Algorithmische Zahlentheorie und Kryptographie

Mitschrift von www.kuertz.name

Hinweis: Dies ist **kein offizielles Script**, sondern nur eine private Mitschrift. Die Mitschriften sind teweilse **unvollständig, falsch oder inaktuell**, da sie aus dem Zeitraum 2001–2005 stammen. Falls jemand einen Fehler entdeckt, so freue ich mich dennoch über einen kurzen Hinweis per E-Mail – vielen Dank!

Max Tuengerthal (max@17q.de)
und Klaas Ole Kürtz (klaasole@kuertz.net)

Inhaltsverzeichnis

Einführung

Inhalt der Vorlesung wird grob sein:

- *Primzahltests*
  - co-NP
  - NP
  - Test von Lehmann (BPP)
  - Rabin-Miller-Test (co-RP)
  - Strassen-Test (co-RP)
  - Agrawal-Test (Polynomzeit)
- *Faktorisierungsalgorithmen*
- *Elliptische Kurven*

Die ersten beiden Punkte stehen u.a. im Zusammenhang mit RSA (erzeugen von Primzahlen, brechen von RSA). Die elliptischen Kurven stellen eine Alternative zu kryptographischen Systemen auf Basis von Primzahlen dar (ElGamal und weitere).

An mathematischen Inhalten wird es neben vielem Rechnen in endlichen Körpern und Polynomringen u.a. den *Primzahlsatz* geben, der besagt, dass die Anzahl von Primzahlen kleiner n asymptotisch gegen $n \cdot (\log n)^{-1}$ geht, in der Vorlesung wird eine abgeschwächte Version benutzt. Eventuell wird auch der Zusammenhang zwischen Primzahlen und der erweiterten Riemannschen Hypothese (ERH) gezeigt.

Literatur:

- Martin Dietzfelbinger: Primality Testing in Polynomial Time: From Randomized Algorithms to „PRIMES is in P“, Lecture Notes in Computer Science, Bd. 3000, Berlin: Springer 2004.

Noch einige **Konventionen**:

- Mit $\log n$ wird der *binäre Logarithmus* (d.h. zur Basis 2) bezeichnet, mit $\ln n$ der natürliche Logarithmus und mit $\operatorname{Log} n$ die Länge der Binärdarstellung.
- Mit $\langle n \rangle_2$ bezeichnen wir die Binärdarstellung der Zahl n.

1 Primzahltests

Ziel ist hier ein Algorithmus, der zu einer gegebenen Zahl n feststellt, ob n eine Primzahl ist, und das in Zeit polynomiell in $\log n$, d.h. polynomiell in Länge der *Speicherdarstellung* der Zahl.

Eine komplexitätstheoretische Formulierung der Frage wäre:

$$\{ \langle n \rangle_2 \mid n \text{ ist Primzahl} \} =: \mathsf{PRIMES} \in \mathsf{P}$$

1.1 Zahlalgorithmen und deren Komplexität

1.1.1 Komplexitätsmaße

Bei der *Bitkomplexität* zählen wir die Operationen auf einzelnen Bits; mit der *arithmetischen Komplexität* wird die Anzahl der Operationen $+$, $-$, $\cdot$, $\div$ bezeichnet.

Wir werden hier immer *sequentielle Algorithmen* betrachten; parallele oder verteilte Algorithmen, aber auch spezielle Hardware werden (nur) in der Übung betrachtet.

1.1.2 $\mathcal{O}$-, Ω-, Θ-Notation

Wir benutzen $\mathcal{O}$-, Ω- und Θ-Notation wie im Grundstudium, dazu einige Lemmata:

Lemma: Seien $f, g, f', g' \colon \mathbb{N} \to \mathbb{R}_{\geq 0}$ mit $f \in \mathcal{O}(f'), g \in \mathcal{O}(g')$. Dann ist

$$f + g \in \mathcal{O}(\max(f', g')) \text{ und } f \cdot g \in \mathcal{O}(f' \cdot g').$$

Lemma: Seien $f, g \colon \mathbb{N} \times \mathbb{N} \to \mathbb{R}_{\geq 0}$ mit $f \in \mathcal{O}(g)$. Falls $F(m,n) = \sum_{i=0}^{n} f(m,i)$ und $G(m,n) = \sum_{i=0}^{n} g(m,i)$ ist, so ist $F \in \mathcal{O}(G)$.

Lemma: Seien $f, g \colon \mathbb{N} \to \mathbb{R}_{\geq 0}$ mit $g > 0$. Falls $\lim \frac{f}{g} = 0$ ist, so gilt $\mathcal{O}(f) \subsetneq \mathcal{O}(g)$.

Definition: Wir definieren die Menge $\widetilde{\mathcal{O}}(g)$ durch

$$\widetilde{\mathcal{O}}(g) = \left\{ f \mid \exists\, n_0\, \exists\, k\, \exists\, c\, \forall\, n \geq n_0 \colon f(n) \leq c \cdot g(n) \cdot \log^k(g(n)) \right\}$$

1.1.3 Komplexität grundlegender Probleme

Proposition: Seien n und m ganze Zahlen. Die *Schulmethode* zum ...

- Addieren benötigt $\mathcal{O}(\log n + \log m)$ Bitoperationen.
- Subtrahieren benötigt $\mathcal{O}(\log n + \log m)$ Bitoperationen.
- Multiplizieren benötigt $\mathcal{O}(\log n \cdot \log m)$ Bitoperationen.
- Dividieren mit Rest benötigt $\mathcal{O}((\operatorname{Log} m - \operatorname{Log} n + 1) \cdot \operatorname{Log} n)$ Bitoperationen.

In der Übung wird Multiplizieren in $(\log m + \log n)^{1.59}$ (mit $1.59 = \log 3 + \varepsilon$) betrachtet.

Satz: Seien n, m ganze Zahlen mit $\operatorname{Log} n, \operatorname{Log} m \leq k$.

1. Die Methode von Schönhagen und Strassen zum Multiplizieren von m und n benötigt $\mathcal{O}(k \cdot \log k \cdot \log\log k) \subseteq \widetilde{\mathcal{O}}(k)$ Bitoperationen.
2. Die Methode von Newton zum Dividieren mit Rest benötigt ebenfalls $\widetilde{\mathcal{O}}(k)$ Bitoperationen.

Beide Methoden basieren auf der diskreten bzw. schnellen Fourier-Transformation.

Proposition: Die modulare Exponentiation $(a^n \mod m)$ kann mit $\mathcal{O}(\log m \log^2 n)$ (Schulmethode) bzw. $\widetilde{\mathcal{O}}(\log m \log n)$ (Schönhagen, Strassen, Newton) Bitoperationen durchgeführt werden.

Beispiel: Perfekte Potenzen

Definition: Eine Zahl n ist eine *perfekte Potenz*, falls es $a, b \in \mathbb{N}$ gibt mit $a, b \geq 2$ und $a^b = n$.

Idee hier: Teste alle b bis zu einer oberen Schranke, wegen $a \geq 2$ gilt $b \leq \log n$. Um dann für ein festes b ein passendes a zu finden, benutzen wir binäre Suche.
Algorithmus mit Vorbedingung $n \geq 4$:

```
1 b = 2;
2 while (2^b ≤ n) {
3    a_min = 1;
4    a_max = n;
5    while ((a_max − a_min) ≥ 2) {
6       a = 1/2 (a_min + a_max);
```

```
7       p = min(a^b, n+1); // Modulare Exponentiat.
8       if (p == n)
9         return "n = a^b";
10      if (p < n)
11        a_min = a;
12      else
13        a_max = a;
14    }
15    b++;
16  }
17  return "no perfect power";
```

Benutze dabei modifizierte modulare Exponentiation!

Proposition: Der obige Test auf perfekte Potenzen ist korrekt und benötigt $\mathcal{O}(\log^4 n \log^2 n)$ (Schulmethode) bzw. $\widetilde{\mathcal{O}}(\log^3 n)$ (Schönhagen, Strassen, Newton) Bitoperationen.

1.2 Grundlagen der Zahlentheorie

1.2.1 Teilbarkeit und größter gemeinsamer Teiler (ggT)

Die Teilbarkeit ist definiert durch $m \mid n :\Leftrightarrow \exists\, x\colon mx = n$.

Lemma:

1. Falls $k \mid m$ und $k \mid l$, so $k \mid xl + ym$.
2. Falls $k \geq 0, l > 0$ und $k \mid l$, so $k \leq l$.
3. Falls $k \mid l$ und $l \mid m$, so $k \mid m$.
4. Falls $k \mid l$, so $-k \mid l$, $k \mid -l$ und $-k \mid -l$.

Definition: $D(n)$ bezeichnet die Menge der nicht negativen Teiler von n:

$$D(n) := \{x \mid x \geq 0 \text{ und } x \mid n\}.$$

Bemerkungen:

1. $D(n) \neq \emptyset$.
2. Falls $n \neq 0$, so ist $D(n)$ endlich.

Definition: Der *größte geimansame Teiler* $\mathrm{ggT}(m,n)$ (kurz: (m,n)) zweier Zahlen m,n ist wie folgt definiert:

$$(m,n) := \mathrm{ggT}(m,n) := \begin{cases} \max(D(m) \cap D(n)) & \text{falls } m \neq 0 \text{ oder } n \neq 0 \\ 0 & \text{sonst} \end{cases}$$

Zwei Zahlen m,n heißen *teilerfremd*, in Zeichen $m \top n$, falls $(m,n) = 1$.

Lemma: Für den größten gemeinsamen Teiler gelten folgende Gesetzmäßigkeiten:

1. $(m,n) = (n,m)$
2. $(m,n) = (-m,n) = (m,-n) = (-m,-n)$
3. $(m,0) = (m,m) = m$
4. $(m,n) = (m, n+xm)$ (insbesondere $(m,n) = (m,n-m)$)

Proposition: Für $n \in \mathbb{Z}$ und $d > 0$ existieren eindeutige q,r mit $0 \leq r < d$, so dass $n = q \cdot d + r$.

Definition: Sei $n = q \cdot d + r$ mit $d > 0$, $0 \leq r < d$. Wir definieren dann

$$n \bmod d := r \quad \text{und} \quad n \operatorname{div} d := q$$

Wegen obiger Proposition ist dies wohldefiniert.

Proposition:

1. Für $m > 0$ gilt, dass $(m,n) = (m, n \bmod m)$ ist.
2. Für alle $m,n \in \mathbb{Z}$ existieren $x,y \in \mathbb{Z}$ mit $(m,n) = xm + yn$.
3. Für alle $m,n \in \mathbb{Z}$ sind m,n teilerfremd genau dann, wenn x,y existieren mit $1 = xm + yn$.
4. Für alle $k,m,n \in \mathbb{Z}$ gilt $|k| \cdot (m,n) = (km,kn)$
5. Sind m,n teilerfremd, so ist $(l,m) = (ln,m)$
6. Sind m,n teilerfremd und $m \mid k$ sowie $n \mid k$, so ist $mn \mid k$.

Beweis:

1. als Übung für den interessierten Leser

2. Zuerst schränken wir uns ein auf $m, n \geq 0$, dies wird bewiesen per Induktion über $m + n$.

   - Induktionsanfang: $m + n = 0$, also $m = n = 0$. Dann gilt $0 = 0 \cdot 0 + 0 \cdot 0$.
   - Induktionsschritt: Falls $m \geq n$ ist, dann ist $m - n \geq 0$ und $(m, n) \stackrel{\text{IA}}{=} (m - n, n)$. Also existieren x', y' mit $(m, n) = x'(m - n) + y'n = x'm + (y' - x')n$. Setze $x = x'$ und $y = y' - x'$.
     Der Fall $n < m$ ist analog.

   Für den allgemeinen Fall beachte $(m, n) = (-m, n)$ etc.

3. als Übung für den interessierten Leser

- *Vorüberlegung*: Falls $m \neq 0$ oder $n \neq 0$ sind, dann ist

$$(m, n) = \min \{ xm + yn > 0 \mid x \in \mathbb{Z}, y \in \mathbb{Z} \} .$$

  Dies ist erfüllt, weil folgendes gilt:

  - Es gilt $(m, n) \in \{ xm + yn > 0 \mid x \in \mathbb{Z}, y \in \mathbb{Z} \}$ wegen 2.
  - Angenommen, $0 < xm + yn < (m, n)$; wegen $(m, n) \mid m$ und $(m, n) \mid n$ würde dann $(m, n) \mid xm + yn$ gelten, also $(m, n) \leq xm + yn$ nach obigem Lemma, Widerspruch.

4. Wir zeigen $|k|(m, n) \leq (km, kn)$ und $|k|(m, n) \geq (km, kn)$:

   - Für alle l mit $l \mid m$ und $l \mid n$ gilt $kl \mid km$ und $kl \mid kn$, also $|k|(m, n) \mid (km, kn)$, also $|k|(m, n) \leq (km, kn)$.
   - Wegen 2. gilt $|k|(m, n) = |k|(xm + yn) = x'km + y'kn$, wegen der Vorüberlegung ist dies $\geq (km, kn)$.

5. Wieder zeigen wir $(l, m) \leq (ln, m)$ und $(l, m) \geq (ln, m)$.

   - trivial
   - Wähle x', y' mit $x'm + y'n = 1$.

$$\begin{aligned} (l, m) &= xl + ym = (xl + ym)(x'm + y'n) \\ &= xy'nl + (xlx' + ymx' + yy'n) \cdot m \geq (nl, m) \end{aligned}$$

     Dabei gilt die letzte Abschätzung wegen der Vorüberlegung.

6. Da $m \top n$ teilerfremd sind, existieren x und y mit $xm + yn = 1$, wähle x' und y' mit $mx' = k$ und $ny' = k$. Damit gilt: $k = kxm + kyn = ny'xm + mx'yn$, damit $mn \mid k$. □

1.2.2 Euklidscher Algorithmus

Vorbedingung ist $m, n \in \mathbb{Z}$, als **Invariante** kann man angeben:

$$(a = xm + yn) \ \wedge \ (b = x^\star m + y^\star n) \ \wedge \ (a \geq b \geq 0) \ \wedge \ ((a, b) = (m, n))$$

```
1  if (|m| ≥ |n|) {
2    (a, b) = (|m|, |n|);
3    (x, x*) = (sgn(m), 0);
4    (y, y*) = (0, sgn(n));
5  } else {
6    (a, b) = (|n|, |m|);
7    (x, x*) = (0, sgn(m));
8    (y, y*) = (sgn(n), 0);
9  }
10 while (b > 0) {
11   q = a / b;
12   (a, b) = (b, a−qb) // parallel
13   (x, y, x*, y*) := (x*, y*, x−qx*, y−qy*)
14 }
```

Am Ende gilt die **Nachbedingung** $a = (m, n) = xm + yn$.

Proposition: Der obige Algorithmus zur Berechnung des ggT zweier Zahlen m und n und einer zugehörigen Linearkombination ist korrekt und kommt mit $\mathcal{O}(\max\{\log m, \log n\})$ arithmetischen und $\mathcal{O}(\log m \cdot \log n)$ Bitoperationen aus.

Beweis:

- **Korrektheit**: Benutze obige Invariante, **Beispiel:**

$$\begin{array}{rcrcl} a & & b & & \\ 27 & = & 15 & \cdot & 1 + 12 \\ 15 & = & 12 & \cdot & 1 + 3 \\ 12 & = & 3 & \cdot & 4 + 0 \end{array}$$

- **Laufzeit**: Vorbetrachtung: Für $0 < b \leq a$ gilt: $a \bmod b < \frac{1}{2}a$. Dazu:

  1. Fall: $b \leq \frac{1}{2}a$, dann gilt sofort $a \bmod b < b \leq \frac{1}{2}a$, also $a \bmod b < \frac{1}{2}a$.

2. Fall: $b > \frac{1}{2}a$, dann gilt $a \text{ div } b = 1$ und $a \bmod b = a - b < \frac{1}{2}a$.

Also führt der Algorithmus die `while`-Schleife höchstens $2 \cdot \max\{\log m + \log n\}$ mal aus, d.h. es gibt nur $\mathcal{O}(\max\{\log m, \log n\})$ viele arithmetische Operationen.

Wir beweisen nun eine vereinfachte Variante, um den Beweis zu verkürzen, in der folgendes benutzt wird:

$$(a, b) = \begin{cases} (b, a \bmod b) & \text{falls} \quad b \neq 0 \\ a & \text{falls} \quad b = 0 \end{cases} .$$

Wenn $T(a, b)$ die Anzahl der Bitoperationen bezeichnet, ist nun zu zeigen:

$$T(a, b) \leq c \cdot \operatorname{Log} a \cdot \operatorname{Log} b + c$$

Es gilt nun per Induktion:

$$\begin{aligned} T(a, b) &\leq T(b, a \bmod b) + d \cdot (\operatorname{Log} a - \operatorname{Log} b + 1) \cdot \operatorname{Log} b + d \\ &\leq c \operatorname{Log} b \operatorname{Log}(a \bmod b) + d \cdot (\operatorname{Log} a - \operatorname{Log} b + 1) \cdot \operatorname{Log} b + d \\ &= c \operatorname{Log} b \operatorname{Log} a + c + \\ &\quad \underbrace{(c \cdot \operatorname{Log}(a \bmod b) + 2d - (c - d) \cdot \operatorname{Log} a - d \operatorname{Log} b) \cdot \operatorname{Log} b}_{=:X \quad \text{zu zeigen: } \leq 0} \end{aligned}$$

Fallunterscheidung:

- Falls $\operatorname{Log} a = \operatorname{Log} b$ ist, so gilt $\operatorname{Log}(a \bmod b) \leq \operatorname{Log} a - 1$. Damit ergibt sich:

$$\begin{aligned} X &\leq c(\operatorname{Log} a - 1) + 2d - (c - d) \operatorname{Log} a - d \operatorname{Log} b \\ &= c(\operatorname{Log} a - \operatorname{Log} a) + d(\operatorname{Log} a - \operatorname{Log} b) + 2d - c \\ &\leq 2d - c \end{aligned}$$

  Für diesen Fall muss also $c \geq 2d$ sein.

- Falls $\operatorname{Log} b < \operatorname{Log} a$ ist, so gilt ebenfalls: $\operatorname{Log}(a \bmod b) \leq \operatorname{Log} b$, also:

$$\begin{aligned} X &\leq c(\operatorname{Log} b) + 2d - (c - d) \operatorname{Log} a - d \operatorname{Log} b \\ &= (d - c)(\operatorname{Log} a - \operatorname{Log} b) + 2d \\ &\leq (d - c) + 2d = 3d - c \end{aligned}$$

  In diesem Fall reicht also $c \geq 3d$. □

Bemerkung: Um den einfachen Algorithmus zu verbessern, kann man folgendes verwenden:

$$\mathrm{ggT}(a,b) = \begin{cases} \mathrm{ggT}(b, \min\{a \bmod b, b - a \bmod b\} & \text{falls} \quad b \neq 0 \\ a & \text{falls} \quad b = 0 \end{cases}$$

1.2.3 Modulare Arithmetik

Definition: Eine *Halbgruppe* $(M, \cdot)$ ist eine Menge M mit einer inneren Verknüpfung $\cdot$, für die das Assoziativgesetz gilt, d.h.

1. Assoziativität: $\forall\, a, b, c \in M \colon (a \cdot b) \cdot c = a \cdot (b \cdot c)$.

Definition: Ein *Monoid* ist eine Halbgruppe $(M, \cdot)$ mit einem neutralen Element 1, d.h. es gilt:

1. Assoziativität: $\forall\, a, b, c \in M \colon (a \cdot b) \cdot c = a \cdot (b \cdot c)$ und
2. Neutrales Element: $\exists\, 1 \in M\, \forall\, a \in M \colon a \cdot 1 = 1 \cdot a = a$.

Definition: Eine *Gruppe* ist ein Paar $(M, \cdot)$ mit einer Menge M und einer inneren Verknüpfung $\cdot$, so dass gilt:

1. Assoziativität: $\forall\, a, b, c \in M \colon (a \cdot b) \cdot c = a \cdot (b \cdot c)$ und
2. Neutrales Element: $\exists\, 1 \in M\, \forall\, a \in M \colon a \cdot 1 = 1 \cdot a = a$ und
3. Inverses Element: $\forall\, a \in M\, \exists\, b \in M \colon a \cdot b = 1$.

Mit $a \equiv b \pmod{m}$ bezeichnet man $m \mid a - b$ für $m > 0$.

Lemma: Für jedes $m > 0$ ist „$\cdot \equiv \cdot \pmod{m}$“ eine *Kongruenzrelation* bezüglich $+$ und $\cdot$, d.h. falls $a \equiv b \pmod{m}$ und $a' \equiv b' \pmod{m}$, so ist $a + a' \equiv b + b' \pmod{m}$ und $aa' \equiv bb' \pmod{m}$.

Definition: Ein *Ring* ist ein Tupel $(R, +, \cdot, 0)$, ein *Ring mit Eins* ist $(R, +, \cdot, 0, 1)$ (mit $0 \neq 1$), wobei jeweils folgende Eigenschaften gelten:

1. $(R, +, 0)$ ist eine kommutative Gruppe,
2. $(R, \cdot)$ ist eine Halbgruppe,

3. es gilt das Distributivgesetz, d.h. für alle $a, b, c \in R$ gilt

$$a \cdot (a + b) = a \cdot b + a \cdot c$$
$$(a + b) \cdot c = a \cdot c + b \cdot c,$$

4. die 1 ist das neutrale Element der Multiplikation.

Bei einem *kommutativen Ring* ist die Multiplikation zusätzlich kommutativ.

Konvention: Wir werden hier im Folgenden nur noch über **kommutative Ringe mit Eins** sprechen.

Proposition: Für jedes $m > 1$ ist $\mathbb{Z}_m$ ein kommutativer Ring mit Eins, d.h. ein Ring in unserem Sinne.

Lemma:

- Falls $m \mid ab$ und $m \top a$, so ist $m \mid b$.
- Falls $m \top a$ und $ab \equiv ac \pmod{m}$, so $b \equiv c \pmod{m}$.

Beweis:

1. Es gilt $xm + ya = 1$ (wegen der Teilerfremdheit), daraus folgt $xmb + yab = b$. Außerdem gilt $mt = ab$ für ein t, also $b = xmb + ymt$, somit ist $b = m(xb + yt)$.
2. Es gilt $m \mid ab - ac = a(b - c)$, daraus folgt wg. des ersten Teils $m \mid b - c$.

□

Definition: Sei R ein Ring.

- Ein *Nullteiler* ist ein Element $a \in R$, so dass $b \in R \setminus \{0\}$ existiert mit $ab = 0$.
- R^* sei die *Menge der Einheiten*, d.h. die Menge der bezüglich $\cdot$ invertierbaren Elemente.

Bemerkung: R^* bildet eine Gruppe, die *Einheitengruppe*.

Proposition: Für $m > 1$ gilt:

$$\mathbb{Z}_m^* = \{ i < m \mid i \top m \}.$$

Beweis:

„$\supseteq$“ Gelte $i < m$ und $i \top m$. Dann ist $xi + ym = 1$, also $xi \equiv 1 \pmod{m}$, damit ist schon $x = i^{-1}$ in $\mathbb{Z}_m$.

„$\subseteq$“ Gelte $i \not\top m$, also existiert $(i, m) = d > 1$. Setze $c = \frac{m}{d}$, dann gilt $m \mid ic = i\frac{m}{d} = dt\frac{m}{d} = tm = 0$, aber $c \neq 0$, also ist i ein Nullteiler und damit keine Eineheit. □

Definition: Die *Eulersche Phi-Funktion* ist definiert als

$$\varphi(m) = |\mathbb{Z}_m^*| .$$

1.2.4 Chinesischer Restsatz

Definition: Seien $R_1 = (R_1, +, \cdot, 0, 1)$ und $R_2 = (R_2, +, \cdot, 0, 1)$ zwei Ringe. Eine Abbildung $f\colon R_1 \to R_2$ heißt *Ringhomomorphismus*, wenn für alle $a, b \in R_1$ gilt:

- $f(a + b) = f(a) + f(b)$
- $f(a \cdot b) = f(a) \cdot f(b)$

Definition: Das **Produkt** $R_0 \times R_1$ auf Ringen $R_0 = (R_0, +_0, \cdot_0, 0_0, 1_0)$, $R_1 = (R_1, +_1, \cdot_1, 0_1, 1_1)$ ist definiert als

$$(R_0 \times R_1, +, \cdot, (0_0, 0_1) =: 0, (1_0, 1_1) =: 1)$$

mit $(a_0, a_1) + (b_0, b_1) := (a_0 +_0 b_0, a_1 +_1 b_1)$ (und für $\cdot$ entsprechend).

Satz (Chinesischer Restsatz): Seien $m, n > 1$ mit $m \top n$. Dann ist die folgende Abbildung ein Ringisomorphismus:

$$\mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n \text{ mit } a \mapsto (a \bmod m, a \bmod n)$$

Beweis: Die Homomorphie-Eigenschaften werden wir nicht nachweisen, jedoch die Bijektivität.
Sei $a = yn \bmod m = 1$ und $a = yn \bmod n = 0$, außerdem $b = xm \bmod m = 0$ und $b = xm \bmod n = 1$. Sei nun $(c, d) \in \mathbb{Z}_m \times \mathbb{Z}_n$. Dann gilt: $ca + db \bmod m = c$ und $ca + db \bmod n = d$, also $ca + db \bmod mn \mapsto (c, d)$. □

Folgerung:

1. $R^* = R_0^* \times R_1^*$.

2. Multiplikativität: Falls $m \top n$ ist mit $m, n > 1$, so ist $\varphi(mn) = \varphi(m)\varphi(n)$.

3. Sei $m \top n$ mit $m, n > 1$ und $a < m, b < m$. Dann existiert genau ein $x < mn$ mit $x \bmod m = a$, $x \bmod n = b$.

1.2.5 Primzahlen

Definition: *Primzahlen* sind Zahlen größer Null mit zwei Teilern größer Null.

Lemma: Jede Zahl, die größer als Eins ist, ist durch eine Primzahl teilbar.

Bemerkung: Ist p Primzahl und $(p, m) \neq 1$, so gilt $p \mid m$.

Satz: Es gibt unendlich viele Primzahlen.

Sei $n \geq 2$. Dann ist das **Sieb des Eratosthenes** folgender Algorithmus:

```
1  m = new int[n+1]; // belegt mit 0
2  j = 2;
3  while (j^2 < n) {
4     if (m[j] == 0) {
5        i = j^2;
6        while (i ≤ n) {
7           if (m[i] == 0)
8              m[i] = j;
9           i += j;
10    } }
11    j++;
12 }
```

Satz: Das Sieb des Eratosthenes ist korrekt bezüglich folgender Nachbedingung:

$$\forall i\colon (2 \leq i \leq n \rightarrow ((m[i] = 0 \leftrightarrow \text{prime}(i)) \\ \wedge (m[i] \neq 0 \rightarrow m[i] \text{ kleinster Primteiler von } i)))$$

Der Algorithmus kommt mit $\mathcal{O}(n \log n)$ Schritten aus (genauer: $\Theta(n \log \log n)$).

Beweis: Die Laufzeitschranke läßt sich abschätzen als

$$\mathcal{O}\left(\sum_{p\leq n}\frac{n}{p}\right)\subseteq\mathcal{O}\left(n\cdot\sum_{i\leq n}\frac{1}{i}\right)\subseteq\mathcal{O}(n\cdot(\ln n+1))$$

□

Definition: Eine *Primfaktorzerlegung* von n ist eine endliche Folge $p_1,\ldots,p_r$ von Primzahlen mit $p_i\leq p_{i+1}$ und $\prod_i p_i = n$.

Satz: Jede positive Zahl besitzt eine Primfaktorzerlegung.

Beweis: über obiges Lemma, dass jede Zahl größer zwei durch eine Primzahl teilbar ist.

Lemma: Falls $p \mid n$ mit einer Primzahl p und $n \geq 1$, so gibt es eine Primfaktorzerlegung von n mit p.

Satz (Fundamentalsatz der Arithmetik): Jede positive ganze Zahl hat *genau* eine Primfaktorzerlegung.

Beweis: Angenommen, n sei eine kleinste Zahl mit mindestens zwei Primfaktorzerlegungen

$$n = p_0^{\alpha_0}\cdot\ldots\cdot p_{r-1}^{\alpha_{r-1}}$$
$$n = q_0^{\beta_0}\cdot\ldots\cdot q_{j-1}^{\beta_{j-1}}$$

O.B.d.A. sei $p_0 < q_0$. Sei nun

$$m = n-(p_0 q_0^{\beta_0-1}\cdot\ldots\cdot q_{j-1}^{\beta_{j-1}}) = (q_0-p_0)\cdot(q_0^{\beta_0-1}\cdot\ldots\cdot q_{j-1}^{\beta_{j-1}})$$

Damit hat m eine Primfaktorzerlegung ohne p_0, indem rechts $(q_0 - p_0)$ durch eine Primfaktorzerlegung ersetzt wird, aber es gilt auch $p_0 \mid m$, also hat m auch eine Zerlegung mit p_0. Dies ist ein Widerspruch zur Minimalität von n. □

Folgerungen:

1. Falls p eine Primzahl ist und $p \mid mn$, so gilt $p \mid m$ oder $p \mid n$.
2. Falls $p_0,\ldots,p_{r-1}$ verschiedene Primzahlen sind und $p_i \mid n$ für alle $i < r$ gilt, so $p_0\cdots p_{r-1} \mid n$.
3. Seien $(p_0,\ldots,p_{r-1})$ und $(q_0,\ldots,q_{r-1})$ Primfaktorzerlegungen von m bzw. n. Dann gilt $m\top n$ genau dann, wenn $\{p_0,\ldots,p_{r-1}\}\cap\{q_0,\ldots,q_{s-1}\}=\emptyset$ ist.

Beweis:

1. m hat eine Primfaktorzerlegung, n hat eine. Daraus ergibt sich *die* Zerlegung von mn. Nach einem obigen Lemma kommt p in *einer* Primfaktorzerlegung von mn vor, also in *der* Primfaktorzerlegung von mn, also auch in einer von m oder einer von n. □

Satz: Sei $n \geq 0$ und $n = p_0^{k_0} \cdots p_{r-1}^{k_{r-1}}$ die Primfaktorzerlegung von n. Dann gilt:

$$\varphi(n) = \prod_{i<r} (p_i - 1) p_i^{k_i - 1} = n \prod_{i<r} \left(1 - \frac{1}{p_i}\right).$$

Beweis: Nach Chinesischem Restsatz brauchen wir nur zu zeigen, dass $\varphi(p^k) = (p-1)p^{k-1}$ gilt.

$$\begin{aligned}
\varphi(p^k) &= \left|\left\{ i < p^k \;\middle|\; i \top p^k \right\}\right| \\
&= \left|\left\{ i < p^k \;\middle|\; p \nmid i \right\}\right| \\
&= p^k - \left|\left\{ i < p^k \;\middle|\; p \mid i \right\}\right| \\
&= p^k - \left|0, p, 2p, \ldots, (p^{k-1} - 1)p\right| \\
&= p^k - p^{k-1}
\end{aligned}$$

□

1.2.6 Primzahlsatz und Satz von Чебышёв

Definition: Die folgende Funktion gibt die Anzahl der Primzahlen kleiner n an:

$$\pi \colon \mathbb{N}_{>0} \to \mathbb{N} \text{ mit } \pi \colon n \mapsto |\{p \in \mathbb{P} \mid p \leq n\}|$$

Der Primzahlsatz gibt an, wie groß $\pi(n)$ wird:

Primzahlsatz (1896, Hadamard, de la Vallée Poussin):

$$\lim_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = \lim_{n\to\infty} \frac{\frac{\pi(n)}{n}}{\frac{1}{\ln n}} = 1$$

Eine abgeschwächte Version ist diese Ungleichung von Чебышёв (Tschebyschow/Chebyshev):

Satz von Чебышёв: Für $n \geq 2$ gilt

$$\frac{n}{\log n} - 2 \leq \pi(n) \leq \frac{3n}{\log n}$$

Beweis des Satzes von Чебышёв: Wir benötigen Binomialkoeffizienten, daher zunächst einige Rechenregeln:

Lemma:

1. $\binom{n}{0} = \binom{n}{n} = 1$
2. $\binom{n}{k} + \binom{n}{k+1} = \binom{n+1}{k+1}$
3. $\binom{n}{k} = \binom{n}{n-k}$
4. $\binom{n}{k} < \binom{n}{k+1}$ für $k < \lfloor \frac{n}{2} \rfloor$
5. $2^n \leq \frac{2^{2n}}{2n} \leq \binom{2n}{n} < 2^{2n}$ für $n > 0$

Wir zeigen nun zunächst die **untere Schranke** $\frac{n}{\log n} - 2 \leq \pi(n)$. Definiere dafür $K_n = \binom{2n}{n}$, seien weiter

$$\nu_p(n) = \max\{i : p^i \mid n\} \text{ und } N_p(n) = \max\{p^i : p^i \mid n\}.$$

Lemma (Legendre):

$$\nu_p(n!) = \sum_{k>0} \left\lfloor \frac{n}{p^k} \right\rfloor.$$

Beweis: Betrachte die Relation $R(p,n) = \{(i,k) : 1 \leq i \leq n, p^k \mid i\}$. Als Matrix für $p = 2$, $n = 16$ ergibt sich:

	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	0	1	0	1	0	1	0	1	0	1	0	1	0	1	0	1
2	0	0	0	1	0	0	0	1	0	0	0	1	0	0	0	1
3	0	0	0	0	0	0	0	1	0	0	0	0	0	0	0	1
4	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	1

Wir summieren einmal *zeilenweise* und einmal *spaltenweise*:

$$\underbrace{\sum_{k>0} \left\lfloor \frac{n}{p^k} \right\rfloor}_{\text{zeilenweise}} = \underbrace{\sum_{1 \leq i \leq n} \nu_p(i)}_{\text{spaltenweise}} \overset{(\star)}{=} \nu_p(n!)$$

Dabei gilt $(\star)$, da es im Falle $p^k \mid n!$ Zahlen $1 \leq i_0 < \ldots < i_{r-1} \leq n$ und $k_0, \ldots, k_{r-1}$ gibt mit $k_0 + \ldots + k_{r-1} = k$ und $p^{k_j} \mid i_j$ für alle $j < r$ nach Folgerung aus dem Fundamentalsatz. □

Lemma: Für alle nicht-negativen reellen Zahlen x gilt

$$\lfloor 2 \cdot x \rfloor - 2 \cdot \lfloor x \rfloor \in \{0, 1\}.$$

Beweis: In der Übung.

Lemma: Für alle p gilt $N_p(K_n) \leq 2n$.

Beweis: Sei p eine beliebige Primzahl. Dann gilt:

$$\begin{aligned}
\nu_p(K_n) &= \nu_p\left(\frac{(2n)!}{n! \cdot n!}\right) = \nu_p((2n)!) - 2\nu_p(n!) \\
&= \sum_{k>0} \left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \sum_{k>0} \left\lfloor \frac{n}{p^k} \right\rfloor = \sum_{k>0} \underbrace{\left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right)}_{\in\{0,1\}} \\
&= \sum_{\substack{k>0 \\ p^k \leq 2n}} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right) \leq \max_k \{p^k \leq 2n\}
\end{aligned}$$

Also gilt:

$$N_p(K_n) \leq p^{\nu_p(K_n)} \leq p^{\max_k \{p^k \leq 2n\}} \leq 2n.$$

□

Lemma: Für $n > 0$ gilt $K_n \leq (2n)^{\pi(2n)}$.

Beweis: Sei $K_n = p_0^{k_0} \cdots p_{r-1}^{k_{r-1}}$ die Primfaktorzerlegung von K_n. Da wir $\nu_p(K_n) = 0$ für $p > 2n$ haben, gilt $p_i \leq 2n$ für alle $i < r$, also $r \leq \pi(2n)$. Insgesamt gilt: $K_n \leq (2n)^{\pi(2n)}$. □

Mit beiden Abschätzungen für K_n zusammen erhalten wir:

$$\frac{2^{2n}}{2n} \leq K_n \leq (2n)^{\pi(2n)}$$

Daraus erhalten wir durch Logarithmieren:

$$2n - \log 2n \leq \pi(2n) \cdot \log 2n \quad \Rightarrow \quad \pi(2n) \geq \frac{2n}{\log 2n} - 1.$$

Hieraus können wir die untere Schranke folgern:

- Für gerades n gilt $\pi(n) \geq \frac{n}{\log n} - 1$.

- Für ungerades n gilt (mit $n = 2m + 1$):

$$\begin{aligned}\pi(n) = \pi(2m+1) \geq \pi(2m) &\geq \frac{2m}{\log 2m} - 1 > \frac{2m}{\log(2m+1)} - 1 \\ &= \frac{2m+1}{\log(2m+1)} - \frac{1}{\log(2m+1)} - 1 \\ &\geq \frac{2m+1}{\log(2m+1)} - 2\end{aligned}$$

Damit ist die untere Schranke bewiesen. □

Wir beweisen nun die **obere Schranke** $\pi(n) \leq \frac{3n}{\log n}$. Sei $B_m = \binom{2m+1}{m}$.

Lemma: Es gilt für $m \in \mathbb{N}$ und Primzahlen p:

$$\prod_{m+2 \leq p \leq 2m+1} p \leq B_m.$$

Beweis: Es gilt:

$$B_m = \frac{(2m+1)!}{(m+1)! \cdot m!} = \frac{(m+2) \cdots (2m+1)}{1 \cdots m}$$

Also gilt für jede Primzahl p mit $m + 2 \leq p \leq 2m + 1$, dass $p \mid B_m$. Daraus folgt die Behauptung. □

Lemma: Es gilt $B_m < 4^m$.

Beweis: Es gilt:

$$2B_m = \binom{2m+1}{m} + \binom{2m+1}{m+1} < \sum_{i=0}^{2m+1} \binom{2m+1}{i} = 2^{2m+1} = 2 \cdot 4^m$$

□

Lemma (Erdös): Für $n \geq 2$ und Primzahlen p gilt:

$$\prod_{p \leq n} p \leq 4^{n-1}.$$

Beweis: Per Indukion über n:

- Induktionsanfang $n = 2$ klar.
- Induktionsschritt: Fallunterscheidung

a) n gerade:

$$\prod_{p \leq n} p = \prod_{p \leq n-1} p \overset{\text{I.V.}}{<} 4^{n-2} \leq 4^{n-1}.$$

b) n ungerade:

$$\begin{aligned}\prod_{p \leq 2m+1} p &= \prod_{p < m+2} p \cdot \prod_{\substack{m+2 \leq p \\ p \leq 2m+1}} p \leq \left(\prod_{p < m+2} p \right) \cdot B_m \\ &< \prod_{p \leq m+1} p \cdot 4^m \overset{\text{I.V.}}{\leq} 4^m \cdot 4^m = 4^{(2m+1)-1}.\end{aligned}$$

□

Lemma: Für alle $k \geq 9$ und verschiedene Primzahlen $p_0, \ldots, p_{k-1}$ gilt

$$2^k k! \leq p_0 \cdots p_{k-1}.$$

Beweis: Per Induktion:

- $k = 9$ per Hand.
- $k > 9$: Annahme: p_{k-1} sei maximal. Dann gilt:

$$\begin{aligned}p_0 \cdots p_{k-1} &= (p_0 \cdots p_{k-2}) p_{k-1} \geq 2^{k-1}(k-1)! \cdot p_{k-1} \\ &\overset{(\star)}{\geq} 2^{k-1}(k-1)!\ 2k = 2^k k!\end{aligned}$$

Dabei gilt $(\star)$, da p_{k-1} größergleich der k-ten Primzahl $\geq 2k$ ist. □

Lemma:

$$\left(\frac{k}{e}\right)^k < k!.$$

Beweis: Zunächst gilt:

$$e^x = \sum \frac{x^i}{i!} \Rightarrow e^k = \sum \frac{k^i}{i!} > \frac{k^k}{k!}.$$

□

Setze nun $k = \pi(n)$. Es gilt:

$$2^k \left(\frac{k}{e}\right)^k < 2^k k! \leq \prod_{p \leq n} p < 4^{n-1}.$$

Also:

$$2^k \left(\frac{k}{e}\right)^k < 4^{n-1} \qquad (\star\star)$$

Wir können 4^{n-1} schreiben als $(2^2)^{n-1}$, dann folgt $k \cdot (\ln k + \ln 2 - 1) < (2 \ln 2)n$. Wir zeigen daraus per Widerspruchsbeweis, dass gilt:

$$k < \frac{2n}{\ln n} \leq \frac{3n}{\log n}$$

Wir nehmen also an: $k \geq \frac{2n}{\ln n}$. Einsetzen in $(\star\star)$ liefert:

$$2(\ln 2)n > \frac{2n}{\ln n}\left(\ln \frac{2n}{\ln n} + \ln 2 - 1\right) = \frac{2n}{\ln n}(\ln n + \ln 2 - \ln \ln n + \ln 2 - 1).$$

Daraus ergibt sich: $(1 - \ln 2) \ln n < \ln \ln n - 2 \ln 2 + 1$. Für $n \geq 27$ ergibt sich ein Widerspruch (siehe Übung), für $n < 27$ läßt sich dies per Hand nachrechnen.

Damit ist der Satz von Чебышёв bewiesen. □

Bemerkung: Zum Lemma von Erdös, das besagt, dass $\prod_{p \leq n} p < 4^{n-1}$ ist, gilt als untere Schranke:

Satz: Für $n \geq 2$ gilt $\prod_{p \leq 2n} p > 2^n$.

Beweis: Gleiche Technik.

1.3 Algebraische Grundlagen

1.3.1 Gruppen und Untergruppen

Definition: Eine *Gruppe* ist $G = (G, \cdot)$ mit $(\cdot)\colon G \times G \to G$ assoziativ und zusätzlich gibt es $1 \in G$ *(neutrales Element)* mit

1. $g \cdot 1 = 1 \cdot g = g$ für alle $g \in G$.
2. für alle $g \in G$ existiert $h \in G$ *(inverses Element zu g, Notation g^{-1})* mit $g \cdot h = h \cdot g = 1$.

Die Gruppe heißt *kommutativ (abelsch)*, falls die Verknüpfung kommutativ ist.

Lemma:

1. Das neutrale Element ist eindeutig bestimmt.

2. Das inverse Element ist für jedes Element aus G eindeutig bestimmt.
3. Für alle $a, b, c \in G$ gilt: Falls $ab = ac$, so $b = c$.

Beweis:

1. Angenommen, 1 und $1'$ sind neutrale Elemente. Dann gilt: $1 = 1 \cdot 1' = 1'$.
2. Angenommen, es gibt h und h' mit $h \cdot g = g \cdot h = 1$ und $h' \cdot g = g \cdot h' = 1$. Dann insbesondere $gh = 1 = gh'$, also $h = h'$ nach 3.
3. Zu $a \in G$ betrachte die Funktion $f\colon b \to a \cdot b$. Sei dazu a' ein inverses zu a, betrachte außerdem $g\colon b \to a'b$. Dann gilt: $(g \circ f)(b) = a'(ab) = (a'a)b = b$, also $g \circ f = \mathrm{id}$. Außerdem: $f \circ g(b) = a(a'b) = (aa')b = b$, also $f \circ g = \mathrm{id}$, also f und g Bijektionen.

Definition: Die *Ordnung* einer Gruppe ist $|G|$ (bei unendlichen Gruppen ist $|G| = \infty$).

Lemma: Sei G eine Gruppe und sei $H \subseteq G$ endlich. Dann ist H Untergruppe von G genau dann, wenn $1 \in H$ und $H \cdot H \subseteq H$ ist.

Beweis: Zu zeigen: Für alle $h \in H$ gilt $h^{-1} \in H$. Betrachte $f\colon H \to H$ mit $a \mapsto ah$. Dann ist f injektiv wegen der Kürzungsregel, also surjektiv, da H endlich. Es existiert $a \in H$ mit $ah = 1$. Zeige: $a = h^{-1}$. Es gilt: $a = a1 = a(hh^{-1}) = (ah)h^{-1} = 1h^{-1} = h^{-1}$.

Definition: Sei G eine Gruppe und H eine Untergruppe. Definiere $\equiv_H$ auf G durch $g \equiv_H h$ genau dann, wenn $gh^{-1} \in H$.

Lemma:

1. Die Relation $\equiv_H$ ist eine Äquivalenzrelation, deren Klassen als Nebenklassen von G bezüglich H bezeichnet werden.
2. Die Äquivalenzklassen von $\equiv_H$ haben dieselbe Mächtigkeit.

Beweis: Zunächst als Rechenregel: $(ab)^{-1} = b^{-1}a^{-1}$, das gilt wegen

$$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = aa^{-1} = 1.$$

1. Die Relation $\equiv_H$ ist reflexiv, da $gg^{-1} = 1 \in H$ ist. Symmetrisch: Sei $gh^{-1} \in H$, dann ist $hg^{-1} = (gh^{-1})^{-1} \in H$. Zu Transitivität: Seien $gh^{-1} \in H$ und $hj^{-1} \in H$. Dann ist $gj^{-1} = g(h^{-1}h)j^{-1} = (gh^{-1})(hj^{-1}) \in HH \subseteq H$.

2. Zu $g \in G$ betrachte $f\colon [1] \to [g]$, definiert durch $a \mapsto ag$, und $h\colon [g] \to [1]$, definiert durch $a \mapsto ag^{-1}$. Dann gilt: $h \circ f\colon a \mapsto agg^{-1} = h$ und $f \circ g\colon a \mapsto ag^{-1}g = a$.

Folgerung:

1. Ist G endlich, so gilt $|H| \mid |G|$
2. Falls $H \subsetneq G$, so ist $|H| \leq \frac{1}{2}|G|$.

Beweis: Seien $1 = g_0, \ldots, g_{r-1}$ Repräsentanten der Äquivalenzklassen von $\equiv_H$. Dann gilt:

$$|G| = \sum_{i<r} |[g_i]| = r \cdot |[1]| = r \cdot |H| \,.$$

1.3.2 Zyklische Gruppen

Definition: Sei $a^0 = 1$, $a^{i+1} = (a^i)a$ und $a^{-i} = (a^i)^{-1}$ für $i \geq 0$.

Lemma:

1. Für alle $i \in \mathbb{Z}$ gilt $(a^i)^{-1} = a^{-i}$.
2. Für alle $i, j \in \mathbb{Z}$ gilt $a^i a^j = a^{i+j}$.
3. Falls $ab = ba$, so gilt $(ab)^i = a^i b^i$.

Definition:

- Die von a erzeugte Untergruppe ist $\langle a \rangle = \{a^0, a^1, a^{-1}, a^2, a^{-2}, \ldots\}$.
- G ist *zyklisch*, falls $g \in G$ existiert mit $\langle g \rangle = G$. Dann heißt g *Erzeuger*.
- Die *Ordnung* eines Elements $g \in G$ ist $o_G(g) = |\langle g \rangle|$.

Lemma: Sei G zyklisch mit $|G| = \infty$. Dann ist $h\colon \mathbb{Z} \to G$ definiert durch $i \mapsto g^i$ ein Isomorphismus für jeden Erzeuger g.

Beweis: Aus obigem Lemma folgt, dass h ein Homomorphismus ist. Aus der Voraussetzung, dass g ein Erzeuger ist, folgt, dass h ein Epimorphismus ist. Zur Injektivität: Angenommen, $g^i = g^j$. Dann ist $g^{i+k} = g^{j+k}$ für alle $k \in \mathbb{Z}$, also $|G| = |\langle g \rangle| \leq |j - i|$, dies ist ein Widerspruch.

Lemma: Sei G zyklisch mit $n := |G| < \infty$ und sei g ein Erzeuger. Dann gilt:

1. $G = \{1, g, \ldots, g^{n-1}\}$ und $g^n = 1$.
2. $g^i = g^j$ genau dann, wenn $n \mid (i - j)$
3. $h\colon i \mapsto g^i$ ist ein Isomorphismus von $\mathbb{Z}_n \to G$.

Beweis:

1. Vorbemerkung: Falls $g^i = g^j$, so gilt $G \subseteq \{g^0, \ldots, g^{j-i-1}\}$ und $|G| \leq j - i$.

   Die Behauptung folgt dann aus der Vorbemerkung.

2. Wegen 1. gibt es i mit $0 \leq i < n$ und $g^n = g^i$. Wäre $i > 0$, so hätten wir $|G| \leq |n - i| < n$, Widerspruch, also $g^n = 1$, also auch $g^i = g^{i+n}$ für alle $i \in \mathbb{Z}$, d.h. $g^i = g^j$, falls $n \mid i - j$.

   Falls $g^i = g^j$, so $1 = g^0 = g^{j-i}$. Außerdem gilt $g^l = 1$ genau dann, wenn $n \mid l$. Daraus folgt die Behauptung.

3. h ist Homomorphismus wegen obigem Lemma und injektiv wegen 1.

Lemma: Falls $|G| < \infty$, so $g^{|G|} = 1$ für alle $g \in G$.

Beweis: $g^{o_G(g)} = 1$ und $o_G(g) \mid |G|$, also

$$g^{|G|} = g^{o_G(g) \cdot m} = (g^{o_G(g)})^m = 1^m = 1.$$

Sätzchen (**Euler**): Sei $m \geq 2$. Dann gilt $i^{\varphi(m)} = 1$ für alle $i \in \mathbb{Z}_m^*$.

Sätzchen (**Kleiner Satz von Fermat**): Sei p Primzahl. Für alle m mit $1 \leq m < p$ gilt $m^{p-1} \bmod p = 1$.

Es gilt sogar: $p > 2$ ist Primzahl genau dann, wenn $m^{p-1} \bmod p = 1$ für alle $1 \leq m < p$ ist.

Lemma: Sei $G = \langle g \rangle$ mit $m = |G|$ und H Untergruppe von G. Dann gilt:

1. H ist zyklisch.
2. $H = \{1, (g^d), (g^d)^2, \ldots, (g^d)^{\frac{m}{d}-1}\}$ für $d = \frac{m}{|H|}$.

3. $H = \left\{ a \in G \mid a^{\frac{m}{d}} = 1 \right\} = \left\{ a \in G \mid a^{|H|} = 1 \right\}$
$= \{ a \in G \mid o(a) \mid |H| \}$.

Beweis:

1. + 2. Falls $H = \{1\}$, so ist die Behauptung trivial. Sei also $|H| > 1$. Sei $d > 0$ minimal mit $g^d \in H$. Dann ist $H' := \{1, (g^d), (g^d)^2, \ldots, (g^d)^{\frac{m}{d}-1}\}$ Untergruppe von H. Angenommen, $g^i \in H \setminus H'$. Sei j maximal mit $dj < i < (d+1)j$. Dann gilt: $g^{dj} \neq g^i$, also

$$1 = g^{dj} \cdot g^{-dj} = g^i g^{-dj} = g^{i-dj}$$

Also ist $H = H'$. Zu $d \mid m$: Angenommen, $d \nmid m$. Sei j maximal mit $dj < m$. Dann gilt wieder wie oben $g^{m-dj} \in H$ und $0 < m - dj < d$, Widerspruch.

3. Aus 2. folgt $H \subseteq \left\{ a \in G \mid a^{\frac{m}{d}} = 1 \right\}$.
Falls $a^{\frac{m}{d}} = 1$ und $a = g^i$, so $(g^i)^{\frac{m}{d}} = g^{i\frac{m}{d}} = 1$ genau dann, wenn $m \mid i\frac{m}{d}$.

□

Lemma: Sei G zyklische Gruppe der Ordnung $m < \infty$ und $s \in \mathbb{Z}$ sowie $G_s = \{g \in G \mid g^s = 1\}$. Dann ist G_s eine zyklische Untergruppe von G mit Ordnung (m, s).

Beweis: Mit vorherigem Lemma folgt

$$\begin{aligned}\{g \in G \mid g^s = 1\} &= \{g \in G \mid o(g) \mid s\} = \{g \in G \mid o(g) \mid s, m\} \\ &= \{g \in G \mid o(g) \mid (s, m)\} = \left\langle g^{\frac{m}{(m,s)}} \right\rangle.\end{aligned}$$

Erinnerung: $D(m)$ ist die Menge der nichtnegativen Teiler von m.

Lemma: Sei G endliche zyklische Gruppe der Ordnung m und $\langle g \rangle = G$.

1. Für jedes i gilt $o_G(g^i) = \frac{m}{(i,m)}$.
2. Für jedes $d \in D(m)$ enthält G genau $\varphi(d)$ Elemente der Ordnung d.

Beweis:

1. Es gilt $o_G(g^i) \mid \frac{m}{(i,m)}$ wegen

$$(g^i)^{\frac{m}{(i,m)}} = (g^m)^{\frac{i}{(i,m)}} = 1^{\frac{i}{(i,m)}} = 1.$$

Weiterhin gilt:

$$(g^i)^j = 1 \iff g^{ij} = 1 \overset{(*)}{\iff} \frac{m}{(i,m)} \mid j$$

Zur Aussage $(*)$:

„$\Leftarrow$“ $\frac{m}{(i,m)} \mid j \Rightarrow \frac{m}{(i,m)} d = j \Rightarrow m \left(\frac{i}{(i,m)} d \right) = ij \Rightarrow m \mid ij \Rightarrow g^{ij} = 1.$

„$\Rightarrow$“ $g^{ij} = 1 \Rightarrow m \mid ij \Rightarrow \frac{m}{(i,m)} \mid ij \overset{\left(\frac{m}{(i,m)}, i\right)=1}{\Rightarrow} \frac{m}{(i,m)} \mid j.$

Für $j = o_G(g^i)$ folgt dann: $\frac{m}{(i,m)} \mid o_G(g^i)$.

2. Sei $d \in D(m)$, wir zählen die Elemente der Ordnung d. Sei $g \in G$ mit $\langle g \rangle = G$, dann hat g^i hat Ordnung d genau dann, wenn $d = \frac{m}{(m,i)}$ ist. Sei also

$$M := \left\{ i < m \;\middle|\; d = \frac{m}{(m,i)} \right\}$$

Zu zeigen ist: $|M| = \varphi(d)$. Es gilt:

$$\begin{aligned} M = \left\{ i < m \;\middle|\; d = \frac{m}{(m,i)} \right\} &= \left\{ i < m \;\middle|\; (i,m) = \frac{m}{d} \right\} \\ &= \left\{ i = j \cdot \frac{m}{d} < m \;\middle|\; (i,m) = \frac{m}{d} \right\} \\ &= \left\{ i = j \cdot \frac{m}{d} < m \;\middle|\; (j,d) = 1 \right\} \end{aligned}$$

Die letzte Gleichheit gilt aufgrund folgender Argumentation:

$$\frac{m}{d} = (i,m) = (j\frac{m}{d}, m) = \frac{m}{d} \cdot (j,d) \Rightarrow (j,d) = 1$$

Damit gilt insgesamt:

$$|M| = \left| \left\{ i = j \cdot \frac{m}{d} < m \;\middle|\; (j,d) = 1 \right\} \right| = |\{ j < d \mid (j,d) = 1 \}| = \varphi(d)$$

□

Folgerung:

$$n = \sum_{d \in D(n)} \varphi(d).$$

Beweis: Sei $G = \mathbb{Z}_n$. Dann gilt

$$n = |G| = \sum_{d \in D(n)} \left| \{ g \mid o_G(g) = d \} \right| = \sum_{d \in D(n)} \varphi(d).$$

□

1.3.3 Ringe und Körper

Erinnerung: Wir betrachten immer kommutative Ringe mit 1 ($\neq 0$).
Bemerkung: In jedem Monoid lässt sich a^i mit $\mathcal{O}(\log i)$ Monoidmultiplikationen berechnen.

Lemma: Die Menge der Einheiten eines Ringes ist eine abelsche Gruppe.

Satz: Sei $m \geq 2$. Dann ist $\mathbb{Z}_m$ ein Körper genau dann, wenn m eine Primzahl ist.

Beweis: $i \in \mathbb{Z}_m$ ist invertierbar genau dann, wenn $i \top m$ ist. Falls m Primzahl, so ist jedes Element invertierbar. Ist m keine Primzahl, so ist jeder Teiler nicht invertierbar, und es gibt einen nicht trivialen Teiler. □

1.3.4 Erzeuger von endlichen Körpern

Satz: Die Einheitengruppe (d.h. die multiplikative Gruppe) eines endlichen Körpers ist zyklisch.

Satz: Jede endliche Untergruppe der multiplikativen Gruppe eines Körpers ist zyklisch.

Wir betrachten den Fall, dass der Körper $\mathbb{Z}_p$ mit einer Primzahl p ist. Zunächst ein Hilfssatz:

Hilfssatz: Sei G eine Gruppe und $g \in G$ mit maximaler Ordnung und $h \in G$ beliebig. Dann gilt: $o_G(h) \mid o_G(g)$.

Beweis: Angenommen, $o_G(g) = q^k \cdot r$ für eine Primzahl q mit $q \nmid r$. Sei $o_G(h) = q^{k'} \cdot r'$. Zeige: $k' \leq k$. Angenommen, $k' > k$. Sei $h' = h^{r'}$. Dann gilt: $o_G(h') = q^{k'}$. Sei $g' = g^{q^k}$. Dann gilt: $o_G(g') = r$. Für $g' \cdot h'$ erhalten wir mit dem Lemma unten, $o_G(g'h') = q^{k'} \cdot r > q^k \cdot r$. Ein Widerspruch zur Maximalität der Ordnung von g. □

Lemma: Sei G eine Gruppe und $g \in G$. Falls $o_G(g) \top o_G(h)$, so

$$o_G(g \cdot h) = o_G(g) \cdot o_G(h).$$

Beweis:

- Zuerst zeigen wir: $\langle g \rangle \langle h \rangle$ ist Gruppe der Ordnung $o_G(g) \cdot o_G(h)$. Die Gruppe hat die Ordnung $k <\leq o(g) \cdot o(h)$ und $o(g) \mid k$ sowie $o(h) \mid k$. Also ist $|\langle g \rangle \langle h \rangle| = o(g) \cdot o(h)$.

- Wir zeigen noch: gh erzeugt die Gruppe. Zu $i < o(g)$ und $j < o(h)$ finden wir (nach chinesischem Restsatz) $l < o(g)o(h)$ mit $l \bmod o(g) = i$ und $l \bmod o(h) = j$. Also: ist $g^i h^j = (gh)^l$.

Nun können wir obigen Satz beweisen:

Erster Beweis: durch Widerspruch. Angenommen, $\mathbb{Z}_p^*$ ist nicht zyklisch. Sei g ein Element maximaler Ordnung, etwa $o_G(g) = m < p - 1$. Dann gilt (siehe Hilfssatz): $o_G(h) \mid m$ für alle $h \in \mathbb{Z}_p^*$. Also hat $x^m - 1$ alle Elemente von $\mathbb{Z}_p^*$ als Nullstellen; Widerspruch, da $x^m - 1$ höchstens m Nullstellen hat.

Zweite Variante des **Beweises**: Mit Hilfe der *Theorie abelscher Gruppen* (Übung).

1.4 Komplexitätsklassen

Wir betrachten hier folgende Komplexitätsklassen[1]:

- **P**olynomial-Time (P)
- (**Co**mplements of) **N**ondeterministic **P**olynomial-Time (NP/co-NP)
- (**Co**mplements of) **R**andomized **P**olynomial-Time (RP/co-RP)
- **B**ounded-Error **P**robabilistic **P**olynomial-Time (BPP)
- **Z**ero-Error **P**robabilistic **P**olynomial-Time (ZPP)

Klasse P: $L \in \mathsf{P}$ genau dann, wenn eine deterministische Turing-Maschine (TM) mit einer Laufzeit polynomiell beschränkt in der Eingabe alle $u \in L$ akzeptiert.

Für die anderen Klassen betrachten wir *nicht-deterministische Turing-Maschinen*, bei denen jede Berechnung *polynomiell* lang ist in der Länge der Eingabe (d.h. bei Zahlen im Logarithmus der Zahl) und bei denen wie üblich durch akzeptierende Zustände akzeptiert wird. Bezeichne diese als *PTM*.

Die verschiedenen Berechnungspfade der Turingmaschine werden als *Berechnungsbaum* bezeichnet, wobei Verzweigungen im Baum entstehen, sobald die Turing-Maschine eine nicht-deterministische Entscheidung trifft.

Klasse NP: $L \in \mathsf{NP}$ genau dann, wenn es eine PTM gibt, so dass

[1] siehe auch `http://www.complexityzoo.com`

- für jedes $u \in L$ im Baum *mindestens ein* Blatt akzeptiert
- für jedes $u \notin L$ im Baum *kein* Blatt akzeptiert

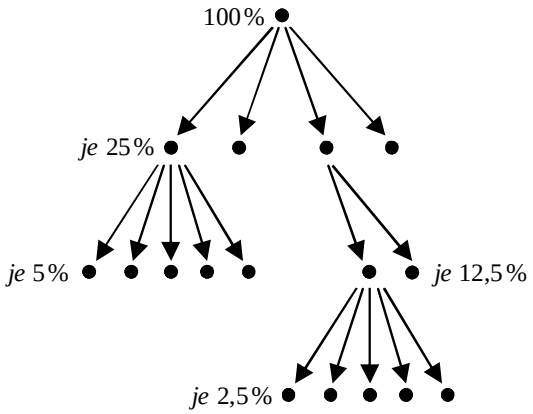
Klasse co-NP: $L \in \mathsf{co\text{-}NP}$ genau dann, wenn es eine PTM gibt, so dass

- für jedes $u \in L$ im Baum *jedes* Blatt akzeptiert
- für jedes $u \notin L$ im Baum *mindestens ein* Blatt nicht akzeptiert

Es gilt damit:

$$L \in \mathsf{co\text{-}NP} \iff (A^* \setminus L) \in \mathsf{NP}$$

Für die restlichen Klassen weisen wir jedem Blatt b im Berechnungsbaum eine Wahrscheinlichkeit $P(b)$ zu, indem wir von Wahrscheinlichkeit 1 an der Wurzel ausgehen und die Wahrscheinlichkeit eines Knotens auf seine Nachfolger gleichmäßig aufgeteilt wird:



Nun können wir weitere Klassen definieren, die beschreiben, mit welcher Wahrscheinlichkeit Worte akzeptiert oder verworfen werden müssen:

Klasse BPP: $L \in \mathsf{BPP}$ genau dann, wenn es eine PTM gibt, so dass

- für jedes $u \in L$ ist $\sum_{\text{Blatt } b \text{ akzeptiert}} P(b) \geq \frac{3}{4}$
- für jedes $u \notin L$ ist $\sum_{\text{Blatt } b \text{ akzeptiert}} P(b) \leq 1 - \frac{3}{4}$

Klasse RP: $L \in \mathsf{RP}$ genau dann, wenn es eine PTM gibt, so dass

- für jedes $u \in L$ ist $\sum_{\text{Blatt } b \text{ akzeptiert}} P(b) \geq \frac{1}{2}$
- für jedes $u \notin L$ ist $\sum_{\text{Blatt } b \text{ akzeptiert}} P(b) = 0$

Klasse co-RP: $L \in$ co-RP genau dann, wenn es eine PTM gibt, so dass

- für jedes $u \in L$ ist $\sum_{\text{Blatt } b \text{ akzeptiert}} P(b) = 1$
- für jedes $u \notin L$ ist $\sum_{\text{Blatt } b \text{ akzeptiert}} P(b) \leq \frac{1}{2}$

Bemerkung: Die eben definierten Klassen kann man auch schärfer formulieren:

Satz:

1. In der Definition von BPP kann man $\frac{3}{4}$ ersetzen durch $f(|n|)$ für jede beliebige Funktion f, für die es ein k gibt, so dass gilt:
$$\frac{1}{2} + \frac{1}{n^k} \leq f(n) \leq 1 - 2^{-n^k}.$$
2. In der Definition von RP und co-RP kann man $\frac{1}{2}$ ersetzen durch $f(|n|)$ für jede belibige Funktion f, für die es ein k gibt, so dass gilt:
$$\frac{1}{n^k} \leq f(n) \leq 1 - 2^{-n^k}.$$

Für die letzte Klasse, ZPP, werden in der Turing-Maschine drei Arten von Zuständen benutzt: akzeptierende, verwerfende und unentschlossene.

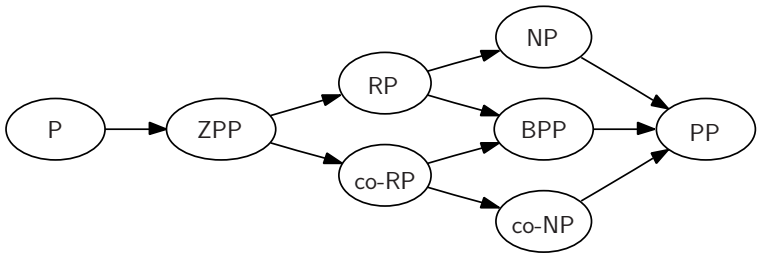
Klasse ZPP: $L \in$ ZPP genau dann, wenn es eine PTM gibt, so dass

- für jedes $u \in L$ ist $\sum_{\text{Blatt } b \text{ akzeptiert}} P(b) \geq \frac{1}{2}$ und $\sum_{\text{Blatt } b \text{ verwirft}} P(b) = 0$
- für jedes $u \notin L$ ist $\sum_{\text{Blatt } b \text{ verwirft}} P(b) \geq \frac{1}{2}$ und $\sum_{\text{Blatt } b \text{ akzeptiert}} P(b) = 0$

Für die Probleme in ZPP gibt es damit jeweils eine modifizierte Turing-Maschine, die die Turing-Maschine aus dem Beweis der ZPP-Zugehörigkeit so lange läuft, bis diese entweder akzeptiert oder verwirft. Die *erwartete Laufzeit* dieser modifizierten Turing-Maschine ist polynomiell in der Eingabe. Es gilt:

$$\text{ZPP} = \text{RP} \cap \text{co-RP}.$$

Zur Beziehung der Komplexitätsklassen untereinander (wobei $X \to Y$ die Beziehung $X \subseteq Y$ bezeichne):



1.5 Der Miller-Rabin-Test

1.5.1 Einfache Primzahltests

Erinnerung: Ein Primzahltest ist ein Entscheidungsalgorithmus für

$$\mathsf{PRIMES} = \{\langle n \rangle_2 \mid n \text{ ist Primzahl}\}.$$

Sofort einsichtig ist folgender Satz:

Satz: PRIMES $\in$ co-NP.

Beweis: Eine passende PTM ist: Zur Eingabe $\langle n \rangle_2$ rate eine Zahl m mit $1 < m < n$. Falls $m \mid n$ gilt (Teilbarkeit kann in $\mathcal{O}(\mathrm{Log}^3\, n)$ getestet werden), so akzeptiere nicht, andernfalls akzeptiere. □

Weniger direkt einsichtig ist folgender Satz:

Satz von **Pratt**: PRIMES $\in$ NP.

Um dies zu zeigen, benötigen wir zunächst folgendes Lemma:

Lemma von **Lucas**: Sei $n \geq 2$. Dann ist n eine Primzahl genau dann, wenn es ein $1 < a < n$ gibt mit

1. $a^{n-1} \equiv 1 \pmod{n}$ und
2. für alle Primzahlen p mit $p \mid n-1$ gilt: $a^{\frac{n-1}{p}} \not\equiv 1 \pmod{n}$.

Die **Idee von Pratt** ist ein rekursiver Ansatz auf der Grundlage des Lemmas: Man rät sowohl a als auch die Primteiler q und überprüft rekursiv, dass es sich tatsächlich um Primzahlen handelt.

Beweis des Lemmas:

„⇒“ Sei n eine Primzahl, dann ist nach Lemma $\mathbb{Z}_n^*$ zyklisch mit Ordnung $n-1$. Wähle einen Erzeuger a. Dann gilt $a^{n-1} \mod n = 1$ und $a^m \mod n \neq 1$ für alle $m < n-1$, insbesondere für $m = \frac{n-1}{q}$.

„⇐“ Sei $G = \mathbb{Z}_n^*$. Aus 1. folgt $a \in G$ mit $o_G(a) \mid n-1$. Falls aber $o_G(a) < n-1$ wäre, so würde es eine Primzahl q geben mit $o_G(a) \mid \frac{n-1}{q}$. Dies ist wegen 2. nicht möglich, damit gilt $o_G(a) = n - 1$. □

Beweis des Satzes von Pratt durch Angabe eines NP-Verfahrens:

1. Rate ein *Zertifikat* (oder *Beleg*) dafür, dass die gegebene Zahl n eine Primzahl ist.

2. Überprüfe, dass es sich tatsächlich um ein Zertifikat handelt.

Frage: Was ist ein Zertifikat?

- Erster Ansatz: Ein Zertifikat sei $C(n) = (a, q_0, \ldots, q_{r-1})$, wobei a wie im Lemma ist und $q_0, \ldots, q_{r-1}$ die Primteiler von $n - 1$ sind.
  - $a^{n-1} \mod n = 1$ lässt sich durch iteriertes Quadrieren überprüfen.
  - dass sich $n-1$ als Produkt von $q_0, \ldots, q_{r-1}$ (oder Potenzen) schreiben lässt, lässt sich auch leicht überprüfen: man dividiert nacheinander durch $q_0, q_1, \ldots$ so lange wie möglich. Falls 1 erreicht wird, so ist $n - 1$ Produkt dieser Zahlen, sonst nicht.
  - Verbleibendes Problem: Sind die q_i Pimzahlen? Ausweg: Benutze verschachtelte Zertifikate.

- Zweiter Ansatz: Induktive Definition der Zertifikate:
  - $(2, 1)$ ist ein Zertifikat
  - Falls $a^{n-1} \mod n = 1$ ist und n sich als Produkt von Potenzen von q_i schreiben lässt, so ist folgendes ein Zertifikat für n (mit Zertifikaten Z_{q_i} für q_i:

$$Z_n := (n, a, Z_{q_0}, \ldots, Z_{q_{r-1}})$$

Beispiel: Ein Zertifikat für 7 ist $(7, 3, (3, 2, (2, 1)), (2, 1))$.

Es ist leicht einzusehen, dass man in polynomieller Zeit in der Länge eines Zertifikates überprüfen kann, dass es sich tatsächlich um eines handelt. Zu zeigen bleibt: Zertifikate haben polylogarithmische Länge in n. Siehe Übung! □

Der **Primzahltest von Lehmann** ist ein weiterer einfacher Test. Vorbedingung: Sei $n \geq 3$ ungerade, $l \geq 2$.

```
for (i ∈ {1, ..., l}) {
  a ∈ {1, ..., n−1}; // zufällig
  c = a^((n−1)/2) mod n;
  if (c ≠ 1 ∧ c ≠ n−1)
    return "probably composite";
  if (c == n−1)
    return "probably prime";
}
return "probably composite";
```

Satz:

1. Für festes l lässt sich Lehmanns Test in Polynomzeit implementieren.
2. Für jedes n ist die Fehlerwahrscheinlichkeit kleinergleich 2^{-l}.
3. PRIMES $\in$ BPP.

Beweis *(mit Lücke!)*:

1. Polynomzeit wird erreicht, wenn die Exponentiation durch iteriertes Quadrieren implementiert wird.
2. Betrachte die Abbildung

$$h\colon \{1,\dots,n-1\} \to \mathbb{Z}_n \text{ mit } a \mapsto a^{\frac{n-1}{2}} \mod n$$

   Fallunterscheidung:

   (a) Sei n eine Primzahl. Dann ist $h\colon \mathbb{Z}_n^* \to \mathbb{Z}_n^*$ sogar ein Gruppenhomomorphismus. Es gilt für alle $a \in \{1,\dots,n-1\}$, dass $h(a)^2 = 1$ ist; daraus folgt (da $\mathbb{Z}_n$ Körper ist), dass $h(a) \in \{1, n-1\}$ ist.
   Damit ist die Fehlerwahrscheinlichkeit gegeben durch $P(h(a) = 1)^l$. Sei dazu nun g ein Erzeuger der zyklischen Gruppe $\mathbb{Z}_n^*$. Betrachte die Menge

$$\begin{aligned}\left\{ i \;\middle|\; (g^i)^{\frac{n-1}{2}} = 1 \right\} &= \left\{ i \;\middle|\; g^{i\cdot\frac{n-1}{2}} = 1 \right\} \\ &= \left\{ i \;\middle|\; n-1 \mid i \cdot \frac{n-1}{2} \right\} \\ &= \{ 1 \le i < n \mid i \text{ gerade} \}\end{aligned}$$

Daraus folgt:

$$\frac{|\{1 \leq i < n \mid i \text{ gerade}\}|}{n-1} = \frac{1}{2}$$

(b) Sei n nun zerlegbar. Dann:

i. Falls $n-1 \notin \text{Bild}(h)$, so ist die Fehlerwahrscheinlichkeit 0.

ii. Den Fall $n-1 \in \text{Bild}(h)$ betrachten wir später!

3. Folgt aus 1. und 2. mit $l = 3$.

1.5.2 Der Fermat-Test

Satz: Sei $n \geq 2$. Dann ist n eine Primzahl genau dann, wenn für alle $a < n$ gilt: $a^{n-1} \mod n = 1$.

Beweis:

„⇒“ Kleiner Satz von Fermat (FLT).

„⇐“ Es folgt $|\mathbb{Z}_n^*| = n-1$, also ist $\mathbb{Z}_n$ Körper, d.h. n ist Primzahl. □

Bemerkung: Für alle $n \geq 3$ ungerade gilt: $1^{n-1} \mod n = 1$ und $(n-1)^{n-1} \mod n = 1$. Konsequenz: 1 und $n-1$ sind keine guten Kandidaten.

Der **Fermat-Test** ist nun folgender Algorithmus mit Vorbedingung $n \geq 3$ ungerade:

```
1 a ∈ {2, ..., n-2}; // zufällig
2 c = a^(n-1) mod n;
3 if (c == 1)
4   return "probably prime";
5 else
6   return "composite";
```

Bemerkung: Der Fermat-Test macht nur für zerlegbare Zahlen Fehler!

Definition: Sei n ungerade und zerlegbar.

- Ein $a \in \{2, \ldots, n-2\}$ mit $a^{n-1} \mod n \neq 1$ heißt *Fermat-Zeuge (F-Zeuge)* für die Zerlegbarkeit von n.
- Ein $a \in \{2, \ldots, n-2\}$ mit $a^{n-1} \mod n = 1$ heißt *Fermat-Lügner (F-Lügner)* für die Zerlegbarkeit von n.
- Die Menge der F-Zeugen bezeichnen wir mit W_n^F, die Menge der F-Lügner mit L_n^F.

Ziel ist nun eine Abschätzung für $\left|L_n^F\right|$. Triviale Abschätzung: $\left|L_n^F\right| \leq n-\varphi(n)$, da die Elemente aus $\mathbb{Z}_n$, die nicht in $\mathbb{Z}_n^*$ sind, nie F-Lügner sein können. Problem ist: Wenn n viele Primfaktoren hat, dann ist $\varphi(n)$ klein!

Satz: Falls $n \geq 3$ ungerade und falls es einen F-Zeugen in $\mathbb{Z}_n^*$ gibt (d.h. $W_n^F \cap \mathbb{Z}_n^* \neq \emptyset$), so ist die Fehlerwahrscheinlichkeit des Fermat-Tests kleiner als $\frac{1}{2}$.

Beweis: Es reicht, zu zeigen, dass L_n^F eine Untergruppe von $\mathbb{Z}_n^*$ ist. Denn falls es dann einen F-Zeugen gibt, muss L_n^F echte Untergruppe sein, also wäre $|L_n^F| \leq \frac{1}{2}|\mathbb{Z}_n^*|$. Wir benutzen das Untergruppenkriterium:

1. Es gilt $1 \in L_n^F$, da $1^{n-1} \mod n = 1$.
2. Zu $L_n^F \cdot L_n^F$: Aus $a^{n-1} \mod n = 1$ und $b^{n-1} \mod n = 1$ folgt

$$(ab)^{n-1} = (a^{n-1})(b^{n-1}) = 1 \cdot 1 = 1.$$

□

Es bleibt noch der Fall, dass es keinen F-Zeugen in $\mathbb{Z}_n^*$ gibt:

Definition: Eine ungerade Zahl $n \geq 3$ heißt *Carmichael-Zahl*, falls für alle $a \in \mathbb{Z}_n^*$ gilt: $a^{n-1} \equiv 1 \mod n$.

Satz von Alford, Granville und **Pomerance:** Es gibt ein x_0, so dass für alle $x \geq x_0$ gilt:

$$|\{y \leq x \mid y \text{ ist Carmichael-Zahl}\}| \geq x^{\frac{2}{7}}.$$

Satz: Jede Carmichael-Zahl hat mindestens drei verschiedene Primfaktoren.

Beweis durch Widerspruch: Wir nehmen an, n ist kein Produkt von mindestens drei Primzahlen. Wir konstruieren einen F-Zeugen in $\mathbb{Z}_n^*$. Fallunterscheidung:

1. Fall: $n = p^k m$ mit p Primzahl, $k \geq 2$ und $p \nmid m$.
   a) Falls $m = 1$, so setze $a = 1 + p$.
   b) Falls $m > 1$, so wähle a als $1 \leq a < p^2 m \leq n$ mit $a \equiv 1 + p \pmod{p^2}$ und $a \equiv 1 \pmod{m}$.

   Wir zeigen, dass a ein F-Zeuge in $\mathbb{Z}_n^*$ ist.

   (i) Es gilt $a \in \mathbb{Z}_n^*$, da $p \nmid a$, denn $p^2 \mid a - (1 + p)$. Außerdem gilt $(m, a) = 1$ nach Wahl von a.

(ii) Es gilt $a \in W_n^F$, Beweis durch Widerspruch: Angenommen, $a^{n-1} \mod n = 1$. Da $p^2 \mid n$, gilt $a^{n-1} \mod p^2 = 1$.

$$\begin{aligned} a^{n-1} &\equiv_{p^2} (1+p)^{n-1} \\ &= 1 + (n-1)p + \sum_{i=2}^{n-1} \binom{n-1}{i} p^i \\ &\equiv_{p^2} 1 + (n-1)p \end{aligned}$$

Also $p^2 \mid (n-1)p$, d.h. $p \mid n-1$. Widerspruch!

2. Fall: $n = pq$ mit $p \neq q$ Primzahlen: Übung! □

1.5.3 Nicht-triviale Quadratwurzeln

Idee: verbessere den Fermat-Test!

Definition: Eine *Quadratwurzel* von 1 modulo n ist eine Zahl $a \in \mathbb{Z}_n$ mit $a^2 = 1$. Die Zahlen 1 und $n-1$ sind *triviale Quadratwurzeln* (von 1 modulo n).

Lemma: Sei p eine Primzahl. Dann gibt es keine nichttrivialen Quadratwurzeln modulo p.

Beweis: Jede Quadratwurzel ist Nullstelle von $x^2 - 1 = 0$, und $x^2 - 1$ ist Polynom zweiten Grades, hat also höchstens zwei Nullstellen. □

Bemerkung: Falls $n = pq$ ist mit Primzahlen $p \neq q$, so gibt es vier Quadratwurzeln modulo n.

Beweis: Es gilt $x^2 - 1 \mod n = 0$ genau dann, wenn $x^2 - 1 \mod p = 0$ und $x^2 - 1 \mod q = 0$ ist, das gilt für $x \mod p \in \{1, -1\}$ und $x \mod q \in \{1, -1\}$ – also gibt es vier Quadratwurzeln, d.h. zwei nichttriviale.

Bemerkung: Allgemein gibt es zu $n = p_1 \cdot \ldots \cdot p_r$ mit unterschiedlichen ungeraden Primzahlen p_i genau 2^r Quadratwurzeln modulo n.

Ansatz: Wähle zufällig $a \in \{2, \ldots, n-2\}$ und teste, ob $a^2 \mod n = 1$ ist. Falls ja, so ist n keine Primzahl. Im obigen Fall ist die Erfolgswahrscheinlichkeit aber nur $\frac{2}{n-3}$, dies ist alleine noch zu wenig.

Definition: Die *Artjuhov-Folge* zu $a \in \{2, \ldots, n-2\}$ und ungeradem $n \geq 3$ sei wie folgt definiert: Wähle k und u mit $n - 1 = 2^k \cdot u$ und $2 \nmid u$. Dann ist die Artjuhov-Folge

$$a^u, a^{2u}, a^{4u}, \ldots, a^{2^k u}$$

Die unterschiedlichen möglichen Artjuhov-Folgen ergeben dann Aufschluß über die Zerlegbarkeit, betrachte folgende Tabelle, wobei $\star$ jeweils eine Zahl $\notin \{1, -1\}$ sei:

Typ	a^u	a^{2u}	$\ldots$	$a^{2^i u}$	$a^{2^{i+1} u}$	$\ldots$	$a^{2^{k-1} u}$	$a^{2^k u}$	Ergebnis
1A	1	1	$\ldots$	1	1	$\ldots$	1	1	keine Aussage
1B	$\star$	$\star$	$\ldots$	-1	1	$\ldots$	1	1	keine Aussage
2	$\star$	$\star$	$\ldots$	$\star$	$\star$	$\ldots$	$\star$	-1	zerlegbar
2	$\star$	$\star$	$\ldots$	$\star$	$\star$	$\ldots$	$\star$	$\star$	zerlegbar
3	$\star$	$\star$	$\ldots$	$\star$	1	$\ldots$	1	1	zerlegbar

Beispiel: $n = 325 = 5^2 \cdot 13$, $n - 1 = 324 = 81 \cdot 2^2$, die Artjuhor-Folge

a	$b_0 = a^{81}$	$b_1 = a^{162}$	$b_2 = a^{324}$
2	252	129	66
7	307	324	1
32	57	324	1
49	324	1	1
65	0	0	0
126	1	1	1
201	226	**51**	1
224	**274**	1	1

Definition:

- Falls n zerlegbar ist, so ist ein A-Zeuge für die Zerlegbarkeit von n eine Zahl $a \in \{1, \ldots, n-1\}$ mit $a^u \bmod n \neq 1$ und $a^{u2^i} \bmod n \neq n-1$ für alle $i < k$; die Nicht-Zeugen heißen A-Lügner.
- Die Menge aller A-Zeugen sei W_n^A, die Menge aller A-Lügner sei L_n^A.

Satz (Miller, Bach): Falls die erweiterte Riemannsche Hypothese gilt, so gibt es zu jeder ungeraden zerlegbaren Zahl ≥ 3 einen A-Zeugen $a < 2 \ln n$.

Bemerkung: Falls die erweiterte Riemannsche Hypothese gilt, braucht man nur alle $a < 2 \ln n$ auf die Zeugen-Eigenschaft zu testen, um einen deterministischen polynomiellen Primzahltest zu erhalten.

Folgerung: Falls die erweiterte Riemannsche Hypothese gilt, so ist $\mathsf{PRIMES} \in \mathsf{P}$.

1.5.4 Einschub: Riemannsche Hypothese

Die *Riemannsche Zeta-Funktion* ist definiert durch:

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s}$$

Diese Funktion konvergiert für $s > 1$. Diese Funktion wird auf die komplexen Zahlen erweitert. Definiere zudem

$$L(s, \chi) = \sum_{n \geq 1} \frac{\chi(s)}{n^s}$$

Dabei ist $\chi(s)$ ein *Dirichlet-Charakter*, der auf einem Modulus $D \in \mathbb{N}$ basiert und folgende Eigenschaften hat: $\chi \colon \mathbb{Z} \to \mathbb{C}$, so dass $\chi(mn) = \chi(m)\chi(n)$, $\chi(m) = \chi(m \bmod D)$ und $\chi(m) \neq 0$ genau dann, wenn $m \top D$.

Als Verbindung zu Primzahlen gibt es die folgende Beziehung:

$$\zeta(s) = \sum_{n \geq 1} \frac{1}{n^s} = \prod_{p \text{ Primzahl}} \frac{1}{1 - p^{-s}}$$

Die (erweiterte) Riemannsche Hypothese ist nun:

Riemannsche Hypothese: Falls $s \in \mathbb{C}$ ist mit $\Re(s) > 0$ und $\zeta(s) = 0$, so ist $\Re(s) = \frac{1}{2}$.

Erweiterte Riemannsche Hypothese: Falls $s \in \mathbb{C}$ ist mit $\Re(s) > 0$ und $L(s, \chi) = 0$, so ist $\Re(s) = \frac{1}{2}$.

1.5.5 Der Miller-Rabin-Test

Algorithmus[2]: Als Vorbedingung sei $n \geq 3$ ungerade.

```
1 (u, k) = soThat(n−1 = 2^k·u);
2 a ∈ {2, ..., n−2}; // zufällig
3 b = a^u mod n;
4 if (b == 1 ∨ b == n−1)
5   return "probably prime";
6 for (i ∈ {1, ..., k−1}) {
7   b = b^2 mod n;
8   if (b == n−1)
9     return "probably prime";
```

[2] siehe auch `http://home.arcor.de/rienhardt/files/miller_rabin.pdf`

```
10    if (b == 1)
11      return "composite";
12  }
13  return "probably prime";
```

Lemma:

1. Der Miller-Rabin-Test macht nur Fehler für zerlegbare Zahlen.
2. Für zerlegbare Nicht-Carmichael-Zahlen ist die Fehlerwahrscheinlichkeit kleinergleich $\frac{1}{2}$.
3. Der Miller-Rabin-Test kommt mit $\mathcal{O}(\log n)$ arithmetischen und $\mathcal{O}(\log^3 n)$ bzw. $\widetilde{\mathcal{O}}(\log^2 n)$ Binäroperationen aus.

Ansatz zum Beweis der Korrektheit: Suche eine echte Untergruppe B_n mit

$$L_n^A \subseteq B_n < \mathbb{Z}_n^*$$

Sei n eine Carmichael-Zahl, $n-1 = u \cdot 2^k$ wie oben. Der *MR-Index* von n ist

$$\nu(n) = \max\left\{ i < k \mid \exists\, a \colon a \in L_n^A \wedge a^{u2^i} \bmod n = n-1 \right\}$$

Bemerkung: $\nu(n)$ ist wohldefiniert (da $(n-1)^u \bmod n = n-1$, also ist die Menge nicht leer) und es gilt $0 \leq \nu(n) < k$.
Definiere nun

$$B_n = \left\{ a \in \mathbb{Z}_n \;\middle|\; a^{\nu(n)} \bmod n \in \{1, -1\} \right\} \subseteq \mathbb{Z}_n^*$$

Lemma:

1. $L_n^A \subseteq B_n$.
2. B_n ist Untergruppe von $\mathbb{Z}_n^*$.
3. B_n ist echte Untergruppe.

Beweis:

1. Falls $a \in L_n^A$, dann gibt es entweder i mit $a^{u2^i} \bmod n = n-1$ oder $a^u \bmod n = 1$, damit ist $a \in B_n$.
2. Mittels Untergruppenkriterium: $1 \in B_n$ und $B_n B_n \subseteq B_n$.

3. Da n eine Carmichael-Zahl ist, gibt es m, m' mit $m \top m'$ und $n = mm'$. Wähle nun ein Element a_0, das in der Definition von $\nu(n)$ das Maximum liefert. Wähle a nach chinesischem Restsatz mit

$$a \bmod m = a_0 \ (\star) \quad \text{und} \quad a \bmod m' = 1 \ (\star\star).$$

Zu zeigen: $a \in \mathbb{Z}_n^*$, aber $a \notin B_n$.

- Aus $a \bmod m = a_0$ und $a_0^{u2^{\nu(n)}} \bmod n = -1$ folgt $a^{u2^{\nu(n)}} \bmod m = -1$. Also ist a invertierbar modulo m und m', also ist $a \in \mathbb{Z}_n^*$.
- Falls $a \in B_n$ wäre, so wäre $a^{u2^{\nu(n)}} \bmod n \in \{1, -1\}$. Die beiden Fälle 1 und -1 führen aber zum Widerspruch:

$$\begin{aligned} a^{u2^{\nu(n)}} \bmod n = 1 \iff & \overbrace{a^{u2^{\nu(n)}} \bmod m = 1}^{\text{widerspricht } (\star)} \\ \text{und} \quad & a^{u2^{\nu(n)}} \bmod m' = 1 \\ \text{oder} \quad a^{u2^{\nu(n)}} \bmod n = -1 \iff & a^{u2^{\nu(n)}} \bmod m = -1 \\ \text{und} \quad & \underbrace{a^{u2^{\nu(n)}} \bmod m' = -1}_{\text{widerspricht } (\star\star)} \end{aligned}$$

Satz: Es gilt sogar:

1. Der Miller-Rabin-Test hat eine Fehlerwahrscheinlichkeit kleiner als $\frac{1}{2}$, sogar kleiner als $\frac{\varphi(n)}{4n} \leq \frac{1}{4}$.
2. PRIMES $\in$ co-RP

Der Miller-Rabin-Test kann auch effizient zur Erzeugung von großen Primzahlen eingesetzt werden, betrachte folgenden Algorithmus zur *Primzahlerzeugung* mit $k \geq 3$ Anzahl der Stellen, und $l > 1$ Anzahl der Primzahltests.

```
1 while (true) {
2   a ∈ {2^(k-1), ..., 2^k} // ungerade, zufällig
3   for (i ∈ {1, ..., l}) {
4     if (MillerRabinTest(a) == "composite")
5       continue next a;
6   }
7   return a;
8 }
```

Satz (Bach, Damgård, Landrock, Pomerance):

1. Der Algorithmus hat erwartete polynomielle Laufzeit.
2. Der Algorithmus liefert mit Wahrscheinlichkeit kleinergleich $\frac{1}{4^l}$ eine zerlegbare Zahl.
3. Für $l = 1$ ist die Wahrscheinlichkeit, dass der Algorithmus eine zerlegbare Zahl liefert, kleinergleich

$$k^2 \frac{1}{4^{\sqrt{k}-2}}.$$

1.6 Der Solovay-Strassen-Test

1.6.1 Quadratische Reste

Definition: Sei $m \geq 2$. Dann ist $a \in \mathbb{Z}$ ein quadratischer Rest modulo m, falls x existiert mit $x^2 \equiv a \pmod{m}$ und $a \top m$. Ein Element a heißt *quadratischer Nicht-Rest*, wenn a kein quadratischer Rest ist, aber $a \top m$ gilt.

Beispiel: Sei $m = 21$. Dann ist die Menge der quadratischen Reste modulo 21 gleich $\{1, 4, 16, 18, \ldots\}$ (mit $9^2 \bmod 21 = 18$).

Bemerkung: Die Menge der quadratischen Reste modulo m in $\mathbb{Z}_m^*$ bildet eine Untergruppe von $\mathbb{Z}_m^*$.

Lemma (**Eulers Kriterium**): Sei p eine ungerade Primzahl.

1. Die Menge der quadratischen Reste in $\mathbb{Z}_p^*$ bildet eine Untergruppe von $\mathbb{Z}_p^*$ der Ordnung $\frac{p-1}{2}$.
2. Für jede Zahl $a \in \mathbb{Z}_p^*$ gilt:
   - Falls a quadratischer Rest ist, so ist $a^{\frac{p-1}{2}} \bmod p = 1$.
   - Falls a ein quadratischer Nicht-Rest ist, so ist $a^{\frac{p-1}{2}} \bmod p = -1$.

Beweis: $\mathbb{Z}_p^*$ ist zyklisch, sei also g ein Erzeuger von $\mathbb{Z}_p^*$.

1. Die Elemente der Form g^{2i} mit $0 < i < \frac{p-1}{2}$ sind unterschiedliche quadratische Reste.

Die Elemente der Form $a = g^{2i+1}$ sind keine quadratischen Reste. Angenommen, a sei ein quadratischer Rest. a ist dann Quadrat eines Elements, also einer Potenz von g, d.h. $g^{2i+1} = a = (g^j)^2 = g^{2j}$. Dann muß aber $p-1 \mid (2i+1)-(2j)$ gelten, dies ist nicht möglich, da $p-1$ gerade ist, die rechte Seite aber ungerade.

2. Für quadratische Reste a gilt $(g^{2i})^{\frac{p-1}{2}} = (g^{p-1})^i = 1$.

   Für quadratische Nicht-Reste gilt $(g^{2i+1})^{\frac{p-1}{2}} = g^{\frac{p-1}{2}} = b$. Es gilt $b \neq 1$, aber $b^2 = 1$, also ist $b = -1$. □

Frage: Kann man leicht Wurzeln ziehen in $\mathbb{Z}_p^*$?

Antwort: Falls $p \equiv 1 \pmod 4$, so ist es „total einfach“ – siehe Übung. Für $p \equiv 3 \pmod 4$ ist es etwas schwieriger.

Definition: Sei p ungerade Primzahl und $a \in \mathbb{Z}$. Folgendes sei das *Legendre-Symbol*:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} \bmod p = \begin{cases} 1 & \text{falls } a \text{ quadratischer Rest modulo } p \\ -1 & \text{falls } a \text{ quadratischer Nicht-Rest modulo } p \\ 0 & \text{sonst} \end{cases}$$

Lemma: Sei p ungerade Primzahl und $a, b \in \mathbb{Z}$. Dann gilt:

1. $\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$
2. $\left(\frac{a \cdot b^2}{p}\right) = \left(\frac{a}{p}\right)$ für $b \top p$
3. $\left(\frac{a+bp}{p}\right) = \left(\frac{a}{p}\right)$, insbesondere $\left(\frac{a}{p}\right) = \left(\frac{a \bmod p}{p}\right)$
4. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, d.h. -1 ist quadratischer Rest genau dann, wenn $p \equiv 1 \pmod 4$ ist

1.6.2 Das Jacobi-Symbol

Definition: Sei $a \in \mathbb{Z}$, $n = p_0 \cdot \ldots \cdot p_{r-1} \geq 3$ ungerade mit Primzahlen p_i. Dann ist folgendes das *Jacobi-Symbol*:

$$\left(\frac{a}{n}\right) = \prod_{i<r} \underbrace{\left(\frac{a}{p_i}\right)}_{\text{Legendre-Symbol}}$$

Lemma: Seien $n, m \geq 3$ ungerade, $a, b \in \mathbb{Z}$. Dann gilt:

1. $\left(\frac{a \cdot b}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$
2. $\left(\frac{a \cdot b^2}{n}\right) = \left(\frac{a}{n}\right)$ für $b \top n$
3. $\left(\frac{a}{nm}\right) = \left(\frac{a}{n}\right)\left(\frac{a}{m}\right)$
4. $\left(\frac{a+bn}{n}\right) = \left(\frac{a}{n}\right)$, insbesondere $\left(\frac{a}{n}\right) = \left(\frac{a \bmod n}{n}\right)$
5. $\left(\frac{2^{2k}a}{n}\right) = \left(\frac{a}{n}\right)$ und $\left(\frac{2^{2k+1}a}{n}\right) = \left(\frac{2}{n}\right)\left(\frac{a}{n}\right)$
6. $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$
7. $\left(\frac{0}{n}\right) = 0$ und $\left(\frac{1}{n}\right) = 1$

Beweis: Nur Nr. 6: Seien $p_0, \ldots, p_{s-1}$ diejenigen Primfaktoren mit $p_i \equiv 3 \pmod 4$. Wir haben

$$n \equiv (p_0 \bmod 4) \cdot \ldots \cdot (p_{r-1} \bmod 4) \equiv (-1)^s \pmod 4$$

Damit ist $\frac{n-1}{2}$ ungerade genau dann, wenn s ungerade ist. Nun gilt:

$$(-1)^{\frac{n-1}{2}} = (-1)^s = \prod_{i<s}\left(\frac{-1}{p_i}\right) = \prod_{i<r}\left(\frac{-1}{p_i}\right) = \left(\frac{-1}{n}\right)$$

Damit ist Nr. 6 bewiesen, die anderen Eigenschaften sind leicht zu zeigen. □

Wir benötigen noch zwei weitere Sätze:

Satz (**Quadratisches Reziprozitätsgesetz**): Seien $m, n \geq 3$ ungerade. Dann gilt:

Falls $m \equiv 1 \pmod 4$ oder $n \equiv 1 \pmod 4$, so ist $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$.
Falls $m \equiv 3 \pmod 4$ und $n \equiv 3 \pmod 4$, so ist $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$.

Satz: Sei $n \geq 3$ ungerade. Dann gilt:

Falls $n \equiv 1 \pmod 8$ oder $n \equiv 7 \pmod 8$, so ist $\left(\frac{2}{n}\right) = 1$.
Falls $n \equiv 3 \pmod 8$ oder $n \equiv 5 \pmod 8$, so ist $\left(\frac{2}{n}\right) = -1$.

Diese werden wir im nächsten Abschnitt beweisen, zunächst können wir nun aber einen Algorithmus angeben, der das Jacobi-Symbol $\left(\frac{a}{n}\right)$ ausgibt. Vorbedingung: $a \in \mathbb{Z}$ und $n \geq 3$ ungerade.

```
1  b = a mod n;
2  c = n;
3  s = 1;
4  while (true) {
5    while (4 | b)
6      b = b / 4;
7    if (2 | b) {
8      if (c mod 8 ∈ {3, 5})
9        s = -s;
10     b = b / 2;
11   }
12   if (b == 1)
13     return s;
14   if (b mod 4 == c mod 4 == 3)
15     s = -s;
16   (b, c) = (c mod b, b);
17 }
```

Satz: Der obige Algorithmus berechnet das Jacobi-Symbol mit $\mathcal{O}(\log n)$ Schleifendurchläufen.

Beweis: Zur Korrektheit benutze obiges Lemma und die Invariante $\left(\frac{a}{n}\right) = s \cdot \left(\frac{b}{c}\right)$; zur Laufzeit: $c_{i+2} \leq \frac{1}{2} c_i$. □

1.6.3 Quadratisches Reziprozitätsgesetz

Wir beweisen in diesem Abschnitt die beiden oben schon genannten Sätze:

Satz (**Quadratisches Reziprozitätsgesetz**): Seien $m, n \geq 3$ ungerade. Dann gilt:

Falls $m \equiv 1 \pmod 4$ oder $n \equiv 1 \pmod 4$, so ist $\left(\frac{m}{n}\right) = \left(\frac{n}{m}\right)$.
Falls $m \equiv 3 \pmod 4$ und $n \equiv 3 \pmod 4$, so ist $\left(\frac{m}{n}\right) = -\left(\frac{n}{m}\right)$.

Wir beweisen dies zunächst für (ungerade) Primzahlen und verallgemeinern dies später auf alle Zahlen. Eine äquivalente Formulierung ist:

$$\left(\frac{m}{n}\right) = (-1)^{\frac{m-1}{2}\cdot\frac{n-1}{2}} \left(\frac{n}{m}\right).$$

Für eine ungerade Primzahl p definieren wir:

$$\begin{aligned} H_p &= \{1, \ldots, \frac{p-1}{2}\} \\ S_p(a) &= \{\, h \cdot a \bmod p \mid\ h \in H_p\} = (H_p \cdot a) \bmod p \quad (\text{für } a \top p) \\ T_p(a) &= S_p(a) \cap H_p \\ R_p(a) &= S_p(a) \setminus H_p \\ k_p(a) &= |R_p(a)| \end{aligned}$$

Lemma: Sei p ungerade Primzahl, $p \top a$. Dann ist

$$H_p = T_p(a) \uplus (p - R_p(a)).$$

Beweis: Zunächst gilt $|S_p(a)| = |H_p| = \frac{p-1}{2}$ nach Definition von $S_p(a)$, da wir in einem Körper rechnen. Wenn wir nun zeigen, dass $T_p(a) \cap (p - R_p(a)) = \emptyset$ ist, sind wir fertig: Wir haben ausreichend Elemente auf der rechten Seite der Gleichung im Lemma, da $|T_p(a)| + |R_p(a)| = |S_p(a)| = |H_p|$ gilt.

Angenommen, $ia \equiv p - ja \pmod p$ für $i, j \in H_p$. Dann ist $(i+j)a \equiv_p p \equiv_p 0$, also $p \mid (i+j)$, aber $0 < i + j < p$! □

Lemma: Sei p ungerade Primzahl mit $a \top p$. Dann ist $\left(\frac{a}{p}\right) = (-1)^{k_p(a)}$.

Beweis: Wir betrachten $\prod_{i \in H_p} i$, spalten nach T_p und R_p auf und kürzen

dann, betrachte dazu in $\mathbb{Z}_p$:

$$\begin{aligned}
\prod_{i\in H_p} i &= \prod_{i\in T_p(a)} i \cdot \prod_{i\in p-R_p(a)} i \\
&= \prod_{i\in T_p(a)} i \cdot \prod_{i\in R_p(a)} (p-i) \\
&= \prod_{i\in T_p(a)} i \cdot \prod_{i\in R_p(a)} i\cdot(-1)^{k_p(a)} \\
&= \prod_{i\in S_p(a)} i\cdot(-1)^{k_p(a)} \\
&= \prod_{i\in H_p} ia\cdot(-1)^{k_p(a)} \\
&= \prod_{i\in H_p} i\cdot a^{\frac{p-1}{2}}\cdot(-1)^{k_p(a)}
\end{aligned}$$

Kürzen liefert nun $a^{\frac{p-1}{2}}\cdot(-1)^{k_p(a)} = 1$, also ist in $\mathbb{Z}_p$:

$$\left(\frac{a}{p}\right) = a^{\frac{p-1}{2}} = (-1)^{k_p(a)}.$$

Um nun von $\mathbb{Z}_p$ auf $\mathbb{Z}$ zu kommen beachte, dass wegen $(-1)^{k_p(a)} \in \{1,-1\}$ in $\mathbb{Z}$ auch gilt, dass $a^{\frac{p-1}{2}} \bmod p = (-1)^{k_p(a)}$.

Folgerung: Sei $n \geq 3$ ungerade. Dann gilt:

Falls $n \equiv 1 \pmod 8$ oder $n \equiv 7 \pmod 8$, so ist $\left(\frac{2}{n}\right) = 1$.
Falls $n \equiv 3 \pmod 8$ oder $n \equiv 5 \pmod 8$, so ist $\left(\frac{2}{n}\right) = -1$.

Beweis: Für $n = p$, ungerade Primzahl, ist dies äquivalent zu folgender Formulierung:

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Bestimme nun $k_p(2)$:

$$\begin{aligned}
k_p(2) &= \left|\left\{ i \in \{2,4,6,\ldots,p-1\} \mid i > \frac{p}{2}\right\}\right| \\
&= \left|\left\{ i \in \{1,2,3,\ldots,\frac{p-1}{2}\} \;\middle|\; i > \frac{p}{4}\right\}\right| = \frac{p-1}{2} - \left\lfloor\frac{p}{4}\right\rfloor
\end{aligned}$$

Nach einer Fallunterscheidung für p mod 8 ergibt sich:

$$\begin{array}{lll} p = 8l+1: & k_p(2) = 4l - 2l = 2l & \text{– gerade} \\ p = 8l+3: & k_p(2) = 4l + 1 - 2l = 2l+1 & \text{– ungerade} \\ p = 8l+5: & k_p(2) = 4l + 2 - 2l - 1 = 2l+1 & \text{– ungerade} \\ p = 8l+7: & k_p(2) = 4l + 3 - 2l - 1 = 2l+2 & \text{– gerade} \end{array}$$

Daraus folgt die Behauptung für Primzahlen.

Nun verallgemeinern wir das obige Resulat und zeigen die Behauptung für beliebige n. Wir führen eine Induktion über die Anzahl der Primfaktoren von n.

Es gilt $\left(\frac{2}{n}\right) = \left(\frac{2}{l}\right)\left(\frac{2}{m}\right)$ für $n = lm$. Dann ist

$$\left(\frac{2}{n}\right) = (-1)^{\frac{l^2-1}{8}}(-1)^{\frac{m^2-1}{8}} = (-1)^{\frac{(ml)^2-1}{8}},$$

wobei benutzt wird: $(ml)^2 - 1 \equiv m^2 - 1 + l^2 - 1$. Weiter gilt dann:

$$\begin{aligned} (ml)^2 - 1 &= (m^2-1)(l^2-1) + m^2 + l^2 - 2 \\ &= (m^2-1)(l^2-1) + (m^2-1) + (l^2-1) \end{aligned}$$

Dies ist jedoch modulo 16 gleich null, da sich die ungeraden m und l jeweils darstellen lassen als $m = 2m' + 1$ bzw. $l = 2l' + 1$, und dann gilt:

$$m^2 - 1 = (2m'+1)^2 - 1 = 4m'^2 + 4m' + 1 - 1 = 4(m'^2 + m')$$

Damit ist die Folgerung auch für zusammengesetzte Zahlen gezeigt. □

Wir definieren nun zusätzlich zu $k_p(a)$ noch

$$\lambda_p(a) = \sum_{i \in H_p} (ai) \text{ div } p.$$

Dann gilt:

$$\lambda_p(a) = \sum_{i \in H_p} (ai) \text{ div } p = \sum_{i \in H_p} \left\lfloor \frac{ai}{p} \right\rfloor = \sum_{i \in H_p} \frac{ai - (ai \bmod p)}{p}$$

Lemma: Sei p ungerade Primzahl mit ungeradem $a \top p$. Dann ist $\left(\frac{a}{p}\right) = (-1)^{\lambda_p(a)}$.

Beweis: Wir bestimmen $\sum_{i \in H_p} i$ und $\sum_{i \in H_p} ia$ und bilden die Differenz, dabei benutzen wir R_p und T_p. Es gilt:

$$
\begin{aligned}
a \cdot \sum_{i \in H_p} i = \sum_{i \in H_p} ia &= \sum_{i \in H_p} (ia - (ia \bmod p)) + \sum_{s \in S_p(a)} s \\
&= \sum_{i \in H_p} (ia - (ia \bmod p)) + \sum_{t \in T_p(a)} t + \sum_{r \in R_p(a)} r \\
&= p \cdot \lambda_p(a) + \sum_{t \in T_p(a)} t + \sum_{r \in R_p(a)} r \\
\sum_{i \in H_p} i &= \sum_{r \in R_p(a)} (p - r) + \sum_{t \in T_p(a)} t \\
&= p \cdot k_p(a) - \sum_{r \in R_p(a)} r + \sum_{t \in T_p(a)} t
\end{aligned}
$$

Nun betrachten wir die Differenz

$$
(a-1) \sum_{i \in H_p} i = p(\lambda_p(a) - k_p(a)) + 2 \sum_{r \in R_p(a)} r
$$

Da a ungerade ist, ist $(a-1)$ gerade. Da aber p ungerade ist und der hintere Term auf der rechten Seite gerade ist, muß auch $\lambda_p(a) - k_p(a)$ gerade sein, d.h. $(-1)^{k_p(a)} = (-1)^{\lambda_p(a)}$. □

Nun können wir zum eigentlichen **Beweis** des Quadratischen Reziprozitätsgesetzes übergehen. Den ersten Fall behandelt folgendes Lemma:

Lemma: Das Quadratische Reziprozitätsgesetz gilt für zwei Primzahlen $p \neq q$.

Beweis über ein Zählargument: Betrache $M = H_p \times H_q$ und teile geschickt auf zwei Mengen auf:

$$
\begin{aligned}
M_p &= \{ (i,j) \in M \mid jp < iq \} \\
M_q &= \{ (i,j) \in M \mid jp > iq \}
\end{aligned}
$$

Dann gilt $M = M_p \uplus M_q$, denn aus $jp = iq$ folgt $q \mid j$ und $p \mid i$, aber $j < \frac{q}{2}$ und $i < \frac{p}{2}$.[3]

Also ist $\frac{p-1}{2}\frac{q-1}{2} = |M| = |M_p| + |M_q|$, wir berechnen nun $|M_p|$ und $|M_q|$:

$$
|M_p| = \sum_{i \leq \frac{p-1}{2}} |\{ j \in H_q \mid jp < iq \}| = \sum_{i \leq \frac{p-1}{2}} \left\lfloor \frac{iq}{p} \right\rfloor = \lambda_p(q)
$$

[3] „Dann haben wir sogar zwei Widersprüche, das reicht!“

Entsprechend folgt $M_q = \lambda_q(p)$, insgesamt also $\frac{p-1}{2}\frac{q-1}{2} = \lambda_p(q) + \lambda_q(p)$, d.h. mit einem alten Lemma folgt:

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\lambda_p(q)}(-1)^{\lambda_q(p)} = (-1)^{\lambda_p(q)+\lambda_q(p)} = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

Damit haben wir das Quadratische Reziprozitätsgesetz für zwei Primzahlen $p \neq q$ bewiesen. □

Wir betrachten nun den allgemeinen Fall des Quadratischen Reziprozitätsgesetzes, d.h. seien $m, n \geq 3$ ungerade. Zu zeigen: $\frac{m}{n} = (-1)^{\frac{m-1}{2}\frac{n-1}{2}}\frac{n}{m}$. Für $m \not| n$ ist die Behauptung trivial (beide Seiten der Gleichung sind null), d.h. ab jetzt seien m und n teilerfremd.

Beweis per Induktion über die Anzahl der Primfaktoren r und s von m bzw. n.

- Induktionsanfang: $r + s = 2$, in diesem Fall sind m und n Primzahlen, diesen Fall haben wir schon bewiesen.
- Induktionsschritt: $r + s > 2$, dann ist m oder n keine Primzahl, etwa n. Schreibe $n = kl$ mit $k, l \geq 3$. Dann gilt nach Induktionsannahme:

  $$\left(\frac{m}{k}\right)\left(\frac{k}{m}\right) = (-1)^{\frac{k-1}{2}\frac{m-1}{2}} \quad \text{und} \quad \left(\frac{m}{l}\right)\left(\frac{l}{m}\right) = (-1)^{\frac{l-1}{2}\frac{m-1}{2}}$$

  Wegen der Multiplikativität des Jacobi-Symbols ($\left(\frac{m}{n}\right) = \left(\frac{m}{k}\right)\left(\frac{m}{l}\right)$) gilt dann:

  $$\begin{aligned}\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) &= \left(\left(\frac{m}{k}\right)\left(\frac{m}{l}\right)\right)\cdot\left(\left(\frac{k}{m}\right)\left(\frac{l}{m}\right)\right)\\ &= \left(\left(\frac{m}{k}\right)\left(\frac{k}{m}\right)\right)\cdot\left(\left(\frac{m}{l}\right)\left(\frac{l}{m}\right)\right)\\ &= (-1)^{\frac{m-1}{2}\frac{l-1}{2}+\frac{m-1}{2}\frac{k-1}{2}}\\ &= (-1)^{\frac{m-1}{2}\frac{k+l-2}{2}}\end{aligned}$$

  Es gilt nun im Exponenten:

  $$\frac{n-1}{2} = \frac{kl-1}{2} = \frac{(k-1)(l-1)+k+l-2}{2} \equiv_2 \frac{k+l-2}{2}$$

  Damit ist der Induktionsschritt gezeigt. □

Somit ist das Quadratische Reziprozitätsgesetz bewiesen.

1.6.4 Der Solovay-Strassen-Test

Lemma: Falls p eine ungerade Primzahl ist, so ist

$$\left(a^{\frac{p-1}{2}} \bmod p\right)\left(\frac{a}{p}\right) = 1 \quad \forall\, a \in \{1, \ldots, p-1\}$$

Beweis: Beide Faktoren sind gleich und jeweils 1 oder -1. □

Der Solovay-Strassen-Test ist nun folgender Algorithmus mit Vorbedingung $n \geq 3$ ungerade:

```
1 a ∈ {2, ..., n−2}; // zufällig
2 x = a^((n−1)/2) mod n;
3 y = Jacobi(a, n);
4 if (x·y == 1)
5   return "probably prime";
6 else
7   return "composite";
```

Satz:

1. Der Solovay-Strassen-Test macht nur bei zerlegbaren Zahlen Fehler, und dann mit Fehlerwahrscheinlichkeit kleiner als $\frac{1}{2}$.
2. PRIMES $\in$ co-RP

Dazu definieren wir wieder Zeugen und Lügner:

Definition: Sei $n \geq 3$ ungerade, $a \in \mathbb{Z}_n^*$.

- Das Element a ist E-Zeuge für Zerlegbarkeit von n, falls gilt:

  $$\left(a^{\frac{p-1}{2}} \bmod p\right)\left(\frac{a}{p}\right) \neq 1$$

  Die anderen Elemente sind Lügner.

- Die Menge der Zeugen sei W_n^E, die Menge der Lügner L_n^E.

Bemerkung: Jeder E-Lügner ist auch F-Lügner, da für $a \in L_n^E$ gilt, dass $a^{\frac{p-1}{2}} \in \{-1, 1\}$ ist, also $a^{p-1} = 1$. Damit ist die Fehlerwahrscheinlichkeit ohnehin kleiner als $\frac{1}{2}$, falls n keine Carmichael-Zahl ist.

Beweis der Schranke für die Fehlerwahrscheinlichkeit: Wir zeigen, dass L_n^E eine echte Untergruppe von $\mathbb{Z}_n^*$ ist. Es gilt $1 \in L_n^E$, und für $a, b \in L_n^E$ gilt

$$\left((ab)^{\frac{p-1}{2}} \bmod p\right)\left(\frac{ab}{p}\right) = \left(a^{\frac{p-1}{2}} \bmod p\right)\left(b^{\frac{p-1}{2}} \bmod p\right)\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = 1$$

Damit ist L_n^E eine Untergruppe. Fallunterscheidung:

a) Falls n keine Carmichael-Zahl ist, so sind wir nach obiger Bemerkung fertig.

b) Falls n eine Carmichael-Zahl ist, dann unterscheide:

   i) Falls $n = p^k m$ mit einer Primzahl p und $k \geq 2$, so liefert der alte Beweis einen Zeugen.

   ii) $n = pm$ mit einer Primzahl p, mit m ungerade und $p \nmid m$. Sei nun $b \in \mathbb{Z}_p^*$ ein quadratischer Nicht-Rest, d.h. $\left(\frac{b}{p}\right) = -1$. Nach dem chinesischen Restsatz existiert a mit $a \equiv b \pmod{p}$ und $a \equiv 1 \pmod{m}$.
   Wir zeigen, dass $a \in W_n^E \cap \mathbb{Z}_n^*$ ist. Da $a \equiv b \pmod{p}$ und $b \in \mathbb{Z}_p^*$ und $a \equiv 1 \pmod{m}$ ist, haben wir $a \top pm$, also $a \in \mathbb{Z}_n^*$. Es gilt nun:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{m}\right) = \left(\frac{b}{p}\right)\left(\frac{1}{m}\right) = (-1) \cdot 1 = -1$$

   Angenommen, a wäre Lügner. Dann müßte $a^{\frac{n-1}{2}} \bmod n = -1$ sein. Dann wäre $a^{\frac{n-1}{2}} \bmod m = -1$, aber wegen $a \equiv 1 \pmod{m}$ gilt $a^{\frac{n-1}{2}} \bmod m = 1$, Widerspruch. Damit ist a ein Zeuge. □

1.7 Polynome

1.7.1 Polynome über Ringen

Sei R ein Ring, wie üblich kommutativ und mit Eins.

Definition:

- Ein *Polynom* über R ist eine unendliche Folge $(a_0, a_1, \ldots)$ mit $a_i \in R$, aber nur endlich viele $a_i \neq 0$. Das spezielle Polynom x sei definiert als $(0, 1, 0, 0, \ldots)$. $R[x]$ sei dann die Menge der Polynome, wir identifizieren darin $(a, 0, 0, \ldots)$ und $a \in R$.

- Für $f = (a_0, a_1, \ldots)$ und $g = (b_0, b_1, \ldots)$ definieren wir:

$$(f + g) = (a_0 + b_0, a_1 + b_1, \ldots)$$

$$(f \cdot g) = (c_0, c_1, \ldots) \text{ mit } c_i = \sum_{j=0}^{i} a_j b_{i-j}$$

- Der *Grad* eines Polynoms sei definiert durch:

$$\deg(f) = \begin{cases} -\infty & \text{falls} \quad f = 0 \\ \max\{i \mid a_i \neq 0\} & \text{falls} \quad f \neq 0 \end{cases}$$

- Der *Leitkoeffizient* ist $a_{\deg(f)}$, ein *normiertes Polynom* hat Leitkoeffizient Eins.[4]

Dann gelten folgende Eigenschaften:

Satz: $R[x]$ bildet mit 0 und 1 einen Ring.

Lemma: Seien $f, g \in R[x]$. Dann gilt:

- $\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$
- $\deg(f \cdot g) \leq \deg(f) + \deg(g)$
- $\deg(f \cdot g) = \deg(f) + \deg(g)$, falls einer der Leitkoeffizienten Einheit ist

Nun können wir Elemente in die Polynome einsetzen:

Definition: Sei R ein Ring und $r \in R$. Der *Einsetzungshomomorphismus* ist folgende Abbildung:

$$h_r \colon R[x] \to S \text{ mit } h_r(f) = \sum_{i=0}^{\deg(f)} a_i r^i$$

Satz: Der Einsetzungshomomorphismus h_r ist ein Ringhomomorphismus, der die Elemente aus R fix läßt und x auf r abbildet.

Wir wollen im weiteren auch Polynome in andere Polynome einsetzen:

[4] Häufig brauchen wir auch Polynome, deren Leitkoeffizient eine Einheit ist, diese haben jedoch keinen speziellen Namen. Beachte außerdem $R^* \subseteq R[x]^*$, aber nicht unbedingt $R^* = R[x]^*$, siehe z.B. $\mathbb{Z}_4[x]$ und $(1 + 2x)^2 = 1$.

Definition: Für jede $f, g \in R[x]$ sei

$$f(g) = \sum_{i=0}^{\deg(f)} a_i g^i \text{ mit } f = (a_0, a_1, \ldots)$$

Einige weitere Eigenschaften von Polynomen:

Satz: Sei p eine Primzahl, und seien $f, g \in \mathbb{Z}_p[x]$. Dann gilt:

1. $(f+g)^p = f^p + g^p$.
2. $(f \cdot g)^p = f^p \cdot g^p$
3. $f^p = f(x^p)$, damit auch $f^{p^k} = f(x^{p^k})$

Beweis:

1. Es gilt:
$$(f+g)^p = f^p + g^p + \sum_{i=1}^{p-1} \binom{p}{i} i f^i g^{p-i} = f^p + g^p$$
Die letzte Gleichheit gilt wegen $p \mid \binom{p}{i}$ für $0 < i < p$, dies folgt aus der Definition des Binomialkoeffizienten mit einer Primzahl p.
2. Gilt, da $Z_p[x]$ wieder ein Ring ist.
3. Für $f = \sum_{i=0}^{d} a_i x^i$ gilt:
$$\begin{aligned} f^p &= (a_d x^d + \ldots + a_0)^p \\ &= a_d^p x^{dp} + \ldots + a_0^p \\ &= (a_d^{p-1}) a_d x^{dp} + \ldots + (a_0^{p-1}) a_0 \\ &= a_d x^{dp} + \ldots + a_0 \end{aligned}$$

1.7.2 Teilen mit Rest und Teilbarkeit von Polynomen

Satz: Seien $f, g \in R[x]$ mit Leitkoeffizient von g in R^*. Dann gibt es eindeutige Polynome h und r mit $f = gh + r$ und $\deg(r) < \deg(g)$.

Beweis: Wir geben folgenden Algorithmus zur Polynomdivision für $f = \sum_{i=0}^{\deg(f)} a_i x^i, g = \sum_{i=0}^{\deg(g)} b_i x^i \in R[x]$ und Leitkoeffizient von g in R^* an:

```
1 if (deg(g) > deg(f))
2   return (0, f);
3 c = a[deg(f)]·b[deg(g)]^-1;
4 e = deg(f) - deg(g);
5 f* = f - c·x^e·g;
6 (h, r) = PolynomialDivision(f*, g)
7 return (c·x^e+h, r);
```

Zur **Korrektheit**: Es gilt:

$$\begin{aligned} g \cdot (c \cdot x^{\deg(f)-\deg(g)} + h) + r &= g \cdot c \cdot x^{\deg(f)-\deg(g)} + gh + r \\ &= g \cdot c \cdot x^{\deg(f)-\deg(g)} + f - c \cdot x^{\deg(f)-\deg(g)} \cdot g \\ &= f \end{aligned}$$

Zur **Terminierung**:

- Der Algorithmus terminiert für f mit $\deg(f) < \deg(g)$.
- Bei jedem rekusiven Aufruf wird der Grad des ersten Arguments echt kleiner, der Grad des zweiten Arguments aber nicht verändert.

Eindeutigkeit: Angenommen, $f = g \cdot h + r$ und $f = g \cdot h' + r'$. Dann gilt $g(h - h') = (r' - r)$. Nun ist der Grad rechts kleiner als $\deg(g)$, der linke Grad ist aber gleich $\deg(g) + \deg(h - h')$, dies ist nur für $h = h'$ möglich, dann ist auch schon $r = r'$. □

Definition: Seien f, g Polynome. Dann gelte $g \mid f$, falls h existiert mit $gh = f$. Dabei ist g ein *echter Teiler* von f, falls $0 < \deg(g) < \deg(f)$.

Nun definieren wir wieder Kongruenzrelationen:

Sei $h \in R[x]$ mit einer Einheit als Leitkoeffizient. Dann sei

$$f \equiv_h g \Leftrightarrow h \mid f - g$$

Lemma: Falls $f \equiv_h f'$ und $g \equiv_h g'$, so ist $f + g \equiv_h f' + g'$ und $f \cdot g \equiv_h f'g'$, zudem gilt $f(g) \equiv_h f(g')$.

Beweis der dritten Eigenschaft:

$$f(g) = \sum a_i g^i \equiv_h \sum a_i (g')^i = f(g')$$

□

Bemerkung: Falls $h' \mid h$ und $f \equiv_h g$, dann ist $f \equiv_{h'} g$.

1.7.3 Quotientenstrukturen von Polynomringen

Definition: Sei $h \in R[x]$ mit einer Einheit als Leitkoeffizient. Definiere dann die Operationen div und mod wie im Satz über die Polynomdivision. Dann seien

$$\begin{aligned} R[x]/(h) &= \{ g \in R[x] \mid \deg(g) < \deg(h) \} \\ g + g' &= (g + g') \bmod h \\ g \cdot g' &= (gg') \bmod h \end{aligned}$$

Satz: Für $h \in R[x]$ mit $\deg(h) > 0$ ist $R[x]/(h)$ ein Ring mit Eins.

Definition: Zwei Polynome f, g heißen *assoziiert*, falls $f = g \cdot e$ für ein $e \in R^*$.

1.7.4 Irreduzible Polynome

Definition: Ein Polynom $f \neq 0$ heißt *irreduzibel*, falls es keien echten Teiler hat, d.h. kein g mit $g \mid f$ und $0 < \deg(g) < \deg(f)$.

Lemma: Sei $f \in F[x]$ für einen Körper F mit f irreduzibel; sei $h \in F[x]$ und $f \nmid h$. Dann gibt es $a, b \in F[x]$ mit $1 = af + bh$.

Beweis: Sei $I = \{ af + bh \mid a, b \in F[x] \}$. Falls ein $s \in F^*$ existiert mit $s \in I$, so ist $1 \in I$. Sei $g \neq 0$ ein Polynom mit minimalem Grad in I.

Sei $f = g \cdot q + r$ mit $\deg(r) < \deg(g)$. Dann ist

$$r = f - g \cdot q = f - (af + bh)q = (1 - a \cdot q)f - b \cdot q \cdot h$$

Damit ist, weil $\deg(r) < \deg(g)$, schon $r = 0$. Dann gilt $g \mid f$, und analog auch $g \mid h$.

Also gibt es ein q mit $f = q \cdot g$. Da aber f irreduzibel, ist $q \in F^*$ oder $g \in F^*$. Aber aus $q \in F^*$ würde $f \mid g$ folgen, mit $g \mid h$ würde $f \mid h$ folgen im Widerspruch zur Voraussetzung. Also ist $g \in F^*$, damit ist die Behauptung gezeigt. □

Lemma: Sei f ein irreduzibles Polynom, das gh teilt. Dann wird g oder h von f geteilt.

Beweis: Da f das Polynom gh teilt, existiert ein c mit $cf = gh$.

Angenommen, f teilt nicht g. Dann existiert nach vorherigem Lemma $a, b \in K[x]$ mit $1 = af + bg$. Mit h multipliziert liefert das $h = ahf + b(gh) = ahf + b(cf) = (ah + bc)f$. □

Satz: Für jedes normierte Polynom $f \neq 0$ gibt es irreduzible normierte Polynome $f_0, \ldots, f_{r-1}$ mit Grad > 0, so dass $f = f_0 \cdots f_{r-1}$ gilt. Diese Polynome sind eindeutig, bis auf Reihenfolge.

Beweis: Existenz: Induktion über den Grad von f.

- Induktionsanfang: Falls $\deg f = 0$, d.h. $f = 1$. Setze also $r = 0$.
- Induktionsschritt: Falls f irreduzibel, so trivial. Ansonsten gibt es g mit $0 < \deg(g) < \deg(f)$ und h, so dass $f = gh$. O.B.d.A. ist g normiert, dann ist aber auch h normiert, da f normiert ist. Nach altem Lemma gilt $\deg(h) < \deg(f)$, also ist die IV anwendbar: Es existieren $f_0, \ldots, f_{r-1}$, $g_0, \ldots, g_{s-1}$ wie gefordert mit $h = f_0 \cdots f_{r-1}$ und $g = g_0 \cdots g_{s-1}$. Dann ist $f_0 \cdots f_{r-1} \cdot g_0 \cdots g_{s-1}$ das gesuchte Produkt.

Eindeutigkeit: Auch per Induktion. Angenommen, $f = f_0 \cdots f_{r-1}$ und $f = f'_0 \cdots f'_{r-1}$ mit f_i, f'_j irreduziebel und normiert. Durch Anwendung des vorigen Lemmas erhalten wir: $f_0 = f'_i$ für ein $i < r'$. O.B.d.A. gilt also: $f = f_0 f'_1 \cdots f'_{s-1}$.

Wir werden nun kürzen: Aus $fg = fh$ mit $f \neq 0$ folgt $g = h$. Dies gilt, da aus $fg = fh$ folgt, dass $f(g - h) = 0$ ist, d.h. wegen des Lemmas über den Grad des Produkts ist $g - h = 0$, also $g = h$.

Es folgt also: $f_1 \cdots f_{r-1} = f'_1 \cdots f'_{s-1}$. Wende dann die Induktionsvoraussetzung an. □

Satz: Sei h ein irreduzibles Polynom über endlichem Körper K. Dann ist $K[x]/(h)$ ein Körper mit $|K|^{\deg(h)}$ Elementen.

Beweis:

1. $K[x]/(h)$ ist Körper. Sei $f \in K[x]/(h)$, $f \neq 0$. Dann gilt $\deg(f) < \deg(h)$, also teilt h das Polynom f nicht. Nach altem Lemma gibt es dann a, b mit $af + bh = 1$. In $K[x]/(h)$ gilt $af = 1$. Also besitzt f ein Inverses.
2. $|K[x]/(h)| = |\{f \mid \deg(f) < \deg(h)\}| = |K|^{\deg(h)}$. □

1.7.5 Nullstellen von Polynomen

Es gilt (immernoch) die Grundannahme, dass $R = K$ ein Körper ist.

Lemma: Jedes Polynom vom Grad $d \geq 0$ hat höchstens d Nullstellen.

Beweis: per Induktion.

- Induktionsanfang: $\deg(f) = 0$, d.h., $f = a$ mit $a \neq 0$, also hat f keine Nullstelle.

- Induktionsschritt: Sei f vom Grad > 0. Angenommen, f habe eine Nullstelle a, dann gibt es q und r, mit $f = q(x-a) + r$ mit $\deg(r) < \deg(x-a) = 1$, also $\deg(r) = 0$ oder $-\infty$. Falls $\deg(r) = 0$, so $r = b \in F^*$. Dann gilt aber, $0 = f(a) = q(a) \cdot 0 + b = b \neq 0$. Widerspruch! Also $r = 0$ bzw. $f = q(x-a)$. Nach altem Lemma gilt $\deg(f) = \deg(q) + \deg(x-a)$, also $\deg(q) < \deg(f)$. Nach Induktionsvoraussetzung hat q also $< \deg(f)$ viele Nullstellen. Wenn wir zeigen können, dass jede Nullstelle von f eine Nullstelle von q ist oder $= a$, sind wir fertig. Also: Angenommen, $f(b) = 0$. Dann gilt $q(b)(b-a) = 0$, d.h., $q(b) = 0$ oder $a = b$. □

Folgerung: Sind f und g Polynome mit $\deg(f), \deg(g) \leq d$, die an $d+1$ Stellen übereinstimmen, dann gilt $f = g$.

Beweis: Übung.

Bemerkung: $x^{rs} - 1 = (x^r - 1)\left(x^{r(s-1)} + x^{r(s-2)} + \ldots + 1\right)$.

1.7.6 Nullstellen des Polynoms $x^r - 1$

Satz: Seien $p \neq r$ Primzahlen. Sei weiterhin h ein irreduzibler normierter Teiler von $\frac{x^r-1}{x-1} = 1 + \ldots + x^{r-1}$. Dann gilt $o_{K^*}(x) = r$ für $K = \mathbb{Z}_p[x]/(h)$.

Beweis: Da x Nullstelle von h und h Teiler von $1 + \ldots + x^{r-1}$ und das wiederum Teiler von $x^r - 1$ ist, gilt $x^r - 1 = 0 \mod h$. Damit gilt $o_{K^*}(x) \mid r$, also $o_{K^*}(x) \in \{1, r\}$, da r Primzahl ist.

Angenommen, es wäre $o_{K^*}(x) = 1$. Dann würde $x = 1$ gelten, da aber x Nullstelle von $1 + \ldots + x^{r-1}$ ist, würde dies $1 + \ldots + 1 = r = 0 \mod p$ bedeuten. Die ist ein Widersruch dazu, dass p Primzahl $\neq r$ ist. □

Satz: Für h wie oben gilt $\deg(h) = o_p(r)$.

Beweis: Setze $d := \deg(h)$ und $k := o_p(r)$. Dann zeigen wir $k = d$ mittels $k \leq d$ und $k \geq d$:

„$\leq$“ Da $o_{K^*}(x) = r$ und $|K^*| = p^d - 1$ ist, gilt $r \mid p^d - 1$. Damit gilt $p^d \equiv 1 \mod r$, also $k \mid d$, insbesondere $k \leq d$.

„$\geq$“ Wir zeigen zuerst $f^{p^k} = f$ für alle $f \in K$ (daraus folgt $f^{p^k-1} = 1$ für alle $f \in K^*$).

– Wir beweisen die Behauptung zunächst für x. Da $p^k - 1 \equiv 0 \mod r$ ist, gibt es m mit $mr + 1 = p^k$, also:

$$x^{p^k} = x^{mr+1} = (x^r)^m x \equiv_h 1 \cdot x = x$$

Dabei folgt der Schritt modulo h aufgrund des Satzes von oben.

– Nun beweisen wir die Aussage für ein $f \in K$. Es gilt $f^{p^k}(x) = f(x^{p^k})$ nach einem alten Satz über $\mathbb{Z}_p[x]$. Nach altem Lemma folgt aus $g \equiv_h g'$, dass $f(g) \equiv_h f(g')$ ist, damit gilt $f(x^{p^k}) \equiv_h f(x)$.

Also gilt, dass jedes Element von k^* eine Ordnung hat, die kleiner p^k ist. Da K^* zyklisch mit Ordnung $p^d - 1$ ist, folgt $k \geq d$. □

1.8 Primzahltest von Agrawal, Kayal, Saxena

1.8.1 Die Grundidee

Lemma: Sei $n \geq 2$ und $a \top n$ mit $a < n$. Dann ist n eine Primzahl genau dann, wenn $(x + a)^n \equiv x^n + a \mod n$ ist.

Beweis:

„⇒“ $(x + a)^n = x^n + \sum_{i=1}^{n-1} \binom{n}{i} x^{n-i} a^i + a^n$. Mit $\sum_{i=1}^{n-1} \binom{n}{i} x^{n-i} a^i = 0 \mod n$ und $a^n = a^{n-1} a = a \mod n$ folgt die Behauptung.

„⇐“ Sei p Primteiler von n für n zerlegbar. Sei p^k maximale p-Potenz in n. Betrachte Koeffizienten von x^{n-p}:

$$\binom{n}{p} a^p = \frac{n!}{p!(n-p)!} a^p = \frac{n}{p} \cdot \frac{(n-1) \cdots (n-p+1)}{(p-1)!} a^p.$$

Dies wird von p nicht geteilt: p teilt nicht mehr $\frac{n}{p}$, weiter gilt $p \nmid n-1, n-2, \ldots, n-p+1$, da $p \mid n$; und wegen $(a, n) = 1$ gilt auch $p \nmid a^p$. Damit gilt $p \nmid \binom{n}{p} a^p$, also folgt $p^k \nmid \binom{n}{p} a^p$, insbesondere $n \nmid \binom{n}{p} a^p$. Damit ist $\binom{n}{p} a^p \neq 0 \mod n$. □

Problem: Die Berechnung von $(x + a)^n \mod n$ ist zu aufwendig, da das Polynom alleine schon exponentiell viele Koeffizienten hat.

Ausweg: Wir rechnen nicht nur modulo n, sondern auch modulo $p(x)$ für ein geeignetes Polynom $p(x)$. Geeignet heisst hier, dass $\deg(p) \in \log^{\mathcal{O}(1)} n$.

Ansatz: Teste $p(x) = x^r - 1$ für geeignetes r.

Probleme:

1. Es ist schwierig, ein geeignetes r zu finden.

2. Selbst wenn man ein geeignetes r findet, müssen mehrere a getestet werden. Weitere Frage: Welche a nutzen wir?

3. Selbst wenn man die ersten beiden Schritte richtig macht, dann scheitert der Test für Primzahlpotenzen.

1.8.2 Primzahltest von Agrawal, Kayal und Saxena

Algorithmus: Vorbedingung sei $n \geq 3$.

```
1  if (PerfectPower(n))
2    return "composite";
3
4  r = 1;
5  o_min = 4·⌈log(n)⌉^2;
6
7  repeat {
8    r++;
9    if (r == n)
10     return "prime";
11   if (r | n)
12     return "composite";
13 } until (prime(r) ∧ o_r(n) > o_min);
14
15 a_max = 2·⌈√r⌉ · ⌈log(n)⌉;
16 for (a ∈ {1, ..., a_max}) {
17   if ((x+a)^n ≢_{x^r−1,n} x^{n mod r}+a)
18     return "composite";
19 }
20
21 return "prime";
```

Bemerkungen zur Implementierung:

1. Der Test auf perfekte Potenzen (Zeile 1) ist wie zu Beginn der Vorlesung implementiert.

2. Primzahltest für r (Zeile 13): Sieb des Eratosthenes, jeweils in Zweierpotenzen im Voraus berechnet, d.h. falls $r = 2^i + 1$ ist, so bestimme alle Primzahlen bis zur Größe 2^{i+1}.

3. Für $o_r(n)$ (Zeile 13) werden $n \mod r, n^2 \mod r, n^3 \mod r, \ldots$ berechnet und jeweils getestet, wann dies 1 wird.

4. Die Berechnung von $\lceil \log n \rceil$ und $\lceil \sqrt{r} \rceil$ (Zeilen 5 und 15) erfolgt nach Standardverfahren.

5. Mittels iteriertem Quadrieren berechnet man $(x+a)^n \not\equiv_{(x^r-1,n)} x^{n \bmod r} + a$ (Zeile 17).

1.8.3 Laufzeitanalyse

Wir bestimmen zunächst die Anzahl der arithmetischen Operationen. Dann berücksichtigen wir, dass die größte auftretende ganze Zahl kleinergleich n^2 ist.
Vorbereitung:

1. Für alle $n \geq 1$ gilt $\sum_{i=1}^{n} i2^i = (n-1)2^{n+1} + 2$.

2. Eine Multiplikation in $\mathbb{Z}_n[x]/(x^r - 1)$ kann in $\mathcal{O}(r^2)$ bzw. $\widetilde{\mathcal{O}}(r)$ (mit diskreter Fouriertransformation) Ringoperationen ($R = \mathbb{Z}_n$) berechnet werden.

Beweis:

1. Übung.

2. Elemente von $\mathbb{Z}_n[x]/(x^r - 1)$ sind Polynome vom Grad $< r$. □

Die eigentliche **Analyse** erfolgt nun in drei Teilen:

1. **Potenztest**: möglich in $\mathcal{O}(\log^2 n \log\log n) \subseteq \widetilde{\mathcal{O}}(\log n)$.

2. Schleife zum **Bestimmen von** r (dabei bezeichne $\rho(n)$ das r, das die Schleife für ein n liefert):

   a) Die Prüfungen, ob $r = n$ oder $r \mid n$ gilt, benötigen
      - pro Schleifendurchlauf eine arithmetische Operation
      - insgesamt $\mathcal{O}(\rho(n))$

   b) **Primzahltest**:
      - „Ein Sieb“ bis 2^{i+1} benötigt $\mathcal{O}(i2^i)$ Operationen,
      - alle Siebe benötigen zusammen

$$\mathcal{O}\left(\sum_{i=1}^{\lceil \log \rho(n) \rceil} i2^i\right) \leq \log(\rho(n))2^{\log(\rho(n))+2} + 2 \in \mathcal{O}(\rho(n)\log\rho(n)).$$

c) Die **Prüfung der Ordnung** ($o_r(n) > 4\lceil \log n \rceil^2$) benötigt
   - für ein einzelnes r: $\mathcal{O}(\log^2 n)$ Operationen,
   - insgesamt $\mathcal{O}(\rho(n) \log^2 n)$ Operationen.

3. Der **Polynomäquivalenztest** ($(x+a)^n \equiv x^{n \bmod r} + a$ in $\mathbb{Z}_n[x](x^r - 1)$) benötigt
   - für ein einzelnes a: $\mathcal{O}(\log n)$ mal Quadrieren, also $\mathcal{O}(r^2 \log n)$ bzw. $\widetilde{\mathcal{O}}(r \log n)$ Operationen,
   - insgesamt $\mathcal{O}(\rho(n)^{\frac{5}{2}} \log^2 n)$ bzw. $\widetilde{\mathcal{O}}(\rho(n)^{\frac{3}{2}} \log^2 n)$ Operationen.

Lemma:

1. Die Anzahl der vom AKS-Test durchgeführten arithmetischen Operationen ist $\mathcal{O}(\rho(n)^{\frac{5}{2}} \log^2 n)$ bzw. $\widetilde{\mathcal{O}}(\rho(n)^{\frac{3}{2}} \log^2 n)$.
2. Die Anzahl der vom AKS-Test durchgeführten binären Operationen ist $\mathcal{O}(\rho(n)^{\frac{5}{2}} \log^4 n)$ bzw. $\widetilde{\mathcal{O}}(\rho(n)^{\frac{3}{2}} \log^3 n)$.

Beweis: Der dritte Teil ist dominant. □

Noch offen: Wir suchen noch eine obere Schranke für $\rho(n)$. Dazu gibt es drei Möglichkeiten:

1. Eine einfache Schranke liefert der Primzahlsatz 1.2.6.
2. Eine bessere Schranke erhält man mit einem tiefliegenden Satz aus der analytischen Zahlentheorie (über die Dichte der Primzahlen p, für die $p-1$ einen großen Primteiler hat).
3. Glaubt man (oder beweist man) die Vermutung über Sophie-Germain-Primzahlen ($p = 2q+1$), erhält man eine noch bessere Schranke.

Wir zeigen hier die erste Variante.

Lemma: Es gilt $\rho(n) \leq 20\lceil \log n \rceil^5$.

Beweis: Für $n \in \{2, 3\}$ ist dies trivial. Für $n \geq 4$ betrachte

$$B = \prod_{i=1}^{4L^2} (n^i - 1) \quad \text{mit } L = \lceil \log n \rceil.$$

Nutze nun eine alte Abschätzung:

$$\prod_{\substack{p \leq 2n \\ p \text{ Primzahl}}} p > 2^m, \text{ also } \prod_{\substack{r \leq 20L^5 \\ r \text{ Primzahl}}} r > 2^{10L^5}.$$

Nun gilt:

$$B < n^1 \cdot n^2 \cdots n^{4L^2} = n^{\frac{(4L^2+1)4L^2}{2}} \leq 2^{L^{\cdots}_{\cdots}} = 2^{8L^5+2L^3} \leq 2^{10L^5}.$$

Damit ergibt sich:

$$B < \prod_{\substack{r \leq 20L^5 \\ r \text{ Primzahl}}} r.$$

Falls $r \mid n$ gilt für eines der r, so wäre $\rho(n) \leq 4L^2$. Also können wir $r \nmid n$ annehmen.
Dann existiert eine Primzahl $r \leq 20L^5$ mit $r \nmid B$. Also ist $r \nmid (n^i - 1)$ für alle $i \leq 4L^2$. Es folgt $n^i \not\equiv 1 \mod r$ für alle $i \leq 4L^2$, damit folgt $o_r(n) > 4L^2$. □

Satz: Der AKS-Test benötigt $\mathcal{O}(\log^{16\frac{1}{2}} n)$ bzw. $\widetilde{\mathcal{O}}(\log^{10\frac{1}{2}} n)$ Binäroperationen.

Verbesserungen aufgrund der anderen Varianten oben:

- mit der zweiten (garantierten) Variante: $\widetilde{\mathcal{O}}(\log^{7.5} n)$ Binäroperationen
- mit der dritten (vermuteten) Variante: $\widetilde{\mathcal{O}}(\log^{6} n)$ Binäroperationen

1.8.4 Korrektheitsbeweis

Dies ist die von *D. J. Bernstein*[5] vereinfachte Version des Korrektheitsbeweises; eine Präsentation von Agrawal über den Primzahltest und dessen Korrektheit ist unter ([6]) zu finden.

Satz: Seien n, r ganze Zahlen mit folgenden Eigenschaften:

(α) $n \geq 3$

(β) $r < n$ Primzahl

(γ) $a \nmid n$ für $2 \leq a \leq r$

(δ) $o_r(n) > 4 \cdot \log^2 n$

(ε) $(x+a)^n = x^n + a$ in $Q = \mathbb{Z}_n[x]/(x^r - 1)$ für a mit $1 \leq a \leq 2\sqrt{r} \log n$

Dann ist n eine Primzahlpotenz.

[5] `http://cr.yp.to/djb.html`
[6] `http://stacs05.fmi.uni-stuttgart.de/invited.html`

Beweis: Sei im Folgenden p ein echter Primteiler von n, weiter sei $l = \lfloor 2\sqrt{r}\log n \rfloor$. Für $q = x^r - 1$ definieren wir zudem:

$$R = \mathbb{Z}_n[x] \qquad Q = \mathbb{Z}_n[x]/(q)$$
$$R' = \mathbb{Z}_p[x] \qquad Q' = \mathbb{Z}_p[x]/(q)$$

Sei $K = \mathbb{Z}_p[x]/(h)$ mit h einem irreduziblen Faktor von $1 + x + \ldots + x^{r-1}$ vom Grad $d = o_p(r)$, und sei zuletzt noch $\zeta = x \bmod h (\in K)$, dann ist $o_{K^*}(\zeta) = r$.

□

Wir werden jetzt in **drei Schritten** vorgehen: Zunächst definieren wir *Introspektivität* (I), eine Schlüsseleigenschaft von ζ. Danach konstruieren wir eine große Gruppe (II), bevor wir zum Endspiel (III) kommen.

Schritt I: Introspektivität

Definition: Die *Introspektivität* ist folgende Relation $I(b, f)$ für $b \geq 1$ und $f \in \mathbb{Z}_p[x] = R'$, die definiert ist durch $f^b = f(x^b)$ in $\mathbb{Z}_p[x]/(q) = Q'$, d.h. $f^b \bmod q = f(x^b) \bmod q$.

Seien nun folgende Mengen definiert:

$$B = \left\{ n^i p^j \;\middle|\; i, j \geq 0 \right\}$$
$$P = \left\{ \prod_{a=1}^{l} (x+a)^{\beta_a} \;\middle|\; \beta_a \geq 0 \right\} \subseteq \mathbb{Z}_p[x] = R'$$

Ziel ist nun zunächst zu zeigen, dass $I(B, P)$ gilt, und danach ein Hauptlemma, das besagt: Für $f \in P$ und $g = f \bmod h$, dann gilt $g^b = f(\zeta^b)$ für alle $b \in B$.

Lemma:

1. $p > r$
2. $r \nmid n$
3. $r \geq l$
4. $1 \leq a' - a \leq p$ für alle a, a' mit $1 \leq a < a' \leq l$
5. $p \leq \frac{1}{2}n$

Beweis:

1. folgt aus (γ)

2. folgt aus (γ)
3. mit (δ) gilt $r > o_r(n) > 4\log^2 n$, also $\sqrt{r} > 2\log n$, daraus folgt die Behauptung nach Definition von l
4. aus $l \leq r < p$ folgt $a, a' < p$
5. folgt aus der Annahme, dass p echter Teiler von n ist □

Lemma: Es gilt $I(n, x + a)$ für alle $1 \leq a \leq l$.

Beweis: Aus (ε) folgt $(x + a)^n - (x^n + a) = q \cdot g$ mit $g \in \mathbb{Z}_n[x]$. In $\mathbb{Z}[x]$ übersetzt heißt das:

$$(x + a)^n - (x^n + a) = qg' + ng'' \text{ für } g', g'' \in \mathbb{Z}[x]$$

Nun gilt aber in $\mathbb{Z}_p[x]/(q)$: $qg' + ng'' = qg' + p\frac{n}{p}g'' = 0$. □

Lemma: Es gilt $I(p, x + a)$ für alle $1 \leq a \leq l$.

Beweis: Für alle $f \in \mathbb{Z}_p[x]$ gilt laut eines Satzes weit oben: $f^p(x) = f(x^p)$. □

Lemma (Multiplikativität in der zweiten Komponente): Aus $I(b, f)$ und $I(b, g)$ folgt $I(b, fg)$.

Beweis: Es gilt:

$$(fg)^b = f^b g^b = f(x^b)g(x^b) = (fg)(x^b)$$

□

Lemma (Multiplikativität in der ersten Komponente): Aus $I(b, f)$ und $I(c, f)$ folgt $I(bc, f)$.

Beweis: Es gilt:

$$f^{bc} = (f^c)^b =_{Q'} (f(x^c))^b = f(x^c) \cdot \ldots \cdot f(x^c) = f^b(x^c)$$

Aus $I(b, f)$ folgt: Es existiert ein $g \in \mathbb{Z}_p[x]$ mit

$$f^b - f(x^b) = gq$$

Durch ersetzen von x durch x^c folgt daraus für $g' = g(x^c)$:

$$f^b(x^c) - f(x^{bc}) = g' \cdot (x^{rc} - 1) = g' \cdot g'' \cdot (x^r - 1) = g' \cdot g'' \cdot q$$

Also gilt $f^b(x^c) = f(x^{bc})$ in $\mathbb{Z}_p[x]/(q)$. Nun gilt insgesamt in $\mathbb{Z}_p[x]/(q)$:

$$f^{bc} = f^b(x^c) = f(x^{bc}).$$

□

Wir hatten oben definiert:

$$B = \left\{ n^i p^j \;\middle|\; i, j \geq 0 \right\}$$
$$P = \left\{ \prod_{a=1}^{l} (x+a)^{\beta_a} \;\middle|\; \beta_a \geq 0 \right\} \subseteq \mathbb{Z}_p[x] = R'$$

Mit den Lemmata können wir nun folgern:

Folgerung: Es gilt $I(B, P)$.

Der nächste Schritt ist, folgendes Hauptlemma zu zeigen:

Hauptlemma: Sei $f \in P$ und $g = f \bmod h$ mit h irreduzibler Faktor von $1 + x + \ldots + x^{r-1}$. Dann gilt für alle $b \in B$ in $\mathbb{Z}_p[x]/(h)$: $g^b = f(\zeta^b)$.

Beweis: In $\mathbb{Z}_p[x]/(h)$ gilt: $f = g$, also $f^b = g^b$. Außerdem gilt $f^b = f(x^b)$ in $\mathbb{Z}_p[x]/(q)$. Da $h \mid q$ ist, gilt auch $f^b = f(x^b)$ in $\mathbb{Z}_p[x]/(h)$.

Zudem gilt $\zeta = x$ in $\mathbb{Z}_p[x]/(h)$, also auch $\zeta^b = x^b$. Insgesamt haben wir damit in $\mathbb{Z}_p[x]/(h)$:

$$g^b = f^b = f(x^b) = f(\zeta^b)$$

□

Schritt II: Eine große Gruppe

Sei $G = P \bmod h$, und $T = \left\{ \zeta^b \;\middle|\; b \in B \right\}$, sei $t = |T|$.

Proposition: $|G| > \frac{1}{2} n^{2\sqrt{t}}$ mit $t > 4 \log^2 n$.

Lemma:

1. $x + a \bmod h \neq x + a' \bmod h$ für $1 \leq a < a \leq l$.
2. $x + a \bmod h \neq 0$ für $1 \leq a \leq l$.

Beweis:

1. Aus $x + a \equiv x + a' \pmod{h}$ folgt $a - a' = 0$ in K, dies widerspricht dem ersten Lemma.
2. Annahme, $x + a \bmod h = 0$ für ein a. Dann muß $h \mid x + a$ gelten, also $h = x + a$. Dann gilt $\zeta = x \bmod h = -a$. Zur Erinnerung: ζ ist primitive r-te Einheitswurzel, $o_p(\zeta) = r$.

Aus $I(n, x+a)$ ergibt sich zudem: $(x+a)^n = x^n + a$ in $\mathbb{Z}_p[x]/(q)$, also ist in $\mathbb{Z}_p[x]$:

$$(x+a)^n = x^n + a + g \cdot q$$
$$(x+\zeta)^n = x^n + \zeta + g \cdot q$$

Nuun liefert Einsetzen von ζ:

$$0 = \zeta^n - \zeta + g(\zeta) \cdot q(\zeta)$$

Dabei ist $q(\zeta) = 0$, da ζ primitive r-te Eineheitswurzel ist. Nun folgt $\zeta = \zeta^n$, d.h. $\zeta^{n-1} = 1$.

Damit ist $r \mid n-1$, d.h. $n \bmod r = 1$, damit ist $o_r(n) = 1$. Dies ist ein Widerspruch zu (δ). □

Lemma: G ist eine Gruppe.

Beweis: G ist eine Menge von Produkten von Elementen von K^*, und da K^* endlich ist, ist damit G eine Gruppe.

Lemma: $r > t > 4\log^2 n$

Beweis:

- Zunächst $r > t$: Wir hatten $t = |T|$ und $T = \left\{ \zeta^b \;\middle|\; b \in B \right\}$ definiert, es gilt aber $T \subseteq \langle\zeta\rangle$ und $|\langle\zeta\rangle| = r$. Es reicht also zu zeigen, dass $\zeta^b \neq 1$ ist für alle $b \in B$.

  Aus $\zeta^b = 1$ würde $r \mid b = n^i p^j$ folgen, das ginge nur für $r \mid n$, Widerspruch zu (γ).

- Nun zeigen wir $t > 4\log^2 n$: Es gilt $\left\{ \zeta^{n^i} \;\middle|\; i \geq 0 \right\} \subseteq T$, es gilt weiterhin $\zeta^{n^i} = \zeta^{n^j}$ genau dann, wenn $r \mid n^i - n^j$ ist.

  Das heißt, dass (mit (δ)) gilt:

$$\left|\left\{ \zeta^{n^i} \;\middle|\; i \geq 0 \right\}\right| = \left|\left\{ n^i \bmod r \;\middle|\; i \geq 0 \right\}\right| = o_r(n) > 4\log^2 n$$

□

Lemma: Falls $f_0 \neq f_1 \in P$ mit $\deg(f_0), \deg(f_1) < t$, so ist $f_0 \bmod h \neq f_1 \bmod h$.

Beweis: Annahme: $g = f_0 \bmod h = f_1 \bmod h$. Benutze das Hauptlemma: Sei $b \in B$ beliebig, dann ist

$$f_0(\zeta)^b = g^b = f_1(\zeta^b)$$

Dann stimmen f_0 und f_1 an mehr als t Stellen überein, sie sind also gleich, Widerspruch! □

Beweis von $|G| > \frac{1}{2}n^{2\sqrt{t}}$: Setze $\mu = \min\{l, t-1\}$. Wir betrachten

$$P' = \left\{ \prod_{1 \le a \le \mu} (x+a)^{\beta_a} \mid \beta_a \in \{0,1\} \right\}.$$

Aus obigen Lemmata folgt, dass $|P'| = 2^\mu$. Nun zeigen wir, $2^\mu > \frac{1}{2}n^{2\sqrt{t}}$.

1. Fall, $\mu = l$: Laut Definition gilt, $l = \lfloor 2\sqrt{r}\log n \rfloor > 2\sqrt{t}\log n - 1$. Also

$$2^\mu = 2^l > 2^{2\sqrt{t}\log n - 1} = \frac{1}{2}(2^{\log n})^{2\sqrt{t}} = \frac{1}{2}n^{2\sqrt{t}}.$$

2. Fall, $\mu = t-1$: Dann gilt,

$$\mu = t - 1 = \sqrt{t}\cdot\sqrt{t} - 1 > \sqrt{t}2\log n - 1,$$

also

$$2^\mu > 2^{\sqrt{t}2\log n - 1} = \frac{1}{2}n^{2\sqrt{t}}.$$

□

Schritt III: Endspiel

Sei $B_0 = \{n^i p^j \mid i,j \le \lfloor\sqrt{t}\rfloor\}$. Dann gibt es $(\lfloor\sqrt{t}\rfloor + 1)^2 > t$ viele Paare (i,j) in der Definition von B_0.

Behauptung: Alle Elemente aus B_0 sind klein, d.h. $b < |G|$ für alle $b \in B_0$.

Beweis: Da p echter Teiler von n ist, gilt:

$$b = n^i p^j \le n^{\lfloor\sqrt{t}\rfloor} \cdot \left(\frac{1}{2}n\right)^{\lfloor\sqrt{t}\rfloor} = \frac{1}{2^{\lfloor\sqrt{t}\rfloor}} n^{2\lfloor\sqrt{t}\rfloor} \le \frac{1}{2}n^{2\sqrt{t}} < |G|.$$

□

Lemma: Es gilt, $\zeta^{b_0} \neq \zeta^{b_1}$ für $b_0, b_1 \in B_0$, $b_0 \neq b_1$.

Beweis: Angenommen, $\zeta^{b_0} = \zeta^{b_1}$ mit $b_0 \neq b_1$. Dann gilt für alle $g \in G$, $g = f \bmod h$:

$$g^{b_0} = f(\zeta^{b_0}) = f(\zeta^{b_1}) = g^{b_1},$$

also $g^{b_0} - g^{b_1} = 0$. Also sind alle Elemente von G Nullstellen von $q = x^{b_0} - x^{b_1}$. Wegen $\deg q < |G|$ folgt dann, $q = 0$, also $b_0 = b_1$. Widerspruch! □

Abschließend zeigen wir nun, dass n eine Potenz von p ist: Aus obigem Lemma und der Bemerkung folgt, dass es Paare $(i, j) \neq (i', j')$ mit $n^i p^j = n^{i'} p^{j'}$ gibt. Trivialerweise gilt etwa $i > i'$. Also $n^{i-i'} = p^{j'-j}$, also ist n eine p-Potenz.

Damit ist der Beweis der Korrektheit des AKS-Tests abgeschlossen. □

1.9 Übersicht über die Primzahtests

- trivialer Algorithmus (1.5.1): co-NP-Verfahren
- mit Lemma von Lukas (1.5.1): NP-Verfahren
- Lehmann-Test (1.5.1): BPP-Verfahren
- Fermat-Test (1.5.2): $\mathcal{O}(\log n)$ Binäroperationen; Fehler für Carmichael-Zahlen
- Berrizbeitia-Bernstein-Test: RP-Verfahren mit $\mathcal{O}(\log^4 n)$ Binäroperationen; einseitiger Fehler für Primzahlen
- Miller-Rabin-Test (1.5.5): co-RP-Verfahren mit $\mathcal{O}(\log^2 n)$ Binäroperationen; einseitiger Fehler für zerlegbare Zahlen mit Wahrscheinlichkeit $\leq \frac{1}{4}$
- Solovay-Strassen-Test (1.6): co-RP-Verfahren mit $\mathcal{O}(\log^2 n)$ Binäroperationen; einseitiger Fehler für zerlegbare Zahlen mit Wahrscheinlichkeit $\leq \frac{1}{2}$
- Agrawal-Kayal-Saxena-Test (1.8): P-Verfahren mit $\mathcal{O}(\log^{7.5} n)$ Binäroperationen; garantiert korrekt

2 Faktorisierungsalgorithmen

2.1 Einleitung

2.1.1 Generelle Vorgehensweise

Eine Primfaktorzerlegung wird normalerweise nach folgendem **Prinzip** durchgeführt:

1. bestimme „kleine“ Faktoren und spalte sie ab (bestimme den größten gemeinsamen Teiler von der Zahl und einem Produkt aus den kleinen Faktoren)
2. rekursive Vorgehensweise:
   (a) ersetze die Zahl durch deren kleinste Wurzel, falls möglich (durch Test auf perfekte Potenzen)
   (b) Primzahltest
   (c) bestimme einen Faktor (durch die entsprechende komplizierte Methode) sowie den „Cofaktor“

2.1.2 Probedivision

Algorithmus: Sei $n \geq 3$ eine Zahl, die keine perfekte Potenz ist, und $b \geq 2$.

```
1 for (p ∈ {2, ..., b})
2   if (p | n) return (p, n / p);
3 return;
```

Bemerkungen:

1. Der obige Algorithmus spaltet nur einen Faktor kleinergleich b ab, kann aber leicht verallgemeinert werden.
2. Pessimale Laufzeit in arithmetischen Operationen ist $\mathcal{O}(\min(b, \sqrt{n})) \subseteq \mathcal{O}(\sqrt{n})$, dabei ist $\sqrt{n} = n^{\frac{1}{2}} = L_n[1, \frac{1}{2}]$ mit folgender Schreibweise:

$$L_n[u, v] = e^{v \cdot \ln^u n (\ln \ln n)^{(1-u)}}$$

   Dabei ist $L_n[1, v] = n^v$ und $L_n[0, v] = (\ln n)^v$, diese Schreibweise deckt also die Spanne der Laufzeiten für Faktorisierungsalgorithmen ab!

2.1.3 Klassifizierung von Faktorisierungsalgorithmen

Wir können die Faktorisierungsalgorithmen folgendermaßen klassifizieren:

- deterministisch oder randomisiert
- exponentiell oder subexponentiell
- Heuristik oder vollständige, analysierte Verfahren
- Siebtechniken (großer Speicherverbrauch)

2.2 Einfache Algorithmen

2.2.1 Fermat-Methode

Lemma: Sei n eine ungerade Zahl größergleich 3. Dann ist n zerlegbar genau dann, wenn es a und b mit $\lceil\sqrt{n}\rceil \leq a \leq \lfloor\frac{n+9}{6}\rfloor$ und $0 \leq b < a-1$ gibt, so dass $a^2 - n = b^2$.

Beweis:

„⇐“ Aus $a^2 - n = b^2$ folgt $n = a^2 - b^2 = (a-b)(a+b)$.

„⇒“ Sei $n = cd$ mit $c > d > 1$. Dann folgt mit $a+b = c$ und $a-b = d$, dass $a = \frac{c+d}{2}$ und $b = \frac{c-d}{2}$. Aus der Gleichung $a^2 - n = b^2$ folgt dann auch $a \geq \lfloor\sqrt{n}\rfloor$.

Der beste Fall wäre $c = d = \sqrt{n}$, der schlechteste Fall wäre $d = 3$ und $c = \frac{n}{3}$ Primzahl, dann wäre

$$a = \frac{c+d}{2} = \frac{\frac{n}{3}+3}{2} = \frac{n+9}{6}$$

□

Algorithmus Fermat-Methode:

```
1 for (a ∈ {⌈√n⌉, ..., ⌊(n+9)/6⌋}) {
2   b = ⌈√(a² − n)⌉};
3   if (b² == a² − n)
4     return a + b;
5 }
```

Satz: Die Fermat-Methode ist korrekt mit pessimaler Anzahl von Operationen $\Theta(n)$.

Bemerkung: Fermat ist „gut“ bei großen Faktoren (d.h. nah an $\sqrt{n}$), die Probedivision bei kleinen Faktoren.

2.2.2 Pollardsche $(p-1)$-Methode

Lemma: Für n und $p \geq 3$ Primfaktor von n sowie m mit $p-1 \mid m$ gilt:

$$p \mid \text{ggT}(2^m - 1, n) = \text{ggT}(2^m - 1 \bmod n, n).$$

Beweis: Es gilt $2^{p-1} \equiv 1 \pmod{p}$, also $2^m \equiv 1 \pmod{p}$, damit gilt $p \mid 2^m - 1$. Da aber $p \mid n$ gilt, teilt p auch den ggT. □

Algorithmus: Sei $m(b) = \text{kgV}(1, \ldots, b)$, und sei $n \geq 3$ zerlegbar.

```
1 m = m(b); // oder Vielfaches
2 a = 2^m mod n;
3 g = ggT(a-1, n);
4 if (1 < g < n)
5   return g;
6 else
7   return;
```

Bemerkung:

1. Es gibt keine Garantien, dass der Algorithmus Faktoren findet!
2. Zeile 2 wird implementiert durch iteriertes Quadrieren.
3. Statt der 2 als Basis kann auch eine zufällige Zahl gewält werden in Zeile 2.
4. Der Aufwand des Algorithmus' wird durch die Berechnung von m bestimmt. Dafür gibt es mehrere Ansätze:
   - $m = b!$
   - $m(b+1) = \frac{(b+1) \cdot m(b)}{\text{ggT}(b+1, m(b))}$
   - $m(b)$ mit Sieb des Eratosthenes bilden
5. Es läßt sich bei Nichterfolg eine zweite Phase anschließen: Wähle $b' > b$ und besimme Primzahlen $q_0 < q_1 < \ldots < q_{r-1}$ aus $(b, b']$, führe danach den obigen Test durch mit $2^{m(b)q_i}$.

   Beachte für die Berechnung:

   $$2^{m(b)q_{i+1}} = 2^{m(b)q_i} \cdot 2^{m(b) \cdot (q_{i+1} - q_i)}$$

   Dabei wird $(q_{i+1} - q_i)$ relativ klein, man kann daher $2^{m(b) \cdot d}$ für kleine d in einer Tabelle abgelegt werden.

2.2.3 Lehmann-Methode

Das **Ziel** ist, einen Faktorisierungsalgorithmus in $\mathcal{O}(n^{\frac{1}{3}})$ zu erhalten.

Die **Idee** ist ähnlich zur Fermat-Methode: Statt $a^2 - n = b^2$ betrachten wir allerdings $a^2 - k \cdot n = b^2$, wobei k eine neue Variable ist. Dann faktorisieren wir $k \cdot n$ und mit etwas Glück gilt $1 < \mathrm{ggT}(n, d) < n$ für einen der Faktoren d.

Algorithmus: Sei $n \geq 21$.

```
1  for (k ∈ {2, ..., n^(1/3)})
2    if (k | n) return k;
3  for (k ∈ {1, ..., n^(1/3)}) {
4    a_min = ⌈2·√(k·n)⌉);
5    a_max = ⌊2·√(k·n) + n^(1/16) / 4·√k⌋);
6    for (a ∈ {a_min, ..., a_max}) {
7     b = sqrt(a^2 − 4·k·n);
8     if (b ∈ ℤ)
9       return ggT(a + b, n);
10   }
11 }
12 return "prime";
```

Satz:

1. Die Lehmann-Methode ist korrekt.
2. Die pessimale Anzahl arithmetischer Operationen, die von der Lehmann-Methode ausgeführt werden, ist $\mathcal{O}(n^{\frac{1}{3}} \log n)$.

Beweis der Laufzeitschranke: Die Probedivision benötigt $\mathcal{O}(n^{\frac{1}{3}})$ Operationen. Der Rest benötigt

$$\left(\sum_{k=1}^{\lceil n^{\frac{1}{3}} \rceil} \left(\frac{n^{\frac{1}{6}}}{4\sqrt{k}} + 1 \right) \cdot t_{\text{Quadratwurzel}} \right) + t_{\text{ggT}}$$

In der Übung wird folgende Abschätzung gezeigt:

$$\sum_{k=1}^{\lceil n^{\frac{1}{3}} \rceil} \left(\frac{n^{\frac{1}{6}}}{4\sqrt{k}} + 1 \right) \in \mathcal{O}(n^{\frac{1}{3}})$$

Berechnen der Quadratwurzel geht in höchstens $\log n$ (vielleicht auch schneller), damit ist die Laufzeitschranke gezeigt. □

Als Vorbereitung für den Beweis der Korrektheit:

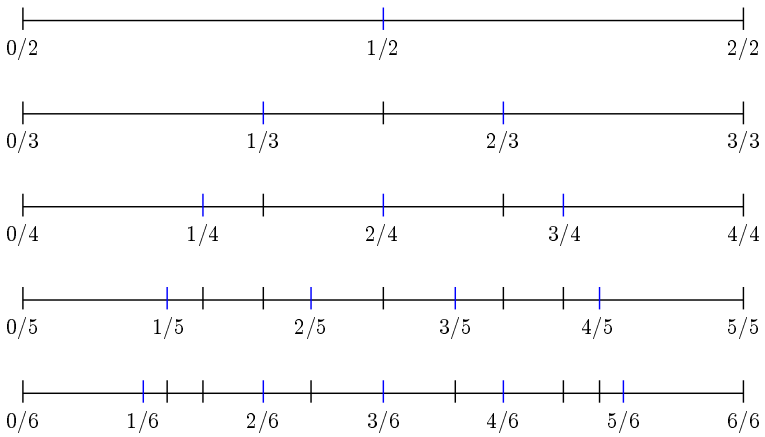
Lemma aus der Zahlentheorie: Für alle $B > 1$ und jede reelle Zahl r gibt es natürliche Zahlen u und v, so dass gilt: $v \leq B$ und

$$\left|\frac{u}{v} - r\right| < \frac{1}{vB}$$

Beweis: Ohne Einschränkung sei $r \in [0, 1]$. Wir betrachten die sogenannte *Farey-Folge* der Ordnung n, d.h. alle Zahlen $\frac{h}{k}$ mit $k \leq n$ und $h \top k_i$, stelle diese geordnet dar:

$$\frac{0}{1} = \frac{h_0}{k_0} < \frac{h_1}{k_1} < \ldots < \frac{h_{s-1}}{k_{s-1}} = \frac{1}{1}.$$

Das Aufbauen dieser Folge über n kann man sich wie folgt vorstellen:



Behauptung: $k_i + k_{i+1} > n$. Sei dazu

$$\alpha = \frac{h_i + h_{i+1}}{k_i + k_{i+1}}.$$

Dann gilt $\alpha \in \left(\frac{h_i}{k_i}, \frac{h_{i+1}}{k_{i+1}}\right)$, denn es gilt:

$$\alpha - \frac{h_i}{k_i} = \frac{h_i + h_{i+1}}{k_i + k_{i+1}} - \frac{h_i}{k_i} = \frac{k_i h_i + k_i h_{i+1} - h_i k_i - h_i k_{i+1}}{k_i(k_i + k_{i+1})}$$
$$= \frac{k_i h_{i+1} - h_i k_{i+1}}{k_i(k_i + k_{i+1})} = \frac{\left(\frac{h_{i+1}}{k_{i+1}} - \frac{h_i}{k_i}\right) k_{i+1}}{k_i + k_{i+1}} > 0$$

und analog

$$\frac{h_{i+1}}{k_{i+1}} - \alpha = \frac{h_{i+1}}{k_{i+1}} - \frac{h_i + h_{i+1}}{k_i + k_{i+1}} = \frac{h_{i+1}k_i + h_{i+1}k_{i+1} - h_i k_{i+1} - h_{i+1}k_{i+1}}{k_{i+1}(k_i + k_{i+1})}$$
$$= \frac{h_{i+1}k_i - h_i k_{i+1}}{k_{i+1}(k_i + k_{i+1})} = \frac{\left(\frac{h_{i+1}}{k_{i+1}} - \frac{h_i}{k_i}\right) k_i}{k_i + k_{i+1}} > 0.$$

Würde nun $k_i + k_{i+1} \leq n$ gelten, so würde α zur Farey-Folge gehören, Widerspruch. Damit gilt $k_i + k_{i+1} > n$.

Sei $r \in (0, 1)$ beliebig. Dann gilt für ein geeignetes i:

$$r \in \left[\frac{h_i + h_{i+1}}{k_i + k_{i+1}}, \frac{h_{i+1}}{k_{i+1}}\right] \quad \text{oder} \quad r \in \left[\frac{h_i}{k_i}, \frac{h_i + h_{i+1}}{k_i + k_{i+1}}\right].$$

- Falls $r \in \left[\frac{h_i+h_{i+1}}{k_i+k_{i+1}}, \frac{h_{i+1}}{k_{i+1}}\right]$, so gilt:

$$0 \leq \frac{h_{i+1}}{k_{i+1}} - r \leq \frac{h_{i+1}}{k_{i+1}} - \frac{h_i + h_{i+1}}{k_i + k_{i+1}} = \frac{h_{i+1}k_i - h_i k_{i+1}}{k_{i+1}(k_i + k_{i+1})}$$
$$\overset{(\star)}{=} \frac{1}{k_{i+1}\underbrace{(k_i + k_{i+1})}_{>n}} < \frac{1}{k_{i+1}n}.$$

  Dabei folgt die Umformung im Zähler in Schritt $(\star)$ aus einem Satz, der besagt, dass $h_{i+1}k_i - h_i k_{i+1} = 1$ gilt – siehe Übung.

  Setze also $u = h_{i+1}$ und $v = k_{i+1}$.

- Falls andererseits $r \in \left[\frac{h_i}{k_i}, \frac{h_i+h_{i+1}}{k_i+k_{i+1}}\right]$, so gilt analog:

$$0 \leq r - \frac{h_i}{k_i} \leq \frac{h_i + h_{i+1}}{k_i + k_{i+1}} - \frac{h_i}{k_i} = \frac{h_{i+1}k_i - h_i k_{i+1}}{k_i(k_i + k_{i+1})}$$
$$\overset{(\star)}{=} \frac{1}{k_i\underbrace{(k_i + k_{i+1})}_{>n}} < \frac{1}{k_i n}.$$

  In diesem Fall setze wir also $u = h_i$ und $v = k_i$.

In jedem Fall gilt dann, dass $\left|r - \frac{u}{v}\right| < \frac{1}{vn}$. Um den Beweis abzuschließen, reicht es also $n = B$ zu wählen. □

Beweis der Korrektheit der Lehmann-Methode: Sei n zerlegbar, ohne Teiler kleinergleich $n^{\frac{1}{3}}$ (d.h. der Probedivisions-Teil aus dem Algorithmus findet keinen Teiler). Dann zeigen wir, dass geeignete a, b existieren.

Da n keine Teiler kleinergleich $n^{\frac{1}{3}}$ hat, muss $n = pq$ mit Primzahlen p, q mit $n^{\frac{1}{3}} < p \leq q \leq n$ gelten. Wende obiges Lemma für $B = n^{\frac{1}{6}}\sqrt{\frac{q}{p}}$ und $r = \frac{p}{q}$ an:

$$\left|\frac{p}{q} - \frac{u}{v}\right| < \frac{1}{vn^{\frac{1}{6}}\sqrt{\frac{q}{p}}},$$

daraus folgt:

$$|pv - qu| < \frac{\sqrt{pq}}{n^{\frac{1}{6}}} = \frac{n^{\frac{1}{2}}}{n^{\frac{1}{6}}} = n^{\frac{1}{3}}. \qquad (\star\star)$$

Setze nun $k = uv$. Dann gilt

$$\begin{aligned} k = uv = \frac{u}{v}v^2 &< v^2\left(\frac{p}{q} + \frac{1}{vB}\right) \\ &= \frac{p}{q}v^2 + \frac{v^2}{vB} \overset{(\star)}{\leq} \frac{p}{q}\frac{q}{p}n^{\frac{1}{3}} + 1 = n^{\frac{1}{3}} + 1. \end{aligned}$$

Die Abschätzung $(\star)$ gilt, da $\frac{v^2}{vB} \leq 1$ ist und $v^2 \leq B^2 = (n^{\frac{1}{6}}\sqrt{\frac{q}{p}})^2 = n^{\frac{1}{3}}\frac{q}{p}$ gilt.

Setze nun $a = uq + vp$, $b = |uq - vp|$. Dann gilt

$$4kn = a^2 - b^2 = u^2q^2 + 2uqvp + v^2p^2 - u^2q^2 + 2uqvp - v^2p^2 = 4uqvp.$$

Aus der Analysis wissen wir, dass $x + y \geq 2\sqrt{xy}$ gilt, also ist

$$a = uq + vp \geq 2\sqrt{uqvp} = 2\sqrt{kn}.$$

Damit ist die untere Schranke für a gezeigt.
Setze nun $\delta = a - 2\sqrt{kn}$. Dann gilt

$$4kn + 4\delta\sqrt{kn} \leq \left(2\sqrt{kn} + \delta\right)^2 = a^2 = 4kn + b^2 \overset{(\star)}{\leq} 4kn + n^{\frac{2}{3}}.$$

Der Schritt $(\star)$ gilt, da $b \leq n^{\frac{1}{3}}$ ist nach $(\star\star)$. Also ist $4\delta\sqrt{kn} \leq n^{\frac{2}{3}}$, d.h.,

$$\delta \leq \frac{n^{\frac{2}{3}}}{4\sqrt{kn}} = \frac{1}{4\sqrt{k}} \cdot \frac{n^{\frac{2}{3}}}{n^{\frac{1}{2}}} = \frac{n^{\frac{1}{6}}}{4\sqrt{k}}.$$

Insgesamt erhalten wir also:

$$\left\lceil 2\sqrt{kn} \right\rceil \leq a \leq \left\lfloor 2\sqrt{kn} + \frac{n^{\frac{1}{6}}}{4\sqrt{k}} \right\rfloor$$

Damit sind a und b Kandidaten für einen positiven Test im Algorithmus. Zu zeigen bleibt: $1 < \text{ggT}(a+b, n) < n$. Wir wissen: $4kn = a^2 - b^2 = (a+b)(a-b)$. Also gilt $n \mid (a+b)(a-b)$. Wenn also $a+b < n$ ist, dann gilt $1 < \text{ggT}(a+b, n) < n$.
Also:

$$\begin{aligned} a+b < n &\Leftrightarrow a + \sqrt{a^2 - 4kn} < n \\ &\Leftrightarrow n - a > \sqrt{a^2 - 4kn} \\ &\Leftrightarrow n^2 - 2an + a^2 > a^2 - 4kn \\ &\Leftrightarrow n > 2a - 4k \\ &\Leftrightarrow 2a < n + 4k \end{aligned}$$

Wir müssen also noch $2a < n + 4k$ zeigen. Es gilt:

$$2a \leq 4\sqrt{kn} + \frac{n^{\frac{1}{6}}}{2\sqrt{k}} \leq 4\sqrt{n^{\frac{1}{3}}} + \frac{1}{2}n^{\frac{1}{6}} = 4n^{\frac{2}{3}} + \frac{1}{2}n^{\frac{1}{6}} \overset{(\star)}{<} n \leq n + 4k$$

Der Schritt $(\star)$ gilt wiederum für n groß genug:

$$4n^{\frac{2}{3}} + \frac{1}{2}n^{\frac{1}{6}} \leq 4n^{\frac{2}{3}} + n^{\frac{2}{3}} = 5n^{\frac{2}{3}} < n$$

gilt für $5 < n^{\frac{1}{3}}$, also für $125 < n$. □

2.2.4 Pollard-Strassen-Multiplikations-Methode

Setze

$$B = \left\lceil n^{\frac{1}{4}} \right\rceil \quad \text{und} \quad f(x) = x(x-1)\cdots(x-B+1)$$

Bemerkung: Es gelten dann:

$$f(m) = \frac{m!}{(m-B)!} \quad \text{und} \quad f(jB) = \frac{(jB)!}{((j-1)B)!}$$

Idee: Versuche, kleine Teiler zu finden.

Algorithmus Pollard-Strassen-Methode: Sei n zerlegbar.

```
1 for (j ∈ {1, ..., ⌈n^(1/4)⌉} {
2   m = f(j·B) mod n;
3   b = ggT(m, n);
4   if (b > 1)
5     for (c ∈ {(j−1)·B, ..., j·B})
6       if (c | n) return c;
7 }
```

Dann ist c der kleinste Primteiler.

Bemerkung: Die Ausführung wie oben dargestellt ist korrekt. Aber, sie liefert *keine* Laufzeitschranke $\widetilde{\mathcal{O}}(n^{\frac{1}{4}})$. Die Idee ist nun, dass die Schleife parallel abgearbeitet wird, d.h. wir berechnen gleichzeitig $f(jB)$ für $j = 1, \ldots, B$.

Zur Auswertung eines Polynoms f vom Grad D an D Stellen $t_0, \ldots, t_{D-1}$ *(multiple Polynomauswertung)*:

Lemma: Sei f wie oben, $g = (x - t_0) \cdots (x - t_{\frac{D}{2}-1})$ und $r = f \bmod g$. Dann gilt $f(t_i) = r(t_i)$ für alle $i < \frac{D}{2}$.

Beweis: Es gibt h mit $f = gh + r$. Dann ist für $i < \frac{D}{2}$:

$$f(t_i) = g(t_i)h(t_i) + r(t_i) = 0 \cdot h(t_i) + r(t_i) = r(t_i)$$

Algorithmus multiple Polynomauswertung: Sei f ein Polynom vom Grad $D - 1$, sei $D = 2^k$ eine Zweierpotenz, und seien $t_0, \ldots, t_{D-1}$ beliebige Stellen.

```
1  if (k == 0) {
2    return {(t_0, f)};
3  } else {
4    T_0 = (t_0, ..., t_{D/2-1});
5    T_1 = (t_{D/2}, ..., t_{D-1});
6    g_0 = (x - t_0) · ... · (x - t_{D/2-1});
7    g_1 = (x - t_{D/2}) · ... · (x - t_{D-1});
8    r_0 = f mod g_0;
9    r_1 = f mod g_1;
10   return recursiveCall(r_0, T_0) ∪ recursiveCall(r_1, T_1);
11 }
```

Laufzeitabschätzung:

1. Die Berechnung aller g_i ist in Zeit $\widetilde{\mathcal{O}}(D)$ möglich – unter Benutzung der schnellen Fourier-Transformation (siehe Übung).
2. Berechung der r_i...

Insgesamt folgt damit eine Laufzeit von $\widetilde{\mathcal{O}}(D)$.

Anwendung bei Pollard-Strassen-Methode:

- $\widetilde{\mathcal{O}}(n^{\frac{1}{4}})$ für die Auswertung,
- ggT $n^{\frac{1}{4}}$-mal: $\widetilde{\mathcal{O}}(n^{\frac{1}{4}})$.
- letzter Test: $\mathcal{O}(n^{\frac{1}{4}})$.

Insgesamt also $\widetilde{\mathcal{O}}(n^{\frac{1}{4}})$.

2.2.5 Pollarsche ρ-Methode

Sei $n = p \cdot q$ mit $p \leq q$. Dann ist ein trivialer Ansatz, um p zu finden, einfach Zahlen $u_0, u_1, \ldots < n$ zu wählen und jeweils den $\mathrm{ggT}(n, u_i)$ zu bilden. Es gibt $q - 1$ viele Kandidaten für u_i, so dass $\mathrm{ggT}(n, u_i) > 1$ ist. Damit läßt sich die Wahrscheinlichkeit abschätzen als:

$$\mathrm{P}[\mathrm{ggT}(n, u_i) > 1] = \frac{q-1}{pq} \approx \frac{1}{p}.$$

Also ist der Erwartungswert für die Anzahl der u_i, bis wir einen Treffer haben, in $\Theta(p)$.

Als *Geburtstagsphänomen* ist bekannt, dass beim Wählen von n Zahlen aus N Zahlen die Wahrscheinlichkeit, dass zwei gleich sind $(p_N(n))$, ungefähr $1 - e^{-\frac{n^2}{2N}}$ ist. Es gilt damit:

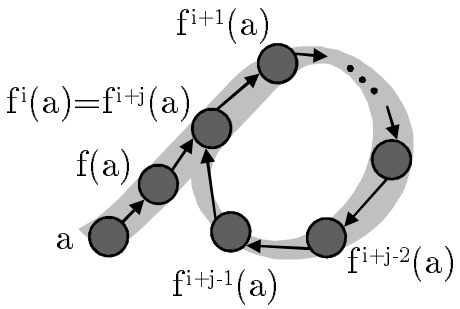
$$\begin{aligned} -e^{-\frac{n^2}{2N}} = \frac{1}{2} &\Leftrightarrow -e^{\frac{n^2}{2N}} = 2 \\ &\Leftrightarrow \frac{n^2}{2N} = \ln 2 \\ &\Leftrightarrow n = \sqrt{2N \ln 2} \end{aligned}$$

In unserem Fall muß für eine Wahrscheinlichkeit von $\frac{1}{2}$ dann die Anzahl der u_i mindestens $\sqrt{2n \ln 2}$ sein.

Neuer Ansatz: Wir suchen nach u_i, u_j mit $p \mid u_i - u_j$ – d.h. wir testen, ob $\mathrm{ggT}(u_i - u_j, n) > 1$ gilt.

Vorteil ist, dass nach dem Geburstagsphänomen der erwartete Erfolg $\Theta(\sqrt{p})$ ist. **Nachteil** jedoch: Wir benötigen bei $\sqrt{p}$ Zahlen auch $\approx (\sqrt{p})^2 = p$ viele Vergleiche (ggTs).

Sei $f\colon S \to S$ eine zufällige Funktion. Die zufällige Folge ist dann $f^0(a)$, $f^1(a)$, $f^2(a)$, ... Suche nach i, j mit $f^i(a) = f^{i+j}(a)$.



Formal: Sei $f\colon S \to S$ eine Funktion, S eine beliebige endliche Menge. Für $a \in S$ sei $f_a^0 = a$ und $f_a^{i+1} = f(f_a^i)$. Eine *Kollision* für a und f ist ein Paar (i, j) mit $f_a^i = f_a^{i+j}$. Sei N_a das kleinste $i + j$, für das (i, j) eine Kollision ist.

Lemma: Für jedes a gibt es eine Kollision $(i, 2i)$ mit $2i \leq cN_a$.

Beweis: Sei (i_0, j_0) eine Kollision mit $N_a = i_0 + j_0$. Dann gilt für alle k, l:

$$f_{i_0+l} = f_{i_0+kj_0+l}.$$

Wähle $l = j_0 - (i_0 \bmod j_0)$ und $i = i_0 + l$. Dann existiert ein k mit $kj_0 = i_0 + l$, also $2(i_0 + l) = i_0 + kj_0 + l$. Nun gilt $l \leq j_0$. Also ist $i_0 + l \leq i_0 + j_0 = N_A$. □

Letzter Schritt: Woher kommen die zufälligen f? Wir probieren $x \mapsto x^2 + b \bmod n$ für $b \in \mathbb{Z}_n$.

Algorithmus: Pollardsche ρ-Methode[7]. Sei n zerlegbar.

```
1  while (true) {
2    a ∈ {1, ..., n}; // zufällig
3    b ∈ {1, ..., n−3}; // zufällig
4    f(x) = x² + b mod n;
5    u = v = a;
6    loop {
7      u = f(u);
8      v = f(f(v));
9      g = ggT(u − v, n);
10   } until (g ≠ 1);
11   if (g ≠ n) return g;
12 }
```

2.3 Das quadratische Sieb

Wir haben bisher folgende Methoden mit Laufzeiten $L_n[1, \frac{1}{x}]$ mit $x \in \{2, 3, 4\}$ kennengelernt:

- Laufzeit $L_n[1, \frac{1}{2}]$: Probedivision
- Laufzeit $L_n[1, \frac{1}{3}]$: Lehmann-Methode
- Laufzeit $L_n[1, \frac{1}{4}]$: Pollard-Strassen-Multiplikations-Methode und Pollardsche ρ-Methode

[7] Diese Methode heißt ρ-Methode, weil ρ aussieht wie ein Lasso!

Das quadratische Sieb ist die erste subexponentielle Methode (unter gewissen Annahmen), d.h. mit Laufzeit

$$L_n\big[\frac{1}{2}, 1 + o(1)\big] = e^{\sqrt{\ln n \cdot \ln\ln n}}.$$

Lemma: Sei $n > 2$ ungerade. Dann ist n zerlegbar genau dann, wenn es $x, y \in \mathbb{Z}_n$ gibt mit $x^2 \equiv y^2 \pmod{n}$, aber $x \not\equiv \pm y \pmod{n}$. Die Zahl $\mathrm{ggT}(n, |x - y|)$ ist echter Teiler von n.

Wir definieren jetzt quadratische (Halb)Kandidaten:

Definitionen:

- Ein *quadratischer Kandidat* ist ein Paar (x, y) mit $x^2 \equiv y^2 \pmod{n}$.
- Ein *quadratischer Halbkandidat* ist ein Paar (x, a) mit $x^2 \equiv a \pmod{n}$.

2.3.1 Idee des quadratischen Siebs

Versuche, nichttriviale Lösungen von $x^2 \equiv y^2 \pmod{n}$ zu bestimmen:

1. Produziere Halbkandidaten und wähle dann eine geeignete Teilnenge (x_0, a_0), (x_1, a_1), $\ldots$, (x_{r-1}, a_{r-1}); multipliziere diese, um Kandidaten zu bekommen:

$$(x_0 \cdot \ldots \cdot x_{r-1})^2 \equiv \underbrace{a_0 \cdot \ldots \cdot a_{r-1}}_{\text{Quadratzahl in } \mathbb{Z}} \pmod{n}$$

2. Um die richtige Auswahl zu treffen, zerlege die a_i in Primfaktoren – um dann eine Quadratzahl zu finden, stelle ein lineares Gleichungssystem über die vorkommenden Primfaktoren auf, so dass jeder Primfaktor nur eine gerade Anzahl mal auftritt!

Definition: Sei eine *Faktorbasis* $F = \{p_0, \ldots, p_{k-1}\}$ eine endliche Menge von Primzahlen. Eine Zahl a heiße *F-glatt*, wenn alle Primfaktoren zu F gehören. Sei weiter

$$\langle a \rangle_F = (e_0, \ldots, e_{k-1}) \quad \text{mit} \quad a = \prod_{j=0}^{k} p_j^{e_j}.$$

Lemma: Sei F eine Faktorbasis und seien $a_0, \ldots, a_{r-1}$ alle F-glatt. Sei $0 \leq i_0 < \ldots < i_{s-1} < r$. Dann ist $a_{i_0} \cdot \ldots \cdot a_{i_{s-1}}$ eine Quadratzahl genau dann, wenn

$$\sum_{j=0}^{s-1} \left\langle a_{i_j} \right\rangle_F^{\mathsf{T}} \equiv \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \pmod 2.$$

Beweis: Eine Zahl $p = a_{i_0} \cdot \ldots \cdot a_{i_{s-1}}$ ist eine Quadratzahl genau dann, wenn in der Primfaktorzerlegung von p jede Primzahl geradzahligen Exponenten hat. Dies ist genau dann der Fall, wenn in dem Vektor $\langle a_{i_0} \rangle^{\mathsf{T}} + \ldots + \langle a_{i_{s-1}} \rangle^{\mathsf{T}}$ nur geradzahlige Elemente hat, was äquivalent dazu ist, dass die Summe dieser Vektoren modulo zwei gleich null ist. □

Beispiel: Wir wollen $n = 1649$ faktorisieren. Es gilt $\sqrt{n} > 40$, wir berechnen also jeweils

$$\begin{aligned} 41^2 &= 1681 \equiv_n 32 = 2^5 \\ 42^2 &= 1764 \equiv_n 115 = 23 \cdot 5 \\ 43^2 &= 1849 \equiv_n 200 = 2^3 \cdot 5^2 \end{aligned}$$

Halbkandidaten sind dann $(41, 2^5)$, $(42, 5 \cdot 23)$ und $(43, 2^3 \cdot 5^2)$. Benutze als Faktorbasis[8] $F = \{2, 3, 5, 23\}$. Dann ergibt sich das folgende Gleichungssystem[9]:

$$y_0 \cdot \begin{pmatrix} 5 \\ 0 \\ 0 \\ 0 \end{pmatrix} + y_1 \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \\ 1 \end{pmatrix} + y_2 \cdot \begin{pmatrix} 3 \\ 0 \\ 2 \\ 0 \end{pmatrix} \equiv_2 \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$$

Lösung des Gleichungssystems ist $y_0 = y_2 = 1$ und $y_1 = 0$. Wir betrachten also $x^2 \equiv y^2 \pmod n$ mit $x = x_0 \cdot x_2 = 41 \cdot 43$ und $y = \sqrt{32 \cdot 200} = 80$. Dann ist $|x - y| = 1683$, womit $\mathrm{ggT}(1649, 1683) = \mathrm{ggT}(1649, 34) = 17$ ist.

2.3.2 Algorithmus des quadratischen Siebs

Grobe Skizze des **Algorithmus**': Vorbedingung sei $n > 1$ zerlegbar.

1. Schritt: Besimme eine Zahl B und setze $F = \{p \leq B \mid p \text{ Primzahl}\}$.

[8] Normalerweise würden zu F auch die Primzahlen zwischen 5 und 23 gehören, diese wurde hier aus Gründen der Übersichtlichkeit weggelassen.

[9] Hier können die Einträge in den Vektoren auch nur modulo zwei berechnet werden.

2. Schritt *(Sieben)*: Suche mindestens $\pi(B)+1$ Halbkandidaten (x,a) mit F-glattem a unter den Paaren $(w+i,(w+i)^2-n)$ mit $i \in \{0,1,\ldots,s\}$ und $w = \lceil\sqrt{n}\rceil$, wobei s eine geeignete große Schranke ist, so dass es genügend F-glatte Halbkandidaten gibt.

3. Schritt *(lineare Algebra)*: Extrahiere Halbkandidaten, die quadratische Kandidaten liefern, und zwar durch Lösen des entsprechenden linearen Gleichungssystems (in $\mathbb{Z}_2$).

4. Benutze die Kandidaten, um den Faktor zu bestimmen.

Im Folgenden wird auf einige Details der Implementierung eingegangen:

2.3.3 Implementierung des Siebens (Schritt 2)

Bemerkung: Wenn p in der Primfaktorzerlgegung von $(w+i)^2-n$ vorkommt, dann ist n quadratischer Rest modulo p. Streiche also aus F alle Primzahlen mit der Eigenschaft, dass n nicht quadratischer Rest modulo p ist.

Lemma: Sei p eine Primzahl und $X = \{a \in \mathbb{Z}_p \mid a^2 \equiv n \pmod p\}$ (beachte $|X| \leq 2$). Dann gilt: $p \mid (w+i)^2 - n$ genau dann, wenn $w+i \equiv b \pmod p$ ist für ein $b \in X$.

Beweis: $p \mid (w+i)^2 - n$ ist äquivalent zu $(w+i)^2 \equiv n \pmod p$, d.h. $(w+i) \bmod p \in X$.

Algorithmus vereinfachtes Sieb: Sei $n > 2$ und $F = \{p_0,\ldots,p_{k-1}\}$ die verwendete Faktorbasis, seien weiter $w, s \in \mathbb{N}$.

```
1  for (i ∈ {0, ..., s−1}) {
2    a[i] = (w+i)^2 − n;
3    v[i] = ∅;
4    c[i] = 1;
5  }
6  for (j ∈ {0, ..., k−1}) {
7    X = { a ∈ Z_p[j] | a^2 mod p[j] ==n mod p[j] };
8    for (b ∈ X) {
9      if (w mod p[j] ≤ b)
10       i = b − (w mod p[j]);
11     else
12       i = p[j] + b − (w mod p[j]);
13     k = max { k | a[i] mod p[j]^k ==0 };
14     v[i] = v[i] ∪ (j, k);
15     c[i] = c[i]·p[j]^k;
```

```
16        i = i + p;
17      }
18    }
```

Beispiel: Für $n = 1649$, $w = 41$ und $s = 8$ sowie $F = \{2, 3, 5\}$ (mit $p_0 = 2$, $p_1 = 3$ und $p_2 = 5$) ergibt sich:

1. Schritt (p_0): $X = \{a \in \mathbb{Z}_2 \mid a^2 \equiv 1649 \pmod 2\} = \{1\}$, also $i = 0, 2, 4, 6, \ldots$
2. Schritt (p_1): $X = \{a \in \mathbb{Z}_3 \mid a^2 \equiv 1649 \pmod 3\} = \emptyset$
3. Schritt (p_2): $X = \{a \in \mathbb{Z}_5 \mid a^2 \equiv 1649 \pmod 5\} = \{2, 3\}$, also zunächst $i = 1, 6, 11, 16, \ldots$ und dann $i = 2, 7, 12, 17$

Die im Algorithmus verwendeten Felder sind dann:

i	0	1	2	3	4	5
w	41	42	43	44	45	46
$a[i]$	32	115	200	287	376	467
$c[i]$	32	5	200	1	8	1
$v[i]$	$\{(0,5)\}$	$\{(2,1)\}$	$\{(0,3),(2,2)\}$	$\emptyset$	$\{(0,3)\}$	$\emptyset$

Nun kann die Liste S aller Halbkandidaten (x, a) mit $x \in [w, w+s)$ zusammen mit den Vektoren $\langle a \rangle_B$ in komprimierter Schreibweise auf folgende Weise generiert werden:

```
1  S = ∅;
2  for (i ∈ {0, ..., s−1})
3    if (a[i] == c[i])
4      S = S ∪ ((w+i, a[i]), v[i]);
```

Bemerkungen:

1. Für das Bestimmen von X gibt es spezielle Polynomzeitverfahren (siehe Übung).
2. Es wäre besser, wenn man auch die höheren Primzahlpotenzen durch Sieben (ohne Division) erledigen könnte. Dies ist machbar, aber nur mittels komplexer Algorithmen. Als Alternative betrachten wir nur solche Zahlen, in denen jede Primzahl mit Exponent ≤ 1 vorkommt.
3. Um die Produktbildung bei den $c[i]$ (Zeile 15 oben) zu vermeiden, rechnet man einfach mit gerundeten Logarithmen und addiert diese.
4. Um in der zweiten Komponente der Halbkandidaten kleine Zahlen zu haben, benutzt man nicht nur $(w+i)$, sondern auch $(w-i)$ und ergänzt dann die Faktorbasis um $\{-1\}$.

2.3.4 Schnelle Matrixmethoden (Schritt 3)

Problem: Löse ein lineares Gleichungssystem über $\mathbb{Z}_2$ mit mehr als K Variablen und K Gleichungen, allerdings mir „wenigen“ von Null verschiedenen Koeffizienten – d.h. eine „schwach besetzte Matrix“.

Ansatz: Hierfür wäre Gauß-Elimination möglich, sie hätte aber die pessimale Laufzeit $\Omega(K^3)$, da sie die dünne Besetzung nicht ausnutzt. Bessere Möglichkeiten sind die Conjugate Gradient Method, die Lanczos-Methode oder die Wiedermann-Methode.

Die ersten beiden stammen aus der numerischen Mathematik, während die dritte Methode von spezieller Natur ist. Für die zweite und dritte Methode lässt sich eine gute Laufzeit beweisen. Die Wiedemann-Methode hat die Laufzeit $\mathcal{O}(K \cdot E)$, wobei E die Anzahl der Matrixeinträge ist, die nicht Null sind.

Weitere Möglichkeiten sind spezielle Hardware (diese arbeitet dann massiv parallel), Sortierverfahren (z. B. „Schimmler Sorting“) und Routingalgorithmen!

2.3.5 Laufzeitanalye für Siebprozess und Optimierung von B

Je kleiner B, um so schneller kann gesiebt werden, aber umso mehr Zahlen müssen gesiebt werden.

Annahme: der Anteil der B-glatten Zahlen an $\{0, \ldots, \sqrt{n}\}$ ist derselbe wie der Anteil der B-glatten Zahlen der Form $(w+i)^2 - n$, für $w = \lceil \sqrt{n} \rceil$.

Es gilt $(w+i)^2 - n \approx (\sqrt{n}+i)^2 - n = n + 2\sqrt{n}i + i^2 - n = 2\sqrt{n}i + i^2$, deshalb macht die Annahme evtl. Sinn.

Wir studieren jetzt die Dichte B-glatter Zahlen, sei dazu (analog zu $\pi(x)$):

$$\psi(x, B) := |\{y \leq x \mid y \text{ ist } B\text{-glatt}\}| .$$

Satz (Pomerance): Sei $\varepsilon > 0$. Es gibt eine Funktion $f(x, u)$, so dass $\frac{f(x,u)}{u}$ für $x \to \infty$ gleichmäßig gegen 0 geht, und so dass für alle $x \geq 10$ und $u \leq (\ln x)^{1-\varepsilon}$ gilt:

$$\psi(x, x^{\frac{1}{u}}) = x u^{-u+f(x,u)}.$$

Als Interpretation der Aussage des Satzes ergibt sich: Eine Zahl x ist $x^{\frac{1}{u}}$-glatt mit Wahrscheinlichkeit

$$\frac{\psi(x, x^{\frac{1}{u}})}{x} \approx u^{-u}.$$

Vereinfachung: Wir nehmen $f = 0$ an.

Wiederholung: Werte von $(w+i)^2 - n$ liegen größenordnungsmäßig um $\sqrt{n} = n^{\frac{1}{2}}$. Matchen von $\psi(n^{\frac{1}{2}}, B)$ mit $\psi(x, x^{\frac{1}{u}})$ liefert dann: $B = (n^{\frac{1}{2}})^{\frac{1}{u}} = n^{\frac{1}{2u}}$. Es gilt also $\frac{\ln B}{\ln u} = \frac{1}{2u}$, also $u = \frac{1}{2}\frac{\ln n}{\ln B}$.

Der Aufwand zum Sieben ist ungefähr die Anzahl der zu siebenden Zahlen $x \ln\ln B$ (ähnlich zum Sieb des Eratosthenes). Die Größe der Faktorbasis ist ungefähr $\frac{1}{2}\pi(B) \approx \frac{B}{2\ln B}$ (Primzahlsatz).

Wenn die Wahrscheinlichkeit dafür, dass eine Zahl B-glatt ist, bei u^{-u} liegt, müssen wir u^u Zahlen testen, um eine zu finden; also müssen wir ungefähr $(K+1)u^u$ viele testen, um mehr als K zu finden. Dann ist die Laufzeit ungefähr $T(B) = u^u K \ln\ln B$.

Durch das Setzen von $S(B) := u\ln u + \ln B$ erhalten wir dann $\ln T(B) \sim S(B)$, denn $\ln T(B) = u\ln u + \ln K + \ln\ln\ln B$, wobei $K \approx \frac{B}{2\ln B}$.

Ableiten liefert (beachte $u = \frac{\ln n}{2\ln B}$):

$$\frac{dS}{dB} = \frac{-\ln n}{2B\ln^2 B}(\ln\ln n - \ln\ln B - \ln 2 + 1) + \frac{1}{B}.$$

Weiter gibt es Konstanten $c, c' > 0$, so dass für die Nullstelle von $\frac{dS}{dB}$ gilt:

$$c\sqrt{\ln n} \le \ln B \le c'\sqrt{\ln n \cdot \ln\ln n} = c'\sqrt{\ln n}\sqrt{\ln\ln n}.$$

Es ergibt sich $\ln B \sim \frac{1}{2}\sqrt{\ln n \cdot \ln\ln n}$ und damit eine asymptotische Laufzeit von

$$e^{\sqrt{\ln n \cdot \ln\ln n}} \quad (= L_n[0.5, 1]).$$

Man sollte also B so wählen, dass gilt:

$$\ln B = \frac{1}{2}\sqrt{\ln n \cdot \ln\ln n}$$

Für die obige Wahl ergibt sich ebenfalls die asymptotische Laufzeit $e^{\sqrt{\ln n \cdot \ln\ln n}}$ für das Gleichungslösen.

Satz: Unter geeigneten Annahmen hat das quadratische Sieb eine Laufzeit von $L_n[\frac{1}{2}, 1 + o(1)]$.

Bemerkung: Je gösser $(w+i)^2 - n$ wird, desto kleiner ist die W'keit, dass die entstehende Zahl glatt ist. Deshalb benutzt man nicht nur $f(x) = (w+x)^2 - n$ als Polynom, um potenzielle Halbkandidaten zu finden, sondern auch andere quadratische Polynome. Dieses Verfahren nennen wir das „Multiple Polynomials Quadratic Sieve" (MPQS).

Bemerkung: Eine große Zahl, die mit MPQS faktorisiert wurde, ist RSA-129[10]:

$$\begin{aligned}
\text{RSA-129} = \; & 114\,381\,625\,757\,888\,867\,669\,235\,779\,976\,146\,612\,010\,218\,296 \\
& 721\,242\,362\,562\,561\,842\,935\,706\,935\,245\,733\,897\,830\,597 \\
& 123\,563\,958\,705\,058\,989\,075\,147\,599\,290\,026\,879\,543\,541 \\
= \; & 3\,490\,529\,510\,847\,650\,949\,147\,849\,619\,903\,898 \\
& 133\,417\,764\,638\,493\,387\,843\,990\,820\,577 \\
* \; & 32\,769\,132\,993\,266\,709\,549\,961\,988\,190\,834\,461 \\
& 413\,177\,642\,967\,992\,942\,539\,798\,288\,533
\end{aligned}$$

Sie wurde im Jahre 1994 mit 600 Rechnern bei einer Rechenzeit von acht Monaten faktorisert, als Preisgeld waren 100$ ausgesetzt.

2.4 Das Zahlkörpersieb

Beim quadratischen Sieb habe wir folgende Zahlen betrachtet:

$$\begin{aligned}
x_0^2 &\equiv a_0 \\
&\vdots \\
x_{r-1}^2 &\equiv a_{r-1}
\end{aligned}$$

Bei dem Zahlkörpersieb wird die Methode für die linken Seite (x_i^2) auch auf die rechte Seite (a_i) übertragen.

Wesentliche **Idee:** Wir sammeln Werte $\theta_0, \ldots, \theta_{r-1}$ in einer algebraischen Erweiterung $\mathbb{Z}[\alpha]$ von $\mathbb{Z}$. Zusätzlich haben wir einen Ring-Homomorphismus $\varphi\colon \mathbb{Z}[\alpha] \to \mathbb{Z}_n$. Eine Auswahl der θ_i soll folgende Eigenschaft haben:

- Das Produkt $\theta_{i_0} \cdot \ldots \cdot \theta_{i_{s-1}}$ soll eine Quadratzahl sein, etwa $\gamma^2 \in \mathbb{Z}[\alpha]$.
- Es gelte $\varphi(\theta_{i_0}) \cdots \varphi(\theta_{i_{s-1}}) \equiv v^2 \pmod{n}$ für ein $v \in \mathbb{Z}_n$.

Dann gilt

$$\varphi(\gamma)^2 = \varphi(\gamma^2) = \varphi(\theta_{i_0} \cdots \theta_{i_{s-1}}) = \varphi(\theta_{i_0}) \cdots \varphi(\theta_{i_{s-1}}) \equiv v^2 \pmod{n}$$

Ein Kanditat für einen Faktor von n ist also $\mathrm{ggT}(\varphi(\gamma) - v, n)$. **Idee:** Siebe, um θ_i zu finden, und löse dann Gleichungen, um die richtigen θ_{i_j} herauszusuchen.

[10] siehe `http://en.wikipedia.org/wiki/RSA-129`
und `http://www.willamette.edu/~mjaneba/rsa129.html`

2.4.1 Algebraische Grundlagen

Betrachte wieder Ringe, wie immer kommutativ mit Eins.

Definition: Sei R ein Teilring von S, $\alpha \in S$. Dann ist $R[\alpha]$ *(R adjungiert α)* der kleinste Teilring von S, der $R \cup \{\alpha\}$ enthält. Es gilt

$$R[\alpha] = \bigcap \{T \leq S \mid R \cup \{\alpha\} \subseteq T\} = \left\{ \sum_{i<d} r_i \alpha^i \;\middle|\; d \in \mathbb{N}, r_i \in R \right\}$$

Definitionen:

- Sei K ein Körper und L eine *Erweiterung*, d.h. $K \leq L$. Schreibe dann $L : K$.
- Für $L : K$ ist L einen K-Vektorraum, insbesondere ist dann $\dim_K L$ definiert, diese nennt man den *Grad der Körpererweiterung*, schreibe $[L : K]$.
- Eine *endliche Körpererweiterung* ist eine solche, die bei der der Grad $[L : K]$ endlich ist.

Definition:

- Seien $L : K$ Körper, $A \subseteq L$. Dann ist $R(A)$ *(R adjungiert A)* der kleinste Teilkörper von L, der $K \cup A$ enthält.
- Ist $L = K(\{\alpha\}) = K(\alpha)$, so nennt man α ein *primitives Element* und L eine *einfache Körpererweiterung*.
- Ein Element α heißt *algebraisches Element* (der Körpererweiterung $L : K$), wenn $f(\alpha) = 0$ für ein $f \in K[x]$ gilt. Andere Elemente heißen *transzendente Elemente*.

Definition: Ein *Zahlkörper* K ist ein Körper mit $\mathbb{C} : K : \mathbb{Q}$ mit $[K : \mathbb{Q}] < \infty$. Ein *quadratische Zahlkörper* ist ein solcher, der durch Adjunktion einer quadratischen Wurzel entsteht; ein *Kreisteilungskörper* entsteht durch Adjunktion einer Einheitswurzel.

Beispiel: $\mathbb{Q}[i] = \mathbb{Q}(i) = \mathbb{Q}/(x^2 + 1)$

Satz: Jeder Zahlkörper K ist eine einfache Erweiterung von $\mathbb{Q}$.

Satz: Ist α algebraisch über K, so gibt es genau ein irreduzibles normiertes Polynom $m_\alpha \in K[x]$ (das *Minimalpolynom*), für das $m_\alpha(\alpha) = 0$ gilt.

Bemerkungen:

1. Für jedes Polynom $g \in K[x]$ ist $g(\alpha) = 0$ genau dann, wenn $m_\alpha \mid g$ gilt.
2. Der Körper $K(\alpha) = K[\alpha]$ ist isomorph zu $K[x]/(m_\alpha)$.
3. Es gilt $[K(\alpha) : K] = \text{grad}(m_\alpha)$.

Beispiel: i ist algebraisch über $\mathbb{Q}$, dann ist $m_i = x^2 + 1$, es gilt $\mathbb{Q}(i) = \{q + ri \mid q, r \in \mathbb{Q}\}$ und damit ist $[\mathbb{Q}(i) : \mathbb{Q}] = 2$, eine Basis von $\mathbb{Q}(i)$ (als Vektorraum über K) ist $\{1, i\}$.

Definition:

- Ein *K-Automorphismus* ist ein Isomorphismus $K \to K$, sei $\text{Aut}(K)$ die Menge der K-Automorphismen.
- Die *Galois-Gruppe* $\mathfrak{G}(L : K)$ ist definiert als

$$\mathfrak{G}(L : K) = \{\sigma \colon L \to L \text{ Automorphismus} \mid \sigma(k) = k \,\forall\, k \in K\}$$

- Der *Fixkörper* $\mathfrak{F}(L, U) \leq L$ für eine Untergruppe $U \leq \text{Aut}(L)$ ist definiert als

$$\mathfrak{F}(L, U) = \{l \in L \mid \sigma(l) = l \,\forall\, \sigma \in U\}$$

Beispiel: $\mathfrak{G}(\mathbb{Q}(i) : \mathbb{Q}) = \{\sigma_0, \sigma_1\}$ mit $\sigma_0 = \text{id}$ und σ_1 Komplexkonjugation.

Definition: Sei $L : K$ eine Körpererweiterung, diese heißt *Galois-Erweiterung*, falls gilt:

$$\mathfrak{F}(L, \mathfrak{G}(L : K)) = K$$

Satz: Ist K ein Zahlkörper mit primitivem Element α, so hat m_α genau $\text{grad}(m_\alpha)$ verschiedene Nullstellen, etwa $\alpha = \alpha_0, \ldots, \alpha_{r-1}$. Diese werden als Konjugierte bezeichnet.

1. $\mathfrak{G}(K : \mathbb{Q})$ hat genau r Elemente, $\mathfrak{G}(K : \mathbb{Q}) = \{\sigma_0, \ldots, \sigma_{r-1}\}$ mit σ_i bestimmt durch $\sigma_i(\alpha) = \alpha_i$ (d.h. insbesondere $\sigma_0 = \text{id}$).
2. $K : \mathbb{Q}$ ist eine Galois-Erweiterung.

Definition: Sei $R[x_0, \ldots, x_{r-1}]$ ein Polynomring in r kommutativen Variablen. Sei S_r die symmetrische Gruppe auf $\{0, \ldots, r-1\}$, und sei $\pi \in S_r$. Das Polynom $f(x_0, \ldots, x_{r-1})$ heißt *symmetrisch*, falls $f(x_0, \ldots, x_{r-1}) = f(x_{\pi(0)}, \ldots, x_{\pi(r-1)})$ ist.

Beispiel: Elementare symmetrische Polynome sind jeweils die Summen aller Produkte aus 0, 1, ..., r Variablen:

$$\begin{gathered} 1 \\ x_0 + \ldots + x_{r-1} \\ x_0x_1 + x_0x_2 + \ldots + x_ix_j + \ldots + x_{r-2}x_{r-1} \\ \vdots \\ x_0x_1 \cdots x_{r-1} \end{gathered}$$

Lemma: Sei K ein Zahlkörper vom Grad r, $s \in \mathbb{Q}[x_0, \ldots, x_{r-1}]$ ein symmetrisches Polynom und $\mathfrak{G}(K : \mathbb{Q}) = \{\sigma_0, \ldots, \sigma_{r-1}\}$. Wir setzen $f_s(x) = s(\sigma_0(x), \ldots, \sigma_{r-1}(x))$. Dann gilt $f_s(a) \in \mathbb{Q}$ für alle $a \in K$.

Definitionen:

- Für $s = x_0 + \ldots + x_{r-1}$ ist $f_s(a) = \sigma_0(a) + \ldots + \sigma_{r-1}(a)$, dies wird als *Spur von* a, in Zeichen $T(a)$, bezeichnet.
- Für $s = x_0 \cdot \ldots \cdot x_{r-1}$ ist $f_s(a) = \sigma_0(a) \cdot \ldots \cdot \sigma_{r-1}(a)$, dies wird als *Norm von* a, in Zeichen $N(a)$, bezeichnet.

Lemma: Sei K Zahlkörper vom Grad r.

1. $N(aa') = N(a)N(a') \in \mathbb{Q}$
2. $N(ba) = b^r N(a)$ für alle $b \in \mathbb{Q}$, insbesondere $N(b) = b^r$.
3. $T(a + a') = T(a) + T(a')$
4. $T(b + a) = r \cdot b + T(a)$ für alle $b \in \mathbb{Q}$, insbesondere $T(b) = r \cdot b$.

Nun können wir von Zahlkörpern zu Zahlringen übergehen.

Definition: Ein Element α heißt *ganz-algebraisch*, falls $f(\alpha) = 0$ für ein normiertes $f \in \mathbb{Z}[x]$ ist. Dann sei

$$\mathbb{A} = \{\alpha \mid \alpha \text{ ganz-algebraisch}\}$$

Ein *Zahlring* ist nicht $\mathbb{Z}[\alpha]$ mit α ganz-algebraisch, sondern $K \cap \mathbb{A}$ mit einem Zahlkörper K.

Satz: Sei α ganz-algebraisch. Dann ist das Minimalpolynom m_α über $\mathbb{Q}$ ein Element aus $\mathbb{Z}[x]$, und außerdem gilt $N(\alpha), T(\alpha) \in \mathbb{Z}$.

Beispiel: Es gilt $N(a+bi) = (a+bi)(a-bi) = a^2 + b^2$, und $T(a+bi) = (a+bi) + (a-bi) = 2a$.

Beweis: Es gilt $m_\alpha \mid f$ mit $f \in \mathbb{Z}[x]$ normiert und $f(\alpha) = 0$.

Annahme: $f = gh$ mit $g, h \in \mathbb{Q}[x]$ und g normiert. Dann ist h normiert, da f normiert ist. Seien $r, s \in \mathbb{N}_0$ minimal mit $rg, sh \in \mathbb{Z}[x]$. Dann haben die Koeffizienten von rg den größten gemeinsamen Teiler Eins, ebenso für sh, da g und h normiert sind.

Wir zeigen nun noch $r = s = 1$: Angenommen, $rs > 1$, dann sei p Primzahl mit $p \mid rs$. Es gilt $rsf = rg \cdot hs \in Z[x]$. Nun gilt $0 = rsf \bmod p = (rg \bmod p)(hs \bmod p)$, aber $rg \bmod p \neq 0$ und $hs \bmod p \neq 0$, Widerspruch! □

Notation: Mit $\mathbb{Z}\langle\alpha\rangle$ bezeichnen wir den kleinsten Zahlring, der α und $\mathbb{Z}$ umfasst:

$$\mathbb{Z}\langle\alpha\rangle = \mathbb{Q}(\alpha) \cap \mathbb{A}$$

Bemerkung: $\mathbb{Z}[\alpha]$ ist gut für gewisse Teile des Algorithmus', verhält sich aber algebraisch schlecht. $\mathbb{Z}\langle\alpha\rangle$ dagegen hat gute Eigenschaften (Dedekind-Ringe: jedes Ideal lässt sich eindeutig als Produkt von Primidealen schreiben).

2.4.2 Idee des Algorithmus'

Wähle α, d und m so, dass gilt:

- α ist die Wurzel eines normierten irreduziblen Polynoms f über $\mathbb{Z}$,
- der Grad des Polynoms ist d,
- es gilt $m \in \mathbb{Z}$ mit $f(m) \bmod n = 0$.

Wie wählen wir diese Zahlen? **Ansatz**: Setze m und $c_i < m$, so dass gilt:

$$m = \left\lfloor n^{\frac{1}{d}} \right\rfloor \quad \text{und} \quad n = m^d + c_{d-1}m^{d-1} + \ldots + c_0.$$

Setzte dann $f(x) = x^d + c_{d-1}x^{d-1} + \ldots + c_0$ – dann gilt offensichtlich $f(m) = n \equiv 0 \pmod{n}$.

Angenommen, f ist nicht irreduzibel. Dann finden wir g und h mit Grad höchstens Eins und $gh = f$. Dann gilt aber $n = f(m) = g(m)h(m)$. Man kann zeigen, dass dies eine nicht-triviale Zerlegung von n ist.

Bemerkung: Betrachte nun $\mathbb{Z}[x]/(f) \cong \mathbb{Z}[\alpha]$ für eine Wurzel α von f. Definiere nun $\varphi_0 \colon \mathbb{Z}[\alpha] \to \mathbb{Z}$ durch Ersetzen von α durch m, d.h.

$$\varphi_0\Big(\sum_{i<d} d_i \alpha^i\Big) := \sum_{i<d} d_i m^i.$$

Dann definieren wir

$$\varphi \colon \mathbb{Z}[\alpha] \to \mathbb{Z},\ \beta \mapsto \varphi_0(\beta) \mod n.$$

Die wichtigste **Idee**: Suche θ_i, so dass $\prod \theta_i$ ein Quadrat in $\mathbb{Z}[\alpha]$ ist und $\prod \varphi_0(\theta_i)$ ein Quadrat in $\mathbb{Z}$ ist.

Suche die θ_i nur unter „einfachen“ Elementen von $\mathbb{Z}[\alpha]$, nämlich nur Elemente der Form $(a - b\alpha)$ mit $a \top b$. Dann bezeichnet $\theta(a, b) = a - b\alpha$ ein solches Element. Es gilt dann:

$$\varphi_0(\theta(a, b)) = \varphi_0(a - b\alpha) = a - bm =: G(a, b).$$

Setze $P = \{(a, b) \mid a \top b\}$. Finde $C \subseteq P$ endlich mit

$$\theta_C := \prod_{(a,b)\in C} \theta(a, b) = \gamma^2 \text{ für } \gamma \in \mathbb{Z}[\alpha]$$
$$m_C := \prod_{(a,b)\in C} G(a, b) = v^2 \text{ für } v \in \mathbb{Z}.$$

Dann ist $\mathrm{ggT}(u - v, n)$ ein Kandidat für einen Faktor von n, wobei $u = \varphi(\gamma)$ ist.

Prinzipielle Vorgehensweise für den Rest:

1. Definiere Glattheit bezüglich der ersten und zweiten Bedingung für Paare (a, b); und für jedes glatte Paar definiere „charakteristische Vektoren“ $v_\theta(a, b)$ und $v_m(a, b)$ über $\mathbb{Z}_2$ derart, dass gilt:
   (a) θ_C ist Quadrat in $\mathbb{Z}[\alpha]$ genau dann, wenn $\sum_{(a,b)\in C} v_\theta(a, b) = 0$ ist – dies ist sehr kompliziert, aber heuristisch machbar, und
   (b) m_C ist Quadrat in $\mathbb{Z}$ genau dann, wenn $\sum_{(a,b)\in C} v_m(a, b) = 0$ ist.
2. Zur Bestimmung der glatten Paare sowie v_θ und v_m benutze die Siebmethode.

3. Außerdem benötigen wir Algorithmen zum Wurzelziehen.

Zu *m-Glattheit* und v_m: Wir fordern, $G(a,b)$ sei B-glatt für ein geeignetes B (wie beim quadratischen Sieb!) und setzen $v_m(a,b) = \langle G(a,b)\rangle_{\{-1,2,3,5,\ldots,B\}}$. Wurzelziehen ist dann kein Problem, und Sieben können wir auch schon!

Erste **Idee** für θ-Glattheit und v_θ: Definiere B-glatt über Primzahlen in $\mathbb{Z}[\alpha]$. Das klappt aber nicht, da $\mathbb{Z}[\alpha]$ im Allgemeinen kein ZPE-Ring[11] ist.

Nun wollen wir in drei Stufen zeigen, dass in 1. (a) die Richtung von links nach rechts gilt und die Rückrichtung mit hoher Wahrscheinlichkeit gilt.

Erste Stufe

Lemma: Wenn β eine Quadratzahl in $\mathbb{Z}[\alpha]$ ist, so ist $N(\beta)$ eine Quadratzahl in $\mathbb{Z}$.

Beweis: Sei $\beta = \gamma^2$. Dann ist $N(\beta) = N(\gamma^2) = N(\gamma)^2 \in \mathbb{Z}$. □

Zur θ-Glattheit: (a,b) ist θ-glatt, wenn $N(\theta(a,b))$ im üblichen Sinne B-glatt ist: $v_\theta(a,b) = \langle N(\theta(a,b))\rangle_{\{-1,2,3,5,\ldots,B\}}$. Aber: die Rückrichtung ist zu häufig falsch!

Zweite Stufe

Bemerkung: Es gilt

$$\begin{aligned} N(\theta(a,b)) &= N(a-b\alpha) = \sigma_0(a-b\alpha)\sigma_1(a-b\alpha)\ldots\sigma_{d-1}(a-b\alpha) \\ &= (a-b\alpha_0)(a-b\alpha_1)\ldots(a-b\alpha_{d-1}) \\ &= b^d\left(\frac{a}{b}-\alpha_0\right)\left(\frac{a}{b}-\alpha_1\right)\ldots\left(\frac{a}{b}-\alpha_{d-1}\right) \\ &= b^d f\left(\frac{a}{b}\right) = F(a,b) \end{aligned}$$

mit $F(x,y) = x^d + c_{d-1}x^{d-1}y + \ldots + c_0y^d$. Damit haben wir die Norm von $\theta(a,b)$ ausgedrückt, ohne α zu verwenden.

Lemma: Für eine Primzahl p und $a \top b$ gilt $F(a,b) \equiv 0 \pmod p$ genau dann, wenn es ein $r < p$ gibt mit $f(r) \equiv 0 \pmod p$ und $a \equiv br \pmod p$.

Beweis:

„⇒“ Es gilt also $F(a,b) \equiv 0 \pmod p$. Dann ist

$$F(a,b) = b^d f(\frac{a}{b}) \equiv 0 \pmod p.$$

[11] ZPE: **Z**erlegung in **P**rimelemente ist **e**indeutig

– Falls $b \not\equiv 0 \pmod{p}$, so gilt $f(\frac{a}{b}) = 0$ in $\mathbb{Z}_p$, also gilt die Bedingung mit $r = \frac{a}{b} \bmod p$.
– Falls $b \equiv 0 \pmod{p}$ ist, so ist $F(a,b) = a^d \equiv 0$ in $\mathbb{Z}_p$. Also $p \mid a, b$. Widerspruch zu $a \top b$.

„⇐“ Einfaches Nachrechnen... □

Definiere nun

$$R(p) := \{r < p \mid f(r) \equiv 0 \pmod{p}\}.$$

Nun hat $v_\theta(a,b)$ für jedes $p \leq B$ und $r \in R(p)$ einen Eintrag $v_\theta^{r,p}(a,b)$ in $\mathbb{Z}_2$ derart, dass gilt:

- Falls $a \equiv br \pmod{p}$ ist, so sei $v_\theta^{r,p}(a,b)$ gleich dem Exponenten von p in der Primfaktorzerlegung von $F(a,b)$.
- Falls $a \not\equiv br \pmod{p}$ ist, so sei $v_\theta^{r,p}(a,b)$ gleich 0.

Lemma: Sei $C \subseteq P$ endlich derart, dass (a,b) (wie oben) B-glatt ist für alle $(a,b) \in C$ und dass $\theta_C = \gamma^2$ ist für $\gamma \in \mathbb{Z}\langle\alpha\rangle$. Dann gilt

$$\sum_{(a,b)\in C} v_\theta(a,b) = 0.$$

Dritte Stufe

Problem: Eine Zahl aus $\mathbb{Z}[\alpha]$, die eine Quadratzahl in $\mathbb{Z}\langle\alpha\rangle$ ist, braucht keine Quadratzahl in $\mathbb{Z}[\alpha]$ zu sein.

Lemma: Sei f normiert und irreduzibel in $\mathbb{Z}[x]$ mit Nullstelle α. Für jedes $\beta \in \mathbb{Z}\langle\alpha\rangle$ gilt $f'(\alpha)\beta \in \mathbb{Z}[\alpha]$.

Also: Falls $\theta_C = \gamma^2$ für $\gamma \in \mathbb{Z}\langle\alpha\rangle$ ist, so ist $(f'(\alpha))^2\theta_C = (f'(\alpha)\gamma)^2$ mit $f'(\alpha)\gamma \in \mathbb{Z}[\alpha]$.

Bemerkung: Es gibt noch drei weitere wichtige Probleme, über die wir uns hier nicht im Detail unterhalten werden – diese sind ringtheoretischer Natur.

Lemma: Seien f, α wie oben. Sei q eine ungerade Primzahl mit $f(s) \equiv 0 \pmod{q}$ und $f'(s) \not\equiv 0 \pmod{q}$ für ein $s \in \mathbb{Z}$. Falls $q \nmid a - bs$ und $(f'(\alpha))^2\theta_C$ eine Quadratzahl in $\mathbb{Z}[\alpha]$ ist, so ist das Legendre-Symbol $\left(\frac{a-bs}{q}\right) = 1$.

Beweis: Übung.

Bemerkung: Falls für genügend Paare (q, s) das obige Legendre-Symbol 1 ist, so ist die Rückrichtung („$\Leftarrow$“) sehr wahrscheinlich.

Dritter Ansatz für $v_\theta(a, b)$: Wähle zusätzliche Primzahlen $q_j > B$ und passende s_j, so dass $f(s_j) \equiv 0 \pmod{q}$ und $f'(s_j) \not\equiv 0 \pmod{q}$ ist. Füge zu v_θ neue Komponenten $v_\theta^j(a, b)$ hinzu, die gegeben sind durch[12]

$$\frac{1}{2}\left(1 - \left(\frac{a - bs_j}{q_j}\right)\right)$$

Heuristische Überlegungen: Wenn genügend viele j betrachtet werden (mehr als $3 \ln n$), dann „folgt“ aus folgender Bedingung, dass $f'(\alpha)^2\theta_C$ eine Quadratzahl in $\mathbb{Z}[x]$ ist:

$$\sum_{(a,b)\in C} v_\theta(a, b) = 0$$

2.4.3 Algorithmus des Zahlkörpersiebs

Vorüberlegung sei, dass n ungerade und zerlegbar sowie keine perfekte Potenz ist.

Algorithmus:

1. Initialisierung:
   (a) Setze folgende Zahlen geschickt:
   $$d = \left\lfloor \left(\frac{3 \cdot \ln n}{\ln \ln n}\right)^{\frac{1}{3}} \right\rfloor \quad \text{und} \quad B = \left\lfloor L_n\left[\frac{1}{3}, \left(\frac{8}{9}\right)^{\frac{1}{3}}\right] \right\rfloor$$
   (b) Wähle m, f, G, F.
   (c) Falls $f = g \cdot h$ ist (Überprüfung per Computeralgebra), bestimme eine passende nichttriviale Zerlegung von n mittels $n = g(m) \cdot h(m)$.
   (d) Bestimme $R(p)$ für $p \leq B$ und $B' = \sum_{p \leq B} |R(p)|$.
   (e) Setze $k = \lfloor 3 \ln n \rfloor$.
   (f) Bestimme die ersten k Primzahlen $q_j > B$ (d.h. $(q_0, \ldots, q_{k-1})$), für die es s_j mit $f(s_j) \equiv 0 \pmod{q)_j}$ ist und $f'(s_j) \not\equiv 0 \pmod{q)_j}$ gibt.
   (g) Setze $V = 1 + \pi(B) + B' + k$ und $M = B$.
2. Sieben:

[12] Diese Formel transformiert $\{1, -1\}$ auf $\{0, 1\}$!

(a) Bestimme durch Sieben eine Menge P mit mehr als V Elementen (a, b), die folgende Eigenschaften haben:

$$0 \leq |a|, |b| \leq M \quad \text{und} \quad F(a,b) \cdot G(a,b) \text{ } B\text{-glatt}$$

(b) Bestimme gleichzeitig für jedes $(a, b) \in C$ den Vektor $v(a, b) = (v_m(a, b), v_\theta(a, b))$.

3. Gleichungslösen:

(a) Bestimme $C \subseteq P$ mit $C \neq \emptyset$, so dass

$$\sum_{(a,b)\in C} v(a,b) = 0$$

4. Wurzelziehen:

(a) Bestimme die Wurzel v aus m_C modulo n mit Hilfe der v_m.

(b) Bestimme die Wurzel γ aus $f'(\alpha)^2\theta_C$ modulo n mit Hilfe von Computeralgebra.

(c) Setze $u = \varphi(\gamma) \bmod n$.

5. Faktorisierung:

(a) Gib $\mathrm{ggT}(u - f'(m)v, n)$ aus.

Laufzeit (heuristisch):

$$L_n\left[\frac{1}{3}, \left(\frac{64}{9}\right)^{\frac{1}{3}} + o(1)\right]$$

3 Elliptische Kurven

3.1 Einleitung

Ziel: Sowohl ein alternatives Public-Key-Verfahren zu gewinnen, als auch Faktorisierungsalgorithmen und sogar Primzahltests (wobei diese nicht von großer Bedeutung sind).[13]

Kurven sind Lösungsmengen von Polynomen mit mehreren Variablen, etwa die Menge der Punkte aus $\mathbb{R}^3$, die folgende Gleichung erfüllen: $x^3 + y^3 = z^3$.

3.2 Kubiken

3.2.1 Affine Kurven

Sei K ein Körper, Dann sein $\bar{K}$ der algebraische Abschluß.

Definition: Der *affine Raum* der Dimension n sei

$$\mathbb{A}^n = \mathbb{A}^n(\bar{K}) = \left\{ (a_1, \ldots, a_n) \mid a_i \in \bar{K} \right\}$$

Dann sei für $\bar{K} : L : K$ die Menge der *L-rationalen Punkte* definiert als

$$\mathbb{A}^n(L) = \left\{ (a_1, \ldots, a_n) \mid a_i \in L \right\}$$

Definition: Eine *ebene affine Kurve* C ist gegeben durch $f \in K[x_1, x_2]$, wobei dann

$$C = C(\bar{K}) = \left\{ (a_1, a_{2)\in \bar{K}^2} \;\middle|\; f(a_1, a_2) = 0 \right\}$$

Wieder sei $C(L)$ die Menge der *L-rationalen Punkte*:

$$C(L) = \left\{ (a_1, a_{2)\in L^2} \;\middle|\; f(a_1, a_2) = 0 \right\}$$

Im Allgemeinen kann man eine *Gerade* darstellen als $a_0 + a_1 x_1 + a_2 x_2$ mit $(a_1, a_2) \neq 0$.

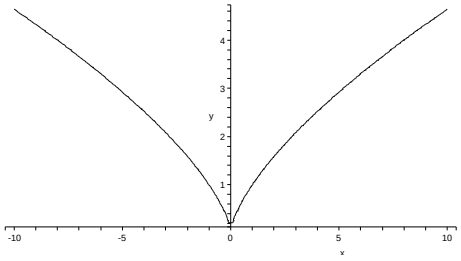
Definition: Ein *absolut irreduzibles Polynom* ist irreduzibel in $\bar{K}[x_1, x_2]$.

Affine Koordinatentransformationen lassen sich mittels $y = Ax + b$ mit einer invertierbaren Matrix A darstellen.

[13] Ein HTML-Tutorial mit Java-Applets zu elliptischen Kurven findet sich unter `http://speedy.et.unibw-muenchen.de/lonline/weiterb/e3/k03/krypver2`.

Definition: In einem *glatten Punkt* läßt sich eine Tangente klar definieren (formal über partielle Ableitung definiert). Andere Punkte heißen *Singularitäten* oder *singuläre Punkte*.

Beispiel: Sei $f(x, y) = x^2 - y^3$, dann ist 0 eine Singularität:



Definition:

- Die *Vielfachheit* eines Punktes a in einem Polynom f in einer Kurve ist die niedrigste Potenz eines Polynoms g, das aus f durch Transformation von a auf 0 entsteht.
- Die *Vielfachheit eines Schnittpunktes* einer Gerade G mit einer Kurve C sei mit $(G \cdot C)_P$ bezeichnet. Man erhält sie durch Einsetzen der parametrisierten Form der Geraden in die Kurve und dann durch die Bestimmung der Vielfachheit der Nullstelle des entstehenden Polynoms[14].

3.2.2 Projektive Kurven

Ansatz: Im affinen Raum schneiden sich zwei ungleiche Geraden in einem oder in keinem Punkt (Parallelen). Einfacher wäre es, wenn sich auch parallele Geraden schneiden, d.h. wenn sich alle Paare von ungleichen Geraden in genau einem Punkt schneiden.

Idee (siehe Graphik 1): Füge für jede Klasse paralleler Gerade (d.h. quasi für jeden möglichen „Winkel“) einen weiteren Punkt ein, der Schnittpunkt dieser Parallelen ist. Dieser Punkt wird als *äußerer Punkt* bezeichnet. Diese bilden zusätzlich z.B. zu der eigentlichen Ebene in der Vorstellung einen Halbkreis. Desweiteren bilden alle äußeren Punkte formal eine Gerade (!).

[14]Für einen Schnittpunkt (a_1, a_2) ist die parametrisierte Form $(a_1 + \delta, a_2 + 2 \cdot \delta)$ für eine Gerade mit Steigung 2, wenn man dieses in die Kurve einsetzt, erhält man ein Polynom über einer Variablen δ, in diesem Polynom kann man dann die niedrigste Potenz betrachten.

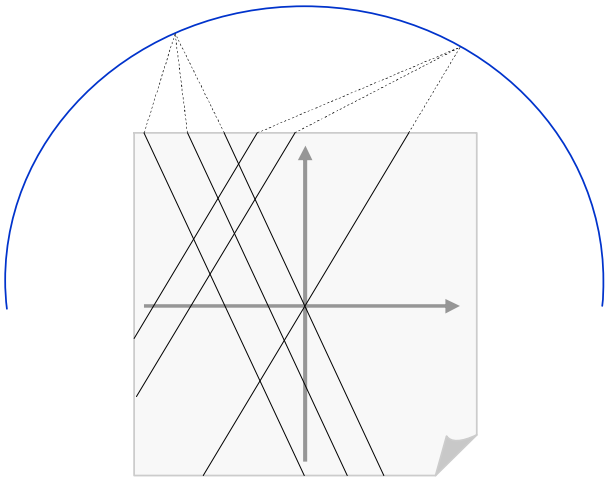


Abbildung 1: Idee der projektiven Ebene

Definition: Definiere eine Äquivalenzrelation $\sim$ auf $\mathbb{A}^{n+1} \setminus \{0\}$ durch

$$(a_0, \ldots, a_n) \sim (b_0, \ldots, b_n) :\Leftrightarrow \exists\, \lambda \in \bar{K}\, \forall i \leq n \colon a_i = \lambda \cdot b_i$$

Die Äquivalenzklassen von $(a_0, \ldots, a_n)$ bezeichnen wir mit $a_0 : \ldots : a_n$.

Definition: Der *projektive Raum* der Dimension n ist

$$\mathbb{P}^n := (\mathbb{A}^{n+1} \setminus \{0\}) / \sim .$$

Die *L-rationalen Punkte* sind dann $\mathbb{P}^n(L) = \{(a_0 : \ldots : a_n) \mid\ a_i \in L\}$.

Als Einbettung von α^n in $\mathbb{P}^n$ kann man nun angeben

$$(a_1, \ldots, a_n) \mapsto (1 : a_1 : \ldots : a_n)$$

Übrig bleiben die Punkte aus $\mathbb{P}^n$ der Form $(0 : a_1 : \ldots : a_n)$, diese sind genau die äußeren Punkte.

Definition: Ein *homogenes Polynom* ist die Summen von Monomen desselben Grades, jeweils mit Koeffizienten.

Beispiel: $2x + \pi y$ und $2xy + ex^2$ sind homogene Polynome, $x + 3$ aber nicht, da 3 den Grad 0 hat und x den Grad 1.

Definition: Eine *projektive Kurve* ist gegeben durch ein homogenes Polynom f:

$$C(\bar{K}) = \{(b_0 : \ldots : b_n) \mid f(b_0, \ldots, b_n) = 0\}.$$

Eine *projektive Gerade* ist gegeben durch das Polynom $a_0x_0 + a_1x_1 + a_2x_2$ mit $(a_0, a_1, a_2) \neq 0$.

Wie kommt man nun von einer affinen Kurve zu einer projektiven Kurve? Sei $f(x_1, \ldots, x_n)$ von Grad d. Dann ist $F(x_0, \ldots, x_n) = x_0^d f(\frac{x_1}{x_0}, \ldots, \frac{x_n}{x_0})$ der *homogene Abschluss*.

Beispiel: Für die affine Ebene gilt: Eine Gerade ist durch $a_0 + a_1x_1 + a_2x_2$ darstellbar. Der homogene Abschluss ist nun

$$x_0^1 \cdot \left(a_0 + a_1\frac{x_1}{x_0} + a_2\frac{x_2}{x_0} \right) = a_0x_0 + a_1x_1 + a_2x_2.$$

Für affine Geraden gilt $(a_1, a_2) \neq 0$. Bildet man nun in der projektiven Ebene eine Gerade dieser Art (d.h. a_0x_0), so erhält man genau die Gerade, die alle äußeren Punkte verbindet.

Definition: Ein projektive *Gerade* ist ein Polynom mit Monomen vom Grad 1, eine *Quadrik* besitzt Monome vom Grad 2 und eine *Kubik* vom Grad 3.

Nun kann man analog zu oben Vielfachheiten sowie Schnittpunkte und deren Vielfachheiten definieren.

Satz: Seien G eine projektive Gerade und C eine projektive Kurve vom Grad d in $\mathbb{P}^2$ mit $G(\bar{K}) \subsetneq C(\bar{K})$. Dann gilt

$$\sum_{P \subseteq G(\bar{K}) \cap C(\bar{K})} (G \cdot C)_P = d.$$

3.2.3 Addition auf Kubiken

Satz: Jede nicht-singuläre Kurve ist absolut irreduzibel.

Folgerung: Jede nicht-singuläre Kubik schneidet jede Gerade in genau drei Punkten (beachte aber Vielfachheiten!).

Notation: Sei G eine Gerade und C eine nicht-reguläre Kubik, und seien P, Q und R die Schnittpunkte von G und C. Dann schreibe:

$$G \cdot C = P + Q + R$$

Sei nun C wie oben, gegeben seien Punkte P, $Q \in C$. Dann ist $\varphi_C(P, Q)$ der Punkt R mit $G \cdot C = P + Q + R$ und G Gerade durch die Punkte P und Q, bei $P = Q$ verwende die Tangente.

Definition: Sei wieder C wie oben, gegeben ein Punkt O definiere eine Gruppe $(C, \oplus_O)$ durch

$$P \oplus_O Q = \varphi_C(\varphi_C(P, Q), O).$$

Satz: Für jede nicht-singuläre Kubik C und jedem Punkt $O \in C$ ist $(C, \oplus_O)$ eine abelsche Gruppe mit neutralem Element O.

Bemerkung: Alle Gruppen $(C, \oplus_O)$ für $O \in C$ sind isomorph.

Definition: Eine *elliptische Kurve* ist die Menge der K-rationalen Punkte einer nicht-singulären ebenen projektiven Kubik (sofern diese Menge nicht leer ist).

Normalformen (für $\operatorname{char} K \neq 2, 3$) nach Koordinatentransformation, projektiv[15]:

$$y^2 z = x^3 + axz^2 + bz^3$$

Dabei kommt genau ein uneigentlicher Punkt $(0 : 1 : 0)$ hinzu und fordert noch $4a^3 + 27b^2 \neq 0$, was vor allem die nicht-singularität (Ableitungen!) benötigt wird.

Nun kann man den einen uneigentlichen Punkt noch auf die affine Null abbilden, damit entsteht eine **affine Normalform**:

$$y^2 = x^3 + ax + b$$

Notation für elliptische Kurven:

$$E_{a,b}(K) = \left\{ (x, y) \mid y^2 = x^3 + ax + b \right\} \cup \{0\}$$

Beispiel: In Graphik 2 sind drei elliptische Kurven eingezeichnet.

Etwas allgemeiner:

$$\begin{gathered} y^2 = x^3 + Cx^2 + Ax + B \\ \text{mit } 0 \neq 4A^3 + 27B^2 - 18ABC - A^2C^2 + 4BC^3 \end{gathered}$$

Nun können wir Addieren und Invertieren in $E_{A,B}(K)$ mit $P_0 = (x_0, y_0)$ und $P_1 = (x_1, y_1)$ definieren, sei dazu O wieder der Punkt im unendlichen:

1. Es gilt $-O = O$.

[15] Dabei entsprechen die neuen x, y, z den alten x_i in folgender Weise: $x_0 = z$, $x_1 = x$ und $x_2 = y$.

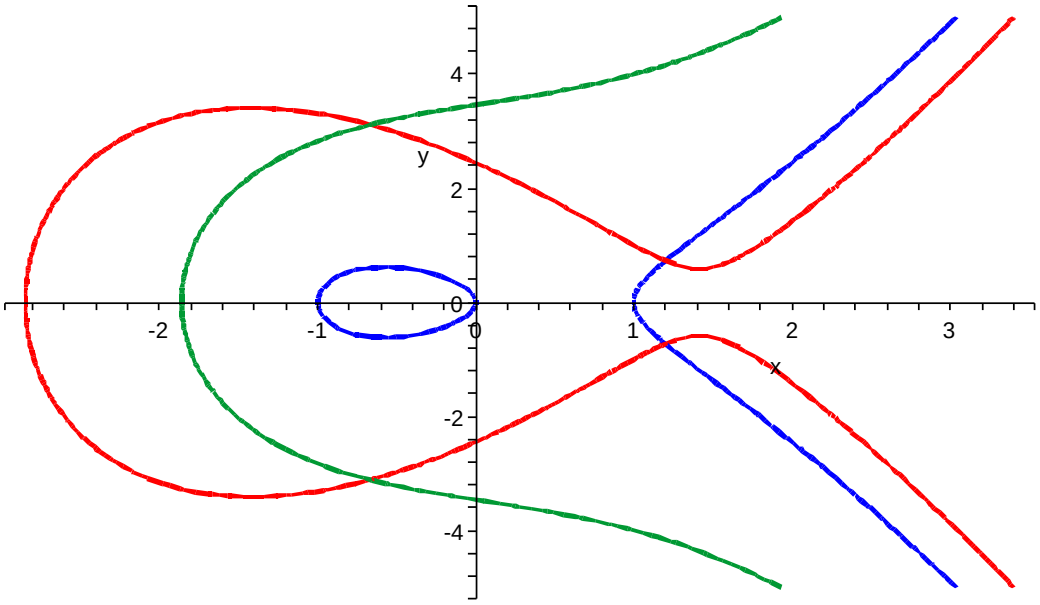


Abbildung 2: elliptische Kurven $y^2 = x^3 - x$ (blaut), $y^2 = x^3 - 6x + 6$ (rot) und $y^2 = x^3 + 3x + 12$ (grün)

2. Es gilt $-P_0 = (x_0, -y_0)$.

3. Falls $P_0 = -P_1$, so ist $P_0 + P_1 = 0$

4. Falls $P_0 \neq -P_1$, dann ist $P_0 + P_1 = (x_2, y_2)$ mit

$$m = \begin{cases} \frac{y_1 - y_0}{x_1 - x_0} & \text{falls} \quad x_0 \neq x_1 \\ \frac{3x_0^2 + 2Cx_0 + A}{2y_0} & \text{falls} \quad x_0 = x_1 \end{cases}$$
$$x_2 = m^2 - C - x_0 - x_1$$
$$y_2 = m \cdot (x_0 - x_2) - y_0$$

   Dabei ist m die Steigung der Geraden, wobei der Fall $x_0 = x_1$ nur noch für $P_0 = P_1$ eintritt (da $y_0 \neq -y_1$ sein muß, also $y_0 = y_1$).

Nun kann man Multiplizieren mit $k \in \mathbb{N}$ durch iteriertes Verdoppeln, d.h. $5P = 2(2P) + P$.

3.3 Lentras Faktorisierungsalgorithmus

Satz (Hasse): Für jede Primzahl P und jede elliptische Kurve E über $\mathbb{Z}_p$ gilt:

$$p - 1 - 2\sqrt{p} < |E| < p + 1 + 2\sqrt{p}.$$

Satz (Cassels): Die Gruppe E einer elliptischen Kurve E über $\mathrm{GF}(p^k)$ ist entweder zyklisch oder isomorph zu $\mathbb{Z}_d \times \mathbb{Z}_e$ mit $d \mid e$ und $d \mid p^k - 1$.

Definition: Eine *pseudo-elliptische Kurve* ist eine elliptische Kurve über $\mathbb{Z}_n$, d.h.

$$E_{a,b}(\mathbb{Z}_n) = \left\{ (x, y) \mid \ y^2 = x^3 + ax + b \right\} \cup \{0\}$$

Die Nebenbedingung sei dieselbe wie oben, die Addition erfolge gemäß der Formeln.

Bemerkung: Dann ist die Addition nur partiell definiert, denn im Fall 4 in der Additions-Definition können bei der Berechnung von m im Nennen nicht-invertierbare Elemente auftreten. *Dann findet man aber einen Faktor von n!*

Lemma: Sei E eine pseudo-elliptische Kurve modulo n, und P_0 und P_1 nicht zu einander inverse, eigentliche Punkte der Kurve. Dann sind äquivalent:

1. Es gibt eine Primzahl $p \mid n$, so dass $(P_0 \bmod p) + (P_1 \bmod p) = O$ in $E \bmod p$.
2. Der Zähler m ist nicht teilerfremd zu n.

Idee (sehr analog zur Pollardschen $(p-1)$-Methode aus Kapitel 2.2.2): Sei n zerlegbar, aber keine perfekte Potenz. Sei $p \mid n$ Primzahl und E eine pseudo-elliptische Kurve über $\mathbb{Z}_n$. Sei m eine Zahl, so dass die Ordnung $|E \bmod p|$ die Zahl m teilt, und sei P ein beliebiger Punkt auf E.

Dann erhält man bei der Berechnung von $m \cdot P$ in E[16] einen Nenner d, der zu n nicht teilerfremd ist. Also ist $\mathrm{ggT}(n, d)$ ein Kandidat für einen Teiler von n.

Lenstras **Algorithmus**:

1. Initialisierung: Wähle die Schranke b und setze $m = \mathrm{kgV}(1, \ldots, b)$.
2. Finde eine pseudo-elliptische Kurve und einen Punkt, d.h. wähle $x, y, a < n$ zufällig und setze $b = y^2 - x^3 - ax \bmod n$. Sei nun $g = \mathrm{ggT}(4a^2 + 27b^2, n)$.

[16] Beachte: $m \cdot P = O$ in $E \bmod p$, wir rechnen aber in E.

- Falls $g = n$ ist, so beginnen wir erneut.
- Falls $1 < g < n$, so haben wir einen Teiler gefunden!
- Falls $g = 1$ ist, haben wir einen Kurve gefunden.

3. Bestimme $m \cdot P$ und gib ggf. den Faktor von n aus, falls in den Nennern der Brüche entsprechendes auftritt.

Laufzeit (heuristisch): $L_p[\frac{1}{2}, \sqrt{2} + o(1)]$ für den kleinsten Primfaktor p von n (beachte: L_p und nicht L_n!).

Anwendung: Man hat mit diesem Verfahren u.a. einen 49 Dezimalstellen großen Primfaktor der Zahl $2^{2071} - 1$ berechnet, sowie mehrere Faktoren der Zahl $2^{677} - 1$.

3.4 Elliptische Kurven in der Kryptographie

Generell kann man dort, wo in der Kryptographie mit dem diskreten Logarithmus gearbeitet wird, auch elliptische Kurven benutzen, z.B. bei ElGamal oder bei Diffie-Hellman Key Exchange.

Problem DL (Diskreter Logarithmus): Zu einer Primzahl p, einem primitiven Element g und einem $h \in \mathbb{Z}_p^*$ wird ein i gesucht, so dass $g^i = h$.

Problem ECDL (Elliptic Curve Discrete Logarithm): Zu einer elliptischen Kurve E und $P, Q \in E$ wird ein n gesucht, so dass $Q = nP$.

Beispiel: Schlüsselaustausch mittels Diffie-Hellman Key Exchange mit elliptischen Kurven (ECDH):

1. Allice und Bob einigen sich auf eine öffentliche elliptische Kurve E über einem endlichen Körper und auf einen öffentlichen Punkt $P \in E$ mit Ordnung n.

2. Alice wählt zufällig $r_A \in \mathbb{N}$ mit $2 \leq r_A \leq n - 2$ und veröffentlicht $Q_A = r_A \cdot P$.

3. Bob wählt zufällig $r_B \in \mathbb{N}$ mit $2 \leq r_B \leq n - 2$ und veröffentlicht $Q_B = r_B \cdot P$.

4. Alice bestimmt $K = r_A \cdot Q_B = r_A(r_B \cdot P) = r_A r_B \cdot P$.

5. Bob bestimmt $K = r_B \cdot Q_A = r_B(r_A \cdot P) = r_A r_B \cdot P$.

Das Protokoll ist dann korrekt, d.h. wenn es so ausgeführt wird, einigen sich Alice und Bob auf den selben Schlüssel. Bei der Wahl der Parameter (elliptische Kurve E sowie Punkt P) muss man vorsichtig sein, da viele Nebenbedingungen berücksichtigt werden müssen. Im Allgemeinen sind aber die Schlüssellängen sehr viel kürzer als bei RSA: Sicherheit (nach heutigem Stand der Erkenntnis) erhält man bereits ab 160 Bits.

Bemerkung: Wenn ECDL effizient lösbar ist, so lässt sich ECDH brechen: Man könnte aus Q_A und Q_B dann r_A oder r_B berechnen und somit K. *Aber:* die Umkehrung ist nicht bekannt – falls ECDH gebrochen wird, muß dies evtl. kein Verfahren für ECDL liefern.

Genauer: Die Sicherheit beruht eigentlich auf der Sicherheit von ECDHP (wobei das P für "Problem„ steht): Zu gegebenen P, rP, sP wird rsP gesucht.

Andere Verfahren, die auf elliptischen Kurven basieren:

- Signaturverfahren: ECDSA, EC-KCDSA (Korean certificate-based)
- Verschlüsselungs-Verfahren: CIES (integrated encryption scheme), PSEC (provably secure)
- Schlüsselvereinbarung: STS (station-to-station), ECMQV (ANSI X 9.63)