar.

4.2.1.1 Anschauliches Beispiel

(i) **Initialisierung** Es sind

$$p = 227 \text{ und } q = 293$$

zwei Primzahlen. Damit erhalten wir die 16-Bit-Zahl

$$n = p \cdot q = 66511.$$

Zur Generierung des öffentlichen und privaten Schlüssels wählen wir $e = 79$ mit

$$1 = \text{ggT}\,(e, (p-1)\,(q-1)) = 31743 \cdot e + (-38) \cdot (p-1)\,(q-1)\,,$$

also

$$f = 31743.$$

Damit ist $(n, e) = (66511, 79)$ der öffentliche und $(n, f) = (66511, 31743)$ der private Schlüssel.

(ii) **Verschlüsselung** Wir wollen nun das Wort `TU` verschlüsseln. Da n eine 16-Bit-Zahl ist, ist unsere Blocklänge 2 und wir können die zugehörige Zahl

$$m = \text{Ascii}\,(T) \cdot 256 + \text{Ascii}\,(U) = 84 \cdot 256 + 85 = 21589$$

als ganzes mit e verschlüsseln:

$$\tilde{m} \equiv m^e \equiv 21589^{79} \equiv 34753 \bmod 66511.$$

Wir senden m.

(iii) **Entschlüsselung** Der Empfänger berechnet mit dem geheimen Schlüssel f:

$$\tilde{m}^f \equiv 34753^{31743} \equiv 21589 \equiv m \bmod 66511,$$

woraus wir das Wort `TU` zurückgewinnen.

4.2.2 Der Diffie-Hellman Schlüsseltausch

Der nach seinen Erfindern Whitfield Diffie und Martin Hellman benannte Schlüsseltausch aus dem Jahre 1976 ([DH76]) war einer der größten Durchbrüche auf dem Gebiet der Kryptographie. Er realisiert, was viele bis dahin für unmöglich gehalten hatten: Zwei Personen, die sich nicht kennen, können über offene Kanäle ein gemeinsames Geheimnis erzeugen. Dazu einigen sich Alice und Bob öffentlich auf eine Gruppe G mit möglichst großem zyklischen Primfaktor C_q und einen Erzeuger γ von C_q, welche einem Angreifer damit auch bekannt sind. Dann geht es weiter mit:

Alice	Bob
wählt ein $a \in \mathbb{N}, a < q$	wählt ein $b \in \mathbb{N}, b < q$
berechnet $\alpha = \gamma^a$	berechnet $\beta = \gamma^b$
sendet α an Bob	sendet β an Alice
berechnet $\beta^a = \gamma^{ba}$	berechnet $\alpha^b = \gamma^{ab}$.

Am Ende kennen Alice und Bob beide das Geheimnis γ^{ab}. Dieses Protokoll ist heute Grundlage vertraulicher Kommunikation zwischen Computern.

4.2.2.1 Sicherheit

Ein Angreifer hat drei Möglichkeiten:

(i) Die Berechnung von a aus γ^a und γ.

(ii) Die Berechnung von b aus γ^b und γ.

(iii) Die Berechnung von γ^{ab} aus γ^a und γ^b.

Die letzte Möglichkeit ist das sogenannte (verallgemeinerte) **Diffie-Hellman Problem** (**DHP**). Es ist klar, daß man dieses Problem lösen kann, wenn man eines der ersten beiden Probleme löst, also den diskreten Logarithmus zur Basis γ in G berechnet. Beschrieben wird dieses Schwierigkeitsverhältnis mit DHP $\leq$ DLP. Bis jetzt konnte man noch nicht herausfinden, ob auch DHP = DLP gilt, es deutet aber vieles darauf hin (siehe [MvOV97]). Wir werden daher im Folgenden DHP = DLP annehmen.

4.2.3 Die ElGamal-Verschlüsselung

Die nach ihrem Erfinder Taher ElGamal benannte ElGamal-Verschlüsselung ([ElG85]) ist ein Diffie-Hellman Schlüsseltausch mit anschließender Ver- und Entschlüsselung einer Nachricht m. Alice und Bob bestimmen je einen geheimen Schlüssel (a bzw. b) und erzeugen sich damit ein gemeinsames Geheimnis γ^{ab}. Die Nachricht m wird dann mittels Multiplikation mit γ^{ab} verschlüsselt und durch $\left(\gamma^{ab}\right)^{-1}$ wieder entschlüsselt. Entsprechend nennt man γ^{ab} **mask** und γ^{b} **clue**.
Wir benötigen wie in 4.2.2 eine abelsche Gruppe G mit folgenden Eigenschaften:

(i) In G sollte das DLP schwer zu lösen sein, das heißt, $\sharp G$ muß genügend groß sein und einen großen Primfaktor enthalten. Von dessen Größe hängt die Sicherheit des Verfahrens ab.

(ii) Das Rechnen in G sollte effizient sein.

(iii) Zur Darstellung von Nachrichten (Zahlen) durch Gruppenelemente ist eine bijektive und in beiden Richtungen leicht zu berechnende Abbildung $f : \{0, \ldots, M\} \to S \subseteq G$ notwendig.

Das allgemeine ElGamal-Verfahren:

(i) **Initialisierung**

  (a) Es sei C_q der große zyklische Faktor von G.
  (b) Wähle $\gamma \in G$ mit Ordnung q beliebig.
  (c) Wähle $a \in \mathbb{N}, a < q$ zufällig und berechne $\alpha := \gamma^a$.
  (d) Öffentlicher Schlüssel: (G, γ, α, q)
  (e) Geheimer Schlüssel: a

(ii) **Verschlüsselung** (durch Bob)

  (a) Es sei $m \in G$ die zu verschlüsselnde Nachricht.
  (b) Wähle $b \in \mathbb{N}, b < q$ zufällig.
  (c) Berechne $m_1 := \gamma^b$ (= clue).
  (d) Berechne $m_2 := m \cdot \alpha^b = m \cdot \gamma^{ab}$.
  (e) Sende (m_1, m_2).

(iii) **Entschlüsselung** (durch Alice)

  (a) Empfange (m_1, m_2).
  (b) Berechne $\tilde{m} = m_2 \cdot m_1^{-a} = m_2 \cdot \left(\gamma^{ab}\right)^{-1}$.

4.2.3.1 Korrektheit Es ist

$$\begin{aligned}\tilde{m} &= m_2 \cdot m_1^{-a} \\ &= \left(m \cdot \alpha^b\right) \cdot \left(\gamma^b\right)^{-a} \\ &= m \cdot \left(\left(\gamma^a\right)^b\right) \cdot \left(\gamma^{ka}\right)^{-1} \\ &= m \cdot 1_G \\ &= m.\end{aligned}$$

4.2.3.2 Sicherheit Ein Angreifer hat wie in 4.2.2.1 drei Möglichkeiten:

(i) Die Berechnung von m aus $m_2 = m \cdot \alpha^b$ und γ. Da aber b zufällig gewählt wurde, geht dies nur über die Berechnung von b aus $m_1 = \gamma^b$ und γ.

(ii) Die Berechnung von a aus $\alpha = \gamma^a$ und γ.

(iii) Die Berechnung von γ^{ka} aus $\alpha = \gamma^a$, $m_1 = \gamma^b$ und γ.

Das heißt, die Sicherheit der ElGamal-Verschlüsselung basiert ebenfalls auf dem DHP, bzw. dem DLP. Da für jeden verschlüsselten Nachrichtenblock ein neuer Schlüssel erzeugt und übermittelt werden muß, verdoppelt sich die Nachrichtenlänge. Will man hingegen einen Schlüssel b für mehrere Nachrichten verwenden, um das Nachrichtenvolumen und die Rechenzeit zu verringern, so ergibt sich folgendes Problem. Viele Nachrichten beginnen mit Standardphrasen, manchmal kann ein Angreifer auch über andere Wege in den Besitz eines unverschlüsselten Teils m einer Nachricht kommen. Sind m und n mit dem gleichen Schlüssel b verschlüsselt, so gilt für die jeweiligen verschlüsselten Nachrichten (m_1, m_2) und (n_1, n_2):

$$m \cdot \frac{n_2}{m_2} = m \cdot \frac{n \cdot \alpha^b}{m \cdot \alpha^b} = n.$$

Aus der Kenntnis einer unverschlüsselten Nachricht m, kann man also alle weiteren Nachrichten n entschlüsseln, die mit dem gleichen b verschlüsselt wurden. Die mehrfache Verwendung eines solchen Schlüssels ist also nicht zu empfehlen.

4.2.3.3 Bemerkung Wir wollen an dieser Stelle kurz auf den Unterschied zwischen der *beliebigen* Wahl eines Elementes wie in Punkt (b) der Initialisierung und der *zufälligen* Wahl eines Elementes wie in Punkt (c) der Initialisierung eingehen. Soll ein Element zufällig gewählt werden, heißt das, daß seine Wahl nicht vorhersagbar sein darf. Viele Verschlüsselungsverfahren konnten erfolgreich angegriffen werden, weil die verwendeten Algorithmen zur Erzeugung von „zufälligen“ Elementen keinen perfekten Zufall gewährleisten konnten und so einzelne Elemente vorhergesagt werden konnten. Die Erzeugung von Pseudozufallszahlen in der Kryptographie ist ein bedeutendes Problem, mit dem wir uns hier aber nicht beschäftigen werden. Wir werden stets annehmen, Elemente völlig zufällig wählen zu können.

Die beliebige Wahl eines Elementes darf dagegen vorhersagbar sein. In unserem Fall stellt die beliebige Wahl von γ kein Sicherheitsrisiko dar, denn wegen

$$\log_\gamma(g) = \frac{\log_\beta(g)}{\log_\beta(\gamma)} \quad \forall\ g \in G$$

ist die Berechnung des diskreten Logarithmus zur Basis γ im Durchschnitt genauso schwierig wie für alle andere Basen $\beta \in \mathbb{Z}_q^\times$. Damit kann γ zum Beispiel so gewählt werden, daß size (γ) möglichst klein ist.

4.2.3.4 Beispiel (Das spezielle ElGamal-Verfahren) Wir wollen das ElGamal-Verfahren in der Gruppe $G = \mathbb{Z}_q^\times$ realisieren. Um für das Verfahren geeignete Kandidaten gemäß 4.2.3 zu finden, kann man folgende Möglichkeit wählen: Es sei $p \in \mathbb{P}$ groß und $f \in \mathbb{N}$ minimal mit $q = f \cdot p + 1 \in \mathbb{P}$. Wegen $q \in \mathbb{P}$ ist dann

$$\sharp\mathbb{Z}_q^\times = \varphi(q) = q - 1 = f \cdot p.$$

$\mathbb{Z}_q^\times$ ist also ebenfalls groß und als multiplikative Gruppe des endlichen Körpers $\mathbb{Z}_q$ zyklisch. Der große Primfaktor p in $\sharp\mathbb{Z}_q^\times = f \cdot p$ verhindert weiterhin Angriffe mit dem Pohlig-Hellman-Algorithmus (siehe Tabelle 4.1). Der Algorithmus sieht wie folgt aus:

Algorithmus `ElGamalZpSetup`

Eingabe : $q = f \cdot p + 1 \in \mathbb{P}$ genügend groß mit $p \in \mathbb{P}$ und $f \in \mathbb{N}$ minimal
Ausgabe: Der öffentliche und geheime Schlüssel

1: **repeat**
2: `Wähle` $\gamma \in \mathbb{N}\ 1 < \gamma < q$ `beliebig`
3: **until** $\gamma^f, \gamma^p \not\equiv 1 \bmod q$
4: `Wähle` $a \in \mathbb{N}, a < q$ `zufällig`
5: $\alpha := \gamma^a \bmod q$
6: **return** $(q, \gamma, \alpha), (q, a)$

Aufwand: $\mathcal{O}\left(\text{size}\,(q)^3\right)$

Algorithmus `ElGamalZpEncrypt`

Eingabe : Der öffentliche Schlüssel (q, γ, α) und die Nachricht $m \in \mathbb{Z}_q$
Ausgabe: Die zu m gehörige verschlüsselte Nachricht

`1:` `Wähle` $b \in \mathbb{N},\ 1 < b < q$ `zufällig`
`2:` $m_1 := \gamma^b \bmod q$
`3:` $m_2 := m \cdot \alpha^b \bmod q$
`4:` **return** (m_1, m_2)

Aufwand: $\mathcal{O}\left(\text{size}\,(q)^3\right)$

Algorithmus `ElGamalZpDecrypt`

Eingabe : Der geheime Schlüssel (q, a) und die Nachricht (m_1, m_2)
Ausgabe: Die entschlüsselte Nachricht m

`1:` **return** $m_2 \cdot m_1^{-a} \bmod q$

Aufwand: $\mathcal{O}\left(\text{size}\,(q)^3\right)$

4.2.3.5 Sicherheit Der schnellste bekannte Algorithmus zur Lösung des DLP in $\mathbb{Z}_q^\times$ ist nach [Buc99] eine Variante des Index-Calculus-Algorithmus, das General Number Field Sieve (GNFS), mit einer subexponentiellen Laufzeit in der Größenordnung von

$$L_q\left[\frac{1}{3}, \sqrt[3]{\frac{64}{9}}\right].$$

Das DLP in $\mathbb{Z}_q^\times$ kann also beliebig schwer gemacht werden durch genügend große q, empfohlen wird heutzutage $q \geq 2^{1024} \approx 10^{308}$.

4.2.3.6 Anschauliches Beispiel

(i) **Initialisierung** Es sind

$$p = 53 \text{ und } q = 2 \cdot p + 1 = 107$$

Primzahlen. Damit ist

$$\mathbb{Z}_{107}^\times \cong C_2 \times C_{53}$$

und jede Zahl γ zwischen 1 und 106 mit $\gamma^2, \gamma^{53} \not\equiv 1 \bmod 107$ ist ein Erzeuger von $\mathbb{Z}_{107}^\times$. Es ist

$$2^2 \equiv 4 \bmod 107 \text{ und } 2^{53} \equiv 106 \bmod 107,$$

also ist $\gamma = 2$ ein Erzeuger von $\mathbb{Z}_{107}^{\times}$. Wir wählen als geheimen Schlüssel $a = 73 < 106 = \sharp\mathbb{Z}_q^{\times}$. Damit ist

$$\alpha \equiv \gamma^a \equiv 2^{73} \equiv 24 \bmod 107.$$

Der öffentliche Schlüssel ist $(q, \gamma, \alpha) = (107, 2, 24)$.

(ii) **Verschlüsselung** Wir können die Zahlen $1, \ldots, 106 = \sharp\mathbb{Z}_q^{\times}$ verschlüsseln. Unsere Nachricht sei

$$m = 42.$$

Zum Verschlüsseln wird nun ein zufälliges

$$b = 54 < 106$$

gewählt und die verschlüsselte Nachricht (m_1, m_2) mit

$$\begin{aligned} m_1 &\equiv \gamma^b \equiv 2^{54} \equiv 105 \bmod 107 \\ m_2 &\equiv m \cdot \alpha^b \equiv 42 \cdot 24^{54} \equiv 62 \bmod 107 \end{aligned}$$

berechnet und gesendet.

(iii) **Entschlüsselung** Der Empfänger berechnet mit Hilfe des geheimen Schlüssels $a = 73$:

$$m \equiv m_2 \cdot m_1^{-a} \equiv 62 \cdot 105^{-73} \equiv 42 \bmod 107.$$

Es war hier

$$\alpha^b \equiv \gamma^{ab} \equiv m_1^a \equiv 83 \bmod 107$$

das gemeinsame Geheimnis (mask) von Sender und Empfänger und

$$m_1 \equiv \gamma^b \equiv 105 \bmod 107$$

der clue, aus dem man das gemeinsame Geheimnis γ^{ab} bei Kenntnis des geheimen Schlüssels a berechnen konnte.

Das DLP ist in $\mathbb{Z}_q$ einfacher zu lösen als in anderen abelschen Gruppen. Das liegt daran, daß $\mathbb{Z}_q$ mehr Struktur als allgemeine Gruppen besitzt und diese einfach zu erfassen ist. Daher ist man auf der Suche nach Gruppen, die dies nicht bieten, und man stieß dabei neben Elliptischen Kurven auch auf die Klassengruppen. Diese zeichnen sich schon einmal dadurch aus, daß man ihre Größe nicht effektiv berechnen kann, mehr noch, die Berechnung ihrer Größe würde darin sogar das DLP einfacher machen. Daß man Klassengruppen trotzdem für das ElGamal-Verfahren benutzen kann, wollen wir in den folgenden Kapiteln zeigen.
In Abschnitt 3.4 wurde gezeigt, daß das Rechnen in $\mathrm{Cl}\,(\Delta)$ effizient ist, die Darstellung von Idealklassen kann durch Reduktion klein gehalten werden.
Um mögliche Angriffe auf die Klassengruppenversionen des ElGamal-Verfahrens abzuwehren, genauer um sie schwer genug zu machen, müssen wir Aussagen über

die Größe der Klassengruppe treffen, bzw. noch schärfer: Wir müssen sicherstellen, daß $\mathrm{Cl}(\Delta)$ einen genügend großen Primfaktor enthält. Wir haben allerdings nur wenig Kontrolle über die Klassenzahl. Es gibt zur Zeit nicht einmal einen probabilistisch effizienten Algorithmus, der Diskriminanten erzeugt, deren zugehörige Klassenzahlen bestimmte interessante Eigenschaften haben, wie zum Beispiel einen großen Primfaktor. Die meisten derzeit verfügbaren Aussagen über die Größe und Struktur der Klassengruppe stützen sich auf Vermutungen von Cohen und Lenstra ([CL84], [CM87]) und Wahrscheinlichkeiten. Gerade diese ungewisse Struktur wird uns dann aber in Fragen der Sicherheit wieder zugute kommen. Es wird sich auf der Basis einiger (empirisch gestützter) Annahmen zeigen, daß man durch geeignete Wahl der Diskriminante das DLP in der zugehörigen Klassengruppe beliebig schwer machen kann.

Kapitel 5

ElGamal für $\Delta < 0$

Nach den Vorbereitungen aus den letzten Kapiteln können wir nun die ElGamal-Verschlüsselung einfach auf Klassengruppen imaginärquadratischer Zahlkörper übertragen. Dabei benutzen wir $\mathrm{Cl}(\Delta)$ als Gruppe G im allgemeinen ElGamal-Verfahren aus Abschnitt 4.2.3. Wie wir in Corollar 3.3.12 gesehen haben, können wir dabei reduzierte Ideale als eindeutige Vertreter der Klassengruppe effizient berechnen. Das Rechnen in Klassengruppen haben wir in Abschnitt 3.4 vorgestellt. Nach der Einführung des Verschlüsselungsalgorithmus in Abschnitt 5.1 untersuchen wir, wie die Sicherheit dieses Verfahrens von der Wahl der Diskriminante abhängt. In Abschnitt 5.3 werden wir das Verfahren anhand eines Beispiels veranschaulichen.

5.1 Der Verschlüsselungsalgorithmus

Algorithmus `ElGamalIQFSetup`

Eingabe : Δ genügend groß
Ausgabe: Der öffentliche und geheime Schlüssel

`1:` `Wähle` $[\mathfrak{c}] \in \mathrm{Cl}(\Delta)$ `beliebig`

`2:` `Wähle` $a \in \mathbb{N}, a < \sqrt{|\Delta|}$ `zufällig`

`3:` $[\mathfrak{a}] := [\mathfrak{c}]^a$

`4:` **return** $(\Delta, [\mathfrak{c}], [\mathfrak{a}]), (\Delta, a)$

Aufwand: $\mathcal{O}\left(\mathrm{size}(\Delta)^3\right)$

Algorithmus `ElGamalIQFEncrypt`

Eingabe: Der öffentliche Schlüssel $(\Delta, [\mathfrak{c}], [\mathfrak{a}])$ und die Nachricht $\mathfrak{m} \in \mathrm{P}_\Delta$
Ausgabe: Die zu $\mathfrak{m}$ gehörige verschlüsselte Nachricht

1: `Wähle` $b \in \mathbb{N}, b < q$ `zufällig`
2: $[\mathfrak{m}_1] := [\mathfrak{c}]^b$
3: $[\mathfrak{m}_2] := [\mathfrak{m}] \cdot [\mathfrak{a}]^b$
4: **return** $([\mathfrak{m}_1], [\mathfrak{m}_2])$

Aufwand: $\mathcal{O}\left(\mathrm{size}\,(\Delta)^3\right)$

Algorithmus `ElGamalIQFDecrypt`

Eingabe: Der geheime Schlüssel (Δ, a) und die Nachricht $([\mathfrak{m}_1], [\mathfrak{m}_2])$
Ausgabe: Die entschlüsselte Nachricht $\mathfrak{m}$

1: $[\mathfrak{m}] := [\mathfrak{m}_2] \cdot [\mathfrak{m}_1]^{-a}$
2: **return** $\mathfrak{m}$

Aufwand: $\mathcal{O}\left(\mathrm{size}\,(\Delta)^3\right)$

5.2 Sicherheit

5.2.1 Definition Es sei $B \in \mathbb{N}$. Eine natürliche Zahl n heißt **B-glatt**, falls

$$p \mid n \Longrightarrow p \leq B \quad \forall\, p \in \mathbb{P}.$$

Wir nennen n **sehr glatt**, falls B sehr klein ist.

5.2.2 Angriffsmöglichkeiten Es gibt folgende Angriffsmöglichkeiten auf den in Abschnitt 5.1 vorgestellten Verschlüsselungsalgorithmus:

(i) Index-Calculus-Methoden (siehe [Coh95, 5.5]) sind probabilistisch subexponentiell in Δ. In [Vol00] wird ein erwarteter Aufwand von $L_{|\Delta|}\left[\frac{1}{2}, \frac{3}{4}\sqrt{2}\right]$ bewiesen, es wird sogar vermutet, daß für eine Klassengruppenversion des MPQS[1] ([Jac99]) eine erwartete Laufzeit von $L_{|\Delta|}\left[\frac{1}{2}, 1\right]$ ausreicht.

(ii) Sogenannte Quadratwurzelalgorithmen wie Shanks Babystep-Giantstep-Algorithmus (deterministisch) und Pollards ρ- und λ- (auch Känguruh-)

[1] Multi Polynomial Quadratic Sieve

Methoden (probabilistisch) haben eine (erwartete) exponentielle Laufzeit proportional zu ord[$\mathfrak{c}$]. Siehe dazu [MvOV97, Kap. 3].

(iii) Ist die Klassenzahl sehr glatt, etwa q ihr größter Primfaktor, so kann man diese erst mit einer abgewandelten $(p-1)$-Methode mit einem Aufwand von $\mathcal{O}(q)$ (siehe dazu [Ham02, Alg. 5.1]) berechnen und kann dann das DLP mit Hilfe des Pohlig-Hellman-Algorithmus schnell lösen, da dieser ebenfalls schneller als eine Index-Calculus-Methode ist, wenn $\mathrm{h}(\Delta)$ sehr glatt ist $\left(\mathcal{O}\left(\sum_{i=1}^{k} e_i \left(\mathrm{size}(n) + \sqrt{p_i}\right)\right)\right.$ für $n = \prod_{i=1}^{k} p_i^{e_i}$, siehe [MvOV97, Kap. 3]$\left.\right)$.

Alle Eigenschaften, die die Sicherheit des in 5.1 vorgestellten Verfahrens erhöhen, hängen also letztendlich von der Wahl der Diskriminante Δ ab, nämlich davon

(i) wie groß $\mathrm{Cl}(\Delta)$ ist,

(ii) wie groß die Wahrscheinlichkeit ist, daß ein zufällig gewähltes Element in $\mathrm{Cl}(\Delta)$ große Ordnung hat,

(iii) wie groß der größte Primfaktor von $\mathrm{h}(\Delta)$ ist.

Satz 3.2.11 und 3.2.10 zeigen, daß wir durch Wahl großer Diskriminanten entsprechend große Klassengruppen bekommen. Das schafft auch die nötigen Voraussetzungen für das Vorhandensein von Elementen großer Ordnung. Als nächstes müssen wir dazu sicherstellen, daß die Klassengruppe einen großen zyklischen Faktor hat.

5.2.1 Der zyklische Anteil einer imaginärquadratischen Klassengruppe

Allein über die Menge der Elemente der Ordnung 2 in der Klassengruppe gibt es konkrete Aussagen:

5.2.1.1 Definition Es sei $\mathrm{Cl}_2(\Delta)$ die Untergruppe von $\mathrm{Cl}(\Delta)$, welche die Elemente der Ordnung ≤ 2 enthält, und $\mathrm{h}_2(\Delta)$ deren Ordnung. Weiterhin bezeichne $\mathrm{Cl}_{\mathrm{odd}}(\Delta)$ den Anteil von $\mathrm{Cl}(\Delta)$ dessen Elemente ungerade Ordnung besitzen und $\mathrm{h}_{\mathrm{odd}}(\Delta)$ die Ordnung von $\mathrm{Cl}_{\mathrm{odd}}(\Delta)$.

5.2.1.2 Lemma *Es sei t die Anzahl der unterschiedlichen Primfaktoren von Δ. Dann ist*

$$\mathrm{h}_2(\Delta) = 2^{\mathrm{t}-1}, \text{ also } \mathrm{Cl}_2(\Delta) \cong \mathrm{C}_2^{\mathrm{t}-1},$$

$\mathrm{Cl}(\Delta)$ enthält also genau $t-1$ gerade Faktoren.

Beweis: [Has63] □

5.2.1.3 Corollar *Es sei* $|\Delta| \in \mathbb{P}$ *und* $\Delta \equiv 1 \bmod 4$. *Dann gilt:* $2 \not| \, \mathrm{h}(\Delta)$.

Man beachte, daß es auch Elemente gerader Ordnung außerhalb von $\mathrm{Cl}_2(\Delta)$ geben kann. Einige Möglichkeiten, den Anteil mit Elementen gerader Ordnung von $\mathrm{Cl}(\Delta)$ in den Griff zu bekommen, liefern die folgenden Aussagen.

5.2.1.4 Lemma *Es sei* $\Delta = -pq$ *mit* $p, q \in \mathbb{P}$, $pq \equiv 3 \bmod 4$ *und* $\left(\frac{p}{q}\right) = -1$. *Dann gilt* $2 \parallel \mathrm{h}(\Delta)$.

Beweis: [Réd28] □

5.2.1.5 Lemma *Es sei* $\Delta = -pq$ *mit* $p, q \in \mathbb{P}$, $p \equiv 1 \bmod 8$, $p + q \equiv 8 \bmod 16$ *und* $\left(\frac{p}{q}\right) = -1$. *Dann gilt* $2^3 \parallel \mathrm{h}(\Delta)$.

Beweis: [Kap76] □

Diskriminanten wie in 5.2.1.3, 5.2.1.4 und 5.2.1.5 haben neben der Kontrolle über den geraden Anteil der Klassenzahl den weiteren Vorteil, daß man von ihnen sofort weiß, daß sie quadratfrei sind. Der Test auf Quadratfreiheit einer Diskriminante ist i. a. ähnlich schwer wie ihre Faktorisierung. Daher ist es sowieso die beste Strategie, die Diskriminante aus gewählten Primzahlen zusammenzusetzen, da ein Primzahltest effizient durchgeführt werden kann. Wird der gerade Anteil der Klassengruppe klein gehalten, verringert sich gleichzeitig die Wahrscheinlichkeit, daß die Klassenzahl glatt ist.
Obwohl wir die Diskriminanten hier einschränken, zeigen Beispielrechnungen ([Ham02, 5.2.4, S. 66]), daß dies die folgenden Vermutungen nicht verzerrt.

5.2.1.6 Vermutung (siehe [CM87] und [CL84]) Es sei $M \in \mathbb{N}$ und Δ eine zufällig gewählte imaginärquadratische Diskriminante mit $|\Delta| \leq M$.

(i) Für die Wahrscheinlichkeit Pr, daß $\mathrm{Cl}_{\mathrm{odd}}(\Delta)$ zyklisch ist, gilt:

$$\lim_{M \to \infty} \Pr\left[\ \mathrm{Cl}_{\mathrm{odd}}(\Delta) \text{ ist zyklisch } \right] = \frac{\zeta(2)\,\zeta(3)}{3 \cdot (2)_\infty\, \zeta(6)} \left(\prod_{k=2}^{\infty} \zeta(k) \right)^{-1} \approx 0,977575,$$

wobei ζ die Riemannsche Zeta-Funktion ist und

$$(p)_\alpha = \prod_{k=1}^{\alpha} \left(1 - p^{-k}\right) \quad \forall\, p \in \mathbb{N}, p \geq 2 \text{ und } \alpha \in \mathbb{N} \cup \{\infty\}.$$

(ii) Es sei $p \in \mathbb{P}$ ungerade, $r \in \mathbb{N}$. Dann gilt:

$$\lim_{M \to \infty} \Pr[\ \operatorname{rank}(\mathrm{Cl}_p(\Delta)) = r\ ] = \frac{(p)_\infty}{p^{r^2}\,(p)_r^2},$$

wobei $\mathrm{Cl}_p(\Delta)$ die p-Sylowgruppe von $\mathrm{Cl}(\Delta)$ ist. Beispiel:

- $p = 3$
  - $r = 0 : 0{,}560126$
  - $r = 1 : 0{,}420095$
  - $r = 2 : 0{,}019692$
  - $r \geq 3 : 0{,}000087$
- $p = 5$
  - $r = 0 : 0{,}760333$
  - $r = 1 : 0{,}237604$
  - $r \geq 2 : 0{,}002063.$

Diese Vermutungen, die durch umfassende empirische Untersuchungen gestützt werden, zeigen also zwei Dinge: Der ungerade Anteil der Klassengruppe eines imaginärquadratischen Zahlkörpers ist fast immer zyklisch, und wenn nicht, dann enthält er mit sehr großer Wahrscheinlichkeit eine große zyklische Untergruppe. Diese Tatsache schafft entscheidende Voraussetzungen für die Anwendung des ElGamal-Verfahrens, da es nun mit großer Wahrscheinlichkeit Elemente großer Ordnung in $\mathrm{Cl}(\Delta)$ gibt, nämlich die Erzeuger der großen zyklischen Untergruppe. Da kein effizienter Algorithmus bekannt ist, die Ordnung eines Gruppenelementes zu berechnen, müssen wir nun sicherstellen, daß wir auch solche Elemente mit hoher Wahrscheinlichkeit finden. Dazu betrachten wir folgendes

5.2.1.7 Lemma *Es sei G eine abelsche Gruppe mit der Primfaktorzerlegung der Gruppenordnung*

$$\sharp G = \prod_{i=1}^{n} p_i^{e_i}$$

und $\gamma \in G$. Dann gilt $\forall\ 1 \leq j \leq n$:

$$\Pr[\ p_j \mid \operatorname{ord}(\gamma)\ ] = 1 - \frac{1}{p_j^{e_j}}.$$

Beweis: Nach dem Hauptsatz für endliche abelsche Gruppen läßt sich G entsprechend seiner Primfaktoren darstellen als

$$G \cong G_1 \times \ldots \times G_n \text{ mit } \sharp G_i = p_i^{e_i} \quad \forall\ 1 \leq i \leq n,$$

wobei wiederum $\forall\ 1 \leq i \leq n$ gilt:

$$G_i \cong C_{p_i^{e_{i,1}}} \times \ldots \times C_{p_i^{e_{i,n_i}}} \text{ mit } \sum_{j=1}^{n_i} e_{ij} = e_i.$$

Es gilt weiterhin: $\forall\ g_i \in G_i : \mathrm{ord}\,(g_i) \mid p_i^{e_i}$. Damit gilt für das isomorphe Bild von γ im direkten Produkt $(\gamma_1, \ldots, \gamma_n) \in G_1 \times \ldots \times G_n$, daß $\mathrm{ord}\,(\gamma_i) \in \{1, p_i, \ldots, p_i^{e_i}\}$ und damit

$$p_i \mid \mathrm{ord}\,(\gamma) \Longleftrightarrow \gamma_i \neq (1, \ldots, 1) \in C_{p_i^{e_{i1}}} \times \ldots \times C_{p_i^{e_{in_i}}}$$

wegen

$$\mathrm{ord}\,\gamma = \prod_{i=1}^{n} \mathrm{ord}\,\gamma_i.$$

Das sind $p_i^{e_i} - 1$ Möglichkeiten für γ_i, also

$$(p_i^{e_i} - 1) \prod_{j=1, i \neq j}^{n} p_j^{e_j} = \sharp G - \frac{\sharp G}{p_i^{e_i}}$$

Möglichkeiten für γ. Daraus folgt die Behauptung. □

Wenn wir also eine Klassengruppe mit einem großen zyklischen Faktor haben, so hängt die Wahrscheinlichkeit, daß ein zufälliges Element in $\mathrm{Cl}\,(\Delta)$ eine große Ordnung hat, davon ab, ob $\mathrm{h}\,(\Delta)$ von großen Primfaktoren geteilt wird. Wir müssen also ausschließen, daß die Klassenzahl sehr glatt ist. Dies verhindert dann gleichzeitig auch Angriffe mit dem Pohlig-Hellman-Algorithmus.

5.2.2 Die Glattheit einer imaginärquadratischen Klassenzahl

5.2.2.1 Vermutung (siehe [CM87]) Es sei $M \in \mathbb{N}$ und Δ eine zufällig gewählte Diskriminante eines imaginärquadratischen Zahlkörpers mit $|\Delta| \leq M$.

(i) Es sei $m \in \mathbb{N}$ ungerade. Dann gilt:

$$\lim_{M \to \infty} \Pr\,[\ m \mid \mathrm{h}_{\mathrm{odd}}\,(\Delta)\ ] = \prod_{p^e \parallel m} \frac{1 - (p)_\infty}{(p)_{e-1}}.$$

Beispiel:

- $\Pr\,[\ 3 \mid \mathrm{h}_{\mathrm{odd}}\,(\Delta)\ ] = 0{,}439874$
- $\Pr\,[\ 5 \mid \mathrm{h}_{\mathrm{odd}}\,(\Delta)\ ] = 0{,}239667$
- $\Pr\,[\ 7 \mid \mathrm{h}_{\mathrm{odd}}\,(\Delta)\ ] = 0{,}163204$
- $\Pr\,[\ 9 \mid \mathrm{h}_{\mathrm{odd}}\,(\Delta)\ ] = 0{,}159811$

(ii) Die obige Gleichung vereinfacht sich für $m = p \in \mathbb{P}$ wie folgt:

$$\lim_{M\to\infty} \Pr[\ p \mid \mathrm{h}_{\mathrm{odd}}(\Delta)\ ] = 1 - \prod_{k=1}^{\infty}\left(1 - \frac{1}{p^k}\right). \tag{5.1}$$

Dabei ist

$$\Pr[\ p \mid \mathrm{h}_{\mathrm{odd}}(\Delta)\ ] < \frac{1}{p} + \frac{1}{p^2} = \frac{1}{p}\left(1 + \frac{1}{p}\right). \tag{5.2}$$

5.2.2.2 Vermutung Es sei $M \in \mathbb{N}$ und Δ eine zufällig gewählte imaginärquadratische Diskriminante mit $|\Delta| \leq M$.

(i) Es sei $p \in \mathbb{P}$ ungerade, $e \in \mathbb{N}$. Dann gilt in Erweiterung zu 5.2.2.1:

$$\lim_{M\to\infty} \Pr[\ p^e \mid \mathrm{h}_{\mathrm{odd}}(\Delta)\ ] \leq \frac{1}{p^e} + \frac{1}{p^{e+1}} = \frac{1}{p^e}\left(1 + \frac{1}{p}\right). \tag{5.3}$$

(ii) Es seien $p_1, \ldots, p_n \in \mathbb{P}$ ungerade und paarweise verschieden, $e_1, \ldots e_n, \in \mathbb{N}$. Dann sind die Wahrscheinlichkeiten in (5.1) unabhängig voneinander:

$$\lim_{M\to\infty} \Pr\left[\ \prod_{i=1}^{n} p_i^{e_i} \mid \mathrm{h}_{\mathrm{odd}}(\Delta)\ \right] = \prod_{i=1}^{n} \Pr[\ p_i^{e_i} \mid \mathrm{h}(\Delta)\ ].$$

Berechnungen, die diese Vermutung stützen, finden sich in [Bue84].

Wir wollen nun die Glattheit einer Klassenzahl mit der Glattheit einer natürlichen Zahl vergleichen. Wegen $\mathrm{h}(\Delta) \approx \sqrt{|\Delta|}$ müssen wir dabei Klassenzahlen mit $\Delta \approx -M$ und natürliche Zahlen $n \approx \sqrt{M}$ miteinander vergleichen. Es gilt der folgende

5.2.2.3 Satz *Es seien $M, B \in \mathbb{N}$, Δ eine zufällig gewählte imaginärquadratische Diskriminante mit $|\Delta| \leq M$ und n eine Zufallszahl mit $n \leq \sqrt{M}$. Unter den beiden Annahmen 5.2.2.1 und 5.2.2.2 gilt dann für $M \to \infty$:*

$$\Pr[\ \mathrm{h}_{\mathrm{odd}}(\Delta)\ \textit{ist B-glatt}\ ] \leq c \ln(\ln M) \cdot \Pr[\ n\ \textit{ist B-glatt}\ ]$$

wobei $c \approx 1,082762$.

Beweis: [Ham02, S. 60] □

5.2.2.4 Bemerkung Wenn wir uns auf $M \leq 2^{4300}$ beschränken, ist $c \ln(\ln M) < 8$. Die Wahrscheinlichkeit, daß die Klassenzahl einer zufälligen Diskriminante Δ mit $|\Delta| \leq M$ B-glatt ist, ist also höchstens 8 mal so groß wie die Wahrscheinlichkeit, daß eine Zufallszahl $n \leq \sqrt{M}$ B-glatt ist.

5.2.2.5 Lemma *Die Wahrscheinlichkeit für eine natürliche Zahl n, B-glatt zu sein, kann man mit Hilfe der* **Dickmannschen Funktion** $\vartheta(u)$ *annähern. Sie ist die stetige Lösung von*

$$\begin{aligned} \vartheta(u) &= 1 \quad \textit{für} \quad 0 \leq u \leq 1 \\ \vartheta(u-1) + u\vartheta'(u) &= 0 \quad \textit{für} \quad u > 1. \end{aligned}$$

und kann numerisch durch

$$\vartheta(u) = \frac{1}{u}\int_{u-1}^{u} \vartheta(t)\,dt \text{ oder } \vartheta(u) = 1 - \int_{1}^{u} \frac{\vartheta(t-1)}{t}dt$$

berechnet werden.

Beweis: [Bue84] □

5.2.2.6 Satz *Es sei $n \leq \sqrt{M}$ und $u = \frac{\ln\sqrt{M}}{\ln B}$. Dann ist*

$$\Pr[\ n \textit{ ist } B\textit{-glatt }\ ] = \vartheta(u)\left(1 + \mathcal{O}_\varepsilon\left(\frac{\operatorname{size}(u+1)}{\operatorname{size}(B)}\right)\right),$$

für $B \geq 2$, $1 \leq u \leq \exp\left((\ln B)^{3/5-\varepsilon}\right)$ und $\varepsilon > 0$. Dabei ist die $\mathcal{O}$-Konstante von einem $\varepsilon > 0$ abhängig.

Beweis: [HS97, Satz 1] □

Wir wollen hier der Einfachheit halber annehmen, daß

$$\Pr[\ n \text{ ist } B\text{-glatt }\ ] \approx \vartheta(u).$$

Es gilt also

$$\Pr[\ \mathrm{h}(\Delta) \text{ ist } B\text{-glatt }\ ] \leq 8\vartheta(u), \tag{5.4}$$

wobei

$$B^u = \sqrt{M} \approx c\sqrt{|\Delta|} \cdot \frac{\mathrm{h}_{\mathrm{odd}}(\Delta)}{\mathrm{h}(\Delta)} \tag{5.5}$$

mit $c \approx 0,461559$ die erwartete Größe der Klassenzahl ist. Wählen wir unsere Diskriminante nach den Voraussetzungen in 5.2.1.3, 5.2.1.4 oder 5.2.1.5, so ist

$$\frac{\mathrm{h}(\Delta)}{\mathrm{h}_{\mathrm{odd}}(\Delta)} \in \{2^0, 2^1, 2^3\}.$$

Dementsprechend sei im Folgenden $e \in \{0, 1, 3\}$. Dann gilt nach (5.5) und (5.4)

$$\Pr[\ \mathrm{h}(\Delta) \text{ ist } B\text{-glatt }\ ] \leq 8\vartheta(u),$$

für

$$|\Delta| \approx (2 \cdot 2^e)^2 \cdot B^{2u} = 2^{2(e+1)} B^{2u}.$$

Wir können also $|\Delta|$ so groß wählen, daß zu gegebenem B die Wahrscheinlichkeit, daß $\mathrm{h}(\Delta)$ B-glatt ist, beliebig nahe bei 0 liegt.
Es gilt:

$$\Pr[\ \mathrm{h}(\Delta)\ \text{ist } B\text{-glatt}\ ] \leq 8\vartheta(u)$$

für

$$|\Delta| \approx 2^{2(e+1)} B^{2u} \leq 2^{4300}.$$

Nach den Betrachtungen in [Ham02] benötigt der $(p-1)$-Algorithmus pro Durchlauf mit einem bestimmten Ideal im Durchschnitt $\frac{q}{\ln 2}$ Gruppenoperationen, wobei q der größte Primfaktor in $\mathrm{h}(\Delta)$ ist. Der maximale Aufwand, den ein Angreifer bereit ist, in einen Durchlauf zu stecken, sei mit $\mathrm{W}_{\max}$ bezeichnet. Den Gesamtaufwand für die Bestimmung von $\mathrm{h}(\Delta)$ wollen wir mit $\mathrm{W}_{\text{total}}$ bezeichnen. B sei diejenige Glattheitsschranke, mit der der $(p-1)$-Algorithmus mit einem Aufwand von $\mathrm{W}_{\max}$ noch Erfolg hat, also $B = \mathrm{W}_{\max} \ln 2$. Es gilt dann

$$\mathrm{W}_{\text{total}} = \frac{\mathrm{W}_{\max}}{\Pr[\ \mathrm{h}(\Delta)\ \text{ist } B\text{-glatt}\ ]}. \tag{5.6}$$

5.2.2.7 Beispiel zur Wahl von Δ Wir nehmen an, daß der Angreifer insgesamt einen Aufwand von $\mathrm{W}_{\text{total}} = 2^{64}$ Gruppenoperationen in Kauf nehmen will, das entspricht der Arbeit, um eine 1024-Bit-Zahl zu faktorisieren. Desweiteren nehmen wir an, daß er für einen Durchlauf des $(p-1)$-Algorithmus maximal $\mathrm{W}_{\max} = 2^{42}$ Operationen zuläßt, was der Arbeit für die Faktorisierung einer 512-Bit-Zahl entspricht. Dies korrespondiert zu einer Glattheitsschranke $B = 2^{42} \ln 2$. Nach (5.6) gilt dann

$$\Pr[\ \mathrm{h}(\Delta)\ \text{ist } B\text{-glatt}\ ] = \frac{\mathrm{W}_{\max}}{\mathrm{W}_{\text{total}}} \approx 2^{-22} = 8\vartheta(u),$$

also ist $\vartheta(u) = 2^{-25}$, was für $u \approx 8$ erfüllt ist. Daher muß also

$$|\Delta| \approx 2^{2(e+1)} B^{16}$$

sein, das sind 666 Bit für $e = 0$ und 672 Bit für $e = 3$.
In [Hüh00b] wurden die Laufzeiten der jeweils besten Algorithmen zum Angriff verschiedener Verschlüsselungssysteme getestet, das heißt das GNFS[2] zum Angriff auf RSA und ElGamal in $\mathbb{Z}_q$ und ein auf Zahlkörper übertragenes MPQS[3] für ElGamal in Klassengruppen. Dabei wurde festgestellt, daß die Arbeit zum Faktorisieren einer 1024-Bit-Zahl der Form $p \cdot q$ mit $p, q \in \mathbb{P}$ ca. $3,55 \cdot 10^{10}$ MIPS-Jahre beträgt, genauso viel wie für die Lösung des DLP in $\mathrm{h}(\Delta)$ mit $\Delta \approx -2^{686}$. In unserem Fall heißt das, daß Δ mindestens 686 Stellen haben muß, was eine Abwehr gegen Angriffe

u	Anzahl der Klassenzahlen	Anteil der Klassenzahlen	$\vartheta(u)$
1,5	63089	0,58756	0,59453
2,0	32047	0,29846	0,30685
2,5	13380	0,12461	0,13033
3,0	4879	0,04544	0,04861
3,5	1580	0,01472	0,01623
4,0	472	0,00440	0,00491
4,5	120	0,00112	0,00137
5,0	30	0,00028	0,00035
5,5	5	0,00005	0,00009
6,0	1	0,00001	0,00002
6,5	1	0,00001	0,00000

Tabelle 5.1: Diskriminanten mit $\sqrt{|\Delta|}^{\frac{1}{u}}$-glatter Klassenzahl.

mit dem Pohlig-Hellman-Algorithmus einschließt. Dann ist das ElGamal-Verfahren mindestens genauso sicher wie das RSA-Verfahren mit $n \approx 2^{1024}$.

In der Tabelle 5.1 aus [Ham02] wurden die Klassenzahlen aller primen Diskriminanten Δ mit $10^{48} < \Delta < 10^{48} - 47523087$ und $\Delta \equiv 1 \bmod 8$ berechnet und faktorisiert. In diesem Intervall gibt es 107374 solcher Diskriminanten. Tabelle 5.1 zeigt, daß in der Praxis die Glattheits-Wahrscheinlichkeiten für natürliche Zahlen und Klassenzahlen fast gleich sind, die Abschätzung 5.4 ist also immer noch sehr grob und wird durch Berechnungen nicht nur bestätigt, sondern sogar übertroffen.

$q = \frac{\mathrm{h}(\Delta)}{\mathrm{ord}[\mathfrak{a}]}$	$\mathfrak{a} = (2,1)$		$\mathfrak{a} = (3,1)$	
	Anzahl	Anteil	Anzahl	Anteil
$q = 1$	86599	0,7537	38857	0,7551
$10^0 < q < 10^1$	22718	0,1977	10073	0,1957
$10^1 \leq q < 10^2$	5007	0,0436	2268	0,0441
$10^2 \leq q < 10^3$	522	0,0045	245	0,0048
$10^3 \leq q < 10^4$	50	0,0004	17	0,0003
$10^4 \leq q < 10^5$	6	0,0000	2	0,0000
Gesamt	114902	1,0000	51462	1,0000

Tabelle 5.2: Ordnung der von $[\mathfrak{a}]$ erzeugten Untergruppen, $|\Delta| \approx 10^{32}$.

Die Tatsache, daß Klassenzahlen ähnlich glatt sind wie natürliche Zahlen, wirkt sich auch positiv auf die in 5.2.1 angesprochene Wahrscheinlichkeit aus, daß eine zufällig gewählte Idealklasse in $\mathrm{h}(\Delta)$ eine große Ordnung hat. In [Ham02] wurde diese Größe

[2] General Number Field Sieve

[3] Multiple Polynomial Quadratic Sieve

$q = \frac{h(\Delta)}{ord[\mathfrak{a}]}$	$\mathfrak{a} = (1009, 1)$		$\mathfrak{a} = (1000003, 1)$	
	Anzahl	Anteil	Anzahl	Anteil
$q = 1$	43562	0,7535	53013	0,7555
$10^0 < q < 10^1$	11481	0,1986	13784	0,1964
$10^1 \leq q < 10^2$	2475	0,0428	3043	0,0434
$10^2 \leq q < 10^3$	263	0,0045	288	0,0041
$10^3 \leq q < 10^4$	27	0,0005	43	0,0006
$10^4 \leq q < 10^5$	2	0,0000	2	0,0000
Gesamt	57810	1,0000	70173	1,0000

Tabelle 5.3: Ordnung der von $[\mathfrak{a}]$ erzeugten Untergruppen, $|\Delta| \approx 10^{32}$.

$q = \frac{h(\Delta)}{ord[\mathfrak{a}]}$	$\mathfrak{a} = (2, 1)$		$\mathfrak{a} = (3, 1)$	
	Anzahl	Anteil	Anzahl	Anteil
$q = 1$	81093	0,7552	29256	0,7530
$10^0 < q < 10^1$	21667	0,1971	7678	0,1976
$10^1 \leq q < 10^2$	4621	0,0430	1701	0,0438
$10^2 \leq q < 10^3$	445	0,0041	196	0,0050
$10^3 \leq q < 10^4$	41	0,0004	19	0,0005
$10^4 \leq q < 10^5$	7	0,0000	1	0,0000
Gesamt	107374	1,0000	38851	1,0000

Tabelle 5.4: Ordnung der von $[\mathfrak{a}]$ erzeugten Untergruppen, $|\Delta| \approx 10^{48}$.

an Beispielen untersucht. Für Diskriminanten wie in Tabelle 5.1 ist $(a, b) = (2, 1)$ nach Satz 3.1.9 ein Ideal, denn

$$\frac{b^2 - \Delta}{4a} = \frac{1 - \Delta}{8} \in \mathbb{Z}.$$

Die Berechnungen in Tabelle 5.2 zeigen, daß $[(2, 1)]$ mit hoher Wahrscheinlichkeit eine sehr große Ordnung hat. Weitere Berechnungen wurden für andere Ideale (Tabelle 5.3) und für andere Bereiche der Diskriminanten (Tabelle 5.4) durchgeführt, um zu zeigen, daß es sich dabei nicht um einen Zufall handelt.

5.2.2.8 Zusammenfassung

(i) $h(\Delta)$ wird groß, wenn $|\Delta|$ groß wird.

(ii) $Cl(\Delta)$ enthält mit großer Sicherheit einen großen zyklischen Faktor. Die Wahrscheinlichkeit, daß ein beliebiges Element einer Klassengruppe fast die gesamte Gruppe erzeugt, ist groß.

(iii) Die Wahrscheinlichkeit, daß $h(\Delta)$ B-glatt ist kann durch die Wahl von Δ beliebig klein gehalten werden. Der gerade Anteil von $h(\Delta)$ kann kontrolliert werden.

5.3 Beispiel

(i) **Initialisierung**

(a) Wir finden eine Primzahl

$$\Delta := -40031 \equiv 1 \bmod 8.$$

Δ ist damit quadratfrei und Diskriminante des imaginärquadratischen Zahlkörpers $\mathbb{Q}\left(\sqrt{\Delta}\right)$. Wegen $-\Delta \in \mathbb{P}$ folgt mit Corollar 5.2.1.3, daß $\mathrm{h}(\Delta)$ ungerade ist, $\mathrm{Cl}(\Delta)$ hat also keine geraden Faktoren. In einem realistischen Fall ist die Diskriminante natürlich so groß, daß man $\mathrm{Cl}(\Delta)$ praktisch nicht berechnen kann. Für $\Delta = -40031$ kann man aber leicht nachrechnen, daß $\mathrm{Cl}(\Delta) \cong C_{311}$. Wir werden diese Information aber nicht benutzen, da sie im Normalfall nicht bekannt ist. Die nach Satz 3.2.10 erwartete Größe der Klassengruppe ist

$$0{,}461559 \cdot \sqrt{|\Delta|} = 0{,}461559 \cdot \sqrt{40031} \approx 92.$$

Voraussage und Wirklichkeit scheinen hier noch sehr weit auseinander zu liegen. Weil wir sehr kleine Klassenzahlen haben, ist ein Faktor 3 noch von großem Gewicht. Bei realistischen Größen von $\mathrm{h}(\Delta)$ spielt er aber kaum noch eine Rolle.

(b) Als nächstes wollen wir bestimmen, welches die maximal Zahl ist, die wir in einem Schritt verschlüsseln können. Wie in Lemma 2.2.5 gezeigt wurde, ist ein Ideal (a, b) mit

$$a \leq \frac{\sqrt{|\Delta|}}{2} \approx 100$$

reduziert. Wir können also keine Zahl $a > 100$ verschlüsseln, da das zugehörige Ideal (a, b) möglicherweise nicht mehr reduziert ist. Ein reduziertes Ideal ist nach Corollar 3.3.12 eindeutig und wir können es in einer Klasse durch Reduktion effizient finden.

Wenn wir $a \leq 100$ verschlüsseln wollen, müssen wir weiterhin eine Wurzel von Δ modulo $4a$ berechnen. Falls eine Wurzel überhaupt existiert, kann man sie nur effektiv berechnen, falls a eine Primzahl mit $a \equiv 1, 3, 5, 7 \bmod 8$ ist. Mit der in 4.1 vorgestellten Abstandseinbettung (zusätzlich $a \not\equiv 1 \bmod 8$) können wir daher nur $a \leq 79$ verschlüsseln.

(c) Da $\mathrm{h}(\Delta)$ nicht viel größer als $\sqrt{|\Delta|} \approx 200$ sein wird, genügt es wenn die Exponenten a und b für Elemente der Klassengruppe kleiner als 200 sind.

(d) $(2, 1)$ ist wegen Satz 3.1.9 ein Ideal, denn es ist

$$\Delta \equiv 1 \bmod 8$$

und damit

$$\frac{b^2 - \Delta}{4 \cdot a} = \frac{1 - \Delta}{8} \in \mathbb{Z}.$$

Wir haben in den Tabellen 5.2 und 5.4 gesehen, daß $\mathfrak{c} := [(2,1)]$ mit großer Wahrscheinlichkeit eine große Ordnung in $\mathrm{Cl}(\Delta)$ hat. In der Tat ist $\langle[\mathfrak{c}]\rangle = \mathrm{Cl}(\Delta)$ wegen $\mathrm{h}(\Delta) = 311 \in \mathbb{P}$, was man normalerweise aber nicht weiß.

(e) Es sei

$$a = 112 < 200 \text{ der geheime Schlüssel.}$$

Damit ist

$$[\mathfrak{a}] = [\mathfrak{c}]^a = [(2,1)]^{112} = [(63,-17)]\,.$$

(f) Wir erhalten den öffentlichen Schlüssel

$$(\Delta, [\mathfrak{c}], [\mathfrak{a}]) = (-40031, [(2,1)]\,, [(63,-17)])$$

und den geheimen Schlüssel

$$(\Delta, a) = (-40031, 112).$$

(ii) **Verschlüsselung**

(a) Unsere Nachricht sei $m = 42 \leq 79$. Wir finden $a = 53$ als nächstgrößere Primzahl mit $\left(\frac{\Delta}{a}\right) = 1$ und $a \equiv 5 \bmod 8$ und $d = -11$ als Entfernung von a zur eigentlichen Nachricht m. Nun läßt sich leicht eine Wurzel $b = 14$ von Δ modulo a berechnen. Wegen $b \not\equiv \Delta \bmod 2$ ist $b := a - b = 53 - 14 = 39$ eine gesuchte Wurzel von Δ modulo $4a$ (siehe Abschnitt 4.1). Damit ist

$$\mathfrak{m} = \eta((a,b)) = (53, 39)$$

ein reduziertes Ideal in $\mathcal{O}_\Delta$ aus dem wir mit Hilfe von d die eigentliche Nachricht m zurückgewinnen können.

(b) Zum Verschlüsseln wird nun ein zufälliges

$$b = 44 < 200$$

gewählt und die verschlüsselte Nachricht

$$\begin{aligned} [\mathfrak{m}_1] &= [\mathfrak{c}]^b = [(2,1)]^{44} = [(70,-3)] \\ [\mathfrak{m}_2] &= [\mathfrak{m}] \cdot [\mathfrak{a}]^b = [(53,39)] \cdot [(63,-17)]^{44} = [(92,9)] \end{aligned}$$

berechnet.

(c) Wir senden

$$([\mathfrak{m}_1], [\mathfrak{m}_2], d) = ([(70,-3)]\,, [(92,9)]\,, -11).$$

(iii) **Entschlüsselung** Der Empfänger berechnet zunächst

$$[\mathfrak{m}] = [\mathfrak{m}_2] \cdot [\mathfrak{m}_1]^{-a} = [(53,39)]$$

und erhält dann

$$m = \mathrm{N}((53,39)) + d = 53 - 11 = 42.$$

Kapitel 6

ElGamal für $\Delta > 0$

In diesem Kapitel wollen wir nun versuchen, die ElGamal-Verschlüsselung auch auf reellquadratische Zahlkörper zu übertragen. Der Aufbau gestaltet sich daher ähnlich wie in Kapitel 5. Wegen des Auftretens von nichttrivialen Einheiten (siehe Satz 3.2.6) unterscheiden sich reellquadratische Zahlkörper massiv von den imaginärquadratischen und sind wegen ihrer komplizierteren Struktur bis jetzt auch weniger verstanden. Wir können deshalb in diesem Kapitel fast nur Vermutungen aufgrund von Berechnungsbeispielen präsentieren, in denen wir eine bestimmte Familie von reellquadratischen Zahlkörpern auf ihre Verwendbarkeit für das ElGamal-Verfahren untersucht haben.
Wir haben bereits in Lemma 3.3.19 gesehen haben, sind reduzierte Ideale in reellquadratischen Ordnungen nun keine eindeutigen Vertreter der Klassengruppe mehr, sondern mehrere dieser Ideale bilden einen Zyklus in einer Klasse. Dies macht auch die Übertragung des ElGamal-Verfahrens auf reellquadratische Zahlkörper etwas komplizierter. Aber es gibt noch ein weiteres Problem:

6.0.1 Vermutung (siehe [CM87]) Es sei $M \in \mathbb{N}$ und Δ eine zufällig gewählte reellquadratische Diskriminante mit $|\Delta| \leq M$. Dann gibt es ähnlich wie in 5.2.2.1 asymptotische Voraussagen für bestimmte Eigenschaften der Klassengruppe. Es gilt z. B. für die Klassenzahl:

- $\Pr[\ h_{odd}(\Delta) = 1\ ] = 0{,}754458$
- $\Pr[\ h_{odd}(\Delta) = 3\ ] = 0{,}125743$
- $\Pr[\ h_{odd}(\Delta) = 5\ ] = 0{,}037723$
- $\Pr[\ h_{odd}(\Delta) = 7\ ] = 0{,}017963$
- $\Pr[\ h_{odd}(\Delta) = 9\ ] = 0{,}015718.$

Man sieht deutlich, was der Satz von Brauer-Siegel prophezeit hat: Der ungerade Anteil der Klassengruppe hat in über 95% der Fälle weniger als 10 Elemente.
In den nächsten beiden Abschnitten wollen wir uns mit der Lösung dieser Probleme beschäftigen.

6.1 Degertsche Zahlkörper

6.1.1 Definition Zahlkörper der Form

$$K = \mathbb{Q}\left(\sqrt{D}\right) \text{ mit } D = N^2 + 1 \text{ quadratfrei und } N \in \mathbb{N}$$

heißen **Degertsche Zahlkörper**. $\Delta(K)$ heißt dann **Degertsche Diskriminante**.

6.1.2 Satz *Es sei $K = \mathbb{Q}\left(\sqrt{D}\right)$ ein Zahlkörper, $D \neq 5$. Es seien weiterhin $N \in \mathbb{N}$ und $r \in \mathbb{Z}$ mit $D = N^2 + r$, $-N < r \leq N$ und $r \mid 4N$. Dann gilt für die Grundeinheit ε_Δ von $\mathcal{O}_\Delta$:*

$$\varepsilon_\Delta := \begin{cases} \frac{N+\sqrt{D}}{\sqrt{|r|}} & \text{für } |r| \in \{1, 4\} \\ \frac{\left(N+\sqrt{D}\right)^2}{|r|} & \text{sonst} \end{cases}$$

Beweis: [Ste74] □

6.1.3 Korollar *Es sei $K = \mathbb{Q}\left(\sqrt{D}\right)$ mit $D = N^2 + 1$ ein Degertscher Zahlkörper. Dann gilt abgesehen vom Spezialfall $D = 5$ für die Grundeinheit ε_Δ:*

$$\varepsilon_\Delta = N + \sqrt{D}$$

also

$$\operatorname{Reg}(\Delta) = \ln\left(N + \sqrt{D}\right) = \mathcal{O}(\operatorname{size}(N)) = \mathcal{O}(\operatorname{size}(\Delta)).$$

6.1.4 Korollar *Für Degertsche Zahlkörper $\mathbb{Q}\left(\sqrt{N^2+1}\right)$ gilt danach für k, die Anzahl reduzierter Ideale in einer Idealklasse:*

$$\frac{2\ln\left(\sqrt{\Delta} + N\right)}{\ln \Delta} \leq k \leq \frac{2\ln\left(\sqrt{\Delta} + N\right)}{\ln 2},$$

also $k = \mathcal{O}(\operatorname{size}(\Delta))$. Damit ist insbesondere der Algorithmus `IdealCycle` *mit einem Aufwand von $\mathcal{O}(\operatorname{size}(\Delta)^3)$ effizient.*

Beweis: Folgt aus Satz 6.1.3 und Lemma 3.3.22. □

Im Hinblick auf den Satz von Brauer-Siegel dürfen wir damit bei Degertschen Zahlkörpern auf eine ähnlich große Klassengruppe wie in imaginärquadratischen Zahlkörpern hoffen. Ein weiteres Lemma garantiert, daß es genug solcher Körper für unsere Zwecke gibt:

6.1.5 Lemma *Für unendlich viele N ist N^2+1 quadratfrei.*

Beweis: [Nar74, Satz 8.8.8] □

Wichtig an dieser Stelle wäre es auch zu wissen, ob es ebenfalls unendlich viele Zahlen $N^2+1 \in \mathbb{P}$ gibt. Darüber scheint es aber noch keine Aussagen zu geben. Man kann aber an Beispielen sehen, daß dies wahrscheinlich ist. Es ist klar, daß der Anteil von primen Zahlen der Form N^2+1 mit wachsendem N immer mehr abnimmt, da schon der Anteil der Primzahlen immer mehr abnimmt. Wir betrachten daher das Verhältnis von

$$M(x) := \sharp\{N^2+1 \in \mathbb{P} \mid N \leq x\} \text{ zu } \tau(x) := \sharp\{p \in \mathbb{P} \mid p \leq x\}.$$

in Tabelle 6.1. Obwohl dieses Verhältnis leicht zu fallen scheint, könnte es sich asymptotisch doch einem positiven Wert nähern.

x	10000	20000	30000	40000	50000	70000	100000
$M(x)$	718	1427	2111	2772	3411	4672	6398
$\tau(x)$	1033	2016	2974	3904	4828	6608	9224
$\frac{M(x)}{\tau(x)}$	0,695	0,708	0,710	0,710	0,707	0,707	0,694

Tabelle 6.1: Verhältnis von $M(x)$ zu $\tau(x)$.

6.2 Der Zyklus reduzierter Ideale

Wie in Corollar 6.1.4 gesehen, sind Zyklen reduzierter Ideale $\mathcal{R}(\mathfrak{a})$ zu einer Degertschen Diskriminante sehr klein. Wegen

$$\mathrm{N}(\varepsilon_\Delta) = \mathrm{N}\left(N + \sqrt{N^2+1}\right) = N^2 - \left(N^2+1\right) = -1$$

gilt $f \sim f^* \ \forall\, f \in \mathrm{Form}(\Delta)$ bzw. $[\mathfrak{a}]^+ = [\mathfrak{a}] \ \forall\, \mathfrak{a} \in \mathrm{P}_\Delta$ wie in Abschnitt 3.3 gesehen. Für Formen $f = (a,b,c) \in \mathrm{Form}(\Delta)$ kann man explizite Transformationen angeben, es gilt:

(i)
$$f^* = f \cdot \begin{pmatrix} \frac{b}{2} - N & -c \\ -a & \frac{b}{2} + N \end{pmatrix} \text{ für } \Delta \equiv 0 \bmod 4 \ \ (N \text{ ungerade})$$

(ii)
$$f^* = f \cdot \begin{pmatrix} b - N & -2c \\ -2a & b + N \end{pmatrix} \text{ für } \Delta \equiv 1 \bmod 4 \ \ (N \text{ gerade}).$$

Um nun festzuhalten, welches Ideal in einem Zyklus wir meinen, um von der Idealklasse wieder auf ein Ideal zu schließen, identifizieren wir zunächst ein eindeutiges Ideal in jedem Zyklus:

6.2.1 Definition Ein reduziertes Ideal $\mathfrak{a} = (a, b)$ heißt **minimal in seinem Zyklus**, falls gilt:

$$\forall \left(\tilde{a}, \tilde{b}\right) \sim \mathfrak{a} \text{ reduziert } \Longrightarrow (a < \tilde{a}) \text{ oder } (a = \tilde{a} \text{ und } b < \tilde{b}).$$

6.2.2 Bemerkung Nach Satz 3.1.9 ist das minimale Ideal in einem Zyklus eindeutig bestimmt.

Der folgende Algorithmus bestimmt die Position des minimalen Ideales in einem Zyklus reduzierter Ideale $\mathcal{R}$.

Algorithmus `IdealMinPos`

Eingabe : Eine Liste $\mathcal{R}$ mit einem Zyklus von reduzierten Idealen
Ausgabe: Die Position des minimalen Ideals in der Liste

```
1: pos := 1
2: (min_a, min_b) := R[1]
3: for i ∈ {2, ..., ♯R} do
4:     (a, b) := R[i]
5:     if a < min_a or (a = min_a and b < min_b) then
6:         (min_a, min_b) := (a, b)
7:         pos := i
8:     end if
9: end for
10: return pos
```

Aufwand: $\mathcal{O}(\text{size}(\Delta))$

6.2.3 Bemerkung Der Aufwand dieses Algorithmus und einiger der folgenden hängt maßgeblich von der Tatsache ab, daß wir Degertsche Zahlkörper verwenden, denn dort kann man den Zyklus reduzierter Ideale effizient durchlaufen. Für allgemeine reellquadratische Zahlkörper sind diese Algorithmen ineffizient, da unter Annahme der Riemannschen Vermutung (siehe z. B. [KV92]) nach Lemma 2.17 aus [BTW95] und Vermutung 6.0.1 $\sharp\mathcal{R}(\mathfrak{a}) = \mathcal{O}\left(\sqrt{\Delta} \cdot \text{size}(\Delta)\right)$ gilt.

Damit sind wir in der gleichen Situation wie im imaginärquadratischen Fall, denn wir können nun jeder Idealklasse wieder effizient ein eindeutiges Ideal zuordnen. Mit diesem Ansatz wäre allerdings die Umwandlung einer Zahl in ein solches minimales Ideal sehr aufwendig, da nicht jedes Ideal, das wir durch `Number2Ideal` erhalten, minimal ist. Verschlüsseln wir statt dessen einfach das minimale Ideal im Zyklus von

$\mathfrak{a} = \texttt{Number2Ideal}(n)$, so wird der zu sendende Abstand zwischen n und $\mathrm{N}(\mathfrak{a})$ wesentlich größer $(= \mathcal{O}\left(\sqrt{\Delta}\right))$. Statt dessen wollen wir hier den Abstand von $\mathfrak{a}$ zum minimalen Ideal in $\mathcal{R}(\mathfrak{a})$ bestimmen $(= \mathcal{O}(\mathrm{size}(\Delta)))$und verschicken. Mit dieser Information läßt sich dann leicht das richtige Ideal bei der Entschlüsselung zurückgewinnen, und alle anderen Algorithmen können wie gewohnt verwendet werden. Der folgende Algorithmus bestimmt die Position des Nachrichtenideals in seinem Zyklus:

Algorithmus `IdealPosInCycle`

Eingabe : Ein reduziertes Ideal $\mathfrak{a}$
Ausgabe: Abstand vom minimalen Ideal in $\mathcal{R}(\mathfrak{a})$ zu $\mathfrak{a}$

1: $(\min_a, \min_b) := \mathfrak{b} := \mathfrak{a}$
2: $\mathrm{pos} := k := 0$
3: **repeat**
4: $\quad k := k + 1$
5: $\quad \mathfrak{a} := (a, b) := \rho(\mathfrak{a})$
6: $\quad$ **if** $a < \min_a$ **or** $(a = \min_a$ **and** $b \leq \min_b)$ **then**
7: $\quad\quad (\min_a, \min_b) := (a, b)$
8: $\quad\quad \mathrm{pos} := -k$
9: $\quad$ **end if**
10: **until** $\mathfrak{a} = \mathfrak{b}$
11: **if** $\mathrm{pos} < 0$ **then** $\mathrm{pos} := \mathrm{pos} + k$ **end if**
12: **return** pos

Aufwand: $\mathcal{O}\left(\mathrm{size}(\Delta)^3\right)$

Schließlich haben wir folgenden Algorithmus, der beim Entschlüsseln aus Ideal und Position die Nachricht wieder herstellt.

Algorithmus `IdealGoToPosInCycle`

Eingabe : Ein reduziertes Ideal $\mathfrak{a}$ und ein $k \in \mathbb{N}$
Ausgabe: Das Ideal an der Position k im Zyklus von $\mathfrak{a}$

1: $\mathcal{R}$:=`IdealCycle(`$\mathfrak{a}$`)`
2: min :=`IdealMinPos(`$\mathcal{R}$`)`
3: **return** $\mathcal{R}[((\min + k - 1) \bmod \sharp\mathcal{R}) + 1]$

Aufwand: $\mathcal{O}\left(\mathrm{size}(\Delta)^3\right)$

6.3 Der Verschlüsselungsalgorithmus

Das Verfahren aus Abschnitt 5.1 läßt sich nun auch auf Degertsche Zahlkörper übertragen.

Algorithmus `ElGamalRQFSetup`

Eingabe : Δ genügend groß
Ausgabe: Der öffentliche und geheime Schlüssel

1: `Wähle` $[\mathfrak{c}] \in \mathrm{Cl}(\Delta)$ `beliebig`
2: `Wähle` $a \in \mathbb{N}, a < \frac{\sqrt{\Delta}}{\mathrm{Reg}(\Delta)}$ `zufällig`
3: $[\mathfrak{a}] := [\mathfrak{c}]^a$
4: **return** $(\Delta, [\mathfrak{c}], [\mathfrak{a}]), (\Delta, a)$

Aufwand: $\mathcal{O}\left(\mathrm{size}(\Delta)^3\right)$

Algorithmus `ElGamalRQFEncrypt`

Eingabe : Der öffentliche Schlüssel $(\Delta, [\mathfrak{c}], [\mathfrak{a}])$ und die Nachricht $\mathfrak{m} \in \mathrm{P}_\Delta$
Ausgabe: Die zu $\mathfrak{m}$ gehörige verschlüsselte Nachricht

1: `Wähle` $b \in \mathbb{N}, b < \frac{\sqrt{\Delta}}{\mathrm{Reg}(\Delta)}$ `zufällig`
2: $[\mathfrak{m}_1] := [\mathfrak{c}]^b$
3: $[\mathfrak{m}_2] := [\mathfrak{m}] \cdot [\mathfrak{a}]^b$
4: m_3 :=`IdealPosInCycle(`$\mathfrak{a}$`)`
5: **return** $([\mathfrak{m}_1], [\mathfrak{m}_2], m_3)$

Aufwand: $\mathcal{O}\left(\mathrm{size}(\Delta)^3\right)$

Algorithmus `ElGamalRQFDecrypt`

Eingabe : Der geheime Schlüssel (Δ, a) und die verschlüsselte Nachricht $([\mathfrak{m}_1], [\mathfrak{m}_2], m_3)$
Ausgabe: Die entschlüsselte Nachricht $\mathfrak{m}$

1: $[\mathfrak{m}] := [\mathfrak{m}_2] \cdot [\mathfrak{m}_1]^{-a}$
2: **return** `IdealGoToPosInCycle(`$\mathfrak{m}, m_3$`)`

Aufwand: $\mathcal{O}\left(\mathrm{size}(\Delta)^3\right)$

6.4 Sicherheit

Die in 5.2.2 vorgestellten Möglichkeiten das Verschlüsselungssystem für $\Delta < 0$ anzugreifen, gibt es genauso auch im reellquadratischen Fall, da die vorgestellten Methoden auch hier eingesetzt werden können. Wir müssen also wie im letzten Kapitel die Größe, den zyklischen Anteil und die Glattheit der Klassengruppe untersuchen, um vor Angriffen mit Hilfe von Index-Calculus-Methoden, Quadratwurzelalgorithmen oder dem Pohlig-Hellman-Algorithmus sicher zu sein. Da wir aber mit den Degertschen Zahlkörpern eine bestimmte Klasse von Zahlkörpern betrachten, die sich dazu in ihren Eigenschaften sehr von den allgemeinen reellquadratischen Zahlkörpern unterscheiden, können wir allgemeine Aussagen wie die Vermutungen von Cohen und Lenstra hier nicht mehr verwenden.
Weitere Untersuchungen müssen zeigen, ob durch die spezielle Wahl der Zahlkörper zusätzliche Angriffsmöglichkeiten entstehen oder sich die oben genannten dadurch beschleunigen lassen. Diese werden wir aber in dieser Arbeit nicht betrachten.
Als Anhaltspunkte für das Verhalten Degertscher Zahlkörper und für Heuristikvorschläge haben wir die Klassengruppen solcher Körper für $3 \leq N \leq 10^4$ und N^2+1 quadratfrei berechnet und ausgewertet. Dabei sind nur 5 der 8951 Klassenzahlen gleich 1, die größte Klassenzahl 3008 gehört zu $N = 9975 = 3 \cdot 5^2 \cdot 7 \cdot 19$. Die Klassengruppe mit dem größten zyklischen Faktor (2570) gehört zu $N = 9675 = 3^2 \cdot 5^2 \cdot 41$. Die Ergebnisse stehen in den folgenden Tabellen und im Anhang A.

6.4.1 Die Größe einer Degertschen Klassengruppe

Der Satz von Brauer-Siegel (3.2.8)sagt voraus, daß

$$\ln\left(\mathrm{Reg}\left(\Delta\right)\mathrm{h}\left(\Delta\right)\right) \sim \ln\left(\sqrt{\Delta}\right).$$

Da für Degertsche Zahlkörper $\mathrm{Reg}\left(\Delta\right)$ sehr klein ist, und man unter Annahme der Riemannschen Vermutung schon

$$\frac{\sqrt{\Delta}}{6\ln\Delta} \leq \mathrm{h}\left(\Delta\right)\mathrm{Reg}\left(\Delta\right) \leq \sqrt{\Delta}\ln\Delta \quad \forall\ \Delta > \Delta_0$$

beweisen konnte (siehe Satz 3.2.12), wollen wir als erstes untersuchen, ob über den Satz von Brauer-Siegel hinaus ähnlich wie im imaginärquadratischen Fall auch

$$\mathrm{Reg}\left(\Delta\right)\mathrm{h}\left(\Delta\right) \sim \sqrt{\Delta}$$

gilt. Dazu definieren wir

$$\mu\left(N\right) := \frac{\mathrm{Reg}\left(\Delta\right)\mathrm{h}\left(\Delta\right)}{\sqrt{\Delta}} \text{ mit } \Delta := \Delta\left(\mathbb{Q}\left(\sqrt{N^2+1}\right)\right).$$

Die Tabellen 6.2 und A.1 zeigen, daß $\mu\left(N\right)$ tatsächlich ein gutes Maß für die Größe einer Klassengruppe im Verhältnis zur Diskriminante ist, da $\mu\left(N\right)$ unabhängig von der

Größe der Diskriminante ist und relativ konstant bleibt. Es ist also zu vermuten, daß sich sich Degertsche Zahlkörper in Bezug auf ihre Größe ähnlich wie imaginärquadratische Zahlkörper verhalten. Der Satz von Brauer-Siegel und Satz 3.2.12 können dies nicht beweisen, sie unterstützen aber diese Vermutung. Als nächstes wollen wir uns ansehen, wie andere Eigenschaften von N die Größe von $\mu(N)$ beeinflussen.

Bereich	Anzahl	$\min \mu(N)$	$\max \mu(N)$	$\overline{\mu(N)}$
$2 < N \leq 1000$	893	0,121	2,607	0,815
$1000 < N \leq 2000$	897	0,138	2,642	0,817
$2000 < N \leq 3000$	895	0,118	3,246	0,819
$3000 < N \leq 4000$	896	0,121	2,874	0,816
$4000 < N \leq 5000$	892	0,121	3,046	0,815
$5000 < N \leq 6000$	896	0,129	2,812	0,814
$6000 < N \leq 7000$	890	0,134	2,858	0,816
$7000 < N \leq 8000$	899	0,136	3,375	0,822
$8000 < N \leq 9000$	894	0,116	2,809	0,814
$9000 < N \leq 10000$	898	0,124	2,986	0,817
gesamt	8950	0,116	3,375	0,817

Tabelle 6.2: Verhalten von $\mu(N)$ mit wachsendem N.

6.4.1.1 Definition Es sei $n \in \mathbb{N}$. Dann definieren wir

$$\delta(n) := \prod_{p \in \mathbb{P}, p \leq n} p.$$

Teiler von N	Anzahl	$\min \mu(N)$	$\max \mu(N)$	$\overline{\mu(N)}$
1	8950	0,116	3,096	0,571
2	4475	0,116	3,096	0,652
2^2	2231	0,344	3,096	0,980
2^3	1116	0,376	2,874	0,979
3	2987	0,216	3,096	0,857
3^2	997	0,247	3,096	0,858
5	1945	0,185	3,096	0,727
7	1280	0,158	2,741	0,668
$2 \cdot \delta(3)$	744	0,712	3,096	1,469
$2 \cdot \delta(5)$	163	1,109	3,096	1,866
$2 \cdot \delta(7)$	23	1,519	2,741	2,136

Tabelle 6.3: Verhalten von $\mu(N)$ mit bestimmten Teilbarkeitseigenschaften.

Tabelle 6.3 zeigt, daß $\mu(N)$ besonders groß wird, wenn N von kleinen Primzahlen und 4 geteilt wird. Es scheint dabei fast keinen Unterschied zu machen, ob $N^2 + 1$

prim ist oder nicht (siehe Tabelle A.2). Aus den Tabellen A.3 und A.4 kann man erkennen, daß diese Eigenschaft unabhängig von der Größe von N ist.
Tabelle A.5 zeigt, daß dies nur bedingt etwas mit der Glattheit von N zu tun hat.

6.4.1.2 Vermutung Degertsche Zahlkörper haben eine besonders große Klassengruppe (im Durchschnitt und Minimum), falls N von der Zahl 4 und möglichst vielen verschiedenen kleinen Primzahlen geteilt wird. Ob N^2+1 dabei prim ist oder nicht, hat keinen Einfluß auf diese Eigenschaft.

6.4.2 Der zyklische Anteil einer Degertschen Klassengruppe

Wie wir im letzten Abschnitt gesehen haben, können wir die Klassenzahl für Degertsche Zahlkörper beliebig groß machen. Nun wollen wir untersuchen, wie groß der zyklische Anteil der Klassengruppe werden kann.

$q := \frac{\mathrm{h}(\Delta)}{\mathrm{h}_{\mathrm{cycl}}(\Delta)}$			davon	$N^2+1 \in \mathbb{P}$		$12 \mid N, N^2+1 \in \mathbb{P}$	
	Anzahl	Anteil	gerade	Anzahl	Anteil	Anzahl	Anteil
$q = 1$	3618	0,4042	0	831	0,9905	142	0,9793
$q \leq 2$	6560	0,7330	2942	831	0,9905	142	0,9793
$q \leq 3$	6598	0,7372	2942	837	0,9976	144	0,9931
$q \leq 4$	8410	0,9397	4754	837	0,9976	144	0,9931
$q \leq 10$	8857	0,9896	5193	838	0,9988	144	0,9931
$q \leq 28$	8946	0,9996	5281	839	1,0000	145	1,0000
$q \leq 64$	8950	1,0000	5285	839	1,0000	145	1,0000
gesamt	8950	1,0000	5285	839	1,0000	145	1,0000

Tabelle 6.4: Verhalten von $\mathrm{h}(\Delta)/\mathrm{h}_{\mathrm{cycl}}(\Delta)$.

Ist die Klassengruppe nicht zyklisch, so sind in über 99% der Fälle die zusätzlichen Faktoren von gerader Ordnung. Wegen Lemma 5.2.1.2 kann man diese Fälle aber alle durch die Forderung $N^2+1 \in \mathbb{P}$ ausschließen, wie man in Tabelle 6.4 sehen kann.
In Tabelle A.6 betrachten analog zu Tabelle 6.3 den Einfluß von Teilern von N auf

$$\lambda(N) := \frac{\mathrm{Reg}(\Delta)\,\mathrm{h}_{\mathrm{cycl}}(\Delta)}{\sqrt{\Delta}} \text{ mit } \Delta := \Delta\left(\mathbb{Q}\left(\sqrt{N^2+1}\right)\right).$$

Dabei ist $\mathrm{h}_{\mathrm{cycl}}(\Delta)$ die Größe des größten zyklischen Faktors von $\mathrm{h}(\Delta)$. Wie zu erwarten, fallen die Verhältnisse allgemein kleiner aus. Diesmal zeigt sich aber ein deutlicher Vorteil für die Fälle wo N^2+1 prim ist. Sowohl der Durchschnitt, als auch das Minimum der $\lambda(N)$ erhöht sich bemerkbar. Auch hier zeigen die Tabellen A.7 und A.8, daß diese Eigenschaft nicht von der Größe von N abhängt.
Wir untersuchen nun die Wahrscheinlichkeit für die Wahl einer Idealklasse großer Ordnung.

6.4.2.1 Lemma *Es sei $D = N^2 + 1 \equiv 1 \bmod 4$, also $N = 2 \cdot N_0$. Dann ist $\mathfrak{a} = \mathfrak{h}(N, p) := (p, 1)$ ein Ideal $\forall\, p \mid N_0$ mit $\mathrm{ord}_{\mathrm{Cl}(\Delta)}([\mathfrak{a}]) > 1$.*

Beweis: [Lan68, IV.3] □

Wir wollen nun analog zu Tabelle 5.4 die Ordnung einer Idealklasse $[\mathfrak{a}]$ mit $\mathfrak{a}$ wie in Lemma 6.4.2.1 betrachten. Wir testen dabei Ideale der Form $\mathfrak{h}(N, p)$ mit p minimal ($p_{\min}$), dann mit jenem p_{best} bei dem $\mathrm{ord}(\mathfrak{h}(p, N))$ am größten ist und schließlich $p = 2$ für den Fall, daß $N \equiv 0 \bmod 4$. Dies haben wir für alle N (Tabelle 6.5), $N^2 + 1 \in \mathbb{P}$ (Tabelle 6.6) und $N^2 + 1 \in \mathbb{P}, 12 \mid N$ (Tabelle 6.7) getan.
Wie zu erwarten, verbessern sich diese Verhältnisse für $N^2 + 1 \in \mathbb{P}$ merklich, da sich mit dem Wegfall von geraden Faktoren von $\mathrm{Cl}(\Delta)$ auch die Möglichkeiten für Klassen verringern, eine von $\mathrm{h}(\Delta)$ verschiedene Ordnung zu haben. Interessant ist, daß sich diese Verhältnisse für glatte N nochmals verbessern (Tabelle 6.7). Diese sind wegen ihrer großen Klassengruppe ohnehin für unsere Zwecke besonders gut geeignet. Tabelle 6.7 zeigt, daß $p = 2$ nicht immer die beste Wahl ist, aber auch nicht sehr viel schlechter. In den Tabellen 6.5 und 6.6 sind die Ergebnisse für $p = 2$ die besten, was daran liegt, daß wir dort etwas glattere N betrachten ($4 \mid N$). Es ist nicht möglich, p_{best} effizient zu bestimmen. Im Vergleich mit den Tabellen 5.2 und 5.4 zeigt sich, daß $[\mathfrak{h}(2, N)]$ für $N^2 + 1 \in \mathbb{P}$ bezüglich der Ordnung ein ähnlich gutes Verhalten hat wie in imaginärquadratischen Zahlkörpern. In den Tabellen A.9 – A.11 haben wir ebenfalls die Entwicklung dieser Werte für steigende N betrachtet.

$q := \frac{\mathrm{ord}[\mathfrak{a}]}{\mathrm{h}(\Delta)}$	$\mathfrak{a} := \mathfrak{h}(N, p_{\min})$		$\mathfrak{a} := \mathfrak{h}(N, p_{\mathrm{best}})$		$\mathfrak{a} := \mathfrak{h}(N, 2)$	
	Anzahl	Anteil	Anzahl	Anteil	Anzahl	Anteil
$q = 1$	839	0,1875	1723	0,3851	835	0,3744
$q \leq 5$	1832	0,4095	2372	0,5302	1813	0,8130
$q \leq 10$	2105	0,4705	2497	0,5581	2061	0,9242
$q \leq 20$	2294	0,5127	2577	0,5760	2185	0,9798
$q \leq 50$	2549	0,5697	2778	0,6209	2225	0,9978
$q \leq 100$	2959	0,6614	3041	0,6797	2230	1,0000
gesamt	4474	1,0000	4474	1,0000	2230	1,0000

Tabelle 6.5: Ordnung von $[\mathfrak{a}] \in \mathrm{Cl}(\Delta)$ für N gerade.

6.4.3 Die Glattheit der Degertschen Klassenzahl

Sind die Klassenzahlen sehr glatt, so erhöht sich die Wahrscheinlichkeit, daß Angriffe mit dem Pohlig-Hellman-Algorithmus erfolgreich sind, da dessen Aufwand hauptsächlich von der Größe des größten Primfaktors von $\mathrm{h}(\Delta)$ abhängt. Ebenso verringert sich die Wahrscheinlichkeit, daß ein zufällig gewähltes Element aus $\mathrm{Cl}(\Delta)$ große Ordnung hat, was wiederum Angriffspunkte für Quadratwurzelalgorithmen liefert, da deren Aufwand von eben jener Ordnung abhängt.

$q := \frac{\mathrm{ord}[\mathfrak{a}]}{\mathrm{h}(\Delta)}$	$\mathfrak{a} := \mathfrak{h}(N, p_{\min})$		$\mathfrak{a} := \mathfrak{h}(N, p_{\mathrm{best}})$		$\mathfrak{a} := \mathfrak{h}(N, 2)$	
	Anzahl	Anteil	Anzahl	Anteil	Anzahl	Anteil
$q = 1$	325	0,3874	653	0,7783	321	0,7589
$q \leq 5$	387	0,4613	707	0,8427	380	0,8983
$q \leq 10$	428	0,5101	738	0,8796	412	0,9740
$q \leq 20$	451	0,5375	752	0,8963	420	0,9929
$q \leq 50$	498	0,5936	771	0,9190	422	0,9976
$q \leq 100$	588	0,7008	805	0,9595	423	1,0000
gesamt	839	1,0000	839	1,0000	423	1,0000

Tabelle 6.6: Ordnung von $[\mathfrak{a}] \in \mathrm{Cl}(\Delta)$ für N gerade und $N^2 + 1$ prim.

$q := \frac{\mathrm{ord}[\mathfrak{a}]}{\mathrm{h}(\Delta)}$	$\mathfrak{a} := \mathfrak{h}(N, p_{\min})$		$\mathfrak{a} := \mathfrak{h}(N, p_{\mathrm{best}})$		$\mathfrak{a} := \mathfrak{h}(N, 2)$	
	Anzahl	Anteil	Anzahl	Anteil	Anzahl	Anteil
$q = 1$	107	0,7379	136	0,9379	107	0,7379
$q \leq 5$	128	0,8828	144	0,9931	128	0,8828
$q \leq 10$	139	0,9586	144	0,9931	139	0,9586
$q \leq 20$	144	0,9931	145	1,0000	144	0,9931
$q \leq 50$	144	0,9931	145	1,0000	144	0,9931
$q \leq 100$	145	1,0000	145	1,0000	145	1,0000
gesamt	145	1,0000	145	1,0000	145	1,0000

Tabelle 6.7: Ordnung von $[\mathfrak{a}] \in \mathrm{Cl}(\Delta)$ für $12 \mid N$ und $N^2 + 1$ prim.

Es sei

$$\nu(N) = \sum_{i=1}^{n} e_i \text{ für } \mathrm{h}(\Delta) = \prod_{\mathrm{i}=1}^{\mathrm{n}} \mathrm{p}_{\mathrm{i}}^{\mathrm{e_i}}$$

die Anzahl der Primfaktoren von $\mathrm{h}(\Delta)$. Man sieht in Tabelle A.12, daß dieser Wert recht hoch ist, im Durchschnitt hat die Klassenzahl hier 4,36 Primfaktoren. Man kann diesen Wert aber wieder drücken durch die Forderung $N^2 + 1 \in \mathbb{P}$, da dadurch alle geraden Faktoren in $\mathrm{Cl}(\Delta)$ wegfallen. Für diesen Fall hat die Klassenzahl durchschnittlich 2,03 Primfaktoren, fordert man zusätzlich $12 \mid N$ sind es 2,28 Primfaktoren. Das ist etwas mehr, scheint sich aber mit wachsendem N dem Wert für den Fall $N \in \mathbb{P}$ anzupassen (siehe Tabelle A.13).

Analog zu Tabelle 5.1 betrachten wir nun in Tabelle 6.8 die Glattheit der Klassenzahlen für Degertsche Zahlkörper und vergleichen sie mit der der ganzen Zahlen. Wie man sieht, fallen die berechneten Werte sogar leicht für wachsende N (siehe Tabelle A.14). Für beliebige N gibt es im Vergleich zu den imaginärquadratischen Zahlkörpern sehr viele glatte Klassenzahlen. Fordert man daß $N^2 + 1 \in \mathbb{P}$, so erhält man Werte, die ungefähr denen imaginärquadratischer Zahlkörper entsprechen. Sie werden sogar besser als diese, wenn man N besonders glatt wählt.

			$N^2+1 \in \mathbb{P}$		$12 \mid N, N^2+1 \in \mathbb{P}$		
u	Anzahl	Anteil	Anzahl	Anteil	Anzahl	Anteil	$\vartheta(u)$
1,0	8945	1,0000	834	1,0000	145	1,0000	1,00000
1,5	7675	0,8580	479	0,5743	58	0,4000	0,59453
2,0	5686	0,6357	261	0,3129	28	0,1931	0,30685
2,5	4163	0,4654	128	0,1535	16	0,1103	0,13033
3,0	2933	0,3279	63	0,0755	7	0,0483	0,04861
3,5	2195	0,2454	31	0,0372	3	0,0207	0,01623
4,0	1584	0,1771	15	0,0180	3	0,0207	0,00491
4,5	1135	0,1269	7	0,0084	2	0,0138	0,00137
5,0	889	0,0994	5	0,0060	2	0,0138	0,00035
5,5	743	0,0831	2	0,0024	1	0,0069	0,00009
6,0	549	0,0614	0	0,0000	0	0,0000	0,00002
6,5	350	0,0391	0	0,0000	0	0,0000	0,00000
7,0	207	0,0231	0	0,0000	0	0,0000	0,00000
10,0	34	0,0038	0	0,0000	0	0,0000	0,00000
15,0	0	0,0000	0	0,0000	0	0,0000	0,00000

Tabelle 6.8: Diskriminanten mit $(\sqrt{\Delta}/\mathrm{Reg}(\Delta))^{\frac{1}{u}}$-glatter Klassenzahl.

6.4.3.1 Beispiel zur Wahl von Δ Analog zum imaginärquadratischen Fall untersuchen wie zunächst die Gefahr des Pohlig-Hellman-Algorithmus. Wie schon für die praktischen Ergebnisse für imaginärquadratische Zahlkörper gilt auch für geeignete ($N^2+1 \in \mathbb{P}, N$ sehr glatt) Degertsche Zahlkörper:

$$\Pr[\ \mathrm{h}(\Delta)\ \text{ist } B\text{-glatt}\ ] \approx \vartheta(u) \text{ für } B = \left(\frac{\sqrt{\Delta}}{\mathrm{Reg}(\Delta)}\right)^{\frac{1}{u}}$$

Setzen wir die gleichen Werte

$$\mathrm{W}_{\mathrm{total}} = 2^{64} \text{ und } \mathrm{W}_{\max} = 2^{42} \left(\text{ also } B = 2^{42}\ln 2\right)$$

wie in 5.2.2.7 voraus, so erhalten wir

$$\vartheta(u) = \Pr[\ \mathrm{h}(\Delta)\ \text{ist } B\text{-glatt}\ ] = \frac{\mathrm{W}_{\max}}{\mathrm{W}_{\mathrm{total}}} \approx 2^{-22},$$

was für $u \approx 8$ erfüllt ist. Daher muß also

$$B^u = \left(2^{42}\ln 2\right)^8 = \frac{\sqrt{\Delta}}{\mathrm{Reg}(\Delta)} \approx \frac{2\sqrt{\Delta}}{\ln \Delta}$$

sein, dies ist für

$$\Delta \approx 2^{679}$$

erfüllt.

Im allgemeinen ($\mathrm{h}(\Delta)$ klein) würde man für reellquadratische Zahlkörper einen Quadratwurzelalgorithmus benutzen, da dieser nur von $\mathrm{h}(\Delta)$ abhängt. Im Falle Degertscher Zahlkörper ($\mathrm{h}(\Delta)$ groß) ist dagegen ein Index-Calculus-Algorithmus schneller. Die Index-Calculus-Algorithmen zur Lösung des DLP in $\mathrm{Cl}(\Delta)$ sind für imaginärquadratische und reellquadratische Zahlkörper im wesentlichen gleich, und deren Aufwand ist nur von $|\Delta|$ abhängig (siehe 5.2.2 und [Jac99]). Da man für reellquadratische Zahlkörper sogar noch den Zyklus reduzierter Ideale durchlaufen muß, um die Äquivalenz von zwei Klassen zu überprüfen, ist der Algorithmus hier sogar um einen Faktor $\mathcal{O}(\mathrm{size}(\Delta))$ langsamer. Das heißt nach [Hüh00b], daß für $\Delta \approx 2^{686}$ die Lösung des DLP in $\mathrm{Cl}(\Delta)$ mindestens genauso schwer ist wie für $\Delta \approx -2^{686}$. Das heißt also insgesamt, daß wieder

$$\Delta \approx 2^{686}$$

sein muß um mindestens die gleiche Sicherheit wie für RSA mit $n \approx 2^{1024}$ zu garantieren.

Unter der Annahme, daß unsere Berechnungen einigermaßen repräsentativ für Degertsche Zahlkörper sind, kommen wir zu folgender

6.4.3.2 Zusammenfassung

(i) $\mathrm{h}(\Delta)$ wird groß, wenn Δ groß wird, es gilt für genügend glattes N

$$\mathrm{h}(\Delta) \geq \frac{\sqrt{\Delta}}{\mathrm{Reg}(\Delta)} \approx \frac{2\sqrt{\Delta}}{\ln \Delta}.$$

(ii) $\mathrm{Cl}(\Delta)$ enthält mit großer Sicherheit einen großen zyklischen Faktor. Die Wahrscheinlichkeit, daß ein beliebiges Element einer Klassengruppe fast die gesamte Gruppe erzeugt, ist groß. Für $\Delta \in \mathbb{P}$ sind die Ergebnisse ähnlich wie für imaginärquadratische Zahlkörper.

(iii) Die Wahrscheinlichkeit, daß $\mathrm{h}(\Delta)$ B-glatt ist, kann durch die Wahl von Δ beliebig klein gehalten werden, für glatte N mit $N^2 + 1 \in \mathbb{P}$ sogar kleiner als für imaginärquadratische Zahlkörper. Der gerade Anteil von $\mathrm{h}(\Delta)$ kann kontrolliert werden.

Unsere Berechnungen legen die Vermutung nahe, daß sich Klassengruppen Degertscher Zahlkörper für sehr glatte N mit $N^2 + 1 \in \mathbb{P}$ in Bezug auf sicherheitsrelevante Eigenschaften ähnlich verhalten wie Klassengruppen imaginärquadratischer Zahlkörper.

6.5 Beispiel

(i) **Initialisierung**

(a) Wir suchen eine sehr glatte Zahl N mit $N^2 + 1 \in \mathbb{P}$, um gemäß der Vermutung 6.4.1.2 einen Zahlkörper mit relativ großer Klassenzahl zu finden. Es sei $N := 2^2 \cdot 3 \cdot 17 = 204$. Dann ist

$$\Delta = N^2 + 1 = 41617 \in \mathbb{P}$$

eine Degertsche Diskriminante mit $\Delta \equiv 1 \bmod 8$. Wegen $\Delta \in \mathbb{P}$ folgt mit Corollar 5.2.1.3, daß $\mathrm{h}(\Delta)$ ungerade ist, $\mathrm{Cl}(\Delta)$ hat also keine geraden Faktoren. In einem realistischen Fall ist die Diskriminante natürlich so groß, daß man $\mathrm{Cl}(\Delta)$ praktisch nicht berechnen kann. Für $\Delta = 41617$ kann man aber leicht nachrechnen, daß $\mathrm{Cl}(\Delta) \cong C_{57}$ mit $\mu(N) \approx 1{,}6796$. Wie zu erwarten, unterscheidet sich die Größe dieser Klassengruppe von der aus dem Beispiel 5.3 ($\mathrm{h}(\Delta) = 311$) ungefähr um einen Faktor $\mathrm{Reg}(\Delta) \approx 6{,}01$. Wir werden diese Information aber nicht benutzen, da sie im Normalfall nicht bekannt ist.

Die nach den Ergebnissen in Tabelle A.2 erwartete Größe der Klassengruppe ist mindestens

$$\frac{\sqrt{|\Delta|}}{\mathrm{Reg}(\Delta)} \approx 33.$$

Voraussage und Wirklichkeit scheinen hier noch weit auseinander zu liegen. Weil wir sehr kleine Klassenzahlen haben, ist ein Faktor 2 noch von großem Gewicht. Bei realistischen Größen von $\mathrm{h}(\Delta)$ spielt er aber kaum noch eine Rolle.

(b) Als nächstes wollen wir bestimmen, welches die maximal Zahl ist, die wir in einem Schritt verschlüsseln können. Wie in Lemma 2.2.5 gezeigt wurde, ist ein Ideal (a, b) mit

$$a \leq \frac{\sqrt{|\Delta|}}{2} \approx 100$$

reduziert. Wir können also keine Zahl $a > 100$ verschlüsseln, da das zugehörige Ideal (a, b) möglicherweise nicht mehr reduziert ist. Wenn wir $a \leq 100$ verschlüsseln wollen, müssen wir eine Wurzel von Δ modulo $4a$ berechnen. Falls eine Wurzel überhaupt existiert, kann man sie nur effizient berechnen, falls a eine Primzahl mit $a \equiv 1, 3, 5, 7 \bmod 8$ ist. Mit der in 4.1 vorgestellten Abstandseinbettung (zusätzlich $a \not\equiv 1 \bmod 8$) können wir daher nur $a \leq 79$ verschlüsseln, da 79 die größte Zahl < 100 ist, die alle oben genannten Eigenschaften besitzt.

(c) Da $\mathrm{h}(\Delta)$ nicht viel größer als 33 sein wird, genügt es wenn die Exponenten a und b für Elemente der Klassengruppe kleiner als 33 sind.

(d) $(2,1)$ ist wegen Satz 3.1.9 ein Ideal, denn es ist

$$\Delta \equiv 1 \bmod 8$$

und damit

$$\frac{b^2-\Delta}{4\cdot a} = \frac{1-\Delta}{8} \in \mathbb{Z}.$$

Allerdings ist $(2,1)$ noch nicht in Standardrepräsentation, wir definieren daher

$$[\mathfrak{c}] := [\eta((2,1))] = [(2,201)]$$

Wir haben gesehen, daß $[\mathfrak{c}]$ mit großer Wahrscheinlichkeit eine große Ordnung in $\mathrm{Cl}\,(\Delta)$ hat. Man kann hier nachrechnen, daß $\langle[\mathfrak{c}]\rangle = \mathrm{Cl}\,(\Delta)$, was man normalerweise aber nicht weiß.

(e) Wir wählen einen zufälligen geheimen Schlüssel

$$a = 26 < 33$$

und berechnen

$$[\mathfrak{a}] = [\mathfrak{c}]^a = [(2,201)]^{26} = [(17,203)]\,.$$

(f) Wir erhalten den öffentlichen Schlüssel

$$(\Delta, [\mathfrak{c}], [\mathfrak{a}]) = (41617, [(2,1)]\,, [(17,203)])$$

und den geheimen Schlüssel

$$(\Delta, a) = (41617, 26).$$

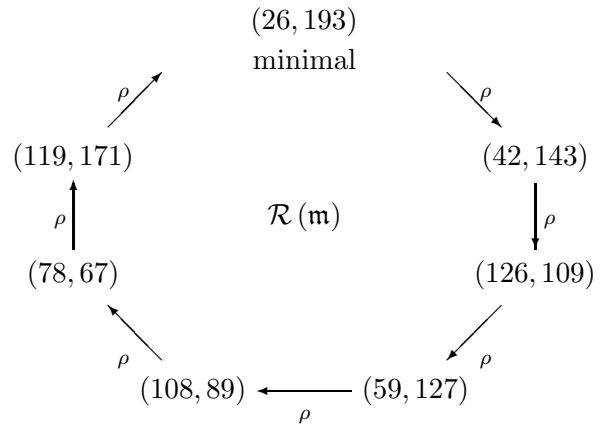
(ii) **Verschlüsselung**

(a) Unsere Nachricht sei $m = 42 \leq 79$. Der Algorithmus `Number2Ideal` liefert $a = 59$ als nächstgrößere Primzahl mit $\left(\frac{\Delta}{a}\right) = 1$ und $a \equiv 3 \bmod 8$ und $d = -17$ als Entfernung von u zur eigentlichen Nachricht m. Nun läßt sich leicht eine Wurzel $b = 9$ von Δ modulo a berechnen. Wegen $b \equiv \Delta \bmod 2$ ist b auch eine gesuchte Wurzel von Δ modulo $4a$ (siehe Abschnitt 4.1). Damit ist

$$\mathfrak{m} = \eta((59,9)) = (59, 9+2\cdot 59) = (59,127)\,.$$

ein reduziertes Ideal in $\mathcal{O}_\Delta$ aus dem wir mit Hilfe von d die eigentliche Nachricht m zurückgewinnen können. In dessen Zyklus befinden sich ins-

gesamt 7 Ideale:



$\mathfrak{m}$ hat den Abstand 3 zum minimalen Ideal $(26, 193)$.

(b) Zum Verschlüsseln wählen wir nun ein zufälliges

$$b = 12 < 33.$$

und berechnen:

$$\begin{aligned} [\mathfrak{m}_1] &= [\mathfrak{c}]^b = [(2, 201)]^{12} = [(11, 185)] \\ [\mathfrak{m}_2] &= [\mathfrak{m}] \cdot [\mathfrak{a}]^b = [(59, 127)] \cdot [(17, 203)]^{12} = [(22, 163)] \\ m_3 &= \texttt{IdealPosInCycle}\,(\mathfrak{m}) = 3. \end{aligned}$$

(c) Wir senden

$$([\mathfrak{m}_1], [\mathfrak{m}_2], m_3, d) = ([(11, 185)], [(22, 163)], 3, -17).$$

(iii) **Entschlüsselung** Der Empfänger berechnet zunächst

$$[\mathfrak{m}] = [\mathfrak{m}_2] \cdot [\mathfrak{m}_1]^{-a} = [(22, 163)] \cdot [(11, 185)]^{-26} = [(119, 171)]$$

und findet dann das gesuchte Ideal im Zyklus $\mathcal{R}(119, 171)$:

$$\texttt{IdealGoToPosInCycle}\,((119, 171), m_3) = (59, 127) = \mathfrak{m}.$$

Schließlich ergibt sich die gesuchte Nachricht durch

$$m = \mathrm{N}(\mathfrak{m}) + d = \mathrm{N}((59, 127)) - 17 = 59 - 17 = 42.$$

Kapitel 7

Anwendung

In diesem Kapitel wollen wir uns der praktischen Seite der vorgestellten Verfahren zuwenden. Dazu werden wir zunächst auf eine Möglichkeit eingehen, den Verschlüsselungsalgorithmus in $\mathrm{Cl}(\Delta)$ etwas zu beschleunigen. In Abschnitt 7.2 werden wir dann Laufzeiten und Speicherbedarf der angesprochenen Verschlüsselungsverfahren anhand von praktischen Berechnungen analysieren und miteinander vergleichen.

7.1 Laufzeitverbesserungen

In den Algorithmen `ElGamalIQFEncrypt` und `ElGamalRQFEncrypt` werden immer die gleichen Ideale ($\mathfrak{a}$ und $\mathfrak{c}$) als Basis in Potenzbildungen verwendet. In diesem Fall lohnt es sich, vorher eine Liste $P_\mathfrak{a}$ der Idealklassen $[\mathfrak{a}]^{2^i}$ anzulegen, um das Potenzieren zu beschleunigen. Es ergeben sich folgende zwei Algorithmen:

Algorithmus `IdealClassPowerList`

Eingabe: Eine Idealklasse $[\mathfrak{a}]$ und ein $n \in \mathbb{N}$
Ausgabe: Eine Liste $P_\mathfrak{a}$ mit $P_\mathfrak{a}[i] = [\mathfrak{a}]^{2^i} \quad \forall\ 0 \leq 0 \leq n-1$

1: $P_\mathfrak{a} := []$
2: **for** $i \in \{1, \ldots, n\}$ **do**
3: $\quad P_\mathfrak{a}[i] := [\mathfrak{a}]$
4: $\quad [\mathfrak{a}] := [\mathfrak{a}]^2$
5: **end for**
6: **return** $P_\mathfrak{a}$

Aufwand: $\mathcal{O}\left(\mathrm{size}\,(\Delta)^2 \,\mathrm{size}\,(n)\right)$

Algorithmus `IdealClassFastPower`

Eingabe: Ein $n \in \mathbb{Z}$ und $P_{\mathfrak{a}}$ mit mindestens $\log_2(n) + 1$ Einträgen
Ausgabe: $[\mathfrak{a}]^n$

```
1: Berechne die binäre Darstellung von |n| = Σ_{i=0}^{k} n_i 2^i
2: [𝔟] := [𝒪]
3: for i ∈ {1, ..., k} do
4:     if n_i = 1 then
5:         [𝔟] := P_𝔞[i] · [𝔟]
6:     end if
7: if n < 0 then
8:     [𝔟] := [𝔟]^{-1}
9: end if
10: return [𝔟]
```

Aufwand: $\mathcal{O}\left(\operatorname{size}(\Delta)^2 \operatorname{size}(n)\right)$

In unserem Fall wäre

$$n = \operatorname{size}\left(\frac{\sqrt{\Delta}}{\operatorname{Reg}(\Delta)}\right).$$

Jetzt sind nur noch die Multiplikationen beim Potenzieren ausschlaggebend für die Laufzeit. Eine Multiplikation im Durchlauf i ist immer dann nötig, wenn in der Binärdarstellung des Exponenten n an der i-ten Stelle eine 1 steht.

7.1.1 Definition Es sei $n \in \mathbb{Z}$ mit Binärdarstellung

$$n = \operatorname{sign} n \cdot \sum_{i=0}^{k} n_i 2^i.$$

Dann heißt

$$\omega(n) := \sum_{i=0}^{k} n_i$$

das **Gewicht** von n.

Damit gibt $\omega(n)$ gerade die Anzahl der nötigen Multiplikationen bei der Berechnung von $[\mathfrak{a}]^n$ an. Je größer das Gewicht von n ist, desto aufwendiger wird die Potenzberechnung mit n als Exponenten. Da der Exponent b beim Verschlüsseln keinerlei zusätzliche Bedingungen erfüllen muß, können wir ihn so wählen, daß er ein geringes Gewicht hat, um das Potenzieren weiter zu beschleunigen.

Dabei schränken wir die Anzahl der möglichen Exponenten ein, was zu einem Sicherheitsproblem werden kann. Es sei k die maximale Bitlänge von b, also

$$b = \left\lfloor \log_2 \sqrt{|\Delta|} \right\rfloor \text{ für } \Delta < 0$$

und

$$b = \left\lfloor \log_2 \frac{\sqrt{\Delta}}{\mathrm{Reg}\,(\Delta)} \right\rfloor \text{ für } \Delta > 0.$$

Dann gibt es $\left(\begin{array}{c} b \\ g \end{array} \right)$ Exponenten mit Gewicht g, also $\sum_{i=1}^{g} \left(\begin{array}{c} b \\ i \end{array} \right)$ Exponenten mit Gewicht höchstens g. Nach [Hei93] kann ein abgewandelter Babystep-Giantstep-Algorithmus $\left(\begin{array}{c} b \\ g \end{array} \right)$ Exponenten in $\left(\begin{array}{c} b \\ \frac{g}{2} \end{array} \right)$ Schritten testen. Dies ist natürlich nur wieder eine Größenordnung für einen solchen Angriff, da wir nicht wissen, wieviel Zeit ein einzelner Schritt kostet. Um trotzdem einen Eindruck zu bekommen wollen wir

$$\sum_{i=1}^{g} \left(\begin{array}{c} b \\ \frac{i}{2} \end{array} \right) \text{ und } L_{|\Delta|}\left[\frac{1}{2}, 1\right], \tag{7.1}$$

vergleichen, da mindestens $L_{|\Delta|}\left[\frac{1}{2}, 1\right]$ Operationen nötig sind, um das System anzugreifen wie wir in 5.2.2 gesehen haben. Es sei $\tilde{g} = \frac{g}{2}$. Nach der Stirlingschen Formel gilt:

$$\ln n! \approx \left(n + \frac{1}{2}\right) \ln(n) - n + \ln\left(\sqrt{2\pi n}\right),$$

also

$$\begin{aligned}
\ln \left(\begin{array}{c} b \\ \tilde{g} \end{array} \right) &= \ln \frac{b!}{\tilde{g}!\,(b-\tilde{g})!} \\
&= \ln b! - (\ln \tilde{g}!) - (\ln (b-\tilde{g})!) \\
&\approx \left(b + \frac{1}{2}\right) \ln(b) - b + \ln\left(\sqrt{2\pi b}\right) \\
&\quad - \left(\left(\tilde{g} + \frac{1}{2}\right) \ln \tilde{g} - \tilde{g} + \ln\left(\sqrt{2\pi\tilde{g}}\right)\right) \\
&\quad - \left(\left((b-\tilde{g}) + \frac{1}{2}\right) \ln(b-\tilde{g}) - (b-\tilde{g}) + \ln\left(\sqrt{2\pi\,(b-\tilde{g})}\right)\right) \\
&= \left(b + \frac{1}{2}\right) \ln(b) - \left(\tilde{g} + \frac{1}{2}\right) \ln \tilde{g} - \left((b-\tilde{g}) + \frac{1}{2}\right) \ln(b-\tilde{g}) \\
&\quad + \ln\left(\sqrt{2\pi b}\right) - \ln\left(\sqrt{2\pi\tilde{g}}\right) - \ln\left(\sqrt{2\pi\,(b-\tilde{g})}\right).
\end{aligned}$$

Wir haben andererseits

$$\begin{aligned} \ln L_{|\Delta|}\left[\frac{1}{2},1\right] &= (1+o(1))\,(\ln|\Delta|)^{\frac{1}{2}}\,(\ln\ln|\Delta|)^{\frac{1}{2}} \\ &\approx \sqrt{\ln|\Delta|\cdot\ln\ln|\Delta|} \\ &\approx \sqrt{2b\ln 2\cdot\ln(2b\ln 2)}. \end{aligned}$$

Numerische Berechnungen zeigen für eine 686-Bit-Diskriminante, daß diese beiden Ausdrücke für $g = 31$ ($\Delta < 0$) bzw. $g = 27$ ($\Delta > 0$) ungefähr gleich sind. Lassen wir nun auch noch Gewichte kleiner als g zu, haben wir hier wegen $\ln \binom{b}{\tilde{g}} \approx \ln \binom{b}{\tilde{g}-1}$ sehr großzügig abgeschätzt.
Der Babystep-Giantstep-Algorithmus stellt dann mit großer Sicherheit trotz eingeschränkter Exponenten keine größere Gefahr dar, als ein Index-Calculus-Algorithmus, allerdings müßte dies an praktischen Beispielen noch einmal genau untersucht werden. Wir haben damit beim Potenzieren höchstens noch 31 Multiplikationen statt durchschnittlich 172. Folgender Algorithmus liefert Pseudozufalls-Zahlen $n < 2^k$ mit Gewicht kleiner g:

Algorithmus `LightRandomInteger`

Eingabe: $k, g \in \mathbb{N}$ mit $g < k$
Ausgabe: $n \in \mathbb{N}$ mit $n < 2^k$ und $\omega(n) \leq g$

1: $C := []$
2: **for** $i \in \{1, \ldots, k\}$ **do**
3: $\quad C[i] := 0$
4: **end for**
5: **for** $i \in \{1, \ldots, g\}$ **do**
6: $\quad$ `Wähle` $1 \leq j \leq k$ `zufällig`
7: $\quad C[j] := 1$
8: **end for**
9: **return** $\sum_{i=0}^{k-1} C[i+1] \cdot 2^i$

Aufwand: $\mathcal{O}(\text{size}(k))$

7.1.2 Bemerkung Für die Potenzierung mit a (siehe Abschnitt 4.2.3)ist es nicht sinnvoll, eine Liste von Potenzen vorher zu berechnen, da immer verschiedene Ideale beim Entschlüsseln mit a potenziert werden. Mit leichten Exponenten spart man dann nur noch die Zeit für die Multiplikationen, aber nicht mehr für das Quadrieren.

Wir haben 10 zufällige 683-Bit-Diskriminanten darin je 10 Idealklassen $[\mathfrak{a}]$ gewählt und nach den oben beschriebenen Verfahren je 10 zufällige Potenzen $[\mathfrak{a}]^a$ berechnet. Wir kamen zu folgendem Ergebnis für die durchschnittlich benötigte Zeit einer solchen Berechnung:

	$\Delta < 0$	$\Delta > 0$
Herkömmliches Potenzieren:	3,98s	4,64s
Potenzieren mit $\omega(a) \leq 31$:	2,10s	2,25s
Erstellen einer Potenzliste $P_{\mathfrak{a}}$ von $\mathfrak{a}$ (342 Einträge):	2,19s	2,39s
Potenzieren mit vorbereiteter Liste:	1,22s	1,52s
Potenzieren mit vorbereiteter Liste und $\omega(a) \leq 31$:	0,21s	0,26s

Tabelle 7.1: Laufzeiten für Potenzbildungen.

7.2 Praktische Beispiele

Hier interessieren wir uns vor allem für die Größenordnungen der Zahlen und die Laufzeiten der einzelnen Schritte. Diese sind mit Hilfe des Computeralgebrasystems KASH implementiert und auf einem AMD Athlon 1800+ Prozessor ausgeführt worden. Die Größen der Moduln bzw. der Diskriminanten wurden so gewählt, daß die Verfahren in etwa die gleiche Sicherheit bieten. Das heißt nach [Hüh00b]:

n	$\approx$	2^{1024}	für RSA	Tabelle 7.2
q	$\approx$	2^{823}	für ElGamal in $\mathbb{Z}_q$	Tabelle 7.3
Δ	$\approx$	-2^{686}	für ElGamal in $\mathrm{Cl}(\Delta), \Delta < 0$	Tabelle 7.4
Δ	$\approx$	2^{686}	für ElGamal in $\mathrm{Cl}(\Delta), \Delta > 0$	Tabelle 7.5.

Wir haben jeweils 10 verschiedene Moduln bzw. Diskriminanten dieser Art betrachtet, dazu jeweils 10 verschiedene Schlüssel und zu jedem Schlüssel wiederum 10 verschiedene Nachrichten. Insgesamt wurden also in jedem Beispiel 1000 Nachrichten verschlüsselt, um mittlere Laufzeiten für die einzelnen Schritte zu ermitteln.
Für die Wahl von $\Delta > 0$ haben wir die Zahl

$$n = \delta(10)^5 \cdot \delta(30) \cdot \delta(60) \cdot \delta(150)$$

so lange mit zufälligen 12-Bit-Zahlen f multipliziert, bis $\Delta = (f \cdot n)^2 + 1 \in \mathbb{P}$. Interessanterweise war für derartige Zahlen ein Primzahltest wesentlich schneller als für beliebige 686-Bit-Zahlen im Beispiel für imaginärquadratische Diskriminanten (Tabelle 7.4).

7.2.1 Vergleich der Verfahren In Tabelle 7.6 haben wir die Daten aus den Tabellen 7.2 – 7.5 miteinander verglichen. Wir haben diese Daten genutzt, um zu bestimmen wie lange die Ver- und Entschlüsselung einer 1024-Bit-Nachricht dauert, da die maximalen Nachrichtenlängen pro Schritt für die Verfahren verschieden sind.

Berechnung	Größe in Bit	Zeit in ms	Aufwand
$p \in \mathbb{P}$	524	13 300,0	$\mathcal{O}\left(\text{size}\,(n)^{7+\varepsilon}\right)$
$q \in \mathbb{P}$	500	7 700,0	$\mathcal{O}\left(\text{size}\,(n)^{7+\varepsilon}\right)$
$n = p \cdot q$	1024	$< 0{,}1$	$\mathcal{O}\left(\text{size}\,(p)\,\text{size}\,(q)\right)$
e	24	67,1	$\mathcal{O}\left(\text{size}\,(n)\right)$
$1 = ef + s(p-1)(q-1)$	1023	$< 0{,}1$	$\mathcal{O}\left(\text{size}\,(p)\,\text{size}\,(q)\right)$
$m \in \mathbb{Z}_n^\times$	1023	–	$\mathcal{O}\,(1)$
$\tilde{m} = m^e \bmod n$	1023	0,9	$\mathcal{O}\left(\text{size}\,(n)^2\,\text{size}\,(e)\right)$
$\tilde{m}^f \bmod n$	1023	38,0	$\mathcal{O}\left(\text{size}\,(n)^2\,\text{size}\,(f)\right)$

Tabelle 7.2: Laufzeiten für RSA.

Berechnung	Größe in Bit	Zeit in ms	Aufwand
$q = f \cdot p + 1, p \in \mathbb{P}, f \in \mathbb{N}$ minimal	830	286 600,0	$\mathcal{O}\left(\text{size}\,(q)^{7+\varepsilon}\right)$
$\langle\gamma\rangle = \mathbb{Z}_q^\times$	15	0,1	$\mathcal{O}\left(\text{size}\,(q)^3\right)$
$a < q$	829	5,2	$\mathcal{O}\left(\text{size}\,(q)\right)$
$\alpha = \gamma^a \bmod q$	829	10,9	$\mathcal{O}\left(\text{size}\,(q)^3\right)$
$m \in \mathbb{Z}_q^\times$	829	–	
$b < q$	829	16,0	$\mathcal{O}\left(\text{size}\,(q)\right)$
$m_1 = \gamma^b \bmod q$	829	10,0	$\mathcal{O}\left(\text{size}\,(q)^3\right)$
$m_2 = m \cdot \alpha^b \bmod q$	829	16,0	$\mathcal{O}\left(\text{size}\,(q)^3\right)$
$m = m_2 \cdot m_1^{-a} \bmod q$	829	18,0	$\mathcal{O}\left(\text{size}\,(q)^3\right)$

Tabelle 7.3: Laufzeiten für ElGamal in $\mathbb{Z}_q$.

Berechnung	Größe in Bit	Zeit in ms	Aufwand
$-\Delta \in \mathbb{P}, \Delta \equiv 1 \bmod 8$	686	48 300,0	$\mathcal{O}\left(\text{size}\,(\Delta)^{7+\varepsilon}\right)$
$\mathfrak{c} = [(2,1)]$	(2,1)	$< 0{,}1$	$\mathcal{O}\,(1)$
$a < \sqrt{-\Delta}, \omega(a) \leq 50$	338	1,4	$\mathcal{O}\left(\text{size}\,(\Delta)\right)$
$P_\mathfrak{c}$	$343 \times (333, 332)$	1 900,0	$\mathcal{O}\left(\text{size}\,(\Delta)^3\right)$
$[\mathfrak{a}] = [\mathfrak{c}]^a$	$(341, 340)$	260,0	$\mathcal{O}\left(\text{size}\,(\Delta)^3\right)$
$P_\mathfrak{a}$	$343 \times (341, 339)$	2 250,0	$\mathcal{O}\left(\text{size}\,(\Delta)^3\right)$
$m < \frac{\sqrt{-\Delta}}{2}$	340	–	
$(d, [\mathfrak{m}]) \in \mathbb{Z} \times \text{Cl}\,(\Delta)$	$(10, (341, 339))$	1 892,0	$\mathcal{O}\left(\text{size}\,(\Delta)^{7+\varepsilon}\right)$
$b < \sqrt{-\Delta}, \omega(b) \leq 50$	337	4,6	$\mathcal{O}\left(\text{size}\,(\Delta)\right)$
$[\mathfrak{m}_1] = [\mathfrak{c}]^b$	$(341, 339)$	355,0	$\mathcal{O}\left(\text{size}\,(\Delta)^3\right)$
$[\mathfrak{m}_2] = [\mathfrak{m}] \cdot [\mathfrak{a}]^b$	$(341, 339)$	384,0	$\mathcal{O}\left(\text{size}\,(\Delta)^3\right)$
$[\mathfrak{m}] = [\mathfrak{m}_2] \cdot [\mathfrak{m}_1]^{-a}$	$(341, 339)$	3 319,0	$\mathcal{O}\left(\text{size}\,(\Delta)^3\right)$
$m = \mathfrak{m} + d$	342	$< 0{,}1$	$\mathcal{O}\left(\text{size}\,(\Delta)\right)$

Tabelle 7.4: Laufzeiten für $\Delta < 0$.

Die Ergebnisse stehen in Tabelle 7.7. In Tabelle 7.8 haben wir noch einmal das Laufzeitverhalten der Verfahren miteinander verglichen.

Berechnung	Größe in Bit	Zeit in ms	Aufwand
$\Delta \in \mathbb{P}$	688	2 200,0	$\mathcal{O}\left(\text{size}\left(\Delta\right)^{7+\varepsilon}\right)$
$\mathfrak{c} = [(2,1)]$	$(2,1)$	$< 0{,}1$	$\mathcal{O}\left(1\right)$
$a < \frac{\sqrt{\Delta}}{\text{Reg}(\Delta)}, \omega(a) \leq 50$	331	1,9	$\mathcal{O}\left(\text{size}\left(\Delta\right)\right)$
$P_{\mathfrak{c}}$	$344 \times (333, 344)$	2 000,0	$\mathcal{O}\left(\text{size}\left(\Delta\right)^3\right)$
$[\mathfrak{a}] = [\mathfrak{c}]^a$	$(341, 344)$	290,0	$\mathcal{O}\left(\text{size}\left(\Delta\right)^3\right)$
$P_{\mathfrak{a}}$	$344 \times (341, 344)$	2 350,0	$\mathcal{O}\left(\text{size}\left(\Delta\right)^3\right)$
$m < \frac{\sqrt{\Delta}}{2}$	342	–	
$(d, [\mathfrak{m}]) \in \mathbb{Z} \times \text{Cl}\left(\Delta\right)$	$(10, (342, 343))$	1 929,0	$\mathcal{O}\left(\text{size}\left(\Delta\right)^{7+\varepsilon}\right)$
$b < \frac{\sqrt{\Delta}}{\text{Reg}(\Delta)}, \omega(b) \leq 50$	328	4,6	$\mathcal{O}\left(\text{size}\left(\Delta\right)\right)$
$k :=$`IdealPosInCycle(`$\mathfrak{m}$`)`	7	24,0	$\mathcal{O}\left(\text{size}\left(\Delta\right)^3\right)$
$[\mathfrak{m}_1] = [\mathfrak{c}]^b$	$(341, 344)$	442,0	$\mathcal{O}\left(\text{size}\left(\Delta\right)^3\right)$
$[\mathfrak{m}_2] = [\mathfrak{m}] \cdot [\mathfrak{a}]^b$	$(341, 344)$	491,0	$\mathcal{O}\left(\text{size}\left(\Delta\right)^3\right)$
$[\tilde{\mathfrak{m}}] = [\mathfrak{m}_2] \cdot [\mathfrak{m}_1]^{-a}$	$(341, 344)$	4 249,0	$\mathcal{O}\left(\text{size}\left(\Delta\right)^3\right)$
$\mathfrak{m} =$ `IdealGoToPos` $(\tilde{\mathfrak{m}}, k)$	$(341, 344)$	35,0	$\mathcal{O}\left(\text{size}\left(\Delta\right)^3\right)$
$m = \text{N}(\mathfrak{m}) + d$	340	$< 0{,}1$	$\mathcal{O}\left(\text{size}\left(\Delta\right)\right)$

Tabelle 7.5: Laufzeiten für $\Delta > 0$.

	RSA	$\mathbb{Z}_q$	$\Delta < 0$	$\Delta > 0$
Initialisierung in ms	21 000	800 000	52 710	6 840
Verschlüsseln in ms	1	91	2 640	2 890
Entschlüsseln in ms	38	43	3 320	4 280
Verschlüsselbare Bitlänge	1024	1024	340	340
Effektiv verschlüsselbare Bitlänge	1023	1024	331	331
Speicher für Verschlüsseler in Bit	1 050	2 080	459 000	464 000
Größe der Sendung in Bit	1 023	2 060	1 360	1 380
Speicher für Entschlüsseler in Bit	2 050	2 060	1 020	1 020

Tabelle 7.6: Laufzeiten im Vergleich.

7.2.2 Bemerkung zu Tabelle 7.6 Wie wir gesehen haben, läßt sich nicht immer jede Zahl verschlüsseln, im Falle der Klassengruppen zum Beispiel können wir eigentlich nur Primzahlen mit bestimmten weiteren Eigenschaften verschlüsseln (siehe Abschnitt 4.1). Ist dann n die Anzahl der verschlüsselbaren Zahlen, so bezeichnen wir $\log_2(n)$ als **effektiv verschlüsselbare Bitlänge**. Der Speicher für Ver- und Entschlüsseler ist die Anzahl von Bits, die sich die jeweilige Partei merken muß, also zum Beispiel n und f für den Entschlüsseler im RSA-Verfahren. Der Verschlüsseler beim ElGamal-Verfahren benötigt daher sehr viel Speicher, wenn er vorbereitete Potenzlisten benutzen will (siehe Abschnitt 7.1). Man kann sich diesen Speicher sparen, wenn man die Listen bei jeder Nachricht neu berechnet. Diese sind dann nur noch vorteilhaft, wenn die Nachrichten sehr lang sind. An dieser Stelle muß man in der Anwendung von Fall zu Fall entscheiden, ob ein geringerer Speicher wichtiger als ge-

ringe Laufzeit ist. Nicht eingerechnet bei diesen Angaben ist Speicher, der benötigt wird, um Rechnungen auszuführen.

	RSA	$\mathbb{Z}_q$	$\Delta < 0$	$\Delta > 0$
Initialisierung in ms	21 000	800 000	52 710	6 840
Verschlüsseln in ms	1	91	7 940	8 710
Entschlüsseln in ms	38	43	10 000	12 900
Größe der Sendung in Bit	1 023	2 060	4 100	4 160

Tabelle 7.7: Laufzeiten für eine 1024-Bit-Nachricht im Vergleich.

	RSA	$\mathbb{Z}_q$	$\Delta < 0$	$\Delta > 0$
Initialisierung	$\mathcal{O}\left(\text{size}\,(n)^{7+\varepsilon}\right)$	$\mathcal{O}\left(\text{size}\,(q)^{7+\varepsilon}\right)$	$\mathcal{O}\left(\text{size}\,(\Delta)^{7+\varepsilon}\right)$	$\mathcal{O}\left(\text{size}\,(\Delta)^{7+\varepsilon}\right)$
Verschlüsseln	$\mathcal{O}\left(\text{size}\,(n)^{3}\right)$	$\mathcal{O}\left(\text{size}\,(q)^{3}\right)$	$\mathcal{O}\left(\text{size}\,(\Delta)^{7+\varepsilon}\right)$	$\mathcal{O}\left(\text{size}\,(\Delta)^{7+\varepsilon}\right)$
Entschlüsseln	$\mathcal{O}\left(\text{size}\,(n)^{3}\right)$	$\mathcal{O}\left(\text{size}\,(q)^{3}\right)$	$\mathcal{O}\left(\text{size}\,(\Delta)^{3}\right)$	$\mathcal{O}\left(\text{size}\,(\Delta)^{3}\right)$

Tabelle 7.8: Laufzeitverhalten im Vergleich.

Für die Verschlüsselungssysteme in den Klassengruppen sind die Algorithmen wesentlich komplizierter und nicht mehr so elementar wie im Falle der Moduln (RSA und ElGamal in $\mathbb{Z}_q$). Daher wird eine optimierte und direkte Implementation dieser Algorithmen in einer hardwarenahen Programmiersprache diese Algorithmen, auch im Verhältnis zu den Modul-Algorithmen, noch erheblich beschleunigen. Ein solches Projekt ist im Rahmen dieser Diplomarbeit allerdings nicht möglich.

Kapitel 8

Zusammenfassung und Ausblick

Wir haben in dieser Arbeit gezeigt, wie man konkret Klassengruppen für die Umsetzung eines kryptographischen Verfahrens benutzen kann und wie die Parameter gewählt werden müssen, um eine mit gängigen Verfahren vergleichbare Sicherheit zu gewährleisten. Durch die komplexere Struktur ist ein Angriff auf Klassengruppenverfahren wesentlich schwerer, und man kann die Sicherheitsparameter (Δ) und die dahinter stehenden Strukturen kleiner wählen als im Fall der Modulverfahren (RSA und ElGamal in $\mathbb{Z}_q$). Dies führt allerdings auch dazu, daß man nicht mehr ganz so große Zahlen verschlüsseln kann. Weiterhin ist bei der Verschlüsselung, genauer bei der Einbettung von Zahlen in Ideale, ein verhältnismäßig aufwendiger Primzahltest nötig. Neue Durchbrüche auf diesem Gebiet ([AKS02]) lassen allerdings darauf hoffen, daß es in Zukunft schnellere Tests gibt. Davon abgesehen haben alle Teile der Klassengruppenverfahren das gleiche Laufzeitverhalten wie Modulverfahren.
Allerdings spiegelt sich die kompliziertere Struktur der Klassengruppe auch in den eigentlichen Laufzeiten wieder, so sind diese schlechter als die der herkömmlichen Verfahren, aber durch effizientere und direkte Implementation der Algorithmen ist auch hier noch erhebliche Verbesserung möglich.
Kryptographie mit Hilfe von Zahlkörpern steckt praktisch noch in den Kinderschuhen, die einzige ernsthafte und mir bekannte Forschung in dieser Richtung wird in einer Arbeitsgruppe um Prof. Dr. J. Buchmann in Darmstadt betrieben. Das liegt zum einen daran, daß die verwendeten Objekte in Zahlkörpern eher unhandlich und schwer zugänglich sind, und zum anderen an den noch viel zu langsamen Algorithmen, aufgrund der Kompliziertheit der beteiligten Objekte. Trotzdem hat die Forschung bis hierher interessante Alternativen und auch praktisch verwendbare neue Verfahren hervorgebracht. Weitere Forschungen können von hier aus in verschiedene Richtungen gehen, von denen wir einige kurz erwähnen wollen:

- **Andere Verfahren.** Es ist klar, daß sich die in dieser Arbeit vorgestellten Verfahren ebenso für einen Diffie-Hellman Schlüsseltausch auf Klassengruppenbasis eignen. Neben diesen gibt es auch andere Verschlüsselungsverfahren die man in Klassengruppen realisieren kann. Viele davon wurden schon erfolgreich auf imaginärquadratische Zahlkörper übertragen, da diese wie gesehen

einfacher zu handhaben sind. Es wurden dabei auch Signaturverfahren von ElGamal, Schnorr und anderen (siehe [BBHM99]) betrachtet. Eine sehr gute Untersuchung einer Vielzahl von Verfahren in imaginärquadratischen Zahlkörpern findet sich in [Ham02].

- **Übertragung auf reellquadratische Zahlkörper.** Etwa durch die Verwendung von speziellen reellquadratischen Zahlkörpern wie in dieser Arbeit geschehen, lassen sich Verfahren aus imaginärquadratischen Zahlkörpern auch auf reellquadratische übertragen. Weitere Möglichkeiten sind zum Beispiel verallgemeinerte Degertsche Zahlkörper, das heißt Zahlkörper, die die Voraussetzungen von Satz 6.1.2 erfüllen (zum Beispiel mit $r = -2$). Dies ist auch für höhere Grade möglich, man spricht dann von **Stender-Körpern** ([Ste75], [BBHM99]). In [BBHM99] wurden ebenfalls Zahlkörper der Form $\mathbb{Q}\left(\sqrt{10^n + 1}\right)$, $n \in \mathbb{N}$ gerade, vorgeschlagen.

- **Verfahren in Nichtmaximal-Ordnungen.** Vielversprechende Verfahren in Nichtmaximal-Ordnungen (d. h. D ist nicht mehr quadratfrei) in imaginärquadratischen Zahlkörpern wie NICE wurden in [Hüh00a], [HPT99] und [HJP97] vorgestellt. NICE ist wahrscheinlich zur Zeit das einzige asymmetrische Verschlüsselungssystem mit quadratischer Entschlüsselungszeit. Auch bei diesen könnte man untersuchen, welche Vorteile deren Anwendung auf reellquadratische Zahlkörper bietet.

- **Verfahren im Zyklus reduzierter Ideale.** Typische reellquadratische Zahlkörper (bzw. allgemein Zahlkörper $\subseteq \mathbb{R}$) haben eine sehr kleine Klassengruppe und einen großen Zyklus reduzierter Ideale in $[\mathcal{O}]$ mit $\sharp\mathcal{R}(\mathcal{O}) \sim \sqrt{\Delta}$. In [BMT96] und [Gro00] werden Möglichkeiten gezeigt, diesen Zyklus statt der Klassengruppe für kryptographische Verfahren zu verwenden. Hier zeigt sich wieder einmal die Schönheit des Satzes von Brauer-Siegel, denn je kleiner die Klassengruppe im Verhältnis zu $\sqrt{\Delta}$ ist, desto größer ist der Zyklus reduzierter Ideale innerhalb einer Idealklasse und umgekehrt. Je weniger also ein reellquadratischer Zahlkörper (wegen zu kleiner Klassengruppe) für die Verwendung eines Klassengruppenverfahrens geeignet ist, desto sicherer ist er für die Verwendung von Verfahren auf der Basis des Zyklus reduzierter Ideale.

- **Zahlkörper höheren Grades.** Die Verwendung von Zahlkörpern K höheren Grades (d. h. $[K : \mathbb{Q}] > 2$) bietet durch kompliziertere Strukturen mehr Sicherheit, aber auch mehr Berechnungsaufwand. Zu Überlegungen, wie man dort kryptographische Verfahren realisieren kann und ob dies Vorteile gegenüber quadratischen Zahlkörpern bietet, gibt es momentan kaum mehr als erste Ansätze wie zum Beispiel [HMNP00]. In [BBHM00] werden am Beispiel von Stender Körpern (siehe [Ste75]) auch erste reelle Zahlkörper höheren Grades mit kleinem Regulator untersucht.

- **Relativerweiterungen.** Die Verwendung von Relativerweiterungen (d. h. Erweiterungen von K und nicht von $\mathbb{Q}$) wäre eine weitere Steigerung der Idee

des letzten Punktes. Derartige Überlegungen sind allerdings noch gänzlich unbeachtet.

Es wird sich zeigen, ob schnellere Algorithmen zur Lösung des DLP in $\mathbb{Z}_q$ oder des IFP[1] die Attraktivität der Klassengruppenverfahren weiter erhöhen. Wir wollten mit dieser Arbeit eine weitere Alternative zu den gängigen Modulverfahren untersuchen und zeigen, wie man sie praktisch realisieren kann. Ebenso wollten wir zeigen wie sich bereits gefundene Möglichkeiten für imaginärquadratische Zahlkörper auf spezielle, den imaginärquadratischen ähnliche, reellquadratische Zahlkörper übertragen lassen. Es scheint allerdings so, als ob diese keine Vorteile gegenüber den imaginärquadratischen Zahlkörpern haben. Ob sich diese Verfahren einmal als sinnvoll erweisen, wird die Zukunft zeigen.

[1] Integer Factorization Problem

Anhang A

Berechnungen zu Degertschen Zahlkörpern

Im Folgenden werden weitere Tabellen aufgelistet, die das Verhalten der Eigenschaften der Klassengruppe noch genauer untersuchen. Einige von diesen wurden bereits in Kapitel 6 zitiert, es kommen aber noch weitere hinzu, viele davon beschäftigen sich mit bestimmten, schon vorher betrachteten Eigenschaften und deren Abhängigkeit von der Größe von N. Dazu haben wir allgemeine Untersuchungen auf folgende 3 Intervalle für N beschränkt

$$\begin{aligned} B_1 &:= [\ 1000,\ 3000\ ] \cap \mathbb{N} \\ B_2 &:= [\ 4500,\ 6500\ ] \cap \mathbb{N} \\ B_3 &:= [\ 8000, 10000\ ] \cap \mathbb{N} \end{aligned}$$

und die Entwicklung der Ergebnisse untersucht.
Um einen Gesamteindruck zu vermitteln, haben wir ebenfalls Auszüge aus den berechneten Werten angegeben. Wir haben alle Einträge nach $\mu(N)$ sortiert und die ersten 50 und die letzten 50 angegeben, jeweils für den allgemeinen Fall und den Fall, daß $N^2+1 \in \mathbb{P}$. Dort ist

$$u(N) := \log_B \left(\frac{\sqrt{\Delta}}{\mathrm{Reg}(\Delta)} \right)$$

wobei

$$B = \max\{p \in \mathbb{P} \mid p \mid \mathrm{h}(\Delta)\} \text{ und } \Delta = \Delta\left(\mathbb{Q}\left(\sqrt{\mathrm{N}^2+1}\right)\right),$$

also jenes u für das $\mathrm{h}(\Delta)$ gerade $\left(\frac{\sqrt{\Delta}}{\mathrm{Reg}(\Delta)}\right)^{\frac{1}{u}}$-glatt ist.

Bereich	Anzahl	$\min \mu(N)$	$\max \mu(N)$	$\overline{\mu(N)}$
$2 < N \leq 1000$	110	0,139	2,453	0,701
$1000 < N \leq 2000$	97	0,143	2,421	0,646
$2000 < N \leq 3000$	94	0,135	2,085	0,634
$3000 < N \leq 4000$	81	0,121	2,874	0,625
$4000 < N \leq 5000$	88	0,121	2,144	0,601
$5000 < N \leq 6000$	86	0,156	2,453	0,685
$6000 < N \leq 7000$	77	0,143	2,011	0,629
$7000 < N \leq 8000$	66	0,136	2,269	0,677
$8000 < N \leq 9000$	65	0,157	2,450	0,670
$9000 < N \leq 10000$	75	0,153	2,504	0,695
gesamt	839	0,121	2,874	0,656

Tabelle A.1: Verhalten von $\mu(N)$ mit wachsendem N, N^2+1 prim.

Teiler von N	Anzahl	$\min \mu(N)$	$\max \mu(N)$	$\overline{\mu(N)}$
1	839	0,121	2,874	0,656
2	839	0,121	2,874	0,656
2^2	423	0,376	2,874	0,986
2^3	211	0,376	2,874	0,980
3	281	0,229	2,874	0,990
3^2	89	0,247	2,874	0,949
5	279	0,190	2,874	0,843
7	108	0,158	2,504	0,709
$2 \cdot \delta(3)$	145	0,712	2,874	1,462
$2 \cdot \delta(5)$	49	1,109	2,874	1,853
$2 \cdot \delta(7)$	4	1,519	2,504	2,232

Tabelle A.2: Verhalten von $\mu(N)$ mit bestimmten Teilbarkeitseigenschaften, N^2+1 prim.

Teiler	Anzahl			$\min \mu(N)$			$\overline{\mu(N)}$		
von $N \in$	B_1	B_2	B_3	B_1	B_2	B_3	B_1	B_2	B_3
1	1793	1793	1793	0,118	0,121	0,116	0,572	0,571	0,572
2	896	897	899	0,118	0,121	0,116	0,652	0,652	0,654
2^2	446	447	449	0,398	0,344	0,374	0,980	0,979	0,981
2^3	224	222	227	0,398	0,388	0,416	0,985	0,977	0,975
3	601	596	598	0,229	0,257	0,273	0,859	0,853	0,858
3^2	200	202	201	0,247	0,257	0,273	0,861	0,862	0,862
5	393	391	393	0,190	0,196	0,185	0,729	0,726	0,723
7	256	256	255	0,169	0,189	0,170	0,665	0,667	0,673
$2 \cdot \delta(3)$	150	147	151	0,731	0,820	0,728	1,466	1,467	1,469
$2 \cdot \delta(5)$	33	34	32	1,375	1,109	1,127	1,860	1,843	1,893
$2 \cdot \delta(7)$	5	5	4	1,644	1,726	1,705	1,892	2,245	2,123

Tabelle A.3: Verhalten von $\mu(N)$ in Abhängigkeit von bestimmten Teilbarkeitseigenschaften und der Größe von N.

Teiler	Anzahl			$\min \mu(N)$			$\overline{\mu(N)}$		
von $N \in$	B_1	B_2	B_3	B_1	B_2	B_3	B_1	B_2	B_3
1	191	164	140	0,135	0,121	0,153	0,641	0,668	0,684
2	191	164	140	0,135	0,121	0,153	0,641	0,668	0,684
2^2	98	84	70	0,432	0,433	0,416	0,938	0,992	1,054
2^3	47	44	34	0,432	0,433	0,416	0,928	1,037	1,073
3	58	57	54	0,229	0,257	0,288	0,975	1,001	0,982
3^2	20	17	19	0,247	0,257	0,343	0,919	0,978	0,990
5	58	57	48	0,190	0,223	0,206	0,854	0,851	0,886
7	21	22	19	0,169	0,189	0,205	0,692	0,727	0,853
$2 \cdot \delta(3)$	27	30	29	0,829	0,895	0,732	1,539	1,447	1,435
$2 \cdot \delta(5)$	10	11	10	1,472	1,109	1,127	1,878	1,769	1,768
$2 \cdot \delta(7)$	0	1	1	0,000	2,453	2,504	-	2,453	2,504

Tabelle A.4: Verhalten von $\mu(N)$ in Abhängigkeit von bestimmten Teilbarkeitseigenschaften und der Größe von N mit N^2+1 prim.

					$N^2+1 \in \mathbb{P}$			
B	Anzahl	$\min \mu(N)$	$\max \mu(N)$	$\overline{\mu(N)}$	Anzahl	$\min \mu(N)$	$\max \mu(N)$	$\overline{\mu(N)}$
∞	8950	0,116	3,375	0,817	839	0,121	2,874	0,656
1000	6834	0,121	3,375	0,871	730	0,139	2,874	0,709
100	3369	0,129	3,375	0,964	433	0,143	2,874	0,805
50	2243	0,145	3,375	1,026	325	0,152	2,874	0,845
20	1072	0,152	3,096	1,130	179	0,152	2,874	0,974
10	312	0,215	2,874	1,243	64	0,221	2,874	1,075
5	59	0,260	1,891	1,050	13	0,260	1,834	0,888
3	11	0,455	0,866	0,631	3	0,508	0,649	0,556

Tabelle A.5: Verhalten von $\mu(N)$ für N B-glatt.

Teiler					$N^2+1 \in \mathbb{P}$			
von $N \in$	Anzahl	$\min \lambda(N)$	$\max \lambda(N)$	$\overline{\lambda(N)}$	Anzahl	$\min \lambda(N)$	$\max \lambda(N)$	$\overline{\lambda(N)}$
1	8950	0,005	3,096	0,369	839	0,056	2,874	0,650
2	4475	0,010	3,096	0,502	839	0,056	2,874	0,650
2^2	2231	0,047	3,096	0,754	423	0,068	2,874	0,976
2^3	1116	0,047	2,874	0,752	211	0,068	2,874	0,961
3	2987	0,024	3,096	0,551	281	0,068	2,874	0,974
3^2	997	0,032	3,096	0,551	89	0,068	2,874	0,922
5	1945	0,012	3,096	0,535	279	0,075	2,874	0,832
7	1280	0,025	2,504	0,426	108	0,068	2,504	0,682
$2 \cdot \delta(3)$	744	0,068	3,096	1,126	145	0,068	2,874	1,434
$2 \cdot \delta(5)$	163	0,283	3,096	1,591	49	0,586	2,874	1,796
$2 \cdot \delta(7)$	23	0,432	2,504	1,702	4	0,818	2,504	1,823

Tabelle A.6: Verhalten von $\lambda(N)$ mit bestimmten Teilbarkeitseigenschaften.

Teiler	Anzahl			$\min\lambda(N)$			$\overline{\lambda(N)}$		
von $N \in$	B_1	B_2	B_3	B_1	B_2	B_3	B_1	B_2	B_3
1	191	164	140	0,135	0,121	0,153	0,641	0,668	0,684
2	191	164	140	0,135	0,121	0,153	0,641	0,668	0,684
2^2	98	84	70	0,432	0,433	0,416	0,938	0,992	1,054
2^3	47	44	34	0,432	0,433	0,416	0,928	1,037	1,073
3	58	57	54	0,229	0,257	0,288	0,975	1,001	0,982
3^3	20	17	19	0,247	0,257	0,343	0,919	0,978	0,990
5	58	57	48	0,190	0,223	0,206	0,854	0,851	0,886
7	21	22	19	0,169	0,189	0,205	0,692	0,727	0,853
$2 \cdot \delta(3)$	27	30	29	0,829	0,895	0,732	1,539	1,447	1,435
$2 \cdot \delta(5)$	10	11	10	1,472	1,109	1,127	1,878	1,769	1,768
$2 \cdot \delta(7)$	0	1	1	0,000	2,453	2,504	-	2,453	2,504

Tabelle A.7: Verhalten von $\lambda(N)$ in Abhängigkeit von bestimmten Teilbarkeitseigenschaften und der Größe von N.

Teiler	Anzahl			$\min\lambda(N)$			$\overline{\lambda(N)}$		
von $N \in$	B_1	B_2	B_3	B_1	B_2	B_3	B_1	B_2	B_3
1	1793	1793	1793	0,012	0,012	0,011	0,381	0,355	0,355
2	896	897	899	0,026	0,020	0,021	0,520	0,484	0,489
2^2	446	447	449	0,067	0,070	0,047	0,784	0,725	0,736
2^3	224	222	227	0,067	0,070	0,047	0,789	0,718	0,725
3	601	596	598	0,024	0,033	0,032	0,574	0,521	0,535
3^3	200	202	201	0,061	0,033	0,032	0,583	0,544	0,513
5	393	391	393	0,051	0,012	0,041	0,559	0,514	0,520
7	256	256	255	0,049	0,044	0,027	0,455	0,400	0,410
$2 \cdot \delta(3)$	150	147	151	0,211	0,131	0,068	1,182	1,066	1,107
$2 \cdot \delta(5)$	33	34	32	0,650	0,432	0,798	1,642	1,422	1,714
$2 \cdot \delta(7)$	5	5	4	0,834	0,432	0,852	1,725	1,289	1,375

Tabelle A.8: Verhalten von $\lambda(N)$ in Abhängigkeit von bestimmten Teilbarkeitseigenschaften und der Größe von N mit N^2+1 prim.

	gesamt	$N \in B_1$	$N \in B_2$	$N \in B_3$
gesamt	89,557	41,007	99,116	153,249
$N^2+1 \in \mathbb{P}$	78,678	39,335	95,098	145,600
$N^2+1 \in \mathbb{P}, 12 \mid N$	2,517	1,370	3,067	3,828

Tabelle A.9: Das Verhalten von $q := \frac{\mathrm{ord}[\mathfrak{h}(N,p_{\min})]}{\mathrm{h}(\Delta)}$ für wachsende N.

	gesamt	$N \in B_1$	$N \in B_2$	$N \in B_3$
gesamt	16,446	9,162	17,497	26,285
$N^2+1 \in \mathbb{P}$	11,501	6,351	12,476	17,271
$N^2+1 \in \mathbb{P}, 12 \mid N$	1,234	1,074	1,267	1,759

Tabelle A.10: Das Verhalten von $q := \frac{\mathrm{ord}[\mathfrak{h}(N,p_{\mathrm{best}})]}{\mathrm{h}(\Delta)}$ für wachsende N.

	gesamt	$N \in B_1$	$N \in B_2$	$N \in B_3$
gesamt	4,011	2,998	4,199	5,824
$N^2+1 \in \mathbb{P}$	2,125	1,694	2,452	2,543
$N^2+1 \in \mathbb{P}$,$12 \mid N$	2,517	1,370	3,067	3,828

Tabelle A.11: Das Verhalten von $q := \frac{\mathrm{ord}[\mathfrak{h}(N,2)]}{\mathrm{h}(\Delta)}$ für wachsende N.

			$N^2+1 \in \mathbb{P}$		$12 \mid N, N^2+1 \in \mathbb{P}$	
	Anzahl	Anteil	Anzahl	Anteil	Anzahl	Anteil
$\nu(N) = 1$	270	0,0302	259	0,3087	33	0,2276
$\nu(N) \leq 2$	1125	0,1257	610	0,7271	90	0,6207
$\nu(N) \leq 3$	2838	0,3170	787	0,9380	131	0,9034
$\nu(N) \leq 5$	6868	0,7672	838	0,9988	144	0,9931
$\nu(N) \leq 8$	8855	0,9892	839	1,0000	145	1,0000
$\nu(N) \leq 11$	8952	1,0000	839	1,0000	145	1,0000
gesamt	8952	1,0000	839	1,0000	145	1,0000

Tabelle A.12: Anzahl der Primfaktoren von $\mathrm{h}(\Delta)$.

	gesamt	$N \in B_1$	$N \in B_2$	$N \in B_3$
gesamt	4,357	4,127	4,475	4,693
$N^2+1 \in \mathbb{P}$	2,029	1,958	2,128	2,264
$N^2+1 \in \mathbb{P}$,$12 \mid N$	2,283	2,333	2,267	2,276

Tabelle A.13: Durchschnittliche Anzahl der Faktoren von $\mathrm{h}(\Delta)$ mit wachsendem N.

				$N^2+1 \in \mathbb{P}$			$12 \mid N, N^2+1 \in \mathbb{P}$		
u	B_1	B_2	B_3	B_1	B_2	B_3	B_1	B_2	B_3
1,5	0,867	0,848	0,852	0,592	0,567	0,593	0,519	0,433	0,310
2,0	0,645	0,617	0,617	0,309	0,342	0,293	0,148	0,233	0,207
2,5	0,481	0,432	0,429	0,162	0,189	0,136	0,074	0,133	0,069
3,0	0,360	0,295	0,272	0,100	0,073	0,057	0,037	0,033	0,000
3,5	0,245	0,248	0,227	0,037	0,043	0,036	0,037	0,000	0,000
4,0	0,172	0,165	0,149	0,021	0,012	0,014	0,037	0,000	0,000
4,5	0,157	0,090	0,112	0,016	0,006	0,000	0,037	0,000	0,000
5,0	0,126	0,090	0,069	0,005	0,006	0,000	0,037	0,000	0,000
5,5	0,080	0,090	0,069	0,000	0,006	0,000	0,000	0,000	0,000
6,0	0,040	0,056	0,069	0,000	0,000	0,000	0,000	0,000	0,000
6,5	0,040	0,030	0,041	0,000	0,000	0,000	0,000	0,000	0,000
7,0	0,040	0,018	0,012	0,000	0,000	0,000	0,000	0,000	0,000
8,0	0,025	0,018	0,012	0,000	0,000	0,000	0,000	0,000	0,000
9,0	0,007	0,016	0,012	0,000	0,000	0,000	0,000	0,000	0,000
10,0	0,000	0,007	0,006	0,000	0,000	0,000	0,000	0,000	0,000
12,0	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000
15,0	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000

Tabelle A.14: $\left(\frac{\sqrt{\Delta}}{\mathrm{Reg}(\Delta)}\right)^{\frac{1}{u}}$-glatte Klassenzahlen für wachsende N.

$\mu(N)$	N	Δ	$\mathrm{h}(\Delta)$	$\mathrm{Cl}(\Delta) \cong$
0,0050	$7697 = 43 \cdot 179$	$2^3 \cdot 5 \cdot 17 \cdot 29 \cdot 61 \cdot 197$	$512 = 2^9$	$C_2^2 \times C_4^2 \times C_8$
0,0105	$3362 = 2 \cdot 41^2$	$5 \cdot 13 \cdot 17 \cdot 53 \cdot 193$	$64 = 2^6$	$C_2^2 \times C_4^2$
0,0109	$8033 = 29 \cdot 277$	$2^3 \cdot 5 \cdot 53 \cdot 109 \cdot 1117$	$432 = 2^4 \cdot 3^3$	$C_2^2 \times C_6 \times C_{18}$
0,0110	$8861 = 8861$	$2^3 \cdot 13 \cdot 17 \cdot 349 \cdot 509$	$640 = 2^7 \cdot 5$	$C_2 \times C_4^2 \times C_{20}$
0,0118	$5527 = 5527$	$2^3 \cdot 5 \cdot 29 \cdot 105337$	$392 = 2^3 \cdot 7^2$	$C_2 \times C_{14} \times C_{14}$
0,0119	$2917 = 2917$	$2^3 \cdot 5 \cdot 13 \cdot 29 \cdot 37 \cdot 61$	$256 = 2^8$	$C_2^3 \times C_4 \times C_8$
0,0120	$9853 = 59 \cdot 167$	$2^3 \cdot 5 \cdot 1721 \cdot 5641$	$576 = 2^6 \cdot 3^2$	$C_2 \times C_{12} \times C_{24}$
0,0124	$6065 = 5 \cdot 1213$	$2^3 \cdot 17 \cdot 53 \cdot 137 \cdot 149$	$512 = 2^9$	$C_2^2 \times C_8 \times C_{16}$
0,0135	$7103 = 7103$	$2^3 \cdot 5 \cdot 13 \cdot 97 \cdot 4001$	$320 = 2^6 \cdot 5$	$C_2^2 \times C_4 \times C_{20}$
0,0150	$7699 = 7699$	$2^3 \cdot 41 \cdot 113 \cdot 6397$	$576 = 2^6 \cdot 3^2$	$C_2 \times C_{12} \times C_{24}$
0,0150	$6277 = 6277$	$2^3 \cdot 5 \cdot 17 \cdot 53 \cdot 4373$	$320 = 2^6 \cdot 5$	$C_2^2 \times C_4 \times C_{20}$
0,0154	$1567 = 1567$	$2^3 \cdot 5 \cdot 41 \cdot 53 \cdot 113$	$144 = 2^4 \cdot 3^2$	$C_2^2 \times C_6^2$
0,0155	$2153 = 2153$	$2^3 \cdot 5 \cdot 13 \cdot 181 \cdot 197$	$128 = 2^7$	$C_2^2 \times C_4 \times C_8$
0,0156	$4679 = 4679$	$2^3 \cdot 17 \cdot 457 \cdot 1409$	$256 = 2^8$	$C_4^2 \times C_{16}$
0,0157	$7327 = 17 \cdot 431$	$2^3 \cdot 5 \cdot 13 \cdot 73 \cdot 5657$	$384 = 2^7 \cdot 3$	$C_2^2 \times C_4 \times C_{24}$
0,0158	$5959 = 59 \cdot 101$	$2^3 \cdot 13 \cdot 53 \cdot 73 \cdot 353$	$320 = 2^6 \cdot 5$	$C_2^2 \times C_4 \times C_{20}$
0,0158	$8627 = 8627$	$2^3 \cdot 5 \cdot 13 \cdot 37 \cdot 15473$	$448 = 2^6 \cdot 7$	$C_2^2 \times C_4 \times C_{28}$
0,0160	$9199 = 9199$	$2^3 \cdot 13 \cdot 53 \cdot 61409$	$600 = 2^3 \cdot 3 \cdot 5^2$	$C_2 \times C_{10} \times C_{30}$
0,0161	$9133 = 9133$	$2^3 \cdot 5 \cdot 17 \cdot 37 \cdot 89 \cdot 149$	$480 = 2^5 \cdot 3 \cdot 5$	$C_2^4 \times C_{30}$
0,0163	$9677 = 9677$	$2^3 \cdot 5 \cdot 13 \cdot 17 \cdot 42373$	$512 = 2^9$	$C_2^2 \times C_4 \times C_{32}$
0,0173	$4181 = 37 \cdot 113$	$2^3 \cdot 13 \cdot 421 \cdot 1597$	$256 = 2^8$	$C_2 \times C_8 \times C_{16}$
0,0173	$6577 = 6577$	$2^3 \cdot 5 \cdot 61 \cdot 70913$	$288 = 2^5 \cdot 3^2$	$C_2 \times C_6 \times C_{24}$
0,0176	$1867 = 1867$	$2^3 \cdot 5 \cdot 13 \cdot 26813$	$128 = 2^7$	$C_2 \times C_8^2$
0,0178	$5183 = 71 \cdot 73$	$2^3 \cdot 5 \cdot 113 \cdot 23773$	$400 = 2^4 \cdot 5^2$	$C_2 \times C_{10} \times C_{20}$
0,0186	$3853 = 3853$	$2^3 \cdot 5 \cdot 13 \cdot 114197$	$256 = 2^8$	$C_2 \times C_8 \times C_{16}$
0,0186	$6073 = 6073$	$2^3 \cdot 5 \cdot 17 \cdot 29 \cdot 7481$	$384 = 2^7 \cdot 3$	$C_2^2 \times C_4 \times C_{24}$
0,0191	$3733 = 3733$	$2^3 \cdot 5 \cdot 53 \cdot 26293$	$256 = 2^8$	$C_2 \times C_8 \times C_{16}$
0,0193	$4217 = 4217$	$2^3 \cdot 5 \cdot 13 \cdot 29 \cdot 53 \cdot 89$	$288 = 2^5 \cdot 3^2$	$C_2^4 \times C_{18}$
0,0199	$4594 = 2 \cdot 2297$	$13 \cdot 17 \cdot 29 \cdot 37 \cdot 89$	$80 = 2^4 \cdot 5$	$C_2^3 \times C_{10}$
0,0200	$7717 = 7717$	$2^3 \cdot 5 \cdot 13 \cdot 41 \cdot 11173$	$512 = 2^9$	$C_2^2 \times C_4 \times C_{32}$
0,0202	$8683 = 19 \cdot 457$	$2^3 \cdot 5 \cdot 17 \cdot 29 \cdot 41 \cdot 373$	$576 = 2^6 \cdot 3^2$	$C_2^4 \times C_{36}$
0,0204	$2503 = 2503$	$2^3 \cdot 5 \cdot 17 \cdot 137 \cdot 269$	$192 = 2^6 \cdot 3$	$C_2^2 \times C_4 \times C_{12}$
0,0208	$697 = 17 \cdot 41$	$2^3 \cdot 5 \cdot 13 \cdot 37 \cdot 101$	$64 = 2^6$	$C_2^2 \times C_4^2$
0,0209	$5321 = 17 \cdot 313$	$2^3 \cdot 41 \cdot 449 \cdot 769$	$384 = 2^7 \cdot 3$	$C_4^2 \times C_{24}$
0,0212	$9274 = 2 \cdot 4637$	$13 \cdot 1093 \cdot 6053$	$200 = 2^3 \cdot 5^2$	$C_{10} \times C_{20}$
0,0213	$3763 = 53 \cdot 71$	$2^3 \cdot 5 \cdot 41 \cdot 34537$	$216 = 2^3 \cdot 3^3$	$C_2 \times C_6 \times C_{18}$
0,0219	$7961 = 19 \cdot 419$	$2^3 \cdot 13 \cdot 37 \cdot 65881$	$432 = 2^4 \cdot 3^3$	$C_2 \times C_6 \times C_{36}$
0,0219	$3197 = 23 \cdot 139$	$2^3 \cdot 5 \cdot 241 \cdot 4241$	$256 = 2^8$	$C_2 \times C_8 \times C_{16}$
0,0222	$1433 = 1433$	$2^3 \cdot 5 \cdot 29 \cdot 73 \cdot 97$	$128 = 2^7$	$C_2^2 \times C_4 \times C_8$
0,0230	$8003 = 53 \cdot 151$	$2^3 \cdot 5 \cdot 13 \cdot 17 \cdot 73 \cdot 397$	$608 = 2^5 \cdot 19$	$C_2^4 \times C_{38}$
0,0231	$8441 = 23 \cdot 367$	$2^3 \cdot 73 \cdot 401 \cdot 1217$	$640 = 2^7 \cdot 5$	$C_4^2 \times C_{40}$
0,0232	$6542 = 2 \cdot 3271$	$5 \cdot 29 \cdot 53 \cdot 5569$	$128 = 2^7$	$C_2 \times C_4 \times C_{16}$
0,0238	$7262 = 2 \cdot 3631$	$5 \cdot 13 \cdot 29 \cdot 101 \cdot 277$	$144 = 2^4 \cdot 3^2$	$C_2^3 \times C_{18}$
0,0239	$9959 = 23 \cdot 433$	$2^3 \cdot 29 \cdot 37 \cdot 113 \cdot 409$	$384 = 2^7 \cdot 3$	$C_2^3 \times C_{48}$
0,0240	$6305 = 5 \cdot 13 \cdot 97$	$2^3 \cdot 29 \cdot 41 \cdot 73 \cdot 229$	$512 = 2^9$	$C_2^2 \times C_4 \times C_{32}$
0,0243	$5767 = 73 \cdot 79$	$2^3 \cdot 5 \cdot 13 \cdot 17 \cdot 101 \cdot 149$	$480 = 2^5 \cdot 3 \cdot 5$	$C_2^4 \times C_{30}$
0,0245	$2427 = 3 \cdot 809$	$2^3 \cdot 5 \cdot 17 \cdot 34649$	$392 = 2^3 \cdot 7^2$	$C_2 \times C_{14} \times C_{14}$
0,0245	$4454 = 2 \cdot 17 \cdot 131$	$13 \cdot 29 \cdot 101 \cdot 521$	$96 = 2^5 \cdot 3$	$C_2 \times C_4 \times C_{12}$
0,0246	$7847 = 7 \cdot 19 \cdot 59$	$2^3 \cdot 5 \cdot 13 \cdot 29 \cdot 16333$	$640 = 2^7 \cdot 5$	$C_2^2 \times C_4 \times C_{40}$
0,0255	$8377 = 8377$	$2^3 \cdot 5 \cdot 13 \cdot 17 \cdot 113 \cdot 281$	$704 = 2^6 \cdot 11$	$C_2^4 \times C_{44}$

Tabelle A.15: Die ersten 50 Einträge der Berechnungstabellen ($\mu(N)$ minimal).

$\mu(N)$	N	Δ	$\mathrm{h}(\Delta)$	$\mathrm{Cl}(\Delta) \cong$
2,0189	$7848 = 2^3 \cdot 3^2 \cdot 109$	$5 \cdot 12318221$	$1640 = 2^3 \cdot 5 \cdot 41$	C_{1640}
2,0211	$7860 = 2^2 \cdot 3 \cdot 5 \cdot 131$	$13 \cdot 4752277$	$1644 = 2^2 \cdot 3 \cdot 137$	C_{1644}
2,0304	$9000 = 2^3 \cdot 3^2 \cdot 5^3$	81000001	$1865 = 5 \cdot 373$	C_{1865}
2,0307	$5340 = 2^2 \cdot 3 \cdot 5 \cdot 89$	28515601	$1169 = 7 \cdot 167$	C_{1169}
2,0340	$7524 = 2^2 \cdot 3^2 \cdot 11 \cdot 19$	56610577	$1591 = 37 \cdot 43$	C_{1591}
2,0544	$3660 = 2^2 \cdot 3 \cdot 5 \cdot 61$	13395601	$845 = 5 \cdot 13^2$	C_{845}
2,0566	$1512 = 2^3 \cdot 3^3 \cdot 7$	$5 \cdot 457229$	$388 = 2^2 \cdot 97$	C_{388}
2,0796	$8580 = 2^2 \cdot 3 \cdot 5 \cdot 11 \cdot 13$	$229 \cdot 321469$	$1830 = 2 \cdot 3 \cdot 5 \cdot 61$	C_{1830}
2,0811	$5460 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 13$	$409 \cdot 72889$	$1222 = 2 \cdot 13 \cdot 47$	C_{1222}
2,0811	$5280 = 2^5 \cdot 3 \cdot 5 \cdot 11$	$41 \cdot 679961$	$1186 = 2 \cdot 593$	C_{1186}
2,0849	$2700 = 2^2 \cdot 3^3 \cdot 5^2$	7290001	$655 = 5 \cdot 131$	C_{655}
2,0992	$6720 = 2^6 \cdot 3 \cdot 5 \cdot 7$	$1049 \cdot 43049$	$1484 = 2^2 \cdot 7 \cdot 53$	C_{1484}
2,1258	$3696 = 2^4 \cdot 3 \cdot 7 \cdot 11$	$73 \cdot 187129$	$882 = 2 \cdot 3^2 \cdot 7^2$	C_{882}
2,1288	$4992 = 2^7 \cdot 3 \cdot 13$	$5 \cdot 4984013$	$1154 = 2 \cdot 577$	C_{1154}
2,1383	$1260 = 2^2 \cdot 3^2 \cdot 5 \cdot 7$	$349 \cdot 4549$	$344 = 2^3 \cdot 43$	C_{344}
2,1436	$4080 = 2^4 \cdot 3 \cdot 5 \cdot 17$	16646401	$971 = 971$	C_{971}
2,1460	$5508 = 2^2 \cdot 3^4 \cdot 17$	$5 \cdot 6067613$	$1270 = 2 \cdot 5 \cdot 127$	C_{1270}
2,1603	$9876 = 2^2 \cdot 3 \cdot 823$	97535377	$2157 = 3 \cdot 719$	C_{2157}
2,1624	$2640 = 2^4 \cdot 3 \cdot 5 \cdot 11$	$137 \cdot 50873$	$666 = 2 \cdot 3^2 \cdot 37$	C_{666}
2,1642	$588 = 2^2 \cdot 3 \cdot 7^2$	$5 \cdot 69149$	$180 = 2^2 \cdot 3^2 \cdot 5$	C_{180}
2,1661	$4488 = 2^3 \cdot 3 \cdot 11 \cdot 17$	$5 \cdot 4028429$	$1068 = 2^2 \cdot 3 \cdot 89$	C_{1068}
2,1895	$7560 = 2^3 \cdot 3^3 \cdot 5 \cdot 7$	$4517 \cdot 12653$	$1720 = 2^3 \cdot 5 \cdot 43$	C_{1720}
2,1993	$3480 = 2^3 \cdot 3 \cdot 5 \cdot 29$	12110401	$865 = 5 \cdot 173$	C_{865}
2,2039	$1680 = 2^4 \cdot 3 \cdot 5 \cdot 7$	$113 \cdot 24977$	$456 = 2^3 \cdot 3 \cdot 19$	C_{456}
2,2262	$9300 = 2^2 \cdot 3 \cdot 5^2 \cdot 31$	$13 \cdot 6653077$	$2106 = 2 \cdot 3^4 \cdot 13$	C_{2106}
2,2456	$840 = 2^3 \cdot 3 \cdot 5 \cdot 7$	$13 \cdot 54277$	$254 = 2 \cdot 127$	C_{254}
2,2542	$7728 = 2^4 \cdot 3 \cdot 7 \cdot 23$	$5 \cdot 11944397$	$1806 = 2 \cdot 3 \cdot 7 \cdot 43$	C_{1806}
2,2691	$7260 = 2^2 \cdot 3 \cdot 5 \cdot 11^2$	52707601	$1719 = 3^2 \cdot 191$	C_{1719}
2,2770	$8448 = 2^8 \cdot 3 \cdot 11$	$5 \cdot 14273741$	$1976 = 2^3 \cdot 13 \cdot 19$	C_{1976}
2,3030	$8700 = 2^2 \cdot 3 \cdot 5^2 \cdot 29$	$17 \cdot 4452353$	$2052 = 2^2 \cdot 3^3 \cdot 19$	C_{2052}
2,3231	$720 = 2^4 \cdot 3^2 \cdot 5$	$13 \cdot 39877$	$230 = 2 \cdot 5 \cdot 23$	C_{230}
2,3364	$4200 = 2^3 \cdot 3 \cdot 5^2 \cdot 7$	$797 \cdot 22133$	$1086 = 2 \cdot 3 \cdot 181$	C_{1086}
2,3700	$8280 = 2^3 \cdot 3^2 \cdot 5 \cdot 23$	$6317 \cdot 10853$	$2020 = 2^2 \cdot 5 \cdot 101$	C_{2020}
2,3742	$7140 = 2^2 \cdot 3 \cdot 5 \cdot 7 \cdot 17$	$997 \cdot 51133$	$1772 = 2^2 \cdot 443$	C_{1772}
2,3837	$9360 = 2^4 \cdot 3^2 \cdot 5 \cdot 13$	$661 \cdot 132541$	$2268 = 2^2 \cdot 3^4 \cdot 7$	C_{2268}
2,3918	$8160 = 2^5 \cdot 3 \cdot 5 \cdot 17$	$7193 \cdot 9257$	$2012 = 2^2 \cdot 503$	C_{2012}
2,4057	$1980 = 2^2 \cdot 3^2 \cdot 5 \cdot 11$	3920401	$575 = 5^2 \cdot 23$	C_{575}
2,4213	$1140 = 2^2 \cdot 3 \cdot 5 \cdot 19$	1299601	$357 = 3 \cdot 7 \cdot 17$	C_{357}
2,4219	$8772 = 2^2 \cdot 3 \cdot 17 \cdot 43$	$5 \cdot 15389597$	$2174 = 2 \cdot 1087$	C_{2174}
2,4331	$9960 = 2^3 \cdot 3 \cdot 5 \cdot 83$	$3697 \cdot 26833$	$2448 = 2^4 \cdot 3^2 \cdot 17$	C_{2448}
2,4500	$8940 = 2^2 \cdot 3 \cdot 5 \cdot 149$	79923601	$2237 = 2237$	C_{2237}
2,4529	$420 = 2^2 \cdot 3 \cdot 5 \cdot 7$	176401	$153 = 3^2 \cdot 17$	C_{153}
2,4561	$6840 = 2^3 \cdot 3^2 \cdot 5 \cdot 19$	$173 \cdot 270437$	$1764 = 2^2 \cdot 3^2 \cdot 7^2$	C_{1764}
2,4985	$5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7$	$101 \cdot 251501$	$1366 = 2 \cdot 683$	C_{1366}
2,5040	$9240 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	85377601	$2355 = 3 \cdot 5 \cdot 157$	C_{2355}
2,5885	$9780 = 2^2 \cdot 3 \cdot 5 \cdot 163$	$433 \cdot 220897$	$2562 = 2 \cdot 3 \cdot 7 \cdot 61$	C_{2562}
2,6179	$2220 = 2^2 \cdot 3 \cdot 5 \cdot 37$	$1889 \cdot 2609$	$692 = 2^2 \cdot 173$	C_{692}
2,8609	$3900 = 2^2 \cdot 3 \cdot 5^2 \cdot 13$	15210001	$1245 = 3 \cdot 5 \cdot 83$	C_{1245}
2,8740	$3240 = 2^3 \cdot 3^4 \cdot 5$	10497601	$1061 = 1061$	C_{1061}
3,0962	$7020 = 2^2 \cdot 3^3 \cdot 5 \cdot 13$	$41 \cdot 1201961$	$2276 = 2^2 \cdot 569$	C_{2276}

Tabelle A.16: Die letzen 50 Einträge der Berechnungstabellen ($\mu(N)$ maximal).

$\mu(N)$	N	Δ	$\mathrm{h}(\Delta)$	$\mathrm{Cl}(\Delta) \cong$	$u(N)$
0,1207	$4786 = 2 \cdot 2393$	22905797	$63 = 3^2 \cdot 7$	C_{63}	3,2159
0,1208	$3274 = 2 \cdot 1637$	10719077	$45 = 3^2 \cdot 5$	C_{45}	3,6786
0,1353	$2026 = 2 \cdot 1013$	4104677	$33 = 3 \cdot 11$	C_{33}	2,2923
0,1356	$7754 = 2 \cdot 3877$	60124517	$109 = 109$	C_{109}	1,4258
0,1359	$3446 = 2 \cdot 1723$	11874917	$53 = 53$	C_{53}	1,5026
0,1367	$3134 = 2 \cdot 1567$	9821957	$49 = 7^2$	C_{49}	3,0226
0,1391	$326 = 2 \cdot 163$	106277	$7 = 7$	C_7	2,0135
0,1426	$2174 = 2 \cdot 1087$	4726277	$37 = 37$	C_{37}	1,5394
0,1428	$1774 = 2 \cdot 887$	3147077	$31 = 31$	C_{31}	1,5667
0,1433	$6254 = 2 \cdot 53 \cdot 59$	39112517	$95 = 5 \cdot 19$	C_{95}	2,2064
0,1456	$6434 = 2 \cdot 3217$	41396357	$99 = 3^2 \cdot 11$	C_{99}	2,7199
0,1459	$1354 = 2 \cdot 677$	1833317	$25 = 5^2$	C_5	3,1958
0,1461	$206 = 2 \cdot 103$	42437	$5 = 5$	C_{26}	2,1949
0,1461	$4414 = 2 \cdot 2207$	19483397	$71 = 71$	C_{71}	1,4512
0,1469	$6806 = 2 \cdot 41 \cdot 83$	46321637	$105 = 3 \cdot 5 \cdot 7$	C_{105}	3,3775
0,1469	$4666 = 2 \cdot 2333$	21771557	$75 = 3 \cdot 5^2$	C_{75}	3,8742
0,1474	$3686 = 2 \cdot 19 \cdot 97$	13586597	$61 = 61$	C_{61}	1,4658
0,1493	$4174 = 2 \cdot 2087$	17422277	$69 = 3 \cdot 23$	C_{69}	1,9570
0,1503	$4006 = 2 \cdot 2003$	16048037	$67 = 67$	C_{67}	1,4507
0,1508	$6046 = 2 \cdot 3023$	36554117	$97 = 97$	C_1	1,4135
0,1519	$26 = 2 \cdot 13$	677	$1 = 1$	C_{98}	1,0000
0,1519	$6134 = 2 \cdot 3067$	37625957	$99 = 3^2 \cdot 11$	C_{99}	2,7021
0,1527	$6514 = 2 \cdot 3257$	42432197	$105 = 3 \cdot 5 \cdot 7$	C_{105}	3,3573
0,1528	$9046 = 2 \cdot 4523$	81830117	$141 = 3 \cdot 47$	C_{141}	1,7733
0,1539	$9826 = 2 \cdot 17^3$	96550277	$153 = 3^2 \cdot 17$	C_{153}	2,4360
0,1543	$4154 = 2 \cdot 31 \cdot 67$	17255717	$71 = 71$	C_{71}	1,4385
0,1557	$9986 = 2 \cdot 4993$	99720197	$157 = 157$	C_{157}	1,3679
0,1557	$5834 = 2 \cdot 2917$	34035557	$97 = 97$	C_{97}	1,4065
0,1558	$3334 = 2 \cdot 1667$	11115557	$59 = 59$	C_{59}	1,4559
0,1568	$2314 = 2 \cdot 13 \cdot 89$	5354597	$43 = 43$	C_{43}	1,4925
0,1570	$8774 = 2 \cdot 41 \cdot 107$	76983077	$141 = 3 \cdot 47$	C_{141}	1,7662
0,1578	$3794 = 2 \cdot 7 \cdot 271$	14394437	$67 = 67$	C_{67}	1,4392
0,1593	$9874 = 2 \cdot 4937$	97495877	$159 = 3 \cdot 53$	C_{159}	1,7394
0,1600	$4366 = 2 \cdot 37 \cdot 59$	19061957	$77 = 7 \cdot 11$	C_{77}	2,5756
0,1603	$3106 = 2 \cdot 1553$	9647237	$57 = 3 \cdot 19$	C_{57}	1,9949
0,1604	$674 = 2 \cdot 337$	454277	$15 = 3 \cdot 5$	C_{15}	2,8198
0,1620	$3314 = 2 \cdot 1657$	10982597	$61 = 61$	C_{61}	1,4428
0,1627	$1306 = 2 \cdot 653$	1705637	$27 = 3^3$	C_{27}	4,6531
0,1634	$2326 = 2 \cdot 1163$	5410277	$45 = 3^2 \cdot 5$	C_{45}	3,4909
0,1635	$8786 = 2 \cdot 23 \cdot 191$	77193797	$147 = 3 \cdot 7^2$	C_{147}	3,4951
0,1636	$9314 = 2 \cdot 4657$	86750597	$155 = 5 \cdot 31$	C_{155}	1,9958
0,1640	$3754 = 2 \cdot 1877$	14092517	$69 = 3 \cdot 23$	C_{69}	1,9269
0,1650	$9494 = 2 \cdot 47 \cdot 101$	90136037	$159 = 3 \cdot 53$	C_{159}	1,7305
0,1660	$3946 = 2 \cdot 1973$	15570917	$73 = 73$	C_{73}	1,4185
0,1663	$646 = 2 \cdot 17 \cdot 19$	417317	$15 = 3 \cdot 5$	C_{15}	2,7971
0,1664	$9406 = 2 \cdot 4703$	88472837	$159 = 3 \cdot 53$	C_{159}	1,7284
0,1671	$94 = 2 \cdot 47$	8837	$3 = 3$	C_3	2,6285
0,1673	$5506 = 2 \cdot 2753$	30316037	$99 = 3^2 \cdot 11$	$C_3 \times C_{33}$	2,6619
0,1677	$5246 = 2 \cdot 43 \cdot 61$	27520517	$95 = 5 \cdot 19$	C_{95}	2,1531
0,1686	$9266 = 2 \cdot 41 \cdot 113$	85858757	$159 = 3 \cdot 53$	C_{159}	1,7250

Tabelle A.17: Die ersten 50 Einträge der Berechnungstabellen mit $N^2+1 \in \mathbb{P}$ ($\mu(N)$ minimal).

$\mu(N)$	N	Δ	$\mathrm{h}(\Delta)$	$\mathrm{Cl}(\Delta) \cong$	$u(N)$
1,6056	$8784 = 2^4 \cdot 3^2 \cdot 61$	77158657	$1443 = 3 \cdot 13 \cdot 37$	C_{1443}	1,8834
1,6206	$240 = 2^4 \cdot 3 \cdot 5$	57601	$63 = 3^2 \cdot 7$	C_{63}	1,8810
1,6243	$9600 = 2^7 \cdot 3 \cdot 5^2$	92160001	$1581 = 3 \cdot 17 \cdot 31$	C_{1581}	2,0037
1,6297	$636 = 2^2 \cdot 3 \cdot 53$	404497	$145 = 5 \cdot 29$	C_{145}	1,3329
1,6320	$2136 = 2^3 \cdot 3 \cdot 89$	4562497	$417 = 3 \cdot 139$	C_{417}	1,1234
1,6463	$5424 = 2^4 \cdot 3 \cdot 113$	29419777	$961 = 31^2$	C_{961}	1,8548
1,6702	$2760 = 2^3 \cdot 3 \cdot 5 \cdot 23$	7617601	$535 = 5 \cdot 107$	C_{535}	1,2347
1,6733	$5700 = 2^2 \cdot 3 \cdot 5^2 \cdot 19$	32490001	$1021 = 1021$	C_{1021}	0,9257
1,6796	$204 = 2^2 \cdot 3 \cdot 17$	41617	$57 = 3 \cdot 19$	C_{57}	1,1970
1,6804	$4260 = 2^2 \cdot 3 \cdot 5 \cdot 71$	18147601	$791 = 7 \cdot 113$	C_{791}	1,3018
1,6887	$9180 = 2^2 \cdot 3^3 \cdot 5 \cdot 17$	84272401	$1579 = 1579$	C_{1579}	0,9289
1,6990	$9324 = 2^2 \cdot 3^2 \cdot 7 \cdot 37$	86936977	$1611 = 3^2 \cdot 179$	C_{1611}	1,3214
1,7095	$6240 = 2^5 \cdot 3 \cdot 5 \cdot 13$	38937601	$1131 = 3 \cdot 13 \cdot 29$	C_{1131}	1,9287
1,7119	$9900 = 2^2 \cdot 3^2 \cdot 5^2 \cdot 11$	98010001	$1713 = 3 \cdot 571$	C_{1713}	1,0884
1,7203	$5964 = 2^2 \cdot 3 \cdot 7 \cdot 71$	35569297	$1093 = 1093$	C_{1093}	0,9225
1,7224	$9120 = 2^5 \cdot 3 \cdot 5 \cdot 19$	83174401	$1601 = 1601$	C_{1601}	0,9263
1,7285	$6420 = 2^2 \cdot 3 \cdot 5 \cdot 107$	41216401	$1173 = 3 \cdot 17 \cdot 23$	C_{1173}	2,0794
1,7294	$3984 = 2^4 \cdot 3 \cdot 83$	15872257	$767 = 13 \cdot 59$	C_{767}	1,4947
1,7579	$6120 = 2^3 \cdot 3^2 \cdot 5 \cdot 17$	37454401	$1143 = 3^2 \cdot 127$	$C_3 \times C_{381}$	1,3371
1,7607	$1320 = 2^3 \cdot 3 \cdot 5 \cdot 11$	1742401	$295 = 5 \cdot 59$	C_{295}	1,2560
1,7713	$5760 = 2^7 \cdot 3^2 \cdot 5$	33177601	$1091 = 1091$	C_{1091}	0,9183
1,7885	$1716 = 2^2 \cdot 3 \cdot 11 \cdot 13$	2944657	$377 = 13 \cdot 29$	C_{377}	1,5891
1,8332	$4920 = 2^3 \cdot 3 \cdot 5 \cdot 41$	24206401	$981 = 3^2 \cdot 109$	C_{981}	1,3392
1,8343	$2304 = 2^8 \cdot 3^2$	5308417	$501 = 3 \cdot 167$	C_{501}	1,0961
1,8506	$960 = 2^6 \cdot 3 \cdot 5$	921601	$235 = 5 \cdot 47$	C_{235}	1,2581
1,8531	$1440 = 2^5 \cdot 3^2 \cdot 5$	2073601	$335 = 5 \cdot 67$	C_{335}	1,2361
1,8551	$300 = 2^2 \cdot 3 \cdot 5^2$	90001	$87 = 3 \cdot 29$	C_{87}	1,1427
1,9252	$7944 = 2^3 \cdot 3 \cdot 331$	63107137	$1581 = 3 \cdot 17 \cdot 31$	C_{1581}	1,9542
1,9291	$6540 = 2^2 \cdot 3 \cdot 5 \cdot 109$	42771601	$1331 = 11^3$	C_{1331}	2,7260
1,9558	$1920 = 2^7 \cdot 3 \cdot 5$	3686401	$455 = 5 \cdot 7 \cdot 13$	C_{455}	2,1246
1,9584	$7596 = 2^2 \cdot 3^2 \cdot 211$	57699217	$1545 = 3 \cdot 5 \cdot 103$	C_{1545}	1,4393
1,9638	$120 = 2^3 \cdot 3 \cdot 5$	14401	$43 = 43$	C_{43}	0,8206
2,0106	$6360 = 2^3 \cdot 3 \cdot 5 \cdot 53$	40449601	$1353 = 3 \cdot 11 \cdot 41$	C_{1353}	1,7535
2,0304	$9000 = 2^3 \cdot 3^2 \cdot 5^3$	81000001	$1865 = 5 \cdot 373$	C_{1865}	1,1522
2,0307	$5340 = 2^2 \cdot 3 \cdot 5 \cdot 89$	28515601	$1169 = 7 \cdot 167$	C_{1169}	1,2418
2,0340	$7524 = 2^2 \cdot 3^2 \cdot 11 \cdot 19$	56610577	$1591 = 37 \cdot 43$	C_{1591}	1,7713
2,0544	$3660 = 2^2 \cdot 3 \cdot 5 \cdot 61$	13395601	$845 = 5 \cdot 13^2$	C_{845}	2,3468
2,0849	$2700 = 2^2 \cdot 3^3 \cdot 5^2$	7290001	$655 = 5 \cdot 131$	C_{655}	1,1794
2,1436	$4080 = 2^4 \cdot 3 \cdot 5 \cdot 17$	16646401	$971 = 971$	C_{971}	0,8891
2,1603	$9876 = 2^2 \cdot 3 \cdot 823$	97535377	$2157 = 3 \cdot 719$	C_{2157}	1,0499
2,1993	$3480 = 2^3 \cdot 3 \cdot 5 \cdot 29$	12110401	$865 = 5 \cdot 173$	C_{865}	1,1594
2,2691	$7260 = 2^2 \cdot 3 \cdot 5 \cdot 11^2$	52707601	$1719 = 3^2 \cdot 191$	C_{1719}	1,2623
2,4057	$1980 = 2^2 \cdot 3^2 \cdot 5 \cdot 11$	3920401	$575 = 5^2 \cdot 23$	C_{575}	1,7466
2,4213	$1140 = 2^2 \cdot 3 \cdot 5 \cdot 19$	1299601	$357 = 3 \cdot 7 \cdot 17$	C_{357}	1,7625
2,4500	$8940 = 2^2 \cdot 3 \cdot 5 \cdot 149$	79923601	$2237 = 2237$	C_{2237}	0,8838
2,4529	$420 = 2^2 \cdot 3 \cdot 5 \cdot 7$	176401	$153 = 3^2 \cdot 17$	C_{153}	1,4588
2,4531	$5880 = 2^3 \cdot 3 \cdot 5 \cdot 7^2$	34574401	$1539 = 3^4 \cdot 19$	$C_3 \times C_{513}$	2,1877
2,5040	$9240 = 2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11$	85377601	$2355 = 3 \cdot 5 \cdot 157$	C_{2355}	1,3541
2,8609	$3900 = 2^2 \cdot 3 \cdot 5^2 \cdot 13$	15210001	$1245 = 3 \cdot 5 \cdot 83$	C_{1245}	1,3750
2,8740	$3240 = 2^3 \cdot 3^4 \cdot 5$	10497601	$1061 = 1061$	C_{1061}	0,8485

Tabelle A.18: Die letzten 50 Einträge der Berechnungstabellen mit $N^2 + 1 \in \mathbb{P}$ ($\mu(N)$ maximal).

Tabellenverzeichnis

Algorithmenverzeichnis

Literaturverzeichnis

[AKS02] M. Agrawal, N. Kayal, and N. Saxena. **Primes is in p**. 2002. preprint by {manindra@cse., kaylin@, nitinsa@cse.}iitk.ac.in.

[AM93] A. O. L. Atkin and F. Morain. **Elliptic curves and primality proving**. *Mathematics of Computation*, 61(203):29–68, 1993.

[BB97] Ingrid Biehl and Johannes Buchmann. **An analysis of the reduction algorithms for binary quadratic forms**. Technical Report TI-26/97, Technische Universität Darmstadt, Fachbereich Informatik, 1997. `www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR`.

[BBHM99] Ingrid Biehl, Johannes Buchmann, Safuat Hamdy, and Andreas Meyer. **Cryptographic protocols based on the intractability of extracting roots and computing discrete logarithms**. Technical Report TI-16/99, Technische Universität Darmstadt, Fachbereich Informatik, 1999. `www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR`.

[BBHM00] Ingrid Biehl, Johannes Buchmann, Safuat Hamdy, and Andreas Meyer. **A signature scheme based on the intractability of extracting roots**. Technical Report TI-1/00, Technische Universität Darmstadt, Fachbereich Informatik, 2000. `www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR`.

[Ber03] Daniel J. Bernstein. **Proving primality in essentially quartic random time**. 2003. preprint at `www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR`.

[BMT96] Ingrid Biehl, Bernd Meyer, and Christoph Thiel. **Cryptographic protocols based on real-quadratic A-fields (extended abstract)**. In Kwangjo Kim and Tsutomu Matsumoto, editors, *Advances in Cryptology – ASIACRYPT '96*, volume 1163 of *Lecture Notes in Computer Science*, pages 15–25. Springer-Verlag, 1996.

[BTW95] Johannes Buchmann, Christoph Thiel, and Hugh C. Williams. **Short representation of quadratic integers**. In Wieb Bosma

and Alf J. van der Poorten, editors, *Computational Algebra and Number Theory, Sydney 1992*, volume 325 of *Mathematics and its Applications*, pages 159–185. Kluwer Academic Publishers, 1995.

[Buc99] Johannes Buchmann. **Einführung in die Kryptographie**. Springer–Verlag, 1999.

[Bue84] Duncan A. Buell. **The expectation of success using a Monte Carlo factoring method – some statistics on quadratic class numbers**. *Mathematics of Computation*, 43(167):313–327, 1984.

[CL84] Henri Cohen and Hendrik W. Lenstra, Jr. **Heuristics on class groups of number fields**. In Hendrik Jager, editor, *Number Theory, Noordwijkerhout 1983*, volume 1068 of *Lecture Notes in Mathematics*, pages 33–62. Springer-Verlag, 1984.

[CM87] Henri Cohen and J. Martinet. **Class groups of number fields: numerical heuristics**. *Mathematics of Computation*, 48(177):123–137, 1987.

[Coh95] Henri Cohen. **A Course in Computational Algebraic Number Theory**, volume 138 of *Graduate Texts in Mathematics*. Springer–Verlag, 1995.

[DH76] Whitfield Diffie and Martin E. Hellman. **New directions in cryptography**. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[ElG85] Taher ElGamal. **A public key cryptosystem and a signature scheme based on discrete logarithms**. *IEEE Transactions on Information Theory*, 31(4):469–472, 1985.

[Gro00] Clemens Gross. **Ein Verschlüsselungsprotokoll auf Basis von reellquadratischen Zahlkörpern**. Master's thesis, Technische Universität Darmstadt, Fachbereich Informatik, 2000. German.

[Ham02] Safuat Hamdy. **Über die Sicherheit und Effizienz kryptographischer Verfahren mit Klassengruppen imaginärquadratischer Zahlkörper**. PhD thesis, Technische Universität Darmstadt, Fachbereich Informatik, Darmstadt, 2002. `www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR`.

[Has63] H. Hasse. **Zahlentheorie**. Berlin: Akademie–Verlag, 2 edition, 1963.

[Has64] H. Hasse. **Vorlesungen über Zahlentheorie**, volume 59 of *Die Grundlehren der Mathematischen Wissenschaften in Einzeldarstellungen*. Springer–Verlag, 2 edition, 1964.

[Hei93] R. Heiman. **A note on discrete logarithms with special structure**. In Rainer A. Rueppel, editor, *Advances in Cryptology – EUROCRYPT '92*, volume 658 of *Lecture Notes in Computer Science*, pages 437–448. Springer-Verlag, 1993.

[HJP97] Detlef Hühnlein, Michael J. Jacobson, Jr., and Sachar Paulus. **A cryptosystem based on non-maximal imaginary quadratic orders with fast decryption**. Technical Report TI-24/97, Technische Universität Darmstadt, Fachbereich Informatik, 1997. `www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR`.

[HMNP00] Tobias Hahn, Andreas Meyer, Stefan Neis, and Thomas Pfahler. **Implementing cryptographic protocols based on algebraic number fields**. Technical Report TI-24/99, Technische Universität Darmstadt, Fachbereich Informatik, 2000. `www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR`.

[HPT99] Michael Hartmann, Sachar Paulus, and Tsuyoshi Takagi. **NICE – new ideal coset encryption**. Technical Report TI-11/99, Technische Universität Darmstadt, Fachbereich Informatik, 1999. `www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR`.

[HS97] Simon Hunter and Jonathan Sorenson. **Approximating the number of integers free of large prime factors**. *Mathematics of Computation*, 66(220):1729–1741, 1997.

[Hüh00a] Detlef Hühnlein. **Faster generation of nice-schnorr-type signatures**. Technical Report TI-8/00, Technische Universität Darmstadt, Fachbereich Informatik, 2000. `www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR`.

[Hüh00b] Detlef Hühnlein. **Quadratic orders for NESSIE – overview and parameter sizes of three public key families**. Technical Report TI-3/00, Technische Universität Darmstadt, Fachbereich Informatik, 2000. `www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR`.

[Jac99] Michael J. Jacobson, Jr. **Subexponential Class Group Computation in Quadratic Orders**. PhD thesis, Technische Universität Darmstadt, Fachbereich Informatik, Darmstadt, 1999.

[Kap76] Pierre Kaplan. **Sur le 2-groupe des classes d'idéaux des corps quadratiques**. *Journal für die reine und angewandte Mathematik*, 283/284:313–363, 1976. French.

[KV92] A. A. Karatsuba and S. M. Voronin. **The Riemann Zeta-Function**. De Gruyter expositions in mathematics. De Gruyter, 1992.

[Lan68] H. Lang. **Über eine Gattung elementar-arithmetischer Klasseninvarianten reell-quadratischer Zahlkörper**. *Journal für die reine und angewandte Mathematik*, 233:123–175, 1968. German.

[Lan91] Serge Lang. **Algebraic number theory**, volume 110 of *Graduate Texts in Mathematics*. Springer–Verlag, 2. edition, 1991.

[LL90] Arjen K. Lenstra and Hendrik W. Lenstra, Jr. **Algorithms in number theory**. In Jan van Leeuwen, editor, *Handbook of theoretical computer science – Algorithms and complexity*, volume A, chapter 12, pages 673–715. Elsevier Science Publishers, 1990.

[Mar77] Daniel A. Marcus. **Number Fields**. Springer–Verlag, 1977.

[Mar00] G. Marsaglia. **The monster, a random number generator with period 10^{2857} times as long as the previously touted longest-period one**. Preprint, 2000.

[Mey97] Andreas Meyer. **Ein neues Identifikations- und Signaturverfahren über imaginärquadratischen Zahlkörpern**. Master's thesis, Technische Universität Darmstadt, Fachbereich Informatik, 1997. `www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR`.

[MvOV97] Alfred J. Menezes, Paul C. van Oorschot, and Scott A. Vanstone. **Handbook of Applied Cryptography**. CRC Press, 1997.

[Nar74] Wladyslaw Narkiewicz. **Elementary and analytic theory of algebraic numbers**. Polish Scientific Publishers, Warszawa, 1974.

[PZ89] Michael E. Pohst and Hans Zassenhaus. **Algorithmic algebraic number theory**. Cambridge University Press, 1989.

[Réd28] L. Rédei. **Über die Klassenzahl des imaginären quadratischen Zahlkörpers**. *Journal für die reine und angewandte Mathematik*, 159:210–219, 1928.

[RSA78] Ronald L. Rivest, Adi Shamir, and Leonard Adleman. **A method for obtaining digital signatures and public-key cryptosystems**. *Communications of the ACM*, 21(2):120–126, 1978.

[Sch99] Joachim Schaub. **Implementierung von Public-Key-Kryptosystemen über imaginär-quadratischen Ordnungen**. Master's thesis, Technische Universität Darmstadt, Fachbereich Informatik, 1999.

[Sil99] Robert D. Silverman. **Exposing the mythical MIPS year**. *IEEE Computer*, 32(8):22–26, 1999.

[Ste74] Hans-Joachim Stender. **Über die Bestimmung der Grundeinheit gewisser reell-quadratischer Zahlkörper**. *Abh. Math. Seminar Univ. Hamburg*, 42:33–40, 1974. German.

[Ste75] Hans-Joachim Stender. **Eine Formel für Grundeinheiten in reinen algebraischen Zahlkörpern dritten, vierten und sechsten Grades**. *Journal of Number Theory*, 7(2):235–250, 1975. German.

[Vol00] Ulrich Vollmer. **Asymptotically fast discrete logarithms in quadratic number fields**. Technical Report TI-6/00, Technische Universität Darmstadt, Fachbereich Informatik, 2000. `www.informatik.tu-darmstadt.de/TI/Veroeffentlichung/TR`.

Stichwortverzeichnis