Skript zum

Proseminar

im Rahmen der Weiterbildung für Lehrer

in der Fassung vom Dezember 2019

V. Schulze FU Berlin

Themen zum Proseminar

Anmerkung: Die mit * gekennzeichneten Vorträge sind von einem etwas höheren Schwierigkeitsgrad.

Ergänzungen

1. Vortrag

Komplexe Zahlen und Einheitswurzeln

(Die komplexen Zahlen werden benötigt zum Vortrag: Der Gaußsche Zahlring)

Menge der komplexen Zahlen: $\mathbb{C} := \{a+bi \mid a,b \in \mathbb{R}\}$ (Ist nur eine andere Schreibweise für das Cartesische Produkt $\mathbb{R} \times \mathbb{R}$)

$a+bi = c+di \Leftrightarrow a=c, b=d$

Auf $\mathbb{C}$ werden zwei Verknüpfungen definiert durch

$(a+bi)+(c+di) := (a+c)+(b+d)i,$

$(a+bi)\cdot(c+di) := (ac-bd)+(ad+bc)i$

$(\mathbb{C},+,\cdot)$ ist ein kommutativer Ring (leicht nachzurechnen)

Schreibweise: $a+0\cdot i = a$ (in diesem Sinn ist $\mathbb{R} \subseteq \mathbb{C}$ und auch $(\mathbb{R},+,\cdot)$ Unterkörper von $\mathbb{C}$).

$0+bi = bi$

$1\cdot i = i$, $(-1)\cdot i = -i$, $a+(-b)\cdot i = a-bi$, $a+bi = a+ib$, $a+bi = bi+a$.

Es gilt $i^2=-1$, $i^3=-i$, $i^4=1$

$a(b+ci) = ab+aci$

$(a+bi)(a-bi) = a^2+b^2$

Für $a^2+b^2 \neq 0$ gilt $(a+bi)\cdot\underbrace{\left(\frac{a}{a^2+b^2} - \frac{b}{a^2+b^2}i\right)}_{=(a+bi)^{-1} = \frac{1}{a+bi}} = 1$ (Schreibweise)

Aus den obigen Rechenregeln folgt

<u>Bem 1</u> $(\mathbb{C},+,\cdot)$ ist ein Körper (Körper der komplexen Zahlen)

Sei $z := a+bi \in \mathbb{C}$.

$\bar{z} := a-bi$ heißt die zu z konjugiert komplexe Zahl

$a =: \operatorname{Re} z$ heißt Realteil von z

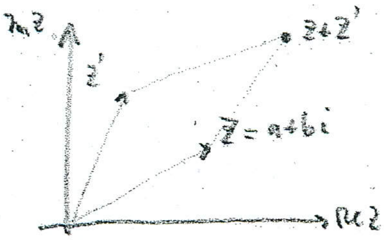
$b =: \operatorname{Im} z$ heißt Imaginärteil von z beachte: $\operatorname{Im} z \in \mathbb{R}$.

Es gilt $z\cdot\bar{z} = a^2+b^2$; $\overline{z_1\cdot z_2} = \bar{z}_1\cdot\bar{z}_2$ (leicht nachzurechnen)

$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{c^2+d^2}$ (falls $c^2+d^2 \neq 0$)

<u>Bsp</u> $\frac{1}{i} = -i$, $\frac{1}{1+i} = \frac{1-i}{(1+i)(1-i)} = \frac{1}{2} - \frac{1}{2}i$.

<u>Gaußsche Zahlenebene</u>



Den komplexen Zahlen werden bijektiv die Punkte der Gaußschen Zahlenebene zugeordnet bzw. Ortsvektoren.

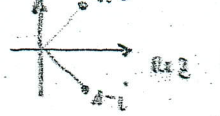
Der Addition in $\mathbb{C}$ entspricht offenbar die Vektoraddition in der Gaußschen Zahlenebene.

$|z| := \sqrt{a^2+b^2}$ (Abstand von z zum Nullpunkt) (Betrag von z)

Es gilt $|z|^2 = z\cdot\bar{z}$.

$\bar{z}$ entsteht aus z durch Spiegelung an der Re-Teil-Achse.

<u>Bsp</u>



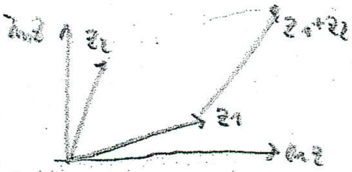
$|1+i| = \sqrt{2}$

Rechenregeln

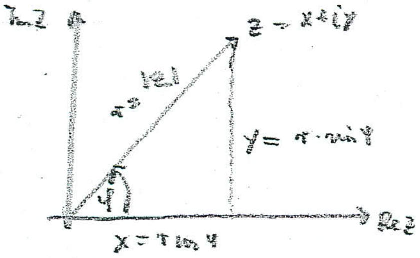
(i) $\overline{z_1 \pm z_2} = \overline{z_1} \pm \overline{z_2}$ ✓

(ii) $|z_1 \cdot z_2| = |z_1| \cdot |z_2|$ $\quad [\,|z_1 \cdot z_2|^2 = z_1 z_2 \overline{z_1 z_2} = z_1 \overline{z_1}\, z_2 \overline{z_2} = |z_1|^2 \cdot |z_2|^2\,]$

(iii) $|z_1 + z_2| \le |z_1| + |z_2|$ (Δ-Ungleichung) [läßt sich elementar nachrechnen; ist anschaulich geometrisch klar in der Gaußschen Zahlenebene]



Polarkoordinaten bei $z \neq 0$.



$z = x+iy = \underbrace{r}_{=|z|} \underbrace{(\cos\varphi + i\sin\varphi)}_{\text{hat Betrag 1}}$; $\underbrace{\arg z := \varphi}_{\text{bis auf Vielfache von } 2\pi \text{ eindeutig bestimmt.}}$

$r = |z| = \sqrt{x^2+y^2}$.

(Für $z=0$ ist $r=0$ und $\arg z$ nicht def.)

Es gilt $\arg \bar{z} = -\arg z$.

Geometrische Bedeutung der Multiplikation

Sei $z_1 = r_1(\cos\varphi_1 + i\sin\varphi_1)$; $r_1 = |z_1|$

$z_2 = r_2(\cos\varphi_2 + i\sin\varphi_2)$; $r_2 = |z_2|$

Dann gilt

$$z_1 \cdot z_2 = \underbrace{r_1 \cdot r_2}_{=|z_1|\cdot|z_2|} \cdot \Big[\underbrace{(\cos\varphi_1\cos\varphi_2 - \sin\varphi_1\sin\varphi_2)}_{=\cos(\varphi_1+\varphi_2)} + i\underbrace{(\cos\varphi_1\sin\varphi_2 + \cos\varphi_2\sin\varphi_1)}_{=\sin(\varphi_1+\varphi_2)}\Big]$$

(Additionstheoreme für sin und cos)

Polarkoordinatendarstellung für $z_1 \cdot z_2$:

$$z_1 \cdot z_2 = \underbrace{|z_1|\cdot|z_2|}_{=|z_1\cdot z_2|}\,(\cos(\varphi_1+\varphi_2) + i\sin(\varphi_1+\varphi_2)).$$

(Produkt der Beträge; Addition der Winkel)

Bsp $(1+i)^2 = 2i$
$(-1+i)^2 = -2i$ (rechne nach und deute das Ergebnis geometrisch)

Potenzen komplexer Zahlen

Sei $z = r(\cos\varphi + i\sin\varphi)$.

Dann: $z^n = r^n \cdot (\cos n\varphi + i\sin n\varphi)$

Im Fall $r=1$ folgt

$$(\cos\varphi + i\sin\varphi)^n = \cos n\varphi + i\sin n\varphi \quad \text{(Formel von Moivre)}$$

Bsp Berechne $\left(\frac{1+i}{\sqrt{2}}\right)^j$ für $j = 2,3,4,\dots$ (durch Ausmultiplizieren und geometrisch)

Inverse komplexer Zahlen

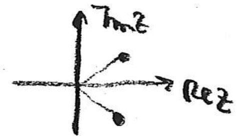
Sei $z \neq 0$.

Dann gilt: $\arg \underbrace{z \cdot \frac{1}{z}}_{=1} = 0 \overset{\text{s. Multiplikation komplexer Zahlen}}{=} \arg z + \arg \frac{1}{z}$; also $\arg \frac{1}{z} = -\arg z$.

Ferner gilt: $\left| z \cdot \frac{1}{z} \right| = 1 \overset{\text{beachte: Der Betrag ist multiplikativ}}{=} |z| \cdot \left|\frac{1}{z}\right|$, also $\left|\frac{1}{z}\right| = \frac{1}{|z|}$.

Es folgt für $z = |z|(\cos\varphi + i\cdot\sin\varphi)\ (\neq 0)$:

$$\frac{1}{z} = \frac{1}{|z|}\left(\cos(-\varphi) + i\sin(-\varphi)\right)$$ (Polarkoordinatendarstellung von $\frac{1}{z}$).



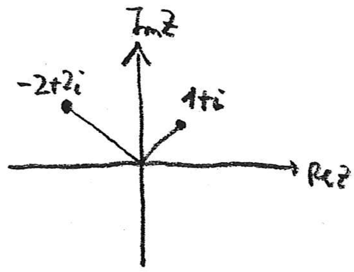
Für $|z| = 1$ folgt speziell: $\frac{1}{z} = \bar{z}$.

Bsp 1 $i = \cos 90° + i\sin 90°$, also $\frac{1}{i} = \cos(-90°) + i\sin(-90°) = -i$.

Bsp 2 Es gilt $\frac{-2+2i}{1+i} = 2i$.

Man rechne dies direkt nach.

Man ermittle das Ergebnis geometrisch.



Bsp 3

Sei $T_6 := \cos 60° + i \cdot \sin 60° = \frac{1}{2} + i\frac{\sqrt{3}}{2}$.

Speziell ist $|T_6| = 1$.

Man zeige: $T_6^2 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $T_6^3 = -1$, $T_6^4 = -\frac{1}{2} - \frac{i\sqrt{3}}{2}$, $T_6^5 = \frac{1}{2} - i\frac{\sqrt{3}}{2}$; $T_6^6 = 1$

Argumentiere dabei geometrisch.

Also ist T_6 eine 6-te Wurzel aus 1.

Wurzeln komplexer Zahlen

Sei $z \neq 0$, $z = |z|(\cos\varphi + i\sin\varphi)$ (Polarkoordinatendarstellung von z).

$a \in \mathbb{C}$ heißt n-te Wurzel von z, wenn $a^n = z$ ist.

Schreibweise für a: $\sqrt[n]{z}$, Achtung: $\sqrt[n]{z}$ ist nicht eindeutig, z.B. ist $\sqrt[2]{1} = 1$ und $\sqrt[2]{1} = -1$

Mit $\sqrt[n]{z}$ wird auch die Menge aller n-ten Wurzeln von z bezeichnet.

Ziel: Bestimme alle n-ten Wurzeln von z (in Polarkoordinatendarstellung).
Aus der geometrischen Deutung der Multiplikation ergibt sich:
Jede n-te Wurzel von z besitzt den Betrag $\sqrt[n]{|z|}$ (positive reelle Wurzeln).

Sei α der Winkel, der zu einer n-ten Wurzel von z gehört.

Dann gilt: $n \cdot \alpha = \varphi + \gamma \cdot 2\pi$ mit $\gamma \in \mathbb{Z}$ (beachte: Der zu einer Komplexen Zahl gehörige Winkel ist nur eindeutig bis auf ganzzahlige Vielfache von 2π).

Die möglichen Winkel für die n-ten Wurzeln aus z sind also genau

$$\frac{\varphi}{n} + \frac{\gamma\, 2\pi}{n} \quad \text{mit } \gamma \in \mathbb{Z}. \qquad (*)$$

Die verschieden möglichen Winkel sind also $\frac{\varphi}{n} + \frac{\gamma \cdot 2\pi}{n}$ für $\gamma = 0, \dots, n-1$
(alle anderen Winkel in $(*)$ unterscheiden sich von diesen nur um Vielfache von 2π).

Also folgt:

Die n-ten Wurzeln von z sind

$$\sqrt[n]{|z|}\left(\cos\frac{\varphi + \gamma \cdot 2\pi}{n} + i\sin\frac{\varphi + \gamma \cdot 2\pi}{n}\right) \text{ für } \gamma = 0, \dots, n-1.$$

Speziell: z besitzt genau n verschiedene n-te Wurzeln.
Diese haben alle den gleichen Betrag; die Winkel unterscheiden sich um Vielfache von $\frac{2\pi}{n}$.

Bsp 4 Man zeige $\sqrt{-i} = \left\{\frac{-1+i}{\sqrt{2}}, -\frac{-1+i}{\sqrt{2}}\right\}$

$\frac{1+i}{\sqrt{2}}$ ist eine 8. Wurzel aus 1; man gebe alle 8-ten Wurzeln von 1 an.

Man zeige: $1+i$ ist eine 4-te Wurzel aus 1.
Man gebe alle 4-ten Wurzeln aus 1 an.

Die n-ten Einheitswurzeln

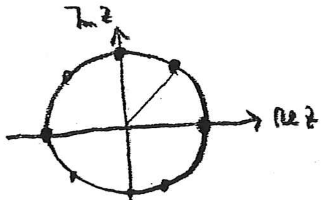
Die n-ten Wurzeln aus 1 heißen n-te Einheitswurzeln.
Die Polarkoordinatendarstellung von 1 ist

$$1 = 1 \cdot (\cos 0 + i \sin 0).$$

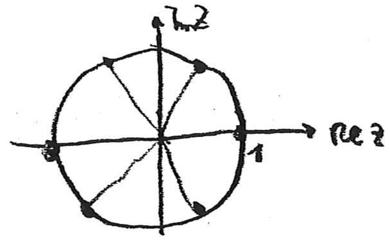
Die n-ten Einheitswurzeln sind also

$$\cos \frac{\nu 2\pi}{n} + i \sin \frac{\nu 2\pi}{n} \quad \text{für } \nu = 0, \dots, n-1.$$

(Für $\nu = 0$ erhält man 1 als n-te Einheitswurzel)



Die 8-ten Einheitswurzeln



Die 6-ten Einheitswurzeln.

In der Gaußschen Zahlenebene liegen die n-ten Einheitswurzeln alle auf dem Kreis um 0 vom Radius 1 und bilden die Eckpunkte eines regelmäßigen n-Ecks.

Für $\nu = 1$ erhält man die n-te Einheitswurzel

$$\zeta_n := \cos \frac{2\pi}{n} + i \sin \frac{2\pi}{n}.$$

Die n-ten Einheitswurzeln sind dann

$$1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}.$$

(Dies ergibt sich aus der geometrischen Deutung der Multiplikation)

Anmerkung: Multipliziert man eine komplexe Zahl z mit ζ_n, so bedeutet dies geometrisch eine Drehung von z um den Nullpunkt mit dem Drehwinkel $\frac{2\pi}{n}$.

Anmerkung: Offenbar ist $\zeta_n^{n-1} = \overline{\zeta_n} = (\zeta_n)^{-1}$ (Begründung?)

2. Vortrag:

Elementare Eigenschaften der Primzahlen

Def 1 Sei $p \in \mathbb{N}$ und $p \neq 1$. Dann:

p Primzahl $:\Leftrightarrow$ p hat in $\mathbb{N}$ nur die (sogenannten) trivialen Teiler 1 und p.

Bem 1 Die ersten Primzahlen sind $2, 3, 5, 7, \dots$

Def 2 Sei $p \in \mathbb{Z}$, $p \neq \pm 1$. Dann:

p Primelement in $\mathbb{Z}$ $:\Leftrightarrow$ p hat in $\mathbb{Z}$ nur die (sogenannten) trivialen Teiler $\pm 1, \pm p$.

Bem 2 Primelemente in $\mathbb{Z}$ sind $\pm 2, \pm 3, \pm 5, \pm 7, \dots$

Def 3 Sei $\mathbb{P} = \{2, 3, 5, 7, \dots\}$ die Menge aller Primzahlen.
Es bezeichne p_n die n-te Primzahl (also $p_1 = 2, p_2 = 3, p_3 = 5, \dots$).

Sei $x \in \mathbb{R}$. Dann bezeichne

$\pi(x)$ die Anzahl aller Primzahlen $\leq x$.

$\pi : \mathbb{R} \to \mathbb{N} \cup \{0\}$ heißt Primzahlfunktion.

Bekanntlich gilt

Satz 1 (Fundamentalsatz der Zahlentheorie) (ohne Bew)
Jedes $n \in \mathbb{N}$ mit $n > 1$ läßt sich (bis auf die Reihenfolge der Faktoren eindeutig) darstellen als Produkt von Primzahlen.

Bem 3 Sei $2\mathbb{N} := \{2n \mid n \in \mathbb{N}\}$ die Menge aller geraden natürlichen Zahlen. Sei $p \in 2\mathbb{N}$. Dann:
p Primzahl in $2\mathbb{N}$ $:\Leftrightarrow$ p besitzt in $2\mathbb{N}$ keinen Teiler
(d.h. p läßt sich nicht darstellen in der Form $p = a \cdot b$ mit $a, b \in 2\mathbb{N}$)

Zum Beispiel sind $2, 2\cdot 5, 2\cdot 7, 2\cdot 5\cdot 7$ Primzahlen in $2\mathbb{N}$.

Es gilt $(2\cdot 5)\cdot(7\cdot 2) = (2\cdot 5\cdot 7)\cdot 2$.

Also gibt es in $2\mathbb{N}$ Elemente, die sich auf unterschiedliche Weise als Produkt von Primzahlen aus $2\mathbb{N}$ darstellen lassen.

Man zeige, daß sich jedes Element aus $2\mathbb{N}$ als Produkt von Primzahlen in $2\mathbb{N}$ darstellen läßt.

Man zeige: Die Primzahlen in $2\mathbb{N}$ sind genau die Elemente $2n$ mit $n \in \mathbb{N}$, n ungerade.

Eine gute Abschätzung für die Anzahl aller Primzahlen $\leq x$ gibt der folgende Satz

<u>Satz 2</u> (Primzahlsatz) (ohne Beweis)

$$\pi(x) \sim \frac{x}{\ln x} \qquad \left(\text{d.h. } \lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1\right)$$

Ferner gilt $p_n \sim n \cdot \ln n$ $\left(\text{d.h. } \lim_{n\to\infty} \frac{p_n}{n\cdot \ln n} = 1\right)$

<u>Bem 4</u> (p_i, p_j) heißen Primzahlzwillinge, wenn p_i, p_j Primzahlen sind und $p_j - p_i = 2$ ist.

z.B. sind $(3,5)$, $(5,7)$, $(11,13)$ Primzahlzwillinge.

Es wird vermutet, daß es unendlich viele Primzahlzwillinge gibt.

<u>Satz 3</u> (Dirichletscher Primzahlsatz). (ohne Bew)

Sei $n \in \mathbb{N}$, $a \in \mathbb{N}$ und $\mathrm{ggT}(a,n) = 1$.

Sei $\pi_{a,n}(x) :=$ Anzahl aller Primzahlen p mit $p \leq x$ und $p \equiv a \pmod n$.

Dann: $\pi_{a,n}(x) \sim \frac{1}{\varphi(n)} \frac{x}{\ln x}$.

Dabei ist $\varphi(n) :=$ Anzahl aller $x \in \mathbb{N}$ mit $1 \leq x \leq n$: $\mathrm{ggT}(x,n) = 1$ (Eulersche φ-Funktion).

[warum ist die Voraussetzung $\mathrm{ggT}(a,n) = 1$ notwendig?]

<u>Satz 4</u>

Es existieren unendlich viele Primzahlen.

Genauer gilt:

(i) $p_n \leq 2^{(2^{n-1})}$ f. a. $n \in \mathbb{N}$

(ii) $\pi(n) > \ln\ln n$ f. a. $n \in \mathbb{N}$, $n \geq 2$.

<u>Beweis</u>

(i) Seien $p_1, \dots, p_n$ die ersten n Primzahlen.

Dann gilt $p_i \nmid (p_1 \cdots p_n + 1)$ für $i = 1, \dots, n$.

(Andernfalls wäre p_i Teiler von $p_1 \cdots p_n + 1$ und von $p_1 \cdots p_n$, also auch Teiler von $(p_1 \cdots p_n + 1) - p_1 \cdots p_n = 1$)

Andererseits ist $p_1 \cdots p_n + 1 > 1$, also ist nach Satz 1 $p_1 \cdots p_n + 1$ darstellbar als Produkt von Primzahlen.

Diese sind aber von $p_1, \dots, p_n$ verschieden und $\leq p_1 \cdots p_n + 1$.

Also existiert p_{n+1} und es gilt $p_{n+1} \leq p_1 \cdots p_n + 1$ (*)

Nun wird (i) durch vollständige Induktion bewiesen:

Ind. Beginn: Für $n = 1$ ist die Behauptung richtig: $p_1 = 2 \leq 2^{(2^0)} = 2$.

Schluß von n auf $n+1$:

$$p_{n+1} \underset{(*)}{\leq} p_1 \cdots p_n + 1 \underset{\boxed{\text{Ind.Vor.}}}{\leq} 2^{2^0} \cdots 2^{(2^{n-1})} + 1 = 2^{(2^n - 1)} + 1$$

$\boxed{\text{beachte: } 1 + 2 + \dots + 2^{n-1} = 2^n - 1 \text{ (geometrische Summe)}}$

$$\leq 2 \cdot 2^{(2^n - 1)} = 2^{(2^n)}.$$

(ii) Sei $n \in \mathbb{N}$, $n \geq 2$ gegeben.

Sei $K \in \mathbb{Z}$ so gewählt, daß $2^{(2^{K-1})} \leq n < 2^{(2^K)}$.

Dann folgt $\ln\ln n < \ln\ln 2^{(2^K)} < \ln\ln e^{(e^K)} = K \underset{(i)}{\leq} \pi\left(2^{(2^{K-1})}\right) \leq \pi(n)$.

<u>Bem 5</u>

Analog zu Satz 4 läßt sich beweisen, daß es unendlich viele Primzahlen

$$p \equiv 3 \pmod 4$$

gibt.

Sind $q_1, \dots, q_n$ die ersten n Primzahlen $\equiv 3 \pmod 4$, so betrachte man

$$(q_1 \cdots q_n)^2 + 2.$$

3. Vortrag

Eine Abschätzung für die n-te Primzahl

Für $n \in \mathbb{N}$ sei p_n die n-te Primzahl, also
$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7, \ldots$.

Für $x \in \mathbb{R}$ sei $\pi(x)$ die Anzahl aller Primzahlen $\leq x$.

Zum Beispiel ist $\pi(1) = 0,\ \pi(2) = 1,\ \pi(6) = 3$.

Das Hauptziel besteht darin zu zeigen, daß es für alle $n \in \mathbb{N}$ mindestens n Primzahlen $\leq 4^n$ gibt.
Speziell folgt daraus, daß es unendlich viele Primzahlen gibt.

Def 1

Sei $n \in \mathbb{N}$ und $x \in \mathbb{N}$ gegeben.
Dann bezeichne $N_n(x)$ die Anzahl aller natürlichen Zahlen $\leq x$, in deren Primfaktorzerlegung höchstens die ersten n Primzahlen $p_1, \ldots, p_n$ vorkommen.

Bsp (i) Sei $n = 3$, $x = 10$.

Dann ist $N_n(x) = N_3(10) = 9$

(ii) $n = 5$ (zu berücksichtigen sind also die 5 Primzahlen 2, 3, 5, 7, 11)

Sei $x = 30$

Die natürlichen Zahlen ≤ 30, die eine Primzahl > 11 als Teiler besitzen, sind $13,\ 2 \cdot 13,\ 17,\ 19,\ 23,\ 29$.

Also ist $N_5(30) = 30 - 6 = 24$.

Bem 1 Sei $n \in \mathbb{N}$ und $x \leq p_n$.

Dann ist $N_n(p_n) = p_n$.

Bew Keine natürliche Zahl $x \leq p_n$ besitzt eine Primzahl $> p_n$ als Teiler.

Bem 2

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

Dann läßt sich n darstellen in der Form

$$n = n_2 \cdot n_1^2 ,$$

wobei $n_1 \in \mathbb{N}$ ist und n_2 das Produkt paarweise verschiedener Primzahlen

Bew Betrachte die Primfaktorzerlegung

$$n = q_1^{a_1} \cdot \ldots \cdot q_r^{a_r} \quad ; \quad q_1, \ldots, q_r \text{ paarweise verschiedene Primzahlen;} \quad a_1, \ldots, a_r \in \mathbb{N}$$

von n und spalte von der größtmögliche Quadrat n_1^2 als Faktor ab.

Satz 1

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

Dann gilt für alle $x \in \mathbb{N}$

$$N_n(x) \leq 2^n \cdot \sqrt{x} .$$

Bew

$N_n(x)$ ist nach Definition die Anzahl aller natürlichen Zahlen m mit: $m \leq x$ und in der Primfaktorzerlegung von m treten höchstens die Primzahlen $p_1, \ldots, p_n$ auf.

Eine solche Zahl m läßt sich nach Bem 2 darstellen in der Form

$$m = 2^{a_1} \cdot 3^{a_2} \cdot 5^{a_3} \cdots p_n^{a_n} \cdot n_1^2 \qquad (*)$$

mit $n_1 \in \mathbb{N}$, wobei $a_1, a_2, \ldots, a_n$ die Werte Null oder Eins annehmen können.

Für $n = 3$ und $m = 90$ gilt zum Beispiel

$$m = 90 = 2 \cdot 5 \cdot 3^2 = 2^1 \cdot 3^0 \cdot 5 \cdot 3^2 ; \text{ also } n_1 = 3.$$

Für $n = 3$ und $m = 200$ gilt zum Beispiel

$$m = 200 = 2^3 \cdot 5^2 = 2^1 \cdot 3^0 \cdot 5^0 \cdot (2 \cdot 5)^2 ; \text{ also } n_1 = 10.$$

Nun soll $N_n(x)$ abgeschätzt werden.

Bei der Darstellung einer natürlichen Zahl $m \leq x$ mit der Eigenschaft (*) gibt es für n_1 höchstens $\sqrt{x}$ Möglichkeiten (da $n_1^2 \leq m \leq x$) und für die $a_1, \dots, a_n$ höchstens 2^n Möglichkeiten (da die $a_1, \dots, a_n$ nur die beiden Werte 0 oder 1 annehmen können.

Also ist $N_n(x) \leq 2^n \cdot \sqrt{x}$.

Natürlich gilt hier nicht das Gleichheitszeichen, da wegen $m \leq x$ nicht unbedingt alle Kombinationsmöglichkeiten auftreten.

Damit ist Satz 1 bewiesen.

<u>Satz 2</u>

Es gibt unendlich viele Primzahlen.

<u>Bew</u>

Annahme: Es gibt nur die endlich vielen Primzahlen $p_1, \dots, p_n$.

Wir leiten daraus einen Widerspruch her.

Aus der Annahme folgt, daß sich jede natürliche Zahl als Produkt von $p_1, \dots, p_n$ darstellen läßt, also $N_n(x) = x$ für alle $x \in \mathbb{N}$.

Nach Satz 1 folgt

$$x = N_n(x) \leq 2^n \sqrt{x} \quad \text{für alle } x \in \mathbb{N},$$

also

$$x \leq 4^n \quad \text{für alle } x \in \mathbb{N}.$$

Dies ist ein Widerspruch, da n eine feste natürliche Zahl ist.

Damit ist Satz 2 bewiesen.

Eine Verschärfung von Satz 2 ist

<u>Satz 3</u>

Für $n \in \mathbb{N}$ gibt es mindestens n Primzahlen $\leq 4^n$.

<u>Bew</u>

Sei p_n die n-te Primzahl. Dann gilt

$$N_n(p_n) \underset{\text{Bem 1}}{=} p_n \underset{\text{Satz 1}}{\leq} 2^n \sqrt{p_n}, \text{ also } p_n \leq 4^n.$$

Die n-te Primzahl p_n ist also $\leq 4^n$.

<u>Anmerkung 1</u>

Man kann mit dieser Methode auch beweisen, daß die Reziprokensumme

$$\sum_{n=1}^{\infty} \frac{1}{p_n}$$

divergiert. (ohne Bew).

<u>Satz 4</u> Für $m \geq 4$ gilt $\pi(m) > \frac{\ln m}{\ln 4} - 1$.

<u>Beweis</u>

Sei $m \in \mathbb{N}$, $m \geq 4$.
Wähle $n \in \mathbb{N}$ so, daß $4^n \leq m < 4^{n+1}$ gilt.

Dann ist $n > \frac{\ln m}{\ln 4} - 1$. (*)

Es folgt $\pi(m) \geq \pi(4^n) \underset{\text{Satz 3}}{\geq} n > \frac{\ln m}{\ln 4} - 1$.

<u>Anmerkung 2</u>

Die Abschätzungen von Satz 3 und Satz 4 lassen sich stark verbessern.

Nach dem Primzahlsatz (ohne Bew.) gilt:

$\pi(n) \sim \frac{n}{\ln n}$, d.h. $\lim\limits_{n\to\infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1$ und

$p_n \sim n \ln n$, d.h. $\lim\limits_{n\to\infty} \frac{p_n}{n \cdot \ln n} = 1$.

4. Vortrag und 5. Vortrag

Die Reziprokensumme der Primzahlen

Für $n \in \mathbb{N}$ sei p_n die n-te Primzahl und
$\pi(n)$ die Anzahl aller Primzahlen $\leq n$.
Zum Bsp. ist $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7, \ldots$.
$\pi(1) = 0$, $\pi(2) = 1$, $\pi(6) = 3$, $\pi(10) = 4, \ldots$.

Eine gute Abschätzung für p_n und $\pi(n)$ liefert der Primzahlsatz

Satz 1

$$\pi(n) \sim \frac{n}{\ln n} \; ; \text{ d.h. } \lim_{n \to \infty} \frac{\pi(n)}{\frac{n}{\ln n}} = 1,$$

$$p_n \sim n \cdot \ln n \; ; \text{ d.h. } \lim_{n \to \infty} \frac{p_n}{n \cdot \ln n} = 1.$$

Der Beweis ist sehr aufwändig.

Hier sollen die folgenden schwächeren Aussagen bewiesen werden:

Satz 2

Für alle $n \in \mathbb{N}$, $n \geq 2$ gilt

(a) $p_n < e^{n+1}$

(b) $\pi(n) > \ln n - 1$

(c) $\frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \ldots + \frac{1}{p_n} > \ln \ln n - 1.$

Anmerkung

Sei $\mathbb{P} := \{2, 3, 5, 7, \ldots\}$ die Menge aller Primzahlen.
Aus Satz 2 (c) folgt:
$\sum_{p \in \mathbb{P}} \frac{1}{p}$ ist divergent (Reziprokensumme der Primzahlen)
Die Reihe divergiert allerdings sehr langsam;
Es gilt $\ln \ln (50 \cdot 10^6) \approx 2{,}875$.
Die Reziprokensumme der Primzahlen für die ersten 50 Millionen Primzahlen ist zB. ≤ 4.

$\frac{1}{1-x} = 1 + x + x^2 + \dots$

Potenzreihen dürfen gliedweise integriert werden, also

$\ln\frac{1}{1-x} = -\ln(1-x) = x + \frac{x^2}{2} + \frac{x^3}{3} + \dots + C \quad (C = 0, \text{ da für } x = 0 \ldots)$

Beweis (v. Satz 2)

Benutzt wird die aus der Analysis bekannte Reihenentwicklung

$$(1) \quad \ln\frac{1}{1-x} = \sum_{\nu=1}^{\infty} \frac{x^\nu}{\nu} \quad \text{für} \quad -1 \le x < 1 .$$

jeder der endlichen vielen ∞ Reihe wird an 1. Summand hervorgezogen

Es folgt

$$(2) \quad \ln \prod_{\substack{p \le n \\ p \in \mathbb{P}}} \frac{1}{1-\frac{1}{p}} = \sum_{\substack{p \le n \\ p \in \mathbb{P}}} \underbrace{\ln\frac{1}{1-\frac{1}{p}}}_{\overset{(1)}{=} \sum_{\nu=1}^{\infty} \frac{1}{\nu \cdot p^\nu}} = \sum_{\substack{p \le n \\ p \in \mathbb{P}}} \frac{1}{p} + \sum_{\substack{p \le n \\ p \in \mathbb{P}}} \sum_{\nu=2}^{\infty} \frac{1}{\nu \cdot p^\nu} .$$

Für den Term rechts erhält man die Abschätzung

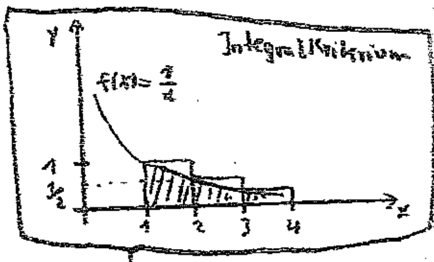
$$(3) \quad \sum_{\substack{p \le n \\ p \in \mathbb{P}}} \sum_{\nu=2}^{\infty} \frac{1}{\nu \cdot p^\nu} \le 1$$

wie folgt:

$$\sum_{p \in \mathbb{P}} \sum_{\nu=2}^{\infty} \frac{1}{\nu \cdot p^\nu} \le \frac{1}{2} \sum_{p \in \mathbb{P}} \sum_{\nu=2}^{\infty} \frac{1}{p^\nu} = \frac{1}{2} \sum_{p \in \mathbb{P}} \Big(\frac{1}{p^2} \underbrace{\sum_{\nu=0}^{\infty} \frac{1}{p^\nu}}_{= \frac{1}{1-\frac{1}{p}} \le \frac{1}{1-\frac{1}{2}} = 2} \Big) \le \sum_{p \in \mathbb{P}} \frac{1}{p^2}$$

$$\le \sum_{\substack{n \in \mathbb{N} \\ n \ge 2}} \frac{1}{n^2} \le \frac{1}{2 \cdot 1} + \frac{1}{3 \cdot 2} + \frac{1}{4 \cdot 3} + \dots = \left(1 - \frac{1}{2}\right) + \left(\frac{1}{2} - \frac{1}{3}\right) + \left(\frac{1}{3} - \frac{1}{4}\right) + \dots = 1 .$$

Gebraucht wird ferner die Abschätzung



$$(4) \quad \prod_{\substack{p \le n \\ p \in \mathbb{P}}} \frac{1}{1-\frac{1}{p}} > \ln n ,$$

die sich wie folgt ergibt:

$$\prod_{\substack{p \le n \\ p \in \mathbb{P}}} \frac{1}{1-\frac{1}{p}} = \prod_{\substack{p \le n \\ p \in \mathbb{P}}} \left(1 + \frac{1}{p} + \frac{1}{p^2} + \dots\right) = \sum_{n' \in \mathbb{N}'} \frac{1}{n'} \ge \sum_{n' \le n} \frac{1}{n'} > \int_1^n \frac{1}{u}\, du = \ln n .$$

$\mathbb{N}' := \{ n \in \mathbb{N} \mid n \text{ besitzt nur Primteiler} \le n \}$

Beweis von (c):

$$\ln \ln n \underset{(4)}{<} \ln \prod_{\substack{p \leq n \\ p \in \mathbb{P}}} \frac{1}{1-\frac{1}{p}} \underset{(2),(3)}{\leq} \sum_{\substack{p \leq n \\ p \in \mathbb{P}}} \frac{1}{p} + 1$$

Beweis von (b):

$$\ln n < \prod_{\substack{p \leq n \\ p \in \mathbb{P}}} \frac{1}{1-\frac{1}{p}} \leq \prod_{m=2}^{\pi(n)+1} \frac{1}{1-\frac{1}{m}} = \prod_{m=2}^{\pi(n)+1} \frac{m}{m-1} = \frac{2}{1} \cdot \frac{3}{2} \cdots \frac{\pi(n)+1}{\pi(n)} = \pi(n)+1$$

Die Anzahl der Faktoren rechts und links ist gleich

$\frac{1}{1-\frac{1}{m}} \geq \frac{1}{1-\frac{1}{p}}$, da $p_m \geq m+1$

Beweis von (a):

Aus $n = \pi(p_n) \underset{(b)}{>} \ln p_n - 1$ folgt $p_n < e^{n+1}$.

Der Satz von Tschebyscheff

Die Primzahlfunktion ist für $n \in \mathbb{N}$ definiert durch $\pi(n) :=$ Anzahl aller Primzahlen $\leq n$.

Eine recht gute Abschätzung der Primzahlfunktion mit sehr elementaren Mitteln liefert

Satz 1 (Tschebyscheff) : Für $n \in \mathbb{N}, n > 1$ gilt

$$\frac{1}{6} \cdot \frac{n}{\ln n} < \pi(n) < 6 \cdot \frac{n}{\ln n}$$

Bew. Wir beweisen nur $\frac{1}{6}\frac{n}{\ln n} < \pi(n)$.

Bew. Der Beweis wird in mehreren Einzelschritten durchgeführt.

(a) $\binom{2n}{n} = \dfrac{2n(2n-1)\cdots(2n-n+1)}{n!} = \dfrac{(2n)!}{(n!)^2}$

(b) Für alle $n \in \mathbb{N}$ gilt: $2^n \leq \binom{2n}{n} < 4^n$

Bew: $4^n = (1+1)^{2n} = \sum_{i=0}^{2n} \binom{2n}{i} > \binom{2n}{n}$

$2 \leq \binom{2}{1}$

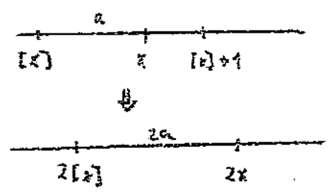
Schluß von n auf $(n+1)$: $2^{n+1} \underset{\text{Ind.Vor.}}{\leq} 2 \cdot \binom{2n}{n} \underset{(a)}{\leq} \dfrac{(2n)!}{(n!)^2} \cdot \dfrac{(2n+1)(2n+2)}{(n+1)(n+1)} \underset{(a)}{=} \binom{2n+2}{n+1}$

(c) Für alle $n \in \mathbb{N}$ gilt $n \ln 2 \leq \ln(2n)! - 2\ln n! < n \ln 4$

Bew: Logarithmiere die Ungl. in (b) und verwende (a)

(d) Für $x \in \mathbb{R}$ ist $[2x] - 2[x] = \begin{cases} 0 \\ 1 \end{cases}$ falls $\begin{matrix} [2x] \text{ gerade} \\ [2x] \text{ ungerade} \end{matrix}$

Bew:



$\Rightarrow \left.\begin{matrix} [2x] = 2[x], \text{ falls } a := x - [x] < \frac{1}{2} \\ [2x] = 2[x]+1, \text{ falls } a := x - [x] \geq \frac{1}{2} \end{matrix}\right\} \Rightarrow$ Beh.

(e) $m! = \prod_{\substack{p \leq m \\ p \in \mathbb{P}}} p^{e_p}$, wobei $e_p = \sum_{\ell=1}^{\infty} \left[\frac{m}{p^\ell}\right]$

Dabei ist $\left[\frac{m}{p^\ell}\right] = 0$, falls $p^\ell > m$, also $\ell > \frac{\ln m}{\ln p}$ (die obige Summe ist also endlich).

Bew Betrachte die Faktoren $1, 2, \ldots, m$ von $m!$

$\left.\begin{matrix} \left[\frac{m}{p}\right] \text{ der Faktoren sind Vielf. von } p \\ \left[\frac{m}{p^2}\right] \quad " \quad p^2 \\ \left[\frac{m}{p^3}\right] \quad " \quad p^3 \\ \vdots \end{matrix}\right\} \Rightarrow$ Beh.

(f) Es gilt

$$\ln (2n)! - 2\ln n! \underset{(e)}{=} \sum_{\substack{p\le 2n\\ p\in\mathbb{P}}} \ln p \left[\sum_{l=1}^{\left[\frac{\ln 2n}{\ln p}\right]} \underbrace{\left(\left[\frac{2n}{p^l}\right] - 2\left[\frac{n}{p^l}\right]\right)}_{\le 1 \text{ nach (d)}} \right]$$

$$\underset{(d)}{\le} \sum_{\substack{p\le 2n\\ p\in\mathbb{P}}} \ln p \cdot \left[\frac{\ln 2n}{\ln p}\right] \le \sum_{\substack{p\le 2n\\ p\in\mathbb{P}}} \ln(2n) = \pi(2n)\cdot \ln(2n).$$

(g) Abschätzung für π nach unten:

$$\pi(2n) \underset{(f)}{\ge} \frac{\ln(2n)! - 2\ln n!}{\ln(2n)} \underset{(c)}{\ge} \frac{n\ln 2}{\ln(2n)} \ge \frac{1}{4}\,\frac{2\cdot n}{\ln 2n} \ge \frac{1}{6}\,\frac{2n}{\ln 2n}$$

$$\boxed{\ln 2 > \frac{1}{2} \Leftrightarrow \ln 4 > 1}$$

$$\pi(2n+1) \ge \pi(2n) \underset{(g)}{>} \frac{1}{4}\,\frac{2n}{\ln 2n} \ge \frac{1}{6}\,\frac{2n+1}{\ln 2n} \ge \frac{1}{6}\,\frac{2n+1}{\ln(2n+1)}.$$

$$\boxed{\frac{2n}{4} \ge \frac{2n+1}{6}}$$

8. Vortrag

Codes

Ziel der Codierungstheorie:

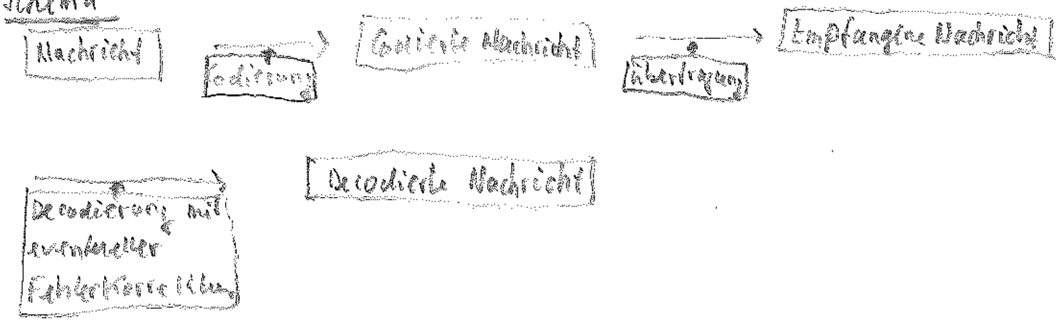
Übertrage digitale Nachrichten, so daß Fehler erkannt und möglichst sogar korrigiert werden können.

Die Ausgangsdaten werden dabei so aufbereitet, daß sie aus einer endlichen Folge von Nullen und Einsen bestehen.

Bsp Von einem Satelliten sollen Daten (zB Bilder) zur Erde übertragen werden. Die Informationen über ein Bild werden umgewandelt in eine endliche Folge von Nullen und Einsen. Wird diese Folge von Nullen und Einsen zur Erde gefunkt, so können leicht Übertragungsfehler auftreten und die empfangene Nachricht ist nicht mehr (gut genug) lesbar (die Bilder werden unscharf).

Deshalb wird die Folge vor Übertragung zur Erde zunächst codiert und die codierte Nachricht wird zur Erde übertragen. Die Codierung soll so erfolgen, daß Übertragungsfehler möglichst erkannt oder sogar korrigiert werden können.

Schema



Die decodierte Nachricht ist wieder die (Ausgangs-) Nachricht, wenn alle Übertragungsfehler korrigiert werden konnten. Um dies zu erreichen, muß das Codierungsverfahren gut gewählt werden.

Bsp 1 (2-facher Wiederholungscode)

Eine Nachricht (bestehend aus einer endlichen Folge von Nullen und Einsen) wird so codiert, daß 0 durch 00 und 1 durch 11 ersetzt wird.

$0 \longmapsto 00$ (00, 11 heißen Codewörter des Codes $C = \{00, 11\}$)
$1 \longmapsto 11$

Tritt bei der Übertragung einer endlichen Folge von Codewörtern in einem Codewort ein Fehler auf, so kann dies erkannt werden.

Sei z.B. 00 00 11 00 11 11 die empfangene Nachricht, so wird diese decodiert zu 0 0 1 0 1 1 (Es ist kein erkennbarer Fehler aufgetreten)

Sei z.B. 00 10 11 00 11 11 die empfangene Nachricht, dann muß ein Übertragungsfehler aufgetreten sein (an der 3. oder 4. Stelle).

Der 2-fache Wiederholungscode ermöglicht also eine Fehlererkennung, wenn an genau einer Stelle eines Codewortes ein Übertragungsfehler eingetreten ist. In diesem Fall könnte die Nachricht noch einmal übertragen werden (bzw. das entsprechende Codewort).
Der Code heißt 1-Fehler-erkennend.

Nachteil: Der Übertragungsaufwand ist 2-fach gegenüber der ursprünglichen Nachricht

Bsp 2 (3-facher Wiederholungscode)

Codierungsvorschrift: $0 \longmapsto 000$
$1 \longmapsto 111$.

(000, 111 sind die Codewörter. Der Code ist die Menge der Codewörter, also $\{000, 111\}$.)

Die beiden Codewörter besitzen die Länge 3.

Tritt bei der Übertragung eines Codewortes genau ein Fehler auf, so wird dies erkannt und der Fehler kann auch korrigiert werden (unter der Annahme, daß nur ein Fehler aufgetreten ist).
Wird z.B. 101 empfangen, so muß ein Übertragungsfehler aufgetreten sein.
Geht man davon aus, daß nur an einer der drei Stellen ein Übertragungsfehler aufgetreten ist, so kann der Fehler auch eindeutig korrigiert werden:
101 wird zu 111 korrigiert
Treten bei der Übertragung eines Codewortes 2 Fehler auf, so kann dies aber nur erkannt werden.

Wird z.B. bei der Übersendung von 000 das Wort 101 empfangen, so ist klar, daß ein Übertragungsfehler aufgetreten ist (die Korrektur wird allerdings falsch, wenn man von einem Übertragungsfehler ausgeht).

Der 3-fache Wiederholungscode ist also 1-Fehler-korrigierend und auch 2-Fehler-erkennend.

Nachteil: Der Übertragungsaufwand ist 3-fach gegenüber der ursprünglichen Nachricht.

Bsp 3

Die Nachricht ist eine endliche Folge von Nullen und Einsen. Diese wird aufgeteilt in Paare von Bits und es werden jeweils die Paare codiert (besteht die Folge aus einer ungeraden Anzahl von Nullen und Einsen, so wird noch eine 0 hinten angefügt).

Die Paare werden dann codiert entsprechend der folgenden Vorschrift:

$00 \longmapsto 0\,0\,0\,0\,0 \quad (=: a_1)$

$01 \longmapsto 0\,1\,1\,0\,1 \quad (=: a_2)$ Die Codewörter besitzen

$10 \longmapsto 1\,0\,1\,1\,0 \quad (=: a_3)$ jeweils die Länge 5.

$11 \longmapsto 1\,1\,0\,1\,1 \quad (=: a_4)$ Der Code ist $C = \{a_1, \dots, a_4\}$.

Je zwei Codewörter unterscheiden sich offenbar an mindestens 3 Stellen. Dies läßt sich leicht durch Ausprobieren verifizieren.

z.B. unterscheiden sich a_3 und a_4 an 3 Stellen;

a_1 und a_4 an 4 Stellen.

Treten bei der Übertragung eines Codewortes 1 oder 2 Fehler auf, so ist das empfangene Wort kein Codewort und es wird erkannt, daß mindestens an einer Stelle ein Übertragungsfehler aufgetreten sein muß.

Tritt bei der Übertragung eines Codewortes 1 Fehler auf, so wird vom Empfänger der Nachricht erkannt, daß ein Übertragungsfehler aufgetreten ist. Geht der Empfänger davon aus, daß nur an einer der 5 Stellen ein Übertragungsfehler aufgetreten ist, so kann er den Fehler auch korrigieren. Es gibt ja nur eine Möglichkeit, das empfangene Wort an einer Stelle so zu korrigieren, daß man ein Codewort erhält.

Tritt bei der Übertragung von a_3 an der 2., 3. und 5. Stelle ein Fehler auf, so geht a_3 über in a_4 und der Fehler kann nicht erkannt werden.

Der Code ist also 1-Fehler-korrigierend und 2-Fehler erkennend.

Nachteil: Der Übertragungsaufwand ist 2,5-fach gegenüber der ursprünglichen Nachricht.

Insgesamt ist der Code aber besser als der in Bsp 2; die Möglichkeiten Fehler zu erkennen bzw. zu korrigieren sind gleich, aber der Übertragungsaufwand ist in Bsp 3 geringer.

Anmerkung

Sei $K := \{0,1\}$ und $(K,+,\cdot)$ der Körper mit 2 Elementen;

also $0+0=0$, $0+1=1$, $1+1=0$
$0\cdot 0=0$, $0\cdot 1=0$, $1\cdot 1=1$.

Betrachte den K-Vektorraum K^5.
Die Elemente von K^5 sind also 5-Tupel:

$$K^5 := \{(a_1, a_2, a_3, a_4, a_5) \mid a_1, \ldots, a_5 \in K\}$$

Dann besitzt K^5 genau $2^5 = 32$ Elemente.

Fasse die Codewörter aus Bsp 3 als Elemente des K-VR K^5 auf.

Dann ist $C := \{a_1, a_2, a_3, a_4\}$ ein Unterraum des K-VR K^5 mit der Basis $B := \{a_2, a_3\}$.

Dazu genügt es zu zeigen, daß a_2 und a_3 linear unabhängig sind und daß sich die Elemente von C als Linearkombination von a_2 und a_3 darstellen lassen.
Man führe dies im Einzelnen aus.

9. Vortrag **Lineare Codes und die Generatormatrix**

Es sei $K := \{0,1\}$ und $(K,+,\cdot)$ der Körper mit 2 Elementen.

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

Dann betrachten wir den K-Vektorraum $K^n := \{(a_1,\dots,a_n) \mid a_1,\dots,a_n \in K\}$.

Dann gilt $(a_1,\dots,a_n) + (a_1',\dots,a_n') = (a_1+a_1',\dots,a_n+a_n')$

und $a\cdot(a_1,\dots,a_n) = (a\cdot a_1,\dots,a\,a_n)$ für $a \in K$.

Der K-VR K^n ist ein Vektorraum der Dimension n.

Es sei C ein Unterraum des K-VR K^n;

d.h. C ist auch wieder ein K-VR.

Dann heißt C linearer Code (der Länge n)

Die Elemente von C heißen Codewörter von C.

Sei m die Dimension von C. Dann heißt C linearer Code der Dimension m; d.h. C besitzt eine Basis aus m Elementen.

Sei $B := \{(a_{11},\dots,a_{1n}),\dots,(a_{m1},\dots,a_{mn})\}$ e. Basis des linearen Codes der Länge n und der Dimension m.

C enthält also genau alle Linearkombinationen der Basiselemente B

Die Matrix

$$G := \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ & \vdots & \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

heißt Generatormatrix von C.

Die Elemente von C sind also genau alle Linearkombinationen der Zeilenvektoren von G.

C besitzt also genau 2^m Elemente (Codewörter). (Begründung?)

In der Praxis wird der Code wie folgt verwendet:

Es soll eine digitale Nachricht übertragen werden, die aus einer endlichen Folge von Nullen und Einsen besteht.
Je m Symbole der Folge werden zusammengefaßt zu einem m-tupel $(a_1, \ldots, a_m) \in K^m$.
$(a_1, \ldots, a_m)$ nennt man dann ein Wort der Nachricht.
Ist die Anzahl der Symbole der Folge nicht Vielfaches von m, so werden am Ende der Folge entsprechend Nullen ergänzt.
Vor der Übertragung der Nachricht wird jedes Wort codiert zu einem Codewort aus C durch die Zuordnung

$$(a_1, \ldots, a_m) \longmapsto (a_1, \ldots, a_m) \begin{pmatrix} a_{11} & \cdots & a_{1n} \\ & \vdots & \\ a_{m1} & \cdots & a_{mn} \end{pmatrix}$$

$$= (a_1 a_{11} + \ldots + a_m a_{m1}, \ldots, a_1 a_{1n} + \ldots + a_m a_{mn}).$$

Die Codierung soll möglichst so gewählt werden, daß erkannt wird, wenn bei der Übertragung des Codewortes durch ein Übertragungskanal Übertragungsfehler erkannt und nach Möglichkeit auch korrigiert werden können.

Bsp.

Betrachte den K-VR K^7.

Dieser besitzt $2^7 (= 128)$ Elemente.

Sei C der Unterraum des K-VR K^7 mit der Generatormatrix

$$B = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix}$$

Man beachte, daß die Zeilenvektoren von B linear unabhängig sind.
C enthält also genau alle Linearkombinationen der Zeilenvektoren von B: also

$$C = \{ \lambda_1 \alpha_1 + \lambda_2 \alpha_2 + \lambda_3 \alpha_3 \mid \lambda_1, \lambda_2, \lambda_3 \in K \}.$$

Insbesondere enthält C genau 8 Elemente.

Bsp2

Sei
$$G := \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

Generatormatrix des Codes C (C heißt Hamming-Code)

C enthält also 2^4 ($=16$) Elemente.

Man kann durch Ausprobieren aller Fälle verifizieren, daß sich je 2 Elemente aus C immer an mindestens 3 Komponenten unterscheiden.

Der Code ist also 1-Fehler-korrigierend und 2-Fehler-erkennend (s. Vorlesung 7).

C ist Unterraum des K-VR K^7. Dieser besitzt 2^7 ($=128$) Elemente.

Nach Lagrange (Gruppentheorie) besitzt die Gruppe $(C,+)$ in $(K^7,+)$ genau $\frac{2^7}{2^4}$ ($=8$) Nebenklassen.

Beh Diese 8 Nebenklassen sind

$$\begin{array}{ll} (0,\dots,0)+C & (=C) \\ (1,0,\dots,0)+C & =\{(1,0,\dots,0)+\alpha \mid \alpha \in C\} \\ (0,0,1,0,\dots,0)+C & \\ \vdots & \\ (0,\dots,0,1)+C & \end{array}$$

Bew Dies ergibt sich wie folgt:

Wegen $(0,\dots,0) \in C$ hat jedes Element $\neq (0,\dots,0)$ aus C mindestens 3 von Null verschiedene Komponenten.

Aus der Gruppentheorie ist ferner bekannt, daß für Nebenklassen folgendes gilt:

$$(a_1,\dots,a_n)+C=(b_1,\dots,b_n)+C \iff (a_1,\dots,a_n)-(b_1,\dots,b_n) \in C.$$

Daraus folgt die Behauptung, denn die Differenz zweier Repräsentanten zweier verschiedener Nebenklassen besitzt höchstens 2 von 0 verschiedene Komponenten.

Folgerung:

Annahme: Das Wort $(a_1,\dots,a_n) \in K^7$ wird empfangen; $(a_1,\dots,a_n) \notin C$.
Dann ist bei mindestens einer Komponente ein Übertragungsfehler aufgetreten.
Das Wort $(a_1,\dots,a_n)$ liege in der Nebenklasse $(\underset{}{0,\dots,0},\underset{i\text{-te Stelle}}{1},0,\dots,0)+C$.

Korrigiert man das Wort $(a_1,\dots,a_n)$ an der i-ten Stelle, so erhält man ein Codewort.

Jedes Wort aus K^7 läßt sich also durch Korrektur von höchstens einer Komponente in ein Codewort umwandeln.

Diese Korrektur ist sogar eindeutig, denn jedes Element aus $(0,\dots,0,1,0,\dots,0)+C$ hat mindestens 2 von Null verschiedene Komponenten.

10. Vortrag **Der duale Code und die Kontrollmatrix**

Es sei $K = \{0,1\}$ der Körper mit 2 Elementen.

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

Betrachte den K-Vektorraum $K^n := \{(a_1, \dots, a_n) \mid a_1, \dots, a_n \in K\}$.

Der K-VR K^n besitzt die Dimension n.

Sei $C \subseteq K^n$ ein Unterraum des K-VR K^n der Dimension m.

Dann heißt C linearer Code der Länge n und der Dimension m.

Sei $B := \{(g_{11}, \dots, g_{1n}), \dots, (g_{m1}, \dots, g_{mn})\}$ eine Basis von C.

Die Matrix

$$G := \begin{pmatrix} g_{11} & \cdots & g_{1n} \\ & \vdots & \\ g_{m1} & \cdots & g_{mn} \end{pmatrix}$$

nennt man auch Generatormatrix von C.
C enthält also genau alle Linearkombinationen der Zeilenvektoren von G.

Wir betrachten das homogene lineare Gleichungssystem

$$\begin{matrix} g_{11} x_1 + \dots + g_{1n} x_n = 0 \\ \vdots \\ g_{m1} x_1 + \dots + g_{mn} x_n = 0 \end{matrix} \qquad (*)$$

oder in anderer Schreibweise

$$G \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$, wobei G die Koeffizientenmatrix von $(*)$ ist.

Sei $C^\perp$ die Lösungsmenge des linearen Gleichungssystems $(*)$.

Bekanntlich ist dann $C^\perp$ ein Unterraum des K-VR K^n.

Da die Zeilenvektoren von G linear unabhängig sind, ist der Rang von G gleich $Rg\,G = m$.

Bekanntlich hat der Lösungsraum $C^\perp$ von $(*)$ dann die Dimension $n - Rg\,G = n - m =: m'$.

$C^\perp$ heißt der zu C duale Code.

$C^\perp \subseteq K^n$ ist ein Code der Länge n und der Dimension $m' (= n - m)$.

Sei $B^* := ((h_{11}, \dots, h_{1n}), \dots, (h_{m'1}, \dots, h_{m'n}))$ eine Basis von $C^\perp$.

Dann ist also

$$H := \begin{pmatrix} h_{11} & \cdots & h_{1n} \\ & \vdots & \\ h_{m'1} & \cdots & h_{m'n} \end{pmatrix}$$

eine Generatormatrix von $C^\perp$.

Ferner ist $\mathrm{Rg}\, H = m'$, da die Zeilenvektoren von H linear unabhängig sind.

<u>Bem 1</u> Es gilt $(C^\perp)^\perp = C$, d.h.

der zu $C^\perp$ duale Code ist wieder C.

<u>Beweis</u>

Die Elemente aus $(C^\perp)^\perp$ sind nach Definition genau die Lösungen des homogenen linearen Gleichungssystems

$$H \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}. \qquad (**)$$

Es gilt $\mathrm{Rg}\, H = m' = n - \mathrm{Rg}\, G = n - m$.

Der Lösungsraum von $(**)$ besitzt also die Dimension

$n - \mathrm{Rg}\, H = n - m' = m = \dim C$.

Jeder Zeilenvektor $(g_{i1}, \dots, g_{in})$ von G ist Lösung von $(**)$, denn nach Def. von H gilt

$$(g_{i1}, \dots, g_{in}) \begin{pmatrix} h_{11} & \cdots & h_{m'1} \\ | & & | \\ h_{1n} & & h_{m'n} \end{pmatrix} = (0, \dots, 0).$$

Dies ist gleichwertig mit

$$H \cdot \begin{pmatrix} g_{i1} \\ | \\ g_{in} \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

Dies ergibt sich durch Transposition der obigen Matrizengleichung.

Also bilden die Zeilenvektoren von G eine Basis des Lösungsraums von $(**)$.

Damit folgt die Behauptung von Bem 1.

Bem2

Nach dem Beweis von Bem1 gilt:

Die Lösungsmenge des homogenen linearen Gleichungssystems (**) ist C.

Also gilt:

$$(c_1,\dots,c_n)\in C \Longleftrightarrow H\begin{pmatrix}c_1\\ \vdots\\ c_n\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}.$$

Praktische Anwendung:

Sei $(a_1,\dots,a_n)\in K^n$ gegeben (bzw. nach der Übertragung eines Codewortes empfangen)

Um zu entscheiden, ob $(a_1,\dots,a_n)\in K^n$ in C liegt (also ein Codewort ist)

genügt es nachzurechnen, ob

$$H\cdot\begin{pmatrix}a_1\\ \vdots\\ a_n\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix} \text{ gilt.}$$

H heißt deshalb Kontrollmatrix von C.

$H\begin{pmatrix}x_1\\ \vdots\\ x_n\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}$ heißt Kontrollgleichungssystem von C.

Gilt $H\begin{pmatrix}a_1\\ \vdots\\ a_n\end{pmatrix}\neq\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}$, so ist sicher ein Übertragungsfehler aufgetreten.

Bsp1 Sei $C:=\{(0,0),(1,1)\}$ (C heißt zweifacher Wiederholungscode). (s. Bsp 1, Vortrag 7)

Berechne eine Kontrollmatrix von C:

Eine Basis von C ist $\{(1,1)\}$; also ist $\dim C=1$.

$G:=(1\ \ 1)$ ist also eine Generatormatrix von C.

Betrachte das Gleichungssystem

$$x_1+x_2=0.$$

Die Lösungsmenge ist ein Unterraum der Dimension 1.

Eine Lösung ist $(1,1)$.

Also ist $(1,1)$ eine Basis von $C^{\perp}$; $(1\ 1)$ ist also eine Kontrollmatrix von C.

Ferner gilt $C^{\perp}=\{(0,0),(1,1)\}$.

Also ist $C=C^{\perp}$. Ein solcher Code heißt selbstdual.

Bsp2 Betrachte den Code C aus Bsp2 (8. Vortrag) mit der Generatormatrix $G=\begin{pmatrix}1&1&0&1&0&0&0\\1&0&1&0&1&0&0\\0&1&1&0&0&1&0\\1&1&1&0&0&0&1\end{pmatrix}$

Eine Kontrollmatrix von C ist dann $H=\begin{pmatrix}1&0&0&1&1&0&1\\0&1&0&1&0&1&1\\0&0&1&0&1&1&1\end{pmatrix}$.

Man beachte: Die Spaltenvektoren von H sind genau alle 7 Elemente $\neq(0,0,0)$ aus K^3.

11. Vortrag Der Hamming-Abstand und Fehler-Korrektur

Es sei $K = \{0,1\}$ der Körper mit 2 Elementen.

Es sei C ein Unterraum des K-Vektorraums K^n der Dimension m. C heißt auch Code.
Es soll ein Maß für den Abstand zweier Elemente aus K^n definiert werden.

Def 1 (Hamming-Abstand)

Seien $c := (c_1, \dots, c_n)$ und $c' := (c'_1, \dots, c'_n)$ zwei Vektoren aus dem K-VR K^n.

Der Hamming-Abstand von c und c' wird definiert durch

$$\Delta(c,c') := \text{Anzahl aller } i \in \{1, \dots, n\} \text{ mit } c_i \neq c'_i.$$

$\Delta(c,c')$ ist also die Anzahl der Komponenten, in denen sich c und c' unterscheiden.

Bsp Sei $c_1 := (1,0,0,1)$, $c_2 := (0,0,0,1)$. Dann ist $\Delta(c_1,c_2) = 1$

Sei $c_1 := (0,0,1,0,1)$, $c_2 := (1,0,0,1,0)$. Dann ist $\Delta(c_1,c_2) = 4$.

Bem 1 Offenbar gilt für Elemente aus K^n:

(i) $\Delta(c,c') = 0 \Leftrightarrow c = c'$

(ii) $\Delta(c,c') = \Delta(c',c)$

(iii) $\Delta(c,c') + \Delta(c',c'') \leq \Delta(c,c'')$ (Dreiecksungleichung)

[Die i-ten Komponenten von c und c'' können nur dann verschieden sein, wenn die i-ten Komponenten von c und c' oder die i-ten Komponenten von c' und c'' verschieden sind.]

(iv) $\Delta(c-c', c''-c') = \Delta(c, c'')$

[$(c-c')$ und $(c''-c')$ unterscheiden sich in der i-ten Komponente genau, wenn sich c und c'' in der i-ten Komponente unterscheiden.]

Def 2 Sei $c = (c_1, \dots, c_n) \in K^n$.

$w(c) :=$ Anzahl der von 0 verschiedenen Komponenten von c.

$w(c)$ heißt Gewicht von c.

Bem 2 Offenbar gilt $w(c) = \Delta(c,0)$ ($0 := (0, \dots, 0)$ bezeichne den Nullvektor)

Bem 3 Es gilt $\Delta(c_1,c_2) \underset{\boxed{\text{Bem 1 (iv)}}}{=} \Delta(c_1-c_2, 0) \underset{\boxed{\text{Bem 2}}}{=} w(c_1-c_2)$

Bsp Sei $c := (1,1,0,1,0,1,1)$. Dann $w(c) = 5$.

Def 3

Sei C ein Unterraum des K-VR K^n ((nennt man dann auch Code). Dann:

$$d(C) := \min \{ \Delta(c,c') \mid c,c' \in C ; c \neq c' \}.$$

$d(C)$ heißt Minimalabstand des Codes C.

Bem 4 Sei C ein Unterraum des K-VR K^n.

Dann unterscheiden sich zwei verschiedene Elemente aus C stets an mindestens $d(C)$ Komponenten (klar nach Def. 3)

Bem 5

Es gilt $d(C) = \min \{ w(c) \mid c \in C \}$

Bew Seien $c, c' \in C$.

Da C Unterraum ist, ist dann auch $c-c' \in C$.

Also gilt $\Delta(c,c') \underset{\boxed{\text{Bem 3 (iv)}}}{=} \Delta(c-c', 0) \underset{\boxed{\text{Def. von } w}}{=} w(c-c')$

Bem 6 (Vergleiche Vortrag ?)

(i) Sei $d(C) \geq 2$.

Dann ist C 1-Fehler-erkennend; d.h.:

ändert man für ein $c \in C$ eine Komponente, so erhält man stets ein Element aus K^n, das nicht in C liegt.

(ii) Sei $d(C) \geq 3$. Dann ist C 2-Fehler-erkennend (analog zu (i)).

Ferner ist C 1-Fehler-korrigierend; d.h.:

Sei $c \in C$. Ändert man eine Komponente von c, so erhält man ein Element c' aus K^n, das nicht in C liegt.

Ändert man in c' eine weitere Komponente, so erhält man ebenfalls ein Element aus K^n, das nicht in C liegt.

Also: Tritt bei der Übertragung eines Codewortes in genau einer Komponente ein Fehler auf, so läßt sich der Fehler eindeutig korrigieren, in dem eine Komponente des empfangenen Wortes korrigiert wird.

Bem 7 Sei $C \subseteq K^n$ ein linearer Code (also C ein Unterraum des K-VR K^n).

Sei H eine Kontrollmatrix von C (s. Vortrag 9)

Sei $H = \begin{pmatrix} h_{11} & \cdots & h_{1n} \\ \vdots & & \vdots \\ h_{r1} & \cdots & h_{rn} \end{pmatrix}$, sei $h_i = \begin{pmatrix} h_{1i} \\ \vdots \\ h_{ri} \end{pmatrix}$ der i-te Spaltenvektor von H.

Dann gilt (s. Vortrag 9):

$$(c_1, \dots, c_n) \in C \underset{\boxed{\text{Kontrollgleichung}}}{\Longleftrightarrow} H\begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \underset{\boxed{\text{Def. des Matrizenproduktes}}}{\Longleftrightarrow} \overbrace{c_1 h_1 + \dots + c_n h_n}^{\text{ist eine Linearkombination der Spaltenvektoren von } H} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \quad (*)$$

Seien je zwei Spalten von H linear unabhängig.

Dann gilt für den Minimalabstand $d(C)$ von C die Ungleichung $d(C) \geq 3$

(nach Bem 6 ist C also 1-Fehler-korrigierend)

Beweis

Annahme: $d(C) < 3$.

Dann ex. $c, c' \in C$ mit $\Delta(c, c') \leq 2$ und $c \neq c'$.

Da C ein Unterraum des K-VR K^n ist, folgt $c - c' \in C$.

c und c' unterscheiden sich an höchstens zwei Komponenten

OBdA besitzt $c - c'$ die Form $c - c' = (1, a_2, 0, \dots, 0)$ mit $a_2 = 0$ oder $a_2 = 1$.

Wegen $c - c' \in C$ ist $h_1 + a_2 h_2 = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ (nach (*)).

Die Spaltenvektoren h_1 und h_2 von H sind also linear abhängig.

Dies ist ein Widerspruch zur Voraussetzung.

Bem 8

Da K nur 2 Elemente besitzt, gilt:

Zwei verschiedene von $(0, \dots, 0)$ verschiedene Vektoren aus K^n sind stets linear unabhängig.

Bew Sei $c = (c_1, c_2, \dots, c_n)$, $a = (a_1, a_2, \dots, a_n)$; $c \neq a$; $c \neq (0, \dots, 0)$, $a \neq (0, \dots, 0)$. Wir nehmen OBdA an, daß sich c und a in der ersten Komponente unterscheiden.

Sei OBdA $c_1 = 0$, $a_1 = 1$.

Gelte $\lambda_1 c + \lambda_2 a = (0, 0, \dots, 0)$. Dann ist zum Nachweis der linearen Unabhängigkeit von a und c zu zeigen: $\lambda_1 = \lambda_2 = 0$.

Beachtet man die 1. Komponente der Vektorgleichung $\lambda_1 c + \lambda_2 a = (0, \dots, 0)$,

so folgt $\lambda_2 = 0$.

Da $c \neq (0, \dots, 0)$ ist, folgt weiter $\lambda_1 = 0$.

12. Vortrag Hamming-Codes und perfekte Codes

Es sei $n \in \mathbb{N}$ gegeben.

Ferner sei $K = \{0,1\}$ der Körper mit zwei Elementen.

Betrachte den K-Vektorraum $K^n = \{(a_1, \dots, a_n) \mid a_1, \dots, a_n \in K\}$.

Dann besitzt K^n genau 2^n Elemente, also genau $2^n - 1$ Elemente $\neq (0, \dots, 0)$ (Null in K^n).

Der K-VR K^n besitzt die Dimension n.

Die Matrix $H = \begin{pmatrix} a_{11} & \dots & a_{1\,2^n-1} \\ \vdots & & \vdots \\ a_{n1} & \dots & a_{n\,2^n-1} \end{pmatrix}$ besitze als Spaltenvektoren genau die

$2^n - 1$ von Null verschiedenen Vektoren aus K^n.

Dann sind die Zeilenvektoren von H linear unabhängig, da H die Spalten $\begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \dots, \begin{pmatrix} 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix}$ enthält.

Bsp 1

Im Fall $n = 3$ kann $H = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix}$ gewählt werden.

Natürlich ist auch jede andere Reihenfolge der Spaltenvektoren möglich.

Es sei $C \subseteq K^{2^n - 1}$ der Code mit der Kontrollmatrix H (siehe 9. Vortrag), d.h.:

C ist ein Unterraum des K-VR K^{2^n-1}; sei $m := 2^n - 1$

Es gilt: $(c_1, \dots, c_m) \in C \iff \underbrace{H \cdot \begin{pmatrix} c_1 \\ \vdots \\ c_m \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}}_{(*)}$ ist (Kontrollgleichungssystem).

Als Lösungsmenge des Gleichungssystems $(*)$ ist C natürlich ein Unterraum des K-VR K^m.

Ferner ist $\dim C = 2^n - 1 - n = m - n$.

C nennt man einen Hamming-Code.

Bem 1 Nach Bem 7 (Vortrag 10) gilt für den Minimalabstand $d(C)$ die Ungleichung

$$d(C) \geq 3.$$

Also ist C 1-Fehler-korrigierend nach Bem 7 und Bem 8 (Vortrag 10).

Je zwei verschiedene Elemente aus C unterscheiden sich also an mindestens drei Komponenten.

Bemk

C besitzt die Dimension $m-n$,

also besitzt C e. Basis mit $m-n$ Elementen,

also besitzt C genau 2^{m-n} Elemente.

Der K-VR K^m besitzt 2^m Elemente.

$(C,+)$ ist eine Untergruppe von $(K^m,+)$.

Nach Lagrange läßt sich die Anzahl der Nebenklassen

$$a + C$$

der Untergruppe C der Gruppe $(K^m,+)$ bestimmen durch

$$\frac{2^m}{2^{m-n}} = 2^n.$$

Aus der Gruppentheorie ist bekannt, daß für 2 Nebenklassen $a+C$ und $b+C$ gilt:

$$a+C = b+C \Leftrightarrow a-b \in C. \qquad \left(\begin{array}{l}\text{beachte:}\\ a,b \in K^{2^n-1}\end{array}\right) \ (*)$$

Die 2^n Nebenklassen von C sind also

$$\begin{array}{l}(0,\ldots\ldots,0)+C, \quad (=C),\\ (1,0,\ldots,0)+C,\\ (0,1,0,\ldots,0)+C;\\ \qquad\vdots\\ (0,\ldots,0,1)+C.\end{array}$$

Dies ergibt sich wie folgt:

Die oben angegebenen 2^n Nebenklassen sind tatsächlich paarweise verschieden nach $(*)$, denn die Differenz zweier verschiedener Repräsentanten hat höchstens zwei von 0 verschiedene Komponenten und liegt damit wegen $d(C) \geq 3$ nicht in C.

Folgerung Annahme: $(a_1,\ldots,a_m)$ wird empfangen.
Ist $(a_1,\ldots,a_m) \in C$, so wird davon ausgegangen, daß kein Übertragungsfehler aufgetreten ist.
Ist $(a_1,\ldots,a_m) \notin C$, so liegt $(a_1,\ldots,a_m)$ in einer Nebenklasse $(0,\ldots,0,\underset{\uparrow\ i\text{-te Stelle}}{1},0,\ldots,0)+C$,
$(a_1,\ldots,a_m)$ besitzt also die Form

$$(a_1,\ldots,a_m) = (0,\ldots,0,\underset{\uparrow\ i\text{-te Stelle}}{1},0,\ldots,0) + c \text{ mit } c \in C$$

Bei der Übertragung zum Empfänger muß bei mindestens einer m-Komponenten ein Fehler aufgetreten sein.

Korrigiert man $(a_1, \dots, a_m)$ bei der i-ten Komponente, so erhält man das Wort $(a_1, \dots, a_m) - (0, \dots, 0, \underset{\uparrow \text{ i-te Stelle}}{1}, 0, \dots, 0) = c$; also ein Codewort.

Korrigiert man $(a_1, \dots, a_m)$ bei der j-ten Komponente $(i \neq j)$, so erhält man kein Codewort, denn es gilt

$$(a_1, \dots, a_m) - (0, \dots, 0, \underset{\uparrow \text{ j-te Stelle}}{1}, 0, \dots, 0) \in C,$$

da

$$(a_1, \dots, a_m) + C = (0, \dots, 0, \underset{\uparrow \text{ i-te Stelle}}{1}, 0, \dots, 0) + C \neq (0, \dots, 0, \underset{\uparrow \text{ j-te Stelle}}{1}, 0, \dots, 0) + C$$

Geht man davon aus, daß bei der Übertragung nur bei einer Komponenten fehlerhaft war, so läßt sich der Fehler eindeutig korrigieren.

<u>Bsp 2</u>

Der zu H aus Bsp 1 gehörige Hamming-Code besitzt

$$G = \begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 \end{pmatrix}$$

als Generatormatrix. (s Bsp 2, Vortrag 9)

Angenommen: $(0\ 1\ 0\ 1\ 0\ 0\ 0)$ wird empfangen.

Dann liefert die Fehlerkorrektur in der 1. Komponente das Codewort

$$(1\ 1\ 0\ 1\ 0\ 0\ 0)$$

<u>Def</u> Sei $C \subseteq K^n$ ein linearer Code.

Läßt sich jedes $(a_1, \dots, a_n) \in K^n$ durch Korrektur bei höchstens einer Komponenten eindeutig in ein Codewort überführen, so heißt C perfekter Code.

<u>Bem 2</u> Nach Bem 1 ist jeder Hamming-Code perfekt.

13 und 14. Vortrag: Fehlerkorrektur linearer Codes

Es sei $K = \{0,1\}$ der Körper mit 2 Elementen.
C sei ein Unterraum des K-VR K^n der Dimension m.
Dann heißt C linearer Code der Länge n und der Dimension m.
Die Zeilen der Matrix

$$G := \begin{pmatrix} g_{11} & \cdots & g_{1n} \\ & \vdots & \\ g_{m1} & \cdots & g_{mn} \end{pmatrix}$$

seien eine Basis von C.
Dann heißt G Generatormatrix von C.

Es sei H eine Kontrollmatrix von G.
Die Zeilenvektoren von H bilden nach Definition also eine Basis des Lösungsraums des homogenen linearen Gleichungssystems

$$G \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}.$$

H besitzt also $n' := n-m$ Zeilenvektoren.

Für alle $c = (c_1, \ldots, c_n) \in K^n$ gilt:

$$c \in C \Leftrightarrow H \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}. \quad \text{(Kontrollgleichungssystem)}$$

<u>Annahme:</u> Bei der Übertragung eines Codewortes aus C wird $y \in K^n$ empfangen.

Ist $y \in C$, so wird davon ausgegangen, daß kein Übertragungsfehler aufgetreten ist.
Allgemein gilt:

Gesucht wird ein $c \in C$ mit kleinstmöglichem Hamming-Abstand von y. (Natürlich muß c nicht eindeutig bestimmt sein).
Man geht dann davon aus, daß c das tatsächlich gesendete Codewort ist.

Dann heißt $e := y - c$ der zugehörige Fehlervektor.
Es entsteht also folgendes Problem:
Zu $y \in K^n$ suche man ein $c \in C$ mit $\Delta(y,c) \leq \Delta(y,c')$ f.a. $c' \in C$.
bzw. $w(\underbrace{y-c}_{=e}) \leq w(y-c')$ f.a. $c' \in C$.

Fehler Korrektur linearer Codes

In der Menge $y - C := \{y - c' \mid c' \in C\}$ wird also ein Element $e := y - c$ mit minimalem Gewicht gesucht.

Es gilt offenbar $y - C = y + C := \{y + c' \mid c' \in C\}$, da C ein Unterraum ist.

In der von y erzeugten Nebenklasse $y + C$ wird als Fehlervektor also ein Element von minimalem Gewicht gesucht.

Bemerke: e ist nicht notwendig eindeutig bestimmt. Man wähle ein solches e. Dieses wird dann Nebenklassenführer der Nebenklasse $y + C$ genannt.

<u>Bem 1</u>

Für $y = (y_1, \ldots, y_n) \in K^n$ wird $H \cdot \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$ das Syndrom von y genannt.

Beachte: H besitzt $n-m$ Zeilen, also ist $H \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} \in K^{n-m}$.

Wegen des Kontrollgleichungssystems gilt $H \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ gdw $y \in C$ ist.

Allgemein gilt:

<u>Bem 2</u> Zwei Vektoren aus K^n besitzen dasselbe Syndrom gdw sie zu derselben Nebenklasse von C gehören.

<u>Beweis</u>: Sei $y = (y_1, \ldots, y_n) \in K^n$, $z = (z_1, \ldots, z_n) \in K^n$. Dann gilt:

$$H \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = H \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} \Leftrightarrow H \begin{pmatrix} y_1 - z_1 \\ \vdots \\ y_n - z_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \underset{\text{Bem 1}}{\Leftrightarrow} y - z \in C \underset{\text{nach Vorlesung}}{\Leftrightarrow} y + C = z + C$$

Beachte: Bekanntlich bilden die Nebenklassen von C in K^n eine Partition von K^n.

Nach diesen Vorbereitungen beschreiben wir nun eine Methode zur Fehlerkorrektur bei linearen Codes.

Der lineare Code $C \subseteq K^n$ sei gegeben.

Bestimme eine Liste der Nebenklassen von C in K^n.

Berechne für jede Nebenklasse von C einen Nebenklassenführer, also ein Element dieser Nebenklasse mit minimalem Gewicht.

Berechne die Syndrome der Nebenklassenführer.

Dann hat man folgende Tabelle für C zur Verfügung:

Nebenklassenführer	Syndrome der Nebenklassenführer
y_1	$H \cdot y_1$
y_2	$H \cdot y_2$
$\vdots$	$\vdots$

Mit Hilfe dieser Tabelle ist eine Fehlerkorrektur für den Code C nun sehr einfach:

Annahme: $y \in K^n$ wird empfangen.

Berechne das Syndrom $H \cdot y$ von y.

$H \cdot y$ tritt in der rechten Spalte der Tabelle an genau einer Stelle auf; etwa bei $H y_i$ (da y in genau einer Nebenklasse von C liegt und wegen (Bem 2)).

Der zugehörige Nebenklassenführer ist dann y_i.

Dann ist die folgende Fehlerkorrektur durchzuführen $y \longmapsto y - y_i$.

Der Fehlervektor ist also y_i.

<u>Bemerkung 3</u>

Es sei $C \subseteq K^n$ ein perfekter Code.

Dann sind die Nebenklassenführer von C genau alle Elemente aus K^n vom Gewicht ≤ 1.

<u>Beweis</u>

Wir zeigen zunächst:

In jeder Nebenklasse $y + C$ von C gibt es höchstens ein Element vom Gewicht ≤ 1:

Seien $y_1, y_2 \in y + C$ mit $w(y_1), w(y_2) \leq 1$. Dann ist $w(y_1 - y_2) \leq 2$ und $y_1 - y_2 \in C$. Dann ist $K_1(0) \cap K_1(y_1 - y_2) \neq \emptyset$, was bei perfekten Codes nicht möglich ist (s. Bem 5 über Hamming-Codes).

Es bleibt zu zeigen:

In jeder Nebenklasse $y + C$ von C gibt es ein Element vom Gewicht ≤ 1.

Zu $y \in K^n$ gibt es nach Definition perfekter Codes ein $c \in C$ mit $y \in K_1(c)$. Dann liegt $y - c$ in der Nebenklasse $y + C$ und es gilt $w(y - c) \leq 1$.

<u>Bsp</u> Die Generatormatrix sei $(1,1,1)$.

Der Code ist dann $C = \{(1,1,1), (0,0,0)\}$; also $C \cong 1$

Der duale Code ist der Lösungsraum von $x_1 + x_2 + x_3 = 0$.

Der Lösungsraum besitzt die Dimension 2, eine Kontrollmatrix von C ist $\begin{pmatrix} 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} =: H$

Die Anzahl der Nebenklassen von C in K^3 ist $\frac{2^3}{2} = 4$.

Die Nebenklassen sind C, $(1,0,0) + C$, $(0,1,0) + C$, $(0,0,1) + C$.

Die angeführten Repräsentanten haben Gewicht ≤ 1, sind also die Nebenklassenführer.

Die Syndrome der Nebenklassenführer sind $H \cdot \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \end{pmatrix}$, $H \cdot \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $H \cdot \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $H \cdot \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

Annahme $(1,1,0)$ wird empfangen

Das Syndrom ist $H \cdot \begin{pmatrix} 1 \\ 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$

Der zugehörige Nebenklassenführer ist $(0,0,1)$

Fehlerkorrektur: $(1,1,0) \longmapsto (1,1,0) - (0,0,1) = (1,1,1)$

15 Vortrag

$\boxed{\text{Kettenbrüche und beste Approximationen}}$

Natürlich läßt sich jede reelle Zahl beliebig gut durch eine rationale Zahl approximieren (warum?).
Das Ziel der Kettenbruchtheorie besteht darin, eine vorgegebene reelle Zahl möglichst gut durch rationale Zahlen mit kleinem Nenner zu approximieren.

Def 1 Sei $r \in \mathbb{R}$, $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Dann:
$\frac{a}{b}$ heißt beste Approximation von r, wenn gilt:

$$|r - \tfrac{a}{b}| \leq |r - \tfrac{c}{d}| \quad \text{f.a. } c \in \mathbb{Z},\ d \in \mathbb{N},\ d \leq b.$$

Bsp 1 Die besten Approximationen von $\frac{3}{2}$ sind 1 und 2 und $\frac{3}{2}$.
Die besten Approximationen von $\frac{7}{5}$ sind $1, \frac{3}{2}, \frac{4}{3}, \frac{7}{5}$.

Def 2 (Kettenbruchentwicklung)
Sei $r \in \mathbb{R}$, OBdA $r \geq 1$.
Approximiere r im 1. Schritt durch $a_0 := [r]$ (größte ganze Zahl $\leq r$)
Beende das Verfahren, falls $r = a_0$. Andernfalls:
Sei $\alpha_1 \in \mathbb{R}$ def. durch $r = a_0 + \frac{1}{\alpha_1}$. Dann ist $\alpha_1 > 1$. Setze $a_1 := [\alpha_1]$
Approximiere r im 2. Schritt durch $a_0 + \frac{1}{a_1}$.
Beende das Verfahren, falls $r = a_0 + \frac{1}{a_1}$. Andernfalls:

Sei $\alpha_2 \in \mathbb{R}$ def. durch $r = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\alpha_2}}$. Offenbar ist wieder $\alpha_2 > 1$. Setze $a_2 := [\alpha_2]$.

Approximiere r im 3. Schritt durch $a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}$.

Beende das Verfahren, falls $r = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2}}$ ist, also der Approximationsfehler gleich 0 ist. Andernfalls:
Setze das Verfahren fort.
Das Verfahren bricht ab, wenn

$$r = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}} \quad \text{ist.}$$

(Dies muß aber nach endlich vielen Schritten nicht der Fall sein)

Bem 1

Bricht das Verfahren in Def 1 nach endlich vielen Schritten ab, so ist r offenbar rational. Es gilt auch die Umkehrung (ohne Bew.)

Def 2 Für $a_0, a_1, \dots, a_n \in \mathbb{N}$ schreibt man

$$[a_0, \dots, a_n] := a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}} \qquad \text{(Kettenbruch)}$$

Def 3

(i) Ist r nicht rational, so schreibt man

$r = [a_0, a_1, \dots]$ und $[a_0, \dots, a_n]$ heißt n-te Näherungsbruch von r ($n \geq 0$).
Dies ist sinnvoll, da die Folge der n-ten Näherungsbrüche gegen r konvergiert (ohne Bew.) s. Bem 4

(ii) Sei r rational und

$$r = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_n}}}, \quad \text{also} \quad r = [a_0, \dots, a_n]$$

Im Fall $a_n > 1$ wird diese Darstellung von r ergänzt durch

$$r = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots\, a_n' + \cfrac{1}{a_{n+1}'}}} \quad \text{mit } a_n' = a_n - 1,\ a_{n+1}' = 1,$$

also $r = [a_0, \dots, a_{n-1}, a_n', a_{n+1}']$

Die i-ten Näherungsbrüche von r werden dann analog definiert für $i = 0, \dots, n$ bzw. für $i = 0, \dots, n+1$ im Fall $a_n > 1$.

Bsp 2 $r = \frac{7}{5} = [1, 2, 2] = [1, 2, 1, 1]$. Die Näherungsbrüche sind $1, \frac{3}{2}, \frac{4}{3}, \frac{7}{5}$.

Bem 2 (ohne Bew.) Sei $r \in \mathbb{R}$, $r \geq 1$. Dann

(i) Für $i \geq 1$ ist der i-te Näherungsbruch ~~von~~ von r beste Approximation von r.

(ii) Eine beste Approximation von r ist i-te Näherungsbruch von r für ein $i \geq 0$.

Bem 3 (Darstellung der Näherungsbrüche durch Brüche) (ohne Bew.)

Seien $a_0, \dots, a_i \in \mathbb{N}$.

Sei $p_0 := a_0, \quad q_0 := 1$

$p_1 := p_0 a_1 + 1, \quad q_1 := a_1$

$p_i := a_i p_{i-1} + p_{i-2}, \quad q_i := a_i q_{i-1} + q_{i-2}$ für $i \geq 2$.

Dann: $[a_0, \dots, a_i] = \frac{p_i}{q_i}$ und $ggT(p_i, q_i) = 1$.

Die obigen Rekursionsformeln erlauben es also auf schnelle Weise, Näherungsbrüche in Brüche umzuwandeln.

Bsp 3 Berechne die Näherungsbrüche von $r = \frac{7}{5}$ mit Hilfe der Formeln aus Bem 3.

Nach Bem 2 ist $\frac{4}{3}$ eine beste Approximation von $\frac{7}{5}$.

15. Vortrag:
Periodische Kettenbrüche

Bem 4 (ohne Bew) Für $n \geq 0$ seien $[a_0, \ldots, a_n] = \frac{p_n}{q_n}$ die Näherungsbrüche der reellen Zahl r (s. 15. Vortrag)

(i) Dann gilt:
$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots \leq r \leq \cdots \leq \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$
Ein Gleichheitszeichen tritt auf gdw r rational ist.

Stets gilt $\left| r - \frac{p_i}{q_i} \right| \leq \frac{1}{q_i^2}$.

(ii) Ist r nicht rational, so konvergieren die n-ten Näherungsbrüche von r gegen r, da nach Bem 3 die $q_i \in \mathbb{N}$ für $i \geq 1$ streng monoton steigen.

Bem 5 (ohne Bew) Sei $a_0, a_1, \ldots$ eine Folge nat. Zahlen.
Dann konvergiert $[a_0, \ldots, a_n]$ für $n \to \infty$ gegen eine reelle Zahl r.
Verschiedene Folgen konvergieren gegen verschiedene reelle Zahlen.
Die Kettenbruchentwicklung von r ist $[a_0, a_1, a_2, \ldots]$.

Bem 6 (ohne Bew) Sei $r \in \mathbb{R}$ und $r = [a_0, a_1, \ldots]$.
Die Kettenbruchentwicklung ist periodisch gdw r Nullstelle eines quadratischen irreduziblen Polynoms $f(x) \in \mathbb{Q}[x]$ ist.

Bsp 4

(i) Sei $\alpha := [1, 1, \ldots] = 1 + \frac{1}{[1,1,\ldots]} = 1 + \frac{1}{\alpha}$.

Dann $\alpha^2 - \alpha - 1 = 0$; α pos., also $\alpha = \frac{1+\sqrt{5}}{2}$.

(ii) $\sqrt{2} = 1 + (\sqrt{2} - 1) = 1 + \frac{1}{\frac{1}{\sqrt{2}-1}} = 1 + \frac{1}{\sqrt{2}+1} = 1 + \frac{1}{2 + (\sqrt{2}-1)} = [1, 2, 2, 2, \ldots]$

(iii) $\alpha := [1, 2, 2, 2, \ldots] = 1 + \frac{1}{[2,2,2,\ldots]} = 1 + \frac{1}{1+\alpha}$, also $\alpha^2 + \alpha = 1 + \alpha + 1 \Rightarrow \sqrt{2} = \alpha$

$$\boxed{[2,2,2,\ldots] = 2 + \frac{1}{2 + \frac{1}{2 \ldots}} = 1 + [1, 2, 2, \ldots] = 1 + \alpha}$$

Beste Approximationen von $\sqrt{2} \approx 1{,}41421 35\ldots$

$1; \quad 1 + \frac{1}{2}; \quad 1 + \frac{1}{2 + \frac{1}{2}} = \frac{7}{5} = 1{,}4$

oder mit Hilfe von Bem 3:

$\underbrace{\frac{p_0}{q_0} = 1}_{\text{ist beste Approx}}$, $\underbrace{\frac{p_1}{q_1} = \frac{3}{2}, \frac{p_2}{q_2} = \frac{7}{5}, \frac{p_3}{q_3} = \frac{17}{12}, \frac{p_4}{q_4} = \frac{41}{29}, \frac{p_5}{q_5} = \frac{99}{70}}_{\text{nach Bem 2}}, \frac{p_6}{q_6} = ?$

$\boxed{\approx 1{,}4142857}$

Approximiere $\sqrt{2}$ möglichst gut durch einen Bruch mit einem Nenner ≤ 50: $\sqrt{2} \approx \frac{41}{29}$

Bsp 3 $\sqrt{3}+2 = [\overline{4}]$; $\sqrt{5} = [2, \overline{4}]$
$\sqrt{3} = [1, \overline{1,2}]$

Bsp 4 $[\overline{3}] = \frac{3}{2} + \frac{\sqrt{13}}{2}$: $\alpha := [\overline{3}] = 3 + \frac{1}{[\overline{3}]} = 3 + \frac{1}{\alpha} \Rightarrow \alpha^2 - 3\alpha - 1 = 0 \Rightarrow \alpha = \frac{3}{2} + \frac{\sqrt{13}}{2}$ ($\alpha > 0$)

17. Vortrag: Der Primzahltest von Fermat und Carmichael-Zahlen

Es sei eine (sehr große) natürliche Zahl n gegeben. Wir wollen uns mit dem Problem beschäftigen, wie man entscheiden kann, ob n Primzahl ist. Dieses Problem spielt in der Kryptographie eine große Rolle.

Um zu zeigen, daß eine natürliche Zahl n eine Primzahl ist, kann man zeigen, daß sie durch keine Primzahl $< \sqrt{n}$ teilbar ist. Dies ist allerdings ein sehr mühsames Verfahren und für sehr große n auch mit einer Großrechenanlage kaum durchführbar.

Ein notwendiges Kriterium für die Primzahleigenschaft ergibt sich aus dem Satz von Fermat:

Ist p Primzahl, so ist $a^{p-1} \equiv 1 \pmod{p}$ für alle $a \in \mathbb{Z}$ mit $p \nmid a$ (Fermat)

Wir sagen: $n \in \mathbb{N}$ hat den Fermat-Test mit der Testbasis a bestanden, wenn $a^{n-1} \equiv 1 \pmod{n}$ gilt. In diesem Fall heißt n Pseudoprimzahl für die Basis a. Ist $\mathrm{ggT}(a,n)=1$ und n nicht Pseudoprimzahl für die Basis a, so ist n keine Primzahl.
Eine Primzahl p ist natürlich Pseudoprimzahl für jede zu p teilerfremde Basis (nach Fermat)

Es gibt aber auch zusammengesetzte Zahlen n, die Pseudoprimzahlen sind für jede zu n teilerfremde Basis. Solche Zahlen heißen Carmichael-Zahlen

Satz 1 Sei $n \geq 2$. $n \in \mathbb{N}$ ist Carmichael-Zahl genau dann, wenn gilt:

(i) n hat die Form $n = p_1 \cdots p_k$; p_i paarweise verschiedene Primzahlen $\neq 2$, $k \geq 3$

(ii) Für jeden Primteiler p_i von n gilt $(p_i - 1) \mid (n-1)$.

Beweis

$\Leftarrow$ Erfüllt n die Bedingungen (i) und (ii) und ist $(a,n)=1$, so folgt wegen

$$a^{p_i-1} \equiv 1 \pmod{p_i} \text{ (Fermat)}$$

also auch $a^{n-1} \equiv 1 \pmod{p_i}$ für $i=1,\dots,r$ und damit $a^{n-1} \equiv 1 \pmod{n}$.

$\Rightarrow$ Sei nun $a^{n-1} \equiv 1 \pmod{n}$ für jedes zu n teilerfremde a und n nicht Primzahl. Dann ist n ungerade, weil sonst aus $(-1)^{n-1} \equiv 1 \pmod{n}$ die Beziehung $n \mid 2$ folgen würde.

Beweis von Satz 1

$\Leftarrow$: Annahme: n erfüllt die Bedingungen (i) und (ii).

Sei $ggT(a,n) = 1$.

Nach Definition einer Carmichael-Zahl ist dann $a^{n-1} \equiv 1 \pmod{n}$ zu zeigen.

Wegen $ggT(a,p_i) = 1$ folgt nach Fermat

$$a^{p_i - 1} \equiv 1 \pmod{p_i} \quad \text{für } i = 1,\dots,k.$$

Nach Voraussetzung ist $n-1$ Vielfaches von p_i, etwa $(n-1) = z_i (p_i - 1)$.

Dann folgt

$$a^{n-1} \equiv (a^{p_i - 1})^{z_i} \equiv 1 \pmod{p_i} \quad \text{für } i = 1,\dots,k.$$

Also ist $a^{n-1} - 1$ Vielfaches von $p_1,\dots,p_k$.

Da $p_1,\dots,p_k$ Primzahlen sind, ist $a^{n-1}-1$ dann auch Vielfaches von $n = p_1 \cdots p_k$.

Also folgt

$$a^{n-1} \equiv 1 \pmod{n}.$$

$\Rightarrow$:

(i) Wir setzen voraus, daß $n > 2$ keine Primzahl ist und für jedes zu n teilerfremde a gilt: $a^{n-1} \equiv 1 \pmod{n}$ (d.h. n ist Carmichael-Zahl)

1. Schritt: Wir zeigen, daß n ungerade ist.

Annahme n ist gerade. Wegen $ggT(-1,n) = 1$ folgt nach Voraussetzung $(-1)^{n-1} \equiv 1 \pmod{n}$.

$n-1$ ist ungerade, also folgt $(-1)^{n-1} \equiv -1 \pmod{n}$.

Zusammen folgt $-1 \equiv 1 \pmod{n}$; also ist $n \mid 2$.

Wegen $n > 2$ ist dies nicht möglich.

2. Schritt

Sei p eine Primzahl mit $p^{\alpha} \mid n$, $p^{\alpha+1} \nmid n$, $\alpha \geq 1$.
Gezeigt wird: Dann ist $\alpha = 1$ (also ist kein Primzahlquadrat Teiler von n).

Es sei $g \in \mathbb{Z}$ eine Primitivwurzel mod p^{α};
d.h. $1 \pmod{p^{\alpha}}, g \pmod{p^{\alpha}}, \ldots, (g^{\varphi(p^{\alpha})-1} \pmod{p^{\alpha}})$ sind paarweise verschiedene Nebenklassen, und es gilt $g^{\varphi(p^{\alpha})} \equiv 1 \pmod{p^{\alpha}}$.
Dabei ist φ die Eulersche φ-Funktion; also $\varphi(p^{\alpha}) = p^{\alpha-1}(p-1)$.
Also folgt

$$(*) \qquad g^{m} \equiv 1 \pmod{p^{\alpha}} \iff m \text{ ist Vielfaches von } \varphi(p^{\alpha}).$$

Die Primitivwurzel $g \in \mathbb{Z}$ ist natürlich nicht eindeutig bestimmt; mit g ist auch jedes g^* Primitivwurzel, falls $g^* \equiv g \pmod{p^{\alpha}}$.
Nach dem Chinesischen Restsatz läßt sich die Primitivwurzel g so wählen, daß

$$g \equiv 1 \left(\bmod \frac{n}{p^{\alpha}}\right)$$

gilt (da $\operatorname{ggT}(p^{\alpha}, \frac{n}{p^{\alpha}}) = 1$).

Dann ist
$$g^{\varphi(p^{\alpha})} \equiv 1 \pmod{p^{\alpha}}$$
$$g^{\varphi(p^{\alpha})} \equiv 1 \left(\bmod \frac{n}{p^{\alpha}}\right),$$
also auch $g^{\varphi(p^{\alpha})} \equiv 1 \pmod{n}$

Da n nach Voraussetzung Carmichael-Zahl ist, gilt
$$g^{n-1} \equiv 1 \pmod{n}, \quad \text{also auch } g^{n-1} \equiv 1 \pmod{p^{\alpha}}.$$
Nach (*) folgt
$$p^{\alpha-1}(p-1) \mid (n-1)$$
Da p Teiler von ist, ist p nicht Teiler von $(n-1)$; also folgt $\alpha = 1$

3. Schritt:

Gezeigt wird: n ist nicht Produkt zweier verschiedener Primzahlen.

Annahme: $n = p \cdot q$; p, q verschiedene Primzahlen.

Betrachtet man Primitivwurzeln mod p und mod q, so erhält man analog zu Schritt 2

$$(p-1) \mid (n-1) \text{ und } (q-1) \mid (n-1)$$

Wegen $n - 1 = p \cdot q - 1 = p(q-1) + (p-1)$

Also ist $(p-1)$ auch Teiler von $p(q-1)$, also auch $(p-1) \mid q-1$.

Analog folgt $(q-1) \mid (p-1)$.

Insgesamt folgt $q - 1 = p - 1$; also $p = q$. Widerspruch.

Damit ist gezeigt, daß (i) gilt.

(ii) Nach (i) ist klar, daß n die Form $n = p_1 p_2 \cdots q_k$ besitzt.

Analog zu Schritt 2 folgt (für $l = 1$)

$$(p_i - 1) \mid (n-1) \quad \text{für } i = 1, \dots, k.$$

Bem.

Es läßt sich leicht nachprüfen, daß

$3 \cdot 11 \cdot 17$

die kleinste Carmichael-Zahl ist.

18. Vortrag

Der Primzahltest von Miller-Rabin

Es sei n eine (sehr große) natürliche Zahl. Wie lässt sich (möglichst schnell) entscheiden, ob n eine Primzahl ist?

Wir wollen hierfür ein probabilistisches Verfahren angeben, das in der Praxis häufig verwendet wird. Dabei handelt es sich um eine Weiterentwicklung des Fermat-Tests.

Bemerkung 1 **(Fermat-Test)**

Sei p Primzahl und $1 \leq a \leq p-1$.

Dann gilt nach Fermat $a^{p-1} \equiv 1 (mod\, p)$.

Sei $n > 2$ gegeben und $a \in \mathbb{N}$ mit $\text{ggT}(a, n) = 1$.

Gilt (i) $a^{n-1} \not\equiv 1 (mod\, n)$,

so ist n keine Primzahl.

Gilt (ii) $a^{n-1} \equiv 1 (mod\, n)$,

so lässt sich keine Aussage darüber machen, ob n Primzahl ist. (Fermat-Test)
Im Fall (ii) heißt n Pseudoprimzahl für die Basis a.

Findet man ein a, so dass n nicht Pseudoprimzahl ist für die Basis a, so ist n keine Primzahl.
Gibt es ein solches a nicht, so lässt sich nicht mit Hilfe des Fermat-Tests entscheiden, ob n Primzahl ist.
Solche Zahlen gibt es, sie heißen Carmichael-Zahlen.

Eine Weiterentwicklung des Fermat-Tests ist der Miller-Rabin-Test.

(nach Gary L. Miller und Michael O. Rabin benannt, die den Test 1976 veröffentlichten. Alternativ auch Miller-Selfridge-Rabin-Test genannt, da John L. Selfridge den Test bereits 1974 anwendete)

Satz 1 **(Der Miller-Rabin-Test)**

Gegeben sei eine natürliche Zahl $n > 2, 2 \nmid n$.

Es gelte $n - 1 = 2^s \cdot m$, m ungerade (also $2^s \mid (n-1), 2^{s+1} \nmid (n-1)$).

Sei $a \in \mathbb{N}$ mit ggT (a,n) = 1.

Man sagt:

n besteht den Miller-Rabin-Test mit der Testbasis a, wenn

(i) $a^m \equiv 1(mod\, n)$

oder

(ii) $a^{2^i} \cdot m \equiv -1\ (mod\, n)$ mit einem i mit $0 \leq i \leq s - i$

gilt.

Dann gilt:
n ist keine Primzahl, wenn n den Miller-Rabin-Test mit der Testbasis a nicht besteht
(also wenn weder (i) noch (ii) gilt).

(Besteht n den Miller-Rabin-Test mit der Basis a, so ist keine Aussage darüber möglich, ob n Primzahl ist)

Beweis

Sei $n = p$ eine Primzahl.

Dann ist zu zeigen, dass (i) oder (ii) gilt.

Nach Fermat gilt $a^{p-1} \equiv a^{2^s \cdot m} \equiv 1\ (mod\, p)$,

Sei $j \in \{0, \dots, s\}$ minimal mit $a^{2^j \cdot m} \equiv 1\ (mod\, p)$

Im Fall $j = 0$ folgt (i) und damit die Behauptung.

Noch zu betrachten ist der Fall $j > 0$.

Sei $i := j - 1$ (dann gilt $0 \leq i \leq s - 1$).

Es folgt $\left(a^{2^i \cdot m}\right)^2 \equiv a^{2^j \cdot m} \equiv 1\ (mod\, p)$

Also ist $\left(a^{2^i \cdot m}\right)^2 - 1 = \left(a^{2^i \cdot m} - 1\right)\left(a^{2^i \cdot m} + 1\right)$

Vielfaches von p. Da p Primzahl ist, folgt $p \mid \left(a^{2^i \cdot m} - 1\right)$ oder $p \mid \left(a^{2^i \cdot m} + 1\right)$

also $a^{2^i \cdot m} \equiv 1\ (mod\, p)$ oder $a^{2^i \cdot m} \equiv -1\ (mod\, p)$.

Die Definition von j ist aber $a^{2^i \cdot m} \not\equiv 1 \ (mod\ p)$.

Es folgt also $a^{2^i \cdot m} \equiv -1 \ (mod\ p)$, also die Kongruenz (ii).

Bemerkung 1

Sei $n > 2$; ggT $(a, n) = 1$.

Gilt (i) oder (ii), so folgt $a^{n-1} \equiv 1 (mod\ n)$.

Also:

Lässt sich mit Hilfe der Testbasis a nach dem Miller-Rabin-Test nicht entscheiden, ob n Primzahl ist, so auch nicht nach dem Fermat-Test. In diesem Sinn ist der Miller-Rabin-Test besser als der Fermat-Test.

Bemerkung 2 (ohne Beweis)

Für den Miller-Rabin-Test gibt es keine Analogie zu den Carmichael-Zahlen.

Genauer gilt:

Sei $n > 2$ keine Primzahl, $2 \nmid n$.

Dann gibt es mindestens $\frac{3}{4}(n-1)$ Testbasen a, deren Verwendung zeigt, dass n keine Primzahl ist.

Beispiel

Betrachte die (Carmichael-) Zahl $3 \cdot 11 \cdot 17 = 561$.

Verwende die Testbasis $a = 2$.

Es gilt $n = 561 - 1 = 2^4 \cdot 35 = 2^s \cdot m$

und weiter

$$2^{35} \equiv 263 \ (mod\ 561) \quad \text{(d.h. (i) gilt nicht)}$$

$$\left.\begin{aligned} 2^{2 \cdot 35} &\equiv 166 \ (mod\ 561) \\ 2^{4 \cdot 35} &\equiv 67 \ (mod\ 561) \\ 2^{8 \cdot 35} &\equiv 1 \ (mod\ 561) \end{aligned}\right\} \text{(d.h. (ii) gilt nicht)}$$

Mit Hilfe der Testbasis $a = 2$ kann also nach dem Miller-Rabin-Test gezeigt werden, dass n keine Primzahl ist. Nach dem Fermat-Test ist dies nicht möglich.

19. Vortrag

Die RSA-Verschlüsselung

Die Kongruenzrechnung findet Anwendung bei vielen Chiffrierverfahren. Betrachtet werden sollen hier sog. public-Key-Systeme.

Allgemein wird an jeden Teilnehmer T ein Chiffrierschlüssel S_T vergeben, durch den eine Verschlüsselungsfunktion V_T definiert wird. Die Grundidee besteht darin, V_T so zu wählen, daß die folgenden drei Bedingungen erfüllt sind:

(i) Das Bild eines Elementes bzgl V_T (die Verschlüsselung) läßt sich relativ leicht berechnen.

(ii) Das Urbild eines Elementes bzgl V_T (die Entschlüsselung) läßt sich – auch wenn V_T bekannt ist – nicht berechnen (zumindest nur mit einem Rechenaufwand, der sich in einem sinnvollen Zeitraum nicht bewältigen läßt)

(iii) Das Urbild eines Elementes bzgl. V_T läßt sich relativ leicht berechnen, wenn gewisse Zusatzinformationen G_T bekannt sind.

Der Sinn des Chiffrierverfahrens besteht darin, daß S_T (und damit V_T) öffentlich bekannt gemacht wird (öffentlich bekannter Chiffrierschlüssel für den Teilnehmer T, ähnlich der Telefonnummer eines Teilnehmers am öffentlichen Telefonnetz), die Zusatzinformation G_T (geheimer Schlüssel für den Teilnehmer T) jedoch nur dem Teilnehmer T (bzw. allen Personen, die authorisiert sind, die Nachrichten an den Teilnehmer T zu entschlüsseln).
Jedem Teilnehmer ist also ein öffentlich bekannter und ein geheimer Schlüssel zugeordnet. Der Vorteil dieses Verfahrens ist, daß jede Person ohne geheime Informationen an jeden Teilnehmer einen chiffrierten Text senden kann, der nur von authorisierten Personen dechiffriert werden kann.
Geheime Informationen zwischen den Teilnehmern müssen nicht ausgetauscht werden.

Das RSA-System

Nach dem RSA-System (Rivest, Shamir, Adleman, 1978) geschieht die Schlüsselvergabe an einen Teilnehmer wie folgt:

Wähle zwei große Primzahlen $p \neq q$.

Berechne $n = p \cdot q$.

Wähle eine natürliche Zahl e mit $(e, (p-1)\cdot(q-1)) = 1$.

Bestimme eine natürliche Zahl d mit $d \cdot e \equiv 1 \pmod{(p-1)\cdot(q-1)}$.

Der öffentliche Schlüssel ist dann (n, e), der geheime Schlüssel ist d.

Jede Nachricht wird in Einzelnachrichten $m \in \{0, \ldots, n-1\}$ zerlegt.

Die Verschlüsselungsfunktion V_T ist dann definiert durch

$$V_T : \{0, \ldots, n-1\} \longrightarrow \{0, \ldots, n-1\};$$
$$V_T(m) := c, \text{ wobei } c \equiv m^e \pmod n, \ 0 \leq c < n.$$

Die Entschlüsselung einer Einzelnachricht c' (mit Hilfe des geheimen Schlüssels d) erfolgt dann durch

$$c' \longmapsto m', \text{ wobei } m' \equiv c'^d \pmod n, \ 0 \leq m' < n$$

(denn wegen $a^{k(p-1)+1} \equiv a \pmod p$ f.a. $a \in \mathbb{Z}$ (für $a \equiv 0 \pmod p$ trivial, sonst nach Fermat (s. Satz 23.9, Seite 42 ~~Vorlesung~~ im Skript: Einf in die Algebra und Zahlentheorie))

und analog $a^{k(p-1)(q-1)+1} \equiv a \pmod q$ f.a. $a \in \mathbb{Z}$), folgt

dann auch $a^{k(p-1)(q-1)+1} \equiv a \pmod n$.

Grundlegend für die Sicherheit des Verfahrens ist die Geheimhaltung der Primzahlen p und q. Um die Faktorisierung des (öffentlich bekannten) n unmöglich zu machen, müssen zur Zeit p und q beide größer als 10^{100} gewählt werden (Zur Faktorisierung einer Zahl in der Größenordnung von 10^{300} wird heute mindestens eine Zeit von ca. 10^7 Jahren benötigt).

Eine Entschlüsselung ist nur möglich, wenn die Geheimzahl d bekannt ist und d läßt sich wiederum nur berechnen, wenn $\varphi(n)=(p-1)(q-1)$, also die Faktorisierung von n bekannt ist (eine Lösung von $x\cdot e \equiv 1 \pmod{(p-1)(q-1)}$ erhält man relativ schnell mit Hilfe des Euklidischen Algorithmus).

Das Verfahren ermöglicht es auch, die Echtheit einer Nachricht (im Rahmen der Sicherheit des Systems) zu garantieren. Will der Teilnehmer T_i mit dem öffentlichen Schlüssel (n_i, e_i) seine Nachricht an den Teilnehmer T_j mit dem öffentlichen Schlüssel (n_j, e_j) "elektronisch unterschreiben", so verschlüsselt T_i seine Nachricht zunächst mit (n_i, d_i) und anschließend mit (n_j, e_j). Zur Entschlüsselung benutzt B_j zunächst d_j, anschließend e_j. Auf diese Weise kann festgestellt werden, ob eine Nachricht wirklich von dem angegebenen Absender stammt (übrigens setzt die Telekom dieses Verfahren ein).

Bsp Wähle $p=7$, $q=13$, also $n=p\cdot q=91$.
Dann ist $\varphi(n)=6\cdot 12=72$.
Der öffentliche Schlüssel sei $e=23$.
Durch Anwendung des euklidischen Algorithmus zeigt man, daß der geheime Schlüssel $d=47$ ist.
Man zeigt, daß die Nachricht "2" zu "65" verschlüsselt wird.
Hilfreich ist dabei die Zerlegung $2^{23}=2^{16}\cdot 2^{4}\cdot 2^{2}\cdot 2$.

20. Vortrag:

Ein Angriff auf die RSA-Verschlüsselung und ein sicheres Verschlüsselungsverfahren

Werden bei der RSA-Verschlüsselung (s. Vortrag 18) die Primzahlen p und q so gewählt, daß n faktorisiert werden kann, so kann die Verschlüsselung natürlich geknackt werden.

Für große p und q ist eine Faktorisierung von n i.a. nicht möglich. Allerdings gibt es spezielle Fälle, in denen die Faktorisierung von n auch für sehr große p und q möglich ist. Eine solche Wahl von p und q muß natürlich vermieden werden.

Bem 1

Sei $p > q$. Da p und q als Primzahlen ungerade sind, ist $p-q$ gerade, etwa $p - q = 2 \cdot \ell$. Sei $k := p - \ell = q + \ell$.

Dann folgt $n = p \cdot q = (k+\ell)(k-\ell) = k^2 - \ell^2$.

Ist ℓ "klein", so läßt sich n also faktorisieren durch das folgende Verfahren:

Teste, ob $n + 1^2$ Quadratzahl ist. Hierfür gibt es sehr schnelle Algorithmen. Ist dies der Fall, so gilt etwa $n + 1^2 = k^2$ und man erhält eine Faktorisierung von n durch

$$n = (k+1)(k-1).$$

Ist $n + 1^2$ keine Quadratzahl, so teste man, ob $n + 2^2$ Quadratzahl ist. Ist dies der Fall, so erhält man eine Faktorisierung von n.

Fortführung dieses Probierverfahrens liefert nach ℓ Schritten die gewünschte Faktorisierung von n.

<u>Bsp1</u> Wähle $n = 391$ $(= 17 \cdot 23)$ und $e = 235$ als öffentlichen Schlüssel für die RSA-Verschlüsselung.

Man verwende die Faktorisierung von n um zu zeigen, daß der geheime Schlüssel $d = 3$ ist.

Faktorisiere n mit Hilfe der Methode aus Bem 1.

<u>Bsp2</u>. Faktorisiere $n = 1517$ und zeige, daß $n = 37 \cdot 41$ ist.

<u>Bem2</u>

Natürlich ist die RSA-Verschlüsselung nur mit sehr großer Wahrscheinlichkeit sicher.

Ein perfekt sicheres Verschlüsselungsverfahren erhält man wie folgt.

Die zu verschlüsselnde Nachricht soll der Einfachheit halber schon als als Folge von Nullen und Einsen vorliegen. Sie bestehe aus n Symbolen; etwa $a_1 \cdots a_n$.

Zum Verschlüsseln erzeuge man eine Zufallsfolge aus Nullen und Einsen mit n Symbolen, etwa $b_1 \cdots b_n$ (geheimer Schlüssel).

Man schreibe die beiden Folgen untereinander und addiere mod 2:

$$\begin{array}{ccc} a_1 & \cdots & a_n \\ b_1 & \cdots & b_n \\ \hline c_1 & \cdots & c_n \end{array}$$

Dann wird $a_1 \cdots a_n$ verschlüsselt zu $c_1 \cdots c_n$.

Kennt der Empfänger den geheimen Schlüssel, so kann er $c_1 \cdots c_n$ leicht entschlüsseln.

Das Verfahren ist absolut sicher, denn alle Folgen aus n Symbolen haben die gleiche Wahrscheinlichkeit als verschlüsselter Text erzeugt zu werden.

Das Verfahren besitzt allerdings zwei gravierende Nachteile:

Der Empfänger muß den Schlüssel kennen, der Schlüsselaustausch ist aber sehr kompliziert.

Außerdem kann ein Schlüssel nur ein Mal verwendet werden, da die Verschlüsselung sonst eventuell durch eine Häufigkeitsanalyse geknackt werden kann.

21. und 22. Vortrag:

Der Wiener Angriff auf die RSA-Verschlüsselung

Seien p und q zwei verschiedene große Primzahlen und $n := p \cdot q$. Sind p und q sehr groß, so läßt sich n nicht faktorisieren, da der Rechenaufwand hierfür zu groß ist.

Bei der RSA-Verschlüsselung wird ein $e \in \mathbb{N}$ gewählt mit $1 < e < \varphi(n) = (p-1)(q-1)$ und $ggT(e, (p-1)\cdot(q-1)) = 1$ (s. Vortrag 20)

Dann ist e der sogenannte öffentliche Schlüssel.

Sind p und q bekannt, also auch $(p-1)(q-1)$, so läßt sich mit Hilfe des Euklidischen Algorithmus ein $d \in \mathbb{N}$ bestimmen mit

$$1 < d < \varphi(n) \quad \text{und} \quad e \cdot d \equiv 1 \pmod{\varphi(n)}.$$

Dann ist d der zu e (und n) gehörige geheime Schlüssel.

Eine Nachricht $m \in \mathbb{N}$ mit $0 < m < n$ wird verschlüsselt zu $c \in \mathbb{N}$ mit $0 < c < n$ und $m^e \equiv c \pmod{n}$.

Die verschlüsselte Nachricht kann entschlüsselt werden durch Bildung von c^d, falls d bekannt ist.

I.a. läßt sich d ohne Kenntnis von p und q nicht bestimmen, die Nachricht c also nicht entschlüsseln.

Unter gewissen Voraussetzungen ist dies aber doch möglich. In der Praxis muß dies natürlich vermieden werden.

Ein Beispiel ist der der Angriff von Wiener.

Satz 1 (Angriff von Wiener)

Bei der RSA-Verschlüsselung seien die Primzahlen p und q so gewählt, daß $q < p < 2q$ ist.

Ferner sei e so gewählt, daß $d < \frac{1}{3} n^{\frac{1}{4}}$ ist.

Dann kann das RSA-Verfahren mit einem schnellen Algorithmus wie folgt gebrochen werden:

Entwickle $\frac{e}{n}$ in einen Kettenbruch (siehe Vortrag 14).

Gelte $\frac{e}{n} = [a_0, a_1, \ldots, a_m]$, dabei sei oBdA $a_m = 1$.

Die Näherungsbrüche von $\frac{e}{n}$ seien $\frac{p_0}{q_0}, \ldots, \frac{p_m}{q_m}$.

Dann ist der geheime Schlüssel d einer der Nenner $q_0, \ldots, q_m$.

Anmerkung:

Die Näherungsbrüche lassen sich auch für sehr große n schnell berechnen und im Vergleich zu n ist m sehr klein.

Testet man durch die Verschlüsselung einiger Nachrichten, welches der $q_0, \ldots, q_m$ zu der richtigen Entschlüsselung führt, so ist der geheime Schlüssel bestimmt.

Bew von Satz 1

(1) Zum Beweis wird die folgende Aussage aus der Theorie der Kettenbrüche verwendet (ohne Bew.)

Seien $m_0, m_1 \in \mathbb{N}$; $p, q \in \mathbb{N}$ und $\left| \frac{m_0}{m_1} - \frac{p}{q} \right| < \frac{1}{2q^2}$

Dann ist $\frac{p}{q}$ ein Näherungsbruch von $\frac{m_0}{m_1}$.

(2) Es gilt $e \cdot d \equiv 1 \pmod{(p-1)(q-1)}$, etwa

$$e \cdot d - 1 = K(p-1)(q-1) \quad \text{mit } K \in \mathbb{N}.$$

Nach (1) genügt es dann zu zeigen, daß

$$\left| \frac{e}{n} - \frac{K}{d} \right| < \frac{1}{2d^2} \qquad (*)$$

gilt

(3) Beweis von $(*)$:

$$\left| \frac{e}{n} - \frac{K}{d} \right| = \left| \frac{ed - K \cdot n}{nd} \right| = \left| \frac{ed - K(p-1)(q-1) - Kn + K(p-1)(q-1)}{nd} \right|$$

$$\underset{(2)}{=} \left| \frac{1 - K \cdot n + K(p-1)(q-1)}{n \cdot d} \right| = \left| \frac{1 - K(n - (p-1)(q-1))}{n \cdot d} \right|$$

$$\underset{\boxed{n-(p-1)(q-1) = p+q-1}}{=} \left| \frac{1 - K(p+q-1)}{n \cdot d} \right| = \frac{K(p+q-1) - 1}{n \cdot d} < \frac{K(p+q)}{n \cdot d} <$$

$$\underset{\boxed{\text{wegen } n = p \cdot q,\ q < p \text{ ist } q < \sqrt{n},\ \text{dann gilt auch } p < 2q < 2\sqrt{n}}}{<} \frac{K \cdot 3\sqrt{n}}{d \cdot n} \leq \frac{1}{d \cdot n^{1/4}} \underset{\text{Vor}}{<} \frac{1}{3d^2} < \frac{1}{2d^2}.$$

Es gilt

$K(p-1)(q-1) \underset{s.o.}{=} e \cdot d - 1$,

$e < (p-1)(q-1)$ nach Vor.;

also $K < \frac{e \cdot d}{(p-1)(q-1)} < d \underset{\text{Vor}}{<} \frac{1}{3} n^{\frac{1}{4}}$

Bsp (für den Angriff von Wiener)

Wähle $n = 391$ $(= 17 \cdot 23)$; $e = 235$.

Versuche den geheimen Schlüssel d zu bestimmen.

Berechne die Kettenbruchentwicklung von $\frac{235}{391}$:

$235 = \underline{0} \cdot 391 + 235$	1. Näherungsbruch von $\frac{235}{391}$: $\underline{0}$	$= [0]$
$391 = \underline{1} \cdot 235 + 156$	2. Näherungsbruch von $\frac{235}{391}$: $\underline{0} + \frac{1}{\underline{1}}$	$= [0,1]$
$235 = \underline{1} \cdot 156 + 79$	3. " : $\underline{0} + \frac{1}{\underline{1} + \frac{1}{\underline{1}}}$	$= [0,1,1]$
$156 = \underline{1} \cdot 79 + 77$	4. " : $0 + \frac{1}{1 + \frac{1}{1 + \frac{1}{1}}}$	$= [0,1,1,1]$
$79 = \underline{1} \cdot 77 + 2$	5. "	$[0,1,1,1,1]$
$77 = \underline{38} \cdot 2 + 1$	6. "	$[0,1,1,1,1,38]$
$2 = \underline{2} \cdot 1$		$[0,1,1,1,1,38,2]$

Mit Hilfe der Rekursionsformeln aus Vortrag 14 erhält man die Näherungsbrüche

$$\frac{0}{1} = 0, \quad 0 + \frac{1}{1} = \frac{1}{1}, \quad \frac{1}{2}, \quad \frac{2}{3}, \quad \frac{3}{5}, \quad \frac{3 \cdot 38 + 2}{5 \cdot 38 + 2} = \frac{116}{192}, \quad \frac{235}{391}$$

Teste, ob einer der Nenner 1, 2, 3, 5, 92, 391 der geheime Schlüssel ist.

$d = 1$ ist nicht möglich, da stets $d > 1$.

$d = 2$ ist nicht möglich: Wähle $m = -1$ als Nachricht.
m wird verschlüsselt zu $c \equiv m^{235} \equiv -1 \pmod{n}$.
Im Fall $d = 2$ würde c entschlüsselt zu $c^2 \equiv 1 \pmod{n}$.
Widerspruch.

Teste $d = 3$: Wähle einige zufällige Nachrichten.
Man stellt fest, daß für $d = 3$ der Text jedes Mal richtig entschlüsselt wird.
$d = 3$ ist wahrscheinlich der geheime Schlüssel.

(Tatsächlich ist dies der Fall, was sich leicht ausrechnen läßt, da p und q bekannt sind) Der Wiener-Angriff führt also zum Ziel.
Allerdings haben wir Glück gehabt, da die Voraussetzung über d in diesem Fall gar nicht erfüllt ist.

23. Vortrag

Das Legendre-Symbol

§9 Das quadratische Reziprozitätsgesetz

Untersucht werden soll die Lösbarkeit einer quadratischen Kongruenz der Form

$$x^2 \equiv a\ (mod p); p > 2\ Primzahl, p \nmid a; a \in \mathbb{Z}.$$

Definition 1 (Legendre-Symbol)

Sei $a \in \mathbb{Z}, p > 2$ Primzahl. Dann wird das Legendre-Symbol definiert durch

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & & x^2 \equiv a\ (mod p)\ lösbar, p \nmid a \\ -1 & \text{falls} & x^2 \equiv a\ (mod p)\ nicht\ lösbar, p \nmid a \\ 0 & & p \mid a \end{cases}$$

Im Fall $\left(\frac{a}{p}\right) = 1$ heißt a Quadratischer Rest $mod p$ (QR $mod p$). (s. Def. 8.1)

Im Fall $\left(\frac{a}{p}\right) = -1$ heißt a Quadratischer Nichtrest $mod p$ (QNR $mod p$).

Bemerkung 1

Sei p eine Primzahl $g \in \mathbb{Z}$, dann heißt g Primitivwurzel $mod p$ (PW $mod p$), falls

$g^0(mod p)$,..., $g^{p-2}(mod p)$ alle von 0 $(mod p)$ verschiedenen Restklassen $(mod p)$ sind.

Dann ist $g^{p-1} \equiv g^0 \equiv 1(mod p)$. Es folgt: $g^i \equiv g^j(mod p) \Leftrightarrow (p-1) \mid (\mathrm{i}-\mathrm{j})$

Satz 1

(a) $a \equiv b\ (mod p) \Longrightarrow \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$ (Beweis trivial)

(b) $\left(\frac{a^2}{p}\right) = 1$,falls $p \nmid a; \left(\frac{1}{p}\right) = 1.$ (Beweis trivial)

(c) $\left(\frac{a}{p}\right) = 1 \Longrightarrow x^2 \equiv a\ (mod p)$ besitzt genau 2 Lösungen

(d) Sei g PW $mod p$ und $a \equiv g^{ind(a)}(mod p)$.
(Dabei ist ind(a) mod (p-1) eindeutig bestimmt). Dann gilt
(siehe obige Bemerkung)

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \text{falls} & 2 \mid ind(a) \\ -1 & & 2 \nmid ind\ (a) \end{cases}$$

(e) Jedes vollständige prime Restsystem $mod p$ enthält genau $\frac{p-1}{2}$

QR $mod p$, nämlich $g^0, g^2, \ldots, g^{p-3} = g^{\frac{p-3}{2}\cdot 2}$ und genau $\frac{p-1}{2}$

QNR $mod p$, nämlich $g, g^3, g^5, \ldots, g^{p-2}$ (Dabei sei g PW $mod p$)

Beweis

(c) Ist x_0 Lösung von $x^2 \equiv a\ (modp)$, so gilt

$x^2 - {x_0}^2 = (x - x_0)(x + x_0) \equiv 0(modp)\ und\ - x_0$ ist die einzige weitere Lösung.

(d) Ist 2 | $ind(a)$, so folgt $(g^{\frac{ind(a)}{2}})^2 \equiv a(modp), also \left(\frac{a}{p}\right) = 1.$

Sei $\left(\frac{a}{p}\right) = 1$, etwa ${x_0}^2 \equiv a\ (modp), x_0 \equiv g\quad (modp)$, so folgt $ind(a) \equiv 2\ \ (mod(p-1))$, also 2 | $ind(a)$.

(e) Klar nach (d).

Besonders wichtig ist

Satz 2 (Multiplikativität des Legendre-Symbols)

$$\left(\frac{a \cdot b}{p}\right) = \left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right)$$

Bew. Klar nach Satz 1 (d).

Führe eine Fallunterscheidung durch.

1. Fall: $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right) = -1$

Dann: $a \equiv g^i(modp), b \equiv g^j(modp)$, i und j ungerade $\Longrightarrow i + j$ gerade

$a \cdot b \equiv g^{i+j}(modp), also \left(\frac{a \cdot b}{p}\right) = +1$

Bem. 1 Zur Berechnung des Legendre-Symbols genügt es also,

$\left(\frac{-1}{p}\right), \left(\frac{2}{p}\right), \left(\frac{q}{p}\right)$ zu kennen, wobei p und q ungerade Primzahlen sind.

Hierfür werden im folgenden 3 Regeln hergeleitet (Reziprozitätsgesetz mit 2 Ergänzungen).

Zunächst gilt

Satz 3 (Euler-Kriterium)

Sei $p > 2\ Primzahl, p \nmid a. Dann\ gilt$

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

Beweis

Sei $\left(\frac{a}{p}\right) = 1$, etwa ${x_0}^2 \equiv a(modp)$. Dann folgt $a^{\frac{p-1}{2}} \equiv {x_0}^{p-1} \underbrace{\equiv}_{\text{(Fermat,S.46)}} 1(modp)$

Sei $\left(\frac{a}{p}\right) = -1$. Dann ist nach Satz 1 (d) ind(a) ungerade, etwa $a \equiv g^{2a+1}(modp)$

Es folgt $a^{\frac{p-1}{2}} \equiv \underbrace{g^{(p-1)a}}_{\equiv 1(\text{mod } p)\text{, S. 46, Fermat}} \cdot g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}}(modp).$

Nun ist aber $g^{\frac{p-1}{2}} \equiv -1(modp)$, denn nach Fermat

ist $g^{\frac{p-1}{2}}$ Lösung von $x^2 - 1 \equiv 0(modp)$, also Lösung

von $(\mathrm{x}-1)(\mathrm{x}+1) \equiv 0(\mathrm{modp})$

Satz 3 ergibt für $\mathrm{a} = -1$

Satz 4 (1. Ergänzung zum quadratischen Reziprozitätsgesetz)

Sei $p \neq 2$ *eine Primzahl*

Dann gilt

$$\left(\frac{-1}{p}\right) \equiv \begin{cases} 1 & falls \; p \equiv 1 \; (mod4) \\ -1 & \; p \equiv 3 \; (mod4) \end{cases}$$

Beweis

Es gilt modp

$$\left(\frac{-1}{p}\right) \underbrace{\equiv}_{Satz\,3} (-1)^{\frac{p-1}{2}} \equiv \begin{cases} 1 & falls \; p \equiv 1(mod4) \\ -1 & \; p \equiv 3(mod4) \end{cases}$$

$\left(\frac{-1}{p}\right)$ kann die Werte ± 1 annehmen.

Ferner gilt $1 \not\equiv -1(modp)$.

Damit folgt die Behauptung.

Satz 5 (2. Ergänzung zum quadratischen Reziprozitätsgesetz) [ohne Beweis]

Sei $p \neq 2$ eine Primzahl

Dann gilt

$$\left(\frac{2}{p}\right) \equiv \begin{cases} 1 & falls \; p \equiv \pm 1 \; (mod8) \\ -1 & \; p \equiv \pm 3 \; (mod8) \end{cases}$$

Im nächsten Vortrag wird das für die Theorie der quadratischen Reste zentrale Quadratische Reziprozitätsgesetz behandelt.

24. Vortrag:

Das quadratische Reziprozitätsgesetz

<u>Satz 1</u> (quadratisches Reziprozitätsgesetz)

Seien p, q zwei verschiedene Primzahlen $\neq 2$.

Dann gilt:

$$\left(\frac{q}{p}\right)=\left(\frac{p}{q}\right) \Leftrightarrow \quad p \equiv 1 \pmod 4 \text{ oder } q \equiv 1 \pmod 4.$$

Dabei bezeichnen $\left(\frac{q}{p}\right)$ bzw. $\left(\frac{p}{q}\right)$ das Legendre-Symbol (s. Vortrag 23).

Beweis (Gauß) [wird nicht durchgeführt]

Betrachte das Halbsystem $\{1,\dots,\frac{q-1}{2}\}$ mod q.

Es bezeichne ν die Anzahl aller Zahlen $p\cdot x$ für $x=1,\dots,\frac{q-1}{2}$, die mod q kongruent sind zu eine der Zahlen $-1,-2,\dots,-\frac{q-1}{2}$.

Nach Lemma 1 ist dann $\left(\frac{p}{q}\right)=(-1)^{\nu}$.

Die Zahl ν wird nun genauer untersucht. Offenbar ist ν die Anzahl aller $x\in\{1,\dots,\frac{q-1}{2}\}$, für die ein $y\in\mathbb{Z}$ existiert mit $-\frac{q}{2}<px-qy<0$

Existiert zu x ein solches y, so gilt: y ist eindeutig bestimmt; $y>0$; $y\le\frac{p-1}{2}$ (wegen $qy<px+\frac{q}{2}<p\cdot\frac{q-1}{2}+\frac{q}{2}=q\left(\frac{p}{2}+\frac{1}{2}\right)-\frac{p}{2}<q\cdot\frac{p+1}{2}$).

(1) $\begin{cases}\text{Also ist } \nu \text{ die Anzahl aller Paare } (x,y) \text{ mit } x\in\{1,\dots,\frac{q-1}{2}\},\ y\in\{1,\dots,\frac{p-1}{2}\}\\ \text{und } -\frac{q}{2}<px-qy<0.\end{cases}$

Bei Vertauschung der Rollen von p und q erhält man analog: $\left(\frac{q}{p}\right)=(-1)^{\nu'}$, wobei ν' die Anzahl aller Paare (x,y) ist mit $x\in\{1,\dots,\frac{p-1}{2}\}$, $y\in\{1,\dots,\frac{q-1}{2}\}$ und $-\frac{p}{2}<qx-py<0$.

Vertauscht man die Bezeichnungen für x und y, so erhält man:

(2) $\begin{cases}\nu' \text{ ist die Anzahl aller Paare } (x,y) \text{ mit } x\in\{1,\dots,\frac{q-1}{2}\},\ y\in\{1,\dots,\frac{p-1}{2}\}\\ \text{und } -\frac{p}{2}<qy-px<0 \text{ bzw. } 0<px-qy<\frac{p}{2}.\end{cases}$ (Man beachte, daß es für die Anzahl ν' keine Rolle spielt, ob ich die Paare (x,y) oder (y,x) betrachte).

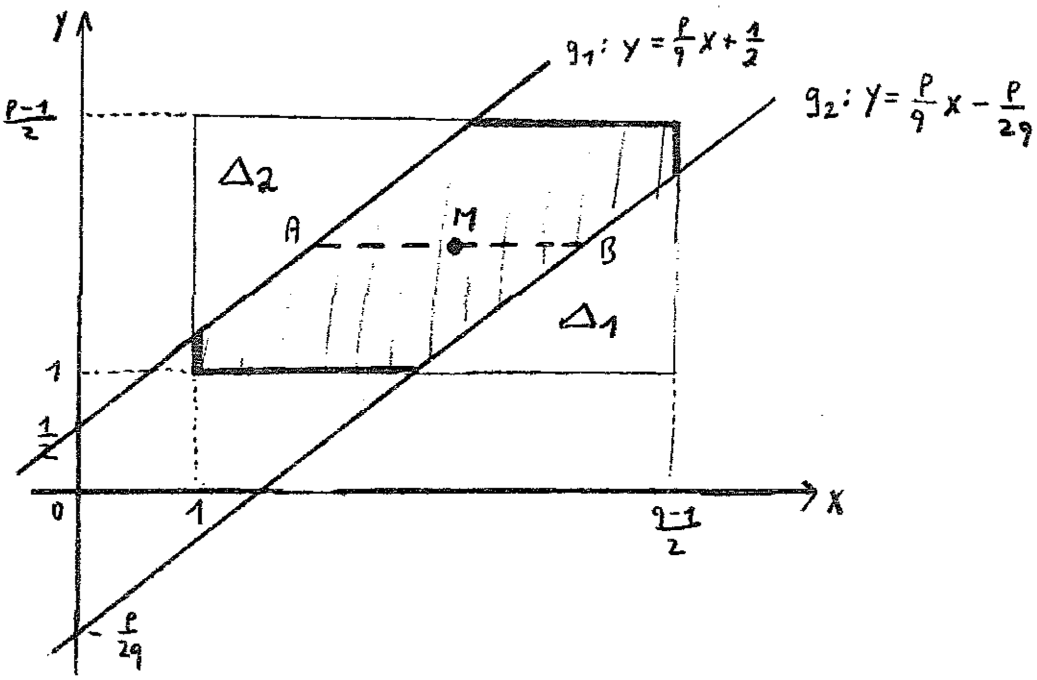
Man beachte, daß $px-qy=0$ nur möglich ist für $p\mid y$ und $q\mid x$; also ist $px-qx\neq 0$ für alle $x\in\{1,\dots,\frac{q-1}{2}\}$, $y\in\{1,\dots,\frac{p-1}{2}\}$. Dann folgt aus (1) und (2):

$\left(\frac{p}{q}\right)\cdot\left(\frac{q}{p}\right)=(-1)^{\nu+\nu'}$, wobei $\nu+\nu'$ die Anzahl aller Paare (x,y) ist mit $x\in\{1,\dots,\frac{q-1}{2}\}$, $y\in\{1,\dots,\frac{p-1}{2}\}$ und $-\frac{q}{2}<px-qy<\frac{p}{2}$.

Dabei ist die letzte Bedingung gleichwertig mit $\frac{p}{q}x-\frac{p}{2q}<y<\frac{p}{q}x+\frac{1}{2}$.

Zum Beweis des Satzes genügt es, $v+v'$ mod 2 zu bestimmen.

Dies geschieht durch eine geometrische Deutung.



Offenbar ist $v+v'$ die Anzahl der Gitterpunkte im schraffierten Bereich, einschließlich des Randes des Rechtecks, aber ausschließlich der Punkte auf den Geraden g_1 oder g_2.

Es bezeichne M den Mittelpunkt des Rechtecks, also $M = \left(\frac{q+1}{4}, \frac{p+1}{4}\right)$.

Es bezeichne A den Schnittpunkt von g_1 mit der Parallelen durch M zur x-Achse.

Es bezeichne B den Schnittpunkt von g_2 mit der Parallelen durch M zur x-Achse.

Dann gilt $A = \left(x_1, \frac{p+1}{4}\right)$ mit $x_1 = \frac{p-1}{4} \cdot \frac{q}{p}$,

$B = \left(x_2, \frac{p+1}{4}\right)$ mit $x_2 = \left(\frac{p+1}{4} + \frac{p}{2q}\right) \cdot \frac{q}{p}$.

Also ist $\frac{x_1+x_2}{2} = \frac{q+1}{4}$; d.h. M hat zu A und B den gleichen Abstand.

Eine Drehung um M um $180°$ überführt dann das Dreieck Δ_1 in das Dreieck Δ_2. Bei dieser Drehung handelt es sich um eine Punktspiegelung am Punkt M, die den dem Punkt P zugehörigen Ortsvektor $\vec{P} = \vec{M} + (\vec{P} - \vec{M})$ abbildet auf $\vec{M} - (\vec{P} - \vec{M}) = 2\vec{M} - \vec{P}$. Da $2\vec{M}$ ganzzahlige Koordinaten : $\frac{q+1}{2}$ und $\frac{p+1}{2}$ besitzt (beachte: p, q sind ungerade Primzahlen), werden bei dieser Spiegelung Gitterpunkte in Gitterpunkte überführt.

Also enthalten Δ_1 und Δ_2 (mit Rand) gleich viele Gitterpunkte, etwa g. Die Anzahl der Gitterpunkte im Rechteck mit Rand beträgt $\frac{q-1}{2} \cdot \frac{p-1}{2}$.

Die Anzahl der Gitterpunkte im schraffierten Bereich ist also $\frac{q-1}{2} \cdot \frac{p-1}{2} - 2g$.

Hieraus folgt die Behauptung.

Das quadratische Reziprozitätsgesetz nimmt eine zentrale Stellung innerhalb der Zahlentheorie ein. Der hier aufgeführte Beweis folgt einer Idee von Gauß. Bis heute sind über Hundert verschiedene Beweise bekannt. Interessant sind vor allem solche Beweise, die verallgemeinerungsfähig sind. Tatsächlich läßt sich das quadratische Reziprozitätsgesetz sehr weitreichend verallgemeinern (z.B. auf Kongruenzen vom Grad ≥ 2) und zu einer tiefliegenden Theorie ausbauen (Klassenkörpertheorie).

<u>Bsp</u> $\left(\frac{3}{37}\right) \underset{5.6}{=} \left(\frac{37}{3}\right) \underset{5.1(a)}{=} \left(\frac{1}{3}\right) \underset{5.1(b)}{=} 1$;

$$\left(\frac{45}{23}\right) \underset{5.2}{=} \left(\frac{3}{23}\right) \cdot \left(\frac{5}{23}\right) \underset{5.6}{=} -\left(\frac{23}{3}\right) \cdot \left(\frac{23}{5}\right) \underset{5.1(a)}{=} -\underbrace{\left(\frac{2}{3}\right)}_{=-1} \left(\frac{3}{5}\right) \underset{5.6}{=} \left(\frac{5}{3}\right) \underset{5.1(a)}{=} \left(\frac{2}{3}\right) = -1$$

Mit Hilfe der bisher bewiesenen Aussagen läßt sich das Legendre-Symbol relativ bequem ausrechnen. Ein Nachteil ist, daß der "Zähler" jeweils in ein Produkt von Primzahlen zerlegt werden muß. Dies kann bei großen Zahlen recht aufwendig sein ~~Im nächsten § wird gezeigt, wie sich dies vermeiden läßt.~~

Bsp 1 (zur Theorie der Quadratischen Reste)

Für welche Primzahlen p ist die Kongruenz $x^2 \equiv 7 \pmod p$ lösbar?

(i) Für $p=2$ ist 1 eine Lösung.

(ii) Sei $p \neq 2$. Dann gilt:

$$\left(\frac{7}{p}\right)=1 \iff \begin{cases} \left(\frac{p}{7}\right)=1, \text{ falls } p \equiv 1 \pmod 4 \\ \text{oder} \\ \left(\frac{p}{7}\right)=-1, \text{ falls } p \equiv 3 \pmod 4 \end{cases} \iff \begin{cases} p \equiv 1,4,2 \pmod 7, \text{ falls } p \equiv 1 \pmod 4 \\ \text{oder} \\ p \equiv 3,5,6 \pmod 7, \text{ falls } p \equiv 3 \pmod 4 \end{cases}$$

Quadratisches Reziprozitätsgesetz

z.B. ist $\left(\frac{3}{7}\right)=\left(\frac{5}{7}\right)=-1$, $\left(\frac{2}{7}\right)=1$.
Dies ergibt sich aus den Rechenregeln für das Legendre-Symbol;
man kann auch alle Restklassen mod 7 durchprobieren

$$\iff \begin{cases} p \equiv 1,25,9 \pmod{28} \\ \text{oder} \\ p \equiv 3,19,27 \pmod{28} \end{cases} \iff p \equiv 1,25,9,3,19,27 \pmod{28}$$

Verwende den Chinesischen Restsatz:
Seien $n_1, n_2 \in \mathbb{N}$, $ggT(n_1,n_2)=1$.
Seien $a_1, a_2 \in \mathbb{Z}$.
Dann ex. ein $a \in \mathbb{Z}$ mit

$a \equiv a_1 \pmod{n_1}$

$a \equiv a_2 \pmod{n_2}$

und a ist mod $n_1 \cdot n_2$ eindeutig bestimmt.
z.B. ist $p \equiv 4 \pmod 7$ und $p \equiv 1 \pmod 4$ gleichwertig mit $p \equiv 25 \pmod{28}$

Die Lösungsmenge läßt sich also durch Restklassen mod 28 beschreiben.

Allgemein gilt (ohne Bew.):

$$\left(\frac{a}{p_1}\right)=\left(\frac{a}{p_2}\right), \text{ falls } p_1 \equiv p_2 \pmod{4|a|} \text{ ist.}$$

Anmerkung (ohne Bew.):
Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $ggT(a,n)=1$.
Dann ex. ∞ viele Primzahlen p mit

$$p \equiv a \pmod n.$$

-63- Sei $\pi^*(m) :=$ Anzahl aller Primzahlen p mit $p \equiv a \pmod n$, $p \leq m$; sei φ die Eulersche φ-Funktion.
Dann gilt:

$$\lim_{m \to \infty} \frac{\pi^*(m)}{\frac{m}{\log m}} = \frac{1}{\varphi(n)} \quad \text{(Dirichletscher Primzahlsatz)}$$

Bsp 2 Bestimmung der Lösungen von

$$(1) \quad 64x^2 + 3x + 1 \equiv 0 \pmod{131}.$$

__Idee__: Wende quadratische Ergänzung an analog wie zur Herleitung der (p,q)-Formel für quadratische Polynome. Notwendig ist dafür eventuell eine Division durch 2. Diese ist in diesem Fall möglich, denn 131 ist Primzahl, der Restklassen $\mathbb{Z}_{131}$ also ein Körper.

__1. Schritt__: Normiere die quadratische Kongruenz (1), d.h. multipliziere sie mit dem multiplikativen Inversen von 64 (mod 131).

Hierfür ist eine Lösung von $64x \equiv 1 \pmod{131}$ zu bestimmen.

Diese erhält man durch Probieren (umständlich), hier besser durch Verwendung des Euklidischen Algorithmus.

Zu bestimmen sind $\lambda, \mu \in \mathbb{Z}$ mit $\lambda \cdot 64 + \mu \cdot 131 = 1$ $(= ggT(64, 131))$.

Betrachte die Gleichungen

$$\begin{aligned} 131 &= 2 \cdot 64 + 3 \\ 64 &= 21 \cdot 3 + 1 \\ 3 &= 3 \cdot 1 + 0. \end{aligned}$$

Es folgt $1 = 64 - 21 \cdot 3 = 64 - 21(131 - 2 \cdot 64) = 43 \cdot 64 - 21 \cdot 131$.

Es folgt $64 \cdot 43 \equiv 1 \pmod{131}$.

Multiplikation von (1) mit 43 liefert

$$(2) \quad x^2 + \underbrace{3 \cdot 43}_{\equiv -2 \pmod{131}} x + 43 \equiv 0 \pmod{131}.$$

__2. Schritt__ Offenbar besitzen (1) und (2) dieselben Lösungen.

Offenbar ist (2) gleichwertig mit

$$(3) \quad (x-1)^2 \equiv -42 \pmod{131} \quad \text{(quadratische Ergänzung)}$$

__3. Schritt__ Wir prüfen zunächst, ob (3) eine Lösung besitzt.

Hierzu wird das Legendre-Symbol $\left(\frac{-42}{131}\right)$ betrachtet.

(3) besitzt eine Lösung gdw $\left(\frac{-42}{131}\right) = 1$ ist.

Nach den Rechenregeln für das Legendre-Symbol gilt:

$$\left(\frac{-42}{131}\right) = \underbrace{\left(\frac{-1}{131}\right)}_{\substack{= -1 \\ (1.\,Erg.)}} \cdot \underbrace{\left(\frac{2}{131}\right)}_{\substack{= -1 \\ (2.\,Erg.)}} \cdot \left(\frac{3}{131}\right) \cdot \left(\frac{7}{131}\right) = 1$$

$$\left(\frac{7}{131}\right) \underset{(QRG)}{=} -\left(\frac{131}{7}\right) = -\left(\frac{5}{7}\right) \underset{(QRG)}{=} -\left(\frac{7}{5}\right) = -\left(\frac{2}{5}\right) \underset{(2.\,Erg.)}{=} 1$$

$$\left(\frac{3}{131}\right) \underset{(QRG)}{=} -\left(\frac{131}{3}\right) = -\left(\frac{2}{3}\right) \underset{(2.\,Erg.)}{=} 1$$

Die Kongruenz (3) ist also lösbar.

__4. Schritt__ Bestimme die Lösungen von (3).

Durch Probieren der endlich vielen Restklassen mod 131 erhält man für $x^2 \equiv -42 \pmod{131}$ genau die Lösungen $\pm 58 \pmod{131}$.

Es gibt schnellere Verfahren, die hier nicht weiter beschrieben werden.

Die Lösungen von (1) mod 131 sind also 1 ± 58.

Der Gaußsche Zahlring und der Euklidische Algorithmus

Wir betrachten die Teilmenge $\mathbb{Z}[i] := \{a+bi \mid a,b \in \mathbb{Z}\}$ von $\mathbb{C}$, also die Menge aller komplexen Zahlen mit ganzzahligem Realteil und ganzzahligem Imaginärteil.

Offenbar ist dann $\mathbb{Z}[i]$ ein Unterring von $\mathbb{C}$. Dieser ist kommutativ (d.h. die Multiplikation ist kommutativ) und nullteilerfrei (d.h.: $z_1, z_2 \in \mathbb{Z}[i]$; $z_1 \cdot z_2 = 0 \Rightarrow z_1 = 0$ oder $z_2 = 0$). Ferner ist $1 \in \mathbb{Z}[i]$.

Also ist $\mathbb{Z}[i]$ ein Integritätsbereich mit Eins.

Als Hauptergebnis wollen wir zeigen, daß $\mathbb{Z}[i]$ ein Euklidischer Ring ist.

Als Vorbereitung betrachten wir dazu die Normfunktion

$N: \mathbb{C} \to \mathbb{R}$ definiert durch $N(a+bi) := (a+bi)(a-bi) = a^2+b^2$.

Bem 1

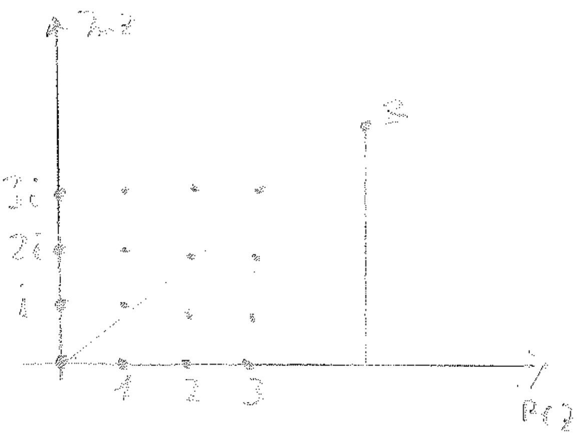
Für $z = a+bi \in \mathbb{C}$ bezeichne $\bar{z} := a-bi$ die zu z konjugiert komplexe Zahl.

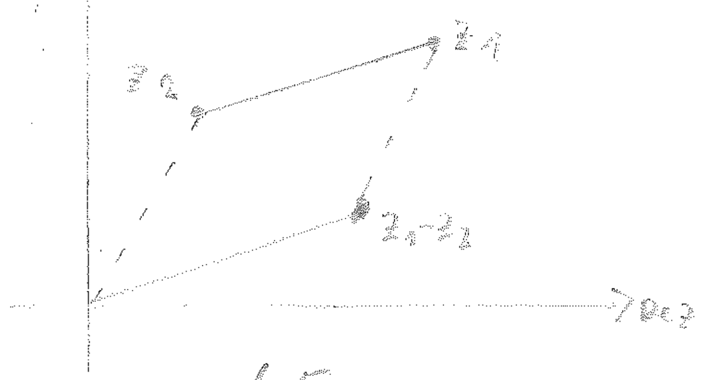
(Es läßt sich leicht nachrechnen, daß stets $\overline{z_1+z_2} = \bar{z}_1 + \bar{z}_2$ und $\overline{z_1 \cdot z_2} = \bar{z}_1 \cdot \bar{z}_2$ gilt. Hieraus folgt sofort $N(z_1 \cdot z_2) = N(z_1) \cdot N(z_2)$ (Multiplikativität der Norm).)

Bem 2 Die Elemente von $\mathbb{Z}[i]$ lassen sich als Gitter in der Gaußschen Zahlenebene vorstellen.

Dann ist $N(z)$ das Quadrat des Abstandes von z zum Nullpunkt (Pythagoras).

Allgemeiner ist $N(z_1 - z_2)$ das Quadrat des Abstandes von z_1 und z_2 in der Gaußschen Zahlenebene.





<u>Def 1</u> Sei $\varepsilon \in \mathbb{Z}[i]$.
Dann heißt ε Einheit von $\mathbb{Z}[i]$, wenn ein $\varepsilon' \in \mathbb{Z}[i]$ existiert mit

$\varepsilon \cdot \varepsilon' = 1$

<u>Bsp 1</u> $1, -1, i$ (beachte $i(-i) = 1$), $-i$ sind Einheiten von $\mathbb{Z}[i]$

<u>Bem 3</u> Sei $\varepsilon \in \mathbb{Z}[i]$. Dann gilt:

ε ist Einheit in $\mathbb{Z}[i]$ $\iff$ $N(\varepsilon) = 1$.
Die Einheiten von $\mathbb{Z}[i]$ sind also genau $1, -1, i, -i$.

Beweis:
$\Rightarrow$: Sei ε Einheit in $\mathbb{Z}[i]$, Dann existiert ein $\varepsilon' \in \mathbb{Z}[i]$ mit $\varepsilon \cdot \varepsilon' = 1$.

Nach Bem 1 folgt $1 = N(1) = N(\varepsilon \cdot \varepsilon') = N(\varepsilon) \cdot N(\varepsilon')$.

Die Norm eines Elementes aus $\mathbb{Z}[i]$ ist offenbar stets eine nicht negative ganze Zahl. Also folgt $N(\varepsilon) = 1$.

$\Leftarrow$ Sei $N(\varepsilon) = \varepsilon \cdot \bar{\varepsilon} = 1$. Offenbar ist dann ε Einheit in $\mathbb{Z}[i]$

<u>Satz 1</u>
Der Gaußsche Zahlring $\mathbb{Z}[i]$ besitzt eine Division mit Rest.
Genauer gilt:
Seien $\alpha, \beta \in \mathbb{Z}[i]$, $\alpha \neq 0$. Dann existieren $\gamma, \rho \in \mathbb{Z}[i]$ mit

$$\beta = \gamma \cdot \alpha + \rho \quad , \; 0 \leq N(\rho) < N(\alpha).$$

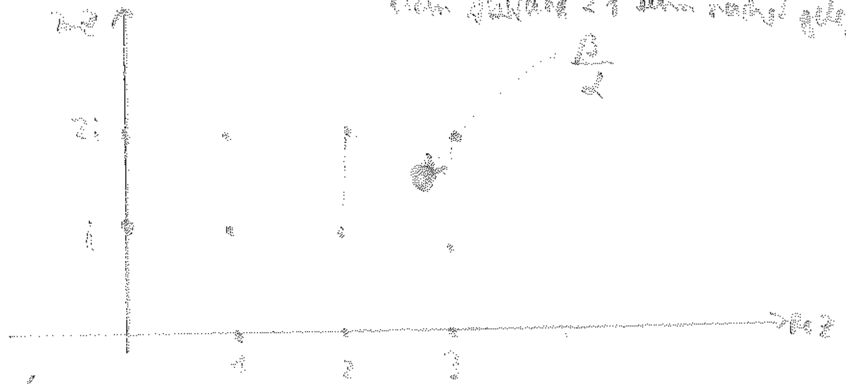
(Also ist $\mathbb{Z}[i]$ ein Euklidischer Ring)
Wegen der Multiplikativität der Norm ist die letzte Bedingung gleichwertig mit

$$\frac{\beta}{\alpha} = \gamma + \frac{\rho}{\alpha} \quad , \; 0 \leq N\left(\frac{\rho}{\alpha}\right) < 1.$$

Dies besagt nach Bem 2, daß sich die komplexe Zahl $\frac{\beta}{\alpha}$ approximieren läßt durch eine Zahl aus $\mathbb{Z}[i]$, so daß der Fehler $\frac{\rho}{\alpha}$ eine Norm < 1 besitzt.

Beweis

Zu $\frac{\beta}{\alpha} \in \mathbb{C}$ ist ein $\gamma \in \mathbb{Z}[i]$ zu suchen mit $N(\frac{\beta}{\alpha} - \gamma) < 1$. $N(\frac{\beta}{\alpha} - \gamma) < 1$ ist gleichbedeutend damit, daß γ von $\frac{\beta}{\alpha}$ in der Gaußschen Zahlenebene einen Abstand < 1 besitzt. Offenbar gibt es aber zu $\frac{\beta}{\alpha}$ in der Gaußschen Zahlenebene einen zu $\mathbb{Z}[i]$ gehörigen Gitterpunkt, der zu $\frac{\beta}{\alpha}$ einen Abstand < 1 besitzt (Im Inneren eines Quadrats mit Seitenlänge 1 hat jeder Punkt einen Abstand < 1 zum nächstgelegenen Eckpunkt).



(Offenbar ist γ nicht eindeutig)

Bsp.:

Dividiere $(1+25i)$ durch $(3+4i)$ in $\mathbb{Z}[i]$ mit Rest.

Es gilt $\frac{1+25i}{3+4i} = \frac{(1+25i)(3-4i)}{(3+4i)(3-4i)} = \frac{103+71i}{25}$.

Wähle $\gamma = 4+3i$.

Dann gilt

$$\frac{1+25i}{3+4i} = \gamma + \frac{3}{25} - \frac{4}{25}i \text{, also } 1+25i = \gamma(3+4i) + 1$$

(Analog läßt sich auch beweisen, daß $\mathbb{Z}[\sqrt{-2}] := \{a + \sqrt{2}\,bi \mid a, b \in \mathbb{Z}\}$ ein euklidischer Ring ist)

27. und 28. Vortrag:

Die Konstruktion regelmäßiger n-Ecke mit Zirkel und Lineal

1. Teil (Vortrag 26)

Untersucht werden soll, welche regelmäßigen n-Ecke mit Zirkel und Lineal konstruiert werden können.

Zunächst einige Vorbereitungen.

Bekanntlich gilt

Satz 1

Sei $1 \in \mathbb{R}$ gegeben, also die Einheitsstrecke und sei $\alpha \in \mathbb{R}$.

Dann ist α mit Zirkel und Lineal konstruierbar gdw gilt:

Es existiert eine reelle Körperkette

(1) $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{\beta_1}) \subsetneq \mathbb{Q}(\sqrt{\beta_1}, \sqrt{\beta_2}) \subsetneq \cdots \subsetneq \mathbb{Q}(\sqrt{\beta_1}, \ldots, \sqrt{\beta_n})$ mit

$\alpha \in \mathbb{Q}(\sqrt{\beta_1}, \ldots, \sqrt{\beta_n})$ und $\beta_i \in \mathbb{Q}(\sqrt{\beta_1}, \ldots, \sqrt{\beta_{i-1}})$ f.a. i.

Bem 1:

In Satz 1 (1) gilt $[\mathbb{Q}(\sqrt{\beta_1}, \ldots, \sqrt{\beta_i}) : \mathbb{Q}(\sqrt{\beta_1}, \ldots, \sqrt{\beta_{i-1}})] = 2$, da $\sqrt{\beta_i}$ Nullstelle von $x^2 - \beta_i \in \mathbb{Q}(\sqrt{\beta_1}, \ldots, \sqrt{\beta_{i-1}})$ ist (s. Satz 4.10, Seite 85 im Skript: Einf. in die Algebra und Zahlentheorie)

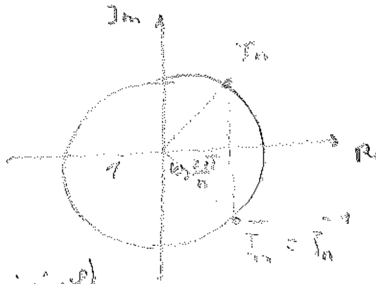
Nach der Körpergradformel (s. Satz 4.1, Skript: Einf. in die Algebra und Zahlentheorie) gilt

$$[\mathbb{Q}(\sqrt{\beta_1}, \ldots, \sqrt{\beta_n}) : \mathbb{Q}] = 2^n$$

und wegen $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{\beta_1}, \ldots, \sqrt{\beta_n})$ folgt wieder aufgrund der Körpergradformel:

Ist α mit Zirkel und Lineal konstruierbar, so ist $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ Potenz von 2.

Bem 2



Für $n \in \mathbb{N}$ sei $\zeta_n := \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.

Dann ist ζ_n n-te Einheitswurzel, d.h. es gilt $\zeta_n^n = 1$. Dies ergibt sich aus der bekannten Formel von Moivre: $(\cos\varphi + i\sin\varphi)^n = \cos n\varphi + i\sin n\varphi$.

Also ist $\zeta_n^{-i} = \zeta_n^{n-i}$.

Ferner gilt $\overline{\zeta_n^i} = \zeta_n^{-i}$, da $\overline{\zeta_n^i} \cdot \zeta_n^i = 1 = \zeta_n^{-i} \cdot \zeta_n^i$

Also ist $\zeta_n^i + \zeta_n^{-i} = 2\,\mathrm{Re}\,\zeta_n^i$, speziell also $\zeta_n + \zeta_n^{-1} = 2\cos\frac{2\pi}{n}$.

Es folgt:

Das regelmäßige n-Eck läßt sich konstruieren mit Zirkel und Lineal gdw sich $\zeta_n + \zeta_n^{-1} = 2\cos\frac{2\pi}{n}$ mit Zirkel und Lineal konstruieren läßt.

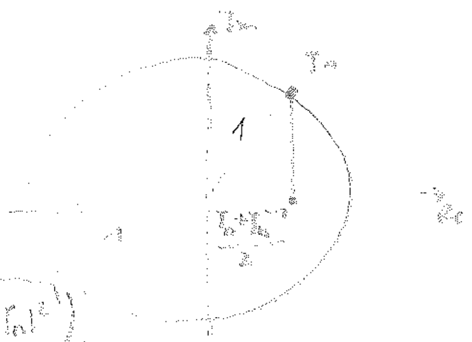
<u>Bem 3</u> Sei $n \in \mathbb{N}, n > 2$.

(i) Dann gilt $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$

(ii) Es gilt $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\zeta_n) \cap \mathbb{R}$

<u>Beweis (i)</u>

Es gilt $\zeta_n = \underbrace{\mathrm{Re}\,\zeta_n}_{= \frac{\zeta_n + \zeta_n^{-1}}{2}} + i\sqrt{1 - (\mathrm{Re}\,\zeta_n)^2}$,



also $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n + \zeta_n^{-1}, \zeta_n) = \mathbb{Q}(\zeta_n + \zeta_n^{-1}, i\sqrt{1 - (\mathrm{Re}\,\zeta_n)^2})$.

Da $i\sqrt{1-(\mathrm{Re}\,\zeta_n)^2}$ Nullstelle von $X^2 + 1 - (\mathrm{Re}\,\zeta_n)^2 \in \mathbb{Q}(\zeta_n + \zeta_n^{-1})[X]$ ist,

folgt $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] \leq 2$.

Da $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ nur reelle Zahlen enthält, nicht aber $\mathbb{Q}(\zeta_n)$, ist $\mathbb{Q}(\zeta_n) \supsetneq \mathbb{Q}(\zeta_n + \zeta_n^{-1})$

Insgesamt folgt die Behauptung.

(ii) Offenbar enthält $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ nur reelle Zahlen, also ist $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subseteq \mathbb{Q}(\zeta_n) \cap \mathbb{R} \subsetneq \mathbb{Q}(\zeta_n)$. Nach der Körpergradformel folgt die Beh.
Offenbar enthält $\mathbb{Q}(\zeta_n)$ nicht nur reelle Zahlen, also ist $\mathbb{Q}(\zeta_n) \cap \mathbb{R} \neq \mathbb{Q}(\zeta_n)$.

<u>Bem 4</u>

(i) Sei p eine Primzahl. Dann ist $\mathrm{Irr}(\zeta_p, \mathbb{Q}) = X^{p-1} + X^{p-2} + \dots + X + 1$. (zur Def. v. $\mathrm{Irr}(\zeta_p, \mathbb{Q})$ s. Bem 4.6, Seite 84 im Skript: Einf. in die Algebra und Zahlentheorie)

(ii) Für $n \in \mathbb{N}$ läßt sich $\mathrm{Irr}(\zeta_n, \mathbb{Q})$ nicht explizit angeben. Es gilt aber

$$\mathrm{grad}\, \mathrm{Irr}(\zeta_n, \mathbb{Q}) = \underbrace{p_1^{a_1 - 1} \cdots p_r^{a_r - 1} (p_1 - 1) \cdots (p_r - 1)}_{= \varphi(n)}, \text{ wobei}$$

$n = p_1^{a_1} \cdots p_r^{a_r}$ (p_i paarweise verschiedene Primzahlen; alle $a_i > 0$). (ohne Beweis)

Beweis von (i)

Es gilt $X^p - 1 = (X - 1)(X^{p-1} + X^{p-2} + \dots + X + 1)$

Da ζ_p Nullstelle von $X^p - 1$, aber nicht Nullstelle von $X - 1$ ist, folgt:

ζ_p ist Nullstelle von $X^{p-1} + X^{p-2} + \dots + X + 1$

Ferner ist $X^{p-1} + X^{p-2} + \dots + X + 1 \in \mathbb{Q}[X]$ irreduzibel (s. Bsp 5.7; Seite 78 im Skript Einführung in die Algebra und Zahlentheorie).

Damit folgt die Behauptung.

<u>Bem 5</u> Bei der Konstruktion regelmäßiger n-Ecke spielen eine besondere Rolle die sog. Fermatschen Primzahlen.

Eine Primzahl p der Form $p = 2^m + 1$ ($m \in \mathbb{N}$) heißt Fermatsche Primzahl.

Zum Beispiel sind $3\ (= 2^{2^0} + 1)$, $5\ (= 2^{2^1} + 1)$, $17 (= 2^{2^2} + 1)$, $257\ (= 2^{2^3})$, $65537\ (= 2^{2^4})$ Fermatsche Primzahlen.

$2^{2^5} + 1$ ist keine (Fermatsche) Primzahl.

Ist $p = 2^m + 1$ Fermatsche Primzahl ($m \in \mathbb{N}$), so ist m Potenz von 2, denn es gilt für $m = r \cdot s$, $r > 1$ ungerade die Gleichung $2^m + 1 = (2^s + 1)\underbrace{(2^{s(r-1)} - 2^{s(r-2)} + \dots - 2^s + 1)}_{r \text{ Summanden}}$.

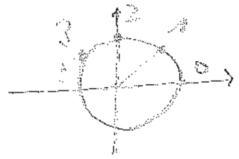
2 Teil: Vorlag 22

Nach diesen Vorbereitungen untersuchen wir nun, welche n-Ecke mit Zirkel und Lineal konstruierbar sind.

Bem 6

Ist das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar und $m|n$, so ist auch das regelmäßige m-Eck konstruierbar mit Zirkel und Lineal.

Bew: Sei $m \cdot m' = n$.
Numeriere die n-Ecken entsprechend der Zeichnung rechts.
Verbinde die Ecke 0 mit der Ecke m',
die Ecke m' " $2m'$
⋮



Bem 7: Seien $k, \ell \in \mathbb{N}$ und $ggT(k,\ell)=1$.
Ist das regelmäßige k-Eck und das regelmäßige ℓ-Eck mit Zirkel und Lineal konstruierbar, so auch das regelmäßige $k \cdot \ell$-Eck.

Bew: Wegen $ggT(k,\ell)=1$ ex. nach dem Euklidischen Algorithmus (s. Satz 3.4.5 auf Seite 69 im Skript: Einf. in die Algebra und Zahlentheorie) $\lambda, \mu \in \mathbb{Z}$ mit $\mu \ell + \lambda k = 1$. Dann gilt

$$\frac{2\pi\mu}{k} + \frac{2\pi\lambda}{\ell} = \frac{2\pi}{k \cdot \ell}.$$

Bei geeigneter Addition bzw. Subtraktion der Winkel $\frac{2\pi}{\ell}$ bzw. $\frac{2\pi}{k}$ erhält man den Winkel $\frac{2\pi}{k \cdot \ell}$.

Bem 8: Sei $\ell \in \mathbb{N}$.
Dann ist das regelmäßige 2^ℓ-Eck mit Zirkel und Lineal konstruierbar (durch wiederholte Halbierung des Winkels π) (wie halbiert man einen Winkel mit Zirkel und Lineal?)

Bem 9: Sei p Primzahl, $p \neq 2$. Ist das p-Eck mit Zirkel und Lineal konstruierbar, so ist p Fermatsche Primzahl (d.h. p hat die Form 2^m+1).

Beweis: Ist das p-Eck konstruierbar, so folgt nach Bem 1 und Bem 2:

$$[\mathbb{Q}(\zeta_p + \zeta_p^{-1}) : \mathbb{Q}] \text{ ist Potenz von } 2.$$

Wegen Bem 3 und der Körpergradformel ist dann

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] \text{ Potenz von } 2.$$

Bekanntlich ist $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \text{grad Irr}(\zeta_p, \mathbb{Q})$ (s. Satz 4.10, Seite 85 im Skript: Einf. in die Algebra und Zahlentheorie]

Nach Bem 4(c) folgt $[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p-1$.

Damit folgt die Behauptung.

Bem 10: Sei p Fermatsche Primzahl.
Dann ist das regelmäßige p-Eck mit Zirkel und Lineal konstruierbar.
(ohne Bew.; zum Beweis wird die Galoistheorie benötigt).

Satz (Gauß)

Sei $1 \in \mathbb{R}$ gegeben (also die Einheitsstrecke) und $n \in \mathbb{N}$.
Dann ist das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar gdw n die Form $n = 2^m p_1 \cdots p_r$ besitzt, wobei p_i paarweise verschiedene Fermatsche Primzahlen sind.

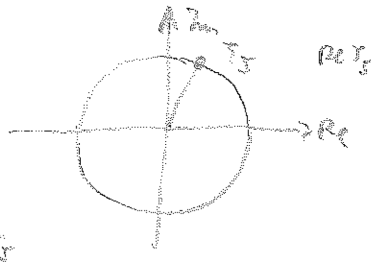
Bew

(a) Besitzt n die angegebene Form, so ist das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar nach den Bemerkungen 7, 8, 9.

(b) Sei das regelmäßige n-Eck konstruierbar und $n = p_1^{a_1} \cdots p_r^{a_r}$ die Primfaktorzerlegung von n.
Nach Bem 6 ist dann auch das p_i-Eck konstruierbar und nach Bem. 9 ist dann p_i Fermatsche Primzahl oder $p_i = 2$.
Sei $a_i > 1$ und $p_i \neq 2$. Dann ist auch das p_i^2-Eck konstruierbar und nach Bem 1 und Bem 2 ist dann $[\mathbb{Q}(\zeta_{p^2} + \zeta_{p^2}^{-1}) : \mathbb{Q}]$ Potenz von 2. Nach Bem 3 ist dann auch $[\mathbb{Q}(\zeta_{p^2}) : \mathbb{Q}]$ Potenz von 2. Wegen $\operatorname{grad} \operatorname{Irr}(\zeta_{p^2}, \mathbb{Q}) = [\mathbb{Q}(\zeta_{p^2}) : \mathbb{Q}]$ und Bem 4 (ii) ist dies ein Widerspruch.

Bem 11 (Konstruktion des regelmäßigen 5-Ecks)

Es gilt $(X - (\zeta_5 + \zeta_5^{-1}))(X - \zeta_5^2 + \zeta_5^{-2}) = X^2 + X - 1$ (*)
Zum Beweis multipliziere man das Produkt links aus, beachte Bem 2 und $\zeta_5^5 = 1$ sowie
$\zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5 + 1 = 0$ (nach Bem 4 (ii))



Re ζ_5 ist positiv.

$X^2 + X - 1$ hat die Nullstellen $-\frac{1}{2} \pm \frac{\sqrt{5}}{2}$.
Eine der Nullstellen ist $\zeta_5 + \zeta_5^{-1}$ wegen (*).
Da $\zeta_5 + \zeta_5^{-1}$ positiv ist, folgt $\zeta_5 + \zeta_5^{-1} = -\frac{1}{2} + \frac{\sqrt{5}}{2}$.
Nun ist die Konstruktion klar.

Frage: Wie läßt sich das regelmäßige 15-Eck konstruieren?

29. und 30. Vortrag: Nichtabelsche Gruppen der Ordnung $2p$

Sei $p \neq 2$ eine Primzahl. Das Ziel des Vortrags besteht darin, alle Gruppen der Ordnung p und $2p$ zu bestimmen, die nicht kommutativ sind.

Bem 1: Eine Gruppe $(G,\cdot)$ mit neutralem Element e ist abelsch, wenn für alle $g \in G$ gilt $g \cdot g = e$
Bew: Nach Vor. gilt $(ab)(ab) = e$, also $ab = b^{-1}a^{-1}$ und $a \cdot a = e$, $b \cdot b = e$, also $a = a^{-1}$, $b = b^{-1}$ □

~~Aufgabe A6~~

Es sei $(G,\cdot)$ eine nicht kommutative Gruppe der Ordnung $2p$, p Primzahl, $p \neq 2$.

Beh 1: G enthält ein Element g der Ordnung p

Bew: Die Ordnung von g ist die kleinste natürliche Zahl n mit $g^n = e$
Die Ordnung von g ist Teiler von $|G|$ (s. Vorlesung) [Lagrange]
Nicht jedes Gruppenelement $\neq e$ kann die Ordnung 2 besitzen (nach ~~Aufgabe 5~~ Bem 1)
Es existiert kein $g \in G$ der Ordnung $2p$, da g sonst G erzeugen würde.
Dies ist nicht möglich, da G nicht kommutativ ist.
Also enthält G ein Element der Ordnung p

Beh 2: Sei $U := \{e, g, \dots, g^{p-1}\}$ die von g erzeugte Untergruppe, $a \notin U$.
Dann gilt $a^p \notin U$

Bew: Offenbar ist $[G:U] = 2$, dann ist U nach Vorlesung Normalteiler in G.
Die Faktorgruppe G/U besitzt 2 Elemente, nämlich U und $a \cdot U$.
Es gilt $(aU)^2 = a^2 U = U$ nach den Rechenregeln in der Faktorgruppe.
Also folgt $a^p U = (aU)^p = aU$; insbesondere $a^p \notin U$.

Beh 3: a hat die Ordnung 2

Bew: Die Ordnung von a ist Teiler von $|G|$, also gleich $1, 2, p$ oder $2p$.
Die Ordnung von a ist $\neq 1$ (da $a \neq e$), $\neq 2p$ (siehe Bew. von Beh 1), $\neq p$ (wegen Beh 2).

Beh 4: G ist isomorph zur Diedergruppe D_p.

Bew: Nach Vorlesung ist die Diedergruppe D_p charakterisiert durch folgende Eigenschaften:
(i) D_p enthält ein Element π_1 der Ordnung 2 und ein Element π_2 der Ordnung p.
(ii) $D_p = \{ id, \pi_2, \dots, \pi_2^{p-1}, \pi_1 \circ id, \pi_1 \circ \pi_2, \dots, \pi_1 \circ \pi_2^{p-1} \}$
(iii) $\pi_1 \circ \pi_2 = \pi_2^{-1} \circ \pi_1$

G erfüllt (i) und (ii) nach Beh 1 und Beh 3.
Wegen $ag \notin U$ hat ag nach Beh 3 die Ordnung 2.
Also gilt in G $(ag)(ag) = e$ und damit $ga = a^{-1}g^{-1}$.
Da $a^2 = e$ ist, folgt $ga = ag^{-1}$.
Damit ist Beh. 4 bewiesen.

Satz: Sei p Primzahl und G eine Gruppe der Ordnung p. Sei $g \in G$, $g \neq e$.
Da die Ordnung von g Teiler von $|G|$ ist, folgt $G = \{e, g, \dots, g^{p-1}\}$; speziell ist G auch kommutativ.

I. Wir wollen zeigen, daß jede Gruppe der Ordnung p^2 (p Primzahl) abelsch ist.

Bem 1 Sei $(G,\cdot)$ eine endliche Gruppe.
Auf G wird eine Relation $\sim$ def. durch
$g_1 \sim g_2 :\Leftrightarrow$ Ex. $x \in G$ mit $g_1 = x g_2 x^{-1}$ (g_1 und g_2 heißen dann konjugiert zueinander).
(i) Man zeige: $\sim$ def. e. Äquivalenzrelation auf G
Es sei $[g]$ die von g erzeugte Äquivalenzklasse.
Für $g \in G$ heißt $N_g := \{x \in G \mid x g x^{-1} = g\}$ Normalisator von g.
(ii) Man zeige: N_g ist eine Untergruppe von G.
(iii) Ferner gilt: $\#[g] = [G : N_g]$ (Index von N_g in G). Speziell gilt $\#[e] = 1$, $\#[g] \mid |G|$.
Bew: $x g x^{-1} = y g y^{-1} \Leftrightarrow y^{-1} x g \underbrace{x^{-1} y}_{=(y^{-1}x)^{-1}} = g \Leftrightarrow y^{-1} x \in N_g \Leftrightarrow y N_g = x N_g$. □

Bem 2 Es sei $(G,\cdot)$ eine Gruppe, deren Ordnung Potenz einer Primzahl p ist. Dann folgt:
(i) Neben dem neutralen Element $e \in G$ ex. mindestens ein weiteres Gruppenelement g mit $\#[g] = 1$.
(ii) Das Zentrum $Z := \{x \in G \mid gx = xg$ f.a. $g \in G\}$ ist eine Untergruppe von G.
(iii) $\{e\} \subsetneqq Z$.

Beweis
(i) Die Äquivalenzklassen bzgl. $\sim$ bilden eine Partition von G.
Die Anzahl der Elemente von G ist Vielfaches von p.
Die Anzahl der Elemente einer Äquivalenzklasse ist 1 oder Vielfaches von p (nach Bem 1(iii))
Ferner ist $[e] = 1$.
Damit folgt die Beh.
(ii) klar
(iii) $\#[g] = 1 \Leftrightarrow x g x^{-1} = g$ f.a. $x \in G \Leftrightarrow xg = gx$ f.a. $x \in G \Leftrightarrow g \in Z$.

Bem 3 Es sei $(G,\cdot)$ eine Gruppe mit dem Zentrum Z und $g \in G$, $g \notin Z$. Dann gilt für den Normalisator N_g von G: $\quad Z \subsetneqq N_g \subsetneqq G$.

Beweis $Z \subsetneqq N_g$: $\quad Z \subseteq N_g$ ist klar nach Def. von Z und N_g
$g \in N_g$ ist klar nach Def. von N_g
$g \notin Z$ gilt nach Voraussetzung
$N_g \subsetneqq G$: $\quad N_g = G \Leftrightarrow x g x^{-1} = g$ f.a. $x \in G \Leftrightarrow xg = gx$ f.a. $x \in G \Leftrightarrow g \in Z$ ↯

Bem 4 Jede Gruppe G der Ordnung p^2 (p Primzahl) ist abelsch.
Bew Annahme: $(G,\cdot)$ ist e. Gruppe der Ordnung p^2, die nicht abelsch ist. Sei Z das Zentrum von G.
Dann gilt $Z \subsetneqq G$.
Also ex. ein $g \in G$ mit $g \notin Z$. Es sei N_g der Normalisator von g.
Es folgt
$$\{e\} \underset{\text{Bem 2(iii)}}{\subsetneqq} Z \underset{\text{Bem 3}}{\subsetneqq} N_g \quad (*)$$
Als Untergruppen von G besitzen Z und N_g eine Ordnung, die Teiler von $|G| (= p^2)$ ist.
Aus $(*)$ folgt $|Z| \geq p$, $|N_g| \geq p^2$.
Ferner gilt $|G| = p^2$ und nach Bem 3 $N_g \subsetneqq G$.
Dies ist ein Widerspruch.

Vortrag 33 und 34:

Endliche Körper

Bem 1 (Die Charakteristik eines endlichen Körpers)
Sei $(K, +, \cdot)$ ein endlicher Körper, also ein Körper mit endlich vielen Elementen.
Ist p Primzahl, so ist zum Beispiel der Restklassenring $\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z}$

ein endlicher Körper.

Sei $1 \in K$ das neutrale Element bzgl. $\cdot$ von K.

Ferner sei $n \in \mathbb{N}$ minimal mit $\underbrace{1 + \dots + 1}_{n \text{ Summanden}} = 0$.

Also ist n die Ordnung von $1 \in K$ in der Gruppe $(K, +)$.

Zum Beispiel gilt dann $-1 = \underbrace{1 + \dots + 1}_{n-1 \text{ Summanden}}$,

$-(1+1) = \underbrace{1 + \dots + 1}_{n-2 \text{ Summanden}}$, falls $n > 2$ ist.

Die von 1 erzeugte Untergruppe von $(K, +)$ enthält also alle möglichen endlichen Summen von $1 \in K$

Man nennt n die Charakteristik von K.

Bsp 1 zB gilt $\underbrace{1 + \dots + 1}_{m\text{-mal}} = 0 \iff n | m$.

Bem 2 Die Charakteristik eines endlichen Körpers ist stets Primzahl.

Bew Annahme:
Die Charakteristik n von K ist keine Primzahl.
Dann läßt sich n in $\mathbb{N}$ zerlegen in der Form $n = n_1 \cdot n_2$ mit $1 < n_1, n_2 < n$.
Es folgt $\underbrace{(1 + \dots + 1)}_{n_1 \text{ Summanden}} \cdot \underbrace{(1 + \dots + 1)}_{n_2 \text{ Summanden}} = \underbrace{1 + \dots + 1}_{n \text{ Summanden}}$.
Dies ergibt sich durch Ausmultiplizieren nach dem Distributivgesetz.
Da jeder Körper nullteilerfrei ist, folgt $\underbrace{(1 + \dots + 1)}_{n_1 \text{ Summanden}} = 0$ oder $\underbrace{(1 + \dots + 1)}_{n_2 \text{ Summanden}} = 0$. Dies ist ein Widerspruch zur Definition von n.

Bem 3

Sei $(K,+,\cdot)$ ein Körper der Charakteristik p.

Betrachte die Abbildung

$$\varphi : \mathbb{Z} \to K$$

definiert durch

$$\varphi(0) := 0$$
$$\varphi(z) := \underbrace{1+\dots+1}_{z \text{ Summanden}} \quad \text{für } z>0$$
$$\varphi(z) := -\underbrace{(1+\dots+1)}_{|z| \text{ Summanden}} \quad \text{für } z<0.$$

Es läßt sich leicht nachrechnen, daß φ ein Ring-Homomorphismus ist.

Offenbar gilt nach Bsp 1

$$\operatorname{Ker} \varphi = p \cdot \mathbb{Z}.$$

Nach dem Homomorphie-Satz folgt

$$\mathbb{Z}_p := \mathbb{Z}/p\mathbb{Z} \cong \varphi(\mathbb{Z}).$$

Also ist $\varphi(\mathbb{Z})$ ein Unterkörper von $(K,+,\cdot)$, er heißt Primkörper von K.
Offenbar enthält $\varphi(\mathbb{Z})$ genau alle p verschiedenen endlichen Summen von $1 \in K$.

Bem 4

Sei $(K,+,\cdot)$ ein endlicher Körper der Charakteristik p.

Nach Bem 2 sei oBdA $\mathbb{Z}_p \subseteq K$.

Gelte $[K:\mathbb{Z}_p] = n$.

Sei $\{a_1,\dots,a_n\}$ eine Basis von $K:\mathbb{Z}_p$.

Dann läßt sich jedes Element aus K eindeutig darstellen in der Form

$$\lambda_1 a_1 + \dots + \lambda_n a_n \quad \text{mit } \lambda_1,\dots,\lambda_n \in \mathbb{Z}_p.$$ Es gibt genau p^n solcher LK.

Insbesondere folgt $|K| = p^n$.

Also: Die Ordnung eines endlichen Körpers ist stets Primzahlpotenz.

__Anmerkung__ (Zerfällungskörper): Sei E eine Körpererweiterung des Körpers $(K,+,\cdot)$; $f(x) \in K[x]$,
seien $\alpha_1,\dots,\alpha_n \in E$ mit $E = K(\alpha_1,\dots,\alpha_n)$ und $f(x) = (x-\alpha_1)\cdots(x-\alpha_n)$,
Dann heißt E Zerfällungskörper von $f(x) \in K[x]$.
Also ist E die kleinste Körpererweiterung von K, über der $f(x)$ in Linearfaktoren zerfällt

Jedes $f(x) \in K[X]$ besitzt einen Zerfällungskörper E. E ist bis auf Isomorphie eindeutig bestimmt (ohne Bew.)

Bem 7

(i) Sei p Primzahl und $f(x) \in \mathbb{Z}_p[X]$ irreduzibel vom Grad n.

Zu gegebenem p und n existiert ein solches Polynom stets (ohne Bew.)

Sei E Zerfällungskörper von $f(x) \in \mathbb{Z}_p[X]$ und $\alpha \in E$ Nullstelle von $f(x)$.

Dann ist $[\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = n$ und $\{1, \alpha, \ldots, \alpha^{n-1}\}$ ist eine Basis von $\mathbb{Z}_p(\alpha) : \mathbb{Z}_p$. Es folgt $|\mathbb{Z}_p(\alpha)| = p^n$.

Also: Zu jeder Primzahl p und jeder natürlichen Zahl n existiert ein Körper der Ordnung p^n.

Ferner: Dieser ist ~~ein~~ Zerfällungskörper von $x^{p^n} - x \in \mathbb{Z}_p[x]$, denn jedes Element aus E ist Nullstelle von $x^{p^n} - x$ (beachte: Die multiplikative Gruppe von E hat $p^n - 1$ Elemente, für jedes $\alpha \in E, \alpha \neq 0$ gilt also $\alpha^{p^n - 1} = 1$). Als Zerfällungskörper ist E bis auf Isomorphie eindeutig (ohne Bew., s.o.)

Vortrag 34

(ii) Ein beliebiges Element aus $\mathbb{Z}_p(\alpha)$ läßt sich eindeutig darstellen in der Form $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$ mit $a_0, \ldots, a_{n-1} \in \mathbb{Z}_p$.

Addition in $\mathbb{Z}_p(\alpha)$:

$$(a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}) + (b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}) = (a_0 + b_0) + (a_1 + b_1)\alpha + \ldots + (a_{n-1} + b_{n-1}$$

Multiplikation in $\mathbb{Z}_p(\alpha)$:

Erste Möglichkeit:

Multipliziere $(a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1})(b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1})$ aus und stelle das Ergebnis dar als Linearkombination der Basiselemente $1, \alpha, \ldots, \alpha^{n-1}$ unter Verwendung von $f(\alpha) = 0$.

Zweite Möglichkeit:

Betrachte
$$g(x) := a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$$
$$h(x) := b_0 + b_1 x + \ldots + b_{n-1}x^{n-1}.$$

Division von $g(x) \cdot h(x)$ durch $f(x)$ mit Rest liefert eine Gleichung der Form

$$g(x) \cdot h(x) = q(x) \cdot f(x) + r(x);$$ $r(x) =$ Nullpolynom oder $\operatorname{grad} r(x) < \operatorname{grad} f(x) = n$.

Einsetzen von α liefert wegen $f(\alpha) = 0$ nach dem Einsetzungshomomorphismus

$$g(\alpha) \cdot h(\alpha) = r(\alpha).$$

Dann ist $r(\alpha)$ die gesuchte Linearkombination.

Bsp 2 (Ein Körper der Ordnung 4)

Das Polynom $f(x) := x^2 + x + 1 \in \mathbb{Z}_2[X]$ ist irreduzibel. (Begründung?)

Sei E Zerfällungskörper von $f(x) \in \mathbb{Z}_2[X]$ und $\alpha \in E$ Nullstelle von $f(x)$.

Dann gilt $[\mathbb{Z}_2(\alpha) : \mathbb{Z}_2] = 2$ und $\mathbb{Z}_2(\alpha) = \{a + b\alpha \mid a, b \in \mathbb{Z}_2\}$.

$\mathbb{Z}_2(\alpha)$ besitzt 4 Elemente.

Es gilt $\alpha^2 = 1 + \alpha$, $\alpha^3 = \alpha(1+\alpha) = 1$; also

$\mathbb{Z}_2(\alpha) = \{0, 1, \alpha, \alpha^2\}$ (Begründung?)

Bsp 3 (Ein Körper der Ordnung 8)

Das Polynom $g(x) := x^3 + x + 1 \in \mathbb{Z}_2[X]$ ist irreduzibel (Begründung?)

Sei E Zerfällungskörper von $f(x) \in \mathbb{Z}_2[X]$ und $\alpha \in E$ Nullstelle von $g(x)$,

Dann gilt $[\mathbb{Z}_2(\alpha) : \mathbb{Z}_2] = 3$ und $\mathbb{Z}_2(\alpha) = \{a + b\alpha + c\alpha^2 \mid a, b, c \in \mathbb{Z}_2\}$,

$\mathbb{Z}_2(\alpha)$ besitzt 8 Elemente.

Man zeige: $\alpha^3 = \alpha + 1$, $\alpha^4 = \alpha^2 + \alpha$, $\alpha^5 = 1 + \alpha + \alpha^2$,

$\alpha^6 = 1 + \alpha^2$.

Also ist $\mathbb{Z}_2(\alpha) = \{0, 1, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6\}$.

Zum Beispiel gilt

$$\alpha^3 + \alpha^4 = (\alpha + 1) + (\alpha^2 + \alpha) = \alpha^2 + 1 = \alpha^6,$$

$$\alpha^4 + \alpha^5 = (\alpha^2 + \alpha) + (1 + \alpha + \alpha^2) = 1.$$

Bem 8 (ohne Bew)

Sei $(K, +, \cdot)$ ein Körper der Ordnung p^n (p Primzahl).

Dann existiert ein $\beta \in K$ mit

$K = \{0, 1, \beta, \beta^2, \ldots, \beta^{p^n-2}\}$. Dann heißt β Primitivwurzel von K.

Bsp 4 (Körper der Ordnung 9)

Das Polynom $h(x) := x^2+1 \in \mathbb{Z}_3[x]$ ist irreduzibel.

Sei E Zerfällungskörper von $h(x) \in \mathbb{Z}_3[x]$ und $\alpha \in E$ Nullstelle von $h(x)$.

Dann gilt $[\mathbb{Z}_3(\alpha):\mathbb{Z}_3]=2$ und $\mathbb{Z}_3(\alpha)=\{a+b\alpha \mid a,b \in \mathbb{Z}_3\}$.

$\mathbb{Z}_3(\alpha)$ besitzt 9 Elemente.

Man zeige:

$$(1+2\alpha)^2 = \alpha \,,$$
$$\alpha^2 = 2 \,,$$

$\beta := 1+2\alpha$ ist eine Primitivwurzel von $\mathbb{Z}_3(\alpha)$. Dies läßt sich leicht zeigen, wenn man die folgende Aussage aus der Vorlesung verwendet.

Die Ordnung eines Elementes aus der multiplikativen Gruppe $(K\setminus\{0\},\cdot)$ eines Körpers $(K,+,\cdot)$ ist Teiler der Gruppenordnung von $(K\setminus\{0\},\cdot)$

35. und 36. Vortrag:

Galoistheorie

Bem 1 (Galoisgruppe)

Sei $E:K$ eine Körpererweiterung.

Ein bijektiver Körper-Isomorphismus $\varphi: E \to E$ heißt Automorphismus von E.

$Gal(E:K)$ bezeichne die Menge aller Automorphismen σ von E mit $\sigma(k) = k$ f.a. $k \in K$.

Dann ist $(Gal(E:K), \circ)$ eine Gruppe (Galoisgruppe von $E:K$).

Als Grundkörper betrachten wir nun stets den Körper $K = \mathbb{Q}$.

Bem 2

Sei $E:\mathbb{Q}$ eine endliche Körpererweiterung, der Körpergrad $[E:K]$ sei n.

(i) Dann existiert ein $\vartheta \in E$ mit $E = \mathbb{Q}(\vartheta)$,
(Satz vom primitiven Element, ohne Beweis)
Dann ist bekanntlich $\{1, \vartheta, \ldots, \vartheta^{n-1}\}$ eine Basis von $E:\mathbb{Q}$, und jedes Element aus E läßt sich eindeutig darstellen in der Form

$$a_0 + a_1\vartheta + \ldots + a_{n-1}\vartheta^{n-1} \text{ mit } a_0, \ldots, a_{n-1} \in \mathbb{Q}.$$

(ii) Sei $\sigma \in Gal(E:\mathbb{Q})$ und $\alpha \in E$ Nullstelle von $f(x) := a_m x^m + \ldots + a_1 x + a_0 \in \mathbb{Q}[x]$.
Dann ist $\sigma(\alpha)$ ebenfalls Nullstelle von $f(x)$.

<u>Beweis von (ii)</u>

$$a_m \alpha^m + \ldots + a_1 \alpha + a_0 = 0$$
$$\Rightarrow \sigma(a_m\alpha^m + \ldots + a_1\alpha + a_0) = \underbrace{\sigma(a_m)}_{=a_m}\sigma(\alpha)^m + \ldots + \underbrace{\sigma(a_1)}_{=a_1}\sigma(\alpha) + \underbrace{\sigma(a_0)}_{=a_0} = 0.$$

(iii) Sei $\vartheta_i \in E$ Nullstelle von $Irr(\vartheta, \mathbb{Q})[x] \in \mathbb{Q}[x]$.
Dann existiert ein $\sigma_i \in Gal(E:\mathbb{Q})$ mit $\sigma_i(\vartheta) = \vartheta_i$ (ohne Bew.)
Dabei ist σ_i eindeutig bestimmt, denn es gilt

$$b_0 + b_1\vartheta + \ldots + b_{n-1}\vartheta^{n-1} \xmapsto{\sigma_i} b_0 + b_1\vartheta_i + \ldots + b_{n-1}\vartheta_i^{n-1}$$

(iv) Aus (ii) und (iii) folgt:

$$|Gal(E:\mathbb{Q})| = \text{Anzahl der Nullstellen von } Irr(\vartheta, \mathbb{Q})[x] \text{ in } E.$$

speziell gilt: $|Gal(E:\mathbb{Q})| \leq n$.

Insbesondere ist $Gal(E:\mathbb{Q})$ endlich.

(V) Ein irreduzibles Polynom $f(x) \in \mathbb{Q}[x]$ kann in seinem Zerfällungskörper keine mehrfache Nullstelle besitzen; die Anzahl der verschiedenen Nullstellen von $f(x)$ ist also $\operatorname{grad} f(x)$. (ohne Beweis)

(VI) Aus (IV) folgt:

$|Gal(E:\mathbb{Q})| = n \iff \operatorname{Irr}(\vartheta, K)(x)$ besitzt in E n verschiedene Nullstellen

$\iff \operatorname{Irr}(\vartheta, K)(x)$ zerfällt in $E[x]$ in ein Produkt von n verschiedenen Linearfaktoren

$\iff E$ ist Zerfällungskörper von $\operatorname{Irr}(\vartheta, \mathbb{Q})(x) \in \mathbb{Q}[x]$.

__Bem3__ (galoissche Erweiterungen)

Sei $E:\mathbb{Q}$ Körpererweiterung vom Grad n und $E = \mathbb{Q}(\vartheta)$. Dann:

$E:\mathbb{Q}$ galoissch $:\iff |Gal(E:\mathbb{Q})| = n$

$\overset{\text{Bem 2(VI)}}{\iff} E$ ist Zerfällungskörper von $\operatorname{Irr}(\vartheta, \mathbb{Q})(x) \in \mathbb{Q}[x]$

$\iff E$ ist Zerfällungskörper eines Polynoms $f(x) \in \mathbb{Q}[x]$

$\boxed{\begin{array}{l}\Rightarrow \text{trivial} \\ \Leftarrow \text{ohne Bew.}\end{array}}$

__Bsp1.__

$\mathbb{Q}(\sqrt{2}):\mathbb{Q}$ ist galoissche Erweiterung, da $\mathbb{Q}(\sqrt{2})$ Zerfällungskörper von $x^2-2 \in \mathbb{Q}[x]$ ist.

$Gal(\mathbb{Q}(\sqrt{2}):\mathbb{Q}) = \{id, \sigma\}$, wobei $\sigma(\sqrt{2}) = -\sqrt{2}$, also

$$a+b\sqrt{2} \overset{\sigma}{\longmapsto} a-b\sqrt{2}.$$

__Bsp2__

Sei $\sqrt[3]{2}$ die reelle 3-te Wurzel aus 2.

Dann ist $\operatorname{Irr}(\sqrt[3]{2}, \mathbb{Q}) = x^3-2$,

$[\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}] = 3$.

$\mathbb{Q}(\sqrt[3]{2})$ enthält nur reelle Zahlen; $\operatorname{Irr}(\sqrt[3]{2}, \mathbb{Q})$ besitzt neben $\sqrt[3]{2}$ noch zwei komplexe Nullstellen.

Ein $\sigma \in Gal(\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q})$ kann also $\sqrt[3]{2}$ nur auf $\sqrt[3]{2}$ abbilden.

Also: $Gal(\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}) = \{id\}$.

$\mathbb{Q}(\sqrt[3]{2}):\mathbb{Q}$ ist keine galoissche Erweiterung.

Bem 5 (Zerfällungskörper)

Sei $(K,+,\cdot)$ ein Körper und $K[x]$ der Polynomring über K.
Ferner sei $f(x) \in K[x]$.
Sei E eine Körpererweiterung von K mit

$$f(x) = (x-\alpha_1)\cdots(x-\alpha_n) \; ; \; \alpha_1,\dots,\alpha_n \in E \quad \text{und}$$
$$E = K(\alpha_1,\dots,\alpha_n).$$

Dann heißt E Zerfällungskörper von $f(x) \in K[x]$.

E ist also eine minimale Körpererweiterung von K, über der $f(x)$ in Linearfaktoren zerfällt.

Bsp 1

(i) Zerfällungskörper von $x^2+1 \in \mathbb{R}[x]$: $\mathbb{R}(i,-i) = \mathbb{R}(i) = \mathbb{C}$

" $x^2+1 \in \mathbb{Q}[x]$: $\mathbb{Q}(i,-i) = \mathbb{Q}(i)$
$= \{a+bi \mid a,b \in \mathbb{Q}\}$.

" $x^2-2 \in \mathbb{Q}[x]$: $\mathbb{Q}(\sqrt{2})$

" $x^2-2 \in \mathbb{R}[x]$: $\mathbb{R}$ (beachte $\sqrt{2} \in \mathbb{R}$).

(ii) (Hauptsatz der Algebra)

Jedes $f(x) \in \mathbb{C}[x]$ zerfällt in $\mathbb{C}[x]$ in ein Produkt von Linearfaktoren.
Also ist für $f(x) \in \mathbb{C}[x]$ stets $\mathbb{C}$ Zerfällungskörper.

Bem 6 (ohne Beweis)

Sei $(K,+,\cdot)$ ein Körper ; $f(x) \in K[x]$.
Dann existiert stets eine Körpererweiterung E von K, so daß E Zerfällungskörper von $f(x) \in K[x]$ ist.
Ferner ist E bis auf Isomorphie eindeutig bestimmt.

Bsp 3

Wir betrachten die Körpererweiterung $\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}$.

Dann gilt $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})] = 2$, $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}] = 2$,

nach der Körpergradformel also $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}] = 4$.

Irr$(\sqrt{3}, \mathbb{Q}(\sqrt{2})) = x^2-3$, da $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$ wegen $\left\{ \begin{array}{l} \sqrt{3} = a+b\sqrt{2};\ a,b \in \\ \Rightarrow 3 = a^2+2b^2+2ab\cdot \\ \text{Wid., da } \sqrt{2} \notin \mathbb{Q} \end{array} \right.$

$\mathbb{Q}(\sqrt{2},\sqrt{3})$ ist Zerfällungskörper von $(x^2-2)(x^2-3) \in \mathbb{Q}[x]$, also ist

$\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}$ galoissche Erweiterung.

Es folgt: $|\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q})| = 4$.

Ein $\sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q})$ ist durch die Bilder $\sigma(\sqrt{2})$ und $\sigma(\sqrt{3})$ bereits eindeutig bestimmt(*); als mögliche Bilder von $\sqrt{2}$ kommen aber nur $\pm\sqrt{2}$ in Frage, und als mögliche Bilder von $\sqrt{3}$ nur $\pm\sqrt{3}$.

Also gilt $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}) = \{id, \sigma_1, \sigma_2, \sigma_3\}$, wobei

$id(\sqrt{2}) = \sqrt{2}, \quad id(\sqrt{3}) = \sqrt{3}$;

$\sigma_1(\sqrt{2}) = \sqrt{2}, \quad \sigma_1(\sqrt{3}) = -\sqrt{3}$;

$\sigma_2(\sqrt{2}) = -\sqrt{2}, \quad \sigma_2(\sqrt{3}) = \sqrt{3}$;

$\sigma_3(\sqrt{2}) = -\sqrt{2}, \quad \sigma_3(\sqrt{3}) = -\sqrt{3}$. (Dann ist $\sigma_3(\sqrt{2}\cdot\sqrt{3}) = \sqrt{2}\cdot\sqrt{3}$).

Verknüpfungstafel:

$\circ$	id	σ_1	σ_2	σ_3
id	id	σ_1	σ_2	σ_3
σ_1	σ_1	id	σ_3	σ_2
σ_2	σ_2	σ_3	id	σ_1
σ_3	σ_3	σ_2	σ_1	id

Offenbar besitzt $\mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q})$ genau 3 echte Untergruppen, nämlich

$U_1 = \{id, \sigma_1\}$, $U_2 = \{id, \sigma_2\}$, $U_3 = \{id, \sigma_3\}$.

(*) $\{1, \sqrt{2}\}$ ist Basis von $\mathbb{Q}(\sqrt{2}):\mathbb{Q}$

$\{1, \sqrt{3}\}$ " $\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})$

Nach der Körpergradformel folgt: $\{1, \sqrt{2}, \sqrt{3}, \sqrt{2}\cdot\sqrt{3}\}$ ist Basis von $\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}$.

Also: Jedes Elem. aus $\mathbb{Q}(\sqrt{2},\sqrt{3})$ läßt sich (eindeutig) darstellen in der Form

$a_0 + a_1\sqrt{2} + a_2\sqrt{3} + a_3\sqrt{6}$; $a_i \in \mathbb{Q}$.

Bem 4

(i) Sei U eine Untergruppe von $Gal(E:K)$ und

$$F_U := \{\alpha \in E \mid \sigma(\alpha) = \alpha \text{ f.a. } \sigma \in U\}.$$

Dann ist F_U ein Körper mit $K \subseteq F_U \subseteq E$.

F_U heißt Fixpunktkörper von U.

(ii) Für Untergruppen U_1, U_2 von $Gal(E:K)$ gilt offenbar:

$$U_1 \subseteq U_2 \quad \Rightarrow F_{U_2} \subseteq F_{U_1}.$$

Sei $E:\mathbb{Q}$ eine galoissche Körpererweiterung. Das Hauptziel der Galoistheorie besteht darin, eine bijektive Zuordnung zwischen den Zwischenkörpern von $E:\mathbb{Q}$ und den Untergruppen von $Gal(E:\mathbb{Q})$ herzustellen.

Satz 1

Sei $E:\mathbb{Q}$ eine galoissche Körpererweiterung.
Sei M_Z die Menge aller Zwischenkörper K von $E:\mathbb{Q}$, also die Menge aller Körper K mit $\mathbb{Q} \subseteq K \subseteq E$.

Sei M_U die Menge aller Untergruppen von $Gal(E:\mathbb{Q})$.

Sei $\varphi_{U,Z} : M_U \to M_Z$ definiert durch $\varphi_{U,Z}(U) := F_U$ (Fixpunktkörper von U).

Sei $\varphi_{Z,U} : M_Z \to M_U$ definiert durch $\varphi_{Z,U}(K) := Gal(E:K)$.

Dann gilt:

(i) (Hauptsatz der Galoistheorie) (ohne Bew)

$\varphi_{U,Z}$ und $\varphi_{Z,U}$ sind bijektive Abbildungen und zueinander invers.

Schreibweise: $U \longleftrightarrow K$ (Galoiskorrespondenz bzgl $E:\mathbb{Q}$) (Dabei ist $K = F_U$, $U = Gal(E:K)$)

(ii) $U_1 \subseteq U_2 \iff F_{U_2} \subseteq F_{U_1}$. (Klar nach Def.)

(iii) Betrachte das Diagramm

$$\begin{array}{ccc} E & \longleftrightarrow & Gal(E:E) = \{id\} \\ | & & \\ K & \longleftrightarrow & U \\ | & & \\ \mathbb{Q} & \longleftrightarrow & Gal(E:\mathbb{Q}) \end{array}$$

(Galoiskorrespondenz).

Dann: $[K:\mathbb{Q}] = [Gal(E:K) : U]$ und $[E:K] = |U|$. (ohne Bew)

<u>Bsp 3</u> (Fortsetzung)

$$\begin{tikzcd}[column sep=small] & \mathbb{Q}(\sqrt{2},\sqrt{3}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ \mathbb{Q}(\sqrt{2}) \arrow[dr, dash] & \mathbb{Q}(\sqrt{3}) \arrow[d, dash] & \mathbb{Q}(\sqrt{2}\cdot\sqrt{3}) \arrow[dl, dash] \\ & \mathbb{Q} & \end{tikzcd} \quad \overset{\text{Galoiskorrespondenz}}{\longleftrightarrow} \quad \begin{tikzcd}[column sep=small] & \{id\} \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\ U_1 \arrow[dr, dash] & U_2 \arrow[d, dash] & U_3 \arrow[dl, dash] \\ & \mathrm{Gal}(\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}) & \end{tikzcd}$$

Insbesondere besitzt $\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}$ genau 3 echte Zwischenkörper.

<u>Bem 5</u> (Konstruktion mit Zirkel und Lineal)

Gegeben sei die Einheitsstrecke, also $1 \in \mathbb{R}$.

Ferner sei $\alpha \in \mathbb{R}$.

Bekanntlich gilt:

(i) α ist mit Zirkel und Lineal konstruierbar $\Rightarrow [\mathbb{Q}(\alpha):\mathbb{Q}]$ ist Potenz von 2.

(ii) α ist mit Zirkel und Lineal konstruierbar $\Longleftrightarrow$

Existiert eine Körperkette $\mathbb{Q} = K_0 \subseteq K_1 \subseteq \ldots \subseteq K_{m-1} \subseteq K_m$

mit $\alpha \in K_m$; $[K_{i+1}:K_i] = 2$ für $i = 0,\ldots,m-1$.

Die Frage, ob eine solche Körperkette existiert läßt sich mit Hilfe der Galoistheorie klären.

Vortrag 37:

Über die Darstellung der Nullstellen eines Polynoms durch Wurzeln

Mit Hilfe der Galoistheorie läßt sich allgemein die Frage beantworten, wann die Nullstellen eines Polynoms durch „Wurzeln" ausgedrückt werden können. Für quadratische Polynome ist dies möglich nach der bekannten Formel von Vieta ($p-q$-Formel), für kubische nach der Formel von Cardano.
Seit der Mitte des 16. Jahrhunderts kennt man auch eine Formel für Polynome 4. Grades. Nach einer Formel für Polynome vom Grad>4 hat man lange gesucht. 1826 bewies Abel, daß es solche Formeln nicht geben kann.
Zur genauen Beschreibung werden zwei weitere Begriffe benötigt, nämlich den der „Radikalerweiterung" und der „auflösbaren Gruppe".

Definition 1. Reine Radikalerweiterung, Radikalerweiterung
Sei $E:K$ Körpererweiterung.

1. $E:K$ reine Radikalerweiterung:$\Leftrightarrow$ E hat die Form $E=K(b)$, wobei b Nullstelle eines $f(x)=x^n-a\in K[x]$ ist.
   Das heißt: E entsteht aus K durch Adjunktion einer n-ten Wurzel eines Elementes $a\in K$;
   die Elemente aus E haben die Form
   $$k_0+k_1\sqrt[n]{a}+\cdots+k_{n-1}\sqrt[n]{a}^{\,n-1},\ k_i\in K.$$

2. $E : K$ Radikalerweiterung:$\Leftrightarrow$ Es existiert eine endliche Körperkette $K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_n = E$.
   wobei $K_{i+1} : K$ reine Radikalerweiterung ist für alle i.
   Das heißt: Die Elemente aus E lassen sich durch „verschachtelte Wurzelausdrücke" von Elementen aus K darstellen.

Definition ~~4.53~~ 2. Durch Radikale Auflösbar
Seien $(K, +, \cdot)$ Körper, $f \in K[x]$.
f heißt durch Radikale auflösbar, wenn der Zerfällungskörper von f über K in einer Radikalerweiterung von K enthalten ist.
Das heißt: Die Nullstellen von f lassen sich durch „verschachtelte Wurzelausdrücke" von Elementen aus K darstellen.

Definition ~~4.54~~ 3. Auflösbar
Sei $(G, \cdot)$ eine Gruppe.
G heißt auflösbar, wenn Untergruppen $N_0, \ldots, N_l$ von G existieren, so daß gilt:

1. $G = N_0 \supseteq \cdots \supseteq N_l = \{e\}$,
2. N_i ist Normalteiler in $Ni - 1$ und N_{i-1}/N_i ist abelsche Gruppe für $i = 1, \ldots, l$.

Satz ~~4.55~~ 1. Sei $(K, +, \cdot)$ Körper mit Char $K = 0$, $f \in K[x]$ und E Zerfällungskörper von f über K. Dann gilt:
f ist über K durch Radikale auflösbar$\Leftrightarrow$ Gal$(E : K)$ ist auflösbar.

Bemerkung ~~4.56~~ 1. Sei E Zerfällungskörper von $f \in K[x]$,
seien $\alpha_1, \ldots \alpha_n$ die Nullstellen von f in E, also $E = K(\alpha_1, \ldots \alpha_n)$.
Jedes $\sigma \in$ Gal$(E : K)$ permutiert die Nullstellen von f (da σ Homomorphismus), und σ ist durch diese Permutation bereits festgelegt.
Also ist Gal$(E : K)$ isomorph zu einer Untergruppe der symmetrischen Gruppe S_n.

Bemerkung ~~4.57~~ 2. Jede Untergruppe einer auflösbaren Gruppe ist auflösbar.
Für $n \leq 4$ ist S_n auflösbar, also ist jedes Polynom $f \in K[x]$ vom Grad$\leq$ durch Radikale auflösbar, falls Char $K = 0$.
Für $n \geq 5$ ist S_n nicht auflösbar.
Es gibt Polynome von Grad 5 (zum Beispiel $x^5 - 6x^3 + 3$), deren Galoisgruppe isomorph ist zu S_5. Diese sind dann nicht durch Radikale auflösbar.

Beweisansatz für Satz 1 für den Fall, daß der Zerfällungskörper des Polynoms Radikalerweiterung ist u. hinreichend viele Einheitswurzeln enthält:

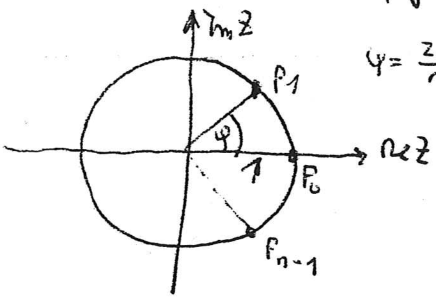
$$\begin{array}{lccccccccccc}
 & \mathbb{Q} =: K_0 & \subseteq & K_1 & \subseteq \cdots \subseteq & K_i & \subseteq & K_{i+1} & \subseteq \cdots \subseteq & K_n = E & \\
\text{Betrachte} & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & & \updownarrow & \text{Galoiskorrespondenz} \\
 & \mathrm{Gal}(E:\mathbb{Q}) & \supseteq & U_1 & \supseteq \cdots \supseteq & U_i & \supseteq & U_{i+1} & \supseteq \cdots \supseteq & \{id\} &
\end{array}$$

Zeige:
U_{i+1} Normalteiler von U_i und U_i/U_{i+1} abelsch
$\Leftrightarrow$ $K_{i+1} : K_i$ ist reine Radikalerweiterung

Die Konstruktion spezieller regelmäßiger n-Ecke mit Zirkel und Lineal

Bem 1 (Vorbereitungen)

Gegeben sei ein regelmäßiges n-Eck.
OBdA nehmen wir an, daß die n Ecken auf einem Kreis vom Radius 1 liegen.
Wir fassen die Ecken auf als Punkte in der Gaußschen Zahlenebene.
Den Punkten sind dann jeweils komplexe Zahlen zugeordnet.



$\varphi = \frac{2\pi}{n}$

$P_0 \longleftrightarrow 1 = \cos 0 + i \sin 0$

$P_1 \longleftrightarrow \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n} =: \zeta_n$

$P_2 \longleftrightarrow \cos 2\cdot\frac{2\pi}{n} + i \sin 2\cdot\frac{2\pi}{n}$

$\vdots$

$P_{n-1} \longleftrightarrow \cos(n-1)\cdot\frac{2\pi}{n} + i \sin\frac{(n-1)\cdot 2\pi}{n}$.

Dann gilt $|\zeta_n| = 1$ und $\zeta_n^j = \cos\left(j\cdot\frac{2\pi}{n}\right) + i\sin\left(j\cdot\frac{2\pi}{n}\right)$. (Begründung?),

Also: $P_0 \leftrightarrow 1$, $P_1 \leftrightarrow \zeta_n$, $P_2 \leftrightarrow \zeta_n^2$, ..., $P_i \leftrightarrow \zeta_n^i$, ..., $P_{n-1} \leftrightarrow \zeta_n^{n-1}$

Weiter gilt offenbar (Begründung?)

$$\zeta_n^n = 1 \qquad (1),$$

$$\zeta_n^i \cdot \zeta_n^{n-i} = 1 \qquad (\text{d.h. } \zeta_n^{n-i} \text{ ist zu } \zeta_n^i \text{ invers}) \qquad (2),$$

$$\zeta_n + \zeta_n^{n-1} = 2\operatorname{Re}\zeta_n = 2\cos\frac{2\pi}{n} \qquad (3).$$

Bem 2 Es gilt $1 + \zeta_n + \zeta_n^2 + \dots + \zeta_n^{n-1} = 0$ für $n > 1$.

Bew: Nach (1) ist ζ_n Nullstelle von $X^n - 1$.
Durch Ausmultiplizieren läßt sich leicht verifizieren, daß

$$X^n - 1 = (X-1)(X^{n-1} + X^{n-2} + \dots + X + 1)$$

gilt. Da ζ_n Nullstelle von $X^n - 1$, aber nicht von $X - 1$ ist, folgt die Behauptung.

Hauptsatz (Gauß) [ohne Bew.]

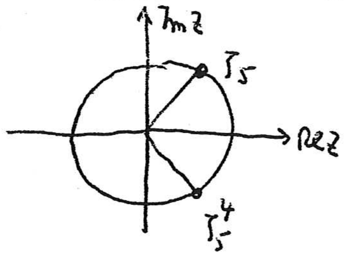
Es sei $1 \in \mathbb{R}$ gegeben (also die Einheitsstrecke) und $n \in \mathbb{N}$.
Dann ist das regelmäßige n-Eck mit Zirkel und Lineal konstruierbar gdw n die Form $n = 2^m \cdot p_1 \cdots p_r$ besitzt, wobei die p_i paarweise verschiedene Fermatsche Primzahlen sind.
Eine Primzahl p heißt dabei Fermatsche Primzahl, wenn $p-1$ Potenz von 2 ist.

Bsp 1 Das regelmäßige 5-Eck und das regelmäßige 17-Eck ist konstruierbar.
Das regelmäßige 7-Eck ist nicht konstruierbar.

Bem 3

Nach (3) gilt offenbar (genaue Begründung?):
Das regelmäßige n-Eck ist konstruierbar gdw $\zeta_n + \zeta_n^{n-1}$ konstruierbar ist.

Bem 4 (Die Konstruktion des regelmäßigen 5-Ecks)



Es ist klar, wie das regelmäßige 5-Eck konstruiert werden kann, wenn $\zeta_5 + \zeta_5^4$ $(= 2\,\mathrm{Re}\,\zeta_5)$ bereits konstruiert ist.

Es gilt $(x - (\zeta_5 + \zeta_5^4))(x - (\zeta_5^2 + \zeta_5^3)) = x^2 + x - 1$.
Zum Beweis multipliziere man das Produkt links aus und beachte (1) und Bemerkung 2.
Also ist $\zeta_5 + \zeta_5^4$ eine Nullstelle von $x^2 + x - 1$.
Die Nullstellen von $x^2 + x - 1$ sind $-\frac{1}{2} \pm \frac{\sqrt{5}}{2}$.
In der Gaußschen Zahlenebene sieht man, daß $\zeta_5 + \zeta_5^4$ eine positive reelle Zahl ist.
Es folgt $\zeta_5 + \zeta_5^4 = -\frac{1}{2} + \frac{\sqrt{5}}{2}$.
Nun ist die Konstruktion des regelmäßigen 5-Ecks klar (beschreibe genau die einzelnen Konstruktionsschritte).

Bem 5

Das regelmäßige 7-Eck ist nicht konstruierbar.

Gleichwertig ist:

$\zeta_7 + \zeta_7^6$ $(= 2\operatorname{Re}\zeta_7)$ ist nicht konstruierbar, wobei

$\zeta_7 := \cos\frac{2\pi}{7} + i\sin\frac{2\pi}{7}$ ist.

Analog zum 5-Eck erhält man (man prüfe dies im Einzelnen nach):

$\zeta_7 + \zeta_7^6$ ist Nullstelle von

$$f(x) := (x-(\zeta_7+\zeta_7^6))(x-(\zeta_7^2+\zeta_7^5))(x-(\zeta_7^3+\zeta_7^4)) = x^3+2x^2-2x+1.$$

$f(x) \in \mathbb{Q}[x]$ ist irreduzibel (das Polynom besitzt in $\mathbb{Q}$ keine Nullstelle (warum?)).

Also folgt $[\mathbb{Q}(\zeta_7+\zeta_7^6):\mathbb{Q}] = 3$. Aber 3 ist keine Potenz von 2.

Damit folgt die Behauptung, denn bekanntlich gilt:

Sei die Einheitsstrecke 1 gegeben.

Dann gilt: Ist $\alpha \in \mathbb{R}$ mit Zirkel und Lineal konstruierbar, so folgt:

$[\mathbb{Q}(\alpha):\mathbb{Q}]$ ist Potenz von 2.

39. Vortrag **Quellencodierung**

Wenn Informationen (digital) übertragen werden sollen, müssen diese zunächst den technischen Gegebenheiten angepasst werden. Hierzu ist eine Codierung (Quellencodierung) erforderlich. Häufig werden dabei Buchstaben codiert zu endlichen Folgen von 0 und 1. Wir beschreiben hier einen allgemeinen Ansatz.

Dazu betrachten wir eine endliche Menge $X = \{x_1, \dots, x_n\}$, die als Quellenalphabet bezeichnet wird. Ein Wort (der Länge m) über X ist eine endliche Folge von Elementen aus X; diese wird i.a. geschrieben in der Form $y_1 \cdots y_m$ mit $y_1, \dots, y_m \in X$. Sei X^* die Menge aller Wörter über X.

Ferner wird eine endliche Menge $A = \{a_1, \dots, a_r\}$ betrachtet, die als Kanalalphabet bezeichnet wird. Häufig ist $A = \{0, 1\}$. Ein Wort (der Länge m) über A ist analog wie bei X eine endliche Folge $a_1 \cdots a_m$ $(m \in \mathbb{N})$ mit $a_1, \dots, a_m \in A$. Sei A^* die Menge aller Wörter über A.

Eine Abbildung $c: X \longrightarrow A^*$ wird Quellencodierer (oder Quellencodierung) genannt. Sprechweise: c codiert jedes Element aus X zu einem Codewort aus A^*.

Sei nun $C := c(X)$ das Bild von X bzgl. der Abbildung c. Dann heißt C Code von X über A (induziert von c). Die Elemente von C heißen Codewörter von C (bzw. von c).

Die Abbildung $c: X \to A^*$ wird nun fortgesetzt zu einer Abbildung $c^*: X^* \to A^*$ durch die Zuordnungsvorschrift

$$c^*(x_1, \dots, x_m) := c(x_1) \dots c(x_m)$$

Wir nennen C (bzw. c) eindeutig decodierbar (bzw. einen sinnvollen Code), wenn $c^*: X^* \to A^*$ eine injektive Abbildung ist. Dann besitzt jedes Element aus C^* bzgl c^* ein eindeutig bestimmtes Urbild.
Dabei ist C^* die Menge aller Wörter über C.

<u>Bsp 1</u> Sei $X := \{x_1, x_2, x_3\}$, $A := \{0,1\}$ und $c: X \to A^*$ definiert durch $x_1 \overset{c}{\longmapsto} 0$, $x_2 \overset{c}{\longmapsto} 1$, $x_3 \overset{c}{\longmapsto} 01$.

Dann ist $C = \{0, 1, 01\}$.

Offenbar ist C nicht eindeutig decodierbar, denn $01 \in A^*$ hat die Urbilder $x_3 \in X^*$ und $x_1 x_2 \in X^*$ (das Element $01 \in A^*$ kann nicht eindeutig decodiert werden).

<u>Bem 1</u>
Haben alle Codewörter dieselbe Länge und ist $c: X \to A^*$ injektiv, so ist c eindeutig decodierbar. (Beweis ?)

<u>Bsp 2</u> Sei $X := \{x_1, x_2, x_3, x_4\}$, $A = \{0,1\}$.

(a) Definiere $c_1: X \to A^*$ durch
$x_1 \mapsto 00$, $x_2 \mapsto 01$, $x_3 \mapsto 10$, $x_4 \mapsto 11$.

Dann ist $C_1 = \{00, 01, 10, 11\}$.

Nach Bem 1 ist C_1 eindeutig decodierbar.

(b) Definiere $c_2: X \to A^*$ durch
$x_1 \mapsto 0$, $x_2 \mapsto 10$, $x_3 \mapsto 110$, $x_4 \mapsto 111$.

Dann ist $C_2 = \{0, 10, 110, 111\}$.

C_2 ist ebenfalls eindeutig decodierbar (Beweis durch Probieren).

Def 1 (Präfixcode, Suffixcode)

Sei $C \subseteq A^*$ ein Code ; seien $v, w \in A^*$.

Dann wird definiert:

v Präfix von w $:\Longleftrightarrow$ Ex. $z \in A^*$ mit $w = vz$.

v Suffix von w $:\Longleftrightarrow$ Ex. $z \in A^*$ mit $w = zv$.

C Präfixcode $:\Longleftrightarrow$ Kein Codewort aus C ist Präfix eines Codewortes aus C.

C Suffixcode $:\Longleftrightarrow$ Kein Codewort aus C ist Suffix eines Codewortes aus C.

Bem 2

Jeder Präfixcode ist eindeutig decodierbar [Hinweis: Decodiere von links]

Jeder Suffixcode ist eindeutig decodierbar [Hinweis: Decodiere von rechts]

Vorteil eines Präfixcodes: Das erste Codewort kann bereits decodiert werden, bevor die nachfolgenden Codewörter bekannt sind.

Bsp 3 Der Code in Bsp 2 (a) ist ein Präfix- und ein Suffixcode.

Der Code in Bsp 2 (b) ist ein Präfixcode, aber kein Suffixcode.

Bsp 4

Sei $C := \{ \overbrace{010}^{c_1}, \overbrace{11010}^{c_2}, \overbrace{01000}^{c_3}, \overbrace{00110}^{c_4} \} \subseteq \{0,1\}^*$ ein Code.

Dann ist C kein Präfixcode und auch kein Suffixcode.

C ist aber eindeutig decodierbar. Dies ergibt sich wie folgt:

Sei $a_1 a_2 \cdots a_n \in C^*$.

Decodiere von rechts.

Offenbar ist $a_n \neq 1$. Wir führen eine vollständige Fallunterscheidung durch:

1. Fall $a_1 a_2 \cdots 00$: c_3 ist das letzte Codewort

2. Fall $a_1 a_2 \cdots 110$: c_4 ist das letzte Codewort

3. Fall $a_1 a_2 \cdots 1010$: c_2 ist das letzte Codewort

4. Fall $a_1 a_2 \cdots 0010$: c_1 ist das letzte Codewort

Def 2 Sei $C \subseteq A^*$ ein Code.

Die Teilmengen $C_0, C_1, C_2, \dots$ von A^* werden definiert durch

$C_0 := C$ und für $n \geq 1$

$C_n := \{ w \in A^* \mid \text{Ex. } v_0 \in C,\ w_1 \in C_{n-1} \text{ mit } v_0 w = w_1 \text{ oder } w_1 w = v_0 \}$.

Sei $C_\infty := \bigcup_{n=1}^{\infty} C_n$.

Bem 3

Offenbar gilt $C_1 = \{ w \in A^* \mid \text{Ex. } v_0, w_1 \in C \text{ mit } v_0 w = w_1 \}$.

Sei $C_1 \cap C \neq \emptyset$, etwa $w \in C$ und $w \in C_1$.

Dann ex. nach Def. von C_1 $w_0, w_1 \in C$ mit $w_0 w = w_1$ und C

(genauer $w_0 w$) ist nicht eindeutig decodierbar.

Bem 4

Nach Def. 2 gilt für $n \geq 1$ offenbar:

$$C_n \subseteq \bigcup_{i=1}^{n-1} C_i \Rightarrow C_m \subseteq \bigcup_{i=1}^{n-1} C_i \text{ für alle } m \geq n \quad \left(\text{also } C_\infty = \bigcup_{i=1}^{n-1} C_i\right).$$

Bew: Aus $w \in C_{n+1}$ folgt $v_0 w = w_1$ oder $w_1 w = v_0$ mit $w_1 \in C_n$, also auch $w_1 \in C_i$ für ein $i < n$.
Damit ist $w \in C_{i+1}$.

Satz 1 (Sardinas – Patterson) (ohne Beweis)

Mit den obigen Bezeichnungen gilt:

C nicht eindeutig decodierbar $\Leftrightarrow C_\infty \cap C \neq \emptyset$.

Bsp 5 Sei $C = \{0, 1, 01\} \subseteq \{0,1\}^*$.

Dann ist $C_1 = \{1\}$, also $1 \in C_\infty \cap C$.

Nach Satz 1 ist C nicht eindeutig decodierbar.

Bsp 6 Sei $C = \{010, 11010, 01000, 00110\} \subseteq \{0,1\}^*$ (s. Bsp 4)

Dann gilt $C_1 = \{00\}$, $C_2 = \{110\}$, $C_3 = \{10\}$, $C_4 = \emptyset$, also $C_\infty = C_1 \cup C_2 \cup C_3$.

Es folgt $C_\infty \cap C = \emptyset$. Nach Satz 1 ist C eindeutig decodierbar.

Bsp 7 Sei $C = \{02, 12, 120, 21\} \subseteq \{0,1,2\}^*$. Dann ist $C_1 = \{0\}$, $C_2 = \{2\}$,
$C_3 = \{1\}$, $C_4 = \{2\}$, also $C_\infty = \{0,1,2\}$, also $C \cap C_\infty = \emptyset$.
C ist also eindeutig decodierbar.

40. Vortrag:

Die Quellencodierung nach Kraft

Wir übernehmen die Bezeichnungen aus dem Vortrag Quellencodierung.

Satz 1 (Mac Millen) (ohne Beweis)

Sei $C = \{w_1, \dots, w_n\} \subseteq \{0,1\}^*$ ein eindeutig decodierbarer Code und l_i die Codewortlänge von w_i für $i = 1, \dots, n$. Dann gilt:

$$\sum_{i=1}^{n} \frac{1}{2^{l_i}} \leq 1.$$

Satz 2 (Kraft)

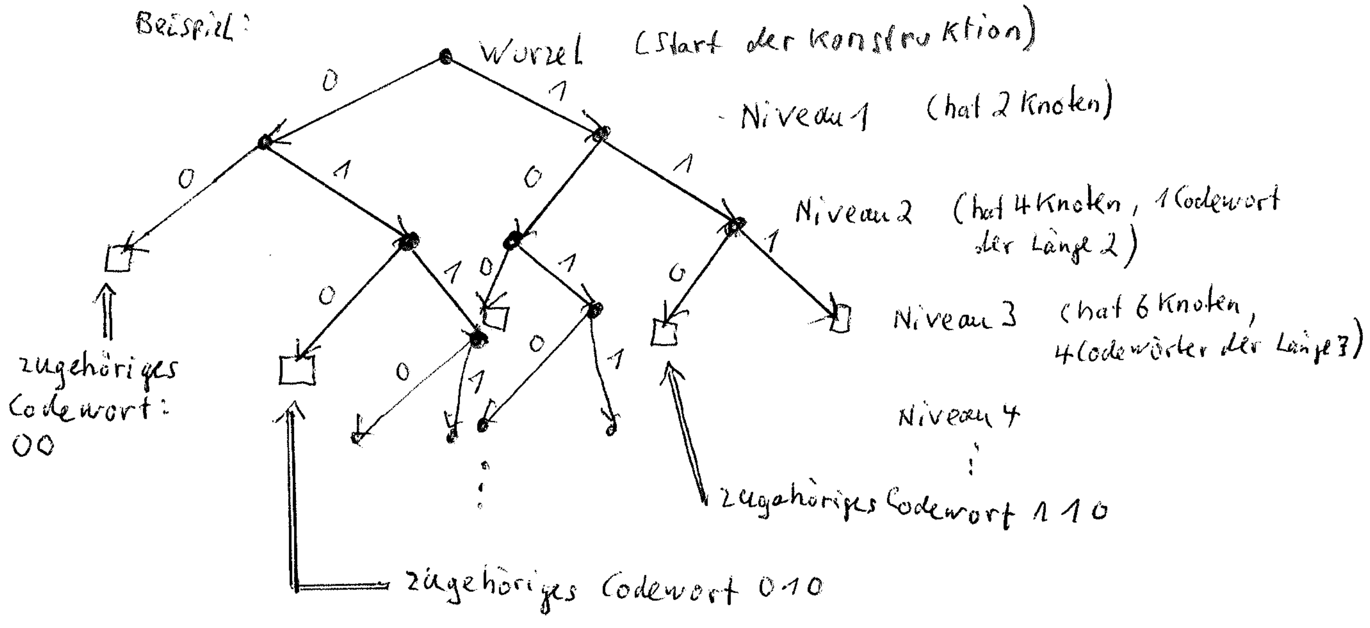
Es seien $l_1, \dots, l_n \in \mathbb{N}$ mit $\sum_{i=1}^{n} \frac{1}{2^{l_i}} \leq 1$.

Dann ex. ein Präfixcode $C = \{w_1, \dots, w_n\} \subseteq \{0,1\}^*$, wobei l_i die Codewortlänge von w_i ist.

Beweis (Konstruktiv)

Wir konstruieren ein Diagramm (Baum) nach folgendem Schema:

Beispiel:



Beschreibung der allgemeinen Konstruktion:

Es sei ein Code C gegeben, $C \subseteq \{0,1\}^*$, die Codewortlängen seien $l_1, \ldots, l_n$.
Sei S_K die Anzahl der Codewörter der Länge K.

Dann werden S_K Knoten auf dem Niveau K mit $\square$ gekennzeichnet.

Bei diesen Knoten wird der Baum nicht auf das nächste Niveau $K+1$ fortgesetzt.

Der Baum wird also fortgesetzt bis zum Niveau $L := \max\{l_1, \ldots, l_n\}$.

Jedem Pfad von der Wurzel zu einem Knoten, der mit $\square$ gekennzeichnet ist, wird ein Codewort zugeordnet (Beispiel, siehe Zeichnung oben).
Die Menge dieser Codewörter sei C. Dann enthält C genau n Codewörter mit den Codewortlängen $l_1, \ldots, l_n$.
Man beachte, daß die Konstruktion nicht eindeutig ist.

Ein mit $\square$ gekennzeichneter Knoten ist stets Endpunkt eines Pfades.

Also ist C ein Präfixcode.

Zu zeigen bleibt:
Die Konstruktion garantiert, daß es auf dem Niveau K jeweils mindestens S_K Knoten gibt, die mit $\square$ gekennzeichnet werden können.

Von den 2^{K+1} möglichen Pfaden von der Wurzel zum Niveau $K+1$ werden einige bereits vor Erreichen des Niveaus $K+1$ abgebrochen.

Ihre Anzahl ist

$$
\begin{array}{llr}
 & S_1 \cdot 2^K & \text{(abgebrochene Pfade der Länge 1)} \\
+ & S_2 \cdot 2^{K-1} & \text{(" 2)} \\
\vdots & & \vdots \\
+ & S_K \cdot 2^1 & \text{(" K),}
\end{array}
$$

Die Anzahl der zur Verfügung stehenden Knoten auf dem Niveau $K+1$ ist also $2^{K+1} - (S_1 2^K + \ldots + S_K 2^1)$.

Es genügt also zu zeigen:

$$s_{k+1} \leq 2^{k+1} - (s_1 2^k + \dots + s_k 2^1).$$

Gleichwertig hierzu ist

$$s_1 2^k + \dots + s_k \cdot 2 + s_{k+1} \leq 2^{k+1}$$

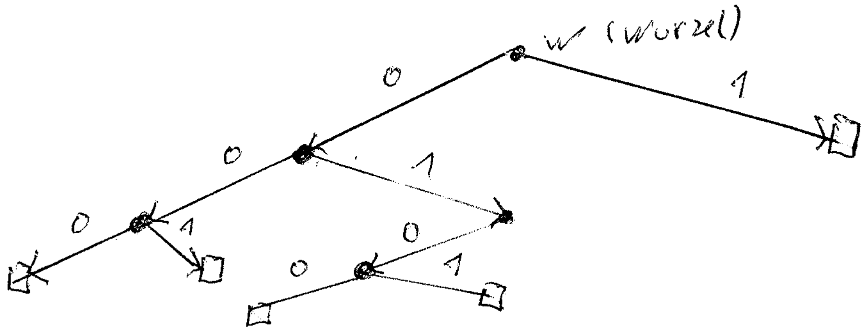
bzw

$$\frac{s_1}{2} + \dots + \frac{s_k}{2^k} + \frac{s_{k+1}}{2^{k+1}} \leq 1.$$

Die Gültigkeit dieser Ungleichung ist wegen der Voraussetzung

$\sum_{i=1}^{n} \frac{1}{2^{l_i}} \leq 1$ gewährleistet. ∎

<u>Bsp 1</u> Konstruiere einen Code $C \subseteq \{0,1\}^*$ mit 5 Elementen und den Codewortlängen $l_1 = 1$, $l_2 = l_3 = 3$, $l_4 = l_5 = 4$.



$$C = \{1, 000, 001, 0100, 0101\}.$$

Man gebe einen sinnvollen Code $C_1 \subseteq \{0,1\}^*$ an mit 5 Elementen, so daß die Summe der Codewortlängen kleiner ist als die entsprechende Summe für C. (Hinweis: Modifiziere den obigen Baum)

Bem 1

Das Verfahren von Kraft läßt sich analog erweitern auf Präfixcodes über einem beliebigen endlichen Alphabet $A = \{a_1, \ldots, a_r\}$. Der Baum ist dabei so zu modifizieren, daß von einem Knoten zum nächst höheren Niveau r Pfade abgehen können.

Genauer gilt:

Es seien $l_1, \ldots, l_n \in \mathbb{N}$ mit $\sum_{i=1}^{n} \frac{1}{r^{l_i}} \leq 1$.

Dann ex. ein Präfixcode $C = \{w_1, \ldots, w_n\} \subseteq A^*$, wobei l_i die Codewortlänge von w_i ist.

Bsp 2 Sei $A = \{0, 1, 2\}$.

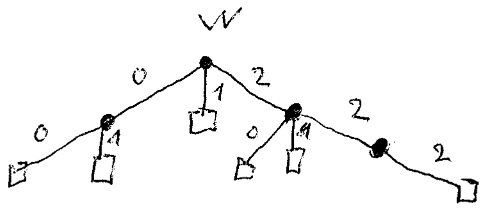
Konstruiere einen Präfixcode über A mit den Codewortlängen

$l_1 = 1, \quad l_2 = \cdots = l_6 = 2, \quad l_7 = l_8 = 3, \quad l_9 = l_{10} = 4,$

$l_{11} = l_{12} = 5.$

Bsp 3

Konstruiere einen Präfixcode über $A = \{0, 1, 2\}$ mit den Codewortlängen $l_1 = 1, \; l_2 = l_3 = l_4 = l_5 = 2, \; l_6 = 3.$



$C = \{1, 00, 01, 20, 21, 222\}.$

41. Vortrag

Die Quellencodierung nach Huffman

Wir übernehmen die Bezeichnungen aus dem Vortrag Quellencodierung.

Es sei $X := \{x_1, \dots, x_n\}$ eine Menge (Quellenalphabet).
Ist bekannt, daß ein Buchstabe x_i aus X in einer zu codierenden Nachricht relativ häufig vorkommt, so erscheint es sinnvoll, die Codierung von X so vorzunehmen, daß das x_i zugeordnete Codewort relativ kurz ist. Diese Idee soll im folgenden optimal umgesetzt werden.

Wir gehen davon aus, daß bei der Übertragung einer Nachricht, der Buchstabe $x_i \in X$ mit der Wahrscheinlichkeit $p_i > 0$ vorkommt (für $i = 1, \dots, n$). Dann ist offenbar $p_1 + \dots + p_n = 1$. $P := (p_1, \dots, p_n)$ heißt Wahrscheinlichkeitsverteilung von X. Das 2-tupel (X, P) wird Quelle genannt und X das zugehörige Quellenalphabet.

Sei nun $C := \{w_1, \dots, w_n\} \subseteq \{0,1\}^*$ ein sinnvoller Code von X über $\{0,1\}$ und (X, P) eine Quelle.
Sei l_i die Codewortlänge von w_i für $i = 1, \dots, n$.
Die mittlere Codewortlänge von C (bzg. P) wird dann definiert durch

$$\overline{L}(C, P) := p_1 l_1 + \dots + p_n l_n.$$

<u>Ziel</u>: Bestimme den Code $C \subseteq \{0,1\}^*$ bei gegebenem P, so daß $\overline{L}(C, P)$ möglichst klein wird.
Sei die Quelle (X, P) gegeben und $M :=$ Menge aller sinnvollen Codes $C \subseteq \{0,1\}^*$ von X. Dann wird definiert

$$\overline{L}(P) := \min_{C \in M} \overline{L}(C, P).$$

<u>Bem 1</u>

Die obige Definition ist sinnvoll, da das Minimum auch tatsächlich angenommen wird.

<u>Bew:</u>

Sei $r \in \mathbb{R}$, $r > 0$ gegeben.
Sei $C \subseteq \{0,1\}^*$ ein Code von X mit $\overline{L}(C,P) \leq r$. Dann gilt für die Codewortlänge l_i eines Codewortes $\omega_i \in C$ offenbar $l_i p_i \leq r$ bzw. $l_i \leq \frac{r}{p_i}$. Die Codewortlängen der Codewörter $\omega_i \in C$ sind also nach oben beschränkt. Also ex. auch nur endlich viele C mit $\overline{L}(C,P) \leq r$.
Daraus folgt die Behauptung.

Ist die Quelle (X,P) gegeben, so ex. nach Bem 1 also ein sinnvoller Code C von X über $\{0,1\}$ mit

$$\overline{L}(C,P) = \overline{L}(P).$$

Ein solcher Code heißt dann optimaler Code von (X,P) über $\{0,1\}$.

<u>Die Konstruktion eines optimalen Codes (Huffman-Codierung):</u>

Gegeben sei die Quelle (X,P) mit $X := \{x_1, \dots, x_n\}$,

$P = (p_1, \dots, p_n)$. OBdA sei $p_1 \geq p_2 \geq \dots \geq p_n > 0$.

Wir entwickeln zunächst das folgende Schema:

$$\begin{array}{llllll}
p_{11} & p_{12} & \dots & & p_{1,n-1} & p_{1n} \\
p_{21} & p_{22} & \dots & & p_{2,n-1} & \\
\vdots & & & & & \\
p_{k1} & p_{k2} & \dots & p_{k,n-k+1} & & \\
p_{k+1,1} & p_{k+1,2} & \dots & p_{k+1,n-k} & & \\
& \vdots & & & & \\
p_{n-1,1} & p_{n-1,2} & & & & \\
\underbrace{p_{n1}}_{=1} & & & & &
\end{array}$$

Dabei ist die erste Zeile des Schemas definiert durch

$p_{1,1} = p_1, \; p_{1,2} = p_2, \ldots, p_{1n} = p_n$.

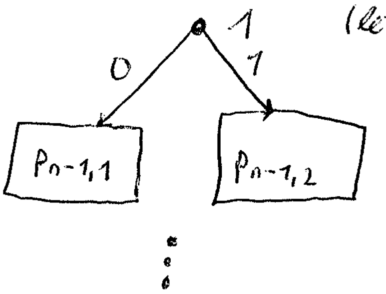
Die $(k+1)$-te Zeile ergibt sich nun aus der k-ten Zeile wie folgt.

In der k-ten Zeile werden die beiden Einträge $p_{k,n-k}$ und $p_{k,n-k+1}$ weggelassen und durch die Summe $p_{k,n-k} + p_{k,n-k+1}$ ersetzt.

Die $(k+1)$-te Zeile besitzt also einen Eintrag weniger als die k-te Zeile, sie besitzt also $n-k$ Einträge. Diese werden wieder der Größe nach geordnet. Damit ist die $(k+1)$-te Zeile festgelegt.

In der n-ten Zeile befindet sich dann also nur noch ein Eintrag, nämlich 1.

Dem obigen Schema wird nun der folgende Baum zugeordnet.



(letzte Zeile des Schemas)

Im obigen Schema werden in der nachfolgenden Zeile jeweils 2 Einträge verschmolzen. Beim Baum wird rückwärts beim Übergang zum nächsten Niveau der Knoten mit dem verschmolzenen Eintrag wieder zu zwei einzelnen Knoten auseinander gezogen.

Dem Baum wird ein (Präfix-) Code zugeordnet (s. Vortrag: Quellencodierung nach Kraft)

Der so konstruierte Code ist ein optimaler Code von (X, P) über $\{0,1\}$ (nach Huffman, ohne Beweis). Beachte: Der Code ist nicht eindeutig bestimmt.

Bem (Nachteil der Huffman-Codierung)

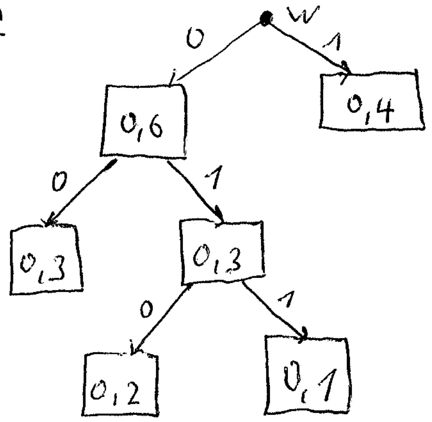
Ändern sich die Wahrscheinlichkeiten nur gering, so kann sich der Code trotzdem stark verändern. In der Praxis sind die Wahrscheinlichkeiten i.a. nicht so genau bekannt, sodaß die Huffman-Codierung in der Praxis nur selten benutzt wird.

Bsp 1 Sei $P = (0{,}4\ ;\ 0{,}3\ ;\ 0{,}2\ ;\ 0{,}1)$.

Schema

p_1	p_2	p_3	p_4
0,4	0,3	0,2	0,1
0,4	0,3	0,3	
0,6	0,4		
1			

Baum



Code $C = \{1, 00, 010, 011\}$.

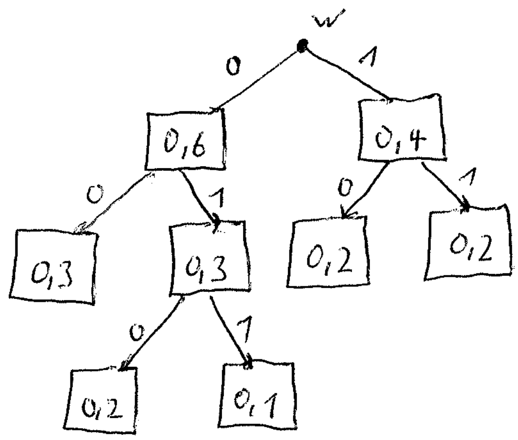
$$L(C,P) = 1 \cdot 0{,}4 + 2 \cdot 0{,}3 + 3 \cdot 0{,}2 + 3 \cdot 0{,}1 = 1{,}9.$$

<u>Bsp2</u> Sei $P = (0{,}3\ ;\ 0{,}2\ ;\ 0{,}2\ ;\ 0{,}2\ ;\ 0{,}1)$.

<u>Schema</u>

p_1	p_2	p_3	p_4	p_5
0,3	0,2	0,2	0,2	0,1
0,3	0,3	0,2	0,2	
0,4	0,3	0,3		
0,6	0,4			
1				

<u>Baum</u>



<u>Code</u>

$C = \{00,\ 010,\ 10,\ 11,\ 011\}$

$L(C,P) = 0{,}3 \cdot 2 + 0{,}2 \cdot 2 + 0{,}2 \cdot 2 + 0{,}2 \cdot 3 + 0{,}1 \cdot 3 = 2{,}3$