Skript zum

Proseminar

im Rahmen der Weiterbildung für Lehrer

V. Schulze 2016 FU Berlin

Themen zum Proseminar

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

Komplexe Zahlen

1. Vortrag: Komplexe Zahlen und Einheitswurzeln (3)

Primzahlen

2. Vortrag: Elementare Eigenschaften der Primzahlen (6)
3. Vortrag: Eine Abschätzung für die n-te Primzahl (9)
4. und 5. Vortrag: Die Reziprokensumme der Primzahlen (13)
6. und 7. Vortrag: Der Satz von Tschebycheff* (16)

Codierungstheorie

8. Vortrag: Codes (18)
9. Vortrag: Lineare Codes und die Generatormatrix (22)
10. Vortrag: Der duale Code und die Kontrollmatrix (25)
11. Vortrag: Der Hammimg-Abstand und Fehlerkorrektur (28)
12. Vortrag: Hammimg-Codes und perfekte Codes (31)
13. und 14. Vortrag: Fehlerkorrektur bei linearen Codes* (34)

Kettenbrüche

15. Vortrag: Kettenbrüche und beste Aproximationen (37)
16. Vortrag: Periodische Kettenbrüche (39)

Primzahltests

17. Vortrag: Der Primzahltest von Fermat und Carmichael-Zahlen (40)
18. Vortrag: Der Primzahltest von Miller-Rabin (44)

Kryptographie

19. Vortrag: Die RSA-Verschlüsslung (47)
20. Vortrag: Ein Angriff auf die RSA-Verschlüsslung und ein sicheres Verschlüsslungsverfahren (50)
21.und 22. Vortrag: Der Wiener Angriff auf die RSA-Verschlüsslung (52)

Quadratische Reste

23. Vortrag: Das Legendre-Symbol (56)
24. Vortrag: Das quadratishe Reziprozitätsgesetz (59)

Ringtheorie

25. und 26. Vortrag: Der Gaußsche Zahring und der Euklidiche Algorithmus (65)

Konstruktionen mit Zirkel und Lineal

27. und 28. Vortrag: Die Konstruktion regelmäßiger n-Ecke mit Zirkel und Lineal (68)

Gruppen spezieller Ordnung

29. und 30. Vortrag: Nichtabelsche Guppen der Ordnung 2p* (72)
31. und 32. Vortrag: Gruppen der Ordnung p^{2*} (73)

4. Vortrag

Komplexe Zahlen und Einheitswurzeln

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

Menge der Komplexen Zahlen: $\mathbb{C} := \{a+bi \mid a,b \in \mathbb{R}\}$ (Gilt 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 $(a+bi)\cdot\underbrace{\left(\frac{a}{a^2+b^2}-\frac{b}{a^2+b^2}i\right)}_{=(a+bi)^{-1}} = 1$, $= \frac{1}{a+bi}$ (Schreibweise)

Aus den obigen Rechenregeln folgt

Bem 1 $(\mathbb{C},+,\cdot)$ ist ein Körper (Körper der Komplexen Zahlen)

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

$\overline{z} := a-bi$ heißt die zu z konjugiert Komplexe Zahl

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

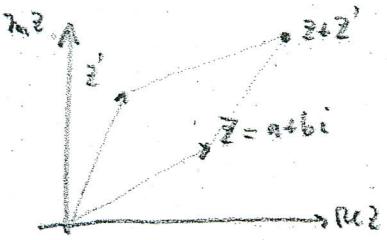
$b =: \mathrm{Im}\,z$ heißt Imaginärteil von z beachte: $\mathrm{Im}\,z \in \mathbb{R}$.

Es gilt $z\cdot\overline{z} = a^2+b^2$. ; $\overline{z_1\cdot z_2} = \overline{z_1}\cdot\overline{z_2}$ (Leicht nachzurechnen)

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

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

Gaußsche Zahlenebene



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

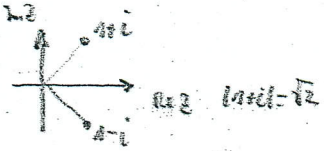
Die Addition in $\mathbb{C}$ entspricht offenbar der Vektoraddition in der Gaußschen Zahlenebene.

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

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

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

Bsp

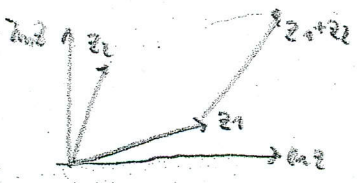


Rechenregeln

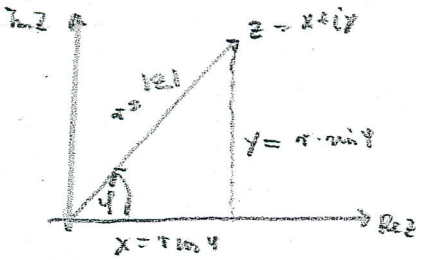
(i) $\overline{z_1 \pm z_2} = \overline{z_1} \pm \overline{z_2}$ ✓

(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) [kann sich jeder selber nachrechnen; ist anschaulich geometrisch klar in der Gaußschen Zahlenebene]



Polarkoordinaten $\quad \operatorname{Im} z \neq 0$.



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

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

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

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

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

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

(Additionstheoreme für sin und cos)

Polarkoordinatendarstellung für $z_1 z_2$:

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

(Produkt der Beträge; Addition der Winkel)

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

$(-1+i)^2 = -2i$

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

Inverse Komplexe Zahlen

Sei $z \neq 0$.

Dann: $\arg \frac{1}{z} \cdot z = 0 = \arg z + \arg \frac{1}{z}$; also $\arg \frac{1}{z} = -\arg z$

$|z \cdot \frac{1}{z}| = 1 = |z| \cdot \frac{1}{|z|}$, also $\left|\frac{1}{z}\right| = \frac{1}{|z|}$.

Zusatz: $|z|=1$ gilt speziell: $\frac{1}{z} = \overline{z}$.

Wurzeln Komplexe Zahlen

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

$a \in \mathbb{C}$ heißt n-te Wurzel von z, falls $a^n = z$ ist (Schreibweise für a: $\sqrt[n]{z}$).

Bemerke: $\sqrt[n]{z}$ ist nicht eindeutig bestimmt. ($z \in \mathbb{R}$: $\sqrt{4} = 1$ und $\sqrt{4} = -2$)

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

Jede n-te Wurzel von z besitzt den Betrag $\sqrt[n]{|z|}$ (positive reelle n-te Wurzel)

Das Argumentwinkel einer n-ten Wurzel von z erfüllt die Eigenschaft:

$n \cdot \alpha = \arg z +$ ganzzahliges Vielfaches von 2π.

Die beiden letzten Aussagen ergeben sich offenbar aus den Regeln für das Potenzieren komplexer Zahlen.

Also folgt:

Die n-ten Wurzeln von z sind

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

Bsp $\sqrt{-1} = \pm\left(\frac{1+i}{\sqrt{2}}\right)$

$\sqrt[3]{-4} = 1+i$ (weitere Wurzeln?)

$\sqrt[8]{1} = \frac{1+i}{\sqrt{2}}$ (Man gebe alle 8-ten Wurzeln von 1 an)

Hinweis: Argumentwinkel geometrisch in der Gaußschen Zahlenebene.

n-te Einheitswurzeln

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

Die n-ten Wurzeln von 1 heißen n-te Einheitswurzeln (EW)

Die n-ten EW sind $\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ für $k = 0, \dots, n-1$ (man gebe eine geometrische Interpretation)

Sei n-te EW ist $\zeta_n := \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$.

Die n n-ten EW sind dann $1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}$.

Eine Multiplikation von z mit ζ_n, so bedeutet dies geometrisch eine Drehung um $\frac{2\pi}{n}$.

Es gilt $\overline{\zeta_n^i} = \zeta_n^{-i}$ (es folgt ja $\zeta_n^i \cdot \zeta_n^{-i} = 1$ und $\zeta_n^i \cdot \overline{\zeta_n^i} = |\zeta_n^i| = 1$)

Ferner gilt $\zeta_n^{n-i} = \zeta_n^{n-i}$ oder $\zeta_n^n = 1$

Satz $1 + \zeta_n + \dots + \zeta_n^{n-1} = 0$ (Die Summe der n n-ten EW ist 0)

Beweis
$$S := 1 + \zeta_n + \dots + \zeta_n^{n-1}$$
$$\zeta_n \cdot S = \zeta_n + \zeta_n^2 + \dots + \zeta_n^n$$
$$\Rightarrow (1-\zeta_n)S = 1 - \zeta_n^n = 0$$

Bsp $x^2 + x - 1$ besitzt die Nst $-\frac{1}{2} \pm \frac{\sqrt{5}}{2}$ und $\zeta_5 + \zeta_5^{-1}$ falls ist $\zeta_5 + \zeta_5^{-1} =$

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 $2, 3, 5, 7, \ldots$.

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 $\pm 2, \pm 3, \pm 5, \pm 7, \ldots$.

Def 3 Sei $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ die Menge aller Primzahlen.

Es bezeichne p_n die n-te Primzahl (also $p_1 = 2, p_2 = 3, p_3 = 5, \ldots$).

Sei $x \subset \mathbb{R}$ Dann bezeichne

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

$\pi: \mathbb{R} \longrightarrow \mathbb{N}_0$ 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 $2, 2\cdot5, 2\cdot7, 2\cdot5\cdot7$ Primzahlen in $2\mathbb{N}$.
Es gilt $(2\cdot5)\cdot(7\cdot2) = (2\cdot5\cdot7)\cdot2$.
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 $n \in \mathbb{N}$, nungerade.

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

Satz 2 (Primzahlsatz) (ohne Beweis)

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

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

Bem 4 (p_i, p_j) heißen Primzahlzwillinge, wenn p_i, p_j Primzahlen sind und $p_j - p_i = 2$ ist.
3 und $(3,5)$, $(5,7)$, $(11,13)$ Primzahlzwillinge.
Es wird vermutet, daß es unendlich viele Primzahlzwillinge gibt.

Satz 3 (Dirichletscher Primzahlsatz). (ohne Bew)
Sei $n \in \mathbb{N}$, $a \in \mathbb{N}$ und $ggT(a,n) = 1$.
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 $1 \leq x \leq n$: $ggT(x,n) = 1$
(Eulersche φ-Funktion).
[Warum ist die Voraussetzung $ggT(a,n) = 1$ notwendig?]

Satz 4

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

Beweis

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

Schluß von n auf $n+1$:

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

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

(beweise: $1 + 2 + \cdots + 2^{n-1} = 2^n - 1$ (geometrische Summe))

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

Bem 5

Analogon 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

$p_1 = 2,\ p_2 = 3,\ p_3 = 5,\ p_4 = 7, \dots$.

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 $p_1, \dots, p_n$ vorkommen.

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

Dann ist $N_3(10) = N_3(10) = 9$.

(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 $x < p_n$.

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

Bew Betrachte die Primfaktorzerlegung

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

von n und spalte von das 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

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

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

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

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

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

Nun soll $N_n(x)$ abgeschätzt werden.

Bei der Darstellung einer natürlichen Zahl $m \leq x$ mit der Eigenschaft $(*)$ gibt es

für a_n höchstens $\sqrt{x}$ Möglichkeiten (da $a_n^2 \leq m \leq x$) und für

die $a_1, \dots, a_{n-1}$ 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.

Satz 2

Es gibt unendlich viele Primzahlen.

Beweis

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

Satz 3

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

Beweis

Sei p_n die n-te Primzahl. Dann gilt

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

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

Anmerkung 1

Man kann mit dieser Methode auch beweisen, daß die Reziprokensumme

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

divergiert. (ohne $\zeta(s)$).

Satz 4 Für $n \geq 4$ gilt $\pi(n) > \frac{\ln n}{\ln 4} - 1$.

Beweis

Sei $m \in \mathbb{N}$, $m \geq 4$.
Wähle $n \in \mathbb{N}_{\geq 2}$, so daß $4^n \leq m < 4^{n+1}$ gilt.

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

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

Anmerkung 2

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

Nach dem Primzahlsatz (ohne $\zeta(s)$) gilt:

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

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

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 $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, ...

$\pi(1) = 0$, $\pi(2) = 1$, $\pi(6) = 3$, $\pi(10) = 4$, ...

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

Satz 1

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

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

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) $p_n < 2^{n+1}$

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

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

Anmerkung

Sei $\mathbb{P} := \{2, 3, 5, 7, \dots\}$ 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 ≥ 4.

$\frac{1}{1-x} = 1 + x + x^2 + \dots$ (geometrische Reihe, gliedweise integriert ergibt)

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

Beweis (v. Satz 2)

Benutzt wird die aus der Analysis bekannte Reihenentwicklung

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

Bei jeder der endlichen vielen ∞ Reihen wird die 1 herausgenommen

Es folgt

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

Für den Term rechts erhält man die Abschätzung

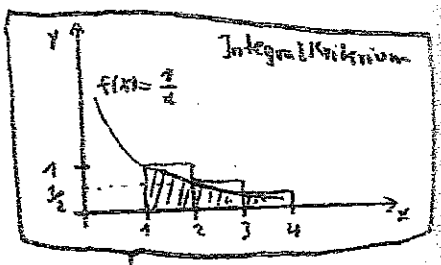
(3) $\sum_{\substack{p \le n \\ p \in \mathbb{P}}} \sum_{\nu=2}^{\infty} \frac{1}{\nu \cdot p^\nu} \le 1$

wie folgt:

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

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

Gebraucht wird ferner die Abschätzung



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

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):

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

Beweis von (b):

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

Die Anzahl der Faktoren rechts und links ist gleich

$\frac{1}{1-\frac{1}{m}} \ge \frac{1}{1-\frac{1}{p}}$ falls $p_m \ge m+1$

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 recht elementaren Mitteln liefert

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

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

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

Idee Der Beweis wird in mehreren Einzelschritten durchgeführt.

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

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

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

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

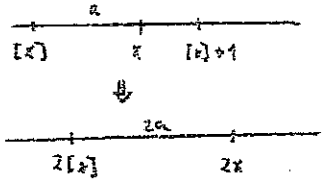
Schluß von n auf $(n+1)$: $2^{n+1} \underset{\text{Ind. Vor.}}{\leq} 2 \cdot \binom{2n}{n} \underset{(a)}{\leq} \frac{(2n)!}{(n!)^2} \cdot \frac{(2n+2)(2n+1)}{(n+1)(n+1)} \underset{(a)}{=} \binom{2n+2}{n+1}$

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

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

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

Bew:



$\Rightarrow$ $[2x] = 2[x]$, falls $a := x - [x] < \frac{1}{2}$
$\Rightarrow$ $[2x] = 2[x] + 1$, falls $a = x - [x] \geq \frac{1}{2}$ $\Rightarrow$ 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)

Idee: Bestimme die Faktoren $1, 2, \ldots, m$ von $m!$:

$\left[\frac{m}{p}\right]$ die Faktoren mit Teilf. von p
$\left[\frac{m}{p^2}\right]$ " " p^2
$\left[\frac{m}{p^3}\right]$ " " p^3
$\vdots$

$\Rightarrow$ Beh.

(f) Es gilt

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

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

(g) Abschätzung für π nachrechnen:

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

$\ln 2 \ge \frac{1}{2} \Leftrightarrow \ln 4 \ge 1$

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

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

8. Vortrag

Codes

Ziel der Codierungstheorie:

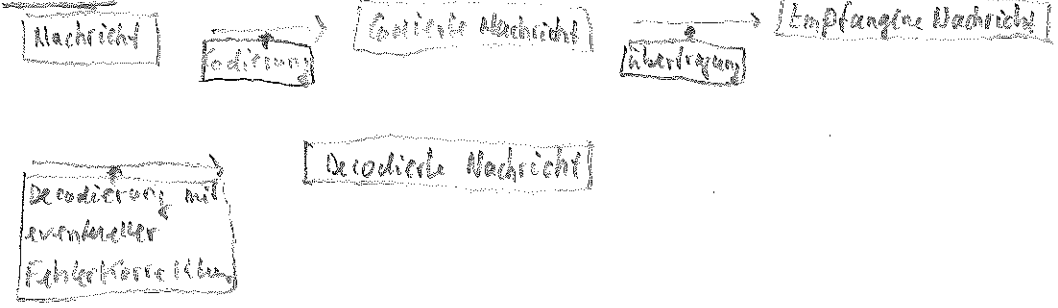
Übertrage digitale Nachrichten, so daß Fehler erkannt und möglichst sogar korrigiert werden können.

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

Bsp Von einem Satelliten sollen Daten (20 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 gesendet, so können leicht Übertragungsfehler auftreten und die empfangene Nachricht ist nicht mehr (gut genug) lesbar (die Bilder werden unscharf).

Deshalb wird die Folge von 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 können. Um dies zu erreichen, muß das Codierungsverfahren gut gewählt werden.

Bsp 1 (2- fache 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 ⟼ 00
1 ⟼ 11

(00, 11 heißen Codewörter des Codes (Folge bleibt!))

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

Sei zB 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 zB 00 10 11 00 11 11 die empfangene Nachricht kann ein
Übertragungsfehler aufgetreten sein (an der 2. Code 4 Stelle).

Der 2- fache Wiederholungscode ermöglicht also eine Fehlererkennung, wenn an
genau einer Stelle ein Übertragungsfehler eingetreten ist. In diesem Fall müsste
die Nachricht noch einmal übertragen werden. (kein decodierbares Codewort!)
Der Code hilft 1- Fehler zu erkennen.

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

Bsp 2 (3- fache Wiederholungs code)

Codierungsvorschrift: 0 ⟼ 000 (000, 111 sind die Codewörter!
1 ⟼ 111 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 zB 101 empfangen, so muß wird ein Übertragungsfehler aufgetreten sein.
Geht man davon aus, daß es in eine der drei Stellen ein Übertragungsfehler
aufgetreten ist, so kann der Fehler auch dadurch korrigiert werden:
101 wird zu 111 korrigiert

Treten bei der Übertragung eines Codewortes 2 Fehler auf, so kann dies
nicht erkannt werden.

Wird zB bei der Übertragung von 000 die Wort 101 empfangen, so ist
klar, daß ein Übertragungsfehler aufgetreten ist. (die Annahme 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.

<u>Bsp 3</u>

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 ergänzt).

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. Das läßt sich leicht durch Ausprobieren verifizieren.

z.B. unterscheiden sich a_1 und a_2 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 die 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_1 an der 2., 3. und 5. Stelle ein Fehler auf, so geht a_1 über in a_2 und der Fehler kann nicht erkannt werden.

der Code ist also 1-Fehler-korrigierend und auch 2-Fehler erkennend.

Insgesamt: 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.

Bemerkung

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

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

Elemente des K-Vektorraums K^5.

Die Elemente von K^5 sind also 5-Tupel x

$$K^5 := \{(x_1, x_2, x_3, x_4, x_5) \mid x_1, \dots, x_5 \in K\}.$$

Dann besteht K^5 genau aus $2^5 = 32$ Elemente.

Falls die Codewörter aus Bsp 3 als Elemente des K-VR K^5 sind,

dann ist $C := \{(x_1, x_2, x_3, x_4, x_5)\}$ ein Unterraum des K-VR K^5

mit der Basis $\mathcal{B} = \{a_1, a_2\}$,

denn genügt es zu zeigen, daß a_1 und a_2 linear unabhängig sind und daß sich die Elemente aus C als Linearkombinationen von a_1 und a_2 darstellen lassen.

Man führe dies im Einzelnen aus.

2. 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 $a \cdot (a_1, \dots, a_n) = (a \cdot a_1, \dots, a \cdot a_n)$ 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 $B := \{(a_{11}, \dots, a_{1n}), \dots, (a_{m1}, \dots, a_{mn})\}$ eine 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 $(a_1, \dots, a_m) \in K^m$.

$(a_1, \dots, a_m)$ 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

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

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

Die Codierung soll möglichst so gewählt werden, daß erkannt wird, wenn bei der Übertragung des Codewortes durch ein Übertragungskanal Übertragungsfehler entstanden 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

$$B = \begin{pmatrix} 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 \\ 0 & 0 & 1 & 0 & 1 & 1 & 1 \end{pmatrix} = \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix}$$

Man beachte, daß die Zeilenvektoren von B linear unabhängig sind.

C enthält also genau alle Linearkombinationen der Zeilenvektoren von B: also

$$C = \{ \gamma_1 a_1 + \gamma_2 a_2 + \gamma_3 a_3 \mid \gamma_1, \gamma_2, \gamma_3 \in K \}.$$

Insbesondere enthält C genau 8 Elemente.

Bsp:

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

$$\begin{aligned} &(0,\dots,0) + C \quad (= C) \\ &(1,0,\dots,0) + C \quad = \{(1,0,\dots,0) + a \mid a \in C\} \\ &(0,0,1,0,\dots,0) + C \\ &\vdots \\ &(0,\dots,0,1) + C \end{aligned}$$

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 folgende 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:
Voraussetzung: Das Wort $(a_1,\dots,a_n) \in K^7$ wird empfangen; $(a_1,\dots,a_n) \notin C$.
Dann ist mindestens eine Komponente ein Übertragungsfehler aufgetreten.
Das Wort $(a_1,\dots,a_n)$ liege in der Nebenklasse $(0,\dots,0,1,0,\dots,0) + C$.
$\uparrow$ i-te Stelle.
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 Komponenten 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.

12. 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

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

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 $\mathrm{Rg}\,G = m$.

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

$C^\perp$ 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 $\operatorname{Rg} H = m'$, da die Zeilenvektoren von H linear unabhängig sind.

Bem 1 Es gilt $(C^\perp)^\perp = C$; d.h.

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

Beweis

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 $\operatorname{Rg} H = m' = n - \operatorname{Rg} G = n - m$.

Der Lösungsraum von (**) besitzt also die Dimension

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

Jeder Zeilenvektor $(g_{i1},\dots,g_{in})$ von G ist Lösung von (**),

denn nach Def. von H gilt

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

Dies ist gleichwertig mit

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

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:

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

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 $H\begin{pmatrix} a_1\\ \vdots\\ a_n\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}$, so ist wieder ein Übertragungsfehler ausgeblieben.

Bsp1 Sei $C=\{(0,0),(1,1)\}$ (Code zweifacher Wiederholungscode). (s. Bsp1, 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 (s. Vortrag) mit der Generatormatrix $G=\begin{pmatrix}1&1&0&1&0&0&0\\0&1&1&0&1&0&0\\1&1&0&0&0&1&0\\1&0&0&0&0&0&1\end{pmatrix}$

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 Fehlerkorrektur

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) $\Delta(c,c') + \Delta(c',c'') \geq \Delta(c,c'')$ (Dreiecksungleichung)

[Die i-ten Komponenten von c und c'' können aus dem verschiedenen 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 dann 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 $w(c) = \Delta(c,0)$ ($0 := (0,\dots,0)$ bezeichnet den Nullvektor)

Bem 3 Es gilt $\Delta(c_1,c_2) = \Delta(c_1-c_2, 0) = w(c_1-c_2)$ (Bem 2 / Bem 1 final)

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 (Manchmal 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 $\Delta(c,c') = \Delta(c-c', 0) = w(c-c')$

(Bem 3 (iv)) (Def von w)

Bem 6 (Vergleiche Vortrag 3)

(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 irgendein 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):

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

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 mehr als 2 Elemente besitzt, gilt:

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

Bew Sei $c = (c_1, c_2, \dots, c_n)$; $c \neq a$; $c \neq (0, \dots, 0)$ wir nehmen o.BdA an, daß sich c und $a = (a_1, a_2, \dots, a_n)$ $a \neq (0, \dots, 0)$, a in der ersten Komponente unterscheiden.
o.BdA $c_1 = 0$, $a_1 = 1$.
Gelte $\gamma_1 c + \gamma_2 a = (0, 0, \dots, 0)$. Dann ist zum Nachweis der linearen Unabhängigkeit von a und c zu zeigen: $\gamma_1 = \gamma_2 = 0$.

Betrachtet man die 1. Komponente der Vektorgleichung $\gamma_1 c + \gamma_2 a = (0, \dots, 0)$, so folgt $\gamma_2 = 0$.

Da $c \neq (0, \dots, 0)$ ist, folgt weiter $\gamma_1 = 0$.

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 $H = \begin{pmatrix} a_{11} & \dots & a_{1\,2^n-1} \\ \vdots & & \vdots \\ a_{n1} & & a_{n\,2^n-1} \end{pmatrix}$ 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.

Bsp1

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. Vorlesung), 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.

Bem1 Nach Bem7 (Vortrag 10) gilt für den Minimalabstand $d(C)$ die Ungleichung

$$d(C) \geq 3$$

Also ist C 1-Fehler-Korrigierend nach Bem7 und Bem8 (Vortrag 10).

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

Bemd

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:

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

Die 2^n Nebenklassen von C sind also

$$\begin{aligned}&(0,\dots,0)+C, \quad (=C),\\ &(1,0,\dots,0)+C,\\ &(0,1,0,\dots,0)+C,\\ &\vdots\\ &(0,\dots,0,1)+C.\end{aligned}$$

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 $d(C)=3$ nicht in C.

Folgerung Hamming: $(a_1,\dots,a_m)$ wird empfangen.

Ist $(a_1,\dots,a_m) \in C$, so wird davon ausgegangen, daß kein Übertragungsfehler aufgetreten ist.

Ist $(a_1,\dots,a_m) \notin C$, so liegt $(a_1,\dots,a_m)$ in einer Nebenklasse $(0,\dots,0,\underset{\uparrow \text{i-te Stelle}}{1},0,\dots,0)+C$,

$(a_1,\dots,a_m)$ besitzt also die Form

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

Bei der Übertragung zum Empfänger sei 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 $(a_1, \dots, a_m) - (0, \dots, 0, \underset{\uparrow}{1}, 0, \dots, 0) = C$; also ein Codewort.
i-te Stelle

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

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

da

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

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

Bsp 2

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, Vorlesung 9)

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

Dann liefert die Fehlerkorrektur in der 1. Komponente das Codewort

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

Def 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.

Bem 2 Nach Bem 1 ist jeder Hamming-Code perfekt.

13 und 14. Vorlesung: 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:

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

Annahme: 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. $c' \in C$.

Fehlerkorrektur 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.

Bem1
Für $y = (y_1 \dots y_n) \in K^n$ 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 $H \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$ genau $y \in C$ ist.

Allgemein gilt:

Bem2 Zwei Vektoren aus K^n besitzen dasselbe Syndrom genau dann, wenn sie zu derselben Nebenklasse von C gehören.

Beweis: Sei $y = (y_1 \dots y_n) \in K^n$, $z = (z_1 \dots z_n) \in K^n$. Dann gilt:

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

Beachte: Insbesondere 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 Hy_i (da y in genau einer Nebenklasse von C liegt und ungleich y_0).

Die zugehörige Nebenklassenführer ist dann y_i.

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

Die Fehlerstelle ist also y_i.

Bemerkung 3

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

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

Beweis

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 beweisen:

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 $w(y - c) \leq 1$.

Bsp Die Generatormatrix sei $(1,1,1)$.
Der Code ist dann $C = \{(1,1,1), (0,0,0)\}$; das $c = 1$
Der duale Code ist die Lösungsmenge 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 $\frac{3^3}{2} = 4$.
Die Nebenklassen sind C, $(1,0,0) + C$, $(0,1,0) + C$, $(0,0,1) + C$.
Die empfindlichen Repräsentanten haben ein 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

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 $\tau \in \mathbb{R}$, $a \in \mathbb{Z}$, $b \in \mathbb{N}$. Dann:

$\frac{a}{b}$ heißt beste Approximation von τ, wenn gilt:

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

Bspl 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 $\tau \in \mathbb{R}$, o.B.d.A. $\tau > 1$.

Approximiere τ im 1. Schritt durch $a_0 := [\tau]$ (größte ganze Zahl $\leq \tau$)

Beende das Verfahren, falls $\tau = a_0$. Andernfalls:

Sei $\alpha_1 \in \mathbb{R}$ def. durch $\tau = a_0 + \frac{1}{\alpha_1}$. Dann ist $\alpha_1 > 1$. Setze $a_1 := [\alpha_1]$

Approximiere τ im 2. Schritt durch $a_0 + \frac{1}{a_1}$.

Beende das Verfahren, falls $\tau = a_0 + \frac{1}{a_1}$. Andernfalls:

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

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

Beende das Verfahren, falls $\tau = a_0 + \cfrac{1}{a_1 + \frac{1}{a_2}}$ ist, also der Approximationsfehler gleich 0 ist. Andernfalls:

Setze das Verfahren fort.

Das Verfahren bricht ab, wenn

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

(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 τ offenbar rational. Es gilt auch die Umkehrung (ohne Bew.)

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

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

Def 3

(i) Ist τ nicht rational, so schreibt man $\tau = [a_0, a_1, \dots]$ und $[a_0, \dots, a_n]$ heißt n-te Näherungsbruch von τ ($n \geq 0$).
Dies ist sinnvoll, da die Folge der n-ten Näherungsbrüche gegen τ konvergiert (ohne Bew.) s Bem 4

(ii) Sei τ rational und

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

Im Fall $a_n > 1$ wird diese Darstellung von τ leicht durch

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

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

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

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

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

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

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

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

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

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

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

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

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

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

Bsp 2 Berechne die Näherungsbrüche von $\tau = \frac{7}{5}$ mit Hilfe der Formeln aus Bem 3.
Nach Bem 2 ist $\frac{5}{3}$ eine beste Approximation von $\frac{7}{5}$.

16. Vorlesung: Periodische Kettenbrüche

Bem 1 Für $n \geq 0$ sei $[a_0, a_1, \dots, a_n] = \frac{p_n}{q_n}$ die Näherungsbrüche der reellen Zahl $\tau \in \mathbb{R}$ (s. 15. Vorlesung)

(ohne Bew) (a) Dann gilt:

$$\frac{p_0}{q_0} < \frac{p_2}{q_2} < \frac{p_4}{q_4} < \cdots < \tau < \cdots < \frac{p_5}{q_5} < \frac{p_3}{q_3} < \frac{p_1}{q_1}.$$

Ein Gleichheitszeichen trifft auf jeden Fall nicht zu, da τ irrational ist.

Stets gilt $\left|\tau - \frac{p_n}{q_n}\right| < \frac{1}{q_n^2}$.

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

Bem 2 Sei $a_0, a_1, \dots$ eine Folge ganzer Zahlen.

(ohne Bew) Dann konvergiert $[a_0, \dots, a_n]$ für $n \to \infty$ gegen eine reelle Zahl τ.

Verschiedene Folgen konvergieren gegen verschiedene reelle Zahlen.

Bem 3 Die (reelle) Kettenbruchentwicklung von τ ist $[a_0, a_1, a_2, \dots]$.

Sei $\tau \in \mathbb{R}$ und $\tau = [a_0, a_1, a_2, \dots]$.

(ohne Bew) Die Kettenbruchentwicklung ist periodisch $\Leftrightarrow$ τ Nullstelle eines quadratischen irreduziblen Polynoms $f(X) \in \mathbb{Q}[X]$ ist.

Bsp 4

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

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

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

(iii) $\alpha := [1, 2, 2, 2, \dots] = 1 + \frac{1}{[2, 2, 2, \dots]} = 1 + \frac{1}{1+\alpha}$, also $\alpha^2 + \alpha = 1 + \alpha + 1$, d.h. $\sqrt{2} = \alpha$

$$[2, 2, \dots] = 2 + \frac{1}{2 + \frac{1}{2 + \cdots}} = 1 + [1, 2, 2, \dots] = 1 + \alpha$$

Beste Approximation von $\sqrt{2} \approx 1,414213\dots$

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

oder mit Hilfe von Bem 2:

$\frac{p_0}{q_0} = 1$ ist beste Approx

$\frac{p_1}{q_1} = \frac{3}{2}$, $\frac{p_2}{q_2} = \frac{7}{5}$, $\frac{p_3}{q_3} = \frac{17}{12}$, $\frac{p_4}{q_4} = \frac{41}{29}$, $\frac{p_5}{q_5} = \frac{99}{70}$, $\frac{p_6}{q_6} = \frac{239}{169}$

nach Bem 2

$\approx 1,414213$

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

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

$\sqrt{3} = [1, \overline{1, 2}]$

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

XX. 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 $\leq \sqrt{n}$ 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 $ggT(a,n) = 1$ 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 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 $i = 1, \ldots, k$ 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 $\operatorname{ggT}(a,n)=1$.

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

Wegen $\operatorname{ggT}(a,p_i)=1$ 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-1, etwa $(n-1)=\gamma_i(p_i-1)$.

Dann folgt

$$a^{n-1} \equiv \left(a^{p_i-1}\right)^{\gamma_i} \equiv 1 \pmod{p_i} \quad \text{für } i=1,\dots,K.$$

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 $\operatorname{ggT}(-1,n)=1$ 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 das 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. $1 \pmod{p^\alpha}, g \pmod{p^\alpha}, \dots, g^{\varphi(p^\alpha)-1} \pmod{p^\alpha}$ sind paarweise verschiedene Restklassen, 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 (denn $\operatorname{ggT}\left(p^\alpha, \frac{n}{p^\alpha}\right) = 1$).

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

$g^{n-1} \equiv 1 \pmod{n}$, also auch $g^{n-1} \equiv 1 \pmod{p^\alpha}$.

Nach $(*)$ folgt

$$p^{\alpha-1}(p-1) \mid (n-1)$$

Da p Teiler von n 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

$(p-1) \mid (n-1)$ 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 $n = p_1 p_2 \cdots p_k$ besitzt.

Analog zu Schritt 2 folgt (p_i prim)

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

Bem. Es läßt sich leicht nachprüfen, daß

$$3 \cdot 11 \cdot 17$$

die kleinste Carmichael-Zahl ist.

4. Vortrag:

Der Primzahltest von Miller-Rabin

Es sei n eine (sehr große) natürliche Zahl.
Wie läßt sich (möglichst schnell) entscheiden, ob n Primzahl ist.
Wir wollen hierfür ein probabilistisches Verfahren angeben, das in der Praxis sehr häufig verwendet wird.
Dabei handelt es sich um eine Weiterentwicklung des Fermat-Tests.

Bem 1 (Fermat-Test).
Sei p Primzahl und $1 \leq a \leq p-1$.
Dann gilt nach Fermat $a^{p-1} \equiv 1 \pmod p$.

Sei $n > 2$ gegeben und $a \in \mathbb{N}$ mit $ggT(a,n) = 1$.
Gilt (1) $a^{n-1} \not\equiv 1 \pmod n$,
so ist n keine Primzahl.

Gilt (2) $a^{n-1} \equiv 1 \pmod n$,
so läßt sich keine Aussage darüber machen, ob n Primzahl ist. (Fermat-Test)
Im Fall (2) 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

Satz 1 (De Miller-Rabin-Test).

Gegeben sei eine natürliche Zahl $n > 2$.

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

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

Man sagt:

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

(1) $a^m \equiv 1 \pmod n$

oder

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

gilt.

Dann:

n ist keine Primzahl, wenn n den Miller-Rabin-Test mit der Testbasis a nicht besteht (also wenn weder (1) noch (2) 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 (1) oder (2) gilt.

Nach Fermat gilt

$$a^{p-1} = a^{2^s \cdot m} \equiv 1 \pmod p.$$

Sei $j \in \{0, \dots, m\}$ minimal mit

$$a^{2^j \cdot m} \equiv 1 \pmod p.$$

Im Fall $j = 0$ folgt (1) 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 $\left(a^{2^i m}\right)^2 = a^{2^j \cdot m} \equiv 1 \pmod p$

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

Vielfaches von p. Da p Primzahl ist, folgt

$p \mid a^{2^{i-1} \cdot m} - 1$ oder $p \mid (a^{2^{i-1} \cdot m} + 1)$,

also $a^{2^{i-1} \cdot m} \equiv 1 \pmod p$ oder $a^{2^{i-1} \cdot m} \equiv -1 \pmod p$.

Dann Def. von j ist aber $a^{2^{j-1} \cdot m} \not\equiv 1 \pmod p$

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

Bem1

Sei $n > 2$; $\operatorname{ggT}(a, n) = 1$

Gilt (1) oder (2), so folgt

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

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.

Bem2 (ohne Beweis)

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

Genauer gilt:

Sei $n > 2$ keine Primzahl.

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

Bsp 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

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

$2^{2 \cdot 35} \equiv 166 \pmod{561}$

$2^{4 \cdot 35} = 67 \pmod{561}$ (d.h. (ii) gilt nicht)

$2^{8 \cdot 35} = 1 \pmod{561}$

Mit Hilfe der Testbasis $a = 2$ kann also nach dem Miller-Rabin-Test gezeigt werden, daß n keine Primzahl ist.

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 autorisiert 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 autorisierten 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 $m \in \{0, \dots, n-1\}$ zerlegt.

Die Verschlüsselungsfunktion V_T ist dann definiert durch

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

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 $a^{\kappa(p-1)+1} \equiv a \pmod{p}$ f.a. $a \in \mathbb{Z}$: (für $a \not\equiv 0 \pmod{p}$ trivial, sonst nach Fermat (1. Satz 23 9, Satz 42 im Skript: Einf in die Algebra und Zahlentheorie)

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

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

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, p_i) seine Nachricht an den Teilnehmer T_j mit dem öffentlichen Schlüssel (n_j, p_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 $k := q+\ell = p-\ell$.

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 gelte 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.

Bsp 1 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.

Bsp 2 Faktorisiere $n = 1517$ und zeige, daß $d = 37$ ist.

Bem 2

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 erzeugt 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 einmal 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 mithilfe 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 verschlüsselt werden durch Bildung von c^d, falls d bekannt ist.

Ja 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 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 $\frac{e}{n} = [a_0, a_1, \dots, a_m]$, dabei sei o.B.d.A. $a_m = 1$.

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

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

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 $q_0, \dots, q_m$ 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

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

Nach (1) genügt es dann zu zeigen, daß

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

gilt

(3) Beweis von (*):

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

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

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

$n - (p-1)(q-1) = p + q - 1$

$$< \frac{K \cdot 3\sqrt{n}}{d \cdot n}$$

wegen $n = p \cdot q$, $q < p$ ist $q < \sqrt{n}$, dann gilt auch $p < 2q < 2\sqrt{n}$

$$\leq \frac{1}{d \cdot n^{\frac{1}{3}}} < \underset{\text{Vor.}}{\frac{1}{3d^2}} < \frac{1}{2d^2}.$$

Es gilt

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

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

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

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 $\frac{235}{391}$: $\frac{0}{1} = [0]$

$391 = \underline{1} \cdot 235 + 156$ — 2. Näherungsbruch von $\frac{235}{391}$: $0 + \frac{1}{1} = [0,1]$

$235 = \underline{1} \cdot 156 + 79$ — 3. " : $0 + \frac{1}{1 + \frac{1}{1}} = [0,1,1]$

$156 = \underline{1} \cdot 79 + 77$ — 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 Vorlesung 14 erhält man die Näherungsbrüche

$$\frac{0}{1} = 0,\ 0 + \frac{1}{1} = \frac{1}{1},\ \frac{1}{2},\ \frac{2}{3},\ \frac{3}{5},\ \frac{3 \cdot 38 + 2}{5 \cdot 38 + 2} = \frac{116}{92},\ \frac{235}{391}$$

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 jeder 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

$$x^2 \equiv a \pmod p \; ; \; p>2 \text{ Primzahl}, \; p \nmid a, \; a \in \mathbb{Z}.$$

Def 1 (Legendre-Symbol)

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

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

Im Fall $\left(\frac{a}{p}\right)=1$ heißt a Quadratischer Rest mod p ($\triangleq$ QR mod p) (s. Def. 8.4)
im Fall $\left(\frac{a}{p}\right)=-1$ heißt a Quadratischer Nichtrest mod p ($\triangleq$ QNR mod p).

Bem: Sei p eine Primzahl, $g \in \mathbb{Z}$. Dann heißt g Primitivwurzel mod p ($\triangleq$ PW mod p), falls $g^0 \pmod p, \dots, g^{p-2} \pmod p$ alle von 0 mod p verschiedenen Restklassen mod p sind. Dann ist $g^{p-1} \equiv g^0 \equiv 1 \pmod p$. Es folgt: $g^i \equiv g^j \pmod p \Leftrightarrow (p-1) \mid (i-j)$.

Satz 1

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

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

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

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

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

(e) Jedes vollständige prime Restsystem mod p enthält genau $\frac{p-1}{2}$ QR mod p, nämlich $g^0, g^2, \dots, g^{p-3} = g^{\frac{p-3}{2} \cdot 2}$ und genau $\frac{p-1}{2}$ QNR mod p, nämlich $g, g^3, g^5, \dots, g^{p-2}$ (Dabei sei g PW mod p).

Beweis

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

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

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

Sei $\left(\frac{a}{p}\right) = 1$, etwa $x_0^2 \equiv a \pmod p$, $x_0 \equiv g^\alpha \pmod p$, so folgt $\operatorname{ind}(a) \equiv 2\alpha \pmod{p-1}$

also $2 \mid \operatorname{ind}(a)$.

(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 §1 (d). Führe eine Fallunterscheidung durch.
1. Fall: $\left(\frac{a}{p}\right) = \frac{b}{p} = -1$. Dann: $a \equiv g^i \pmod p$, $b \equiv g^j \pmod p$, i, j ungerade $\Rightarrow i+j$ gerade, $a \cdot b \equiv g^{i+j} \pmod p$
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

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

Beweis

Sei $\left(\frac{a}{p}\right) = 1$, etwa $x_0^2 \equiv a \pmod p$. Dann folgt $a^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 \pmod p$
(Fermat, §4.6)

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

Es folgt $a^{\frac{p-1}{2}} \equiv \underbrace{g^{(p-1)\alpha}}_{\equiv 1 \pmod p,\ §4.6,\ \text{Fermat}} \cdot g^{\frac{p-1}{2}} \equiv g^{\frac{p-1}{2}} \pmod p$.

Nun ist aber $g^{\frac{p-1}{2}} \equiv -1 \pmod p$, denn nach Fermat ist $g^{\frac{p-1}{2}}$ Lösung von $x^2 - 1 \equiv 0 \pmod p$, also Lösung von $(x-1)(x+1) \equiv 0 \pmod p$.

Satz3 ergibt für $a = -1$

Satz4 (1. Ergänzung zum quadratischen Reziprozitätsgesetz)

Sei $p \neq 2$ eine Primzahl

Dann gilt

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 & \text{falls } p \equiv 1 \pmod 4 \\ -1 & \text{falls } p \equiv 3 \pmod 4. \end{cases}$$

Beweis

Es gilt

$$\left(\frac{-1}{p}\right) \underset{\text{Satz3}}{\equiv} (-1)^{\frac{p-1}{2}} \equiv \begin{cases} 1 & \text{falls } p \equiv 1 \pmod 4 \\ -1 & \text{falls } p \equiv 3 \pmod 4 \end{cases}$$

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

Ferner gilt $1 \not\equiv -1 \pmod p$.

Damit folgt die Beh.

Satz5 (2. Ergänzung zum quadratischen Reziprozitätsgesetz) [ohne Bew]

Sei $p \neq 2$ eine Primzahl.

Dann gilt

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

24. Vortrag:

Das quadratische Reziprozitätsgesetz

Satz 1 (quadratisches Reziprozitätsgesetz)

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

Dann gilt:

$$\left(\frac{2}{p}\right)=\left(\frac{p}{q}\right) \Leftrightarrow p \equiv 1 \pmod 4 \text{ oder } q \equiv 1 \pmod 4.$$

Dabei bezeichne $\left(\frac{q}{p}\right)$ 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 einer 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; $y > 0$; $y \leq \frac{p-1}{2}$ (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) Also ist ν die Anzahl aller Paare (x,y) mit $x \in \{1, \dots, \frac{q-1}{2}\}$, $y \in \{1, \dots, \frac{p-1}{2}\}$ und $-\frac{q}{2} < px - qy < 0$.

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

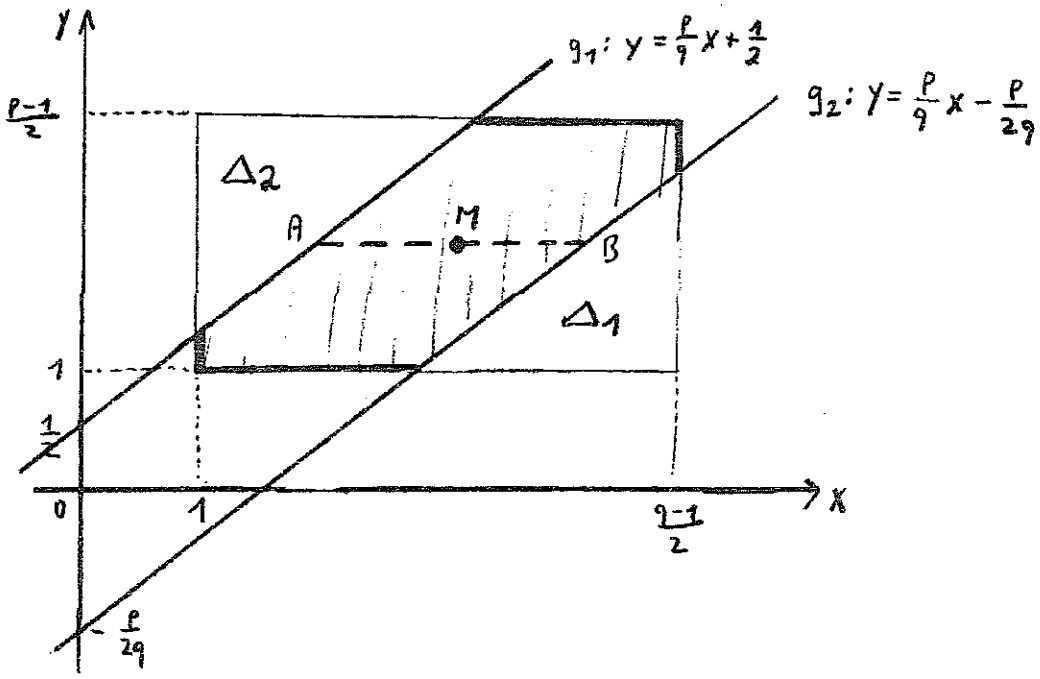
Man beachte, daß $px - qy = 0$ nur möglich ist für $p \mid y$ und $q \mid x$; also ist $px - qy \neq 0$ für alle $x \in \{1, \dots, \frac{q-1}{2}\}$, $y \in \{1, \dots, \frac{p-1}{2}\}$. Dann folgt aus (1) und (2):

$\left(\frac{p}{q}\right) \cdot \left(\frac{q}{p}\right) = (-1)^{\nu + \nu'}$, 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 ausgeführte 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).

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

$$\left(\frac{15}{23}\right) \underset{5.2}{=} \left(\frac{3}{23}\right) \cdot \left(\frac{5}{23}\right) \underset{5.6}{=} -\left(\frac{23}{3}\right) \cdot \left(\frac{23}{5}\right) \underset{5.1(a)}{=} \underbrace{-\left(\frac{2}{3}\right)}_{=-1} \left(\frac{3}{5}\right) \underset{5.6}{=} \left(\frac{5}{3}\right) \underset{5.1(a)}{=} \left(\frac{3}{3}\right) = -1$$

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 (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:

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

Quadratisches Reziprozitätsgesetz

Da gilt $\left(\frac{3}{7}\right)=\left(\frac{5}{9}\right)=-1$, $\left(\frac{2}{7}\right)=1$.
Dies ergibt sich aus den Berechnungen 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 $n_1, n_2 \in \mathbb{N}$ mit $\operatorname{ggT}(n_1,n_2)=1$.
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.
Da 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 Beweis):

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

Darstellung (ohne Beweis):
Sei $n \in \mathbb{N}$ und $a \in \mathbb{Z}$ mit $\operatorname{ggT}(a,n)=1$.
Dann ex. unendlich 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:

$$\lim_{m \to \infty} \frac{\pi^*(m)}{\frac{m}{\varphi(n)}} = \frac{1}{\varphi(n)}$$

(Dirichletscher Primzahlsatz)

Bsp 2 Bestimmung der Lösungen von

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

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 Restklassenring $\mathbb{Z}/131\mathbb{Z}$ 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), bzw. besser durch Verwendung des Euklidischen Algorithmus.

Zu bestimmen sind $s, t \in \mathbb{Z}$ mit $s \cdot 64 + t \cdot 131 = 1$ ($= \operatorname{ggT}(64, 131)$).

Betrachte die Gleichungen

$$131 = 2 \cdot 64 + 3$$
$$64 = 21 \cdot 3 + 1$$
$$3 = 3 \cdot 1 + 0.$$

Es folgt $1 = 64 - 21 \cdot 3 = 64 - 21 \cdot (131 - 2 \cdot 64) = 43 \cdot 64 - 21 \cdot 131$.

Es folgt $64 \cdot 43 \equiv 1 \pmod{131}$.

Multiplikation von (1) mit 43 liefert

(2) $x^2 + \underbrace{2 \cdot 43}_{\equiv -2 \pmod{131}} x + 43 \equiv 0 \pmod{131}$.

2. Schritt: Offenbar besitzen (1) und (2) dieselben Lösungen.

Offenbar ist (2) gleichwertig mit

(3) $(x+1)^2 \equiv -42 \pmod{131}$ (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 $\Leftrightarrow \left(\frac{-42}{131}\right) = 1$ ist.

Nach den Rechengesetzen für das Legendre-Symbol gilt:

$$\left(\frac{-42}{131}\right) = \underbrace{\left(\frac{-1}{131}\right)}_{=1 \text{ (1. Erg.)}} \cdot \underbrace{\left(\frac{2}{131}\right)}_{=-1 \text{ (2. Erg.)}} \cdot \left(\frac{3}{131}\right) \cdot \left(\frac{7}{131}\right) = 1$$

$$= \underset{(QRG)}{-\left(\frac{131}{3}\right)} \cdot -\left(\frac{5}{7}\right) = \underset{(QRG)}{\left(\frac{3}{5}\right)} \cdot \left(\frac{2}{7}\right) = -\left(\frac{2}{3}\right) \cdot -\left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -\left(\frac{5}{3}\right) = 1 \text{ (1. Erg.)}$$

$$= \underset{(QRG)}{-\left(\frac{131}{3}\right)} = -\left(\frac{2}{3}\right) = 1 \text{ (2. Erg.)}$$

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.

25 und 26. Vortrag:

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.: $\forall z_1, z_2 \in \mathbb{Z}[i]: z_1 \cdot z_2 = 0 \Rightarrow z_1 = 0$ 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

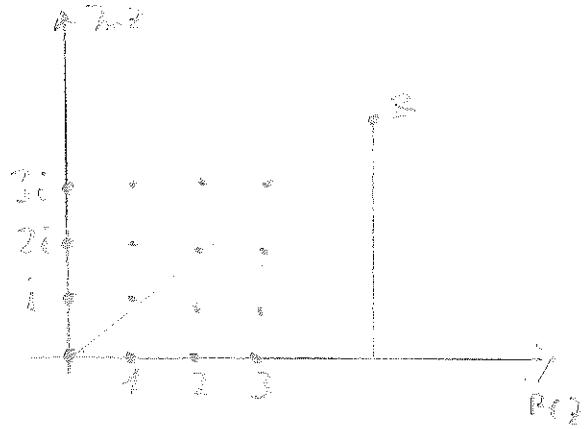
Für $z = a+bi \in \mathbb{C}$ bezeichne $\overline{z} := a-bi$ die zu z konjugiert komplexe Zahl.

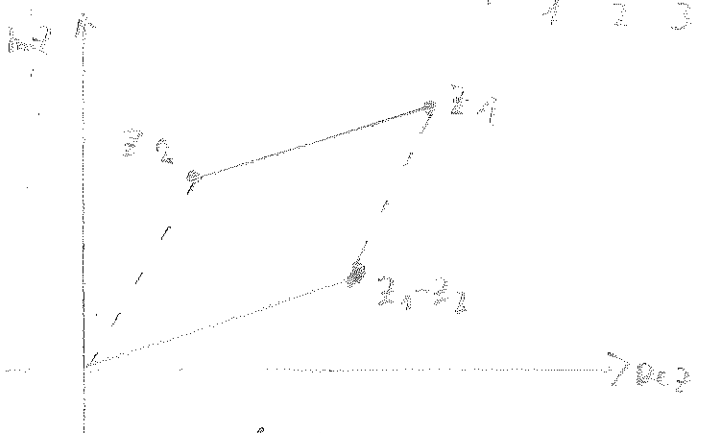
Es läßt sich leicht nachrechnen, daß stets $\overline{z_1+z_2} = \overline{z_1}+\overline{z_2}$ und $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$ gilt. Hieraus folgt sofort $N(z_1 z_2) = N(z_1) N(z_2)$ (multiplikativität der Norm).

Bem 2 Die Elemente von $\mathbb{Z}[i]$ lassen sich als Punkte in der Gaußschen Zahlenebene darstellen.

Dann ist $N(z)$ das Produkt des Abstandes von z zum Nullpunkt (Pythagoras).

Allgemein ist $N(z_1 - z_2)$ das Quadrat des Abstandes der Punkte z_1 und z_2 in der Gaußschen Zahlenebene.





Def 1 Sei $\varepsilon \in \mathbb{Z}[i]$.
Dann heißt ε Einheit von $\mathbb{Z}[i]$, wenn ein $\varepsilon' \in \mathbb{Z}[i]$ existiert mit

$$\varepsilon \cdot \varepsilon' = 1$$

Bsp 1 $1, -1, i$ (besser $i^4 = 1$), $-i$ sind Einheiten von $\mathbb{Z}[i]$

Satz 1 Sei $\varepsilon \in \mathbb{Z}[i]$. Dann gilt:

ε ist Einheit in $\mathbb{Z}[i] \Leftrightarrow N(\varepsilon) = 1$.

Beweis: Die Einheiten von $\mathbb{Z}[i]$ sind also genau $1, -1, i, -i$.

$\Rightarrow$: Sei ε Einheit in $\mathbb{Z}[i]$, dann existiert ein $\varepsilon' = \mathbb{Z}[i]$ mit $\varepsilon \cdot \varepsilon' = 1$.

Nach Satz 1 gilt $1 = N(1) = N(\varepsilon \cdot \varepsilon') = N(\varepsilon) \cdot N(\varepsilon')$

Die Norm einer Elemente aus $\mathbb{Z}[i]$ ist offenbar ≥ 0, eine negative ganze Zahl. Also folgt $N(\varepsilon) = 1$.

$\Leftarrow$: Sei $N(\varepsilon) = \varepsilon \cdot \bar{\varepsilon} = 1$, Offenbar ist dann ε Einheit in $\mathbb{Z}[i]$

Satz 1

Der Ganzheitsring $\mathbb{Z}[i]$ besitzt eine Division mit Rest.
Genauer gilt:
Sind $\alpha, \beta \in \mathbb{Z}[i]$, $\alpha \neq 0$. Dann existieren $\gamma, \delta \in \mathbb{Z}[i]$ mit

$$\beta = \gamma \cdot \alpha + \delta \quad , \quad 0 \leq N(\delta) < N(\alpha).$$

(Also ist $\mathbb{Z}[i]$ ein Euklidischer Ring)

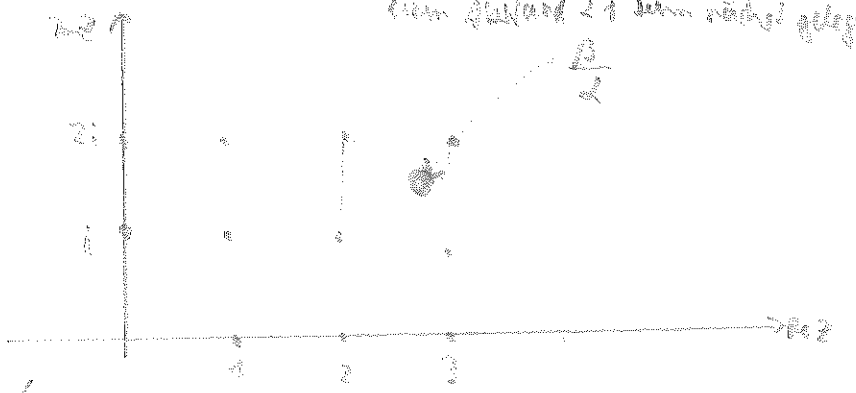
Wegen der Multiplikativität der Norm ist die letzte Bedingung gleichbedeutend mit

$$\frac{\beta}{\alpha} = \gamma + \frac{\delta}{\alpha} \quad , \quad 0 \leq N\left(\frac{\delta}{\alpha}\right) < 1.$$

Dies bedeutet nach Satz 1, daß sich die komplexe Zahl $\frac{\beta}{\alpha}$ approximieren läßt durch eine Zahl aus $\mathbb{Z}[i]$, sodaß der Fehler $\frac{\delta}{\alpha}$ eine Norm < 1 besitzt.

Beweis

Sei $\frac{p}{q} \in \mathbb{C}$ mit $\exists c \in \mathbb{Z}[i]$ so dass $\forall a \in \mathbb{Z}[i]$ $N(\frac{p}{q} - a) < 1$. $N(\frac{p}{q} - c) < 1$ ist gleichbedeutend damit, dass $\frac{p}{q}$ von $\frac{p}{q}$ in der Gaußschen Zahlenebene einen Abstand < 1 besitzt. Offenbar gibt es aber in $\frac{p}{q}$ in der Gaußschen Zahlenebene einen von $\mathbb{Z}[i]$ verschiedenen Gitterpunkt, der in $\frac{p}{q}$ einen Abstand < 1 besitzt! (In Inneren eines Quadrats mit Seitenlänge hat jeder Punkt einen Abstand < 1 zum nächst gelegenen Eckpunkt).



(offenbar ist $\frac{p}{q}$ nicht eindeutig)

Bsp.:

Dividiere $(4+25i)$ durch $(3+4i)$ in $\mathbb{Z}[i]$ mit Rest.

Ergibt $\frac{4+25i}{3+4i} = \frac{(4+25i)(3-4i)}{(3+4i)(3-4i)} = \frac{103+71i}{25}$

Wähle $c = 4+2i$

Dann gilt

$\frac{4+25i}{3+4i} = 7 + \frac{3}{25} - \frac{1}{25}i$, also $4+25i = 7(3+4i) + 1$

(Analog kann man beweisen, daß $\mathbb{Z}[\sqrt{-2}] := \{a+2bi \mid a,b \in \mathbb{Z}\}$ ebenfalls euklidisch 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 $\alpha \in \mathbb{R}$ 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

(*) $\mathbb{Q} \subsetneq \mathbb{Q}(\sqrt{\beta_1}) \subsetneq \mathbb{Q}(\sqrt{\beta_1}, \sqrt{\beta_2}) \subsetneq \cdots \subsetneq \mathbb{Q}(\sqrt{\beta_1}, \ldots, \sqrt{\beta_n})$ 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, Satz 8.5 im Skript: Einf. in die Algebra und Zahlentheorie) gilt

Nach der Körpergradformel (s. Satz 4.1, Skript: Einf. in die Algebra und Zahlentheorie) gilt

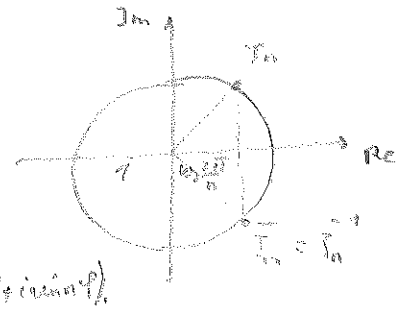
$$[\mathbb{Q}(\sqrt{\beta_1}, \ldots, \sqrt{\beta_n}) : \mathbb{Q}] = 2^n$$

und wegen $\mathbb{Q} \subseteq \mathbb{Q}(\alpha) \subseteq \mathbb{Q}(\sqrt{\beta_1}, \ldots, \sqrt{\beta_n})$ folgt wieder aufgrund der Körpergradformel:

$\exists N$ mit Zirkel und Lineal konstruierbar, so ist $[\mathbb{Q}(\alpha) : \mathbb{Q}]$ Potenz von 2.

Bem 2

Sei $n \in \mathbb{N}$ mit $\zeta_n := \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$.



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 $\zeta_n^i + \zeta_n^{-i} = 2 \operatorname{Re} \zeta_n^i$, speziell also $\zeta_n + \zeta_n^{-1} = 2\cos\frac{2\pi}{n}$.

Es folgt:

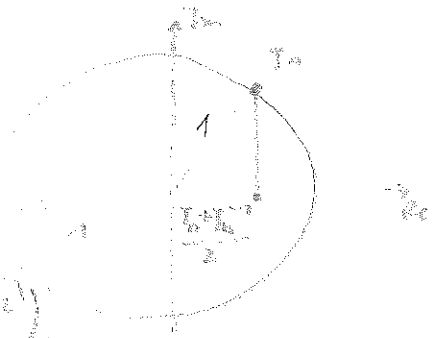
Das regelmäßige n-Eck läßt sich konstruieren mit Zirkel und Lineal gdw sich $\zeta_n + \zeta_n^{-1} = 2\cos\frac{2\pi}{n}$ mit Zirkel und Lineal konstruieren läßt.

Bem 3 $\zeta_n \in \mathbb{C}$, $n \geq 2$.

(i) Dann gilt $[\mathbb{Q}(\zeta_n) : \mathbb{Q}(\zeta_n + \zeta_n^{-1})] = 2$

(ii) Es gilt $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) = \mathbb{Q}(\zeta_n) \cap \mathbb{R}$

Beweis (i)



Es gilt $\zeta_n = \underbrace{\frac{\operatorname{Re}\zeta_n}{\zeta_n + \zeta_n^{-1}}}_{= \zeta_n + \zeta_n^{-1}} + i\sqrt{1 - (\operatorname{Re}\zeta_n)^2}$,

also $\mathbb{Q}(\zeta_n) = \mathbb{Q}(\zeta_n + \zeta_n^{-1}, i) = \mathbb{Q}(\zeta_n + \zeta_n^{-1}, \sqrt{1 - (\operatorname{Re}\zeta_n)^2})$.

Da $i\sqrt{1-(\operatorname{Re}\zeta_n)^2}$ Nullstelle von $x^2 + 1 - (\operatorname{Re}\zeta_n)^2 \in \mathbb{Q}(\zeta_n + \zeta_n^{-1})[X]$ 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 $\mathbb{Q}(\zeta_n) \neq \mathbb{Q}(\zeta_n + \zeta_n^{-1})$

Insgesamt folgt die Behauptung.

(ii) Offenbar enthält $\mathbb{Q}(\zeta_n + \zeta_n^{-1})$ nur reelle Zahlen, also ist $\mathbb{Q}(\zeta_n + \zeta_n^{-1}) \subseteq \mathbb{Q}(\zeta_n) \cap \mathbb{R} \subsetneq \mathbb{Q}(\zeta_n)$.
Offenbar enthält $\mathbb{Q}(\zeta_n)$ nicht nur reelle Zahlen, also ist $\mathbb{Q}(\zeta_n) \cap \mathbb{R} \neq \mathbb{Q}(\zeta_n)$.

Bem 4

(i) Sei p eine Primzahl. Dann ist $\Phi_p(\zeta_p, \mathbb{Q}) = x^{p-1} + x^{p-2} + \dots + x + 1$. (zur Def. v. $\Phi_p(\zeta_p, \mathbb{Q})$ s. Bem 4.6, Kap. 04 im Skript: Einf. in die Algebra und Zahlentheorie)

(ii) Für $n \in \mathbb{N}$ läßt sich $\Phi_n(\zeta_n, \mathbb{Q})$ nicht explizit angeben. Es gilt aber

$$\operatorname{grad} \Phi_n(\zeta_n, \mathbb{Q}) = \underbrace{p_1^{a_1 - 1} \cdots p_r^{a_r - 1}(p_1 - 1) \cdots (p_r - 1)}_{= \varphi(n)}, \text{ wobei}$$

$n = p_1^{a_1} \cdots p_r^{a_r}$ (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. Satz 3.1; Kap. 04 im Skript Einführung in die Algebra und Zahlentheorie).

Damit folgt die Behauptung.

Bem 5 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 $3\ (= 2^1 + 1)$, $5\ (= 2^2 + 1)$, $17 (= 2^{2^2} + 1)$, $257\ (= 2^{2^3})$, $65537\ (= 2^{2^4})$ Fermatsche Primzahlen.

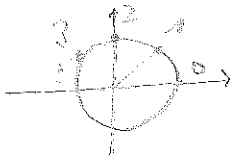
$2^{2^5} + 1$ ist keine (Fermatsche) Primzahl.

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 $2^m + 1 = (2^s + 1)(\underbrace{2^{s(r-1)} - 2^{s(r-2)} \pm \dots - 2^s + 1}_{r \text{ Summanden}})$.

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 ist $m \mid n$, 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' mit der Ecke $2m'$
usw.



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 in 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:

$[\mathbb{Q}(T_p + T_p^{-1}) : \mathbb{Q}]$ ist Potenz von 2.

wegen Bem 3 und der Körpergradformel ist dann

$[\mathbb{Q}(T_p) : \mathbb{Q}]$ Potenz von 2.

Bekanntlich ist $[\mathbb{Q}(T_p) : \mathbb{Q}] = \operatorname{grad}_{\mathbb{Q}}(T_p, \mathbb{Q})$ (s. Satz 4.10, Folie 85 im Skript: Einf. in die Algebra und Zahlentheorie)

Nach Bem 4 (i) folgt $[\mathbb{Q}(T_p) : \mathbb{Q}] = p - 1$.

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 2 (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.

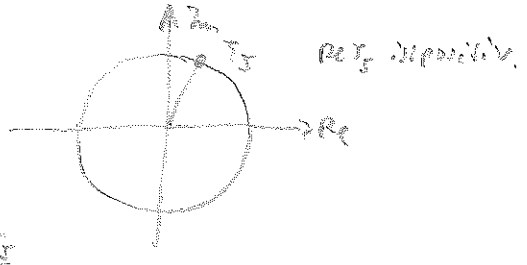
Bew

(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 $[\mathbb{Q}(\zeta_p) : \mathbb{Q}]$ Potenz von 2. wegen $\operatorname{grad}_{\mathbb{Q}}(\zeta_p, \mathbb{Q}) = \Gamma(\mathbb{Q}(\zeta_p) : \mathbb{Q})$ 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, benutze Bem 2 und $\zeta_5^5 = 1$ sowie
$\zeta_5^4 + \zeta_5^3 + \zeta_5^2 + \zeta_5 + 1 = 0$ (nach Bem 4(i))



$X^2 + X - 1$ 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?

9. und 10. Vorlesung: 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 $a = a^{-1}$, $b = b^{-1}$ □

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 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 $(aU)^2 = a^2U = U$ nach den Rechenregeln in der Faktorgruppe.

Also folgt $a^pU = (aU)^p = aU$; 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 $|G| = p$ ist, folgt $G = \{e, g, \dots, g^{p-1}\}$;
insbesondere ist G auch kommutativ.

31 und 32. Vortrag – Gruppen der Ordnung p^2

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 zeigt: $\sim$ def. eine 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: $x g x^{-1} = y g y^{-1} \Leftrightarrow y^{-1} x g \underbrace{x^{-1} y}_{=(y^{-1}x)^{-1}} = g \Leftrightarrow y^{-1}x \in N_g \Leftrightarrow yN_g = xN_g$. □

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 $Z := \{x \in G \mid gx = xg \text{ f.a. } g \in G\}$ ist eine Untergruppe von G.
(iii) $\{e\} \subsetneq Z$.

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) $\#[g] = 1 \Leftrightarrow xgx^{-1} = g$ 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: $Z \subsetneq N_g \subsetneq G$.

Beweis $Z \subsetneq N_g$: $Z \subseteq N_g$ 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
$N_g \subsetneq G$: $N_g = G \Leftrightarrow xgx^{-1} = g$ 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 eine Gruppe der Ordnung p^2, die nicht abelsch ist. Sei Z das Zentrum von G.
Dann gilt $Z \subsetneq G$.
Also ex. ein $g \in G$ mit $g \notin Z$. Es sei N_g der Normalisator von g.
Es folgt

$$\{e\} \underset{\text{Bem 2 (iii)}}{\subsetneq} Z \subsetneq \underset{\text{Bem 3}}{N_g} \quad (*)$$

Alle 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 $N_g \subsetneq G$.
Dies ist ein Widerspruch.