# Primzahltests und Faktorisierungsalgorithmen

Skript zur Vorlesung von
Prof. Dr. Peter Hauck

Sommersemester 2007

LaTeX-Fassung von Rainer Boie

# Inhaltsverzeichnis

# Einführung

## Leitende Fragen der Vorlesung

- Gegeben ein $n \in \mathbb{N}$. Wie kann man feststellen (und mit welchem Aufwand), ob $n$ eine Primzahl ist?
- Gegeben eine zusammengesetzte Primzahl $n$. Wie und mit welchem Auufwand kann man $a$ und $b$ bestimmen mit: $a, b \in \mathbb{N}; a, b > 1$ und $ab = n$.

Die Motivation zur Behandlung dieser Fragen kommt einerseits aus der Informatik, wo man am komplexitätstheoretischen Status dieser Probleme interessiert ist, andererseits aus der Kryptographie. Hierauf gehen wir kurz ein.

## Public-Key-Kryptographie

(Diffie, Hellman 1976)

Jeder Teilnehmer besitzt zwei Schlüssel:

- Der öffentliche Schlüssel (public key) dient der Verschlüsselung und ist öffentlich bekannt.
- Der private Schlüssel (private key) dient der Entschlüsselung und ist nur dem Besitzer bekannt.

Verschlüsselungsfunktionen sind Einwegfunktionen (Geheimtürfunktionen).
$x \longrightarrow f(x)$: einfach.
$f(x) \longrightarrow x$: schwer, außer man besitzt den geheimen Schlüssel, dann ist es einfach.

## RSA-Verfahren

(Rivest, Shamir, Adleman 1978)

Wähle zwei große Primzahlen $p, q$ (jeweils $\sim 500$ Bit) mit $p \neq q, n = pq$.
Nun sei folgende Funktion definiert:
$\varphi(n) = |\{x \in \mathbb{N}, 1 \leq x \leq n, ggT(x, n) = 1\}|$. Dann ist $\varphi(n) = (p-1)(q-1)$.
Desweiteren ist $e$ zu bestimmen mit:
$1 \leq e \leq \varphi(n)$ und $ggT(e, \varphi(n)) = 1$.
Der öffentliche Schlüssel bestimmt sich nun zu $(n, e)$.

Für den privaten Schlüssel $d$ gilt: $1 \leq d \leq \varphi(n), ed \equiv 1(mod\ \varphi(n))$.
Der erweiterte Euklidische Algorithmus (siehe 1.4) liefert
$s, t \in \mathbb{Z}$ mit $s\ \varphi(n) + t\ e = 1$.
Der private Schlüssel ergibt sich nun zu $d = t\ mod\ \varphi(n)$.

Verschlüsselung:
Die Verschlüsselungsfunktion ist $f : x \to x^e\ mod\ n$. Sei $0 \leq m < n$. $m$ wird verschlüsselt zu $m^e\ mod\ n = c$ (Chiffretext). $e$ wird häufig relativ klein gewählt, damit die Verschlüsselung schnell geht.

Entschlüsselung:

| | |
|---|---|
| $c^d\ mod\ n$ | |
| $= m^{ed}\ mod\ n$ | |
| $= m^{1+k\varphi(n)}\ mod\ n$ | |
| $= m\ (\underbrace{m^{\varphi(n)}}_{=1})^k\ mod\ n$ | nach Satz von Euler (vgl. 1.10a)) gilt: |
| $= m\ mod\ n = m$ | $m^{\varphi(n)}\ mod\ n = 1$, falls $ggT(m, n) = 1$ |

Ist $ggT(m, n) \neq 1$, so gilt $c^d\ mod\ n = m$ ebenfalls (mit einer etwas anderen Argumentation).

**Zur Sicherheit von RSA:**
Ein Angreifer hat den öffentlichen Schlüssel $(n, e)$. Um daraus den privaten Schlüssel $d$ zu berechnen, muss er $\varphi(n)$ und somit $p$ und $q$ mit $n = pq$ bestimmen. Dies ist ein (momentan) sehr zeitaufwändiges Faktorisierungsproblem.

# 1 Hilfsmittel aus der Algebra

**Die wichtigsten algebraischen Strukturen, die wir benötigen, sind Gruppen und Ringe.**

## 1.1 Definition

a) Eine Gruppe ist eine Menge $G \neq \emptyset$ mit der Verknüpfung $\cdot$, $(g,h) \to g \cdot h \in G$. Dabei gilt:

1. Assoziativgesetz: $(g \cdot h) \cdot k = g \cdot (h \cdot k) \quad \forall \quad g,h,k \in G$.
2. Existenz eines neutralen Elements $e$: $\quad g \cdot e = e \cdot g = g \quad \forall \quad g \in G$.
3. Existenz von inversen Elementen: $\forall \ g \in G \ \exists \ g^{-1} \in G : g \cdot g^{-1} = g^{-1} \cdot g = e$.

b) G heißt *abelsch* oder *kommutativ*, falls

4. $g \cdot h = h \cdot g \quad \forall \ g,h \in G$

c) Anzahl der Elemente von G: |G|, *Ordnung* von G.

d) $\emptyset \neq H \subseteq G$ heißt *Untergruppe*, falls $(H, \cdot)$ selbst Gruppe ist. Schreibweise: $H \leq G$. ($H$ hat dann dasselbe neutrale Element wie $G$.)

## 1.2 Bemerkung

a) Das neutrale Element und die Inversen sind eindeutig bestimmt.

b)
- Potenzen von $g$: $g \in G : g^0 = e$. $n \in \mathbb{N} : g^n = g^{n-1}g$,

  $g^{-n} = (g^{-1})^n = (g^n)^{-1}$

  $\left.\begin{matrix} g^n g^m = g^{n+m} \\ (g^n)^m = g^{nm} \end{matrix}\right\} \forall \ n,m \in \mathbb{Z}$

  Im Allgemeinen ist zu beachten: $(gh)^n \neq g^n h^n$
- Vielfache von $g$ wenn die Verknüpfung $+$ ist:

  $ng = \underbrace{g + ... + g}_{n}$

  $(-n)g = \underbrace{(-g) + ... + (-g)}_{|n|}$

  $0 \cdot g = 0$ (neutrales Element)

## 1.3 Beispiele

a) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$ und $(\mathbb{R}, +)$ sind jeweils Gruppen.

b) $(\mathbb{Z}, \cdot)$ ist keine Gruppe wegen der Inversen: $z \in \mathbb{Z} \Rightarrow \frac{1}{z} \notin \mathbb{Z}$ für $z \neq \pm 1$.

c) Sei $\mathbb{Z}_n = \{0, 1, ..., n-1\}$ mit $a \oplus b = (a + b)\ mod\ n$.
$(\mathbb{Z}_n, \oplus)$ ist eine Gruppe. Für die Inverse gilt: $a \in \mathbb{Z}_n \Rightarrow n - a \in \mathbb{Z}_n$

d) Gegeben $\mathbb{Z}_n$ mit $a \odot b = (ab)\ mod\ n$. Das Assoziativgesetz gilt ebenso wie das Kommutativgesetz und das neutrale Element ist $e = 1$.
Welche Elemente haben in $\mathbb{Z}_n$ Inverse bezüglich der Verknüpfung $\odot$?
$x \in \mathbb{Z}_n$ ist invertierbar $\Leftrightarrow ggT(x, n) = 1$.
Sei nun $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n : ggT(x, n) = 1\}$ (die Null ist nie enthalten). Dies ist eine Gruppe bezüglich $\odot$. Die Inversen berechnet man am besten mit dem Erweiterten Euklidischen Algorithmus (1.4).

## 1.4 Erweiterter Euklidischer Algorithmus

(Euklid, ca. 365-300 v.Chr.)

a) Gegeben $a, b \in \mathbb{N}$ mit $a \geq b > 0$. Als Ergebnis bekommt man den $ggT(a, b)$ und $s, t \in \mathbb{Z}$ mit $ggT(a, b) = sa + tb$.

Algorithmus:
$x = a, y = b$
$s_1 = 1, s_2 = 0, s = 0$
$t_1 = 0, t_2 = 1, t = 1$
*while* $x\ mod\ y \neq 0$ *do*
$g = x\ div\ y,\ r = x\ mod\ y$
$s = s_1 - gs_2, t = t_1 - gt_2$
$s_1 = s_2, s_2 = s, t_1 = t_2, t_2 = t$
$x = y, y = r$
Output: $y = ggT(a, b)$ und $s, t$ mit $y = as + bt$

Beispiel: $a = 14, b = 5$

| $x\ mod\ y$ | $x$ | $y$ | $s_1$ | $s_2$ | $s$ | $t_1$ | $t_2$ | $t$ | $g$ | $r$ |
|---|---|---|---|---|---|---|---|---|---|---|
| | 14 | 5 | 1 | 0 | 0 | 0 | 1 | 1 | | |
| 4 | 5 | 4 | 0 | 1 | 1 | 1 | -2 | -2 | 2 | 4 |
| 1 | 4 | 1 | 1 | -1 | -1 | -2 | 3 | 3 | 1 | 1 |
| 0 | | | | | | | | | | |

$ggT(14, 5) = 1 = (-1) \cdot 14 + 3 \cdot 5$

b) Bestimmung der Inversen in $(\mathbb{Z}_n{}^*, \odot)$:
$x \in \mathbb{Z}_n{}^*$: Erweiterter Euklidischer Algorithmus liefert $s, t \in \mathbb{Z}$ mit $1 = ggT(x, n) = s \cdot x + t \cdot n$
$x^{-1}$ bezüglich $\oplus$: $s \ mod \ n$
$(s \ mod \ n) \ \odot \ x = ((s \ mod \ n) \cdot x) \ mod \ n = (s \cdot x) \ mod \ n = (1 - tn) \ mod \ n = 1$
(vgl. Modulo-Regeln 1.5)
$5 \in \mathbb{Z}_{14}{}^* \Rightarrow 5^{-1} = 3$ bzgl. $\odot$: $\quad 5 \odot 3 = (5 \cdot 3) \ mod \ 14 = 1$

## 1.5 Modulo-Regeln

$(a + b) mod \ n = ((a \ mod \ n) + (b \ mod \ n)) \ mod \ n$ und ebenso für die Multiplikation.

Beispiel:
$2^{300} \ mod \ 7$
$= (2^3)^{100} \ mod \ 7$
$= (8 \ mod \ 7)^{100} \ mod \ 7$
$= 1.$

Genauso:
$2^{300} \ mod \ 9$
$= (2^3)^{100} \ mod \ 9$
$= (-1)^{100} \ mod \ 9$
$= 1$

## 1.6 Satz von Lagrange

(J.L. Lagrange, 1736-1813)

Ist $G$ eine endliche Gruppe und $H$ eine Untergruppe in $G$, so gilt $|H| \ \Big| \ |G|$. Die Ordnung von $H$ ist Teiler der Ordnung von $G$.

Beweisidee:
$x \in G \rightarrow xH = \{xh : h \in H\}$; $xH$ heißt Nebenklasse von H in G.

(1) $x, y \in G$: Entweder ist $xH = yH$ oder $xH \cap yH = \emptyset$
$x \in G : x \in xH \quad (x = x \cdot 1 \in xH)$
$G = \bigcup_{i=1}^{r} x_i H$ Vereinigung der verschiedenen Nebenklassen.

(2)
$$\text{Für } x \in G \text{ ist } \begin{cases} H \rightarrow xH \\ h \rightarrow xh \end{cases} \quad \text{eine bijektive Abbildung.}$$

$|H| = |xH|$ und daher $|G| = r \cdot |H|$ $\quad$ nach (1).
Beweis für die Injektivität:
$xh_1 = xh_2$

$x^{-1}(xh_1) = x^{-1}(xh_2)$
$1 \cdot h_1 = 1 \cdot h_2 \Rightarrow h_1 = h_2$

## 1.7 Satz

Sei $G$ eine Gruppe und $g \in G$.

a) Sei $\langle g \rangle = \{g^m : m \in \mathbb{Z}\}$. Dann ist $\langle g \rangle \leq G$. $\langle g \rangle$ heißt die von $g$ erzeugte *zyklische* Gruppe.

b) $\langle g \rangle$ ist unendlich $\Leftrightarrow g^m \neq g^l \quad \forall \quad m, l \in \mathbb{Z}, m \neq l$.

c) Ist $\langle g \rangle$ endlich, so existiert ein kleinstes $n \in \mathbb{N}$ mit $g^n = e$. $n$ ist die *Ordnung* von $g$: $o(g) = n$.
Es ist $\langle g \rangle = \{g^0 = e, g^1 = g, g^2, ..., g^{n-1}\}$, wobei $g^0, ..., g^{n-1}$ paarweise verschieden sind.
$o(g) = n = |\langle g \rangle|$.

d) Ist $o(g) = n$ endlich und $m \in \mathbb{Z}$, so gilt: $g^m = g^r$, wobei $r = m \ mod \ n$, d.h. $m = qn + r, 0 \leq r < n - 1$.
Insbesondere gilt $g^m = e \Leftrightarrow n \mid m$.
Nach Satz 1.6 folgt: $n = o(g) = |\langle g \rangle| \ \Big| \ |G| : g^{|G|} = e$.

e) Ist $o(g) = n$ endlich, so folgt:
$m \in \mathbb{Z} : o(g^m) = \frac{n}{ggT(n,m)}$.
Insbesondere gilt: $\langle g \rangle =< g^m > \quad \Leftrightarrow \ ggT(n, m) = 1$.

Beweis:

a) Folgt aus 1.2 b)

b), c), d) Angenommen $g^n = g^m$ für gewisse $n, m (n > m)$.
Dann $g^{n-m} = e$. Daher existiert ein kleinstes $k \in \mathbb{N}$ mit $g^k = e$.
Dann:
$g^0 = e, g^1, \dots g^{k-1}$ paarweise verschieden.
$g^l \in \langle g \rangle, \quad l \in \mathbb{Z}$,
$l = tk + r, \quad 0 \leq r < k, \quad g^l = g^{tk+r} = (g^k)^t \cdot g^r = g^r \in \{e, g^1, \dots, g^{k-1}\}$.
Also: $\langle g \rangle = \{g^0, g^1, \dots, g^{k-1}\}$.
$k = o(g) = |\langle g \rangle| \ \big| \ |G|, |G| = s \cdot k, g^{|G|} = g^{sk} = (g^k)^s = e$

e) Sei $ggT(l, k) = s$. $(g^l)^{\frac{k}{s}} = g^{\frac{lk}{s}} = (g^k)^{\frac{l}{s}} = e, o(g^l) \leq \frac{k}{s}$.
Sei $o(g^l) = u$, dann $g^{lu} = e \Rightarrow k | lu \Rightarrow \frac{k}{s} | \frac{l}{s} \cdot u$.
Da $\frac{k}{s}, \frac{l}{s}$ teilerfremd sind, folgt $\frac{k}{s} | u = o(g^l)$. Also $o(g^l) = \frac{k}{s}$.

## 1.8 Beispiel

a) $(\mathbb{Z}, +)$ unendliche zyklische Gruppe, denn $\mathbb{Z} =< 1 >=< -1 >$

b) $(\mathbb{Z}_n, \oplus)$ zyklische Gruppe der Ordnung $n$, denn $\mathbb{Z}_n =< 1 >$:
$1 = 1 \cdot 1,\ 2 = 2 \cdot 1,\ \ldots,\ n-1 = (n-1) \cdot 1,\ n \cdot 1 = n = 0$

## 1.9 Bemerkung

$G = \langle g \rangle$ unendlich
$G = \{g^i | i \in \mathbb{Z}\}$

$$\text{Die Abbildung } \varphi : \begin{cases} G \to \mathbb{Z} \\ g^i \mapsto i \end{cases} \quad \text{ist}$$

bijektiv, Homomorphismus: $\varphi(g^i \cdot g^j) = \varphi(g^{i+j}) = i + j = \varphi(g^i) + \varphi(g^j)$, also Isomorphismus.
Also $G \cong \mathbb{Z}$.

Ähnlich:
Ist $G = \langle g \rangle$ endlich von der Ordnung $n$, dann $G \cong (\mathbb{Z}_n, \oplus)$.

## 1.10 Satz

a) (Satz von Euler; L. Euler, 1707-1783)
Sei $n \in \mathbb{N}, a \in \mathbb{Z}, ggT(a, n) = 1$.
Dann ist $a^{\varphi(n)} \equiv 1 (mod\ n)$, wobei $\varphi$ die Eulersche Funktion $\varphi(n) = |\{x \in \mathbb{N} : 1 \leq x \leq n \quad ggT(x, n) = 1\}|$.
$[n = {p_1}^{a_1} ... {p_r}^{a_r}$ wobei $p_i$ Primzahlen sind, $p_i \neq p_j$ für $i \neq j$:
$\varphi(n) = \varphi({p_1}^{a_1}) ... \varphi({p_r}^{a_r}) = {p_1}^{a_1 - 1}(p_1 - 1) ... {p_r}^{a_r - 1}(p_r - 1)]$

b) (kleiner Satz von Fermat; P. de Fermat, 1601-1665)
Sei $p$ eine Primzahl und $a \in \mathbb{Z}, p \nmid a$.
Dann ist $a^{p-1} \equiv 1 (mod\ p)$.

Beweis:
a) $(\mathbb{Z}_n, \odot)$. Invertierbare Elemente bilden eine Gruppe bzgl. $\odot$
${\mathbb{Z}_n}^* = \{x : 1 \leq x < n, ggT(x, n) = 1\}$ vgl. 1.4b)
$|{\mathbb{Z}_n}^*| = \varphi(n)$
$ggT(a, n) = 1 \qquad \tilde{a} = a\ mod\ n \qquad ggT(\tilde{a}, n) = 1$
$\tilde{a} \in {\mathbb{Z}_n}^*$ 1.6: $\tilde{a}^{\varphi(n)} = 1$ Potenzierung in ${\mathbb{Z}_n}^*$ bzgl. $\odot$
Potenzierung in $\mathbb{Z} \quad \tilde{a}^{\varphi(n)} \equiv 1 (mod\ n)$; $\quad (a\ mod\ n)^{\varphi(n)} \equiv 1 (mod\ n)$ und daher $a^{\varphi(n)} \equiv 1 (mod\ n)$

b) folgt aus a) mit $\varphi(p) = p - 1$

## 1.11 Chinesischer Restsatz

Seien $m_1, ..., m_r \in \mathbb{N}$, paarweise teilerfremd, und seien $a_1, ..., a_r \in \mathbb{Z}$. Dann gibt es genau eine Zahl $x \in \mathbb{Z}$ mit $0 \leq x < m_1 ... m_r$ und
$x \equiv a_j (mod\ m_j)$ für $j = 1, ..., r$
d.h. $x\ mod\ m_j = a_j\ mod\ m_j$

Beweis:
Setze $m = \prod_{i=1}^{r} m_i, M_j = \frac{m}{m_j}, j = 1, ..., r$. Dann ist der $ggT(m_j, M_j) = 1$.
(erw. Eukl. Alg. 1.4): $\exists y_j, z_j \in \mathbb{Z}$ mit $y_j M_j + z_j m_j = 1, j = 1, ..., r$.
Also gilt: $y_j M_j \equiv 1 (mod\ m_j)$. Dann $a_j y_j M_j \equiv a_j (mod\ m_j), j = 1, ..., r$
Aber: $a_j y_j M_j \equiv 0 (mod\ m_i), i \neq j$.

$x = \sum_{j=1}^{r} a_j y_j M_j\ mod\ m.$
Dann $x\ mod\ m_i \equiv a_i\ mod\ m_i, i = 1, ..., r$, d.h. $x \equiv a_i\ mod\ m_i$.

## 1.12 Beispiel zum Chinesischen Restsatz

$x \equiv 2 (= a_1)\ mod\ 3 (= m_1)$
$x \equiv 4 (= a_2)\ mod\ 11 (= m_2)$
$x \equiv 1 (= a_3)\ mod\ 26 (= m_3)$
Nach 1.11 folgt:
$\exists$ genau ein $x, 0 \leq x \leq 3 \cdot 11 \cdot 26 = 858$.
$M_1 = 286, M_2 = 78, M_3 = 33, m_1 = 3, m_2 = 11, m_3 = 26$
Erw. Eukl. Alg. (1.4 ): $1 \cdot 286 + (-95) \cdot 3 = 1 \quad y_1 = 1$
$1 \cdot 78 + (-7) \cdot 11 = 1 \quad y_2 = 2$
$15 \cdot 33 + (-9) \cdot 26 = 1 \quad y_3 = 15$
$x = (2 \cdot 1 \cdot 286 + 4 \cdot 1 \cdot 78 + 1 \cdot 15 \cdot 33)\ mod\ 858 = 1379\ mod\ 858 = 521$

## 1.13 Definition

a) $R \neq \emptyset$ mit zwei Verknüpfungen $+, \cdot$ heißt *kommutativer* Ring, falls gilt:

   1. $(R, +)$ ist kommutative Gruppe (neutrales Element 0, Nullelement)
   2. $(R, \cdot)$ erfüllt Kommutativ- und Assoziativgesetz
   3. $a \cdot (b + c) = a \cdot b + a \cdot c, (a + b) \cdot c = a \cdot c + b \cdot c$ (Distributivgesetze)

b) Hat $(R, \cdot)$ ein neutrales Element $1 \neq 0$ (Einselement, Eins), so heißt R *Ring mit Eins*.

## 1.14 Beispiele zu Ringen

a) $(\mathbb{Z}, +, \cdot)$ ist kommutativer Ring mit Eins, ebenso $(\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot)$

b) $(\mathbb{Z}_n, \oplus, \odot), n > 1$, ist kommutativer Ring mit Eins.

## 1.15 Bemerkung

Sei $R$ ein Ring.

a) $a \cdot 0 = 0 \quad \forall \quad a \in R$

b) $a \cdot (-b) = (-a) \cdot b = -(a \cdot b) \quad \forall \quad a, b \in R$

c) $(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^k b^{n-k} \quad \forall \quad a, b \in R$ (Dabei: $a^0 b^n = b^n, a^n b^0 = a^n$)

Beweis:

a) $a \cdot 0 = a \cdot (0+0) = a \cdot 0 + a \cdot 0$ Addiere $-(a \cdot 0)$
$0 = a \cdot 0 + 0 = a \cdot 0$

b) $a \cdot (-b) + a \cdot b = a \cdot (-b+b) \underbrace{=}_{a)} 0$, ebenso $a \cdot (-b) = -(a \cdot b)$ und $(-a) \cdot b = -(a \cdot b)$

c) Wie in $\mathbb{Z}$ per Induktion nach $n$.

## 1.16 Definition

$R$ kommutativer Ring mit Eins:

a) $r \in R$ heißt *Einheit*, falls $r$ bezüglich der Multiplikation ein Inverses $r^{-1} \in R$ besitzt, d.h.: $r \cdot r^{-1} = 1$. 0 ist nie eine Einheit. Menge der Einheiten: $R^*$. $(R^*, \cdot)$ ist Gruppe, aber zusammen mit $+$ nie ein Ring, da die 0 nicht enthalten ist.

b) $R$ heißt *Körper*, falls $R^* = R \setminus \{0\}$.

## 1.17 Beispiele

a) $\mathbb{Z}^* = \{1, -1\}$

b) ${\mathbb{Z}_n}^* = \{x \in \mathbb{Z}_n : ggT(x, n) = 1\}$

c) $\mathbb{Q}, \mathbb{R}$ Körper; endlicher Körper: $(\mathbb{Z}_p, \oplus, \odot)$, wenn $p$ eine Primzahl ist.

## 1.18 Bemerkung

$K$ sei ein Körper, $a, b \in K$. Ist $a \cdot b = 0$, so ist $a = 0$ oder $b = 0$.

Beweis: $a = 0$ fertig. Ist $a \neq 0$, dann existiert $a^{-1}$. $0 = a^{-1} \cdot 0 = a^{-1} \cdot (a \cdot b) = 1 \cdot b = b$, also $b = 0$.

## 1.19 Definition und Satz

Sei $R$ ein kommutativer Ring mit Eins.
$R[x] = \{\sum_{i=0}^{n} a_i x^i \quad : a_i \in R, n \in \mathbb{N}_0\}$.
Elemente von $R[x]$: Polynome in einer Variablen über $R$.

Addition: $(\sum_{i=0}^{n} a_i x^i) + (\sum_{i=0}^{m} b_i x^i) = \sum_{i=0}^{max(n,n)} (a_i + b_i) x^i$, wobei $a_i = 0$, wenn $i > n$ und $b_i = 0$, wenn $i > m$.

Multiplikation: $(\sum_{i=0}^{n} a_i x^i) \cdot (\sum_{i=0}^{m} b_i x^i) = (\sum_{i=0}^{n+m} c_i x^i), \quad c_i = \sum_{j=0}^{i} a_j \cdot b_{i-j}$, wobei $a_j = 0$, wenn $j > n$ und $b_j = 0$, wenn $j > m$. $0 \cdot x^i$ kann weggelassen werden, $1 \cdot x^i = x^i$ und $a_0 \cdot x^0 = a_0$

$R[x]$ kommutativer Ring mit Eins. Nullelement 0 (alle $a_i = 0$), Einselement $1 (a_0 = 1, \ a_i = 0 \ \forall \ i > 1)$
*Polynomring* (in einer Variablen) über $R$.
Größtes $n$ mit $a_n \neq 0$: *Grad* des Polynoms. Grad(0):$= -\infty$

Beispiel:
$\mathbb{Z}_3[x] : (x^2 + 2x + 1)(x^3 + x + 2) = x^5 + 2x^4 + x^3 + x^3 + 2x^2 + x + 2x^2 + 4x + 2 = x^5 + 2x^4 + 2x^3 + x^2 + 2x + 2$

Ist $Grad(f) = n$, und $a_n = 1 : f$ ist *normiert*.
$a \cdot (\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} (a \cdot a_i) x^i$, wobei $a \in R$ also ein Polynom vom Grad $\leq 0$.
$x \cdot (\sum_{i=0}^{n} a_i x^i) = \sum_{i=0}^{n} a_i x^{i+1}$.

## 1.20 Satz

Sei $K$ ein Körper, $f, g \in K[x]$.

a) $Grad(fg) = Grad(f) + Grad(g)$

b) $K[x]^* = K \setminus \{0\}$ Polynome vom Grad 0

c) Es existieren eindeutig bestimmte Polynome $q, r \in K[x]$ mit $f = q \cdot g + r$, wobei $Grad(r) < Grad(g)$ (Division mit Rest).
Falls $r = 0$: $g$ teilt $f \quad (g \mid f)$
$q = f\ div\ g, r = f\ mod\ g$.

Beweis:

a) $(\sum_{i=0}^{n} a_i x^i) \cdot (\sum_{i=0}^{m} b_i x^i) = a_n b_m x^{n+m} + ...$, wobei $a_n \neq 0, b_m \neq 0$ also $a_n \cdot b_m \neq 0$ nach 1.18.

b) Folgt aus a).

c) Beweist man wie in $\mathbb{Z}$.

## 1.21 Beispiel

$$
\begin{array}{rl}
2x^4 + x^3 + 2x + 1 = \left(x^2 + x + 2\right)\left(2x^2 - x - 3\right) + 7x + 7 \\
\underline{-2x^4 - 2x^3 - 4x^2} \\
\quad -x^3 - 4x^2 + 2x \\
\quad \underline{x^3 + x^2 + 2x} \\
\quad\quad -3x^2 + 4x + 1 \\
\quad\quad \underline{3x^2 + 3x + 6} \\
\quad\quad\quad 7x + 7
\end{array}
$$

$f\ div\ g = 2x^2 - x - 3$, $f\ mod\ g = 7x + 7$
Fasst man $f$ und $g$ z.B. als Polynome in $\mathbb{Z}_3[x]$ auf, so muss man die obigen Ergebnisse *modulo 3* reduzieren, d.h. dann
$f\ div\ g = 2x^2 + 2x$ und
$f\ mod\ g = x + 1$.

## 1.22 Definition

$f, g \in K[x]$, nicht beide $= 0$.
$ggT(f, g) =$ normiertes Polynom maximalen Grades, das $f$ und $g$ teilt.
$(h \mid f, a \neq 0, a \in K$, so $ah \mid f$, denn $f = qh = (a^{-1}q)(ah))$

Eindeutigkeit von $ggT(f, g)$ folgt aus:

## 1.23 Satz von Bezout

(E. Bezout, 1730-1783)

$f, g \in K[x]$, nicht beide 0. Dann existieren $u, v \in K[x]$ mit $ggT(f,g) = u \cdot f + v \cdot g$

Daraus folgt: Jeder gemeinsame Teiler von $f$ und $g$ teilt $ggT(f,g)$.
Die $ggT$-Berechnung erfolgt mit dem Euklidischen Algorithmus, die Berechnung von $u, v$ mit dem erweiterten Euklidischen Algorithmus (1.24).

## 1.24 Erweiterter Euklidischer Algorithmus in K[x]

Gegeben:
$f(x)$ und $g(x) \neq 0, Grad\ f(x) \geq Grad\ g(x)$

1. Setze
   $s(x) := f(x),\ t(x) := g(x)$
   $u_1(x) := 1,\ u_2(x) := 0,\ u(x) := 0$
   $v_1(x) := 0,\ v_2(x) := 1,\ v(x) := 1$

2. Solange $s(x)\ mod\ t(x) \neq 0$, wiederhole
   $q(x) := s(x)\ div\ t(x),\ r(x) := s(x)\ mod\ t(x)$
   $u(x) := u_1(x) - q(x)\ u_2(x),\ v(x) := v_1(x) - q(x)\ v_2(x)$
   $u_1(x) := u_2(x),\ u_2(x) := u(x)$
   $v_1(x) := v_2(x),\ v_2(x) := v(x)$
   $s(x) := t(x),\ t(x) := r(x)$

3. Sei a der höchste Koeffizient $\neq 0$ von $t(x)$.
   $t(x) := a^{-1}t(x),\ u(x) := a^{-1}u(x),\ v(x) := a^{-1}v(x)$

4. Ausgabe:
   $t(x)$ $\quad (= ggT(f(x), g(x)))$
   $u(x), v(x)$ $\quad (t(x) = u(x)\ f(x) + v(x)\ g(x))$

## 1.25 Beispiel

$f(x) = 2x^4 + x^3 + 2x + 1,\ g(x) = x^2 + x + 2\ \in \mathbb{Z}_3[x]$

1. $s(x) := f(x),\ t(x) := g(x)$
   $u_1(x) := 1,\ u_2(x) := 0,\ u(x) := 0$
   $v_1(x) := 0,\ v_2(x) := 1,\ v(x) := 1$

2. $s(x)\ mod\ t(x) = x + 1 \neq 0$
   $q(x) = s(x)\ div\ t(x) = 2x^2 + 2x$
   $r(x) = s(x)\ mod\ t(x) = x + 1$
   $u(x) = u_1(x) - q(x)\ u_2(x) = 1$

$v(x) = v_1(x) - q(x)\ v_2(x) = x^2 + x$
$u_1(x) = 0,\ u_2(x) = 1,\ v_1(x) = 1,\ v_2(x) = x^2 + x$
$s(x) = x^2 + x + 2,\ t(x) = x + 1$

$s(x)\ mod\ t(x) = 2 \neq 0$
$q(x) = x,\ r(x) = 2$
$u(x) = 2x,\ v(x) = 2x^3 + 2x^2 + 1$
$u_1(x) = 2x,\ u_2(x) = 2x$
$v_1(x) = x^2 + x,\ v_2(x) = 2x^3 + 2x^2 + 1$
$s(x) = x + 1,\ t(x) = 2$

$s(x)\ mod\ t(x) = 0$

3. $t(x) = 1,\ u(x) = x,\ v(x) = x^3 + x^2 + 2$

4. Ausgabe:
   $1 = ggT(f(x), g(x))$
   $= x \cdot (2x^4 + x^3 + 2x + 1) + (x^3 + x^2 + 2) \cdot (x^2 + x + 2)$

## 1.26 Satz

$f \in K[x], Grad(f) = n \geq 1$.
$K[x]_n = \{g \in K[x] : Grad(g) < n\}$ wird kommutativer Ring mit Eins durch folgende Verknüpfungen:

Addition: Addition in $K[x]$.

Multiplikation: $\odot_f$
$g \odot_f h = (gh)\ mod\ f$
$(K[x]_n, +, \odot_f)$ wird auch mit $K[x]/(f)$ bezeichnet. ${K[x]_n}^* = \{g \in K[x]_n : ggT(f, g) = 1\}$

Bestimmung der Inversen von $g \in K[x]_n^*$ bezüglich $\odot_f$: Erw. Eukl.Alg (1.24): $u, v \in K[x]$.
$1 = ggT(f, g) = u \cdot f + v \cdot g, g^{-1} = v\ mod\ f$.

## 1.27 Beispiel

$f = 2x^4 + x^3 + 2x + 1 \in \mathbb{Z}_3[x],\ \mathbb{Z}_3[x]_4 = \{g \in \mathbb{Z}_3[x] : Grad(g) < 4\}$
$g = x^2 + x + 2.$ $\quad 1 = ggT(f, g) \underbrace{=}_{1.24} x \cdot f + (x^3 + x^2 + 2) \cdot g$ (erw. Eukl. Alg.)
$g^{-1} = x^3 + x^2 + 2$, d.h. $(x^3 + x^2 + 2) \odot_f (x^2 + x + 2) = 1$.

## 1.28 Definition

Polynom $f \in K[x]$ vom $Grad \geq 1$ heißt *irreduzibel*, falls aus
$f = gh$ mit $g, h \in K[x]$ folgt, dass $Grad(g) = 0$ oder $Grad(h) = 0$.
(Beachte: Faktorisierung, wobei ein Faktor Grad 0 hat, ist immer möglich:
$f = a \cdot (a^{-1} \cdot f)$)

## 1.29 Satz

Ist $f$ ein irreduzibles Polynom vom $Grad\ n$, so ist $(K[x]_n, +, \odot_f)$ ein Körper.
Speziell: $K = \mathbb{Z}_p$ ($p$ Primzahl), $f$ irreduzibel in $\mathbb{Z}_p[x]$ vom $Grad\ n$, so ist
$Z_p[x]/(f) = (\mathbb{Z}_p[x]_n, +, \odot_f)$ ein Körper mit $p^n$ Elementen.
Beweis: Folgt aus 1.26.

## 1.30 Beispiel

Körper der Ordnung 4: $f = x^2 + x + 1 \in \mathbb{Z}_2[x]$ ist irreduzibel, da es nicht in zwei Faktoren vom Grad 1 zerlegt werden kann, denn sonst hätte es eine Nullstelle, da Polynome von Grad 1 eine Nullstelle haben. $f$ hat aber keine Nullstellen in $\mathbb{Z}_2$.

| $\odot_f$ | 0 | 1 | $x$ | $x+1$ |
|---|---|---|---|---|
| 0 | 0 | 0 | 0 | 0 |
| 1 | 0 | 1 | $x$ | $x+1$ |
| $x$ | 0 | $x$ | $x+1$ | 1 |
| $x+1$ | 0 | $x+1$ | 1 | $x$ |

$f \equiv 0\ mod\ f$, d.h.
$x^2 + x + 1 \equiv 0\ mod\ f$, also
$x^2 \equiv x + 1\ mod\ f$

## 1.31 Bemerkung

a) Zu jeder Primzahl $p$ und jeder natürlichen Zahl $n$ existiert ein irreduzibles Polynom vom Grad $n$ in $\mathbb{Z}_p[x]$, also auch ein Körper der Ordnung $p^n$.

b) Ist $K$ ein endlicher Körper, so existiert Primzahl $p$ und $n \in \mathbb{N}$ mit $|K| = p^n$.
$p = o(1)$ in $(K, +) : p$ ist minimal mit $\underbrace{1 + 1 + ... + 1}_{\leftarrow p \rightarrow} = 0$.

c) $K, L$ endliche Körper, $|K| = |L|$, so ist $K \cong L$.
D.h. es existiert bijektive Abbildung $\varphi : K \to L$ mit
$\varphi(k_1 + k_2) = \varphi(k_1) + \varphi(k_2)$
$\varphi(k_1 k_2) = \varphi(k_1)\varphi(k_2) \quad \forall \quad k_1, k_2 \in K$.

d) Ist K endlicher Körper mit $|K| = m$, so ist $(K^*, \cdot)$ eine zyklische Gruppe, d.h. es existiert $g \in K$ mit $K^* = \{g^0, g, ..., g^{m-2}\}$

(Beweis: z.B. in [15], Kap. 6)

# 2 Arithmetische Algorithmen und deren Komplexität

Der (Zeit-)Aufwand zahlentheoretischer Algorithmen wird gemessen:

- in der Anzahl der arithmetischen Operationen (Additionen, Multiplikationen).

oder

- in der Anzahl der Bitoperationen.

Komplexität: worst-case-complexity $f(n)$
Algorithmus benötigt für jede Eingabe der Länge $n$ maximal $f(n)$ Operationen.
Input: natürliche Zahlen $m$, $m$ ist binär oder dezimal, aber nicht unär (Anzahl an Strichen) codiert. Die Inputlänge für $m$ ist $log_2(m)$.

## 2.1 Definition

$f, g : \mathbb{N} \to \mathbb{R}_{>0}$:
$f \in O(g) \Leftrightarrow \exists c > 0 : f(n) \leq c \cdot g(n) \ \forall \ n \in \mathbb{N}$ (es genügt:$\forall \ n \geq n_0$)
Statt $f \in O(g)$ schreibt man auch: $f = O(g)$ bzw. $f(n) = O(g(n))$
Beachte: $n^2 = O(n^2)$ und $n^2 = O(n^5)$, aber $O(n^2) \neq O(n^5)$.
$2 + sin(n) = O(1)$, $O(1)$ = Menge der beschränkten Funktionen.

Wichtige Funktionen:

- $log_a(n), a = 2, 10, ... \quad log_a(n) = log_a(b) \cdot log_b(n)$
  $\Rightarrow log_a(n) = O(log_b(n)) \ \forall a, b > 1$
- $n^a, a > 0$
- $2^n$
- $n^n$

| $n$ | 10 | 100 | 1000 |
|---|---|---|---|
| $log_2(n)$ | 3,32 | 6,64 | 9,97 |
| $nlog_2(n)$ | 33,2 | 664 | $9,97 \cdot 10^3$ |
| $n^2$ | $10^2$ | $10^4$ | $10^6$ |
| $n^5$ | $10^5$ | $10^{10}$ | $10^{15}$ |
| $2^n$ | 1024 | $1,27 \cdot 10^{30}$ | $1,07 \cdot 10^{301}$ |
| $n^n$ | $10^{10}$ | $10^{200}$ | $10^{3000}$ |

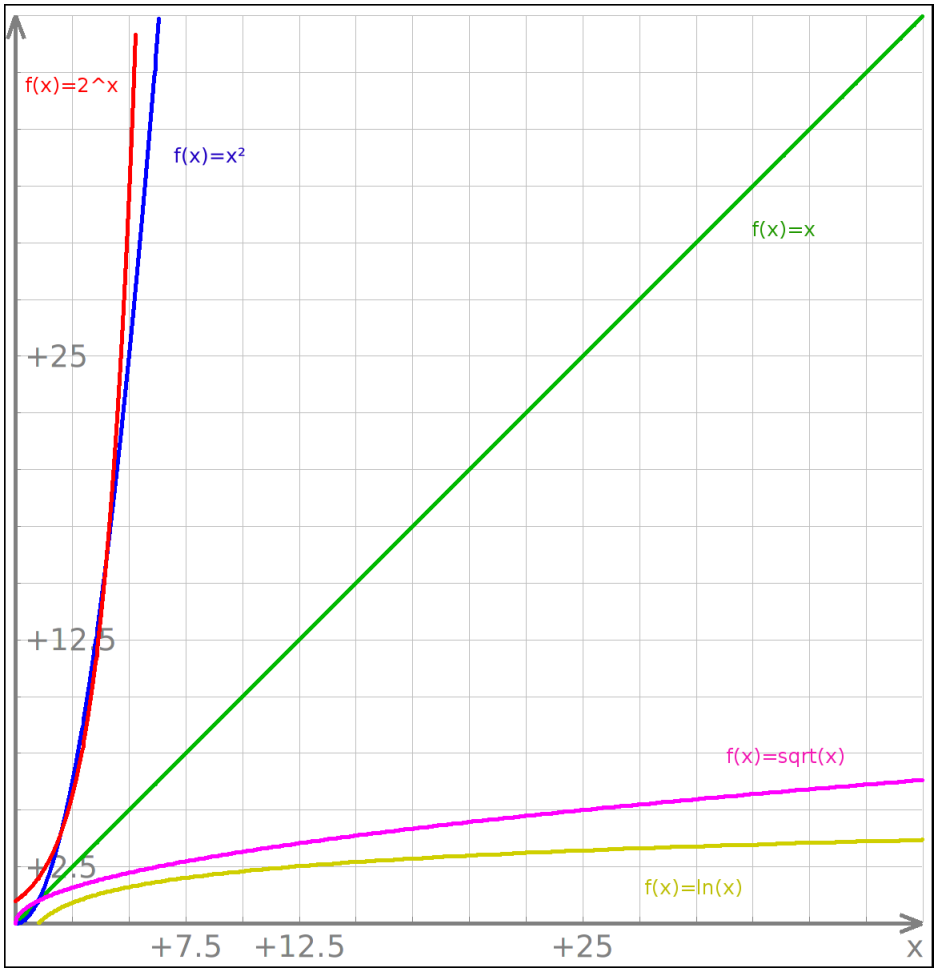



Abbildung 2.1: verschiedene Kurven

$n = 1000$
Benötigte Zeit bei 10 GFlops:

| | |
|---|---|
| $log_2(n)$ | $10^{-9} sec$ |
| $n$ | $10^{-7} sec$ |
| $n\ log(n)$ | $10^{-6} sec$ |
| $n^2$ | $10^{-4} sec$ |
| $n^5$ | $2,75h$ |
| $2^n$ | $3,4 \cdot 10^{283} Jahre$ |

Zum Vergleich: Alter des Universums $10^{10} - 2 \cdot 10^{10}$ Jahre.

## 2.2 Satz

$n, m \in \mathbb{N}$ in Binärdarstellung.

a) Die Berechnung von $n \pm m$ erfordert $O(max(log\ n, log\ m))$ viele Bitoperationen.

b) Die Berechnung von $nm$ erfordert nach der klassischen Methode $O((log\ n)\ (log\ m))$ viele Bitoperationen.

c) Die Berechnung von $nm, n \geq m$ nach dem Schönhage-Strassen-Algorithmus erfordert $O(log\ n(log\ n(log\ n))(log\ n(log\ n(log\ n))))$ viele Bitoperationen.

d) Division mit Rest von $n$ durch $m$ $(n \geq m)$ erfordert $O(log\ n(log\ n - log\ m + 1))$ viele Bitoperationen.

Beweis:

a) und b) klar

c) Für Schönhage-Strassen-Algorithmus (mit Hilfe FFT) vergleiche:
[16] (Kap. 8)
[3] (Kap. 9)
[4] (Kap. 4)

d) [5] (Kap. 3.2)

Also:
Ein Algorithmus, dessen Komplexität bezüglich der Anzahbl der arithm. Operationen polynomial beschränkt ist, hat auch bezüglich der Anzahl der Bitoperationen polynomial beschränkte Komplexität (anderes Polynom!), falls die Länge der auftretenden Zahlen polynomial in der Inputlänge beschränkt ist.

## 2.3 Satz

Der (erweitere) Euklidische Algorithmus für zwei Zahlen $a, b \in \mathbb{N}$ erfordert $O((loga) \cdot (logb))$ viele Bitoperationen.

Beweisidee:
Sei $a > b$. Man benötigt eine Abschätzung für die Anzahl der Divisionen mit Rest (Anzahl der Schleifendurchläufe): $O(logb)$

$l =$ Anzahl der Divisionen mit Rest.
$a_{i-1} = q_i a_i + a_{i+1}$ mit $i = 1, ..., l;\ a_0 = a, a_1 = b$
Es folgt: $a_{i-1} \geq a_i + a_{i+1} > 2a_{i+1}$

$$\prod_{2 \leq i < l} a_{i-1} > \prod_{2 \leq i < l} 2a_{i+1} = 2^{l-2} \prod_{2 \leq i < l} a_{i+1}$$

$a_1 a_2 > 2^{l-2} a_{l-1} a_l$. $a_{l-1} \geq 2 \ \Rightarrow 2^{l-2} < \frac{a_1 a_2}{a_{l-1} a_l} \leq \frac{a_1^2}{2}$, $2^{l-1} \leq a_1^2 (a_1 = b), l - 1 < 2log_2(b)$

Genauer Beweis: siehe [16] Kap. 3 bzw. [4]

## 2.4 Bemerkung

Mit 2.2 und 2.3 sieht man: Arithmetische Operationen in $(\mathbb{Z}_n, \oplus, \odot)$ (einschließlich der Invertierung in $\mathbb{Z}_n^*$) sind in $O((logn)^2)$ Bitoperationen durchführbar.

## 2.5 Satz

Modulare Exponentiation ($a^e \ mod \ n, 0 \leq a < n$) ist mit $O\,(log(e))$ vielen Multiplikationen in $\mathbb{Z}_n$ berechenbar. (Methode des iterierten Quadrierens)

Beweis:
$e = 2^k + e_{k-1} 2^{k-1} + ... + e_1 2 + e_0, e_i \in 0, 1$ (Binärdarstellung)
$a^e = (...((a^2 a^{e_{k-1}})^2 a^{e_{k-2}})^2 ... \ a^{e_1})^2 a^{e_0}$

Das liefert folgenden Algorithmus:

$b = a$
For $i = k-1,\ k-2, \ldots, 0$ do
  if $a_i = 1$ then $b = b^2 \cdot a \ mod \ n$
  else $b = b^2 \ mod \ n$

Output: $b = a^e \ mod \ n$.

## 2.6 Satz

$f, g \in K[x], Grad(f) = n \geq Grad(g) = m$, so erfordert der erweiterte Euklidische Algorithmus für $f$ und $g$
$O(m)$ Invertierungen in $K$

und $O(nm)$ Multiplikationen und Additionen in K.

Beweis: [16] (Kap. 3)

# 3 Primzahltests - Die „klassischen“ Methoden

Ist $n \in \mathbb{N}$, so $n = p_1^{e_1} ... p_r^{e_r}$, $p_i$ paarweise verschiedene Primzahlen, $e_i > 0$. Die Darstellung ist (bis auf die Reihenfolge) eindeutig.

## 3.1 Test auf Divisoren (trial divisions)

Methode: Man verwendet nacheinander Testdivisoren, um eine teilweise oder vollständige Faktorisierung von $n$ zu erhalten.

Testdivisoren: Z.B. alle Primzahlen $\leq \sqrt{n}$. ($n = ab$, so $a \leq \sqrt{n}$ oder $b \leq \sqrt{b}$). Wenn keine dieser Primzahlen $n$ teilt, so ist $n$ eine Primzahl.
I.d.R. hat man keine Liste aller Primzahlen $\leq \sqrt{n}$. Daher werden auch gewisse zusammengesetzte Zahlen als Testdivisoren verwendet.

Typisches Vorgehen: $m$ erste Primzahlen $p_1, ..., p_m \leq \sqrt{n}$. Bsp.: $m = 3,\ p_1 = 2, p_2 = 3, p_3 = 5$. Teile solange durch 2, 3, 5, bis es nicht mehr geht. Liefert $n'$ teilerfremd zu 30. $n = 2^{a_1} 3^{a_2} 5^{a_3} n'$.
Teiler von $n'$ sind teilerfremd zu 30, kongruent zu $1, 7, 11, 13, 17, 19, 23, 29$ *mod* 30. Die Abstände der zu testenden Zahlen wiederholen sich periodisch *mod* 30. Man merkt sich die Abstände. Ablauf: Beginne Division durch 7, addiere zu 7 die 4, liefert 11, dividieren, add, div, ...
Man erhält das sogenannte 'Rad' (4, 2, 4, 2, 4, 6 , 2, 6) als eine endliche Folge von Additionsinstruktionen, die beliebig oft angewendet werden kann (zyklisch). Die entstehenden Zahlen sind die Testdivisoren.
Aufwand: $O(\sqrt{n})$ Divisionen

## 3.2 Sieb des Eratosthenes

(Eratosthenes, ca. 284-200 v.Chr.)

Methode: Bestimme allein durch Additionen sämtliche Primzahlen $\leq n$.
Tabelle der Länge $n$-1 (entspricht den Zahlen von 2 bis $n$). Am Anfang bekommt jedes Feld den Eintrag 1. Lasse die 1 im ersten Feld stehen und gehe in 2er Schritten durch die Tabelle und ändere dort die 1 zur 0. Gehe zur ersten 1 rechts von der ersten 1 (entspricht 3). Gehe nun in 3er Schritten durch die Tabelle und setze erneut alle Felder auf 0 (eine vorhandene 0 bleibt 0). Fahre in dieser Weise fort.
Bei jedem Durchgang entspricht das erste Feld mit einer 1 einer Primzahl $p$; geändert

werden die Einträge in den Feldern $mp \leq n$ zu 0. Sind schon alle Eintrage $mp \leq n = 0$ (es wird nichts geändert), so ist $p^2 > n$. An dieser Stelle kann man aufhören. Alle Felder mit Einsen gehören jetzt zu Primzahlen.

Beweis:
Sei $p$ wie oben, d.h. alle Einträge in den Feldern $2p,\ 3p, \ldots \leq n$ seien schon gleich 0. Dann ist $p^2 > n$. Wenn Eintrag 1 bei Zahl $q > p$ steht ($q \leq n$), so ist $q$ durch keine Primzahl $\leq p$ teilbar. Angenommen, $q$ ist durch Primzahl $r$ teilbar, $r < q$. Dann $r > p$ und $\frac{q}{r} > p$, also $q > p^2 > n$, Widerspruch.

Das Sieb des Eratosthenes erfordert ca. $\sum_{p \leq \sqrt{n}} \frac{n}{p} = O(n\ log(log(n)))$ Additionen. Vgl. [17] Theorem 427

Durch clevere Tricks: Sieb mit $O(\frac{n}{log\ log\ n})$ Additionen (Mairson, Pritchard, 1981).

Verwendet man das Sieb des Eratosthenes als Primzahltest, so hört man auf, wenn das letzte Feld (für die Zahl $n$) eine Null enthält (dann $n$ zusammengesetzt und kleinster Primteiler bekannt). Wenn dies nicht geschieht, so lange fortfahren, wie oben beschrieben (dann $n$ Primzahl).

## 3.3 Satz (Fermat)

Sei $n \in \mathbb{N},\ n \geq 2$

a) $n$ ist eine Primzahl $\Leftrightarrow a^{n-1} \equiv 1(mod\ n)$ für alle $a \in \mathbb{N}, 2 \leq a \leq n-1$

b) $n$ ist eine Primzahl $\Rightarrow a^n \equiv a(mod\ n)$ für alle $a \in \mathbb{Z}$

Beweis: a) $\Rightarrow$: Kleiner Satz von Fermat (1.10b)
$\Leftarrow$: Angenommen $n$ ist keine Primzahl, dann existiert eine Primzahl $p \mid n$ mit $2 \leq p \leq n-1$. Setze nun $p$ für $a$ ein: $p^{n-1} \equiv 1(mod\ n), p|n$ und $n|p^{n-1} - 1 \Rightarrow p|p^{n-1} - 1$ und $p|p^{n-1} \Rightarrow p|1$, Widerspruch.
b) Falls $n \nmid a$, so $ggT(a,n) = 1 : a^{n-1} \equiv 1(mod\ n) \Rightarrow a^n \equiv a(mod\ n)$.
Falls $n \mid a$, so $a \equiv 0(mod\ n), a^n \equiv 0(mod\ n) \Rightarrow a^n \equiv a(mod\ n)$

## 3.4 Fermat-Test

Sei $n > 2$.
Wähle $2 \leq a \leq n-1$. Berechne $b := a^{n-1} mod\ n$.

- Ist $b \neq 1$, so ist $n$ keine Primzahl (3.3a)
- Ist $b = 1$, so wähle ein neues $a$.

Ist $a^{n-1} mod\ n = 1$ für alle $a \in \{2, ..., n-1\}$, so ist $n$ eine Primzahl.
Komplexität: $O(n)$ Exponentiationen. Exponentieller Algorithmus: $n = 2^{log\ n}$, wobei Inputlänge: $log\ n$.

Frage: Muss man tatsächlich alle $2 \leq a \leq n-1$ testen, bis man sicher weiß, dass $n$ Primzahl ist.
Bei der Wahl von $a$ wird man zunächst $ggT(a,n) = 1$ testen. Falls $ggT(a,n) \neq 1$, so ist $n$ zusammengesetzt.

Frage: Was kann man über natürliche Zahlen $n$ sagen, mit der folgenden Eigenschaft: $a^{n-1} \equiv 1(mod\ n)$ für alle $2 \leq a \leq n-1$ mit $ggT(a,n) = 1$?

## 3.5 Definition

Sei $n$ zusammengesetzt, $2 \leq a \leq n-1, ggT(a,n) = 1$.
$n$ heißt *Pseudoprimzahl zur Basis* $a$, falls $a^{n-1} \equiv 1(mod\ n)$

Beispiel: $341 = 11 \cdot 31, 2^{340} \equiv 1(mod\ 341)$: 341 ist eine Pseudoprimzahl zur Basis 2.
$91 = 7 \cdot 13, 3^{90} \equiv 1(mod\ 91)$: 91 ist eine Pseudoprimzahl zur Basis 3.

Wie groß ist die Chance, dass eine zusammengesetzte Zahl eine Pseudoprimzahl zu Basis $a$ ist?

## Satz (Erdös, 1950)

(Paul Erdös, 1913 - 1996)

Sei $a \geq 2, a \in \mathbb{N}$.
Sei $\pi(x)$ = Anzahl der Primzahlen $\leq x$ (Primzahlfunktion)
Sei $\pi_a(x)$ = Anzahl der Peudoprimzahlen zur Basis $a$, die $\leq x$ sind.
$lim_{x \to \inf} \frac{\pi_a(x)}{\pi(x)} = 0$ („relativ wenige“ Pseudoprimzahlen zur Basis $a$ im Vergleich zu Primzahlen.)

Andererseits: Zu jedem $a \geq 2$ gibt es unendlich viele Pseudoprimzahlen zur Basis $a$.
([3] Th. 3.3.4)

## 3.6 Definition

Eine zusammengesetzte Zahl $n$ heißt *Carmichael-Zahl*, falls $n$ Pseudoprimzahl zu jeder Basis $a$, $2 \leq a \leq n-1, ggT(a,n) = 1$.
(Carmichael 1912, Korselt 1899)

## Satz (Alford, Granville, Pomerance, 1994)

Sei $C(x)$ = Anzahl der Carmichael-Zahlen $\leq x$. Es existiert $x_0$ mit $C(x) > x^{\frac{2}{7}}$ für alle $x \geq x_0$.
Insbesondere folgt: Es existieren unendlich viele Carmichael-Zahlen.

Kleinste Carmichael-Zahl: $561 = 3 \cdot 11 \cdot 17$.

Im Vergleich dazu:

## Primzahlsatz (Hadamard; de la Vallée Poussin; 1896)

(J. Hadamard, 1865-1963; C.J.G.N. de la Vallée Poussin, 1866-1962)

$\pi(x) \sim \frac{x}{ln\ x}$ $\quad$ ($\lim\limits_{x\to\infty} \frac{\pi(x)}{x(ln(x))} = 1$, wobei $\frac{x}{ln(x)} \leq \pi(x)$ für $x \geq 11$).

Beispiel: $\pi(10^8) = 5761455$ und $[\frac{10^8}{ln(10^8)}] = 5428681$

## 3.7 Satz

Sei $n$ eine zusammengesetzte Zahl. Dann sind äquivalent

1. $n$ ist Carmichael-Zahl.
2. $a^{n-1} \equiv 1(mod\ n)$ für alle $n \in \mathbb{Z}$ mit $ggT(a,n) = 1$.
3. $a^n \equiv a(mod\ n)$ für alle $a \in \mathbb{Z}$.
4. Für alle Primzahlen $p$ mit $p \mid n$ gilt: $p^2 \nmid n$ und $p-1 \mid n-1$.

Beweis:

(1) $\Rightarrow$ (2): Sei $a \in \mathbb{Z}$, $ggT(a,n) = 1$. Sei $a = kn + r$, $1 \leq r \leq n-1$.
Dann $ggT(r,n) = 1$. Da $a \equiv r(mod\ n)$, ist $a^{n-1} \equiv r^{n-1}(mod\ n)$.
Nach Voraussetzung ist $r^{n-1} \equiv 1(mod\ n)$, also auch $a^{n-1} \equiv 1(mod\ n)$.

(2) $\Rightarrow$ (4): Sei $p$ eine Primzahl, $p \mid n$.
Da $\mathbb{Z}_p^*$ zyklisch ist (1.31d), existiert $b$, $1 \leq b \leq p-1$, mit $o(b) = p-1$ (Ordnung bezüglich Multiplikation),
d.h. $b^{p-1} \equiv 1(mod\ p)$ aber $b^i \not\equiv 1(mod\ p)$ für alle $1 \leq i \leq p-1$.
Seien $p_2, \ldots, p_s$ die übrigen Primteiler von $n$. Nach dem Chinesischen Restsatz (1.11) existiert $a \in \mathbb{Z}$ mit $a \equiv b(mod\ p)$ und $a \equiv 1(mod\ p_j)$, $j = 2, \ldots, s$.
Da $ggT(b,p) = 1$, ist folglich $ggT(a,n) = 1$. Außerdem $a^i \equiv b^i(mod\ p)$ für alle $i$, d.h. $o(a) = p-1$ (in $(\mathbb{Z}_p^*)$.
Nach Voraussetzung ist $a^{n-1} \equiv 1(mod\ n)$, also auch $a^{n-1} \equiv 1(mod\ p)$. Nach

(1.7d) ist daher $p-1 = o(a) \mid n-1$.
Angenommen, $p^2 \mid n$.
Es ist $(p+1)^p = p^p + \binom{p}{1}p^{p-1} + \cdots + \binom{p}{p-1}p + 1$. Alle Terme auf der rechten Seite (bis auf 1) sind durch $p^2$ teilbar. Also ist die Ordnung von $p+1$ in $(\mathbb{Z}_{p^2})^*$ genau $p$. Mit dem Chinesischen Restsatz erhält man ein $a \in \mathbb{Z}$ mit

$$a \equiv p+1 (mod\ p^2) \text{ und } a \equiv 1 (mod\ p_j), \quad j = 2, \ldots, s$$

Also ist $ggT(a,n) = 1$ und nach Voraussetzung ist $a^{n-1} \equiv 1 (mod\ n)$, also auch $a^{n-1} \equiv 1 (mod\ p^2)$. Da $a$ und $p+1$ wegen $a \equiv p+1\ (mod\ p^2)$ die gleiche Ordnung in $(\mathbb{Z}_{p^2})^*$ haben, also $p$, folgt $p \mid n-1$. Dies ist ein Widerspruch zu $p \mid n$.

(4) $\Rightarrow$ (3): Nach Voraussetzung ist $n = p_1 \cdots p_s$, $p_i$ Primzahlen, $p_i \neq p_j$ für $i \neq j$.
Sei o.B.d.A. $ggT(a,n) = p_1 \ldots p_r$, $0 \leq r \leq s$ ($r = 0$, falls $ggT(a,n) = 1$). Es ist $a^n \equiv a \equiv 0 (mod\ p_j)$ für $j = 1, \ldots, r$.
Nach dem Satz von Fermat (3.3 e) ist
$a^{p_j - 1} \equiv 1 (mod\ p_j)$ für $j = r+1, \ldots, s$, also $a^{n-1} \equiv 1 (mod\ p_j)$, da nach Voraussetzung $p_j - 1 \mid n-1$.
Daher ist auch $a^n \equiv a (mod\ p_j)$ für $j = r+1, \ldots, s$.
Aus $n = p_1 \cdots p_s$, $p_i \neq p_j$, folgt dann $a^n \equiv a (mod\ n)$.

(3) $\Rightarrow$ (1): Ist $ggT(a,n) = 1$, so existiert $a^{-1}$ in $(\mathbb{Z}_n)^*$.
Da nach Voraussetzung $a^n \equiv a (mod\ n)$, folgt $a^n \cdot a^{-1} \equiv a \cdot a^{-1}\ (mod\ n)$, d.h $a^{n-1} \equiv 1 (mod\ n)$.

Aus 3.7 folgt, dass alle Primteiler einer Carmichael-Zahl ungerade sind und dass es mindestens 3 verschiedene Primteiler gibt.

Gegeben: $n$. $a^{n-1} \equiv 1 (mod\ n)$ für alle $a \leq n-1, ggT(a,n) = 1 \Rightarrow n$ Primzahl oder Carmichael-Zahl.
Dieses Kriterium muss verfeinert werden, um Primzahltest zu erhalten.

## Miller-Rabin-Test (Motivation)

$p$ Primzahl. Nach Fermat: $a^{p-1} \equiv 1 (mod\ p)$, d.h. $a^{p-1}\ mod\ p = 1$
Sei $p - 1 = 2^s d, 2 \nmid d$.

$a^{p-1} = a^{2^s d} = (a^{2^{s-1} d})^2 \equiv 1\ mod\ p$.

Also ist $a^{2^{s-1} d}\ mod\ p$ eine Wurzel aus 1 in $\mathbb{Z}_p$, d.h. eine Nullstelle von $x^2 - 1 \in \mathbb{Z}_p[x]$.
Über Körpern (wie $\mathbb{Z}_p$) hat ein Polynom vom *Grad* 2 höchstens 2 Nullstellen.

Also sind 1 und -1 (= $p$-1 in $\mathbb{Z}_p$) die einzigen Wurzeln von 1 in $\mathbb{Z}_p$,
d.h. $a^{2^{s-1} d} \equiv \pm 1 (mod\ p)$.

Hat $n$ mehrere verschiedene Primteiler, so hat 1 mehr als 2 Wurzeln $mod\ n$. Ist z.B. $n = p \cdot q$ ($p, q$ verschiedene Primzahlen), so gibt es nach dem Chinesischen Restsatz (1.11) vier Zahlen $1 \leq x_1, x_2, x_3, x_4 < n$ mit
$x_1 \equiv 1(mod\ p),\ x_1 \equiv 1(mod\ q)$ (also $x_1 = 1$)
$x_2 \equiv -1(mod\ p),\ x_2 \equiv -1(mod\ q)$ (also $x_2 = n - 1 \equiv -1(mod\ n)$)
$x_3 \equiv 1(mod\ p),\ x_3 \equiv -1(mod\ q)$
$x_4 \equiv -1(mod\ p),\ x_4 \equiv 1(mod\ q)$.

Dann ist $x_i^2 \equiv 1(mod\ n)$ für $i = 1, \ldots, 4$.

Bsp.
$n = 15$:
$1^2 \equiv 1(mod\ 15)$
$(-1)^2 = 14^2 \equiv 1(mod\ 15)$
$4^2 \equiv 1(mod\ 15)$
$11^2 = 1(mod\ 15)$,
1, 14, 4, 11 sind die Wurzeln aus 1 in $\mathbb{Z}_{15}$.

Wenn also $n$ keine Primzahl ist, so muss (in der obigen Beziehung) $a^{2^{s-1} \cdot d}$ nicht notwendig $\equiv \pm 1(mod\ n)$ sein. Damit kann man den Fermat-Test verschärfen.

## 3.8 Satz

$p$ Primzahl, $p \neq 2, a \in \mathbb{Z}, ggT(a, p) = 1$ und $p - 1 = 2^s d, 2 \nmid d$. Dann folgt:
Entweder $a^d \equiv 1(mod\ p)$
oder $\exists\ r \in \{0, ..., s-1\}$ mit $a^{2^r d} \equiv -1(mod\ p)$ (Dann: $a^{2^{r+1} d} \equiv 1(mod\ p)$)

Beweis:
Das kann man wie in der Vorbemerkung beweisen oder folgendermaßen:
$a^{p-1} - 1 = a^{2^s d} - 1$
$= \underbrace{(a^d - 1)(a^d + 1)}_{a^{2d}-1}(a^{2d} + 1)(a^{4d} + 1)(a^{8d} + 1) + ... + (a^{2^{s-1} d} + 1)$
$a^{p-1} \equiv 1(mod\ p) \Rightarrow p | a^{p-1} - 1$
$\Rightarrow p | a^d - 1$(d.h. $a^d \equiv 1\ mod\ p$) oder $p | a^{2^r d} + 1$ für ein $r \in \{0, ..., s-1\}$

## 3.9 Definition

$n \geq 3$ ungerade, $2 \leq a \leq n - 1, ggT(a, n) = 1, n - 1 = 2^t e, 2 \nmid e$.

a) Ist $n$ zusammmengesetzt und ist
   - entweder $a^e \equiv 1(mod\ n)$
   - oder $a^{2^r e} \equiv -1(mod\ n)$ für ein $r \in \{0, ..., t-1\}$,

   so heißt $n$ *starke Pseudoprimzahl* bzgl. $a$. ($n$ ist dann auch Pseudoprimzahl zur Basis $a$, da $a^{n-1} \equiv 1(mod\ n)$)

b) Ist $a^e \not\equiv 1(mod\ n)$ und $a^{2^r e} \not\equiv 1(mod\ n)$ für alle $r \in \{0, ..., t-1\}$, so ist $n$ zusammengesetzt. $a$ heißt dann *Zeuge* gegen die Primzahleigenschaft von $n$.

Beispiel: $n = 91 = 7 \cdot 13$, $n - 1 = 2 \cdot 45$. Zu testen, ob $a^{45} \equiv 1(mod\ 91)$ oder $a^{45} \equiv -1(mod\ 91)$.
$10^{45} \equiv -1(mod\ 91)$ 91 ist eine starke Pseudoprimzahl zur Basis 10.
$3^{45} \equiv 27(mod\ 91)$ 3 ist ein Zeuge gegen die Primzahleigenschaft von 91.
$3^{90} \equiv 1(mod\ 91)$ 91 ist eine Pseudoprimzahl zur Basis 3, aber keine starke Pseudoprimzahl zur Basis 3.

Frage: Wenn $n$ zusammengesetzt ist, gibt es dann Zeugen gegen die Primzahleigenschaft von $n$?
Antwort: Ja, sogar viele.

## 3.10 Satz (Monier, Rabin; 1980)

Sei $n > 9$ eine ungerade zusammengesetzte Zahl. Dann gibt es mindestens $3/4\varphi(n)$ Zeugen gegen die Primzahleigenschaft von $n$.

Beweis: Wir zeigen nur, dass es mindestens $\varphi(n)/2$ Zeugen gegen die Primzahleigenschaft von $n$ gibt.

1. Sei zunächst $n = p_1 \cdot \cdots \cdot p_l, p_i$ Primzahlen, $p_i \neq p_j$ für $i \neq j$, $n - 1 = 2^t \cdot e, 2 \nmid e$.
   Ist jedes $a$, $2 \leq a \leq n-2$ mit $ggT(a, n) = 1$ Zeuge gegen die Primzahleigenschaft von $n$, so fertig ($\varphi(n) - 2 \geq \varphi(n)/2$, da $\varphi(n) = \varphi(p_1) \cdots \varphi(p_l) = (p_1 - 1) \cdots (p_l - 1) > 4$, denn $l \geq 2$ ungerade)
   OBdA: Also gibt es Nichtzeugen, das heißt, $a \in \mathbb{Z}, 2 \leq a \leq n-2$, $ggT(a, n) = 1$, so dass $a^e \equiv 1(mod\ n)$ (*) oder $a^{2^r \cdot e} \equiv -1(mod\ n)$ (**) für ein $r \in \{0, 1, \ldots, t-1\}$. Existiert ein $a$ mit (*), dann erfüllt $n - a(\equiv -a(mod\ n))$ Bedingung (**) mit $r = 0$. Sei $k$ der größte Wert, für den es $a$ mit $2 \leq a \leq n-2$ und $ggT(a, n) = 1$ gibt mit $a^{2^k \cdot e} \equiv -1(mod\ n)$; setze $m = 2^k \cdot e$.
   Setze $L := \{b \in \mathbb{Z}_n : ggT(b, n) = 1, b^m \equiv \pm 1(mod\ n)\}$. Jeder Nichtzeuge liegt in $L$. $L$ ist Untergruppe von $(\mathbb{Z}_n^*, \cdot)$. Zeige: $L$ ist echte Untergruppe von $\mathbb{Z}_n^*$.
   (Denn dann: #Nichtzeugen $\leq |L| \overset{1.6}{\leq} \frac{|\mathbb{Z}_n^*|}{2} = \frac{\varphi(n)}{2}$)
   Wähle $a$ mit $2 \leq a \leq n-2$, $ggT(a, n) = 1$ und $a^m \equiv -1(mod\ n)$. Chinesischer Restsatz (1.11): Es existiert $b$ mit $1 \leq b \leq n-1$ mit $b \equiv a(mod\ p_1)$, $b \equiv a^2(mod\ p_i)$, $i = 2, \ldots, l$.
   Dann $b^m \equiv a^m \equiv -1(mod\ p_1), b^m \equiv a^{2m} \equiv 1(mod\ p_i), i = 2, \ldots, l$
   Klar: $b \in \mathbb{Z}_n^*$.
   Angenommen $b\ a^2\ mod\ n \in L$.
   Dann $b^m a^{2m} \equiv 1$ oder $-1(mod\ n)$. $a^{2m} \equiv 1(mod\ n)$. Also $b^m \equiv 1$ oder $-1(mod\ n)$.
   Angenommen
   - $b^m \equiv 1(mod\ n) \Rightarrow b^m \equiv 1(mod\ p_1)$.
     Andererseits $b^m \equiv -1(mod\ p_1)$, Widerspruch, da $p_1 \neq 2$.

· $b^m \equiv -1(mod\ n) \Rightarrow b^m \equiv -1(mod\ p_2)$.
Andererseits $b^m \equiv 1(mod\ p_2)$. Widerspruch, da $p_2 \neq 2$.

Damit ist Fall (a) abgeschlossen.

2. Allgemeiner Fall:
Ist $n$ Carmichael-Zahl, so fertig mit a) und (3.7). Ist $n$ keine Carmichael-Zahl, so existiert $a \in \mathbb{Z}$, $2 \leq a \leq n-2$, $ggT(a,n) = 1$ mit $a^{n-1} \equiv 1(mod\ n)$. Setze

$$K = \{b \in \mathbb{Z}_n : 1 \leq b \leq n-1, ggT(b,n) = 1, b^{n-1} \equiv 1(mod\ n)\} \subseteq \mathbb{Z}_n^*$$

Alle Nichtzeugen liegen in $K$. $a \notin K$. $K$ echte Untergruppe von $Z_n^*$.

## 3.11 Miller-Rabin-Test

*(Miller, 1976; Rabin, 1976; Vorläufer: Selfridge, 1974)*

Sei $n \geq 3$ ungerade.

(1) Wähle $a \in \{2, ..., n-2\}$ zufällig.

(2) Bestimme $ggT(a,n)$. Gilt $ggT(a,n) \neq 1$, Ausgabe „$n$ ist zusammengesetzt“.
Falls $ggT(a,n) = 1$:

(3) Bestimme t mit $n-1 = 2^t e, 2 \nmid e$.

(4) $b = a^e\ mod\ n$

(5) Ist $b = 1$ oder $b = n-1$, so Ausgabe „$n$ ist Primzahl oder starke Pseudoprimzahl bzgl. der Basis $a$“.
Andernfalls setze $j$=1 und

(6) Wiederhole solange $j < t$:
$b = b^2\ mod\ n$.
Ist $b = n-1$, so $j = t+1$ und Ausgabe „$n$ ist Primzahl oder starke Pseudoprimzahl bzgl. der Basis $a$“,
ansonsten $j = j+1$

(7) Ist $j = t$, so Ausgabe „$n$ ist zusammengesetzt“.

Miller-Rabin mit Ausgabe „$n$ ist Primzahl“ statt „$n$ ist Primzahl oder starke Pseudoprimzahl“: probabilistischer Primzahltest (Monte-Carlo-Algorithmus)

- „$n$ ist zusammengesetzt“ (korrekt)
- „$n$ ist Primzahl“ (Fehlerwahrscheinlichkeit $\leq \frac{1}{4}$) - bei $k$-fachem Durchlauf: Fehlerwahrscheinlichkeit $\leq \frac{1}{4^k}$

$k$ Durchläufe von Monte-Carlo-Miller-Rabin: Wenn $n$ zusammengesetzt, so ist die Wahrscheinlichkeit für die Ausgabe „$n$ ist Primzahl“ $\leq \frac{1}{4^k}$.
Wir interessieren uns für die Wahrscheinlichkeit, dass $n$ Primzahl ist, falls M-C-M-R ausgibt „$n$ ist Primzahl“?
Wir brauchen zuerst einen Bereich $\{1, ..., N\}$, aus dem $n$ gewählt wird.
Zufallsvariable $X$ bezeichne das Ereignis, dass die zu testende Zahl $n \leq N$ zusammengesetzt ist. $\bar{X}$ bezeichne das Ereignis, dass $n$ Primzahl ist. Zufallsvariable $Y$ bezeichne das Ereignis, dass M-C-M-R nach $k$ Durchläufen ausgibt „$n$ ist Primzahl“.

$P(Y|X) \leq \frac{1}{4^k}$ ($n$ ist zusammengesetzt und Algorithmus sagt, es sei eine Primzahl.)
$P(\bar{X}) \approx \frac{1}{ln(N)}$ (Primzahlsatz: $\pi(N) \approx \frac{N}{ln(N)}$ siehe oben)
$P(X) \approx 1 - \frac{1}{ln(N)} \leq 1$, $P(Y) \geq P(\bar{X})$.
Wir suchen: $P(\bar{X}\,|Y) = 1 - P(X|Y)$.

Bayes'sche Formel: $P(X|Y) = \frac{P(Y|X)P(X)}{P(Y)} \leq \frac{\frac{1}{4^k}}{P(\bar{X})} = \frac{ln(N)}{4^k}$,
d.h. $P(\bar{X}\,|Y) \geq 1 - \frac{ln(N)}{4^k}$.
Soll $P(\bar{X}\,|Y) \geq 1 - \epsilon$ gelten, so wähle $k$ so, dass $\frac{ln(N)}{4^k} \leq \epsilon$, d.h. $k \geq \frac{ln(ln(N)) - ln(\epsilon)}{ln(4)}$.

## 3.12 Satz

Sei $0 < \epsilon < 1$. Sei $N \in \mathbb{N}$ und $k = \lceil \frac{ln(ln(N)) - ln(\epsilon)}{ln(4)} \rceil$. Wählt man eine ungerade Zahl $n$ zufällig aus $\{3, ..., N\}$, so gilt:
Gibt Monte-Carlo Miller-Rabin nach $k$ Durchläufen „$n$ ist Primzahl“ aus, so ist $n$ mit Wahrscheinlichkeit $\geq 1 - \epsilon$ eine Primzahl.

Beispiel: $N = 2^{500}, \epsilon = 10^{-3}$ (Wahrscheinlichkeit $\geq 0,999$) $\rightarrow k = 10$.

Tatsächlich gibt es in der Regel viel mehr Zeugen gegen die Primzahleigenschaft einer zusammengesetzten Zahl $n$ als $\frac{3\varphi(n)}{4}$. Daher sind die Wahrscheinlichkeitsaussagen eigentlich deutlich besser als die oben angegebenen; in der Praxis wird Miller-Rabin daher häufig nur mit einem oder zwei verschiedenen $a$ durchgeführt.

## 3.13 Bemerkung

a) Komplexität von einer Runde in 3.11: $O((log\ n)^3)$. Folgt aus Kapitel 2.

b) (Bach 1985) Gilt die verallgemeinerte Riemannsche Vermutung, so existiert zu jeder ungeraden zusammengesetzten Zahl $n$ ein Zeuge $a$ gegen die Primzahleigenschaft von $n$ mit $a < 2(ln\ n)^2$.
Teste alle $a \in \{2, ..., \lfloor 2(ln\ n)^2 \rfloor\}$. Wenn dann $n$ nicht als zusammengesetzt erkannt worden ist, dann ist $n$ eine Primzahl.
$\rightarrow$ deterministischer Primzahltest der Komplexität $O((log\ n)^5)$. Polynomialer Test, falls die verallgemeinerte Riemannsche Vermutung gilt.

## 3.14 Lemma

a) Ist $2^m - 1$ eine Primzahl, so ist $m$ eine Primzahl.

b) Ist $2^m + 1$ eine Primzahl, so ist $m = 2^n$.

Beweis:

a) Angenommen $m = rs$. $\quad 2^m - 1 = (2^r - 1)(2^{(s-1)r} + 2^{(s-2)r} + ... + 2^r + 2^0)$. $s$ muss nun 1 sein und $m$ somit eine Primzahl.

b) $m = 2^k d, 2 \nmid d$. $\quad 2^m + 1 = (2^{2^k} + 1)(2^{2^k(d-1)} - 2^{2^k(d-2)} + ... - 2^{2^k} + 2^0)$, da $d$ ist ungerade ist. Dann muss $d = 1$ sein.

## 3.15 Definition

a) Ist $p$ eine Primzahl, so heißt $M(p) = 2^p - 1$ *Mersenne-Zahl* (M. Mersenne, 1588-1648).

b) Ist $n \in \mathbb{N}_0$, so heißt $F_n = 2^{2^n} + 1$ *Fermat-Zahl*.

Primzahltests für Fermat-Zahlen beruhen auf:

## 3.16 Satz

(Lucas, 1876; F.E. Lucas, 1842-1891) Sei $m \in \mathbb{N}$. Dann gilt:
$m$ Primzahl $\Leftrightarrow \exists\, a, 1 \leq a \leq m-1$, mit $a^{m-1} \equiv 1 (mod\ m)$ und $a^{\frac{m-1}{q}} \not\equiv 1 (mod\ m)$ für alle Primteiler $q$ von $m$-1.
Beweis:

$\Rightarrow$ Fermat: $a^{m-1} \equiv 1 (mod\ m) \quad \forall\ 1 \leq a \leq m-1$.
$\mathbb{Z}_m$ Körper, $\mathbb{Z}_m^* = \{1, ..., m-1\}$ Gruppe bzgl. $\odot$. 1.31d: $\mathbb{Z}_m^*$ zyklisch.
$\mathbb{Z}_m^* =< a >= \{a^0, ..., a^{m-2}\} \qquad o(a) = m-1 \Rightarrow$ Behauptung

$\Leftarrow$ $a^{m-1} \equiv 1 (mod\ n) \Rightarrow a \in \mathbb{Z}_m^* (a^{-1} = a^{m-2} (mod\ n))$. $a^{\phi(m)} \equiv 1 (mod\ m)$.
$o(a) = m-1$ und $a^{\phi(m)} = 1$ (in $\mathbb{Z}_m^*$) $\underbrace{\Rightarrow}_{1.7d}$ $m-1 \mid \phi(m) \leq m-1$. $\phi(m) = m-1$.
$m$ Primzahl.

## 3.17 Korollar

$F_n = 2^{2^n} + 1$ Primzahl $\Leftrightarrow$ $\exists a, 1 \leq a \leq F_n - 1$ mit $a^{\frac{F_n-1}{2}} \equiv -1 (mod\ F_n)$.

Es reicht in 3.17, a=3 zu wählen:

## 3.18 Satz: (Pepin 1877, Proth 1878)

$F_n = 2^{2^n} + 1$ Primzahl $\Leftrightarrow$ $3^{\frac{F_n-1}{2}} \equiv 1 (mod\ F_n)$.
Beweis: [3]Th. 4.1.2.

## 3.19 Bemerkung

Es ist unbekannt, ob es unendlich viele Fermat-Primzahlen gibt.
Die einzig bekannten Fermat-Primzahlen sind: $F_0, ..., F_4$. Von 230 Fermat-Zahlen ist bekannt, dass sie zusammengesetzt sind. Eine vollständige Faktorisierung existiert von $F_0, ..., F_{11}$. $F_n$ ist zusammengesetzt für $5 \leq n \leq 32$. (Für $n = 14, 20, 22, 24$ ist kein Faktor bekannt.)
*http://www.prothsearch.net/fermat.html*

Primzahltests für Mersenne-Zahlen beruhen auf dem Lucas-Lehmer-Test (D. H. Lehmer, 1905-1991).
Grundlage: Kettenbruchentwicklung und Lucas-Folgen.

## 3.20 Lucas-Lehmer-Test für Mersenne-Zahlen

Sei $(v_k)_{k \geq 0}$ rekursiv definiert durch: $v_0 = 4, v_{k+1} = v_k^2 - 2$.
Sei $p$ eine ungerade Primzahl. $M(p) = 2^p - 1$ ist Primzahl $\Leftrightarrow M(p) \mid v_{p-2}$.
Beweis: [3]Th. 4.2.6.

## 3.21 Bemerkung

a) 3.20 $\rightarrow$ Primzahltest für $M(p)$; rechne $mod\ M(p)$.
$v_{p-2}\ mod\ M(p) = 0$? Problem: Größe der Zahlen.

b) Es ist unbekannt, ob unendlich viele Mersenne-Primzahlen existieren.
Derzeit sind 44 Mersenne-Primzahlen bekannt. Die Größte ist $M(32582667)$. September 2006 GIMPS-Projekt (Cooper, Boone)

M(1039) wurde faktorisiert *(März 2007)*
*http://www.mersenne.org*

# 4 Der AKS-Algorithmus

Agrawal, Kayal, Saxena (2002)

## 4.1 Satz

Sei $a \in \mathbb{Z}, n \in \mathbb{N}, n \geq 2, ggT(a,n) = 1$. Dann:
$n$ ist Primzahl $\Leftrightarrow (x+a)^n \equiv x^n + a (mod\ n)$
($(x+a)^n \equiv x^n + a (mod\ n)$, d.h. Gleichheit nach Reduktion der Koeffizienten $mod\ n$: Gleichheit in $\mathbb{Z}_n[x]$)

Beweis: In $\mathbb{Z}[x]$ : $(x+a)^n = x^n + \sum_{i=1}^{n-1} \binom{n}{i} a^i x^{n-i} + a^n$ (1.15c)
$\Rightarrow$: $n$ Primzahl: $a^n \equiv a (mod\ n)$ Fermat
$1 \leq i \leq n-1$ : $\binom{n}{i} = \frac{n!}{i!(n-i)!}$ ist durch $n$ teilbar, weil $n$ eine Primzahl ist, $\binom{n}{i} \equiv 0 (mod\ n)$
$\Leftarrow$: Angenommen $n$ sei keine Primzahl: Sei $q$ Primzahl mit $q \mid n$ (also $q < n$). $q^k \mid n, q^{k+1} \nmid n$.
Koeffizient von $x^q$ in $(x+a)^n$. $\binom{n}{n-q} a^{n-q} = \binom{n}{q} a^{n-q}$
$q^k \nmid \binom{n}{q} = \frac{n!}{(n-q)!q!} = \frac{(n-q+1)\ldots(n-1)n}{q!}$, denn $q \mid n$ und $(n-q+1)\ldots(n-1)$ teilerfremd zu $q$.
$q^k \nmid \binom{n}{q} a^{n-q}$, da $ggT(a,n) = 1$. $\quad n \nmid \binom{n}{q} a^{n-q}, \quad \binom{n}{q} a^{n-q}\ mod\ n \neq 0$.

Möglicher Primzahltest: Wähle $a$ mit $ggT(a,n) = 1$. $(a < n)$
Prüfe nach, ob alle Koeffizienten von $x^{n-1}, \ldots, x$ in $(x+a)^n$ durch $n$ teilbar sind. $a^n \equiv a (mod\ n)$ (Fermat-Test)
Komplexität (Koeffizientenvergleiche): $O(n) = O(2^{log\ n})$ - nicht polynomial.

Idee des AKS-Algorithmus:
Rechne in $(\mathbb{Z}_n[x]_r, +, \odot_{x^r-1}) = \mathbb{Z}_n[x]/(x^r - 1)$ (wie in 1.26 mit $\mathbb{Z}_n$ statt $K$) für geeignetes kleines $r$. D.h. man rechnet in $\mathbb{Z}_n[x]$ modulo $x^r - 1$.
Schreibweise: (*) $(x+a)^n \equiv x^n + a (mod\ x^r - 1, n)$, falls $(x+a)^n$ und $(x^n + a)$ modulo $x^r - 1$ übereinstimmen. $(x+a)^n\ mod\ x^r - 1$ und $(x^n + a)\ mod\ x^r - 1$ haben nur $r$ Koeffizienten, die man vergleichen muss.
Im AKS-Algorithmus wählt man $r$, das polynomial in $log(n)$ ist.
Man testet dann (*). Klar: Falls $(x+a)^n \equiv x^n + a (mod\ n)$, so auch $(x+a)^n \equiv x^n + a (mod\ x^r - 1, n)$. Die Umkehrung braucht nicht zu gelten. Agrawal, Kayal und Saxena zeigen aber, dass man bei geeignetem $r$ (s. oben) nur $k$ viele $a$ testen muss, wobei $k$ polynomial in $log(n)$, um sicher zu sein, ob $n$ Primzahl ist oder nicht.

Bezeichnung:

$r, n \in \mathbb{N}$ :
$(ggT(r,n) = 1) \quad o_r(n) = \textit{Ordnung von } n \textit{ modulo } r$ = kleinstes $d$ mit $n^d \equiv 1 (mod\ r)$
= Ordnung von $(n\ mod\ r)$ in $\mathbb{Z}_r^*$.
Beachte: $d \leq |\mathbb{Z}_r^*| \leq \varphi(r) \leq r - 1$

## 4.2 AKS-Algorithmus

Eingabe: $n > 1$.

1. Wenn $n = b^c$ für $b, c \in \mathbb{N}, c > 1$, so Ausgabe „$n$ ist zusammengesetzt“.
2. Finde das kleinste $r$ mit $ggT(r,n) = 1$ und $o_r(n) > 4(log\ n)^2$.
   (Man kann zeigen: $r < \lceil 16(log\ n)^5 \rceil$; siehe 4.5)
3. Wenn $1 < ggT(a,n) < n$ für ein $a < r$, so Ausgabe „$n$ ist zusammengesetzt“.
4. Wenn $r \geq n$, so Ausgabe „$n$ ist Primzahl“.
5. Für $a = 1, \ldots, \lfloor 2\sqrt{\varphi(r)}\ log\ n \rfloor$:
   Wenn $(x + a)^n \not\equiv x^n + a (mod\ x^r - 1, n)$, so Ausgabe „$n$ ist zusammengesetzt“.
6. Ausgabe „$n$ ist Primzahl“.

(Der Test in 1. ist in polynomialer Zeit möglich. Dazu testet man für $c = 2, \ldots, \lfloor log(n) \rfloor$, ob $n$ $c$-te Potenz ist. Dies geschieht durch binäre Suche (Intervallhalbierungsverfahren): Man startet mit dem Intervall $[u, v] = [1, n]$, bestimmt den „ganzzahligen Mittelpunkt“ $x = \lfloor \frac{v-u}{2} \rfloor$ und testet, ob $x^c = n, < n$ oder $> n$. Im ersten Fall ist man fertig, im zweiten setzt man $u = x$, im dritten $v = x$ und fährt dann mit dem neuen Intervall $[u, v]$ in derselben Weise fort. Spätestens nach $\lceil log(n) \rceil + 1$ Schritten haben die Intervallgrenzen Abstand 1, und der Algorithmus endet.)

## 4.3 Satz

AKS-Algorithmus gibt „$n$ ist Primzahl“ aus genau dann, wenn $n$ Primzahl ist.

Die eine Richtung des Satzes ist einfach zu beweisen:

## 4.4 Lemma

Ist $n$ Primzahl, so gibt AKS-Algorithmus „$n$ ist Primzahl aus“.

Beweis:

Falls $n$ Primzahl ist, so gibt der Algorithmus in den Zeilen 1 und 3 niemals „$n$ ist zusammengesetzt“ aus. Ist $n$ Primzahl, so gilt nach Satz 4.1 für alle $a$ mit $ggT(a,n)=1$, dass $(x+a)^n \equiv x^n + a (mod\ n)$, also auch $(x+a)^n \equiv x^n + a (mod\ x^r - 1, n)$.
Ist $n$ eine Primzahl, so gibt der Algorithmus in Zeile 5 nie „$n$ ist zusammengesetzt“ aus, denn dann ist $ggT(a,n)=1$ (nach Zeile 3) und daher $x^n + a \equiv (x+a)^n (mod\ n)$ (4.1), also auch $x^n + a \equiv (x+a)^n (mod\ x^r - 1, n)$.
Also gibt der Algorithmus in Zeile 4 oder 6 „$n$ ist Primzahl“ aus.

Wir zeigen jetzt den schwierigen Teil von Satz 4.3, nämlich:
Gibt der Algorithmus „$n$ ist Primzahl“ aus, so ist $n$ Primzahl.

Wir zeigen zunächst, dass der Algorithmus in Zeile 2 ein $r$ findet, und zwar „schnell“.

Dazu benötigen wir:
**S**atz (Nair, 1982) Ist $m \geq 9$, so ist $kgV(1,2,\ldots,m) \geq 2^m$.

(Der Beweis ist nicht sehr schwierig: siehe [18])

## 4.5 Lemma

Es gibt ein $r \leq \lceil 16(log\ n)^5 \rceil$ mit $o_r(n) > 4(log\ n)^2$.

Beweis:
Sei $k := 4(log\ n)^2$. Seien $r_1, \ldots, r_t$ alle diejenigen Zahlen, für die gilt: $o_{r_i}(n) \leq k$.
(Für diese $r_i$ gilt: $r_i \mid n^{d_i} - 1$ für ein $d_i \leq k$; also gibt es nur endlich viele.)
Jedes dieser $r_i$ teilt das folgende Produkt
$\prod_{i=1}^{\lfloor k \rfloor}(n^i - 1) < n \cdot n^2 \cdot \cdots \cdot n^{\lfloor k \rfloor} = n^{\frac{\lfloor k \rfloor \cdot (\lfloor k \rfloor + 1)}{2}} \leq n^{k^2} = n^{16(log\ n)^4} = 2^{16(log\ n)^5}$.
Nach Satz von Nair: $kgV(1,2,\ldots,\lceil 16 \cdot (log\ n)^5 \rceil) \geq 2^{16 \cdot (log\ n)^5}$.
Also gibt es eine Zahl $r < \lceil 16 \cdot (log\ n)^5 \rceil$, die $\prod_{i=1}^{\lfloor k \rfloor}(n^i - 1)$ nicht teilt. Dann: $o_r(n) > k = 4(\log n)^2$.

Wenn der Algorithmus in Zeile 4 „$n$ ist Primzahl“ ausgibt, (d. h. $r \geq n$), so ist $n$ eine Primzahl, denn sonst hätte der Algorithmus in Zeile 3 einen Teiler von $n$ gefunden.

Also **Annahme** ab jetzt:
Der Algorithmus gibt in Zeile 6 „$n$ ist Primzahl“ aus.

Wir haben zu zeigen:
Es gibt keinen Teiler von $n$, der größer als $r$ ist.
(Teiler $\leq r$ wären in Zeile 3 gefunden worden.)

Also **Zweite Annahme**:
Es existiert eine Primzahl $p$, $r < p < n$, mit $p \mid n$.

Beachte: $ggT(n,r) = 1$ nach Zeile 2 des Algorithmus. Also $p\ mod\ r\ ,\ n\ mod\ r\ \in \mathbb{Z}_r^*$.

Sei $l = \lfloor 2\sqrt{\varphi(r)} \log n \rfloor$ die Grenze für die Tests der $a'$s in Zeile 5.
Dann:
$(x+a)^n \equiv x^n + a (mod\ x^r - 1, n)$ für alle $1 \leq a \leq l$.
Also auch:

$(x+a)^n \equiv x^n + a (mod\ x^r - 1, p)$ für alle $1 \leq a \leq l$.
Nach 4.1:
$(x+a)^p \equiv x^p + a (mod\ x^r - 1, p)$ für alle $1 \leq a \leq l$.

## 4.6 Definition

Seien $p$ und $r$ wie oben, $f \in \mathbb{Z}[x]$ ein ganzzahliges Polynom.
Eine Zahl $m \in \mathbb{Z}$ heißt *p-artig* für $f(x)$, falls $f(x)^m \equiv f(x^m) (mod\ x^r - 1, p)$.

Also: $n$ und $p$ sind $p$-artig für alle $x + a$, $1 \leq a \leq l$.

Wir zeigen nun, dass $p$-artige Zahlen für ein festes Polynom abgeschlossen sind unter Multiplikation und dass umgekehrt die Menge aller Polynome, für die eine feste Zahl $p$-artig ist, ebenfalls abgeschlossen ist unter Multiplikation.

## 4.7 Lemma

Sind $m, m'$ $p$-artig für ein Polynom $f(x)$, so auch $m \cdot m'$.

Beweis:

(1) $(f(x))^{mm'} \equiv (f(x^m))^{m'} (mod\ x^r - 1, p)$.
Aus $f(x)^{m'} \equiv f(x^{m'}) (mod\ x^r - 1, p)$ folgt durch Ersetzen von $x$ durch $x^m$
$f(x^m)^{m'} \equiv f(x^{mm'}) (mod\ x^{mr} - 1, p)$.

Da $x^r - 1 \mid x^{mr} - 1$, gilt auch

(2) $f(x^m)^{m'} \equiv f(x^{mm'}) (mod\ x^r - 1, p)$.
Aus (1) und (2) folgt die Behauptung.

## 4.8 Lemma

Ist $m$ $p$-artig für $f(x)$ und $g(x)$, so auch für $f(x) \cdot g(x)$.

Beweis:
$(f(x) \cdot g(x))^m = f(x)^m \cdot g(x)^m \equiv f(x^m) g(x^m) (mod\ x^r - 1, p)$.
Wir setzen jetzt:
$I = \{n^i \cdot p^j \mid i, j \geq 0\}$
$P = \{\prod_{a=1}^{l} (x+a)^{f_a} \mid f_a \geq 0\}$
$(l = \lfloor 2\sqrt{\varphi(r)} \log n \rfloor$ wie oben)
Nach 4.7 und 4.8 gilt:
Jede Zahl aus $I$ ist $p$-artig für jedes Polynom aus $P$.

Wir definieren nun zwei Gruppen $G$ und $H$, die für den weiteren Beweis besonders wichtig sind.

**Definition der Gruppe** $G$
$G := \{k \ mod \ r \mid k \in I\} \subseteq Z_r^*$
Da $I$ abgeschlossen bezüglich Multiplikation ist, ist $G$ Untergruppe von $\mathbb{Z}_r^*$.
Sei $|G| = t$. Dann ist $t \mid \varphi(r)$ nach dem Satz von Lagrange (1.6), denn $|\mathbb{Z}_r^*| = \varphi(r)$.
Da $o(n \ mod \ r) = o_r(n) > 4(\log n)^2$ und $o(n \ mod \ r) \mid |G| = t$, folgt $t > 4(\log n)^2$.

Bevor wir die Gruppe $H$ definieren können, eine Vorbemerkung:

Wir fassen $x^r - 1$ als Polynom in $\mathbb{Z}_p[x]$ auf. Es ist $ggT(r, p) = 1$, da $r < p$, $p$ Primzahl.

Wir verwenden den folgenden Satz aus der Algebra (Stichwort: Kreisteilungspolynome; siehe z.B. [19] Abschnitt 2.4):

**Satz:**
Es existiert ein irreduzibles Polynom $h = h(x) \in \mathbb{Z}_p[x]$ mit

(1) $h(x) \mid x^r - 1$

(2) $ggT(h(x), x^s - 1) = 1$ für alle $s \mid r$, $s < r$.

Es ist $F = \mathbb{Z}_p[x]/(h)$ ein endlicher Körper (1.29). Außerdem ist $F \supseteq \mathbb{Z}_p$, wobei $\mathbb{Z}_p$ identifiziert ist mit den konstanten Polynomen.
Jedem Polynom $f$ aus $\mathbb{Z}[x]$ ist in natürlicher Weise ein Element $\overline{f}$ aus $F$ zugeordnet als Bild der Hintereinanderausführung der beiden folgenden Homomorphismen:
$f \in \mathbb{Z}[x] \to \tilde{f} \in \mathbb{Z}_p[x] \to \overline{f} = \tilde{f} \ mod \ h \in F$, wobei der erste Homomorphismus durch die Reduktion der Koeffizienten modulo $p$ gegeben ist.

**Definition der Gruppe** $H$
$H = \{g \ mod \ h \mid g \in P, \ g \ mod \ h \neq 0\} \subseteq F^*$
$P$ ist abgeschlossen bezüglich Multiplikation, also ist $H$ Untergruppe von $F^*$.
Es ist $H = \langle \overline{x + a} \mid 1 \leq a \leq l, \overline{x + a} \neq 0 \rangle$.
($\overline{x + a} = 0$ ist nur möglich, falls $x + a$ (genauer $\widetilde{x + a}$) $= h(x)$.)

Wir zeigen nun: $|H|$ ist groß im Vergleich zu $t = |G|$. Dies ist das entscheidende Lemma in der Arbeit von Agrawal, Kayal und Saxena.

## 4.9 Lemma

$|H| \geq \binom{t+l-2}{t-1}$

Beweis:
$x^r \equiv 1 (mod \ x^r - 1, p)$, also auch $x^r \equiv 1 (mod \ h(x), p)$, d. h. $\overline{x}^r = 1$ in $F^*$.
Nach 1.7d ist daher $o(\overline{x})$ ein Teiler von $r$.
Wäre $o(\overline{x}) = s, s < r$, so wäre $x^s \equiv 1 (mod \ h(x), p)$, d. h. $h(x) \mid x^s - 1$ in $\mathbb{Z}_p[x]$, im Widerspruch zu (2) oben.
Also gilt:

a) $o(\overline{x}) = r$

b) Sind $f, g \in P$ mit $f \neq g$ und Grad $(f)$, Grad $(g) < t$, so ist $\overline{f} \neq \overline{g}$:
Angenommen $\overline{f} = \overline{g}$. Sei $m \in I$.
Dann $\overline{f}^m = \overline{g}^m$, d. h. $f(x)^m \equiv g(x)^m (mod\ h(x), p)$.
Da $f, g \in P, m \in I$, ist $f(x)^m \equiv f(x^m)(mod\ x^r - 1, p)$, also auch $f(x)^m \equiv f(x^m)(mod\ h(x), p)$ und analog für $g$. Also ist $f(x^m) \equiv g(x^m)(mod\ h(x), p)$.
Das bedeutet aber: $\overline{x}^m$ ist Nullstelle von $q(y) = \overline{f}(y) - \overline{g}(y) \in F[y]$.
Da $o(\overline{x}) = r$, gilt daher für beliebige $m_1, m_2 \in I$ mit $m_1\ mod\ r \neq m_2\ mod\ r$, dass $\overline{x}^{m_1} \neq \overline{x}^{m_2}$.
Also hat $q$ mindestens $|G| = t$ viele verschiedene Nullstellen in $F$. Dies ist ein Widerspruch, da Grad $(q) \leq$ Grad $(\overline{f}) < t$.
Also: $\overline{f} \neq \overline{g}$.

c) $\overline{x+1}, \ldots, \overline{x+l}$ sind paarweise verschiedene Elemente in $F$:
Sei $1 \leq i \neq j \leq l$. Dann $i \neq j$ in $\mathbb{Z}_p$ (d. h. genauer $i \not\equiv j\ mod\ p$), denn:
$l = \lfloor 2\sqrt{\varphi(r)} \log n \rfloor < 2\sqrt{r} \log n \leq r < p$, wobei die vorletzte Ungleichung wegen $r \geq \varphi(r) \geq o_r(n) > 4(\log n)^2$ gilt.
Daraus folgt c).

d) Beweisabschluss:
$H$ enthält mindestens $l - 1$ viele Elemente $\overline{x + a_i}$ (nämlich alle $\overline{x+j}, 1 \leq j \leq l$, außer evtl. ein $\overline{x+a} = 0$, falls $h(x) = x + a$).
Bildet man zwei verschiedene Polynome $f$ und $g$ vom Grad $< t$, die jeweils Produkte von einigen $x + a_i$ sind, so ist $\overline{f} \neq \overline{g}$ nach b).
Wie viele solche Polynome gibt es? Dies ist genau die Anzahl der Auswahlen von $t - 1$ vielen Elementen aus $\{1, x - a_1, \ldots, x - a_{l-1}\}$ mit Wiederholung ohne Berücksichtigung der Anordnung.
Diese Anzahl ist $\binom{l+(t-1)-1}{t-1} = \binom{l+t-2}{t-1}$.
Also: $|H| \geq \binom{l+t-2}{t-1}$.

Wir zeigen nun, dass $|H|$ andererseits „klein“ sein muss, wenn $n$ nicht Potenz von $p$ ist.

## 4.10 Lemma

Ist $n$ keine Potenz von $p$, so $|H| < \frac{1}{2} n^{2\sqrt{t}}$.

Beweis:
Setze $I' = \{n^i \cdot p^j \mid o \leq i, j \leq \lfloor \sqrt{t} \rfloor\} \subseteq I$.
Angenommen, $n^i \cdot p^j = n^{i'} \cdot p^{j'}$. Ist $i \neq i'$, etwa $i > i'$, so $n^{i-i'} = p^{j'-j}$, also $n$ Potenz von $p$, Widerspruch.
Damit $i = i'$ und dann auch $j = j'$. Daher: $|I'| = (\lfloor \sqrt{t} \rfloor + 1)^2 > (\sqrt{t})^2 = t$.
Es ist $|G| = t$. Also existieren $m_1, m_2 \in I'$ mit $m_1 \neq m_2$ und $m_1\ mod\ r = m_2\ mod\ r$.
Sei etwa $m_1 > m_2$.
Dann ist $x^{m_1 - m_2} \equiv 1 (mod\ x^r - 1, p)$, also $x^{m_1} \equiv x^{m_2} (mod\ x^r - 1, p)$.
Ist $f \in P$, so ist $f(x)^{m_1} \equiv f(x^{m_1}) \equiv f(x^{m_2}) \equiv f(x)^{m_2} (mod\ x^r - 1, p)$, und dann auch

$f(x)^{m_1} \equiv f(x)^{m_2} (mod\ h(x), p)$.
Also gilt in $F$: $\overline{f(x)}^{m_1} = \overline{f(x)}^{m_2}$. Daher ist $\overline{f(x)}$ Nullstelle des Polynoms $q'(y) = y^{m_1} - y^{m_2} \in F[y]$. Folglich hat $q'$ mindestens $|H|$ viele Nullstellen in $F$. Die Anzahl der Nullstellen eines Polynoms über einem Körper ist aber höchstens so groß wie der Grad des Polynoms. Damit folgt:
$|H| \leq \text{Grad } (q') = m_1 \leq (n \cdot p)^{\lfloor \sqrt{t} \rfloor} < \frac{1}{2} n^{2\sqrt{t}}$. Dabei gilt die zweite Ungleichung nach Definition von $I'$ und die letzte, da $p \mid n, p \neq n$.

Wir können nun den Beweis von Satz 4.3 abschließen.

## 4.11 Lemma

Gibt der AKS-Algorithmus „$n$ ist Primzahl“ aus, so ist $n$ Primzahl.
Wir benötigen zwei einfache Eigenschaften von Binomialkoeffizienten:

(i) Ist $c \geq b \geq a$, so $\binom{c}{a} \geq \binom{b}{a}$
Insbesondere: Ist $c \geq b \geq 0$, so $\binom{a+c}{c} \geq \binom{a+b}{b}$

(ii) $\binom{2a-1}{a} \geq 2^a$ für $a \geq 3$.

Beweis von 4.11:
Angenommen, der Algorithmus gibt „$n$ ist Primzahl“ in Zeile 6 aus. Angenommen, $n$ ist keine Primzahl.
Dann gilt mit $|G| = t, l = \lfloor 2\sqrt{\varphi(r)} \log n \rfloor$:

$$
\begin{aligned}
|H| &\geq \tbinom{t+l-2}{t-1} && \text{(nach 4.9)} \\
&\geq \tbinom{l-1+\lfloor 2\sqrt{t}\log n \rfloor}{\lfloor 2\sqrt{t}\log n \rfloor} && \text{(mit (i), da } t > 4(\log n)^2\text{, also } t > \lfloor 2\sqrt{t}\log n \rfloor) \\
&\geq \tbinom{2\lfloor 2\sqrt{t}\log n \rfloor - 1}{\lfloor 2\sqrt{t}\log n \rfloor} && \text{(mit (i), da } t \leq \varphi(r) \text{ und} \\
& && \text{daher } l = \lfloor 2\sqrt{\varphi(r)\log n} \rfloor \geq \lfloor 2\sqrt{t}\log n \rfloor) \\
&\geq 2^{\lfloor 2\sqrt{t}\log n \rfloor} && \text{(mit (ii))} \\
&\geq 2^{2\sqrt{t}\log n - 1} \\
&= \tfrac{1}{2} n^{2\sqrt{t}}.
\end{aligned}
$$

Nach 4.10 ist also $n$ eine Potenz von $p$. Also dann hätte der Algorithmus in Zeile 1 „$n$ ist zusammengesetzt“ ausgegeben, Widerspruch.

## 4.12 Satz

AKS-Algorithmus hat polynomiale Komplexität in der Inputlänge (also in $log(n)$).
Genauer: Bitkomplexität $O((log\ n)^{10,5}) \cdot f(log(log(n))))$, wobei $f$ ein Polynom ist.

Beweis:
Die erste Behauptung folgt sofort aus Lemma 4.5 und der Bemerkung nach 4.2. Die genauere Aussage erhält man mit Hilfe der Ergebnisse aus Kapitel 2.

## 4.13 Bemerkung

Erweiterungen / Verbesserungen

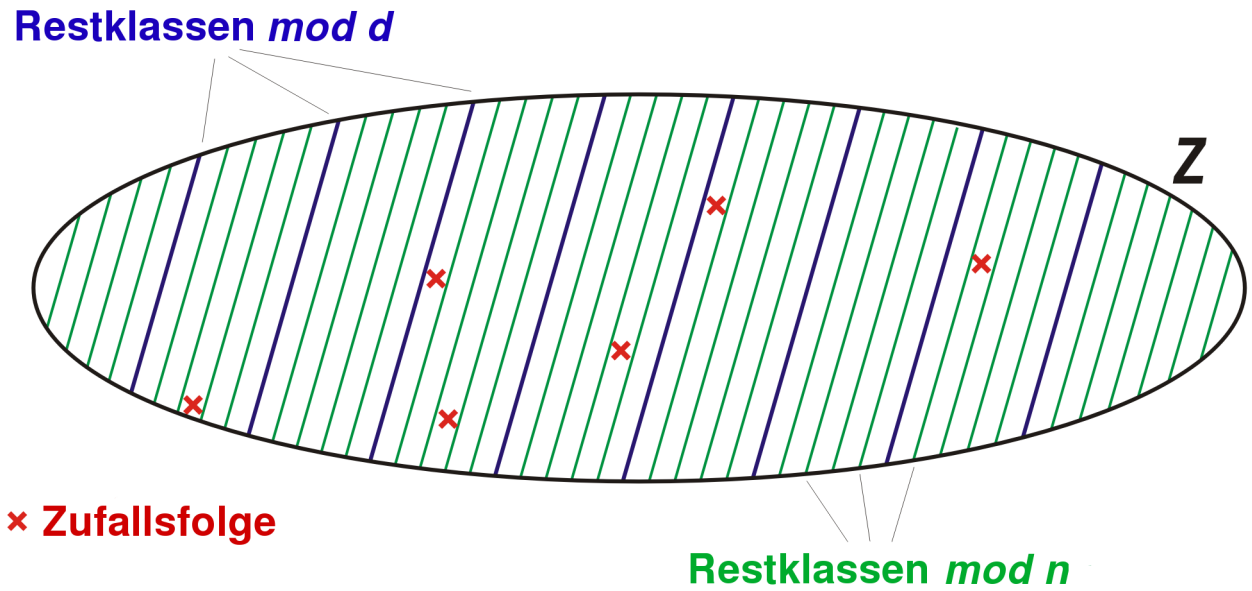
- Bernstein (2003): randomisierter Algorithmus, Erwartungswert $O((log\ n)^{4+\epsilon})$
- Lenstra, Pomerance (2003): deterministischer Algorithmus $O((log\ n)^{6+\epsilon})$

*http://cr.yp.to/primality.html (Bernstein)*
*http://primes.utm.edu (Crandl, Pomerance)*
*http://fatphil.org/maths/AKS/ (Implementationen des AKS)*

# 5 Die Pollard'schen Faktorisierungsalgorithmen

Primzahltests geben keine Faktorisierung an. Dafür brauchen wir aufwändigere Faktorisierungsalgorithmen.
Voraussetzung: $n$ ist zusammengesetzt.

## Pollards $\rho$-Methode (1975)




Idee:
Ist $d$ ein echter Teiler von $n$, so gibt es weniger Restklassen $mod\ d$ (nämlich $d$), als Restklassen $mod\ n$. Jede Restklasse $mod\ d$ ist Vereinigung von $\frac{n}{d}$ Restklassen $mod\ n$. Wählt man möglichst gleichverteilte $x_j \in \mathbb{Z}$, so ist die Hoffnung $x_i, x_j$ zu finden, die in der gleichen Restklasse $mod\ d$ liegen (also $d \mid x_i - x_j$) aber in verschiedenen Restklassen $mod\ n$ (also $n \nmid x_i - x_j$).

Dann $d \mid \underbrace{ggT(x_1 - x_2, n)}_{\text{nicht trivialer Teiler von } n} \neq n.$

Wie bestimmt man die $x_i$?
$x_0 \in \mathbb{Z}_n$, $f : \mathbb{Z}_n \to \mathbb{Z}_n$
$x_{i+1} = f(x_i)$
Bestimme nun alle $ggT(x_i - x_j, n)\ \forall\ i > j$.
Folge $x_0, x_1, \ldots$ wird irgendwann periodisch. (Sieht wie ein $\rho$ aus. Daher der Name 'Rho-Methode'.)

Beispiel:
$n = 143 (= 11 \cdot 13)$
$x_0 = 2$, $f(x) = x^2 + 1\ mod\ 143$
Keine linearen Funktionen verwenden, da die Verteilung sonst schlecht ist.

| $x_0$ | $x_1$ | $x_2$ | $x_3$ | $x_4$ | $x_5$ | $x_4$ |
|---|---|---|---|---|---|---|
| 2 | 5 | 26 | 105 | 15 | 83 | 26 |

$ggT(x_1 - x_0, 143) = 1$
$ggT(x_2 - x_0, 143) = 1$
$ggT(x_2 - x_1, 143) = 1$
$\vdots$
$ggT(x_4 - x_0, 143) = (13, 143) = 13$, Faktor gefunden

Frage: Wie lange muss man warten, bis man $x_i, x_j$ mit $ggT(x_i - x_j, n) \neq 1, n$ gefunden hat?

## 5.1 Satz

$\mathscr{F} = \{f : \mathbb{Z}_n \to \mathbb{Z}_n\}$. $f \in \mathscr{F}, x_0 \in \mathbb{Z}_n, x_{i+1} = f(x_i)$.
Sei $\lambda > 0, \lambda \in \mathbb{R}, l = 1 + \lfloor\sqrt{2\lambda d}\rfloor, d \mid n$.
Dann: *(Geburstagsparadoxon)*

$$\frac{|\{(f,x_0): f \in \mathscr{F}, x_o \in \mathbb{Z}_n, x_0, x_1, \ldots, x_l \text{ paarweise nichtkongruent } mod\ d\}|}{|\{(f,x_0): f \in \mathscr{F}, x_0 \in \mathbb{Z}_n\}|} \leq e^{-\lambda}$$

Beweis:
Nenner: $n^{n+1}$, da $n$ Möglichkeiten für $x_0$ , $n^n$ Möglichkeiten für $f$.
Zähler: $x_0$: $n$ Möglichkeiten
$f(x_0) = x_1$: $n - \frac{n}{d}$ Möglichkeiten
$f(x_1) = x_2$: $n - \frac{2n}{d}$ Möglichkeiten ...
$f(x_{l-1}) = x_l$: $n - \frac{nl}{d}$ Möglichkeiten. Die Werte der Abbildung $f$ an den Stellen $\neq x_0, x_1, \ldots, x_{l-1}$ sind beliebig wählbar, es existieren also $n^{n-l}$ Möglichkeiten.
Insgesamt: $n \cdot \left(n - \frac{n}{d}\right) \cdot \cdots \cdot \left(n - \frac{nl}{d}\right) \cdot n^{n-l} = n^{n+1} \prod_{j=1}^{l} \left(1 - \frac{j}{d}\right)$

Verhältnis: $\prod_{j=1}^{l}\left(1-\frac{j}{d}\right)$. Logarithmieren und anwenden, dass $\ln(1-x) < -x$ für $0 < x < 1$, ergibt:

$$\ln\left(\prod_{j=1}^{l}\left(1-\frac{j}{d}\right)\right) = \sum_{j=1}^{l}\ln\left(1-\frac{j}{d}\right) < \sum_{j=1}^{l}-\frac{j}{d} = -\frac{l(l+1)}{2d} < \frac{-l^2}{2d} < -\lambda$$

Wegen Wahl von $l$ folgt Behauptung.

Wähle z.B. $\lambda = 1\ e^{-1} \approx 0,37\ l = 1 + \lfloor\sqrt{2d}\rfloor$.
Angenommen $d \approx 10^{12}, l \approx 1,4 \cdot 10^6$
Bei mindestens 63 % aller Paare $(f, x_0)$ findet man unter den ersten $1,4 \cdot 10^6$ Folgegliedern zwei, die kongruent mod $d$ sind.

Wie wählt man $f$?

- $f$ nicht linear
- $f$ quadratisch, aber nicht $f(x) = x^2, x^2 - 2$
- übliche Wahlen: $f(x) = x^2 \pm 1, x^2 + x + 1, x^2 + 2$

Vermeidung der vielen ggT-Berechnungen (Brent, 1980):

## 5.2 Pollard-Brent-Rho-Methode (1980)

Input: $n$ zusammengesetzt.

1. Wähle nicht-lineares Polynom $f : \mathbb{Z}_n \to \mathbb{Z}_n (f \neq x^2, x^2 - 2)$ und $x_0 \in \mathbb{Z}_n$.
2. Wiederhole für $k = 1, 2, \ldots$
   $x_k = f(x_{k-1})$
   Ist $2^a \leq k < 2^{a+1}$ (d.h. k ist $(a+1)$-Bit-Zahl), so setze $j = 2^a - 1$
   Bestimme $ggT(x_k - x_j, n)$.
   Ist $1 < ggT(x_k - x_j, n) < n$, so Ausgabe: $d = ggT(x_k, x_j, n)$ nicht-trivialer Teiler von $n$.

5.2 erfordert in einer Runde nur eine ggT-Berechnung, statt $k$ ggT-Berechnungen von $n$ mit $x_k - x_{k-1}, \ldots, x_k - x_0$.

Man kann zeigen: Falls $k_0, j_0$ existieren mit $1 < ggT(x_{k_0} - x_{j_0}, n) < n, k_0 > j_0$, so existiert $k \leq 4k_0$, so dass der Algorithmus 5.2 in Schritt $k$ nicht-trivialen Teiler von $n$ findet.

Beweis:
Angenommen $k_0$ hat $h$ Bits. Setze $j = 2^h - 1$, $k = j + (k_0 - j_0)$. $k$ ist $(h+1)$-Bit-Zahl. Im $k$-ten Schritt von (5.2) wird $ggT(x_k - x_j, n)$ gebildet. Es ist $x_{k_0} \equiv x_{j_0} (mod\ d)$ für einen echten Teiler $d$ von $n$.
$f$ Polynom $\Rightarrow f(x_{k_0}) \equiv f(x_{j_0}) (mod\ d)$.

$x_k = f^{k-k_0}(x_{k_0}) \equiv f^{k-k_0}(x_{j_0}) \equiv x_{j_0+k-k_0} \equiv x_j (mod\ d)$.
$k < 2^{h+1} = 4 \cdot 2^{h-1} \leq 4k_0$.

Beispiel:
$n = 4087, f(x) = x^2 + x + 1\ mod\ n,\ x_0 = 2$
$x_1 = f(2) = 57 \quad ggT(x_1 - x_0, n) = ggT(7 - 2, 4078) = 1$
$x_2 = f(7) = 7 \quad ggT(x_1 - x_0, n) = ggT(7 - 2, 4078) = 1$
$x_3 = f(57) = 3307 \quad ggT(x_1 - x_0, n) = ggT(7 - 2, 4078) = 1$
$x_4 = f(3307) = 2745 \quad ggT(x_4 - x_3, n) = ggT(2745 - 3307, 4078) = 1$
$x_5 = f(2745) = 1343 \quad ggT(x_5 - x_3, n) = ggT(1343 - 3307, 4078) = 1$
$x_6 = f(1343) = 2626 \quad ggT(x_6 - x_3, n) = ggT(2626 - 3307, 4078) = 1$
$x_7 = f(2626) = 3734 \quad ggT(x_7 - x_3, n) = ggT(3734 - 3307, 4078) = 61$
$4087 = 61 \cdot 67$

## 5.3 Komplexität der Rho-Methode

Rho-Methode ist probabilistischer Algorithmus, der nicht notwendig einen nicht-trivialen Teiler findet. (*keine Erfolgsgarantie*)
Sei $p$ kleinster Primteiler von $n$. Heuristik zur Komplexität: Verhält sich $f$ (mit $x_0$) wie eine „Zufallsfunktion", so kann man mit der Wahrscheinlichkeit $1 - e^{-\lambda}$ nach $O(\sqrt{\lambda p})$ vielen Schritten eine Kollision erwarten. (d.h. man findet $x_j, x_k$ mit $p \mid x_j - x_k$).
Hält man $\lambda$ fest (z.B. $\lambda = 10000$), so $O(\sqrt{p})$ Schleifen im Algorithmus. Der Algorithmus ist folglich gut, wenn $p$ klein ist. In jedem Fall gilt: $p \leq \sqrt{n}$. Also $O(\sqrt[4]{n})$ Schleifen mit jeweils einer ggT-Berechnung.

## 5.4 Pollard'sche ($p$-1)-Methode (1974)

Diese Methode funktioniert gut, wenn $n$ einen Primteiler $p$ hat, wobei in $p$-1 nur kleine Primteiler vorkommen.

$n$ ist zusammengesetzt, $p$ Primzahl, $p \mid n$.
Fermat: $a^{p-1} \equiv 1 (mod\ p)$, falls $p \nmid a$ (insbesondere falls $ggT(a, n) = 1$).
Ist $p - 1 \mid m$, so auch $a^m \equiv 1 (mod\ p)$.
Also $p \mid ggT(a^m - 1, n)$ für alle Primteiler $p$ von $n$, so dass $p - 1 \mid m$.

Prinzip der ($p$-1)-Methode:
Bestimme Zahlen $m$, die viele Divisoren der Form $p$-1, $p$ Primzahl, haben, und teste in einem Durchgang durch Berechnung von $ggT(a^m - 1, n)$, ob man dabei einen Teiler von $n$ gefunden hat.

Einfachste Möglichkeit zur Bestimmung von $m$:
$m = m(k) = kgV(1, \ldots, k)$, $k$ feste Schranke (z.B. $k = 1000$)

Die Berechnung ist einfach:

- Ist $k + 1$ keine Primzahlpotenz, so $m(k + 1) = m(k)$.

- Ist $k+1 = q^a$, $q$ Primzahl, so $m(k+1) = q \cdot m(k)$.

Sei $p \mid n$. Angenommen $p$-1 hat nur Primzahlpotenzteiler $\leq k$, so $p-1 \mid m$.
Es folgt: $p \mid ggT(a^m - 1, n)$ (evtl. ergibt sich $ggT = n$).

Die ($p$-1)-Methode funktioniert gut, wenn eine Primzahl $p$ existiert mit $p \mid n$ und wo $p-1$ lauter „kleine" Primzahlpotenzfaktoren enthält.
Vgl. [3] 5.4

Beispiel:
$n = 6283, k = 5, m = kgV(1,2,3,4,5) = 60, a = 2$
$ggT(2^{60} - 1, 6283) = 61$
$\rightarrow 6283 = 61 \cdot 103$
$61 - 1 = 2^2 \cdot 3 \cdot 5$ (kleine $p$'s)

# 6 Das quadratische Sieb

Pomerance (1982,85), Vorläufer: Dixon (1981)

## 6.1 Bemerkung

Sei $n$ eine ungerade Zahl. Es gibt eine 1-1-Beziehung zwischen Faktorisierungen $n = ab$ von $n$ und Darstellungen $n = t^2 - s^2$, $s, t \in \mathbb{N}_0$.
$n = ab : t = \frac{a+b}{2}, s = \frac{a-b}{2}$: $t^2 - s^2 = ab = n$.
$n = t^2 - s^2 = (t+s)(t-s)$

## 6.2 Fermat-Faktorisierung (Grundversion)

$n = ab$, $\quad a, b$ etwa gleich groß (d.h. beide liegen in der Nähe von $\sqrt{n}$)
$t = \frac{a+b}{2}$ in der Nähe von $\sqrt{n}$ (etwas größer wegen $n = t^2 - s^2, s = \frac{a-b}{2}$).

Teste $t = \lceil\sqrt{n}\rceil, \lceil\sqrt{n}\rceil + 1, \lceil\sqrt{n}\rceil + 2, \ldots$ bis $t^2 - n = s^2$ eine Quadratzahl
$n = (t+s)(t-s)$ Faktorisierung.

Beispiel:
$n = 200819$, $\lceil\sqrt{n}\rceil = 449$
$449^2 - 200819 = 782$ keine Quadratzahl
$450^2 - 200819 = 1681 = 41^2$
$200819 = 450^2 - 41^2 = (450 + 41) \cdot (450 - 41) = 491 \cdot 409$

Liegen $a$ und $b$ nicht nahe beieinander, so braucht 6.2 lange. Dann besser folgendes Vorgehen:

## 6.3 Fermat-Faktorisierung (erweiterte Version)

Wähle kleines $k \in \mathbb{N} (k < \frac{2}{3}\sqrt{n})$. Falls $k$ gerade, so $4 \mid k$.
Setze $t = \lceil\sqrt{kn}\rceil, \lceil\sqrt{kn}\rceil + 1, \ldots$ bis $t^2 - kn = s^2$ ein Quadrat ist.
Dann sind $ggT(t+s, n)$ und $ggT(t-s, n)$ nicht-triviale Teiler von $n$.

Beweis:
Es ist $(t+s)(t-s) = kn$.
Angenommen, $ggT(t+s, n) = 1$. Dann $t+s \mid k$ und $n \mid t-s$.
Also: $kn = t^2 - s^2 = (t+s)(t-s) > (t-s)^2 \geq n^2$, $k > n$, Widerspruch.
Derselbe Beweis funktioniert, wenn $ggT(t-s, n) = n$.

Angenommen, $ggT(t+s,n) = n$.
Dann $n \mid t+s$. Da $t > s$, folgt $2t > t+s \geq n$, d. h. $t \geq \frac{n+1}{2}$.
Sei $n = ab, a \leq \sqrt{n}, b \geq \sqrt{n}$ (möglich, da $n$ zusammengesetzt).

Wir betrachten zunächst den Fall, dass $k$ ungerade ist.
Dann ist $kn = (\frac{ka+b}{2})^2 - (\frac{ka-b}{2})^2$. Beachte $ka+b, ka-b$ sind gerade, da $k, a, b$ ungerade.
Klar: $\frac{ka+b}{2} \geq \sqrt{kn}$.
Da $t$ die erste Zahl $\geq \sqrt{kn}$ ist, für die $t^2 - kn$ ein Quadrat ist, ist $t \leq \frac{ka+b}{2}$.
Aus $t \geq \frac{n+1}{2}$ folgt daher
$ab = n < n+1 \leq 2t \leq ka+b \leq \frac{2\sqrt{n}}{3}a + b$ (nach Wahl von $k$)
$\leq \frac{2ab}{3} + b = b(\frac{2a}{3} + 1) \leq ab$ (da $a \geq 3$), Widerspruch.

Sei nun $k$ gerade. Dann nach Voraussetzung $k = 4 \cdot k'$.
Es ist $kn = (k'a+b)^2 - (k'a-b)^2$. Klar: $k'a + b \geq \sqrt{kn}$.
Wie im obigen Fall ist dann $t \leq k'a + b$.
Aus $t \geq \frac{n+1}{2}$ folgt
$ab = n < n+1 \leq 2t \leq 2k'a + 2b = \frac{1}{2}ka + 2b \leq \frac{1}{3}\sqrt{n}a + 2b \leq \frac{1}{3}ab + 2b = (\frac{1}{3}a + 2)b \leq ab$
(da $a \geq 3$), Widerspruch.

Da aus $ggT(t-s,n) = 1$ folgt, dass $ggT(t+s,n) = n$, ist auch $ggT(t-s,n) = 1$ nicht möglich.

**Bemerkung**
In (6.3) wurde vorausgesetzt, dass für gerades $k$ schon 4 ein Teiler von $k$ sein muss, da ansonsten keine $s$ und $t$ mit $kn = t^2 - s^2$ existieren. Denn $t^2 - s^2 = (t-s)(t+s)$ ist stets ungerade oder durch 4 teilbar.

Beispiel:
$n = 141467$ (6.2 braucht 38 Versuche)
Wähle in 6.3: $k = 3$
$t = \lceil \sqrt{3n} \rceil = 652, 653, \ldots \quad 655 : 655^2 - 3 \cdot 141467 = 68^2$
$ggT(655 + 68, 141467) = 241, \; n = 241 \cdot 587$

Verallgemeinerung:
Gesucht s,t mit $t^2 = s^2 (mod\ n), \; t \not\equiv \pm s (mod\ n)$.
Dann: $ggT(s+t,n)$ oder $ggT(s-t,n)$ ist ein nicht-trivialer Teiler von $n$.
$n \mid (s+t)(s-t)$. Also ist $ggT(s+t,n) = 1 = ggT(s-t,n)$ nicht möglich.
Auch $ggT(s+t,n) = n$ oder $ggT(s-t,n) = n$ unmöglich, denn sonst
$n \mid s+t$ d.h. $t \equiv -s (mod\ n)$ oder $n \mid s-t$ d.h. $t \equiv s (mod\ n)$.

Hat man eine Chance, solche $s, t$ zu finden?

## 6.4 Satz

Sei $n$ ungerade und $p_1, \ldots, p_r$ die verschiedenden Primzahlen, die $n$ teilen.
Ist $a$ ein Quadrat mod $n$, $a \not\equiv 0 (mod\ n)$, d.h. $\exists\, b \in \mathbb{N} : a \equiv b^2 (mod\ n)$, so gibt es genau

$2^r$ viele $b_i$, mit $b_i \not\equiv b_j (mod\ n)\ \forall\ i \neq j$ und $b_i^2 \equiv a (mod\ n)$.

Beweisidee:
Sei $a \equiv b^2 (mod\ n)$. Sei $p \mid n, p^\alpha \bar{|} n$ $(p^\alpha \mid n, p^{\alpha+1} \nmid n)$. In $\mathbb{Z}_p$ hat $a\ mod\ p$ genau 2 Wurzeln: $b\ mod\ p,\ -b\ mod\ p$ $(p \neq 2)$ ($\mathbb{Z}_p$ ist Körper, $\bar{a} = a\ mod\ p,\ X^2 - \bar{a} \in \mathbb{Z}_p[X]$ hat höchstens zwei Nullstellen). Dann kann man zeigen: In $Z_{p^\alpha}$ sind $b\ mod\ p^\alpha,\ -b\ mod\ p^\alpha$ die einzigen Wurzeln von $a\ mod\ p^\alpha$.
Der Chinesische Restesatz (1.11) liefert $2^r$ viele Wurzeln $(mod\ n)$.

Beispiel:
$n = 15$ 4 hat mod 15 vier Wurzeln: 2, -2=13, 8, -8=7 → 2, 7, 8, 13.

Wir definieren für das Quadratische Sieb in Abweichung von der üblichen Berechnungsweise:
$a$ mod $n$ = betragsmäßig kleinster Rest mod $n$, $a\ mod\ n \in \{-\frac{n-1}{2}, \ldots, 0, \ldots, \frac{n-1}{2}\}$

## 6.5 Definition

$n$ ungerade (zusammengesetze Zahl).

a) Eine *Faktorbasis* ist eine Menge $B = \{p_1, p_2, \ldots, p_h\}$, wobei $p_i$ verschiedene Primzahlen sind. (ggf. $p_1 = -1$)

b) $b \in \mathbb{Z}$ heißt *B-Zahl* (bzgl. $n$), falls $b^2\ mod\ n$ Produkt von Zahlen aus $B$ ist.

Beispiel:
$n = 4633, B = \{-1, 2, 3\}$: 67, 68, 69 $B$-Zahlen
$67^2 \equiv -144\ (mod\ n)$
$68^2 \equiv -9\ (mod\ n)$
$69^2 \equiv 128\ (mod\ n)$

## 6.6 Grundidee des Quadratischen Siebs

Faktorbasis $B = \{p_1, p_2, \ldots, p_h\}$
Bestimme $B$-Zahlen $b_1, \ldots, b_r$ mit
$b_i^2\ mod\ n = p_1^{a_{i1}} p_2^{a_{i2}} \cdots p_n^{a_{in}},\ i = 1, \ldots, r$
$(b_1^2\ mod\ n) \cdot (b_2^2\ mod\ n) \cdots (b_r^2\ mod\ n) = p_1^{a_{11}+a_{21}+\ldots+a_{r1}} \cdots p_h^{a_{1h}+a_{2h}+\ldots+a_{rh}}$, wobei
$d_1 = a_{11} + a_{21} + \ldots + a_{r1}, \ldots, d_h = a_{1h} + a_{2h} + \ldots + a_{rh}$ alle gerade.
Setze $b = b_1 \cdots b_r,\ c = p_1^{\frac{d_1}{2}} \cdots p_h^{\frac{d_h}{2}}$, so: $b^2 \equiv c^2 (mod\ n)$.

Ist $b \not\equiv \pm c (mod\ n)$, so ist $ggT(b+c, n)$ oder $ggT(b-c, n)$ ein nicht-trivialer Teiler von $n$.

Beispiel:
$n = 1829,\ B = -1, 2, 3, 5, 7, 11, 13$

$b_1 = 42$, $b_1^2 \ mod \ n = -5 \cdot 13$
$b_2 = 43$, $b_2^2 \ mod \ n = 2^2 \cdot 5$
$b_3 = 61$, $b_3^2 \ mod \ n = 3^2 \cdot 7$
$b_4 = 85$, $b_4^2 \ mod \ n = -7 \cdot 13$
$b_5 = 86$, $b_5^2 \ mod \ n = 2^4 \cdot 5$
$(b_2^2 \ mod \ n) \cdot (b_5^2 \ mod \ n) = (2^3 \cdot 5)^2$
$b_2 \cdot b_5 \ mod \ n = 40 = 2^3 \cdot 5$
Diese Wahl führt zu keinem nicht-trivialen Teiler von $n$.
$(b_1^2 \ mod \ n) \cdot (b_2^2 \ mod \ n) \cdot (b_3^2 \ mod \ n) \cdot (b_4^2 \ mod \ n) = (2 \cdot 3 \cdot 5 \cdot 7 \cdot 13)^2$
$b_1 b_2 b_3 b_4 \ mod \ n = -370$
$2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \ mod \ n = 901 \ ggT(-370 + 901, 1829) = 59$
$n = 59 \cdot 31$

Beachte: Statt sämtliche Exponenten $(a_{i1}, \ldots, a_{ih})$ der $b_i^2 \ mod \ n$ zu behandeln, genügt es nur die Vektoren $(a_{i1} \ mod \ 2, \ldots, a_{ih} \ mod \ 2)$ zu betrachten und Linearkombinationen zu finden, die in $\mathbb{Z}_2^h$ den Nullvektor ergeben, Dazu kann man Methoden der linearen Algebra verwenden.

## 6.7 Dixon-Algorithmus und Pomerance-Algorithmus

a) Dixon-Algorithmus (1981)
$B = \{-1, p_2, \ldots, p_h\}$ wobei $p_2, \ldots, p_h$ die ersten $h$-1 Primzahlen sind.
$B$-Zahlen: Zufallswahlen und Test ob $B$-Zahl.

b) Pomerance-Algorithmus (Quadratischen Sieb) (1982, 1985)
Wähle $b$'s so, dass $b^2 \ mod \ n$ betragsmäßig klein;
z.B. in der Nähe von $\lceil \sqrt{kn} \rceil$ mit kleinem $k$.
Wähle $B$ so, dass es die Primteiler der kleinen Absolutbeträge der $b^2 \ mod \ n$ enthält; üblicherweise alle Primzahlen bis zu gewisser Schranke $y$ (z.B. $n \approx 10^{50}$, so $y \approx 10^5 - 10^6$).
Pomerance Algorithmus hat Komplexität von $O\left(e^{(1+\epsilon_n)\sqrt{ln(n) \cdot ln(ln(n))}}\right)$, $\epsilon_n \to 0$ für $n \to \infty$; subexponentieller Algorithmus.

## 6.8 Bemerkung

Das Quadratische Sieb lässt sich verallgemeinern zum *Zahlkörpersieb* (Grundidee: Pollard, J.M., 1987). Statt in $\mathbb{Z}$ wird in Ringen $\mathbb{Z}[X]/f\mathbb{Z}[X]$ ($f$ irreduzibles Polynom) gearbeitet: Untersuchung von bestimmten quadratischen Kongruenzen.
Unter gewissen unbewiesenen heuristischen Annahmen gilt für dessen Komplexität:

$$O\left(e^{(c \sqrt[3]{\ln n} \sqrt[3]{(\ln \ln n)^2})}\right)$$

Einzelheiten: [3] 6.2

# 7 Faktorisierung mit elliptischen Kurven

Sei $K$ ein Körper. Allgemein ist eine elliptische Kurve über $K$ gegeben durch eine Gleichung

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,\ a_i \in K$$

wobei die Kurve glatt sein soll. (Dies bedeutet, dass an keinem Punkt $(x, y)$ über dem algebraischen Abschluss von $K$ beide partiellen Ableitungen der Kurve verschwinden.) Die Bezeichnung der Koeffizienten, insbesondere das fehlende $a_5$, hat historische Gründe und hat sich eingebürgert.

Elliptische Kurven sind ein wichtiges Thema der Analysis und algebraischen Geometrie. Ihren Namen haben sie erhalten, weil sie in Verbindung stehen mit sog. elliptischen Integralen, die z. B. bei der Umfangsbestimmung von Ellipsen auftreten. Seit ca. 1985 haben elliptische Kurven aber auch eine wichtige Bedeutung im Zusammenhang mit kryptografischen Systemen, Primzahltests und Faktorisierungsalgorithmen gewonnen. Auf Letzteres wollen wir hier eingehen.

Wir werden im Folgenden nur elliptische Kurven über Körpern der Charakteristik $\neq 2$ und 3 (d. h. $1 + 1 \neq 0$, $1 + 1 + 1 \neq 0$) betrachten. In diesen Fällen lässt sich jede elliptische Kurve nach geeigneten Koordinatentransformationen auf eine einfache Form bringen, die wir für uns zur Definition von elliptischen Kurven verwenden.

## 7.1 Definition

Sei $K$ ein Körper, Char $K \neq 2, 3$.
Eine *elliptische Kurve* über $K$ ist gegeben durch eine Gleichung

$$y^2 = x^3 + ax + b,\ a, b \in K$$

wobei $4a^3 + 27b^2 \neq 0$. (4 und 27 stehen für $4 \cdot 1$ und $27 \cdot 1$ in $K$).

Die Bedingung $4a^3 + 27b^2 \neq 0$ entspricht der Glattheitsbedingung; sie ist äquivalent damit, dass die kubische Gleichung auf der rechten Seite keine Mehrfachnullstellen besitzt.
Zur Veranschaulichung geben wir eine elliptische Kurve über $\mathbb{R}$ an:

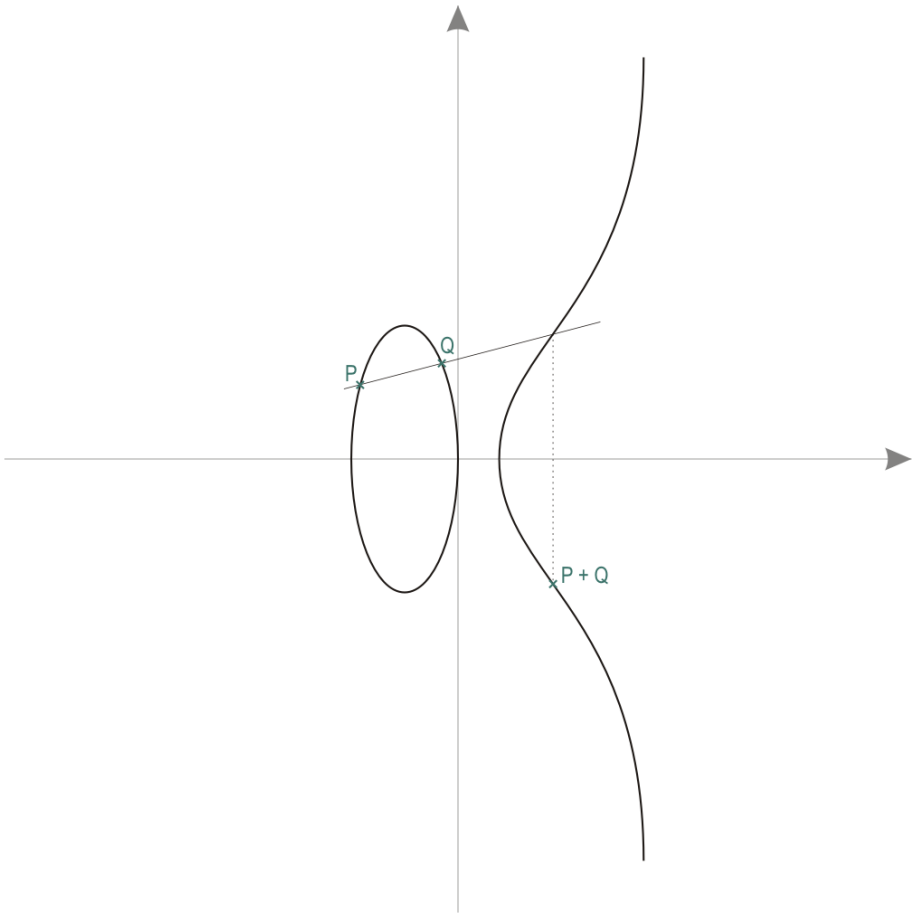



Abbildung 7.1: Addition auf elliptischen Kurven

Für unsere Zwecke ist die wichtigste Eigenschaft elliptischer Kurven, dass man auf ihnen (d. h. auf der Menge der Punkte $(x, y)$, die die Gleichung aus 7.1 erfüllen) eine Addition definieren kann, so dass daraus eine abelsche Gruppe entsteht. Dabei muss dieser Menge noch ein weiterer („unendlich ferner “) Punkt $O$ hinzugefügt werden. Wir bezeichnen die Menge dieser Punkte, die zu einer elliptischen Kurve über $K$ gehören, mit $E(K)$.

Für elliptische Kurven über $\mathbb{R}$ lässt sich die Addition auf $E(\mathbb{R})$ geometrisch einfach veranschaulichen (und ebenso die Inversen). Das beruht im Wesentlichen darauf, dass die Gerade durch zwei Punkte $P, Q(\neq O)$ auf $E(\mathbb{R})$ mit verschiedenen $x$-Koordinaten die Kurve in genau einem weiteren Punkt trifft; dessen Spiegelbild an der $x$-Achse liegt auch auf $E(\mathbb{R})$ und ist $P + Q$.

Das neutrale Element ist der unendlich ferne Punkt $O$, das Inverse $-P$ eines Punktes $P \neq O$ ist das Spiegelbild von $P$ an der $x$-Achse. Für den Fall $P = Q$ lässt sich die Addition $P + P$ auch geometrisch beschreiben: an die Stelle der Gerade durch $P$ und $Q$ tritt die Tangente an $P$. Wichtig ist, dass man diese geometrische Definition der Addition auf elliptischen Kurven ßüber $\mathbb{R}$ auch algebraisch beschreiben kann, d. h. die Koordinaten der Punkte $P+Q$ bzw. $-P$ lassen sich durch die Koordinaten von $P$ und $Q$ beschreiben.

Diese Beschreibung der Addition lässt sich nun auf elliptische Kurven über beliebigen Körpern (der Charakteristik $\neq 2, 3$) übertragen, und man kann zeigen, dass dadurch immer eine abelsche Gruppe definiert wird. Dies ist der Inhalt des folgenden Satzes.

## 7.2 Satz

Sei $K$ ein Körper, Char $K \neq 2, 3$, $\quad y^2 = x^3 + ax + b$ eine elliptische Kurve über $K$.

Dann wird $E(K) = \{(x, y) \in K^2 : y^2 = x^3 + ax + b\} \cup \{O\}$ eine abelsche Gruppe durch folgende Definition:

(1) $P + O = O + P = P \quad$ für alle $P \in E(K)$

(2) $-O = O$; ist $P = (x, y)$, so ist $-P = (x, -y)$.

(3) Sind $P = (x_1, y_1), Q = (x_2, y_2), x_1 \neq x_2$, so hat $P + Q$ die Koordinaten
$x_3 = (\frac{y_2 - y_1}{x_2 - x_1})^2 - x_1 - x_2$
$y_3 = (\frac{y_2 - y_1}{x_2 - x_1})(x_1 - x_3) - y_1$

(4) Ist $P = (x_1, y_1), Q = (x_1, y_2)$, so ist $y_2 = \pm y_1$.
Ist $y_2 = -y_1 \quad$ (d. h. $Q = -P$), so ist $P + Q = O$.
Ist $y_2 = y_1 \neq 0 \quad$ (d. h. $Q = P$), so hat $P + P$ die Koordinaten
$x_3 = (\frac{3x_1^2 + a}{2y_1}) - 2x_1$
$y_3 = (\frac{3x_1^2 + a}{2y_1})(x_1 - x_3) - y_1$

Beweis:
Der Beweis dieses Satzes kann elementar durchgeführt werden, ist aber ziemlich mühsam. Insbesondere der Nachweis des Assoziativgesetzes ist aufwändig und erfordert mehrere Fallunterscheidungen.
(Beweis siehe z. B.: [20])

Für endliche Körper $K$, $\mid K \mid = q$ ($q$ ist also eine Primzahlpotenz nach 1.31 b) kann man eine gute Abschätzung der Größe $\mid E(K) \mid$ für eine elliptische Kurve geben. Dies ist ein tiefliegender Satz von Hasse (zum Beweis siehe z. B. [21]):

## 7.3 Satz (Hasse)

(H. Hasse, 1898-1979)

Sei $K$ ein endlicher Körper, $\mid K \mid = q, N = \mid E(K) \mid$ für eine elliptische Kurve über $K$. Dann ist

$$(q+1) - 2\sqrt{q} \leq N \leq (q+1) + 2\sqrt{q}.$$

Zur Beschreibung der Faktorisierungsmethode mit elliptischen Kurven benötigen wir noch folgende Definition:

## 7.4 Definition

Sei $n \in \mathbb{N}$, $\frac{a_1}{b_1}, \frac{a_2}{b_2} \in \mathbb{Q}$, $ggT(b_1, n) = ggT(b_2, n) = 1$.
$\frac{a_1}{b_1} \equiv \frac{a_2}{b_2} (mod\ n)$, falls $\frac{a_1}{b_1} - \frac{a_2}{b_2}$ in gekürzter Form einen durch $n$ teilbaren Zähler besitzt.

**Beachte:** Ist $ggT(n, b) = 1$, so ist $b\ mod\ n$ in $\mathbb{Z}_n$ invertierbar. Daher ist für jedes $a \in \mathbb{Z}$ dann $\frac{a}{b} \equiv c (mod\ n)$, wobei $c$ eine durch $\frac{a}{b}$ eindeutig bestimmte ganze Zahl ist mit $0 \leq c \leq n$. Wir bezeichnen diese Zahl auch mit $\frac{a}{b} (mod\ n)$.

Die Grundidee der Faktorisierungsmethode mit elliptischen Kurven, die von H. W. Lenstra jr. 1986 entwickelt wurde, ist folgende:

Angenommen wir haben eine Gleichung $y^2 = x^3 + ax + b,\ a, b \in \mathbb{Z}$, und einen Punkt $P = (x, y)$, der diese Gleichung erfüllt.
Wir nehmen an, dass $4a^3 + 27b^2 \neq 0$.

Sei $n$ eine zusammengesetzte Zahl, $ggT(6, n) = 1$. Wir setzen voraus, dass $ggT(4a^3 + 27b^2, n) = 1$ ist.
Reduziert man die Koeffizienten $a$ und $b$ modulo $p$ für einen Primteiler $p$ von $n$, so erhält man also eine elliptische Kurve über $\mathbb{Z}_p$.

Nun betrachten wir die obige Gleichung und reduzieren die Koeffizienten modulo $n$. Über $\mathbb{Z}_n$ lässt sich mit den Gleichungen aus 7.2 keine Gruppenstruktur definieren, und zwar deshalb, weil die Divisionen in 7.2 (3) bzw. (4) nur möglich sind, falls die Nenner

teilerfremd zu $n$ sind. (Beachte: $\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n \mid ggT(a,n) = 1\}$ nach 1.17b)

Dies ist aber gerade der entscheidende Punkt an Lenstras Methode. Man versucht Vielfache $kP$ des Punktes $P$ zu bilden, und zwar über $\mathbb{Z}_n$ entsprechend den Additionsregeln aus 7.2. Dabei muss man ein Verfahren zur Berechnung von $kP$ wählen (z. B. iterierte Verdopplung entsprechend der iterierten Quadrierung bei Potenzbildung, vgl. 3.4). Das geht so lange gut (vgl. Bemerkung nach 7.4), solange nicht irgendwann ein Nenner $r$ auftaucht, der nicht teilerfremd zu $n$ ist. Dann ist $ggT(r,n) \neq 1$ ein Teiler von $n$, und falls $ggT(r,n) \neq n$, hat man einen nicht-trivialen Faktor von $n$ gefunden (mit Euklidischem Algorithmus).

Wann tritt ein solcher Fall ein?

## 7.5 Satz

Sei $n$ eine zusammengesetzte Zahl, $ggT(6,n) = 1$.
Sei $E$ eine elliptische Kurve, gegeben durch $y^2 = x^3 + ax + b$ mit $a, b \in \mathbb{Z}$, $ggT(4a^3 + 27b^2, n) = 1$.
Seien $P_1, P_2$ Punkte auf $E(Q) \setminus \{O\}$, wobei die Nenner der Koordinaten teilerfremd zu $n$ seien; es sei $P_1 \neq -P_2$.
Dann gilt:
Die Koordinaten von $P_1 + P_2$ haben (in gekürztem Zustand) Nenner, die teilerfremd zu $n$ sind, genau dann, wenn es keine Primzahl $p \mid n$ gibt mit $P_1 \mod p = -(P_2 \mod P)$. Dabei bezeichnen wir mit $P \mod p$ die Punkte auf der elliptischen Kurve über $\mathbb{Z}_p$, die aus $y^2 = x^3 + ax + b$ durch Reduktion der Koeffizienten $a, b$ modulo $p$ entsteht.

Beweis:
Der Beweis dieses Satzes ist nicht schwierig, aber etwas langwierig, da man die möglichen Fälle der Addition in 7.2 betrachten muss. Einen Beweis findet man z. B. in [6] (Prop. VI.3.1.).

## 7.6 Lenstras Algorithmus

Input: $n$ zusammengesetzte Zahl, $ggT(n,6) = 1$, $n$ keine echte Potenz.

(1) Wähle Schranken $B$ und $C$ (z. B. $B = 20, C = 100.000$)

(2) Wähle $a, x, y \in \mathbb{Z}$, berechne $b = y^2 - x^3 - ax \mod n$.
Ist $ggT(4a^3 + 27b^2, n) = g \neq 1, n$, so gebe $g$ als nicht-trivialen Faktor von $n$ aus.
Ist $g = n$, so wähle neue $a, x, y$.
Ist $g = 1$, so ist $P = (x, y)$ Punkt auf der elliptischen Kurve mit Koeffizienten $a, b$.

(3) Sei $k = \Pi_{(p \leq B)} p^{\alpha_p}$ mit $\alpha_p$ maximal, so dass $p^{\alpha_p} \leq C$. Berechne mit den Gleichungen aus 7.2 $kP \mod n$, falls möglich.

Tritt in einem Zwischenschritt bei der Berechnung von $k_1P = k_2P + k_3P \; mod \; n$ ($k_1 \leq k$) ein Nenner $r$ auf mit $ggT(n,r) \neq 1$, so beende die Berechnung von $kP$.
Ist $d = ggT(n,r) \neq n$, so gebe $d$ als nicht-trivialen Faktor von $n$ aus.
Ist $d = n$, so wähle neue elliptische Kurve und neuen Punkt in (2) und wiederhole das Verfahren.

## 7.7 Bemerkung

a) Tritt in (3) der Fall auf, dass $k_1P = k_2P + k_3P$ modulo $n$ nicht berechenbar ist, so folgt aus 8.5, dass $k_1P \mod p = O$ für einen Primteiler $p \mid n$.
Dies tritt z. B. dann auf, wenn $k_1$ ein Vielfaches der Ordnung $N$ von $E(\mathbb{Z}_p)$ ist (zu der elliptischen Kurve $y^2 = x^3 + ax + b$, Koeffizienten reduziert modulo $p$). Nach dem Satz von Hasse, 7.3, ist $N \in [(p+1) - 2\sqrt{p}, (p+1) + 2\sqrt{p}]$. Ist also $C > (p+1) + 2\sqrt{p}$ für einen Primteiler $p$ von $n$ und ist $N$ nur durch kleine Primzahlen teilbar (alle kleiner als $B$), so ist $k$ ein Vielfaches von $N$ und wir werden in Schritt (3) bei dem Versuch, $k_1P \mod n$ zu berechnen, einen Nenner $r$ finden mit $ggT(n,r) \neq 1$. $ggT(n,r) = n$ wird nur auftreten, wenn für $k_1P \mod O$ für alle $p \mid n$ (dies folgt aus den Rechnungen, die man zum Beweis von 7.5 durchführen muss).
Das ist sehr unwahrscheinlich, vor allem, wenn $n$ mehrere große Primfaktoren besitzt.

b) Der Vorteil des Lenstra-Algorithmus besteht vor allem darin, dass man eine große Anzahl von Wahlmöglichkeiten der elliptischen Kurve hat. Insbesondere wenn $n$ relativ kleine Primteiler besitzt, werden diese schnell gefunden (vgl. a)).

Beispiel: $n = 5429$, $B = 3, C = 92$
($C$ wurde so gewählt, da für einen Primteiler $p < \sqrt{n} = 73$ dann $(p+1) + 2\sqrt{p} < 74 + 2\sqrt{73} < 92$ gilt; vgl. Bemerkung 7.7)
Wähle $y^2 = x^3 + 2x - 2, \quad P = (1,1)$. Es ist $k = 3^4 \cdot 2^6$.
Wir versuchen $2P, 2^2P, 2^3P, 2^6P, 3P, 3^2P, 3^4P, 3 \cdot 2^6P, 3^2 \cdot 2^6P, 3^4 \cdot 2^6P$ zu berechnen.
Beim Versuch der Berechnung von $3^2 \cdot 2^6P$ erhält man einen Nenner, der nicht teilerfremd zu $n$ ist und als größter gemeinsamer Teiler des Nenners und $n$ ergibt sich 61.
Es folgt $n = 61 \cdot 89$.

## 7.8 Komplexität des Lenstra-Algorithmus

Abschätzungen der Komplexität des Lenstra-Algorithmus beruhen vor allem darauf, Aussagen über die Verteilung der Ordnungen $N$ elliptischer Kurven modulo $p$ im „Hasse-Intervall“ $p + 1 - 2\sqrt{p} < N < p + 1 + 2\sqrt{p}$ zu gewinnen und zu ermitteln, wie viele von diesen Ordnungen nur durch kleine Primzahlen teilbar sind.

Mit einer plausiblen, aber bisher noch nicht bewiesenen Vermutung hinsichtlich des

letzten Punktes erhält man eine Komplexität von

$$O\left(e^{\left(\sqrt{(2+\varepsilon)\cdot\ln(p)\cdot\ln(\ln(p))}\ \right)}\right)$$

wobei $p$ der kleinste Primteiler von $n$ ist. Im schlimmsten Fall ($n$ ist Produkt zweier etwa gleich großer Primzahlen) erhält man eine Komplexität von

$$O\left(e^{\left(\sqrt{(1+\varepsilon)\cdot\ln(n)\cdot\ln(\ln(n))}\ \right)}\right)$$

Dies entspricht der Komplexität des quadratischen Siebs.

# Literaturverzeichnis


[1] D. M. Bressoud: Factorization and Primality Testing. Springer, 1989.

[2] J. Buchmann: Einführung in die Kryptographie. Springer, 2001.

[3] R. Crandall, C. Pomerance: Prime Numbers - A Computational Perspective. Springer, 2005

[4] D. E. Knuth: The Art of Computer Programming, Vol.2. Addison-Wesley, 1998. (Übersetzung von [4], Chapter 4: D.E. Knuth: Arithmetik. Springer, 2001)

[5] A. Petho: Algebraische Algorithmen. Vieweg, 1999.

[6] N. Koblitz: A Course in Number Theory and Cryptography. Springer, 1994.

[7] A. K. Lenstra, H. W. Lenstra, jr.: Algorithms in Number Theory. Chap. 12 in Handbook of Theoretical Computer Science (Ed. J. van Leeuwen). Elsevier, 1990.

[8] P. Ribenboim: The Little Book of Bigger Primes. Springer, 2004.

[9] H. Riesel: Prime Numbers and Computer Methods for Factorization. Birkhäuser, 1985.

[10] V. Shoup: A Computational Introduction to Number Theory and Algebra. Cambridge University Press, 2005.

[11] S. Y. Yan: Number Theory for Computing. Springer, 2002.

[12] M. Wolff, P. Hauck, W. Küchlin: Mathematik für Informatik und Bioinformatik. Springer, 2004.

[13] K.-U. Witt: Algebraische Grundlagen der Informatik. Vieweg, 2001.

[14] K. Meyberg: Algebra - Teil 1. Hanser, 1980.

[15] K. Meyberg: Algebra - Teil 2. Hanser, 2002.

[16] I. von zur Gathen, I. Gerhard: Modern Computer Algebra. Cambridge University Press, 1999.

[17] Hardy, Wright: An Introduction to the Theory of Numbers. Oxford University Press, 1980.

[18] M. Nair: On Chebyshev-type inequalities for primes. The American Mathematical Monthly 89, 126 - 129, 1982.

[19] R. Lidl, H. Niederreiter: Introduction to finite fields and their applications. Cambridge University Press, 1994.

[20] A. Werner: Elliptische Kurven in der Kryptographie. Springer, 2002.

[21] J. Silverman: The Arithmetic of Elliptic Curves. Springer, 1986.

# Index