Zahlentheorie

Alexander May

Fakultät für Mathematik
Ruhr-Universität Bochum

Sommersemester 2015

Organisatorisches

- Vorlesung: **Mo 12–14** in HZO 70, **Mi 10–12** in HZO 60 (9 CP)
- Übung: **Di 08–10, 12–14, 14–16**
- Zentralübung: **Mo 14–16**
- Gruppenleiter: **Robert Kübler, Elisabeth Kramza, Andreas Hessemann**
- SHKs: **Katharina Schütte, Elisabeth Kramza, Andreas Hessemann, Matthias Bednarski**
- Übungsbetrieb:
  - Präsenzübung, Start 14. April
  - Zentralübung, Start 20. April, **Mo 14–16** in NA 1/64
- Übungsaufgaben werden korrigiert.
- Gruppenabgaben bis 3 Personen
- Bonussystem: Zusätzlich zu den 100 Punkten in der Klausur können Bonuspunkte über die Übungen erworben werden.
  - 1 Punkt ab 5%, 2 Punkte ab 15%, . . . , 10 Punkte ab 95%.
- Klausurtermin: voraussichtlich Mitte Juli

Literatur

Vorlesung richtet sich nach

- Stefan Müller-Stach, Jens Piontkowski, “Elementare und algebraische Zahlentheorie”, Vieweg+Teubner, 2. Auflage, 2011.

Weitere Literatur:

- Peter Bundschuh, “Einführung in die Zahlentheorie”, Springer, 2002
- Alexander Schmidt, “Einführung in die algebraische Zahlentheorie”, Springer, 2007
- Rainer Schulze-Pillot, “Einführung in Algebra und Zahlentheorie”, Springer, 2008
- Helmut Koch, “‘Zahlentheorie”, Vieweg, 1997
- Reinhold Remmert, Peter Ullrich, “Elementare Zahlentheorie”, Birkhäuser, 1995
- Friedhelm Padberg, “Elementare Zahlentheorie”, Spektrum, 2008

Primzahlen

Definition Primzahl

Wir definieren die Menge der *Primzahlen*

$$\mathbb{P} = \{x \in \mathbb{N} \setminus \{1\} \mid x \text{ ist nur durch sich selbst und 1 teilbar.}\}$$

- Können wir effizient entscheiden, ob $x \in \mathbb{P}$?

Algorithmus Naiver Primzahltest

EINGABE: $x \in \mathbb{N}$

1. Falls x durch eine der Zahlen $2, \ldots, \lceil \sqrt{x} \rceil$ teilbar, Ausgabe “$x \notin \mathbb{P}$”.
2. Sonst Ausgabe “$x \in \mathbb{P}$”.

- **Korrektheit:** Falls x zusammengesetzt ist, so besitzt es einen Teiler der Größe höchstens $\sqrt{x}$.
- **Laufzeit:** Algorithmus benötigt höchstens $\sqrt{x} - 1$ Divisionen.
- Später: Primzahltests mit Laufzeit polynomiell in $\log_2(x)$.

Landau-Notation

Definition Landau-Notation

Seien $f, g : \mathbb{N} \to \mathbb{N}$ Funktionen. Es gilt

1. $f(n) = \mathcal{O}(g(n))$ gdw
   $$\exists n_0 \in \mathbb{N}, c \in \mathbb{R}, c > 0 \text{ mit } f(n) \leq c \cdot g(n) \text{ für alle } n \geq n_0.$$
2. $f(n) = \Omega(g(n))$ gdw
   $$\exists n_0 \in \mathbb{N}, c \in \mathbb{R}, c > 0 \text{ mit } f(n) \geq c \cdot g(n) \text{ für alle } n \geq n_0.$$
3. $f(n) = \Theta(g(n))$ gdw $f(n) = \mathcal{O}(g(n))$ und $f(n) = \Omega(g(n))$

Bsp:

- $2n = \mathcal{O}(n^2)$ und $2n = \mathcal{O}(n)$.
- $3n^2 + n \log n + 7 = \mathcal{O}(n^2)$
- $\sum_{i=1}^{n} i = \frac{n(n+1)}{2} = \mathcal{O}(n^2)$
- $\sum_{i=0}^{n} \frac{1}{i} = \mathcal{O}(\log n)$
- $n! = \mathcal{O}(n \left(\frac{n}{e}\right)^n)$

Sieb des Erasthostenes

Ziel: Berechne alle Primzahlen bis n.

Algorithmus Sieb des Erasthostenes

EINGABE: $n \in \mathbb{N}$

1. Schreibe alle Zahlen $2, \ldots, n$ in eine Liste L.
2. For $i = 2$ to n: Falls $i \in L$, entferne alle Vielfachen $2i, 3i, \ldots$ aus L.

AUSGABE: $L = \{x \in \mathbb{P} \mid x \leq n\}$

Korrektheit:

- Alle aus L entfernten Zahlen sind nicht in $\mathbb{P}$.
- Jede Nicht-Primzahl wird entfernt, sobald i ihr kleinster Teiler ist.
- Damit verbleiben in L nur Primzahlen.

Laufzeit:

- Schritt 1: $\mathcal{O}(n)$
- Schritt 2: höchstens $\frac{n}{2} + \frac{n}{3} + \ldots + 1 = \mathcal{O}(n \log n)$ Operationen.
- D.h. die Gesamtlaufzeit ist $\mathcal{O}(n \log n)$.

Unendlich viele Primzahlen

Satz von Euklid

Es existieren unendlich viele Primzahlen.

Beweis:

- Annahme: Sei $\mathbb{P} = \{p_1, \ldots, p_n\}$ endlich mit $p_1 < \ldots < p_n$.
- Sei $P = \prod_{i=1}^{n} p_i + 1$. Da $P > p_n$ folgt $P \notin \mathbb{P}$.
- D.h. P besitzt einen nicht-trivialen kleinsten Teiler a, $1 < a < P$.
- Sei $a \notin \mathbb{P}$. Dann besitzt a einen nicht-trivialen Teiler a', $1 < a' < a$, der ein Teiler von P ist (Widerspruch zur Minimalität von a).
- Es folgt $a \in \mathbb{P}$. Damit lässt $P = \prod_{p \in \mathbb{P}} p + 1$ bei Teilung durch a Rest 1. (Widerspruch: a teilt P.)

Wie konstruiert man Primzahlen?

Vermutung von Fermat: $F_k = 2^{2^k} + 1 \in \mathbb{P}$. Falsch schon für $k = 5$.

Lemma

Falls $b > 1$ ungerade oder $m \neq 2^k$, $m \geq 3$ so ist $b^m + 1$ nicht prim.

Beweis:

- Falls $b > 1$ ungerade, ist auch $b^m > 1$ ungerade. Damit ist $b^m + 1 > 2$ gerade und kann keine Primzahl sein.
- Ist $m \neq 2^k$, so gilt $m = pm'$ für einen ungeraden Faktor $3 \leq p \leq m$.
- Damit gilt $b^m + 1 = (b^{m'})^p + 1$. Wir wollen $(b^{m'})^p + 1$ faktorisieren.
- Betrachte dazu das Polynom $X^p + 1$ mit Nullstelle (-1). Es gilt
$$X^p + 1 = (X+1)(X^{p-1} - X^{p-2} + X^{p-3} - \ldots - X + 1).$$
- Einsetzen von $X = b^{m'}$ liefert den nicht-trivialen ersten Faktor
$$1 < b^{m'} + 1 < b^m + 1.$$

Mersenne Primzahlen

Mersenne-Primzahlen sind Primzahlen der Form $2^p - 1$ für $p \in \mathbb{P}$.

Lemma

Falls m zusammengesetzt ist, so ist auch $2^m - 1$ zusammengesetzt.

Beweis:

- Sei $m = pq$ mit $1 < p, q < m$. Damit ist $2^m - 1 = (2^p)^q - 1$. Es gilt
$$X^q - 1 = (X - 1)(X^{q-1} + \ldots + X + 1).$$
- Einsetzen von $X = 2^p$ liefert nicht-trivialen Faktor
$$1 < 2^p - 1 < 2^m - 1.$$

Anmerkung:

Die größten *bekannten* Primzahlen sind oft von der Mersenne-Form.

Wiederholung: Gruppe

Definition Gruppe

Eine *Gruppe* ist ein Tupel $(G, \circ)$ bestehend aus einer Menge G und einer Verknüpfung $\circ : G \times G \to G$ mit

1. **Neutrales Element:** $\exists! e \in G$ mit $e \circ g = g \circ e = g$ für alle $g \in G$.
2. **Inverses Element:** Für alle $g \in G$ existiert ein $g^{-1} \in G$ mit
$$g \circ g^{-1} = g^{-1} \circ g = e.$$
3. **Assoziativität:** Für alle $g, h, r \in G$ gilt $(g \circ h) \circ r = g \circ (h \circ r)$.

G heißt *abelsch* (kommutativ), falls $g \circ h = h \circ g$ für alle $g, h \in G$.

Beispiele für Gruppen

Bsp:

- $(\mathbb{Z}, +)$ ist eine abelsche Gruppe.
- $(\mathbb{Z}^n, +)$ ist eine abelsche Gruppe.
- $(\mathbb{N}, +)$ ist *keine* Gruppe.
- Die Bijektionen $\{1, \ldots, n\} \to \{1, \ldots, n\}$ bilden zusammen mit der Komposition von Funktionen die *symmetrische Gruppe S_n*.
  Für $n \geq 3$ ist S_n nicht abelsch:
  $$(123) \circ (13)(2) = (1)(23) \neq (12)(3) = (13)(2) \circ (123).$$
- Die invertierbaren $(n \times n)$-Matrizen über $\mathbb{Z}$ bilden eine Gruppe unter Matrixmultiplikation, bezeichnet als $GL(n, \mathbb{Z})$.
  Für $n \geq 2$ ist $GL(n, \mathbb{Z})$ nicht abelsch.

Wiederholung: Ringe und Ideale

Definition Ring

Ein *Ring* ist ein Tupel $(R, +, \cdot)$ bestehend aus einer Menge R und zwei assoziativen Verknüpfungen $+, \cdot : R \times R \to R$ mit

- $(R, +)$ ist eine abelsche Gruppe mit neutralem Element 0.
- $(R, \cdot)$ besitzt ein neutrales Element 1.
- **Distributivität:** Für alle $a, b, c \in R$ gilt
$$(a+b)c = ac + bc \text{ und } a(b+c) = ab + ac.$$

Statt $(R, +, \cdot)$ schreiben wir meist nur R.

Integritätsbereich

Definition

Ein Ring R heißt

- **kommutativer Ring** falls $a \cdot b = b \cdot a$ für alle $a, b \in R$.
- **Integritätsbereich** falls R kommutativ und Nullteiler-frei ist, d.h.
$$ab \neq 0 \text{ für } a, b \neq 0.$$
- **Schiefkörper** falls $(R \setminus \{0\}, \cdot)$ eine Gruppe ist.
- **Körper** falls R ein kommutativer Schiefkörper ist.

Bsp:

- $(\mathbb{Z}, +, \cdot)$ ist ein Integritätsbereich.
- $(\mathbb{Z}^{n \times n}, +, \cdot)$ ist ein Ring, der nicht kommutativ ist.
- Wir definieren den ganzzahligen Polynomring in einer Variablen
$$\mathbb{Z}[X] = \{\sum_{i=0}^{\infty} a_i X^i | a_i \in \mathbb{Z}, \text{ endlich viele } a_i \neq 0\}.$$
Dann ist $(\mathbb{Z}[X], +, \cdot)$ ein Integritätsbereich.
- $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$ sind Körper.

Ideale

Definition Ideal

Sei R ein Ring. $I \subseteq R$ heißt *Links-Ideal* (bzw. Rechts-Ideal), falls

- $(I, +)$ eine Gruppe ist,
- $R \cdot I \subseteq I$ (bzw. $I \cdot R \subseteq I$), d.h. $r \cdot f \in I$ für alle $r \in R, f \in I$.

I heißt *Ideal*, falls I sowohl Links- als Rechts-Ideal ist.

Notationen:

- Wird I von $f_1, \ldots, f_m$ erzeugt, so schreiben wir $I = \langle f_1, \ldots, f_m \rangle$.
- Falls $I = \langle f \rangle$, so heißt I Hauptideal.

Bsp:

- Im Ring $\mathbb{Z}$ sei $I_1 = \langle 6, 8 \rangle = \{a \cdot 6 + b \cdot 8 \mid a, b \in \mathbb{Z}\}$.
- I_1 ist ein Hauptideal, denn $I_1 = \langle 2 \rangle$.
- Im Ring $\mathbb{Q}[X]$ sei $I_2 = \langle 2X^2, X^4 \rangle = \{a \cdot 2X^2 + b \cdot X^4 \mid a, b \in \mathbb{Q}[X]\}$.
- I_2 ist ein Hauptideal, denn $I_2 = \langle X^2 \rangle$.

Teilbarkeit

Definition Teilbarkeit

Sei R ein Integritätsring und $a, b \in R$.

- Element a *teilt* b, falls $b = ac$ für ein $c \in R$. Wir schreiben $a \mid b$. Falls b nicht von a geteilt wird, schreiben wir $a \nmid b$.
- *Einheiten* R^* von R sind die Teiler der Eins, d.h.
$$R^* := \{u \in R \mid u \mid 1\}.$$
- Die Elemente a, b heißen *assoziert*, falls $a = bc$ für ein $c \in R^*$.

Bsp:

- In $\mathbb{Z}[X]$ gilt $-X - 1 \mid X^2 - 1$ und $\mathbb{Z}[X]^* = \{1, -1\}$.
- Ferner sind $X + 1$ und $-X - 1$ assoziiert.
- In $\mathbb{Q}[X]^*$ sind genau die Polynome vom Grad 0.

Elementare Teilbarkeitsaussagen

Lemma Teilbarkeit

Sei R ein Integritätsring und $a, b \in R$. Dann gilt

1. $a \mid b \Rightarrow a \mid bd$
2. $a \mid b_1$ und $a \mid b_2 \Rightarrow a \mid d_1 b_1 + d_2 b_2$ für alle $d_1, d_2 \in R$
3. $a \mid b \Leftrightarrow da \mid db$
4. $a \mid b$ und $b \mid d \Rightarrow a \mid d$
5. $a \mid b$ und $b \mid a \Leftrightarrow a, b$ sind assoziiert.

Beweis: Übungsaufgabe.

Euklidische Ringe

Definition Euklidischer Ring

Sei R ein Integritätsring. R heißt *euklidisch*, falls eine Bewertungs-Funktion

$$N : R \setminus \{0\} \to \mathbb{N}_0$$

existiert, so dass für alle $a, b \in R$ mit $b \neq 0$ Elemente $q, r \in R$ existieren mit $a = qb + r$ und entweder $r = 0$ oder $N(r) < N(b)$.

Satz

Der Ring $\mathbb{Z}$ ist euklidisch.

Beweis:

- Wähle als Bewertungsfunktion den Betrag $N = |\cdot|$ und $q = \lfloor \frac{a}{b} \rfloor$.
- Damit gilt $r = a - qb = a - \lfloor \frac{a}{b} \rfloor b$ mit
$$0 \leq |r| < \max\{|a - (\tfrac{a}{b} - 1)b|, |a - (\tfrac{a}{b} + 1)b|\} = |b|.$$

Übung: Zeigen Sie, dass $\mathbb{Q}[X]$ euklidisch ist.

Die Gaußschen Zahlen besitzen euklidische Division.

Satz

Der Ring der Gaußschen Zahlen

$$\mathbb{Z}[i] := \mathbb{Z} \oplus i\mathbb{Z} = \{x + iy \mid x, y \in \mathbb{Z}\} \subset \mathbb{Q}[i] \subset \mathbb{C}$$

ist euklidisch.

Beweis:

- Sei $z = x + iy \in \mathbb{Z}[i]$ mit konjugiert Komplexem $\bar{z} = x - iy$.
- Wir definieren eine Bewertungsfunktion vermöge der Norm
$$N(z) := z\bar{z} = ||z||^2.$$
- Offenbar gilt
$$N(z) = (x + iy)(x - iy) = x^2 + y^2 \geq 0 \text{ und } N(z) = 0 \Leftrightarrow z = 0.$$
- Die Normfunktion ist multiplikativ, denn
$$N(wz) = wz\overline{wz} = w\bar{w}z\bar{z} = N(w)N(z).$$

Die Gaußschen Zahlen besitzen euklidische Division.

Beweis: (Fortsetzung)

- Seien $a, b \in \mathbb{Z}[i]$. Wir berechnen $c = \frac{a}{b} = u + iv \in \mathbb{Q}[i]$.
- Wir definieren $q = \lfloor u \rceil + i \lfloor v \rceil \in \mathbb{Z}[i]$. Es folgt
$$N(c-q) = ||c-q||^2 \leq (\tfrac{1}{2})^2 + (\tfrac{1}{2})^2 = \tfrac{1}{2}.$$
- Wir definieren $r = a - bq$. Damit folgt
$$N(r) = N(a-bq) = N(cb-bq) = N(c-q) \cdot N(b) < N(b).$$

Bsp:

- Sei $a = 3 - 2i$ und $b = 1 - 2i$. Dann folgt $b^{-1} = \frac{1}{5}(1+2i) \in \mathbb{Q}[i]$.
- Damit ist $c = \frac{1}{5}(7+4i) \in \mathbb{Q}[i]$ und wir runden zu $q = 1 + i \in \mathbb{Z}[i]$.
- Für $r = a - bq = (3-2i) - (1-2i)(1+i) = -i$ gilt
$$N(r) = 1 < 5 = N(b).$$

Übung: Zeigen Sie mittels Normfunktion $N(\cdot)$, dass $\mathbb{Z}[i]^* = \{\pm 1, \pm i\}$.

Hauptidealring

Definition Hauptideal

Sei R ein Integritätsring. R heißt *Hauptidealring*, falls jedes Ideal $I \subseteq R$ ein Hauptideal ist, d.h. $I = \langle b \rangle := Rb := \{rb \mid r \in R\}$ für ein $b \in R$.

Satz

Jeder euklidische Ring R ist ein Hauptidealring.

Beweis:

- Falls $I = \{0\}$, gilt $I = \langle 0 \rangle$. Sei also im Folgenden $I \neq \{0\}$.
- Wähle $b \in I$ mit minimalem $N(b)$. Offenbar gilt $\langle b \rangle \subseteq I$.
- Z.z.: $I \subseteq \langle b \rangle$. Sei $a \in I$ beliebig. Wir müssen $a \in \langle b \rangle$ zeigen.
- Da R euklidisch ist, können wir $a = qb + r$ für $q, r \in R$ schreiben.
- Wegen $r = a - qb$ und $a, b \in I$ folgt $r \in I$.
- Aus $N(r) < N(b)$ und der Minimalität von $N(b)$ folgt $r = 0$.
- Damit gilt $a = qb$ und daher $a \in \langle b \rangle$.

Anmerkung:

Generatoren sind eindeutig bis auf Multiplikation mit Einheiten.

Prim versus irreduzibel

Definition Irreduzibilität

Sei R ein Integritätsbereich und $p \in R \setminus (R^* \cup \{0\})$.

- Wir bezeichnen p als *prim*, falls für alle $r, s \in R$ gilt
$$p | rs \Rightarrow p | r \text{ oder } p | s.$$
- Wir bezeichnen p als *irreduzibel*, falls
$$p = rs \Rightarrow r \in R^* \text{ oder } s \in R^*.$$
- Wir bezeichnen p als *reduzibel*, falls p nicht irreduzibel ist.

Prime Elemente sind irreduzibel.

Satz

Sei R ein Integritätsring und $p \in R$ prim. Dann ist p irreduzibel.

Beweis:

- Sei $p = ab$. Wir müssen zeigen, dass $a \in R^*$ oder $b \in R^*$.
- Da p prim ist, gilt $p|a$ oder $p|b$. OBdA $p|a$.
- Es folgt $pr = a$ für ein $r \in R$. Damit gilt $p = ab = prb$.
- Kürzen von p liefert $rb = 1$ und daher $b \in R^*$.

Irreduzible Elemente müssen nicht prim sein.

Bsp: Wir betrachten $z = 2 + \sqrt{-5} \in \mathbb{Z}[\sqrt{-5}]$.

- Wir wollen zunächst zeigen, dass z irreduzibel ist. Wir betrachten
$$N(z) = z\bar{z} = (2 + \sqrt{-5})(2 - \sqrt{-5}) = 2^2 - (-5) = 9.$$
- Sei $r \in \mathbb{Z}[\sqrt{-5}]^*$. Dann gilt $rs = 1$ und
$$N(r)N(s) = N(rs) = N(1) = 1.$$
- Da die Normfunktion nur positive Wert annimmt, folgt $N(r) = 1$.
- D.h. eine nicht-triviale Zerlegung von $z = z_1 z_2$ erfüllt
$$N(z_1) = N(z_2) = 3.$$
- Sei $z_1 = x + y\sqrt{-5}$ mit $N(z_1) = x^2 + 5y^2$.
- Da $x^2 + 5y^2 = 3$ keine Lösung $(x, y) \in \mathbb{Z}^2$ besitzt, existieren in $\mathbb{Z}[\sqrt{-5}]$ keine Elemente mit Norm 3. D.h. z ist irreduzibel.
- Andererseits gilt $z | 3 \cdot 3$ wegen $z \cdot \bar{z} = 9$.
- Gleichzeitig gilt aber $z \nmid 3$. Damit ist z nicht prim in $\mathbb{Z}[\sqrt{-5}]$.

Anmerkung: 9 besitzt in $\mathbb{Z}[\sqrt{-5}]$ zwei verschiedene Faktorisierungen
$$9 = (2 + \sqrt{-5})(2 - \sqrt{-5}) = 3 \cdot 3.$$
Ebenso ist 3 nicht prim in $\mathbb{Z}[\sqrt{-5}]$.

Faktorieller Ring

Definition

Sei R ein Integritätsring. R heißt *faktoriell* falls jedes $p \in R \setminus (R^* \cup \{0\})$ in ein Produkt von Primelementen zerlegt werden kann.

Korollar

Sei R faktoriell und $p \in R$ irreduzibel. Dann ist p prim.

Beweis:

- Da p sich nicht weiter zerlegen lässt, aber ein Produkt aus Primelementen ist, muss es selbst prim sein.

Eindeutigkeit der Primelementzerlegung

Satz Eindeutigkeit der Primelementzerlegung

Sei R faktoriell. Dann lässt sich jedes $r \in R$ bis auf Assoziiertheit und Reihenfolge eindeutig in Primelemente zerlegen.

Beweis:

- Seien $r = p_1 p_2 \dots p_n = q_1 q_2 \dots q_m$ zwei Primelementzerlegungen.
- Wegen $p_1 \mid q_1 q_2 \dots q_m$ und p_1 prim, folgt $p_1 \mid q_j$ für ein $j \in [m]$.
- ObdA $p_1 \mid q_1$, d.h. $q_1 = sp_1$. Da q_1 irreduzibel ist, gilt $s \in R^*$.
- Damit sind p_1, q_1 assoziiert. Teilen durch p_1 liefert
$$p_2 p_3 \dots p_n = q_2' q_3 \dots q_m \text{ mit } q_2' = sq_2.$$
- Zeige analog die paarweise Assoziiertheit der restlichen Faktoren.

Anmerkung:

In $\mathbb{Z}[i]$ sind die folgenden Zerlegungen äquivalent

$$12 = 3(1+i)^2(1-i)^2 = 3i(1+i)(1-i)^3 \ .$$

Äquivalenzaussagen zu faktoriellen Ringen

Satz Äquivalenzaussagen zu faktoriellen Ringen

Sei R ein Integritätsring und $p \in R \setminus (R^* \cup \{0\})$. Es sind äquivalent:

1. R ist faktoriell.
2. p lässt sich eindeutig in ein Produkt von Primelementen zerlegen. (Eindeutigkeit bis auf Reihenfolge und Assoziiertheit)
3. p lässt sich eindeutig in ein Produkt von irreduziblen Elementen zerlegen. Ferner ist jedes irreduzible Element prim.
4. p lässt sich in ein Produkt von irreduziblen Elementen zerlegen. Ferner ist jedes irreduzible Element prim.

Beweis:

- $1 \Rightarrow 2$: Satz zur Eindeutigkeit der Primelementzerlegung.
- $3 \Rightarrow 4$: trivial.
- $4 \Rightarrow 1$: Definition eines faktoriellen Rings.

Äquivalenzaussagen zu faktoriellen Ringen

Beweis: (Fortsetzung)

- $2 \Rightarrow 3$: Jedes prime Element ist irreduzibel. Damit erhalten wir eine eindeutige Zerlegung jedes Elements in irreduzible Faktoren.
- Bleibt zu zeigen, dass jedes irreduzible Element prim ist.
- Sei r irreduzibel und teile ab, d.h. $rc = ab$. Seien $a = \prod_i a_i$, $b = \prod_j b_j$, $c = \prod_k c_k$ Zerlegungen in irreduzible Faktoren.
- Damit erhalten wir 2 Zerlegungen von ab in irreduzible Faktoren
$$r \prod_k c_k = \prod_i a_i \prod_j b_j.$$
- Aus der Eindeutigkeit der Zerlegung bis auf Reihenfolge und Assoziiertheit ist r zu einem der a_i oder b_j assoziiert.
- D.h. r teilt a oder r teilt b.

Hauptidealringe sind faktoriell.

Satz

Jeder Hauptidealring R ist faktoriell.

Beweis: Wir zeigen Eigenschaft 4 des vorherigen Satzes.

- **Zerlegung in irreduzible Faktoren:** Sei $r \in R \setminus (R^* \cup \{0\})$.
- Solange $r_1 = r$ reduzibel ist, zerlegen wir es weiter.
- Annahme: Zerlegung stoppt nicht, d.h. wir erhalten eine unendliche Kette $r_i = r_{i+1}c$ echter Zerlegungen mit $c \notin R^*$.
- Wegen $r_{i+1} \mid r_i$ und $c \notin R^*$ gilt für die Ideale $\langle r_i \rangle \subset \langle r_{i+1} \rangle$.
- D.h. wir erhalten eine unendlich aufsteigende Kette von Idealen
$$\langle r_1 \rangle \subset \langle r_2 \rangle \subset \langle r_3 \rangle \subset \ldots.$$
- Daher ist auch $I = \bigcup_{i \in \mathbb{N}} \langle r_i \rangle$ ein Ideal (Übungsaufgabe).
- Da R ein Hauptidealring ist, gilt $I = \langle r' \rangle$. Wegen $r' \in I$ folgt $r' \in \langle r_i \rangle$ für ein geeignetes i. Damit gilt $\langle r_i \rangle = \langle r_{i+1} \rangle = \ldots.$
- D.h. unsere Kette von Idealen stabilisiert (Widerspruch).

Hauptidealringe sind faktoriell.

Beweis: (Fortsetzung)

- **Jedes irreduzible Element ist prim:** Sei p irreduzibel.
- Es gelte $p \mid ab$ und $p \nmid a$. Wir müssen zeigen, dass $p \mid b$.
- Betrachte das Ideal $I = \langle p, a \rangle$. Da R Hauptidealring ist, gilt $I = \langle r \rangle$.
- Wegen $p \in \langle r \rangle$ gilt $p = rc$ und folglich $r \mid p$. Analog gilt $r \mid a$.
- Aus $p = rc$ und der Irreduzibilität von p folgt $r \in R^*$ oder $c \in R^*$.
- Für $c \in R^*$ sind p und r assoziiert, aber $p \nmid a$ und $r \mid a$. (Widerspruch)
- D.h. es muss $r \in R^*$ gelten. Es folgt $I = \langle p, a \rangle = \langle r \rangle = R$.
- Damit können wir jedes Element aus R als Linearkombination von p und a mit Koeffizienten aus R darstellen.
- Insbesondere existieren $x, y \in R$ mit $xp + ya = 1$.
- Multiplikation mit b und Verwendung von $ab = pc'$ liefert
$$xpb + yab = p(xb + yc') = b.$$
- Damit gilt $p \mid b$.

Beispiel: Primelemente in den Gaußschen Zahlen

Satz Primelemente in $\mathbb{Z}[i]$

Für die Primelemente $\pi \in \mathbb{Z}[i]$ gilt bis auf Assoziiertheit

1. $N(\pi) = p$ für ein $p \in \mathbb{P}$ oder
2. $\pi = p$ für ein $p \in \mathbb{P}$ mit $p \neq x^2 + y^2$ für $(x, y) \in \mathbb{Z}^2$.

Vorüberlegung notwendige Bedingung für die Primheit von π:

- Sei $\pi \in \mathbb{Z}[i]$ prim. Wegen $\pi\bar{\pi} = N(\pi)$ gilt $\pi \mid N(\pi)$.
- Sei $N(\pi) = p_1 \cdot \ldots \cdot p_n$ die Primzerlegung von $N(\pi)$.
- Da π prim ist, folgt $\pi | p$ für ein $p = p_i$. Sei also $\pi c = p$.
- Wegen $N(\pi) \cdot N(c) = p^2$ und $N(\pi) > 1$, muss gelten
$$N(\pi) = p \text{ oder } N(\pi) = p^2.$$

Beweis:

- **Fall 1** $N(\pi) = p$: Aus $\pi = ab$ folgt $N(\pi) = p = N(a) \cdot N(b)$.
- Damit ist entweder $N(a)$ oder $N(b)$ eine Einheit, π also irreduzibel.
- Da $\mathbb{Z}[i]$ faktoriell ist, muss π damit prim sein.

- **Fall 2** $N(\pi) = p^2$: Aus $\pi = ab$ folgt $N(\pi) = p^2 = N(a) \cdot N(b)$.
- Dies ist eine nicht-triviale Zerlegung für $a = x + iy$, falls
$$N(a) = p = x^2 + y^2.$$
- D.h. π ist reduzibel gdw $p = x^2 + y^2$ für ein $(x, y) \in \mathbb{Z}^2$.
- Für irreduzibles π mit $N(\pi) = p^2$ gilt $\pi = p$ bis auf Assoziiertheit.

Übung: Faktorisieren Sie 30 in $\mathbb{Z}[i]$ in Primelemente.

Satz Polynomring

Sei R ein faktorieller Ring. Dann ist auch der Polynomring $R[X]$ faktoriell.

(ohne Beweis)

Größte gemeinsame Teiler

Definition ggT

Sei R ein faktorieller Ring und $a, b \in R$, nicht beide 0. Ein Element c heißt $\mathrm{ggT}(a, b)$ – *größter gemeinsamer Teiler von a und b*– falls

$$c|a,\ c|b \text{ und für jeden Teiler } d \text{ von } a \text{ und } b \text{ gilt } d|c.$$

Falls $\mathrm{ggT}(a, b) = 1$, so heißen a, b *teilerfremd*. Wir definieren

$$\mathrm{ggT}(a_1, \ldots, a_n) = \mathrm{ggT}(a_1, \mathrm{ggT}(a_2, \ldots, \mathrm{ggT}(a_{n-1}, a_n))).$$

Einfache Eigenschaften

Lemma

Der ggT ist eindeutig bis auf Assoziiertheit.

Beweis:

- Seien $c = \mathrm{ggT}(a, b)$ und $c' = \mathrm{ggT}(a, b)$.
- Nach der Eigenschaft des ggT muss $c|c'$ und $c'|c$ gelten.
- D.h. $cd = c'$ und $c'd' = c$, woraus $cdd' = c$ folgt.
- Wir erhalten $dd' = 1$ bzw. $d, d' \in R^*$.
- Damit sind c und c' in R assoziiert.

Einfache Eigenschaften des ggT:

- Symmetrie: $\mathrm{ggT}(a, b) = \mathrm{ggT}(b, a)$
- Spezielle Elemente: $\mathrm{ggT}(a, 0) = a$ und $\mathrm{ggT}(a, 1) = 1$
- Multiplikativität: $\mathrm{ggT}(ca, cb) = c \cdot \mathrm{ggT}(a, b)$
- Teiler: $a|b \Leftrightarrow \mathrm{ggT}(a, b) = a$
- Teilbarkeit: $\mathrm{ggT}(a, b)|\mathrm{ggT}(a, bc)$
- Additivität: $\mathrm{ggT}(a, b) = \mathrm{ggT}(a, b + ca)$

Mehr Eigenschaften

Lemma ggT-Eigenschaften

Sei R ein faktorieller Ring und $a, b, c \in R$. Dann gilt

1. $\operatorname{ggT}(a, b) = 1 \Rightarrow \operatorname{ggT}(a^i, b^j) = 1$ für $i, j \in \mathbb{N}$
2. $a|bc$ und $\operatorname{ggT}(a, b) = 1 \Rightarrow a|c$
3. $\operatorname{ggT}(a, b) = 1 \Rightarrow \operatorname{ggT}(a, bc) = \operatorname{ggT}(a, c)$

Beweis:

(1) Annahme: $p|\operatorname{ggT}(a^i, b^j)$ für ein primes p.

- Da p prim ist, folgt $p|a$, $p|b$ und damit $p|\operatorname{ggT}(a, b)$. (Widerspruch)

(2) Betrachte die Primfaktorzerlegungen von a, b und c.

- Da $\operatorname{ggT}(a, b) = 1$, besitzen a und b keine gemeinsamen Faktoren.
- Wegen $a|bc$ müssen damit alle Faktoren von a in c enthalten sein.

(3) Nach Teilbarkeit gilt $\operatorname{ggT}(a, c)|\operatorname{ggT}(a, bc)$.

- Wir zeigen $\operatorname{ggT}(a, bc)|\operatorname{ggT}(a, c)$. Sei $d = \operatorname{ggT}(a, bc)$.
- Dann gilt $d|a$ und $d|bc$. Wegen $\operatorname{ggT}(a, b) = 1$ folgt $\operatorname{ggT}(d, b) = 1$.
- Mit (2) folgt $d|c$ und damit $d|\operatorname{ggT}(a, c)$.

Existenz und Eindeutigkeit des ggT

Satz Existenz und Eindeutigkeit des ggT

In einem faktoriellen Ring R mit $a, b \in R$, nicht beide 0, existiert $\operatorname{ggT}(a, b)$ und ist eindeutig bis auf Assoziiertheit.

Beweis: Die Eindeutigkeit wurde schon gezeigt.

- Falls $a = 0$ oder $b = 0$ ist die Existenz trivial. Seien also $a, b \neq 0$.
- Sei $P = \{p \in R \mid p \text{ taucht als Primfaktor von } a \text{ oder von } b \text{ auf}\}$.
- Wir schreiben die Primfaktorzerlegung von a und b in der Form
$$a = u \prod_{p \in P} p^{n_p},\ b = v \prod_{p \in P} p^{m_p} \text{ für } u, v \in R^*.$$
- Wir definieren $c = \prod_{p \in P} p^{\min\{n_p, m_p\}}$.
- Offenbar gilt $c|a$ und $c|b$, d.h. c ist gemeinsamer Teiler von a, b.
- Ferner ist jeder gemeinsamer Teiler von der Form
$$d = \prod_{p \in P} p^{k_p} \text{ mit } k_p \leq \min\{n_p, m_p\}.$$
- Damit folgt $d|c$ und c ist der größte gemeinsame Teiler von a, b.

Bsp: In $\mathbb{Z}$ gilt $93 = 3 \cdot 31$ und $42 = 2 \cdot 3 \cdot 7$, d.h. $\operatorname{ggT}(93, 42) = 3$.

ggT als Linearkombination

Lemma von Bézout

Sei R ein Hauptidealring und $a, b \in R$. Dann existieren $x, y \in R$ mit

$$xa + yb = \mathrm{ggT}(a, b).$$

Wir bezeichnen x, y als *Bézout-Koeffizienten* von a, b.

Beweis:

- Wir betrachten das Ideal $I = \langle a, b \rangle = \{xa + yb \mid x, y \in R\}$.
- Da R ein Hauptidealring ist, gilt $I = \langle c \rangle$.
- Behauptung: $c = \mathrm{ggT}(a, b)$.
- Wegen $a, b \in I$ gilt $a = ec$ und $b = e'c$. D.h. $c|a$ und $c|b$.
- Ist ferner d ein gemeinsamer Teiler von a und b, so teilt d jedes Element der Form $xa + yb$, d.h. jedes Element in I.
- Insbesondere gilt $d|c$, d.h. c muss der ggT sein.
- Da $c \in I = \{xa + yb \mid x, y \in R\}$ existieren $x, y \in R$ mit

$$xa + yb = c = \mathrm{ggT}(a, b).$$

Anmerkung:

(x, y) nicht eindeutig, $(x - kb, y + ka)$ erfüllt Gleichung für alle $k \in R$.

Euklidischer Algorithmus (um 300 v.Chr.)

Ziel: Berechne $\mathrm{ggT}(a, b)$ effizient, ohne Primfaktorzerlegung.

Szenario: Sei R ein euklidischer Ring mit Bewertungsfunktion $N(\cdot)$.

Algorithmus EUKLID

EINGABE: $a_0, a_1 \in R$ mit $N(a_0) \geq N(a_1)$

1. Setze $i := 1$.
2. While $(a_i \neq 0)$
    1. Berechne mittels euklidischer Division q_i, a_{i+1} mit
       $$a_{i-1} = q_i a_i + a_{i+1} \text{ und } N(a_{i+1}) < N(a_i) \text{ oder } a_{i+1} = 0.$$
    2. Setze $i := i + 1$.

AUSGABE: $a_{i-1} = \mathrm{ggT}(a_0, a_1)$

Korrektheit des Euklidischen Algorithmus

Satz Euklid

Bei Eingabe $a_0, a_1 \in R$ berechnet Algorithmus EUKLID $\mathrm{ggT}(a_0, a_1)$.

Beweis:

- Da die Bewertungsfunktion nur positive Werte annimmt und $N(a_1) > N(a_2) > \ldots$, muss EUKLID mit einem $a_k = 0$ terminieren.
- Für alle $0 < i < k$ gilt

$$\begin{aligned} \mathrm{ggT}(a_{i-1}, a_i) &= \mathrm{ggT}(q_i a_i + a_{i+1}, a_i) = \mathrm{ggT}(a_{i+1}, a_i) \\ &= \mathrm{ggT}(a_i, a_{i+1}). \end{aligned}$$

- Es folgt

$$\mathrm{ggT}(a_0, a_1) = \ldots = \mathrm{ggT}(a_{k-1}, a_k) = \mathrm{ggT}(a_{k-1}, 0) = a_{k-1}.$$

Übung: In $\mathbb{Z}$ kann $\mathrm{ggT}(a_0, a_1)$ in Zeit $\mathcal{O}(\log^2 N(a_0))$ berechnet werden.

Bsp. Euklidischer Algorithmus

Bsp: Berechne $\mathrm{ggT}(93, 42)$ mittels EUKLID.

$$\begin{array}{rcll} 93 & - & 2 \cdot 42 & = 9 \\ 42 & - & 4 \cdot 9 & = 6 \\ 9 & - & 1 \cdot 6 & = 3 \\ 6 & - & 2 \cdot 3 & = 0 \end{array}$$

- D.h. $\mathrm{ggT}(93, 42) = 3$.
- Durch Rücksubstitution erhalten wir die Bézout-Koeffizienten x, y mit $x \cdot 93 + y \cdot 42 = 3$.

$$\begin{array}{rcl} 3 & = & 9 - 1 \cdot 6 \\ & = & 9 - 1 \cdot (42 - 4 \cdot 9) = -42 + 5 \cdot 9 \\ & = & -42 + 5 \cdot (93 - 2 \cdot 42) = 5 \cdot 93 - 11 \cdot 42. \end{array}$$

Erweiterter Euklidischer Algorithmus (EEA)

Algorithmus Erweiterter Euklidischer Algorithmus (EEA)

EINGABE: a_0, a_1 mit $N(a_0) \geq N(a_1)$

1. Setze $i := 1$, $x_0 := 1$, $y_0 := 0$, $x_1 := 0$ und $y_1 := 1$.
2. While $(a_i \neq 0)$
    1. Berechne mittels euklidischer Division q_i, a_{i+1} mit
    $$a_{i-1} = q_i a_i + a_{i+1} \text{ und } N(a_{i+1}) < N(a_i) \text{ oder } a_{i+1} = 0.$$
    2. Setze $x_{i+1} := x_{i-1} - q_i x_i$.
    3. Setze $y_{i+1} := y_{i-1} - q_i y_i$.
    4. Setze $i := i + 1$.

AUSGABE: $a_{i-1}, x_{i-1}, y_{i-1}$ mit $a_{i-1} = \mathrm{ggT}(a_0, a_1) = x_{i-1} a_0 + y_{i-1} a_1$

Korrektheit von EEA

Satz Korrektheit von EEA

Bei Eingabe $a_0, a_1 \in R$ berechnet EEA $\mathrm{ggT}(a_0, a_1)$, x, y mit

$$x \cdot a_0 + y \cdot a_1 = \mathrm{ggT}(a_0, a_1).$$

Beweis:

- Der Algorithmus terminiert mit $a_k = 0$ und $a_{k-1} = \mathrm{ggT}(a_0, a_1)$.
- Wir beweisen per Induktion die Invariante
$$a_i = x_i \cdot a_0 + y_i \cdot a_1 \text{ für } 0 \leq i < k.$$
- Bei Terminierung gilt also
$$a_{k-1} = \mathrm{ggT}(a_0, a_1) = x_{k-1} a_0 + y_{k-1} a_1.$$
- IA für $i = 0$ und $i = 1$:
$$a_0 = x_0 a_0 + y_0 a_1 = 1 \cdot a_0 + 0 \cdot a_1 \text{ und } a_1 = 0 \cdot a_0 + 1 \cdot a_1.$$
- IS für $i \to i + 1$:
$$\begin{aligned} a_{i+1} &= a_{i-1} - q_i a_i \overset{\mathrm{IV}}{=} (x_{i-1} a_0 + y_{i-1} a_1) - q_i(x_i a_0 + y_i a_1) \\ &= (x_{i-1} - q_i x_i) a_0 + (y_{i-1} - q_{i+1} y_i) a_1 = x_{i+1} a_0 + y_{i+1} a_1 \end{aligned}$$

Bsp. EEA

Bsp: Wir berechnen wieder $\mathrm{ggT}(93, 42)$.

i	a_i	q_i	x_i	y_i
0	93	–	1	0
1	42	2	0	1
2	9	4	1	-2
3	6	1	-4	9
4	3	2	5	-11
5	0			

Damit gilt $\mathrm{ggT}(93, 42) = 3 = 5 \cdot 93 - 11 \cdot 42$.

kleinstes gemeinsames Vielfaches (kgV)

Definition kgV

Sei R ein faktorieller Ring und $a, b \in R \setminus \{0\}$. Dann ist das *kleinste gemeinsame Vielfache* $\mathrm{kgV}(a, b)$ von a und b definiert als ein

$c \in R$ mit $a|c$, $b|c$ und für jedes d, das von a und b geteilt wird, gilt $c|d$.

Satz Existenz kgV

Sei R ein faktorieller Ring und $a, b \in R \setminus \{0\}$. Dann existiert $\mathrm{kgV}(a, b)$ und ist eindeutig bis auf Assoziiertheit.

Beweis:

- **Eindeutigkeit:** Analog zu $\mathrm{ggT}(a, b)$.
- **Existenz:** Analog zu $\mathrm{ggT}(a, b)$ betrachte die Primzerlegung

$$a = u \prod_{p \in P} p^{n_p} \text{ und } b = v \prod_{p \in P} p^{m_p} \text{ für } u, v \in R^*.$$

- Es gilt $\mathrm{kgV}(a, b) = \prod_{p \in P} p^{\max\{n_p, m_p\}}$, denn jedes gemeinsame Vielfache von a, b ist von der Form $\prod_{p \in P} p^{k_p}$, $k_p \geq \max\{n_p, m_p\}$.

Zusammenhang ggT und kgV

Satz ggT und kgV

Sei R ein faktorieller Ring und $a, b \in R \setminus \{0\}$. Dann gilt

$$\operatorname{kgV}(a,b) = \frac{ab}{\operatorname{ggT}(a,b)} \qquad \text{(bis auf Assoziiertheit).}$$

Beweis:

- Schreibe wieder $a = u \prod_{p \in P} p^{n_p}$ und $b = v \prod_{p \in P} p^{m_p}$. Dann gilt

$$\begin{aligned} ab = uv \prod_{p \in P} p^{n_p + m_p} &= uv \prod_{p \in P} p^{\min\{n_p, m_p\} + \max\{n_p, m_p\}} \\ &= uv \cdot \operatorname{ggT}(a,b) \cdot \operatorname{kgV}(a,b). \end{aligned}$$

Kongruenzrechnung

Definition Kongruenz modulo n

Seien $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$. Wir sagen a ist *kongruent* zu b modulo n, falls $n \mid (a - b)$. Wir schreiben $a \equiv b \bmod n$.

Anmerkungen:

- Es gilt $a \equiv b \bmod n$ gdw $a = b + k \cdot n$ für ein $k \in \mathbb{Z}$.
- Sei $a = qn + r$ und $b = q'n + r$. Dann gilt
$$a - b = (q - q')n \text{ und damit } a \equiv b \bmod n.$$
- D.h. $a \equiv b$ gdw a, b lassen bei Division durch n denselben Rest.

Bsp:

- Es gilt $2 \equiv 7 \equiv (-3) \bmod 5$.
- a ist gerade gdw $a \equiv 0 \bmod 2$.

Repräsentanten-Unabhängigkeit

Satz Repräsentanten-Unabhängigkeit

Seien $a \equiv b \bmod n$ und $c \equiv d \bmod n$. Dann gilt

$$a + c \equiv b + d \bmod n \text{ und } ac \equiv bd \bmod n.$$

Beweis:

- Es gilt $a = b + kn$ und $c = d + \ell n$ für $k, \ell \in \mathbb{Z}$. Damit ist
$$a + c = b + d + (k + \ell)n\,.$$
- D.h. $a + c \equiv b + d \bmod n$.
- Analog gilt für die Multiplikation
$$ac = (b + kn)(d + \ell n) = bd + (kd + b\ell + k\ell n)n.$$
- Es folgt $ac \equiv bd \bmod n$.

Korollar

Für $a \equiv b \bmod n$ gilt $a^m \equiv b^m \bmod n$ für alle $m \in \mathbb{N}_0$.

Bsp. Repräsentanten-Unabhängigkeit

Bsp:

- Die letzte Dezimalstelle von 3^{100} ist
$$3^{100} = 9^{50} \equiv (-1)^{50} \equiv 1 \bmod 10.$$
- Sei $a = \sum_i a_i 10^i$ mit $a_i \in \{0, \ldots, 9\}$ die Dezimaldarstellung von a.
- Es gilt $a \equiv \sum_i a_i (1)^i = \sum_i a_i \bmod 3$.
- D.h. $3 \mid a$ gdw die Quersumme von a durch 3 teilbar ist.
- Analog gilt $a \equiv \sum_i a_i (-1)^i \bmod 11$. D.h. $11 \mid a$ gdw die alternierende Quersumme von a durch 11 teilbar ist.

Binomische Formel mod p

Lemma Binomische Formel mod p

Seien $a, b \in \mathbb{Z}$ und $p \in \mathbb{P}$. Dann gilt

$$(a+b)^p \equiv a^p + b^p \bmod p.$$

Beweis:

- Nach Binomischer Formel gilt
  $$(a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^i b^{p-i} = a^p + b^p + \sum_{i=1}^{p-1} \binom{p}{i} a^i b^{p-i}.$$
- Wir wollen zeigen, dass $p \mid \binom{p}{i}$ für $1 \leq i < p$. Daraus folgt
  $$(a+p)^p \equiv a^p + b^p \bmod p.$$
- Es gilt $\binom{p}{i} \cdot i! = \frac{p!}{(p-i)!} = \prod_{j=0}^{i-1}(p-j)$.
- Wegen $i \geq 1$ teilt p die rechte Seite der Gleichung.
- Da p die rechte Seite teilt, muss p auch die linke Seite teilen.
- Wegen $i < p$ und p prim gilt aber $p \nmid i!$. Damit folgt $p \mid \binom{p}{i}$.

Anmerkung: Die Abbildung $f : \mathbb{Z} \to \mathbb{Z}, x \mapsto x^p \bmod p$ ist linear, d.h.

$$f(a+b) \equiv f(a) + f(b) \bmod p\ .\ (f \text{ heißt } \textit{Frobenius}.)$$

Kleiner Satz von Fermat

Satz Kleiner Satz von Fermat

Sei $p \in \mathbb{P}$. Dann gilt

$$a^p \equiv a \bmod p \text{ für alle } a \in \mathbb{Z}.$$

Beweis:

- Wir führen zunächst eine Induktion für $a \geq 0$ durch.
- **IA** $a = 0$**:** $0^p \equiv 0 \bmod p$.
- **IS** $a \to a + 1$**:** Nach vorigem Lemma gilt
$$(a + 1)^p \equiv a^p + 1^p \equiv a + 1 \bmod p.$$
- Damit gilt der Satz für alle $a \in \mathbb{N}_0$.
- Für $a < 0$ gilt $(-a)^p \equiv -a \bmod p$ mit $-a > 0$.
- Für $p = 2$ ist $-a \equiv -a + 2a = a \bmod p$. Daraus folgt die Aussage.
- Für ungerades p folgt
$$-a \equiv (-a)^p = (-1)^p a^p = -a^p \bmod p.$$
- Multiplikation mit (-1) liefert die gewünschte Identität.

Kleiner Satz von Fermat

Korollar Kleiner Satz von Fermat (Variante)

Sei $p \in \mathbb{P}$. Dann gilt

$$a^{p-1} \equiv 1 \mod p \text{ für alle } a \in \mathbb{Z} \text{ mit } p \nmid a.$$

Beweis:

- Wir wissen $p \mid a^p - a$ bzw. $p \mid a(a^{p-1} - 1)$.
- Da p prim und $p \nmid a$ folgt $p \mid a^{p-1} - 1$ und damit $a^{p-1} \equiv 1 \mod p$.

Anwendung:

- Bei Rechnung modulo p reduziere Exponenten modulo $p - 1$.
- Modulo $p = 5$ gilt z.B.

$$2^{99} = 2^{3+96} = 2^3 \cdot (2^4)^{24} \equiv 2^3 \cdot 1^{24} = 2^3 \equiv 3 \mod 5.$$

Teiler und Vielfache

Lemma über Teiler und Vielfache

Für $a, b \in \mathbb{Z}$ und $n, m \in \mathbb{N}$ gilt:

1. Falls $a \equiv b \bmod n$ und $m|n$, dann ist $a \equiv b \bmod m$.
2. Es gilt $a \equiv b \bmod n$ gdw $ma \equiv mb \bmod mn$.

Beweis:

(1) Aus $n|a-b$ und $m|n$ folgt $m|a-b$.

(2) $\Rightarrow$: Aus $n|a-b$ folgt $mn|m(a-b)$.

$\Leftarrow$: Aus $nm|m(a-b)$ folgt $nmc = m(a-b)$ und damit $nc = a-b$.

Lösbarkeit linearer Gleichungen

Satz Lösbarkeit linearer Gleichungen

Seien $a, b \in \mathbb{Z}$ und $n \in \mathbb{N}$ mit $ax \equiv b \bmod n$. Sei $d = \mathrm{ggT}(a, n)$.

1. Falls eine Lösung $x \in \mathbb{Z}$ existiert, so gilt $d \mid b$.
2. Sei $d \mid b$. Seien $y, z \in \mathbb{Z}$ mit $ya + zn = \mathrm{ggT}(a, n) = d$.
   Ein $x \in \mathbb{Z}$ ist Lösung gdw
   $$x \equiv y\tfrac{b}{d} \bmod \tfrac{n}{d}.$$

Beweis:

(1) Sei x eine Lösung mit $ax \equiv b \bmod n$. Dann gilt $ax = b + kn$ bzw.
$$b = ax - kn.$$
$d = \mathrm{ggT}(a, n)$ teilt beide Summanden rechts. Damit gilt $d \mid b$.

(2) $\Leftarrow$: Sei $x \equiv y\frac{b}{d} \bmod \frac{n}{d}$, d.h. $x = y\frac{b}{d} + k\frac{n}{d}$. Es folgt
$$\begin{aligned} ax &= ay\tfrac{b}{d} + ak\tfrac{n}{d} = (d - zn)\tfrac{b}{d} + ak\tfrac{n}{d} \\ &= b + n(-z\tfrac{b}{d} + \tfrac{a}{d}k) \equiv b \bmod n \end{aligned}$$

- Wegen $ax \equiv b \bmod n$ ist x eine Lösung.

Lösbarkeit linearer Gleichungen

Beweis: (Fortsetzung)

$\Rightarrow$: Sei x eine Lösung mit $ax \equiv b \bmod n$. Dann gilt

$$yax = (d - nz)x \equiv dx \equiv yb \bmod n.$$

Aus der letzten Kongruenz folgt $x \equiv y\frac{b}{d} \bmod \frac{n}{d}$.

Anmerkung:

Für $\mathrm{ggT}(a, n) = 1$ existiert immer eine Lösung $x \equiv yb \bmod n$.

Bsp:

- Berechne die Lösungsmenge von $4x \equiv 2 \bmod 6$.
- Der Erw. Euklidische Algorithmus liefert $\mathrm{ggT}(4, 6) = -1 \cdot 4 + 6 = 2$.
- Damit gilt $x \equiv -\frac{2}{2} \equiv 2 \bmod 3$. D.h. die Lösungsmenge ist $2 + 3\mathbb{Z}$.

Lösung von simultanen Kongruenzen

Ziel:

- Bestimme alle Lösungen des Kongruenzensystems
$$\left| \begin{array}{ll} cx \equiv a & \mod n \\ dx \equiv b & \mod m \end{array} \right|$$
- Falls $c, d \neq 1$ löse nach x auf (voriger Satz). Ersetze n bzw. m.
- D.h. wir können oBdA annehmen, dass $c = d = 1$.

Satz Chinesischer Restsatz (CRT, Version 1)

Seien $a, b \in \mathbb{Z}$ und $n, m \in \mathbb{N}$. Sei $d = \mathrm{ggT}(n, m) = yn + zm,\ y, z \in \mathbb{Z}$.

1. Falls das System $\left| \begin{array}{ll} x \equiv a & \mod n \\ x \equiv b & \mod m \end{array} \right|$ lösbar ist, gilt $a \equiv b \mod d$.
2. Sei $a \equiv b \mod d$. Ein $x \in \mathbb{Z}$ ist eine Lösung gdw
$$x \equiv a - yn\frac{a-b}{d} \mod \frac{nm}{d}.$$

Beachte: Für teilerfremde n, m ist das System *immer* lösbar.

Chinesischer Restsatz

Beweis:

(1) Sei x eine Lösung mit $x \equiv a \bmod n$ und $x \equiv b \bmod m$.

Da $d \mid n$ und $d \mid m$ folgt $\left| \begin{array}{ll} x \equiv a & \bmod d \\ x \equiv b & \bmod d \end{array} \right|$. Damit gilt $a \equiv b \bmod d$.

(2) $\Leftarrow$: Sei $x \equiv a - yn\frac{a-b}{d} \bmod \frac{nm}{d}$.

- Wegen $d|n$ und $d|m$ können wir x modulo n und m betrachten.
- Modulo n gilt $x \equiv a - yn\frac{a-b}{d} \equiv a \bmod n$ und modulo m gilt $x \equiv a - yn\frac{a-b}{d} \equiv a - (d - zm)\frac{a-b}{d} \equiv a - (a-b) + zm\frac{a-b}{d} \equiv b \bmod m$.
- Damit ist x eine Lösung des simultanen Kongruenzensystems.

$\Rightarrow$: Seien x, x' Lösungen. Wir zeigen, dass dann $x \equiv x' \bmod \frac{nm}{d}$.

- Wegen $x \equiv a \equiv x' \bmod n$ und $x \equiv b \equiv x' \bmod m$ folgt $n \mid x - x'$ und $m \mid x - x'$. D.h. $x - x'$ ist gemeinsames Vielfaches von n und m.
- $\mathrm{kgV}(n, m)$ ist *kleinstes* gemeinsames Vielfaches von n und m, d.h.
$$\mathrm{kgV}(n, m) \mid x - x'.$$
- Wegen $\mathrm{kgV}(n, m) = \frac{nm}{\mathrm{ggT}(n,m)} = \frac{nm}{d}$ folgt $x \equiv x' \bmod \frac{nm}{d}$.

Chinesischer Restsatz

Bsp: Löse das folgende System simultaner Kongruenzen

$$\left| \begin{array}{ll} x \equiv 3 & \mod 6 \\ x \equiv 7 & \mod 10 \end{array} \right| .$$

- Es gilt $d = \mathrm{ggT}(6, 10) = -3 \cdot 6 + 2 \cdot 10 = 2$.
- Lösung existiert wegen $3 \equiv 7 \bmod 2$ und besitzt die Form
$$x \equiv 3 + 3 \cdot 6 \cdot \tfrac{3-7}{2} \equiv 3 + (-6) \equiv 27 \bmod 30.$$
- D.h. alle Lösungen sind von der Gestalt $27 + 30\mathbb{Z}$.

Chinesischer Restsatz für mehr Gleichungen

Satz Chinesischer Restsatz

Die Lösungsmenge des Systems von simultanen Kongruenzen

$$a_i x \equiv b_i \bmod n_i \quad \text{für } i = 1, \ldots, n$$

kann induktiv berechnet werden.

Beweis:

- Löse zunächst alle linearen Gleichungen nach x auf. Dies liefert
$$x \equiv c_i \bmod n'_i \quad \text{für } c_i \in \mathbb{Z}, n'_i \in \mathbb{N}.$$
- Löse mittels Chinesischem Restsatz die Kongruenzen
$$\left| \begin{array}{ll} x \equiv c_1 & \bmod n'_1 \\ x \equiv c_2 & \bmod n'_2 \end{array} \right| .$$
- Die Lösungen kombinieren wir mit $x \equiv c_3 \bmod n'_3$, usw.
- D.h. wir fassen jeweils zwei Kongruenzen zusammen, bis nur noch eine Kongruenz verbleibt.

Übung: Geben Sie eine explizite Formel für x falls $n = 3$.

Kongruenz ist Äquivalenzrelation

Lemma Kongruenz ist Äquivalenzrelation

Die Kongruenz modulo n ist eine Äquivalenzrelation auf $\mathbb{Z}$. D.h. für alle $a, b, c \in \mathbb{Z}$ gilt

1. **Reflexivität:** $a \equiv a \mod n$
2. **Symmetrie:** $a \equiv b \mod n \Rightarrow b \equiv a \mod n$.
3. **Transitivität:** $a \equiv b \mod n$ und $b \equiv c \mod n \Rightarrow a \equiv c \mod n$.

Beweis:

(1) Es gilt $n \mid a - a$, da jede Zahl die Null teilt.

(2) Aus $n|a - b$ folgt $n| - (a - b)$ bzw $n|b - a$.

(3) Aus $n|a - b$ und $n|b - c$ folgt $n|(a - b) + (b - c)$ bzw. $n|a - c$.

Die Restklassen $\mathbb{Z}/n\mathbb{Z}$

Definition Restklassen $\mathbb{Z}/n\mathbb{Z}$

Die vorigen Äquivalenzklassen heißen *Restklassenklassen modulo n*.
Wir definieren $\bar{a} := a + n\mathbb{Z} := \{a + kn \in \mathbb{Z} \mid k \in \mathbb{Z}\}$ für $a \in \mathbb{Z}$.
Ein Element $b \in \bar{a}$ heißt *Repräsentant* der Restklasse $\bar{a}$.
Die Mengen aller Restklassen modulo n bezeichnen wir mit

$$\mathbb{Z}/n\mathbb{Z} := \{a + n\mathbb{Z} \mid a \in \mathbb{Z}\}.$$

Bsp: $\mathbb{Z}/3\mathbb{Z} = \{0 + 3\mathbb{Z}, 1 + 3\mathbb{Z}, 2 + 3\mathbb{Z}\} = \{\bar{0}, \bar{1}, \bar{2}\} = \{\bar{0}, \bar{1}, \overline{-1}\}$

Definition Vollständiges Repräsentantensystem

$R \subseteq \mathbb{Z}$ heißt *vollständiges Repräsentantensystem* für $\mathbb{Z}/n\mathbb{Z}$ falls gilt

1. $\mathbb{Z}/n\mathbb{Z} = \{r + n\mathbb{Z} \mid r \in R\}$,
2. $r_1 + n\mathbb{Z} \neq r_2 + n\mathbb{Z}$ für verschiedene $r_1, r_2 \in R$.

Repräsentantensystem für $\mathbb{Z}/n\mathbb{Z}$

Lemma Repräsentantensystem für $\mathbb{Z}/n\mathbb{Z}$

$R = \{0, 1, \ldots, n-1\}$ ist ein vollständiges Repräsentantensystem für $\mathbb{Z}/n\mathbb{Z}$. Insbesondere ist $|\mathbb{Z}/n\mathbb{Z}| = n$.

Beweis:

(1) **Vollständigkeit:** Sei $\bar{a}$ eine beliebige Restklasse modulo n.
- Euklidische Division von a durch n liefert $a = qn + r$ mit $|r| < n$.
- Es gilt entweder $r \in R$ oder $r' := r + n \in R$. Ferner ist $\bar{a} = \bar{r} = \bar{r}'$.
- D.h. wir können $\bar{a}$ mittels eines Repräsentanten aus R darstellen.

(2) Annahme: $r_1 + n\mathbb{Z} = r_2 + n\mathbb{Z}$ für zwei verschiedene $r_1, r_2 \in R$.
- Dann gilt $r_1 - r_2 \equiv 0 \mod n$. Es gilt aber $-n < r_1 - r_2 < n$.
- Damit folgt $r_1 - r_2 = 0 \cdot n = 0$ bzw $r_1 = r_2$. (Widerspruch)

Da R ein vollständiges Repräsentantensystem für $\mathbb{Z}/n\mathbb{Z}$ ist, gilt

$$|\mathbb{Z}/n\mathbb{Z}| = |R| = n.$$

$\mathbb{Z}/n\mathbb{Z}$ besitzt Ringstruktur.

Satz $\mathbb{Z}/n\mathbb{Z}$ besitzt Ringstruktur.

$\mathbb{Z}/n\mathbb{Z}$ ist mit den wie folgt definierten Operationen ein Ring

$$\bar{a} + \bar{b} := \overline{a+b} \text{ und } \bar{a} \cdot \bar{b} := \overline{a \cdot b} \text{ für alle } a, b \in \mathbb{Z}.$$

Beweis:

- Die Repräsentantenunabhängigkeit der Addition und Multiplikation modulo n haben wir bereits auf Folie 46 gezeigt.
- Die Ringeigenschaften – wie neutrale Elemente und Distributivität – vererben sich von $\mathbb{Z}$ auf $\mathbb{Z}/n\mathbb{Z}$.

Bsp: Verknüpfungstafel für $\mathbb{Z}/4\mathbb{Z}$:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{0}$	$\bar{1}$	$\bar{2}$

$\cdot$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$
$\bar{2}$	$\bar{0}$	$\bar{2}$	$\bar{0}$	$\bar{2}$
$\bar{3}$	$\bar{0}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

Ringhomomorphismen

Lemma $\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$

Die Abbildung $f : \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}, x \mapsto x + n\mathbb{Z}$ ist ein Ringhomomorphismus.

Beweis:

- Es gilt $f(a+b) = \overline{a+b} = \bar{a} + \bar{b} = f(a) + f(b)$.
- Analog folgt $f(a \cdot b) = \overline{a \cdot b} = \bar{a} \cdot \bar{b} = f(a) \cdot f(b)$.
- Ferner ist $f(1) = 1 + n\mathbb{Z} = \bar{1}$ das neutrale Element in $\mathbb{Z}/n\mathbb{Z}$.

Lemma $\mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$

Seien $n, m \in \mathbb{N}$ mit $m|n$. Die Abbildung
$f : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}, x + n\mathbb{Z} \mapsto x + m\mathbb{Z}$ ist ein Ringhomomorphismus.

Beweis: Folgt aus dem Lemma über Teiler und Vielfache auf Folie 51.

CRT reloaded

Satz Chinesischer Restsatz (Version 2)

Seien $m, n \in \mathbb{N}$ teilerfremd. Dann ist die Abbildung

$$\begin{array}{rccc} \Phi: & \mathbb{Z}/nm\mathbb{Z} & \to & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} \\ & x + nm\mathbb{Z} & \mapsto & (x + n\mathbb{Z}, x + m\mathbb{Z}) \end{array}$$

ein Isomorphismus. Sei $xn + ym = 1$ für $x, y \in \mathbb{Z}$. Dann gilt

$$\begin{array}{rccc} \Phi^{-1}: & \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z} & \to & \mathbb{Z}/nm\mathbb{Z} \\ & (\bar{a}, \bar{b}) & \mapsto & \overline{a(1-xn) + b(1-ym)}. \end{array}$$

Beweis:

- Dass Φ ein Homomorphismus ist, folgt aus dem vorigen Lemma.
- Bleibt zu zeigen, dass Φ bijektiv ist. Es gilt
$$|\mathbb{Z}/nm\mathbb{Z}| = nm = |\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}|.$$
- Daher genügt es zu zeigen, dass Φ injektiv ist.
- Die 1.Version des CRT liefert aber gerade, dass jedes $(\bar{a}, \bar{b}) \in \mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$ genau eine Lösung $\bar{x} \in \mathbb{Z}/nm\mathbb{Z}$ besitzt.

2. Variante des CRT

Beweis: (Fortsetzung)

- Wir wollen noch die explizite Formel für Φ^{-1} herleiten.
- Nach Lemma von Bézout existieren $x, y \in \mathbb{Z}$ mit $xn + ym = 1$.
- Es gilt

$$\Phi(\overline{1-xn}) = (\overline{1-xn}, \overline{1-xn}) = (\bar{1}, \overline{ym}) = (\bar{1}, \bar{0}) \text{ und}$$

$$\Phi(\overline{1-ym}) = (\overline{1-ym}, \overline{1-ym}) = (\overline{xn}, \bar{1}) = (\bar{0}, \bar{1}).$$

- Aus der Linearität des Ringhomomorphismus folgt

$$\Phi(\overline{a(1-xn)+b(1-ym)}) = \Phi(\bar{a})\Phi(\overline{1-xn}) + \Phi(\bar{b})\Phi(\overline{1-ym}) = (\bar{a}, \bar{b}).$$

- Anwendung von Φ^{-1} auf beide Seiten liefert die Formel.

Korollar

Seien $n_1, \ldots, n_k \in \mathbb{N}$ paarweise teilerfremd. Dann gilt

$$\mathbb{Z}/n_1 \ldots n_k\mathbb{Z} \simeq \mathbb{Z}/n_1\mathbb{Z} \times \ldots \times \mathbb{Z}/n_k\mathbb{Z}.$$

Beweis: Folgt induktiv aus vorigem Satz für $n = n_1 \ldots n_{k-1}$, $m = n_k$.

Die Einheitengruppe U_n

Definition Einheitengruppe U_n

Wir bezeichnen die Einheiten von $\mathbb{Z}/n\mathbb{Z}$ als

$$U_n := (\mathbb{Z}/n\mathbb{Z})^* = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \bar{a} | \bar{1}\}.$$

Satz Struktur der Einheitengruppe U_n

Es gilt $U_n = \{a + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z} \mid \mathrm{ggT}(a, n) = 1\}$. Ferner ist $(U_n, \cdot)$ eine Gruppe.

Beweis:

- $\bar{a} \in \mathbb{Z}/n\mathbb{Z}$ ist eine Einheit falls $\bar{a}\bar{x} = \bar{1}$ für ein $\bar{x} \in \mathbb{Z}/n\mathbb{Z}$.
- Dies ist äquivalent mit $ax \equiv 1 \mod n$. Nach Folie 52 existiert eine Lösung für x gdw $\mathrm{ggT}(a, n) | 1$, d.h. $\mathrm{ggT}(a, n) = 1$.
- Nach Definition von U_n besitzen also alle Elemente ein Inverses.

Die Eulersche φ-Funktion

Bsp: $U_{12} = \{\bar{1}, \bar{5}, \bar{7}, \overline{11}\}$ und $U_p = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$ für $p \in \mathbb{P}$.

Definition Eulersche φ-Funktion

Die *Eulersche φ-Funktion* ist definiert als

$$\varphi : \mathbb{N} \to \mathbb{N} \text{ mit } n \mapsto |U_n|.$$

Bsp: $\varphi(12) = 4$ und $\varphi(p) = p - 1$ für $p \in \mathbb{P}$.

Eulersche φ-Funktion für Primpotenzen

Lemma Eulersche φ-Funktion für Primpotenzen

Sei $p \in \mathbb{P}$ und $r \in \mathbb{N}$. Dann gilt

$$\varphi(p^r) = p^{r-1}(p-1).$$

Beweis:

- Es gilt $$\begin{aligned} U_{p^r} &= \{a + p^r\mathbb{Z} \in \mathbb{Z}/p^r\mathbb{Z} \mid \mathrm{ggT}(a, p^r) = 1\} \\ &= \mathbb{Z}/p^r\mathbb{Z} \setminus \{a + p^r\mathbb{Z} \in \mathbb{Z}/p^r\mathbb{Z} \mid \mathrm{ggT}(a, p^r) > 1\}. \end{aligned}$$
- Wir stellen $\mathbb{Z}/p^r\mathbb{Z}$ mittels der Repräsentanten $0, 1, \ldots, p^r - 1$ dar.
- Folgende p^{r-1} Repräsentanten besitzen nicht-triviale ggTs mit p^r: $$0, p, 2p, \ldots, (p^{r-1} - 1)p\,.$$
- Damit gilt $$\begin{aligned} \varphi(p^r) = |U_{p^r}| &= |\mathbb{Z}/p^r\mathbb{Z}| - |\{a + p^r\mathbb{Z} \in \mathbb{Z}/p^r\mathbb{Z} \mid \mathrm{ggT}(a, p^r) > 1\}| \\ &= p^r - p^{r-1} = p^{r-1}(p-1). \end{aligned}$$

Eulersche φ-Funktion

Lemma Eulersche φ-Funktion für teilerfremde Zahlen

Seien $n, m \in \mathbb{N}$ teilerfremd. Dann gilt

$$U_{nm} \cong U_n \times U_m \text{ und } \varphi(nm) = \varphi(n) \cdot \varphi(m).$$

Beweis: Nach Chinesischem Restsatz gilt

$$\begin{aligned} U_{nm} = (\mathbb{Z}/nm\mathbb{Z})^* &\cong (\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z})^* \\ &= (\mathbb{Z}/n\mathbb{Z})^* \times (\mathbb{Z}/m\mathbb{Z})^* = U_n \times U_m. \end{aligned}$$

Es folgt $\varphi(nm) = |U_{nm}| = |U_n \times U_m| = |U_n| \cdot |U_m| = \varphi(n) \cdot \varphi(m)$.

Satz Eulersche φ-Funktion

Sei $n \in \mathbb{N}$ mit Primfaktorzerlegung $n = \prod_{i=1}^{s} p_i^{r_i}$. Dann gilt

$$\varphi(n) = \prod_{i=1}^{s} p_i^{r_i - 1}(p_i - 1).$$

Beweis: Nach den vorigen beiden Lemmata gilt

$$\varphi(n) = \prod_{i=1}^{s} \varphi(p_i^{r_i}) = \prod_{i=1}^{s} p_i^{r_i - 1}(p_i - 1).$$

Satz von Euler

Satz von Euler

Sei $(G, \cdot)$ eine endl. abelsche Gruppe. Dann gilt $a^{|G|} = 1$ für alle $a \in G$.

Beweis:

- Sei $G = \{g_1, \ldots, g_n\}$ und $a \in G$. Betrachte die Abbildung
$$f : G \to G, g \mapsto ag.$$
- Da $a \in G$, besitzt a ein Inverses. D.h. f ist eine Bijektion auf G.
- Damit gilt $\{g_1, \ldots, g_n\} = \{f(g_1), \ldots, f(g_n)\} = \{ag_1, \ldots, ag_n\}$.
- Es folgt $\prod_{i=1}^n g_i = \prod_{i=1}^n ag_i = a^n \prod_{i=1}^n g_i$.
- Kürzen von $\prod_{i=1}^n g_i$ liefert $a^n = a^{|G|} = 1$.

Korollar 1

Sei $n \in \mathbb{N}$. Für alle $\bar{a} \in U_n$ gilt $\bar{a}^{|U_n|} = \bar{a}^{\varphi(n)} = \bar{1}$.

Korollar 2 Kleiner Fermat

Sei $p \in \mathbb{P}$. Für alle $\bar{a} \in U_p$ gilt $\bar{a}^{|U_p|} = \bar{a}^{p-1} = \bar{1}$.

Satz von Lagrange

Definition Gruppen-Notation

Sei $(G, \cdot)$ eine endliche abelsche Gruppe. Sei $a \in G$. Wir definieren

1. $\mathrm{ord}(a) = \min\{i \in \mathbb{N} \mid a^i = 1\}$ ist die *Ordnung von a*.
2. $H \subseteq G$ ist *Untergruppe* von G, falls $(H, \cdot)$ eine Gruppe ist.
3. $\langle a \rangle = \{a, a^2, \ldots, a^{\mathrm{ord}(g)}\}$ ist die von a erzeugte Untergruppe.

Bsp: In U_7 gilt $\langle \bar{2} \rangle = \{\bar{2}, \bar{4}, \bar{1}\}$.

Satz von Lagrange

Sei $(G, \cdot)$ eine endl. abelsche Gruppe. Für alle $a \in G$ gilt $\mathrm{ord}(a) \mid |G|$.

Beweis:

- Annahme: $\mathrm{ord}(a) \nmid |G|$. Dann liefert Euklidische Division
$$|G| = q \cdot \mathrm{ord}(a) + r \text{ mit } 0 < r < \mathrm{ord}(a).$$
- Nach Satz von Euler gilt
$$1 = a^{|G|} = a^{q \cdot \mathrm{ord}(a) + r} = (a^{\mathrm{ord}(a)})^q \cdot a^r = 1^q \cdot a^r = a^r.$$
- D.h. $a^r = 1$, $r < \mathrm{ord}(a)$. (Widerspruch zur Minimalität von $\mathrm{ord}(a)$)

Diffie-Hellman Schlüsselaustausch

Ziel:

Austausch eines *geheimen* Schlüssels über einen *öffentlichen* Kanal.

Definiere die Funktion $\exp_{\bar{g}} : \mathbb{Z}/(p-1)\mathbb{Z} \to U_p$, $\bar{a} \mapsto \bar{g}^{\bar{a}} = \bar{g}^a$

Protokoll Diffie-Hellman Schlüsselaustausch (1976)

öffentliche Parameter: $p \in \mathbb{P}$ und $\bar{g} \in U_p$ mit $\langle \bar{g} \rangle = U_p$

1. Alice wählt $a \in \mathbb{Z}/(p-1)\mathbb{Z}$ und sendet $\exp_{\bar{g}}(a) = \bar{g}^a$ an Bob.
2. Bob wählt $b \in \mathbb{Z}/(p-1)\mathbb{Z}$ und sendet $\exp_{\bar{g}}(b) = \bar{g}^b$ an Alice.
3. Alice berechnet $\exp_{\bar{g}^b}(a) = \bar{g}^{ab}$, Bob berechnet $\exp_{\bar{g}^a}(b) = \bar{g}^{ab}$.

gemeinsamer Schlüssel: $\bar{g}^{ab}$

Sicherheit:

- Ein Angreifer muss aus $p, \bar{g}, \bar{g}^a, \bar{g}^b$ den Wert $\bar{g}^{ab}$ berechnen.
- Dies kann auf das *Diskrete Logarithmus Problem* zurückgeführt werden: Berechne a aus $p, \bar{g}, \bar{g}^a$.
- *Vermutung:* $\exp_g(\cdot)$ ist eine sogenannte *Einwegfunktion*, d.h. leicht zu berechnen, aber schwer zu invertieren.

Das RSA-Kryptosystem

Ziel: Public-Key Kryptographie, d.h. Verschlüsselung ohne vorherigen Austausch eines geheimen Schlüssels.

Protokoll RSA Public Key Verschlüsselung (1977)

1. **Schlüsselgenerierung** von Alice: Wähle $p, q \in \mathbb{P}$ und berechne $N = pq$ und $\varphi(N)$. Wähle $e \in U_{\varphi(N)}$. Berechne $d \in U_{\varphi(N)}$ mit $ed \equiv 1 \bmod \varphi(N)$. Veröffentliche (N, e), d bleibt geheim.
2. **Verschlüsselung** von Bob: Für ein $\bar{m} \in \mathbb{Z}/N\mathbb{Z}$ berechne
$$\mathrm{Enc}_{N,e} : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z},\ \bar{m} \mapsto \bar{m}^e.$$
3. **Entschlüsselung** durch Alice: Für ein $\bar{c} = \bar{m}^e \in \mathbb{Z}/N\mathbb{Z}$ berechne
$$\mathrm{Dec}_{N,d} : \mathbb{Z}/N\mathbb{Z} \to \mathbb{Z}/N\mathbb{Z},\ \bar{c} \mapsto \bar{c}^d.$$

Korrektheit:

- Nach Satz von Euler gilt für alle $\bar{m} \in U_N$
$$\mathrm{Dec}_{N,d}(\mathrm{Enc}_{N,e}(\bar{m})) = (\bar{m}^e)^d = \bar{m}^{1+k\varphi(N)} = \bar{m} \cdot (\bar{m}^{\varphi(N)})^k = \bar{m}.$$
- **Übung:** Zeigen Sie die Korrektheit für $\bar{m} \in (\mathbb{Z}/N\mathbb{Z}) \setminus U_N$.

Sicherheit von RSA

Sicherheit von RSA:

- Kann man $N = pq$ faktorisieren, so kann man entschlüsseln.
- Berechnung von $\varphi(N)$ ist so schwer wie die Faktorisierung von N.
- Sei $\varphi(N) = (p-1)(q-1) = N - p - q + 1$ bekannt.
- Dann sind auch die Koeffizienten folgenden Polynoms bekannt
$$(x-p)(x-q) = x^2 - (p+q)x + N.$$
- Dessen Nullstellen p, q können effizient bestimmt werden (z.B. mittels Newton-Iteration).
- Damit erhält man die Faktorisierung von N.
- Das Berechnen von d ist so schwer wie Faktorisieren (nicht trivial).
- **Offenes Problem:**
Ist das Invertieren von $\bar{m} \mapsto \bar{m}^e$ so schwer wie Faktorisieren?

Endliche Körper

Satz Endliche Körper

Sei $p \in \mathbb{N}$. $\mathbb{Z}/p\mathbb{Z}$ ist ein Körper gdw $p \in \mathbb{P}$.

Beweis:

- $(\mathbb{Z}/p\mathbb{Z}, +)$ ist eine abelsche Gruppe. Kommutativität der Multiplikation und Distributivität vererben sich von $\mathbb{Z}$ auf $\mathbb{Z}/p\mathbb{Z}$.

$\Leftarrow$: Sei p prim. Dann gilt $\mathrm{ggT}(a, p)$ für alle $a \in \mathbb{Z}$ mit $p \nmid a$.

- Damit ist $U_p = \mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}$, d.h. $(\mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}, \cdot)$ ist eine Gruppe.

$\Rightarrow$: Sei $p = a \cdot b$ mit $1 < a, b < p$.

- Dann ist $(\mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}, \cdot)$ nicht abgeschlossen, da
$$\bar{a} \cdot \bar{b} = \bar{p} = \bar{0}, \text{ aber } \bar{a}, \bar{b} \neq \bar{0}.$$
- Damit ist $(\mathbb{Z}/p\mathbb{Z} \setminus \{\bar{0}\}, \cdot)$ keine Gruppe.

Endliche Körper $\mathbb{F}_p$

Definition Endliche Körper

Sei $p \in \mathbb{P}$. Wir bezeichnen den endlichen Körper $\mathbb{Z}/p\mathbb{Z}$ mit

$$\mathbb{F}_p \text{ bzw. } GF(p).$$

Bsp:

- In $\mathbb{F}_5$ gilt $\frac{\bar{3}}{\bar{2}} + \bar{1} = \bar{3} \cdot \overline{2^{-1}} + \bar{1} = \bar{3} \cdot \bar{3} + \bar{1} = \bar{0}$.
- In $\mathbb{F}_7$ gilt $\frac{\bar{3}}{\bar{2}} + \bar{1} = \bar{3} \cdot \overline{2^{-1}} + \bar{1} = \bar{3} \cdot \bar{4} + \bar{1} = \overline{-1}$.

Mehr endliche Körper

Ziel: Konstruktion von Körpern mit p^r Elementen für $r \geq 2$.

- Wir betrachten den Polynomring $\mathbb{F}_p[X]$ mit Koeffizienten aus $\mathbb{F}_p$.
- Aus den Übungen wissen wir, dass $\mathbb{F}_p[X]$ euklidisch ist mit der Gradfunktion $\deg(\cdot)$ als Bewertungsfunktion.
- Damit ist $\mathbb{F}_p[X]$ ein Hauptidealring und faktoriell.
- Für die Einheiten von $\mathbb{F}_p[X]$ gilt
$$(\mathbb{F}_p[X])^* = \{f \in \mathbb{F}_p[X] \mid \deg(f) = 0\}.$$
- Ein $f \in \mathbb{F}_p[X]$ heißt damit irreduzibel (bzw. prim), falls
$$f = rs \Rightarrow \deg(r) = 0 \text{ oder } \deg(s) = 0.$$

Mehr endliche Körper

- Setze $R_p := \mathbb{F}_p[X]$. Für $f, g, h \in \mathbb{F}_p[X]$ definieren wir
$$f \equiv g \bmod h \Leftrightarrow h | f - g.$$
- Die Äquivalenzklassen dieser Relation besitzen die Form
$$\bar{f} = f + R_p h = \{f + k \cdot h \mid k \in R_p\}.$$
- Die Menge aller Restklassen bezeichnen wir mit
$$R_p/h = \mathbb{F}_p[X]/h = \{f + k \cdot q \mid f \in \mathbb{F}_p[X]\}.$$
- Sei $\deg(q) = r$. Ein vollst. Repräsentantensystem für $\mathbb{F}_p[X]/h$ ist
$$R = \{f_0 + f_1 X + \ldots f_{r-1} X^{r-1} \in \mathbb{Z}[X] \mid f_i \in \{0, \ldots, p-1\}.\}$$
- Insbesondere gilt $|\mathbb{F}_p[X]/h| = |R| = p^r$.
- Ferner ist $\mathbb{F}_p[X]/h$ ein Körper gdw h irreduzibel ist über $\mathbb{F}_p$.
- Da für jedes p, r ein über $\mathbb{F}_p$ irreduzibles h mit $\deg(h) = r$ existiert, existiert stets ein Körper $\mathbb{F}_{p^r}$ mit p^r Elementen.

- **Warnung:** $\mathbb{F}_{p^r}$ ist nicht isomorph zu $\mathbb{Z}/p^r\mathbb{Z}$ (letzterer ist kein Körper).

Beispiel $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3+X+1)$

Bsp: Wir konstruieren einen Körper $\mathbb{F}_8 = \mathbb{F}_{2^3}$.

- Das Polynom $h = X^3 + X + 1$ ist irreduzibel über $\mathbb{F}_2$, da es weder 0 noch 1 als Nullstelle besitzt, d.h. kein Linearfaktor teilt h.
- Damit erhalten wir $\mathbb{F}_8 = \mathbb{F}_2[X]/(X^3+X+1)$. D.h. in $\mathbb{F}_8$ gilt
  $$X^3 + X + 1 \equiv 0 \bmod 2 \text{ bzw. } X^3 \equiv -X - 1 \equiv X + 1 \bmod 2.$$
- Wir bestimmen $(X+1)^{-1}$ in $\mathbb{F}_8$. D.h. wir bestimmen $a, b, c \in \mathbb{F}_2$ mit $(X+1)(aX^2+bX+c) \equiv 1 \Leftrightarrow a(X+1)+bX^2+cX+aX^2+bX+c \equiv 1$.
- Koeffizientenvergleich liefert
  $$\left| \begin{array}{cc} a+b & \equiv 0 \\ a+b+c & \equiv 0 \\ a+c & \equiv 1 \end{array} \right| \text{ bzw. } a \equiv 1,\ b \equiv 1 \text{ und } c \equiv 0.$$
- Test: $(X+1)(X^2+X) \equiv X^3 + 2X^2 + X \equiv 2X^2 + 2X + 1 \equiv 1$.

Hinweis: Verschiedene irreduzible h liefern isomorphe Körper.

Satz von Wilson

Satz von Wilson

Eine Zahl $p \in \mathbb{N}$ ist prim gdw $(p-1)! \equiv (-1) \bmod p$.

Beweis:

$\Leftarrow$ Sei $p = ab$ mit $1 < a, b < p$.

- Fall 1 ($a \neq b$): Es gilt $ab|(p-1)!$ und daher $(p-1)! \equiv 0 \bmod p$.
- Fall 2 ($p = 4$:) Es gilt $3! \equiv 2 \bmod 4$.
- Fall 3 ($p = a^2$ mit $a > 2$:) Wegen $2a < p$ gilt $a \cdot 2a|(p-1)!$.
- Damit folgt $(p-1)! \equiv 0 \bmod 2a^2$ bzw. $(p-1)! \equiv 0 \bmod p$.

$\Rightarrow$ Sei $p \in \mathbb{P}$. Dann ist $\mathbb{F}_p$ ein Körper.

- D.h. jedes $\bar{a} \in \mathbb{F}_p \setminus \{\bar{0}\}$ besitzt ein Inverses $\bar{a}^{-1} \in \mathbb{F}_p \setminus \{\bar{0}\}$.
- Nur $\bar{1}$ und $\overline{-1} = \overline{p-1}$ sind selbstinvers, da $X^2 - 1$ über einem Körper nur maximal zwei Nullstellen besitzen kann.
- D.h. im Produkt $(p-1)!$ in $\mathbb{F}_p$ sind außer $1, p-1$ je zwei Elemente paarweise 1. Damit folgt $(p-1)! \equiv p-1 \equiv (-1) \bmod p$.

Erzeuger von Gruppen

Definition Erzeuger

Sei G eine Gruppe und $S \subseteq G$.

1. Wir bezeichnen mit $\langle S \rangle$ die von S *erzeugte* Untergruppe, d.h. die kleinste Untergruppe von G, die S enthält.
   Die Elemente von S heißen Erzeuger von $\langle S \rangle$.
2. G heißt *zyklisch*, falls $G = \langle g \rangle$ für ein $g \in G$.
3. G heißt *endlich erzeugt*, falls $G = \langle S \rangle$ für ein endliches S.

Bsp:

- $G = (\mathbb{Z}, +)$, $S = \{12, 21\}$, $\langle S \rangle = \langle 3 \rangle = 3\mathbb{Z}$.
- $(\mathbb{Z}, +) = \langle 1 \rangle = \langle -a \rangle$
- $(\mathbb{Z}/n\mathbb{Z}, +) = \langle \bar{1} \rangle = \langle \bar{a} \rangle$ für alle a mit $\mathrm{ggT}(a, n) = 1$.

Lemma *G* besitzt $\mathbb{Z}$-Modulstruktur

Sei $(G, +)$ eine abelsche Gruppe und $g \in G$, $n \in \mathbb{N}_0$. Dann ist G zusammen mit folgender Skalarmultiplikation ein $\mathbb{Z}$-Modul:

$$n \cdot g := \underbrace{g + \ldots + g}_{n-mal},\ 0g := 0 \text{ und } (-n)g := -(ng).$$

Beweis:

- Offenbar gilt für alle $r, s \in \mathbb{N}_0$
$$1 \cdot g = g,\ r(sg) = (rs)g \text{ und } (r+s)g = rg + sg.$$
- Aus der Kommutativität von G folgt für $g, g' \in G$ und $r \in \mathbb{N}_0$
$$r(g + g') = \underbrace{g + g' + \ldots + g + g'}_{r-\mathrm{mal}} = rg + rg'.$$

Erzeugung aus endlichen Mengen

Lemma Erzeugung aus endlichen Mengen

Sei $(G, +)$ eine abelsche Gruppe und $S \subseteq G$. Dann gilt

$$\langle S \rangle = \left\{ \sum_{g \in S'} n_g g \mid S' \subseteq S \text{ endlich}, n_g \in \mathbb{Z} \right\}.$$

Beweis:

$\supseteq$ Es gilt $g \in S' \subseteq S \subseteq \langle S \rangle$.

- Mit der $\mathbb{Z}$-Modulstruktur und Abgeschlossenheit von $\langle S \rangle$ sind auch
$$n_g g \in \langle S \rangle \text{ und } \sum_{g \in S'} n_g g \in \langle S \rangle.$$

$\subseteq$ Die linke Seite ist die kleinste Untergruppe, die S enthält.

- Wir bezeichnen die Menge auf der rechten Seite mit H.
- Da $S \subseteq H$, folgt $\langle S \rangle \subseteq H$, wenn H eine Untergruppe ist.
- Abgeschlossenheit: Seien $h = \sum_{g \in S'} n_g g$ und $h' = \sum_{g \in S''} n'_g g$.
- Wir schreiben $h = \sum_{g \in S' \cup S''} n_g g$ mit $n_g = 0$ für $g \in S'' \setminus S'$.
- Analog ist $h' = \sum_{g \in S' \cup S''} n'_g g$ mit $n'_g = 0$ für $g \in S' \setminus S''$.
- Dann gilt $h - h' = \sum_{g \in S' \cup S''} (n_g - n'_g) g \subseteq H$.

Zyklische Gruppen

Lemma

Sei $(G, +)$ eine Gruppe. Dann gilt $\langle g \rangle = \{ng \mid n \in \mathbb{Z}\}$ für alle $g \in G$.

Beweis:

- Wie zuvor mit $S' = S = \{g\}$ als einziger nichtleerer Teilmenge.
- Kommutativität wird nicht benötigt, da nur g aufsummiert wird.

Satz zyklisch $\Rightarrow$ abelsch

Jede zyklische Gruppe G ist abelsch.

Beweis:

- Sei $G = \langle g \rangle = \{ng \mid n \in \mathbb{Z}\}$ für einen Erzeuger $g \in G$.
- Kommutativität folgt aus

$$ng + mg = (n + m)g = (m + n)g = mg + ng.$$

Isomorphiesatz

Satz Isomorphiesatz für zyklische Gruppen

Jede zyklische Gruppe ist isomorph zu $\mathbb{Z}$ oder $\mathbb{Z}/n\mathbb{Z}$ für ein $n \in \mathbb{N}$.

Beweis:

- Wir betrachten den Gruppenhomorphismus
$$\Phi : \mathbb{Z} \to G, m \mapsto mg.$$
- Der Kern $\mathrm{Ker}(\Phi) \subseteq \mathbb{Z}$ ist ein Ideal, denn $0 \in \mathrm{Ker}(\Phi)$ und für $a, b \in \mathrm{Ker}(\Phi)$ gilt $a + b \in \mathrm{Ker}(\Phi)$ und $ma \in \mathrm{Ker}(\Phi)$ für $m \in \mathbb{Z}$.
- Da $\mathbb{Z}$ ein Hauptidealring ist, gilt $\mathrm{Ker}(\Phi) = n\mathbb{Z}$ für ein $n \geq 0$.
- Nach Homomorphiesatz gilt für einen Homomorphismus $f : A \to B$
$$\mathrm{Im}(f) \cong A/\mathrm{Ker}(f).$$
- D.h. $G \cong \mathbb{Z}$ für $n = 0$ bzw. $G \cong \mathbb{Z}/n\mathbb{Z}$ für $n \geq 1$.

Erzeuger besitzen Ordnung G.

Lemma Ordnung eines Erzeugers

Sei $(G, +)$ eine endliche zyklische Gruppe. Für ein $g \in G$ gilt

$$G = \langle g \rangle \ \text{ gdw } \ \mathrm{ord}(g) = |G|.$$

Beweis:

$\Rightarrow$ Sei $G = \langle g \rangle = \{g, 2g, \ldots, \mathrm{ord}(G)g\}$.

- z.z.: Alle Elemente in $\{g, 2g, \ldots, \mathrm{ord}(G)g\}$ sind verschieden.
- Annahme: $ig = jg$ für $1 \leq i < j \leq \mathrm{ord}(G)$.
- Dann gilt $(j - i)g = 1$ mit $0 < j - i < \mathrm{ord}(G)$. (Widerspruch)
- Damit gilt $|G| = |\{g, 2g, \ldots, \mathrm{ord}(G)g\}| = \mathrm{ord}(g)$.

$\Leftarrow$ Sei $\mathrm{ord}(g) = |G|$.

- In $\langle g \rangle = \{g, 2g, \ldots, \mathrm{ord}(G)g\}$ sind je zwei Elemente verschieden.
- Da $|\langle g \rangle| = |G|$, muss $\langle g \rangle$ alle Elemente aus G enthalten.

Darstellung von Gruppen

Definition Darstellung von Gruppen

Sei G eine endlich erzeugte abelsche Gruppe mit Erzeugern $S = (g_1, \dots, g_k) \in G^k$. Elemente des Kerns von

$$\varphi_S : \mathbb{Z}^k \to G, (m_1, \dots, m_k) \mapsto \sum_{i=1}^k m_i g_i$$

heißen *Relationen von S*. Sei $\mathrm{Ker}(\varphi_S)$ erzeugt von $r_1, \dots, r_\ell$. Sei R eine Matrix mit Spaltenvektoren r_i, d.h. $R : \mathbb{Z}^\ell \to \mathbb{Z}^k$. Dann heißt

$$\mathbb{Z}^\ell \xrightarrow{R} \mathbb{Z}^k \xrightarrow{S} G$$

eine *Präsentation* oder *Darstellung* der Gruppe G.

Anmerkungen:

- Es gilt $\mathrm{Ker}(\varphi_S) = \mathrm{Im}(R)$. Aus dem Homomorphiesatz folgt
$$G \cong \mathbb{Z}^k/\mathrm{Ker}(\varphi_S) = \mathbb{Z}^k/\mathrm{Im}(R).$$
- D.h. man kann den Isomorphietyp von G an der Matrix R ablesen.
- Wir müssen noch zeigen, dass $\mathrm{Ker}(\varphi_S)$ endlich erzeugt ist.

Bsp. Darstellung von Gruppen

Bsp: Darstellung von Gruppen

- Für ein zyklisches G mit $G \cong \mathbb{Z}$ erhalten wir die Darstellung
$$0 \to \mathbb{Z} \xrightarrow{1} \mathbb{Z}.$$
- Für ein zyklisches G mit $G \cong \mathbb{Z}/n\mathbb{Z}$ erhalten wir die Darstellung
$$\mathbb{Z} \xrightarrow{(n)} \mathbb{Z} \xrightarrow{(\bar{1})} \mathbb{Z}/n\mathbb{Z}.$$
- $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ können wir darstellen als
$$\mathbb{Z}^2 \xrightarrow{\begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}} \mathbb{Z}^2 \xrightarrow{((\bar{1},\bar{0}),(\bar{0},\bar{1}))} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$
- Eine andere (weniger schöne) Darstellung von $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ ist
$$\mathbb{Z}^3 \xrightarrow{\begin{pmatrix} 3 & 1 & 1 \\ 1 & 3 & 1 \\ 1 & 1 & 1 \end{pmatrix}} \mathbb{Z}^3 \xrightarrow{((\bar{1},\bar{0}),(\bar{0},\bar{1}),(\bar{1},\bar{1}))} \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}.$$

$\mathrm{Ker}(\varphi_S)$ ist endlich erzeugt.

Lemma

Jede Untergruppe $H \subseteq \mathbb{Z}^k$ ist endlich erzeugt.

Beweis: per Induktion nach k

- **IA** für $k = 1$: Sei $H \subseteq \mathbb{Z}$. Dann ist H ein Ideal.
- Da $\mathbb{Z}$ ein Hauptidealring ist, gilt $H = n\mathbb{Z}$ für ein $n \geq 0$.
- **IS** $k - 1 \to k$.
- Sei $\pi : \mathbb{Z}^k \to \mathbb{Z}$ die Projektion auf die letzte Komponente.
- Analog zur Argumentation oben gilt $\pi(H) = n\mathbb{Z}$ für ein $n \geq 0$.
- Sei $g \in \pi^{-1}(n) \cap H$.
- Nach IA ist die Projektion $H' = H \cap (\mathbb{Z}^{k-1} \times 0)$ endlich erzeugt.
- Behauptung: Die Erzeuger von H' zusammen mit g erzeugen H.

$\mathrm{Ker}(\varphi_S)$ ist endlich erzeugt.

Beweis: (Fortsetzung)

- zu zeigen: Für jedes $h \in H$ existiert ein $\ell \in \mathbb{Z}$ mit $h - \ell g \in H'$.
- Es gilt $\pi(h) \in \pi(H) = n\mathbb{Z}$. Damit ist
$$\pi(h) = \ell \cdot n = \ell \cdot \pi(g) \text{ für ein } \ell \in \mathbb{Z}.$$
- Es folgt $\pi(h - \ell g) = \pi(h) - \ell \cdot \pi(g) = 0$.
- Damit ist $h - \ell g \in H'$.

Korollar

$\mathrm{Ker}(\varphi_S) \subseteq \mathbb{Z}^k$ ist endlich erzeugt.

Elementare Operationen

Ist $S = (g_1, \ldots, g_k) \in G^k$ ein Erzeugersystem von G, dann auch

1. $(g_1, \ldots, -g_i, \ldots, g_k)$,
2. $(g_{\pi(1)}, \ldots, g_{\pi(k)})$ für eine Permutation $\pi \in \mathrm{Perm}(k)$,
3. $(g_1, \ldots, g_i + \lambda g_j, \ldots, g_k)$ für $i \neq j$ und $\lambda \in \mathbb{Z}$.

Definition Elementarmatrizen

Die folgenden quadratischen Matrizen heißen *Elementarmatrizen*:

1. E_i: Einheitsmatrix mit Diagonalelement -1 statt 1 an Position (i, i).
2. $P(\pi)$ für $\pi \in \mathrm{Perm}(k)$: In Spalte i steht Einheitsvektor $\mathbf{e}_{\pi(i)}$.
3. $E_{ij}(\lambda)$ für $i \neq j$: Einheitsmatrix mit Eintrag λ an Position (i, j).

Anmerkung:

- Obige Operationen entsprechen Rechts-Multiplikation von S mit
$$E_i,\ P(\pi) \text{ und } E_{ji}(\lambda).$$
- Multiplikation mit einer Elementarmatrix ist invertierbar:
$$E_i^{-1} = E_i,\ P(\pi)^{-1} = P(\pi^{-1}) \text{ und } E_{ij}(\lambda)^{-1} = E_{ij}(-\lambda).$$

Transformation von Darstellungen

Lemma Transformation einer Darstellung

Sei $\mathbb{Z}^\ell \xrightarrow{R} \mathbb{Z}^k \xrightarrow{S} G$ Darstellung einer endl. erzeugten abelschen Gruppe G. Seien E, E' Elementarmatrizen der Größe k bzw. ℓ. Dann ist auch

$$\mathbb{Z}^\ell \xrightarrow{ERE'} \mathbb{Z}^k \xrightarrow{SE^{-1}} G \text{ eine Darstellung von } G.$$

Beweis:

- Sei $S = (g_1, \ldots, g_k) \in G^k$ und damit auch SE^{-1} Erzeuger von G.
- Die Spalten $r_1, \ldots, r_\ell$ von R erzeugen $\mathrm{Ker}(\varphi_S)$. D.h. es gilt
$$\varphi_S(r_i) = \sum_{j=1}^{k} r_{ij} g_j = 0 \text{ für alle } i.$$
- Wir können dies als inneres Produkt von S und r_i auffassen:
$$S \cdot r_i = 0 = S \cdot E^{-1} \cdot E \cdot r_i.$$
- D.h. Erzeugerwechsel durch Rechts-Multiplikation von S mit E^{-1} erfordert Links-Multiplikation von R mit E.
- Weiterhin ändert sich durch Elementaroperationen auf den r_i das Erzeugnis von R nicht. D.h. wir können R durch RE' ersetzen.

Darstellung mittels Diagonalmatrix

Ziel: Wandle R in $R' = ERE'$, so dass R' eine Diagonalmatrix ist.

Satz Darstellung mittels Diagonalmatrix

Sei G eine endlich erzeugte abelsche Gruppe mit Darstellung $\mathbb{Z}^\ell \xrightarrow{R} \mathbb{Z}^k \xrightarrow{S} G$, wobei

$$R = \left(\begin{array}{ccc|c} n_1 & & & 0 \\ & \ddots & & \vdots \\ & & n_r & 0 \\ \hline 0 & \ldots & 0 & 0 \end{array}\right) \in \mathbb{Z}^{k\times\ell}.$$

Dann gilt $G \cong \mathbb{Z}^{k-r} \times \prod_{i=1}^{r} \mathbb{Z}/n_i\mathbb{Z}$.

Beweis: Aus dem Homomorphiesatz folgt

$$G \cong \mathbb{Z}^k/\mathrm{Im}(R) \text{ mit } \mathrm{Im}(R) = n_1\mathbb{Z} \times \ldots \times n_r\mathbb{Z} \times 0^{k-r}.$$

Klassifikationssatz für endlich erzeugte Gruppen

Satz Klassifikationssatz für endlich erzeugte abelsche Gruppen

Jede endlich erzeugte Gruppe G ist isomorph zu einem endlichen Produkt zyklischer Gruppen.

Beweis:

- Sei $\mathbb{Z}^\ell \xrightarrow{R} \mathbb{Z}^k \xrightarrow{S} G$ eine beliebige Darstellung von G.
- zu zeigen: Es existieren Elementarmatrizen E, E', so dass $R' = ERE'$ Diagonalgestalt besitzt.
- Geben dazu Algorithmus TRANSFORM an, der R in R' überführt.
- Mit vorigem Satz: G ist ein Produkt zyklischer Gruppen.

Korrektheit von TRANSFORM (s. nächste Folie):

- Bei Terminierung liefert TRANSFORM eine Diagonalmatrix.
- Der Algorithmus muss terminieren, da in Schritt 3 der Absolutbetrag des Minimums der Restmatrix verringert wird.

Algorithmus TRANSFORM

Algorithmus TRANSFORM

EINGABE: Restmatrix $R \in \mathbb{Z}^{k \times \ell}$

Solange eine nicht-triviale Restmatrix existiert, wiederhole:

1. Falls R Nullzeilen bzw. Nullspalten enthält, tausche diesen an den unteren bzw. rechten Rand.
2. Solange eine Position (i, j) in der Restmatrix existiert, so dass $r_{ij} \neq 0$, aber alle anderen Einträge in Zeile i und Spalte j Null sind, tausche Zeile $1 \leftrightarrow i$ und Spalte $1 \leftrightarrow j$ in der Restmatrix.
3. Bestimme ein Element $r_{i_0 j_0} \neq 0$ minimalen Betrags.
    1. Für alle Zeilen $i \neq i_0$: Bestimme $r_{ij_0} = q_i r_{i_0 j_0} + r'_{ij_0}$ mit $0 \leq r'_{ij_0} < r_{i_0 j_0}$. Subtrahiere das q_i-fache der i_0-ten Zeile von der i-ten Zeile.
    2. Für alle Spalten $j \neq j_0$: Bestimme $r_{i_0 j} = q_j r_{i_0 j_0} + r'_{i_0 j}$ mit $0 \leq r'_{i_0 j} < r_{i_0 j_0}$. Subtrahiere das q_j-fache der j_0-ten Spalte von der j-ten Spalte.

AUSGABE: Diagonalmatrix R'

Beispiel Diagonalisieren

Bsp: Diagonalisieren mittels TRANSFORM

$$\begin{pmatrix} 3 & 6 & 19 \\ -3 & 6 & -29 \\ \underline{2} & 4 & 16 \\ 3 & 18 & 19 \end{pmatrix} \xrightarrow{3.1} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 14 & 3 \\ \underline{2} & 4 & 16 \\ 1 & 14 & 3 \end{pmatrix} \xrightarrow{3.2} \begin{pmatrix} \underline{1} & 0 & -5 \\ 1 & 12 & -5 \\ 2 & 0 & 0 \\ 1 & 12 & -5 \end{pmatrix} \xrightarrow{3.1}$$

$$\begin{pmatrix} \underline{1} & 0 & -5 \\ 0 & 12 & 0 \\ 0 & 0 & 10 \\ 0 & 12 & 0 \end{pmatrix} \xrightarrow{3.2} \left(\begin{array}{c|cc} 1 & 0 & 0 \\ \hline 0 & 12 & 0 \\ 0 & 0 & \underline{10} \\ 0 & 12 & 0 \end{array}\right) \xrightarrow{2} \left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 10 & 0 \\ \hline 0 & 0 & 12 \\ 0 & 0 & \underline{12} \end{array}\right) \xrightarrow{3.1}$$

$$\left(\begin{array}{cc|c} 1 & 0 & 0 \\ 0 & 10 & 0 \\ \hline 0 & 0 & 0 \\ 0 & 0 & \underline{12} \end{array}\right) \xrightarrow{1} \left(\begin{array}{ccc} 1 & 0 & 0 \\ 0 & 10 & 0 \\ 0 & 0 & 12 \\ \hline 0 & 0 & 0 \end{array}\right)$$

Damit ist $G \cong \mathbb{Z} \times \mathbb{Z}/\mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z} \cong \mathbb{Z} \times \mathbb{Z}/10\mathbb{Z} \times \mathbb{Z}/12\mathbb{Z}$.

Primteiler-Normalform

Korollar Primteiler-Normalform

Jede endlich erzeugte abelsche Gruppe G ist isomorph zu

$$\mathbb{Z}^r \times \prod_{i=1}^{s} \prod_{j=1}^{s_i} \mathbb{Z}/p_i^{r_{ij}}\mathbb{Z}$$

für geeignete $p_i \in \mathbb{P}$, $r, s \in \mathbb{N}_0$ und $s_i, r_{ij} \in \mathbb{N}$.
Die Zahl r sowie die $\mathbb{Z}/p_i^{r_{ij}}\mathbb{Z}$ sind bis auf Reihenfolge eindeutig.

Beweis:

- Wir wissen bereits, dass $G \cong \mathbb{Z}^r \times \prod_{i=1}^{\ell} \mathbb{Z}/n_i\mathbb{Z}$.
- Für $n_i = \prod_{j=1}^{\ell_i} p_j^{r_{ij}}$ folgt mit CRT
$$\mathbb{Z}/n_i\mathbb{Z} \cong \prod_{j=1}^{\ell_i} \mathbb{Z}/p_j^{r_{ij}}\mathbb{Z}.$$
- Umsortieren der Faktoren liefert die obige Normalform.
- **Übung:** Beweis der Eindeutigkeit.

Anmerkung: r heißt der *Rang* der Gruppe G.

Bsp zuvor liefert $G \cong \mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$.

Elementarteiler

Korollar Elementarteiler-Normalform

Jede endliche erzeugte abelsche Gruppe G ist isomorph zu

$$\mathbb{Z}^r \times \prod_{i=1}^{\ell} \mathbb{Z}/n_i\mathbb{Z},$$

für geeignete $r \in \mathbb{N}_0$, $n_i \in \mathbb{N}$ mit $n_i > 1$ und $n_{i+1}|n_i$ für $i = 1, \ldots, \ell - 1$. Die Zahlen n_i heißen *Elementarteiler* und sind eindeutig bestimmt.

Beweis:

- Wir wissen bereits, dass $G \cong \mathbb{Z}^r \times \prod_{i=1}^{s} \prod_{j=1}^{s_i} \mathbb{Z}/p_i^{r_{ij}}\mathbb{Z}$.
- Durch Umsortieren erreichen wir $r_{i1} \geq r_{i2} \geq \ldots$ für jedes i.
- Wir definieren $n_j := \prod_{i=1}^{s} p_i^{r_{ij}}$ mit $r_{ij} = 0$ für $i > s_i$.
- Aus dem CRT folgt die Form $G \cong \mathbb{Z}^r \times \prod_{i=1}^{\ell} \mathbb{Z}/n_i\mathbb{Z}$.
- Die Eigenschaft $n_{i+1} \mid n_i$ folgt aus der Sortierung der r_{ij}, da jede Primpotenz von n_i von den Primpotenzen von n_{i+1} geteilt wird.
- **Übung:** Beweis der Eindeutigkeit.

Bsp zuvor liefert $G \cong \mathbb{Z} \times \mathbb{Z}/60\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.

Bsp. Struktur der Einheitengruppe

Bsp: Struktur der Einheitengruppe U_n für kleine n

- $U_2 = \{\bar{1}\} \cong \{0\}$, kongruent zur trivialen Gruppe.
- $U_3 = \{\bar{1}, \bar{2}\} \cong \mathbb{Z}/2\mathbb{Z}$, $\bar{2}$ generiert U_3.
- $U_4 = \{\bar{1}, \bar{3}\} \cong \mathbb{Z}/2\mathbb{Z}$, $\bar{3}$ generiert U_4.
- $U_5 = \{\bar{1}, \bar{2}, \bar{4} = \bar{2}^2, \bar{3} = \bar{2}^3\} \cong \mathbb{Z}/4\mathbb{Z}$, $\bar{2}$ generiert U_5.
- $U_6 = \{\bar{1}, \bar{5}\} \cong \mathbb{Z}/2\mathbb{Z}$, $\bar{5}$ generiert U_6.
- $U_7 = \{\bar{1}, \bar{3}, \bar{2} = \bar{3}^2, \bar{6} = \bar{3}^3, \bar{4} = \bar{3}^4, \bar{5} = \bar{3}^5\} \cong \mathbb{Z}/6\mathbb{Z}$, $\bar{3}$ generiert U_6.
- $U_8 = \{\bar{1}, \bar{3}, \bar{5}, \bar{7}\} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. $(\bar{3}, \bar{5})$ generieren U_8, denn
$$3 \cdot 5 \equiv 7 \bmod 8 \text{ und } 3^2 \equiv 1 \bmod 8.$$

Anmerkung:

- Sei g ein Erzeuger der Gruppe U_n.
- Der Isomorphismus $(\mathbb{Z}/\varphi(n)\mathbb{Z}, +) \cong (U_n, \cdot)$ ist gegeben durch
$$\exp\colon \mathbb{Z}/\varphi(n)\mathbb{Z} \to U_n \text{ mit } i + \varphi(n)\mathbb{Z} \mapsto g^i + n\mathbb{Z}.$$

Untergruppen endlicher Körper

Satz Untergruppen zyklischer Gruppen

Sei $\mathbb{F}$ ein Körper. Jede endliche Untergruppe $(G, \cdot)$, $G \subseteq \mathbb{F}$ ist zyklisch.

Beweis:

- Da G endlich ist, ist G auch endlich erzeugt und besitzt Rang 0.
- Nach Klassifikationssatz für endl. erzeugte abelsche Gruppen gilt
$$G \cong \prod_{i=1}^{s} \prod_{j=1}^{s_i} \mathbb{Z}/p_i^{r_{ij}}\mathbb{Z} \text{ für } s, s_i, r_{ij} \in \mathbb{N},\ p_i \in \mathbb{P}.$$
- Falls $s_i = 1$ für alle i, dann gilt nach CRT
$$G \cong \prod_{i=1}^{s} \mathbb{Z}/p_i^{r_{ij}}\mathbb{Z} \cong \mathbb{Z}/(\prod_{i=1}^{s} p_i^{r_{ij}})\mathbb{Z}.$$
- Da die rechte Seite zyklisch ist, ist auch G zyklisch.
- Bleibt zu zeigen, dass $s_i = 1$ für $i = 1, \ldots, s$.

Untergruppen endlicher Körper

- Annahme: $s_i > 1$ für ein i, oBdA $s_1 > 1$.
- Wir betrachten die Untergruppe $H \cong \prod_{j=1}^{s_1} \mathbb{Z}/p_1^{r_{1j}}\mathbb{Z} \times 0 \subseteq G$.
- Sei $r := max_j\{r_{1j}\}$. Es gilt $|H| = \prod_{j=1}^{s_1} p_1^{r_{1j}} > p_1^r$.
- Für alle $h \in H$ gilt $\mathrm{ord}(h) \mid p_1^r$. Es folgt
$$h^{p_1^r} = 1 \text{ für alle } h \in H \subseteq G \subseteq \mathbb{F}.$$
- Damit sind alle $h \in H \subseteq \mathbb{F}$ Nullstellen von $X^{p_1^r} - 1$.
- Dies sind $|H| > p_1^r$ Nullstellen für ein Polynom vom Grad p_1^r.
(Widerspruch: In $\mathbb{F}$ kann $X^{p_1^r} - 1$ nur max. p_1^r Nst. besitzen.)

U_p ist zyklisch.

Satz U_p ist zyklisch

Sei p prim. Dann ist $U_p = \mathbb{F}_p^*$ zyklisch, d.h. $U_p \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

Beweis:

- Da $\mathbb{F}_p$ ein endlicher Körper ist, ist $U_p \subseteq \mathbb{F}_p^*$ zyklisch.
- Wegen $|U_p| = p-1$ folgt aus dem Isomorphiesatz für zyklische Gruppen (Folie 84), dass $U_p \cong \mathbb{Z}/(p-1)\mathbb{Z}$.

Definition Primitivwurzel

Ein $g \in \mathbb{Z}$, das U_n erzeugt, heißt *Generator* oder *Primitivwurzel* mod n.

Übung: Zeigen Sie: Es gibt $\varphi(\varphi(n))$ viele Primitivwurzeln modulo n.

Test auf Primitivwurzel

Ziel: Entscheide effizient, ob g eine Primitivwurzel ist.

Satz Test auf Primitivwurzel

Sei $p \in \mathbb{P}$. Ein $g \in \mathbb{Z}$, $g \not\equiv 0 \bmod p$ ist Primitivwurzel modulo p gdw

$$g^{\frac{p-1}{q}} \not\equiv 1 \bmod p \text{ für alle Primteiler } q \text{ von } p-1.$$

Beweis:

$\Rightarrow$ Sei g eine Primitivwurzel, d.h. $\mathrm{ord}(g) = p-1$.

- Damit gilt $p-1 = \min\{i \in \mathbb{N} \mid g^i \equiv 1 \bmod p\}$. Es folgt
$$g^{\frac{p-1}{q}} \not\equiv 1 \bmod p, \text{ wegen } \frac{p-1}{q} < p-1.$$

$\Leftarrow$ Aus Satz von Lagrange folgt $\mathrm{ord}(g) | p-1$, d.h. $\mathrm{ord}(g) \cdot c = p-1$.

- Annahme: $c > 1$. Dann besitzt c einen Primteiler q und es gilt
$$g^{\frac{p-1}{q}} = g^{ord(g)\cdot\frac{c}{q}} = (g^{ord(g)})^{\frac{c}{q}} \equiv 1 \bmod p. \quad \text{(Widerspruch)}$$
- Aus $c = 1$ folgt $\mathrm{ord}(g) = p-1$.
- Damit ist g eine Primitivwurzel modulo p.

Bsp: 3 ist Primitivwurzel von U_7, denn $3^2 \equiv 2 \bmod 7$ und $3^3 \equiv 6 \bmod 7$.

Liften von Lösungen

Ziel: Wir zeigen, dass U_{p^r} mit $p \in \mathbb{P} \setminus \{2\}$, $r \geq 2$ zyklisch ist.

Lemma Liften mod p

Sei $x \in \mathbb{Z}$. Für $p \in \mathbb{P} \setminus \{2\}$ und $r \geq 2$ gilt

$$x \equiv 1 \mod p^{r-1} \Leftrightarrow x^p \equiv 1 \mod p^r$$

Beweis:

$\Rightarrow$ Sei $x \equiv 1 \mod p^{r-1}$, d.h. $x = 1 + cp^{r-1}$ für ein $c \in \mathbb{Z}$. Es folgt

$$x^p = (1 + cp^{r-1})^p = 1 + pcp^{r-1} + \sum_{i=2}^{p} \binom{p}{i} c^i p^{(r-1)i}.$$

- Für $i, r \geq 2$ gilt $(r-1)i \geq 2(r-1) = r + (r-2) \geq r$.
- Damit folgt $x^p \equiv 1 \mod p^r$.

Liften von Lösungen

Beweis: (Fortsetzung)

$\Leftarrow$ Wir zeigen $x^p \equiv 1 \mod p^r \Rightarrow x \equiv 1 \mod p^{r-1}$ per Induktion über r.

- **IA** für $r = 2$. Nach Kleinem Satz von Fermat gilt $x^p \equiv x \mod p$.
- Aus $x^p \equiv 1 \mod p^2$ folgt $x^p \equiv 1 \mod p$ und damit $x \equiv 1 \mod p$.
- IS $r \to r + 1$: Sei $x^p \equiv 1 \mod p^{r+1}$.
- Es folgt $x^p \equiv 1 \mod p^r$. Nach IV folgt damit $x \equiv 1 \mod p^{r-1}$ bzw.
$$x = 1 + cp^{r-1} \text{ für ein } c \in \mathbb{Z}.$$
- Falls $p \mid c$, dann folgt die Behauptung $x \equiv 1 \mod p^r$. Es gilt
$$1 \equiv x^p = (1 + cp^{r-1})^p = 1 + cp^r + \sum_{i=2}^{p} \binom{p}{i} c^i p^{(r-1)i} \mod p^{r+1}.$$
- Wir wissen bereits, dass $p | \binom{p}{i}$ für $2 \leq i < p$.
- Damit enthält die Summe einen Term $p^{(r-1)i+1}$ mit
$$(r-1)i + 1 \geq 2(r-1) + 1 = r + 1 + (r-2) \geq r + 1.$$
- Für $i = p$ ist
$$(r-1)i = (r-1)p \geq 3(r-1) = r + 1 + 2(r-2) \geq r + 1.$$
- Damit erhalten wir $1 \equiv 1 + cp^r \mod p^{r+1}$ bzw. $cp^r \equiv 0 \mod p^{r+1}$.
- Es folgt $p | c$ wie gewünscht.

Liften von Lösungen modulo 2

Übung:

- An welcher Stelle im vorigen Beweis benötigen wir $p \neq 2$?
- Geben Sie ein Gegenbeispiel für voriges Lemma für $p = 2, r = 3$.
- Modifizieren Sie den Beweis, um das folgende Lemma zu zeigen.

Lemma Liften mod 2

Sei $x \in \mathbb{Z}$ mit $x \equiv 1 \bmod 4$. Für $r \geq 2$ gilt

$$x \equiv 1 \bmod 2^{r-1} \Leftrightarrow x^2 \equiv 1 \bmod 2^r$$

U_{p^r} ist zyklisch für $p \geq 3$

Satz

Für $p \in \mathbb{P} \setminus \{2\}$ und $r \in \mathbb{N}$ ist U_{p^r} zyklisch, d.h. $U_{p^r} \cong \mathbb{Z}/\varphi(p^r)\mathbb{Z}$.

Beweis:

- Wir wissen bereits, dass U_p zyklisch ist. Sei g ein Generator.
- Behauptung: U_{p^r} wird von g oder von $g' := g + p$ generiert.
- Wir müssen zeigen, dass $g^{\frac{\varphi(p^r)}{q}} \not\equiv 1 \bmod p^r$ (oder analog für g') für alle Primteiler q von $\varphi(p^r) = p^{r-1}(p-1)$.
- **Fall 1** $q \mid p-1$: Offenbar gilt $g \equiv g' \bmod p$.
- Da g ein Generator von U_p ist, folgt $g'^{\frac{p-1}{q}} \equiv g^{\frac{p-1}{q}} \not\equiv 1 \bmod p$.
- $(r-1)$-malige Anwendung des Lift-Lemmas (Folie 103) liefert

$$g^{\frac{p^{r-1}(p-1)}{q}} \not\equiv 1 \bmod p^r. \text{ (bzw. für } g'\text{)}$$

U_{p^r} ist zyklisch für $p \geq 3$

Beweis: (Fortsetzung)

- **Fall 2** $q = p$. Wir müssen zeigen, dass entweder
$$g^{p^{r-2}(p-1)} \not\equiv 1 \bmod p^r \text{ oder } g'^{p^{r-2}(p-1)} \not\equiv 1 \bmod p^r.$$
- $(r-2)$-malige Anwendung unseres Lemmas liefert
$$g^{(p-1)} \not\equiv 1 \bmod p^2 \text{ oder } g'^{(p-1)} \not\equiv 1 \bmod p^2.$$
- Annahme: $g^{(p-1)} \equiv 1 \bmod p^2$ und $(g+p)^{(p-1)} \equiv 1 \bmod p^2$
- Es folgt
$$1 \equiv (g+p)^{p-1} \equiv g^{p-1} + (p-1)g^{p-2}p \equiv 1 + (p-1)g^{p-2}p \bmod p^2.$$
- Damit ist $-g^{p-2}p \equiv 0 \bmod p^2$ bzw. $g^{p-2} \equiv 0 \bmod p$.
(Widerspruch: $(U_p, \cdot)$ ist abgeschlossen und $0 \notin U_p$.)

Test auf Primitivwurzel für U_{p^r}

Korollar

Sei g ein Generator von U_p, $p \in \mathbb{P}$. Für $r > 1$ ist ein Generator von U_{p^r}

$$\begin{cases} g & \text{falls } g^{p-1} \not\equiv 1 \bmod p^2 \\ g+p & \text{sonst} \end{cases}.$$

Beweis: Folgt direkt aus dem Beweis zuvor.

Bsp:

- 2 ist Generator von U_5 wegen $2^{\frac{5-1}{2}} = 4 \not\equiv 1 \bmod 5$.
- Wegen $2^4 = 16 \not\equiv 1 \bmod 25$ ist 2 auch Generator für U_{5^r} mit $r \geq 2$.

Die Potenzen von 2

Der folgende Satz zeigt, dass U_{2^r} für $r \geq 3$ nicht zyklisch ist.

Satz

Für $r \geq 3$ gilt $U_{2^r} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z}$.

Beweis:

- Wir zeigen, dass die folgende Abbildung ein Isomorphismus ist:
$$\Psi : \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2^{r-2}\mathbb{Z} \to U_{2^r} \text{ mit } (\bar{i}, \bar{j}) \mapsto \overline{(-1)}^i \bar{5}^j.$$
- Da $\bar{j} = j + 2^{r-2}\mathbb{Z}$, benötigen wir $\mathrm{ord}(\bar{5}) = 2^{r-2}$, damit wir im Exponenten mod 2^{r-2} rechnen können. (Wohldefiniertheit von Ψ)
- Wir zeigen zunächst, dass $5^{2^{r-2}} \equiv 1 \mod 2^r$.
- $(r-2)$-malige Anwendung des Lift-Lemmas mod 2 liefert
$$5^{2^{r-2}} \equiv 1 \mod 2^r \Leftrightarrow 5 \equiv 1 \mod 2^2.$$
- Damit gilt $\mathrm{ord}(\bar{5}) | 2^{r-2}$. Falls $\mathrm{ord}(\bar{5}) \nmid 2^{r-3}$ folgt $\mathrm{ord}(\bar{5}) = 2^{r-2}$.
- Es gilt $5^{2^{r-3}} \not\equiv 1 \mod 2^r \Leftrightarrow 5 \not\equiv 1 \mod 2^3$.

Die Potenzen von 2

Beweis: (Fortsetzung)

- Bleibt zu zeigen, dass Ψ bijektiv ist. Da Urbild- und Bildmenge Kardinalität 2^{r-1} besitzen, genügt es, Injektivität zu zeigen.
- Dazu zeigen wir, dass $\mathrm{Ker}(\Psi)$ trivial ist, d.h.
$$\Psi(\bar{i},\bar{j}) = \bar{1} \Rightarrow (\bar{i},\bar{j}) = (\bar{0},\bar{0}).$$
- Sei $\Psi(\bar{i},\bar{j}) = (-1)^i 5^j \equiv 1 \bmod 2^r$ für $r \geq 3$.
- Insbesondere gilt $(-1)^i \equiv 1 \bmod 4$. D.h. $i \equiv 0 \bmod 2$ bzw. $\bar{i} = \bar{0}$.
- Damit gilt $\Psi(\bar{0},\bar{j}) = 5^j \equiv 1 \bmod 2^r$.
- Wegen $\mathrm{ord}(\bar{5}) = 2^{r-2}$ folgt $j \equiv 0 \bmod 2^{r-2}$ bzw. $\bar{j} = 0$.

Klassifikation der zyklischen U_p

Satz Klassifikation der zyklischen U_p

Für $n \in \mathbb{N}$ ist die Einheitengruppe U_n zyklisch gdw

$$n = 2, 4,\ n = p^r \text{ oder } n = 2p^r \text{ für } p \in \mathbb{P} \setminus \{2\} \text{ und } r \in \mathbb{N}.$$

Beweis:

- Es gilt $U_2 = \{\bar{1}\}$ und $U_4 = \{\bar{1}, \bar{3}\}$ mit Generatoren $\bar{1}$ bzw. $\bar{3}$.
- Dass U_{p^r} zyklisch ist, wurde auf Folie 106 gezeigt.
- Ferner gilt nach CRT (Lemma auf Folie 68)
$$U_{2p^r} \cong U_2 \times U_{p^r} \cong U_{p^r}.$$
- Damit ist auch U_{2p^r} zyklisch.
- Alle anderen n schreiben wir als
$$n = a \cdot b \text{ für teilerfremde } a, b \text{ mit } 2 < a, b < n.$$
- Nach CRT (Lemma auf Folie 68) gilt $U_n \cong U_a \times U_b$.
- D.h. U_n ist isomorph zu einem Produkt nicht-trivialer Gruppen.

k-te Wurzeln in U_n

- Sei U_n zyklisch mit Primitivwurzel g.
- Wir haben bereits den folgenden Isomorphismus studiert:
$$\exp_g : (\mathbb{Z}/\varphi(n)\mathbb{Z}, +) \to (U_n, \cdot) \text{ mit } \bar{i} \mapsto \bar{g}^i.$$
- Damit gilt $\exp_g(x+y) = \exp_g(x) \cdot \exp_g(y)$.
- Die Umkehrfunktion ist der Diskrete Logarithmus
$$\log_g : (U_n, \cdot) \to (\mathbb{Z}/\varphi(n)\mathbb{Z}, +) \text{ mit } \bar{g}^i \mapsto \bar{i}.$$
- Damit ist $\log_g(xy) = \log_g(x) + \log_g(y)$ und $\log_g(x^k) = k \log(x)$.

Ziel: Finde alle Lösungen $x \in U_n$ von $x^k \equiv a \bmod n$.

- Anwendung von $\log_g$ liefert $k \log_g x \equiv \log_g a \bmod \varphi(n)$.
- Wir können nun diese lineare Gleichung nach $\log_g x$ auflösen.
- Wenn wir $\log_g a$ berechnen, erhalten wir alle Lösungen für $\log_g x$.
- Anwenden von exp auf diese Lösungen liefert alle Lösungen für x.

Bsp. Berechnen einer 3-ten Wurzel in U_7

Bsp: Berechne alle Lösungen von $x^3 \equiv 6 \bmod 7$

- Wir wissen bereits, dass $\bar{3}$ eine Primitivwurzel von U_7 ist.
- Anwendung von $\log_3$ liefert $3 \cdot \log_3 x \equiv \log_3 6 \bmod 6$.
- Wir bestimmen $\log_3 \bar{6} = \bar{3}$ mittels folgender Wertetabelle

i	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{5}$
$\exp_3(i)$	$\bar{1}$	$\bar{3}$	$\bar{2}$	$\bar{6}$	$\bar{4}$	$\bar{5}$

- Wegen $\mathrm{ggT}(3,6) = 3$ erhalten wir die Lösungen
$$\log_3 x \equiv \frac{3}{3} = 1 \bmod 2.$$
- In U_7 erfüllen diese Kongruenz die Restklassen $\bar{1}$, $\bar{3}$ und $\bar{5}$.
- Durch Anwendung von $\exp_3$ erhalten wir alle 3 Lösungen
$$\exp_3(\bar{1}) = \bar{3}, \exp_3(\bar{3}) = \bar{6} \text{ und } \exp_3(\bar{5}) = \bar{5}.$$
- Wir testen $3^3 \equiv 6^3 \equiv 5^3 \equiv 6 \bmod 7$.

Anmerkung: In U_n kostet das Berechnen der Wertetabelle Zeit $\Omega(n)$.

Übung: Zeigen Sie:
$f_k : U_n \to U_n, \bar{x} \mapsto \bar{x}^k$ ist für $\mathrm{ggT}(k, \varphi(n)) = 1$ ein Isomorphismus.
Geben Sie einen Alg. zum Berechnen von f_k^{-1} in Zeit $\mathcal{O}(\log^3 n)$.

Baby-Step Giant-Step Algorithmus

Ziel: Berechnen von $\log_g a$ in U_n in Zeit und Platz $\mathcal{O}(\sqrt{n} \log n)$.

Idee: Baby-Step Giant-Step Algorithmus

- Sei $x \equiv \log_g a \bmod \varphi(n)$ mit $0 \leq x < \varphi(n)$, d.h. $g^x \equiv a \bmod n$.
- Setze $A := \lceil \sqrt{\varphi(n)} \rceil$.
- Schreibe $x = x_1 A + x_0$ mit $x_0, x_1 < A = \lceil \sqrt{\varphi(n)} \rceil$.
- Es gilt die Identität $(g^A)^{x_1} \equiv a \cdot g^{-x_0} \bmod n$.
- Erstelle zwei Listen mit Kandidaten für $(g^A)^{x_1}$ bzw. $a \cdot g^{-x_0}$.
- Zwei gleiche Listenelemente liefern (x_0, x_1) und damit x.

Baby-Step Giant-Step Algorithmus

Algorithmus Baby-Step Giant-Step

EINGABE: n, a, $\varphi(n)$

1. Setze $A := \lceil \sqrt{\varphi(n)} \rceil$.
2. Erstelle Liste L mit Einträgen $(x_1, (g^A)^{x_1} \bmod n)$ für $0 \leq x_1 < A$.
3. Sortiere L nach der zweiten Komponente.
4. Für alle $x \in \{0, \ldots, A-1\}$
    1. Falls $ag^{-x0} \bmod n$ in einer der zweiten Komponenten von $(x_1, (g^A)^{x_1} \bmod n)$ in L auftaucht, EXIT.

AUSGABE: $x = x_1 A + x_0 \equiv \log_g a \bmod \varphi(n)$

Laufzeit:

- Wir vernachlässigen hier die Berechnung der Gruppenoperation.
- Schritt 2: $\mathcal{O}(A)$, Schritt 3: $\mathcal{O}(A \log A)$, Schritt 4: $\mathcal{O}(A \log A)$.
- Damit ist die Gesamtlaufzeit $\mathcal{O}(A \log A) = \mathcal{O}(\sqrt{n} \log n)$.

Bsp. Diskreter Logarithmus mit Baby-Step Giant Step

Bsp:

- Wir berechnen $\log_2 \bar{5}$ in U_{13}.
- Setze $A := \lceil \sqrt{12} \rceil = 4$. Wir erhalten

i	$(2^4)^i \bmod 13$	$5(2^{-1})^i \bmod 13$
0	1	5
1	3	**9**
2	**9**	11
3	1	12

- Wir erhalten für $(x_1, x_0) = (2, 1)$ das gleiche Element 9.
- Damit folgt $x = x_1 A + x_0 = 2 \cdot 4 + 1 = 9$.
- Wir testen, dass $2^9 = (2^3)^3 \equiv (-1) \cdot 8 \equiv 5 \bmod 13$.

Die Wurzeln der (-1)

Lemma Wurzeln der (-1)

Für $p \in \mathbb{P} \setminus \{2\}$ ist $x^2 \equiv (-1) \bmod p$ ist lösbar gdw $p \equiv 1 \bmod 4$.
Die beiden Lösungen sind $\pm g^{\frac{p-1}{4}}$ für einen Generator g von U_p.

Beweis:

- $g^{\frac{p-1}{2}}$ ist Nullstelle von $X^2 - 1$ in $\mathbb{F}_p$, wegen $g^{p-1} \equiv 1 \bmod p$.
- Da $g^{\frac{p-1}{2}} \not\equiv 1 \bmod p$, muss $g^{\frac{p-1}{2}} \equiv (-1) \bmod p$ gelten. D.h.
$$\log_g(-1) \equiv \frac{p-1}{2} \bmod p-1.$$
- Die Kongruenz $x^2 \equiv (-1) \bmod p$ ist äquivalent zu
$$2\log_g x \equiv \log_g(-1) \equiv \frac{p-1}{2} \bmod p-1.$$
- Die lineare Kongruenz ist lösbar gdw $\mathrm{ggT}(2, p-1) | \frac{p-1}{2}$.
- Wegen $\mathrm{ggT}(p-1, 2) = 2$ bedeutet dies $2 | \frac{p-1}{2}$ bzw. $p \equiv 1 \bmod 4$.
- Sei also $p \equiv 1 \bmod 4$. Wir erhalten $\log_g x \equiv \frac{p-1}{4} \bmod \frac{p-1}{2}$ bzw.
$$\log_g x_1 \equiv \frac{p-1}{4} \bmod p-1 \text{ und } \log_g x_2 \equiv \frac{p-1}{4} + \frac{p-1}{2} \bmod p-1.$$
- Dies liefert die Lösungen $x_1 \equiv g^{\frac{p-1}{4}} \bmod p$ und $x_2 \equiv -g^{\frac{p-1}{4}} \bmod p$.

Lösen allgemeiner quadratischer Gleichungen

Ziel: Effiziente Berechnung der Lösungen von

$$X^2 \equiv d \bmod p \text{ für } p \in \mathbb{P}, d \in \mathbb{Z}.$$

Beobachtung: Sei $p \in \mathbb{P} \setminus \{2\}$.

- Das Lösen von $ay^2 + by + c \equiv 0 \bmod p$ kann für $a \not\equiv 0 \bmod p$ auf das Lösen von $x^2 \equiv d \mod p$ zurückgeführt werden.
- Wir multiplizieren obiges Polynom mit dem Inversen von a in U_p:
$$y^2 + \frac{b}{a}y + \frac{c}{a} \equiv 0 \bmod p \Leftrightarrow \left(y + \frac{b}{2a}\right)^2 \equiv \left(\frac{b}{2a}\right)^2 - \frac{c}{a} \bmod p.$$
- Sei $d = \left(\frac{b}{2a}\right)^2 - \frac{c}{a}$ die Diskriminante. Wir lösen $x^2 \equiv d \bmod p$.
- Falls x eine Lösung ist, dann ist auch $-x$ eine Lösung.
- Beide Lösungen sind für $p \geq 3$, $x \not\equiv 0 \bmod p$ verschieden, denn
$$x \equiv -x \bmod p \Leftrightarrow 2x \equiv 0 \bmod p \Leftrightarrow x \equiv 0 \bmod p.$$
- Für unsere Ausgangskongruenz erhalten wir folgende Lösungen
$$\begin{cases} -\frac{b}{2a} \bmod p & \text{falls } d \equiv 0 \bmod p. \\ -\frac{b}{2a} \pm x \bmod p & \text{falls } x \text{ Lösung von } x^2 \equiv d \bmod p \text{ ist.} \\ \text{keine Lösung} & \text{sonst.} \end{cases}$$

Quadratische Reste und das Legendre-Symbol

Definition Quadratischer Rest

Sei $p \in \mathbb{P}$. Ein $a \in \mathbb{Z}$ mit $a \not\equiv 0 \mod p$ heißt *quadratischer Rest modulo* p, falls ein $b \in \mathbb{Z}$ existiert mit $b^2 \equiv a \mod p$.
Sonst heißt a *quadratischer Nicht-Rest*.

Definition Legendre-Symbol

Für $p \in \mathbb{P}$, $a \in \mathbb{Z}$ definieren wir das *Legendre-Symbol* als

$$\left(\frac{a}{p}\right) = \begin{cases} +1 & \text{falls } a \text{ quadratischer Rest modulo } p. \\ -1 & \text{falls } a \text{ quadratischer Nicht-Rest modulo } p. \\ 0 & \text{falls } a \equiv 0 \mod p. \end{cases}$$

Bsp:

- In U_7 gilt $\bar{1}^2 = \bar{6}^2 = \bar{1}$, $\bar{2}^2 = \bar{5}^2 = \bar{4}$ und $\bar{3}^2 = \bar{4}^2 = \bar{2}$. Damit ist $\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1$, $\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = (-1)$ und $\left(\frac{0}{7}\right) = 0$.

Struktur der quadratischen Reste

Lemma Struktur der quadratischen Reste

Sei $p \in \mathbb{P} \setminus \{2\}$ und g ein Generator von U_p. Ein $g^i \bmod p$, $i = 0, \ldots, p-2$, ist quadratischer Rest gdw i gerade ist.

Beweis:

$\Leftarrow$: Sei $i = 2k$, $k \in \mathbb{N}$, dann ist $(g^k)^2 \equiv g^i \bmod p$.

$\Rightarrow$: Sei $g^i \bmod p$ ein quadratischer Rest.

- Dann existiert ein $b \in \mathbb{Z}$ mit $b^2 \equiv g^i \bmod p$.
- Da g Generator von U_p, existiert ein $k \in \mathbb{N}$ mit $g^k \equiv b \bmod p$.
- Es folgt $2k \equiv i \bmod p-1$ bzw.
$$i = 2k + c(p-1) = 2(k + c \cdot \tfrac{p-1}{2}) \text{ für ein } c \in \mathbb{Z}.$$
- Damit ist i gerade.

Korollar

Für genau die Hälfte aller $\bar{a} \in U_p$ gilt $(\frac{a}{p}) = 1$.

- Genau die $\frac{p-1}{2}$ Elemente $a \in \{g^0, g^2, \ldots, g^{p-3}\}$ liefern $\left(\frac{a}{p}\right) = 1$.

Eigenschaften des Legendre-Symbols

Satz Eigenschaften des Legendre-Symbols

Sei $p \in \mathbb{P} \setminus \{2\}$ und $a, b \in \mathbb{Z}$. Es gilt

1. $a \equiv b \bmod p \Rightarrow (\frac{a}{p}) = (\frac{b}{p})$ (auch für $p = 2$).
2. Euler-Identität: $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \bmod p$.
3. $(\frac{-1}{p}) = (-1)^{\frac{p-1}{2}} = \begin{cases} +1 & \text{falls } p \equiv 1 \bmod 4 \\ -1 & \text{falls } p \equiv 3 \bmod 4 \end{cases}$.
4. Multiplikativität: $(\frac{ab}{p}) = (\frac{a}{p})(\frac{b}{p})$.
5. $(\frac{ab^2}{p}) = (\frac{a}{p})$ für $b \not\equiv 0 \bmod p$.

Eigenschaften des Legendre-Symbols

Beweis:

(1) Für $a \equiv b \equiv 0 \mod p$ ist die Aussage klar. Ansonsten gilt

$$(\frac{a}{p}) = 1 \Leftrightarrow \exists c \in \mathbb{Z} \text{ mit } c^2 \equiv a \equiv b \mod n \Leftrightarrow (\frac{b}{p}) = 1.$$

- D.h. $(\frac{a}{p}) = (\frac{b}{p})$, da das Legendre-Symbol nur Werte ± 1 annimmt.

(2) Für $a \equiv 0 \mod p$ sind beide Seiten 0. Sei also $a \not\equiv 0$.

- Wir schreiben $a \equiv g^i \mod p$ für einen Generator g von U_p.
- Lemma Folie 120: Für die linke Seite gilt $(\frac{g^i}{p}) = 1 \Leftrightarrow i \equiv 0 \mod 2$.
- Behauptung: $a^{\frac{p-1}{2}} \equiv g^{i\frac{p-1}{2}} \equiv 1 \mod p \Leftrightarrow i \equiv 0 \mod 2$.
- Aus dieser Behauptung folgt die Euler-Identität.
- $\Leftarrow$: Für gerades $i = 2k$ gilt $g^{i\frac{p-1}{2}} \equiv g^{k(p-1)} \equiv 1 \mod p$.
- $\Rightarrow$: Sei $g^{i\frac{p-1}{2}} \equiv 1 \mod p$. Dann gilt

$$p-1 \mid i\frac{p-1}{2} \text{ bzw. } i\frac{p-1}{2} \equiv 0 \mod p-1 \text{ und damit } i \equiv 0 \mod 2.$$

Eigenschaften des Legendre-Symbols

(3) Aus (2) folgt $(\frac{-1}{p}) \equiv (-1)^{\frac{p-1}{2}} \mod p$.
- Da beide Seiten in $\mathbb{Z}$ nur Werte aus ± 1 annehmen, gilt Gleichheit.
- Es gilt $(-1)^{\frac{p-1}{2}} = 1$ gdw $\frac{p-1}{2} \equiv 0 \mod 2$ bzw $p \equiv 1 \mod 4$.
- Es gilt $(-1)^{\frac{p-1}{2}} = (-1)$ gdw $\frac{p-1}{2} \equiv 1 \mod 2$ bzw $p \equiv 3 \mod 4$.

(4) Aus (2) folgt $(\frac{ab}{p}) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (\frac{a}{p})(\frac{b}{p}) \mod p$.
- Die Identität über $\mathbb{Z}$ folgt wieder aus der ± 1-Wertigkeit.

(5) Aus (4) folgt $(\frac{ab^2}{p}) = (\frac{a}{p})(\frac{b}{p})^2 = (\frac{a}{p})$ für $b \not\equiv 0 \mod p$.

Übung: $(\frac{a}{p})$ kann in Zeit $\mathcal{O}(\log^2(a) + \log^3 p)$ berechnet werden.

Legendre-Symbol von 2

Lemma Legendre-Symbol von 2

Sei $p \in \mathbb{P} \setminus \{2\}$. Dann gilt

$$\left(\frac{2}{p}\right) = \begin{cases} +1 & \text{falls } p \equiv \pm 1 \bmod 8 \\ -1 & \text{falls } p \equiv \pm 3 \bmod 8 \end{cases}.$$

Beweis:

- Nach Euler-Identität wissen wir, dass $(\frac{2}{p}) \equiv 2^{\frac{p-1}{2}} \bmod p$.
- In $\mathbb{Z}[i]$ gilt $2 = (-i) \cdot 2i = (-i)(1+i)^2$. Damit folgt
$$2^{\frac{p-1}{2}} = (-i)^{\frac{p-1}{2}}(1+i)^{p-1} = (-i)^{\frac{p-1}{2}} \frac{(1+i)^p}{(1+i)}.$$
- Modulo p (für Real-/Imaginärteil separat) gilt $(1+i)^p \equiv (1+i^p)$.
- Wir schreiben $p = 2k+1$ mit $k \in \mathbb{N}$ und erhalten
$$2^{\frac{p-1}{2}} \equiv (-i)^k \cdot \frac{1+i^{2k+1}}{1+i} = (-i)^k \cdot \frac{1+(-1)^k i}{1+i} \bmod p \quad (*).$$

Legendre-Symbol von 2

Beweis: (Fortsetzung)

- Der Term $\frac{1+(-1)^k i}{1+i}$ ist 1 für gerades k. Für ungerade k gilt
$$\frac{1-i}{1+i} = \frac{(1-i)^2}{1-i^2} = \frac{-2i}{2} = (-i).$$
- In $\mathbb{Z}[i]$ ist $\mathrm{ord}(-i) = 4$. D.h. es genügt, $k \bmod 4$ zu betrachten.
- Für $k \equiv 0, 1, 2, 3$ liefert die rechte Seite von $(*)$ die Werte
$$(-i)^0 = 1,\ (-i)^2 = (-1),\ (-i)^2 = (-1) \text{ und } (-i)^4 = 1.$$
- Aus $k \equiv \frac{p-1}{2} \bmod 4$ folgt $p \equiv 2k + 1 \bmod 8$.
- Für $k \equiv 0, 3$ erhalten wir $(\frac{2}{p}) = 1$ und $p \equiv \pm 1 \bmod 8$.
- Für $k \equiv 1, 2$ erhalten wir $(\frac{2}{p}) = (-1)$ und $p \equiv \pm 3 \bmod 8$.

Übung: Zeigen Sie $(-1)^{\frac{p^2-1}{8}} = \begin{cases} +1 & \text{falls } p \equiv \pm 1 \bmod 8 \\ -1 & \text{falls } p \equiv \pm 3 \bmod 8 \end{cases}.$

Gaußsumme

Definition Gaußsumme

Sei $p \in \mathbb{P} \setminus \{2\}$ und $\xi = e^{\frac{2\pi i}{p}} \in \mathbb{C}$ eine p-te Einheitswurzel. Für $a \in \mathbb{Z}$ mit $a \not\equiv 0 \mod p$ definieren wir die *Gaußsumme*

$$g_a = \sum_{j=1}^{p-1} (\tfrac{j}{p}) \xi^{aj} \in \mathbb{Z}[\xi].$$

Lemma Gaußsumme

Seien $p, q \in \mathbb{P} \setminus \{2\}$ verschieden und $a \in \mathbb{Z}$, $a \not\equiv 0 \mod p$. Dann gilt

1. $g_a = (\frac{a}{p}) g_1 \in \mathbb{Z}[\xi]$
2. $g_1^2 = (\frac{-1}{p}) p \in \mathbb{Z}$
3. $g_1^q \equiv g_q \mod q$ in $(\mathbb{Z}/q\mathbb{Z})[\xi]$ (mod q komponentenweise).

Gaußsumme

Beweis:

(1) Wegen $(\frac{a}{p}) = (\frac{a}{p})^{-1}$ zeigen wir $(\frac{a}{p})g_a = g_1$. Es gilt

$$(\tfrac{a}{p})g_a = \textstyle\sum_{j=1}^{p}(\tfrac{a}{p})(\tfrac{j}{p})\xi^{aj} = \sum_{i=1}^{p-1}(\tfrac{aj}{p})\xi^{aj}.$$

- Für $a \not\equiv 0 \mod p$ ist $U_p \to U_p$, $\bar{j} \mapsto \overline{aj}$ ein Isomorphismus.
- D.h. $\overline{aj}$ durchläuft für $j = 1, \ldots, p-1$ alle Elemente $\bar{1}, \ldots, \overline{p-1}$.
- Damit folgt $(\frac{a}{p})g_a = \sum_{j=1}^{p-1}(\frac{aj}{p})\xi^{aj} = \sum_{\ell=1}^{p-1}(\frac{\ell}{p})\xi^{\ell} = g_1$.

(2) Wir betrachten zunächst $\sum_{j=1}^{p-1}\xi^{\ell j}$. Für $\ell \not\equiv 0 \mod p$ ist dies

$$(-1) + \textstyle\sum_{j=0}^{p-1}(\xi^{\ell})^j = (-1) + \frac{(\xi^{\ell})^p - 1}{\xi^{\ell}-1} = (-1) + \frac{(\xi^{p})^{\ell} - 1}{\xi^{\ell}-1} = (-1).$$

- Für $\ell \equiv 0 \mod p$ gilt $\sum_{j=1}^{p-1}\xi^{\ell j} = \sum_{j=1}^{p-1}1^j = p-1$. Wir rechnen

$$g_1^2 = \left(\textstyle\sum_{j=1}^{p-1}(\tfrac{j}{p})\xi^j\right)\left(\sum_{k=1}^{p-1}(\tfrac{k}{p})\xi^k\right) = \sum_{j=1}^{p-1}\sum_{k=1}^{p-1}(\tfrac{jk}{p})\xi^{j+k}.$$

Gaußsumme

Beweis: (Fortsetzung)

- Wir nutzen wieder den Isomorphismus $\bar{k} \mapsto \overline{jk}$ für $\bar{j} \in U_p$

$$\begin{aligned}\sum_{j=1}^{p-1}\sum_{k=1}^{p-1}\left(\tfrac{jk}{p}\right)\xi^{j+k} &= \sum_{k=1}^{p-1}\sum_{j=1}^{p-1}\left(\tfrac{j^2k}{p}\right)\xi^{j+jk}\\ &= \sum_{k=1}^{p-1}\left(\tfrac{k}{p}\right)\sum_{j=1}^{p-1}\xi^{j(1+k)}.\end{aligned}$$

- Unter Ausnutzen unserer Identitäten für $\sum_{j=1}^{p-1}\xi^{\ell j}$ formen wir um zu

$$\sum_{k=1}^{p-2}\left(\tfrac{k}{p}\right)(-1) + \left(\frac{p-1}{p}\right)(p-1) = \left(\frac{p-1}{p}\right)p - \sum_{k=1}^{p-1}\left(\tfrac{k}{p}\right).$$

- Genau die Hälfte aller $\bar{a} \in U_p$ sind quadratische Reste.
- Somit enthält die Summe je $(\frac{p-1}{2})$-mal die Summanden 1 und -1.
- Wir erhalten insgesamt $g_1^2 = \left(\frac{p-1}{p}\right)p - \sum_{k=1}^{p-1}\left(\frac{k}{p}\right) = \left(\frac{-1}{p}\right)p$.

(3) Mit unserer Binomischen Formel mod q (Frobenius) erhalten wir

$$\begin{aligned} g_1^q &= \left(\sum_{j=1}^{p-1}\left(\tfrac{j}{p}\right)\xi^j\right)^q \equiv \sum_{j=1}^{p-1}\left(\left(\tfrac{j}{p}\right)\xi^j\right)^q = \sum_{j=1}^{p-1}\left(\tfrac{j}{p}\right)^q\xi^{jq}\\ &= \sum_{j=1}^{p-1}\left(\tfrac{j}{p}\right)\xi^{jq} = g_q \bmod q.\end{aligned}$$

Quadratisches Reziprozitätsgesetz (Gauß)

Satz Quadratisches Reziprozitätsgesetz (Gauß)

Seien $p, q \in \mathbb{P} \setminus \{2\}$ mit $p \neq q$. Dann gilt

$$\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \left(\frac{p}{q}\right) = \begin{cases} -(\frac{p}{q}) & \text{für } p \equiv q \equiv 3 \bmod 4 \\ (\frac{p}{q}) & \text{sonst} \end{cases}.$$

Beweis:

- In $\mathbb{Z}[\xi]$ gilt nach dem vorigen Lemma
$$(\tfrac{q}{p})g_1 \overset{(1)}{=} g_q \overset{(3)}{\equiv} g_1^q = g_1(g_1^2)^{\frac{q-1}{2}} \equiv g_1 \left(\frac{g_1^2}{q}\right) \bmod q.$$
- Multiplikation mit g_1 liefert $(\frac{q}{p})g_1^2 \equiv g_1^2 \left(\frac{g_1^2}{q}\right) \bmod q$.
- Alle Terme sind nun in $\mathbb{Z}$. Wegen $p \neq q$ gilt $g_1^2 \overset{(2)}{=} (\frac{-1}{p})p \not\equiv 0 \bmod q$.
- Kürzen von g_1^2 liefert
$$\begin{aligned}\left(\frac{q}{p}\right) &\equiv (\tfrac{g_1^2}{q}) = \left(\frac{(-1)^{\frac{p-1}{2}}p}{q}\right) = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \cdot (\tfrac{p}{q}) \equiv \left((-1)^{\frac{q-1}{2}}\right)^{\frac{p-1}{2}} \cdot (\tfrac{p}{q}) \\ &= (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} \cdot (\tfrac{p}{q}) \bmod q\end{aligned}$$

Quadratisches Reziprozitätsgesetz (Gauß)

Beweis: (Fortsetzung)

- Alle Terme sind ± 1, d.h. die Kongruenz ist eine Gleichheit.
- Der Exponent von (-1) ist ungerade gdw $\frac{p-1}{2}$ und $\frac{q-1}{2}$ ungerade.
- Es gilt $\frac{p-1}{2} \equiv 1 \bmod 2$ gdw $p \equiv 3 \bmod 4$. (analog für q)

Bsp:

- Frage: Besitzt die Gleichung $x^2 \equiv 19 \bmod 31$ Lösungen?
- Dazu berechnen wir
$$\left(\frac{19}{31}\right) = -\left(\frac{31}{19}\right) = -\left(\frac{12}{19}\right) = -\left(\frac{2}{19}\right)\left(\frac{2}{19}\right)\left(\frac{3}{19}\right) = \left(\frac{19}{3}\right) = \left(\frac{1}{3}\right) = 1.$$
- Durch Ausprobieren erhalten wir die beiden Lösungen
$$(\pm 9)^2 = 81 \equiv 19 \bmod 31.$$

Problem:
Berechnung des Legendre-Symbols erfordert Faktorisierung in $\mathbb{Z}$.

Das Jacobi-Symbol

Definition Jacobi-Symbol

Sei $n \in \mathbb{N}$ ungerade mit Primfaktorzerlegung $n = \prod_{i=1}^{s} p_i^{r_i}$. Wir definieren das *Jacobi-Symbol* $\left(\frac{a}{n}\right) := \prod_{i=1}^{s} \left(\frac{a}{p_i}\right)^{r_i}$.

Anmerkungen:

- Falls a quadratischer Rest mod n ist, dann gilt $a \equiv b^2 \bmod n$ und
$$\left(\tfrac{a}{n}\right) = \left(\tfrac{b^2}{n}\right) = \prod_{i=1}^{s}\left(\tfrac{b^2}{p_i}\right)^{r_i} = \prod_{i=1}^{s}\left(\tfrac{b}{p_i}\right)^{2r_i} = 1.$$
- Falls $\left(\frac{a}{n}\right) = 1$, dann muss a kein quadratischer Rest mod n sein.
- Es gilt z.B. $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)^2 = 1$.
- Nach CRT müsste jede Lösung von $x^2 \equiv 2 \bmod 15$ auch eine Lösungen von $x^2 \equiv 2 \bmod 3$ und $x^2 \equiv 2 \bmod 5$ sein.
- Beide Kongruenzen besitzen aber keine Lösungen.

Übung:

$\left(\frac{a}{n}\right)$ ist multiplikativ in a und n. D.h. für $a = a_1 a_2$ und $n = n_1 n_2$ gilt
$$\left(\tfrac{a}{n}\right) = \left(\tfrac{a}{n_1}\right)\left(\tfrac{a}{n_2}\right) = \left(\tfrac{a_1}{n_1}\right)\left(\tfrac{a_2}{n_1}\right)\left(\tfrac{a_1}{n_2}\right)\left(\tfrac{a_2}{n_2}\right).$$

Reziprozität für Jacobi-Symbol

Satz Reziprozität

Seien $m \neq n \geq 3$ ungerade natürliche Zahlen. Dann gilt

1. $(\frac{-1}{n}) = (-1)^{\frac{n-1}{2}}$.
2. $(\frac{2}{n}) = (-1)^{\frac{n^2-1}{8}}$.
3. $(\frac{m}{n}) = (-1)^{\frac{m-1}{2} \cdot \frac{n-1}{2}} (\frac{n}{m})$.

Beweis:

- Obige Identitäten gelten für prime n, m. Die linken Seiten sind multiplikativ in n, m, können also in die Primteiler zerlegt werden.
- Genügt zu zeigen: Die rechten Seiten sind multiplikativ in n, m.
- Sei $n = n_1 n_2$ ungerade, d.h. n_1, n_2 sind ebenfalls ungerade.

(1) Wir zeigen $(-1)^{\frac{n_1 n_2 - 1}{2}} = (-1)^{\frac{n_1-1}{2}} \cdot (-1)^{\frac{n_2-1}{2}}$. Dies ist äquivalent zu

$$\frac{n_1 n_2 - 1}{2} \equiv \frac{n_1 + n_2 - 2}{2} \mod 2$$

$$\Leftrightarrow \quad n_1 n_2 - n_1 - n_2 + 1 = (n_1 - 1)(n_2 - 1) \equiv 0 \mod 4$$

- Da $n_1 - 1$ und $n_2 - 1$ beide gerade sind, folgt die Korrektheit.

Reziprozität für Jacobi-Symbol

Beweis: (Fortsetzung)

(2) zu zeigen: $(-1)^{\frac{n_1^2 n_2^2-1}{8}} = (-1)^{\frac{n_1^2-1}{8}}(-1)^{\frac{n_2^2-1}{8}}$. Dies ist äquivalent zu
$\frac{n_1^2 n_2^2-1}{8} \equiv \frac{n_1^2-1}{8} + \frac{n_2^2-1}{8} \mod 2 \Leftrightarrow n_1^2 n_2^2 - n_1^2 - n_2^2 + 1 \equiv 0 \mod 16.$

- Wir formen weiter um zu
  $(n_1^2-1)(n_2^2-1) = (n_1+1)(n_1-1)(n_2+1)(n_2-1) \equiv 0 \mod 16.$
- Die Korrektheit folgt, da alle vier Terme $n_1 \pm 1$, $n_2 \pm 1$ gerade sind.

(3) Aus (1) folgt die Multiplikativität von

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

Anmerkung: Für ungerades n und $m = 2^k m'$ mit ungeradem m' gilt

$$\left(\frac{m}{n}\right) = \left(\frac{2}{n}\right)^k \cdot \left(\frac{m'}{n}\right) = \left(\frac{2}{n}\right)^k \cdot (-1)^{\frac{(m'-1)(n-1)}{4}} \left(\frac{n}{m'}\right).$$

Rekursive Berechnung des Jacobi Symbols

Definition $a \bmod n$

Sei $a \in \mathbb{Z}$ und $n \in \mathbb{N}$. Dann bezeichnen wir mit $a \bmod n$ dasjenige $b \in \mathbb{Z}$ mit $b \equiv a \bmod n$ und $0 \leq b < n$. D.h. $b = a - \lfloor \frac{a}{n} \rfloor \cdot n$.

Algorithmus Jacobi-Symbol

EINGABE: m, n mit n ungerade und $\mathrm{ggT}(m, n) = 1$.

1. Falls $m = 1$, Ausgabe 1.
2. Sei $m = 2^k m'$ mit m' ungerade.
3. Ausgabe $(-1)^{\frac{k(n^2-1)}{8}} \cdot (-1)^{\frac{(m'-1)(n-1)}{4}} \cdot \text{Jacobi-Symbol}(n \bmod m', m')$

AUSGABE: $\left(\frac{m}{n}\right)$

Laufzeit:

- Analog zum Euklidischen Alg. erhalten wir $\mathcal{O}(\log \max\{m, n\})$ rekursive Aufrufe, jeder dieser benötigt $\mathcal{O}(\log^2 \max\{m, n\})$.
- D.h. die Gesamtlaufzeit ist $\mathcal{O}(\log^3 \max\{m, n\})$.

Berechnung von Wurzeln für $p \equiv 3 \bmod 4$

Bsp: Berechnung von $(\frac{22}{39})$

$$(\tfrac{22}{39}) = (\tfrac{2}{39}) \cdot (\tfrac{11}{39}) = -(\tfrac{39}{11}) = -(\tfrac{6}{11}) = -(\tfrac{2}{11}) \cdot (\tfrac{3}{11}) = -(\tfrac{11}{3}) = -(\tfrac{2}{3}) = 1.$$

Ziel: Falls $X^2 \equiv d \bmod p$ mit $(\frac{d}{p}) = 1$, berechne beide Lösungen $\pm X$.

Satz Wurzeln für $p \equiv 3 \bmod 4$

Sei $p \in \mathbb{P}$ mit $p \equiv 3 \bmod 4$ und $d \in \mathbb{Z}$ mit $(\frac{d}{p}) = 1$. Dann sind die Lösungen von $X^2 \equiv d \bmod p$ von der Form $\pm d^{\frac{p+1}{4}}$.

Beweis:

- Es gilt $(\pm d^{\frac{p+1}{4}})^2 = d^{\frac{p+1}{2}} = d^{\frac{p-1}{2}} \cdot d \equiv (\frac{d}{p}) \cdot d = d \bmod p$.
- Es gilt $d^{\frac{p+1}{4}} \not\equiv -d^{\frac{p+1}{4}} \bmod p$, da $\overline{d^{\frac{p+1}{4}}} \in U_p$ und $p > 2$.
- Da $\mathbb{F}_p$ ein Körper ist, sind dies die einzigen beiden Lösungen.

Berechnen allgemeiner Quadratwurzel

Idee des Algorithmus von Tonelli und Shanks:

- Sei $p - 1 = 2^s \cdot q$ mit q ungerade.
- Erster Ansatz: Berechne $a \equiv d^{\frac{q+1}{2}} \mod p$. Dann gilt
$$a^2 \equiv (d^{\frac{q+1}{2}})^2 = d^q \cdot d \mod p.$$
- Falls $d^q \equiv 1 \mod p$, dann ist a bereits die gesuchte Quadratwurzel.
- Es gilt $U_p \cong \mathbb{Z}/\varphi(p)\mathbb{Z} \cong \mathbb{Z}/2^s\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. Wir schreiben $x \cong (x_1, x_2)$.
- Für die Abbildung $f : U_p \to U_p, x \mapsto x^q$ gilt
$$f(x) = x^q \cong q(x_1, x_2) = (qx_1, qx_2) = (qx_1, 0) \in \mathbb{Z}/2^s\mathbb{Z} \times 0.$$
- D.h. q-ten Potenzen sind in einer Untergruppe H der Ordnung 2^s.
- Wir wollen nun einen Erzeuger g von H konstruieren.
- Sei $z \in U_p$ mit $(\frac{z}{p}) = (-1)$. Dann gilt $g :\equiv z^q \mod p \in H$ und
$$g^{2^{s-1}} \equiv z^{q2^{s-1}} = z^{\frac{p-1}{2}} \equiv (-1) \mod p \text{ und } g^{2^s} \equiv z^{p-1} \equiv 1 \mod p.$$
- D.h. g ist Generator von H und $d^q \equiv g^\ell \mod q$ für ein $0 \leq \ell < 2^s$.
- ℓ ist gerade, da $g^\ell \equiv d^q \equiv \frac{a^2}{d} \mod p$ quadratischer Rest ist. Es folgt
$$(a \cdot g^{-\frac{\ell}{2}})^2 \equiv d \mod p.$$
- Damit ist $a \cdot g^{-\frac{\ell}{2}}$ unsere gesuchte Quadratwurzel.

Berechnen des Diskreten Logarithmus modulo 2^s

Lemma Berechnen des Diskreten Logarithmus modulo 2^s

Sei p prim mit $p-1 = 2^s q$, q ungerade. Sei $H = \langle g \rangle \subseteq U_p$ mit $\mathrm{ord}(g) = 2^s$. Für $x = g^\ell \in H$ kann ℓ in $\mathcal{O}(\log^4 p)$ berechnet werden.

Beweis:

- Wir schreiben $\ell = \sum_{i=0}^{s-1} \ell_i \cdot 2^i$ und berechnen $\ell_0, \ldots, \ell_{s-1}$.
- Berechnung von ℓ_0: Wir berechnen $x^{2^{s-1}} \bmod q$. Es gilt
$$x^{2^{s-1}} \equiv g^{\ell \cdot 2^{s-1}} = g^{\sum_{i=0}^{s-1} \ell_i \cdot 2^{s-1+i}} \equiv g^{\ell_0 2^{s-1}} \bmod p.$$
- Da $x^{2^s} \equiv 1 \bmod p$, muss $x^{2^{s-1}} \equiv \pm 1 \bmod p$ gelten.
- Falls $x^{2^{s-1}} \equiv (-1) \bmod p$, dann ist $\ell_0 = 1$, sonst ist $\ell_0 = 0$.
- Sei nun $\ell_0, \ldots, \ell_{j-1}$ bekannt. Wir wollen ℓ_j berechnen.
- Berechnung von ℓ_j: Setze $g^{\sum_{i=j}^{s-1} \ell_i 2^i} \equiv x g^{-\sum_{i=0}^{j-1} \ell_i 2^i} := x'$. Damit ist
$$(x')^{2^{s-1-j}} \equiv g^{\sum_{i=j}^{s-1} \ell_i \cdot 2^{s-1-j+i}} \equiv g^{\ell_j 2^{s-1}} \bmod p.$$
- Damit gilt analog wie zuvor $\ell_j = 1$ gdw $(x')^{2^{s-1-j}} \equiv (-1) \bmod p$.
- Jedes ℓ_j kann in Zeit $\mathcal{O}(\log^3 p)$ berechnet werden.

Algorithmus von Tonelli und Shanks

Algorithmus Berechnen von Quadratwurzeln mod p

EINGABE: $p \in \mathbb{P}$, d mit $(\frac{d}{p}) = 1$

1. Sei $p - 1 = 2^s q$ mit q ungerade.
2. Setze $x \equiv d^q \bmod p$ und $\ell = 0$.
3. Wähle $z \bmod p$ zufällig bis $(\frac{z}{p}) = (-1)$. Setze $g :\equiv z^q \bmod p$.
4. For $j = 1$ to $s - 1$
   1. If $((x \cdot g^{-\ell})^{2^{s-1-j}} \equiv (-1) \bmod p)$ then $\ell := \ell + 2^j$.
5. Berechne $a \equiv d^{\frac{q+1}{2}} g^{-\frac{\ell}{2}} \bmod p$.

AUSGABE: a mit $a^2 \equiv d \bmod p$

- **Korrektheit:** Folgt aus den beiden Folien zuvor.
- **Laufzeit:** Erwartete Laufzeit $\mathcal{O}(\log^4 p)$.

Übung: Modifizieren Sie den Algorithmus zum Berechnen 3. Wurzeln.

Algorithmus von Tonelli und Shanks

Bsp: Wir berechnen die Lösungen von $y^2 \equiv 2 \bmod 41$.

- Es gilt $41 - 1 = 2^3 \cdot 5$.
- Wir setzen $x \equiv 2^5 = 32 \equiv -9 \bmod 41$.
- Es gilt $(\frac{3}{41}) = (\frac{41}{3}) = (\frac{2}{3}) = (-1)$.
- Wir setzen $g = 3^5 = 81 \cdot 3 \equiv (-3) \bmod 41$.
- Damit gilt $g^{-1} \equiv (-14) \bmod 41$.
- Für $j = 1$ ist $x^2 = (-9)^2 = 81 \equiv (-1) \bmod 41$, d.h. $\ell_1 = 1$.
- Für $j = 2$ ist $x \cdot g^{-\ell} = (-9) \cdot (-14)^2 \equiv (-1) \bmod 41$, d.h. $\ell_2 = 1$.
- Damit gilt $\ell = 6$ und $a \equiv 2^3(-14)^3 \equiv 24 \bmod 41$.
- Wir testen $(\pm 24)^2 \equiv 2 \bmod 41$.

Kettenbrüche

Definition Kettenbruch

Ein *endlicher Kettenbruch* ist eine Sequenz $[a_0, \ldots, a_n]$ mit $a_i \in \mathbb{R}$ und

$$\text{Wert } [a_0] := a_0 \text{ und } [a_0, \ldots, a_n] := [a_0, \ldots, a_{n-1} + \tfrac{1}{a_n}] \text{ für } n \in \mathbb{N}.$$

Der Wert ist eines *unendlichen Kettenbruchs* $[a_0, a_1, \ldots]$ ist definiert als $\lim_{n\to\infty}[a_0, \ldots, a_n]$.

Anmerkung: Aus der Definition folgt

$$[a_0, \ldots, a_n] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \ldots + \frac{1}{a_n}}}.$$

Ziel: Konstruiere $[a_0, a_1, \ldots]$ mit $a_0 \in \mathbb{Z}$ und $a_i \in \mathbb{N}$ für $i \geq 1$.

Bsp:

- $\frac{43}{30} = 1 + \frac{13}{30} = 1 + \frac{1}{\frac{30}{13}} = 1 + \frac{1}{2 + \frac{4}{13}} = 1 + \frac{1}{2 + \frac{1}{\frac{13}{4}}} = 1 + \frac{1}{2 + \frac{1}{3 + \frac{1}{4}}} = [1, 2, 3, 4].$
- Sei $\Phi = [1, 1, \ldots]$. Für den Grenzwert muss gelten $\Phi = 1 + \frac{1}{\Phi}$.
- Positive Lösung von $\Phi^2 - \Phi - 1 = 0$ ist der goldene Schnitt $\frac{1+\sqrt{5}}{2}$.

Kettenbruchalgorithmus

Algorithmus KETTENBRUCH

EINGABE: $x \in \mathbb{R}$

1. Berechne $a_0 = \lfloor x \rfloor \in \mathbb{Z}$ und $t_0 := x - a_0 \in [0,1[$. Setze $n = 0$.
2. Solange $t_n \neq 0$
   1. Berechne
      $$r_n := \frac{1}{t_n} > 1,\ a_{n+1} := \lfloor r_n \rfloor \in \mathbb{N} \text{ und } t_{n+1} := r_n - a_{n+1} \in [0,1[.$$
   2. Setze $n := n + 1$.

AUSGABE: $x = [a_0, \ldots, a_n]$ mit $a_0 \in \mathbb{Z}$, $a_1 \ldots, a_n \in \mathbb{N}$.

Bsp: KETTENBRUCH FÜR $\frac{43}{30}$:

i	a_i	t_i	r_i
0	1	$\frac{13}{30}$	$\frac{30}{13}$
1	2	$\frac{4}{13}$	$\frac{13}{4}$
2	3	$\frac{1}{4}$	4
3	4	0	–

Korrektheit von KETTENBRUCH

Satz Korrektheit von KETTENBRUCH

Bei Terminierung liefert KETTENBRUCH bei Eingabe $x \in \mathbb{R}$ Ausgabe

$$x = [a_0, \ldots, a_n] \text{ mit } a_0 \in \mathbb{Z} \text{ und } a_1, \ldots, a_n \in \mathbb{N}.$$

Beweis:

- Wir beweisen die Invariante $x = [a_0, \ldots, a_n, r_n]$ per Induktion.
- **IA** für $n = 0$: Es gilt $x = [x] = [a_0 + t_0] = [a_0 + \frac{1}{r_0}] = [a_0, r_0]$.
- **IS** $n \to n + 1$: Es gilt

$$\begin{aligned}
[x] &\overset{IV}{=} [a_0, \ldots, a_n, r_n] = [a_0, \ldots, a_n, a_{n+1} + t_{n+1}] \\
&= [a_0, \ldots, a_n, a_{n+1} + \tfrac{1}{r_{n+1}}] = [a_0, \ldots, a_n, a_{n+1}, r_{n+1}].
\end{aligned}$$

Terminierung von KETTENBRUCH

Satz Terminierung von KETTENBRUCH

Algorithmus KETTENBRUCH terminiert gdw $x \in \mathbb{Q}$.
Für $x = \frac{p}{q} \in \mathbb{Q}$ benötigt KETTENBRUCH Zeit $\mathcal{O}(\log^3(\max\{|p|, q\}))$.

Beweis:

$\Rightarrow$: Falls KETTENBRUCH mit $x = [a_0, a_1, \ldots, a_n]$ terminiert, so können wir x zu einem Bruch $\frac{p}{q}$ mit $p \in \mathbb{Z}, q \in \mathbb{N}$ umformen.

$\Leftarrow$: Sei $x = \frac{p}{q} =: \frac{b_0}{b_1}$.

- Wir zeigen, dass KETTENBRUCH dieselbe Rekursion durchführt wie der Euklidische Algorithmus (EA) bei Eingabe b_0, b_1.
- EA führt die Rekursion $b_i = q_i b_{i+1} + b_{i+2}$ mit $q_i = \lfloor \frac{b_i}{b_{i+1}} \rfloor$ durch.
- KETTENBRUCH berechnet die Rekursion $t_i = \frac{1}{t_{i-1}} - a_i$.
- Für $t_i := \frac{b_{i+2}}{b_{i+1}}$ und $a_i = q_i$ folgt

$$t_i = \frac{1}{t_{i-1}} - a_i \Leftrightarrow \frac{b_{i+2}}{b_{i+1}} = \frac{b_i}{b_{i+1}} - q_i \Leftrightarrow b_i = q_i b_{i+1} + b_{i+2}.$$

Terminierung von KETTENBRUCH

Beweis: (Fortsetzung)

- Wir müssen noch zeigen, dass beide Rekursionen dieselben Startwerte besitzen. Es gilt $a_0 = \lfloor x \rfloor = \lfloor \frac{b_0}{b_1} \rfloor = q_0$ und
$$a_1 = \lfloor r_0 \rfloor = \lfloor \frac{1}{x - a_0} \rfloor = \lfloor \frac{1}{\frac{b_0}{b_1} - \frac{b_0 - b_2}{b_1}} \rfloor = \lfloor \frac{b_1}{b_2} \rfloor = q_1.$$
- Ferner gilt $t_0 = x - a_0 = \frac{b_0}{b_1} - \lfloor \frac{b_0}{b_1} \rfloor = \frac{b_0}{b_1} - q_0 = \frac{b_0}{b_1} - \frac{b_0 - b_2}{b_1} = \frac{b_2}{b_1}$ und
$$t_1 = \frac{1}{t_0} + a_1 = \frac{b_1}{b_2} - q_1 = \frac{b_1}{b_2} - \frac{b_1 - b_3}{b_2} = \frac{b_3}{b_2}.$$
- EA bricht nach $\mathcal{O}(\log(\max\{|p|, q\}))$ Iterationen für ein $b_k = 0$ ab.
- Damit ist $t_{k-2} = 0$ und KETTENBRUCH terminiert.
- D.h. auch KETTENBRUCH benötigt $\mathcal{O}(\log(\max\{|p|, q\}))$ Iterationen.
- KETTENBRUCH läuft damit insgesamt in Zeit $\mathcal{O}(\log^3(\max\{|p|, q\}))$.

Anmerkung: Kettenbrüche sind nicht eindeutig. Für $a_n > 1$ gilt $[a_0, \ldots, a_{n-1}, a_n] = [a_0, \ldots, a_{n-1}, a_n - 1 + \frac{1}{1}] = [a_0, \ldots, a_{n-1}, a_n - 1, 1]$.

Übung: Zeigen Sie die Eindeutigkeit eines Kettenbrüche für x, wobei vorausgesetzt ist, dass das letzte Element größer als 1 ist.

Näherungsbrüche

Definition *n*-ter Näherungsbruch

Sei $x = [a_0, a_1, \ldots]$. Dann heißt $\frac{p_n}{q_n} := [a_0, \ldots, a_n]$ für $n \geq 0$ der *n-te Näherungsbruch* von x.

Ziel: Wir wollen zeigen, dass die Folge $(\frac{p_n}{q_n})_{n\geq 0}$ stets konvergiert.

- Wir definieren $\begin{array}{lll} p_{-1} = 1 & p_{-2} = 0 & p_n = a_n p_{n-1} + p_{n-2} \\ q_{-1} = 0 & q_{-2} = 1 & q_n = a_n q_{n-1} + q_{n-2}. \end{array}$
- Dann gilt $\frac{p_0}{q_0} = \frac{a_0}{1} = [a_0]$ und $\frac{p_1}{q_1} = \frac{a_1 a_0 + 1}{a_1} = a_0 + \frac{1}{a_1} = [a_0, a_1]$.
- Wir können die Rekursion in Matrix-Schreibweise darstellen.
- Die Startwerte sind $\begin{pmatrix} p_{-1} & p_{-2} \\ q_{-1} & q_{-2} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.
- Die Rekursionsgleichung können wir in folgender Form schreiben.

$$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \begin{pmatrix} p_{n-1} & p_{n-2} \\ q_{n-1} & q_{n-2} \end{pmatrix} \begin{pmatrix} a_n & 1 \\ 1 & 0 \end{pmatrix}$$

- Damit können wir die Rekursion einfach auflösen zu

$$\begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \prod_{i=0}^{n} \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix}.$$

Näherungsbrüche

Lemma Näherungsbrüche

Für alle $n \in \mathbb{N}_0$ und alle positiven $r \in \mathbb{R}$ gilt

$$[a_0, a_1, \ldots, a_n] = \frac{p_n}{q_n} \text{ und } [a_0, a_1, \ldots, a_n, r] = \frac{rp_n + p_{n-1}}{rq_n + q_{n-1}}.$$

Beweis:

- Wir zeigen zunächst die zweite Gleichung per Induktion über n.
- **IA** für $n = 0$: $[a_0, r] = \frac{ra_0+1}{r} = a_0 + \frac{1}{r}$.
- **IS** für $n - 1 \to n$: Wir schreiben $[a_0, \ldots, a_n, r]$ als

$$[a_0, \ldots, a_n + \tfrac{1}{r}] \stackrel{IV}{=} \frac{(a_n+\frac{1}{r})p_{n-1}+p_{n-2}}{(a_n+\frac{1}{r})q_{n-1}+q_{n-2}} = \frac{p_n+\frac{1}{r}p_{n-1}}{q_n+\frac{1}{r}q_{n-1}} = \frac{rp_n+p_{n-1}}{rq_n+q_{n-1}}.$$

- Aus der 2. Gleichung erhalten wir

$$[a_0, a_1, \ldots, a_{n-1}, r] = \frac{rp_{n-1}+p_{n-2}}{rq_{n-1}+q_{n-2}} \text{ für alle } r \in \mathbb{R}.$$

- Einsetzen von $r = a_n$ liefert $[a_0, a_1, \ldots, a_n] = \frac{a_n p_{n-1}+p_{n-2}}{a_n q_{n-1}+q_{n-2}} = \frac{p_n}{q_n}$.

Eigenschaften von Näherungsbrüchen

Lemma Eigenschaften von Näherungsbrüchen

Es gilt

1. $q_{n+1} > q_n \geq n$ für $n \in \mathbb{N}$.
2. $p_n q_{n-1} - p_{n-1} q_n = (-1)^{n+1}$ für $n \in \mathbb{N}_0$.
3. $p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$ für $n \in \mathbb{N}_0$.
4. $\mathrm{ggT}(p_n, q_n) = 1$.

Beweis:

(1) **IA** für $n = 1$: Es gilt $q_0 = 1$, $q_1 = a_1 \geq 1$ und damit

$$q_2 = a_2 q_1 + q_0 \geq q_1 + q_0 > q_1 \geq 1.$$

- **IS** $n \to n+1$: Es gilt

$$q_{n+1} = a_n q_n + q_{n-1} \geq q_n + q_{n-1} > q_n.$$

- Aus $q_n > \ldots > q_1 > 1$ folgt $q_n \geq n$.

(2) Wir schreiben $p_n q_{n-1} - p_{n-1} q_n$ als

$$\det \begin{pmatrix} p_n & p_{n-1} \\ q_n & q_{n-1} \end{pmatrix} = \det \prod_{i=0}^{n} \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} = \prod_{i=0}^{n} \det \begin{pmatrix} a_i & 1 \\ 1 & 0 \end{pmatrix} = (-1)^{n+1}.$$

Eigenschaften von Näherungsbrüchen

Beweis: (Fortsetzung)

(3) Aus (2) folgt

$$\begin{aligned} p_n q_{n-2} - p_{n-2} q_n &= (a_n p_{n-1} + p_{n-2}) q_{n-2} - p_{n-2}(a_n q_{n-1} + q_{n-2}) \\ &= a_n (p_{n-1} q_{n-2} - p_{n-2} q_{n-1}) = a_n (-1)^n. \end{aligned}$$

(4) Sei $d = \mathrm{ggT}(p_n, q_n)$. Damit gilt $d | p_n q_{n-1} - p_{n-1} q_n$.

- Aus (2) folgt $d | (-1)^{n+1}$ und damit $d = \pm 1$.

Konvergenz von Kettenbrüchen

Satz Konvergenz von Kettenbrüchen

Sei $(a_n)_{n\in\mathbb{N}}$ eine Folge mit $a_0 \in \mathbb{Z}$ und $a_i \in \mathbb{N}$ für $i \geq 1$. Dann gilt:

1. Die Brüche $\frac{p_n}{q_n} = [a_0, \ldots, a_n]$ bilden eine konvergente Folge.
2. Die Teilfolge $\frac{p_{2n}}{q_{2n}}$ wächst streng monoton, die Teilfolge $\frac{p_{2n+1}}{q_{2n+1}}$ fällt streng monoton.

Beweis:

(1) Aus $p_i q_{i-1} - p_{i-1} q_i = (-1)^{i+1}$ folgt

$$\frac{p_i}{q_i} - \frac{p_{i-1}}{q_{i-1}} = \frac{(-1)^{i+1}}{q_{i-1} q_i} \text{ für alle } i \in \mathbb{N}_0.$$

- Wir entwickeln in einer Teleskopsumme

$$\frac{p_n}{q_n} = \sum_{i=1}^{n} \left(\frac{p_i}{q_i} - \frac{p_{i-1}}{q_{i-1}}\right) + \frac{p_0}{q_0} = a_0 + \sum_{i=1}^{n} \frac{(-1)^{i+1}}{q_{i-1} q_i}.$$

- Die $\frac{1}{q_{i-1} q_i}$ bilden eine streng monotone Nullfolge.
- **Leibniz-Kriterium:** Ihre alternierende Reihe ist konvergent.
- Damit konvergieren auch die $\frac{p_n}{q_n}$.

Konvergenz von Kettenbrüchen

Beweis: (Fortsetzung)

(2) Aus $p_n q_{n-2} - p_{n-2} q_n = (-1)^n a_n$ folgt

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} = \frac{(-1)^n a_n}{q_{n-2} q_n} \text{ für alle } n \in \mathbb{N}_0.$$

- Für $n \geq 2$ sind a_n, q_n, q_{n-2} positiv und daher ist der Term

$$\frac{p_n}{q_n} - \frac{p_{n-2}}{q_{n-2}} \begin{cases} \text{positiv} & \text{für } n \text{ gerade.} \\ \text{negativ} & \text{für } n \text{ ungerade.} \end{cases}$$

- D.h. die Teilfolge $\frac{p_{2n}}{q_{2n}}$ wächst streng monoton und die Teilfolge $\frac{p_{2n+1}}{q_{2n+1}}$ fällt streng monoton.

Konvergenz der Kettenbruchentwicklung

Satz Konvergenz der Kettenbruchentwicklung

Sei $x \in \mathbb{R} \setminus \mathbb{Q}$ mit Kettenbruch $x = [a_0, a_1, \ldots]$. Dann konvergieren die Näherungsbrüche $\frac{p_n}{q_n} = [a_0, \ldots, a_n]$ gegen x. Es gilt für $n \in \mathbb{N}$

$$\left|x - \frac{p_n}{q_n}\right| < \frac{1}{q_n q_{n+1}} \leq \frac{1}{n(n+1)}.$$

Beweis:

- Sei $x = [a_0, a_1, \ldots, a_n, r_n] = \frac{r_n p_n + p_{n-1}}{r_n q_n + q_{n-1}}$ für ein $r_n \in \mathbb{R}_{>0} \setminus \mathbb{N}$.
- Damit folgt

$$\begin{aligned} x - \frac{p_n}{q_n} &= \frac{(r_n p_n + p_{n-1})q_n - p_n(r_n q_n + q_{n-1})}{q_n(r_n q_n + q_{n-1})} \\ &= \frac{p_{n-1}q_n - p_n q_{n-1}}{q_n(r_n q_n + q_{n-1})} = \frac{(-1)^n}{q_n(r_n q_n + q_{n-1})}. \end{aligned}$$

- Wegen $a_{n+1} := \lfloor r_n \rfloor$ und $r_n \notin \mathbb{N}$ folgt $r_n > a_{n+1}$ bzw. $\frac{1}{r_n} < \frac{1}{a_{n+1}}$. D.h.

$$\left|x - \frac{p_n}{q_n}\right| < \frac{1}{q_n(a_{n+1}q_n + q_{n-1})} = \frac{1}{q_n q_{n+1}} \leq \frac{1}{n(n+1)}.$$

- Damit konvergieren die Näherungsbrüche $\frac{p_n}{q_n}$ gegen x.

Kettenbruch der Euler-Zahl

Bsp: : Kettenbruchentwicklung der Euler-Zahl

- Euler zeigte 1744 , dass
$$e = [2, 1, 2, 1, 1, 4, 1, 1, 6, 1, 1, 8, 1, 1, 10, 1, 1, \ldots].$$
- Dies liefert die folgenden Approximationen für e.

$[a_0, a_1, \ldots, a_n]$	$\frac{p_n}{q_n}$	$e - \frac{p_n}{q_n}$
$[2]$	2	$7 \cdot 10^{-1}$
$[2, 1]$	3	$-3 \cdot 10^{-1}$
$[2, 1, 2]$	$\frac{8}{3}$	$5 \cdot 10^{-2}$
$[2, 1, 2, 1]$	$\frac{11}{4}$	$-3 \cdot 10^{-2}$
$[2, 1, 2, 1, 1]$	$\frac{19}{7}$	$4 \cdot 10^{-3}$
$[2, 1, 2, 1, 1, 4]$	$\frac{87}{32}$	$-5 \cdot 10^{-4}$

Übung:

Zeigen Sie, dass Kettenbrüche eine *Bestapproximation* liefern. D.h.
$$|x - \tfrac{p_n}{q_n}| \leq |x - \tfrac{p}{q}| \text{ für alle Brüche } \tfrac{p}{q} \in \mathbb{Q} \text{ mit } q \leq q_n.$$

Auftreten von Näherungsbrüchen

Ziel: Jeder Bruch, der x sehr gut approximiert, ist ein Näherungsbruch.

Satz Auftauchen von Näherungsbrüchen

Sei $x \in \mathbb{R}$. Sei $\frac{p}{q} \in \mathbb{Q}$ mit $\mathrm{ggT}(p, q) = 1$, $q > 0$ und $\left|x - \frac{p}{q}\right| < \frac{1}{2q^2}$.
Dann ist $\frac{p}{q}$ ein Näherungsbruch in der Kettenbruchentwicklung von x.

Beweis:

- Sei $\frac{p}{q} = [a_0, a_1, \ldots, a_n]$. Falls $x = \frac{p}{q}$, sind wir fertig.
- Ansonsten existiert ein $r_n \in \mathbb{R}$ mit $x = [a_0, a_1, \ldots, a_n, r_n]$.
- Wir definieren $r_i := [a_{i+1}, \ldots, a_n, r_n]$ für $i = 0, \ldots, n-1$. Damit gilt

$$\begin{aligned} & [a_0, a_1, \ldots, a_i, r_i] = [a_0, a_1, \ldots, a_i, [a_{i+1}, \ldots, a_n, r_n]] \\ = \quad & [a_0, a_1, \ldots a_n, r_n] = x \quad \text{für } 0 \le i \le n. \end{aligned}$$

- Ferner ist $r_i = [a_{i+1}, r_{i+1}] = a_{i+1} + \frac{1}{r_{i+1}}$ für $0 \le i < n$.
- Z.z.: $[a_0, \ldots, a_i, r_i]$ ist für $0 \le i \le n$ Kettenbruchentwicklung von x.

Auftreten von Näherungsbrüchen

Beweis: (Fortsetzung)

- Zeigen $r_i > 1$ für $i \leq n$, dann ist $a_{i+1} = \lfloor r_i \rfloor$ in KETTENBRUCH.
- Sei $r_n > 1$. Dann gilt $r_{n-1} = a_n + \frac{1}{r_n} > 1$.
- Es folgt induktiv, dass $r_{n-2}, \ldots, r_0 > 1$. Bleibt z.z.: $r_n > 1$.
- Nach dem Lemma für Näherungsbrüche (Folie 146) gilt
$$\frac{p}{q} = \frac{p_n}{q_n} \text{ und } x = \frac{p_n r_n + p_{n-1}}{q_n r_n + q_{n-1}}.$$
- $\frac{p}{q}, \frac{p_n}{q_n}$ sind gekürzte Brüche mit $q, q_n > 0$, d.h. $p = p_n$ und $q = q_n$.
- Aus unserer Voraussetzung folgt
$$\begin{aligned} \frac{1}{2q_n^2} &> \left| x - \frac{p}{q} \right| = \left| \frac{p_n r_n + p_{n-1}}{q_n r_n + q_{n-1}} - \frac{p_n}{q_n} \right| = \left| \frac{q_n p_{n-1} - p_n q_{n-1}}{q_n(q_n r_n + q_{n-1})} \right| \\ &= \left| \frac{(-1)^n}{q_n(q_n r_n + q_{n-1})} \right| = \frac{1}{q_n(q_n r_n + q_{n-1})}. \end{aligned}$$
- Es folgt $q_n + q_{n-1} < 2q_n < q_n r_n + q_{n-1}$ und damit $r_n > 1$.

Brechen von RSA mit kleinem geheimen Schlüssel

Satz von Wiener (1990)

Sei (N, e) ein öffentlicher RSA Schlüssel mit $2 < e < \varphi(N)$ und $N = pq$, p, q gleicher Bitgröße. Sei $ed \equiv 1 \bmod \varphi(N)$ mit $d < \frac{1}{3}N^{\frac{1}{4}}$. Dann liefert die Kettenbruchentwicklung von $\frac{e}{N}$ das geheime d.

Beweis:

- Aus $ed \equiv 1 \bmod \varphi(N)$ folgt für ein $k \in \mathbb{N}$
  $$ed = 1 + k\varphi(N) = 1 + k(p-1)(q-1) = 1 + kN - k(p+q-1).$$
- Jeder gemeinsame Teiler von k und d teilt 1. D.h. $\mathrm{ggT}(k, d) = 1$.
- Teilen durch dN liefert $\frac{e}{N} - \frac{k}{d} = \frac{1-k(p+q-1)}{dN}$.
- Falls $\left|\frac{1-k(p+q-1)}{dN}\right| = \frac{k(p+q-1)-1}{dN} < \frac{1}{2d^2}$, dann taucht der gekürzte Bruch $\frac{k}{d}$ in der Kettenbruchentwicklung von $\frac{e}{N}$ auf.
- Diese Bedingung ist äquivalent zu $2d(k(p+q-1)-1) < N$.

Brechen von RSA mit kleinem geheimen Schlüssel

- Wir beweisen die stärkere Bedingung $2dk(p+q) < N$.
- Dazu benötigen wir obere Schranken für k und $p+q$.
- Es gilt $k = \frac{ed-1}{\varphi(N)} < \frac{e}{\varphi(N)} \cdot d < d$.
- OBdA gelte $p \leq q$. Da p, q gleiche Bitgröße besitzen, folgt
$$p \leq \sqrt{N} \leq q < 2p \leq 2\sqrt{N}.$$
- D.h. wir erhalten $p + q < 3\sqrt{N}$. Dies erfüllt unsere Bedingung:
$$2dk(p+q) < 2d^2(p+q) < \tfrac{2}{9}\sqrt{N} \cdot 3\sqrt{N} < N.$$
- Damit erhalten wir das geheime d aus dem Kettenbruch von $\frac{e}{N}$.

Übung: Seien $a \in \mathbb{Z}$, $n \in \mathbb{N}$ mit $\mathrm{ggT}(a, n) = 1$. Konstruieren Sie mit Hilfe eines Kettenbruchs ein Inverses x von a in U_n, d.h. $ax \equiv 1 \bmod n$.

Definition Pellsche Gleichung

Sei $d \in \mathbb{N}$ kein Quadrat. Dann heißt $x^2 - dy^2 = 1$ *Pellsche Gleichung*.

Pellsche Gleichung

Satz Pellsche Gleichung

Alle Lösungen $(p, q) \in \mathbb{N}^2$ der Pellschen Gleichung treten als Näherungsbruch $\frac{p}{q}$ in der Kettenbruchentwicklung von $\sqrt{d}$ auf.

Beweis:

- Sei (p, q) eine Lösung, d.h. $1 = p^2 - dq^2 = (p + \sqrt{d}q)(p - \sqrt{d}q)$.
- Es folgt $p - \sqrt{d}q = \frac{1}{p+\sqrt{d}q}$. Teilen durch q liefert
$$\frac{p}{q} - \sqrt{d} = \frac{1}{pq+\sqrt{d}q^2} = \frac{1}{(\frac{p}{q}+\sqrt{d})q^2}.$$
- Wegen $p = \sqrt{1 + dq^2} > q$ folgt $\frac{p}{q}, \sqrt{d} > 1$ und
$$\frac{p}{q} - \sqrt{d} < \frac{1}{2q^2}.$$
- Damit taucht $\frac{p}{q}$ in der Kettenbruchentwicklung von $\sqrt{d}$ auf.

Primzahltest für Mersenne-Primzahlen

Satz Lucas-Lehmer Test

Sei $n = 2^p - 1 \in \mathbb{N}$ für $p \in \mathbb{P} \setminus \{2\}$. Wir definieren die Folge S_k durch $S_1 = 4$ und $S_k = S_{k-1}^2 - 2$. Falls $n | S_{p-1}$, dann ist n prim.

Beweis:

$\Rightarrow$ Seien $\omega = 2 + \sqrt{3}, \bar{\omega} = 2 - \sqrt{3}$ im Ring $\mathbb{Z}[\sqrt{3}] = \mathbb{Z} \oplus \mathbb{Z}\sqrt{3}$.

- Wir zeigen zunächst $S_k = \omega^{2^{k-1}} + \bar{\omega}^{2^{k-1}}$ per Induktion über k.
- **IA** für $k = 1$: $\omega + \bar{\omega} = 4 = S_1$.
- **IS** $k - 1 \rightarrow k$: Wegen $\omega\bar{\omega} = 1$ gilt

$$S_k = S_{k-1}^2 - 2 \overset{IV}{=} (\omega^{2^{k-2}} + \bar{\omega}^{2^{k-2}})^2 - 2 = \omega^{2^{k-1}} + 2 + \omega^{2^{k-1}} - 2.$$

Primzahltest für Mersenne-Primzahlen

Beweis: (Fortsetzung)

- Nach Voraussetzung gilt $n|S_{p-1}$, d.h. $cn = S_{p-1} = \omega^{2^{p-2}} + \bar{\omega}^{2^{p-2}}$.
- Multiplikation mit $\omega^{2^{p-2}}$ liefert $\omega^{2^{p-1}} = -1 + cn\omega^{2^{p-2}}$.
- Annahme: n ist zusammengesetzt.
- D.h. es existiert ein primes $q|n$ mit $2 < q \leq \sqrt{n}$. Es folgt
$$\omega^{2^{p-1}} \equiv -1 \bmod q \text{ und } \omega^{2^p} \equiv 1 \bmod q.$$
- Damit ist $\mathrm{ord}(\omega) = 2^p$ in $R := \mathbb{Z}[\sqrt{3}]/q\mathbb{Z}[\sqrt{3}] = \mathbb{Z}/q\mathbb{Z} \oplus (\mathbb{Z}/q\mathbb{Z})\sqrt{3}$.
- Es gilt $R^* \subseteq R \setminus \{0\}$ und damit $|R^*| \leq q^2 - 1$. Es folgt
$$2^p = \mathrm{ord}(\omega) \leq |R^*| \leq q^2 - 1 < n. \text{ (Widerspruch: } n = 2^p - 1)$$

Anmerkung: Man kann auch die Umkehrung n prim $\Rightarrow n|S_{p-1}$ zeigen.

Lucas-Lehmer Primzahltest

Algorithmus Lucas-Lehmer Primzahltest

EINGABE: $n = 2^p - 1 \in \mathbb{N}$ für $p \in \mathbb{P} \setminus \{2\}$.

1. Setze $S_1 = 4$
2. For $i = 2$ to $p - 1$
   1. Berechne $S_i := S_{i-1}^2 - 2 \bmod n$.

AUSGABE: $\begin{cases} \text{prim} & \text{falls } S_{p-1} \equiv 0 \bmod n. \\ \text{zusammengesetzt} & \text{sonst.} \end{cases}$

- **Korrektheit:** Folgt aus vorigem Satz, inklusive Anmerkung.
- **Laufzeit:** $\mathcal{O}(p \log^2 n) = \mathcal{O}(\log^3 n)$.
- Bsp: $n = 2^3 - 1 = 7$ ist prim, denn $S_2 = S_1^2 - 2 = 14 \equiv 0 \bmod 7$.

Lucas-Test

Satz Lucas-Test

Ein $n \in \mathbb{N}$ ist prim gdw ein $a \bmod n$ existiert mit

$$a^{n-1} \equiv 1 \bmod n, \text{ aber } a^{\frac{n-1}{q}} \not\equiv 1 \bmod n \text{ für alle Primteiler } q \text{ von } n-1.$$

Beweis:

$\Rightarrow$ Sei n prim. Dann ist U_n zyklisch und die obigen Identitäten gelten falls a eine Primitivwurzel modulo n ist.

$\Leftarrow$ Aus den Identitäten folgt $\mathrm{ord}(a) = n-1$ in U_n. D.h. $n-1 | \varphi(n)$.

- Damit gilt $n-1 \leq \varphi(n) < n$, woraus $\varphi(n) = n-1$ folgt.
- Annahme: $n = ab$ mit $1 < a, b < n$.
- Da $0 | n$ und $a | n$, gilt $\varphi(n) \leq n-2$. (Widerspruch)

Bsp: 11 ist prim, denn

$$2^{10} \equiv 1 \bmod 11,\ 2^5 \equiv (-1) \bmod 11 \text{ und } 2^2 = 4 \bmod 11.$$

Nachteil: Lucas-Test benötigt vollständige Faktorisierung von $n-1$.

Pocklington-Test

Satz Pocklington-Test

Ein $n \in \mathbb{N}$, $n-1 = RF$, $F \geq \sqrt{n}$, ist prim gdw ein $a \bmod n$ existiert mit

$$a^{n-1} \equiv 1 \bmod n \text{ und } \mathrm{ggT}(a^{\frac{n-1}{q}} - 1, n) = 1 \text{ für alle Primteiler } q \text{ von } F.$$

Beweis:

$\Rightarrow$ Sei n prim und a Generator von U_n. Dann gilt $a^{n-1} \equiv 1 \bmod n$ und $a^{\frac{n-1}{q}} \not\equiv 1 \bmod n$, d.h. $\mathrm{ggT}(a^{\frac{n-1}{q}} - 1, n) = 1$.

$\Leftarrow$ Annahme: n ist zusammengesetzt.

- Sei p Primteiler von n mit $p \leq \sqrt{n}$. Sei $d = \mathrm{ord}(a^R)$ in U_p.
- Es gilt $(a^R)^F = a^{n-1} \equiv 1 \bmod n$ und damit $(a^R)^F \equiv 1 \bmod p$.
- D.h. $d|F$. Wir zeigen $d = F$. Sei q ein Primteiler von $\frac{F}{d}$. Dann gilt
  $$1 \equiv (a^R)^d \Rightarrow 1 \equiv (a^R)^{\frac{F}{q}} = a^{\frac{n-1}{q}} \bmod p \text{ bzw. } \mathrm{ggT}(a^{\frac{n-1}{q}} - 1, n) \geq p.$$
- Sei also $d = F$. Wegen $d = \mathrm{ord}(a^R)$ in U_p folgt $d|p-1$ und damit
  $$F = d \leq p - 1 < \sqrt{n}. \quad \text{(Widerspruch: } F \geq \sqrt{n}\text{)}$$

Bsp: : 11 ist prim, da $2^{10} \equiv 1 \bmod 10$ und $\mathrm{ggT}(2^2 - 1, 11) = 1$.

Pocklington Primzahltest

Algorithmus Pocklington

EINGABE: $n \in \mathbb{N}$

1. Faktorisiere $n-1$ partiell in RF mit $F > \sqrt{n}$.
2. For $a = 1, \ldots, n-1$
   1. Falls $a^{n-1} \equiv 1 \bmod n$ und $\mathrm{ggT}(a^{\frac{n-1}{q}} - 1, n) = 1$ für alle Primteiler q von F, Ausgabe "prim" und Abbruch.
3. Ausgabe "zusammengesetzt".

Laufzeit:

- Schritt 1: Es ist kein Algorithmus mit Laufzeit $\mathrm{poly}(\log n)$ bekannt.
- Schritt 2: Für zusammengesetzte Zahlen n Schleifendurchläufe.
- D.h. der Algorithmus ist schlechter als eine naive Probedivision.
- Der Pocklington-Test liefert allerdings ein Zertifikat für Primheit.

Zeigen nun, dass der Test $a^{n-1} \equiv 1 \bmod n$ leider nicht genügt.

Carmichael-Zahlen

Definition Carmichael-Zahl

Ein zusammengesetztes $n \in \mathbb{N}$ heißt *Carmichael-Zahl*, falls $a^{n-1} \equiv 1 \bmod n$ für alle $a \in U_n$.

Lemma Struktur der (n-1)-ten Einheitswurzeln

Sei $n = 2^r \prod_{i=1}^{s} p_i^{r_i} \in \mathbb{N}$ und $G = \{x \in U_n \mid x^{n-1} = 1\}$. Dann ist

$$U_n/G \cong U_{2^r} \times \prod_{i=1}^{s} \mathbb{Z}/m_i\mathbb{Z} \text{ mit } m_i = \frac{p_i^{r_i-1}(p_i-1)}{\mathrm{ggT}(p_i-1, n-1)}.$$

Beweis: (s. [M-S,P], S.92)

Struktur von Carmichael-Zahlen

Satz Struktur von Carmichael-Zahlen

Sei $n \in \mathbb{N}$ zusammengesetzt.

1. n ist Carmichael gdw n keine mehrfachen Primteiler besitzt und
$$p-1 | n-1 \text{ für jeden Primteiler } p \text{ von } n.$$
2. Jede Carmichael-Zahl ist ungerade und besitzt ≥ 3 Primteiler.

Beweis:

(1) n ist eine Carmichael-Zahl gdw $\{x \in U_n \mid x^{n-1} = 1\} = U_n$.

- Mit vorigem Lemma muss damit die folgende Gruppe trivial sein
$$U_n/G \cong U_{2^r} \times \prod_{i=1}^{s} \mathbb{Z}/m_i\mathbb{Z}.$$
- Insbesondere gilt damit $m_i = 1$ für alle i. D.h.
$$m_i = \frac{p_i^{r_i-1}(p_i-1)}{\mathrm{ggT}(p_i-1, n-1)} = 1 \text{ für alle } i.$$
- Dies ist äquivalent zu
$$r_i = 1 \text{ und } \mathrm{ggT}(p_i-1, n-1) = p_i - 1 \text{ bzw. } p_i - 1 | n-1.$$
- Wegen $r_i = 1$ besitzt n keine mehrfachen Primteiler.

Struktur von Carmichael-Zahlen

Beweis: (Fortsetzung)

(2) Sei n Carmichael. Aus $U_n/G \cong U_{2^r} \times \prod_{i=1}^{s} \mathbb{Z}/m_i\mathbb{Z}$ folgt $r \leq 1$.

- Annahme: $r = 1$.
- Da $n \notin \mathbb{P}$ enthält n einen ungeraden Primteiler q.
- Mit (1): Das gerade $q-1$ teilt das ungerade $n-1$. (Widerspruch)
- Annahme: n besitzt nur zwei Primteiler, d.h. $n = pq$ mit $p < q$.
- Aus $q - 1 | n - 1$ folgt
$$0 \equiv n - 1 = pq - 1 = p(q-1) + p - 1 \equiv p - 1 \mod q - 1.$$
- Es folgt $p \equiv 1 \mod q - 1$. Wegen $p < q$ gilt $p = 1$. (Widerspruch)

Bsp: Die drei kleinsten Carmichael Zahlen sind

$$561 = 3 \cdot 11 \cdot 17,\ 1105 = 5 \cdot 13 \cdot 17 \text{ und } 1729 = 7 \cdot 13 \cdot 19.$$

Solovay-Strassen Primzahltest

Satz Solovay-Strassen Primzahltest

Ein ungerades $n \geq 3$ ist prim gdw für alle $a \in \mathbb{Z}$ mit $\mathrm{ggT}(a, n) = 1$ gilt

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \mod n.$$

Falls $a \notin \mathbb{P}$, so gilt die Kongruenz für höchstens die Hälfte aller a.

Beweis:

$\Rightarrow$ Falls n prim ist, so ist die Kongruenz die Euler-Identität.

$\Leftarrow$ Für alle zu n teilerfremden $a \mod n$ gelte $a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \mod n$.

- Annahme: n ist zusammengesetzt.
- Quadrieren liefert $a^{n-1} \equiv 1 \mod n$. D.h. n ist eine Carmichael-Zahl.
- Damit gilt $n = \prod_{i=1}^{s} p_i$ mit $s, p_i \geq 3$.
- CRT liefert einen Isomorphismus $\Phi : U_n \to U_{p_1} \times \ldots \times U_{p_s}$.
- Sei g ein Generator modulo p_1. Damit gilt $(\frac{g}{p_1}) = -1$.
- Sei $a \in \mathbb{Z}$ mit $\Phi(a) = (g, 1, \ldots, 1)$. Für das Jacobi Symbol gilt
  $$\left(\frac{a}{n}\right) = \prod_{i=1}^{s}\left(\frac{a}{p_i}\right) = \prod_{i=1}^{s}\left(\frac{a \mod p_i}{p_i}\right) = \left(\frac{g}{p_1}\right)\prod_{i=2}^{s}\left(\frac{1}{p_i}\right) = (-1).$$

Solovay-Strassen Primzahltest

Beweis: (Fortsetzung)

- Wir zeigen nun, dass $a^{\frac{n-1}{2}} \not\equiv (-1) \bmod n$.
- Es gilt $\Phi(-1) = (-1, \ldots, -1)$, aber $\Phi(a^{\frac{n-1}{2}}) = (g^{\frac{n-1}{2}}, 1, \ldots, 1)$.
- Da $p_i \geq 3$ für alle i, folgt $(-1, \ldots, -1) \neq (g^{\frac{n-1}{2}}, 1, \ldots, 1)$.
- Für dieses a gilt also die Kongruenz nicht. (Widerspruch)

- Sei $A := \{a \in U_n \mid a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right)\}$. Wir zeigen, dass $|A| \leq \frac{1}{2}|U_n|$.
- Wir wissen bereits, dass $A \subsetneq U_n$.
- Ferner ist A eine Untergruppe von U_n. (Übung)
- Damit teilt $|A|$ die Ordnung $|U_n|$, und es folgt $|A| \leq \frac{1}{2}|U_n|$.

Definition Euler-Zeugen

$A := \{a \in U_n \mid a^{\frac{n-1}{2}} = \left(\frac{a}{n}\right)\}$ heißt Menge der *Euler-Zeugen*.

Solovay-Strassen Primzahltest

Algorithmus Solovay-Strassen Primzahltest

EINGABE: $n \in \mathbb{N}$ ungerade, $\ell \in \mathbb{N}$

1. FOR $i = 1$ to ℓ
    1. Wähle $a_i \in \{1, \ldots, n-1\}$ zufällig.
    2. Falls $\mathrm{ggT}(a_i, n) > 1$, Ausgabe "zusammengesetzt" und Abbruch.
    3. Falls $a_i^{\frac{n-1}{2}} \not\equiv (\frac{a_i}{n}) \bmod n$, Ausgabe "zusammengesetzt" und Abbruch.
2. Ausgabe "prim".

Laufzeit: $\mathcal{O}(\ell \log^3 n) = \mathcal{O}(\log^3 n)$ für konstantes ℓ.

Fehlerws Solovay-Strassen Primzahltest

Korrektheit:

- Falls n prim ist, so ist die Ausgabe korrekt.
- Falls n zusammengesetzt ist, erhalten wir Ausgabe "prim" mit

$$\begin{aligned}\mathrm{Ws}[\text{Ausgabe "prim"} \mid n \notin \mathbb{P}] &= \mathrm{Ws}[a_1, \ldots, a_\ell \in A] \\ &= \prod_{i=1}^{\ell} \mathrm{Ws}[a_i \in A] \leq (\tfrac{1}{2})^\ell.\end{aligned}$$

- D.h. wir erhalten $\mathrm{Ws}[\text{Ausgabe "zusammenges."} \mid n \notin \mathbb{P}] \geq 1 - 2^{-\ell}$.
- Für Anwendungen wählt man gewöhnlich $\ell \geq 80$.
- *Vorsicht:* Die Fehlerwahrscheinlichkeit ist nicht höchstens 2^{-80}.
- Ein Fehler entsteht, falls die Ausgabe "prim" ist, obwohl $n \notin \mathbb{P}$.
- D.h. die Fehlerwahrscheinlichkeit des Algorithmus ist

$$\mathrm{Ws}[n \notin \mathbb{P} \mid \text{Ausgabe "prim"}] = \frac{\mathrm{Ws}[\text{Ausgabe "prim"} \mid n \notin \mathbb{P}] \cdot \mathrm{Ws}[n \notin \mathbb{P}]}{\mathrm{Ws}[\text{Ausgabe "prim"}]}$$

$$\leq \quad \frac{\mathrm{Ws}[\text{Ausgabe "prim"} \mid n \notin \mathbb{P}] \cdot \mathrm{Ws}[n \notin \mathbb{P}]}{\mathrm{Ws}[n \in \mathbb{P}]} \approx 2^{-\ell} \log n. \quad \text{(ohne Beweis)}$$

Miller-Rabin Primzahltest

Idee: Für primes n gilt $a^{n-1} \equiv 1 \bmod n$.
Sukzessives Wurzelziehen auf beiden Seiten liefert ± 1.

Satz Miller-Rabin Primzahltest

Ein ungerades $n \geq 3$, n keine Primpotenz mit $n - 1 = 2^r d$, d ungerade, ist prim gdw für alle zu n teilerfremden $a \in \mathbb{Z}$ gilt

$$a^d \equiv 1 \bmod n \text{ oder } a^{2^k d} \equiv (-1) \bmod n \text{ für ein } 0 \leq k < r.$$

Falls $a \notin \mathbb{P}$, erfüllt höchstens ein Viertel aller a die Bedingung.

Beweis:

$\Rightarrow$ Sei n prim und $a \in U_n$ beliebig. Es gilt $a^{n-1} = 1$.

- Falls $a^d \neq 1$, existiert ein minimales $0 \leq k < r$ mit $a^{2^{k+1} d} = 1$.
- Da $a^{2^k d} \neq 1$, gilt $a^{2^k d} = (-1)$, weil 1 die Wurzeln ± 1 besitzt.

$\Leftarrow$ Wir definieren die Primzeugen

$$S := \{a \in U_n | a^d \equiv 1 \bmod n \text{ oder } a^{2^k d} \equiv (-1) \bmod n \text{ für ein } k\}.$$

- Nach Voraussetzung gilt $S = U_n$.
- Damit folgt $a^{n-1} = 1$ für alle $a \in U_n$.

Miller-Rabin Primzahltest

Beweis: (Fortsetzung)

- Angenommen $n \notin \mathbb{P}$. Dann ist n eine Carmichael-Zahl mit $n = \prod_{i=1}^{s} p_i$, $s \geq 3$, p_i ungerade.
- Wir müssen zeigen, dass in diesem Fall $|S| \leq \frac{1}{4}\varphi(n)$.
- Sei $k := \max_{j \in \mathbb{N}_0}\{\exists b \in U_n \text{ mit } b^{2^j d} = (-1)\}$ und $m = 2^k d$.
- Wir definieren die folgenden drei Mengen $K \supseteq L \supseteq M$ mit

$$\begin{aligned} K &:= \{a \in U_n \mid a^m \equiv \pm 1 \bmod p_i \text{ für alle } i\} \\ L &:= \{a \in U_n \mid a^m \equiv \pm 1 \bmod n\} \\ M &:= \{a \in U_n \mid a^m \equiv 1 \bmod n\}. \end{aligned}$$

- Alle Mengen sind Untergruppen von U_n. Es gilt $S \subseteq L$.
- Wir zeigen $|L| = 2|M|$ und $|K| \geq 2^s|M|$. Damit gilt

$$\varphi(n) \geq |K| \geq 2^s|M| = 2^{s-1}|L| \geq 2^{s-1}|S|.$$

- Wegen $s \geq 3$ folgt die Behauptung.

Miller-Rabin Primzahltest

Beweis: (Fortsetzung)

- z.z.: $|L| = 2|M|$. Sei $b \in U_n$ mit $b^m = (-1)$.
- Für jedes $a \in M$ ist $ba \in L$, aber $ba \notin M$.
- Es folgt $L = M \cup b \cdot M$ und damit $|L| = 2|M|$.
- z.z.: $|K| \geq 2^s|M|$.
- Wir konstruieren zu jedem $\epsilon \in \{\pm 1\}^s$ ein $b_\epsilon \in U_n$ mit
$$b_\epsilon^m \equiv \epsilon_i \bmod p_i \text{ für alle } i = 1, \ldots, s.$$
- Dazu betrachten wir wieder $b \in U_n$ mit $b^m \equiv (-1) \bmod n$. Es folgt
$$b^m \equiv (-1) \bmod p_i \text{ und } b^{2m} \equiv 1 \bmod p_i \text{ für alle } i.$$
- Wir konstruieren b_ϵ mittels CRT als Lösung der Kongruenzen
$$x \equiv \begin{cases} b \bmod p_i & \text{falls } \epsilon_i = (-1) \\ b^2 \bmod p_i & \text{falls } \epsilon_i = 1 \end{cases}.$$
- Für die Lösung b_ϵ gilt $b_\epsilon^m \equiv \epsilon_i \bmod p_i$ für alle i.

Miller-Rabin Primzahltest

Beweis: (Fortsetzung)

- Wir definieren $M_a := \{ab_\epsilon | \epsilon \in \{-1,1\}^s\}$ für $a \in M$.
- Es gilt $M_a \subseteq K$. Falls $M_a \cap M_{a'} = \emptyset$ für $a \neq a'$, folgt $|K| \geq 2^s|M|$.
- Annahme: $M_a \cap M_{a'} \neq \emptyset$ für $a \neq a'$ mit $a, a' \in M$.
- Dann existieren ϵ, ϵ' mit $ab_\epsilon \equiv a'b_{\epsilon'} \mod n$. Es folgt
$$(\frac{b_\epsilon}{b_{\epsilon'}})^m \equiv (\frac{a}{a'})^m \equiv 1 \mod n, \text{ da } a, a' \in M.$$
- Es folgt $(\frac{b_\epsilon}{b_{\epsilon'}})^m \equiv 1 \mod p_i$ für alle i.
- b_ϵ, $b_{\epsilon'}$ nehmen mod p_i entweder die Werte b oder b^2 an.
- Falls $b_\epsilon \not\equiv b_{\epsilon'} \mod p_i$ folgt $(\frac{b_\epsilon}{b_{\epsilon'}})^m \equiv (-1) \mod p_i$.
- D.h. $b_\epsilon \equiv b_{\epsilon'} \mod p_i$ für alle i und damit $b_\epsilon \equiv b_{\epsilon'} \mod n$.
- Aus $ab_\epsilon \equiv a'b_{\epsilon'} \mod n$ folgt $a \equiv a' \mod n$. (Widerspruch)

Algorithmus Miller-Rabin Primzahltest

Algorithmus Miller-Rabin Primzahltest

EINGABE: $n \geq 3$ ungerade, $\ell \in \mathbb{N}$

1. Falls n eine Primpotenz ist, Ausgabe "zusammengesetzt".
2. Berechne $n - 1 = 2^r d$ mit d ungerade.
3. Für $i = 1, \ldots, \ell$
   1. Wähle $a_i \in \{1, \ldots, n-1\}$ zufällig.
   2. Falls $\mathrm{ggT}(a_i, n) > 1$, Ausgabe "zusammengesetzt".
   3. Setze $k = 0$. Berechne $a_k := a_i^d \bmod n$
   4. While $a_k \not\equiv 1 \bmod n$ und $k < r$
      1. Setze $k := k + 1$. Berechne $a_k := a_{k-1}^2 \bmod n$.
   5. Falls $k = r$ und $a_k \not\equiv 1 \bmod n$, Ausgabe "zusammengesetzt".
   6. Falls $k > 0$ und $a_{k-1} \not\equiv (-1) \bmod n$, Ausgabe "zusammengesetzt".
4. Ausgabe "prim".

Algorithmus Miller-Rabin Primzahltest

- **Laufzeit:** $\mathcal{O}(\ell \log^3 n) = \mathcal{O}(\log^3 n)$ für konstantes ℓ.
  Übung: Schritt 1 kann in Laufzeit $\mathcal{O}(\log^3 n)$ realisiert werden.
- **Korrektheit:** Für primes n ist die Ausgabe stets korrekt.
- Für $n \notin \mathbb{P}$ gilt analog zur Analyse des Solovay-Strassen Tests

$$\begin{aligned} \mathrm{Ws}[\text{Ausgabe "prim"} \mid n \notin \mathbb{P}] &= \mathrm{Ws}[a_1, \ldots, a_\ell \in S] \\ &= \textstyle\prod_{i=1}^{\ell} \mathrm{Ws}[a_i \in S] \leq (\frac{1}{4})^\ell. \end{aligned}$$

- D.h. wir benötigen für die gleiche Schranke wie im Solovay-Strassen Test nur die Hälfte der Iterationen ℓ.
- Man kann sogar zeigen, dass $S \subseteq A$.
- D.h. die Primzeugen sind in den Euler-Zeugen enthalten.
- Seien also $a_1, \ldots, a_\ell$ eine Wahl der Zahlen in Schritt 3.1, so dass der Miller-Rabin Test $n \notin \mathbb{P}$ irrtümlich als prim ausweist.
- Dann irrt auch der Solovay-Strassen Test für $a_1, \ldots, a_\ell$.
- D.h. der Miller-Rabin Test beinhaltet den Solovay-Strassen Test.

Agarwal-Kayal-Saxena Primzahltest (2002)

Satz AKS-Primzahltest

Ein $n \in \mathbb{N}$, n keine Primzahlpotenz, ist prim gdw für alle $a \in \mathbb{Z}$ gilt

$$(X+a)^n \equiv X^n + a \mod n \text{ im Polynomring } (\mathbb{Z}/n\mathbb{Z})[X].$$

Beweis:

$\Rightarrow$ Sei n prim. Mit der Binomischen Formel mod n (Folie 48) gilt

$$(X+a)^n \equiv X^n + a^n \equiv X^n + a \mod n.$$

$\Leftarrow$ Sei $n \notin \mathbb{P}$. Schreibe $n = p^\ell m$ für $p \in \mathbb{P}$, $\ell \geq 1$ und $\mathrm{ggT}(p,m) = 1$.

- Wir zeigen $(X+1)^n \not\equiv X^n + 1 \mod n$. Der Koeffizient von X^p ist
$$\binom{n}{p} = \frac{n(n-1)\ldots(n-p+1)}{p(p-1)\ldots 1} \in \mathbb{N}.$$
- Im Zähler ist $n = p^\ell m$ durch p teilbar.
- Damit sind $n-1, n-2, \ldots, n-(p-1)$ nicht durch p teilbar.
- Im Nenner taucht ebenfalls ein p auf. Damit können wir schreiben
$$\binom{n}{p} = p^{\ell-1} m' \text{ mit } \mathrm{ggT}(p,m) = 1.$$
- Es folgt $\binom{n}{p} \not\equiv 0 \mod p^\ell$ und mittels CRT auch $\binom{n}{p} \not\equiv 0 \mod n$.
- D.h. der Koeffizient von X^p verschwindet in $(X+1)^n$ nicht.

Agarwal-Kayal-Saxena Primzahltest

Anmerkung:

- Im AKS-Algorithmus (2002) wird $(X + a)^n \equiv X^n + a \bmod n$ modulo Polynomen $X^r - 1$ kleinen Grades $r = \mathcal{O}(\log^{\frac{15}{2}} n)$ getestet.
- Dies führt zu einem deterministischen Primzahltest ohne Fehler.
- Allerdings ist der AKS-Test deutlich langsamer als Miller-Rabin.

Faktorisierungsalgorithmen

Idee: Konstruiere $x, y \in \mathbb{Z}$ mit $x^2 \equiv y^2 \bmod n$ und $x \not\equiv \pm y \bmod n$.
Ziel: Berechne nicht-trivialen Teiler von n, faktorisiere rekursiv.

Lemma Differenz von Quadraten

1. Sei $n \notin \mathbb{P}$ ungerade. Dann existieren $x, y \in \mathbb{N}_0$ mit
$$n = x^2 - y^2 \text{ und } x \not\equiv \pm y \bmod n.$$
2. Sei $x^2 \equiv y^2 \bmod n$ mit $x, y, c \in \mathbb{Z}$ und $x \not\equiv \pm y \bmod n$. Dann sind $a := \mathrm{ggT}(x+y, n)$ und $b := \mathrm{ggT}(x-y, n)$ nicht-triviale Teiler von n.

Beweis:

(1) Sei $n = ab$ mit $2 < b \leq a \leq n$. Setze $x = \frac{a+b}{2}, y = \frac{a-b}{2} \in \mathbb{N}_0$.

- Dann gilt $x^2 - y^2 = \frac{(a+b)^2-(a-b)^2}{4} = \frac{4ab}{4} = n$.
- Wir zeigen $x \not\equiv y \bmod n$. Analog folgt $x \not\equiv -y \bmod n$.
- Aus der Annahme $x \equiv y \bmod n$ folgt
$\frac{a+b}{2} \equiv \frac{a-b}{2} \bmod n \Leftrightarrow 2b \equiv 0 \bmod 2n \Leftrightarrow b \equiv 0 \bmod n$. (Widerspruch)

Differenz von Quadraten

(2) Aus $x^2 - y^2 = cn$ folgt $(x+y)(x-y) \equiv n$, d.h. $n | (x+y)(x-y)$.

- Wegen $x \pm y \not\equiv 0 \mod n$ sind beide Faktoren kein Vielfaches von n.
- D.h für $a = \mathrm{ggT}(x+y, n)$ und $b = \mathrm{ggT}(x-y, n)$ gilt $a, b < n$.
- Annahme: $a = \mathrm{ggT}(x+y, n) = 1$ (analog für b). Dann gilt

  $$n = \mathrm{ggT}((x+y)(x-y), n) = \mathrm{ggT}(x-y, n) = b \text{ (Widerspruch).}$$
- D.h. für beide Teiler a, b von n gilt $1 < a, b < n$.

Fermat Faktorisierung

Algorithmus Fermat Faktorisierung

EINGABE: $n \in \mathbb{N}$ zusammengesetzt

1. Setze $x := \lceil \sqrt{n} \rceil - 1$.
2. REPEAT
   1. Setze $x := x + 1$ und $z := x^2 - n$.
   2. Falls $z = y^2$ berechne y.
3. UNTIL $z = y^2$ für ein $y \in \mathbb{N}$ und $x \not\equiv \pm y \mod n$.

AUSGABE: $\mathrm{ggT}(x \pm y, n)$

Korrektheit: folgt aus vorigem Lemma.

Bsp. Fermat Faktorisierung

Bsp:

- Für $n = 187$ gilt $x = \lceil \sqrt{n} \rceil = 14$ und $x^2 - n = 196 - 187 = 3^2$.
- Es gilt $14 \not\equiv \pm 3 \mod 187$.
- Wir erhalten $\mathrm{ggT}(14 \pm 3, 187) = \{11, 17\}$ mit $11 \cdot 17 = 187$.
- Für $n = 175$ ist $x = 14$. Die erste Quadratzahl ist
$$(x+6)^2 - n = 20^2 - n = 400 - 175 = 225 = 15^2.$$
- Es gilt $20 \not\equiv \pm 15 \mod 175$.
- Wir erhalten $\mathrm{ggT}(20 \pm 15, 175) = \{5, 35\}$ mit $5 \cdot 35 = 175$.

Laufzeit Fermat Faktorisierung

Laufzeit:

- Sei $n = ab$ ungerade mit $1 < b \leq \sqrt{n} \leq a < n$.
- Für $x = \frac{a+b}{2} \geq \sqrt{ab} = \sqrt{n}$ ist $x^2 - n = y^2$ mit $y = \frac{a-b}{2}$.
- Es folgt $(x + \sqrt{n})(x - \sqrt{n}) = y^2$.
- Die Iterationen in Schritt 2 sind damit beschränkt durch
$$x - \sqrt{n} = \frac{y^2}{x+\sqrt{n}} \leq \frac{(\frac{a-b}{2})^2}{2\sqrt{n}} \leq \frac{(a-b)^2}{8\sqrt{n}}.$$
- D.h. für $n = ab$ mit Differenz $a - b = \mathcal{O}(n^{\frac{1}{4}})$ ist dies konstant.
- Für $n = ab$ mit a, b gleicher Bitgröße gilt $a - b = \mathcal{O}(\sqrt{n})$ und damit $x - \sqrt{n} = \mathcal{O}(\sqrt{n})$. Dies ist vergleichbar mit Probedivision.
- I. Allg. gilt $a - b = \mathcal{O}(n)$ und wir erhalten $\mathcal{O}(n^{\frac{3}{2}})$ Iterationen.

Motivation Faktorbasis

Bsp: : Wir betrachten die Fermat Faktorisierung von $93 = 3 \cdot 31$.

- Es gilt $\lceil \sqrt{93} \rceil = 10$. Wir erhalten folgende Liste

x	10	11	12	13	14	15	16	17
$x^2 - 93$	7	28	51	76	103	132	163	196

- D.h. das erste Quadrat taucht bei $17 = \frac{3+31}{2}$ auf.
- Aus den ersten beiden Einträgen folgt aber
$$10^2 \equiv 7 \bmod 93 \text{ und } 11^2 \equiv 28 = 2^2 \cdot 7 \bmod 93.$$
- Multiplikation beider Gleichungen liefert
$$(10 \cdot 11)^2 \equiv (17)^2 \equiv 2^2 \cdot 7^2 = (14)^2 \bmod 93.$$
- Es gilt $17 \not\equiv \pm 14 \bmod 93$ und $\mathrm{ggT}(17 \pm 14, 93) = \{3, 31\}$.

Ziel: Kombiniere die Gleichungen, so dass ein Quadrat entsteht.

Faktorbasis

Definition Faktorbasis

Für ein $b \in \mathbb{N}$ definieren wir die Faktorbasis

$$F_b = \{-1\} \cup \{p \in \mathbb{P} \mid p \leq b\}.$$

Ein $n \in \mathbb{Z}$ heißt *b-glatt*, falls $n = \prod_{p \in F_b} p^{e_p}$ mit $e_p \in \mathbb{N}_0$.

Bsp: -28 ist 7-glatt, aber nicht 5-glatt.

High-Level Faktorisierung mit Faktorbasen

Algorithmus FAKTORBASIS

EINGABE: $n \in \mathbb{N}$

1. Wähle $b \in \mathbb{N}$ geeignet. Sei $F_b = \{p_1, \ldots, p_s\}$.
2. Definiere leere Matrix E.
3. For $i = 0 \ldots s$
   1. Wähle x_i solange, bis $z_i \equiv x_i^2 \bmod n$ b-glatt. Schreibe $z_i = \prod_{j=1}^{s} p_j^{e_{i,j}}$.
   2. Nimm $(e_{i,1} \bmod 2, \ldots, e_{i,s} \bmod 2)$ als Zeile in E auf.
4. Berechne $f \in \mathbb{F}_2^{s+1} \setminus \{0\}^{s+1}$ mit $fE = \{0\}^s$ über $\mathbb{F}_2$, d.h.
$$\sum_{i=1}^{s+1} f_i e_{i,j} \equiv 0 \bmod 2 \text{ für alle } j = 1, \ldots, s.$$
5. Setze $x \equiv \prod_{i=1}^{s+1} x_i^{f_i} \bmod n$ und $y \equiv \prod_{j=1}^{s} p_j^{\frac{\sum_{i=1}^{s+1} f_i e_{i,j}}{2}} \bmod n$.
6. Falls $x \equiv \pm y \bmod n$, zurück zu Schritt 4 (oder zu Schritt 3).

AUSGABE: $\mathrm{ggT}(x \pm y, n)$

Korrektheit Faktorbasen-Faktorisierung

Korrektheit: Es gilt

$$\begin{aligned} x^2 \equiv \prod_{i=1}^{s+1}(x_i^2)^{f_i} \equiv \prod_{i=1}^{s+1} z_i^{f_i} &= \prod_{i=1}^{s+1} \prod_{j=1}^{s} p_j^{f_i e_{i,j}} \\ &= \prod_{j=1}^{s} p_j^{\sum_{i=1}^{s+1} f_i e_{i,j}} \equiv y^2 \bmod n. \end{aligned}$$

Wahl der Faktorbasis:

- Wahl eines kleinen b führt zu kleiner Anzahl Iterationen von Schritt 3, allerdings auch zu einer kleinen Ws b-glatter z_i in Schritt 3.1.
- Analyse der Dichte von b-glatten Zahlen führt zur optimalen Wahl
$$b = \exp(\tfrac{1}{2}\sqrt{\ln n \ln \ln n}).$$
- Wir integrieren bei der Fermat-Faktorisierung mit $z_i = x_i^2 - n$ nur solche $p \in F_b$ in der Faktorbasis, bei denen $(\frac{n}{p}) = 1$ gilt.
- Sei p ein Teiler von z_i. Wegen $z_i = x_i^2 - n$ folgt $x_i^2 \equiv n \bmod p$.
- D.h. n muss ein quadratischer Rest modulo p sein.

Ziel: Wähle x_i so, dass $z_i \equiv x_i^2 \bmod n$ mit großer Ws b-glatt ist. Für

$$x_i = \lceil \sqrt{n} \rceil + i \text{ gilt } z_i \approx 2i\sqrt{n}.$$

Kettenbruch Faktorisierung von Morrison-Brillhart

Idee der Kettenbruch Faktorisierung:

- Berechne den Kettenbruch von $\sqrt{n}$ mit Näherungsbrüchen $\frac{p_i}{q_i}$.
- Wähle $z_i := p_i^2 - nq_i^2$. Insbesondere gilt dann $z_i \equiv p_i^2 =: x_i^2 \mod n$.

Lemma

Sei $n \in \mathbb{N}$ kein Quadrat und $\frac{p_i}{q_i}$ Näherungsbruch von $\sqrt{n}$. Dann gilt

$$|p_i^2 - nq_i^2| < 2\sqrt{n}.$$

Beweis: Für Näherungsbrüche gilt $|\sqrt{n} - \frac{p_i}{q_i}| \leq \frac{1}{q_i q_{i+1}}$. Es folgt

$$\begin{aligned} |p_i^2 - nq_i^2| &= q_i^2 |n - (\tfrac{p_i}{q_i})^2| = q_i^2 |\sqrt{n} - \tfrac{p_i}{q_i}| \cdot |2\sqrt{n} + \tfrac{p_i}{q_i} - \sqrt{n}| \\ &\leq \frac{q_i}{q_{i+1}} (2\sqrt{n} + \frac{1}{q_i q_{i+1}}) \end{aligned}$$

- Die Behauptung folgt mittels $q_{i+1} \geq q_i + 1$ aus

$$\begin{aligned} |p_i^2 - nq_i^2| - 2\sqrt{n} &\leq 2\sqrt{n}\left(\frac{q_i}{q_{i+1}} + \frac{1}{2\sqrt{n}q_{i+1}^2} - 1\right) \\ &< 2\sqrt{n}\left(\frac{q_i}{q_{i+1}} + \frac{1}{q_{i+1}} - 1\right) \leq 0. \end{aligned}$$

Wahl der Faktorbasis bei Morrison-Brillhart

Faktorbasis bei Morrison-Brillhart:

- Wir wählen wiederum nur solche $p \in B$ mit $(\frac{n}{p}) = 1$.
- Sei p ein Primteiler von $z_i = p_i^2 - nq_i^2$.
- Aus $z_i = p_i^2 - nq_i^2$ folgt daher $(\frac{p_i}{q_i})^2 \equiv n \mod p$, falls $q_i \in U_p$.
- Damit ist n ein quadratischer Rest modulo p.
- Annahme: $q_i \notin U_p$, d.h. $p|q_i$.
- Aus $p|z_i$ und $p|q_i$ folgt $p|z_i + nq_i^2$.
- Damit gilt $p|p_i$ und $\mathrm{ggT}(p_i, q_i) \geq p$. (Widerspruch: $\mathrm{ggT}(p_i, q_i) = 1$)

Bsp. Morrison-Brillhart Faktorisierung

Bsp: Wir faktorisieren $n = 133 = 7 \cdot 19$.

- Wir wählen $b = 5$ als Glattheitsschranke. Es gilt
$$\left(\frac{133}{2}\right) = \left(\frac{1}{2}\right) = 1, \left(\frac{133}{3}\right) = \left(\frac{1}{3}\right) = 1 \text{ und } \left(\frac{133}{5}\right) = \left(\frac{3}{5}\right) = (-1).$$
- D.h. wir wählen die Faktorbasis $B = \{-1, 2, 3\}$.
- Der Kettenbruchalgorithmus liefert
$$\sqrt{133} = [11, 1, 1, 7, 5, 1, 1, 1, 2, 1, 1].$$
- Die ersten Näherungsbrüche sind damit $11, 12, \frac{23}{2}, \frac{173}{15}, \frac{888}{77}, \frac{1061}{92}$.
- Unser Algorithmus FAKTORBASIS liefert uns folgende Relationen.

$x_i \equiv p_i \bmod n$	$z_i = p_i^2 - nq_i^2$	e_i	$e_i \bmod 2$
11	$-12 = (-1) \cdot 2^2 \cdot 3$	$(1, 2, 1)$	$(1, 0, 1)$
12	11		
23	$-3 = (-1) \cdot 3$	$(1, 0, 1)$	$(1, 0, 1)$
40	$4 = 2^2$	$(0, 2, 0)$	$(0, 0, 0)$
90	-13		
130	$9 = 3^2$	$(0, 0, 2)$	$(0, 0, 0)$

Bsp. Morrison-Brillhart Faktorisierung

- Die letzte Relation liefert
$$130^2 \equiv 3^2 \bmod 133.$$
- Allerdings gilt $130 \equiv -3 \bmod 133$. D.h. die Relation ist nutzlos.
- Die ersten beiden Relationen sind linear abhängig und liefern
$$(11 \cdot 23)^2 \equiv 120^2 \equiv ((-1)^1 2^1 3^1)^2 = (-6)^2 \bmod 133.$$
- Es gilt $120 \not\equiv \pm 6 \bmod 133$ und damit
$$\mathrm{ggT}(120 \pm 6, 133) = \mathrm{ggT}(-13 \pm 6, 133) = \{7, 19\}.$$
- Ebenso erhält man die Faktorisierung aus der 3. Relation
$$40^2 \equiv 2^2 \bmod 133.$$

Anmerkung:

- Oft liefern die Näherungsbrüche nicht genügend viele Relationen.
- Hier betrachtet man zusätzlich die Kettenbrüche von
$$\sqrt{kn} \text{ für kleine } k \in \mathbb{N}.$$
- *Vorsicht:* In diesem Fall kann man nur Primzahlen p mit $(\frac{kn}{p}) = (-1)$ für alle k in der Fakorbasis ausschließen.

Quadratisches Sieb

Idee: Statt Teilbarkeit für die z_i sukzessive zu testen, berechne für viele z_i gleichzeitig die Teilbarkeit durch $p_i^{e_i}$ mit $p_i \in B$.

Prinzip des Siebens:

- Im Fermat Algorithmus ist $z_i := x_i^2 - n$ durch p teilbar gdw
$$x^2 \equiv n \bmod p.$$
- D.h. wir berechnen die Lösungen $\pm x_p$ dieser Kongruenz.
- Diese Lösungen existieren, da $(\frac{n}{p}) = 1$ für alle $p \in B$.
- Damit sind genau diejenigen z_i mit $x_i \equiv \pm x_p \bmod p$ durch p teilbar.
- Diese z_i werden durch p dividiert.
- Analog verfährt man für die Primpotenzen. D.h. wir berechnen Lösungen von $x^2 \equiv n \bmod p^r$ für hinreichend großes r.
(Einen Algorithmus dafür werden wir später kennenlernen.)
- Durch sukzessives Dividieren werden die b-glatten z_i zu 1.

Bsp. Quadratisches Sieb

Bsp: Wir faktorisieren die Zahl $91 = 7 \cdot 13$.

- Als Glattheitsschranke wählen wir $b = 5$.
- Wir faktorisieren nur positive Zahlen $z_i := x_i^2 - n = (10 + i)^2 - n$.
- Daher wählen wir $B = \{2, 3, 5\}$. Es gilt $(\frac{n}{p}) = 1$ für alle $p \in B$.
- Wir wollen die Zahlen z_i im Intervall $0 \leq i \leq 9$ sieben.
- Damit gilt $z_i \leq z_9 = 19^2 - n = 270$.
- Wir berechnen alle Lösungen von $x^2 \equiv 91 \bmod p^r$ mit $p^r \leq 270$.

$p \backslash r$	1	2	3	4	5
2	1	–	–	–	–
	(11)				
3	± 1	± 1	± 19	± 46	± 127
	$(10, 11)$	$(10, 17)$	$(19, 35)$	$(46, 35)$	$(127, 35)$
5	± 1	± 21	± 96		
	$(11, 14)$	$(29, 21)$	$(29, 96)$		

Bsp. Quadratisches Sieb

- Für eine Lösung $\pm x_{p^r}$ steht in der Klammer das kleinste $x_i \geq 10$ mit $x_i \equiv x_{p^r} \mod p^r$ bzw. $x_i \equiv -x_{p^r} \mod p^r$.
- Bsp: z_{10} ist durch 3^2 teilbar und damit auch alle $z_{10+3^2\mathbb{Z}}$.
- Wir erhalten die folgenden partiellen Faktorisierungen.

x_i	$z_i = x_i^2 - n$	teilbar durch	Cofaktor
10	9	3^2	1
11	30	$2 \cdot 3 \cdot 5$	1
12	53	–	53
13	78	$2 \cdot 3$	13
14	105	$3 \cdot 5$	7
15	134	2	67
16	165	$3 \cdot 5$	11
17	198	$2 \cdot 3^2$	11
18	233	–	233
19	270	$2 \cdot 3^3 \cdot 5$	1

Bsp. Quadratisches Sieb

- Die Zeilen 11 und 19 liefern die Kongruenz
$$(11 \cdot 19)^2 \equiv 27^2 \equiv (2 \cdot 3^2 \cdot 5)^2 = 90^2 \equiv (-1)^2 \bmod 91.$$
- Es gilt $27 \not\equiv \pm 1 \bmod 91$ und $\mathrm{ggT}(27 \pm 1, 91) = \{7, 13\}$.

Anmerkungen:

- In der “Large Prime”-Variante des Siebs werden Zeilen mit demselben Co-Faktor verwendet.
- Bsp.: Für $x_i = 16$ und 17 erhalten wir die zusätzliche Relation
$$(16 \cdot 17 \cdot 11^{-1})^2 \equiv 2 \cdot 3^3 \cdot 5 \bmod 91.$$
- **Laufzeit:** Das Quadratischen Sieb benötigt Zeit $e^{\sqrt{\ln n \ln \ln n}}$. (unter geeigneten Glattheitsannahmen)
- Dies ist superpolynomiell aber supexponentiell in $\ln n$.

Pollards $p-1$ Methode

Idee:

- Sei $n = pr$ mit $1 < p < n$, p prim, $p \nmid r$. D.h. $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/r\mathbb{Z}$.
- Sei $p-1$ b-glatt, d.h. $p-1 = \prod_{p \in B} p^{e_B}$.
- Sei k ein Vielfaches von $\prod_{p \in B} p^{e_B}$. Dann gilt

$$a^k \equiv 1 \bmod p \text{ für alle } a \in U_n.$$

- Falls zusätzlich $a^k \not\equiv 1 \bmod r$ folgt $p \leq \mathrm{ggT}(a^k - 1, n) < n$.

Algorithmus Pollards $p-1$-Methode

EINGABE: $n = pr$ zusammengesetzt, p prim, Schranke C mit $p \leq C$.

1. Wähle b geeignet, so dass $p-1$ b-glatt ist. Sei $B = \{p_1, \ldots, p_s\}$.
2. Wähle $a \in_R \{2, \ldots, n-1\}$. Falls $\mathrm{ggT}(a, n) > 1$, Ausgabe des ggTs.
3. Für $i = 1 \ldots s$
    1. Wähle e_i maximal mit $p_i^{e_i} < C$. Berechne $a := a^{p_i^{e_i}} \bmod N$.
4. Falls $\mathrm{ggT}(a-1, N) \notin \{1, N\}$, Ausgabe des ggTs.

Analyse von Pollards $p-1$-Methode

Korrektheit:

- In Schritt 3.1 wird $a^k \bmod N$ berechnet mit $k = \prod_{i=1}^{s} p_i^{e_i}$.
- Falls $p-1$ b-glatt ist, gilt $p-1|k$.
- Damit ist $\mathrm{ggT}(a^k-1, n) \geq p$.
- D.h. wir finden einen nicht-trivialen Teiler, falls $\mathrm{ggT}(a^k-1, n) < n$.
- Sei q ein Primteiler von r, so dass $q-1$ nicht b-glatt ist.
- Damit existiert ein $q'|q-1$, $q' \in \mathbb{P}$ mit $q' > b$.
- Ferner gelte $q'|\mathrm{ord}(a)$ in U_q. Dann gilt
$$a^k \not\equiv 1 \bmod q \text{ und damit } \mathrm{ggT}(a^k-1, n) < n.$$
- Wir berechnen die Ws, dass $q'|\mathrm{ord}(a)$ in U_q.
- Sei U_q zyklisch mit Generator g. Wir schreiben $a \equiv g^i \bmod q$.
- Es folgt $\mathrm{ord}(a) = \frac{q-1}{\mathrm{ggT}(i,q-1)}$ in U_q. Falls $q' \nmid i$, gilt $q'|\mathrm{ord}(a)$.
- Da a zufällig gewählt ist, geschieht dies mit Ws $1 - \frac{1}{q'}$.

Analyse von Pollards $p-1$-Methode

Laufzeit:

- Schritt 3 benötigt Zeit $\mathcal{O}(s \log C \log N^2) = \mathcal{O}(s \log^3 N)$.

Problem der $p-1$-Methode:

- Die Laufzeit ist abhängig von der Ordnung von U_p.
- Sei $\frac{p-1}{2} \in \mathbb{P}$ mit $\frac{p-1}{2} \approx \sqrt{n}$.
- Dann benötigen wir $p_s \approx \sqrt{n}$ und damit
$$s = |\{x \in \mathbb{P} \mid x \leq p_s\}| \approx \frac{\sqrt{n}}{\log n}.$$
- In diesem Fall ist die Laufzeit nicht besser als bei Probedivision.

Quadratische Erweiterung

Ziel:

- $\mathbb{F}_{p^2}^*$ besitzt Ordnung $|\mathbb{F}_{p^2}^*| = p^2 - 1 = (p+1)(p-1)$.
- Wir konstruieren eine Untergruppe von $\mathbb{F}_{p^2}^*$ mit Ordnung $p+1$.
- Unsere Hoffnung ist, dass $p+1$ in kleine Primfaktoren zerfällt.

Definition

Sei R ein kommutativer Ring, $D \in R$ kein Quadrat. $R[\sqrt{D}] = R \oplus R\sqrt{D}$ heißt *quadratische Erweiterung* von R. Sei $\omega = x + y\sqrt{D} \in R[\sqrt{D}]$.

1. Das zu ω *konjugierte* Element ist definiert als $\bar{\omega} = x - y\sqrt{D}$.
2. Die *Spur* ist definiert als $\mathrm{Tr} : R[\sqrt{D}] \to R, \omega \mapsto \omega + \bar{\omega}$ mit
$$\mathrm{Tr}(x + y\sqrt{D}) = 2x.$$
3. Die *Norm* ist definiert als $N : R[\sqrt{D}] \to R$, $\omega \mapsto \omega\bar{\omega}$ mit
$$N(x + y\sqrt{D}) = x^2 - Dy^2.$$

Anmerkung: Die Spur ist additiv, die Norm multiplikativ.

Eigenschaften von Norm und Spur

Lemma Eigenschaften von Norm und Spur

Sei $\omega \in R[\sqrt{D}]$ beliebig. Es gilt

1. $\omega \in R[\sqrt{D}]^*$ gdw $N(\omega) \in R^*$.
2. $\omega, \bar{\omega}$ sind Nullstellen des Polynoms $X^2 - \mathrm{Tr}(\omega)X + N(\omega)$.

Beweis:

(1) $\Rightarrow$: Sei $\omega \in (R[\sqrt{D}])^*$. Dann gilt

$$1 = N(1) = N(\omega\omega^{-1}) = N(\omega)N(\omega^{-1}).$$

- D.h. $N(\omega)|1$ und damit $N(\omega) \in R^*$.
- $\Leftarrow$: Sei $N(\omega) \in R^*$. Für $\omega^{-1} := \bar{\omega}N(\omega)^{-1}$ gilt

$$\omega\omega^{-1} = \omega\bar{\omega}N(\omega)^{-1} = N(\omega)N(\omega)^{-1} = 1.$$

(2) Offenbar sind ω und $\bar{\omega}$ Nullstellen des Polynoms

$$(X - \omega)(X - \bar{\omega}) = X^2 - (\omega + \bar{\omega})X + \omega\bar{\omega} = X^2 - \mathrm{Tr}(\omega)X + N(\omega).$$

Der Körper $\mathbb{F}_{p^2}$

Satz Körper $\mathbb{F}_{p^2}$

Sei p prim und $(\frac{D}{p}) = (-1)$. Dann ist $\mathbb{F}_{p^2} := \mathbb{F}_p[\sqrt{D}]$ ein Körper mit p^2 Elementen.

Beweis:

- Wir betrachten die Norm-Abbildung $N : \mathbb{F}_{p^2} \to \mathbb{F}_p$ mit $\omega \mapsto \omega\bar{\omega}$.
- Zeigen $N(\omega) \not\equiv 0 \mod p$ für alle $\omega = x + y\sqrt{D} \in \mathbb{F}_p[\sqrt{D}] \setminus \{0\}$.
- Damit ist $N(\omega) \in \mathbb{F}_p^*$ und ω ist invertierbar.
- Annahme: $N(\omega) = x^2 - y^2 D \equiv 0 \mod p$.
- Damit gilt $x^2 \equiv y^2 D \mod p$.
- Es gilt $y \in U_p$, denn für $y \equiv 0$ folgt $x \equiv 0$. (Widerspruch: $\omega \neq 0$)
- Es folgt $D \equiv (\frac{x}{y})^2 \mod p$. (Widerspruch: D ist ein Nichtrest.)
- Ferner gilt $\mathbb{F}_p[\sqrt{D}] \cong \mathbb{F}_p \oplus \mathbb{F}_p\sqrt{D}$. D.h. $|\mathbb{F}_p[\sqrt{D}]| = p^2$.

Der Frobenius-Automorphismus

Definition Froebenius-Automorphismus

Sei $p \in \mathbb{P} \setminus \{2\}$. Der *Frobenius-Automorphismus* auf $\mathbb{F}_{p^2}$ ist die Abbildung

$$f_p : \mathbb{F}_{p^2} \to \mathbb{F}_{p^2} \text{ mit } \omega \mapsto \omega^p.$$

Anmerkungen:

- Wir wissen bereits, dass f_p homomorph ist, d.h.
$$f_p(xy) = f_p(x)f_p(y) \text{ und } f_p(x+y) = f_p(x) + f_p(y).$$
- Damit ist f_p ein Ring-Homomorphismus.
- Da $\mathrm{Ker}(f_p) = \{0\}$ ist f_p bijektiv, d.h. f_p ist ein Automorphismus.

Eigenschaften des Frobenius

Satz Eigenschaften des Frobenius

Sei $p \in \mathbb{P} \setminus \{2\}$. Dann gilt

1. $\{\omega \in \mathbb{F}_{p^2} \mid f_p(\omega) = \omega\} = \mathbb{F}_p$
2. $f_p(\omega) = \bar{\omega}$ für alle $\omega \in \mathbb{F}_{p^2}$.

Beweis:

(1) Mittels Kleinem Fermat gilt $f_p(x) = x^p = x$ für alle $x \in \mathbb{F}_p$.

- Damit gilt $f_p(\omega) = \omega = \bar{\omega}$ bereits für alle $\omega \in \mathbb{F}_p$.
- Das Polynom $g(X) = X^p - X$ besitzt also die p Nullstellen $\omega \in \mathbb{F}_p$.
- $g(X)$ kann aber in $\mathbb{F}_{p^2}$ höchstens p Nullstellen besitzen.
- D.h. die Fixpunkte des Frobenius sind genau die Elemente aus $\mathbb{F}_p$.

(2) Sei $\omega \in \mathbb{F}_{p^2} \setminus \mathbb{F}_p$ und damit $f_p(\omega) \neq \omega$. Wir betrachten das Polynom

$$h(X) = X^2 - \mathrm{Tr}(\omega)X + N(\omega).$$

- Wir wissen $h(\omega) = 0$. Mit Hilfe der Linearität des Frobenius folgt
$$h(f_p(\omega)) = f_p(h(\omega)) = f_p(0) = 0.$$
- Damit ist $f_p(\omega)$ eine Nullstelle von $h(X)$.
- Die einzigen beiden Nullstellen sind aber ω und $\bar{\omega}$. D.h. $f_p(\omega) = \bar{\omega}$.

Eigenschaften des Frobenius

Korollar

Es gilt $N(\omega) = \omega\bar{\omega} = \omega^{p+1}$ für alle $\omega \in \mathbb{F}_{p^2}$.

Satz Norm-1 Gruppe

Sei $p \in \mathbb{P} \setminus \{2\}$ und $G_p := \{\omega \in \mathbb{F}_{p^2}^* \mid N(\omega) = 1\}$. Dann ist $(G_p, \cdot)$ eine Gruppe mit Ordnung $p + 1$.

Beweis:

- Da die Norm multiplikativ ist, bildet $(G_p, \cdot)$ eine Gruppe.
- z.z.: $|G_p| = p + 1$. Betrachte die Norm-Abbildung $N : \mathbb{F}_{p^2}^* \to \mathbb{F}_p^*$.
- $N(\omega) = \omega^{p+1} = 1$ kann in $\mathbb{F}_{p^2}^*$ höchstens $p + 1$ Lösungen besitzen.
- Damit gilt $|G_p| = |\mathrm{Ker}(N))| \leq p + 1$.
- Außerdem gilt $|\mathrm{Im}(N)| \leq |\mathbb{F}_p^*| = p - 1$. Insgesamt erhalten wir
$$|\mathbb{F}_{p^2}^*| = p^2 - 1 = (p + 1)(p - 1) = |\mathrm{Ker}(N)| \cdot |\mathrm{Im}(N)|.$$
- Damit folgt $|\mathrm{Im}(N)| = p - 1$ und $|G_p| = |\mathrm{Ker}(N)| = p + 1$.

Quadratwurzeln, revisited

Korollar

Es gilt $|\{\omega \in \mathbb{F}_{p^2} | N(\omega) = a\}| = p + 1$ für alle $a \in \mathbb{F}_p^*$.

Beweis: Alle Nebenklassen von G_p besitzen Kardinalität $p + 1$.

Idee des Quadratwurzel-Ziehens in quadratischen Erweiterungen:

- Sei $a \in U_p$ mit $(\frac{a}{p}) = 1$. Gesucht ist ein x mit $x^2 \equiv a \bmod p$.
- Wir konstruieren dazu ein $\omega \in \mathbb{F}_{p^2}^*$ mit $N(\omega) = a$.
- Setze $x :\equiv \omega^{\frac{p+1}{2}} \bmod p$. Es folgt $x^2 \equiv \omega^{p+1} \equiv N(\omega) \equiv a \bmod p$.

Ziel: Konstruktion von $\omega \in \mathbb{F}_{p^2}^*$ mit $N(\omega) = a$.

Konstruktion eines Elements mit Norm a

Lemma Konstruktion eines Elements mit Norm a

Sei $p \in \mathbb{P} \setminus \{2\}$, $(\frac{a}{p}) = 1$. Sei $b \in \mathbb{F}_p$, $D := b^2 - a$ mit $(\frac{D}{p}) = (-1)$.

1. Das Element $\omega := b + \sqrt{D} \in \mathbb{F}_p[\sqrt{D}]$ besitzt Norm $N(\omega) = a$.
2. Die Anzahl aller $b \in \mathbb{F}_p$ mit $(\frac{b^2-a}{p}) = (-1)$ ist mindestens $\frac{1}{2}(p-1)$.

Beweis:

(1) Für $\omega = b + \sqrt{D} \in \mathbb{F}_p[\sqrt{D}]$ gilt

$$N(\omega) = (b + \sqrt{D})(b - \sqrt{D}) = b^2 - D = a.$$

(2) Für alle $\omega \in \mathbb{F}^*_{p^2} \setminus \mathbb{F}^*_p$ mit $N(\omega) = a$ gilt für $b := \frac{1}{2}\mathrm{Tr}(\omega)$

$$\omega^2 - 2b\omega + a \equiv 0 \bmod p, \text{ d.h. } \omega = b \pm \sqrt{b^2 - a}.$$

- Wegen $\omega \notin \mathbb{F}^*_p$ folgt, dass für dieses b gilt $(\frac{b^2-a}{p}) = (-1)$.
- Wir zählen die Anzahl der $\omega \in \mathbb{F}^*_{p^2} \setminus \mathbb{F}^*_p$ mit verschiedener Spur.
- Jedes dieser ω liefert ein verschiedenes $b \in \mathbb{F}_p$ mit $(\frac{b^2-a}{p}) = (-1)$.
- Korollar zuvor: Für $M = \{\omega \in \mathbb{F}_{p^2} \mid N(\omega) = a\}$ gilt $|M| = p + 1$.

Konstruktion eines Elements mit Norm a

Beweis: (Fortsetzung)

- M enthält beide Quadratwurzeln von a in $\mathbb{F}_p$, d.h. $|M \setminus \mathbb{F}_p| = p - 1$.
- Falls für $\omega \in M \setminus \mathbb{F}_p$ auch das konjugierte $\bar{\omega} \in M \setminus \mathbb{F}_p$, entferne $\bar{\omega}$.
- Die entstehende Menge M' besitzt Kardinalität mindestens $\frac{p-1}{2}$.
- Angenommen es existieren zwei verschiedene Elemente $m_1 = x + y\sqrt{D}, m_2 = x + y'\sqrt{D} \in M'$ mit gleicher Spur.
- Es folgt $x^2 - Dy^2 = a = x^2 - Dy'^2$ und $D(y^2 - y'^2) \equiv 0 \mod p$.
- Wegen $D \not\equiv 0 \mod p$ folgt mit $m_1 \neq m_2$ dass $y \equiv -y' \mod p$. (Widerspruch: Konjugierte wurden aus M' entfernt.)
- Damit besitzen in M' alle Elemente verschiedene Spur. Es folgt
$$|\{b \in \mathbb{F}_p | (\tfrac{b^2-a}{p}) = (-1)\}| \geq |M'| \geq \tfrac{p-1}{2}.$$

Algorithmus von Cippola

Algorithmus von Cippola

EINGABE: $p \in \mathbb{P}$, $a \bmod p$ mit $(\frac{a}{p}) = 1$

1. REPEAT
   1. Wähle $b \in \{1, \ldots, p-1\}$ zufällig. Setze $D := b^2 - a$.

   UNTIL $(\frac{D}{p}) = (-1)$.
2. Berechne $x := (b + \sqrt{D})^{\frac{p+1}{2}}$ in $\mathbb{F}_p[\sqrt{D}]$.

AUSGABE: $x \bmod p$ mit $x^2 \equiv a \bmod p$

Laufzeit: erwartete Laufzeit $\mathcal{O}(\log^3 p)$.

Bsp: : Wir berechnen die Quadratwurzel von $a = 2$ in $\mathbb{F}_7$.

- Für $b = 1$ gilt $(\frac{D}{p}) = (\frac{-1}{7}) = (-1)$. Es folgt

$$(b + \sqrt{D})^{\frac{p+1}{2}} = (1 + \sqrt{-1})^4 = (2\sqrt{-1})^2 = -4 \equiv 3 \bmod 7.$$

- Wir prüfen $3^2 = 9 \equiv 2 \bmod 7$.

Williams $p + 1$ Methode

Idee von Williams $(p + 1)$-Methode:

- Sei $n = pr$ mit $1 < p < n$, p prim, $p \nmid r$.
- Sei $D \in \mathbb{N}$ mit $\mathrm{ggT}(D, n) = 1$. Falls $(\frac{D}{p}) = (-1)$, dann gilt für
$$G_p = \{\omega \in (\mathbb{F}_p[\sqrt{D}])^* \mid N(\omega) = 1\}, \text{ dass } |G_p| = p + 1.$$
- Sei $p + 1$ b-glatt, d.h. $p + 1 = \prod_{p \in B} p^{e_B}$.
- Sei k ein Vielfaches von $\prod_{p \in B} p^{e_B}$. Dann gilt
$$\omega^k = x + y\sqrt{D} \equiv 1 \mod p \text{ für alle } \omega \in (\mathbb{Z}/n\mathbb{Z})[\sqrt{D}]^* \text{ mit } N(\omega) = 1.$$
- Falls zusätzlich $x \not\equiv 1 \mod r$ folgt $p \leq \mathrm{ggT}(x - 1, n) < n$.

Williams $p+1$ Methode

Algorithmus Williams $p+1$-Methode

EINGABE: $n = pr$ zusammengesetzt, p prim, Schranke C mit $p \leq C$.

1. Wähle b geeignet. Sei $B = \{p_1, \ldots, p_s\}$.
2. Wähle $a \in_R \{1, \ldots, n-1\}$. Falls $\mathrm{ggT}(a, n) > 1$, Ausgabe des ggT.
3. Setze $D := a^2 - 1$ und $\omega := a + \sqrt{D}$.
4. Für $i = 1 \ldots s$
   1. Wähle e_i maximal mit $p_i^{e_i} < C$. Berechne $\omega := \omega^{p_i^{e_i}}$ in $(\mathbb{Z}/n\mathbb{Z})[\sqrt{D}]$.
5. Sei $\omega = x + y\sqrt{D}$. Falls $\mathrm{ggT}(x-1, N) \notin \{1, N\}$, Ausgabe des ggT.

Korrektheit: In Schritt 3 wählen wir ein $\omega \in (\mathbb{Z}/n\mathbb{Z})[\sqrt{D}]^*$ mit

$$N(\omega) = a^2 - D = a^2 - (a^2 - 1) = 1.$$

- Mit Ws $\approx \frac{1}{2}$ gilt $\left(\frac{D}{p}\right) = (-1)$. Falls $\left(\frac{D}{p}\right) = 1$, ist $(\mathbb{Z}/p\mathbb{Z})[\sqrt{D}]^* = U_p$.
- In diesem Fall ist Williams Methode genau die $(p-1)$-Methode.
- Die sonstige Korrektheit folgt analog zur $(p-1)$-Methode.

Laufzeit: $\mathcal{O}(s \log^3 n)$ analog zur $(p-1)$-Methode.

Elliptische Kurven Faktorisierung

Idee der Elliptischen Kurven Faktorisierung (Lenstra 1993):

- Rechne auf einer elliptischen Kurve mit den Punkten $E(n) := \{(x,y) \in (\mathbb{Z}/n\mathbb{Z})^2 \mid y^2 = x^3 + ax + b \text{ mit } a, b \in \mathbb{Z}/n\mathbb{Z}\} \cup \mathcal{O}$.
- Für primes n besitzen die Punkte $E(n)$ eine Gruppenstruktur.
- Für $n = pr$ gilt $E(n) \cong E(p) \times E(r)$.
- Für zufällige $a, b \in \mathbb{Z}/n\mathbb{Z}$ ist $|E(p)|$ annähernd uniform verteilt in
$$[p+1-2\sqrt{p}, p+1+2\sqrt{p}].$$
- Wir wählen solange a, b, bis $|E(p)|$ in kleine Primfaktoren zerfällt.
- D.h. im Gegensatz zu Pollards und Williams Methode können wir die Glattheit der Gruppenordnung über die Wahl von a, b steuern.
- Die Laufzeit der Elliptischen Kurven Faktorisierung ist
$$L_p[\tfrac{1}{2}, \sqrt{2}] = e^{\sqrt{2 \ln p \ln \ln p}}.$$

Faktorisieren auf Quantenrechnern

Idee von Shors Faktorisierungsalgorithmus (1994):

- Wir wählen ein zufälliges $a \in U_n$ und berechnen $\mathrm{ord}(a)$.
- Falls $\mathrm{ord}(a)$ ungerade, so wählen wir ein neues a.
- Falls $\mathrm{ord}(a)$ gerade, gilt $a^{\mathrm{ord}(a)} \equiv 1 \bmod n$ und $a^{\frac{\mathrm{ord}(a)}{2}} \not\equiv 1 \bmod n$.
- Sei zusätzlich $a^{\frac{\mathrm{ord}(a)}{2}} \not\equiv -1 \bmod n$, dies geschieht mit $\mathrm{Ws} \geq \frac{1}{2}$.
- Dann liefert $\mathrm{ggT}(a^{\frac{\mathrm{ord}(a)}{2}} \pm 1, n)$ nicht-triviale Teiler von n.
- Auf Quantenrechnern kann sehr effizient die diskrete Fouriertransformation (DFT) ausgerechnet werden.
- Die DFT eignet sich zur Periodenbestimmung von Funktionen.
- Als Funktion wählen wir die Exponentierfunktion
$$\exp : \mathbb{Z} \to U_n \text{ mit } i \mapsto a^i.$$
- Wegen $\exp(i + \mathrm{ord}(a)\mathbb{Z}) = \exp(i)$ besitzt $\exp(\cdot)$ Periode $\mathrm{ord}(a)$.
- Laufzeit von Shors Algorithmus auf Quantenrechnern: $\mathcal{O}(\log^3 n)$.

Liften von Lösungen quadratischer Gleichungen

Motivation:

- Quadratisches Sieb: Wir benötigen Lösungen von $X^2 \equiv n \bmod p^k$.
- Für $k = 1$ berechne Lösungen mittels Tonelli-Shanks/Cippola.
- Liefern die Lösungen für $k = 1$ auch die Lösungen für $k > 1$?

Satz Liften von Lösungen quadratischer Gleichungen

Sei $p \in \mathbb{P} \setminus \{2\}$, $(\frac{a}{p}) = 1$ und $k \in \mathbb{N}$. Sei x_k Lösung für $x_k^2 \equiv a \bmod p^k$, d.h. $x_k^2 - a = c_k' p^k$. Dann wird $x_{k+1}^2 \equiv a \bmod p^{k+1}$ gelöst von

$$x_{k+1} := x_k + c_k p^k \text{ mit } c_k \equiv -\frac{c_k'}{2x_k} \bmod p.$$

Beweis:

- Falls $x_{k+1}^2 \equiv a \bmod p^{k+1}$, gilt $x_{k+1}^2 \equiv a \bmod p^\ell$ für alle $\ell \leq k + 1$.
- Dies liefert den Ansatz $x_{k+1} \equiv x_k \bmod p^k$ bzw. $x_{k+1} = x_k + c_k p^k$.
- Wir suchen nun c_k.
- Da x_{k+1} modulo p^{k+1} definiert ist, bestimmen wir c_k modulo p.

Liften von Lösungen quadratischer Gleichungen

Beweis: (Fortsetzung)

- Mit Hilfe des Ansatzes $x_{k+1} = x_k + c_k p^k$ erhalten wir
$$\begin{aligned} 0 \equiv x_{k+1}^2 - a &= x_k^2 + 2x_k c_k p^k + (c_k p^k)^2 - a \\ &\equiv x_k^2 - a + 2x_k c_k p^k \mod p^{k+1}. \end{aligned}$$
- Wegen $x_k^2 - a = c'_k p^k$ folgt
$$0 \equiv x_k^2 - a + 2x_k c_k p^k = (c'_k + 2x_k c_k) p^k \mod p^{k+1}.$$
- Teilen durch p^k und Auflösen nach c_k liefert $c_k \equiv -\frac{c'_k}{2x_k} \mod p$.

Anmerkung:

- Wir definieren $c_0 := x_1$. Dann gilt
$$\begin{aligned} x_k &= c_{k-1}p^{k-1} + x_{k-1} = c_{k-1}p^{k-1} + c_{k-2}p^{k-2} + x_{k-2} \\ &= c_{k-1}p^{k-1} + c_{k-2}p^{k-2} + \ldots + c_1 p^1 + x_1 = \sum_{i=0}^{k-1} c_i p^i. \end{aligned}$$
- D.h. x_k lässt sich mittels der $c_{k-1} \ldots c_0$ zur Basis p darstellen.

Liften von Lösungen quadratischer Gleichungen

Bsp: Wir berechnen die Lösungen von $x_k^2 \equiv 2 \bmod 7^k$ für $k \leq 5$.

- Die Lösung $x_1 \equiv 3 \bmod 7$ finden wir mittels Cippola-Algorithmus.
- Wir wenden danach unsere Formel zum Liften an.

k	x_k	7^k	c'_k	c_k
1	3	7	1	$-\frac{1}{6} \equiv 1$
2	10	49	2	$-\frac{1}{3} \equiv 2$
3	108	343	34	$-\frac{6}{2 \cdot 3} \equiv 6$
4	2166	2401	23	$-\frac{2}{2 \cdot 3} \equiv 2$
5	4567	–	–	–

- Wir erhalten $x_5 = 2 \cdot 7^4 + 6 \cdot 7^3 + 2 \cdot 7^2 + 1 \cdot 7 + 3$.
- Wir würden gerne $x_\infty = \lim_{k \to \infty} x_k = \sum_{i=0}^{\infty} c_i 7^i$ berechnen.
- Damit hätten wir eine Lösung für alle Gleichungen $X^2 \equiv 2 \bmod 7^k$.
- Im Allgemeinen wird ein solcher Grenzwert aber nicht existieren.

Die p-adischen Zahlen

Definition p-adische Zahlen

Sei $p \in \mathbb{P}$. Wir definieren die *ganzen p-adischen Zahlen* als

$$\mathbb{Z}_p := \{(x_k) \in \prod_{k=0}^{\infty} \mathbb{Z}/p^{k+1}\mathbb{Z} \mid x_{k+1} \equiv x_k \bmod p^{k+1}\}.$$

Ferner definieren wir $\epsilon : \mathbb{Z} \to \mathbb{Z}_p$ mit $x \mapsto (x)_{k\in\mathbb{N}_0} = (x, x, x, \ldots)$.

Bsp: In $\mathbb{Z}_3$ erhalten wir

- $\epsilon_3(-1) = (-1, -1, -1, -1, -1, \ldots) = (2, 8, 26, 80, 242, \ldots)$.
- $\epsilon_3(101) = (101, 101, 101, \ldots) = (2, 2, 20, 20, 101, 101, \ldots)$.
- Aus dem Beispiel auf der Folie zuvor erhalten wir in $\mathbb{Z}_7$
$$\epsilon_7(\sqrt{2}) = (3, 10, 108, 2166, 4567, \ldots).$$

Reduzierte und Potenzreihen-Darstellung

Definition Reduzierte und Potenzreihen-Darstellung

Ein $(x_k) \in \mathbb{Z}_p$ ist in *reduzierter Darstellung* falls $0 \leq x_k < p^{k+1}$.
Sei (x_k) in reduzierter Darstellung und $x_{-1} := 0$. Die *Potenzreihen-Darstellung* von (x_k) ist $\sum_{k=0}^{\infty} c_k p^k$ mit $c_k := \frac{x_k - x_{k-1}}{p^k}$.

Anmerkungen:

- Aus $x_k \equiv x_{k-1} \mod p^k$ folgt $p^k | x_k - x_{k-1}$ bzw. $c_k \in \mathbb{Z}$.
- Gleichfalls gilt $x_k = c_k p^k + x_{k-1}$.
- Wegen $0 \leq x_k < p^{k+1}$ und $0 \leq x_{k-1} < p^k$ folgt $0 \leq c_k < p$.
- Es gilt $\sum_{k=0}^{n} c_k p^k = \sum_{k=0}^{n} \frac{x_k - x_{k-1}}{p^k} \cdot p^k = x_n - x_{-1} = x_n$.

Bsp: Für die Beispiele zuvor erhalten wir folgende Potenzreihen.

- $101 = 2 \cdot 3^0 + 2 \cdot 3^2 + 1 \cdot 3^4$.
- $-1 = \sum_{i=0}^{\infty} 2 \cdot 3^i$. Für alle $p \in \mathbb{P}$ gilt $-1 = \sum_{i=0}^{\infty} (p-1)p^i$, da $\sum_{i=0}^{\infty} (p-1)p^i = \sum_{i=0}^{\infty} p^{i+1} - \sum_{i=0}^{\infty} p^i = \sum_{i=1}^{\infty} p^i - \sum_{i=0}^{\infty} p^i = (-1)$.
- $\epsilon_7(\sqrt{2}) = (3, 1, 2, 6, 2, \ldots)$.

Addition und Multiplikation in $\mathbb{Z}_p$

Addition und Multiplikation in $\mathbb{Z}_p$:

- Wir addieren und multiplizieren Potenzreihen wie gewöhnlich.
- Durch Überträge bringen wir die Koeffizienten wieder in $[0, p-1]$.

- **Bsp:** Berechne das Doppelte von $(1 \cdot 3^0 + 2 \cdot 3^1 + 2 \cdot 3^2) = 25$.

$$
\begin{array}{rrrrl}
 & 2 \cdot 3^0 + & 4 \cdot 3^1 + & 4 \cdot 3^2 & \\
= & 2 \cdot 3^0 + & (3+1) \cdot 3^1 + & (3+1) \cdot 3^2 & \\
= & 2 \cdot 3^0 + & 1 \cdot 3^1 + & 2 \cdot 3^2 & +1 \cdot 3^3 = 50.
\end{array}
$$

- **Bsp:** Berechne $(3 \cdot 5^0 + 2 \cdot 5^1)(4 \cdot 5^0 + 1 \cdot 5^1) = 13 \cdot 9$.

$$
\begin{array}{rrrrl}
 & (3 \cdot 4) \cdot 5^0 + & (3 \cdot 1 + 2 \cdot 4) \cdot 5^1 + & (2 \cdot 1) \cdot 5^2 & \\
= & (2 \cdot 5 + 2) \cdot 5^0 + & (2 \cdot 5 + 1) \cdot 5^1 + & 2 \cdot 5^2 & \\
= & 2 \cdot 5^0 + & 3 \cdot 5^1 + & 4 \cdot 5^2 & = 117.
\end{array}
$$

- $(\mathbb{Z}_p, +, \cdot)$ ist ein kommutativer Ring.

Hensels Lemma

Lemma von Hensel

Sei $f \in \mathbb{Z}_p[X]$ und $\tilde{x} \in \mathbb{Z}_p$ mit $f(\tilde{x}) \equiv 0 \bmod p^k$ für ein $k \in \mathbb{N}$. Für ein $a \in \mathbb{Z}$ gilt $f(\tilde{x} + ap^k) \equiv 0 \bmod p^{k+1}$ gdw $f'(\tilde{x})a \equiv -\frac{f(\tilde{x})}{p^k} \bmod p$.

Beweis:

- Sei $d = \mathrm{grad}(f)$. Wir schreiben f als Polynom in $X - \tilde{x}$, d.h.
$$f(X - \tilde{x}) = \sum_{i=0}^{d} c_i (X - \tilde{x})^i \text{ mit } c_i \in \mathbb{Z}_p.$$
- Es folgt $f(\tilde{x}) = c_0$ und $f'(\tilde{x}) = c_1$. Damit gilt
$$f(\tilde{x} + ap^k) = \sum_{i=0}^{d} c_i (ap^k)^i \equiv f(\tilde{x}) + f'(\tilde{x})ap^k \bmod p^{k+1}.$$
- Wir erhalten also $f(\tilde{x} + ap^k) \equiv 0 \bmod p^{k+1}$ gdw
$$f'(\tilde{x})ap^k \equiv -f(\tilde{x}) \bmod p^{k+1} \Leftrightarrow f'(\tilde{x})a \equiv -\frac{f(\tilde{x})}{p^k} \bmod p.$$

Existenz der Liftungen

Korollar

Sei $f \in \mathbb{Z}_p[X]$ und $\tilde{x} \in \mathbb{Z}_p$ mit $f(\tilde{x}) \equiv 0 \mod p$ und $f'(\tilde{x}) \not\equiv 0 \mod p$. Dann existiert ein eindeutiges $x \in \mathbb{Z}_p$ mit $f(x) = 0$ und $x \equiv \tilde{x} \mod p$.

Anmerkungen:

- Aus Hensels Lemma folgt die Eindeutigkeit von $a \mod p$.
- Die Bedingung $f(\tilde{x}) \equiv 0 \mod p$ und $f'(\tilde{x}) \not\equiv 0 \mod p$ bedeutet, dass $\tilde{x}$ eine einfache Nullstelle von f ist.
- Damit lässt sich jede einfache Nullstelle von f modulo p eindeutig zu einer Nullstelle von f in $\mathbb{Z}_p$, d.h. modulo aller p^k, liften.

Beispiel: Liften modulo 7

Bsp: Wir berechnen alle Nst von $f(X) = X^3 + X^2 + 4X + 1 \mod 49$.

- Wir bestimmen zunächst die Lösungen modulo 7. Es gilt $f(1) = 7 \equiv 0 \mod 7$, $f(2) = 21 \equiv 0 \mod 7$ und $f(3) = 49 \equiv 0 \mod 7$.
- Damit sind $1, 2$ und 3 alle Nullstellen modulo 7.
- Für die Ableitung $f'(X) = 3X^2 + 2X + 4$ gilt
$$f'(1) \equiv 2 \mod 7,\ f'(2) \equiv (-1) \mod 7 \text{ und } f'(3) \equiv 2 \mod 7.$$
- Damit können wir alle Nullstellen anheben. Wir berechnen $\mod 7$ $a_1 \equiv -\frac{7}{7} \cdot 2^{-1} \equiv 3$, $a_2 \equiv -\frac{21}{7} \cdot (-1)^{-1} \equiv 3$ und $a_3 \equiv -\frac{49}{7} \cdot 2^{-1} \equiv 0$.
- Damit erhalten wir modulo 49 genau die drei Nullstellen.
$$x_1 = 1 + 3 \cdot 7 = 22,\ x_2 = 2 + 3 \cdot 7 = 23 \text{ und } x_3 = 3 + 0 \cdot 7 = 3.$$

Beispiel: Liften modulo 2

Bsp: Wir berechnen alle Nullstellen von $f(X) = X^2 + 7 \bmod 16$.

- Modulo 2 ist 1 die einzige Nst. Es gilt aber $f'(X) = 2X \equiv 0 \bmod 2$.
- Nach Hensels Lemma kann eine Nullstelle $\tilde{x} \bmod 2^k$ in diesem Fall angehoben werden gdw $\frac{f(\tilde{x})}{2^k} \equiv 0 \bmod 2$.
- Falls $\tilde{x}$ angehoben wird, dann zu $\tilde{x}$ **und** $\tilde{x} + p^k$.
- Für $k = 1$ gilt $\frac{f(1)}{2} = \frac{8}{2} = 4 \equiv 0 \bmod 2$.
- D.h. wir erhalten die Nullstellen 1 und 3 modulo 4.
- Für $k = 2$ gilt $\frac{f(1)}{4} = \frac{8}{4} \equiv 0 \bmod 2$ und $\frac{f(3)}{4} = \frac{16}{4} \equiv 0 \bmod 2$.
- D.h. wir erhalten die vier Nullstellen $1, 5, 3$ und 7 modulo 8.
- Für $k = 3$ gilt modulo 2
$$\frac{f(1)}{8} = \frac{8}{8} \equiv 1,\ \frac{f(3)}{8} = \frac{16}{8} \equiv 0,\ \frac{f(5)}{8} = \frac{32}{8} \equiv 0 \text{ und } \frac{f(7)}{8} = \frac{56}{8} \equiv 1.$$
- D.h. 3 wird modulo 16 zu 3 und 11 geliftet und 5 zu 5 und 13.
- Für $k > 3$ kann man zeigen, dass stets 2 Nst angehoben werden.
- Dies führt schließlich zu zwei 2-adischen Lösungen
$$x_1 = (1, 1, 5, 5, \ldots) \text{ und } x_2 = (1, 3, 3, 11, \ldots).$$

Lösen von Gleichungen modulo n

Algorithmus Lösen von Gleichungen modulo n

EINGABE: $n = \prod_{i=1}^{s} p_i^{e_i}$, Polynom $f(X) \in \mathbb{Z}[X]$

1. For $i = 1, \ldots, s$: Bestimme Nullstellen von $f(X) \bmod p_i$.
   1. For $j = 2, \ldots, e_i$: Lifte Nullstellen modulo p_i^j.
2. Setze Nullstellen modulo $p_1^{e_1}, \ldots, p_s^{e_s}$ mittels CRT zusammen.

AUSGABE: Alle Nullstellen von $f(X)$ modulo n

Bsp: Wir bestimmen alle Nullstellen von $f(X) = X^2 + 7 \bmod 2^3 \cdot 11$.

- Modulo 8 kennen wir bereits die Lösungen $1, 3, 5, 7$.
- Modulo 11 gilt $f(X) \equiv X^2 - 4$, d.h. die Lösungen sind $2, -2 \equiv 9$.
- Damit erhalten wir in $\mathbb{Z}/8\mathbb{Z} \times \mathbb{Z}/11\mathbb{Z}$ die Lösungen
$$(1,2), (1,9), (3,2), (3,9), (5,2), (5,9), (7,2) \text{ und } (7,9).$$
- Modulo 88 sind dies alle 8 Lösungen
$$57, 9, 35, 75, 13, 53, 79 \text{ und } 31.$$

Euklidische Division

1. Euklidische Division:

- Landau Notation: $f(n) = \mathcal{O}(g(n))$.
- Definitionen: Gruppe, Ring, Ideal
- Teilbarkeit und Teilbarkeit mit Rest (euklidisch)
- Beispiel für euklidische Ringe
  - $\mathbb{Z}$ euklidisch mit $N(x) = |x|$
  - $\mathbb{Z}[i]$ mit $N(z) = z\bar{z}$
  - $\mathbb{Q}[X]$ mit $N(p) = \mathrm{grad}(p)$
- Prim $\Rightarrow$ irreduzibel, aber irreduzibel $\not\Rightarrow$ prim.
- Faktoriell: In Primelemente zerlegbar.
- Euklidisch $\Rightarrow$ Hauptidealring $\Rightarrow$ faktoriell
- ggT, Lemma von Bézout: $\exists x, y$ mit $\mathrm{ggT}(a, b) = xa + yb$.
- Euklidischer Algorithmus, Erweiterter Euklidischer Algorithmus

Kongruenzrechnung

2. Kongruenzrechnung:

- $a \equiv b \bmod n \Leftrightarrow n|(a-b)$
- Binomische Formel mod p: $(a+b)^p \equiv a^p + b^p \bmod p$.
- Kleiner Fermat: $a^p \equiv a \bmod p$.
- Lemma über Teiler und Vielfache:

$$a \equiv b \bmod n \text{ gilt modulo aller Teiler von } n \text{ und}$$
$$a \equiv b \bmod n \Leftrightarrow ma \equiv mb \bmod mn.$$

- Lineare Gleichungen $ax \equiv b \bmod n$. Sei $d = \mathrm{ggT}(a,n) = ya + zn$. Löse als $x \equiv y\frac{b}{d} \bmod \frac{n}{d}$.
- Wichtiger Spezialfall $d = 1$: Multipliziere mit $y = a^{-1} \bmod n$.
- Chinesischer Restsatz: Lösung für $a_i x \equiv b_i \bmod n_i$, $i = 1, \ldots, n$. Sei $n = \prod_{i=1}^{s} p_i^{r_i}$. Dann gilt $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}/p_1^{r_1}\mathbb{Z} \times \ldots \times \mathbb{Z}/p_s^{r_s}\mathbb{Z}$.

3. Restklassen:

- Additive Gruppe: $\mathbb{Z}/n\mathbb{Z} := \{a + n\mathbb{Z} | a \in \mathbb{Z}\}$.
- Multiplikative Gruppe: $U_n = (\mathbb{Z}/n\mathbb{Z})^* = \{\bar{a} \mid \mathrm{ggT}(a, n) = 1\}$.
- Eulersche φ-Funktion: $\varphi(n) := |U_n|$.
- Für $n = \prod_{i=1}^{s} p_i^{r_i}$ gilt $\varphi(n) = \prod_{i=1}^{s} p_i^{r_i - 1}(p_i - 1)$. Mittels CRT gilt
$$U_n \cong U_{p_1^{r_1}} \times \ldots \times U_{p_s^{r_s}}.$$
- Satz von Euler: $a^{|G|} = 1$.
- Satz von Lagrangre: $\mathrm{ord}(a) || G|$.
- Endliche Körper $\mathbb{F}_p$: $\mathbb{Z}/p\mathbb{Z}$ ist ein Körper gdw p prim.
- Konstruktion von $\mathbb{F}_{p^r}$ mittels irreduziblem $q(X)$, $\mathrm{grad}(q(X)) = r$.

Struktur abelscher Gruppen

4. Struktur abelscher Gruppen

- Jede zyklische Gruppe ist abelsch.
- Isomorphiesatz:

  Jede zyklische Gruppe ist isomorph zu $\mathbb{Z}$ oder $\mathbb{Z}/n\mathbb{Z}$.
- Darstellung von Gruppen
- Klassifikationssatz: Für endlich erzeugte G gilt
  $$G \cong \mathbb{Z}^r \times \prod_{i=1}^{\ell} \mathbb{Z}/n_i\mathbb{Z}.$$
- Normalformen: Primteiler und Elementarteiler.
- U_n ist zyklisch gdw $n = 2, 4$, $n = p^r$ oder $n = 2p^r$.

Quadratische Gleichungen

5. Quadratische Gleichungen:

- Allgemeine Wurzelberechnung mit Hilfe des diskreten Logarithmus, Baby-Step Giant-Step Algorithmus
- Quadratische Reste und das Legendre-Symbol
- Euler-Identität: $(\frac{a}{p}) \equiv a^{\frac{p-1}{2}} \mod p$.
- $(\frac{-1}{p}) = (-1) \Leftrightarrow p \equiv 3 \mod 4$, $(\frac{2}{p}) = (-1) \Leftrightarrow p \equiv \pm 3 \mod 8$.
- Reziprozität: $(\frac{q}{p}) = -(\frac{p}{q}) \Leftrightarrow p \equiv q \equiv 3 \mod 4$, sonst $(\frac{q}{p}) = (\frac{p}{q})$.
- Berechnung des Jacobi-Symbols (analog Euklidischer Alg.).
- Quadratwurzel-Berechnung: Algorithmus von Tonelli und Shanks.

Kettenbrüche und Primzahltests

6. Kettenbrüche:

- Kettenbruchalgorithmus (analog zum Euklidischen Algorithmus)
- Terminierung des Algorithmus gdw Eingabe rational.
- Konvergenz der Näherungsbrüche und Best-Approximation.
- Jede sehr gute rationale Approximation ist ein Näherungsbruch.

7. Primzahltests:

- Lucas-Lehmer: $n = 2^p - 1$ prim $\Leftrightarrow n | S_{p-1} (S_1 = 4, S_k = S_{k-1}^2 - 2)$.
- Lucas-Test: $a^{n-1} \equiv 1 \mod n$, $a^{\frac{n-1}{q}} \not\equiv 1 \mod n$.
- Pocklington-Test: $a^{n-1} \equiv 1 \mod n$ und $\mathrm{ggT}(a^{\frac{n-1}{q}} - 1, n) = 1$.
- Carmichael-Zahlen: $a^{n-1} \equiv 1 \mod n$ für alle $a \in U_n$.
- Solovay-Strassen Test: $a^{\frac{n-1}{2}} \stackrel{?}{\equiv} (\frac{a}{n}) \mod n$.
- Miller-Rabin Test: $a^d \equiv 1$ oder $a^{2^k d} \equiv (-1)$ für $n - 1 = 2^r d$, $k < r$.

Faktorisierung und Lösen polynomieller Gleichungen

8. Faktorisierung:

- Fermat Faktorisierung: Konstruiere Quadrat $y^2 = x^2 - n$.
- Faktorisierung mit Faktorbasen
  - Morrison-Brillhart mittels Kettenbrüchen
  - Quadratisches Sieb
- Pollards $(p-1)$-Methode: Berechne Vielfaches k von $p-1$.
- Quadratische Erweiterung $\mathbb{F}_{p^2} = \mathbb{F}_p[\sqrt{D}] \cong \mathbb{F}_p[X]/(X^2 - D)$.
- Frobenius-Automorphismus $f_p : x \mapsto x^p \bmod p$
- Cippolas Algorithmus
- Williams $(p+1)$-Methode

9. Lösen polynomieller Gleichungen:

- Liften quadratischer Gleichungen, p-adische Zahlen
- Hensel-Lemma: $f(\tilde{x} + ap^k) \equiv 0 \bmod p^{k+1} \Leftrightarrow f'(\tilde{x})a \equiv -\frac{f(\tilde{x})}{p^k} \bmod p$.
- Lösen von Gleichungen modulo n mittels Liften und CRT.