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: 20. 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

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.

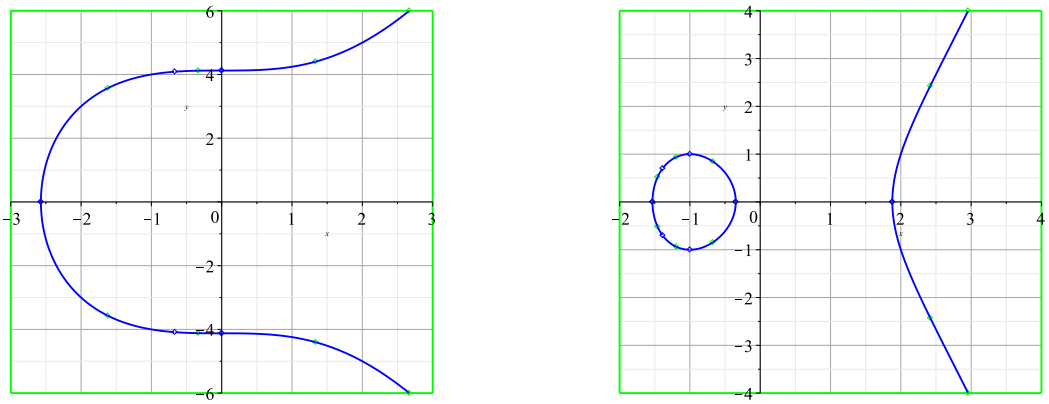

Abbildung 1: Die Kurven E_1 (links) und E_2 (rechts).

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.

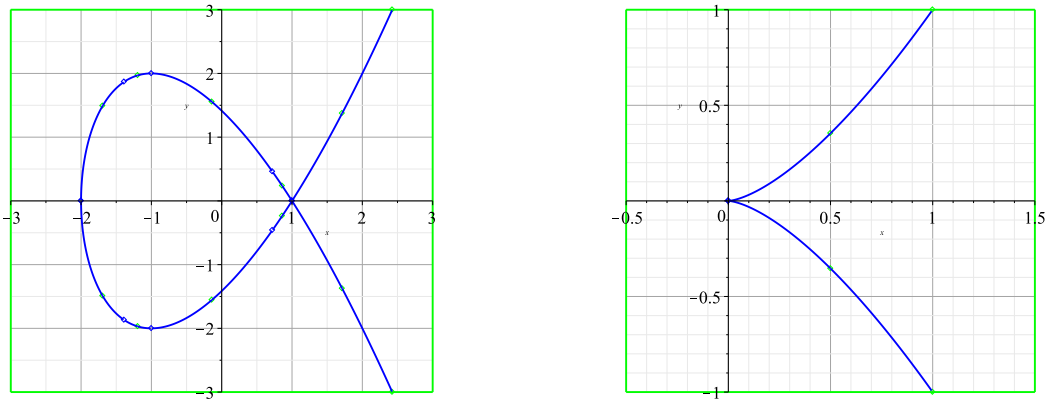

Abbildung 2: Die Kurven C_1 (links) und C_2 (rechts). C_1 ist nicht glatt im Punkt $(1, 1)$, C_2 nicht im Punkt $(0, 0)$.

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 1.1.1.1 (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 1.1.1.2 (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 1.1.1.3 (abelsche Gruppe)
Eine Gruppe $(G, *, e)$ heißt **abelsch** bzw. **kommutativ**, falls für alle $a, b \in G$ gilt: $a * b = b * a$.

Definition 1.1.1.4 (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 1.1.1.5
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 1.1.1.6 (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 1.1.1.7 (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 1.1.1.8

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 1.1.1.9 (g-adische Darstellung)

Die Ziffernfolge $c_k, c_{k-1}, \ldots c_0$ aus Satz 1.1.1.8 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 1.1.1.10

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

Beispiel 1.1.1.11

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

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 1.1.1.8 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 1.1.1.12 (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 1.1.1.13
$3 \mid 12$, $4 \mid 0$, $0 \mid 0$, $7 \nmid 12$, $0 \nmid 4$. Es kann 0 nur die 0 teilen.

Definition 1.1.1.14 (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 1.1.1.15 (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 1.1.1.16
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 1.1.1.21. 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 1.1.1.21 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 1.1.1.17 (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 1.1.1.18
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 1.1.1.19 (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 1.1.1.20 (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 1.1.1.21
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 1.1.1.20 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 $\mathrm{sgn}(a) \cdot (xba + yca) = xb \cdot |a| + yc \cdot |a| = |a| \cdot (xb + yc) = |a| \,\mathrm{ggT}(b,c)$. □

1.1.2 Kongruenzenrechnen und die modulare Brille

Wir behandeln nun, wie man mit Teilmengen von $\mathbb{Z}$ und neuen Definitionen von "$+$" und "$\cdot$" zu neuen algebraischen Strukturen (Gruppe, Ringe, Körper) kommt. Dazu ist das Kongruenzenrechnen modulo m wesentlich.

Definition 1.1.2.1 (Kongruenz, Modul)
Sei $m \in \mathbb{N}$. Dann heißen $a \in \mathbb{Z}$ und $b \in \mathbb{Z}$ **kongruent modulo** m, wenn $m \mid (b-a)$. Wir schreiben dann $a \equiv b \bmod m$ oder $a \equiv b\ (m)$. Die Zahl m heißt der **Modul** der Kongruenz.

Folgerung 1.1.2.2

(1) $a \equiv b \bmod m$ bedeutet, dass a und b bei Division durch m denselben kleinsten nichtnegativen (absolut kleinsten) Rest lassen.

(2) $a \equiv b \bmod m, b \equiv c \bmod m \Rightarrow a \equiv c \bmod m$

(3) $a_1 \equiv b_1 \bmod m, a_2 \equiv b_2 \bmod m \Rightarrow a_1 + a_2 \equiv b_1 + b_2 \bmod m, a_1 \cdot a_2 \equiv b_1 \cdot b_2 \bmod m$.

(4) $ca \equiv cb \bmod m \Rightarrow a \equiv b \bmod \left(\frac{m}{\mathrm{ggT}(c,m)}\right)$, insbesondere $a \equiv b \bmod m$, falls $\mathrm{ggT}(c,m) = 1$.

(5) $a \equiv b \bmod m_i$ für $i = 1, \ldots, k \Rightarrow a \equiv b \bmod \mathrm{kgV}(m_1, \ldots, m_k)$

Dies zeigt, dass $\equiv$ für festes m eine Äquivalenzrelation ist und $\mathbb{Z}$ in m paarweise disjunkte Äquivalenzklassen zerlegt.

Definition 1.1.2.3 (Restklasse)
Die Äquivalenzklassen von $\equiv$ modulo m heißen **Restklassen** modulo m. (auch: Kongruenzklassen modulo m).

Folgerung 1.1.2.4
Die Restklassen modulo m sind Teilmengen von $\mathbb{Z}$ der Gestalt $x + m\mathbb{Z} := \{x + ma : a \in \mathbb{Z}\}$. Die Restklasse $x + m\mathbb{Z}$ heißt auch die Restklasse von x modulo m. Davon gibt es m Stück; wird in jeder Restklasse ein Element x_i, $i = 1, \ldots, m$ ausgewählt, können die m Restklassen mit $x_1 + m\mathbb{Z}, x_2 + m\mathbb{Z}, \ldots, x_m + m\mathbb{Z}$ angegeben werden; die Menge $\{x_1, \ldots, x_m\}$ heißt dann **vollständiges Restsystem** modulo m. Sind $y_1, \ldots, y_m \in \mathbb{Z}$ so, dass $y_i \not\equiv y_j \bmod m$ für alle $i \neq j$, $1 \leq i, j \leq m$, gilt (d.h. die y_i sind paarweise inkongruent modulo m), dann ist $\{y_1, \ldots, y_m\}$ ein vollständiges Restsystem modulo m. Die Zahl x heißt **Repräsentant** der Restklasse $x + m\mathbb{Z}$, und $x + m\mathbb{Z} = z + m\mathbb{Z} \Leftrightarrow x \equiv z \bmod m$, weil laut Definition in der Restklasse von $x \mod m$ genau alle zu x kongruenten Zahlen liegen.

Beispiel 1.1.2.5
$\{0, 1, 2\}$ ist vollständiges Restsystem modulo 3, und vollständige Restsysteme modulo 8 sind etwa $\{1, \ldots, 8\}$ und $\{3, 6, 9, 12, 15, 18, 21, 24\} = \{3a : 1 \leq a \leq 8\}$, da $12 \equiv 4 \bmod 8, 15 \equiv 7 \bmod 8, 18 \equiv 2 \bmod 8, 21 \equiv 5 \bmod 8, 24 \equiv 0 \bmod 8$. Die Menge $\{2a : 1 \leq a \leq 8\}$ ist kein vollständiges Restsystem modulo 8. Die Reste $0, 1, \ldots, m-1$ könnte man auch als "Standardrepräsentanten" modulo m bezeichnen, da sie immer ein vollständiges Restsystem modulo m bilden.

Folgerung 1.1.2.6
Ist $\{x_1, \ldots, x_m\}$ ein vollständiges Restsystem modulo m und $a \in \mathbb{Z}, c \in \mathbb{Z}$ mit $\mathrm{ggT}(c,m) = 1$, so sind auch $\{x_1 + a, x_m + a\}$ und $\{x_1 \cdot c, \ldots, x_m \cdot c\}$ vollständige Restsysteme modulo m (vgl. (4) aus Folgerung 1.1.2.2).

Das nützliche an den Restklassen modulo m ist, dass wir nun durch folgende naheliegende Definitionen von $\oplus$ und $\odot$ mit ihnen neue algebraische Strukturen gewinnen können:

Definition 1.1.2.7 (Addition und Multiplikation auf $\mathbb{Z}_m$)
Ist der Modul m klar, schreiben wir auch $\underline{x} := x + m\mathbb{Z}$ für die Restklasse von x modulo m. Wir definieren für $x, y \in \mathbb{Z}$ dann

$$\underline{x} \oplus \underline{y} := \underline{x + y}$$
$$\underline{x} \odot \underline{y} := \underline{x \cdot y}$$

Weiter sei $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}/m := \{x + m\mathbb{Z} : x \in \mathbb{Z}\}$ die Menge der m vielen Restklassen modulo m.

Folgerung 1.1.2.8
Wir addieren bzw. multiplizieren zwei Restklassen, indem wir Repräsentanten x, y auswählen und diese addieren bzw. multiplizieren. Das ist nur sinnvoll, wenn bei unterschiedlicher Repräsentantenwahl dieselbe Restklasse als Ergebnis herauskommt. Man sagt, die Definition von $\oplus$ und $\odot$ ist wohldefiniert, da repräsentantenunabhängig. Dies ist klar: $\underline{x_1} = \underline{x_2}$ und $\underline{y_1} = \underline{y_2} \Rightarrow x_1 \equiv x_2 \bmod m$ und $y_1 \equiv y_2 \bmod m \Rightarrow x_1 + y_1 \equiv x_2 + y_2 \bmod m \Rightarrow \underline{x_1 + y_1} = \underline{x_2 + y_2}$, also erhalten wir so dieselbe Restklasse für $\underline{x_1} \oplus \underline{y_1}$ und $\underline{x_2} \oplus \underline{y_2}$, wenn $\underline{x_1} = \underline{x_2}$ und $\underline{y_1} = \underline{y_2}$ (analog für die Multiplikation). Damit kann $(\mathbb{Z}_m, \oplus)$ oder $(\mathbb{Z}/m, \odot)$ auf algebraische Strukturen hin untersucht werden. Wir schreiben ab jetzt auch $+$ für $\oplus$ und $\cdot$ für $\odot$.

Folgerung 1.1.2.9
$(\mathbb{Z}_m, +)$ ist eine abelsche Gruppe mit neutralem Element $\underline{0} = 0 + m\mathbb{Z}$, denn Kommutativität und Assoziativität gelten wie in $\mathbb{Z}$, und $\underline{0} + \underline{x} = \underline{0 + x} = \underline{x}$ gilt für alle $x \in \mathbb{Z}$, sowie $\underline{x} + \underline{-x} = \underline{x - x} = \underline{0}$, sodass $-\underline{x} = \underline{-x} = \underline{m - x}$ für alle $x \in \mathbb{Z}$ gilt. Ebenso gilt, dass $(\mathbb{Z}_m, +, \cdot)$ ein kommutativer Ring mit 1 ist.

Das Beispiel $\underline{2} \cdot \underline{0} = \underline{0}, \underline{2} \cdot \underline{1} = \underline{2}, \underline{2} \cdot \underline{2} = \underline{0}$ modulo 4 zeigt, dass es Restklassen ohne Inversen bezüglich $\cdot$ geben kann. Der folgende Satz gibt an, welche Restklassen invertierbar sind, d.h. im Ring $\mathbb{Z}_m$ eine Einheit sind:

Satz 1.1.2.10 (Einheiten in $\mathbb{Z}_m$)
Zu $\underline{x} \in \mathbb{Z}_m$ existiert genau dann ein multiplikatives Inverses, d.h. ein $\underline{y} \in \mathbb{Z}_m$ mit $\underline{x} \cdot \underline{y} = \underline{1} \Leftrightarrow x \cdot y \equiv 1 \bmod m$, falls $\mathrm{ggT}(x, m) = 1$. Wir schreiben dann $\underline{x}^{-1}$ oder $\underline{x}^*$ für $\underline{y}$, die Bezeichnungen $\frac{1}{\underline{x}}$ oder $1/\underline{x}$ sind didaktisch ungeschickt.

Beweis
"⇒": Sei $\underline{y} \in \mathbb{Z}_m$ mit $\underline{x} \cdot \underline{y} = 1$, d.h. $xy \equiv 1 \bmod m$, also existiert $k \in \mathbb{Z}$ mit $1 - xy = km \Rightarrow xy + km = 1$. Wäre $d = \mathrm{ggT}(x, m) > 1$, so folgt $d \mid xy + km = 1 \lightning$.

"⇐": Sei $\mathrm{ggT}(x, m) = 1$. Nach Satz 1.1.1.20 existiert $y, k \in \mathbb{Z}$ mit $1 = yx + km$, also folgt $\underline{x} \cdot \underline{y} = 1$. □

Fazit: Mit dem euklidischen Algorithmus können wir also Inverse schnell explizit berechnen.

Definition 1.1.2.11 (Prime Reste, Eulersche φ-Funktion)
$\underline{x} = x + m\mathbb{Z}$ heißt **prime** oder **reduzierte Restklasse** modulo m, falls $\mathrm{ggT}(x, m) = 1$ gilt. Diese sind genau die Einheiten in $(\mathbb{Z}_m, +, \cdot)$, d.h.

$$\mathbb{Z}_m^* = \{\underline{x} \in \mathbb{Z}_m : \mathrm{ggT}(x, m) = 1\}$$

Die Anzahl der Einheiten sei $\varphi(m) := \#\mathbb{Z}_m^* = \#\{a \in \mathbb{N} : a \leq m, \mathrm{ggT}(a, m) = 1\}$, die so erklärte Funktion $\varphi \colon \mathbb{N} \to \mathbb{N}$ heißt **Eulersche φ-Funktion**. Jedes Repräsentantensystem $\{x_1, \ldots, x_{\varphi(m)}\}$ von $\mathbb{Z}_m^*$ heißt **reduziertes** oder **primes Restsystem** modulo m.´

Satz 1.1.2.12 (Multiplikativität von φ)
Es ist $\varphi(p^k) = p^k - p^{k-1}$ für alle p prim, alle $k \in \mathbb{N}$, und $\varphi(mn) = \varphi(m) \cdot \varphi(n)$, falls $\mathrm{ggT}(m, n) = 1$.

Beweis
Unter den Zahlen $1, 2, \ldots, p^k$ sind genau die Vielfachen von p zu p^k nicht teilerfremd, d.h. $p, 2p, \ldots, p^{k-1} \cdot p$, was p^{k-1}-viele Zahlen sind. Zur Multiplikativität siehe Zusatz 1.1.2.18.
Ist $n = \prod_{p|n} p^{e(p)}$ die Primfaktorzerlegung von n, folgt aus Satz 1.1.2.12:

$$\varphi(n) = \prod_{p|n} \left(p^{e(p)} - p^{e(p)-1} \right) = \prod_{p|n} p^{e(p)} \cdot \left(1 - \frac{1}{p}\right) = n \cdot \prod_{p|n} \left(1 - \frac{1}{p}\right)$$

Folgerung 1.1.2.13
$(\mathbb{Z}_m^*, \cdot)$ ist eine Gruppe, die multiplikative Gruppe von $\mathbb{Z}_m$, und die Gruppe $(\mathbb{Z}_m, +)$ heißt additive Gruppe von $\mathbb{Z}_m$. Im Fall $\mathbb{Z}_m^* = \mathbb{Z}_m \setminus \{0\}$ ist $(\mathbb{Z}_m, +, \cdot)$ ein Körper; dies ist genau dann richtig, wenn $m = p$ Primzahl ist, weil genau dann alle $1, 2, \ldots, m-1$ zu m teilerfremd sind. Wir bezeichnen für p prim diesen Körper mit p Elementen mit $\mathbb{F}_p$. Der Körper $\mathbb{F}_p$ hat die Eigenschaft, dass $p \cdot a := \sum_{i=1}^{p} a = 0$ in $\mathbb{F}_p$ für alle $a \in \mathbb{F}_p$ gilt. Wir sagen, er hat die Charakteristik p.

Weitere endliche Körper später

Definition 1.1.2.14 (Charakteristik)
Sei k ein Körper. Er hat die **Charakteristik** 0, falls für alle $m \in \mathbb{N}$ gilt: $m \cdot 1 := \underbrace{1 + \ldots + 1}_{m\text{-mal}} \neq 0$.
Falls es ein $m \in \mathbb{N}$ mit $m \cdot 1 = 0$ gibt, so heißt das kleinste solche $m \in \mathbb{N}$ die Charakteristik von k. Wir schreiben kurz $\mathrm{char}(k) = 0$ bzw. $\mathrm{char}(k) = m$.
Zum Beispiel ist $\mathrm{char}(\mathbb{Q}) = \mathrm{char}(\mathbb{R}) = \mathrm{char}(\mathbb{C}) = 0$ und $\mathrm{char}(\mathbb{F}_p) = p$.

Bemerkung
Die Charakteristik eines Körpers k ist entweder 0 oder eine Primzahl, denn sonst wäre $0 = (m \cdot n) \cdot 1 = m \cdot (n \cdot 1) = (m \cdot 1) \cdot (n \cdot 1) \Rightarrow m \cdot 1 = 0$ oder $n \cdot 1 = 0$, da $k^* = k \setminus \{0\}$. Widerspruch zu $m \cdot n$ minimal.
Die Struktur der Zahlringe $(\mathbb{Z}_m, +, \cdot)$ versteht man besser, indem man sie auf "kleinere" Zahlringe zurückführt:

Satz 1.1.2.15 (Chinesischer Restsatz für Zahlringe)
Sei $m > 1$ eine natürliche Zahl und $m = m_1 \cdot m_2 \cdot \ldots \cdot m_r$ eine Zerlegung von m in paarweise teilerfremde Zahlen $m_i > 1$. Dann ist die Abbildung

$$\begin{aligned} F \colon \mathbb{Z}/m\mathbb{Z} &\longrightarrow (\mathbb{Z}/m_1\mathbb{Z}) \times \ldots \times (\mathbb{Z}/m_r\mathbb{Z}) \\ x + m\mathbb{Z} &\longmapsto (x + m_1\mathbb{Z}, \ldots x + m_r\mathbb{Z}) \end{aligned}$$

ein Isomorphismus von Ringen.

Satz 1.1.2.16 (Chinesischer Restsatz für simultane Kongruenzen)
Seien $m_1, \ldots, m_r > 1$ paarweise teilerfremde Zahlen und sei $a_1, \ldots, a_r \in \mathbb{Z}$. Dann ist das simultane Kongruenzensystem

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ &\vdots \\ x &\equiv a_r \bmod m_r \end{aligned}$$

in x lösbar, die Lösungen sind alle kongruent modulo $m_1 \cdots m_r$.

Bemerkung
Satz 1.1.2.16 folgt aus 1.1.2.15 wegen der Bijektivität von F, denn $(a_1 + m_1\mathbb{Z}, \ldots, a_r + m_r\mathbb{Z})$ hat dann genau ein Urbild $x + m\mathbb{Z}$.

Zusatz 1.1.2.17 (zu Satz 1.1.2.16)
Genau alle $x \equiv x_0 \bmod m_1 \cdots m_r$ lösen das oben angegebene System, wobei $x_0 = a_1 M_1^* M_1 + \ldots + a_r M_r^* M_r$ mit $M_i := \frac{m_1 \cdots m_r}{m_i}$ und $M_i^* \in \mathbb{Z}$ ein multiplikatives Inverses von $M_i \mod m_i$ repräsentiert, d.h. es gilt $M_i^* \cdot M_i \equiv 1 \bmod m_i$, wobei die M_i^* mit dem euklidischen Algorithmus (schnell) berechnet werden können.

Zusatz 1.1.2.18 (zu Satz 1.1.2.15)
Die Gruppe $\mathbb{Z}_m^*$ ist isomorph zu $\mathbb{Z}_{m_1}^* \times \ldots \times \mathbb{Z}_{m_r}^*$, beide Gruppen haben dann gleich viele Elemente, es folgt

$$\varphi(m) = \varphi(m_1) \cdot \varphi(m_2) \cdots \varphi(m_r),$$

d.h. die Multiplikativität von φ ist ein Korollar des chinesischen Restsatzes.

Beweis von Satz 1.1.2.16
Existenz: Ist $x \equiv x_0 \bmod m_1 \cdots m_r$, wie in Zusatz 1.1.2.17 angegeben, so folgt für alle $1 \leq i \leq r$:

$$x \equiv x_0 = \underbrace{a_1 M_1^* M_1}_{\equiv 0 \bmod m_i} + \ldots + \underbrace{a_i M_i^* M_i}_{\equiv a_i \cdot 1 \bmod m_i} + \ldots + \underbrace{a_r M_r^* M_r}_{\equiv 0 \bmod m_i} \equiv a_i \bmod m_i$$

Eindeutigkeit modulo $m_1 \cdots m_r$: Ist $y \in \mathbb{Z}$ eine weitere Lösung des Kongruenzensystems, so gilt für alle $j \neq i$: $y \equiv a_j \bmod m_j$, also $\underbrace{M_j^* \cdot M_j}_{\equiv 1 \bmod m_j} \cdot y \equiv a_j \bmod m_j$ und $M_i M_i^* a_i \equiv 0 \bmod m_j$ (Division durch m_j), und somit

$$y \equiv a_j \bmod m_j \equiv \sum_{j=1}^{k} M_j M_j^* a_j \bmod m_j \equiv x_0 \bmod m_j \text{ für alle } j = 1, \ldots, r.$$

Damit folgt, dass m_j Teiler von $y - x_0$ ist. Da die $m_1, \ldots, m_r$ alle paarweise teilerfremd sind, folgt daraus $y \equiv x_0 \bmod m_1 \cdots m_r$, vgl. 1.1.2.2 (5). □

Beispiel zum chinesischen Restsatz
Das System

$$x \equiv 2 \bmod 7$$
$$x \equiv 3 \bmod 8$$

hat die Lösung $x \equiv 2 \cdot 1 \cdot 8 + 3 \cdot (-1) \cdot 7 = -5 \equiv 51 \bmod 56$, denn $1 \equiv 8^{-1} \bmod 7$ und $-1 \equiv 7^{-1} \bmod 8$.
Beispiel-Textaufgabe dazu: Gegeben seien zwei Tüten mit gleich vielen Bonbons. Beim gleichmäßigen Aufteilen der einen Tüte an sieben Kinder bleiben zwei Bonbons übrig. Beim Aufteilen der anderen auf acht Kinder bleiben drei Bonbons übrig. Wie viele Bonbons waren in einer Tüte?
Lösung: Möglich sind 51, 107, 163, …Stück.

Beispiele zum Rechnen mit Kongruenzen

- Es ist $5x \equiv 4 \bmod 12 \Leftrightarrow 5^{-1} \cdot 5x \equiv 4 \cdot 5^{-1} \bmod 12 \Leftrightarrow x \equiv 4 \cdot 5^{-1} \equiv 4 \cdot 5 = 20 \equiv 8 \bmod 12$.
  Analog rechnet man in der Restklasse modulo 12:
  $5x \cdot 4 \Leftrightarrow x = 5^{-1} \cdot 4 = 4 \cdot 5 = 20 = 8$.

- Es ist

$$\begin{aligned} & 8x^2 - 2x + 3 \equiv -1 \bmod 7 \\ \Leftrightarrow \quad & (x-1)^2 - 2 + 3 \equiv -1 \bmod 7 \\ \Leftrightarrow \quad & (x-1)^2 \equiv -2 \equiv 5 \bmod 7 \end{aligned}$$

man spricht auch von quadratischen Resten modulo 7

Da nun wegen $0^2 \equiv 0 \bmod 7, 1^2 \equiv 1 \bmod 7, 2^2 \equiv 4 \bmod 7, 3^2 \equiv 2 \bmod 7$ die Zahl 5 kein Quadrat modulo 7 ist, hat die Kongruenz keine Lösung.
Die Kongruenz $(x-1)^2 \equiv 4 \bmod 7$ hat die beiden Lösungen $x \equiv 3 \bmod 7$ und $x \equiv -1 \bmod 7$.

- Die Kongruenz $(x-3) \cdot 4 \equiv 1 \bmod 33$ ist schreibbar als System:

$$(x-3) \cdot 4 \equiv 1 \bmod 3$$
$$(x-3) \cdot 4 \equiv 1 \bmod 11$$

Die beiden einzelnen Kongruenzen haben die Lösungen $x \equiv 1 \bmod 3$ sowie $x \equiv 6 \bmod 11$. Mittels chinesischem Restsatz erhält man eine Lösung der Ausgangskongruenz modulo 33:
$x \equiv 1 \cdot 2 \cdot 11 + 6 \cdot 4 \cdot 3 = 22 + 6 \cdot 12 = 94 \equiv -5 \equiv 28 \bmod 33$

- Bei manchen zahlentheoretischen Aufgaben, wie z.B. die Frage, ob es ganzzahlige Lösungen zu bestimmten Gleichungen geben kann, ist die "modulare Brille" ein nützliches Hilfsmittel. Hier ein Beispiel, wo wir die modulare Brille modulo 8 aufsetzen, um mehr zu sehen:
Betrachte die Gleichung $8x + 7 = u^2 + v^2 + w^2$ in $u, v, w, x \in \mathbb{N}_0$. Sie ist unlösbar, denn modulo 8 erhalten wir $7 \equiv u^2 + v^2 + w^2 \bmod 8$. Alle quadratischen Reste modulo 8 sind $0, 1$ und 4:

z	0	± 1	± 2	± 3	4
z^2	0	1	4	1	0

Daher ist $v^2 + w^2 \equiv 0, 1, 4, 2, 5 \bmod 8$, also $u^2 + v^2 + w^2 \equiv 0, 1, 4, 2, 5, \quad 1, 2, 5, 3, 6, \quad 4, 5, 0, 6, 1 \bmod 8$, aber nie $\equiv 7 \bmod 8$. Es kann keine Lösungen modulo 8 geben, also auch keine in $\mathbb{Z}$.

1.1.3 Gruppen

[4] Die Gruppen $(\mathbb{Z}_m, +, 0)$ und $(\mathbb{Z}_m^*, \cdot)$ sind endliche abelsche Gruppen. Wir untersuchen ein paar ihrer allgemeinen Eigenschaften und führen dabei ein paar Grundbegriffe ein.

Definition 1.1.3.1 (Gruppenordnung)
Die **Ordnung** einer endlichen Gruppe G ist die Anzahl ihrer Elemenete, kurz $\mathrm{ord}(G) := \#G$.

Definition 1.1.3.2 (Untergruppe)
Eine Teilmenge H einer Gruppe G mit Verknüpfung $*$ heißt **Untergruppe**, falls auch $(H, *)$ eine Gruppe ist.

Satz 1.1.3.3 (Satz von Lagrange)
Ist $(G, *)$ eine endliche Gruppe, so ist die Ordnung einer Untergruppe H stets ein Teiler von $\mathrm{ord}(G)$.

Beweis
Die **Linksnebenklassen** $a * H := \{a * h : h \in H\}$ für $a \in G$ sind paarweise disjunkt, das heißt es gilt stets $a * H = b * H$ oder $a * H \cap b * H = \emptyset$.
(Denn: ist $c \in a * H \cap b * H$, so ist $c = a * g = b * h$ für $g, h \in H$, also $a = b * (h * g^{-1})$, somit $a * H = \{a * m : m \in H\} = \{b * h * g^{-1} * m : m \in H\} = \{b * n : n \in H\} = b * H$.)
Also ist G die disjunkte Vereinigung endlich vieler Linksnebenklassen $a_1 * H, \ldots, a_r * H$. Da $\#(a * H) = \#H$ für alle $a \in G$ gilt, folgt mit $\mathrm{ord}(G) = r \cdot \mathrm{ord}(H)$ die Behauptung. □

Definition 1.1.3.4 (Erzeugnis, zyklisch)
Sei $(G, +)$ eine abelsche Gruppe und $a \in G$. Für $k \in \mathbb{Z}$ definieren wir $ka := \underbrace{a + \ldots + a}_{k\text{-mal}}$, falls $k > 0$, $k \cdot 0 := 0$

klar! und $k \cdot a := -(-k) \cdot a$, falls $k < 0$. Dann ist $\langle a \rangle := \{ka : k \in \mathbb{Z}\}$ eine Untergruppe von G. Wir nennen $\langle a \rangle$ die

von a **erzeugte Untergruppe** bzw. das **Erzeugnis** von a und a einen **Erzeuger**. Ist $\langle a \rangle$ eine endliche Untergruppe, heißt ihre Ordnung die **Ordnung** von a, kurz $\mathrm{ord}(a) := \#\langle a \rangle$. Eine Gruppe G mit Erzeuger a, das heißt $G = \langle a \rangle$, heißt **zyklisch**.

Schreibt man die Gruppe multiplikativ mit Verknüpfung "$\cdot$", so setzt man $a^k := \underbrace{a \cdots a}_{k\text{-mal}}$, falls $k > 0$, $a^0 := 1$, $a^k := \left(a^{(-k)}\right)^{-1}$, falls $k < 0$, und $\langle a \rangle := \{a^k : k \in \mathbb{Z}\}$. Ansonsten ist bis auf Schreibweise die Begrifflichkeit und Theorie zu Erzeugern und Ordnungen dieselbe.
Nach dem Satz von Lagrange gilt für jede endliche Gruppe G und $a \in G$ stets $\mathrm{ord}(a) \mid \mathrm{ord}(G)$.

Beispiel 1.1.3.5
$\mathbb{Z}/m\mathbb{Z} = \{0, 1, \ldots, m-1\}$ ist "die" zyklische Gruppe mit $\mathrm{ord}(G) = m$. Ist $m = p$ prim, können außer $\{0\}$ und $\mathbb{Z}/p\mathbb{Z}$ keine weiteren Untergruppen existieren.

Lemma 1.1.3.6
Sei $(G, +)$ eine Gruppe, $a \in G$. Es ist $\mathrm{ord}(a)$ die kleinste natürliche Zahl m mit $ma = 0$. Es gilt: $ka = 0 \Leftrightarrow \mathrm{ord}(a) \mid k$.
(Bei multiplikativer Schreibweise: $\mathrm{ord}(a) = \min\{m \in \mathbb{N} : a^m = 1\}$ und $a^k = 1 \Leftrightarrow \mathrm{ord}(a) \mid k$.)

Beweis
Der erste Teil ist klar. Zum zweiten Teil:

"⇒": Falls $k \in \mathbb{N}$ mit $ka = 0$ ist, nehme Division von k durch $\mathrm{ord}(a)$ vor: $k = q \cdot \mathrm{ord}(a) + r$ mit $0 \leq r < \mathrm{ord}(a)$. Wegen $0 = ka = q \cdot \underbrace{\mathrm{ord}(a) \cdot a}_{=0} + ra$ folgt $ra = 0$, wegen der Minimalität von $\mathrm{ord}(a)$ also $r = 0$, also $\mathrm{ord}(a) \mid k$.

"⇐": Für $k = m \cdot \mathrm{ord}(a)$ folgt $ka = m \cdot (\mathrm{ord}(a) \cdot a) = 0$. □

Folgerung 1.1.3.7
$\mathrm{ord}(G) \cdot a = 0$ bzw. multiplikativ: $a^{\mathrm{ord}(G)} = 1$, da $\mathrm{ord}(a) \mid \mathrm{ord}(G)$ nach Lemma 1.1.3.6

Folgerung 1.1.3.8 (Kleiner Satz von Fermat)
Da $\mathrm{ord}((\mathbb{Z}/m\mathbb{Z})^*) = \varphi(m)$, ist $a^{\varphi(m)} \equiv 1 \bmod m$, falls $\mathrm{ggT}(a, m) = 1$. Für p prim: $a^{p-1} \equiv 1 \bmod p$ für $p \nmid a$.

Bemerkung 1.1.3.9 (Satz von Euler-Fermat)
Die Kongruenz $a^{\varphi(m)} \equiv 1 \bmod m$, falls $\mathrm{ggT}(a, m) = 1$, heißt auch **Satz von Euler-Fermat**. Als Ordnung eines $a \in \mathbb{Z}_m^*$ (Notation: $\mathrm{ord}_m(a)$) kommt also nur ein Teiler von $\varphi(m)$ in Frage.

Beispiel 1.1.3.10
Wir haben $\varphi(15) = \varphi(3) \cdot \varphi(5) = 2 \cdot 4 = 8$. Die möglichen Ordnungen von Zahlen $a \mod 15$ mit $\mathrm{ggT}(a, 15) = 1$ sind also $0, 1, 2, 4, 8$.
Wegen $4^2 = 16 \equiv 1 \bmod 15$ ist zum Beispiel $\mathrm{ord}_{15}(4) = 2$. Bei anderen Zahlen muss man unter Umständen Potenzen mit größeren Exponenten ausrechnen, um die Ordnung zu bestimmen.

Generell stellt sich in Anwendungen die Frage, wie man leicht und schnell (modulare) Potenzen $a^k \bmod m$ mit großem k berechnen kann. Der Satz von Euler-Fermat erlaubt bereits eine Reduktion von $k \bmod \varphi(m)$: Ist $k =$

$q \cdot \varphi(m) + r$ mit $0 \leq r < \varphi(m)$, folgt

$$a^k = a^{\varphi(m)\cdot q + r} = \left(a^{\varphi(m)}\right)^q \cdot a^r \equiv 1^q \cdot a^r = a^r \bmod m.$$

Ist aber auch $\varphi(m)$ bzw. r groß, hilft man sich mit folgender Methode des schnellen Potenzierens weiter:

Lemma 1.1.3.11 (Methode des schnellen Potenzierens)
Gegeben sei eine Gruppe $(G, \cdot)$, zu berechnen ist für $r \in \mathbb{N}, a \in G$ die Potenz a^r in der Gruppe G.

1. Schritt: Mit höchstens $d := \left\lfloor \frac{\log r}{\log 2} \right\rfloor$ vielen Verknüpfungen in G berechne durch sukzessives Quadrieren $a^2, \left(a^2\right)^2 = a^4, \ldots, a^{2^d}$.

2. Schritt: Schreibe r als Binärzahl: $r = \sum_{i=0}^{d} c_i \cdot 2^i$ mit $c_i \in \{0, 1\}$.

3. Schritt: Berechne $a^r = a^{c_0} \cdot a^{2c_1} \cdot a^{2^2 c_2} \cdots a^{2^d c_d} = (a^{c_0}) \cdot \left(a^2\right)^{c_1} \cdot \left(a^{2^2}\right)^{c_2} \cdots \left(a^{2^d}\right)^{c_d}$ mit maximal d weiteren Verknüpfungen in G.

Somit reichen höchstens $2d = \mathcal{O}(\log r)$ viele Anwendungen der Gruppenverknüpfung "$\cdot$". Bei additiver Schreibweise einer Gruppe $(G, +)$ geht das Verfahren zur Berechnung von $r \cdot a$ analog. Man nennt es dann auch das **dual and add**-Verfahren.

Beispiel 1.1.3.12
$5^{12} = 5^{2^2+2^3} = 5^{2^2} \cdot 5^{2^3}$. Modulo 11 rechnen wir:

$$5^2 \equiv \bmod 11, 5^{2^2} \equiv 3^2 \equiv -2 \bmod 11, 5^{2^3} \equiv (-2)^2 \equiv 4 \bmod 11,$$

also $5^{12} \equiv (-2) \cdot 4 \equiv 3 \bmod 11$. Das geht schneller als 5^{12} von Hand auszurechnen und durch 11 zu teilen.

Anwendung 1.1.3.13 (Lösen quadratischer Kongruenzen)
Im Fall $p \equiv 3 \bmod 4$ prim können wir Lösungen quadratischer Kongruenzen modulo p bestimmen: Sei $p = 4k + 3$ prim und a mit $p \nmid a$ ein quadratischer Rest modulo p, d.h. es existiert ein $b \in \mathbb{Z}$ mit $a \equiv b^2 \bmod p$, und wir möchten $\pm b \bmod p$ ausrechnen können. Nach dem kleinen Fermat folgt $b^{4k+2} = b^{p-1} \equiv 1 \bmod p$. Es folgt $\left(a^{k+1}\right)^2 \equiv \left(b^2\right)^{2(k+1)} = b^{(4k+2)+2} \equiv 1 \cdot b^2 \equiv a \bmod p$, d.h. die LÖsungen von $b^2 \equiv a \bmod p$ sind $b = \pm a^{k+1} \bmod p$. Da $a^{k+1} \not\equiv -a^{k+1} \bmod p \Leftrightarrow 2a^{k+1} \not\equiv 0 \bmod p$, gibt es genau zwei Lösungen modulo p, die wir etwa im Restsystem $\{0, 1, \ldots, p-1\}$ angeben können und mit $\pm a^{k+1} \bmod p$ berechnen können, zum Beispiel mit dem schnellen Potenzieren.

Anwendung 1.1.3.14
Sei nun n eine zusammengesetze Zahl, etwa $n = pq$ mit $p \equiv q \equiv 3 \bmod 4$ prim, etwa $p = 4k + 3$, $q = 4l + 3$ mit $k, l \in \mathbb{N}_0$, und sei $p \neq q$. Sei $a \bmod n$ ein quadratischer Rest modulo n. Gesucht seien die Lösungen der Kongruenz $a \equiv x^2 \bmod n$. Nach dem chinesischen Restsatz gilt $x^2 \equiv a \bmod n \Leftrightarrow x^2 \equiv a \bmod p$ und $x^2 \equiv a \bmod q$, und die jeweiligen Lösungen $\pm a^{k+1} \bmod p$ und $\pm a^{l+1} \bmod q$ kann man zusammensetzen zu (maximal) vier Lösungen modulo n. Es sind genau vier Lösungen, die explizit wie folgt bestimmt werden können:
Sind $r, s \in \mathbb{Z}$ gegeben mit $rp + sq = 1$, d.h. die Bézout-Elemente von p und q, und ist $\pm b$ Lösung von $x^2 \equiv a \bmod p$ sowie $\pm c$ Lösung von $x^2 \equiv a \bmod q$, so liefert die Formel des chinesischen Restsatzes

$$x = \pm b \cdot s \cdot q \pm c \cdot r \cdot p$$

genau vier Lösungen von $x^2 \equiv a \bmod pq$. Diese müssen paarweise inkongruent modulo pq sein, da wir laut chinesischem Restsatz den Ringisomorphismus $\mathbb{Z}_{pq} \simeq \mathbb{Z}_p \times \mathbb{Z}_q$ haben und die vier verschiedenen Lösungspaare $(b, c), (-b, c), (b, -c), (-b, -c)$ deswegen genau vier Restklassen in $\mathbb{Z}_{pq}$ entsprechen.

Beispiel 1.1.3.15
Betrachte $p = 11$, $q = 19$, d.h. $k = 2, l = 4$. Wähle $a = 47$.
Die Lösungen von $x^2 \equiv 47 \equiv 3 \bmod 11$ sind $\pm 3^3 \equiv \pm 5 \bmod 11$, die Lösungen von $x^2 \equiv 47 \equiv 9 \bmod 19$ sind $\pm 3 \bmod 19$.
Bézout-Elemente bestimmen: Das Inverse von $19 \equiv 8 \bmod 11$ ist 7, das von $11 \bmod 19$ ist 7.
$\Rightarrow s = r = 7$ und $x \equiv \mp 5 \cdot 7 \cdot 19 \pm 3 \cdot 7 \cdot 11 \bmod (11 \cdot 19)$ ergibt $x \in \{\pm 16, \pm 60\}$.
Probe: $16^2 \equiv 47 \bmod (11 \cdot 19), 60^2 \equiv 47 \bmod (11 \cdot 19)$. ✓

Man beachte, dass wir hier benötigen, dass a ein quadratischer Rest modulo 11 und modulo 19 sein muss. Würde man a zufällig wählen, wäre das nicht unbedingt der Fall. Dann ist $x^2 \equiv a \bmod n$ ohnehin unlösbar, falls a kein quadratischer Rest modulo $11 \cdot 19$ ist.

Anwendung 1.1.3.16 (Faires Münzwurfknobeln)
Zwei Spieler, Alice (A) und Bob (B), möchten etwas ausknobeln (zum Beispiel, wer beim Fernschach beginnen soll und dann einen Vorteil hat, etc.), allerdings sprechen sie sich am Telefon oder mailen sich, und können sich daher nicht sehen. A wirft eine Münze, und B denkt vorher ”Kopf” oder ”Zahl”, verrät das aber nicht (Würde A die Wahl von B vorher kennen, so würde B das mitgeteilte Ergebnis des Münzwurfs unter Umständen anzweifeln). A teilt B das Ergebnis mit, und B verkündet, wer gewonnen hat: A, wenn ihr Münzwurfergebnis mit der Wahl von B übereinstimmt, ansonsten gewinnt B. Sei B’s geheime Wahl ”Zahl”.
Teilt A mit, dass sie ”Zahl” geworfen hat, akzeptieren A und B den Spielausgang, weil dann A gewinnt und B ihr dies verkündet. Falls A jedoch mitteilt, dass sie ”Kopf” geworfen hat, teilt B mit, dass A verloren habe, was A natürlich nicht akzeptieren würde.
Problem: Wie kann bei Ergebnis ”Kopf” Spieler B seine Mitspielerin A überzeugen, dass er vor dem Münzwurf die Wahl ”Zahl” getroffen hat?
Unsere Antwort: Wenn B dann eine Zahl $n = pq$ faktorisieren könnte, deren Primteiler p, q ansonsten nur A kennt.

Erläuterung 1.1.3.17
Das Verfahren funktioniert wie folgt:

Schritt 1: A wählt Primzahlen $p, q \equiv 3 \bmod 4$, $p \neq q$, berechnet $n = pq$ und schickt n an B.

Schritt 2: B wählt $1 \leq b \leq n - 1$ zufällig und behält b geheim, er berechnet $a \equiv b^2 \bmod n$ und schickt a an A.

Schritt 3: A berechnet die vier Lösungen von $x^2 \equiv a \bmod n$ (vgl. 1.1.3.14), die vier Lösungen seien $\pm b, \pm c \in \mathbb{Z}$, (mit b von B), die Lösungen $\pm c$ sind andere, die B nicht kennt.

Soweit die Vorbereitung, dann der eigentliche Münzwurf:

Schritt 4: A wählt eine der vier Lösungen zufällig aus (etwa durch Münzwurf!), das heißt entweder $\pm b$ oder $\pm c$, und schickt B das Ergebnis. A kann nicht wissen, dass B die Zahl b gewählt hat. Die Vereinbarung ist nun: Schickt A eine der Zahlen $\pm b$, gewinnt A. Schickt A eine der Zahlen $\pm c$, gewinnt B, und das verkündet B.

Schritt 5: Es erfolgt die Verifikation, dass A wirklich verloren hat im 2. Fall, dazu muss A sich davon überzeugen, dass B vorher wirklich $\pm b$ gewählt hat. Das kann B nun beweisen, indem er ihr die Primfaktoren von n nennt: Er berechnet $b + c \bmod n$ und $d := \mathrm{ggT}(b + c, n)$ mit dem euklidischen Algorithmus. Dann ist $d = p$ oder $d = q$. (Denn aus $b^2 \equiv a \equiv c^2 \bmod pq$ folgt: $pq \mid (b - c)(b + c) = b^2 - c^2$, und da $b \not\equiv c \bmod p, b \not\equiv c \bmod q$ folgt $q \mid b + c$ oder $p \mid b + c$, und $d \neq n$, weil sonst $b \equiv -c \bmod n$ wäre ↯.)
Also kann B, weil er c kennt, die von A gewählten Primfaktoren bestimmen und A mitteilen und auf diese Art A überzeugen. Das konnte B nur, weil er vorher auch wirklich nicht die von A genannte Lösung $\pm b$ hatte. Damit ist das Spiel fair.

In der praktischen Umsetzung wird noch ein Verfahren zur Erzeugung großer, möglichst zufälliger Primzahlen p, q gebraucht. Man kennt in der Praxis schnelle Tests (den Miller-Rabin-Test), um zu entscheiden, ob eine große Zahl n (mit evtl. hunderten von Stellen in Dezimaldarstellung) zusammengesetzt ist oder (sehr wahrscheinlich) prim. Daher erzeugt man solange Zufallszahlen, bis der Primzahltest ”anschlägt”.

Index

Liste der Sätze und Definitionen