Elementare Zahlentheorie

Die Mitarbeiter von http://mitschriebwiki.nomeata.de/

11. März 2017

Inhaltsverzeichnis

Bezeichnungen und Vorraussetzungen

- Logische Zeichen: $\Longrightarrow$, $\Longleftrightarrow$, $\forall$, $\exists$, $\exists^1$ (es gibt genau ein), $\wedge$ (und), $\vee$ (oder)
- Zeichen der Mengenlehre: z.B. $\cup$, $\cap$, $\mathbb{N} := \{x \in \mathbb{Z} | x \geq 0\}$
- Induktion als Beweistechnik
- $\#M$ Kardinalität der Menge M, z.B. $\#\mathbb{N} = \infty$
- $\mathbb{N} = \{0, 1, 2, 3, \ldots\}$, $\mathbb{N}_+ = \{1, 2, 3, 4, \ldots\}$ (natürliche Zahlen)
- $\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}$ (Ring der ganzen Zahlen)
- $\mathbb{Q} = \{\frac{z}{n} | z \in \mathbb{Z}, n \in \mathbb{N}_+\}$ (Körper der rationalen Zahlen)
- $\mathbb{R}$ Körper der reelen Zahlen
- $\mathbb{F}_q$ Körper mit $q < \infty$ Elementen ($= GF(q)$ in der Informatik)
- $\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, \ldots\}$ Menge aller Primzahlen

1 Primzerlegung

1.1 Faszination Primzahlen: Primzahlsatz (o.Bew.), gelöste und ungelöste Probleme über Primzahlen

Satz 1.1 (Euklid, ca. 300 v. Chr.)

$$\#\mathbb{P} = \infty$$

Bemerkung: Analysis:

$$\sum_{n \in \mathbb{N}} \frac{1}{n} = \infty$$
$$\sum_{n \in \mathbb{N}} \frac{1}{n^2} < \infty$$

Euler:

$$\sum_{p \in \mathbb{P}} \frac{1}{p} = \infty$$

Definition
$p \in \mathbb{P}$ heiße Zwillingsprimzahl $\iff p, p+2 \in \mathbb{P}$

$\{p, p+2\}$ heißt Primzahlzwilling

Frage: Gibt es unendlich viele Primzahlzwillinge? Kein Mensch hat eine Idee, wie das zu zeigen ist.

Satz 1.2 (Primzahlzwillingsatz von Viggo Brun, ca. 1915)

$$\sum_{p \text{ Zwillingsprimzahl}} \left(\frac{1}{p} + \frac{1}{p+2} \right) < \infty$$

Pierre de Fermat (1601 – 1665) schreibt auf den Rand seines Exemplars von Arithmetica des Diophant: „Die Gleichung $x^n + y^n = z^n$ (mit $n \in \mathbb{N}$, $n > 2$) hat keine Lösung mit $x, y, z \in \mathbb{N}_+$“.
Heute: Fermat hat recht. (Wiles 1995/96)

Fermat schrieb auch: Die Zahlen $F_n = 2^{(2^n)} + 1$ sind prim. Die Aussage ist ok für $n = 0, 1, 2, 3, 4$. **Euler** konnte zeigen, dass $F_5 = 4294967297 = 641 \cdot 6700417$. Noch 2000 ist unbekannt, ob F_{24} prim ist.

Möglichkeiten:

(1) Kein F_n mit $n > 24$ ist prim.

(2) Nur endlich viele F_n sind prim.

(3) $\#\{F_n | F_n \in \mathbb{P}\} = \infty$

(4) $\#\{F_n | F_n \notin \mathbb{P}\} = \infty$

Niemand weiß oder vermutet, was richtig ist, keine Beweisideen!

Definition
$M_p = 2^p - 1$ heißt p-te Mersenne-Zahl

Satz 1.3
M_p ist höchsten dann prim, wenn $p \in \mathbb{P}$

Beweis
Übungsaufgabe ■

Die größte bekannte Primzahl ist seit längerem eine Mersenne-Primzahl, da es gute Tests gibt, z.B. Lucas/Lehmer, verbessert von Grandall. Heute: $M_p \in \mathbb{P}$ für $p = 3021327$, $M_p > 10^{2000000}$.

Eine weitere Frage an Primzahlen ist die nach der Verteilung von $\mathbb{P}$ in $\mathbb{N}$. Bei dieser Frage spielt die Analysis eine Rolle.

Satz 1.4 (Elementarer Primzahlsatz)
Sei $\Pi(x) = \#\{p \in \mathbb{P} | p \leq x\}$ $(x \in \mathbb{R})$. Dann gilt:

$$\Pi(x) \sim \frac{x}{\log x} \text{ (fast asymptotisch gleich)}$$

Der Satz wurde 1792 von Gauß vermutete und 1896 von Hadamard und von de la Vaille-Poussin nach Vorarbeiten von Riemann bewiesen

Folgerung 1.5
Sei p_n die n-te Primzahl der Größe nach $(p_1 = 2, p_2 = 3, p_3 = 5, \ldots)$. Dann gilt:

$$p_n \sim n \cdot \log n \quad (n \to \infty)$$

Beweis
$p_n = x \implies n = \Pi(x)$

$$\begin{aligned}
\lim_{n\to\infty} \frac{n \cdot \log n}{p_n} &= \lim_{n\to\infty} \frac{\Pi(x)\log\Pi(x)}{x} \\
&= \lim_{n\to\infty} \frac{\Pi(x)}{x/\log x} \cdot \frac{x}{\log x} \cdot \frac{\log\Pi(x)}{x} \\
&= \lim_{n\to\infty} \frac{\log\Pi(x)}{\log x} \\
&= \lim_{n\to\infty} \frac{1}{\log x} \cdot \log \frac{\Pi(x)}{x/\log x} x/\log x \\
&= \lim_{n\to\infty} \frac{1}{\log x} \left(\log \frac{\Pi(x)}{x/\log x} + (\log x - \log\log x) \right) \\
&= 1 - \lim_{x\to\infty} \frac{\log(\log x)}{\log x} \\
&= 1 - \lim_{t\to\infty} \frac{\log t}{t} \\
&= 1 - \lim_{n\to\infty} \frac{n}{e^n} = 1
\end{aligned}$$

■

Folgerung 1.6
$\forall \varepsilon > 0\ \exists N \in \mathbb{N}\ \forall x \geq N\ \exists p \in \mathbb{P}$:

$$x \leq p \leq x(1+\varepsilon)$$

Riemann (1826–66): „Über die Anzahl der Primzahlen unter einer gegebenen Größe“ stellt Zusammenhang mit Riemanns ζ-Funktion her.

$$\zeta(s) = \sum_{n\in\mathbb{N}_+} \frac{1}{n^s}, s \in \mathbb{C}$$

$\zeta(s)$ konvergiert für $\operatorname{Re} s > 1$ und hat eindeutige Fortsetzung zum analytischer Funktion $\mathbb{C}\setminus 1 \to \mathbb{C}$ mit Pol in $s = 1$. Man kann zeigen: Primzahlsatz $\iff$ ζ hat keine Nullstelle mit $\operatorname{Re} \geq 1$.

Vermutung: Alle nichtreellen Nullstellen von ζ liegen auf $\frac{1}{2} + i\mathbb{R}$. Gauß vermutet: Besser als $x/\log x$ approximiert

$$\operatorname{li}(x) = \int_2^x \frac{du}{\log u} \quad \text{(Integrallogarithmus).}$$

Man will möglichst gute Abschätzung des Restglieds $R(x) = |\Pi(x) - \operatorname{li}(x)|$.

Fakt: Je größer die nullstellenfreien Gebiete von ζ, desto bessere Restgliedabschätzung möglich. Demnach: Beste Restgliedabschätzung möglich, wenn Riemanns Vermutung stimmt.

$$R(x) \leq \text{Const} \cdot x^{\frac{1}{2}} \log x$$

Fakt 2: Von der Qualität der Restgliedabschätzung hängen in der Informatik viele Aussagen über die theoretische Effektivität von numerischen Algorithmen ab.

1.2 Elementare Teilbarkeitslehre in integren Ringen

In dieser Vorlesung gilt die Vereinbarung, dass ein Ring definitionsgemäß genau ein Einselement 1_R besitzt.

Definition
Ein Ring R heißt *integer*, wenn gilt:

(1) R ist kommutativ.

(2) $\forall a, b \in R: \; ab = 0 \iff a = 0 \vee b = 0.$

Beispiel
Jeder Unterring eines Körpers ist integer.

Definition
Die Menge

$$R^\times := \{a \in R | \; \exists x \in R: \; ax = 1 = xa\}$$

heißt *Einheitengruppe* $R^\times$ des (allgemeinen) Ringes R.
Leicht zu sehen ist, dass $R^\times$ eine Gruppe ist, x ist das eindeutig bestimmte Inverse a^{-1} von a.

Beispiel
$\mathbb{Z}^\times = \{\pm 1\}$ (klar!)
$\mathbb{Z}^{n\times n}$ ist der Ring der ganzzahligen $n\times n$-Matrizen, $GL(\mathbb{Z}) = (\mathbb{Z}^{n\times n})^\times$. Beispielsweise für $n = 2$:

$$A = \begin{pmatrix} 2 & 5 \\ 1 & 3 \end{pmatrix}, \; A^{-1} = \begin{pmatrix} 3 & -5 \\ -1 & 2 \end{pmatrix}, \; A\,A^{-1} = I = A^{-1}\,A \Rightarrow A \in GL_2(\mathbb{Z}).$$

$R = K[X]$ ist der Ring der Polynome in X über dem Körper K. $R^\times = \{\alpha \in K^\times = K\backslash\{0\}\}$ (Konstante, von 0 verschiedene Polynome)
$\mathbb{Z}, K[X]$ sind integere Ringe.

Ab jetzt sei R ein integerer Ring, $a, b, c, d, x, y, u, v, w \in R$.

Problem: Gleichung $ax = b$ mit der Variablen x. Beispielsweise ist $3x = 5$ in $R = \mathbb{Z}$ nicht lösbar, $3x = 6$ hingegen schon.

Definition

$$a|b \iff \exists x \in R: \; ax = b$$

Sprechweise: a teilt b, b ist Vielfaches von a, a ist Teiler von b.

$\neg a|b \iff a \nmid b$ (a teilt nicht b).

Beispiel
$R = \mathbb{Z}$: $3 \nmid 5, \; 3|0, \; \pm 3, \; \pm 6 \ldots$
$R = K[X]$: $(X-1)|(X^2-1)$.
In jedem $R: \; \forall a \in R: 1|a$ (denn $a = a \cdot 1$) $\wedge$ $a|0$ (denn $0 = 0 \cdot a$).

Satz 1.7 (Elementare Teilbarkeitseigenschaften)

(1) $|$ ist mit $\cdot$ verträglich:
$a|b \ \wedge \ c|d \Rightarrow ac|bd.$

(2) $|$ ist mit Linearkombinationen verträglich:
$a|b \ \wedge \ a|c \Rightarrow \ \forall x, y \in R: \ a|xb + yc.$

(3) $|$ ist eine transitive und reflexive Relation und für $a \neq 0$ gilt:
$a|b \ \wedge \ b|a \iff \exists e \in R^\times : \ a = eb.$

Beweis
Treppenbeweis © Dr. Rehm. ∎

Bemerkung: (2) hat einen häufigen Spezialfall: $a|b \ \wedge \ a|c \Rightarrow a|b \pm c$.
Anwendungsbeispiel: $a|b^2 \ \wedge \ a|b^2 + 1 \Rightarrow a|\underbrace{b^2 + 1 - b^2}_{=1}$.

Folgerung: $e \in R^\times : \ a|b \iff ea|b \iff a|eb.$
Grund: $b = xa = (xe^{-1})ea.$
Merke: Einheitsfaktoren ändern Teilbarkeit nicht!
Folge 2: R ist disjunkte Vereinigung aller Mengen $R^\times a = \{ea|e \in R^\times\}$.
Grund: $u \in R^\times a \cap R^\times b \iff u|a \ \wedge \ a|u \ \wedge \ u|b \ \wedge b|u$, also $R^\times a = R^\times u (= R^\times b$, $eu \in R^\times a \Rightarrow R^\times u \subset R^\times a$, genauso zeigt man $R^\times a \subset R^\times u$.

Definition (Normierung)
Auswahl je eines festen a_{nor} in $R^\times a$. Man wählt immer $e_{nor} = 1, \ 0_{nor} = 0$.
Standard-Normierung: $R = \mathbb{Z}, \ R^\times a = \{\pm a\}, \ a_{nor} = \max\{R^\times a\} = |a|$.
$R = K[X], \ 0 \neq f = \alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n$ mit $\alpha_n \neq 0$. Dann ist $f_{nor} = \frac{1}{\alpha_n} f$.

Klar ist: Jedes $a \in R$ hat die trivialen Teiler $e \in R^\times$ und $ea, e \in R^\times$. Nichttriviale Teiler heißen auch echte Teiler.

Beispiel
$R = \mathbb{Z}$, triviale Teiler von 6 sind $\pm 1, \ \pm 6$. Echte Teiler sind $\pm 2, \ \pm 3$.

Definition

(1) $a \in R$ heißt unzerlegbar oder irreduzibel, falls $a \neq 0, \ a \notin R^\times$ und a hat nur triviale Teiler.

(2) $R = \mathbb{Z}$. $p \in \mathbb{Z}$ heißt Primzahl $\iff$ p normiert und irreduzibel.

(3) $R = K[X]$. $f \in R$ heißt Primpolynom $\iff$ f irreduzibel.

Größter gemeinsamer Teiler und kleinstes Gemeinsames Vielfaches

Definition
d heißt ein größter gemeinsamer Teiler von $a_1, a_2, \ldots, a_n :\iff$

(1) $d|a_1 \ \wedge \ d|a_2 \ \wedge \ \cdots \ \wedge \ d|a_n$ (d ist gemeinsamer Teiler)

(2) $u|a_1 \ \wedge \ u|a_2 \ \wedge \ \cdots \ \wedge \ u|a_n \Rightarrow u|d$

Bemerkung: (1) Bei $R = \mathbb{Z}$ ist ein bezüglich $\leq$ größter gemeinsamer Teiler ein normierter ggT.

(2) Eindeutigkeit des ggT: Ist d ein ggT von $a_1, a_2, \ldots, a_n$, so ist auch d_{nor} ein ggT und d_{nor} ist durch $a_1, a_2, \ldots, a_n$ eindeutig bestimmt: $d = d_{nor} = \text{ggT}(a_1, a_2, \ldots, a_n)$
Grund: $e \in R^\times$ spielt bei Teilbarkeit keine Rolle, und $d_{nor} = ed$ für ein $e \in R^\times$. Sind d, d' ggTs von $a_1, a_2, \ldots, a_n \Rightarrow d|d' \ \wedge \ d'|d \iff d' = ed$, da normiert $\Rightarrow d = d'$.

Der kgV wird analog zum ggT unter Umkehrung aller Teilbarkeitsrelationen definiert:
Definition
k heißt ein kgV von $a_1, a_2, \ldots, a_n :\iff$

(1) $a_1|k \ \wedge \ a_2|k \ \wedge \ \cdots \ \wedge \ a_n|k$ (k ist gemeinsames Vielfaches)

(2) $a_1|u \ \wedge \ a_2|u \ \wedge \ \cdots \ \wedge \ a_n|u \Rightarrow k|u$

Die Eindeutigkeitsaussage des ggT gilt für den kgV ebenfalls.

Satz 1.8 (Euklids Primzahlsatz)
Für $R = \mathbb{Z}$ gilt:

$$\#\mathbb{P} = \infty$$

Beweis
Es seien $p_j, \ j = 1, 2, \ldots, n$ paarweise verschiedene Primzahlen. Betrachte $1 + \prod p_i > 0$.
Aussage: Ist $a \in \mathbb{N}, \ a > 1$, so ist $\min\{d \in \mathbb{N} : d|a\}$ eine Primzahl und das Minimum existiert wegen $a|a$. Benutzt, dass jede Teilmenge der natürlichen Zahlen eine kleinste Zahl enthält $\Rightarrow$ Behauptung, da ein echter Teiler kleiner wäre $\Rightarrow \exists p \in R : \ p|1 + \prod p_j$.
Wäre $p = p_j$ für ein $j \in \{1, 2, \ldots, n\}$, so $p|\prod p_j$. $p|\underbrace{1 + \prod p_j - 1(\prod p_j)}_{=1} \iff p|1 \Rightarrow p \in \mathbb{Z}^\times \Rightarrow$ Widerspruch. ∎

1.3 Primzerlegung in Euklidischen Ringen, Faktorielle Ringe

In diesem Abschnitt sei R integerer Ring, $a, b, c, d, \ldots \in R$.
Sprechweise: $a = qb + r$. Man sagt r ist der Rest bei Division von a durch b, q ist der Quotient (Division mit Rest).
Mathematischer Wunsch: Rest r soll im geeigneten Sinn kleiner sein als der Divisor b. Man benötigt dafür eine Größenfunktion $gr : \ R \mapsto \mathbb{N}$.
Definition
Ein Ring R, beziehungsweise ein Paar (R, gr) heißt euklidisch $:\iff$

(1) R ist integer

(2) Man hat Division mit Rest, das heißt:
$\forall a, b \in R, \ b \neq 0, \ \exists q, r \in R : a = qb + r$, wobei $r = 0$ oder $gr(r) < gr(b)$.

Es ist $(\mathbb{Z}, |\cdot|)$ ein euklidischer Ring.

Beweis

O.b.d.A: $b > 0$, da $|b| = gr(b) = gr(-b)$.

$q = \lfloor \frac{a}{b} \rfloor$ ist geeignet: $0 \leq \frac{a}{b} - q < 1 | \cdot b \Rightarrow 0 \leq a - qb = r < b \Rightarrow gr(r) = |r| = r < b = |b| = gr(b)$ ■

Viele Porgrammiersprachen, etwa MAPLE, bieten einen modulo-Operator:
`r := (a mod b)` $= a - \lfloor \frac{a}{|b|} \rfloor$.

Im $K[X]$ ist die Division mit Rest möglich bezüglich $gr(f) := \operatorname{grad} f = n$, $(f \neq 0)$.

Der Ring $R = \mathbb{Z} + \mathbb{Z}i \subset \mathbb{C}$, also $R = \{x + iy | x, y \in \mathbb{Z}\}$ heißt „Ring der ganzen Gaußschen Zahlen“. R ist euklidisch mit $gr(x, iy) = |x + iy| = \sqrt{x^2 + y^2}$. Die Idee für die Division mit Rest ist: Suche einen Gitterpunkt nahe $\frac{a}{b}$. (siehe Übung)

Lemma 1.9

R integer, $a = qb + r$, $a, b, q, r \in R$. Dann gilt

$$\operatorname{ggT}(a, b) = \operatorname{ggT}(b, r)\,,$$

und falls eine Seite existiert, so auch die andere.

Beweis

Sind $u, v \in R$, so kann Existenz und $\operatorname{ggT}(u, v)$ abgelesen werden an

$$T(u, v) = \{d \in R \big| d | u \wedge d | v\}\,,$$

der Menge der gemeinsamen Teiler. Es ist aber $T(a, b) = T(b, r)$:
„$\subseteq$“: $d|a \wedge d|b \implies d|r$ (Linearkombination)
„$\supseteq$“: $d|r \wedge d|b \implies d|a$ (Linearkombination) ■

Euklids glänzende Idee ist nun: Bei der Division mit Rest verkleinert der Übergang von (a, b) zu (b, r) das Problem. Sein Algorithmus ist wie folgt:

```
ggT := proc(a,b);            # Prozedur, die ggT = ggT(a,b)
aus $a$,$b$ berechnet if b = 0
  then normiere(a)           # es ist immer ggT(a,0) = a_nor
  else ggT(b, a mod b)       # terminiert wegen gr(a mod b) < gr(b)
fi
```

Idee: r ist Linearkombination von a und a, b. Die Hoffnung dabei ist: Auch $d := \operatorname{ggT}(a, b)$ lässt sich linear kombinieren.

Satz 1.10 (Satz der Linearkombination des ggT)

Sei R ein euklidischer Ring. Dann existiert $d = \operatorname{ggT}(a, b)$ für alle $a, b \in R$ und ist als R-Linearkombination von a, b, darstellbar:

$$\exists x, y \in R : d = \operatorname{ggT}(a, b) = xa + yb$$

Beweis

I Falls $b = 0$ („Induktionsanfang") gilt $d = a_{\text{nor}} = e \cdot a + 0 \cdot b$ mit geeignetem $e \in R^{\times}$

II Falls $b \neq 0$: Division mit Rest $a = qb + r$
Falls $r = 0$ ist $d = b_{\text{nor}}$, fertig!
Falls $r \neq 0$, so gilt $\text{ggT}(a,b) = \text{ggT}(b,r) = d$ und $gr(r) < gr(b)$

Induktionshypothese: $\exists x_0, y_0 \in R$: $d = x_0 b + y_0 r = x_0 b + (a - qb)y_0 = y_0 a + (x_0 - qy_0)b = xa + yb$
Induktionsschritt geleistet. ∎

Die Idee ist, dass ein Ring *faktoriell* heißt, wenn man in ihm eine eindeutige Primzerlegung, wie aus $\mathbb{Z}$ bekannt, hat. Ein Ziel der Vorlesung ist die Feststellung, dass euklidische Ringe faktoriell sind (Euler-Faktoriell-Satz).

Definition
Ein Ring R heißt faktoriell (älter: „ZPE-Ring") wenn gilt:

(i) R ist integer

(ii) Es gibt eine Menge $P \subseteq R$, bezüglich der jedes $a \in R$ mit $a \neq 0$ eine „eindeutige Primzerlegung" hat, also:

$\exists e(a) \in \mathbb{R}^{\times}$ $\exists v_p(a) \in \mathbb{N}$, mit nur endlich vielen $v_p(a) \neq 0$ mit

$$a = e(a) \cdot \prod_{p \in P} p^{v_p(a)} \text{ „Primzerlegung von } a\text{"}$$

Eindeutigkeit heißt: Durch a sind $e(a)$ und alle $v_p(a)$ eindeutig bestimmt.

Der Fall $R = \mathbb{Z}$ ist aus der Schule bekannt, und wird nicht bewiesen. Ein Beispiel ist $-100 = -1 \cdot 2^2 \cdot 5^2$, also $e(-100) = -1$, $v_2(-100) = v_5(-100) = 2$ und $\forall p \in P, p \neq 2, p \neq 5 : v_p(-100) = 0$

Im Fall $R = K$, wobei K ein Körper ist, gilt $R^{\times} = \mathbb{K} \setminus \{0\}$ und $P = \emptyset$.

Ist R faktoriell, so ist die Standardnormierung

$$a_{\text{nor}} = \prod_{p \in P} p^{v_p(a)} .$$

Bemerkung: P besteht aus unzerlegbaren Elementen. Hätte man nämlich $p = uv$ mit echten Teilern u, v, so gilt $u, v \notin R^{\times}$, also $\forall p_1, p_2 \in P$: $v_{p_1} > 0, v_{p_2} > 0$. Nun haben wir zwei Primzerlegungen, da $v_p(p) = 1$, $\forall q \in P, q \neq p, v_q(p) = 0$ und damit $p = 1 \cdot p^1 = 1 \cdot p_1^1 \cdot p_2^1$

Ein Zweck der Primfaktorzelegung ist, dass die Multiplikation in R auf die $R^{\times}$ und die Addition in $\mathbb{N}$ zurückgeführt werden kann. Denn mit $a = e(a) \cdot \prod_{p \in P} p^{v_p(a)}$, $b = e(b) \cdot \prod_{p \in P} p^{v_p(b)}$ gilt:

$$\begin{aligned} ab &= e(a) \cdot e(b) \cdot \prod_{p \in P} p^{v_p(a) + v_p(b)} \\ &= e(ab) \cdot \prod_{p \in P} p^{v_p(ab)} \end{aligned}$$

Aus der Eindeutigkeit folgt nun: $e(ab) = e(a) \cdot e(b)$ und $v_p(ab) = v_p(a) + v_p(b)$. $v_p(a)$ heißt „additiver p-Wert von a“. v_p heißt (additive) p-adische Bewertung von R.

Ein weiterer Zweck liegt in der Rückführung der Teilbarkeit auf $\leq$ in $\mathbb{N}$: Für $a, b \neq 0$ gilt

$$b|a \iff \forall p \in P : v_p(b) \leq v_p(a)$$

Begründung: $nb = a \implies v_p(b) \leq v_p(b) + \underbrace{v_p(n)}_{\geq 0} = v_p(a)$

Eine Folgerung davon ist, dass $\forall p \in P$ gilt: $v_p(\mathrm{ggT}(a, b)) = \min\{v_p(a), v_p(b)\}$ und allgemeiner: $v_p(\mathrm{ggT}(a_1, \ldots, a_n)) = \min\{v_p(a_1), \ldots, v_p(a_n)\}$. (Damit das auch bei $a = 0$ Sinn macht, kann man $v_p(0) = \infty$ definieren, was auch üblich ist.) Ebenso gilt: $\forall p \in P$: $v_p(\mathrm{kgV}(a, b)) = \max\{v_p(a), v_p(b)\}$.

Allerdings ist zur Bestimmung von $\mathrm{kgV}(a, b)$ folgener Algorithmus besser als der Weg über die Primfaktorzelegung:

(1) Berechne $\mathrm{ggT}(a, b)$ mit Euklids Algorithmus

(2) Verwende: Sind a, b normiert, so gilt:

$$\mathrm{ggT}(a, b) \cdot \mathrm{kgV}(a, b) = ab$$

Begründung: $\min\{v_p(a), v_p(b)\} + \max\{v_p(a), v_p(b)\} = v_p(a) + v_p(b)$ und $ab = \prod_{p \in P} p^{v_p(a)+v_p(b)}$

Anwendungsbeispiel: Ist $m, n \in \mathbb{N}_+$, so gilt $\mathrm{ggT}(a^m, b^n) = 1 \iff \mathrm{ggT}(a, b) = 1$

Zusammenfassung: Für alle $a, b \in R$, $a, b \neq 0$ gilt:

- $v_p(ab) = v_p(a) + v_p(b)$
- $a \in R^\times \iff \forall p \in P : v_p(a) = 0$
- $v_p(a + b) \geq \min\{v_p(a), v_p(b)\}$
- $v_p(\mathrm{ggT}(a, b)) = \min\{v_p(a), v_p(b)\}$

Noch zu zeigen: $v_p(a + b) \geq \min(v_p(a), v_p(b))$.
O.B.d.A: $v_p(a) \leq v_p(b)$, also $\min(v_p(a), v_p(b)) = v_p(a)$. $a = p^{v_p(a)} \cdot a_0$, $b = p^{v_p(b)} b_0$ mit $a_0, b_0 \in \mathbb{R}$.
$a + b = p^{v_p(a)}(a_0 + p^{v_p(b)-v_p(a)} b_0) \Rightarrow p^{v_p(a)} | a + b \Rightarrow v_p(p^{v_p(a)}) = v_p(a) \leq v_p(a + b)$

Bemerkung: Ist R (integrer Rang) enthalten in einem Körper, so ist $K = \{\frac{a}{b} = x | a, b \in R, b \neq 0\}$ ein Körper.
Man kann v_p auf K ausdehnen: $v_p(x) = v_p(a) - v_p(b)$ $(x \neq 0)$ Ist R faktoriell, so hat man die „Primzerlegung“ von $x = \frac{a}{b}$:

$$x = e(x) \cdot \prod_{p \in P} p^{v_p(x)}$$

mit $e(x) \in R^\times, v_p(x) \in \mathbb{Z}$. Nur endlich viele $v_p(x)$ sind $\neq 0$.
$x \in R \Leftrightarrow v_p(x) \geq 0$ $(\forall p \in P)$. Die Rechenregeln 1-4 gelten auch auf K (siehe R [Beweis leicht]).

Beispiel
$v_7(\frac{7}{25}) = 1, v_5(\frac{7}{25}) = -2, v_p(\frac{7}{25}) = 0$ sonst

Lemma 1.11
Sei R euklidisch, dann gibt es eine „Größenfunktion“ $gr : R \to \mathbb{N}$ für die (zusätzlich) gilt:

- Ist $e \in R^\times, a \in R, a \neq 0 : gr(ea) = gr(a)$
- Ist b ein *echter* Teiler von $a \neq 0$, so ist $gr(b) < gr(a)$

Beweis
Idee: Ist gr die gegebene Größenfunktion, so erfüllt

$$gr^*(a) = \min\{gr(ea) | e \in R^\times\}$$

die beiden Punkte des Lemmas. (Beweis wird auf die Homepage gestellt!) ∎

Für $R = \mathbb{Z}$ und $R = K[X]$ sind beide ohnehin richtig.
(z.B. $\mathbb{Z}, gr(a) = |a|, b$ echter Teiler. $a = bu, u \in \mathbb{Z}^\times = \{\pm 1\} \Rightarrow |a| > 1 \Rightarrow gr(a) = |a| = |b||u|, gr(b) = |b| = \frac{|a|}{|u|} < |a| = gr(a)$. Ähnlich in $K[x]$)

Lemma 1.12
R sei euklidisch, $p \in R$ irreduzibel, $a, b \in R$. Dann gilt:

$$p|ab \implies p|a \text{ oder } p|b$$

Beweis
O.B.d.A.: p normiert, die normierten Teiler von p sind 1 und p.
Annahme: $p \nmid a \wedge p \nmid b$
Falls $p \nmid a \Rightarrow \mathrm{ggT}(p, a) = 1$
(anderenfalls $\mathrm{ggT}(p, a) = p$, damit $p|a$, Widerspruch!).
$p \nmid b \Rightarrow \mathrm{ggT}(p, b) = 1$.
Nach dem Linearkombinations-Satz:

$$\exists x_0, y_0, x_1, y_1 \in R : 1 = x_0 p + y_0 a = x_1 p + y_1 b$$
$$1 = 1 \cdot 1 = \underbrace{(...)}_{\in R} p + y_0 y_1 ab$$

$p|ab \Rightarrow p|1 \Rightarrow p \in R^\times$, also nicht irreduzibel, Widerspruch! ∎

Beweis
Des Euler-Faktoriell-Satzes: R euklidisch $\Rightarrow R$ faktoriell.
$P = \{p_{\text{nor}} | p \text{ irreduzibel}\}$ (z.B. $P = \mathbb{P}$ für $R = \mathbb{Z}$).
Existenz der Primzerlegung für $a \in R$ $(a \neq 0)$

I Fall: $a \in R^\times$, Primzerlegung $a = e(a), \forall p \in P$: $v_p(a) = 0$

II Fall: a irreduzibel $\Rightarrow p = a_{\text{nor}} \in P$, $a = ea_{\text{nor}} = ep, e \in R^\times, e(a) := e, v_p(a) = \begin{cases} 1 & q = p \\ 0 & q \neq p \end{cases}$

Allgemeiner Fall wird durch Induktion nach $gr(a)$ bewiesen.
Es ist nur noch $a \in R, a \neq 0, a \notin R^\times$, a nicht unzerlegbar zu betrachten $\Rightarrow a = u \cdot v$ mit u, v echte Teiler. Induktions-Hypothese mit Hilfe des Lemma 1.11 $\Rightarrow gr(u) < gr(a) \wedge gr(v) < gr(a)$, also haben u, v Primzerlegung $\Rightarrow$ (Durch Ausmultiplizieren) a hat Primzerlegung: $e(a) = e(u) \cdot e(v) \in R^\times$, $v_p(a) = v_p(u) + v_p(v)$

Eindeutigkeit: $a = e(a) \cdot \prod p^{v_p(a)} = e'(a) \cdot \prod p^{v'_p(a)}$ seien zwei Primzerlegungen.
Zu zeigen: $e(a) = e'(a)$, $\forall p \in P : v_p(a) = v'_p(a)$
Induktion nach $n =: \sum_{p \in P}(v_p(a) + v'_p(a)) \in \mathbb{N}$
Induktionsanfang: $n = 0 \Rightarrow \forall p : v_p(a) = 0 = v'_p(a) \Rightarrow e(a) = e'(a)$
Induktionsschritt: $n > 0 \Rightarrow \exists p : v_p(a) > 0 \vee v'_p(a) > 0$, O.B.d.A.: $v_p(a) > 0 \Rightarrow p | a = e'(a) \prod_{q \in P} q^{v'_q(a)}$
Aus Lemma 1.12 leicht induktiv: $p | a_1 \cdot ... \cdot a_n \Rightarrow \exists j : p | a_j \Rightarrow \underbrace{p | e'(a)}_{\text{geht nicht}} \vee \exists q \in \mathbb{P} : p | q^{v'_q(a)} \Rightarrow p | q$
$\Rightarrow p$ ist normierter Teiler von $q \Rightarrow p = q$ ($p = 1$ geht nicht) $\Rightarrow p | p^{v'_p(a)} \Rightarrow v'_p(a) > 0$
$\tilde{a} = e(a) p^{v_p(a)-1} \prod_{q \neq p} p^{v_p(a)} = e'(a) p^{v'_p(a)-1} \prod_{q \neq p} q^{v'_p(a)}$
Zwei Primzerlegungen von $\tilde{a}$ mit $n-2$ statt n. Induktionshypothese anwendbar auf $\tilde{a} \Rightarrow e(a) = e'(a), \forall q \neq p : v_p(a) = v'_q(a)$. $v_p(a) - 1 = v'_p(a) - 1 \Rightarrow$ Induktionsschritt geleistet. ∎

Primzerlegung hat viele Anwendungen, z.B.: $\mathrm{ggT}(a, b) = 1 \Rightarrow \mathrm{ggT}(a^n, b^m) = 1$

Satz 1.13 (Irrationalitätskriterium)
Sei $\alpha \in \mathbb{C}$ eine Nullstellen von $f = X^m + \gamma_1 X^{m-1} + ... + \gamma_{m-1} X + \gamma_m \in \mathbb{Z}[X]$ (d.h. $\gamma_1, ..., \gamma_m \in \mathbb{Z}$) Ist dann $\alpha \notin \mathbb{Z}$, so $\alpha \notin \mathbb{Q}$.

Beweis
Annahme $\alpha \in \mathbb{Q}$, $\alpha = \frac{z}{n}, z \in \mathbb{Z}, n \in \mathbb{N}_+$, $\mathrm{ggT}(z, n) = 1$
$0 = f(\frac{z}{n}) = \frac{z^m}{n^m} + \gamma_1 \frac{z^{m-1}}{n^{m-1}} + ... + \gamma_{m-1} \frac{z}{n} + \gamma_m$, multiplizieren mit $n^m \Rightarrow$
$0 = z^m + n \underbrace{(...)}_{\in \mathbb{Z}} \Rightarrow n | z^m \Rightarrow n | \mathrm{ggT}(z^m, n) = 1$, da $\mathrm{ggT}(z, n) = 1$ (s.o.)
$n | 1 \Rightarrow \alpha = \frac{z}{n} = z \in \mathbb{Z}$. ∎

Anwendung: z.B. auf $f = X^k - a, a \in \mathbb{Z} (k > 1)$. Ist a keine k-te Potenz in $\mathbb{Z}, \alpha$ eine Nullstelle von f in $\mathbb{C}$ (sozusagen $\alpha = \sqrt[k]{a}$), so ist α irrational.

[$\alpha \in \mathbb{Z} : a = \alpha^k$ ist k-te Potenz in $\mathbb{Z}$] Tritt zum Beispiel ein, wenn $\exists p \in \mathbb{P} : k \nmid v_p(a)$ (denn $a = z^k \Rightarrow v_p(a) = k \cdot v_p(z)$. Etwa $\sqrt[k]{q}, q \in \mathbb{P}$ ist immer irrational, z.B. $\sqrt{2}$.

Die erste Grundlagenkrise der Mathematik Die Pythagoräer glaubten, alle Naturwissenschaften seien durch $\mathbb{N}$ „mathematisierbar“. Zum Beispiel wurde Folgendes als selbstverständlich betrachtet:
Man kann kleinen Einheitsmaßstab e (verdeutlicht durch einen gezeichneten Streckenstab mit kleinen Einheiten) wählen, so dass die Strecke a und die Strecke b in der Form $a = n \cdot e, b = m \cdot e$ ist, mit $n, m \in \mathbb{N} \Leftrightarrow \frac{b}{a} \in \mathbb{Q}$.
Modern ist die Aussage $\frac{b}{a} = \sqrt{2} \Rightarrow$ Seite und Diagonale erfüllen nicht dem Glauben.

Der Glaube besagt: Nur natürliche und rationale Zahlen sind Zahlen. $\Rightarrow$ Die Länge einer Strecke ist keine Zahl.

Der Dozent glaubt, dies hat die Griechen daran gehindert „reelle Zahlen" zu erfinden, d.h. mit Längen von Strecken wie in einem Körper zu rechnen (wirkt über 1000 Jahre, relle Zahlen exakt erst seit ca. 1800 exakt erklärt!).
Heute bekannt: Die Proportionenlehre von Eudoxos von Knidos ist logisch äquivalent zu der Konstruktion der rellen Zahlen.

2 Arithmetische Funktionen

2.1 Einführung

Erklärung: Eine zahlentheoretische Funktion ist eine Abbildung $\alpha : \mathbb{N} \to \mathbb{C}$, also nichts anderes als eine Folge $\alpha_n = \alpha(n)$ komplexer Zahlen ($n \in \mathbb{N}$).

Beispiel
p_n: $n \to p_n$ (n-te Primzahl) ist eine zahlentheoretische Funktion.

Kurzbezeichnung: $\sum_{d|n} = \sum_{\{d \in \mathbb{N}_+ \big| d|n\}}$
Standardbezeichnungen (*in vielen Büchern*):

- $\varphi(n) = \#\{x \in \mathbb{N} | 1 \leq x \leq n \wedge \mathrm{ggT}(x,n) = 1\}$ („*Eulersche Funktion*“)
- $\tau(n) = \sum_{d|n} 1 = \#\{x \in \mathbb{N}; x|n\}$
- $\sigma(n) = \sum_{d|n} d$ „Teilersumme“
- $\sigma_k(n) = \sum_{d|n} d^k$, $k \in \mathbb{N}$, also $\sigma_0 = \tau$, $\sigma_1 = \sigma$
- $\omega(n) = \#\{p \in \mathbb{P} \big| p|n\}$
- $\mu(n) = \begin{cases} 0 & \exists p \in \mathbb{P} : p^2 | n \\ (-1)^{\omega(n)} & \text{sonst, d.h. „}n\text{ quadratfrei“} \end{cases}$ „Möbiusfunktion“

Zeichen in dieser Vorlesung:

- c_a: Konstante Funtion, also $\forall n \in \mathbb{N} : c_a(n) = a$
- δ: $\delta(n) = \begin{cases} 1 & n = 1 \\ 0 & \text{sonst} \end{cases} = \delta_{1,n}$ „Kronecker-Delta“
- $\Pi_k(n) = n^k$ „Potenzfunktion“

Sprechweise für den Fall $\mathrm{ggT}(x,n) = 1 \iff x$ und n sind „relativ prim“.
Beispiel

(1) $\varphi(12) = \#\{1, 5, 7, 11\} = 4$

(2) $p \in \mathbb{P}$, $n \in \mathbb{N}_+$, $\varphi(p^n) = ?$

$\mathrm{ggT}(x, p^n) = 1 \iff p \nmid x$
$\{x \in \mathbb{N}_+ | \mathrm{ggT}(x, p^n) = 1, x \leq p^n\} = \{x \in \mathbb{N}_+ | p \nmid x, x \leq p^n\}$
$= \{1, \ldots, p^n\} \setminus \{p, 2p, \ldots, p^n\} = \{1, \ldots, p^n\} \setminus p\{1, 2, \ldots, p^{n-1}\}$
$\varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1) = p^n(1 - \frac{1}{p})$

2.2 Dirichlet-Reihen

Benannt nach Peter Gustav Lejeune Dirichlet, 1805-59.

Definition
Sei α eine zahlentheoretische Funktion. Ist $s \in \mathbb{R}$ oder besser $s \in \mathbb{C}$, so definiert man:

$$L(s, \alpha) = \sum_{n \in \mathbb{N}_+} \frac{\alpha(n)}{n^s}$$

Beispiel
$L(s, c_1) = \zeta(s)$ („Riemanns ζ-Funktion“)

Wir rechnen nun formal. α, β seien zahlentheoretische Funktionen:

$$\begin{aligned} L(s, \alpha) \cdot L(s, \beta) &= \sum_{n \in \mathbb{N}_+} \frac{\alpha(n)}{n^s} \cdot \sum_{n \in \mathbb{N}_+} \frac{\beta(n)}{n^s} \\ &= \sum_{n,u \in \mathbb{N}_+} \sum_{n,u; nu=m} \frac{\alpha(n) \cdot \beta(u)}{(nu)^s} \\ &= \sum_{m \in \mathbb{N}_+} \frac{(\alpha * \beta)(m)}{m^s} \end{aligned}$$

mit der *Dirichlet-Faltung*:

$$(\alpha * \beta)(n) = \sum_{u,v \in \mathbb{N}_+; uv=n} \alpha(u)\beta(v) = \sum_{d|n} \alpha(d)\beta\left(\frac{n}{d}\right)$$

Als Ergebnis erhalten wir jetzt (formal):

$$L(s, \alpha) \cdot L(s, \beta) = L(s, \alpha * \beta)$$

2.3 Arithmetische Funktionen allgemein

R sei jetzt ein faktorieller Ring.

Definition

$$R_{\text{nor}} = \{q_{\text{nor}} | q \neq 0\}$$

(z.B.: $\mathbb{Z}_{\text{nor}} = \mathbb{N}_+$))

Bemerkung: $\{d|n \big| d \in R_{\text{nor}}\}$, $(n \neq 0)$, ist *endlich.*

$n = e(n) \cdot \prod_{p \in \mathbb{P}} p^{v_p(n)}$ hat endlich viele $v_p(n) \neq 0$, etwa $p = p_1, \ldots, p_l$

$d|n, d = \prod_{p \in \mathbb{P}} p^{m_p}$ mit $m_p \leq v_{p_1}(n), \ldots, m_{p_l} \leq v_{p_l}(n)$, $m_p = 0$ sonst.

Definition

(1) Jede Abbildung $\alpha : R_{\text{nor}} \to K$ (K ein Körper) heißt in dieser Vorlesung (K-wertige) arithmetische Funktion (auf R). Die Menge dieser Funktoin wird hier mit Arfun $=$ Arfun$_{R,K}$ bezeichnet.

(2) Für $\alpha, \beta \in$ Arfun wird definiert:

- $\alpha + \beta$ durch $(\alpha + \beta)(n) = \alpha(n) + \beta(n)$
- $c\alpha$, ($c \in K$), durch $(c\alpha)(n) = c \cdot \alpha(n)$

(3) Dirichlet-Faltung $\alpha * \beta$ durch

$$(\alpha * \beta)(n) = \sum_{d|n} \alpha(d) \cdot \beta(\frac{n}{d})$$

(Das Inverse wird mit α^{-1} bezeichnet, also $\alpha * \alpha^{-1} = 1$)

Satz 2.1 (Arfun-Ring-Satz)

- (Arfun,+,$*$) ist *integrer* Ring und K-Vektorraum.
- $\alpha \in \text{Arfun}^{\times} \iff \alpha(1) \neq 0$.

Beweis

Die Vektorraumeigenschaft wird wie in der Analysis gezeigt. Wir zeigen die Ringeigenschaft:

Einselement ist $1_{\text{Arfun}} = \delta$:

$$(\delta * \alpha)(n) = \sum_{d|n} \delta(d)\alpha(\frac{n}{d}) = \delta(1) \cdot \alpha(\frac{n}{1}) = \alpha(n)$$

Die Kommutativität von $*$ ist offensichtlich. Die Distributivregel gilt auch:

$$\begin{aligned}
\alpha * (\beta + \gamma)(n) &= \sum_{d|n} \alpha(d) \cdot (\beta + \gamma)\left(\frac{n}{d}\right) \\
&= \sum_{d|n} \alpha(d) \cdot \left(\beta\left(\frac{n}{d}\right) + \gamma(\frac{n}{d})\right) \quad (\cdot \text{ ist distributiv in } \mathbb{C}) \\
&= \sum_{d|n} \left(\alpha(d) \cdot \beta\left(\frac{n}{d}\right) + \alpha(d) \cdot \gamma\left(\frac{n}{d}\right)\right) \\
&= \sum_{d|n} \alpha(d) \cdot \beta\left(\frac{n}{d}\right) + \sum_{d|n} \alpha(d) \cdot \gamma\left(\frac{n}{d}\right) \\
&= (\alpha * \beta)(n) + (\alpha * \gamma)(n) \\
&= ((\alpha * \beta) + (\alpha * \gamma))(n)
\end{aligned}$$

Bemerkung:

$$(\alpha * \beta)(n) = \sum_{u,v \in R_{\text{nor}};\ u \cdot v = n} \alpha(u)\beta(v)$$

Nun zeigen wir noch die Assoziativregel:

$$\begin{aligned}((\alpha * \beta) * \gamma)(n) &= \sum_{u,v;\ uv=n} (\alpha * \beta)(u)\gamma(v) \\ &= \sum_{uv=n;\ xy=u} (\alpha(x)\beta(y))\gamma(v) \\ &= \sum_{xyv=n} \alpha(x)\beta(y)\gamma(v) \\ &= \sum_{xu=n;\ yv=u} \alpha(x)(\beta(y)\gamma(v)) \\ &= \sum_{xu=n} \alpha(x)((\beta * \gamma)(u)) \\ &= (\alpha * (\beta * \gamma))(u)\end{aligned}$$

Den Beweis, dass Arfun ein integrer Ring ist, führen wir nur für $R = \mathbb{Z}$, lässt sich aber mit etwas Scharfsinn auf beliebige R übertragen.

$\alpha \neq 0,\ \beta \neq 0 \implies \exists u = \min\{x \in \mathbb{N}_+ | \alpha(x) \neq 0\},\ v = \min\{y \in \mathbb{N}_+ | \beta(y) \neq 0\}.\ n := uv.$

$(\alpha * \beta)(n) = \sum_{xy=n} \alpha(x)\beta(y).\ x < u \implies \alpha(x) = 0,\ x > u \implies y = \frac{n}{x} < \frac{n}{u} = v \implies \beta(y) = 0.$

Also: $(\alpha * \beta)(n) = \alpha(u)\beta(\frac{n}{u}) = \alpha(u)\beta(v) \neq 0$, da K integer $\implies \alpha * \beta \neq 0$

Die Existenz von Inversen: $\alpha \in \mathrm{Arfun}^\times \iff \exists \beta \in \mathrm{Arfun} : \beta * \alpha = \delta (= 1_{\mathrm{Arfun}})$

β existiere $\implies 1 = \delta(1) = (\beta * \alpha)(1) = \sum_{d|1} \beta(1)\alpha(\frac{1}{d}) = \beta(1)\alpha(1) \implies \alpha(1) \neq 0$

Sei $\alpha(1) \neq 0$. Setze $\beta(1) = \frac{1}{\alpha(1)}$ (geht, da K ein Körper ist und $\alpha(1) \neq 0$). β ist so zu definieren, dass für $n \in R_{\mathrm{nor}}$, $n \neq 1$, gilt:

$$(*) \quad 0 = \delta(n) = (\beta * \alpha)(n) = \sum_{d|n} \beta(d)\alpha(\frac{n}{d}) \tag{2.1}$$

■

Induktion nach $\mathrm{len}(n) = \sum_{p \in \mathbb{P}} v_p(n)$, $\mathrm{len}(n) = 0$, dann $n = 1$, also OK.

Bemerkung: $d|n, d \neq n\ (d = d_{\mathrm{nor}}) \implies \mathrm{len}(d) < \mathrm{len}(n)$

Induktiv darf man $\beta(d)$ schon als definiert annehmen.

$$(2.1) \iff \beta(n) = -\frac{1}{\alpha(1)} \sum_{d|n,\ d \neq m} \beta(d)\alpha(\frac{d}{n}).$$

Die rechte Seite ist schon erklärt, die linke Seite dadurch gewonnen. β also rekursiv, also definiert, so dass $\beta * \alpha = \delta$. Im Prinzip wird β als „Programm“ realisiert.

2.4 Multiplikative arithmetische Funktionen

Definition
$\alpha \in \mathrm{Arfun}_{R,K}$, $(\alpha \neq 0)$, heiße *multiplikativ* $\iff$

$$\forall m, n \in R_{\mathrm{nor}} \text{ mit } \mathrm{ggT}(m,n) = 1 : \quad \alpha(mn) = \alpha(m)\alpha(n)$$

α multiplikativ $\implies \alpha\left(\prod_{p\in\mathbb{P}} p^{v_p(n)}\right) = \prod_{p\in\mathbb{P}} \alpha(p^{v_p(n)})$

Ein Beispiel für eine Anwendung folgt aus der Multiplikativität der Eulerfunktion φ, welche wir später zeigen werden:

$$\varphi(p^{v_p(n)}) = p^{v_p(n)}(1-\frac{1}{p}) \text{ für } p\in\mathbb{P} \implies \varphi(n) = n\cdot\prod_{p\in\mathbb{P},p|n}\left(1-\frac{1}{p}\right) \qquad \text{„Eulers Formel“}$$

Beispiel
Π_k ist multiplikativ. ($\Pi_k(n) = n^k$)

Satz 2.2 (Multiplikativitätssatz für Arfun)

(1) Ist $\alpha \in$ Arfun multiplikativ, so ist $\alpha(1) = 1$

(2) Die multiplikativen Funktionen bilden eine Untergruppe von (Arfun$^\times$, $*$), also α, β multiplikativ, so auch $\alpha * \beta$ und α^{-1}.

Beweis

(1) α ist multiplikativ $\implies \alpha(1) = \alpha(1\cdot 1) \overset{\mathrm{ggT}(1,1)=1}{=} \alpha(1)\cdot\alpha(1) \overset{\text{Körper!}}{\implies} \alpha(1) = 1$ oder $\alpha(1) = 0$. Falls $\alpha(1) = 0$, so $\forall n \in R_{nor}$ $\alpha(n) = \alpha(n\cdot 1) \overset{\mathrm{ggT}(n,1)=1}{=} \alpha(n)\cdot\underbrace{\alpha(1)}_{=0} = 0 \implies \alpha \equiv 0$ und das ist nach Definition *nicht* multiplikativ, also gilt $\alpha(1) = 1$.

(2) Zu zeigen: α, β multiplikativ $\implies \alpha * \beta$ multiplikativ und α^{-1} ist ebenfalls multiplikativ.

$$(\alpha*\beta)(n_1 n_2) = (\alpha*\beta)(n_1)\cdot(\alpha*\beta)(n_2), \tag{2.2}$$

falls $\mathrm{ggT}(n_1, n_2) = 1$. $(\alpha*\beta)(1) = \sum_{d|n}\alpha(d)\beta(\frac{1}{d}) = \alpha(1)\beta(1) \overset{\alpha,\beta \text{ mult.}}{=} 1\cdot 1 \implies$ (2.2) ist ok, wenn $n_1 = 1$ oder $n_2 = 1$. Sei nun $n_1 \neq 1,\ n_2 \neq 1$.
Behauptung: $n = n_1 n_2$: Jeder Teiler $d|n$ ist eindeutig in der Form $d = d_1, d_2$ mit $d_1|n_1$ und $d_2|n_2$ darstellbar.
Folgende Funktion f ist bijektiv:

$$f : \begin{cases} \{(d_1,d_2)\big|d_1|n_1,\ d_2|n_2\} & \to & \{d\big|d|n\} \\ (d_1,d_2) & \mapsto & d_1 d_2 \end{cases}$$

Die Behauptung ist klar, wenn man die Primzahlzerlegung anschaut ($n_1,\ n_2 \neq 1$): $n_1 = \prod_{i=1}^t p_i^{v_i}$, $n_2 = \prod_{i=1}^l q_i^{w_i}$, die p_i sowie die q_i sind jeweils paarweise verschiedene Primzahlen. $\mathrm{ggT}(n_1,n_2) = 1 \iff \{p_1,p_2,\ldots,p_t\}\cap\{q_1,q_2,\ldots,q_l\} = \emptyset$.

$d|n, d = \underbrace{\prod_{i=1}^t p_i^{u_i}}_{=d_1}\cdot\underbrace{\prod_{i=1}^l q_i^{y_i}}_{=d_2}$ mit $u_j \le v_j,\ y_k \le w_k$.

Es gilt weiterhin $\mathrm{ggT}(d_1, d_2) = 1 = \mathrm{ggT}\left(\frac{n_1}{d_1}, \frac{n_2}{d_2}\right)$.

$$\begin{aligned}
(\alpha * \beta)(\underbrace{n}_{=n_1 n_2}) &= \sum_{d|n} \alpha(d)\beta(\frac{n}{d}) \\
&= \sum_{d_1|n_1,\ d_2|n_2} \alpha(d_1 d_2)\beta\left(\frac{n_1}{d_1}\frac{n_2}{d_2}\right) \\
&\overset{\alpha,\ \beta \text{ mult.}}{=} \sum_{d_1|n_1,\ d_2|n_2} \alpha(d_1)\alpha(d_2)\beta\left(\frac{n_1}{d_1}\right)\beta\left(\frac{n_2}{d_2}\right) \\
&= \sum_{d_1|n_1,\ d_2|n_2} \left(\alpha(d_1)\beta\left(\frac{n_1}{d_1}\right)\right) \cdot \left(\alpha(d_2)\beta\left(\frac{n_2}{d_2}\right)\right) \\
&\overset{\text{distributiv}}{=} \sum_{d_1|n_1} \alpha(d_1)\beta\left(\frac{n_1}{d_1}\right) \cdot \sum_{d_2|n_2} \alpha(d_2)\beta\left(\frac{n_2}{d_2}\right) \\
&= (\alpha * \beta)(n_1) \cdot (\alpha * \beta)(n_2).
\end{aligned}$$

Zeige nun noch: α multiplikativ $\implies$ $\beta = \alpha^{-1}$ ist multiplikativ. In der Vorlesung wird nur die Idee gezeigt, der Rest bleibt als Übung. Sei also γ die multiplikative Funktion mit $\gamma(1) = 1$ und $\gamma(p^k) = \beta(p^k)$, $(p \in P, k \in \mathbb{N}_+$ (nach (3))) Mit Hilfe der Multiplikativität von γ leicht nachzuweisen: $\alpha * \gamma = \delta \implies \gamma = \alpha^{-1} = \beta \implies \beta$ ist multiplikativ. ■

Beispiel
Anwendungsbeispiele für diesen Satz: Π_k ist multiplikativ, $c_1 = \Pi_0$ auch. Daraus folgt, dass $\Pi_k * c_1$ auch multiplikativ ist. Wegen $(\Pi_k * c_1)(n) = \sum_{d|n} \Pi_k(d)c_1(\frac{n}{d}) = \sum_{d|n} d^k = \sigma_k(n)$ ist also auch σ_k, insbesondere σ und τ, multiplikativ.

Zum Beispiel: $\sigma_k(p^t) = \sum_{d|p^t} d^k = \sum_{j=0}^{t} (p^j)^k = \frac{p^{k(t+1)}}{p^k - 1}$.
Das liefert die Formel $\sigma_k(n) = \prod_{p\in\mathbb{P}, p|n} \frac{p^{k(v_p(n)+1)}-1}{p^k-1}$
sowie $\tau(p^t) = t + 1 \implies \tau(n) = \prod_{p|n}(v_p(n) + 1)$ und

$$\sigma(n) = \prod_{p|n} \frac{p^{v_p(n)+1} - 1}{p - 1}. \tag{2.3}$$

Eine konkrete Berechnung ist $\sigma(100) = \frac{2^3-1}{2-1} \cdot \frac{5^3-1}{5-1} = 7 \cdot 31$.

Historischer Exkurs

$\sigma(n) = \sum_{d|n} d$ (Teilersumme), $\sigma^*(n) = \sum_{d|n,\ d\neq n} d = \sigma(n) - n$.

Benennung (Griechen): $n \in \mathbb{N}_+$ heißt $\left\{\begin{array}{c}\text{defizient}\\ \text{abundand}\\ \text{vollkommen}\end{array}\right\} \iff \sigma^*(n) \left\{\begin{array}{c}<\\ >\\ =\end{array}\right\} n.$

Beispielsweise ist jede Primzahl defizient, 12 abundant und 6 ist die kleinste vollkommene Zahl.

Satz 2.3 (Euklid, Euler)
Die geraden vollkommenen Zahlen sind genau die der Form

$$n = 2^{p-1} M_p \quad p \in \mathbb{P},\ M_p = 2^p - 1 \in \mathbb{P} \text{ Mersenne-Primzahl.}$$

Unbekannt: Gibt es unendlich viele Mersenne-Primzahlen? Gibt es unendlich viele vollkommene Zahlen? Gibt es wenigstens *eine* ungerade vollkommene Zahl (Es gibt mindestens 100 Arbeiten zu den Eigenschaften der ungeraden vollkommenen Zahlen, aber leider hat noch niemand eine gefunden)?

Beweis
„$\Leftarrow$" Sei $n = 2^{p-1} M_p$ wie oben.

$$\begin{aligned}\sigma(n) &= \sigma(2^{p-1}) \cdot \sigma(M_p) = \left(\underbrace{\frac{2^{p-1+1}-1}{2-1}}_{\text{vgl. (2.3)}}\right) \cdot \underbrace{(1+M_p)}_{M_p \text{ ist prim}} \\ &= (2^p - 1)2^p = 2 \cdot 2^{p-1} \cdot M_p = 2n \implies \sigma^*(n) = n \implies n \text{ vollkommen.}\end{aligned}$$

„$\Rightarrow$ " n sei vollkommen und $2|n$, also $\sigma(n) = 2n$. $n = 2^r \cdot x, x \in \mathbb{N}_+,\ 2 \nmid x \implies \operatorname{ggT}(2^r, x) = 1$.

$$\sigma(n) \overset{\text{mult.}}{=} \sigma(2^r)\sigma(x) = \frac{2^{r+1}-1}{2-1}\sigma(x) \overset{n \text{ vollkommen}}{=} 2n = 2^{r+1}x \tag{2.4}$$

$\operatorname{ggT}(2^{r+1}, 2^{r+1}-1) = 1 \implies 2^{r+1}|\sigma(x)$, also $\sigma(x) = 2^{r+1}y$ mit $y \in \mathbb{N}_+$
$\overset{(2.4)}{\implies} x = \underbrace{(2^{r+1}-1)}_{=:b} y = by$. $T(x) \subseteq \{1, y, b, by\}$ mit $b > 1$ wegen $r > 0$. $\sigma(x) = (b+1)y = y + by,\ y < by$ wegen $b > 1$.
$\implies T(x) = \{y, by\} \implies y = 1,\ x = b,\ T(x) = \{1, b\} = \{1, x\} \implies x = 2^{r+1} - 1$ ist prim.
Mit Aufgabe 3a, Übungsblatt 1 $\implies r + 1 = p \in \mathbb{P},\ x = M_p \implies$ Behauptung. ∎

Satz 2.4 (ohne Beweis, nach Abdul Hassan Thâ bit Ibn Kurah, ca. 900)
Sind $u = 3 \cdot 2^{n-1} - 1,\ v = 3 \cdot 2^n - 1,\ w = 9 \cdot 2^{n-1}$ alle prim, so sind $2^n uv$ und $2^n w$ befreundet. Zwei Zahlen n, m aus $\mathbb{N}_+$ heißen befreundet, genau wenn $\sigma(n) = \sigma(m)$ gilt (zum Beispiel 220 und 284).

Zur Eulerschen Funktion φ: $\operatorname{Relp}(n, d) := \{x \in \mathbb{N}_+ | x \leq n,\ \operatorname{ggT}(n, x) = d\}$.
$\varphi(n) = \# \operatorname{Relp}(n, 1)$.

Lemma 2.5 (Gauß)

$$n = \sum_{d|n} \varphi(d)$$

Beweis
Die Abbildung $f : \begin{cases} \text{Relp}(\frac{n}{d},1) & \to & \text{Relp}(n,d) \\ x & \mapsto & dx \end{cases}$ ist bijektiv.
$\text{ggT}(\frac{n}{d},x)=1,\ d=d\cdot 1=\text{ggT}(d\frac{n}{d},d\cdot 1)=\text{ggT}(n,d),\ x\le \frac{n}{d} \iff dx\le n.$ $\bigcup_{d|n}\text{Relp}(n,d)=\{1,2,\ldots,n\}$ (wenn $\text{ggT}(y,n)=d$, so $y\in\text{Relp}(n,d),\ y\le n$.
$n=\#\{1,2,\ldots,n\}=\sum_{d|n}\#\,\text{Relp}(n,d)\overset{\text{wg. obiger Bijektion}}{=}\sum_{d|n}\#\,\text{Relp}(\frac{n}{d},1)=\sum_{d|n}\varphi\left(\frac{n}{d}\right)=\sum_{d'|n}\varphi(d'),\quad \left(d'=\frac{n}{d'}\right).$ ∎

Lemma von Gauß sagt: $\Pi_1=\varphi * c_1,\ \Pi_1(n)=n^1=n$. Da Π_1 und c_1 multiplikativ sind $\implies \varphi=\Pi_1 * c_1^{-1}$ ebenfalls multiplikativ (aus Multiplikativitätssatz) $\implies \varphi(n)=n\Pi_{p_n}(1-\frac{1}{p})$ (früher).

Definition
Ist $\alpha\in$ Arfun, dann heißt $\hat\alpha$ Möbiustransformierte von (oder Summatorische Funktion zu) α, wenn:

$$\hat\alpha(n):=\sum_{d|n}\alpha(d)$$

(Das heißt: $\hat\alpha=\alpha * c_1$.)

Problem: Wie kann man α aus $\hat\alpha$ gewinnen (bzw. berechnen)?
Lösung: $\hat\alpha=\alpha * c_1 \implies \alpha=\hat\alpha * \mu$, mit $\mu=c_1^{-1}$.
$\mu=c_1^{-1}$ heißt Möbiusfunktion.
Rest: Bestimmung von μ, da μ multiplikativ ist, reicht es aus,
$\mu(p^l)=c_p,\ p\in P, l\in\mathbb{N}_+$ zu ermitteln.
$\mu(1)=1$
$0=\delta(p^l)=\mu * c_1(p^l)=\sum_{d|p^l}\mu(d)=\sum_{j=0}^{l}\mu(p^j)$
$l=1:\quad 0=\mu(1)+\mu(p) \implies \mu(p)=-1$
$l=2:\quad 0=\mu(1)+\mu(p)+\mu(p^2) \implies \mu(p^2)=0$
...
$\mu(p^i)=0$ für $j\ge 2$. Also folgt, weil μ multiplikativ ist:

$$\mu(n)=\begin{cases}0 & \exists p\in\mathbb{P}:\ p^2|n,\ \text{d.h. } n \text{ ist nicht quadratfrei}\\ (-1)^t & \text{falls } n=p_1\cdot p_2\cdot\cdots\cdot p_t \text{ mit } t \text{ verschiedenen Primzahlen}\end{cases}$$

Ergebnis:

Satz 2.6 (Umkehrsatz von Möbius)
Sei α arithmetische Funktion, $\hat\alpha$ die Möbiustransformierte von α, dann gilt $\alpha=\hat\alpha * \mu$ mit der Möbiusfunktion μ, das heißt:

$$\alpha(n)=\sum_{d|n}\hat\alpha(d)\mu\left(\frac{n}{d}\right)\qquad \text{Möbiussche Umkehrformel}$$

und μ wie oben.

Lineraturhinweise zu den Arithmetischen Funktionen:

(1) Für Algebra-Freunde: „Der Ring Arfun ist selbst faktoriell“, siehe Cashwell, Everett: The Ring of Numbertheoretic Functions, Pacific Math.J., 1955, S. 975ff.

(2) Umkehrformeln gibt es für allgemeinere geordnete Mengen als $(R_{\text{nor}}, |)$, siehe Johnson, Algebra I.

(3) Für Analysis-Freunde: Viel Analysis über zahlentheoretische Funktionen. Viele Sätze über asymptotisches Verhalten (ähnlich $p_n \sim n \cdot \log n$), siehe Schwarz, Spieker, „Arithmetical functions“, Cambridge University Press, 1994.

3 Kongruenzen und Restklassenringe

In diesem Kapitel betrachten wir entweder $R = \mathbb{Z}$ oder $R = K[X]$, wobei K ein Körper ist.

Grundbegriffe

In den betrachteten Ringen gibt es eine eindeutige Restwahl: In $R = \mathbb{Z}$ ist die Division mit Rest $a = qm + r$ mit $0 \leq r < |m|$. Andere Restwahl wäre etwa $a = qm + r'$ mit $-\frac{|m|}{2} < r' \leq \frac{|m|}{2}$. Es besteht folgender Zusammenhang:

$$r' = \begin{cases} r, & 0 \leq r \leq \frac{|m|}{2} \\ r - |m|, & \frac{|m|}{2} < r \leq |m| \end{cases}$$

In $R = K[X]$ haben wir $a = qm + r$ mit $\operatorname{grad} r < \operatorname{grad} m$.

Diese Reste sind eindeutig: Haben wir $a = qm + r = \tilde{q}m + \tilde{r}$ mit $0 \leq r, \tilde{r}, |m|$. Dann ist $(q - \tilde{q})m = \tilde{r} - r \implies |m| \big| \tilde{r} - r$. Annahme: $q - \tilde{q} \neq 0 \implies |\tilde{r} - r| \geq m$, Wid. Also ist $q = \tilde{q}$ und $r = \tilde{r}$. Der Beweis für $R = K[X]$ funktioniert ähnlich.

Definition (Gauß für $\boldsymbol{R} = \mathbb{Z}$)
$m, a, b, \in R$

(1)

$$a \equiv b \mod m \text{ (lies } a \text{ kongruent } b \text{ modulo } m$$

$$\iff a \mod m = b \mod m$$

Gauß schreibt „Zwei Zahlen heißen kongruent mod m, wenn sie bei Division durch m den selben Rest lassen."

(2) $\overline{a} := \{b \in R | b \equiv a \mod m\}$ heißt Restklasse modulo m.

(3) $\overline{R} := R/mR := \{\overline{a} | a \in R\}$ heißt Restklassenring modulo m.

Warum ist Letzeres ein „Ring"? Der Dozent führt einen schönen Beweis durch Aufwickeln einer Schnur auf einer Tesa-Rolle durch.

Beispiel
$\mathbb{Z}/2\mathbb{Z} = \{\overline{0}, \overline{1}\}$ mit $\overline{0} = \{0, \pm 2, \pm 4, \ldots\}$ (die geraden Zahlen) und $\overline{1} = \{\pm 1, \pm 3, \ldots\}$ (die ungeraden Zahlen). Aus der Schule sind folgende Regeln bekannt:

(1) $\overline{0} + \overline{0} = \overline{0}$, „gerade + gerade = gerade"

(2) $\overline{0} + \overline{1} = \overline{1}$, „gerade + ungerade = ungerade"

(3) $\overline{1} + \overline{1} = \overline{0}$, „ungerade + ungerade = gerade“

Bemerkung:

$$\text{(i) } a \equiv b \mod m \iff \text{(ii) } \overline{a} = \overline{b} \iff \text{(iii) } m | a - b$$

Merke: Kongruenz ist Gleichheit der Restklassen.

$\overline{qm} = \overline{0}$. Die Idee: In $\overline{R}$ wird alles durch m teilbare als „unwesentlich“ angesehen und durch 0 ersetzt.

Beweis
$(i) \iff (ii)$: Kongruenz mod m ist Offensichtlich eine Äquivalenzrelation auf R. $\overline{a}$ ist die Äquivalenzklasse von a. Lineare Algebra: Zwei Elemente sind genau dann äquivalent, wenn die zugehörigen Äquivalenzklassen überstimmen.

$(i) \implies (iii)$: $r = a \mod m = b \mod m \implies a = qm + r, b = q'm + r$ (Division mit Rest) $\implies a - b = (q - q')m \implies m | a - b$ ■

Um mit Restklassen zu rechnen, brauchen wir folgende Definitionen:

Definition
Jedes $b \in \overline{a}$ heißt Vertreter der Klasse $\overline{a} \in \overline{R}$. Die Idee ist, die Operationen + und − vertreterweise zu definieren. Wir haben also:

$$(\overline{R}, +, \cdot) \text{ mit } \overline{a} + \overline{b} := \overline{a + b},\ \overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

Zu zeigen: Die Definition ist vertreterunabhängig, also : $\overline{a} = \overline{a'} \implies \overline{a + b} = \overline{a' + b}$ und $\overline{a \cdot b} = \overline{a' \cdot b}$. Das ist klar:

$$\begin{aligned} \overline{a} = \overline{a}' \iff m | a - a' = a + b - (a' + b) &\implies \overline{a + b} = \overline{a' + b} \\ m | a - a' \implies m | (a - a')b = ab - a'b &\implies \overline{ab} = \overline{a'b} \end{aligned}$$

Bemerkung: $e \in R^\times, m \in R \implies R/mR = R/emR$ (da $m|x \iff em|x$). Ohne Beschränkung der Allgemeinheit kann man m also normiert annehmen.

$m = 0$, dann $a \mod m = b \mod m \iff a = b$, also $\overline{a} = \{a\}$„ = “a. Also: $R/oR = R$ und $R/eR = R/R = \{\overline{0}\}$ („Nullring“)

Diese uninteressanten Fälle werden meist beiseite gelassen.

Satz 3.1 (Restklassenring-Satz)
Sei R ein euklidischer Ring, $m \in R$.

(1) $(\overline{R} = R/mR, +, \cdot)$ ist ein Ring

(2) $\overline{R}^\times = \{\overline{a} \in \overline{R} |\ \mathrm{ggT}(a, m) = 1\}$

Zusatz: Zu $\overline{a} \in \overline{R}^\times$. Kann $\overline{a}^{-1}$ effektiv mit Euklids Algorithmus berechnet werden.

Definition
$\overline{a} \in \overline{R}^{\times}$ heißt eine prime Restklasse modulo m, $\overline{R}^{\times}$ heißt prime Restklassengruppe modulo m. (Sprachlich besser wäre eigentlich: Gruppe der zu m relativ primen Restklassen)

Beweis

(1) Alle Ringaxiome vererben sich von den Vertretern auf die Klassen. $\overline{a}+\overline{b} = \overline{a+b} = \overline{b+a} = \overline{b}+\overline{a} \implies (\overline{R},+)$ ist kommutativ. $0 := 0_{\overline{R}} = \overline{0}$, da $\overline{a}+\overline{0} = \overline{(a+0)} = \overline{a}$. $1_{\overline{R}} = \overline{1}$ ebenso.

Assoziativität der Addition: $(\overline{a}+\overline{b})+\overline{c} = \overline{a+b}+\overline{c} = \overline{(a+b)+c} = \overline{a+(b+c)} = \overline{a}+\overline{b+c} = \overline{a}+(\overline{b}+\overline{c})$, Assoziativität der Multiplikation und Distributivgesetzt analog.

(2) $\overline{a} \in \overline{R}^{\times} \overset{\text{Def.}}{\iff} \exists x \in R : \overline{xa} = 1_{\overline{R}} = \overline{1} \iff 1 \equiv ax \mod m \iff \exists q \in R : 1 = ax+qm \implies \mathrm{ggT}(a,m) = 1$, (da normal).

Der LinKom-Satz 1.10 liefert: $d = \mathrm{ggT}(a,m) \implies \exists x,y \in R : d = ax+by$. Diesen Satz dürfen wir anwenden, da R euklidisch ist. Wir wenden ihn mit $d = 1, q = y$ an und erhalten $1 = ax+qm$, wobei x durch Euklids Algorithmus geliefert wird. $\implies \overline{1} = \overline{ax}+\overline{qm} = \overline{ax}$. Resultat: $\overline{a}^{-1} = \overline{x}$ mit dem so berechnetem x. ∎

Folgerung 3.2
Ist $m \in \mathbb{N}_+$, dann gilt für Eulers Funktion φ:

$$\varphi(m) = \#\{R/mR\}^{\times}$$

Der Grund ist dass $R/mR = \{\overline{0},\dots,\overline{m-1}\}$ und $(R/mR)^{\times} = \{\overline{r} | 0 \leq r < m, \mathrm{ggT}(r,m) = 1\}$, derer es $\varphi(m)$ gibt.

Im Allgemeinen ist $\overline{R}$ nicht integer. Beispielsweise in $\mathbb{Z}/4\mathbb{Z} = \overline{R}$ gilt: $\overline{2}\cdot\overline{2} = \overline{4} = 0_{\overline{R}} = 0$, aber $\overline{2} \neq 0$

Folgerung 3.3
Falls m unzerlegbar (also m Primzahl oder -polynom). Dann gilt: R/mR ist ein Körper.

Speziell:

(1) $\mathbb{F}_p := \mathbb{Z}/p\mathbb{Z}$, $p \in \mathbb{P}$ ist Körper mit p Elementen.

(2) Ist $f \in K[X]$, f irreduzibel, so ist $K[X]/f\cdot K[X] = \overline{R}$ ein Körper.

Grund: m sei unzerlegbar. Dann $\overline{a} \in \overline{R}$, $\overline{a} \neq 0 = \overline{0} \iff m \nmid a \implies \mathrm{ggT}(m,a) = 1$ ($1, m$ sind die einzigen normierten Teiler von m!) $\implies a \in \overline{R}^{\times}$. Es gilt also $\overline{R}^{\times} = \overline{R} \setminus \{0\} \implies \overline{R}$ ist Körper.

$\overline{R} = R/mR \ni \overline{a} = a+Rm := \{a+qm \big| q \in R\}$ Restklasse von a.
Rechne in $\overline{R}$: **Idee**: Kodiere die Restklasse $\overline{a}$ durch den Vertreter $a \mod m$.

Beliebige Vertretersysteme (ohne Einschränkung $m \in \mathbb{N}_+, m > 1$)

<u>R = $\mathbb{Z}$</u>:
$\mathrm{Versys}_m = \{0,1,\dots,m-1\}$ „*System Betrag kleinster positiven Reste*“ oder $\mathrm{Versys}_m = \{v \in \mathbb{Z} \big| -\frac{m}{2} < r \leq \frac{m}{2}\}$ „*Symmetrisches Restsystem*“

$\underline{\mathrm{R} = K[X]}$:
$\mathrm{Versys}_m = \{f \in K[X] \big| \mathrm{Grad}\ f < \ \mathrm{Grad}\ m\}$ (Grad $m > 0$)

Klar:

$$\begin{array}{rcl} \mathrm{Versys}_m & \longrightarrow & R/mR \text{ (Ist bijektiv)} \\ r & \longmapsto & \overline{r} \\ a & \longmapsto & \overline{a} \mod m \text{ (Umkehrung)} \end{array}$$

Transportiere die Struktur $(\mathrm{Versys}_m, \oplus, \odot)$, wobei gilt:

$$r \oplus s := r + s \mod m \qquad r \odot s := rs \mod m$$

Klar, $r \mapsto \overline{r}$ ist ein Ringisomorphismus.

Vorzug bei $R = \mathbb{Z}$:

$r + s \mod m$ mit 1-Addition: Zahlen $< 2m$

$r \cdot s$: Zahlen $< m^2$

($m \mod \frac{m^2}{4}$ bei symmetrischen Resten)

Vorzug bei $R = K[X]$:

Ist $n =$ Grad f, so ist Versys_m ein K-Vektorraum der Dimension n (Basis z.B.: $1, X, X^2, ..., X^{n-1}$)

Grad $f < m$, Grad $g < m \implies$ Grad $(f + g) < m \implies f \oplus g = f + g \implies \oplus = +$

Versys_m enthält K als Teilkörper (konstante Polynome), da:
$\alpha, \beta \in K \subset K[X] \implies \alpha \odot \beta = \alpha\beta \mod m = \alpha\beta$

Folgerung 3.4
$\overline{R} = K[X]/mK[X]$ ist ein K-Vektorraum der dim $n =$ Grad m mit Basis $1, \overline{X}, \overline{X}^2, ..., \overline{X}^{n-1}$.
Identifiziert man $\alpha \in K$ mit der Restklasse $\overline{\alpha}$, so enthält $\overline{R}$ den Körper R.

Folgerung 3.5
Ist $m \in \mathbb{F}_p[X] = R$ irreduzibel, so ist $R/mR = \overline{R}$ ein Körper mit $q = p^n$ ($n =$ Grad m) Elementen!
Grund: $\mathbb{F}_p$-Basis ist $1, \overline{X}, \overline{X}^2, ..., \overline{X}^{n-1}$.
$\overline{R} = \{\alpha_0 \cdot 1 + \alpha_1 \overline{X} + ... + \alpha_{n-1}\overline{X}^{n-1} \big| \alpha_0, ..., \alpha_{n-1} \in \mathbb{F}_p\}$ mit $\#\overline{R} = p^n$

Zum Rechnen in $\overline{R}$ wird empfohlen $\overline{\alpha} \in \mathbb{F}_p$ durch $r = a \mod p$ zu ersetzen, mit $r \in \mathrm{Versys}_p$.
$f \in \mathrm{Versys}_p[X]$ hat die Form $f = \sum_{i=0}^n c_i X^i$, $c_i \in \mathrm{Versys}_p$.
Bei der Bestimmung von $f + g, f \cdot g$ ist bei allen Rechnungen mit Koeffizienten $c_1, ..., c_n$, $+$ durch $\oplus$ und $\cdot$ durch $\odot$ zu ersetzen. Man kann auch $f + g, f \cdot g$ in $\mathbb{Z}[X]$ berechnen und dann zu allen Koeffizienten die Reste $\mod p$ nehmen.

Beispiel
$\mathbb{F}_3[X]$, $\mathbb{F}_3 = \{\overline{0}, \overline{1}, \overline{2}\}$, $\mathrm{Versys}_3 = \{0, 1, 2\}$

$$\begin{array}{rcl} \underbrace{(X^2 + 2X + 1)}_{(= \overline{1} \cdot X^2 + \overline{2} \cdot X + \overline{1} \text{ in } \overline{R}[X])} \cdot (2X + 1) & = & 2X^3 + \underbrace{2 \odot 2}_{=1 \text{ in } \mathbb{Z}[X]} X^2 + 2X + X^2 + 2X + 1 \\ & = & 2X^3 + 4X^2 + 2X + X^2 + 2X + 1 \\ & = & 2X^3 + \underbrace{5}_{2 \mod 3} X^2 + \underbrace{4}_{1 \mod 3} X + 1 \\ & = & 2X^3 + (1 \oplus 1)X^2 + (2 \oplus 2)X + 1 \\ & = & 2X^3 + 2X^2 + X + 1 \end{array}$$

Beispiel
$\mathbb{F}_4 = \{\underbrace{0, 1}_{\mathbb{F}_2}, \underbrace{\overline{x}}_{=:\varrho}, \overline{x} + 1\}$, wenn m irreduzibel in $\mathbb{F}_2[X]$, Grad $f = 2$
$X^2 + 1 = (X + 1)^2$ $(= X^2 + \underbrace{\overline{2}}_{=0} X + 1 = X^2 + 1$ in $\mathbb{F}_2[X])$
$X^2 + X + 1$ ist irreduzibel. (Alle Polynome vom Grad 1 sind $X, X+1, X^2, X(X+1), (X+1)^2 = X^2 + 1$ sind von m verschieden $\implies$ irreduzibel)
$\mathbb{F}_4 = \{0, 1, \varrho, \varrho + 1\}$, $\varrho^2 = ?$
$(\overline{X})^2 = \underbrace{\overline{X^2 \mod m}}_{\in \text{Versys}_m} = \overline{X + 1} = \overline{X} + 1 = \varrho + 1$
$X^2 - 1 \cdot (X^2 + X + 1) = -X - 1 = X + 1$ in $\mathbb{F}_2[X]$
Rechenregel: $\varrho^2 = \varrho + 1 \implies$ Multiplikationstafel

Bemerkung:

- $R \to \overline{R} = R/mR$, $\kappa : a \mapsto \overline{a} = \kappa(a)$, so ist κ surjektiver Ringhomomorphismus. $\kappa(a + b) = \overline{a} + \overline{b} = \overline{a + b} = \kappa(a + b)$
- Ist R ein Ring und $z \in \mathbb{Z}$, so definiert man:

$$z \cdot \varrho := sgn(z) \underbrace{(\varrho + \varrho + ... + \varrho)}_{|z|-\text{Stück}}$$

Beispiel
$\overline{R} = \mathbb{Z}/m\mathbb{Z}, z \in \mathbb{Z}$
$z\overline{a} = \overline{za}$ (leicht selbst nachzuweisen) $m \cdot 1_{\overline{R}} = m \cdot \overline{1} = \overline{m} = 0_{\overline{R}}$

Rechenregeln: $z, z_1, z_2 \in \mathbb{Z}, \varrho, \varrho_1, \varrho_2 \in R$

$$(z_1 + z_2)\varrho = z_1\varrho + z_2\varrho$$

$$z(\varrho_1 + \varrho_2) = z\varrho_1 + z\varrho_2$$

$$(z_1 z_2)\varrho = z_1(z_2\varrho)$$

$$z(\varrho_1\varrho_2) = (z\varrho_1)\varrho_2 = \varrho_1(z\varrho_2) \text{ (Beweis leicht)}$$

Für $f \in \mathbb{Z}[X], \overline{a} \in \mathbb{Z}/\mathbb{Z}m$ ist definiert ($f = \sum_{i=0}^{n} z_i X^i$):

$$f(\overline{a}) = \sum_{i=0}^{n} z_i \overline{a}^i \in \overline{R} \; (= \sum_{i=0}^{n} \overline{z_i a^i} = \overline{f(a)}$$

Ergebnis: $f(\overline{a}) = \overline{f(a)}$

3.1 Zyklische Gruppen

Aufgabe: Berechne $3^{10^{500}} \mod \underbrace{167}_{=:p}$ (Rechne in Versys_{167} !)

Mathematische Hilfsmittel: Ordnung eines Gruppenelements.

Definition
Sei G eine (ohne Einschränkung multiplikative) endliche Gruppe, $x \in G$. (Das neutrale Element werde mit $1 = 1_G$ bezeichnet)

(i) $\operatorname{ord}(x) = \min\{n \in \mathbb{N}_+ \big| x^n = 1\}$ heißt „*Ordnung von x*"

(ii) $\#G$ heißt „*Ordnung von G*"

Bemerkung: $\operatorname{ord}(x)$ existiert, da $n > m, n, m \in \mathbb{N}_+$ vorhanden sind mit $x^n = x^m$, da G endlich. $\implies$ $x^{n-m} = 1$. In allgemeinen Gruppen kann sein $\{n \in \mathbb{N}_+ \big| x^n = 1\} = \emptyset$, dann schreibt man $\operatorname{ord}(x) = \infty$

Satz 3.6 (Elementordnungssatz)
Sei G eine endliche Gruppe, $x \in G$, $m, n \in \mathbb{Z}$. Dann gelten:

(i) $x^m = x^n \iff m \equiv n \mod \operatorname{ord}(x)$
Insbesondere $x^m = x^{m \mod \operatorname{ord}(x)}$ und $\mod x^m = 1 \iff \operatorname{ord}(x) \big| m$

(ii) $x^{\#G} = 1$ (d.h. nach (i) $\operatorname{ord}(x) \big| \#G$)

(iii) $\operatorname{ord}(x^m) = \frac{\operatorname{ord}(x)}{\operatorname{ggT}(m, \operatorname{ord}(x))}$

Anwendung:

Satz von Euler: Sei $m, x \in \mathbb{Z}, m > 0, \operatorname{ggT}(x, m) = 1, \varphi$ sei die Eulersche Funktion. Dann gilt: $x^{\varphi(m)} \equiv 1 \mod m$

(Kleine) Satz von Fermat: Sei $p \in \mathbb{P}, x \in \mathbb{Z}$. Dann gilt: $x^p \equiv x \mod p$

Zum Satz von Euler:
$G = (R/Rm)^\times, \#G = \varphi(m)$. $\overline{x} \in G \iff \operatorname{ggT}(x, m) = 1$. Elementordnungssatz (ii) $\implies \overline{1} = 1_g = \overline{x}^{\#G} = \overline{x}^{\varphi(m)} = x^{\varphi(m)} \iff 1 \equiv x^{\varphi(m)} \mod m$

Zum Satz von Fermat:
$\varphi(p) = p - 1$. Aussage klar, wenn $p \big| x (x \equiv 0 \equiv xp)$. $p \nmid x \implies \operatorname{ggT}(p, x) = 1 \implies \overline{x}^{p-1} = \overline{x}^{\#G} = \overline{1} \implies \overline{x}^p = \overline{x} \implies x^p \equiv x \mod p$

Beweis (Elementordnungssatz)
Sei $x \in G$, $\operatorname{ord}(X) =: l$.

(1) $x^m = x^n \iff x^{m-n} = 1 = 1_G \iff 1 = x^{ql+r} = (w^l)^q \cdot x^r = 1^q \cdot x^r = 1x^r = x^r$ (Falls $r \neq 0$, so haben wir einen Widerspruch zur Minimalwahl von l) $\iff r = 0 \iff l \mid m - n \iff m \equiv n \mod l$.

Insbesondere: $x^m = 1 \iff l \mid m$, $x^n = x^{n \mod l}$

(2) $x^{\#G} = 1$. Dies wird in dieser Vorlesung nur für kommutative G benötigt und bewiesen. Betrachte die Abbildung $G \to G$, $x \mapsto y \cdot x$. Sie ist bijektiv (die Umkehrabbildung ist $y \mapsto yx^{-1}$), also $\{y \mid y \in G\} = G = \{yx \mid y \in G\}$.

$$\prod_{y \in G} y = \prod_{y, x \in G} (yx) = \prod_{y \in G} y \cdot x^{\#G} \implies x^{\#G} = 1$$

■

Also laut (1): $\operatorname{ord}(x) \mid \#G$

(3) $\operatorname{ord}(x^m) = k \implies 1 = (x^m)^k = x^{mk} \overset{(1)}{\implies} l \mid mk$. Sei $d = \operatorname{ggT}(m, l) \implies \frac{l}{d} \mid \frac{md}{\cdot}k \implies \frac{l}{d} \mid k$. Warum sind $\frac{l}{d}$ und $\frac{m}{d}$ relativ prim? $d = \operatorname{ggT}(m, l) = d \cdot \operatorname{ggT}(\frac{m}{d}, \frac{l}{d}) \implies \operatorname{ggT}(\frac{m}{d}, \frac{l}{d}) = 1$. Aber $k \mid \frac{l}{d}$ wegen $(x^m)^{\frac{l}{d}} = x^{l \cdot \frac{m}{d}} = 1^{\frac{m}{d}} = 1$, $k = \operatorname{ord}(x^m)$ nach (1).

Ergebnis: $k = \frac{l}{d} = \frac{\operatorname{ord}(x)}{\operatorname{ggT}(\operatorname{ord}(x), m)}$

Hilfestellungen zur Berechnung von $\operatorname{ord}(x)$

Bemerkungen:
(i) $\operatorname{ord}(a) \mid \#G$ (*wirklich a?*)

(ii) Sei $x^d = 1$. Dann gilt: $d = \operatorname{ord}(x) \iff \forall p \in \mathbb{P}$ mit $p \mid d$: $x^{\frac{d}{p}} \neq 1$.

Beweis (Der Bemerkung (ii))
„$\Longrightarrow$“: Klar

„$\Longleftarrow$“: Sei $x^d = 1$, $x \neq \operatorname{ord}(x)$. Nach (1): $\operatorname{ord}(x) \mid d \implies \exists p \in \mathbb{P} : \operatorname{ord}(x) \mid \frac{d}{p} \implies x^{\frac{d}{p}} = 1$ ∎

Zur Berechnung von x^n: Naive rekursive Berechnung: $x^{j+1} = x^j \cdot x$. Hier hätten wir n Produkte zu berechnen! Westentlich bessere Methode: Stelle n binär da: $n = \sum_{i=0}^{t} c_i \cdot 2^i$, $c_t \neq 0$, $c_i \in \{0, 1\}$. Bezeichnung $n = (c_t, c_{t-1}, \dots, c_0)_2$ mit den Binärziffern c_j.

$$x^n = x^{\sum_{i=0}^{t} c_i \cdot 2^i} = \prod_{i=0}^{t} \left(x^{2^i}\right)^{c_i} = \prod_{i=0,\ c_i \neq 0}^{t} x^{(2^i)}$$

Rekursiv: $x^{2^0} = x^1 = x$ und $x^{2^{i+1}} = (x^{2^i})^2$. t ist etwa $\log_2 n$, man hat ungefähr $2 \cdot \log_2 n$ Produkte zu berechnen.

Beispiel
$G = \mathbb{F}_9^\times$, $\#G = 9 - 1 = 8$. Mögliche $\operatorname{ord}(\alpha)$ für ein $\alpha \in G$: 1,2,4, oder 8.

$$\begin{aligned}
\operatorname{ord}(\alpha) = 1 &\iff \alpha = 1 \\
\operatorname{ord}(\alpha) = 2 &\iff \alpha \neq 1, \alpha^2 = 1 \iff \alpha = -1_G = -1 \\
\operatorname{ord}(\alpha) = 4 &\iff \alpha^4 = 1, \alpha^2 \neq 1 \text{ (d.h. } \alpha \neq \pm 1) \\
\operatorname{ord}(\alpha) = 8 &\iff \alpha^4 \neq 1
\end{aligned}$$

$\mathbb{F}_9 = \mathbb{F}_3[X]/m \cdot \mathbb{F}_3[X]$, $\operatorname{ord}(m) = 2$, m irreduzibel. Beispielsweise ist $X^2 + 1$ in $R = \mathbb{F}_3[X]$ irreduzibel.

$\mathbb{F}_9$ hat $\mathbb{F}_3$-Basis $1; \overline{x}$. $\mathbb{F}_9 = \{\underbrace{0, 1, -1,}_{\mathbb{F}_3 = \text{Versys}_3} \dots\} = \{a + b\overline{x} \mid a, b \in \mathbb{F}_3\}$

$m = X^2 + 1 \equiv 0 \mod m \implies X^2 \equiv -1 \mod m \implies \overline{X}^2 = -1 = -1_{\mathbb{F}_9} = -1_{\mathbb{F}_3} \implies \overline{X}^4 = (-1)^2 = 1 \implies \operatorname{ord}(\overline{X}) = 4$.

$(\overline{X} + 1)^2 = \overline{X}^2 + 2\overline{X} + 1 = -1 + 1 + 2X = -X \neq 1$, $(\overline{X} + 1)^4 = (-\overline{X})^2 = \overline{X}^2 = -1 \implies \operatorname{ord}(\overline{X} + 1) = 8$

Zurück zum Problem $3^{(10^{500})} \mod 167$, $167 \in \mathbb{P}$. $G = \mathbb{F}_{167}$, $\#G = \varphi(167) = 166 = 2 \cdot 83$, also gilt $\operatorname{ord}(n) \in \{1, 2, 83, 166\}$.

Laut Ordnungsatz: $3^{10^{500}} \equiv 3^{10^{500} \mod \operatorname{ord}(\overline{3})}$.

Wir brauchen ord(3): $\overline{3}^2 = \overline{9} \neq 1_G \implies \operatorname{ord}(\overline{3}) \neq 1, 2$, $\operatorname{ord}(\overline{3}) = 83 \iff \overline{3}^{83} = 1_G = \overline{1}$. $83 = (1010011)_2 = 64 + 16 + 2 + 1$. Tabelle: 3^{2^0} in $\mathbb{F}_{167}$ ist 3, 3^{2^1} in $\mathbb{F}_{167}$ ist $3^2 = 9$, 3^{2^2} in $\mathbb{F}_{167}$ ist $9^2 = 81$, 3^{2^3} in $\mathbb{F}_{167}$ ist $81^2 = 6651 = 30 \cdot 167 + 48 \equiv 48$, 3^{2^4} in $\mathbb{F}_{167}$ ist $48^2 \equiv 133$, 3^{2^5} in $\mathbb{F}_{167}$ ist $133^2 = 17629 \equiv 154$, 3^{2^6} in $\mathbb{F}_{167}$ ist $154^2 =\equiv 2$. Also: $\overline{3}^{83} = \overline{3} \cdot \overline{9} \cdot \overline{133} \cdot \overline{2} \cdot \overline{7182} \cdot \overline{1} = 1_G$. Ergebnis: $\operatorname{ord}(\overline{3}) = 83$.

$3^{10^{500}} = 3^{10^{500} \mod 83}$. Noch zu berechnen: $10^{500} \mod 83$. Man kann $\overline{10}$ in $\mathbb{F}_{83}$ berechnen. Reicht auch $\overline{10}^{500} = 10^{500 \mod \varphi(83)}$. $\varphi(83) = 82$, $500 \equiv 8 \mod 82 \implies 10^{500} \equiv 10^8 \equiv 23 \mod 83$

Also: $\overline{3}^{10^{500}} = \overline{3}^{23} = \overline{124} = \overline{-33}$ und somit $3^{100^{500}} = 124 \mod 167$

Satz 3.7 (Mersenne-Teiler-Satz)
Es seien $p, q \in \mathbb{P}$ mit $q \mid M_p = 2^p - 1$. Dann gilt: $q \equiv 1 \mod p$

Beweis
$q \mid M_p \iff M_p = 2^p - 1 \equiv 0 \mod q \iff \overline{2}^p = 1$ in $\mathbb{F}_q^\times = G \implies \operatorname{ord}(\overline{2}) = p$, da 1 nicht geht und $\operatorname{ord}(\overline{2}) \mid p$ nach dem Ordnungsatz. $\operatorname{ord}(\overline{2}) \mid \#G = \varphi(q) = q - 1 \implies q - 1 \equiv 0 \mod p \implies q \equiv 1 \mod p$ ∎

Bezeichnungen:

(1) $\langle x \rangle = \{1, x, x^2, \dots, x^{l-1}\}$, ($l = \operatorname{ord}(x)$), heißt die von x erzeugte zyklische Untergruppe von G.

(2) G heißt zyklisch $\iff \exists x \in G : G = \langle x \rangle \iff \exists x \in G : \operatorname{ord}(x) = \#G$

Bemerkung: Die Abbildung $(\mathbb{Z}/\mathbb{Z}l, +) \to (\langle x \rangle, \cdot)$ mit $\overline{m} \mapsto x^m$ ist ein Isomorphismus von Gruppen.

3.2 Primitivwurzeln

Vorbereitungen über $R = K[X]$, K ein Körper.

Bemerkung: Sei $\alpha \in K$, $f \in R$, $\operatorname{ord}(f) > 0$. Dann gilt:

$$0 = f(\alpha) \iff X - \alpha \mid f \iff v_{X-\alpha}(f) > 0 \quad (X - \alpha \in \mathbb{P}_R)$$

$v_{X-\alpha}$ heißt Vielfachheit der Nullstelle α von f.

Beweis
Division mit Rest: $f = q \cdot (X - \alpha) + r$. $\operatorname{grad} r < \operatorname{grad}(X - \alpha) = 1 \implies r \in K$ (konstantes Polynom), insbesondere $r(\alpha) = r$. $f(\alpha) = q(\alpha)(\alpha - \alpha) + r(\alpha) = r$. Also: $r(\alpha) = 0 \iff r = 0 \iff X - \alpha \mid f$ ∎

Satz 3.8 (Nullstellenanzahls-Satz)
$f \in K[X]$, $f \neq 0$, $n = \operatorname{grad} f$, so gilt: f hat höchstens n verschiedene Nullstellen in K.

Beweis
$\alpha_1, \ldots, \alpha_l$ seien l Nullstellen. $v_{X-\alpha_j}(f) > 0 \implies \prod_{j=1}^{l}(X-\alpha_j) \mid f$, wegen $v_{X-\alpha_i}(\prod_{j=1}^{l}(X-\alpha_j)) = 1$ und $v_m(\prod_{j=1}^{l}(X-\alpha_j)) = 0$ für alle anderen $m \in \mathbb{P}$ sowie $v_{X-\alpha_j}(f) \geq 1$. Daraus folgt: $l \leq \operatorname{grad} f$ ■

Der Spezialfall $K = \mathbb{F}_p$ ergibt den

Satz 3.9 (Satz von Lagrange)
Sei $p \in \mathbb{P}$, $f = \sum_{i=0}^{n} c_i X^n \in \mathbb{Z}[X]$. Es gibt ein $j \in \{0, \ldots, n\}$ mit $c_j \not\equiv 0 \mod p$. Dann fallen die „Lösungen“ $x \in \mathbb{Z}$ der Kongruenz

$$f(x) \equiv 0 \mod p$$

in höchstens n verschiedene Restklassen modulo p.

Beweis
Der Satz ist eine Übersetzung des Nullstellenanzahls-Satzes auf Kongruenzen. Betrachte die $\overline{c_j} = \alpha_j \in \mathbb{F}_p \implies \exists j : \overline{c_j} \neq 0 \implies f = \sum_{i=0}^{n} \overline{c_j} X^j \neq 0$ in $\mathbb{F}_p[X]$, $\operatorname{ord}(f) \leq n$. $f(x) = 0 \mod p \iff \overline{f(x)} = f(\overline{x}) = 0_{\mathbb{F}_p}$. Es gibt höchstens n Nullstellen $\overline{x}$, das heißt lösende Kongruenzklassen. ■

$p \in \mathbb{P}$ wird gebraucht, Aussage modulo m, $m \notin \mathbb{P}$, im Allgemeinen falsch. Beispiele: $m = 6$, $f = X^2 + X$ hat in $\mathbb{Z}/6\mathbb{Z}$ die Nullstellen $\overline{0}$, $\overline{2}$, $\overline{3}$, $\overline{5}$. $m = 9$, $f = X^2$ hat in $\mathbb{Z}/9\mathbb{Z}$ die Nullstellen $\overline{0}$, $\overline{3}$, $\overline{-3}$.

Satz 3.10 (Primitivwurzelsatz)
Sei K Körper, G eine *endliche* Untergruppe von $K^\times$. Dann ist G zyklisch. Genauer gilt: $\#\{\alpha \in K \,|\, \operatorname{ord}(\alpha) = \#G\} = \varphi(\#G)$ (φ die Eulersche Funktion)

Bemerkung: Ist $\operatorname{ord}(\alpha) = \#G$, so heißt α primitive $\#G$-te Einheitswurzel, da $\alpha^{\#G} = 1$, sozusagen $\alpha = \sqrt[\#G]{1}$. primitiv, da $\alpha^m = 1$, wobei $\#G \mid m$.

Spezialfälle

(1) $K = \mathbb{F}_q$, also ein Körper mit $q < \infty$ Elementen. $G = \mathbb{F}_q^\times = \mathbb{F}_q \setminus \{0\}$, $\#G = q - 1$. Nach dem Satz ist $F_q^\times$ zyklisch α mit $\langle\alpha\rangle = \mathbb{F}_q^\times$ heißt primitives Element.

(2) Noch spezieller: $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ mit $p \in \mathbb{P}$ besitzt $\varphi(p-1)$ primitive Elemente $\alpha = \overline{w}$, $(0 \leq w < p-1)$. Solve w heißen Primitivwurzel modulo p.

Beweis
Sei $l = \#G$, G wie im Satz.

Für die $d \mid l$, $d \in \mathbb{N}_+$, sei $\lambda(d) = \#\{\alpha \in G \mid \operatorname{ord}(\alpha) = d\}$. Laut Elementordnungssatz gilt: $l = \sum_{d|l} \lambda(d) = \sum_{d|l} \varphi(d)$ (Lemma von Gauß). Man will zeigen: $\lambda(d) \leq \varphi(d)$ $(*)$, denn dann muss gelten: $\forall d \mid l : \lambda(d) = \varphi(d)$, denn sonst würde gelten: $\sum_{d|l} \lambda(d) < \sum_{d|l} \varphi(d)$.

$(*)$ ist klar, wenn $\lambda(d) = 0$. Sei also $\lambda(d) \neq 0 \implies \exists \alpha \in G : \operatorname{ord}(\alpha) = d$. Sei $A = \langle \alpha \rangle = \{1, \alpha, \alpha^2, \dots, \alpha d - 1\}$. Klar: $(\alpha^d)^d = 1 \implies \alpha^j$ ist eine Nullstelle von $X^d - 1$. Wegen $\#A = d$ sind das d Nullstellen von $X^d - 1$, also alle solche. $B = \{\beta \in G \mid \operatorname{ord}(\beta) = d\}$, dann $\beta^d = 1 \implies \beta$ Nullstelle von $X^d - 1 \implies \beta \in A$. $B \subseteq A$.

$\alpha^j \in B \iff \operatorname{ord}(\alpha^j) = d \implies d = \operatorname{ord}(\alpha^j) = \frac{\operatorname{ord}(\alpha)}{\operatorname{ggT}(d,j)}$ (Elementordnungssatz) $\implies \operatorname{ggT}(d,j) = 1 \implies B \subseteq \{\alpha^j \mid \operatorname{ggT}(d,j) = 1, 0 \leq j \leq d\}$. $\#B = \lambda(d) \leq \#\{\alpha^j \mid \operatorname{ggT}(d,j) = 1, 0 \leq j \leq d\} = \varphi(d)$

Der folgende Satz ist eine Anwendung des Primitivwurzelsatzes:

Satz 3.11 (Eulers Quadratkriterium)
Sei $\alpha \in \mathbb{F}_q^\times$ ($\mathbb{F}_q$ ein Körper mit q Elementen, $2 \mid q$). Dann gilt:

$$\alpha \text{ ist ein Quadrat in } \mathbb{F}_q^\times \iff \alpha^{\frac{q-1}{2}} = 1$$

Anderenfalls gilt: $\alpha^{\frac{q-1}{2}} = -1$

Euler formuliert den Satz so: Sei $p \in \mathbb{P}$, $p > 2$, $n \in \mathbb{Z}$, $p \mid m$. Dann existiert ein $x \in \mathbb{Z}$ mit $x^2 \equiv m \mod p \iff m^{\frac{p-1}{2}} \equiv 1 \mod p$. Solche $m \mod p$ heißen quadratische Reste.

Wenn Kongruenz als Gleichung in $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ gelesen wird, so gilt:

$$\alpha = \overline{x} \text{ Quadrat in } \mathbb{F}_p^\times \iff x \text{ quadratischer Rest modulo } p$$

Beweis
Sei ζ eine Primitivwurzel (Existenz folgt aus dem Primitivwurzelsatz).

„$\Longleftarrow$“: Sei $\alpha^{\frac{q-1}{2}} = 1$ und $\alpha = \zeta^j$. $\zeta^{j \cdot \frac{q-1}{2}} = 1 \implies q - 1 = \operatorname{ord}(\zeta) \mid j^{\frac{q-1}{2}} \implies \frac{j}{2} \in \mathbb{Z} \implies 2 \mid j \implies \beta = \zeta^{\frac{j}{2}}$ zeigt den Satz: $\beta^2 = \zeta^j = \alpha$

„$\Longrightarrow$“: α Quadrat $\iff \exists \beta \in \mathbb{F}_q : \alpha = \beta^2 \implies \exists k \in \mathbb{Z} : \beta = \zeta^k$. $\alpha = \zeta^{2k} \implies \alpha^{\frac{q-1}{2}} = \zeta^{(q-1)k} = 1$, da $\operatorname{ord}(\zeta) = q - 1$

$\alpha^{\frac{q-1}{2}}$ ist Nullstelle von $X^2 - 1$. Alle Nullstellen sind $\{1, -1\}$. 1 entfällt, also ist $\alpha^{\frac{q-1}{2}} = -1$ ■

Eulers Formulierung „m nicht quadratischer Rest“, auch „quadratischer Nichtrest“. $\operatorname{ggT}(m,p) = 1 \implies m^{\frac{p-1}{2}} \equiv -1 \mod p$

3.3 Zifferndarstellung nach Cantor

In diesem Abschnitt seien $R = \mathbb{Z}$ oder $R = K[X]$, K ein Körper.

Ausgangspunkt ist die Folge $\gamma = (m_0, m_1, m_2, \ldots)$, $m_j \in R$ mit $m > 1$ bei $R = \mathbb{Z}$ oder $\text{grad}(m_j) > 0$ bei $R = K[X]$.

Definiere $M_0 = 1$, $M_k = m_0 \cdot \ldots \cdot m_{k-1}$.

Satz 3.12 (Ziffernsatz)
Jedes $n \in \mathbb{N}_+$ bzw. $n \in K[X]$, $n \neq 0$ hat eine eindeutige Darstellung

$$n = z_r M_r + z_{r-1} M_{r-1} + \cdots + z_1 M_1 + z_0 \quad (*)$$

wobei $r \in \mathbb{N}$ und $0 \leq z_j < m_j$ bzw. $\text{grad}(z_j) < \text{grad}(m_j)$

Bezeichnungen: Die z_j heißen γ-adische Ziffern und $(*)$ Zifferndarstellung (vorlesungs-spezifisch). Kurzbezeichnung: $n = (z_r, z_{r-1}, \ldots, z_0)_\gamma$. Die Kommata dürfen bei Eindeutigkeit weggelassen werden.

Spezialfall: $m_0 = m_1 = m_2 = \cdots =: m$ gibt Zifferndarstellung $n = z_r m^r + z_{r-1} m^{r-1} + \cdots + z_0 = (z_r, \ldots, z_0)_m$ heißt m-adische Darstellung von n.

Spezialbenennungen:

m	Zifferndarstellung	Ziffern	
10	Dezimaldarstellung	0,1,...,9	bei Menschen beliebt (10 Finger)
2	Binär oder dyadisch	0,1	bei Comptern beliebt (0,1 gut realisierbar)
8	Oktaldarstellung	0,...,7	
16	Hexadezimal	0,...,9,A,B,C,D,E,F	Speicherverwaltung im Rechner

Beispiel

$$\begin{aligned}(A8C)_{16} &= 10 \cdot 16^2 + 8 \cdot 16 + 12 \cdot 1 \\ &= 2700 := (2700)_{10} \\ &= (10101001100)_2 \\ &= (5214)_8\end{aligned}$$

$\gamma = (m_0, m_1, ...), m_j \in \mathbb{Z}$ (bzw. $K[X]$), $m_j > 1$ bzw. Grad $m_j > 0$
$M_0 = 1, M_k = m_0 \cdot ... \cdot m_{k-1}$

γ-adische Entwicklung von $n \in \mathbb{N}_+$ bzw. $n \in K[X], n \neq 0:$

$$n = z_r M_r + z_{r-1} M_{r-1} + ... + z_1 M_1 + z_0 \cdot 1 \tag{3.1}$$

γ-adische Darstellung, wenn $0 \leq z_j < m_j$ (bzw. Grad $z_j <$ Grad m_j)

Beweis (Ziffernsatz)
Fall (3.1) vorliegt: Wegen $M_k | M_{k+1} | M_{k+2} | ... :$
$n \equiv z_{k-1}M_{k-1} + z_{k-2}M_{k-2} + ... + z_0 \mod M_k$

Speziell: $n \equiv z_0 \mod M_1 = m_0 \implies n - z_0 = n'm_0, n' \in \mathbb{Z}$ bzw. $K[X]$

Beweisidee: Induktion nach n bzw. Grad n (hier nur $\mathbb{Z}, K[X]$ fast genau so)

Behauptung: Sei $n \in \mathbb{Z}_+$. Dann existiert für alle γ's dieser Art die γ-dische Darstellung (3.1).
Induktion nach n:
Falls $n < m_0$, dann $z_0 = n, n = z_0 M_0$ ist $(\star)$
Falls $n \geq m_0, z_0 = (n \mod m_0), n'$ aus $n - z_0 = n'm_0 (n' = \frac{n-z_0}{m_0})$. Klar $0 \leq z_0 < m_0 \leq n \implies 0 < n' < n$.
Induktionshypothese anwendbar auf n' mit $\gamma' = (m'_1, m'_2, ...), m'_j = m_{j+1} (j \geq 0)$.

$\exists \gamma'$-adische Darstellung von n':
$n' = z'_{r'}M'_{r'} + z_{r'-1}M'_{r'-1} + ... + z'_1 M'_1 + z'_0 (r' \in \mathbb{N}, z'_{r'} \neq 0)$
$n \leq z'_j < m'_j = m_{j+1} \implies n = n'm_0 + z_0 = z'_{r'}M_{r'+1} + ... + z'_1 M_1 + z_0$
Das ist die gesuchte γ'-adische Darstellung von n mit $r := r' + 1, z'_j = z_j + 1 (j = 0, ..., r')$ also $0 \leq z_{j+1} = z_j < m'_j = m_{j+1}$
Dies ist ein Algorithmus, wenn die Abbildung $j \mapsto m_j$ berechenbar ist.

Eindeutigkeit: Ebenfalls Induktion. z_0 muss $n \mod m_0$ sein. Induktionshypothese n' eindeutig dargestellt $\implies$ Darstellung von n eindeutig (Details: selbst!) ∎

Bemerkung: Zur Berechnung von $(n_1 + / \cdot n_2)_\gamma$ aus $(n_1)_\gamma$ und $(n_2)_\gamma$ ähnliche Algorithmen wie für $()_{10}$.

3.4 Simultane Kongruenzen

3.4.1 Prinzip des Parallelen Rechnens

$R_j (j = 1, ..., l)$ seien algebraische Strukturen gleicher Art mit gleichbezeichneten Verknüpfungen $*$, zum Beispiel:

Gruppen $* \in \{\cdot\}$

Abelsche Gruppen $* \in \{+\}$

Ringe $* \in \{+, \cdot\}$

Vektorräume $* \in \{+, \text{Skalarmultiplikation}\}$

Dann ist auch $S = \prod_{i=1}^{l} R_j = R_1 \times ... \times R_l$ eine algebraische Struktur mit Verknüpfungen (komponentenweise):
$S \ni (a_1, ..., a_l), (b_1, ..., b_l), a_j, b_j \in R_j$
$(a_1, ..., a_l) * (b_1, ..., b_l) := (a_1 * b_1, ..., a_l * b_l)$
$\alpha(a_1, ..., a_l) := (\alpha a_1, ..., \alpha a_l)$ bei K-Vektorräumen.
Sind $_j$ Ringe/Gruppen/Abelsche Gruppen/Vektorräume, so auch S.

Grund: Alles vererbt sich von den Komponenten!
Zum Beispiel Ringe: $0_S = (0_{R_1}, ..., 0_{R_l}), 1_S = (1_{R_1}, ..., 1_{R_l})$, kurz: $0 = (0, ..., 0), 1 = (1, ..., 1)$, $-(a_1, ..., a_l) = (-a_1, ..., -a_l)$
Zum Beispiel Assoziativität:
$((a_1, ..., a_l) * (b_1, ..., b_l)) * (c_1, ..., c_l) = ((a_1 * b_1) * c_1, ..., (a_l * b_l) * c_l) = (a_1, ..., a_l) * ((b_1, ..., b_l) * (c_1, ..., c_l))$

Warnung! Sind die R_j Körper, so ist für $l > 1$, S kein Körper.
Zum Beispiel: $\underbrace{(1, 0)}_{\neq 0} \cdot \underbrace{(0, 1)}_{\neq 0} = (1 \cdot 0, 0 \cdot 1) = (0, 0) = 0$

Lemma 3.13
Sind dir R_j Ringe, so $S^\times = \prod_{j=1}^{l} R_j^\times$

Grund: Muss sein $(a_1, ..., a_l)^{-1} = (a_1^{-1}, ..., a_l^{-1})$

Falls ein Isomorphismus $\psi : R \to S = \prod_{j=1}^{l} R_j$ vorliegt, so wird das Rechnen in R zurückgeführt auf das gleichzeitig („*parallele*“) Rechnen in dem R_j wie folgt:
$\psi(a) = (a_1, ..., a_l), \psi(b) = (b_1, ..., b_l)$
$a * b = \psi^{-1}(\psi(a * b)) = \psi^{-1}(\psi(a) * \psi(b)) = \psi^{-1}((a_1 * b_1, ..., a_l * b_l))$

Praxis: Berechne die $a_j * b_j$ gleichzeitig auf verschiedenen Prozessoren. Wende ψ, ψ^{-1} wie oben an. Nützt nur, wenn ψ, ψ^{-1} gut und schnell berechenbar sind.

3.4.2 Der Chinesische Restsatz

Frage: Morgen ist Freitag, der 2. Juni. Nach wievielen ($x = ?$) Tagen fällt frühestens der Dienstag auf einen 17. des Monats?

Vorraussetzung: Chinesische Kalender vor ca. 2000 Jahren: Alle Monate haben 20 Tage.

Wochentag	Fr	Sa	So	Mo	Di	Mi	Do	Fr	Sa	So
Wochentagsnr.	0	1	2	3	4	5	6	0	1	2
Monatstagnr.	2	3	4	5	6	7	8	9	10	11

(Wochentagsnummer modulo 7, Monatstagnummer modulo 30)

Gesucht ist also die kleinste positive Lösung x der Kongruenzen:

$$\begin{aligned} x &\equiv 4 && \bmod 7 \\ x &\equiv 17 - 2 && \bmod 30 \end{aligned}$$

R sei euklidischer Ring, $a_1, \dots, a_l, m_1, \dots, m_l \in R$

$$x \equiv a_j \mod m_j, \ (j = 1, \dots, l) \tag{3.2}$$

heißt *System simultaner Kongruenzen* (mit gesuchter Lösung $x \in R$).

Bemerkung: Im Allgemeinen gibt es *keine* Lösung.
$x \equiv a \mod m \implies x \equiv a \mod m$, falls $d \mid m$
System: $x \equiv 1 \mod 4, x \equiv 0 \mod 6 \implies x \equiv 1 \mod 2, x \equiv 0 \mod 2 \implies 1 \equiv 0 \mod 2 \implies$ Widerspruch!

Satz 3.14 (Chinesischer Restsatz, rechnerische Form)
Sei R ein euklidischer Ring, $m_1, ..., m_l \in R$, $a_1, ..., a_l \in R$ derartig, dass $\forall i, j \in \mathbb{Z}$ mit $1 \leq i < j \leq l$ gilt:

$$\mathrm{ggT}(m_i, m_j) = 1 \text{ („paarweise relativ prime } m_j\text{“)}$$

Dann hat das System simultaner Kongruenzen (3.2) eine Lösung. Sämtliche Lösungen bilden eine Restklasse modulo m mit $m = m_1 \cdot \ldots \cdot m_l$

Beweis
$l = 1$: $x = a_1$ oder $x = (a_1 \mod m_1) \iff (x \equiv a_1) \mod m_1$ und $0 \leq x \leq m_1$

$l = 2$: $x \equiv a_1 \mod m_1$. x muss in der Form $x = a_1 + um_1, u \in R$ angesetzt werden.
Idee: Bestimme u so, dass $x \equiv a_2 \mod m_2$. Also in $\overline{R} = R/m_2R$ soll werden:
$\overline{a}_1 + \overline{um}_1 = \overline{a_1 + um_1} = \overline{a}_2$, daher tut es: $\overline{u} = (\overline{a}_2 - \overline{a}_1)\overline{m}_1^{-1}$
Geht, da $\overline{m}_1^{-1}$ existiert und da $\overline{m}_1 \in (R/m_2R)^\times$. Nach dem Restklassensatz: $\overline{m}_1 \in (R/m_2R)^\times \iff \mathrm{ggT}(m_1, m_2) = 1$
Algorithmisch $\overline{u} = \overline{m}_1^{-1}$, u kann mit LinKom-Satz, also euklidischem Algorithmus, bestimmt werden. *Erinnerung*: $\mathrm{ggT}(m_1, m_2) = um_1 + vm_2,\ u, v$ berechnet der Algorithmus.
$1 = \overline{um}_1, \overline{m}_2 = 0, \overline{u} = \overline{m}_1^{-1}$
Für dieses $u \in R$ ist $x = a_1 + um_1$ (eventuell $\mod m, m_2$) die gesuchte Lösung.

$l > 2$: Induktionshypothese löst $x' \equiv a_j \mod m_j (j = 1, ..., l-1)$.
Löse dann $x \equiv x' \mod m_1 \cdot ... \cdot m_{l-1}$ ($\implies x \equiv x' \equiv a_j \mod m_j, j = 1, ..., l-1) \implies$
$x \equiv a_l \mod m_l \implies x$ ist die gesuchte Lösung. ∎

Beispiel
Gegeben sind die Kongruenzen:

$$\begin{aligned} x &\equiv 4 && \mod 7 \\ x &\equiv 19 && \mod 30 \end{aligned}$$

Ansatz: $x = 4 + u \cdot 7 \equiv 19 \mod 30$. Im $\mathbb{Z}/30\mathbb{Z}$: $\overline{4} + \overline{u} \cdot \overline{7} = \overline{19} \implies \overline{u} = (\overline{19} - \overline{4})^{-1} \cdot \overline{7}^{-1}$. Es ist $\overline{7}^{-1} = \overline{13}$, also $u \equiv 13 \cdot 15$, etwa $x = 4 + 13 \cdot 15 \cdot 7 \equiv 109 \mod 210$.

Wir fügen eine Bedingung hinzu: $x \equiv 1 \mod 77$. So ist nun zu lösen:

$$\begin{aligned} x &\equiv 109 && \mod 30 \\ x &\equiv 1 && \mod 11 \end{aligned}$$

Es ist $\overline{210}^{-1} = \overline{1}$ im $\mathbb{F}_{11}$, also $x = 109 + 2 \cdot 210 \equiv 529 \mod 11 \cdot 3 \cdot 7$

Bemerkung (zur Praxis): Das Sytem $x \equiv x_i \mod m_i$, $(i = 0, \dots, l)$. Der Beweis liefert eine γ-adische Darstellung von x und $m = y\ \gamma = (m_0, \dots, m_l)$ wie folgt: $y = z_{l-1}M_{l-1} + \dots + z_0$. Die z_i sind rekursiv aus $z_0 = x_0 \bmod m_0$, $y' \equiv x'_i \bmod m_j$, $(i = 1, \dots, l)$. Also $y' = \frac{x-z_0}{m_0}$, $x'_i = (x_i - z_0)u_{i0} \bmod m_j$. $\overline{u_{i0}} = \overline{m_0^{-1}}$ in $\mathbb{Z}/m_i\mathbb{Z}$. x'_i in γ'-adischer Darstellung nach Induktions-Voraussetzung ($\gamma' = (m_1, \dots, m_l)$).

Empfehlung zur Praxis, vor allem wenn viele Kongruenzen zu den selben m_i zu lösen sind:

(1) Berechne die u_{ij} nur einmal.

(2) Belasse die Ergebnisse m in der Form $x = (z_{l-1}, \dots, z_0)_\gamma$

Zum paralellen Rechnen: Seien $R, m_1, \dots, m_l$ wie im chinesischen Restsatz. Betrachte die Abbildung

$$\begin{aligned} R/mR &\to \prod_{j=1}^{l}(R/m_jR) \\ \psi : x + mR &\mapsto (\dots, x + m_jR, \dots) \end{aligned}$$

ψ ist wohldefiniert: $x + mR = x' + mR \iff x \equiv x' \mod m \iff x \equiv x' \mod m_j$ und ein Ringhomomorphismus (leicht zu sehen).

Wir beobachten: Ist $\psi : A \to B$ eine Abbildung, so gilt, dass ψ injektiv genau dann ist wenn die Gleichung $\psi(x) = b$ höchstens eine Lösung x hat. Surjektivität heißt analog, dass jede Gleichung $\psi(x) = b$ mindestens eine Lösung x hat. ψ bijektiv ist dann gleichbedeutend damit, dass $\psi(x) = b$ genau eine Lösung hat.

Für obiges ψ gilt: $b = (\dots, a_j + m_jR, \dots)$. $\psi(x + m_jR) = b$: $(\dots, x + m_jR, \dots) = (\dots, a_j + m_jR, \dots) = b$. $x + mR$ Urbild von $b \iff \forall j : x + m_jR_j = a_j + m_jR \iff \forall j : x \equiv a_j \mod m_j$. Also:

- ψ surjektiv $\iff \forall b \exists$Lösung $x \equiv a_j \mod m_j$
- ψ injektiv $\iff$ Lösung x ist eindeutig modulo m

Ergebnis: Der chinesische Restsatz wie oben ist gleichbedeutend mit:

Satz 3.15 (Theorem B, Chinesischer Restsatz, theoretische Form)
R ein euklidischer Ring, $m_1, \dots, m_l \in R$, $\operatorname{ggT}(m_i, m_j) = 1$ für $i \neq j$. Dann hat man den Ringisomorphismus:

$$\begin{aligned} R/mR &\to \prod_{j=1}^{l}(R/m_jR) \\ \psi : x + mR &\mapsto (\dots, x + m_jR, \dots) \end{aligned}$$

Bemerkung (Zur Praxis): ψ^{-1} wird gegeben durch lösen simultaner Kongruenzen. „Komponentenweises Rechnen: Rechnen im R/mR ersetzt durch paralleles Rechnen in den R/m_jR“

Bemerkung (Theoretische Anwendung): Voraussetzungen wie im Satz. Die Einheitengruppe $(R/mR)^\times$ ist isomorph durch ψ zu $\prod_{j=1}^{l}(R/m_jR)^\times$. Ist $R = \mathbb{Z}$, so gilt $\varphi(m) = \prod_{j=1}^{l}\varphi(m_j)$, also ein neuer Beweis für die Multiplikativität von φ.

3.5 Ausgewählte Anwendungen von Kongruenzen

3.5.1 Diophantische Gleichungen

Sei $0 \neq f \in \mathbb{Z}[X_1, \ldots, X_n]$ (Polynom mit n Unbekannten und Koeffizienten aus $\mathbb{Z}$), $x = (x_1, \ldots, x_n) \in \mathbb{Z}^n$.

Eine diophantische Gleichung ist eine Gleichung der Form $f(x) = 0$, f wie oben, mit eine „Lösung x“.

Der Wunsch hier ist: Man finde möglichst viel Informationen über die Menge $\mathcal{V}_f(\mathbb{Z}) := \{x \in \mathbb{N}^n \mid f(x) = 0\}$ aller ganzzahligen Lösungen.

Das Problem ist oft extrem schwierig. Zum Beispiel die diophantischen Gleichungen $x^n + y^n + z^n = 0$, $x = (x, y, z)$, auch bekannt als das Fermatproblem.

Information für Logik-Freunde: Das 10. Hilbertsche Problem (Paris 1900):

> Man finde einen Algorithmus, der zu gegebenem $f \in \mathbb{Z}[X1, \ldots, X_n]$ entscheidet, ob $\mathcal{V}_f(\mathbb{Z}) = \emptyset$ oder $\mathcal{V}_f(\mathbb{Z}) \neq \emptyset$ ist.

Satz von Julia Robison (1910-85), J. Matjasevič: Es gibt keinen solchen Algorithmus!

Triviale, aber wichtige Methode: $f(x) = 0$ hat Lösung $x \in \mathbb{Z}^n \implies f(x) = 0$ hat Lösung $x \in \mathbb{R}^n$ (Analysis) und $\forall m \in \mathbb{Z} : f(x) \equiv 0 \mod m$ lösbar $\iff \forall t \in \mathbb{N}_+ \forall p \in \mathbb{P} : f(x) \equiv 0 \mod p^t$ lösbar. Die Folgerung ist, dass falls für ein $m \in \mathbb{N}_+$ gilt, dass für alle $(x_1, \ldots, x_n) \in \mathbb{Z}^n$, $0 \leq x_j < m_j$ gilt: $f(x) \not\equiv 0 \mod m$, so gilt $\mathcal{V}_j(\mathbb{Z}) = \emptyset$, es gibt also keine Lösung.

Beispiel
$f = X_1^2 + X_2^2 - k$, $k \in \mathbb{Z}$, diophanischsche Gleichung $x_1^2 + x_2^2 = k$. Unlösbar für $k < 0$ (da keine Lösung in $\mathbb{R}^2$). Nur interessant: $k > 0$.

Betrachtung modulo 4:

$$0^2 = 0, (\pm 1)^2 = 1, (\pm 2)^2 = 0 \implies (x_1^2 + x_2^2) \bmod 4 = \begin{cases} 0+0 \\ 0+1 \\ 1+1 \end{cases} \in \{0, 1, 2\}.$$

Für $k \equiv 3 \mod 4$ hat $x_1^2 + x_2^2 = k$ also keine ganzzahlige Lösung!

Es kann eine Primzahl $p \neq 2$ nur dann Summe zweier Quadrate sein, wenn $p \equiv 1 \mod 4$ ist. Hier gilt auch die Umkehrung, Beweis folgt eventuell später.

Beispiel
$f = X_1^2 + X_2^2 + X_3^2 - k$, also $x^2 + y^2 + z^2 = k$. Modulo 4 führt hier zu keiner Aussage. Wie betrachten modulo 8: $0^2 = 0$, $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 1$, $(\pm 4)^2 = 0$. Also gilt:

$$(x_1^2 + x_2^2 + x_3^2) \bmod 8 = \begin{cases} 0+0+0 \\ 0+1+0 \\ 1+1+1 \\ 1+1+1 \\ 0+4+0 \\ \quad\vdots \end{cases} \in \{0,1,2,3,4,5,6\}.$$

Ergebnis: Für $k < 0$ oder $k \equiv 7 \mod 8$ hat die Diophantische Gleichung $x_1^2+x_2^2+x_3^2 = k$ keine Lösung.

Zur Information, nach Gauß: Die Umkehrung gilt auch für ungerade k.

Satz von Lagrange: $x_1^2 + x_2^2 + x_3^2 + x_4^2 = k$ $(k \in \mathbb{N})$ hat immer Lösungen.

Gelegentlich erlangt man Ergebnisse auch über andere Gleichungen:
Beispiel
Gesucht sind Lösungen von $9^x + x^3 = k$ mit $x \in \mathbb{N}_+$.

Betrachtung modulo 9: $9^x \equiv 0 \mod 9$. $0^3 = 0$, $(\pm1)^3 = \pm1$, $(\pm2)^3 = \mp1$, $(\pm3)^3 = 0$, $(\pm4)^3 = \pm1 \implies x^x + x^3 \equiv 0, \pm1 \mod 9$. Ergebnis: Für $k \equiv 2,3,4,5,6,7 \mod 9$ hat die Gleichung keine Lösung in $x \in \mathbb{Z}$.

3.5.2 Interpolation

Hier sei $R = K[X] \ni f$, $\alpha, \beta \in K$:

$$\begin{aligned} f(\alpha) = \beta &\iff (f-\beta)(\alpha) = 0 \\ &\iff (X-\alpha) \mid f - \beta \\ &\iff f \equiv \beta \mod (X-\alpha) \end{aligned}$$

Das Sytem $f \equiv \beta_j \mod (X-\alpha_j)$ $(j = 0,\dots,n) \iff \forall j = 0,\dots,n : f(\alpha_j) = \beta_j$ (Vorraussetzung $\alpha_i \neq \alpha_j$ für $i \neq j$, d.h $\mathrm{ggT}(X-\alpha_i, X-\alpha_j) \neq 0$).

Der Chinesische Restsatz ergib nun: Zu gegebenen $n+1$ Punkten $\alpha_0,\dots,\alpha_n \in K$ $(\alpha_i \neq \alpha_j)$ und Punkten $\beta_0,\dots,\beta_n \in K$ gibt es genau ein $f \bmod (X-\alpha_0)\cdots(X-\alpha_n)$, also $\mathrm{ord}(f) \leq n$ mit $f(\alpha_j) = \beta_j$. Damit ist das Interpolationsproblem gelöst.

Frage: Kann man bei Interpolation die Tangentensteigung (allgemein $f^{(j)}(\alpha_k)$) auch vorschreiben (Hermitesche Interpolationsaufgabe)? Ja für $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ (Übung).

$f \in K[X]$, $(X-\alpha)$-adische Darstellung. Ziffern $z_j \in K[X]$ haben Grad $z : j < \mathrm{grad}(X-\alpha) = 1$, das heißt $z_j \in K$. $f = \sum_{j=0}^n z_j(X-\alpha)^j$, das ist die Taylor-Entwicklung in α. z_j gegeben durch $\frac{f^{(j)}(\alpha)}{j!}$.

$$f \equiv g_{\alpha,d} \mod (X-\alpha)^{\alpha+1}, \qquad g_{\alpha,d} := \sum_{j=0}^{d} z_j(X-\alpha^j) \tag{3.3}$$

$g_{\alpha,d}$ ist gegeben durch $f(\alpha), f'(\alpha), \dots, f^{(d)}(\alpha)$.
System (3.3) entspricht der Vorgabe der $f^{(j)}(\alpha)$, Interpolation mit $m_{j,k} = (X-\alpha_k)^{d_j}$ ist lösbar mit dem Restsatz.

3.5.3 Rechnen im Computer mit großen ganzen Zahlen

Prinzip: Gleicheit in $\mathbb{Z}$ entspricht Kongruenz und einer passender Abschätzung.

Bemerkung: $m \in \mathbb{N},\ m > 1$, etwa $2 \nmid m$. Ist $u \equiv v \mod m$ und $|u|, |v| \leq \frac{m}{2}$, so ist $u = v$, weil u, v sind im symmetrischen Versys_m.

Wende dies an auf die Berechnung von $f(x), f \in \mathbb{Z}[X_1, \ldots, X_n],\ x = (x_1, x_2, \ldots, x_n) \in \mathbb{Z}^n$. Kennt man eine Schranke $|f(x)| < \frac{m}{2}$, so genügt es, $f(x) \mod m$ auszurechnen. $f(x) \mod m$ kann für $m = m_1 \cdot \cdots \cdot m_l$ durch Berechnen von $y_j = f(x) \mod m_j$ $(j = 1, \ldots, l)$ ersetzt werden, das ergibt simultane Kongruenz $y = y_j \mod m_j$, die mit dem chinesischen Restsatz gelöst werden kann.

3.6 Struktur der Primrestklassengruppe mod m

R euklidisch, $m = \prod_{i=1}^{l} p_i^{t_i}$ Primzerlegung, $t_j \in \mathbb{N}_+$. Aus dem Chinesischen Restsatz: $(R/mR)^\times \cong \prod_{j=1}^{l}(R/p_j^{t_j}R)$ (beachte: $\mathrm{ggT}(p_i^{t_i}, p_j^{t_j}) = 1$ für $i \neq j$). Es genügt also $G := R/p^tR$ mit $p \in P,\ t \in \mathbb{N}_+$ zu betrachten. Hier nur der Fall $R = \mathbb{Z}$ ($R = \mathbb{F}_p[X]$ geht ähnlich).

Erinnerung: $t = 1,\ \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p,\ \mathbb{F}_p^\times$ ist zyklich, es existiert eine Primitivwurzel $w \mod p$.

Frage: Wie ist der Fall für $t > 1$?

Für $p > 2$ existiert eine Primitivwurzel!

Gesucht ist also eine Primitivwurzel u, das heißt $\mathrm{ord}\,\overline{u} = \varphi\left(p^t\right) = (p-1)p^{t-1}$ in G. Es genügt $u_1, u_2 \in \mathbb{Z}$ mit $p - 1 \mid \mathrm{ord}\,\overline{u}_1$ und $p^{t-1} \mid \mathrm{ord}\,\overline{u}_2$ zu finden. Wegen $\mathrm{ord}\,\overline{u}_j \mid \#G = (p-1)p^{t-1}$ gilt $s \mid p - 1$. Daraus folgt, für $v_1 := u_1^{p^{t-1}}, v_1 := u_2^{p-1}$ ist

$$\mathrm{ord}\,\overline{v}_1 = \mathrm{ord}\,\overline{u}_1^{p^{t-1}} = \frac{\mathrm{ord}\,\overline{u}_1}{\mathrm{ggT}\left(\mathrm{ord}\,\overline{u}_1, p^{t-1}\right)} = \frac{(p-1)p^r}{p^r} = p - 1.$$

Ebenso: $\mathrm{ord}\,\overline{v}_2 = p^{t-1}$ (Nachrechnen). Aus Übungsaufgabe 3 (a) Blatt 7 folgt mit $u := v_1v_2 \mod p^t$, $\mathrm{ord}\,\overline{u} = (p-1)p^{t-1}$. Bevor wir fortfahren, benötigen wir noch ein Lemma, das wir zum Beweis eines Hilfssatzes benötigen.

Lemma 3.16 (($1 + p$)–Lemma)
$p \in \mathbb{P},\ p > 2,\ r \in \mathbb{N}_+,\ u \in \mathbb{Z}$. Dann gilt: $(1 + up)^{p^{r-1}} \equiv 1 + up^r \mod p^{r+1}$.

Beweis
Beweis via Induktion nach r.

$r = 1$: $(1 + up)^{p^{1-1}} = 1 + up \equiv 1 + up^1 \mod p^2 \quad \checkmark$.

$r > 1$: Induktionshypothese (für $r - 1$):

$$(1 + up)^{p^{r-2}} \equiv 1 + up^{r-1} \mod p^r.$$

$\implies (1+up)^{p^{r-2}} = 1 + up^{r-1} + zp^r$ mit $z \in \mathbb{Z} \implies (1+up)^{p^{r-1}} = \left((1+up)^{p^{r-2}}\right)p = \left(1 + \left(up^{r-1} + zp^r\right)\right)^p = 1 + \sum_{i=1}^p \underbrace{\binom{p}{i}}_{\in\mathbb{Z}} \underbrace{\left(up^{r-1} + zp^r\right)^i}_{=(p^{r-1}(u+zp))^i =: c_i}$.

$r \geq 2,\ i > 2$: $v_p(c_i) = \underbrace{v_p\left(\binom{p}{i}\right)}_{\geq 0} + v_p\left(p^{(r-1)i}\right) + \underbrace{v_p(u+zp)^i}_{\geq 0} \geq (r-1)i \geq (r-1)r > r+1 \implies p^{r+1} \mid c_1 \implies c_i \equiv 0 \mod p^{r+1}$.

$i = 2$: $v_p(c_2) = \underbrace{v_p\left(\frac{p(p-1)}{2}\right)}_{\geq 1} + \underbrace{v_p\left(p^{2(r-1)}\right)}_{=2(r-1)} + \underbrace{v_p(u+zp)^2}_{\geq 0} \geq 2r - 2 + 1 = 2r - 1 \geq r + 1 \implies c_2 \equiv 0 \mod p^{r+1}$.

$i = 1$: $c_1 = p \cdot p^{r-1}(u+zp) = up^r + zp^{r+1} \equiv up^r \mod p^{r+1}$.

$\implies$ Behauptung. ∎

Hilfssatz
Sei $p \in \mathbb{P},\ p > 2,\ t \in \mathbb{N}_+$.

(1) Ist w eine Primitivwurzel $\mod p$, so gilt in $G = \left(\mathbb{Z}/p^t\mathbb{Z}\right)^\times$: $p - 1 \mid \operatorname{ord} \overline{w},\ \overline{w} = w + p^t\mathbb{Z}$. ($u_1 = w$ *wählbar*).

(2) $\operatorname{ord}(\overline{1+p}) = p^{t-1}$ ($v_2 = 1 + p$ *wählbar*).

Beweis

(1) Sei $l = \operatorname{ord} \overline{w}$, also $\overline{w}^l = 1$, das heißt $w^l \equiv 1 \mod p^t$. $t \geq 1 \implies w^l \equiv 1 \mod p^1 \implies$ in $\mathbb{F}_p$ ist $\overline{w}^l = 1$, $\operatorname{ord} \overline{w} = p - 1 \implies p \cdot a \mid l$ (Elementar-Ordnungssatz).

(2) Folgt aus Lemma 3.16

$(1+p)^{p^{t-1}} \equiv 1 + 1 \cdot p^t \mod p^{t-1} \implies (1+p)^{p^{t-1}} \equiv 1 \mod p^t \implies \overline{1+p}^{p^{t-1}} \implies \operatorname{ord} \overline{1+p} \mid p^{t-1}$. Für $t \geq 2$ ist noch zu zeigen: $(1+p)^{p^{t-2}} \not\equiv 1$. $(1+p)^{p^{t-2}} \equiv 1 + p^{t-1} \mod p^t$ (nach Lemma 3.16). $\overline{1+p}^{p^{t-2}} = \overline{1} + \underbrace{\overline{p^{t-1}}}_{\neq 0} \neq \overline{1} = 1$. ∎

Gezeigt (für $p > 2$):

Satz 3.17 (Struktursatz für $(\mathbb{Z}/p^t\mathbb{Z})^\times$, eigentlich ein Theorem)
Sei $p \in \mathbb{P},\ t \in \mathbb{N}_+$. Dann gilt:

(1) Falls $p > 2$, so ist $(\mathbb{Z}/p^t\mathbb{Z})^\times$ zyklisch (das heißt, es gibt eine Primitivwurzel $u \mod p^t$, also $(\mathbb{Z}/p^t\mathbb{Z})^\times = \{1, \overline{u}, \ldots, \overline{u}^{p^{t-1}(p-1)-1}\}$

(2) Falls $p = 2$: $(\mathbb{Z}/2\mathbb{Z})^\times$, $(\mathbb{Z}/4\mathbb{Z})^\times$ zyklisch. Für $t > 2$ ist $(\mathbb{Z}/2^t\mathbb{Z})^\times$ *nicht* zyklisch, doch es gilt: Jedes $\overline{a} \in (\mathbb{Z}/2^t\mathbb{Z})^\times$ lässt sich eindeutig in der Form $\overline{a} = \overline{(-1)}^\varepsilon \cdot \overline{5}^s$ schreiben, mit $\varepsilon \in \{0,1\}, s \mod 2^{t-2}$ (eindeutig). $(\mathbb{Z}/2^t\mathbb{Z})^\times$ ist sozusagen bis auf das Vorzeichen $(-1)^\varepsilon$ zyklisch.

Info:
Man kann sagen: Ist $u \in \mathbb{Z}$ Primitivwurzel mod p^2, so auch mod p^t $\forall t \in \mathbb{N}_+$

Es gibt viele Arbeiten über Primitivwurzeln, z. B. analytische Zahlentheorie (sehr schwierig) gibt Schranken $s(p)$ so, dass in $\{2, \dots, s(p)\}$ PW mod p zu finden.

Artins Vermutung: 2 (oder jedes $n \in \mathbb{N}_+, n \neq 1$) ist Primitivwurzel für ∞-viele $p \in \mathbb{P}$.

Rechnen in $(\mathbb{Z}/m\mathbb{Z})^x$ auf dem Computer, falls viele Produkte zu berechnen sind.
Primzerlegung $m = p_1^{t_1} \cdot \ldots \cdot p_l^{t_l}$ $t_j \in \mathbb{N}_+$
Kodiere $a + m\mathbb{Z} = \overline{a}$ wie folgt:
Berechne vorab PW u_j mod $p_j^{t_j}$

$$\begin{array}{rcl} (\mathbb{Z}/m\mathbb{Z})^x & \to & \prod_{j=1}^{l} (\mathbb{Z}/p^j\mathbb{Z})^x \\ \alpha = a + m\mathbb{Z} & \mapsto & (\dots, a + p_j, \dots) \end{array}$$

$$\begin{array}{lrcl} \text{Bijektiv:} & \alpha & \leftrightarrow & (\dots, r(\alpha, j), \dots) \\ & \alpha \cdot \beta & \leftrightarrow & (\dots, r(\alpha, j) + r(\beta, j) \bmod p_j^{t_j - 1}(p_j - 1), \dots) \end{array}$$

α^{-1} ähnlich

Zum Rechnen mit großen ganzen Zahlen (Skizze)

Prinzip: Gleichheit in $\mathbb{Z}$ = Kongruenz + passende Abschätzung
Bemerkung: $m \in \mathbb{N}, m > 1$, etwa $2 \nmid m$. Ist $u \equiv v \bmod m$ und $|u| \leq \frac{m}{2}$, $|v| \leq \frac{m}{2}$, so ist $u = v$.
Grund: u, v sind in Versys$_m$ (symm. Vertretersystem der Reste mod m), also $u = v$.

Wende dies an auf die Berechnung von $f(x), f \in \mathbb{Z}[X_1, \dots, X_n], x = (x_1, \dots, x_n) \in \mathbb{Z}$. Kennt man Schranke $|f(x)| < \frac{m}{2}$ so genügt es $f(x)$ mod m auszurechnen.
$f(x)$ mod m kann für $m = m_1 \cdot \ldots \cdot m_l$ durch Berechnen von $f(x)$ mod $m_j =: y_j$ $(j = 1, \dots, l)$ ersetzt werden + 1x chinesischer Restsatz: $y \equiv y_j$ mod m_j.

Aufgabe:
Berechne mit dem Computer $\det A$ (exakt), $A \in \mathbb{Z}^{n \times n}$
Soll sein n mäßig groß, $A = (a_{ij})$, die a_{ij} mäßig groß.
Naives Verfahren: Gauß-Algorithmus in $\mathbb{Q}$:
Ärger: Sehr große Integer-Zahlen als Zähler und Nenner entstehen während der Rechnung unkontrolliert. Mögliche bessere Vorgehensweise, etwa $|a_{ij}| \leq s$ (Schranke)
Leibnitzformel: $\det A = \sum_{\pi \in S_n} \operatorname{sgn}(\pi) \prod_{i=1}^{n} a_{i,\pi(i)}$ liefert Abschätzung $|\det A| \leq s^n \cdot n!$ $(n! = \#S_n)$
Schranke $S = 2 \cdot |\det A| = 2 \cdot s^n \cdot n!$ kann sehr groß sein. Wähle Primzahlen $(\neq 2)$ $p_1, \dots, p_t$ (t verschieden) mit $S \leq p_1 \cdot \ldots \cdot p_t$. Dann $|\det A| \leq \frac{p_1 \cdot \ldots \cdot p_t}{2} = \frac{m}{2}$, $m = p_1 \cdot \ldots \cdot p_t$
Kann oft sein: t mäßig groß, alle p_j mäßig groß. (z. B.: $s = 100$, $n = 100 \Rightarrow S = 100^{100} \cdot 2 \cdot 100! \leq 2 \cdot 100^{120}$ Es reichen also 130 p_j's mit $p_j > 100$, diese können < 1000 gewählt werden $\Rightarrow$ in $\mathbb{F}_{p_j}$ kann sehr gut und schnell gerechnet werden!
$\Rightarrow$ Berechnung von $\det \overline{A}$, $\overline{A} = (\overline{a_{ij}})$ in $\mathbb{F}_{p_j}^{n \times n}$ kann durch Herstellen von Dreiecksform von $\overline{A}$ für mäßig große n schnell berechnet werden. (Durch Arbeiten in Versys$_p$ entstehen niemals große Zahlen!) Das ergibt $y_j \in$ Versys$_p$ mit $\det A \mod p_j = y_j$. Es ist dann $y \equiv y_j$ mod p_j zu lösen (simultane Kongruenz $m = p_1 \cdot \ldots \cdot p_t$). Daher für $y \in$ Versys$_m$ (symm.) ist $\det A = m$. y kann sehr groß sein, aber die Kongruenz ergibt sehr große Zahlen nur kontrolliert! (Mäßig große Zahlen, falls man mit γ-adischer Darstellung von $y = \det A$, $\gamma = (p_1, \dots, p_t, \dots)$ zufrieden ist.

4 Endliche Körper und der Satz von Chevalley

Schon bekannt:

(1) $\forall p \in \mathbb{P}$ gibt es den Körper $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ mit $\#\mathbb{F}_p = p$

(2) Hat man ein irred. Polynom (Primpolynom) g in $R = \mathbb{F}_p[X]$ mit Grad $g = n$, so ist $\overline{R} = R/gR$ ein Körper mit $q = p^n$ Elementen, der $\mathbb{F}_p$ als Teilkörper enthält.

(3) Jeder endl. Körper L enthält primitives ζ, $L^x = L \setminus 0 = \{1, \zeta, ...\}$.

4.1 Untersuchung eines endl. Körpers L mit $\#L = q$

ord(1) $= p =$min$\{n \in \mathbb{N}_+ | n \cdot 1_L = 0\}$ (Ordnung in $(L, +)$, neutr. Element ist 0, statt x^n steht nx)
Beh.: $p \in \mathbb{P}$
Ann.: $p = uv$ zerlegbar, $1 \leq u < p$, $1 \leq u < p$, $uv \cdot 1 = (u \cdot 1)(v \cdot 1) = 0$
$\Rightarrow u \cdot 1 = 0$ oder $v \cdot 1 = 0$, Widerspruch. $\Rightarrow L$ enthält $\mathbb{F}_p$, wenn man $\mathbb{F}_p \cong \text{Versys}_p = \{0, \ldots, p-1\} \ni z$ nimmt und $z \cdot 1$ mit $\overline{z}$ identifiziert (inj. Ringhomomorphismus $\mathbb{F}_p \to L$, $\overline{z} \mapsto z \cdot 1$)
Außerdem ist L ein $\mathbb{F}$-Vektorraum, wenn die Skalarmultiplikation so erklärt wird:
$\alpha \in L, \overline{z} \in \mathbb{F}_p : \overline{z}\alpha = (z \cdot 1) \cdot \alpha$ (VR-Axiome leicht nachprüfbar!)
$\#L = q < \infty \Rightarrow n := \dim\, L < \infty$.
LA I: Basiswechsel liefert einen VR-Isomorphismus $L \to \mathbb{F}_p^n$
$\Rightarrow q = \#L = \#\mathbb{F}_p^n = p^n$

(1) Gesucht zu $n \in \mathbb{N}_+, p \in \mathbb{P}$ ein Körper mit $q = p^n$ Elementen.

(2) Wie eindeutig ist L. (Wunsch: Je zwei solche L's sind isomorph)

Idee: "Kleiner Fermat"gilt in L, d.h. $\forall \alpha \in L : \alpha^q = \alpha$
$\Rightarrow L$ besteht aus allen Nullstellen α von $X^q - X$
$\Rightarrow X^q - X = \prod_{\alpha \in L}(X - \alpha)$
Suche "große"Körper $K \supset \mathbb{F}_p$, so dass $X^q - X$ so zerfällt!
Hoffnung: Die Nullstellen α von $X^q - X$ bilden dann den gesuchten Körper.

Durchführung der Idee: Kette von Hilfssätzen

Hilfssatz (1)
Ist R ein Ring der $\mathbb{F}_p$ als Teilring enthält, so gilt $\forall \alpha, \beta \in R, n \in \mathbb{N}_+, a = p^n$

$$(\alpha \pm \beta)^a = \alpha^a \pm \beta^a$$

Beweis
In $\mathbb{Z}$ gilt für $1 \leq i \leq p : (1 \cdot 2 \cdot \ldots \cdot i)\binom{p}{i} = p \cdot (p-1) \cdot \ldots \cdot (p-i+1)$ In $\mathbb{F}_p$ gilt für $1 \leq i \leq p : \underbrace{(\overline{1} \cdot \overline{2} \cdot \ldots \cdot \overline{i})}_{\in \mathbb{F}_p^x} \overline{\binom{p}{i}} = \overline{0} \ldots = \overline{0}$
$\Rightarrow \overline{\binom{p}{i}} = \overline{0}$
$\Rightarrow (\alpha + \beta)^p = \alpha^p + \beta^p + \sum_{i=1}^{p-1} \binom{p}{i} \alpha^i \beta^{p-i} = \alpha^p + \beta^p$, ok für n = 1 (− ähnlich)
Rest Induktion, sei $j > 1$
$(\alpha + \beta)^{p^j} = (\alpha + \beta)^{p^{j-1} \cdot p} = (\alpha^{p^{j-1}} + \beta^{p^{j-1}})^p = \alpha^{p^{j-1} \cdot p} + \beta^{p^{j-1} \cdot p} = \alpha^{p^j} + \beta^{p^j}$ ∎

Hilfssatz (2)
Sei K ein Körper, der $\mathbb{F}_p$ als Teilkörper enthält, so dass $(q = p^n, n \in \mathbb{N}_+)$

$$X^q - X = \prod_{j=0}^{q-1} (X - \alpha_j) \text{ mit } \alpha_0, \ldots, \alpha_{q-1} \in K$$

Dann ist $L := \{\alpha_0, \ldots, \alpha_{q-1}\}$ ein Körper mit q Elementen.

Beweis
$K \ni \alpha$ Nullstelle von $X^q - X \Leftrightarrow \alpha^q - \alpha = 0 \Leftrightarrow \alpha^q = \alpha$
$\alpha \in L \Leftrightarrow \alpha^q = \alpha$
Prüfe nach: $(L, +)$ ist Untergruppe von $(K, +)$, $(L^x = L \setminus 0, \cdot)$ ist Untergruppe von $(K^x, \cdot) \Leftrightarrow$ Teilkörper, $\mathbb{F}_p \subseteq L$ wegen $\alpha^p = \alpha = \alpha^q$ für $\alpha \in \mathbb{F}_p$
$0 \in L \neq \emptyset$
$\alpha, \beta \in L \Rightarrow \alpha^q = \alpha, \beta^q = \beta \Rightarrow (\alpha - \beta)^q = \alpha^q - \beta^q$ (HS1) $= \alpha - \beta \Rightarrow \alpha - \beta \in L$ also L Untergruppe von K.
Analog L^x $\alpha, \beta \in L^x \Rightarrow \alpha^q = \alpha, \beta^q = \beta \Rightarrow \alpha^q (\beta^q)^{-1} = \alpha\beta^{-1} \Rightarrow \alpha\beta^{-1} \in L^x$, also L^x Untergruppe von K^x.
Wieso $\#L = q$? Wieso hat $X^q - X$ in K nur einfache Nullstellen?
$\alpha \in L$, Wende HS1 an auf $K[X]$
$X^q - X = (X - \alpha)^q = X^q - \alpha^q - (X - \alpha) \Rightarrow 0 = (X - \alpha)^q - (X - \alpha) = (X - \alpha)\big((X - \alpha)^{q-1} - 1\big)$,
α ist nicht Nullstelle von $(X - \alpha)^{q-1} - 1$
Die NST ist einfach, Hinweis: $L = \{\zeta - \alpha | \zeta \in L\}$ ∎

Existenz von L: Suche $K \supseteq \mathbb{F}_p$ (Körper), so dass K q NST von $X^q - X$ enthält.

Hilfssatz (3)
Ist K ein Körper, $f \in K[X]$, Grad $f > 0$, $K \supseteq \mathbb{F}_p$ (als Teilkörper), so gibt es einen endl. Körper $\tilde{K}$, der K (und damit $\mathbb{F}_p$) als Teilkörper enthält und ein $\alpha \in \tilde{K}$ mit $f(\alpha) = 0$

Beweis
Primzerlegung von f, sei $f = g_1^{m_1} \cdot \ldots \cdot g_t^{m_t}$, g_j irred. in $K[X]$ (EuFa-Satz)
$f(\alpha) = 0 \Rightarrow 0 = g_1(\alpha)^{m_1} \cdot \ldots g_t(\alpha)^{m_t} \Rightarrow \exists j : g_j(\alpha) = 0$
So ein α ist gesucht! (und $\tilde{K}$)
$\tilde{K} := K[X]/g_j K[X]$ ist ein Körper, der K als Teilkörper enthält.
$\alpha = \overline{X}$ ist NST von g_j, also f! $g_j(\overline{X}) = \overline{g_j(X)} = \overline{0} = 0$ ∎

Hilfssatz (4)
Es gibt einen endl. Körper K, in dem $f \in \mathbb{F}_p[X]$ (Grad $f > 0$, f normiert) in Linearfaktoren zerfällt, d.h.

$$f = \prod_{j=1}^{m} (X - \alpha_j) \quad (\alpha_1, \ldots, \alpha_m \in K)$$

Beweis
Induktion nach $m =$ Grad f, $m = 1$, $f = X - \alpha$, $\alpha \in \mathbb{F}_p$

$m > 1$ $\tilde{\mathbb{F}}_p$ nach HS3 mit $\alpha \in \tilde{\mathbb{F}}_p$, $f(\alpha) = 0$
$\Rightarrow X - \alpha | f$ in $\tilde{\mathbb{F}}_p[X]$
$\Rightarrow f = (X - \alpha)\tilde{f}$, Grad $\tilde{f} =$ Grad f -1
IH für $\tilde{f} \Rightarrow$ Beh. ∎

Hilfssatz (5)
Sei M ein Körper mit p^n Elementen, $R = \mathbb{F}_p[X]$, $\xi \in M$, $g \in R$ mit $g(\xi) = 0$ und g irreduzibel.

Ist dann entweder $\operatorname{grad} g = n$ oder ξ ein primitives Element von M, so seind die Körper M und $R/gR = \overline{R}$ isomorph. Ein irreduzibles Polynom, das ξ als Nullstelle hat, hat den Grad n.

Beweis
$\psi : \overline{R} \to M, \overline{h} \mapsto h(\xi) = \psi(\overline{h})$ ist der gesuchte Isomorphismus.

(1) ψ ist wohldefiniert:

$$\begin{aligned} \overline{h_1} = \overline{h_2} &\iff h_1 \equiv h_2 \mod g \\ &\iff \exists u \in R : h_2 = h_1 + ug \\ &\implies h_2(\xi) = h_1(\xi) + u(\xi) \cdot g(\xi) = h_1(\xi) \end{aligned}$$

(2) ψ ist ein Ringisomorphismus, also $\psi(\overline{h_1} + \overline{h_2}) = \psi(\overline{h_1}) + \psi(\overline{h_2})$:

Klar wegen $(h_1 \pm h2)(\xi) = h_1(\xi) \pm h_2(\xi)$

(3) ψ ist injektiv:

Es genüg zu zeigen: $\operatorname{Kern} \psi = \{0\}$.

Ann: $\alpha \in \operatorname{Kern} \psi$, $\alpha \neq 0$. $1 = \psi(1) = \psi(\alpha^{-1}\alpha) = \psi(\alpha^{-1})\psi(\alpha) = 0$, Wid!

(4) ψ ist surjektiv:

a) $\operatorname{grad} g = n \implies \#\overline{R} = p^n$, $\psi : M \to \overline{R}$ injektiv. Da $\#M = p^n \implies \psi$ surjektiv.

b) ξ primitiv $\iff M = \{0, \xi, \xi^2, \dots, \xi^{q-2}\}$. $\psi(\overline{R}) \ni h(\xi)$ für z.B. $h = X^n$ $(n \in \mathbb{N})$ $\implies \psi(\overline{R}) \ni X^n(\xi) = \xi^n \implies \psi(\overline{R}) \supseteq M \implies \psi$ surjektiv. ∎

Satz 4.1 (Endliche-Körper-Raum)
(1) Ist L ein endlicher Körper, $\#L = q$, dann $\exists p \in \mathbb{P}$, $n \in \mathbb{N}_+$ mit $q = p^n$. (Genauer: Dann ist $\mathbb{F}_p$ ein Teilkörper von L und K ein $\mathbb{F}_p$-Vektorraum der Dimension n).

(2) Zu jedem $n \in \mathbb{N}_+$, $p \in \mathbb{P}$, existiert ein Körper mit $q = p^n$ Elementen.Zusätzlich gilt: Es gibt ein irreduzibles Polynom $g = \mathbb{F}_p[X]$ mit $\operatorname{grad} g = n$. Es ist $g \mid X^q - X$.

(3) Je zwei Körper mit q Elementen sind isomorph.

Also ist es gerechtfertigt, von *dem* Körper $\mathbb{F}_q$ oder $GF(q)$ zu sprechen.

Beweis

(1) Wurde bereits geleistet. (*Aber wo?*)

(2) Erinnerung: Es gibt einen Körper K, der $\mathbb{F}_p$ enthält, so dass $X^q - X = \prod_{j=0}^{q-1}(X - \alpha_j)$, $(\alpha_j \in K)$, $L = \{\alpha_j \mid j = 0, \ldots, q-1\}$ ist Körper mit q Elementen.

(3) M, L seien Körper mti $q = p^n$ Elementen. ξ sei ein primitives Element von M (Existenz: Satz vom primitiven Element). $X^q - X = \prod_{\alpha \in L}(X - \alpha)$. Betrachte die Primzerlegung $X^q - X = \prod_{j=1}^{t} p_j^{n_j}$ in $\mathbb{F}_p[X]$, p_j irreduzibel in R, die es nach dem EuFa-Satz gibt.

Wegen $(X^q - X)(\xi) = 0 = \prod_{j=1}^{t} p_j(\xi)^{n_j}$ existiert ein $j \in \{1, \ldots, t\}$, $p_j(\xi) = 0$, $p_j = g$ irreduzibel in $\mathbb{F}_p[X]$. Hilfssatz 5 liefert: $M \cong R/gR$ und $\operatorname{grad} g = n$ (wo $\#M = p^n$). Wir folgern also: Jedes p_j (also auch g) ist Produkt gewisser $(X - \alpha)$ (EuFa-Satz für $L[X]$) $\implies \exists \alpha \in L : X - \alpha \mid g \implies g(\alpha) = 0$. Wir benutzen nun den Hilfssatz für L statt M und erhalten: $\overline{R} = R/gR \cong L$. Damit erhalten wir: $L \cong M$. ■

Satz 4.2 (Teilkörpersatz)

(1) Sei K ein Teilkörper von $\mathbb{F}_q$ mit $q = p^n$ wie oben. Dann existiert ein $d \in \mathbb{N}$ mit $d \mid n$ und $K \cong \mathbb{F}_{p^d}$.

(2) Ist $d \mid n$, so gibt es genau einen Teilkörper von $\mathbb{F}_q$ mit $\#K = p^d$

Fazit: Teilkörper enpsrechen bijektiv den Teilern d von n.

Beweis

Bemerkung: Ist K ein Teilkörper von L, so ist L ein K-Vektorraum (Skalare Multiplikation ist die von L).

Also ist $\mathbb{F}_q$ ein K-Vektorraum $\implies$ (Basiswahl) $\mathbb{F}_q \cong K^{d'}$; d' ist die Dimension des K-Vektorraums $\mathbb{F}_q = q^n = q = \#K_q = (p^d)^{d'}$, (da $\#K = p^d$) $\implies n = dd' \implies d \mid n$.

Ist $\#K = p^d$, $d \mid n$, K Teilkörper von $\mathbb{F}_q$, so muss K aus den Nullstellen von $X^{p^d} - X$ in $\mathbb{F}_p$ bestehen, also ist K eindeutig bestimmt. ($K = \{\alpha^{p^{\frac{n}{d}}} \mid \alpha \mathbb{F}_p\}$). ■

4.2 Die Sätze von Chevalley und Warming

Es sei generell hier $K = \mathbb{F}_q$, $q = p^n$ wie oben, mit dem wichtigsten Fall $n = 1$, $K = \mathbb{F}_p$.

Das Problem ist: $f \in K[X_1, \ldots, X_n]$ liege vor mit $f(\underline{0}) = 0$, $\underline{0} = (0, \ldots, 0) \in K^n$. Gesucht: Möglichst gute Bedingungen, so dass f eine nicht-triviale Nullstelle $\underline{x} = (\alpha_1, \ldots, \alpha_n) \in K^n$ besitzt. (nicht-trivial: $\underline{x} \neq \underline{0}$).

Bezeichnungen:

(1) $f = \sum_{\underline{m} \in \mathbb{N}^n} \alpha_{\underline{m}} X^{\underline{m}}$, wobei $\underline{m} = (m_1, \ldots, m_n)$, $\underline{0} = (0, \ldots, 0)$, $\alpha_{\underline{m}} \in K$, davon nur endlich viele $\neq 0$.

(2) $X^{\underline{m}} := X_1^{m_1} \cdots X_n^{m_n}$

(3) Setze $|\underline{m}| = m_1 + \cdots + m_n$. Damit ist der Gesamtgrad $\operatorname{grad} f$ wie folgt definiert: $\operatorname{grad} 0 = -\infty$, $f \neq 0$: $\operatorname{grad} f = \max\{|m| \mid \alpha_m \neq 0\}$.

Satz 4.3 (von Warming)
Sei $f \in \mathbb{F}_q[X_1, \dots, X_n]$, $\operatorname{grad} f < n$. Dann ist die Anzahl der Nullstellen von f in $\mathbb{F}_q^n$ durch p teilbar.

Dabei heißt $\mathcal{V}_f(k) := \{\underline{x} \in K^n \mid f(\underline{x}) = 0\}$ die Nullstellenmannigfaltigkeit von f in K.

Allgemeiner: $f_1, \dots, f_l \in K[X_1, \dots, K_n]$: $\mathcal{V}_{f_1,\dots,f_l}(K) = \{\underline{x} \in K^n \mid f_1(\underline{x}) = \cdots = f_l(\underline{x}) = 0\} = \bigcap_{i=1}^{l} \mathcal{V}_{f_j}(K)$

Die Aussage des Satzen ist nun: Ist $\operatorname{grad} f < n$, so gilt $p \mid \#\mathcal{V}_f(K)$

Satz 4.4 (Satz von Chevalley)
Sei $f \in K[X_1, \dots, X_n]$, $f(\underline{0}) = 0$ und $\operatorname{grad} f < n$. Dann hat f ein nichttriviale Nullstelle.

Es ist klar: Satz von Warming impliziert den Satz von Chevalley, da: $f(\underline{0}) = 0 \implies \underline{0} \in \mathcal{V}_f(K) \implies \#\mathcal{V}_f(K) > 0$. $p \mid \mathcal{V}_f(K) \implies \#\mathcal{V}_f(K) \geq p \geq 2$

Spezielles Beispiel:

Satz 4.5
Seien $\alpha_1, \dots, \alpha_{n+1} \in \mathbb{Z}$, $d \leq n$, $d \in \mathbb{N}$. Dann hat die Kongruenz $\alpha_1 x_1^d + \cdots + \alpha_{n+1} x_{n+1}^d \equiv 0 \mod p$ stets eine nicht-triviale Lösung $x = (x_1, \dots, x_n) \in \mathbb{Z}^{n+1}$

Noch spezieller: $\alpha_1 x_1^2 + \alpha_2 x_2^2 + \alpha_3 x_3^2 \equiv 0$ hat stets nicht-triviale Lösung $(x_1, x_2, x_3 \in \mathbb{Z})$.

Beweis
$\operatorname{grad} \alpha_1 x X^d + \cdots \alpha_{n+1} X_{n+1}^d \leq d \leq n+1$ (Variablenzahl). Satz von Chevalley liefert die Behauptung. ∎

Gegenbeispiel: $x_1^2 + x_2^2 \equiv 0 \mod 3$: $x_j^2 \in \{0, 1\} \implies$ Jede Lösung hat $3 \mid x_1$ und $3 \mid x_2$

Weitere Sätze (siehe z.B. Lidl/Niederreiter, Finite Fields):

Satz 4.6 (Satz I)
Sei $d = \operatorname{grad} f_1 + \cdots + \operatorname{grad} f_l < n$ und $f_j \in \mathbb{F}_q[X_1, \ldots, X_n]$. Falls $\mathcal{V}_{f_1,\ldots,f_l}(\mathbb{F}_q) \neq \emptyset$, so gilt: $\#\mathcal{V}_{f_1,\ldots,f_l}(\mathbb{F}_q) \geq w^{n-d}$

Satz 4.7 (Satz II)
Falls $f \in \mathbb{F}_1[X_1, \ldots, X_n]$, $0 < \operatorname{grad} f = d$, so gilt: $\#\mathcal{V}_f(\mathbb{F}_q) \leq d \cdot 1^{n-1}$

Satz 4.8
Sei $0 \neq f \in \mathbb{Z}[X_1, \ldots, X_n]$. Dann gibt e es eine konstante c_f unabhängig von p, so dass

$$\forall p \in \mathbb{P} : |\#\mathcal{V}_f(\mathbb{F}_q) - p^{n-1}| \leq c_f \frac{p^{n-1}}{\sqrt{p}}$$

Der Beweis ist äußerst schwierig, bereits für $n = 2$.

Beweis
Der Beweis des Satzes von Warming **??** gliedert sich in mehrere Ideen, wie bringen sie hier schön isoliert. In vielen Büchern ist der Beweis ziemlich unübersichtlich.

Idee 1: Das Kronecker-δ ist als Polynom darstellbar.

Lemma 4.9
$\delta : K \to K$ sei definiert wie folgt:

$$\delta(\alpha) = \delta_0(\alpha) = \begin{cases} 1, & \alpha = 0 \\ 0, & \text{sonst} \end{cases}$$

Dann $\delta(\alpha) = 1 - \alpha^{q-1} = (1 - X^{q-1})(\alpha)$, weil $\alpha^{q-1} = 1$, wenn $\alpha \in K^\times = \mathbb{F}_q^\times$ und $\alpha^{q-1} = 0$, wenn $\alpha = 0$.

Satz 4.10
Jede Funktion $\mathbb{F}_1 \to \mathbb{F}_1$ ist als Polynom darstellbar.

Beweis
Übung. ∎

Idee 2: Aus f kann man eine Funktion F konstruieren, so dass F die Nullstellen von f zählen hilft.
$F = A - f^{q-1}$. Dann

$$F(x) = 1 - f(x)^{q-1} = \delta_{0,\,f(x)} = \begin{cases} 1, & x \in V_f(K) \\ 0, & \text{sonst} \end{cases}$$

Es folgt die Formel $\sum_{x \in K^n} = \#V_f(K) \cdot 1_K$.

Idee 3: Versuche die linke Seite der Formel zu berechnen, nämlich $\sum_{x \in K^n} g(x)$, $g \in K[X_1, X_2, \ldots, X_n]$.
Beginne mit $n = 1,\ g = X^k$. $\sum_{\alpha \in K} \alpha^k = ?$.

Lemma 4.11
Ist $k \in \mathbb{N}$ und $k = 0$ oder $q - a \nmid k$, so ist $\sum_{\alpha \in K} \alpha^k = 0$ (Dabei muss $0^0 = 1$ definiert werden).

Beweis
$k = 0$: $\sum_{\alpha \in K} \alpha^0 = \sum_{\alpha \in K} 1 = q \cdots 1_K = 0$ und $1_K q = p^n$.
$k > 0$: Dann existiert ein primitives Element $\xi \in K$, das heißt, $K^\times = K \setminus \{0\} = \{1, \xi, \xi^2, \ldots, x^{q-2}\}$ und $\operatorname{ord} \xi = q - 1$, daraus folgt $\xi^k \neq 1$ (laut Elementarordnungssatz).

$$\sum_{\alpha \in K} \alpha^k = \sum_{\alpha \in K \setminus \{0\}} \alpha^k = \sum_{j=0}^{q-2} \xi^{j-k} = \sum_{j=0}^{q-2} \left(\xi^k\right)^j = \frac{\xi^{k(q-1)} - 1}{\xi^k - 1} \text{ (geometrische Reihe!)}$$

(wegen $\xi^{q-1} = 1$). ■

Lemma 4.12
Sei $g \in K[X_1, X_2, \ldots, X_n]$, $\operatorname{grad} g < n(q-1)$, dann ist $\sum_{x \in K^n} g(x) = 0$.

Beweis
Ohne Beschränkung der Allgemeinheit ist $g = x^m$ mit $|m| < n(q-1),\ m \in K^n$, denn wenn $g = \sum \beta_m X^m$, dann $\forall m$ mit $\beta_m \neq 0 :\ |m| < n(q-1)$, denn die Summe von Nullen ergibt null. Weiterhin gilt

$$\sum_{x \in K^n} X^m(x) = \sum_{(\alpha_1, \alpha_2, \ldots, \alpha_n) \in K^n} \alpha_1^{m_1} \cdot \alpha_2^{m_2} \cdot \cdots \cdot \alpha_n^{m_n}$$

(Durch Ausmultiplizieren erhält man

$$\prod_{j=1}^{n} \left(\sum_{\alpha_j \in K} \alpha_j^{m_j} \right) = \sum_{(\alpha_1, \alpha_2, \ldots, \alpha_n) \in K^n} \alpha_1^{m_1} \cdot \alpha_2^{m_2} \cdot \cdots \cdot \alpha_n^{m_n}.$$

(Kann man, wenn man Lust hat, mit Induktion beweisen))
Voraussetzung: $m_1 + m_2 + \cdots + m_n < n(q-1) \implies \exists j \in \{1, 2, \ldots, n\}$ mit $m_j < q-1 \implies m_j = 0$ oder $q - 1 \mid m_j$. Anwendung von Lemma 4.11 mit $k = m_j$

$$\implies \sum_{\alpha_j \in K} \alpha_j^{m_j} = 0 \implies \prod \sum \alpha_j^{m_j} = 0 = \sum X^m(x).$$

■

Wende das Lemma 4.12 an auf $g = F = 1 - f^{q-1}$. $\operatorname{grad} g = (q-1)\underbrace{\operatorname{grad} f}_{<n} \implies$ $\operatorname{grad} g < (q-1)n$, also kann letztes Lemma angewandt werden

$$\implies \sum_{x \in K^n} F(x) = 0 = \#V_f(K) \cdots 1_k \implies p = \operatorname{ord} 1_K \mid \#V_f(K).$$

■

5 Quadratische Kongruenzen

5.1 Einführende Diskussion

Problem: Gegeben $a, b, c \in \mathbb{Z}$. Wann ist die quadratische Kongruenz $ax^2 + bx + c \equiv 0 \mod m$ lösbar und wann nicht? In diesem Rahmen wird nur der Fall $a = 1$ behandelt (andere Wahl von a ergibt keine schönen Ergebnisse).

1. Gedanke: Mittels des Chinesischen Restsatzes reicht die Betrachtung des Falls $m = p^t,\ p \in \mathbb{P},\ t \in \mathbb{N}_+$ aus.
$p = 2$: Explizite Aussage möglich (Übung). Hier betrachten wir nur $p > 2$. Dann gilt aber ohne Beschränkung der Allgemeinheit $2 \mid b$, denn $\overline{b} = \overline{2}\,\underbrace{(\overline{2}^{-1}b)}_{=:b_0} = 2\overline{b}_0$.

$$x^2 + 2b_0x + c = \underbrace{(x + b_0)^2}_{=:x'} + \underbrace{c - b_0^2}_{=:-k} = x' - k$$

Dann genügt zu zeigen: Wann ist $x^2 \equiv k \mod p^t$ lösbar. $k = p^{v_p(k)}k_0,\ p \nmid k_0$, falls $v_p(k) \geq t \implies$ lösbar mit $x = 0$. Falls $v_p(k) = u < t$: Ansatz $x = p^{v_p(x)}x_0,\ p \nmid x_0$, falls x Lösung ist, dann gilt für ein $c \in \mathbb{Z}$:

$$p^{2v_p(x)}x_0^n = p^k k_0 + cp^t = p^k(\underbrace{k_0 + cp^{t-u}}_{\not\equiv 0 \mod p}),\ t - u > u \implies u = wv_p(x),$$

also $2 \mid u$ und $x_0 \equiv k_0 \mod p^{t-u}$ mit $p \nmid k_0$. Die Umkehrung gilt auch. Ergebnis: Die Kongruenz $x^2 \equiv k \mod p^t$ ist lösbar, wenn $v_p(k) \geq t$, wenn $v_p(k) < t$, so genau dann lösbar, wenn $2 \mid v_p(k)$ und die Kongruenz $x_0^2 \equiv k_0 \mod p^{t-u}$ lösbar ist. Hiernach genügt es, den Fall $x^2 \equiv k \mod p^t$ mit $p \nmid k$ zu behandeln, also $\overline{k} \in G = (\mathbb{Z}/p^t\mathbb{Z})^\times$.

Hilfssatz
Sei $t \in \mathbb{N}_+,\ p \in \mathbb{P},\ p > 2,\ p \nmid k$. Dann gilt:

$$x^2 \equiv k \mod p^t \text{ lösbar} \iff x^2 \equiv k \mod p \text{ lösbar.}$$

Beweis
„$\Longrightarrow$" trivial
„$\Longleftarrow$" Induktion nach t. $t = 1$ ist klar. Sei also $t > 1$ und $x_0 \in \mathbb{Z}$ mit $x_0^2 \equiv k \mod p^{t-1}$. Gesucht x, nötig $x \equiv x_0 \mod p^{t-1}$.
Ansatz: $x = x_0 + cp^{t-1},\ x_0^2 = k + vp^{t-1}\ (c, v \in \mathbb{Z})$.
Idee: Bestimme c, so dass $x^2 \equiv k \mod p^t$.

$$\begin{aligned}
x^2 = \left(x_0 + cp^{t-1}\right)^2 \qquad & = k + vp^{t-1} + 2x_0cpt - 1 + c^2 + \underbrace{p^{2t-2}}_{\equiv 0 \mod p^t} \\
& \stackrel{!}{\equiv} k \mod p^t \\
\iff \quad vp^{t-1} & \equiv -2x_0cp^{t-1} \mod p^t \\
\iff \quad v & \equiv -2x_0c \mod p
\end{aligned}$$

Klappt mit $\bar{c} = \bar{v}(\overline{-2x_0})^{-1}$ in $\mathbb{F}_p$, da $p \nmid x_0$ (wegen $x_0^2 \equiv k \neq 0 \mod p$), $p \nmid 2 \implies \overline{-2x_0} \in \mathbb{F}_p^\times$. ■

Resultat der Diskussion: Frage der Lösbarkeit von quadratischen Kongruenzen lässt sich zurückführen auf die Frage, welche k mit $p \nmid k$ für prime p größer zwei quadratische Reste sind oder nicht. Erinnerung an Eulers Quadratkriterium!

5.2 Grundaussagen über Potenzreste

Bezeichnung

(1) $(G, \cdot)$ abelsche Gruppe, $l \in \mathbb{N}_+ :\ G^{(l)} := \{x^l :\ x \in G\}$, $G^{(l)}$ ist Untergruppe von G (Ist mit Untergruppenkriterium schnell gezeigt).

(2) $k \in \mathbb{Z}$ heißt l-ter *Potenzrest* $\mod m$, $m \in \mathbb{N}_+ \iff k \in ((\mathbb{Z}/m\mathbb{Z})^\times)^{(l)} \iff \mathrm{ggT}(m,k) = 1$ und es existiert $x \in \mathbb{Z}$ mit $x^l \equiv k \mod m$.

Lemma 5.1
$(G, \cdot)$ abelsche Gruppe, $n = \#G < \infty$.
$d := \mathrm{ggT}(n, l)$. Dann ist $G^{(l)} = G^{(d)}$.

Beweis
$x \in G$, $\underbrace{x^l}_{\in G^{(l)}} = \underbrace{x^{\frac{l}{d}d}}_{\in G^{(d)}}$, also ist $G^{(l)} \subset G^{(d)}$. Der LinKom-Satz 1.10 liefert $d = un + vl$ mit $u, v \in \mathbb{Z}$.
$\underbrace{x^d}_{\in G^{(d)}} = \underbrace{x^{nu}}_{=1 (\text{EOS})} x^{lv} = (x^v)^l \in G^{(l)}$, also ist $G^{(d)} \subset G^{(l)}$. Folglich sind beide Mengen gleich. ■

Nächste Frage: Was ist $\#\left(((\mathbb{Z}/p^t\mathbb{Z})^\times)^{(d)}\right)$?

Klar: Falls $G = \langle\zeta\rangle = \left\{1, \zeta, \ldots, \zeta^{m-1}\right\}$ dann $d = \mathrm{ggT}(k, m)$
$G^{(k)} = G^{(d)} = \left\{1, \zeta^d, \zeta^{2d}, \ldots, \zeta^{\left(\frac{m}{d}-1\right)d}\right\}$
$\implies \#G^{(k)} = \#G^{(d)} = \frac{m}{d}$
Ergebnis also

Satz 5.2 (Potenzrestklassenanzahlsatz)

(i) Sei $p \in \mathbb{P}$, $p > 2$, $k, t \in \mathbb{N}_+$. Dann gilt

$$\#\left(\left(\mathbb{Z}/p^t\mathbb{Z}\right)^\times\right)^{(k)} = \frac{\varphi(p^t)}{\mathrm{ggT}(\varphi(p^t), k)}$$

(In Worten: Es gibt genau $\frac{\varphi(p^t)}{\mathrm{ggT}(\varphi(p^t),k)}$ k-te Potenzrestklassen.

(ii) Für $2 \nmid k$ ist $\left(\left(\mathbb{Z}/2^t\mathbb{Z}\right)^\times\right)^{(k)} = \left(\mathbb{Z}/2^t\mathbb{Z}\right)^\times$.
Für $t > 2$ und $2 \mid k$ ist $\left(\left(\mathbb{Z}/2^t\mathbb{Z}\right)^\times\right)^{(k)}$ zyklisch und hat $\frac{2^{t-2}}{\text{ggT}(2^{t-1},k)}$ Elemente.

(iii) (Potenzrestkriterium a la Euler)
Sei $p \in \mathbb{P}$, $p > 2$, $t, k \in \mathbb{N}_+$, $d = \text{ggT}(\varphi(p^t), k)$
r ist k-ter Potenzrest mod $p^t \iff r^{\frac{\varphi(p^t)}{d}} \equiv 1 \bmod p^t$.

Beweis
Beweise (iii) wie Eulerkriterium, benutze primitives Element!

Folge: $p \in \mathbb{P}$, $p > 2 \implies$ Es gibt genau $\frac{p-1}{2}$ quadratische Reste und $\frac{p-1}{2}$ quadratische Nichtreste.
Grund: (i) mit $k = d = 2$, $t = 1$, $\varphi(p) = p - 1$
Bsp: $p = 11$

x	±1	±2	±3	±4	±5	
x^2 mod 11	1	4	9	5	3	$\leftarrow$ quadratische Reste

$\{2, 6, 7, 8, 10\} \leftarrow$ quadratische Nichtreste

5.3 Quadratische Reste und das quadratische Reziprozitätsgesetz

$p \in \mathbb{P}$, $p > 2$

Definition
(1)

$$\begin{aligned} k \text{ quadratischer Rest} \quad \bmod p &\iff \overline{k} \in \left((\mathbb{F}_p)^\times\right)^{(2)} \\ k \text{ quadratischer Nichtrest} \quad \bmod p &\iff \overline{k} \in \mathbb{F}_p^x \setminus \left((\mathbb{F}_p)^\times\right)^{(2)} \end{aligned}$$

(2) Die Frage der Lösbarkeit quadratischer Kongruenzen lässt sich zurückführen auf die Frage, ob k quadratischer Rest ist oder nicht (mod p).

Definition
Sei $p \in \mathbb{P}$, $p > 2$, $u \in \mathbb{Z}$, so sei

$$\left(\frac{u}{p}\right) = \begin{cases} 1 & u \text{ quadratischer Rest} \quad \bmod p \\ -1 & u \text{ quadratischer Nichtrest} \quad \bmod p \\ 0 & \text{sonst, d. h. } p \mid u \end{cases}$$

$\left(\frac{u}{p}\right)$ heißt *Legendre-Symbol.*

Satz 5.3 (Legendre-Symbol-Satz)
Sei $a, b \in \mathbb{Z}$, $p \in \mathbb{P}$, $p > 2$, dann gelten

(i) $a \equiv b \bmod p \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$, und $\left(\frac{a}{p}\right) \in \{0, \pm 1\}$

(ii) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$, insbesondere hat man den Gruppenhomomorphismus

$$\chi_p : \mathbb{F}_p^\times \to \mathbb{C}^\times,\ \chi_p(\overline{a}) = \left(\frac{a}{p}\right) =: \left(\frac{\overline{a}}{p}\right)$$

(Homomorphismen $G \to \mathbb{C}^\times$, G abelsche Gruppe, heißen traditionell <u>Charaktere</u> der Gruppe G, χ_p heißt Dirichlet-Charakter)

(iii) $\left(\frac{ab^2}{p}\right) = \left(\frac{a}{p}\right)$ falls $p \nmid b$.

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

Beweis

(i) Definition.

(iv) Eulerkriterium:

$$\begin{aligned} a \text{ quadratischer Rest} &\iff \overline{a}^{\frac{p-1}{2}} = 1 \text{ in } \mathbb{F}_p \\ a \text{ quadratischer Nichtrest} &\iff \overline{a}^{\frac{p-1}{2}} = -1 \text{ in } \mathbb{F}_p \end{aligned}$$

$p \mid a \iff p \mid a^{\frac{p-1}{2}}$

(ii) $\left(\frac{ab}{p}\right) \overset{\text{(iv)}}{\equiv} (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. Wegen $-\frac{p}{2} < \left(\frac{a}{p}\right) < \frac{p}{2} \implies \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$

(iii) $\left(\frac{ab^2}{p}\right) \overset{\text{(ii)}}{=} \left(\frac{a}{p}\right)\left(\frac{b^2}{p}\right) = \left(\frac{a}{p}\right)\underbrace{\left(\frac{b}{p}\right)^2}_{=1} = \left(\frac{a}{p}\right)$ ∎

Satz gibt Algorithmus zur Berechnung von $\left(\frac{a}{p}\right)$.

Skizze:

(1) $\left(\frac{a}{p}\right) = \left(\frac{a \text{ mods } p}{p}\right) = \left(\frac{r}{p}\right) = \left(\frac{\operatorname{sgn}(r)}{p}\right)\left(\frac{|r|}{p}\right)$

(2) Primzerlegung von $|r| = p_1^{n_1} \cdot \ldots \cdot p_t^{n_t}$
$\left(\frac{2}{p}\right)$ elementar „Ergänzungssatz“
$\left(\frac{q}{p}\right)$ $q \in \mathbb{P}$, $q > 2$, $q \neq p$ geht zurück auf $\left(\frac{p}{q}\right)$ mittels des quadratischen Reziprozitätsgesetzes.

Nämlich:

Legendre: Experimente zeigen unerwartete und „unerklärliche“ Zusammenhänge zwischen $\left(\frac{p}{q}\right)$ und $\left(\frac{q}{p}\right)$. Zum Beispiel $\left(\frac{p}{5}\right) = \left(\frac{5}{p}\right)$ $(\star)$ oder $\left(\frac{p}{7}\right) = -\left(\frac{7}{p}\right)$ und Ähnliche.
$(\star)$ Beweisversuch: Wenn $x \in \mathbb{Z}$ mit $x^2 \equiv 5 \mod p$ $(p \mid x^2 - 5)$ so
konstruiere $y \in \mathbb{Z}$, $y = y(x, 5, p)$ mit $y^2 \equiv p \mod 5$ $(5 \mid y^2 - p)$.
Bis heute eine Formel für so ein y unbekannt!

Der folgende Satz ist der berühmteste Satz der Elementaren Zahlentheorie.

Satz 5.4 (Quadratisches Reziprozitätsgesetz von Gauß)
(i) Es seinen $p, q \in \mathbb{P}$, $p > 2$, $q > 2$, $p \neq q$. Dann gilt

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

(ii) „Ergänzungssätze“ $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1 & p \equiv 1 \mod 4 \\ -1 & p \equiv -1 \mod 4 \end{cases}$

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1 & p \equiv \pm 1 \mod 8 \\ -1 & p \equiv \pm 3 \mod 8 \end{cases}$$

Gauß gab 7 wesentlich verschiedene Beweise, heute 200 bekannt. Kein „Eselsbeweis“ dabei. Heute befriedigender Beweis via „Artins“ Reziprozitätsgesetz.

Artins Hauptsatz der sog. „Klassenkörpertheorie“ stellt eine Isomorphie her zwischen den Automorphismusgruppen („Galoisgruppen“), sog. abelschen Zahlkörper und sog. Strahlklassengruppen (verallg. Restklassengruppen).

Beweis
Hier: Raffinierter Beweis mit endlichen Körpern
In $L = \mathbb{F}_{p^{q-1}}$ existiert $\omega \in L^\times$ mit $\operatorname{ord}(\omega) = q$
Dann ist für $\alpha \in \overline{a}$ in $\mathbb{F}_q$ <u>wohldefiniert</u> $\omega^\alpha := \omega^a$ (Elementordnungssatz)
Fasse $\left(\frac{a}{q}\right) =: \left(\frac{\alpha}{q}\right)$ als Element von L auf $\left(= \begin{matrix} 0_L \\ \pm 1_L \end{matrix}\right)$
Bezeichung $\tau := \sum_{\alpha \in \mathbb{F}_q} \left(\frac{\alpha}{q}\right) \cdot \omega^\alpha$ $(\in L)$ heißt Gaußsche Summe.
$\left[\text{Gauß benutzte statt } \omega\ \zeta = e^{\frac{2\pi i}{q}} \in \mathbb{C} \text{ (ord } \zeta = q \text{ in } \mathbb{C}^\times)\right]$

Formeln a la Gauß $\tau^2 = q \cdot \left(\frac{-1}{q}\right) \cdot 1_L$ (a)

$$\tau^{p-1} = \left(\frac{p}{q}\right) \cdot 1_L \quad \text{(b)}$$

Aus diesen Formeln ergibt sich das Gesetzt mit dem Eulerkriterium
$\left(\frac{q}{p}\right) \equiv q^{\frac{p-1}{2}} \mod p$ (also $\left(\frac{q}{p}\right) \cdot 1_L = q^{\frac{p-1}{2}} \cdot 1_L$)

$$\left(\frac{q}{p}\right) \cdot 1_L = (q \cdot 1_L)^{\frac{p-1}{2}}$$
$$\overset{(a)}{=} \left(\left(\frac{-1}{q}\right)\tau^2\right)^{\frac{p-1}{2}} = \left(\frac{-1}{q}\right)^{\frac{p-1}{2}} \tau^{p-1} \overset{(ii)}{=} (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}} \cdot \tau^{p-1}$$
$$\overset{(b)}{=} (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}} \cdot \left(\frac{p}{q}\right) \cdot 1_L$$
$$\Longrightarrow \left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{q-1}{2}\cdot\frac{p-1}{2}}$$

$\left[\text{Hinweis: } \left(\frac{p}{q}\right) \in \{\pm 1\} \implies \left(\frac{p}{q}\right)^{-1} = \left(\frac{p}{q}\right)\right]$

Details: 1. Man verschaffe sich ω: $L = \mathbb{F}_{p^{q-1}}$ enthält primes Element ζ, ord $\zeta = p^{q-1} - 1$. Bekanntlich $p^{q-1} \equiv 1 \bmod q$ wegen $\overline{p} \in \mathbb{F}_q^x$ (Euler)

$\implies q \mid p^{q-1} - 1 = \operatorname{ord} \zeta$. Setze $\omega = \zeta^{\frac{\operatorname{ord} \zeta}{q}}$

$\implies \operatorname{ord} \omega = q$.

Nachrechnen (b): Verwende: In Körper L mit $\mathbb{F}_p$ Teilkörper ist $(\alpha + \beta)^p = \alpha^p + \beta^p$

$\tau^p = \sum_{\alpha \in \mathbb{F}_q} \underbrace{\left(\frac{\alpha}{p}\right)^p}_{=\left(\frac{\alpha}{q}\right)} \omega^{\alpha p} \qquad \{\alpha p \mid \alpha \in \mathbb{F}_q\} = \mathbb{F}_q$ da $p \in \mathbb{F}_q^x$.

$\left[\text{Summationstransfer: } \beta = \alpha p \implies \left(\frac{\alpha}{q}\right) = \left(\frac{\beta \overline{p}^{-1}}{q}\right) = \left(\frac{\beta}{q}\right)\left(\frac{\overline{p}}{q}\right)^{-1} \text{(da } \chi_q \text{ Homomorphismus)}\right]$

$\implies \tau^p = \sum_{\beta \in \mathbb{F}_q} \underbrace{\left(\frac{\overline{p}}{q}\right)^{-1}}_{\left(\frac{p}{q}\right)} \left(\frac{\beta}{q}\right) \omega^\beta = \left(\frac{p}{q}\right) \sum_{\beta \in \mathbb{F}_q} \left(\frac{\beta}{q}\right) \omega^\beta = \left(\frac{p}{q}\right) \tau$

Wegen $\tau \neq 0$ (folgt aus a) (b) OK.

(a) später

Zu den Ergänzungssätzen

$\left(\frac{-1}{q}\right) \equiv (-1)^{\frac{p-1}{2}} \bmod p$, $-\frac{p}{2} < \left(\frac{-1}{q}\right), (-1)^{\frac{p-1}{2}} < \frac{p}{2}$

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

Demnach	-1 quadratischer Rest mod p	$\iff p \equiv 1 \bmod 4$, also für $p = 5, 13, 17, 23, \ldots$
	-1 quadratischer Nichtrest mod p	$\iff p \equiv -1 \bmod 4$, also für $p = 3, 7, 11, \ldots$

Bsp: $-1 \in \mathbb{F}_{13}$ $5^2 \equiv -1 \bmod 13$ ■

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

$\tau = \sum_{\alpha \in \mathbb{F}_q} \left(\frac{\alpha}{q}\right) \omega^\alpha$, $\operatorname{ord}(\omega) = q$, Gaußsche Summe

Berechnung τ^2:

Sei $\left(\frac{0}{q}\right) = 0,\ \alpha \in \mathbb{F}_q^\times$:

$$\begin{aligned}
\tau^2 &= \sum_{\alpha \in \mathbb{F}_q} \left(\frac{\alpha}{q}\right) \omega^\alpha \cdot \sum_{\beta \in \mathbb{F}_q} \left(\frac{\beta}{q}\right) \omega^\beta \\
&= \sum_{\alpha \in \mathbb{F}_p^\times} \sum_{\beta \in \mathbb{F}_q} \left(\frac{\alpha}{q}\right) \left(\frac{\beta}{q}\right) \omega^{\alpha+\beta}, \qquad (\mathbb{F}_q = \{\underbrace{\alpha+\beta}_{:=\gamma} | \beta \in \mathbb{F}_q) \\
&= \sum_{\alpha \in \mathbb{F}_q^\times} \sum_{\gamma \in \mathbb{F}_q} \left(\frac{\alpha}{q}\right) \left(\frac{\gamma-\alpha}{q}\right) \omega^\gamma \\
&= \sum_{\gamma \in \mathbb{F}_q} \underbrace{\sum_{\alpha \in \mathbb{F}_q^\times} \left(\frac{\alpha}{q}\right) \left(\frac{\gamma-\alpha}{q}\right)}_{=:C_\gamma}
\end{aligned}$$

$\underline{\gamma = 0:}$ $C_0 = \sum_{\alpha \in \mathbb{F}_q^\times} \underbrace{\left(\frac{-\alpha^2}{q}\right)}_{\left(\frac{-1}{q}\right)} = (q-1)\left(\frac{-1}{q}\right) \cdot 1_L$

$\underline{\gamma \neq 0:}$ $\left(\frac{\alpha}{q}\right)\left(\frac{\gamma-\alpha}{q}\right) = \underbrace{\left(\frac{\alpha}{q}\right)\left(\frac{\alpha}{q}\right)}_{=1} \left(\frac{\gamma\alpha^{-1}-1}{q}\right)$

$$\begin{aligned}
C_\gamma &= \sum_{\alpha \in \mathbb{F}_q^\times} \left(\frac{\gamma\alpha^{-1}-1}{q}\right) \\
&\left[X := \{\gamma\alpha^{-1} | \underbrace{\alpha \in \mathbb{F}_q^\times,\ \alpha \neq \gamma}_{q-2\ \alpha\text{'s}}\} \subseteq \mathbb{F}_q^\times \implies \#X = q-2,\ -1 \notin X \implies X = \mathbb{F}_q^\times \setminus \{-1\} \right] \\
&= \sum_{\sigma \in \mathbb{F}_q^\times \setminus \{-1\}} (\frac{\sigma}{q}) \\
&= \underbrace{\sum_{\sigma \in \mathbb{F}_q^\times} (\frac{\sigma}{q})}_{\substack{= \left(\frac{q-1}{2}\right) \cdot 1 - (\frac{q-1}{2}) \\ \text{(da gleich viele quadratische} \\ \text{Reste wie Nichtreste)}}} - \left(\frac{-1}{q}\right) \\
&= -\left(\frac{-1}{q}\right)
\end{aligned}$$

$$\begin{aligned}\tau^2 &= \sum_{\gamma\in\mathbb{F}_q} C_\gamma \omega^\gamma \\ &=(q-1)\left(\frac{-1}{q}\right)\cdot 1_L + \sum_{\gamma\in\mathbb{F}_q^\times} -\left(\frac{-1}{q}\right)\omega^\gamma \\ &=(q-1)\left(\frac{-1}{q}\right)\cdot 1_L - (\frac{-1}{q})\sum_{j=0}^{q-1}\omega^j + \underbrace{\left(\frac{-1}{q}\right)}_{\text{Kompensiert } j=0} \\ &=q\left(\frac{-1}{q}\right)\cdot 1_L - \underbrace{\left(\frac{-1}{q}\right)\frac{\omega^q-1}{\omega-1}}_{=0, q=\mathrm{ord}(\omega),\text{ da } \omega^q=1}\end{aligned}$$

Ergebnis: $\tau^2 = q\left(\frac{-1}{q}\right)\dot{1}_L$ (a)
Ergänzungssatz $\left(\frac{2}{q}\right)$: Übung

Anwendung der Eulerformel und des quadratischen Reziprozitätsgesetzes Hiervon gibt es viele. Hier über $\mathbb{F}_n$.
Euler: $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \mod p, p > 2, p \nmid a \implies \overline{a}^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)$ in $\mathbb{F}_p$
$\left(\frac{a}{p}\right) = -1 \implies \mathrm{ord}(\overline{a}) \nmid \frac{p-1}{2}$, immer $\mathrm{ord}(\overline{a}) \mid p-1$
Also: $v_2(\mathrm{ord}(\overline{a})) = v_2(p-1)$
Sagt am Meisten, wenn $p-1 = 2^k, k > 0$. Dann $\mathrm{ord}(\overline{a}) \mid 2^k, \mathrm{ord}(\overline{a}) \nmid 2^{k-1} \implies \mathrm{ord}(\overline{a}) = p-1 = 2^k \implies \overline{a}$ ist primitiv.

Falls $2^k + 1 = p \in \mathbb{P}$, so ist a Primitivwurzel $\iff (\frac{a}{p}) = -1 (p \in \mathbb{P} \implies k = 2^n, n \in \mathbb{N}_+, p = F_n = 2^{2^n} + 1$ n-te Fermatzahl (1. Übungsblatt).

Falls das so ist, so ist 3 eine Primitivwurzel $\mod p$.
Berechne $(\frac{3}{p})$. $p = 2^k + 1 \equiv 1 \mod 4 (k \geq 2) \implies (-1)^{\frac{p-1}{2}} = 1 \implies (\frac{3}{p})(\frac{p}{3}) = (-1)^{\frac{2}{2}\cdot\frac{p-1}{2}} = 1 \implies (\frac{3}{p}) = (\frac{p}{3})$ (quadratisches Reziprozitätsgesetz!)
Berechne $p \mod 3$. $p = F_n = 2^{2^n} + 1, n \geq 1$. (Folgende Äquivalenz stimmt wohl nicht ganz, bitte überprüft das jemand) $2 \equiv -1 \mod 3, p \equiv (-1)^{2^n} + 1 \equiv 1 + 1 \equiv -1 \mod 3 \implies \left(\frac{3}{p}\right) = (\frac{p}{3}) = (\frac{-1}{3})$

Satz 5.5 (Fermat-Zahl-Satz)
(1) Sei $k \in \mathbb{N}_+, p = 2^k + 1$. Dann gilt $p \in \mathbb{P} \implies k = 2^n (n \in \mathbb{N}) \implies p = F_n = 2^{2^n} + 1$
(2) Ist $p = F_n \in \mathbb{P}, a \in \mathbb{Z}, p \nmid a, n \geq 1$, so gilt: a Primitivwurzel $\mod a \iff (\frac{a}{p}) = -1$. Trifft zu auf $a = 3$
(3) Pepins-Test: Sei $n \in \mathbb{N}_+$. Dann gilt: $F_n = 2^{2^n} + 1 \in \mathbb{P} \iff 3^{2^{(2^n-1)}} \equiv -1 \mod F_n$

Beweis
(1) ✓

(2) ✓

(3) „$\Longrightarrow$“: $F_n = p \in \mathbb{P} \implies 3$ Primitivwurzel $\mod p$, $\mathrm{ord}(\overline{3}) \mid p-1 = 2^{2^n} \implies \overline{3}^{2^{2^n-1}} = \overline{3}^{\frac{2^{2^n}}{2}} = \pm 1$. Bei $+1$ keine Primitivwurzel.
„$\Longleftarrow$“: Sei $p \in \mathbb{P}, p \mid F_n = 2^{2^n}+1$. $3^{2^{2^n-1}} \equiv -1 \mod F_n \implies 3^{2^{2^n-1}} \equiv -1 \mod p, 3^{2^{2^n}} \equiv 1 \mod F_n \implies 3^{2^{2^n}} \equiv 1 \mod p$. $F_n - 1 = \mathrm{ord}(\overline{3}) = 2^{2^n} \leq p-1$ ($\mathrm{ord}(\overline{3})$ in $\mathbb{F}_p$ teilt $\#\mathbb{F}_p^\times = p-1$) ∎

5.3.1 Jacobi-Symbol

Definition
Sei $a \in \mathbb{Z},\ m \in \mathbb{N}_+,\ 2 \nmid n,\ \mathrm{ggT}(a,m) = 1$ $(\star)$. Definiere in diesem Fall das Jacobi-Symbol $\left(\frac{a}{m}\right)$ durch:

$$\left(\frac{a}{m}\right) = \prod_{\substack{p \in \mathbb{P} \\ p \mid m}} \left(\frac{a}{p}\right)_L^{v_p(m)},$$

andernfalls ist $\left(\frac{a}{m}\right)$ nicht definiert. Hierbei ist $\left(\frac{a}{p}\right)_L$ das Legendre-Symbol.

Klar:

$\left(\frac{a}{1}\right) = \left(\frac{1}{m}\right) = 1$

$m \in \mathbb{P}, m > 2$, so ist Jacobi $\left(\frac{a}{m}\right) =$ Legendre $\left(\frac{a}{m}\right)$

Satz 5.6 (Jacobi-Symbolsatz)
Falls $a, a' \in \mathbb{Z}, m, m' \in \mathbb{Z}$, so gelten, falls die vorhandenen Jacobi-Symbole definiert sind:

(i) $a \equiv b \mod m \implies \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$

(ii) $\left(\frac{aa'}{m}\right) = \left(\frac{a}{m}\right)\left(\frac{a'}{m}\right),\ \left(\frac{a}{mm'}\right) = \left(\frac{a}{m}\right)\left(\frac{a}{m'}\right)$

(iii) $\left(\frac{a}{m}\right)\left(\frac{m}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{m-1}{2}}$ (Reziprozitätsgesetz)

(iv) $\left(\frac{-1}{m}\right) = (-1)^{\frac{m-1}{2}}, \left(\frac{2}{m}\right) = (-1)^{\frac{m-1}{8}}$ (Ergänzungssätze)

Algorithmus-Skizze zur Berechnung von $\left(\frac{a}{m}\right)$

0. $m = 1 : \left(\frac{a}{m}\right) = \left(\frac{a}{1}\right) = 1$
1. $m > 1, 2 \nmid m, \left(\frac{a}{m}\right) = \left(\frac{r}{m}\right)$ mit $r = a$ mods m (also $|r| < \frac{m}{2}$)
2. Stelle r dar als $r = \mathrm{sign}(r) 2^{v_2(r)} r_0$ (also $r_0 > 0, 2 \nmid r_0, |r| < \frac{m}{2}$)
   Rechenaufwand minimal!

$$\left(\frac{r}{m}\right) = \underbrace{\left(\frac{\operatorname{sign}(r)}{m}\right)\left(\frac{2}{m}\right)^{v_2(r)}}_{=:\Upsilon}\left(\frac{r_0}{m}\right)$$

Rechenaufwand für Υ ist ebenfalls minimal.

3. $\left(\frac{r_0}{m}\right) = \left(\frac{m}{r_0}\right)(-1)^{\frac{r_0-1}{2}\cdot\frac{m-1}{2}}$, wende Verfahren auf $\left(\frac{m}{r_0}\right)$ an. Problem reduziert von m auf r_0 mit $0 < r_0 < \frac{m}{2}$. Schleife wird ca. $\log_2 m$ mal durchlaufen.
! Primzerlegung kommt nirgends vor **!**

Bemerkung Aus $\left(\frac{a}{m}\right) = 1$ folgt <u>nicht</u>, dass a quadratischer Rest $\mod m$ ist.

Beispiel
$\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$. 2 ist quadratischer Nichtrest $\mod 3$ und erst recht quadratischer Nichtrest von $\mod 15$

Beweis (Jacobi-Symbolsatz 5.6)

(i) $p \mid m, p \in \mathbb{P}, a \equiv b \mod m \implies a \equiv b \mod p \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) \implies \left(\frac{a}{m}\right) = \left(\frac{b}{m}\right)$

(ii) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$ (Legendre Symbol) $\implies \left(\frac{a}{m}\right)\left(\frac{b}{m}\right) = \left(\frac{ab}{m}\right)$
$\left(\frac{a}{mm'}\right) = \prod_{p\in\mathbb{P}}\left(\frac{a}{p}\right)^{v_p(mm')} = \prod_{p\in\mathbb{P}}\left(\frac{a}{p}\right)^{v_p(m)+v_p(m')} = \prod_{p\in\mathbb{P}}\left(\left(\frac{a}{p}\right)^{v_p(m)}\left(\frac{a}{p}\right)^{v_p(m')}\right) =$
$\prod_{p\in\mathbb{P}}\left(\frac{a}{p}\right)^{v_p(m)} \cdot \prod_{p\in\mathbb{P}}\left(\frac{a}{b}\right)^{v_p(m')} = \left(\frac{a}{m}\right)\left(\frac{a}{m'}\right)$

(iii) $\left(\frac{a}{m}\right)\left(\frac{m}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{m-1}{2}}$ klar für $m = 1$ oder $a = 1$. Also $m > 1, a > 1$ voraussetzbar. $2 \nmid m, 2 \nmid a$.
Falls $m \in \mathbb{P}$ und $a \in \mathbb{P}(\operatorname{ggT}(m,n) = 1)$, so steht das quadratische Reziprozitätsgesetz für das Legendre Symbol da.
Also nur noch zu beweisen, wenn a oder $m \notin \mathbb{P}$ etwa $m = uv,\ 1 < v < m$.
Induktion nach a, m:
Induktionhypothese: $\left(\frac{a}{u}\right)\left(\frac{u}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{u-1}{2}}$, $\left(\frac{a}{v}\right)\left(\frac{v}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{v-1}{2}}$
$\left(\frac{a}{uv}\right)\left(\frac{uv}{a}\right) \overset{(ii)}{=} \left(\frac{a}{u}\right)\left(\frac{a}{v}\right)\left(\frac{u}{a}\right)\left(\frac{v}{a}\right) \overset{\text{I.H.}}{=} (-1)^{\frac{a-1}{2}\cdot\frac{u-1}{2}}(-1)^{\frac{a-1}{2}\cdot\frac{v-1}{2}} \overset{?}{=} (-1)^{\frac{a-1}{2}\cdot\frac{uv-1}{2}}$
Genügt: $n-1+v-1 = uv-1 \mod 4$. Das stimmt, weil $2 \nmid u, 2 \nmid v$ und $u, v \equiv \pm 1 \mod 4$

(iv) Ähnliche Induktion ■

6 Primzahltests

Ein Primzahltest ist ein Algorithmus $Prim(m)$, der zu $m \in \mathbb{N}_+$ entscheidet, ob $m \in \mathbb{P} \vee m \notin \mathbb{P}$.

Einteilung der Tests ($\neg$disjunkt):

a) + Allgemeiner Test ($\forall m \in \mathbb{N}$)

- Spezieller Test (nur gewisse $m \in \mathbb{N}$)

b) + Voll bewiesener Test

- Test abhängig von einer Vermutung (zB Riemann-Vermutung)

c) + Sicherer Test

- Propabilistischer Test (Monte-Carlo-Methode)

d) + Praktikabler Test (geht für „große“ m)

- Unpraktischer Test

Beispiel

a) Pepins Test: nur für $F_n = 2^{2^n} + 1$

d) Naiver Test: Probiere $a \mid m, \forall a \in \mathbb{N}, 1 < a \leq \sqrt{m}$

d) Wilsons Test: $m \in \mathbb{P} \Leftrightarrow (m-1)! \equiv -1 \mod m$, es sind mindestens m „Aktionen“ nötig

Beweis (Wilsons Test)

„$\Rightarrow$“: $m = p \in \mathbb{P}$. In $\mathbb{F}_p$:
$(m-1)! = \prod_{\alpha \in \mathbb{F}_p^\times} \alpha = \overline{1} \cdot (\overline{-1})$. Paare $\alpha\alpha^{-1}$ heben sich weg. Wenn $\alpha \neq \alpha^{-1}$ verbleibt $\alpha^2 = 1$, da $\alpha = \pm 1 \Rightarrow (m-1)! \equiv -1 \mod m$

„$\Leftarrow$“: $m \notin \mathbb{P} \Rightarrow \text{ggT}((m-1)!, m) = d > 1 \Rightarrow (m-1)! \not\equiv 1 \mod m$ (sonst $d \mid -1$) ∎

Prinzip moderner PZTests:
Meist ohne Einschränkung $m > 2, 2 \nmid m$. (Rechnung für große m aufwändig, daher gewöhnlich erst $p \mid m$ probiert für die $p \in \mathbb{P}$, etwa $p \leq 100000 \vee p \leq 1000000$.). Man konstruiert Gruppe G_m derart, dass die Struktur von G_m für $m \in \mathbb{P} \wedge m \notin \mathbb{P}$ verschieden ausfällt. Die Strukturverschiedenheit soll mit möglichst wenig und schnellen Rechnungen festgestellt werden.
EZT: Meist $G_m = (\mathbb{Z}/m\mathbb{Z})^\times$
Höhere ZT: Etwa $G_m = (\sigma_k / \sigma_k \cdot m)^\times$, webei σ_k ein Ring „ganzer algebraischer Zahlen „ im algebraischen Zahlenkörper K ist.

Beispiel

$K = \mathbb{Q} + \mathbb{Q}i, \sigma_k = \mathbb{Z} + \mathbb{Z}i$ (Ring der ganzen Gaußschen Zahlen)
Algebraische Geometrie: G_r konstruiert aus „elliptischer Kruve“, die über $\mathbb{Z}$ definiert ist. Vorzug:

Es gibt ∞ viele elliptische Kurven und Zahlenkörper. Man kann versuchen, möglichst „geeignete“ zu finden. Hier $G_m = (\mathbb{Z}/m\mathbb{Z})^\times$.

(A) Ein $\neg$ganz geklückter Versuch
Strukturaussage für $G_p (p \in \mathbb{P})$:
Satz von Euler-Fermat: $\overline{a}^{p-1} = 1$.

Definition
Sei ohne Einschränkung $m > 2, 2 \nmid m$. $a \in \mathbb{Z}$ heiße Carmichael-Zeuge (für die Zerlegbarkeit von m), wenn gilt:

(i) $\mathrm{ggT}(a, m) = 1$

(ii) $a^{m-1} \not\equiv 1 \mod m$

Klar: Wenn Zeuge gefunden: $m \notin \mathbb{P}$.
Leider: $\exists m \in \mathbb{N}$ mit $m \notin \mathbb{P}$, aber kein Zeuge vorhanden!

Definition
Solche $m \notin \mathbb{P}$ (also die mit $\forall a \in \mathbb{Z}, 1 < a < m, \mathrm{ggT}(a, m) = 1$ ist $a^{m-1} \equiv 1 \mod m$) heißen Carmichael Zahlen.

Satz 6.1 (Carcmichael, $\sim$ 1920)
Sei $m \in \mathbb{N}_+, m > 2, \mathbb{P}_m := \{p \in \mathbb{P} \big| p \mid m\}$. Dann: m ist Carmichael Zahl $\Leftrightarrow$ Es gelten:

(i) $2 \nmid m$

(ii) m ist qf (???) ($\forall p \in \mathbb{P} : v_p(m) \leq 1$)

(iii) $\forall p \in \mathbb{P}_m : p - 1 \big| m - 1$

(iv) m hat mindestens 3 verschiedene Primteiler ($\#\mathbb{P}_m \geq 3$)

Beispiel
Kleinste Carmichael-Zahl: $m = 561 = 3 \cdot 11 \cdot 17$ - $2, 10, 16 \mid 560$

Beweis
„$\Leftarrow$“: $\left.\begin{matrix} \text{Zeige } (i) - (iv) \\ \mathrm{ggT}(a, m) = 1 \end{matrix}\right\} \Rightarrow a^{m-1} \equiv 1 \mod m.$

$\forall p \in \mathbb{P}_m$: in $\mathbb{F}_p^\times$: $\mathrm{ord}\,\overline{a} \mid p - 1 \overset{(iii)}{\mid} m - 1 \Rightarrow \overline{a}^{m-1} = 1$ in $\mathbb{F}_p \Leftrightarrow a^{m-1} \equiv 1 \mod p \Leftrightarrow p \mid a^{m-1} - 1 \overset{(ii) qf}{\Rightarrow} m = \prod_{p \in \mathbb{P}_m} p \mid a^{m-1} - 1 \Rightarrow a^{m-1} \equiv 1 \mod m$

„$\Rightarrow$“: (-1) kein Zeuge $\Rightarrow (-1)^{m-1} \equiv 1 \mod m$. Falls $2 \mid m \Rightarrow -1 \equiv 1 \mod m \Rightarrow m = 1, 2$ (Widerspruch!). Also $2 \nmid m \rightsquigarrow (i)$.
Zu (ii), (iii):
Für $p \in \mathbb{P}_m$ ist $t := v_p(m) \geq 1. \exists PW a \mod p$ mit $\mathrm{ggT}(a, m) = 1$ (Sei w PW $\mod p$, lose das System $a \equiv w \mod p (ChRS), a \equiv 1 \mod q (q \in \mathbb{P}, q \neq p)$. $\Rightarrow q \nmid a, p \nmid a \Rightarrow \mathrm{ggT}(a, m) = 1$)
In $(\mathbb{Z}/p^t\mathbb{Z})^\times$ ist $\overline{a}^{m-1} = 1$ (wegen $a^{m-1} \equiv 1 \mod m \Rightarrow a^{m-1} \equiv 1 \mod p^t$) $\Rightarrow \mathrm{ord}\,\overline{a} = \phi(p^t) = p^{t-1}(p-1) \mid m - 1 \Rightarrow p - 1 \mid m - 1 \rightsquigarrow (iii)$

Wäre $t > 1 \Rightarrow p \mid m-1$ (Wiederspruch zu $p \mid m$).
Also $v_p(m) = 1 \rightsquigarrow$ (ii)
Noch zu widerlegen: $\mathbb{P}_m = \{p, q\}, p \neq q$, etwa $2 < p < q(\star)$
$m = pq$ laut (ii), $q - 1 \overset{(iii)}{\mid} m - 1 = pq - 1 = p(q-1) + p - 1 \Rightarrow q - 1 \mid q - 1 \Rightarrow q \leq p$
(Widerspruch ($\star$)) ∎

(B) Ein geglückter Versucht
$m \in \mathbb{N}, m > 2, 2 \nmid m$. Schreibe $m - 1 = 2^t \cdot u$ mit $t = v_2(m-1)$ also $2 \nmid u, t > 0$.

Definition
$a \in \mathbb{N}$ heiße Miller-Zeuge (für die Zerlegbarkeit von m), wenn gilt:

(i) $\mathrm{ggT}(a, m) = 1$

(ii) $a^u \not\equiv 1 \mod m$

(iii) $\forall s \in \{0, ..., t-1\} : a^{u\dot{2}^s} \not\equiv -1 \mod m$

Satz 6.2
Miller-Rabin-PZTest Sei $m \in \mathbb{N}, m > 2, 2 \nmid m$. Dann: $m \notin \mathbb{P} \Leftrightarrow \exists$ Miller-Zeuge a. $(0 < a < m)$

Zusatz (Rabin): Es gibt dann höchstens $\frac{3}{4}\phi(m) \leq \frac{3}{4}(m-1)$ ¬Zeugen
$\rightsquigarrow$ Liefert voll bewiesenen Test:
Test, ob $\frac{1}{4}(m-1) + 1$ as Zeugen sind.
Sobald Zeugen gefunden $\Rightarrow m \notin \mathbb{P}$.
Kein Zeuge gefunden $\Rightarrow m \in \mathbb{P}$.
Aber immer noch unpraktisch (ca $\frac{1}{4}m$ Aktionen). Es gibt einen sehr praktischen propabilistischen Test:
Teste, ob k zufällig ausgewählte Restklassen $\overline{a}$ $(1 < a < m)$ Zeuge sind (falls $\mathrm{ggT}(a, m) = d > 1$, so $m \notin \mathbb{P}$, sonst $\mathrm{ggT}(a, m) = 1$). Falls Zeuge gefunden $\Rightarrow m \notin \mathbb{P}$. Falls kein Zeuge gefunden: Die WK (???), dass man sich mit der Annahme „m ist prim“ irrt, ist $< \frac{1}{4^k}$.
Für große m scheint die WK sogar viel kleiner als $\frac{1}{4^k}$. [experiment. Faktoren]

$m <$	Zeuge, falls $m \notin \mathbb{P}$
2047	2
1373653	$2 \vee 3$
3215031753	$2, 3 \vee 5$

Beweis

„$\Leftarrow$“: $m = p \in \mathbb{P}, \overline{a} \in \mathbb{F}_p^\times$
$ord\overline{a} \mid \phi(p) = p - 1 = 2^t\dot{u}$
$ord\overline{a} = 2^s \cdot v, 2 \nmid v, s \leq t, v \mid u$

1. Fall: $s = 0 \Rightarrow \overline{a}^v = 1 \Rightarrow \overline{a}^u = 1 \Rightarrow a^u \equiv 1 \mod p$, kein Zeuge

2. Fall: $s > 0 \Rightarrow \overline{a}^{2^s\dot{v}} = 1, \overline{a}^{2^{s-1}\dot{v}} \equiv -1 \mod m$, $s \in \{0, ..., t-1\} \Rightarrow$ kein Zeuge ∎

Weiter bei der letzten Vorlesung:

$m-1=2^t u, 2 \nmid u$
Millerzeuge a: $\mathrm{ggT}(a,m)=1, a^u \not\equiv 1 \mod m$
$\forall s=0,...,t-1 : a^{u2^s} \not\equiv 1 \mod m$

Rest:
$m \notin \mathbb{P} \Rightarrow \exists$ Millerzeuge

Fall I: $\#\mathbb{P}_m \geq 2, \mathbb{P}_m = \{p_1,...,p_l\}$
$a \equiv -1 \mod p_1$
$a \equiv 1 \mod p_j (j>1)$
(mit Chinesischem Restsatz lösen)
$a^u \equiv (-1)^u \equiv -1 \mod p_1$, also ist $a^u \equiv 1 \mod m$ falsch (sonst $-1 \equiv 1 \mod p_2 \Rightarrow p_1 = 2$ [Widerspruch!]), also $a^u \not\equiv 1 \mod m$
$a^{u2^s} \equiv 1^{u2^s} \equiv 1 \mod p_j (j>1) \Rightarrow a^{u2^s} \equiv -1 \mod m$ ist falsch, also $a^{u2^s} \not\equiv 1 \mod m$
Gesehen: a ist Millerzeuge

Fall II: $m = p^t, p \in \mathbb{P}, t > 1$: ist a Primitivwurzel $\mod m = p^t$, so ist a Millerzeuge.
$ord(\overline{a}) = \phi(p^t) = (p-1)p^{t-1}$

- $\Rightarrow \overline{a}^u \neq 1$, weil sonst $ord(\overline{a}) \mid u \Rightarrow p \mid u \mid m-1$ (Widerspruch zu $p \mid m$)
- $\Rightarrow \overline{a}^{u2^s} = -1 \Rightarrow \overline{a}^{us^{s+1}} = 1 \Rightarrow ord(\overline{a}) = (p-1)p^{t-1} \mid u2^{s+1} \Rightarrow p \mid u \mid m-1$ (Widerspruch!) $\Rightarrow a^{u2^s} \equiv -1 \mod m$

Stand der Technik:

1.) Primzahlen $< 10^{130}$ mit guter Sicherheit „leicht“ auffindbar, z.B. mit Miller Rabin

2.) Zahlen der Größe $> 10^{130}$, erstrecht $m = pq, p, q \geq 10^{130}$ können nicht faktorisiert werden.

Praktischer Test von Rumely, fast in Polynomial-Zeit, vorhanden (Zeit $\approx \log(m)^{c \log\log\log m}$). Falls die verallgemeinterte Riemann-Vermutung gilt, so ist dieser Test sogar in Polynomial-Zeit.

Kayal, Saxena, Aal 2002: Voll bewiesener Primzahltest in Polynomial-Zeit. Fraglich ob dies ein praktischer Test ist.

Faktorisierung großer Nichtprimzahlen schein ein viel härteres Problem zu sein.

Idee von Fermat:
$\mathbb{N}_+ \ni m = x^2 - y^2, x, y \in \mathbb{N}, m = (x-y)(x+y), x \geq y$ ist Faktorisierung, wenn $x - y \neq 1.m, x-y = 1$ und $x+y \neq m.1, x+y = m \Rightarrow x = \frac{m+1}{2}, y = \frac{m-1}{2}$ also echte Teiler, wenn $x, y \neq \frac{m\pm1}{2}$

Viele moderne Tests arbeiten so: Suche $x, y \in \mathbb{N}$ mit $x^2 \equiv y^2 \mod m, x \not\equiv \pm y \mod m$

Gute Chance, dass $\mathrm{ggT}(m, x-y)$ oder $\mathrm{ggT}(m, x+y)$ echter Teiler von m ist. Sehr viel Test, um die Suche nach solchen x, y zu beschleunigen: Siehe z.B. Förster, Algorithmic number theory

6.1 Anwendung der EZT in der Kryptographie

Rivests öffentliches Chiffrier System. m große Zahl.
Nachricht ist hier $N \in \mathrm{Versys}_m^\times = \{a \in \mathbb{N} \big| 0 < a < m, \geq (a,m) = 1\}$ (Falls $m = p_1^{n_1} \cdot \ldots \cdot p_l^{n_l}, p1 < \ldots < p_l \in \mathbb{P}, n_j \in \mathbb{N}_+$, so sind alle $N \in \mathbb{N}$ mit $1 \leq N < p_1$ im Versys_m. N kodiert Textabschnitt mit k Zeichen, z.B. Leerstelle $=$ 000, Jedes Zeichen erhält Ziffern < 1000.

Beispiel

$$N = \begin{array}{cccccccccc} \mathrm{K} & \mathrm{O} & \mathrm{M} & \mathrm{M} & & \mathrm{N} & \mathrm{I} & \mathrm{C} & \mathrm{H} & \mathrm{T} & \\ 011 & 015 & 013 & 013 & 000 & 014 & 009 & 003 & 008 & 020 & < 10^{3k} \end{array}$$

Definition

(i) Eine Chiffre ist (für uns) eine bijektive Abbildung $P : \mathrm{Versys}_m^\times \to \mathrm{Versys}_m^\times, N' = P(N)$ ist die „chriffrierte“ Nachricht.

(ii) ein „öffentliches Chiffresystem“ ist eine Liste („öffentliches Adressbuch“):
$(T, P_T), T \in \tau =$ Menge von Teilnehmern. P_T Chiffre, derart, dass $T \neq T' \Rightarrow P_T \neq P_{T'}$

(a) Jeder Teilnehmer $T \in \tau$ erhaält das Adressbuch $(T, P_T)_{T \in \tau}$

(b) T und nur T erhält P_T^{-1} (Umkehrabbildung von P_T)
Praktisch: T muss P_T^{-1} besonders gut sichern, gegen Diebstahl, Ausspähen, Hacker, usw.

Technische Anforderungen:

1.) $P_T(N), P_T^{-1}(N)$ müssen in vernüftiger Realzeit berechenbar sein

2.) Nicht einmal ein Supercomputer kann P_T^{-1} aus P_T ermitteln (P_T *Trapdoor*-Funktion)

3.) Nur T hat P_T^{-1}. Der Systemadministrator hat am Anfang die P_T's und die P_T^{-1}'s. Nach Absenden von P_T^{-1} an T vernichtet er P_T^{-1}

Anwendungen:

I) Geheime Nachricht über öffentlich zugängliche Kanäle (etwa Internet) übermitteln T von A zu B, $A, B \in \tau$ ohne das Unbefugte N gewinnen können.
Methode: A berechnet $P(N) = N'$ und sendet N' an B. Nur B kann aus N' wieder $N = P_B^{-1}(N')$ ermitteln.
Beispiel:

- A Spion des Geheimdienstes, $B = =$ Geheimdienstzentrale, C, D die gegnerischen Geheimdienste
- A ist Bank, B ist Kunde, $N =$ Kontostand

II) Geheimnachricht mit elektronischer Unterschrift
Methode: A sendet an B: „$N = P_B P_A^{-1}(N)$, Gruß A“. Nur A kann N' herstellen, nur B kann daraus $N = P_A P_B^{-1}(N')$ gewinnen.

Beispiel:
$A =$ Kunde, $B =$ Bank, $N =$ „Überweisen Sie 200'000.- von meinem Konto an C"

III) Sichere Speicherung von Nachrichten
Methode: Speichere $N' = P_{A_t}^{-1}(N)...P_{A_1}^{-1}(N)$. Benötigt werden $A_1, ..., A_t \in \tau(t = 1)$. Nur mit Willen von allen Mitwirkenden $A_1, ..., A_t$ kann N aus N' wieder rekonstruiert werden.

EZT kann z.B. zum Erfüllen der technischen Vorraussetzungen verwendet werden.
Rivests Vorschlag $\subseteq$ RSA-Code (Rinest, Shamn, Adleman 1978)
Adressbuch: Liste$(T, m_T, s_T), m_T, s_T \in \mathbb{N}, m_T = p_1^{n_1}...p_l^{n_l}, p_i$ zu Anfang dem Administrator bekannt, öffentlich nur m_T's, s_T's ziemlich groß.
Chiffre $P_T(N) := (N^{s_T} \mod m_i)$. Dann theoretisch $P_T^{-1}(N') = N'^{t_T}$, wobei $t_T s_T \equiv 1 \mod \phi(N)$ (Euler Funktion). Hiermit erhält T auch noch t_T. t_T ist nur berechenbar, wenn $\phi(m) = m \prod_{p|m}(1-\frac{1}{p})$ bekannt, dass geht nur (nach heutigem Wissen), wenn Primzerlegung, also die p_i bekannt sind.

7 Ganzzahlige lineare Gleichungen und Moduln über euklidischen Ringen

7.1 Der Elementarteileralgorithmus

7.1.1 Matrizen über euklidischen Ringen

Sei (R, gr) ein Euklidischer Ring.

Definition

(i) $GL_n(R) = (R^{n\times n})$ heißt *allgemeine lineare Gruppe* über R (GL = general linear)

(ii) $1_n := 1_{GL_n(R)}$ ($n \times n$-Einheitsmatrix)

Lemma 7.1
$GL_n(R) = \{U \in R^{n\times n} \big| \det U \in R^\times\}$
(falls $R = \mathbb{Z}, U \in GL_n(\mathbb{Z}) \Leftrightarrow U \in \mathbb{Z}^{n\times n}, \det U = \pm 1$)

Beweis

(i) $U \in (R^{n\times n})^\times \Leftrightarrow \exists V \in R^{n\times n}, VU = UV = 1_n \Rightarrow 1 = \det 1_n = \det(UV) = \underbrace{\det U}_{\in R} \cdot \underbrace{\det V}_{\in R} \Rightarrow$ $\det U \in R^\times$

(ii) Sei $U \in R^{n\times n}, \det U \in R^\times$. In LA I zeigt man für die Adjungierte $U^\#$ von U: $UU^\# = U^\# U = \det U \cdot 1_n$
$U^\#$ wird aus $\det W$ gewonnen, wo W Untermatrizen von U sind, also $\det W \in R \Rightarrow U^\# \in R^{n\times n}, \det U \in R^\times \Rightarrow U^{-1} = \frac{1}{\det U} U^\# \in R^{n\times n} \Rightarrow U \in (R^{n\times n})^\times$ ■

Definition
$B = (b_{ij}) \in R^{m\times n}$, so sei $\mathrm{ggT}(B) := \mathrm{ggT}(b_{ij})$ ($i = 1, ..., m$ und $j = 1, ..., n$)

Lemma 7.2
$A \in R^{l\times m}, B \in R^{m\times n}$. Dann gilt:

(i) $\mathrm{ggT}(A) \mid \mathrm{ggT}(AB), \mathrm{ggT}(B) \mid \mathrm{ggT}(AB)$

(ii) $U \in GL_m(R), V \in GL_n(R)$, so ist $\mathrm{ggT}(UBV) = \mathrm{ggT}(B)$

Beweis

(i) $A = (a_{ij}), B = (b_{kl}), d = \text{ggT}(A) \Rightarrow a_{ij} = d \cdot a'_{ij}, a'_{ij} \in R$. $AB = C = (c_{rs}), c_{rs} = \sum_{j=1}^{m} d_{rj} b_{js} = d \cdot \sum_j a'_{ij} \cdot b_{js} \Rightarrow \forall r, s : d \mid c_{rs} \Rightarrow d \mid \text{ggT}(C) = \text{ggT}(c_{rs} \big| r, s)$.
$\text{ggT}(B) = \text{ggT}(AB)$ genau so.

(ii) $\text{ggT}(B) \mid \text{ggT}(UB) \mid \text{ggT}(U^{-1}(UB)) = \text{ggT}(B) \Rightarrow \text{ggT}(B) = \text{ggT}(UB)$.
$\text{ggT}(UB) = \text{ggT}((UB)V)$ genau so ∎

Spezielle Matrizen:
E_{ij} „Matrizeneinheiten“, $E_{ij,kl} = \delta_{ik}\delta jl$. Es steht in der i-ten Zeile und der j-ten Spalte eine 1.

Beispiel: $\begin{pmatrix} 0 & & & 0 \\ & \ddots & 1 & \\ & & \ddots & \\ 0 & & & 0 \end{pmatrix}$

Elementarmatrizen sollen folgende Matrizen genannt werden (in $R^{n\times n}$):

1.) *Additionsmatriizen*: $A_{ij}(b) = \underbrace{1_n}_{=E_n} + b \cdot E_{ij} (i \neq j)$.

Beispiel: $\begin{pmatrix} 1 & & & 0 \\ & \ddots & b & \\ & & \ddots & \\ 0 & & & 1 \end{pmatrix}$

2.) *Vertauschungsmatrizen*: $V_{ij} = 1_n - E_{ii} - E_{jj} + E_{ij} + E_{ji}$.

Beispiel: $\begin{pmatrix} 1 & & & & & 0 \\ & \ddots & & & & \\ & & 0 & 1 & & \\ & & 1 & 0 & & \\ & & & & \ddots & \\ 0 & & & & & 1 \end{pmatrix}$

3.) *„Einheitsdiagonalmatrizen“*:

$$diag_j(\epsilon) = \begin{pmatrix} 1 & & & & & & \\ & \ddots & & & & & \\ & & 1 & & & & \\ & & & \epsilon & & & \\ & & & & 1 & & \\ & & & & & \ddots & \\ & & & & & & 1 \end{pmatrix}, \epsilon \in R^\times$$

Laut LA: $\det A_{ij}(b) = 1, \det(V_{ij}) = -1 (i \neq j), \det diag_j(\epsilon) = \epsilon \Rightarrow$
Alle Elementarmatriizen sind in $GL_n(R)$

Weiter Matrizen besonderer Form:
Diagonalmatrizen: $D = \text{diag}(d_1, ..., d_r, 0, ..., 0)$ (in $R^{m\times n}$). Für $r = 0 : D = 0$.

Beispiel: $\begin{pmatrix} d_1 & & & & 0 \\ & \ddots & & & \\ & & d_r & & \\ & & & 0 & \\ 0 & & & & \ddots \end{pmatrix}$

Bemerkung: Eine Matrix $B \in R^{n \times n}$ heiße in „*Elementarteilerform*“ $\Leftrightarrow B = \operatorname{diag}(d_1, ..., d_r, 0, ...0), d_1, ..., d_r$ normiert und $d_r \neq 0$ und $d_1 \mid d_2 \mid ... \mid d_r$ (dann $d_1 = \operatorname{ggT}(B)$)

Eine Elementaroperation (ausgeübt auf $B \in R^{m \times n}$) ist eine der folgenden Operationen:
Zu Γ Elementarmatrix bilde $B' = \Gamma B$ oder $B' = B\Gamma$ und setzte wieder $B := B'$.

Liste:

Zeilenoperationen	bewirkt
$B \to B =: B' = A_{ij}(b) \cdot B$	Addition des b-fachen der j-ten Zeile von B zur i-ten
$B \to B =: B' = V_{ij} \cdot B$	Vertauschen der i-ten mit der j-ten Zeile
$B \to B =: B' = \operatorname{diag}_j(\epsilon) \cdot B$	Multiplikation der j-ten Zeile mit ϵ

Spaltenoperationen	bewirkt
$B \to B =: B' = B \cdot A_{ij}(b)$	Addition der i-ten Sapte $*b$ zur j-ten
$B \to B =: B' = B \cdot V_{ij}$	Vertauschen der i-ten mit der j-ten Spalte
$B \to B =: B' = B \cdot \operatorname{diag}_j(\epsilon)$	Multiplikation der j-ten Spalte mit ϵ

Jeder Algorithmus der eine Matrix A durch eine endliche Folge von Elementaroperationen in Elementarteilerform überführt, heißt *Elementarteileralgorithmus.*

Vorschlag:
Bearbeite Tripel $(U, B, V) \in GL_m(R) \times R^{m \times n} \times GL_n(R)$ beginnend mit $(1_m, A, 1_n)$, so dass immer $B = UAV$ ist.

Elementaroperationen hier $(U, B, V) \to (U, B, V) := (\underbrace{\Gamma U}_{=U'}, \underbrace{\Gamma B}_{=B'}, \underbrace{V}_{=V'})$ (Zeilenoperation) oder $(U, B, V) \to (U, B, V) := (\underbrace{U}_{=U'}, \underbrace{B\Gamma}_{=B'}, \underbrace{V\Gamma}_{=V'})$ (Spaltenoperation).
Bedingung okay: $\underbrace{\Gamma UAV}_{U'A'V'} = \Gamma B = B'$, ebenso $UAV\Gamma = B\Gamma = B'$

Ziel: Steure die Operationen so, dass nach endlich vielen Elementaroperationen ein (U, B, V) entsteht, mit $B =: D$ eine Elementarteilerform, also $A = UDV$.
Falls man so einen Algorithmus hat, so beweist das:

Satz 7.3 (Elementarteilersatz)
Sei R ein euklidischer Ring, $m, n \in \mathbb{N}_+, A \in R^{m \times n}$

(i) Dann gibt es ein $U \in GL_m(R), V \in GL_n(R)$ und $D \in R^{m\times n}, D$ in Elementarform, derart, dass $\underline{A = UDV}$

(ii) D ist durch A eindeutig bestimmt

Zur Eindeutigkeit (Beweis-Skizze):
$d_1 = \text{ggT}(D) = \text{ggT}(UDV) = \text{ggT}(A)$. Man kann zeigen: $d_1 \cdot \ldots \cdot d_j$ ist der ggT der Determinanten aller $j \times j$-Untermatrizen von A.

Bemerkung: 1.) $A \in R^{m\times n}$, so $\det A = \det U \det D \det V$. Dann zur Berechnung von $\det A$ benutzt werden.

2.) Idee für LGS: Für $A = D$ in Elementarteilerform kann Lösung unmittelbar abgelesen werden $\Rightarrow$ Lösung für A wird mittels Rücktransformation ermittelt.

<u>LGS:</u>
$xA = b, A \in R^{m\times n}, b \in R^{1\times n}$ (Zeile) ist gegeben. Gesucht „Lösung“ $x \in R^{1\times m}$ (Zeile). (LA oft $Ax = b$ mit Spalten, $Ax = b \Leftrightarrow x^T A^T = b^T$)
Besser: Information über die *Lösungsmenge*: $\mathcal{L}(A,B) = \{x \in R^m = R^{1\times m} \big| xA = b\}$

Antwort sehr leicht, falls $A = D = \begin{pmatrix} d_1 & & \\ & \ddots & \\ & & d_r \end{pmatrix}$ in Elementarteilerform. $y = (y_1, ..., y_m) \in \mathcal{L}(D,c), c = (c_1, ..., c_n) \Leftrightarrow yD = \underbrace{(y_1 d_1, ..., y_r d_r, 0, ..., 0)}_{\text{n-Stück}} \overset{!}{=} (c_1, ..., c_n)$

Lösbarkeitsbedingung (notwendig und hinreichend): $\mathcal{L}(D,C) \neq \emptyset \Leftrightarrow c_{r+1} = c_{r+1} = ...c_n = 0$ <u>und</u> $d_1 \mid c_1, d_2 \mid c_2, ..., d_r \mid c_r$

Falls Bedingung erfüllt, so hat man die „spezielle Lösung“ (wo $c_j = d_j y_j$, Bezeichnung $y_j = d_j^{-1} c_j$).
$y \overset{(0)}{=} (d_1^{-1} c_1, ..., d_r^{-1} c_r, 0, ..., 0)$.

Die „allgemeine“ Lösung hat die Form:
$y = y_0 + \sum_{j=r+1}^n a_j e_j, e_j = (0, ..., 0, 1, 0, ..., 0)$ Einheitsvektor, $a_j \in R$

$$\begin{aligned} y \in \mathcal{L}(D,c) \quad &\Leftrightarrow yD = c (\text{auch } y_0 D = c) \\ &\Leftrightarrow (y - y_0) D = 0 \\ &\Leftrightarrow z = (y - y_0) \text{ ist Lösung des zugehörigen homogenen Systems} \\ &\quad zD = 0, \text{ d.h. von der Form } \textstyle\sum_{j=r+1}^n a_j e_j \end{aligned}$$

Es muss $z_j d_j = 0$, also $z_0 = 0$ für $j = 1, ..., r$ gelten.

Man transformiert $xA = b$ wie folgt auf Diagonalform: $xA = b \Leftrightarrow \underbrace{xU^{-1}}_{y}\underbrace{UAV}_{D} = \underbrace{bV}_{c} = 0$.

$yD = c$, wo $c = bV$ und $y = xU^{-1}$, also $x = yU$ ist.
$\underline{\mathcal{L}(A,b) = \mathcal{L}(D, bV) \cdot U}$

$(U, B, V) \in GL_m(R) \times R^{m\times n} \times GL_n(R)$, $B = UAV$.

Elementarteileralgorithmus Idee: Falls $B \neq 0$, so setzte

$$gr(B) = \min\{gr(b_{ij},\ i = 1, 2, \ldots, m,\ j = 1, 2, \ldots, n,\ b_{ij} \neq 0\}.$$

Wenn es gelingt durch Elementaroperationen von B nach B' überzugehen, so dass $gr(B') < gr(B)$, so ist man induktiv fertig.

Zuerst benötigen wir einen Unteralgorithmus: ggTnachVorn(A):
Er soll zu einem $0 \neq A \in R^{m\times n}$ (U_1, B_1, V_1) mit $U_1 \in GL_m(R),\ v_1 \in GL_n(R),\ b_1 = U_1AV_1$ gilt, wobei

$$B = \left(\begin{array}{c|c} d_1 & 0 \\ \hline 0 & A' \end{array}\right), \quad d_1 = \mathrm{ggT}(A).$$

Skizze:

0. Initialisierung: $(U, B, V) := (1_m, A, 1_n)$.
1. Bestimme(k, l) mit $gr(b_{kl} = gr(B)$.
2. Fall I: Es gibt eine Zeile i mit $B_{kl} \nmid b_{il}$. Division mit Rest: $b_{ij} = qb_{kl} + r$. Addiere $(-q)$–faches der k–ten Zeile. Das ergibt B' mit $b'_{il} = b_{il} - qb_{kl} = r$. Induktiv sind wir fertig, denn: $gr(r) < gr(b_{kl}) = gr(B)$. Weiter bei Schritt 1.
3. Fall II: Es gibt eine Spalte j mit $b_{kl} \nmid b_{kj}$. Genau wie bei Schritt 2, nur mit Spaltenoperationen erhalten wir $b_{kj} = q'b_{kl} + r'$. Addieren wir nun das $(-q')$–fache der l-ten Spalte auf die j–te Spalte, erhalten wir B' mit $gr(B') < gr(B)$.
4. Fall III: $b_{kl} \mid b_{il}$ und $b_{kl} \mid_{kj}$, $\forall i, j$ aber $\exists (i, j)$ mit $b_{kl} \nmid b_{ij}$. $b_{il} = q''b_{kl},\ i \neq k, l \neq j$. Addiere $(1 - q'')$-faches der k-ten Zeile zur i-ten hinzu:
   $b'_{il} = \underbrace{b_{ij}}_{q'b_{kl}} + (1 - q'')b_{kl} = b_{kl}$
   $b'_{ij} = b_{ij} + (1 - q'')b_kj \implies b_{kl} = b'il' \nmid b_{ij}$ (wegen $b_kl \nmid b_{ij}$, $b_{kl} \mid b_{kl}$)
   Fall II liegt vor mit i-ter statt k-ter Zeile. $B := B'$, $(k, l) := (i, l)$, weiter bei Schritt 3.
5. $\forall i, j :\ b_{kl} \mid b_{ij}$ (letzter möglicher Fall). Vertausche k-te und 1. Zeile und l-te und j-te Spalte. Entsteht b mit $0 \neq b_{11} \mid b_{ij}\ \forall i, j \implies b_{11}$ ist ein ggT, $\implies \exists \epsilon \in R^\times : d_1 = \epsilon b_{11} = \mathrm{ggT}(B) \overset{\text{Lemma 2}}{=} \mathrm{ggT}(A) \implies$ Multipliziere 1. Zeile mit ϵ: Es entsteht Matrix mit $b_{11} = d_1 = \mathrm{ggT}(A)$. Wie bei Gaußalgorithmus erzeugt man jetzt in der ersten Spalte und ersten Zeile Nullen außer bei b_{11}. Jetzt hat man (U, B, V) mit $A = UBV)$ und $B = \left(\begin{array}{c|c} d_1 & 0 \\ \hline 0 & A' \end{array}\right)$. Ausgabe: $(U_1, B_1, V_1) := (U, B, V)$

Klar: Man kann genauso mit A' weitermachen: Braucht: $d_n = \mathrm{ggT}(A) = ggt(B_1) \mid \mathrm{ggT}(A')$. Im Detail:

ELT(A) :

(1) Falls $A \neq 0$, Ausgabe: $(1_m, A, A_n)$.

(2) Anderfalls liefert ggTnachVorn(A) (U_1, B_1, V_1) wie oben: Falls $n = 1$ oder $M = 1$, so fertig. Ausgabe $(U, D, V) := (U_1, B_1, V_1)$. Falls m,n>1 und $A' = 0$, so wieder fertig. Ausgabe wie

oben.
Falls $A' \neq 0$, so liefert ELT(A') (U', D', V') mit $U'D'V' = A'$ und

$$\begin{aligned} & U_1 \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & U' \end{array}\right) \left(\begin{array}{c|c} d_1 & 0 \\ \hline 0 & D' \end{array}\right) \left(\begin{array}{c|c} 1 & 0 \\ \hline 0 & V' \end{array}\right) V_1 \\ =& U_1 B = \left(\begin{array}{c|c} d_1 & 0 \\ \hline 0 & \underbrace{U'D'V'}_{=A'} \end{array}\right) V_1 \\ =& U_1 B_1 V_1 \\ =& A \end{aligned}$$

Ausgabe (U, D, V) mit U, D, V passend wie in obiger Formel.

Einschub Beispielrechnung (folgt vielleicht später, hab' grade keine Lust, die zwei DinA4-Blätter abzutippen)

7.2 Ganzzahlige Lösungen eines ganzzahligen linearen Gleichungssystems

Betrache LGS $xA = B$, gegeben $a \in R^{m\times n},\ b \in R^{1\times n}$.
Gesucht:$\mathcal{L}(A, B) = \{x \in R^{1\times m} = R^m :\ xA = b\}$

Elementarteilersatz: $A = UDV,\ D = \text{diag}(d_1, d_2, \dots, d_r, 0, \dots)$ in Elementarteilerform. $U \in GL_m(R),\ V \in GL_n(R)$. Gesehen: $\mathcal{L}(A, b) = \mathcal{L}(D, bV)U$. $c := bV = (c_1, c_2, \dots, c_n)$.

Satz 7.4 (LGS-Satz)
Mit diesen Voraussetzungen und Bezeichnungen gilt:

(1) $\mathcal{L}(A, b) \neq \emptyset \iff d_i \mid c_i,\ i = 1, 2, \dots, r,\ c_{r+1} = c_{r+2} = c_n = 0.$

(2) Lösung des homogenen Systems $xA = 0$:
$\mathcal{L}(A, 0) = \mathcal{L}(D, 0)U = \bigoplus_{j=r+1}^{m} R(e_jU)$. e_j ist der j-te Einheitsvektor in R^m. Das heißt, eine R-Basis von $\mathcal{L}(A, 0)$ ist gegeben durch Basis $b_{r+1}, b_{r+2}, \dots, b_m$, mit $b_j = e_jU$, also die j-te Zeile von U ist. Falls $m \leq r$, so $\mathcal{L}(A, 0) = 0$, d-h- jede Lösung $y \in \mathcal{L}(A, 0)$ hat eindeutige Darstellung $y = \sum_{j=r+1}^{m} a_jb_j,\ a_j \in R$.

(3) Falls das LGS lösbar ist, so erhalt man die allgemeine Lösung x aus einer speziellen Lösung x_0 in der Form $x = x_0 + y,\ y \in \mathcal{L}(A, 0)$. Mann kann wählen: $x_0 = (d_1^{-1}c_1, d_2^{-1}c_2, \dots, d_r^{-1}c_r, 0, \dots, 0)$.

Beweis
Alles schon bewiesen. . .

Bemerkungen:
(1) Ist $A \in R^{n\times n}$, so gilt
$$A \in GL_n(R) \iff D = 1_n$$

(2) Jedes $U \in GL_n(R)$ ist Produkt von Elementarmatrizen.

Beweis

(1) $A = UDV$, $U, V \in GL_n(R)$. $D \in GL_n(R) \iff n = r,\ d_1, \ldots, d_n = 1 \implies D = 1_n$

(2) $A \in GL_n(R) \iff D = 1_n \implies A = UV \implies$ Behauptung ■

Freunde der Algebra mögen beachten, dass für ein R-Modul M die selben Axiome wie für einen Vektorraum gelten, nur dass R ein Ring statt einem Körper ist. Das $\mathbb{Z}$-Modul ist (fast) das selbe wie eine (additive) abelsche Gruppe. Die Hauptneuheit ist, dass man im Allgemeinen in M eine R-Basis hat.

Ein Beispiel dazu ist mit $R = \mathbb{Z}$ das Modul $M = (\mathbb{Z}/2\mathbb{Z}), +)$. Wäre die Basis die leere Menge, so wäre $M = 0$, Widerspruch. Ist nun b ein Element der Basis, so wären alle $z \cdot b$, $z \in \mathbb{Z}$ verschieden, also $\#M = \infty$, was auch ein Widerspruch ist.

In der Algebra zeigt man leicht: Ist $M = \langle u_1, \ldots, u_m \rangle = \{\sum_{i=1}^m \alpha_i u_i \mid \alpha_i \in R\}$, so existiert ein $A \in R^{m \times n}$ mit $M \cong R^n / R^m \cdot A$. Klar: $A = UDV$ wie im Elementarsatz, also $R^m = R^m \cdot U$, $R^n = V \cdot R^n$

$$
\begin{aligned}
\implies M &\cong R^n / R^m UDV \\
&= R^n V / R^m DV \\
&\cong R^n / R^m D \\
&= (R \oplus \cdots \oplus R)/(Rd_1 \oplus \cdots \oplus Rd_r \oplus 0 \oplus \cdots \oplus 0) \\
&\cong R/Rd_1 \oplus \cdots \oplus R/R_d r \oplus R \oplus \cdots \oplus R
\end{aligned}
$$

Damit ist die Struktur bestimmt. So kann die Eindeutigkeit von D auch bewiesen werden.

Ist $R = \mathbb{Z}$, so ist $(\mathbb{Z}/d\mathbb{Z}, +)$ zyklisch, erzeugt von $1 + d\mathbb{Z} = \overline{1}$, $\mathbb{Z}$ sowieso zyklisch.

Als Ergebnis haben wir: Jede endlich erzeugbare abelsche Gruppe ist direktes Produkt zyklischer Gruppen.

Die R-lineare Abbildung $R^l \to R^k$ beschriebung durch Darstellungsmatrizen in $R^{l \times k}$. Der Elementarteiler-Algorithmus liefert Mittel Kern(f) und Bild(f) explizit zu beschreiben.

8 Ganzzahlige quadratische Formen

8.1 Grundbegriffe und Bezeichnungen

Problem: Man diskutiert die diophantische Gleichung

$$k = ax^2 + bxy + cy^2 \quad (*)$$

Gegeben sind $a, b, z, k \in \mathbb{Z}$, gesucht ist ein $\underline{x} = (x, y) \in \mathbb{Z}^2$, für die $(*)$ gilt.

Gegeben $Q = aX^2 + bXY + cY^2 \in \mathbb{Z}[X, Y]$, $a, b, c \neq 0$, mit Kurzbezeichnung $Q = [a, b, c]$. Dieses Q heißt ganzzahlige binäre (wegen den 2 Variablen) quadratische ($\operatorname{grad} q = 2$) Form.

Nun betrachtet man Q als Abbildung $\mathbb{Z}^2 \to \mathbb{Z}^2$, $\underline{x} = (x, y) \mapsto Q(x, y)$.

Definition

(1) $\underline{x}$ primitiv $\iff$ $\operatorname{ggT}(x, y) = 1$

(2) Q primitiv $\iff$ $\operatorname{ggT}(a, b, c) = 1$

(3) Q stellt $k \in \mathbb{Z}$, $k \neq 0$ (primitiv) da $\iff$ $\exists \underline{x} \in \mathbb{Z}^3$ ($\underline{x}$ primitiv), mit $Q(\underline{x}) = k$

Problem: Welche Formen stellen welche Zahlen dar? $Q(\mathbb{Z}^2) = ?$

Falls $k \in Q(\underline{x})$, welche weiteren $\underline{x}'$ erzeugen $k = Q(\underline{x}')$? $Q^{-1}(\{k\}) = ?$

Bemerkung: (1) $z \in \mathbb{Z}$, so $Q(z \cdot \underline{x}) = z^2 \cdot Q(\underline{x})$

(2) Mit Q ist auch mQ eine Quadratische Form ($m \in \mathbb{Z}$, $m \neq 0$)

Wegen (1) genügt es meist, primitive Darstellungen zu betrachten.

Aus der Linearen Algebra ist über reelle Quadriken bekannt: Es gibt Darsellungsmatrixen $A_Q = \mathbb{R}^{2\times 2}$ mit $Q(x) = xA_Qx^\top$, wobei

$$A_Q = \begin{pmatrix} a & \frac{b}{2} \\ \frac{b}{2} & c \end{pmatrix}$$

Idee (Gauß?) Wegen $\mathbb{Z}^2 U = \mathbb{Z}^2$ für $U \in GL_2(\mathbb{Z})$ gilt $Q(\mathbb{Z}^2) = Q \cdot (\mathbb{Z}^2 U)$. $Q(\underline{x}U) = \underline{x}U \cdot A_Q \cdot (xU)^\top = \underline{x}(UA_QU^\top)x^\top$

Definition

(1) Zu Q sei $U.Q$ die Quadratische Form mit Darstellungsmatrix $UA_QU^\top$

(2) Q und $Q^\top$ heißen (eigentlich) äquivalent ($Q \sim Q'$ bzw $Q \approx Q'$) $\iff$ $\exists U \in GL_2(\mathbb{Z})$ (bzw. $\exists I \in SL_2(\mathbb{Z})$, wobei $SL_2(\mathbb{Z}) = \{U \in \mathbb{Z}^{2\times 2} \mid \det U = 1\}$) mit $Q' = U.Q$.

$\sim$, $\approx$ unterscheiden sich wenig, sozusagen höchstens um eine Matrix $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$.

Bemerkung: (1) $1_2.Q = Q$, $U, V \in GL_2(\mathbb{Z})$. $(UV).Q = U.(V.Q)$.
„$GL_2(\mathbb{Z})$ bzw. $SL_2(\mathbb{Z})$ operiert auf der Menge der Quadratischen Formen“

(2) $\sim$, $\approx$ sind Äquivalenzrelationen

(3) Äquivalente Formen stellen die selben Zahlen dar.

Beweis

(1) $UV.Q$: $UVA_Q(UV)^\top = U(VA_QV^\top)U^\top : U.(V.Q)$.

Folgt $Q' = U.Q$, so $U^{-1}.Q' = U^{-1}.(U.Q) = (U^{-1}U).Q = 1_2.Q = Q$.

Also ist $\sim$ symetisch: $Q \sim Q$.

Transitivität: $Q \sim Q'$, $Q' = U.Q$ und $Q' \sim Q''$, $Q'' = V.Q$, mit $U, V \in GL_2(\mathbb{Z})$, so ist $Q'' = V.(U.Q) = (VU).Q \implies Q'' \sim Q$ ■

8.2 Die Diskriminante

Sei $Q = [a, b, c]$ eine Quadratische Form.

Definition

$\Delta = -4 \cdot \det A_Q = b^2 - 4ac = \operatorname{dis}(Q) \in \mathbb{Z}$ heißt Diskriminante von Q.

Bemerkung aus der Linearen Algebra: $\mathcal{V} = \mathcal{V}_{Q-k}(\mathbb{R}) = \{\underline{x} \in \mathbb{R}^2 \mid Q(\underline{x}) = k\}$ ist reelle Quadrik, abgesehen von ausgearteten Fällen gilt: $\Delta < 0$: $\mathcal{V}$ Ellipse, $\Delta > 0$, $\mathcal{V}$ Hyperbel.

Beispiel

$X^2 + 5Y^2$ Ellipse: $\Delta = 0 - 4 \cdot 5 = -20 < 0$
$X^2 + -2Y^2$ Hyperbel: $\Delta = 0 - 4 \cdot (-2) = 8 > 0$

Problem: Welche $(x, y) \in \mathbb{Z}^2$ (Gitterpunkte) liegen auf $\mathcal{V}$.

Satz 8.1 (Diskriminantensatz)
Sei Q eine Quadratische Form.

(1) Ist $Q \sim Q'$, so gilt $\operatorname{dis}(Q) = \operatorname{dis}(Q')$.

(2) Ist $\Delta = \operatorname{dis} Q$ ein Quadrat in $\mathbb{Z}$ $\iff$ „Q zerfällt über $\mathbb{Z}$“, also $\exists u, v, w, z \in \mathbb{Z}$ mit $Q = (uX + vY)(wX + zY)$

(3) Ist $\operatorname{dis} Q \neq 0$, so gilt

$$\begin{aligned} Q \text{ definit} &\iff \operatorname{dis} Q < 0 \\ Q \text{ indefinit} &\iff \operatorname{dis} Q > 0 \end{aligned}$$

(4) $0 \neq d \in \mathbb{Z}$ ist Diskriminante $\iff$ $d \equiv 0, 1 \mod 4$

Anwendung: $\Delta = \operatorname{dis} Q$ sei ein Quadrat $Q(\underline{x}) = k \neq 0 \iff \exists d \in \mathbb{Z}, dk$: $ux + vy = d$, $wx + zy = \frac{k}{d}$. Die Frage nach den darstellbaren k läuft zurück auf a) Bestimmung aller Teiler von k, b) Diskussion eines ganzzahligen LSG.

Ab jetzt interessieren nur noch nichtquadratische Diskriminanten.

Beweis

(4) $\delta = \operatorname{dis} Q = b^2 - 4ac \equiv b^2 \equiv 0, 1 \mod 4$.
$d \equiv 0 \mod 4$: $Q = [1, 0, -\frac{d}{4}]$
$d \equiv 1 \mod 4$: $Q = [1, 1, -\frac{1-d}{4}]$
Für diese Formen gilt $\operatorname{dis} Q = d \equiv \Delta$. Diese Form heißt „Hauptform“ der Diskriminante.

(1) $\det U A_Q A^\top = \det U \cdot \det U^\top \cdot \det A_Q = (\det U)^2 \cdot \det A_Q = \det A_Q \implies$ Behauptung.

(2) (Skizze)

„$\Leftarrow$“ Nachrechnen

„$\Rightarrow$“ $\Delta = \operatorname{dis} Q = q^2$. Sei $t = \operatorname{ggT}(a, \frac{b-a}{2})$, dann (Übung):

$$Q = (\frac{a}{t}X + \frac{b-q}{2t}Y)(tX + \frac{b+q}{2\frac{a}{t}}Y)$$

(3) $a = 0 \implies \Delta > 0$, $Q = bXY + cY^2 = (bX + cY)Y$ indefinit
$a \neq 0$: $aQ = (aX + bY)^2 - \frac{1}{4}\Delta Y^2$. Offensichtlich: $\Delta < 0$: definit, $\Delta > 0$: indefinit ■

<++>

8.3 Darstellung von Zahlen durch QFen

Vor. Q QF, $\operatorname{dis} Q = \Delta$ sei kein Quadrat.
$U.Q$ QF mit Matrix $UA_qU^T, U \in GL_2(\mathbb{Z})$
$U = \begin{pmatrix} r & s \\ u & v \end{pmatrix} \Rightarrow U.Q = [Q(r,s), 2rU \cdot a + (rv + su)b + 2sv \cdot c, Q(u,v)]$

Spezialfälle:
$Q' = \begin{pmatrix} 1 & 0 \\ t & 1 \end{pmatrix}.Q = [a, t \cdot 2a + b, at^2 + bt + c]$
$Q' = \begin{pmatrix} \cdot & 1 \\ -1 & t \end{pmatrix}.Q = [c, -b + 2ct, ct^2 - bt + a]$
$Q' = \begin{pmatrix} \cdot & 1 \\ -1 & \cdot \end{pmatrix}.Q = [c, -b, a]$
$Q' = \begin{pmatrix} 1 & \cdot \\ 1 & 1 \end{pmatrix}.Q = [a, 2a + b, a + b + c]$

Wunsch:
Algorithmus der feststellt, ob Q k darstellt oder nicht.

Satz 8.2 (1. Darstellungssatz)
Q stellt $0 \neq k \in \mathbb{Z}$ genau dann primitiv dar, wenn: $\exists Q' = [k, l, m]$ mit $Q' \approx Q \wedge -|k| < l \leq |k|$.

Hat man also einen Algorithmus, der feststellt, ob $Q \approx Q' \vee Q \not\approx Q'$, so hat man einfach $2k$ Formen zu testen (auf Äquivalenz zu Q). ($m = \frac{l^2-\Delta}{4k}$)

Spezialfall:
$k = 1, Q$ stellt 1 dar $\Leftrightarrow Q \approx [1, 0, \frac{-\Delta}{4}]$ (für $\Delta \equiv 0 \mod 4$)
–HIER FEHLT NOCH EINE ZEILE, WELCHE NICHT RICHTIG KOPIERT WURDE –

$Q \approx [1, 1, \frac{1-\Delta}{4}]$ (für $\Delta \equiv 1 \mod 4$).
Ergebnis: Genau die zur Hauptform äquivalenten Formen stellen 1 dar.

Beweis
„$\Leftarrow$": $Q'(1, 0) = k$. Hat man $Q' \approx Q \Rightarrow Q$ stellt k dar

„$\Rightarrow$": $k = Q(x, y), \mathrm{ggT}(x, y) = 1$. LinKomSatz liefert $u, v \in \mathbb{Z}$ mit $xv - yu = 1 \Rightarrow U := \begin{pmatrix} x & y \\ u & v \end{pmatrix} \in Sl_2(\mathbb{Z})$

$Q_1 := U.Q = [\underbrace{Q(x, y)}_{=k}, l', \text{irgendwas}], l := l' \text{ mods } 2|k|, \exists t : l = l' + 2tk \Rightarrow Q' = \begin{pmatrix} 1 & \cdot \\ t & 1 \end{pmatrix} .Q_1$ wie verlangt. ∎

Satz 8.3 (2. Darstellungssatz)
Sei $k \in \mathbb{Z}, k \neq 0$. Genau dann gibt es eine Form Q mit $\operatorname{dis} Q = \Delta$, die k primitiv darstellt, wenn die Kongruenz $l^2 \equiv \Delta \mod 4k$ so lösbar ist, dass $\mathrm{ggT}(k, l, \frac{l^2-\Delta}{4k}) = 1$.

Beweis
„$\Leftarrow$": Einfach, die Form $[k, l, \frac{l^2-\Delta}{4k}]$ tut es

„$\Rightarrow$": k so darstellbar $Q \approx Q' = [k, l, \frac{l^2-\Delta}{4k}]$ nach *1. Darstellungssatz* (für (mindestens) ein l) $\Rightarrow \frac{l^2-\Delta}{4k} \in \mathbb{Z} \Rightarrow l^2 \equiv \Delta \mod 4k$ [ggT stimmt auch] ∎

Spezialfälle:
Sei $k = p \in \mathbb{P}$

- $p \nmid \Delta, p \neq 2 : p$ so darstellbar $\Leftrightarrow (\frac{\Delta}{p}) = 1$
- $p \mid \Delta, p \neq 2 : p$ so darstellbar $\Leftrightarrow v_p(\Delta) = 1$
- $p = 2 \mid \Delta$: 2 so darstellbar $\Leftrightarrow \Delta \equiv 8, 12 \mod 16$

Zu den Spezialfällen

- $p \nmid \Delta : (\frac{\Delta}{p}) = 1$ lösbar, $l_1^2 \equiv \Delta \mod p \Leftrightarrow l_1^2 \equiv \Delta \mod 4p \rightsquigarrow ChRs$
- $2 \neq p \mid \Delta$: Löse $l \equiv 0 \equiv \Delta \mod p (*)$, $l^2 \equiv \mod 4 \Rightarrow l^2 \equiv \Delta \mod 4p$
  $\text{ggT}(\underbrace{p, l}_{\text{ggT}=p}, \frac{l^2-\Delta}{4p}) = 1 \Leftrightarrow p \nmid \frac{l^2-\Delta}{4p} \Leftrightarrow p^2 \nmid l^2 - \Delta \Leftrightarrow p^2 \nmid \Delta$, da $p^2 \mid l^2$ nach $(*)$. ($\Rightarrow v_p(\Delta) = 1$)
- $p = 2 \mid \Delta$: Ü.

Definition
Die Klassenzahl $h(\Delta)$ ist die Anzahl der Klassen eigentlich äquivalenter Formen mit Diskriminante Δ. „Schöne Resultate“, falls $h(\Delta) = 1$.
$\Rightarrow$ Alle Formen der Diskriminante Δ stellen k dar $\Leftrightarrow$ Bed. 2. DarstSatz.

Später. $h(-4) = 1, Q = [1, 0, 1]$ Ergebnis: $2 \neq p \in \mathbb{P}$ wird durch $Q = x^2 + y^2$ dargestellt $\Leftrightarrow 1 = (\frac{-4}{p}) = \frac{-1}{p} = (-1)^{\frac{p-1}{2}} \Leftrightarrow p \equiv 1 \mod 4$ Andere Beispiele, etwa $\Delta = -164$ (Klassenzahl 1, betragsmäßig größte negative Zahl. Im positiven unbekannt)

8.4 Reduktion der definiten Formen

Sei $\Delta < 0$ [und damit „Nicht-Quadrat“], $\Delta = b^2 - 4ac \Rightarrow ac > 0$. Ohne Einschränkung positiv definit, d.h. $a > 0, c > 0$.

Definition (Gauß)
Q (mit Diskr Δ) heißt reduziert $\Leftrightarrow |b| \leq a \leq c$

In dieser Vorlesung:
Q heißt vollreduziert $\Leftrightarrow Q$ ist reduziert und falls $(c = 0 \wedge b \neq 0) \vee (|b| = a)$ auch noch $b > 0$ ist.

Idee (Gauß):
Setzte $|Q| := a + |b|$. Versuche $Q' \approx Q$ zu finden mit $|Q'| < |Q|$. Das geht, solange Q nicht reduziert ist.

Fall I: $a > c, Q' := \begin{pmatrix} \cdot & 1 \\ -1 & \cdot \end{pmatrix}, Q = [\underbrace{c}_{-a'}, \underbrace{-b}_{b'}, \underbrace{a}_{c'}]$. $|Q'| = a' + |b'| = |b| + c < |b| + a = |Q|$

Fall II: $a \leq c, |b| > a$ (da Q nicht-reduziert) Division von b mit Rest durch $2a$: $\exists t \in \mathbb{Z} : b = b' - 2ta, -a < b' \leq a$. $Q' = \begin{pmatrix} 1 & \cdot \\ t & 1 \end{pmatrix} .Q = [a, \underbrace{b + 2ta}_{b'}, c']$. $|Q'| = |b'| + a \leq a + \underbrace{|a|}_{=a(\text{ da } -a \leq a)}$

Dies ergibt Vollreduktionsalgorithmus $red(Q)$, der $\tilde{Q}$ berechnet mit $\tilde{Q} \approx Q \wedge \tilde{Q}$ vollreduziert. Wiederholte Anwendung von $Q := Q'$ aus Fall I,II endet nach endlich vielen Schritten mit reduziertem $Q_1 \approx Q$. Falls Q_1 vollreduziert, so $\tilde{Q} := Q_1$.
Falls Q_1 nicht vollreduziert, so 2 Fälle für $Q_1 = [a, b, c]$

- $c = a$, aber $b < 0 : \tilde{Q} := \begin{pmatrix} \cdot & 1 \\ -1 & \cdot \end{pmatrix} .Q_1 = [a, -b, a]$, jetzt $-b > 0$

- $|b| = a$, also $b = -a < 0$. $\tilde{Q} = \begin{pmatrix} 1 & \cdot \\ 1 & 1 \end{pmatrix}.[a,-a,c] = [a,a,c], c' = a+b+c = c$ ist vollreduziert ($b' = a > 0$).

Ziel: 2 vollreduzierte Formen der Disk Δ sind äquivalent $\Leftrightarrow$ sie sind gleich. Es folgt:
$Q \approx Q' \Leftrightarrow$ red $Q =$ red Q'. Daher gibt es einen Algorithmus, der entscheidet, ob $Q \approx Q' \vee Q \not\approx Q'$

Hilfsatz:
$Q = [a,b,c]$ sei reduziert. Dann:

(i) $a = \min Q(\mathbb{Z}^2 \backslash 0)$

(ii) Für $a < c$ ist $Q^{-1}(\{a\}) = \{\pm(1,0)\}$ (klar: $Q(\underline{x}) = Q(-\underline{x})$)
Für $0 \le b < a = c$ ist $Q^{-1}(\{a\}) = \{\pm(1,0), \pm(0,1)\}$. (Für $|b| = a = c$ ($=1$, da Q primitiv) $Q[1,\pm1,1] = x^2 \pm yx + y^2 \Rightarrow \#Q^{-1}\{a\} = 6$)

$|b| \le a \le c$
$(*)$ $Q(x,y) = ax^2+bxy+cy^2 \overset{(1)}{\ge} ax^2-|bxy|-ay^2 \ge a(|x|-|y|)^2+(2a-|b|)|xy| \ge a(\underbrace{(|x|-|y|)^2+|xy|}_{\in\mathbb{Z},\neq 0, \text{ wenn } (x,y)\neq 0, \text{ also } \ge 1} \overset{(4)}{\ge} a$.

Erinnerung:
$Q = [a,b,c]$ reduziert $\Leftrightarrow |b| \le a \le c$
Vollreduziert: Falls $a = c \wedge b \neq 0 \vee a = c = |b|$, so $b > 0 \rightsquigarrow$ Vollreduktionsalgorithmus red.

Sei $Q(x,y) = a \Rightarrow$ in $(*)$ überall „c“
$a < c \Rightarrow y = 0$ (sonst bei (1) $>$)
„$=$“ bei (4) $\Rightarrow (|x|-|y|)^2 + |xy| = 1 \Rightarrow (x,y) \in M = \{\pm(1,0), \pm(0,1), (\pm1,\pm1)\}$

Fall I: $Q^{-1}(a) = \{\pm(1,0)\}, \#Q^{-1}(a) = 2$

Fall II: $a = c$, aber $|b| < a \Rightarrow 2a - |b| > a \Rightarrow$ „$=$“ nur für $|xy| = 0$. $Q^{-1}(a) = \{\pm(1,0), \pm(0,1)\}$

Fall III: $a = c = |b|$, etwa $b > 0$, so $x^2 + xy + y^2 = 1$ von $(\pm1,\pm1)$ in M nur $\pm(1,-1)$ [dazu noch $\pm(1,0), \pm(0,1)$] $\Rightarrow \#Q^{-1}(a) = 6$

Folgerung: Sei Q, Q' vollständig reduziert und $Q \approx Q'$, so ist $Q = Q'$.

Beweis
$a = \min(Q(\mathbb{Z}^2 \backslash 0)) = \min(Q'(\mathbb{Z}^2 \backslash 0)) = a'$.

Fall I: $a < c \wedge U = \begin{pmatrix} r & s \\ u & v \end{pmatrix}$ mit $U.Q = Q'$. $a = Q(1,0) = Q'(1,0) = Q((1,0)U) = Q(r,s) \Rightarrow (r,s) = \pm(1,0) \Rightarrow s = 0, \pm U = \begin{pmatrix} 1 & 0 \\ 0(?) & 1 \end{pmatrix} = U$.
$Q' = (a, b+2au, *(?)), |b| \le a, Q'$ red. $|b'| = |b+2au| < a$. Wegen $|b| < a \Rightarrow U = 0, \pm U = \begin{pmatrix} 1 & \cdot \\ \cdot & 1 \end{pmatrix} \Rightarrow Q = Q'$

Fall II: $a = c, |b| \neq a$. $\#Q^{-1}(a) = 4 \Rightarrow$ II liegt auch für Q' vor $\Rightarrow a = a' = c' \Rightarrow b^2 = b'^2 \Rightarrow b' = \pm b$, aber nur b möglich, da Q' vollständig reduziert $\Rightarrow Q' = Q$.

Fall III: $a = c = |b| = b \Rightarrow$ Fall II auch für $Q' \Rightarrow a = a' = c' = b'$ ■

Satz 8.4 (Hauptsatz über definite QFen)
Sei $\Delta \in \mathbb{Z}, \Delta \equiv 0, 1 \mod 4, \Delta < 0$.

(i) Zwei Formen Q, Q' mit Diskriminante Δ sind nau dann eigentlich äquivalent, wenn red $(Q) =$ red (Q') (mit VollredAlgo red)

(ii) Die vollreden Formen der Diskriminanten Δ bilden ein volles Vertretersystem aller eigentlichen Formenklassen, insbesondere ist die Klasse zu U $h(\Delta)$ endlich.

Beweis

(i) $\exists U, U'$ mit red $Q = U.Q$, red $Q' = U'.Q'(U, U' \in Sl_2(\mathbb{Z}))$ können in red berechnet werden. Multipliziere die Matrizen bei den Reduktionsschritten, $Q \approx$ red $Q, Q' \approx$ red Q'. $Q \approx Q' \Leftrightarrow$ red $Q \approx$ red $Q' \overset{\text{Folgerung}}{\Leftrightarrow}$ red$(Q) =$ red(Q').

(ii) Q reduziert $\Leftrightarrow |b| \leq a \leq c \Rightarrow b^2 \leq ac \Rightarrow |\Delta| = -\Delta = -b^2 + 4ac \geq -b^2 + 4b^2 = 3b^2$. Abschätung: $|b| \leq \sqrt{\frac{|\Delta|}{3}} \Rightarrow$ Nur endlich viele reduzierte Qs.
Dies ergibt Algorithmus zur Bestimmung von $h(\Delta)$: $h(\Delta) = \#$ vollreduzierten Formen zu Δ. Reduzierte Form $Q = [a, b, c] \Leftrightarrow |b| \leq \sqrt{\frac{|\Delta|}{3}}, \equiv \Delta \mod 2$, da $b^2 \equiv \Delta \mod 4$. $|b| \leq a \leq c \leq ac = \frac{b^2 - \Delta}{4}$. Stelle alle diese (a, b, c) auf, streiche die nicht vollreduzierten. ■

Satz 8.5 (Heegner/Stark (1969))
Für $\Delta < 0$ gilt: $h(\Delta) = 1 \Leftrightarrow \Delta \in \{-3, -4, -7, -8, -11, -12, -16, -19, -27, -28, -43, -67, -163\}$

Beweis im Netz!

Satz 8.6 (Siegel)
Für negative Diskriminanten Δ gilt $\lim_{|\Delta| \to \infty} h(\Delta) = \infty$

($\Rightarrow$ Für jedes feste $\hat{h} \in \mathbb{N}$ gibt es ∞ viele Δ mit $h(\Delta) = \hat{h}$.)

Gauß definiert eine Verknüpfung (Komposition) zweier Formen $Q_1, Q_2 \Rightarrow Cl(\Delta) =$ Menge aller Formenklassen wird (endliche abelsche Gruppe „Klassengruppe“ genannt.
$\rightsquigarrow$ viele Vermutungen, wenige Sätze bis heute Gaußsche Geschlechtertheorie ersetzt $h(\Delta) = 1$ durch etwas schwächere Bedingung.

8.5 Reduktion indefiniter Formen

Vor: $Q = [a, b, c], \Delta = b^2 - 4ac > 0, \sqrt{\Delta} \notin \mathbb{Q}$ (Δ kein Quadrat in $\mathbb{Z}$) [aber $a, c \neq 0$]
Ärger: Theorie viel komplizierter als bei $\Delta < 0$

Definition

(i) Q heißt halbreduziert $\Leftrightarrow \sqrt{\Delta} - |2a| < b < \sqrt{\Delta}$

(ii) Q heißt reduziert $\Leftrightarrow 0 < b < \sqrt{\Delta} \wedge \sqrt{\Delta} - b < |2a| < \sqrt{\Delta} + b$

Satz 8.7 (Reduktionsungleichungen)
Für eine reduzierte Form $Q = [a, b, c]$ gilt:

$$ac < 0$$

$$0 \overset{(1)}{<} b \overset{(2)}{<} \sqrt{\Delta}$$

$$\sqrt{\Delta} - b \overset{(3)}{<} |2a| \overset{(5)}{<} \sqrt{\Delta} + b$$

$$\sqrt{\Delta} - b \overset{(4)}{<} |2c| \overset{(6)}{<} \sqrt{\Delta} + b$$

Q ist genau dann reduziert, wenn $(2), (3), (4)$ gelten.

Beweis
Abschätzen $\rightsquigarrow$ Netz ■

Folgerung 8.8 (Reduktionskriterium)
Sei Q halbreduziert. Dann ist Q reduziert, wenn eine der folgenden Ungleichungen gilt:

(i) $|a| \leq |c|$

(ii) $\sqrt{\Delta} - b < |2c|$

Beweis
$(2), (3)$ ok bei halbreduzierten Formen

(ii) fordert (4)

(i) Bei $|a| \leq |c| : (3) \Rightarrow (4)$ ■

Bemerkung: Zu $Q = [a, b, c] \exists! t \in \mathbb{Z}$ mit $Q' = \begin{pmatrix} \cdot & 1 \\ -1 & t \end{pmatrix}.Q$ halbreduziert, denn $Q' = [\underbrace{c}_{=a'}, \underbrace{-b + 2ct}_{=b'}, ct^2 - bt + c]$.
Zu erreichen. $\sqrt{\Delta} - \underbrace{|2a'|}_{|2c|} < b' < \sqrt{\Delta} \exists! t$, so dass das stimmt.

Benennungen:

(i) $Q' = [a', b', c']$ heißt rechter (linker) Nachbar von $Q = [a, b, c]$, wenn gilt: $b + b' \equiv 0 \mod 2c$ und $a' = c$ $(a = c')$ und Q' halbreduziert.

(ii) $T =: T_Q$ aus Bew (oder Bem?) heiße Nachbarmatrix (also $Q' = T_Q.Q$)

Leicht zu sehen: Jede QF hat je genau einen reuzierten rechten bzw. linken Nachbarn.

Reduktionsalgorithmus:
Wiederhole das Bilden des rechten Nachbars so lange, bis reduzierte Form erreicht ist.
Wieso terminiert? Ist $Q' = [c, -b + 2ct, c']$ nicht-reduziert, so muss (i) im Reduktionskriteriumg nicht vorliegen, d.h. $|a'| = |c| > |c'|$ (für Q'). Der Koeffizient $|c|$ kann nicht unendlich oft verkleinert werden.

Satz 8.9 (Nachbarreduktionssatz)

(i) Ist $Q = [a, b, c]$ reduziert, so ist auch der rechte Nachbar Q' von Q reduziert und es ist $\operatorname{sign}(a) = -\operatorname{sign}(a')$

(ii) Es gibt nur endlich viele reduzierte Formen.

Beweis

(i) Abschätzen $\rightsquigarrow$ mühsam

(ii) Klar. Nur endlich viele b zu Δ. Nur endlich viele a, c laut Ungleichungen zu $B \Rightarrow$ Algorithmus zur Aufstellung aller reduzierten Formen. ■

$\Delta = -1$ bzw $\Delta = -4m, m \in \mathbb{N}, qf, 2 \nmid m$. Dann: Formen zu Δ stellen $p \in \mathbb{P}$ dar mit $p \mid m$ kann zur Faktorisierung von m ausgenutzt werden. Hierzu schneller, hochgezüchteter Algorithmus von Shanks:

WH: Q indefinit, $\Delta > 0, \sqrt{\Delta} \notin \mathbb{Q}$

1. $Q = [a, b, c]$ halbreduziert $\Leftrightarrow 0 < b < \sqrt{\Delta}, \sqrt{\Delta} - b < |2a| < \sqrt{\Delta} + b$. Rechter (halbreduzierter) Nachbar von Q ist $Q' = [a', b', c'], Q' = \begin{pmatrix} \cdot & 1 \\ -1 & t \end{pmatrix} .Q, t$ mit $\sqrt{\Delta} - |2c| < -bt2ct < \sqrt{\Delta}$. Also $t = \operatorname{sign}(c) \cdot \lfloor \frac{\sqrt{\Delta}+b}{|2c|} \rfloor$.

Algorithmus: Wiederholtes Nachbarbilden ergibt (irgendwann) reduzierte Form.

Sei $Q = Q_0$ reduziert.$Q_{j+1} = Q_j' (j \geq 0)$. Da es nur endlich viele reduzierte Formen gibt, muss vorkommen: $\exists k, l \in \mathbb{N}, l > 0$ mit $Q_k = Q_{k+l}$.
Der reduzierte linke Nachbar ist $Q_{k-1} = Q_{kl-1}$ (da eindeutig bestimmt, usw gibt $Q_0 = Q_l$ (mit $l > 0$)). Ist hier l minimal, so $2 \mid l$ (wegen $\operatorname{sign}(a') = -\operatorname{sign}(a)$)), und $Q_0, ..., Q_{l-1}$ sind alle verschieden.

Benennung:
$\zeta(Q) = [Q_0, Q_1, ..., Q_{l-1}]$ heißt Zyklus von Q (Q reduziert)

Klar: Die Menge der reduzierten Formen zerfällt disjunkt in Zyklen.

Satz 8.10 (Satz von Mertens)
Sei $U \in Sl_2(\mathbb{Z}), U \neq \pm 1_2$. Die Formen Q und $\tilde{Q} := U.Q$ seien reduziert. Dann ist eine der Matrizen $\pm U, \pm U^{-1}$ ein Produkt von Nachbarmatrizen aufeinanderfolgender rechter Nachbarn. Insbesondere sind Q und $\tilde{Q}$ im selben Zyklus.

Folgerung 8.11
Für 2 definite QFen Q_1, Q_2 sei $\Delta > 0$ usw (<- kein Quadrat) und es gilt:
$Q_1 \approx Q_2 \Leftrightarrow \mathrm{red}(Q_2)$ ist im Zyklus $\zeta(\mathrm{red}(Q_1)) \Leftrightarrow \zeta(\mathrm{red}(Q_2)) = \zeta(\mathrm{red}(Q_1))$.

Klar:

1. Es gibt einen Algorithmus, der entscheidet, ob $Q_1 \approx Q_2$ oder nicht
2. Die Zyklen entsprechen den Formklassen zu $\Delta \Rightarrow$ ist Algorithmus, der $h(\Delta)$ berechnet (stelle alle reduzierten Formen auf, berechne Zyklen!).

Zum Beweis des Satzes von Merteus: Viele mühsame Abschätzungen.

$U.Q = (-U).Q, \text{da}\, U = \begin{pmatrix} r & s \\ u & v \end{pmatrix}, -U = \begin{pmatrix} -r & -s \\ -u & -v \end{pmatrix}, 1 = \det U = rv - us.\ U^{-1} = \begin{pmatrix} v & -s \\ -u & r \end{pmatrix}, -U^{-1} = \begin{pmatrix} -v & s \\ u & -r \end{pmatrix}$.

Die richtige Wahl entscheidet sich für passende positive Vorzeichen.
Ohne Einschränkung $r > 0, v > 0$, setzte $U' = UT_Q^{-1} = \begin{pmatrix} r' & s' \\ u' & v' \end{pmatrix}$. Man zeigt: IU, IU^{-1} keine Nachbarmatrix $\neq \pm 1 \Rightarrow 0 < r' < r$
Induktionshypothese für $U', Q' \Rightarrow$ Behauptung.

Über $h(\Delta)$ und Struktur der Klassengruppe bei $\Delta > 0$ „fast“ keine allgemeine Sätze bekannt. Unbekannt z.B: existieren unendlich viele Δ mit $h(\Delta) = 1$?

8.6 Automorphismengruppen

Definition

(i) $U \in Sl_2(\mathbb{Z})$ heißt <u>eigentlicher Automorphismus</u> der QF $Q = [a,b,c] :\Leftrightarrow U.Q = Q$.

(ii) $Aut_+(Q) = \{U \in Sl_2(\mathbb{Z}) : U.Q = Q\}$ (ist UGR von $Sl_2(\mathbb{Z}) \rightsquigarrow$ Untergruppenkriterium) heißt <u>eigentliche Automorphismengruppe</u> von Q.

Beweis

(i) $\Delta > 0 \Rightarrow \mathrm{Aut}_+(Q)$ abelsch und $\#\mathrm{Aut}(Q) = \infty . Q(\Delta) = k, U \in \mathrm{Aut}_+(Q) \Rightarrow k = U.Q(\underline{x}) = Q(\underline{x}U)$. Mit $\underline{x}$ stellt auch $\underline{x}U$ die Zahl k dar $\Rightarrow$ existieren unendlich viele $\underline{y} \in \mathbb{Z}^2 : Q(\underline{y}) = k$. Man kann zeigen: Es gibt $\underline{x}_1, ...\underline{x}_l, l \in \mathbb{N}_+$, so dass $\{\underline{x} \big| Q(\underline{x}) = k\} = \underline{x}_1 G \dot\cup .. \dot\cup \underline{x}_l G$ mit $G = \mathrm{Aut}_+(Q)$ (falls k überhaupt darstellbar) ∎

Definition
$[Q_0, ..., Q_{2l-1}] = \zeta(Q), Q = Q_0$ reduziert. Die Matrix $-T_Q, T_Q =: R$ heißt Doppelnachbarmatrix zu Q (Q' rechter Nachbar). $B : R_{2l-2} \cdot ... \cdot R_2 \dot{R}_0$ heißt Grundmatrix zu Q.

Klar nach Definition: $B.Q = Q$, d.h. $B \in \mathrm{Aut}_+(Q)$. Betrachte $V \in \mathrm{Aut}_+(Q)$, so $\pm V, \pm V^{-1}$ (eines davon) nach Satz von Mertes ein Produkt von Nachbarmatrizen.

$\Rightarrow$ Eine dieser Matrizen ist Potenz von B! [würde sonst irgendwo mitten im Zyklus stehenbleiben]

Satz 8.12
$\mathrm{Aut}_+(Q) = \{\pm B^m \big| m \in \mathbb{Z}\}$ ist sogar abelsch.

Wieso unendlich? Man zeigt leichct: R hat alle Koeffizienten $> 0 \Rightarrow B$ auch $\Rightarrow$ Alle Matrizen $\pm B^m$ sind verschieden.

Es gibt auch Aussagen für nicht-reduziertes Q. Ist $Q' = V.Q, V \in Sl_2(\mathbb{Z})$, so ist die Abbildung $\phi : \mathrm{Aut}_+(Q) \to \mathrm{Aut}_+(Q'), U \mapsto VUV^{-1} =: \phi(U)$ ein Isomorphismus von Gruppen.

Moderne Theorie: Theorie der QFen zu Δ weitgehend äquivalent zur algZT in quadratischem „Zahlkörper“ $K = Q(\sqrt{\Delta})$. Norm $n(a + b\sqrt{\Delta}) = (a + b\sqrt{\Delta})(a - b\sqrt{\Delta}) = a^2 - b^2\Delta$ ist QF für a,b.