Westfälische Wilhelms-Universität Münster

Fachbereich 10 Mathematik und Informatik

Elliptische Kurven und Kryptographie

gelesen von PD Dr. Karin Halupczok

Zusammenfassung von Phil Steinhorst

Sommersemester 2015

Hier kommt bald ein Bild hin!

http://wwwmath.uni-muenster.de/u/karin.halupczok/ellKKSoSe15/

Stand: 17. April 2015

Vorwort

Der vorliegende Text ist eine inhaltliche Aufbereitung zur Vorlesung Elliptische Kurven und Kryptographie, gelesen von PD Dr. Karin Halupczok an der WWU Münster im Sommersemester 2015. Der Inhalt entspricht weitestgehend dem handschriftlichen Skript, welches auf der Vorlesungswebsite bereitsgestellt wird. Dieses Werk ist daher keine Eigenleistung des Autors und wird nicht von der Dozentin der Veranstaltung korrekturgelesen. Für die Korrektheit des Inhalts wird keinerlei Garantie übernommen. Bemerkungen, Korrekturen und Ergänzungen kann man folgenderweise loswerden:

- persönlich durch Überreichen von Notizen oder per E-Mail
- durch Abändern der entsprechenden TeX-Dateien und Versand per E-Mail an mich
- direktes Mitarbeiten via GitHub. Dieses Skript befindet sich im `latex-wwu`-Repository von Jannes Bantje:

  https://github.com/JaMeZ-B/latex-wwu

Literatur

- Blake, Seroussi, Smart: Elliptic curves in cryptography
- Menezes, van Oorschot, Vanstone: Handbook of applied cryptography
- Silverman: The arithmetic of elliptic curves
- Silverman: A friendly introduction to number theory, chap. 40-45
- Washington: Elliptic curves, number theory and cryptography
- Werner: Elliptische Kurven in der Kryptographie

Kommentar der Dozentin

In der Vorlesung beschäftigen wir uns mit den arithmetischen und geometrischen Eigenschaften elliptischer Kurven sowie deren Anwendungen in der Kryptographie. Dabei werden wir auch einen Vergleich mit Anwendungen der elementaren Zahlentheorie in der Kryptographie ziehen. Wir verfolgen eine elementare Herangehensweise, d.h. Kenntnisse der algebraischen Geometrie und der Funktionen- oder Zahlentheorie werden nicht benötigt. Es genügen die Vorkenntnisse aus den Grundvorlesungen.

Vorlesungswebsite

Das handgeschriebene Skript sowie weiteres Material findet man unter folgendem Link:

http://wwwmath.uni-muenster.de/u/karin.halupczok/ellKKSoSe15/

Titelbild

Das fehlt noch. Über Ideen und Anregungen freue ich mich sehr!

Phil Steinhorst
p.st@wwu.de

Inhaltsverzeichnis

0 Motivation und Einführung **4**

1 Allgemeines über Kryptographieverfahren **7**

1.1 Grundlagen aus der elementaren Zahlentheorie und Gruppentheorie 7

1.1.1 Zahlen, Darstellung von Zahlen 7

Index **13**

0 Motivation und Einführung

Kryptologie

[1] Die **Kryptologie** besteht aus den folgenden beiden Gebieten:

Kryptographie: Studium mathematischer Techniken zur Verschlüsselung von Informationen oder geheimen Nachrichten und dem Schutz von Daten.

Kryptoanalyse: Beschreibung der Rückgewinnung von Informationen aus verschlüsselten Texten, der Entschlüsselung.

Oft meint man mit "Kryptographie" die Kryptologie.

Früher wurde die Kryptographie vor allem im militärischen oder diplomatischen Sektor verwendet, heutzutage steht in unserer vernetzten Welt vor allem auch der praktische Nutzen im Alltag im Vordergrund: im Internet einkaufen, Online-Banking, persönliche Daten geheimhalten bzw. Datenschutz, Nachrichten und Dokumente digital unterschreiben etc. Das Internet liefert schnelle Informationswege über öffentliche Kanäle, die leicht abgehört werden können, sodass die Verschlüsselung schützenswerter Daten unumgänglich wird. Auch die Möglichkeit zur Signierung wird nötig, weil sehr leicht Absenderangaben gefälscht werden können. Eventuell nicht abhörsichere Kanäle können außer dem Internet aber auch Briefe, Radio, Boten, etc. sein.

Bei der **symmetrischen Verschlüsselung** von Daten gibt es einen Sender S und einen Empfänger E, die sich beide auf einen gemeinsamen Schlüssel geeinigt haben, der zum Ver- und Entschlüsseln dient. Beim **Caesar-Code** z.B. ist dies die Vereinbarung, jeden Buchstaben durch den dritten nachfolgenden im Alphabet zu ersetzen, also $A \mapsto D, B \mapsto E, C \mapsto F$, usw. Die Entschlüsselung ist klar. Derartige **monoalphabetische Chiffrierungen**, bei der jeder Buchstabe des Alphabets stets durch denselben Geheimtextbuchstaben chiffriert wird, sind durch Häufigkeitsanalysen durch einen Angreifer, der die verschlüsselten Nachrichten abhört, sehr leicht zu entschlüsseln. Übrigens gibt es auch heutzutage PDF-Verschlüsselungsprogramme, die so arbeiten!
In dieser Vorlesung behandeln wir die heutzutage gängigen modernen Methoden, die als sicher gelten. Worauf diese starke Sicherheit beruht, hat mathematische Gründe, die wir besprechen möchten. Vor allem interessiert uns, wie und welche Mathematik in die Kryptologie kommt, sodass wir deren Verfahren verstehen können.

Die Anwendungen erfordern die Lösung folgender Probleme bei symmetrischen Verschlüsselungsverfahren:

- Schlüsselaustausch über öffentliche Kanäle (**öffentliche Schlüssel**)
- Verschlüsselung ohne vorherigen Schlüsselaustausch (mit **geheimen Schlüsseln**, die nicht versendet werden)
- Digitale Signierung und Autentifizierung

Dies können **asymmetrische Verfahren** leisten (auch **Public Key-Kryptographie** genannt) und gehen zurück auf Ideen von Diffie[1] und Hellman[2] aus den 70er Jahren:

Jeder Nutzer eines Kommunikationskanals hat einen privaten Schlüssel, den er geheim hält und niemand sonst kennt, sowie einen öffentlichen Schlüssel, den jeder einsehen kann. Eine Nachricht wird dann unter Ausnutzung einer Funktion $x \mapsto f(x)$ verschlüsselt, die zwar leicht zu berechnen, aber praktisch nur mit Kenntnis des privaten Schlüssels des rechtmäßigen Empfängers entschlüsselt werden kann. Der Sender der Nachricht wird dafür den

[1] Whitfield Diffie, http://de.wikipedia.org/wiki/Whitfield_Diffie
[2] Martin Hellman, http://de.wikipedia.org/wiki/Martin_Hellman

öffentlichen Schlüssel des Empfängers zur Verschlüsselung benutzen. Eine derartige Funktion heißt **Einwegfunktion**.

Beispiele

- **RSA-Verfahren**: $(p, q) \mapsto p \cdot q$ mit p, q prim.
- **ECC-Verfahren**: $x \mapsto mx$ in einer Gruppe auf einer elliptischen Kurve.

In einem ersten Teil der Vorlesung stellen wir gängige Verfahren dar, die leicht mit dem Zahlring $\mathbb{Z}$ und Strukturen darin realisiert werden können. Dabei werden wir nur einige Hilfsmittel der elementaren Zahlentheorie entwickeln und dafür heranziehen. In einem zweiten Teil studieren wir die Eigenschaften elliptischer Kurven als interessante geometrische und arithmetische Objekte, die sich in der Praxis der Kryptographie als nützlich erwiesen haben. Wir besprechen dann auch die Sicherheit und Implementierung dieser Verfahren und vergleichen sie miteinander.

Elliptische Kurven

Was sind elliptische Kurven? Jedenfalls sind elliptische Kurven **keine** Ellipsen. Ellipsen lassen sich durch Gleichungen der Form

$$\left(\frac{x}{a}\right)^2 + \left(\frac{y}{b}\right)^2 = 1 \text{ mit } a, b \in \mathbb{R} \setminus \{0\}$$

beschreiben. Durch die Parametrisierung $x(t) = a \cdot \cos(t), y(t) = b \cdot \sin(t)$ ergibt sich für die Bogenlänge der Ellipse ein elliptisches Integral zweiter Art, nämlich

$$\int_0^{2\pi} \sqrt{\left(\frac{dx(t)}{dt}\right)^2 + \left(\frac{dy(t)}{dt}\right)^2} dt = 4 \int_0^{2\pi} \sqrt{a^2 \cos^2(t) + b^2 \cdot \sin^2(t)} dt$$

Im Allgemeinen lässt sich dies nicht elementar integrieren (außer natürlich, falls $a = b$, d.h. ein Kreis vorliegt). Mit Hilfe von elliptischen Kurven findet man jedoch nicht-elementare Stammfunktionen für diese Integrale ($\Rightarrow$ Funktionentheorie). Aufgrund dieses Zusammenhangs haben elliptische Kurven ihren Namen, sie haben ansonsten nichts mit Ellipsen zutun.

Was sind nun elliptische Kurven? Es sind "abelsche Varietäten der Dimension 1". Elliptische Kurven sind spezielle algebraische Kurven über einem Körper k. Es handelt sich dabei um glatte kubische Kurven, deren definierende algebraische Gleichung sich meist in die Form

$$E\colon y^2 = x^3 + ax + b \text{ mit } a, b \in k$$

bringen lässt. Als Punktmenge haben wir dafür

$$E(k) := \{(x, y) \in k^2 : y^2 = x^3 + ax + b\} \cup \{\mathcal{O}\},$$

die Kurve hängt nur von a, b ab. Die Rolle des zusätzlichen so genannten "unendlich fernen Punkts" $\mathcal{O}$ werden wir dabei noch näher beleuchten.

Zwei typische Beispiele für elliptische Kurven:

1) $E_1\colon y^2 = x^3 + 17$, hier liegen sogar Punkte mit ganzzahligen Koordinaten auf E_1, nämlich $(-2, 3), (-1, 4), (2, 5)$. Die Kurve besteht aus einer Zusammenhangskomponente.
2) $E_2\colon y^2 = x^3 + ax + b$, wenn $f(x) = x^3 + ax + b$ drei verschiedene Nullstellen hat, z.B. $a = -3, b = -1$. Die Kurve besteht dann aus zwei Zusammenhangskomponenten.

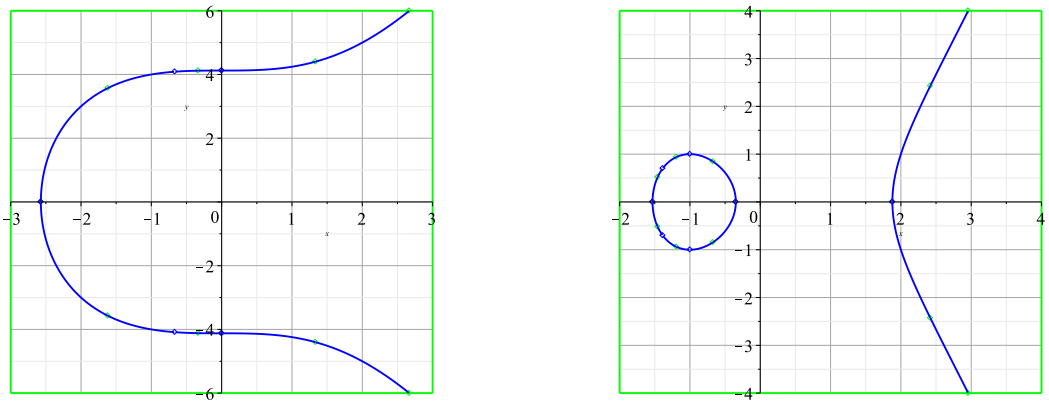

Abbildung 1: Die Kurven E_1 (links) und E_2 (rechts).

Bemerkung
Die kubischen Kurven $C_1 \colon y^2 = x^3 - 3x + 2$ und $C_2 \colon y^2 = x^3$ z. B. sind jedoch keine elliptischen Kurven, weil diese nicht glatt sind.

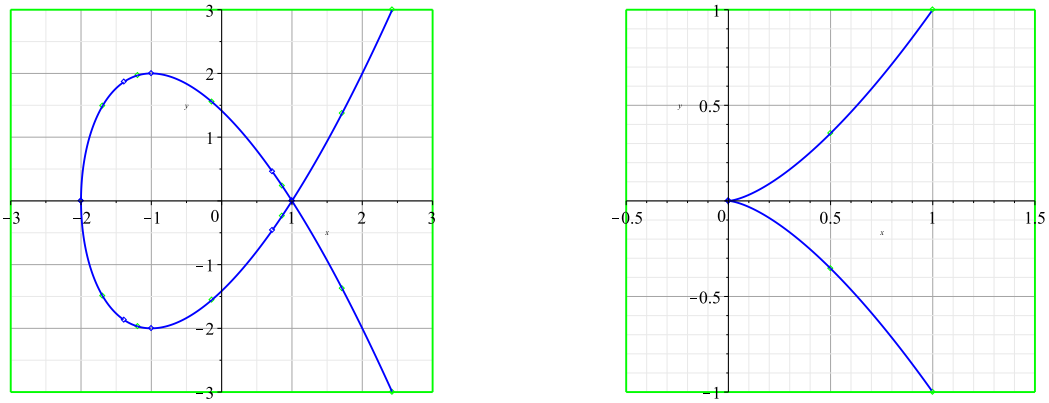

Abbildung 2: Die Kurven C_1 (links) und C_2 (rechts). C_1 ist nicht glatt im Punkt $(1, 1)$, C_2 nicht im Punkt $(0, 0)$.

Für die Kryptographie sind elliptische Kurven interessant, weil sich eine Verknüpfung auf ihrer Punktemenge definieren lässt, mit der diese zu einer Gruppe wird. Dabei gerade auch endliche Körper k zuzulassen, macht diese Verknüpfung auf Rechenmaschinen realisierbar. Die Sicherheit der darauf beruhenden elliptic curve cryptography (ECC) beruht darauf, dass das Problem des diskreten Logarithmus auf einer elliptischen Kurve E, nämlich die Umkehrung der Funktion $P \mapsto mP$ für $m \in \mathbb{N}$ fest, nach heutigem Wissensstand rechnerisch im Allgemeinen extrem schwer realisierbar ist.

1 Allgemeines über Kryptographieverfahren

1.1 Grundlagen aus der elementaren Zahlentheorie und Gruppentheorie

1.1.1 Zahlen, Darstellung von Zahlen

Die Zahlbereiche $\mathbb{N} \subseteq \mathbb{Z} \subseteq \mathbb{Q} \subseteq \mathbb{R} \subseteq \mathbb{C}$ sind aus den Grundvorlesungen bekannt. Bezüglich den Verknüpfungen $+$ und $\cdot$ sind verschiedene Axiome erfüllt, die diese Zahlbereiche zu interessante algebraische Strukturen machen: [2]

Halbgruppe	Gruppe	Ring	Körper
$(\mathbb{N}, +), (\mathbb{N}, \cdot)$			
$(\mathbb{Z}, +), (\mathbb{Z}, \cdot)$	$(\mathbb{Z}, +, 0)$	$(\mathbb{Z}, +, \cdot)$	
$(\mathbb{Q}, +), (\mathbb{Q}, \cdot)$	$(\mathbb{Q}, +, 0), (\mathbb{Q} \setminus \{0\}, \cdot, 1)$	$(\mathbb{Q}, +, \cdot)$	$(\mathbb{Q}, +, \cdot)$
$(\mathbb{R}, +), (\mathbb{R}, \cdot)$	$(\mathbb{R}, +, 0), (\mathbb{R} \setminus \{0\}, \cdot, 1)$	$(\mathbb{R}, +, \cdot)$	$(\mathbb{R}, +, \cdot)$
$(\mathbb{C}, +), (\mathbb{C}, \cdot)$	$(\mathbb{C}, +, 0), (\mathbb{C} \setminus \{0\}, \cdot, 1)$	$(\mathbb{C}, +, \cdot)$	$(\mathbb{C}, +, \cdot)$

Weiter sind $\mathbb{Q}$ und $\mathbb{R}$ angeordnete Körper, d.h. es gibt eine Anordnungsrelation $\leq$, die sich mit $+$ und $\cdot$ verträgt. Für $\mathbb{C}$ ist eine solche Anordnung nicht mehr möglich.

Definition 1 (Halbgruppe)
Eine Menge $H \neq \emptyset$ mit Verknüpfung $*\colon H \times H \to H$ heißt **Halbgruppe**, falls $*$ assoziativ ist, d.h. für alle $a, b, c \in H$ gilt $a * (b * c) = (a * b) * c$.

Definition 2 (Gruppe)
Eine Halbgruppe $(G, *)$ heißt **Gruppe**, falls es ein neutrales Element $e \in G$ gibt mit $e * g = g * e = g$ für alle $g \in G$, und falls zu jedem $g \in G$ ein inverses Element $h \in G$ existiert mit $h * g = g * h = e$. Wir schreiben auch g^{-1}, $\frac{1}{g}$ oder $-g$ für h.

Definition 3 (abelsche Gruppe)
Eine Gruppe $(G, *, e)$ heißt **abelsch** bzw. **kommutativ**, falls für alle $a, b \in G$ gilt: $a * b = b * a$.

Definition 4 (Ring)
Ein **Ring** $(R, +, \cdot)$ ist eine Menge $R \neq \emptyset$ und zwei Verknüpfungen $+$ und $\cdot$ so, dass $(R, +, 0)$ eine Gruppe ist, $(R, \cdot, 1)$ eine Halbgruppe mit neutralem Element 1, und so, dass die Distributivgesetze gelten, d.h. $(a + b) \cdot c = a \cdot c + b \cdot c$ und $c \cdot (a + b) = c \cdot a + c \cdot b$. Ring mit Eins

Bemerkung 5
Die Addition $+$ ist in einem Ring stets kommutativ. Ein Ring heißt kommutativ, wenn die Multiplikation $\cdot$ kommutativ ist. Soll der Nullring $R = \{0\}$ mit $1 = 0$ ausgeschlossen werden, fordert man zusätzlich noch $1 \neq 0$ in den Ringaxiomen.

Definition 6 (Einheit, Einheitengruppe)
Die in einem Ring $(R, +, \cdot)$ bezüglich $\cdot$ invertierbaren Elemente heißen **Einheiten**. Die Menge der Einheiten in R wird mit R^* bezeichnet, d.h. also $R^* := \{a \in R : \exists b \in R \text{ mit } a \cdot b = b \cdot a = 1\}$. Damit ist $(R^*, \cdot, 1)$ also eine Gruppe.

Definition 7 (Körper)
Ein **Körper** $(K, +, \cdot)$ ist ein kommutativer Ring mit $1 \neq 0$, für den $K^* = K \setminus \{0\}$ gilt.

Algebraische Strukturen dieser Art können wir auch in Teilmengen von $\mathbb{Z}$ auffinden und diese für kryptographische Anwendungen ausnutzen. Darum geht es in §1 dieser Vorlesung. Dabei wird klar, dass die Anwendungen auch – teilweise – in beliebigen Gruppen, Ringen und Körpern möglich sind. Die Gruppen, die durch elliptische Kurven gegeben sind, haben sich in der Praxis dann als vorteilhaft herausgestellt.

Wenn wir Teilmengen von $\mathbb{Z}$ auch praktisch untersuchen möchten, wird die Frage wichtig, wie man ganze Zahlen auf geschickte und kompakte Art darstellen kann. Dafür benutzen wir im Alltag das Dezimalsystem, für Rechenmaschinen ist auch das Binär- und das Hexadezimalsystem nützlich. Dabei werden die Ziffern $0, 1, \ldots 9$ bzw. $0, 1$ bzw. $0, 1, \ldots, 9, A, \ldots, F$ verwendet. Allgemein erhalten wir die g-adische Darstellung von $n \in \mathbb{N}$ so:

Satz 8
Sei $g \in \mathbb{N}, g \geq 2$ und $n \in \mathbb{N}$. Dann gibt es ein $k \in \mathbb{N}_0$ und $c_k, c_{k-1}, \ldots, c_0 \in \{0, \ldots, g-1\}$ (genannt "Ziffern"), sodass $n = c_k g^k + c_{k-1} g^{k-1} + \ldots + c_0 = \sum_{i=0}^{k} c_i g^i$. Fordern wir $c_k \neq 0$, ist k und die Folge $c_k, \ldots, c_1, c_0$ eindeutig bestimmt.

Beweis

Existenz: Sei $k \in \mathbb{N}_0$ so, dass $g^k \leq n < g^{k+1}$ gilt, das heißt wir setzen $k := \left\lfloor \frac{\log(n)}{\log(g)} \right\rfloor$. Zeige durch Induktion nach k die Existenz:
$k = 0$: Setze $c_0 := n$.
$k \rightsquigarrow k+1$: Sei $g^{k+1} \leq n < g^{k+2}$. Setze $n' = n - \left\lfloor \frac{n}{g^{k+1}} \right\rfloor \cdot g^{k+1}$. Es folgt $0 \leq n' < g^{k+1}$, d.h. auf n' ist die Induktionsvoraussetzung anwendbar. Nach dieser hat n' eine g-adische Zifferndarstellung $n' = \sum_{i=0}^{k} c_i g^i$.
Wegen $1 \leq \frac{n}{g^{k+1}} < g$ ist $1 \leq \left\lfloor \frac{n}{g^{k+1}} \right\rfloor < g$, also setze $c_{k+1} := \left\lfloor \frac{n}{g^{k+1}} \right\rfloor$.
$\Rightarrow n = c_{k+1} g^{k+1} + n' = \sum_{i=0}^{k+1} c_i g^i$.

Eindeutigkeit: Sind $\sum_{i=0}^{k} a_i g^i = m = \sum_{i=0}^{r} b_i g^i$ zwei verschiedene Darstellungen von $m \in \mathbb{N}$. Ist $r > k$, so sei $a_{k+1} = \ldots = a_r := 0$, sonst sei $b_{r+1} = \ldots = b_k := 0$, falls $r < k$. Dann sei $l := \max\{i \in \mathbb{N}_0 : i \leq \max\{k, r\}, a_i \neq b_i\}$ die größte Stelle, an der sich die Darstellungen unterscheiden.
$\Rightarrow 0 = \sum_{i=0}^{l} \underbrace{(a_i - b_i)}_{=0 \text{ für } i>l} g^i \Rightarrow \underbrace{|b_l - a_l|}_{\geq 1} g^l = \left| \sum_{i=0}^{l-1} (a_i - b_i) g^i \right|$
$\Rightarrow g^l \leq \sum_{i=0}^{l-1} |a_i - b_i| g^i \leq \sum_{i=0}^{l-1} (g-1) g^i = (g-1) \frac{g^l - 1}{g-1} = g^l - 1 \quad \lightning$ □

Definition 9 (g-adische Darstellung)
Die Ziffernfolge $c_k, c_{k-1}, \ldots c_0$ aus Satz 8 heißt **g-adische Darstellung** von n. Die Zahl c_k heißt **Leitziffer**, die Zahl c_0 die **Endziffer**. Die Zahl $k+1$ heißt **Stellenzahl** bzw. **Länge** der g-adischen Darstellung. Die Zahl g heißt auch **Basis** der Darstellung. Eine **m-Bit-Zahl** ist eine Zahl $n \in \mathbb{N}$ der Länge $\leq m$ zur Basis 2.

Bemerkung 10
Wir können jede natürliche (und dann auch jede ganze) Zahl n also eindeutig schreiben als Linearkombination endlich vieler Potenzen von g.

Beispiel 11

$$\begin{aligned} 163_{(10)} &= 1 \cdot 10^2 + 6 \cdot 10^1 + 3 \cdot 10^0 \\ 43_{(10)} &= 1 \cdot 2^5 + 0 \cdot 2^4 + 1 \cdot 2^3 + 0 \cdot 2^2 + 1 \cdot 2^1 + 1 \cdot 2^0 = 101011_{(2)} \\ &= 2 \cdot 16^1 + 11 \cdot 16^0 = 2B_{(16)} \end{aligned}$$

Die bekannten schriftlichen Additions- und Multiplikationsrechnungen, die unter Beachtung von Überträgen ziffernweise geschehen, können in jeder Basis ausgeführt werden. Es gibt weiter für die Multiplikation großer Zahlen (d.h. mit großer Stellenzahl bis etwa $2 \cdot 10^{10}$) schnelle Algorithmen, die wir hier aber nicht näher behandeln möchten; etwa mit der schnellen Fouriertransformation (FFT) nach Schönhage/Strassen[3].
Der Beweis von Satz 8 zeigt, dass die Länge von n gleich $\left\lfloor \frac{\log(n)}{\log(g)} \right\rfloor + 1$ ist, so viele Ziffern müssen zum Hinschreiben bzw. Eintippen von n angegeben werden. Bei verschiedenen Basen ändert sich hier nur der Faktor $\frac{1}{\log(g)}$. Deswegen sagt man, die Länge sei $\mathcal{O}(\log(n))$ und meint damit die Aussage: Es existiert eine Konstante $C > 0$, sodass $k + 1 \leq C \cdot \log(n)$. (Landau-Symbolik[4], "Groß-O-Notation")
Entscheidend für das Studium von $\mathbb{Z}$ ist der Grundbegriff der Teilbarkeit.

Definition 12 (Teilbarkeit)
Für $a, b \in \mathbb{Z}$ heißt a **Teiler** von b bzw. a **teilt** b, in Zeichen $a \mid b$, falls ein $c \in \mathbb{Z}$ existiert mit $ac = b$. Ist a kein Teiler von b, schreibt man $a \nmid b$.

Beispiel 13
$3 \mid 12, 4 \mid 0, 0 \mid 0, 7 \nmid 12, 0 \nmid 4$. Es kann 0 nur die 0 teilen.

Definition 14 (Primzahl)
Eine natürliche Zahl $p \in \mathbb{N}$ heißt **Primzahl** bzw. **prim**, wenn sie genau zwei Teiler in $\mathbb{N}$ besitzt (nämlich 1 und p, $1 \neq p$). Eine natürliche Zahl $n > 1$ heißt **zusammengesetzt**, falls n keine Primzahl ist.

Primzahlen sind die "Bausteine" der natürlichen Zahlen:

Satz 15 (Satz von der eindeutigen Primfaktorzerlegung, Hauptsatz der Arithmetik)
Jede natürliche Zahl $n > 1$ besitzt genau eine Darstellung

$$n = p_1^{e_1} \cdot p_r^{e_r} = \prod_{i=1}^{r} p_i^{e_i}$$

mit $r \in \mathbb{N}$, Primzahlen $p_1, \ldots, p_r$ mit $e_1, \ldots, e_r \in \mathbb{N}$ und $p_1 < p_2 < \ldots < p_r$. Diese heißt die **Primfaktorzerlegung** (PFZ) von n.

Bemerkung 16
Lässt man die letzte Bedingung weg, ist die Darstellung eindeutig bis auf die Reihenfolge der Primpotenzen. Die Zahl e_i ist dabei die Vielfachheit (auch **Exponent** genannt), mit der p_i als Faktor in n auftritt, d.h. $p_i^{e_i} \mid n$, aber $p^{e_i+1} \nmid n$. Dafür gibt es das Symbol $p^{e_i} \parallel n$, und die Primfaktorzerlegung lässt sich kompakt auch schreiben als $n = \prod_p p^{e(p)}$, wobei $e(p) := e$ mit $p^e \parallel n$, falls $p \mid n$, und $e(p) := 0$, falls $p \nmid n$. Weiter ist $\omega(n) := r$ die Anzahl der verschiedenen Primteiler von n.

[3] siehe http://de.wikipedia.org/wiki/Sch%C3%B6nhage-Strassen-Algorithmus
[4] siehe http://de.wikipedia.org/wiki/Landau-Symbole

Beweis

Existenz: Ist n prim, ist nichts zu zeigen, und ist n nicht prim, gibt es $k, l \in \mathbb{N} \setminus \{1\}$ mit $n = kl$. Da $\min\{k, l\} > 1$, folgt $\max\{k, l\} < n$. Nach Induktionsvoraussetzung sind also k, l Produkte von Potenzen von Primzahlen, also auch $n = kl$.

Eindeutigkeit: Sei $n > 1$ minimal mit zwei verschiedenen Zerlegungen $n = \prod_{i=1}^{r} p_i^{e_i} = \prod_{i=1}^{s} q_i^{f_i}$, die p_i, q_i prim und angeordnet. Da $p_1 \neq q_i$ für alle i gilt (sonst hätte $\frac{n}{p_1} < n$ zwei verschiedene Zerlegungen), ist $\mathrm{ggT}(p_1, q_i) = 1$, und mit den Zerlegungen folgt $p_1 \mid q_1^{f_1 - 1}$ aus Lemma 21. Die Fortsetzung des Verfahrens zeigt schließlich $p_1 \mid q_s$, was wegen $\mathrm{ggT}(p_1, q_s) = 1$ ein Widerspruch ist. □ (Beachte: Zum Beweis von Lemma 21 wurde nie die Eindeutigkeit der Primfaktorzerlegung benutzt.)

Die Eindeutigkeit der Primfaktorzerlegung zeigt, dass auch diese eine Möglichkeit zur Darstellung natürlicher Zahlen ist. Diese ist jedoch unpraktisch, weil das folgende Problem im Allgemeinen schwer zu lösen ist, worauf einige kryptographische Verfahren (insb. RSA) beruhen.

Definition 17 (Faktorisierungsproblem)
Zu einer natürlichen zusammengesetzten Zahl $n > 1$ bestimme man einen nichttrivialen Teiler t mit $1 < t < n$.

Klar: Ist das Faktorisierungsproblem rechnerisch leicht zu machen, kann auch (durch Iteration) die Primfaktorzerlegung von n leicht bestimmt werden. In der Praxis, wenn n nicht gerade schon von einer speziellen Form ist, können Teiler großer Zahlen n jedoch nur sehr schwer aufgefunden werden.

- Das derzeit schnellste algorithmische Verfahren zur Faktorisierung (auf einem klassischen Computer) ist das **Zahlkörpersieb** mit einer Laufzeit von nur $\mathcal{O}(\exp(C(\log n)^{1/3}(\log\log n)^{2/3}))$, d.h. es handelt sich um so genanntes **subexponential schnelles Verfahren**, weil $(\log n)^B \ll \exp(C(\log n)^{1/3}(\log\log n)^{2/3}) \ll \exp(D \log n) = n^D$.

- Peter Shor[5] entdeckte um 1994, dass das Faktorisierungsproblem auf einem Quantencomputer mit einer Laufzeit von (meist) nur $\mathcal{O}((\log n)^3)$ sehr (d.h. polynomiell) schnell gelöst werden kann, was die Sicherheit gängiger Kryptoverfahren wie RSA untergräbt. Allerdings ist die Konstruktion solcher Quantencomputer (physikalisch) extrem schwierig, diverse Forschergruppen arbeiten daran. Am 2.1.2014 meldete die Washington Post unter Berufung auf Dokumente von Edward Snowden[6], dass die NSA an der Entwicklung eines kryptographisch mützlichen Quantencomputers arbeitet[7]. Zum Begriff Quantencomputer siehe Wikipedia.

Im Folgenden besprechen wir noch den ggT zweier natürlicher Zahlen, der sich in vielerlei Hinsicht als wichtig und nützlich erweist:

Definition 18
Seien $a, b \in \mathbb{Z}$. Der **größte gemeinsame Teiler** (ggT) von a und b in $\mathbb{N}$ ist die Zahl $d := \max\{t \in \mathbb{N} : t \mid a \wedge t \mid b\}$. Notation: $\mathrm{ggT}(a, b) := d$. Ist $\mathrm{ggT}(a, b) = 1$, heißen a und b **teilerfremd**.

Haben wir für a und b die Primfaktorzerlegungen $a = \prod_p p^{e(p)}$ und $b = \prod_p p^{f(p)}$ vorliegen, kann ihr ggT leicht bestimmt werden als $\mathrm{ggT}(a, b) = \prod_p p^{\min(e(p), f(p))}$, z.B. $\mathrm{ggT}(2^3 \cdot 3^6 \cdot 5^4, 2^4 \cdot 3^5) = 2^3 \cdot 3^5$. Wegen des Faktorisierungsproblems kann dies aber so nicht praktisch umgesetzt werden. Stattdessen benutzt man den (polynomiell) schnellen euklidischen Algorithmus, vgl. Übungsaufgabe.

[5] http://de.wikipedia.org/wiki/Peter_Shor
[6] http://de.wikipedia.org/wiki/Edward_Snowden
[7] Link zum Artikel

Satz 19 (Teilen mit Rest)
Zu $a \in \mathbb{Z}, b \in \mathbb{N}$ existieren eindeutigen $q, r \in \mathbb{Z}, 0 \leq r < b$ mit $a = qb + r$, nämlich $q = \left\lfloor \frac{a}{b} \right\rfloor = \max\{m \in \mathbb{Z} : m \leq \frac{a}{b}\}$ und $r = a - qb$. Dabei heißt r der **kleinste nichtnegative Rest**. Statt $0 \leq r < b$ kann auch $r \in \mathbb{Z}$, $|r| < \frac{b}{2}$, erfüllt werden; r heißt dann der **absolut kleinste Rest** (bei Division durch b).

Satz 20 (Euklidischer Algorithmus)
Seien $a, b \in \mathbb{N}$. Durch fortgesetztes Teilen mit Rest erhalten wir als letzten Rest $\neq 0$ den $\mathrm{ggT}(a, b)$, sowie $x, y \in \mathbb{Z}$ mit $\mathrm{ggT}(a, b) = xa + yb$ (siehe Schema).

Beschreibung des Rechenverfahrens
Rechnen sukzessive mit $r_{-1} := a, r_0 := b$:

$$\begin{aligned} r_{-1} &= q_0 r_0 + r_1 \\ r_0 &= q_1 r_1 + r_2 \\ r_1 &= q_2 r_2 + r_3 \\ &\vdots \end{aligned}$$

Das Verfahren wird fortgeführt, bis erstmals ein Rest $r_{m+1} = 0$ auftritt, was wegen $r_0 > r_1 > r_2 > \ldots$ nach höchstens $b + 1$ vielen Schritten der Fall sein wird. Sind die Quotienten $q_0, \ldots, q_m$ bekannt, können mit den Rekursionen

$$c_{-2} = 0, c_{-1} = 1 \text{ und } c_k = q_k c_{k-1} + c_{k-2}, k = 0, 1, 2, \ldots, n$$
$$d_{-2} = 1, d_{-1} = 0 \text{ und } d_k = q_k d_{k-1} + d_{k-2}, k = 0, 1, 2, \ldots, n$$

die **Bézout-Elemente** als $x = (-1)^{n-1}, y = (-1)^n c_{n-1}$ berechnet werden.
Wir behaupten also:

(1) Es ist $\mathrm{ggT}(a, b) = r_n$.

(2) $\mathrm{ggT}(a, b) = \underbrace{(-1)^{n-1} d_{n-1}}_{x} a + \underbrace{(-1)^n c_{n-1}}_{y} b$

Beweis
zu (1) : Da $r_n \mid r_{n-1}, r_n \mid r_{n-2}, \ldots, r_n \mid r_0 = b, r_n \mid r_{-1} = a$, ist r_n ein Teiler von a und b (Teilen mit Rest von unten nach oben). Ist d irgendein Teiler ≥ 1 von a und b, folgt $d \mid r_1 = a - q_0 b \Rightarrow d \mid r_2 = r_0 - q_1 r_1 \Rightarrow d \mid r_3 = \ldots$, also auch r_n, sodass $d \leq r_n$ folgt (Teilen mit Rest von oben nach unten). Somit ist $r_n = \mathrm{ggT}(a, b)$.

zu (2) : Induktiv kann $c_{k-1} d_k - c_k d_{k-1} = (-1)^k$ gezeigt werden. Daher genügt zu zeigen: $c_n = \frac{a}{\mathrm{ggT}(a,b)}, d_n = \frac{b}{\mathrm{ggT}(a,b)}$.
Mit den $\frac{c_k}{d_k}$ wird die Kettenbruchentwicklung von $\frac{a}{b}$ berechnet und diese bricht bei $\frac{c_n}{d_n} = \frac{a}{b}$ ab. Da bei der Kettenbruchentwicklung alle Brüche $\frac{c_k}{d_k}$ gekürzt sind wegen $c_{k-1} d_k - c_k d_{k-1} = (-1)^k$, folgt dies.

Details siehe EZT-Skript Lorenz

Der Satz vom Euklidischen Algorithmus sichert uns konstruktiv also die Existenz ganzer Zahlen $x, y \in \mathbb{Z}$ mit $\mathrm{ggT}(a, b) = xa + yb$. Die Zahlen x und y heißen auch **Bézout-Elemente** von a und b. Deren Existenz ist auch in der Theorie immer wieder wichtig, z.B. hierfür:

Lemma 21
Seien $a, b, c \in \mathbb{Z}$ und $b, c \neq 0$. Gilt $c \mid ab$ und $\mathrm{ggT}(b, c) = 1$, dann ist $c \mid a$.

Beweis
Aus den Voraussetzungen und $c \mid ac$ folgt, dass $c \mid \mathrm{ggT}(ab, ac) = |a| \cdot \mathrm{ggT}(b, c) = |a|$, also $c \mid a$. Zur ersten Gleichheit: Nach Satz 20 existieren $x, y \in \mathbb{Z}$ mit $\mathrm{ggT}(b, c) = xb + yc$.

$|a| \cdot \mathrm{ggT}(b, c)$ teilt $|a| \cdot b$ und $|a| \cdot c$, also auch ba und ca, d.h. die rechte Seite ist ein gemeinsamer Teiler von ba und ca. Ist t irgendein solcher, so teilt t auch $\mathrm{sgn}(a) \cdot (xba + yca) = xb \cdot |a| + yc \cdot |a| = |a| \cdot (xb + yc) = |a| \,\mathrm{ggT}(b, c)$.
□

Index

absolut kleinster Rest, 11

Bézout-Elemente, 11

Caesar-Code, 4

Divison mit Rest, 11

ECC-Verfahren, 5
Einheit, 7
Einwegfunktion, 5
Endziffer, 8
Euklidischer Algorithmus, 11
Exponent, 9

g-adische Darstellung, 8
Gruppe, 7
    abelsch, 7
größter gemeinsamer Teiler, 10

Halbgruppe, 7

kleinster nichtnegativer Rest, 11
Körper, 7

Leitziffer, 8

n-Bit-Zahl, 8

Primfaktorzerlegung, 9
Primzahl, 9

Ring, 7
RSA-Verfahren, 5

Stellenzahl, 8

Teiler, 9
teilerfremd, 10

Zahlkörpersieb, 10
zusammengesetzt, 9

Liste der Sätze und Definitionen

Satz 8		8
Satz 15	Satz von der eindeutigen Primfaktorzerlegung, Hauptsatz der Arithmetik	9
Satz 19	Teilen mit Rest	10
Satz 20	Euklidischer Algorithmus	11