Mathematik und Logik

2011W

Institut für Algebra
Johannes Kepler Universität Linz

Vorlesung im 2011W

http://www.algebra.uni-linz.ac.at/Students/Win/ml

Inhalt

Was ist Logik?
Elementare Zahlentheorie
Natürliche Zahlen
Teilbarkeit
Gemeinsame Teiler
Diophantische Gleichungen
Teilerfremde Zahlen
Modulare Arithmetik
Primzahlen
RSA-Verschlüsselung
Logik
Aussagenlogik
Logische Implikation, $\Rightarrow$
Logische Konjunktion, $\wedge$
Logische Äquivalenz, $\Longleftrightarrow$
Logische Disjunktion, $\vee$
Prädikatenlogik
Allquantor, $\forall$
Existenzquantor, $\exists$
Datentypen

Das ist doch logisch!

- Dieser Stein fällt zu Boden.
- Ist das wirklich logisch?
- **N E I N !**
- Um dies zu erkennen, ist ein Experiment notwendig.
- Bedeutung der Begriffe: „Dieser Stein“, „fällt“, „zu Boden“?

Logisches Schließen

- Wir nehmen an:
  - Jeder Körper fällt zu Boden.
  - Dieser Stein ist ein Körper.
- Dann gilt:
- Dieser Stein fällt zu Boden.
- **Das ist LOGISCH.**
- Dafür ist **kein** Experiment notwendig.
- Die Bedeutung der Begriffe „Dieser Stein“, „fällt“, „zu Boden“, „Körper“ ist dabei irrelevant.
- Ebenfalls irrelevant: Wahrheitsgehalt der Annahmen.
- Dieselbe logische Schlußregel kann auf gänzlich andere Situationen angewandt werden, z.B.:
  - Jeder Mensch ist sterblich.
  - Aristoteles ist ein Mensch.
  - Also: Aristoteles ist sterblich.

Definierende Eigenschaften

Definition

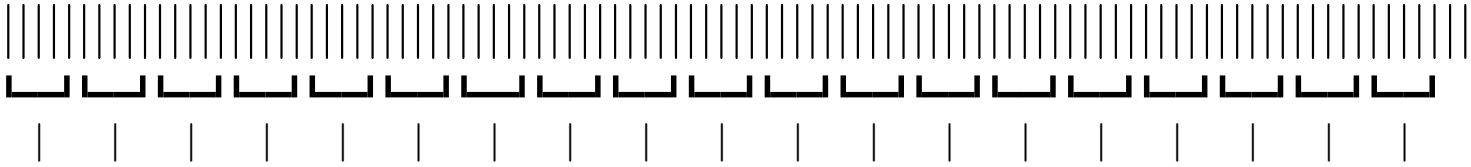
- 0 ist eine natürliche Zahl;
- Zu jeder natürlichen Zahl n gibt es einen Nachfolger Sn;
- Alle natürlichen Zahlen lassen sich auf diese Weise konstruieren
- Zwei natürliche Zahlen sind genau dann gleich, wenn sie gleich konstruiert wurden.

Beispiel

$0, S0, S(S0), S(S(S0)), \ldots, S(S(S(S(S(S(S(S(S(S(S(S(S(S0)))))))))))))$
oder einfacher:
|||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||||

Eukidsche Division

Wir gruppieren:

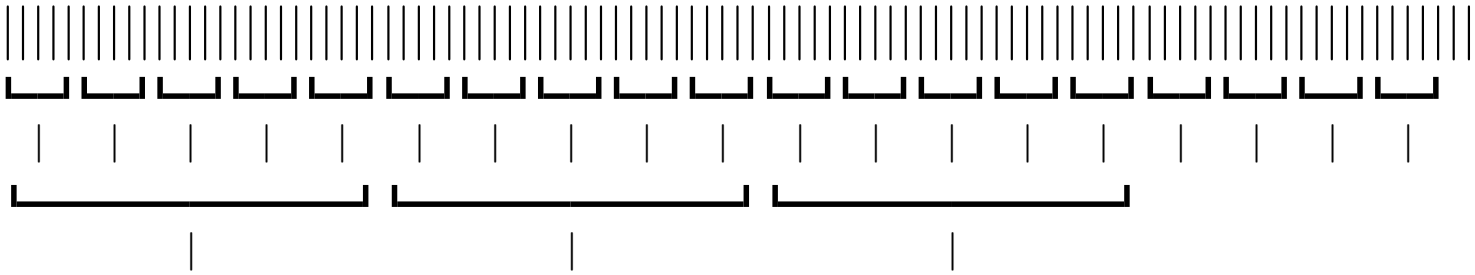


Satz (Euklidische Division)

Seien m und b natürliche Zahlen
und $b \neq 0$.
Dann gibt es eindeutig bestimmte natürliche Zahl q, r, sodaß

$$m = q \cdot b + r \quad \textit{und} \quad r < b.$$

Diese Idee läßt sich wiederholen:



$= 3 \cdot 5^2 + 4 \cdot 5 + 2 = (342)_5$ (Stellenwertsystem zur Basis 5).

Stellenwertsystem

Satz

Seien m und b natürliche Zahlen, mit $b \neq 0$.
Dann gibt es eine eindeutig bestimmte Liste von natürlichen Zahlen $r_0, r_1, \ldots, r_{n-1}$, sodaß

- $r_k < b$, *für alle* $k \in \{1, \ldots, n-1\}$
- $r_{n-1} \neq 0$.
- $m = r_{n-1} \cdot b^{n-1} + \ldots + r_1 \cdot b + r_0 \quad \left(= \sum_{k=0}^{n-1} r_k \cdot b^k \right)$.

Beispiel

Dezimalsystem Basis 10, in den meisten Kulturen üblich;

Duodezimalsystem Basis 12, von der Uhr bekannt;

Sexagesimalsystem Basis 60, altbabylonisch, Uhr;

Dualsystem Basis 2, verwenden die meisten Digitalcomputer;

Oktalsystem Basis 8, Variante des Dualsystems, da $8 = 2^3$;

Hexadezimalsystem Basis $16 = 2^{2^2}$, heute gängigere Variante.

Beweis für b-adische Darstellung

Beweis.

Ist $m = 0$, so erfüllt die leere Liste (und nur diese) die gewünschten Eigenschaften.

Ansonsten bestimmen wir mittels Euklidischer Division natürliche Zahlen q und r, sodaß $m = q \cdot b + r$ und $r < b$.

Wir nehmen an, daß q die eindeutige Darstellung

$$q = \sum_{k=0}^{n-1} r_k \cdot b^k$$

besitzt. Dann gilt

$$m = \left(\sum_{k=0}^{n-1} r_k \cdot b^k\right) \cdot b + r = \sum_{k=0}^{n-1} r_k \cdot b^{k+1} + r$$
$$= \sum_{k=1}^{n} r_{k-1} \cdot b^k + r \cdot b^0.$$

Damit haben wir eine passende Darstellung gefunden.

Es bleibt noch zu zeigen, daß diese eindeutig ist. (Übung!) □

Teilbarkeit

Axiom (Introduktionsregel für Teilbarkeit)

Wenn d, n, q ganze Zahlen sind, sodaß $q \cdot d = n$,
Dann gilt: d teilt n.

Beispiel

Weil $6 \cdot 2 = 12$, gilt: 2 teilt 12.

Beispiel

Wenn wir die Aussage „4 teilt 20“ beweisen möchten, so reicht es, eine ganze Zahl q zu konstruieren, sodaß $q \cdot 4 = 20$.

Bemerkung

Seien d, n beliebige ganze Zahlen. Wenn wir eine Aussage der Form

$$d \text{ teilt } n$$

beweisen möchten, so reicht es, dazu eine ganze Zahl q zu konstruieren (abhängig von d und n), sodaß $q \cdot d = n$.

Axiom (Eliminationsregel für Teilbarkeit)

Es seien d und n ganze Zahlen, sodaß gilt: d teilt n.
Dann gibt es eine ganze Zahl q, sodaß $q \cdot d = n$.

Teilbarkeit

Notation

Statt „d teilt n“ schreiben wir abkürzend „$d \mid n$“, und wir nennen dann die Zahl d einen Teiler von n.

Satz

Eine Zahl $d \in \mathbb{Z}$ ist genau dann ein Teiler von $n \in \mathbb{Z}$, wenn es ein $q \in \mathbb{Z}$ gibt, sodaß $n = q \cdot d$. D.h.

$$\forall_{d \in \mathbb{Z}} \forall_{n \in \mathbb{Z}} \quad d \mid n \iff \exists_{q \in \mathbb{Z}} \; n = q \cdot d.$$

Satz

Teilbarkeit ist transitiv, d.h. jeder Teiles eines Teilers ist ein Teiler:

$$\forall_{a,b,c \in \mathbb{Z}} \quad a \mid b \wedge b \mid c \implies a \mid c$$

Beweis.

Seien $a \mid b$ und $b \mid c$.
Dann gibt es $x, y \in \mathbb{Z}$, sodaß $b = x \cdot a$ und $c = y \cdot b$.
Einsetzen ergibt $c = y \cdot (x \cdot a) = (y \cdot x) \cdot a$,
d.h. $a \mid c$.

Ordnungseigenschaften der Teilbarkeit

Satz

Seien $a, b \in \mathbb{Z}$. *Dann gilt:* $a \mid b \iff |a| \mid |b|$

Satz

Für alle $a, b, c \in \mathbb{Z}$ *gilt:*

Reflexivität: $a \mid a$;

Transitivität: $a \mid b \wedge b \mid c \implies a \mid c$;

„Fast“-Antisymmetrie: $a \mid b \wedge b \mid a \iff |a| = |b|$.

Satz

Für alle $a \in \mathbb{Z}$ *gilt:*

- $1 \mid a$;
- $a \mid 1 \iff |a| = 1$;
- $a \mid 0$;
- $0 \mid a \iff a = 0$.

Somit ist 1 *die kleinste und* 0 *die größte Zahl (bezüglich Teilbarkeit).*

Teilbarkeit und Grundrechnungsarten

Satz

Seien $d, n, m, z \in \mathbb{Z}$ und $d \mid n$, $d \mid m$. Dann gelten auch $d \mid n + m$, $d \mid n - m$, und $d \mid z \cdot n$.

Lemma

Seien $m, n \in \mathbb{Z}$ und $m = qn + r$, mit $q, r \in \mathbb{Z}$, und $d \in \mathbb{Z}$ ein Teiler von n.
Dann ist d genau dann ein Teiler von m, wenn es ein Teiler von r ist.

Beweis.

Annahmen: $d \mid n$, $m = qn + r$. Wir haben zu zeigen, daß $d \mid m \iff d \mid r$.
Aus $d \mid n$ erhalten wir sofort $d \mid qn$.
Wenn $d \mid m$, dann gilt auch $d \mid (m - qn)$, und somit $d \mid r$.
Wenn $d \mid r$, dann gilt auch $d \mid (qn + r)$, und somit $d \mid m$.
Somit gilt $d \mid m \iff d \mid r$. □

Gemeinsame Teiler

Definition

Man nennt d einen gemeinsamen Teiler von $n, m \in \mathbb{Z}$, wenn $d \mid n$ und $d \mid m$ gilt.

Satz

Jeder Teiler eines gemeinsamen Teilers ist wieder ein gemeinsamer Teiler.

Beweis.

Dies folgt direkt aus der Transitivität der Teilbarkeitsrelation. □

Definition

Ein gemeinsamer Teiler $d \in \mathbb{N}$ heißt ein größter gemeinsamer Teiler, wenn jeder weitere gemeinsame Teiler ein Teiler von d ist.

Lemma

Gibt es zu zwei Zahlen einen größten gemeinsamen Teiler, so ist dieser eindeutig bestimmt.

Berechnung des größten gemeinsamen Teilers

Theorem (Euklidischer Algorithmus)

Seien $m, n \in \mathbb{Z}$. Dann gibt es genau einen größten gemeinsamen Teiler $d \in \mathbb{N}$ von m und n.

Beweis.

Wir beweisen mit Induktion nach $|n|$.
Ist $n = 0$, so ist $|m|$ ein größter gemeinsamer Teiler von m und n.
Ist $|n| > 0$, dann gibt es Zahlen q, r mit $m = qn + r$ und $0 \leq r < |n|$.
Laut Induktionsvoraussetzung haben n und r einen größten gemeinsamen Teiler d. Da die gemeinsamen Teiler von m und n dieselben sind wie die gemeinsamen Teiler von n und r, ist d auch der größte gemeinsame Teiler von m und n. □

Definition

Den größten gemeinsamen Teiler von m und n bezeichnen wir mit $\mathrm{ggT}(m, n)$. Laut obigem Beweis erfüllt dieser die beiden Gleichunen:

$$\mathrm{ggT}(m, 0) = |m|\,,$$
$$\mathrm{ggT}(m, n) = \mathrm{ggT}(n, r), \qquad \text{für } m = q \cdot n + r.$$

Gleichungen über den ganzen Zahlen

Problem

Es seien $m, n, d \in \mathbb{Z}$. Wir suchen nach ganzzahligen Lösungen der Gleichung

$$x \cdot m + y \cdot n = d.$$

Bemerkung

- *Jeder gemeinsame Teiler von m und n teilt auch d; insbesondere $\mathrm{ggT}(m, n) \mid d$.*
- *Falls $x_1 \cdot m + y_1 \cdot n = d$ gilt, dann erhalten wir daraus für jedes $q \in \mathbb{Z}$, $q \cdot x_1 \cdot m + q \cdot y_1 \cdot n = q \cdot d$, und somit auch eine Lösung von $x \cdot m + y \cdot n = q \cdot d$.*
- *Es ist daher von Interesse, ob diese Gleichung stets lösbar ist, wenn $d = \mathrm{ggT}(m, n)$.*
- *Die Differenz zweier Lösungen dieses Systems ist eine Lösung von $x \cdot m + y \cdot n = 0$ (die zugehörige homogene Gleichung).*

Lösung Diophantischer Gleichungen

Theorem (Erweiterter Euklidischer Algorithmus)

Seien $m, n \in \mathbb{Z}$, *und* $d = \mathrm{ggT}(m, n)$. *Dann gibt es* $x, y \in \mathbb{Z}$, *sodaß*

$$d = xm + yn.$$

Beweis.

Wir beweisen mit Induktion nach $|n|$.
Ist $n = 0$, so ist $d = |m|$. Aus $d = \operatorname{sgn} m \cdot m + 0n$ ergibt sich die passende Lösung.
Ist $|n| > 0$, dann gibt es Zahlen q, r mit $m = qn + r$ und $0 \leq r < |n|$. Es gilt dann $d = \mathrm{ggT}(n, r)$ und laut Induktionsvoraussetzung gibt es $x, y \in \mathbb{Z}$, sodaß $d = xn + yr$. Wegen $r = m - qn$ ergibt sich somit $d = xn + yr = xn + y(m - qn) = ym + (x - yq)n$. Damit haben wir eine passende Lösung gefunden. □

Bemerkung

$\mathrm{xggT}(m, 0) = (\operatorname{sgn} m, 0)$,
$\mathrm{xggT}(m, n) = (y, x - yq)$, *wobei* $m = qn + r$ *und* $(x, y) = \mathrm{xggT}(n, r)$.

Teilerfremde Zahlen

Definition

Zwei Zahlen $m, n \in \mathbb{Z}$ heißen teilerfremd, wenn $\mathrm{ggT}(m, n) = 1$.

Satz

Teilt eine Zahl ein Produkt und ist zu einem der beiden Faktoren teilerfremd, dann teilt sie den anderen Faktor. Genauer: Für alle $a, b, d \in \mathbb{Z}$ gilt:

$$d \mid ab \wedge \mathrm{ggT}(d, a) = 1 \implies d \mid b.$$

Beweis.

Wegen $\mathrm{ggT}(d, a) = 1$ gibt es $x, y \in \mathbb{Z}$, sodaß $dx + ay = 1$.
Dann ist $b = 1b = (dx + ay)b = dxb + aby$.
Da $d \mid ab$ teilt d auch diese Summe, somit $d \mid b$. □

Kongruenz modulo m

Definition

Sei $m \in \mathbb{N}$; dann heißen ganze Zahlen $a, b \in \mathbb{Z}$ kongruent modulo m falls m ein Teiler von deren Differenz $a - b$ ist:

$$a \equiv_m b : \Longleftrightarrow \; m \mid (a - b)$$

Satz

Die Kongruenz modulo m ist eine Äquivalenzrelation, d.h sie erfüllt:

Reflexivität: $a \equiv_m a$;

Symmetrie: $a \equiv_m b \implies b \equiv_m a$;

Transitivität: $a \equiv_m b \wedge b \equiv_m c \implies a \equiv_m c$.

Satz

Die Kongruenz modulo m ist mit der Addition, der Subtraktion und der Multiplikation verträglich, d.h. sind $a \equiv_m b$ und $c \equiv_m d$, so gelten auch

$$a + c \equiv_m b + d \qquad a - c \equiv_m b - d \qquad a \cdot c \equiv_m b \cdot d.$$

Restklassenring

Definition

Sei $m \in \mathbb{N}$. Wir betrachten jetzt ganze Zahlen bereits als gleich, wenn sie modulo m gleich sind. Dadurch entsteht eine neue Menge, die Faktormenge $\mathbb{Z}/_{\equiv_m}$. Sie heißt der Restklassenring modulo m und wird mit $\mathbb{Z}_m$ bezeichnet.

Bemerkung

- *Weil die Kongruenz modulo m eine Äquivalenzrelation ist, kommt sie als Gleichheitsbegriff in Frage.*
- *Die Tatsache, daß die Kongruenz modulo m mit Addition, Subtraktion und Multiplikation verträglich ist, garantiert, daß diese Operationen auch in $\mathbb{Z}_m$ wohldefiniert sind.*
- *Zu jedem $n \in \mathbb{Z}$ gibt es genau ein $r \in \mathbb{N}$, sodaß $n \equiv_m r$ und $r < m$. D.h. die Menge $\mathbb{Z}_m$ besteht aus m Elementen.*
- *In $\mathbb{Z}_m$ kann es vorkommen, daß das Produkt zweier von Null verschiedener Zahlen gleich Null ist (Nullteiler).*
  Beispiel: $2 \cdot 3 \equiv_6 0$, obwohl $2 \not\equiv_6 0$ und $3 \not\equiv_6 0$.

Dividieren modulo m

Problem

Wir versuchen eine lineare Gleichung modulo m zu lösen, d.h. wir suchen eine Lösung von $a \cdot x \equiv_m b$.

Bemerkung

Seien $a, b \in \mathbb{Z}$.
Dann gilt $a \equiv_m b$ *genau dann wenn es ein* $y \in \mathbb{Z}$ *gibt, sodaß* $a + m \cdot y = b$.

Bemerkung

Seien $a, b \in \mathbb{Z}$.
Dann gibt es genau dann ein $x \in \mathbb{Z}$, *sodaß* $a \cdot x \equiv_m b$, *wenn es* $x, y \in \mathbb{Z}$ *gibt, sodaß* $a \cdot x + m \cdot y = b$.

Folgerung

Die Gleichung $a \cdot x \equiv_m b$ *ist genau dann lösbar wenn* $\mathrm{ggT}(a, m) \mid b$.

Satz

a *ist modulo* m *invertierbar (d.h. es gibt eine Lösung von* $a \cdot x \equiv_m 1$*), wenn* $\mathrm{ggT}(a, m) = 1$.

Eulersche φ-Funktion

Definition

Die Menge der invertierbaren Elemente von $\mathbb{Z}_m$ sei mit $\mathbb{Z}_m^*$ bezeichnet.

Satz

$\mathbb{Z}_m^*$ ist gegenüber Multiplikation abgeschlossen.

Beweis.

Ist $a \cdot a^{-1} \equiv_m 1$ und $b \cdot b^{-1} \equiv_m 1$, dann ist wegen der Vertäglichkeit auch $(a \cdot a^{-1}) \cdot (b \cdot b^{-1}) \equiv_m 1$, bzw. $(a \cdot b) \cdot (a^{-1} \cdot b^{-1}) \equiv_m 1$. Somit ist auch $a \cdot b$ invertierbar und $(a \cdot b)^{-1} = a^{-1} \cdot b^{-1}$. □

Bemerkung

Man nennt daher $\mathbb{Z}_m^*$ auch eine Gruppe, weil Multiplikation und Invertieren nicht aus der Menge hinaus führen und die üblichen Rechenregeln gelten.

Definition

Sein $m \epsilon \mathbb{N}$. Dann bezeichnet $\varphi(m)$ die Anzahl der Elemente von $\mathbb{Z}_m^*$ (bzw die Anzahl der Zahlen $k \epsilon \mathbb{N}$, $k < m$, welche zu m teilerfremd sind). Die Funktion φ heißt die Eulersche φ-Funktion.

Potenziern mit der φ-Funktion

Satz (Euler)

Für $m \in \mathbb{N}$ und $a \in \mathbb{Z}_m^*$ (d.h. $\mathrm{ggT}(a, m) = 1$) gilt

$$a^{\varphi(m)} \equiv 1 \pmod{m}.$$

Beweis.

Später. □

Folgerung

Sei $a \in \mathbb{Z}_m^*$ und $e \equiv_{\varphi(m)} f$.
Dann gilt $a^e \equiv_m a^f$.

Folgerung

Sei $a \in \mathbb{Z}_m^*$ und $e \cdot d \equiv_{\varphi(m)} 1$.
Dann gilt $(a^e)^d \equiv_m a$.

Bemerkung

Wir können also im Restklassenring auch Wurzelziehen, sofern wir $\varphi(m)$ kennen.

Sukzessives Quadrieren

Satz

Die Berechnung von $a^n \epsilon \mathbb{Z}_m$ ist durch sukzessives Quadrieren (und sofortiges Reduzierem modulo m) effizient möglich.

Beweis.

Wir verwenden die Gleichungen;

$$\begin{aligned} a^0 &= 1; \\ a^{2n} &= (a^n)^2; \\ a^{2n+1} &= a(a^n)^2. \end{aligned}$$

□

Bemerkung

Für ganze Zahlen bringt das nichts, weil sie bei jedem Quadrieren doppelt so lange werden.
Wenn wir aber in jedem Schritt modulo m reduzieren können, bleiben alle Zwischenergebnisse durch m beschränkt.

Simultane Kongruenzen

Satz (Chinesischer Restsatz)

Seien $p, q \in \mathbb{N}$, $d = \mathrm{ggT}(p, q) = r \cdot p + s \cdot q$, $v = \mathrm{kgV}(p, q)$, *und* $a, b \in \mathbb{Z}$. *Dann gilt*

$$\begin{aligned} x &\equiv_p a, \\ x &\equiv_q b \end{aligned} \quad \Leftrightarrow \quad \begin{aligned} a &\equiv_d b, \\ x &\equiv_v s \cdot \tfrac{q}{d} \cdot a + r \cdot \tfrac{p}{d} \cdot b. \end{aligned}$$

Beweis.

$x \equiv_p a$ gilt genau dann wenn $x = a + k \cdot p$, für ein $k \in \mathbb{Z}$.
Einsetzen in die 2. Kongruenz: $a + k \cdot p \equiv_q b$.
Umformen ergibt: $k \cdot p \equiv_q b - a$.
Dies gilt genau dann wenn $d \mid (b - a)$ und und $k \equiv_q r \cdot \frac{a-b}{d}$.
Einsetzen in die 1. Kongruenz und Vereinfachen ergibt dann die gewünschte Form.
Zur Eindeutigkeit:
Sei y eine zweite Lösung.
Wegen $x \equiv_p a$ und $y \equiv_p a$ gilt $x - y \equiv_p 0$, d.h. $p \mid (x - y)$.
Analog ist $q \mid (x - y)$.
Und somit $v \mid (x - y)$.

□

Primzahlen

Definition

Ein natürliche Zahl $n > 1$ heißt Primzahl wenn sie keine echten Teiler hat (also nur 1 und n selbst). 1 ist per Definition keine Primzahl.

Lemma

Eine natürliche Zahl $p > 1$ ist genau dann eine Primzahl, wenn gilt:

$$\forall_{n,m \epsilon \mathbb{N}} \big(p \mid n \cdot m \implies p \mid n \vee p \mid m\big).$$

Beweis.

Sei $n = q \cdot p + r$.
Falls $r = 0$, dann gilt $p \mid n$.
Falls $0 < r < p$, dann ist $\mathrm{ggT}(n, p) = \mathrm{ggT}(p, r) = 1$. Gemäß einem Satz über teilerfremde Zahlen, muß somit $p \mid m$ gelten. □

Eindeutige Zerlegung in Primfaktoren

Theorem (Fundamentalsatz der Arithmetik)

Jede natürliche Zahl $n > 0$ hat eine eindeutige Zerlegung in Primfaktoren

$$n = p_1^{k_1} \dots p_m^{k_m},$$

wobei alle p_i Primzahlen sind, mit $p_i < p_{i+1}$, und $k_i > 0$.

Beweis.

- Existenz: Wenn n eine Primzahl ist, dann ist $n = n^1$ bereits die gewünschte Zerlegung. Ansonsten gibt es eine nicht-triviale Faktorisierung $n = a \cdot b$. Die eindeutigen Zerlegungen von a und b müssen dann nur noch kombiniert werden.
- Eindeutigkeit: Sei $n = {p'_1}^{k'_1} \dots {p'_{m'}}^{k'_{m'}}$ eine zweite derartige Zerleung. Dann muß gelten: $p_1 \mid {p'_1}^{k'_1} \dots {p'_{m'}}^{k'_{m'}}$. Da p_1 eine Primzahl ist, muß sie einen der Faktoren teilen. Sei p'_i dieser Faktor, d.h. $p_1 \mid p'_i$. Weil beide Primzahlen sind, folgt daraus $p_1 = p'_i$. Wir dividieren beide Seiten durch diesen Faktor und fahren in der selben Weise fort. □

Berechnung der φ-Funktion

Satz

- *Sei p eine Primzahl. Dann ist $\varphi(p) = p - 1$.*
- *Ist weiters $k > 1$, dann ist $\varphi(p^k) = p \cdot p^{k-1}$.*
- *Sind n und m teilerfremd, dann ist $\varphi(n \cdot m) = \varphi(n) \cdot \varphi(m)$.*

Bemerkung

Die φ-Funktion kann damit leicht berechent werden, wenn die Primfaktorzerlegung bekannt ist.

Potenzieren modulo Primzahlen

Satz (Fermat)

Sei p ein Primzahl, $a \in \mathbb{Z}$ beliebig. Dann gilt $a^p \equiv_p a$.

Folgerung (von Chinesischem Restsatz)

Seien p, q teilerfremd. Dann gilt: $x \equiv_p y \wedge x \equiv_q y \implies x \equiv_{p \cdot q} y$.

Satz

Seien p und q verschiedene Primzahlen, $m = p \cdot q$, und $n \equiv_{\varphi(m)} 1$. Dann gilt für beliebige $a \in \mathbb{Z}$

$$a^n \equiv_m a.$$

Beweis.

Wir zeigen zuerst, daß $a^n \equiv_p a$.

Wenn $a \equiv_p 0$, dann trivial.

Wenn $a \not\equiv_p 0$, dann ist $a \in \mathbb{Z}_p^*$ (weil p prim). Sei $n = 1 + k \cdot \varphi(m)$.

Somit

$$a^n = a^{1+k\cdot\varphi(m)} = a^{1+k\cdot\varphi(p)\cdot\varphi(q)} = a \cdot \left(a^{\varphi(p)}\right)^{k\cdot\varphi(q)} \equiv_p a \cdot 1^{\varphi(q)} \equiv_p a.$$

Analog ist $a^n \equiv_q a$.

Der Chinesische Restsatz (Eindeutigkeitsteil) liefert die Kongruenz modulo dem Produkt $p \cdot q$. □

Berechnung der Primfaktorzerlegung

Problem

Man finde die Primfaktorzerlegung für eine gegebene Zahl $n \in \mathbb{N}$.

Satz

Sei p *der kleinste nicht-triviale Teiler einer Zahl* $n \in \mathbb{N}$, *dann ist*

- $n = p$, *und somit* n *eine Primzahl, oder*
- $p^2 < n$.

Bemerkung

- *Um den kleinsten Teiler von* n *zu finden, muß man maximal alle Primzahlen bis* $\sqrt{n}$ *testen.*
- *Ist* $n \approx 2^k$, *dann ca* $O(2^{k/2})$ *Teilbarkeitstests.*
- *Grundrechnungsarten: ca* $O(k)$.
- *Es ist keine deutlich bessere allgemeine Methode bekannt.*
- *Faktorisieren viel schwieriger als Multiplizieren.*
- *Die Korrektheit einer Faktorisierung läßt sich leicht überprüfen.*
- *Ein Quantencomputer mit mindestens* k *Qubits könnte das Problem effizient lösen.*

Primzahltests

Problem

Man entscheide, ob eine gegebene Zahl $p \in \mathbb{N}$ eine Primzahl ist.

Satz

Für jede Primzahl p und jedes $a \in \mathbb{N}$, $a > 0$, gilt: $a^{p-1} \equiv_p 1$.

Bemerkung

- *Wenn $a^{p-1} \not\equiv_p 1$, dann muß p eine zusammengesetzte Zahl sein.*
- *Diese Tatsache gibt jedoch keinen Hinweis darauf, wie eine Faktorisierung aussehen könnte.*
- *Dieser Test läßt sich beliebig oft wiederholen.*
- *Wenn $a^{p-1} \equiv_p 1$, für viele verschiedene a, dann ist das ein deutlicher Hinweis, daß p eine Primzahl sein könnte.*
- *Durch eine Verfeinerung dieses Verfahres kann man die Fehlerwahrscheinlichkeit beliebig klein machen.*
- *Es gibt inzwischen auch ein halbwegs effizientes Verfahren, welches gegebenenfalls einen Beweis liefert, daß p eine Primzahl ist.*

Unendlich viele Primzahlen

Satz (Euklid)

Es gibt unendlich viele Primzahlen.

Beweis.

Zu jeder endlichen Mengen von Primzahlen konstruieren wir eine weitere Primzahl, die nicht darin vorkommt:
Es seien $p_1, \ldots, p_n$ Primzahlen.
Wir bilden das Produkt $m = p_1 \cdot \ldots \cdot p_n + 1$.
Wegen dem Fundamentalsatz der Arithmetik gibt es eine Primzahl, die m teilt.
Aber $m \equiv_{p_i} 1$, für alle $i = 1, \ldots, n$.
Es muß also mindestens eine weitere Primzahl geben. □

Bemerkung

- *Mit etwas mehr Theorie gelangt man zu wesentlich besseren Schranken.*
- *Der durchschnittliche Abstand zwischen zwei n-stelligen Primzahlen betägt ungefähr $2n$.*

Verschlüsselung

- Man wähle zwei große Primzahlen p und q.
- Sei $m = p \cdot q$. Es gilt: $\varphi(m) = (p-1)(q-1)$.
- Wähle $e \epsilon \mathbb{Z}^*_{\varphi(m)}$.
- Sei $a \epsilon \mathbb{Z}_m$, die Nachricht, Klartext.
- Berechne: $b \equiv_m a^e$. (Verschlüsselung)
- (m, e) ist der öffentliche Schlüssel.
- b ist das Kryptogramm (Geheimtext).
- Sei d das Inverse von $e \pmod{\varphi(m)}$.
- Dann gilt $b^d \equiv_m a$. (Entschlüsselung)
- (m, d) ist der geheime Schlüssel.
- Um aus aus dem öffentlichen Schlüssel (m, e) das d für den geheimen Schlüssel zu bestimmen, brauchen wir $\varphi(m)$, und dazu brauchen wir die Faktorisierung von m.
- Diese Methode (das RSA-Verfahren) funktioniert, weil das Problem der Faktorisierung schwierig ist.
- Das Verfahren gilt als sicher, wenn $m \approx 2^{1024} \approx 10^{308}$
- ... und noch ein paar zusätzliche Nebenbedingungnen gelten.