Elementare Zahlentheorie (Version 2)

(Winter Semester, 2005-6)

1 Einführung

Literatur

1. *An Introduction to the Theory of Numbers*, Oxford University Press, von Hardy und Wright.
2. *A Classical Introduction to Modern Number Theory*, Springer Verlag, von Ireland und Rosen.
3. *Seminumerical Algorithms*, Addison Wesley, von D. Knuth.
4. Skript zu dieser Vorlesung im Internet.

1.1 Einige bekannte Ergebnisse und Vermutungen

- Fermat's Großer Satz: Es existeren keine natürlichen Zahlen $a, b, c \in \mathbb{N}$, $n > 2$ mit $a^n + b^n = c^n$.
- Goldbach's Vermutung: Sei $n > 3$ eine gerade Zahl. Dann existieren zwei Primzahlen p_1 und p_2 mit $n = p_1 + p_2$.

  (Es gilt auf jeden Fall: Satz (Chen 1975): $\exists p_1, p_2, p_3$ mit $n = p_1 + p_2 \cdot p_3$, vorausgesetzt n sei 'hinreichend groß'.)
- Für jedes $n \in \mathbb{N}$ sei $\pi(n)$ die Anzahl der Primzahlen nicht größer als n. z.B.

  $\pi(20) = 8$ — d.h. die Zahlen: $2, 3, 5, 7, 11, 13, 17, 19$

  $\pi(1) = 0$, u.s.w...

  Der Primzahlsatz (Hadamard und de la Vallée Poussin 1896): Es gilt

  $$\pi(n) \sim \frac{n}{\log n}$$

  d.h.

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

  Aber auch (Dirichlet 1837): Sei $m > 1$ und $0 < a < m$ mit $\mathrm{ggt}(a, m) = 1$ (d.h. der größte gemeinsame Teiler). Dann gibt es unendlich viele Primzahlen p mit $p = a \bmod m$.
- Sei $\pi = 3,14159\ldots$. Dann gibt es kein nicht-triviales Polynom mit Integerkoeffizienten

  $$P(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

  mit $P(\pi) = 0$. Mit anderen Worten: π ist *transzendent* (d.h. nicht *algebraisch*). Auch

  $$e = 1 + 1 + \frac{1}{2!} + \frac{1}{3!} + \cdots = \exp(1)$$

  ist transzendent. (Auch e^α ist transzendent, falls α algebraisch.) Aber niemand weiß, ob etwa π^e oder 2^e oder sogar $\pi + e$ algebraisch oder transzendent sind. (Es ist jedenfalls bekannt, daß etwa die Zahlen e^π, $e \cdot \pi$, $2^{\sqrt{2}}$ irrational sind.)
- Sei $n \in \mathbb{N}$. Ist n eine Primzahl? Falls nicht, wieviele Rechenschritte würde ein Computer brauchen, um einen Primfaktor $p|n$ zu finden? Sicherlich weniger als $\sqrt{n}$. D.h. die Anzahl der Rechenschritte ist $O(\sqrt{n})$. Aber auch (Dixon 1978): ein Algorithmus existiert mit $O(n^{\sqrt{8 \log\log n / \log n}})$.

Zur Notation:
$\mathbb{N}$ = die natürlichen Zahlen: $1, 2, 3, \ldots$
$\mathbb{N}_0$ = die natürlichen Zahlen, wobei auch die '0' vorkommen darf.
$\mathbb{Z}$ = die Integerzahlen.
$\mathbb{Q}$ = die rationalen Zahlen.
$\mathbb{R}$ = die reellen Zahlen.
$\mathbb{C}$ = die komplexen Zahlen.

2 Die Approximation von irrationalen Zahlen durch rationalen Zahlen

Bekanntlich ist

$$\pi \approx \frac{22}{7} = 3,14285714285714\ldots.$$

Aber $\pi = 3,141592653589\ldots$. D.h. $\frac{22}{7} - \pi < 0,0013$. Dies ist eine *viel* kleinere Zahl als $\frac{1}{7} = 0,142857142857\ldots$.

Noch viel besser ist

$$\pi \approx \frac{355}{113} = 3,1415929204\ldots.$$

Hier ist $\frac{355}{113} - \pi < 0,0000003$. Dies ist sogar eine sehr, sehr viel keinere Zahl als $\frac{1}{113}$! Wie findet man solche gute Approximationen?

Definition 2.1. Seien $a, b \in \mathbb{N}$. Der größte gemeinsame Teiler von a und b, $\mathrm{ggt}(a, b)$ ist die größte Zahl $c \in \mathbb{N}$ mit $c|a$ und $c|b$. (D.h. $\exists\ d \in \mathbb{N}$ mit $c \cdot d = a$, u.s.w.)

Satz 1. *Seien* $a, b \in \mathbb{N}$ *und* $c = ggt(a, b) \Rightarrow \exists d, e \in \mathbb{Z}$ *mit*

$$a \cdot d + b \cdot e = c.$$

Beweis: siehe 'Lineare Algebra I'. Aber auch ...

Definition 2.2. Sei $S \subseteq \mathbb{Z}$, wobei für alle $x, y \in S$ gilt $x + y \in S$ und $x - y \in S$. Dann heißt S ein 'Modulus'. Die Zahl 0 alleine ist der triviale Modulus.

Z.B. $S = \{a \cdot u + b \cdot v : u, v \in \mathbb{Z}\}$ ist offensichtlich ein Modulus für alle $a, b \in \mathbb{N}$.

Satz 2. *Sei* $S \neq \emptyset$ *irgendein nicht trivialer Modulus. Dann existiert ein* $d \in \mathbb{N}$ *mit* $S = \{w \cdot d : w \in \mathbb{Z}\}$.

Beweis. $S \cap \mathbb{N} \neq \emptyset$ ist klar. Sei daher d die kleinste Zahl in $S \cap \mathbb{N}$. Dann ist $\{w \cdot d : w \in \mathbb{Z}\} \subseteq S$. Dies folgt, da d, $d + d = 2d$, $d - 2d = -d$, u.s.w. in S sind. Kann es sein, daß $S \neq \{w \cdot d : w \in \mathbb{Z}\}$? Sei $n \in S - \{w \cdot d : w \in \mathbb{Z}\}$. Sei etwa $n = q \cdot d + r$, wobei $q \in \mathbb{Z}$ und $0 < r < d$. Aber dann ist $n - q \cdot d = r \in S \cap \{w \cdot d : w \in \mathbb{Z}\}$; ein Widerspruch, da $r < d$. □

Daher sei

$$S = \{a \cdot u + b \cdot v : u, v \in \mathbb{Z}\} = \{w \cdot d : w \in \mathbb{Z}\}.$$

Dann existieren $s, t \in \mathbb{Z}$ mit $a \cdot s + b \cdot t = d$. Behauptung: $d = \mathrm{ggt}(a, b)$, denn

1. $d|a$ und $d|b$, da $a, b \in S$.
2. Angenommen $d' > d$ mit $d'|a$ und $d'|b \Rightarrow$ für alle $u, v \in \mathbb{Z}$ gilt $d'|a \cdot u + b \cdot v$. D.h. insbesondere $d'|d$; ein Widerspruch.

Definition 2.3. Sei $n \in \mathbb{N}$. Die Farey Zahlen der Ordnung n sind die Bruchzahlen $\frac{a}{b}$ mit $0 < b \leq n$, $a \in \mathbb{Z}$ und $\mathrm{ggt}(a, b) = 1$.

Sei $\mathcal{F}_n$ die Menge aller solcher Zahlen. Z.B. die Zahlen in $\mathcal{F}_5$ zwischen 0 und 1 sind:

$$\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}.$$

Satz 3. *Sei $x \in \mathbb{R}$ irgendeine reelle Zahl und sei $n \in \mathbb{N}$. Dann existiert ein*

$$\frac{h}{k} \in \mathcal{F}_n$$

mit

$$\left| x - \frac{h}{k} \right| < \frac{1}{k \cdot n}.$$

Beweis. (nach Dirichlet): Für jede reelle Zahl $y \in \mathbb{R}$ definieren wir $[y]$ als die größte Integerzahl, die kleiner oder gleich y ist. (Z.B. $[\pi] = 3$, $[3/4] = 0$, u.s.w.) Sei dann auch $(y) = y - [y]$. Daher ist stets $(y) \in [0, 1)$ für alle $y \in \mathbb{R}$. Es gibt offensichtlich $n + 1$ Zahlen der Art $(0), (x), (2x), \ldots, (nx)$ in diesem Intervall. Andererseits gibt es n Intervalle

$$\left[0, \frac{1}{n}\right), \left[\frac{1}{n}, \frac{2}{n}\right), \ldots, \left[\frac{n-1}{n}, \frac{n}{n}\right).$$

Daher gibt es mindestens zwei Punkte in einem Intervall, etwa (ix) und (jx) mit $0 \leq i < j \leq n$ und

$$|(jx) - (ix)| < \frac{1}{n}.$$

Sei $k = j - i$. Dann ist $0 \leq k \leq n$, und es gilt

$$\begin{aligned} |(jx) - (ix)| &= |jx - [jx] - ix + [ix]| \\ &= |jx - ix - h| \\ &= |kx - h| < \frac{1}{n} \end{aligned}$$

wobei $h = [jx] - [ix] \in \mathbb{Z}$. D.h.

$$\frac{1}{k} \cdot |kx - h| < \frac{1}{l \cdot n}$$

oder

$$\left| x - \frac{h}{k} \right| < \frac{1}{k \cdot n}$$

□

Man sieht daher: es ist immer möglich, reelle Zahlen 'gut' durch Farey Zahlen zu approximieren. Aber wie können wir die bestmögliche Approximation finden?

Satz 4. *Seien $\frac{h}{k}$ und $\frac{h'}{k'}$ zwei direkt nacheinanderfolgende Zahlen in $\mathcal{F}_n$. Dann gilt*

$$kh' - hk' = 1.$$

Beweis. Da $\mathrm{ggt}(h, k) = 1$, gibt es $x, y \in \mathbb{Z}$ mit $kx - hy = 1$ (Satz 1). Aber

$$kx - hy = k(x + rh) - h(y + rk) = 1$$

für alle $r \in \mathbb{Z}$. Wähle insbesondere r so, daß

$$n - k < y + rk \leq n.$$

Sei $y_0 = y + rk$. D.h. $0 \leq n - k < y_0 \leq n$. Sei $x_0 = x + rh$. Dann ist $\frac{x_0}{y_0} \in \mathcal{F}_n$, da ja $y_0 \leq n$. Wir haben $kx_0 - hy_0 = 1$, daher

$$\frac{x_0}{y_0} = \frac{h}{k} + \frac{1}{y_0 k} > \frac{h}{k}.$$

Folglich

$$\frac{x_0}{y_0} > \frac{h}{k}$$

in $\mathcal{F}_n$. Ist $\frac{x_0}{y_0}$ der direkte Nachfolger von $\frac{h}{k}$? Falls nicht, sei etwa $\frac{h'}{k'}$ der direkte Nachfolger mit

$$\frac{h}{k} < \frac{h'}{k'} < \frac{x_0}{y_0}.$$

Wir haben

$$\frac{x_0}{y_0} - \frac{h'}{k'} = \frac{k'x_0 - h'y_0}{y_0k'} \geq \frac{1}{y_0k'}$$

(da sonst $\frac{x_0}{y_0} = \frac{h'}{k'}$). Aber auch

$$\frac{h'}{k'} - \frac{h}{k} = \frac{kh' - hk'}{k'k} \geq \frac{1}{k'k}$$

Daher

$$\begin{aligned}
\frac{1}{y_0k} &= \frac{kx_0 - hy_0}{y_0k} \\
&= \frac{x_0}{y_0} - \frac{h}{k} \\
&\geq \frac{1}{y_0k'} + \frac{1}{k'k} \\
&= \frac{k + y_0}{kk'y_0} \\
&> \frac{n}{kk'y_0} \quad (\text{da: } n - k < y_0 \leq n, \text{ d.h. } n < k + y_0) \\
&\geq \frac{1}{ky_0} \quad (\text{da } n \geq k')
\end{aligned}$$

Insgesamt: $\frac{1}{ky_0} > \frac{1}{ky_0}$, ein Widerspruch. □

Satz 5. *Seien $\frac{h}{k}$, $\frac{h''}{k''}$, $\frac{h'}{k'}$ drei direkt nacheinander folgende Zahlen in $\mathcal{F}_n$. Dann gilt*

$$\frac{h''}{k''} = \frac{h + h'}{k + k'}.$$

Beweis. Nach Satz 4 gilt

$$\begin{aligned}
kh'' - hk'' &= 1 \\
k''h' - h''k' &= 1
\end{aligned}$$

Multipliziere die Gleichungen mit h' und h, bzw. k' und k, und wir erhalten die Gleichung

$$\begin{aligned}
h + h' &= h(k''h' - h''k') + h'(kh'' - hk'') \\
&= h''(h'k - hk') + \underbrace{hk''h' - h'hk''}_{0}
\end{aligned}$$

auch

$$\begin{aligned}
k + k' &= k(k''h' - h''k') + k'(kh'' - hk'') \\
&= k''(h'k - hk') + \underbrace{k'kh'' - kh''hk'}_{0}
\end{aligned}$$

$$\Rightarrow \frac{h + h'}{k + k'} = \frac{h''}{k''}$$

Da $\frac{h}{k} \neq \frac{h'}{k'}$, d.h. $h'k - hk' \neq 0$. □

Korollar 5.1. *Seien $\frac{h}{k}$, $\frac{h'}{k'}$ direkt nacheinander folgende Zahlen in $\mathcal{F}_n$. Dann ist $k + k' > n$.*

Beweis. Sonst wäre $\frac{h+h'}{k+k'}$ dazwischen. □

2.1 Bemerkungen über Kettenbruchzahlen

Eine Bruchzahl der Art

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{\cdots + \cfrac{1}{a_n}}}}}$$

mit $a_0 \in \mathbb{Z}$ und $a_i \in \mathbb{N}$ für $i = 1, \ldots, n$ heißt eine einfache, endliche Kettenbruchzahl. Jede rationale Zahl kann als einfache endliche Kettenbruchzahl dargestellt werden (und natürlich auch umgekehrt). Einfachheitshalber schreibt man auch

$$x = a_0 + \frac{1}{a_1+}\ \frac{1}{a_2+} \cdots \frac{1}{a_n}.$$

Noch einfacher ist die Notation

$$x = [a_0, a_1, \ldots, a_n].$$

Eine (unendliche) Kettenbruchzahl ist dann eine Zahl der Art

$$y = [a_0, a_1, \ldots] = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{a_3 + \cfrac{1}{a_4 + \cdots}}}}$$

wobei wieder $a_0 \in \mathbb{Z}$ und $a_i \in \mathbb{N}$ für $i > 0$. Zum Beispiel:

$$\sqrt{2} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{2 + \cdots}}} = [1, 2, 2, \ldots] = [1, \overline{2}].$$

Sei

$$\begin{aligned} y_0 &= [a_0] = a_0, \\ y_1 &= [a_0, a_1] = \frac{a_1 a_0 + 1}{a_1}, \\ y_2 &= [a_0, a_1, a_2] = \frac{a_2 a_1 a_0 + a_2 + a_0}{a_2 a_1 + 1}, \quad \ldots \quad \text{u.s.w.} \end{aligned}$$

Dann konvergiert die Folge y_n gegen eine irrationale Zahl y. Es gilt: für alle $m \in \mathbb{N}$ ist

$$y_{2(m-1)} < y_{2m} < y < y_{2m+1} < y_{2(m-1)+1}.$$

Noch mehr: sei $y_n = \frac{p_n}{q_n}$, etwa. Dann gilt

$$y_{2m+1} - y_{2m} < \frac{1}{q_n q_{n+1}}.$$

Insbesondere ist $y_n \in \mathcal{F}_{q_n}$ näher als jede andere Zahl in $\mathcal{F}_{q_n}$ zu y. Dies folgt, da benachbarte Farey Zahlen der Ordnug n mindestens

$$\frac{1}{n-1} - \frac{1}{n} = \frac{1}{n(n-1)} > \frac{1}{n^2}$$

auseinander liegen. (Siehe Hardy und Wright (Kapitel X) für die entsprechenden Beweise.)

2.2 Der Satz von Liouville

Definition 2.4. Sei $\zeta \in \mathbb{R}$ eine beliebige reelle Zahl. Die Zahl ζ wird durch Bruchzahlen zur 'Ordnung n' approximiert, falls eine Konstante $K(\zeta)$ existiert, mit

$$\left|\frac{h}{k} - \zeta\right| < \frac{K(\zeta)}{k^n}$$

für unendlich viele verschiedene Bruchzahlen $\frac{h}{k}$ mit $\mathrm{ggt}(h,k) = 1$.

Bemerkung. *Nach Satz 3 läßt sich* jede *irrationale Zahl durch Bruchzahlen zur Ordnung 2 approximieren.*

Definition 2.5. Eine (komplexe) Zahl $w \in \mathbb{C}$ heißt eine 'algebraische Zahl' der Ordnung n, falls ein Polynom

$$P(x) = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Q}[x]$$

($a_i \in \mathbb{Q}$ für alle i, und $a_n \neq 0$) existiert, mit $P(w) = 0$. Falls $a_i \in \mathbb{Z}$ für alle i und $a_n = 1$, dann heißt w eine algebraische Integerzahl.

(Offensichtlich ist $r \in \mathbb{Q}$ eine algebraische Integerzahl $\Leftrightarrow r \in \mathbb{Z}$.)

Satz 6 (Liouville 1851). *Sei $\zeta \in \mathbb{R}$ eine reelle, irrationale algebraische Zahl der Ordnung n. D.h.*

$$P(\zeta) = a_n \zeta^n + \cdots + a_1 \zeta + a_0 = 0,$$

wobei $a_i \in \mathbb{Q}$ und $a_n \neq 0$. Dann gibt es kein $m > n$, so daß ζ durch Bruchzahlen zur Ordnung m approximiert werden kann.

Beweis. Die reelle Funktion

$$f(x) = \sum_{i=0}^{n} a_i x^i$$

ist beliebig oft stetig differenzierbar. Das Intervall $[\zeta-1, \zeta+1]$ ist kompakt. Folglich ist $f'([\zeta-1, \zeta+1]) \subset \mathbb{R}$ kompakt und daher gibt es eine feste Zahl $0 < M \in \mathbb{R}$ mit $|f'(x)| < M$ für alle $x \in [\zeta-1, \zeta+1]$. D.h.

$$\frac{1}{|f'(x)|} > \frac{1}{M}.$$

Ein Polynom vom Grad n hat höchstens n verschiedene Nullstellen. Sei $\Delta > 0$ der Abstand von ζ zur nächsten Nullstelle oder die Zahl 1, falls keine andere Nullstelle existiert. Sei $\epsilon = \min\{\Delta/2, 1\}$. Sei nun $\frac{a}{b}$ eine Bruchzahl, die ζ approximiert mit $|\frac{a}{b} - \zeta| < \epsilon$. Nun, $\zeta \neq \frac{a}{b}$, da ζ eine irrationale Zahl ist, und folglich ist $f(\frac{a}{b}) \neq 0$. Es gilt sogar

$$\begin{aligned} \left|f\left(\frac{a}{b}\right)\right| &= \left|a_n \left(\frac{a}{b}\right)^n + \cdots + a_1 \left(\frac{a}{b}\right) + a_0\right| \\ &= \left|\frac{a_n a^n + \cdots + a_1 a b^{n-1} + a_0 b^n}{b^n}\right| \\ &\geq \frac{1}{b^n}. \end{aligned}$$

Die letzte Ungleichung gilt, da $|a_n a^n + \cdots + a_1 a b^{n-1} + a_0 b^n|$ eine Integerzahl ungleich Null sein muß.

Nach dem Mittelwertsatz der Analysis gibt es ein x zwischen $\frac{a}{b}$ und ζ mit

$$f\left(\frac{a}{b}\right) = f\left(\frac{a}{b}\right) - \underbrace{f(\zeta)}_{0} = \left(\frac{a}{b} - \zeta\right) f'(x).$$

Folglich ist $f'(x) \neq 0$. Aber

$$\left|\frac{a}{b} - \zeta\right| = \left|\frac{f\left(\frac{a}{b}\right)}{f'(x)}\right| > \frac{1}{Mb^n}.$$

D.h. ζ kann nicht zur Ordnung höher als n approximiert werden, da sonst unendlich viele solche Bruchzahlen auch näher als ϵ zu ζ wären. □

Bemerkung. *Nach Roth (1955) gibt es* keine *algebraische Zahl, die zur Ordnung > 2 approximiert werden kann.*

3 Die Primzahlen

Definition 3.1. Eine Zahl $p \in \mathbb{N}$, $p > 1$ ist 'prim', falls für alle a, $b \in \mathbb{N}$ mit $p|ab$ stets entweder $p|a$ oder $p|b$ gilt.

$$\mathfrak{P} = \{2, 3, 5, 7, 13, 17, 19, 23, \dots\}$$

ist die Menge der Primzahlen.

Satz 7. *Folglich ist* $\mathrm{ggt}(a, p) = 1$ *für alle* $a \in \mathbb{N}$ *mit* $1 \leq a < p \in \mathfrak{P}$.

Beweis. Sonst wäre etwa $p > \mathrm{ggt}(a, p) = b > 1$. Insbesondere $b|p$. D.h. $p = bd$ etwa, wobei auch $1 < d < p$. Aber dann wäre sowohl $p \not| b$ als auch $p \not| d$. □

Satz 8. *[Fundamentalsatz der Arithmetik] Sei* $1 < n \in \mathbb{N}$. *Dann existieren* $p_1, \dots, p_m \in \mathfrak{P}$ *mit* $n = p_1 \cdots p_m$, *und diese Darstellung ist eineindeutig.*

Beweis. Falls $n \notin \mathfrak{P}$, dann ist etwa $n = ab$, mit $1 < a, b < n$, u.s.w.[1] Eine Induktion führt zur Faktorisierung in Primzahlen. Angenommen nun zwei <u>verschiedene</u> Primfaktorisierungen

$$n = p_1 \cdots p_m = q_1 \cdots q_l$$

existieren. Sei dann n die kleinste Zahl mit einer zweideutigen Primfaktorisierung. Offensichtlich ist $p_i \neq q_j$ für alle möglichen i und j. Aber

$$p_1 | n = q_1 \cdot (q_2 \cdots q_l).$$

Da q_1 prim ist, ist $p_1 \not| q_1$ daher $p_1 | q_2 \cdots q_l$. u.s.w. Letztendes muß $p_1 | q_i$; aber dies ist auch unmöglich: ein Widerspruch. □

Satz 9 (Euklid). $\mathfrak{P}$ *ist unendlich groß.*

Beweis. Sei sonst etwa $\mathfrak{P} = \{p_1, \dots, p_n\}$, und sei $m = p_1 \cdots p_n + 1$. Dann ist $p_i \not| m$ für alle $i = 1, \dots, n$, im Widerspruch zu Satz 8. □

Nicht ganz so trivial ist der folgende Satz.

Satz 10. *Sei* $\mathfrak{P} = \{p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11, \dots\}$ *die Menge der Primzahlen. Dann ist die Reihe*

$$\sum_{i=1}^{\infty} \frac{1}{p_i}$$

<u>nicht</u> konvergent.

Beweis. Für $j \in \mathbb{N}$ sei

$$\mathfrak{P}_j = \{p_1 = 2, p_2 = 3, \dots, p_j\}.$$

Für jedes $x \in \mathbb{N}$ sei dann $N(x)$ die Anzahl der $n \leq x$ in $\mathbb{N}$ mit $p \not| n$ für alle $p \notin \mathfrak{P}_j$. (D.h. alle Primfaktoren von n sind nicht größer als p_j.) Wie groß ist $N(x)$?

Sei $n \leq x$. Schreibe $n = m \cdot n_1^2$, wobei m quadratfrei ist. D.h.

$$m = p_1^{b_1} p_2^{b_2} \cdots p_j^{b_j}, \qquad b_i = 0 \text{ oder } 1.$$

Offensichtlich gibt es höchstens 2^j solche m. Auch muß $n_1 \leq \sqrt{n} \leq \sqrt{x}$. D.h. $N(x) \leq 2^j \cdot \sqrt{x}$.

<u>Andererseits</u>, falls $\sum \frac{1}{p_i}$ konvergiert, dann sei $j \in \mathbb{N}$ so groß, daß

$$\sum_{i=j+1}^{\infty} \frac{1}{p_i} < \frac{1}{2}.$$

[1] Sei etwa $n|cd$, wobei $n \not| c$ und $n \not| d$ (und $c, d > 1$). Sei $k = \mathrm{ggt}(n, c)$. Dann ist $1 < k < n$ und $k|n$. (Warum $1 < k$? Sonst gäbe es Integerzahlen x, y mit $xn + yc = xcd + yc = 1$. Oder $xd + y = 1/c$. Unmöglich, da $c > 1$ und $xd + y \in \mathbb{N}$.)

Sei jetzt x die besondere Zahl $x = 2^{2j+2}$. Nehme irgendeine Primzahl p_i mit $i > j$. Es gibt höchstens x/p_i Zahlen n, die kleiner oder gleich x sind, mit $p_i | n$. Nun, $x - N(x)$ ist die Anzahl der Zahlen, die kleiner oder gleich x sind, und die durch eine Primzahl größer als p_j teilbar sind. D.h.

$$x - N(x) \leq \sum_{i=j+1}^{\infty} \frac{x}{p_i} < \frac{1}{2}x$$

$$\Rightarrow \qquad \frac{1}{2}x < N(x)$$

$$\Rightarrow \qquad \frac{1}{2}x < 2^j\sqrt{x}.$$

Aber $x = 2^{2j+2}$. D.h. $2^{2j+1} < 2^j \cdot 2^{j+1} = 2^{2j+1}$; ein Widerspruch. □

Es gilt aber doch:

Satz 11 (Brun 1919). *Sei $\mathfrak{P}_{Zwillinge}$ die Menge der 'Primzwillinge'. Dann ist die Reihe*

$$\sum_{p \in \mathfrak{P}_{Zwillinge}} \frac{1}{p}$$

konvergent.

Beweis. Auch relativ elementar, aber zu zeitaufwendig für diese Vorlesung. □

3.1 Der Satz von Tschebyscheff

Sei $\pi(n)$ die Anzahl der Primzahlen, die nicht größer als n sind. Der Primzahlsatz lautet dann

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

Dieser Satz ist erst im Jahre 1896 bewiesen worden mit einem 'komplizierten' Beweis. (Verschiedene Ideen aus der Funktionentheorie werden verwendet.) Selbert (1948) hat dann einen 'elementaren' (aber auch ziemlich komplizierten) Beweis gefunden. Aber schon im Jahre 1852 hat Tschebyscheff einen etwas schwächeren Satz bewiesen, den wir nachvollziehen werden.

Satz 12 (Tschebyscheff). *Es existieren Konstanten $C_1 < C_2$ mit*

$$C_1 \cdot \frac{n}{\log n} < \pi(n) < C_2 \cdot \frac{n}{\log n}$$

für alle $n \in \mathbb{N}$.

Zuerst einige Vorergebnisse:

1. Welche Eigenschaften hat die 'log' Funktion? Seien a, b und c positive reelle Zahlen, mit $a^b = c$. Dann gilt $b \cdot \log a = \log c$. Außerdem gilt

   $$\log(\prod_{i=1}^{n} a_i) = \sum_{i=1}^{n} \log(a_i),$$

   wobei $a_i > 0$ für $i = 1, \ldots, n$.

2. Seien $m \leq n$ positive Integerzahlen. Dann ist

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

   stets eine Integerzahl.

3. Für x eine reelle Zahl, sei $\lceil x \rceil$ die größte Integerzahl, die kleiner oder gleich x ist. Sei $n \in \mathbb{N}$ und sei $p \in \mathfrak{P}$. Dann gibt es $\lceil \frac{n}{p} \rceil$ Zahlen in der Menge $\{1, 2, \ldots, n\}$, die Vielfache von p sind. Es gibt auch $\lceil \frac{n}{p^2} \rceil$ Zahlen in $\{1, 2, \ldots, n\}$, die Vielfache von p^2 sind, u.s.w. Folglich ist

$$n! = \prod_{p \in \mathfrak{P}} p^{j(n,p)}$$

wobei

$$j(n, p) = \sum_{m=1}^{\infty} \left\lceil \frac{n}{p^m} \right\rceil .$$

4. Wir definieren nun eine Funktion wie folgt. Sei $x \in \mathbb{R}$, $x > 0$ beliebig. Dann ist:

$$\theta(x) = \sum_{p \leq x} \log p = \log \left(\prod_{p \leq x} p \right) .$$

5. Es gilt

$$\binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \underbrace{\frac{n+1}{1} \cdot \frac{n+2}{2} \cdots \frac{2n}{n}}_{\text{alle} \geq 2} \geq 2^n .$$

6. Für alle $n \in \mathbb{N}$ gilt $\log n < 2\sqrt{n}$. Dies folgt, da

$$e^{2\sqrt{n}} = \sum_{i=0}^{\infty} \frac{(2\sqrt{n})^i}{i!} = 1 + 2\sqrt{n} + \frac{4n}{2} + \cdots > n.$$

Oder $\log(e^{2\sqrt{n}}) = 2\sqrt{n} > \log n$.

7. Sei $k > 0$ eine reelle Zahl. Dann ist

$$\lim_{x \to \infty} \frac{\log kx}{\sqrt{x}} = 0.$$

D.h. für alle $\epsilon > 0$ existiert ein $x_\epsilon > 0$, mit $\log kx/\sqrt{x} < \epsilon$, für alle $x > x_\epsilon$. Nehme z.B. $x_\epsilon = 24k/\epsilon^4$. Dann gilt für solche $x > x_\epsilon = 24k/\epsilon^4$,

$$x < \frac{\epsilon^4 x^2}{24k}.$$

Oder

$$x < \frac{1}{k} + \frac{\epsilon\sqrt{x}}{k} + \frac{\epsilon^2 x}{2k} + \cdots + \frac{\epsilon^4 x^2}{24k} + \cdots$$

Oder

$$kx = e^{\log kx} < 1 + \epsilon\sqrt{x} + \frac{\epsilon^2 x}{2} + \cdots + \frac{\epsilon^4 x^2}{24} + \cdots = e^{\epsilon\sqrt{x}}.$$

Lemma (A). $\theta(n) < 2n \log 2$ *für alle* $n \in \mathbb{N}$.

Beweis. Nach dem Binomialsatz ist

$$(a + b)^k = \sum_{l=0}^{k} \binom{k}{l} a^{k-l} b^l.$$

Insbesondere, für den speziellen Fall $a = b = 1$ und $k = 2m + 1$ gilt

$$2^{2m+1} = (1 + 1)^{2m+1} = \sum_{l=0}^{2m+1} \binom{2m+1}{l}.$$

Nun, $2m+1$ ist ungerade; daher sind die zwei mitteleren Terme in dieser Summe gleich

$$M = \binom{2m+1}{m} = \frac{(2m+1)\cdot(2m)\cdots(m+2)}{m!}.$$

D.h. $2M < 2^{2m+1}$ oder $M < 2^{2m}$ oder $\log M < 2m\log 2$.

Sei jetzt $p \in \mathfrak{P}$ mit $m+1 < p \leq 2m+1$. Dann ist sicherlich $p|(2m+1)\cdot(2m)\cdots(m+2)$ aber $p \not| m!$. Insgesamt ist das Produkt

$$\prod_{m+1<p\leq 2m+1} p$$

Teiler von M, und folglich ist

$$\theta(2m+1) - \theta(m+1) = \sum_{m+1<p\leq 2m+1} \log p \leq \log M < 2m\log 2.$$

Das Lemma wird nun mittels Induktion über n bewiesen. Für $n = 1$ oder 2 ist Lemma A wahr. Sei daher $n > 2$. Falls n eine gerade Zahl, dann ist offensichtlich $\theta(n) = \theta(n-1)$, und trivialerweise gilt

$$\theta(n) = \theta(n-1) < 2(n-1)\log 2 < 2n\log 2.$$

Für n ungerade gilt etwa $n = 2m+1$ (mit $m \in \mathbb{N}$) und

$$\begin{aligned}\theta(n) = \theta(2m+1) &= \theta(2m+1) - \theta(m+1) + \theta(m+1)\\ &< 2m\log 2 + 2(m+1)\log 2\\ &= 2(2m+1)\log 2 = 2n\log 2.\end{aligned}$$

□

Lemma (B). *Eine Konstante C_2 existiert mit*

$$\pi(x) < C_2 \cdot \frac{x}{\log x},$$

für alle $x \geq 2$.

Beweis. Sei $x \in \mathbb{N}$. Dann gilt $\log x < 2\sqrt{x}$. Für $x \geq 2$ ist auch $\log x \neq 0$ und

$$\sqrt{x} < \frac{2x}{\log x}.$$

Es gilt

$$\begin{aligned}\theta(x) &\geq \sum_{\sqrt{x}<p\leq x} \log p\\ &\geq (\log\sqrt{x})\cdot(\pi(x) - \pi(\sqrt{x}))\\ &\geq (\log\sqrt{x})\cdot\pi(x) - \underbrace{\sqrt{x}}_{\text{sicherlich } >\pi(\sqrt{x})}\cdot\log(\sqrt{x})).\end{aligned}$$

$$\begin{aligned}\Rightarrow\quad \pi(x) &\leq \frac{\theta(x) + \sqrt{x}\log(\sqrt{x})}{\log(\sqrt{x})}\\ &= \frac{\theta(x)}{\log(\sqrt{x})} + \sqrt{x}\\ &= \frac{2\theta(x)}{\log x} + \sqrt{x}\\ &< \underbrace{\frac{4x\log 2}{\log x}}_{\text{Lemma A}} + \underbrace{\frac{2x}{\log x}}_{\text{von oben}}\\ &= (4\log 2 + 2)\frac{x}{\log x}\\ &= C_2\frac{x}{\log x}.\end{aligned}$$

□

Lemma (C). *Sei*

$$k(n,p) = \sum_{k=1}^{t_p} \left(\left\lceil \frac{2n}{p^k} \right\rceil - 2 \left\lceil \frac{n}{p^k} \right\rceil \right),$$

wobei t_p *die größte Zahl ist, mit* $p^{t_p} \leq 2n$.[2] *Dann gilt*

$$\binom{2n}{n} = \prod_{p \in \mathfrak{P}} p^{k(n,p)}.$$

Beweis. Es gilt $\binom{2n}{n} = \frac{(2n)!}{(n!)^2}$. Daher ist nach Vorergebnis 5

$$\binom{2n}{n} = \prod_{p \in \mathfrak{P}} p^{k(n,p)}.$$

□

Aber für alle $x \in \mathbb{R}$ gilt stets

$$\lceil 2x \rceil - 2\lceil x \rceil = \begin{cases} 1, & \text{falls } x - \lceil x \rceil \geq 1/2; \\ 0, & \text{falls } x - \lceil x \rceil < 1/2. \end{cases}$$

D.h.

$$\begin{aligned} k(n,p) &= \sum_{k=1}^{t_p} \left(\left\lceil \frac{2n}{p^k} \right\rceil - 2 \left\lceil \frac{n}{p^k} \right\rceil \right) \\ &\leq \sum_{k=1}^{t_p} 1 = t_p \leq \left\lceil \frac{\log 2n}{\log p} \right\rceil. \end{aligned}$$

Lemma (D). *Eine Zahl* C_1 *existiert, mit*

$$C_1 \frac{n}{\log n} < \pi(n),$$

für alle hinreichend große $n \in \mathbb{N}$.

Beweis. Es gilt

$$2^n \leq \binom{2n}{n} = \prod_{p < 2n} p^{k(n,p)}.$$

(Die Ungleichungen folgen aus Vorergebnissen 3 bzw. 5.) Oder

$$\begin{aligned} n \log 2 &\leq \sum_{p<2n} k(n,p) \log p \\ &\leq \sum_{p<2n} \left\lceil \frac{\log 2n}{\log p} \right\rceil \log p \\ &= \sum_{p \leq \sqrt{2n}} \left\lceil \frac{\log 2n}{\log p} \right\rceil \log p + \sum_{\sqrt{2n} < p < 2n} \left\lceil \frac{\log 2n}{\log p} \right\rceil \log p. \end{aligned}$$

Aber für $\sqrt{2n} < p < 2n$ gilt

$$\frac{1}{2} \log 2n < \log p < \log 2n.$$

[2] D.h.

$$t_p \log p \leq \log 2n$$

oder

$$t_p \leq \left\lceil \frac{\log 2n}{\log p} \right\rceil.$$

D.h.

$$\left\lceil \frac{\log 2n}{\log p} \right\rceil = 1.$$

Daher ist

$$\sum_{p \le \sqrt{2n}} \left\lceil \frac{\log 2n}{\log p} \right\rceil \log p + \sum_{\sqrt{2n} < p < 2n} \left\lceil \frac{\log 2n}{\log p} \right\rceil \log p =$$

$$\begin{aligned} &= \sum_{p \le \sqrt{2n}} \left\lceil \frac{\log 2n}{\log p} \right\rceil \log p + \sum_{\sqrt{2n} < p < 2n} \log p \\ &\le \underbrace{\sqrt{2n} \log 2n}_{\text{da } \left\lceil \frac{\log 2n}{\log p} \right\rceil \le \frac{\log 2n}{\log p}} + \theta(2n). \end{aligned}$$

D.h.

$$\begin{aligned} \theta(2n) &\ge n \log 2 - \sqrt{2n} \log 2n \\ &= n \cdot \left(\log 2 - \frac{\sqrt{2} \log 2n}{\sqrt{n}} \right). \end{aligned}$$

Nach unserem Vorergebnis 7 gibt es ein $T > 0$ mit

$$\frac{\sqrt{2} \log 2n}{\sqrt{n}} < \frac{1}{2} \log 2,$$

für $n > T$. D.h. $\theta(2n) > n \log 2/2$. Für n gerade und 'hinreichend groß', ist dann

$$\theta(n) = \theta(2 \cdot \frac{n}{2}) > \left(\frac{n}{2}\right) \frac{1}{2} \log 2.$$

D.h. $\theta(n) > \frac{n}{4} \log 2$. Falls n ungerade, dann ist

$$\theta(n) \ge \theta(n-1) > \frac{(n-1)}{4} \log 2 > \frac{n}{8} \log 2,$$

falls $n > 2$. Sei daher $C_1 = \frac{1}{8} \log 2$. Dann gilt $\theta(n) > C_1 \cdot n$ für alle hinreichend große n. Aber

$$\theta(n) = \sum_{p \le n} \log p \le \pi(n) \log n.$$

$$\Rightarrow \quad \pi(n) \ge \frac{\theta(n)}{\log n} > C_1 \frac{n}{\log n}.$$

Somit ist der Satz von Tschebyscheff bewiesen. □

Satz 13. *Sei p_n die n-te Primzahl. ($p_1 = 2$, $p_2 = 3$, $p_3 = 5$, u.s.w.) Dann gibt es Konstanten C_3, C_4 mit*

$$C_3 n \log n < p_n < C_4 n \log n.$$

Beweis. Nach Satz 12 ist

$$n = \pi(p_n) < C_2 \frac{p_n}{\log p_n}$$

oder

$$p_n > \frac{n}{C_2} \log p_n > \frac{n}{C_2} \log n.$$

Andererseits ist

$$C_1 \frac{p_n}{\log p_n} < \pi(p_n) = n,$$

d.h.

$$C_1 < \frac{n \log p_n}{p_n}.$$

Da

$$\lim_{n\to\infty} \frac{\log p_n}{\sqrt{p_n}} = 0,$$

gilt

$$\frac{\log p_n}{\sqrt{p_n}} < C_1 < \frac{n \log p_n}{p_n}$$

für hinreichend große n. Insbesondere gilt hier $p_n < n^2$ oder $\log p_n < 2 \log n$. D.h.

$$C_1 p_n < n \log p_n < 2n \log n.$$

D.h.

$$p_n < \frac{2}{C_1} n \log n.$$

□

Satz 14. *Es existiert eine Konstante* C_5 *mit*

$$\sum_{2<p\le n} \frac{1}{p} < C_5 \log\log n,$$

für alle $n \ge 3$.

Beweis. Nach Satz 13 gilt

$$\frac{1}{p_n} < \frac{1}{C_3 n \log n}.$$

Daher ist

$$\begin{aligned}
\sum_{2<p\le n} \frac{1}{p} &< \frac{1}{C_3} \sum_{r=2}^{\pi(n)} \frac{1}{r \log r} \\
&\le \frac{1}{C_3} \sum_{r=2}^{n} \frac{1}{r \log r} \\
&< \frac{1}{C_3} \left(\frac{1}{2\log 2} + \int_2^n \frac{dt}{t \log t} \right) \\
&< \frac{1}{C_3 2 \log 2} + \frac{1}{C_3} (\log\log n) \\
&< C_5 \log\log n.
\end{aligned}$$

□

4 Der Ring der arithmetischen Funktionen

Definition 4.1. Eine Abbildung $f : \mathbb{N} \to \mathbb{C}$ heißt eine *arithmetische Funktion*. Die Menge aller arithmetischen Funktionen wird mit $\mathcal{A}$ bezeichnet.

$f \in \mathcal{A}$ heißt multiplikativ, falls

- $\exists k \in \mathbb{N}$ mit $f(k) \neq 0$, und
- $f(n)f(m) = f(nm)$, für alle $n, m \in \mathbb{N}$ mit $ggt(n, m) = 1$.

Falls $f(n)f(m) = f(nm)$ für *alle* $n, m \in \mathbb{N}$, dann heißt f *vollständig multiplikativ*.

Zwei abstrakte Operationen '$+$' und '$*$' werden definiert, und zwar:

$$(f+g)(n) = f(n) + g(n), \quad \text{und}$$

$$(f*g)(n) = \sum_{d|n} f(d)g(n/d),$$

für alle $n \in \mathbb{N}$ und $f, g \in \mathcal{A}$. Die Operation $f*g$ heißt die *Faltung* von f und g.

Bemerkung. *Als Übung wird gezeigt, daß das (Faltungs)produkt von zwei multiplikativen Funktionen wieder multiplikativ ist.*

Insbesondere werden wir die folgenden Funktionen betrachten:

$$0(n) = 0, \text{ für alle } n,$$

$$\epsilon(n) = 1, \text{ für alle } n,$$

$$\eta(n) = \begin{cases} 1, & \text{falls } n = 1 \\ 0, & \text{sonst,} \end{cases}$$

$$\mu(n) = \begin{cases} 1, & n = 1 \\ (-1)^r, & \text{falls } n = p_1 \cdots p_r \text{ und } p_i \neq p_j \text{ für } i \neq j \\ 0, & \text{sonst.} \end{cases}$$

Die Funktionen ϵ, η, und μ sind offensichtlich multiplikativ. Nach einer kleinen Überlegung sieht man auch, daß $\epsilon * \mu = \eta$.

Satz 15. *$\mathcal{A}$ ist ein kommutativer Ring mit Nullelement 0 und Einselement η. Eine Funktion $f \in \mathcal{A}$ ist genau dann eine Einheit, wenn $f(1) \neq 0$.*

Beweis. Daß 0 ein Nullelement ist, ist klar. Aber es gilt auch

$$(f*\eta)(n) = \sum_{d|n} f(d)\eta(n/d) = f(n)\eta(n/n) = f(n),$$

für alle $f \in \mathcal{A}$, und $n \in \mathbb{N}$. Daher ist η das Einselement.

Man bestätigt leicht, daß die Distributivität gilt:

$$\begin{aligned} f*(g+h)(n) &= \sum_{d|n} f(d)\,(g(n/d) + h(n/d)) \\ &= \sum_{d|n} f(d)g(n/d) + \sum_{d|n} f(d)h(n/d) \\ &= (f*g)(n) + (f*h)(n). \end{aligned}$$

u.s.w.

Sei nun $f \in \mathcal{A}$, mit $f(1) = 0$. Angenommen, ein $g \in \mathcal{A}$ existiert, mit $f*g = \eta$. Insbesondere wäre dann

$$1 = \eta(1) = f*g(1) = \sum_{d|1} f(d)g(1/d) = f(1)g(1) = 0.$$

Ein Widerspruch.

Andererseits, sei $f(1) \neq 0$. Wir konstruieren ein $h \in \mathcal{A}$ wie folgt. Erstens wird $h(1) = 1/f(1)$ festgelegt. Dadurch ist $h*f(1) = 1 = \eta(1)$. Sei nun angenommen, daß $n > 1$ gegeben ist, und $h(j)$ steht schon fest, für $1 \leq j < n$. Dann soll gelten:

$$0 = \eta(n) = h*f(n) = \sum_{d|n} h(d)f(d/n) = h(n)f(1) + \sum_{\substack{d|n \\ d<n}} h(d)f(n/d).$$

Sei daher

$$h(n) = \frac{-1}{f(1)} \sum_{\substack{d|n \\ d<n}} h(d)f(n/d).$$

□

Satz 16. *Sei $f \in \mathcal{A}$ multiplikativ. Dann ist $f(1) = 1$ und das Inverse zu f ist auch multiplikativ.*

Beweis. Es existiert zumindest ein $k \in \mathbb{N}$, mit $f(k) \neq 0$. Da stets $ggt(k,1) = 1$, gilt $f(k) = f(k \cdot 1) = f(k)f(1)$. Folglich ist $f(1) = 1$. Da $f(1) = 1 \neq 0$, gibt es ein Inverses $g \in \mathcal{A}$ zu f mit $g * f = \eta$. Ist g multiplikativ?

Dazu sei die Funktion $h \in \mathcal{A}$ definiert wie folgt. Für jedes $n \in \mathbb{N}$ sei $n = p_1^{e_1} \cdots p_r^{e_r}$ die eindeutige Primzahlfaktorizierung. (Daher $p_i \neq p_j$ für $i \neq j$, und $e_j \in \mathbb{N}$ für jedes j.) Dann ist

$$h(n) = h(p_1^{e_1} \cdots p_r^{e_r}) = \prod_{j=1}^{r} g(p_j^{e_j}).$$

Die Funktion h ist offensichtlich multiplikativ. Daher ist $f * h$ (als Produkt von zwei multiplikativen Funktionen) auch multiplikativ. Es gilt

$$(f * h)(p^e) = (f * g)(p^e) = \eta(p^e) = 0,$$

für $p > 1$ eine Primzahl und $e \in \mathbb{N}$. Daher ist

$$(f * h)(p_1^{e_1} \cdots p_r^{e_r}) = \eta(p_1^{e_1} \cdots p_r^{e_r}) = 0,$$

da auch η multiplikativ ist. Insgesamt gilt $f * h = \eta$. Aber

$$h = \eta * h = g * f * h = g * \eta = g.$$

D.h. g ist multiplikativ. □

Satz 17 (Möbius Umkehrformel). *Sei $f \in \mathcal{A}$ und $F = \epsilon * f$. Dann ist $f = \mu * F$.*

Beweis. $f = \eta * f = \mu * \epsilon * f = \mu * F$. □

Oder ausgeschrieben, lautet der Formel:
Sei

$$F(n) = \sum_{d|n} f(d).$$

Dann gilt

$$f(n) = \sum_{d|n} \mu(d)F(n/d).$$

Definition 4.2. Für jedes $n \in \mathbb{N}$, sei $\phi(n)$ die Anzahl der Zahlen $k \in \{1, \ldots, n\}$ mit $ggt(k,n) = 1$.

Offensichtlich ist auch ϕ eine multiplikativ Funktion in $\mathcal{A}$. Daher ist auch $\epsilon * \phi$ multiplikativ, und für Primzahlen p, und $r \in \mathbb{N}$ gilt

$$\epsilon * \phi(p^r) = p^r.$$

Denn $\phi(p^r) = p^r - p^{r-1}$ (nur Vielfachen von p sind *nicht* dabei). Daher

$$\epsilon * \phi(p^r) = \sum_{k=0}^{r} \epsilon(p^k)\phi(p^{r-k}) = 1 + \sum_{k=1}^{r} (p^k - p^{k-1}) = p^r,$$

und wegen der Multiplikativität gilt dann $\epsilon * \phi(n) = n$, für alle n. D.h. nach Satz 17:

Satz 18. *Es gilt*

$$\sum_{d|n} \phi(d) = n \qquad \textit{und} \qquad \phi(n) = \sum_{d|n} \mu(n/d)d.$$

5 Kongruenzen

Definition 5.1. Seien $n \in \mathbb{N}$ und $a, b \in \mathbb{Z}$. Falls eine weitere Zahl $m \in \mathbb{Z}$ existiert, mit $a - b = m \cdot n$, dann heißen a und b 'kongruent' modulo n, geschrieben

$$a \equiv b \bmod n$$

oder auch

$$a \equiv b(n).$$

Kongruenz modulo n ist eine Äquivalenzrelation. D.h.

- $a \equiv a(n)$,
- $a \equiv b(n) \Leftrightarrow b \equiv a(n)$,
- $a \equiv b(n)$ und $b \equiv c(n) \Rightarrow a \equiv c(n)$.

Die Menge der Äquivalenzklassen wird normalerweise in der Zahlentheorie mit $\mathbb{Z}/n\mathbb{Z}$ bezeichnet. Aber diese Schreibweise scheint mir zu schwerfällig hier in der elementaren Zahlentheorie. Ich werde stattdessen die einfachere Bezeichnung '$\mathbb{Z}_n$' benutzen.[3] Die n verschiedenen Äquivalenzklassen modulo n werden wir auch einfach durch die Menge $\{0, 1, \ldots, n-1\}$ beschreiben. (D.h. etwa die Zahl '1' ist hier stellvertretend für die Äquivalenzklasse

$$[1] = \{m \cdot n + 1 : m \in \mathbb{Z}\},$$

und so weiter.) Seien $a \equiv b(n)$ und $c \equiv d(n)$. Dann gilt[4]

- $a + c \equiv b + d \bmod n$, und auch
- $a \cdot c \equiv b \cdot d \bmod n$.

Wir können daher einfach die Äquivalenzklassen als 'Zahlen' betrachten: Seien etwa $[a]$ und $[b]$ die Äquivalenzklassen, die a bzw. b enthalten. Dann gilt

- $[a] + [b] = [a + b]$ und
- $[a] \cdot [b] = [a \cdot b]$.

Falls p eine Primzahl ist, dann ist $\mathrm{ggt}(a, p) = 1$ für alle $1 \leq a < p$. Daher existieren $x, y \in \mathbb{Z}$ mit $xa + yp = 1$. D.h. $xa - 1 = yp$ oder anders geschrieben, $xa \equiv 1(p)$. Somit ist die Äquivalenzklasse $[x] = ([a])^{-1}$. Insgesamt ist $\mathbb{Z}_p$ ein Körper, falls $p \in \mathfrak{P}$.

Falls $n \notin \mathfrak{P}$, dann existiert ein $a > 1$ in $\mathbb{Z}_n$ mit $\mathrm{ggt}(a, n) = c > 1$. Kann es sein, daß $\mathbb{Z}_n$ ein Körper ist? Nein, denn sonst gäbe es ein $d \in \mathbb{Z}_n$ mit $da \equiv 1(n)$, daher $da - mn = 1$ für irgendein $m \in \mathbb{Z}$: ein Widerspruch.

[3] Leider wird die Notation $\mathbb{Z}_p$ in der Theorie der p-addischen Zahlen für etwas anderes benützt. Sie sollten daher wissen, daß es *nicht* üblich ist, die "Restklassen modulo n" durch $\mathbb{Z}_n$ zu bezeichnen! (Traditionalerweise sagt man *Restklasse* statt Äquivalenzklasse. u.s.w!)

[4] Seien etwa $a - b = m_1 n$ und $c - d = m_2 n$. Dann ist

$$\begin{aligned} (a+c) - (b+d) &= (m_1 + m_2)n \quad \text{und} \\ ac - bd &= (ac - bc) + (bc - bd) \\ &= cm_1 n + bm_2 n \\ &= (cm_1 + bm_2)n \end{aligned}$$

5.1 Die Gruppe der Einheiten

Wir interessieren uns nun zunächst für die Arithmetik von $\mathbb{Z}_n$, wobei n nicht notwendigerweise eine Primzahl ist.

Definition 5.2. Sei $n \in \mathbb{N}$. Eine Zahl $a \in \mathbb{Z}_n$ heißt eine 'Einheit modulo n', falls $x \in \mathbb{Z}_n$ existiert mit $xa \equiv 1(n)$. Die Menge aller Einheiten modulo n heißt $U(\mathbb{Z}_n)$.

Satz 19. $a \in U(\mathbb{Z}_n) \Leftrightarrow ggt(a, n) = 1$.

Beweis. D.h. x, $y \in \mathbb{Z}$ existieren, mit $ax + ny = 1$. □

Es ist üblich in der Zahlentheorie, die Anzahl der Einheiten modulo n mit $\phi(n)$ zu bezeichnen. Z.B. $\phi(6) = 2$, da $U(\mathbb{Z}_6) = \{1, 5\}$. Aber auch $\phi(p) = p - 1$ für alle $p \in \mathfrak{P}$.

Satz 20. *Für jedes $n > 1$ in $\mathbb{N}$ ist $U(\mathbb{Z}_n)$ eine Gruppe unter Multiplikation.*

Beweis. Seien a, $b \in U(\mathbb{Z}_n)$. Dann existieren $a^{-1} \in U(\mathbb{Z}_n)$ und $b^{-1} \in U(\mathbb{Z}_n)$. Daher ist $b^{-1} \cdot a^{-1} \in \mathbb{Z}_n$ auch ein Element von $\mathbb{Z}_n$ und wir haben

$$(b^{-1} \cdot a^{-1}) \cdot (a \cdot b) = b^{-1} \cdot (a^{-1} \cdot a) \cdot b = b^{-1} \cdot b = [1].$$

Somit ist $ab \in U(\mathbb{Z}_n)$. Die andere Gruppenaxiome sind auch trivialerweise erfüllt. □

Satz 21. *Sei G eine endliche Gruppe mit n Elementen und sei $H \subset G$ eine Untergruppe mit m Elementen. Dann gilt $m|n$.*

Beweis. Wir definieren eine Äquivalenzrelation zwischen den Elementen von G wie folgt. $a \sim b \Leftrightarrow a^{-1}b \in H$. Dies ist eine Äquivalenzrelation, denn

- $a \sim a$, da $a^{-1}a = e \in H$ (wobei e das 'eins' Element von G und H ist).
- $a \sim b \Leftrightarrow b \sim a$, da $(b^{-1}a)^{-1} = a^{-1}b$ und für jedes $h \in H$ ist auch $h^{-1} \in H$.
- $a \sim b$ und $b \sim c$ gibt $a \sim c$, da $(a^{-1}b)(b^{-1}c) = a^{-1}c \in H$.

Diese Äquivalenzrelation spaltet G in eine Sammlung von disjunkten Äquivalenzklassen. Für jedes beliebige $x \in G$ sei $[x]$ die Äquivalenzklasse, die x enthält. Es gibt dann eine Bijektion

$$f : H \to [x],$$

wobei $f(h) = x \cdot h$, für alle $h \in H$. D.h.

- $xh \sim x$, da $(xh)^{-1}x = h^{-1}x^{-1}x = h^{-1} \in H$,
- Seien $h_1 \neq h_2 \in H$. Dann auch $xh_1 \neq xh_2$ (denn sonst wäre $x^{-1}xh_1 = x^{-1}xh_2$; d.h. $h_1 = h_2$). f ist daher ein Monomorphismus.
- Sei $y \in [x]$ beliebig. Aber $x \sim y$ heißt $x^{-1}y \in H$ und $y = x \cdot (x^{-1}y) = f(x^{-1}y)$. f ist daher ein Epimorphimus.

Nun, die Äquivalenzklassen sind alle disjunkt, mit gleich vielen Elementen (gleich viele wie H selbst). Folglich muß $m|n$. □

Sei nun G irgendeine endliche Gruppe und sei $a \in G$. Wir betrachten die Menge $\{a, a^2, a^3, \ldots, a^n\}$, für verschiedene $n \in \mathbb{N}$. Da G endlich ist, gibt es ein $n \in \mathbb{N}$ so, daß $a^n = a^m$ für ein $m < n$. Aber in diesem Fall ist $a^{n-m} = e$. Sei $s \geq 1$ die kleinste Zahl mit $a^s = e$. Diese Zahl s heißt die 'Ordnung' von a in G. Aber die Teilmenge $\{a, a^2, \ldots, a^s = e\} \subset G$ ist sicherlich auch eine Untergruppe von G, daher ist s auch Teiler der Gruppenordnung (die Anzahl der Elemente in G). Angenommen, G enthält k Elemente. Da $s|k$, können wir etwa $k = s \cdot t$ schreiben, für ein $t \in \mathbb{N}$. Dann gilt

$$a^k = a^{st} = (a^s)^t = e^t = e.$$

Insbesondere, wenn wir die Gruppe der Einheiten modulo n nehmen, dann erhalten wir:

Satz 22. $a^{\phi(n)} \equiv 1(n)$ *für jedes Element* $a \in U(\mathbb{Z}_n)$.

Satz 23 (Fermat's kleiner Satz). *Für alle* $p \in \mathfrak{P}$ *und* $a \in \mathbb{N}$ *mit* $p \not| a$ *gilt* $a^{p-1} \equiv 1(p)$.

Beweis. Dies folgt, da $\phi(p) = p - 1$ für $p \in \mathfrak{P}$ und $p \not| a \Rightarrow [a] \in U(\mathbb{Z}_p)$. □

Bemerkung. *Dadurch erhalten wir einen praktischen (wenn doch nicht besonders zuverlässigen) Test für Primzahlen. Sei* $n \in \mathbb{N}$ *vorgegeben. Ist* n *eine Primzahl? Wenn* n *z.B. 1000 Dezimalstellen hat, dann ist diese Frage im allgemeinen nicht so einfach zu beantworten. Andererseits gibt es die Möglichkeit, die Zahl* 2^{n-1} *mod* n *auszurechnen. (Das Multiplizieren und Potenzieren von 2er Potenzen kann—mit Hilfe von 'Bit-verschiebungen'—in einem Computer schnell durchgeführt werden.) Falls* n *doch keine Primzahl ist, dann ist es sehr, sehr wahrscheinlich, daß* $2^{n-1} \not\equiv 1(n)$. *Das würde dann definitiv heißen, daß* n *keine Primzahl ist. Andererseits gibt es leider auch Zahlen* n, *die nicht prim sind, wobei* $2^{n-1} \equiv 1(n)$ *trotzdem gilt.*

5.2 Die Gleichung $ax \equiv b$ mod n

Betrachten wir nun die Gleichung $ax \equiv b(n)$. Hier sind sowohl $n \in \mathbb{N}$ als auch $a, b \in \mathbb{Z}_n$ vorgegeben. Gibt es dann eine Lösung $x \in \mathbb{Z}_n$?

Satz 24. *Sei* $d = ggt(a, n)$. *Die Gleichung* $ax \equiv b(n)$ *ist lösbar genau dann, wenn* $d|b$. *In diesem Fall gibt es genau* d *verschiedene Lösungen, und zwar die (Äquivalenzklassen der) Zahlen*

$$x_0 + k \cdot \left(\frac{n}{d}\right), \quad k = 0, \ldots, d-1$$

wobei x_0 *irgendeine bestimmte Lösung ist.*

Beweis. Zunächst sei x_0 eine Lösung mit $ax_0 \equiv b(n)$. Da $ax_0 - b = mn$, für ein $m \in \mathbb{Z}$, gilt $b = ax_0 - mn$. Aber $d|a$ und $d|n$, daher gilt $d|b$. Ferner ist auch

$$a(x_0 + k \cdot \left(\frac{n}{d}\right)) = ax_0 + k \cdot \left(\frac{a}{d}\right) n \equiv ax_0 \equiv b \bmod n$$

eine Lösung für alle $k \in \mathbb{Z}$. (Dies gilt, da $\frac{a}{d} \in \mathbb{N}$.) Seien jetzt $k_1 \neq k_2$ in $\{1, \ldots, d-1\}$. Dann ist

$$\left|\left(x_0 + k_1 \cdot \left(\frac{n}{d}\right)\right) - \left(x_0 + k_2 \cdot \left(\frac{n}{d}\right)\right)\right| = \left|(k_1 - k_2)\left(\frac{n}{d}\right)\right| < n,$$

da $0 \leq k_i \leq d - 1$. Folglich ist

$$x_0 + k_1 \cdot \left(\frac{n}{d}\right) \not\equiv x_0 + k_2 \cdot \left(\frac{n}{d}\right) \bmod n.$$

Allgemein, sei x_1 eine beliebige weitere Lösung, mit $ax_1 \equiv b(n)$. Dann ist

$$0 = b - b \equiv a(x_0 - x_1) \bmod n$$

$$\Rightarrow n|a(x_0 - x_1) \Rightarrow \frac{n}{d} \left| \frac{a}{d}(x_0 - x_1) \right. .$$

Aber $\frac{n}{d}$ und $\frac{a}{d}$ haben keinen gemeinsamen Teiler (d ist doch der größte). Folglich ist $\frac{n}{d}|x_0 - x_1$. D.h. $x_0 - x_1 = k \cdot \frac{n}{d}$ für ein $k \in \mathbb{Z}$. Oder

$$x_1 = x_0 - k\left(\frac{n}{d}\right).$$

Aber dann gibt es ein $0 \leq k' \leq d - 1$ mit

$$x_0 - k\left(\frac{n}{d}\right) \equiv x_0 - k'\left(\frac{n}{d}\right) \bmod n.$$

D.h. $(x_0 - k\frac{n}{d}) - (x_0 - k'\frac{n}{d}) = (k - k')\frac{n}{d} = mn$, für ein $m \in \mathbb{Z}$, oder $k - k' = md$. Wähle nun m so, daß $k' = k - md \in \{0, \ldots, d-1\}$.

Umgekehrt, sei $d|b$. Da $d = ggt(a, n)$, gibt es zwei Zahlen, $u, v \in \mathbb{Z}$ mit $au + nv = d$. Sei $c = \frac{b}{d} \in \mathbb{N}$. Dann ist $a(cu) \equiv b \bmod n$, denn

$$a(cu) + ncv = \frac{aub}{d} + \frac{nvb}{d} = b\left(\frac{au + nv}{d}\right) = b\frac{d}{d} = b.$$

D.h. eine Lösung (nämlich cu) existiert. □

5.3 Der Chinesische Restklassensatz

Satz 25. *Seien* $m_1, \ldots, m_t \in \mathbb{N}$ *mit ggt*$(m_i, m_j) = 1$, *für alle* $i \neq j$. *Seien* $b_1, \ldots, b_t \in \mathbb{Z}$ *beliebig. Dann gibt es ein* $x_0 \in \mathbb{Z}$ *mit* $x_0 = b_i(m_i)$ *für alle* i. *Ferner ist* $x_0 + rm$ *auch eine Lösung, für alle* $r \in \mathbb{Z}$ *(wobei* $m = m_1 \cdot m_2 \cdots m_t$*), und jede Lösung hat diese Gestalt.*

Beweis. Für jedes $i \in \{1, \ldots, t\}$ sei

$$\frac{m}{mi} = m_1 \cdots m_{i-1} \cdot m_{i+1} \cdots m_t = n_i.$$

Nach dem Fundamentalsatz der Arithmetik ist dann $ggt(m_i, n_i) = 1$. Nehme jeweils r_i, $s_i \in \mathbb{Z}$ mit

$$r_i m_i + s_i n_i = 1$$

und sei $l_i = s_i n_i \in \mathbb{Z}$. D.h. $l_i \equiv 1(m_i)$, aber auch $l_i \equiv 0(m_j)$ für $j \neq i$, da doch n_i die Zahl m_j als Faktor enthält. Die Zahl

$$x_0 = b_1 l_1 + \cdots + b_t l_t$$

ist dann offensichtlich eine Lösung, da $x_0 \equiv b_i(m_i)$ für alle i. Sei nun $r \in \mathbb{Z}$ beliebig. Dann ist auch $rm \equiv 0(m_i)$ für alle i, da jeweils $m_i | m$. D.h. $x_0 + rm$ ist auch eine Lösung, für alle $r \in \mathbb{Z}$.

Gegeben eine beliebige Lösung $y \in \mathbb{Z}$, dann gilt $y - x_0 \equiv 0(m_i)$ für alle i. D.h. $m_i | y - x_0$. Da die verschiedenen m_i keine gemeinsamen Teiler haben, muß (nach dem Fundamentalsatz der Arithmetik) auch

$$m = m_1 \cdots m_t | y - x_0.$$

Folglich ist $y = x_0 + rm$, für ein $r \in \mathbb{Z}$. □

5.4 Die Struktur der Einheitengruppe

Satz 26. *Seien wieder* $m_1, \ldots, m_t \in \mathbb{N}$ *mit ggt*$(m_i, m_j) = 1$, *für alle* $i \neq j$ *und sei* $m = m_1 \cdots m_t$. *Dann gilt*

$$U(\mathbb{Z}_m) \simeq U(\mathbb{Z}_{m_1}) \times \cdots \times U(\mathbb{Z}_{m_t})$$

(das kartesische Produkt der Gruppen).

wobei

Definition 5.3. Seien $G_1, \ldots, G_t$ jeweils Gruppen. Das kartesische Produkt $G = G_1 \times \cdots \times G_t$ ist die Gruppe

$$G = \{(g_1, \ldots, g_t) : g_i \in G_i, \forall i\}$$

mit Multiplikation

$$(g_1, \ldots, g_t) \cdot (h_1, \ldots, h_t) = (g_1 h_1, \ldots, g_t h_t).$$

Beweis. (des Satzes) Die Abbildung

$$f : U(\mathbb{Z}_m) \to U(\mathbb{Z}_{m_1}) \times \cdots \times U(\mathbb{Z}_{m_t})$$

sei wie folgt definiert. Für $a \in U(\mathbb{Z}_m)$ sei jeweils $a_i \equiv a(m_i)$. Dann ist

$$f(a) = (a_1, \ldots, a_t).$$

Ist $a_i \in U(\mathbb{Z}_{m_i})$? Da $a \in U(\mathbb{Z}_m)$, gibt es ein $b \in \mathbb{Z}_m$ mit $ab \equiv 1(m)$. Da $m_i | m$, gilt auch $ab \equiv 1(m_i)$. In $\mathbb{Z}_{m_i}$ sei $b_i \equiv b(m_i)$, daher ist $a_i b_i \equiv 1(m_i)$. Folglich $a_i \in U(\mathbb{Z}_{m_i})$.

Ist f ein Homomorphismus? Sei $a' \in U(\mathbb{Z}_m)$ und $a'_i \equiv a'(m_i)$ für alle i. Dann ist

$$\begin{aligned} f(a \cdot a') &= (aa' \bmod m_1, \ldots, aa' \bmod m_t) \\ &= (a_1 a'_1 \bmod m_1, \ldots, a_t a'_t \bmod m_t) \\ &= f(a) f(a'). \end{aligned}$$

Nach Satz 21 ist f eine Bijektion. □

Wir können insbesondere $n = p_1^{l_1} \cdots p_t^{l_t}$ schreiben, wobei die p_i jeweils verschiedene Primzahlen sind und $l_i \in \mathbb{N}$. Dann ist

$$U(\mathbb{Z}_n) = U(\mathbb{Z}_{p_1^{l_1}}) \times \cdots \times U(\mathbb{Z}_{p_t^{l_t}}).$$

Welche Struktur hat dann $U(\mathbb{Z}_{p^l})$ für $p \in \mathfrak{P}$ und $l \in \mathbb{N}$? Wie wir später sehen werden, ist $U(\mathbb{Z}_{p^l})$ stets eine zyklische Gruppe, falls $p > 2$. (Die Situation für $U(\mathbb{Z}_{2^l})$ ist aber doch etwas komplizierter.)

6 Primitivwurzeln

Definition 6.1. Sei G eine endliche Gruppe mit n Elementen. G heißt 'zyklisch', falls ein Element $a \in G$ existiert, mit

$$G = \{a, a \cdot a = a^2, \ldots, a^n = 1\}.$$

Das Element a heißt dann ein 'erzeugendes Element' für die Gruppe. Falls $U(\mathbb{Z}_n)$ zyklisch ist, für ein $n \in \mathbb{N}$ mit einem erzeugenden Element $a \in U(\mathbb{Z}_n)$, dann heißt a eine 'Primitivwurzel' modulo n.

6.1 Primitivwurzeln modulo p, für p eine Primzahl

Satz 27. *Für $p \in \mathfrak{P}$ prim ist $U(\mathbb{Z}_p)$ stets zyklisch.*

Zuerst einige Vorergebnisse.

Satz 28. *Für alle $n \in \mathbb{N}$ gilt $\sum_{d|n} \phi(d) = n$.*

Beweis. Dies ist eigentlich ein Teil von Satz 18. □

Satz 29. *Sei F ein Körper und seien $P(x)$, $Q(x) \in F[x]$ zwei Polynome mit $n := Grad(P) = Grad(Q)$. Angenommen, $n+1$ verschiedene Elemente $a_1, \ldots, a_{n+1} \in F$ existieren, mit $P(a_i) = Q(a_i)$ für alle $i = 1, \ldots, n+1$. Dann ist $P = Q$.*

Beweis. Sei $R(x) = P(x) - Q(x)$. Dann ist R ein Polynom vom Grad n mit $n+1$ verschiedenen Nullstellen. Folglich ist $R = 0$. (Bemerkung: für jede Nullstelle, etwa a_1 gibt es die Faktorisierung $R(x) = (x - a_1)T(x)$ mit Grad(T) kleiner als Grad(R), u.s.w. Allgemein: ein Polynom vom Grad n kann höchstens n verschiedene Nullstellen haben.) □

Satz 30. *Im Körper $\mathbb{Z}_p$ gilt die Polynomgleichung*

$$x^{p-1} - 1 \equiv (x-1)(x-2)\cdots(x-p+1) \bmod p.$$

Beweis. Nach Fermat's kleinem Satz ist $m^{p-1} - 1 \equiv 0 \bmod p$, für alle $1 \le m \le p-1$. Trivialerweise ist auch m eine Nullstelle von $(x-1)(x-2)\cdots(x-p+1)$ für alle solche m. Aber

$$x^{p-1} - 1 - (x-1)(x-2)\cdots(x-p+1)$$

ist ein Polynom vom Grad $p-2$. □

Satz 31 (Wilson's Satz). $(p-1)! \equiv -1 \bmod p$.

Beweis. Betrachte den Fall $x = 0$ in Satz 30. □

Satz 32. *Sei $p \in \mathfrak{P}$ prim und sei $d|p-1$. Dann besitzt die Gleichung $x^d \equiv 1 \bmod p$ genau d verschiedene Lösungen. D.h. die Menge $\{a \in \mathbb{Z}_p : a^d \equiv 1 \bmod p\}$ hat genau d Elemente.*

Beweis. Sei etwa $p - 1 = w \cdot d$ mit $w \in \mathbb{N}$. D.h. $(x^d)^w = x^{p-1}$.

$$\begin{aligned} \Rightarrow \quad x^{p-1} - 1 &\equiv (x^d - 1)((x^d)^{w-1} + \cdots + (x^d)^2 + x^d + 1) \\ &\equiv (x-1)(x-2)\cdots(x-p+1) \bmod p. \end{aligned}$$

Folglich hat $(x^d - 1)(x^{d(w-1)} + \cdots + x^d + 1)$ immerhin $p-1$ <u>verschiedene</u> Nullstellen. Aber das Polynom $x^{d(w-1)} + \cdots + x^d + 1$ mit Grad $d(w-1)$ hat höchstens $d(w-1)$ verschiedene Nullstellen. Daher gibt es noch d weitere Nullstellen zum Polynom $x^d - 1$. □

Definition 6.2. Sei $m \in U(\mathbb{Z}_n)$. Nach Fermat's kleinem Satz ist $m^{\phi(n)} \equiv 1 \bmod n$. Sei $1 \le d \le \phi(n)$ die kleinste Zahl mit $m^d \equiv 1 \bmod n$. (Es gilt daher $d|\phi(n)$.) d heißt die 'Ordnung' von m modulo n. Falls $n = p \in \mathfrak{P}$ eine Primzahl, dann ist $\phi(p) = p - 1$. Für alle möglichen Zahlen $1 \le d \le p-1$ mit $d|p-1$ sei $\psi_p(d)$ die Anzahl der Zahlen $m \in U(\mathbb{Z}_p)$ mit Ordnung d modulo p.

Satz 33. *Es gilt*

$$\sum_{d|p-1} \psi_p(d) = p - 1.$$

Beweis. Jede Zahl m zwischen 1 und $p-1$ ist eine Einheit modulo p, daher einmal gezählt in der Aufzählung von $\psi_p(d)$, mit d die Ordnung von m modulo p. Es gibt genau $p-1$ solche Zahlen. □

Satz 34. $\psi_p(d) \leq \phi(d)$, *für* $p \in \mathfrak{P}$ *und* $d|p-1$.

Beweis. Falls $\psi_p(d) > 0$, dann sei $a \in U(\mathbb{Z}_p)$ mit Ordnung d modulo p. Die Gleichung $x^d \equiv 1 \bmod p$ hat Grad d und die d verschiedenen Zahlen $\{a, a^2, \ldots, a^d = 1\}$ sind alle Lösungen, nämlich

$$(a^k)^d = (a^d)^k \equiv 1^k = 1 \bmod p$$

für alle $1 \leq k \leq d$. Folglich gibt es <u>keine</u> anderen Lösungen und jede Zahl $m \in U(\mathbb{Z}_p)$ mit Ordnung d modulo p ist von der Gestalt $m = a^k$, für ein $k \in \{1, \ldots, d\}$. Andererseits, falls $k|d$ mit etwa $d = wk$, dann hat $m = a^k$ eine kleinere Ordnung als d, nämlich

$$m^w = (a^k)^w = a^{wk} = a^d \equiv 1 \bmod p.$$

Um den Satz zu beweisen, sei a^k gegeben mit Ordnung d modulo p. Sei $\text{ggt}(k, d) = h \in \mathbb{N}$. Dann gilt

$$1 = 1^{\frac{k}{h}} \equiv (a^d)^{\frac{k}{h}} = (a^k)^{\frac{d}{h}} \bmod p.$$

Da die Ordnung von a^k modulo p doch d ist, muß gelten $h = 1$. D.h. ein Element, das einmal in der Aufzählung von $\psi_p(d)$ gezählt wird, wird auch gezählt in $\phi(d)$. □

Zusammen mit den Sätzen 28 und 33 folgt:

Satz 35. $\psi_p(d) = \phi(d)$.

Aber für $p \in \mathfrak{P}$ eine ungerade Primzahl, ist $\phi(p-1) > 0$ (z.B. $\text{ggt}(1, p-1) = 1$). Die einzige gerade Primzahl ist 2, mit $U(\mathbb{Z}_2) = \{1\}$—offensichtlich auch eine zyklische Gruppe. Somit ist Satz 27 vollständig bewiesen.
Zum Schluß, zwei (immer noch) offene Fragen in der Mathematik:

1. Für $p \in \mathfrak{P}$, sei g_p die kleinste Primitivwurzel modulo p. Ist $g_p = 2$ für unendlich viele p?
2. Es ist bekannt (Pillai 1944), daß eine Konstante $C > 0$ existiert, wobei $g_p > C \log\log p$ für unendlich viele p. Auch (Grosswald 1981) $g_p < p^{0,499}$, falls $p > e^{e^{24}}$. Gibt es bessere Abschätzungen?

6.2 Primitivwurzeln modulo p^l, für $p \geq 3$ und $l \geq 2$

Die nächste Idee ist, zu zeigen, daß auch die Gruppe $U(\mathbb{Z}_{p^l})$ stets zyklisch ist, zumindest in dem Fall, wo p eine ungerade Primzahl ist.

Satz 36. *Sei* $p \in \mathfrak{P}$, $0 < j < p$. *Dann gilt* $p \left| \binom{p}{j} \right.$.

Beweis.

$$\binom{p}{j} = \frac{p!}{j!(p-j)!}.$$

Daher

$$p! = j!(p-j)!\binom{p}{j}.$$

Nun, $p|p!$, aber $p \not| j!$ und $p \not| (p-j)!$. □

Als triviale Folgerung des Binomialsatzes erhalten wir dann:

Satz 37. *Für alle* $a, b \in \mathbb{Z}_p$ *gilt* $(a+b)^p \equiv a^p + b^p \bmod p$.

Satz 38. *Angenommen,* $a \equiv b \bmod p^l$, *für ein* $l \in \mathbb{N}$. *Dann gilt* $a^p \equiv b^p \bmod p^{l+1}$.

Beweis. $a \equiv b \bmod p^l$ heißt $a - b = cp^l$, für ein $c \in \mathbb{Z}$. D.h. $a = b + cp^l$ oder

$$\begin{aligned} a^p &= (b + cp^l)^p \\ &= b^p + \binom{p}{1} b^{p-1} cp^l + A \\ &= b^p + \left(b^{p-1} cp^{l+1} + A\right) \end{aligned}$$

wobei $(cp^l)^2 | A$. Insbesondere $p^{l+1} | A$. □

Satz 39. *Angenommen* $l \geq 2$ *und* $p \geq 3$*. Dann gilt*

$$(1 + ap)^{p^{l-2}} \equiv 1 + ap^{l-1} \bmod p^l$$

für alle $a \in \mathbb{Z}$*.*

Beweis. Induktion über l. Der Fall $l = 2$ ist einfach die Aussage, daß $1 + ap = 1 + ap$. Sei daher $l > 2$ und $(1 + ap)^{p^{l-3}} \equiv 1 + ap^{l-2} \bmod p^{l-1}$. Nach Satz 38 ist

$$\left((1 + ap)^{p^{l-3}}\right)^p \equiv (1 + ap)^{p^{l-2}} \equiv \left(1 + ap^{l-2}\right)^p \bmod p^l.$$

Aber

$$\left(1 + ap^{l-2}\right)^p = 1 + p \cdot ap^{l-2} + B,$$

wobei

$$B = \sum_{i=2}^{p} \binom{p}{i} \left(ap^{l-2}\right)^i.$$

Für $i > 2$ (und $l \geq 3$) gilt $l \leq (l-2)i$; d.h. $p^l | p^{(l-2)i}$. Der besondere Fall $l = 3$, $i = 2$ ist

$$\binom{p}{2} \left(ap^{3-2}\right)^2 = \frac{p(p-1)}{2} \cdot a^2 p^2$$

und daher gilt auch

$$p^l = p^3 \left| \binom{p}{2} \left(ap^{3-2}\right)^2 = \binom{p}{2} a^2 p^2. \right.$$

□

Satz 40. *Wieder* $p \geq 3$*, und sei* $a \in \mathbb{Z}$ *mit* $p \not| a$*. Dann hat die Zahl* $1 + ap$ *die Ordnung* p^{l-1} *modulo* p^l*.*

Beweis. Sei $r \in \mathbb{N}$ die Ordnung von $1 + ap$ modulo p^l. Nach Satz 39 ist

$$(1 + ap)^{p^{l-1}} \equiv 1 + ap^l \bmod p^{l+1}$$

und daher $(1 + ap)^{p^{l-1}} \equiv 1 \bmod p^l$. D.h. $r | p^{l-1}$ und r ist eine Potenz von p. Welche Potenz? Da $p \not| a$ gilt

$$(1 + ap)^{p^{l-2}} \equiv 1 + ap^{l-1} \not\equiv 1 \bmod p^l.$$

Daher $r = p^{l-1}$. □

Satz 41. *Primitivwurzeln modulo* p^l *existieren, für alle ungerade Primzahlen* p *und* $l \in \mathbb{N}$*. Sei* g *eine beliebige Primitivwurzel modulo* p *mit* $g^{p-1} \not\equiv 1 \bmod p^2$*. Dann ist* g *auch Primitivwurzel modulo* p^l*.*

Beweis. Sei g eine Primitivwurzel modulo p. Falls $g^{p-1} \equiv 1 \bmod p^2$, sei $g' = g + p$. Dann ist $g' \equiv g \bmod p$ auch Primitivwurzel modulo p und

$$\begin{aligned} g'^{p-1} \equiv (g + p)^{p-1} &\equiv g^{p-1} + (p-1)g^{p-2}p \bmod p^2 \\ &\equiv 1 + (p-1)g^{p-2}p \bmod p^2 \\ &\not\equiv 1 \bmod p^2, \end{aligned}$$

da $p \not| p-1$ und $p \not| g^{p-2}$. Wir können daher einfach annehmen, daß g unsere Bedingung erfüllt ($g^{p-1} \not\equiv 1 \bmod p^2$).

Es bleibt nur zu zeigen, daß g auch Primitivwurzel modulo p^l ist, für alle $l \geq 2$. Sei nun $n \in \mathbb{N}$ irgendeine Zahl mit $g^n \equiv 1 \bmod p^l$. Es gilt

$$g^{p-1} \equiv 1 \bmod p \Longrightarrow g^{p-1} - 1 = ap$$

für ein $a \in \mathbb{Z}$. Aber

$$g^{p-1} \not\equiv 1 \bmod p^2 \Longrightarrow p^2 \not| g^{p-1} - 1 \Longrightarrow p \not| a.$$

Nach Satz 40 hat g^{p-1} die Ordnung p^{l-1} modulo p^l. Aber

$$1 \equiv (g^n)^{p-1} = \left(g^{p-1}\right)^n \bmod p^l.$$

Folglich gilt $p^{l-1}|n$, oder $n = cp^{l-1}$ mit $c \in \mathbb{Z}$. Nach Fermat's kleinem Satz ist $g^p \equiv g \bmod p$, daher auch

$$g^{p^2} = (g^p)^p \equiv g^p \equiv g \bmod p,$$

u.s.w. Insbesondere ist $g^{p^{l-1}} \equiv g \bmod p$. Da

$$g^n \equiv 1 \bmod p^l \Longrightarrow g^n \equiv 1 \bmod p,$$

folgt auch

$$g^n \equiv (g^{p^{l-1}})^c \equiv g^c \equiv 1 \bmod p.$$

Aber g ist Primitivwurzel modulo p. D.h. $p-1|c$. Da

$$\mathrm{ggt}(p-1, p^{l-1}) = 1$$

muß gelten

$$\phi(p^l) = (p-1)p^{l-1} | cp^{l-1} = n.$$

D.h. g ist Primitivwurzel modulo p^l. □

6.3 Der Fall 2^l, für $l \geq 2$

Es ist kein Geheimnis, daß 1 eine Primitivwurzel modulo 2, und 3 eine Primitivwurzel modulo 4 ist.

Satz 42. $5^{2^{l-3}} \equiv 1 + 2^{l-1} \bmod 2^l$ *für* $l \geq 3$.

Beweis. Induktion über l. Falls $l = 3$, dann ist dies die Gleichung $5 \equiv 1 + 4 \bmod 8$; offensichtlich doch wahr. Sei nun $l > 3$ und sei $5^{2^{l-4}} \equiv 1 + 2^{l-2} \bmod 2^{l-1}$. Nach Satz 38 gilt

$$\begin{aligned} 5^{2^{l-3}} = \left(5^{2^{l-4}}\right)^2 &= (1 + 2^{l-2})^2 \\ &= 1 + 2 \cdot 2^{l-2} + 2^{2l-4} \\ &= 1 + 2^{l-1} + 2^{2l-4} \\ &\equiv 1 + 2^{l-1} \bmod 2^l, \end{aligned}$$

da $2l - 4 \geq l$, für $l > 3$. □

Satz 43. *Die Ordnung von 5 modulo* 2^l *ist* 2^{l-2} *(wobei* $l \geq 3$*).*

Beweis. Sei n die Ordnung von 5 modulo 2^l. Da

$$5^{2^{l-2}} \equiv 1 + 2^l \bmod 2^{l+1},$$

gilt $5^{2^{l-2}} \equiv 1 \bmod 2^l$. Folglich muß $n|2^{l-2}$; insbesondere ist n eine Potenz von 2. Die nächstkleinste Möglichkeit ist $n = 2^{l-3}$. Aber $5^{2^{l-3}} \equiv 1 + 2^{l-1} \not\equiv 1 \bmod 2^l$. □

Satz 44. *Für* $l \geq 3$ *ist*

$$U(\mathbb{Z}_{2^l}) = \{(-1)^a 5^b \bmod 2^l : 0 \leq a \leq 1, 0 \leq b < 2^{l-2}\}$$

und diese Darstellung der Elemente von $U(\mathbb{Z}_{2^l})$ *ist eineindeutig.*

Beweis. $\phi(2^l) = 2^{l-1}$. (Die Hälfte der Zahlen, nämlich die ungeraden Zahlen, sind zu 2^l relativ prim.) Andererseits gibt es genau 2^{l-1} Paare der Art (a, b) mit $0 \leq a \leq 1$ und $0 \leq b < 2^{l-2}$. Sind sie alle verschieden? Falls

$$(-1)^{a'} 5^{b'} \equiv (-1)^a 5^b \bmod 2^l$$

dann ist auf jeden Fall $5^b = (1+4)^b = 1 + 4b + \cdots \equiv 5^{b'} \bmod 4$. Folglich ist $(-1)^a \equiv (-1)^{a'} \bmod 4$: daher $a' = a$ und $5^b \equiv 5^{b'} \bmod 2^l$. D.h. $5^{b-b'} \equiv 1 \bmod 2^l$, und nach Satz 43 gilt $2^{l-2} | b - b'|$. Daher $b \equiv b' \bmod 2^{l-2}$, und wir schließen, daß $b = b'$. □

Satz 45. $U(\mathbb{Z}_{2^l})$ *ist <u>nicht</u> zyklisch, falls* $l \geq 3$.

Beweis. Denn nach Satz 43 hat jedes Element der Art $(-1)^a 5^b$ die Ordnung 2^{l-2} modulo 2^l. □

Satz 46. *Die Zahlen* $n \in \mathbb{N}$*, die Primitivwurzeln, modulo* n *besitzen, sind genau die Zahlen 2, 4,* p^k *und* $2p^k$*, für beliebige ungerade Primzahlen* p *und* $k \in \mathbb{N}$.

Beweis. Da $U(\mathbb{Z}_{2p^k}) = U(\mathbb{Z}_{p^k})$, gibt es auch Primitivwurzeln modulo $2p^k$. Andererseits, sei $n \geq 2$ nicht von dieser Gestalt. Wir können dann schreiben $n = m_1 m_2$ mit $m_1, m_2 < n$ und $\text{ggt}(m_1, m_2) = 1$. D.h. $U(\mathbb{Z}_n) = U(\mathbb{Z}_{m_1}) \times U(\mathbb{Z}_{m_2})$, wobei $U(\mathbb{Z}_i)$ nicht trivial ist, für $i = 1, 2$. Aber eine solche Gruppe kann niemals zyklisch sein. Z.B. um einen Widerspruch zu finden, sei doch $g = (v, w) \in U(\mathbb{Z}_{m_1}) \times U(\mathbb{Z}_{m_2})$ eine Primitivwurzel. Dann gibt es nur zwei Lösungen der Gleichung $x^2 \equiv 1 \bmod n$, nämlich $x \equiv 1$ und $x \equiv g^{\phi(n)/2} \bmod n$.[5] Aber alle vier Elemente $(1,1)$, $(1,-1) \equiv (1, m_2 - 1)$, $(-1,1) \equiv (m_1 - 1, 1)$ und $(-1,-1) \equiv (m_1 - 1, m_2 - 1)$ sind doch verschiedene Lösungen in $U(\mathbb{Z}_n)$. Ein Widerspruch. □

7 Quadratische Reziprozität

Sei $p \in \mathfrak{P}$ eine ungerade Primzahl und sei $1 \leq a \leq p - 1$. Die Gleichung, die wir in diesem Kapitel betrachten werden, ist

$$x^2 \equiv a \bmod p.$$

Gibt es überhaupt eine Lösung? Falls ja, und falls $a \not\equiv 0 \bmod p$, dann heißt a ein 'quadratischer Rest' modulo p.

Falls $a = 1$, dann ist die Situation ziemlich trivial. Wir haben $1^2 \equiv 1 \bmod p$, aber auch $(-1)^2 \equiv (p-1)^2 \equiv 1 \bmod p$. Allgemeiner, sei u^2 ein quadratischer Rest modulo p. Dann ist sicherlich auch $u^2 \equiv (-u)^2 \equiv ((p-1)u)^2 \bmod p$. Da p ungerade ist, ist

$$u \not\equiv (p-1)u \bmod p.$$

D.h.

$$u - (p-1)u = 2u - up \not\equiv 0 \bmod p.$$

Aber die Gleichung $x^2 - a \equiv 0 \bmod p$ kann höchstens zwei verschiedene Lösungen besitzen. Falls daher x_0 eine Lösung ist, dann gibt es nur die zwei Lösungen $\pm x_0$.

Satz 47. *Für* p *eine ungerade Primzahl gibt es* $\frac{p-1}{2}$ *quadratische Reste modulo* p*, und die restlichen* $\frac{p-1}{2}$ *Zahlen sind infolgedessen nicht quadratische Reste modulo* p.

[5] Die Elemente der Gruppe sind $\{g, g^2, \ldots, g^t, \ldots, g^{\phi(n)} \equiv 1\}$. Für welche t gilt

$$(g^t)^2 = g^{2t} \equiv g^{\phi(n)} \equiv 1 \bmod n?$$

Da g eine Primitivwurzel ist, gilt doch $\phi(n) | 2t$, und dies ist nur möglich, falls $t = \phi(n)/2$ oder $t = \phi(n)$; d.h. $g^{\phi(n)/2}$ und $g^{\phi(n)} \equiv 1 \bmod n$.

Beweis. Seien

$$U = \{1, 2, \ldots, \frac{p-1}{2}\}, \quad \text{und} \quad V = \{\frac{p+1}{2}, \ldots, p-1\}.$$

Falls $u \in U$, dann ist sicherlich $-u = p - u \in V$. Auch $u^2 \equiv (-u)^2 \bmod p$. Und $u \not\equiv -u \bmod p$. Folglich gibt es $\frac{p-1}{2}$ *verschiedene* Zahlen der Art

$$1^2,\ 2^2, \ldots,\ \left(\frac{p-1}{2}\right)^2.$$

Die restlichen quadratischen Reste

$$(-1)^2,\ (-2)^2, \ldots,\ \left(-\frac{p-1}{2}\right)^2$$

geben die identische Menge. Daher gibt es keine weitere quadratische Reste. □

Definition 7.1. Sei p eine ungerade Primzahl, und sei $a \in \mathbb{Z}$. Das Legendre Symbol $\left(\frac{a}{p}\right)$ wird wie folgt definiert.

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{falls } p|a, \\ +1, & \text{falls } a \text{ ein quadratischer Rest modulo } p \text{ ist}, \\ -1, & \text{sonst.} \end{cases}$$

Satz 48. *Sei p eine ungerade Primzahl und sei $1 \leq a \leq p-1$. Dann gilt: a ist quadratischer Rest modulo p genau dann, wenn*

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p.$$

Beweis. Falls $x^2 \equiv a \bmod p$, dann ist

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

Umgekehrt, sei

$$a^{\frac{p-1}{2}} \equiv 1 \bmod p.$$

Sei g eine Primitivwurzel modulo p. Sei $g^n \equiv a \bmod p$. Dann ist

$$(g^n)^{\frac{p-1}{2}} = g^{(p-1)\frac{n}{2}} \equiv 1 \bmod p.$$

Da $p-1$ die Ordnung von g ist, folgt $p-1|(p-1)\frac{n}{2}$. D.h. $\frac{n}{2}$ ist eine ganze Zahl, und daher ist n gerade. Folglich ist

$$\left(g^{\frac{n}{2}}\right) \equiv a \bmod p.$$

□

Satz 49. *p, a wie vorher. Dann gilt*

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

Beweis. Nach Fermat's kleinem Satz ist $a^{p-1} \equiv 1 \bmod p$. D.h.

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

und daher $a^{\frac{p-1}{2}} \equiv \pm 1 \bmod p$. Nach Satz 48 ist dann a ein quadratischer Rest genau dann, wenn $\left(\frac{a}{p}\right) = 1$. Falls $p|a$, dann ist der Satz sowieso trivial. □

Satz 50. $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. *Insbesondere ist -1 ein quadratischer Rest modulo p nur dann, wenn $p \equiv 1 \bmod 4$.*

Satz 51. *Sei* p *eine ungerade Primzahl,* $p \not| a$ *und* $p \not| b$*. Dann ist*

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

Beweis. $(ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \bmod p$. □

Wir betrachten jetzt verschiedene Zahlen, der Art $ka \bmod p$, für $k = 1, 2, \ldots$. Jede solche Zahl ka ist entweder 'positiv'—d.h. $ka \equiv r \bmod p$ mit $1 \leq r \leq \frac{p-1}{2}$, oder 'negativ' mit $ka \equiv -r' \bmod p$ und $1 \leq r' \leq \frac{p-1}{2}$. Oder anders gesagt, die 'positiven' Zahlen sind

$$U = \{1, 2, \ldots, \frac{p-1}{2}\}$$

und die 'negativen' Zahlen sind

$$V = \{\frac{p+1}{2}, dots, p-1\}.$$

Satz 52 (Gauss's Lemma). *Wieder* $p \not| a$*. Dann ist* $\left(\frac{a}{p}\right) = (-1)^{\mu}$*, wobei* μ *die Anzahl der 'negativen' Zahlen (modulo* p*) in der Menge*[6] $W = \{a, 2a, \ldots, \frac{1}{2}(p-1)a\}$ *ist.*

Beweis. Kann es sein, daß $ka \equiv \pm la \bmod p$, für $1 \leq k, l \leq \frac{p-1}{2}$? (D.h. beide Zahlen $k, l \in U$.) Multipliziere auf beiden Seiten mit a^{-1}. Dann haben wir $k = \pm l$; aber für beide $k, l \in U$ muß gelten $k = +l$. Sei $\nu = \frac{p-1}{2} - \mu$ und sei $\{r_1, \ldots, r_\nu\}$ die Menge der 'positiven' Zahlen in W; dann ist $\{-r'_1, \ldots, -r'_\mu\}$ die Menge der 'negativen' Zahlen in W. Daher muß gelten

$$\{r_1, \ldots, r_\nu, r'_1, \ldots, r'_\mu\} = \{1, 2, \ldots, \frac{p-1}{2}\}.$$

Also ist

$$\begin{aligned} a \cdot 2a \cdot \cdots \cdot \frac{1}{2}(p-1)a &\equiv 1 \cdot 2 \cdot 3 \cdots \frac{1}{2}(p-1)a^{\frac{p-1}{2}} \\ &\equiv r_1 \cdot r_2 \cdots r_\nu \cdot (-r'_1) \cdot (-r'_2) \cdots (-r'_\mu) \\ &\equiv (-1)^{\mu} 1 \cdot 2 \cdot 3 \cdots \frac{1}{2}(p-1) \bmod p \end{aligned}$$

und

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

□

Satz 53. $\left(\frac{2}{p}\right) \equiv 2^{\frac{1}{2}(p-1)} \equiv (-1)^{\frac{1}{8}(p^2-1)} \bmod p$*. Mit anderen Worten: 2 ist ein quadratischer Rest modulo* p *genau dann, wenn* $p \equiv \pm 1 \bmod 8$*.*

Beweis. $\{1 \cdot 2,\ 2 \cdot 2,\ 3 \cdot 2, \ldots, \left(\frac{p-1}{2}\right) \cdot 2\} = \{2, 4, 6, \ldots, p-1\}$ sind hier die entsprechenden Zahlen. Es gibt demnach zwei Fälle:

1. Falls $\frac{p-1}{2}$ gerade ist, dann ist $\mu = \frac{p-1}{4}$ und

$$\left(\frac{2}{p}\right) \equiv (-1)^{\frac{1}{4}(p-1)} \bmod p.$$

2. Falls $\frac{p-1}{2}$ ungerade ist, dann ist $\mu = \frac{p+1}{4}$ und

$$\left(\frac{2}{p}\right) \equiv (-1)^{\frac{1}{4}(p+1)} \bmod p.$$

[6] Einfachheitshalber schreiben wir hier a, $2a$, u.s.w. Aber gemeint ist natürlich stets $a \bmod p$, $2a \bmod p$, u.s.w.

Es ist jetzt nur eine kleine Übung, zu zeigen[7], daß in beiden Fällen

$$\mu \equiv \frac{1}{8}(p^2 - 1) \bmod 2.$$

□

Satz 54 (über die quadratische Reziprozität). *Seien $p, q \in \mathfrak{P}$ ungerade Primzahlen. Dann gilt*

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

Wir brauchen einige weitere Ideen, bevor wir diesen Satz beweisen können. Zuerst, um die Formeln einfacher zu gestalten, sei $p' := \frac{p-1}{2}$ und $q' := \frac{q-1}{2}$. Die Berechnung von $\left(\frac{q}{p}\right)$ benutzte die Zahlen $kq \bmod p$. Eine andere Art, solche Zahlen darzustellen, ist die folgende.

$$kq = p\left\lceil \frac{kq}{p} \right\rceil + u_k,$$

wobei $1 \leq u_k \leq p-1$ und $u_k \equiv kq \bmod p$. Für $k = 1, \ldots, p'$ durchläuft dann u_k die Zahlen r_i, $i = 1, \ldots, \nu$ und $-r'_j$, $j = 1, \ldots, \mu$. Wir unterscheiden die zwei Fälle:

1. Falls u_k 'positiv' ist (d.h. $1 \leq u_k \leq p'$), dann schreibe $u_k = v_k$.
2. Falls u_k 'negativ' ist (d.h. $p' < u_k \leq p-1$), dann schreibe $u_k = w_k$; daher $1 \leq (p - w_k) \leq p'$ und $r'_i = p - w_k$, für ein i zwischen 1 und μ.

Sei nun

$$R = \sum_{i=1}^{\nu} r_i = \sum_{k=1}^{p'} v_k,$$

(wo wir $v_k = 0$ nehmen, falls u_k 'negativ' ist) und

$$R' = \sum_{j=1}^{\mu} r'_j = \mu p - \sum_{k=1}^{p'} w_k.$$

(Dieses mal ist $w_k = 0$, falls u_k 'positiv' ist.) Es gilt

$$R + R' = \sum_{k=1}^{p'} k = \frac{1}{2}p'(p'+1) = \frac{(p-1)(p+1)}{8} = \frac{p^2-1}{8}.$$

Aber auch

$$R + R' = \sum_{k=1}^{p'} v_k + \mu p - \sum_{k=1}^{p'} w_k.$$

Daher

$$\mu p + \sum_{k=1}^{p'} v_k - \sum_{k=1}^{p'} w_k = \frac{1}{8}(p^2 - 1).$$

Sei nun

$$S(q,p) = \sum_{s=1}^{p'} \left\lceil \frac{sq}{p} \right\rceil.$$

[7] Bemerkung: sei die ungerade Zahl $p = 2n+1$, $n \in \mathbb{N}$. Dann ist $p^2 = 4n^2 + 4n + 1$ und folglich ist $p^2 - 1 = 4(n^2 + n)$ durch 8 teilbar, egal ob n gerade oder ungerade ist.

Dann ist

$$\begin{aligned}\frac{1}{8}(p^2-1)q = \left(\sum_{k=1}^{p'} k\right) q &= \sum_{k=1}^{p'} kq \\ &= \sum_{k=1}^{p'} \left(p\left\lceil\frac{kq}{p}\right\rceil + u_k\right) \\ &= pS(q,p) + \sum_{k=1}^{p'} u_k \\ &= pS(q,p) + \sum_{k=1}^{p'} v_k + \sum_{k=1}^{p'} w_k.\end{aligned}$$

Wir subtrahieren die zwei Gleichungen:

$$\frac{1}{8}(p^2-1)(q-1) = pS(q,p) - \mu p + 2\sum_{k=1}^{p'} w_k.$$

Nun, $8|p^2-1$, und $q-1$ ist gerade. Daher ist die linke Seite dieser Gleichung gerade. Außerdem ist p ungerade. Daher muß gelten

Satz 55. $S(q,p) \equiv \mu \bmod 2$. *D.h.* $\left(\frac{q}{p}\right) = (-1)^{\mu} = (-1)^{S(q,p)}$.

Folglich ist $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{S(q,p)+S(p,q)}$. Um Satz 54 zu beweisen, brauchen wir nun lediglich....

Satz 56. $S(q,p) + S(p,q) = p'q'$.

Beweis. Seien $s,t \in \mathbb{N}$ mit $s \le p'$, $t \le q'$. Da p und q prim sind, gilt $\operatorname{ggt}(p,q) = 1$; da $s \le p'$ und $t \le q'$, ist $\frac{s}{t} \neq \frac{p}{q}$. Tatsächlich ist entweder

- $\frac{s}{t} < \frac{p}{q}$; d.h. $s \le \left\lceil\frac{tp}{q}\right\rceil$ oder
- $\frac{s}{t} > \frac{p}{q}$; d.h. $t \le \left\lceil\frac{sq}{p}\right\rceil$.

Daher ist

$$\begin{aligned}p'q' &= \sum_{s=1}^{p'}\sum_{t=1}^{q'} 1 \\ &= \underbrace{\left(\sum_{s=1}^{p'}\sum_{t=1}^{q'} 1\right)}_{s\le\left\lceil\frac{tp}{q}\right\rceil} + \underbrace{\left(\sum_{s=1}^{p'}\sum_{t=1}^{q'} 1\right)}_{t\le\left\lceil\frac{sq}{p}\right\rceil} \\ &= \sum_{t=1}^{q'}\left(\sum_{s=1}^{\left\lceil\frac{tp}{q}\right\rceil} 1\right) + \sum_{s=1}^{p'}\left(\sum_{t=1}^{\left\lceil\frac{sq}{p}\right\rceil} 1\right) \\ &= \sum_{t=1}^{q'}\left\lceil\frac{tp}{q}\right\rceil + \sum_{s=1}^{p'}\left\lceil\frac{sq}{p}\right\rceil \\ &= S(p,q) + S(q,p)\end{aligned}$$

□

8 Einige Diophantinische Gleichungen

Satz 57. *Sei* p *eine ungerade Primzahl und sei* $p \not| m, k$*. Angenommen, die Diophantinische Gleichung* $x^2 - my^2 = kp$ *ist lösbar. Dann gilt* $\left(\frac{m}{p}\right) = 1$*.*

Beweis. Kann es sein, daß $p|x$? In diesem Fall wäre auch $p|y$, da $p \not| m$. Folglich wäre $p^2|x^2 - my^2 = kp$; ein Widerspruch. Daher ist $p \not| x$, und dieselbe Idee gibt auch $p \not| y$. D.h. $x, y \in U(\mathbb{Z}_p)$ und $x^2 \equiv my^2 \bmod p$, oder $m \equiv \left(xy^{-1}\right)^2 \bmod p$; ein quadratischer Rest. □

Satz 58 (Thue's Satz). *Sei* $n \in \mathbb{N}$ *keine Quadratzahl (d.h. kein* $m \in \mathbb{N}$ *existiert, mit* $m^2 = n$*) und sei* $z \in \mathbb{Z}$ *beliebig. Dann existieren zwei Zahlen* $x, y \in \mathbb{Z}$*, nicht beide gleich null, mit* $|x|, |y| < \sqrt{n}$ *und*

$$xz \equiv y \bmod n.$$

Beweis. Es gilt $\lceil \sqrt{n} + 1 \rceil^2 > n$. D.h. es gibt mehr als n Paare von Zahlen (x, y) mit

$$1 \leq x, y \leq \lceil \sqrt{n} + 1 \rceil,$$

aber nur n Zahlen in $\mathbb{Z}_n$. Daher gibt es zwei <u>verschiedene</u> Paare $(x_1, y_1) \neq (x_2, y_2)$ mit

$$x_1 z - y_1 \equiv x_2 z - y_2 \bmod n.$$

D.h.

$$(x_1 - x_2)z \equiv (y_1 - y_2) \bmod n$$

und entweder $x_1 - x_2 \neq 0$ oder $y_1 - y_2 \neq 0$ und

$$|x_1 - x_2|,\ |y_1 - y_2| \leq \lceil \sqrt{n} + 1 \rceil - 1 < \sqrt{n}.$$

□

Satz 59. *Sei* p *eine ungerade Primzahl. Dann existieren* x *und* y *mit* $p = x^2 + y^2$ *genau dann, wenn* $p \equiv 1 \bmod 4$*.*

Beweis.

$$\begin{aligned} \text{Falls} \quad p = x^2 + y^2 &\implies x^2 \equiv -y^2 \bmod p \\ &\implies \left(xy^{-1}\right)^2 \equiv -1 \bmod p \\ &\implies p \equiv 1 \bmod 4 \quad \text{(Satz 50)} \end{aligned}$$

Andererseits, falls $p \equiv 1 \bmod 4$, dann existiert $z \in U(\mathbb{Z}_p)$ mit $z^2 \equiv -1 \bmod p$. Nach Thue's Satz gibt es x und y mit $|x|, |y| < \sqrt{p}$ und $xz \equiv y \bmod p$.

$$\begin{aligned} &\implies (xz)^2 \equiv -x^2 \equiv y^2 \bmod p \\ &\implies x^2 + y^2 \equiv 0 \bmod p \\ &\implies x^2 + y^2 = p, \end{aligned}$$

da $x^2 + y^2 < p + p = 2p$. □

Satz 60. *Sei* $\left(\frac{m}{p}\right) = 1$*. Dann existieren* x*,* y*, (nicht beide null) und* k *mit* $|k| \leq |m|$ *und* $x^2 - my^2 = kp$*.*

Beweis. Da $\left(\frac{m}{p}\right) = 1$, gibt es ein z mit $z^2 \equiv m \bmod p$. Nach Thue's Satz existieren dann x, y, nicht beide null, $|x|, |y| < \sqrt{p}$ und $zy \equiv x \bmod p$. D.h. $my^2 \equiv x^2 \bmod p$ und daher $x^2 - my^2 = kp$ für ein $k \in \mathbb{Z}$. Wie gross ist k? Es gilt

$$\begin{aligned} |k|p = |kp| &= \left|x^2 - my^2\right| \\ &\leq x^2 + |m|y^2 \\ &< p + |m|p \\ &= p(1 + |m|) \\ \implies |k| < 1 + |m| &\implies |k| \leq |m|. \end{aligned}$$

□

Satz 61. *Sei $p \in \mathcal{P}$ eine ungerade Primzahl. Dann existieren $x, y \in \mathbb{Z}$ mit*

$$x^2 - y^2 = p.$$

Beweis. Nehme

$$x = \frac{p+1}{2}, \quad y = \frac{p-1}{2}.$$

Dann ist

$$x^2 - y^2 = (x+y)(x-y) = p \cdot 1 = p.$$

□

Satz 62. *Sei p ungerade. Dann gilt $\left(\frac{-2}{p}\right) = 1 \iff x$ und y existieren, mit $x^2 + 2y^2 = p$.*

Beweis. '$\Longrightarrow$' Falls $\left(\frac{-2}{p}\right) = 1$ dann existiert ein z mit $z^2 \equiv -2 \bmod p$. Nach Thue's Satz existieren x, y, nicht beide null, $|x|, |y| < \sqrt{p}$ und $zy \equiv x \bmod p$. D.h.

$$-2y^2 \equiv x^2 \bmod p$$

oder

$$x^2 + 2y^2 \equiv 0 \bmod p.$$

Aber $x^2 + 2y^2 < p + 2p = 3p$. Kann es sein, daß $x^2 + 2y^2 = 2p$? Dann ist x gerade, etwa $x = 2n$. Daher $4n^2 + 2y^2 = 2p$, oder $y^2 + 2n^2 = p$. Dies ist auch eine Lösung.

'$\Longleftarrow$' $x^2 + 2y^2 = p \Rightarrow x \neq 0 \neq y$. Daher

$$-2 \equiv \left(xy^{-1}\right)^2 \bmod p$$

und $\left(\frac{-2}{p}\right) = 1$. □

Satz 63. *Sei p ungerade. Dann gilt $\left(\frac{2}{p}\right) = 1 \iff x$ und y existieren, mit $x^2 - 2y^2 = p$.*

Beweis. '$\Longleftarrow$' ist wie oben. Für '$\Longrightarrow$', sei $z^2 \equiv 2 \bmod p$. Wie immer, existieren x, y mit $zy \equiv x \bmod p$ oder $x^2 - 2y^2 = kp$. Was ist k? Da $x^2 < p$ und $y^2 < p$, folgt $k = 0$ oder ± 1. Nun, $k = 0$ ist nicht möglich, da $\sqrt{2} \notin \mathbb{Q}$. Falls $k = -1$, dann setze

$$\begin{aligned} u &= x + 2y \\ v &= x + y. \end{aligned}$$

$$\Longrightarrow u^2 - 2v^2 = (x+2y)^2 - 2(x+y)^2 = -x^2 + 2y^2 = p.$$

□

8.1 Die Gleichung $x^2 + y^2 = z^2$

Es ist sicherlich bekannt, daß diese Gleichung lösbar ist. Z.B. $3^2 + 4^2 = 5^2$. Wir verlieren nichts, wenn wir annehmen, daß $\mathrm{ggt}(x, y) = 1$. Für jedes $n \in \mathbb{N}$ gilt[8] entweder $n^2 \equiv 0 \bmod 4$ oder $n^2 \equiv 1 \bmod 4$. Folglich ist eine der beiden Zahlen gerade, die andere ungerade. Allgemeiner gilt...

Satz 64. *Jede positive Lösung von $x^2 + y^2 = z^2$ mit $ggt(x, y) = 1$ und $2|x$ ist von der Art*

$$x = 2ab, \quad y = a^2 - b^2, \quad , z = a^2 + b^2$$

wobei beliebige Paare (a, b), die die Bedingungen: $a > b > 0$, $ggt(a, b) = 1$, $a \not\equiv b \bmod 2$ erfüllen, genommen werden können.

[8] Falls $n = 2m$ gerade, dann ist $n^2 = 4m^2 \equiv 0 \bmod 4$. Falls $n = 2m + 1$ ungerade, dann ist $n^2 = 4m^2 + 4m + 1 \equiv 1 \bmod 4$.

Beweis. Zuerst nehme a, b beliebig mit $a > b > 0$ und $\text{ggt}(a,b) = 1$, wobei $a \not\equiv b \bmod 2$. Die Gleichung

$$x^2 + y^2 = (2ab)^2 + (a^2 - b^2)^2 = (a^2 + b^2)^2 = z^2$$

ist klar. Da $\text{ggt}(a,b) = 1$ folgt $\text{ggt}(x,y) = 1$ oder 2.[9] Aber $2 \not| y = a^2 - b^2$, eine ungerade Zahl. Daher ist $\text{ggt}(x,y) = 1$.

Sei jetzt $x^2 + y^2 = z^2$ eine gegebene Lösung (mit unseren Bedingungen), und nehme die Integerzahlen $\frac{z-y}{2}$ und $\frac{z+y}{2}$. Wir haben[10]

$$\begin{aligned} \text{ggt}\left(\frac{z-y}{2}, \frac{z+y}{2}\right) &= \text{ggt}\left(\frac{z-y}{2} + \frac{z+y}{2}, \frac{z+y}{2} - \frac{z-y}{2}\right) \\ &= \text{ggt}(y,z) \\ &= \text{ggt}(x,y) = 1 \end{aligned}$$

und

$$\left(\frac{x}{2}\right)^2 = \left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right).$$

Daher sind sie beide Quadratzahlen, und wir nehmen

$$a = \sqrt{\frac{z+y}{2}}, \quad b = \sqrt{\frac{z-y}{2}}.$$

□

9 Summen von Quadratzahlen

Wir haben schon gesehen (Satz 59), daß alle Primzahlen der Art $p \equiv 1 \bmod 4$ als Summe von zwei Quadratzahlen dargestellt werden können. In diesem Kapitel werden wir sehen, daß <u>alle</u> positive Integerzahlen n als Summe

$$n = a^2 + b^2 + c^2 + d^2,$$

mit $a, b, c, d \in \mathbb{Z}$ dargestellt werden können. Wir benutzen hierbei die folgende, interessante Schreibweise.

Definition 9.1. Sei $m \in \mathbb{N}$. Dann ist die Menge $\boxed{m} \subset \mathbb{N}$ die Menge aller natürlichen Zahlen, die als Summe von m Quadratzahlen erscheinen.

Mit dieser Schreibweise kann Satz 59 dann wie folgt formuliert werden: Falls $p \in \mathcal{P}$ mit $p \equiv 1 \bmod 4$, dann ist $p \in \boxed{2}$.

Satz 65. *Seien* $a, b \in \boxed{2} \Longrightarrow ab \in \boxed{2}$.

Beweis. Sei etwa $a = x_a^2 + y_a^2$ und $b = x_b^2 + y_b^2$. Dann ist

$$(x_a^2 + y_a^2)(x_b^2 + y_b^2) = (x_a x_b + y_a y_b)^2 + (x_a y_b - y_a x_b)^2$$

□

Satz 66. *Sei* $p \in \mathcal{P}$ *mit* $p \equiv 3 \bmod 4$. *Dann ist* $p \notin \boxed{2}$.

Beweis. Denn $x^2 \equiv 0$ oder $1 \bmod 4$, für alle mögliche Integerzahlen $x \in \mathbb{Z}$. □

Allgemeiner gilt

[9] Ein gemeinsamer Teiler von x und y teilt offensichtlich auch z, da doch $x^2 + y^2 = z^2$. Folglich teilt er sowohl $y + z = 2a^2$ als auch $z - y = 2b^2$. Aber $\text{ggt}(2a^2, 2b^2) = 2$.

[10] Falls u gerade und v ungerade dann ist $\text{ggt}(u,v) = \text{ggt}(u+v, u-v)$. Denn sei $d = \text{ggt}(u+v, u-v)$. Es gilt

$$d|(u+v) + (u-v) = 2u.$$

Auch $d|2v$. Aber $u + v$ ist ungerade. Daher $d|u$ und $d|v$.

Satz 67. *Sei* $n = 2^{\alpha} p_1^{\alpha_1} \cdots p_k^{\alpha_k}$*, die Primfaktorzerlegung von* n*. Dann gilt* $n \in \boxed{2}$ *genau dann, wenn* α_i *gerade ist, für alle* p_i *mit* $p_i \equiv 3 \bmod 4$*.*

Beweis. '$\Longleftarrow$' Es gilt $2 \in \boxed{2}$, da $2 = 1^2 + 1^2$. Auch $p_i \in \boxed{2}$, falls $p_i \equiv 1 \bmod 4$. Aber auch $p_j^2 = p_j^2 + 0^2 \in \boxed{2}$, obwohl $p_j \equiv 3 \bmod 4$. Daher ist $n \in \boxed{2}$ nach Satz 65.

'$\Longrightarrow$' Wir benutzen Induktion über n. Sei $n = a^2 + b^2$ und nehme ein $p \in \mathcal{P}$ mit $p|n$ und $p \equiv 3 \bmod 4$. D.h. $a^2 + b^2 \equiv 0 \bmod p$. Falls $p \not| a$, dann ist a eine Einheit modulo p und daher existiert ein w mit $aw \equiv 1 \bmod p$. Daher

$$0 \equiv w^2(a^2 + b^2) \equiv 1 + w^2 b^2 \bmod p.$$

Folglich ist $\left(\frac{-1}{p}\right) = 1$ und $p \equiv 1 \bmod 4$; ein Widerspruch. Daher ist sowohl $p|a$ als auch $p|b$ und

$$p^2 | a^2 + b^2 = n.$$

Sei nun $n = p^2 n_1$. Da $n_1 < n$, ist $n_1 \in \boxed{2}$ nach der induktiven Hypothese (und trivialerweise ist auch $p^2 \in \boxed{2}$). Daher ist nach Satz 65 auch $n \in \boxed{2}$. □

Satz 68. $x, y \in \boxed{4} \Longrightarrow xy \in \boxed{4}$.

Beweis. Seien

$$\begin{aligned} x &= x_1^2 + x_2^2 + x_3^2 + x_4^2 \quad \text{und} \\ y &= y_1^2 + y_2^2 + y_3^2 + y_4^2. \\ \Longrightarrow x \cdot y &= (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 \\ &\quad + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 \\ &\quad + (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 \\ &\quad + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2. \end{aligned}$$

□

Satz 69. $p \in \boxed{4}$ *für alle* $p \in \mathcal{P}$*.*

Beweis. Wir brauchen nur den Fall $p \equiv 3 \equiv -1 \bmod 4$ zu betrachten. Für solche p's gilt $\left(\frac{-1}{p}\right) = -1$ (Satz 50). Sei nun $0 < b < p$ die kleinste Zahl mit $\left(\frac{b}{p}\right) = -1$. Wir haben

$$\left(\frac{-b}{p}\right) = \left(\frac{-1 \cdot b}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{b}{p}\right) = (-1)(-1) = +1.$$

Daher existiert $x \in \mathbb{Z}_p$ mit $x^2 \equiv -b \bmod p$. Nehme insbesondere ein $x \in \mathbb{Z}$ in mit[11]

$$-\frac{(p-1)}{2} \leq x \leq +\frac{(p-1)}{2},$$

daher $|x| < \frac{p}{2}$. Da b als kleinste solche Zahl gewählt worden ist, gilt $\left(\frac{b-1}{p}\right) = +1$. Sei $y^2 \equiv b - 1 \bmod p$ und $|y| < \frac{p}{2}$. Wir haben

$$x^2 + y^2 + 1 \equiv -b + b - 1 + 1 \equiv 0 \bmod p$$

oder $x^2 + y^2 + 1 = gp$ für ein $1 \leq g < p$.

Sei $M_p = \{1 \leq m < p : mp \in \boxed{4}\}$. Es gilt dann $g \in M_p \neq \emptyset$. Sei h die kleinste Zahl in M_p. Es ist unser Ziel, zu zeigen, daß $h = 1$. Um einen Widerspruch zu finden, sei angenommen, daß $h > 1$. Nun, sei

$$hp = x_1^2 + x_2^2 + x_3^2 + x_4^2$$

und nehme jeweils $y_i \equiv x_i \bmod h$ mit $-\frac{h}{2} < y_i \leq \frac{h}{2}$. Kann es sein, daß $y_i = 0$, für $i = 1, \ldots, 4$? Dann wäre

$$h^2 | x_1^2 + x_2^2 + x_3^2 + x_4^2 = hp.$$

[11] Falls $x = \frac{p+1}{2}$, dann ist $x \equiv \frac{p+1}{2} - p \equiv -\frac{p-1}{2} \bmod p$.

Folglich $h|p$; ein Widerspruch. Aber $\sum_{i=1}^{4} y_i^2 \equiv 0 \bmod h$, daher $\sum_{i=1}^{4} y_i^2 = kh$, mit $k \geq 1$. Es gilt

$$k = \frac{y_1^2 + y_2^2 + y_3^2 + y_4^2}{h} \leq \frac{4\left(\frac{h}{2}\right)^2}{h} = h.$$

Behauptung: $k < h$, denn sonst wäre $y_i = \frac{h}{2}$, für $i = 1, \ldots, 4$. (Insbesondere wäre h gerade) und dann

$$x_i \equiv y_i = \frac{h}{2} \bmod h$$

und[12]

$$x_i^2 \equiv \left(\frac{h}{2}\right)^2 \bmod h^2.$$

Aber das heißt

$$hp \equiv x_1^2 + x_2^2 + x_3^2 + x_4^2 \equiv 4\left(\frac{h}{2}\right)^2 \equiv h^2 \equiv 0 \bmod h^2.$$

Folglich $h|p$; ein Widerspruch.

Nach Satz 68 gibt es vier Integerzahlen $z_1, \ldots, z_4$ mit

$$(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = z_1^2 + z_2^2 + z_3^2 + z_4^2,$$

mit $z_1 = \sum_{i=1}^{4} x_i y_i$, u.s.w. Aber $\sum_{i=1}^{4} x_i^2 = ph$ und $\sum_{i=1}^{4} y_i^2 = kh$. Daher

$$\sum_{i=1}^{4} z_i^2 = ph^2k.$$

Es gilt

$$z_1 \equiv \sum_{i=1}^{4} x_i y_i \equiv \sum_{i=1}^{4} x_i^2 \equiv 0 \bmod h.$$

Allgemeiner, $x_i y_j \equiv x_j y_i \bmod h$, und so

$$z_2 \equiv z_3 \equiv z_4 \equiv 0 \bmod h.$$

Für jedes $i = 1, \ldots, 4$ sei $z_i = u_i h$ etwa, und dann $z_i^2 = u_i^2 h^2$. Dann gilt

$$ph^2k = \sum_{i=1}^{4} u_i^2 h^2$$

oder $pk = \sum_{i=1}^{4} u_i^2 \in \boxed{4}$; ein Widerspruch, da $k < h$. □

Insgesamt haben wir daher bewiesen...

Satz 70. $\boxed{4} = \mathbb{N}$.

Dieser Satz ist vor längerer Zeit von Lagrange bewiesen worden. Eine verallgemeinerte Frage ist die folgende. Für jedes $k \in \mathbb{N}$ sei $g(k)$ die kleinste Zahl (falls existent), mit der Eigenschaft, daß für alle $n \in \mathbb{N}$ existieren $x_1, \ldots, x_{g(k)} \in \mathbb{Z}$ mit

$$n = \sum_{i=1}^{g(k)} x_i^k.$$

Was ist $g(k)$? Wir haben gerade bewiesen, daß $g(2) = 4$. Im allgemeinen hat Hilbert gezeigt, daß $g(k) < \infty$, für alle k.

[12] Sei $x_i = h/2 + ch = h(1/2 + c)$ mit $c \in \mathbb{Z}$. Dann ist

$$x_i^2 = h^2\left(\frac{1}{4} + c + c^2\right) = \left(\frac{h}{2}\right)^2 + h^2\left(c + c^2\right) = \left(\frac{h}{2}\right)^2 + dh^2,$$

wobei $d \in \mathbb{Z}$.

10 Das RSA Kryptosystem

Es geht darum, einen Text zu verschlüsseln und danach wieder zu entschlüsseln. Z.B. etwa die Standardnachricht in der Informationstechnologie: “Hallo Welt!”

Vielleicht ist das primitivste System, einfach den Buchstaben Zahlen zuzuordnen. Dadurch wird ‘a’ zu 1, ‘b’ zu 2, u.s.w. bis ‘z’ zu 26 zugeordnet. Unsere Standardnachricht hieße dann

$$8:1:12:12:15::23:5:12:20$$

Dieses System ist nicht besonders sicher!

Im Allgemeinen, wird in diesem System eine Kette von Zahlen

$$n_1, n_2, \ldots, n_m$$

gesendet.

Um die Sicherheit zu erhöhen, ist man auf die Idee gekommen, irgendeine feste Zahl a zu nehmen. Die gesendete Nachricht wird dann weiter verschlüsselt, indem jeweils die Zahl

$$n_i + a \bmod 26,$$

statt einfach n_i gesendet wird.

Lange Zeit galt diese Methode als sicher genung. Trotzdem gibt es die Möglichkeit, auch solche Systeme zu entschlüsseln, ohne die Zahl a vorher zu kennen. Man braucht nur die 26 verschiedenen möglichen a's auszuprobieren, um zu sehen, ob etwas Vernünftiges herauskommt.

Die nächste Idee war, eine vorgegebene Folge von Zahlen

$$a_1, a_2, \ldots, a_m$$

zu benutzen, um dann jeweils die Zahl

$$n_i + a_i \bmod 26$$

zu senden. Dieses System ist sicherlich viel schwieriger zu entschlüsseln als das einfachere System mit nur einem einzigen a. Das Problem ist jedoch, daß die Folge $a_1, a_2, \ldots, a_m$ vorhanden sein muß, sowohl für das Verschlüsseln als auch für das Entschlüsseln. Eine Möglichkeit wäre, z.B. einen allgemein bekannten Text zu nehmen — etwa Shakespear's ‘Hamlet’ — und dann wird die Buchstabenfolge aus einer bestimmten Szene genommen, um die Folge der a_i zu bestimmen. Die Schwierigkeit hier liegt darin, daß die Möglichkeit des Verrats doch sehr groß ist.[13]

Das RSA Verschlüsselungssystem ist die Lösung. Es wird überall im Internet benutzt. Dabei kann etwa ein privater PC (auch wenn er voll mit Viren, Würmern, Troyanern, u.s.w. ist) Nachrichten verschlüsseln, und trotzdem bleiben diese Nachrichten unlesbar für Außenseiter. Nur der *eigentliche* Empfänger kann die Nachricht entschlüsseln.

Wie funktioniert es?

10.1 Der Algorithmus

Die Zahlen p, q, e, und d

1. Wähle zwei große (größer als 10^{100} oder so), verschiedene Primzahlen p und q. Sei $N = pq$.
2. Dann ist $\phi(N) = (p-1)(q-1)$.
3. Wähle eine Zahl e zwischen 1 und $\phi(N)$ mit $\mathrm{ggt}(e, \phi(N)) = 1$. (Hier gibt es, wie bei der Wahl der Primzahlen p und q, *sehr* viele Möglichkeiten!)
4. Finde die Zahl d, mit $ed \equiv 1 \bmod \phi(N)$.

Nun, “die Zentrale” (z.B. die Bank) veröffentlicht die Zahlen N und e. Die Zahlen p, q, und d bleiben geheim im Tresor bei der Zentrale. Der folgende Algorithmus wird “öffentlich” verwendet, um eine Nachricht zu verschlüsseln.

[13] Und tatsächlich führte dieses System zu verschiedenen, unschönen menschlichen Tragödien! Wie schön ist es, daß die Mathematik imstande ist, solche Umstande aufzulösen.

Die Verschlüsselung

Zunächst wird nicht einfach Buchstabe für Buchstabe verschlüsselt, wie vorher. Stattdessen werden Blöcke von Buchstaben, etwa jeweils 25 Buchstaben lang, gebildet. Ein Block ist dann eine große Zahl, etwa die Zahl

$$K = \sum_{i=1}^{25} n_i \cdot 100^{i-1}.$$

Diese Zahlen werden dann eine nach der anderen verschlüsselt. Und zwar ist die verschlüsselte Version von K die Zahl

$$C = K^e \bmod N.$$

Die Entschlüsselung

ist ziemlich trivial. Es gilt

$$K = C^d \bmod N.$$

Warum funktioniert es?

Daß heißt, wir müssen zunächst zeigen, daß $K \equiv C^d = K^{ed} \bmod N$, für alle $0 \leq K < N$. Nun, da $ed \equiv 1 \bmod \phi(N)$ folgt, daß ein $u \in \mathbb{Z}$ existiert, mit

$$ed = 1 + u\phi(N).$$

Falls $K \in U(\mathbb{Z}_N)$, gilt nach Fermat's kleinem Satz:

$$K^{ed} \equiv K^{1+u\phi(N)} = K \cdot \left(K^{\phi(N)}\right)^u \equiv K \cdot 1^u = K \bmod N.$$

Andererseits, falls etwa $p|K$, dann ist $K \equiv 0 \bmod p$. Daher

$$K^{ed} \equiv K \equiv 0 \bmod p.$$

Aber auch (wieder Fermat's kleiner Satz)

$$K^{ed} \equiv K^{1+u\phi(N)} \equiv K \cdot K^{u\phi(N)} \equiv K \cdot K^{u(p-1)(q-1)} \equiv K \cdot \left(K^{q-1}\right)^{u(p-1)} \equiv K \cdot 1^{u(p-1)} = K \bmod q.$$

Nach dem Chinesischen Restwertsatz ist dann auch wieder

$$K^{ed} \equiv K \bmod N.$$

(Natürlich ist der Fall $q|K$ analog.)

Warum ist die Entschlüsslung schwierig für einen Außenseiter?

Obwohl kein formaler Beweis existiert, daß die Primfaktorisierung von großen Zahlen schwierig sein muß, scheint es trotzdem in der Praxis unmöglich zu sein, Zahlen von der Art $N = pq$, wobei beide Primzahlen p und q groß sind, zu faktorisieren. Aber alle (wahrscheinlich falschen) Versuche, N als Primproduckt darzustellen

$$N \stackrel{??}{=} p_1 q_1$$

werden *ganz* andere Zahlen

$$\phi_{??}(N) \stackrel{??}{=} (p_1 - 1)(q_1 - 1)$$

liefern. Daher gibt es ganz falsche Werte für $d_1 \stackrel{??}{\equiv} e^{-1} \bmod \phi_{??}(N)$. Für solche falsche Versuche gibt es (fast) mit Sicherheit die Ungleichung

$$K^{ed_1} \not\equiv K \bmod N.$$

11 Wie findet man große Primzahlen?

Sei $n \in \mathbb{N}$ eine ungerade Zahl. Falls n prim ist, dann (nach Satz 27) gibt es ein Primitivwurzel modulo n. Sei x ein solcher Primitivwurzel. Dann ist die Ordnung von x modulo n genau $n-1$. D.h.

$$x^{n-1} \equiv 1 \bmod n$$

und

$$x^m \not\equiv 1 \bmod n,$$

für alle $1 \leq m < n-1$.

Es ist zwar richtig, daß Primzahlpotenzen auch Primitivwurzel besitzen (Satz 41). Aber ein Primitivwurzel für p^l (wobei p eine ungerade Primzahl ist) hat die Ordnung $\phi(p^l) = p^{l-1}(p-1) \neq p^l - 1$. Daher gilt: eine ungerade Zahl n ist prim genau dann, wenn eine Zahl x existiert mit Ordnung $n-1$ modulo n.

Sei daher n gegeben, und wir suchen eine Zahl x mit Ordnung $n-1$ modulo n. Hierbei ist zu beachten, daß x die Ordnung $n-1$ modulo n hat genau dann, wenn

1. $x^{n-1} \equiv 1 \bmod n$, und
2. $x^{(n-1)/p} \not\equiv 1 \bmod n$, für alle Primzahlen p, die $n-1$ teilen.

Denn falls $x^{n-1} \equiv 1 \bmod n$, jedoch die Ordnung von x kleiner als $n-1$ ist, dann ist diese Ordnung auf jeden Fall ein Teiler von $n-1$.

Die Methode

Sei n eine etwa 100 stellige Zahl.

1. Falls n gerade ist, dann ist n nicht prim.
2. Versuche $n-1$ zu faktorisieren. Es ist nicht unwahrscheinlich, daß viele kleine, order zumindest mittelgroße Primfaktoren für $n-1$ erscheinen.
3. Mit Glück haben wir nun eine Primzahlfaktorisierung: $n-1 = p_1 p_2 \cdots p_k$.
4. Wir probieren, ob unsere Bedingungen ($x^{n-1} \equiv 1 \bmod n$ und $x^{(n-1)/p_i} \not\equiv 1 \bmod n$, für alle p_i, $i = 1, \ldots, k$) gelten für $x = 2$, $x = 3$, u.s.w. Falls — nach einer angemessener Zeit — eine Lösung x erscheint, dann ist n prim. Falls nicht, dann versuchen wir es doch lieber mit irgendein anderer Zahl.[14]

Auf jeden Fall ist klar, daß ein guter Faktorisierungsalgorithmus wichtig ist, wenn es darum geht, zu testen ob eine Zahl prim ist.

12 Die Faktorisierung von (ziemlich) großen Zahlen

Gegeben eine 'große' Integerzahl n, wie können wir in der Praxis die Primfaktoren von n bestimmen? Nun, es ist sicherlich so, daß Zahlen in der Großenordnung von 200 Stellen normalerweise einfach zu groß sind. Als Beispiel einer interessanten (aber ziemlich historischen) Faktorisierung: (IBM - 1975)

$$2^{2^7} + 1 = 2^{128} + 1 = 59649589127497217 \times 5704689200685129054721$$

Natürlich sind die Mikrocomputer von heute viel schneller als die monströse 'Mainframes' aus der Vergangenheit. Ich habe gerade diese Zahl in mein Laptop Rechner eingegeben und den "factor" Funktion in dem Program MuPAD aufgerufen. Die (richtige) Antwort ist nach etwa 8 Minuten und 50 Sekunden erschienen.

[14] Das Buch *Seminumerical Algorithms* von D. Knuth beschreibt auch weitere Ideen zu diesem Thema.

Ein Faktorisierungsalgorithmus

Gegeben: eine positive Integerzahl n, die ziemlich groß aussieht, wo man weiß (etwa mit Hilfe des kleinen Satzes von Fermat), daß diese Zahl nicht Prim sein kann.

Finde: eine Zahl $1 < a < n$ mit $a|n$.

Verfahren: probiere zunächst die 'kleinen' Primzahlen. (Der Computer könnte zunächst einige tausend probieren. Falls nichts gefunden wird, dann: Versuche Zahlen $0 < x, y < n$ zu finden, mit

$$x \neq y, \quad x + y \neq n \quad \text{jedoch} \quad x^2 \equiv y^2 \bmod n.$$

Dann gilt

$$x^2 - y^2 = (x + y)(x - y) \equiv 0 \bmod n,$$

(d.h. $(x + y)(x - y) = kn$ etwa, für ein $k \neq 0$.) Aber $n \not| x + y$ und $n \not| x - y$. Folglich muß entweder $\text{ggt}(n, x + y) > 1$ oder $\text{ggt}(n, x - y) > 1$. Auf jeden Fall ist der Euklidische Algorithmus in der Lage, einen großten gemeinsamen Teiler zu finden, und dies ist ein Teiler von n.

Wie findet man solche Zahlen x und y?

- (Fermat's Methode): Gegeben n, betrachte die Zahl $x^2 - n$, für verschiedene x. Es ist zu hoffen, daß $x^2 - n = y^2$, eine Quadratzahl. Hierfür ist es sehr hilfreich, zu beobachten, daß eine mehrstellige Quadratzahl nur eine begrenzte Anzahl von letzten zwei Ziffern haben kann. Und zwar sind die Möglichkeiten $\{00, g1, g4, 25, u6, g9\}$, wobei 'g' eine gerade und 'u' eine ungerade Ziffer bedeutet.
- (Computer Methode): Versuche ein x zu finden mit $x^2 \equiv a \bmod n$, wobei a 'klein' ist. Was heißt 'klein'? Sei $p_1, \ldots, p_m$ eine kleine Liste von kleinen Primzahlen z.B. 2, 3, 5, 7, 11, u.s.w. 'Klein' heißt dann, daß

$$a = p_1^{e_1} \cdots p_m^{e_m}.$$

Angenommen, der Computer findet mehrere Lösungen

$$x_i^2 \equiv a_i \bmod n,$$

$i = 1, \ldots, t$, mit jeweils

$$a_i = p_1^{e_{i1}} \cdots p_m^{e_{im}}.$$

Die Zahl a_i entspricht also einer Art 'Vektor' $(e_{11}, \ldots, e_{im})$, wobei die Komponenten e_{ij} niemals negativ sind. Um trotzdem Ideen aus der linearen Algebra verwenden zu können, betrachten wir diese Zahlen in dem einfachen Körper Z_2.

Falls t Lösungen gefunden werden mit $t \geq m + 1$, dann gibt es in $\mathbb{Z}_2$ irgendeine nicht-triviale lineare Kombination

$$\sum_{\nu=1}^{t} k_\nu (e_{\nu 1}, \ldots, e_{\nu m}) \equiv (0, \ldots, 0) \bmod 2,$$

wobei $k_\nu = 0$ oder $k_\nu = 1$ für alle ν und nicht alle k_ν sind 0. Das heißt

$$\sum_{\nu=1}^{t} k_\nu (e_{\nu 1}, \ldots, e_{\nu m}) = (2e'_1, \ldots, 2e'_m)$$

mit $e'_i \geq 0$ für alle i, wobei nicht alle e'_i gleich 0 sind. Sei nun

$$y = p_1^{e'_1} \cdots p_m^{e'_m}.$$

Dann ist

$$\begin{aligned} y^2 &= p_1^{2e'_1} \cdots p_m^{2e'_m} \\ &= \left(x_1^2\right)^{k_1} \cdots \left(x_t^2\right)^{k_t} \\ &= \left(x_1^{k_1}\right)^2 \cdots \left(x_t^{k_t}\right)^2 \\ &= \left(x_1^{k_1} \cdots x_t^{k_t}\right)^2 \\ &\equiv x^2 \bmod n, \end{aligned}$$

wobei $x = x_1^{k_1} \cdots x_t^{k_t}$.

Die Frage ist dann, wie findet man geeignete Lösungen x, wobei $x^2 \bmod n$ 'klein' sind? Nun, $x^2 \equiv a \bmod n$ heißt

$$x^2 - a = (kd^2)n$$

etwa, mit $k \in \mathbb{Z}$ quadratfrei und $d \in \mathbb{N}$. Wir suchen dann eine kleine Zahl

$$a = x^2 - d^2(kn).$$

oder anders gesagt,

$$\frac{x}{d} \sim \sqrt{kn}.$$

Jetzt sehen wir, daß wir zur Frage der Approximation von irrationalen Zahlen durch rationalen Zahlen zurückgekehrt sind. Setze irgendein 'geeignetes' k in diesen Ausdruck für $\sqrt{kn}$ ein (wiederum enthält das Buch von Donald Knuth mehr Details), und mit Hilfe des Kettenbruchverfahrens wird eine best-mögliche Approximation $\frac{x}{d}$ gefunden.

13 Etwas über die algebraische Zahlen

13.1 Die Zahlen i und ρ

Die Suche nach einem Beweis des großen Fermat'schen Satzes (d.h. zu zeigen, daß $a^n + b^n = c^n$ für a, b, c und $n \in \mathbb{N}$ nur möglich ist, wenn $n \leq 2$) hat Jahrhunderte gedauert. Viele Ideen sind dabei entstanden, und manche von diesen Ideen konnten später auch für andere Zwecke verwendet werden. Wir wollen jetzt einiges über die algebraischen Zahlen kennenlernen.

Eine sehr spezielle Klasse von algebraischen Zahlen ist die Klasse der 'zyklotomischen' Zahlen. Dies sind (komplexwertige) Lösungen der Gleichung $x^n = 1$. Es gibt immer n verschiedene Lösungen, und zwar alle komplexen Zahlen der Art

$$e^{\frac{2\pi k i}{n}}$$

für $k = 0, 1, \ldots, n-1$. Die Zahl 1 ist immer dabei (nämlich wenn $k = 0$). Falls n gerade, dann ist -1 eine Lösung ($k = n/2$). Im übrigen sind die Lösungen als Punkte, die gleich verteilt sind um den Einheitskreis in der komplexen Zahlenebene, vorzustellen. Sei $\gamma_n = e^{\frac{2\pi i}{n}}$. Dann sind diese Zahlen

$$\{\gamma_n, \gamma_n^2, \gamma_n^3, \ldots, \gamma_n^n = 1\}.$$

Die Zahl γ_n ist jeweils eine algebraische Integerzahl.[15]

Insbesondere werden wir die zwei einfachen Fälle $\rho := \gamma_3$ und $i =: \gamma_4$ betrachten, da die Multiplikation von Integerzahlen dann besonders einfach zu beschreiben ist. Bekanntlich ist $i^2 = -1$; daher gilt für beliebige Integerzahlen

$$(a + bi)(c + di) = (ac - bd) + (ad + bc)i.$$

Weiter gilt $\rho^2 + \rho + 1 = 0$, daher $\rho^2 = -1 - \rho$. Auch $\rho^2 = \overline{\rho}$, (hier ist $\overline{\rho}$ die zu ρ konjugierte komplexe Zahl), und

$$(a + b\rho)(c + d\rho) = ac + bd\rho^2 + (ad + bc)\rho = (ac - bd) + (ad + bc - bd)\rho.$$

13.2 Die Gauss'schen Integerzahlen, $\mathbb{Z}[i]$

Wir betrachten zunächst die Arithmetik in $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$. Sei $\alpha = a + bi$. Die 'Norm' $N(\alpha)$ wird als $N(\alpha) = a^2 + b^2$ definiert. Mit anderen Wörten, sei $\overline{\alpha} = a - bi$ die zu α komplexe konjugierte

[15] Eine algebraische Integerzahl ist eine Lösung der Gleichung

$$x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0,$$

wobei $a_k \in \mathbb{Z}$ für alle $k = 0, \ldots, n-1$. In unserem Fall ist γ_n eine Lösung der Gleichung $x^n - 1 = 0$.

Zahl. Dann ist $N(\alpha) = \alpha\overline{\alpha} = |\alpha|^2$, wobei $|\alpha|$ die übliche 'absolut Betrag' Funktion ist. Offensichtlich ist $N(\alpha) \in \mathbb{N}_0$ für alle $\alpha \in \mathbb{Z}[i]$. Sei nun $\beta = c + di$. Es gilt

$$\begin{aligned} N(\alpha)N(\beta) &= (a^2 + b^2)(c^2 + d^2) \\ &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\ &= (ac - bd)^2 + (ad + bc)^2 = N(\alpha\beta). \end{aligned}$$

Wir werden sagen, daß α die Zahl β teilt, geschrieben $\alpha|\beta$, falls ein $\gamma = e + fi$ existiert, mit

$$\alpha\gamma = (a + bi)(e + fi) = (ae - bf) + (af + be)i = c + di = \beta.$$

Offensichtlich gilt $\epsilon|\alpha$, falls $\epsilon = \pm 1, \pm i$, für jedes $\alpha \in \mathbb{Z}[i]$. Solche Zahlen wie ϵ heißen 'Einheiten' in $\mathbb{Z}[i]$. Es ist klar, daß $N(\epsilon) = 1$ für die Einheiten, aber $N(\alpha) > 1$ für alle nicht-Einheiten in $\mathbb{Z}[i]$ (abgesehen von $\alpha = 0$). Die nicht-Einheit $\rho \in \mathbb{Z}[i]$ heißt 'prim', falls $\rho|\alpha\beta \implies \rho|\alpha$ oder $\rho|\beta$, für alle relevante α, $\beta \in \mathbb{Z}[i]$.

Satz 71. *Gegeben $\alpha, \beta \in \mathbb{Z}[i]$ mit $\beta \neq 0$, dann existieren γ, $\kappa \in \mathbb{Z}[i]$ mit $\alpha = \kappa\beta + \gamma$, wobei $N(\gamma) < N(\beta)$.*

Beweis. In $\mathbb{C}$ (der Körper der komplexen Zahlen) sei

$$\frac{\alpha}{\beta} = R + Si,$$

mit $R, S \in \mathbb{R}$. Seien $x, y \in \mathbb{Z}$ mit

$$|R - x| \leq \frac{1}{2}, \quad |S - y| \leq \frac{1}{2}$$

und $\kappa = x + yi$; dann sei $\gamma = \alpha - \kappa\beta$. Aber

$$\begin{aligned} N(\gamma) &= N(\alpha - \kappa\beta) \\ &= N(\beta)N(\alpha/\beta - \kappa) \\ &= N(\beta)N((R - x) + (S - y)i) \\ &= N(\beta)\{(R - x)^2 + (S - y)^2\} \leq \frac{N(\beta)}{2}. \end{aligned}$$

□

Definition 13.1. Seien $\alpha, \beta \in \mathbb{Z}[i]$ nicht null. Die Zahl γ ist ein 'größter gemeinsamer Teiler', falls $\gamma|\alpha$ und $\gamma|\beta$, und falls für alle anderen gemeinsamen Teiler κ mit $\kappa|\alpha$ und $\kappa|\beta$ gilt $\kappa|\gamma$.

Satz 72. *Seien $\alpha, \beta \in \mathbb{Z}[i]$ nicht null. Dann existieren größte gemeinsame Teiler, und sie sind eindeutig, bis auf Produkte mit Einheiten.*

Beweis. Sei etwa $N(\beta) \leq N(\alpha)$. Sei $\alpha = \kappa\beta + \gamma$ mit $N(\gamma) < N(\beta)$. Falls $\gamma \neq 0$, dann ist jeder Teiler von α und β auch ein Teiler von γ. Falls $\gamma = 0$, dann ist β ein größter gemeinsamer Teiler von α und β, und β ist dabei eindeutig bestimmt, bis auf Produkte mit Einheiten. □

Genau wie bei 'normalen' Zahlen (wir werden hier die Primzahlen $\mathcal{P} \subset \mathbb{N}$ als 'rationale Primzahlen' bezeichnen) gilt dann...

Satz 73. *Falls 1 ein größter gemeinsamer Teiler von α und $\beta \in \mathbb{Z}[i]$ ist, dann existieren γ, $\delta \in \mathbb{Z}[i]$ mit $\gamma\alpha + \delta\beta = 1$.*

Satz 74. *Falls 1 ein größter gemeinsamer Teiler von α und $\beta \in \mathbb{Z}[i]$ ist, und $\beta|\alpha\eta$, dann gilt $\beta|\eta$.*

Beweis. Sei $\gamma\alpha + \delta\beta = 1$ mit γ, $\delta \in \mathbb{Z}[i]$. Dann ist $\gamma\alpha\eta + \delta\beta\eta = \eta$. Da $\beta|\alpha\eta$ folgt $\beta|\eta$. □

Satz 75. *Falls $\alpha \in \mathbb{Z}[i]$ nicht prim, dann gibt es eine prim $\rho \in \mathbb{Z}[i]$ mit $\rho|\alpha$.*

Beweis. Angenommen, α ist ein kleinstes Gegenbeispiel (d.h. $N(\alpha)$ ist am kleinsten). Sei $\alpha|\beta\gamma$, wobei $\alpha \not| \beta$ und $\alpha \not| \gamma$. Dann ist der größter gemeinsamer Teiler von α und β etwa ξ, wobei $1 < N(\xi) < N(\alpha)$. Falls ξ eine Primzahl ist, dann sind wir fertig. Anderenfalls gibt es ein Primfaktor für ξ. (Es gibt nur endlich viele Elemente von $\mathbb{Z}[i]$ mit Norm kleiner als $N(\alpha)$, und $N(\alpha)$ war doch ein kleinstes Gegenbeispiel.) □

Satz 76. *Falls* $N(\rho) \in \mathcal{P}$ *eine Primzahl in* $\mathbb{Z}$ *ist, dann ist* ρ *prim in* $\mathbb{Z}[i]$.

Beweis. Sonst (nach Satz 75) gibt es eine Primzahl $\gamma \in \mathbb{Z}[i]$ mit $\rho = \epsilon \cdot \gamma$. Daher $N(\rho) = N(\epsilon)N(\gamma)$. Da $N(\rho)$ prim ist in $\mathbb{Z}$ und $N(\gamma) > 1$ folgt, daß $N(\epsilon) = 1$. D.h. ϵ ist nur eine Einheit und ρ ist prim in $\mathbb{Z}[i]$. □

Dann folgt..

Satz 77. *Die Darstellung* $\alpha = \rho_1\rho_2\cdots\rho_r$ *als Produkt von Primzahlen in* $\mathbb{Z}[i]$ *ist (bis auf Einheiten und Reihenfolge) eineindeutig.*

Welche Zahlen sind eigentlich prim in $\mathbb{Z}[i]$?

Satz 78. *Sei* $\rho \in \mathbb{Z}[i]$ *prim. Dann gibt es eine einzige rationale Primzahl* $p_\rho \in \mathcal{P} \subset \mathbb{N}$ *mit* $\rho | p_\rho$.

Beweis. Es gilt $\rho\overline{\rho} \in \mathbb{N}$. D.h. $\rho | N(\rho) \in \mathbb{N}$. Sei $p \in \mathbb{N}$ die kleinste Zahl mit $\rho | p$. Kann es sein, daß p nicht prim (in $\mathbb{N}$) ist, etwa $p = n_1n_2$ mit n_1, $n_2 \in \mathbb{N}$? Aber dann gilt $\rho | n_1$ oder $\rho | n_2$, und zumindest eine von diesen Zahlen muß eine Einheit sein. (D.h. die Zahl 1 in $\mathbb{N}$.) Daher ist p eine rationale Primzahl. Kann es sein, daß $\rho | p'$ für eine andere rationale Primzahl $p' \neq p$? Aber dann gibt es x, $y \in \mathbb{Z}$ mit $xp + yp' = 1$ und $\rho | 1$. Dies ist unmöglich, da ρ keine Einheit in $\mathbb{Z}[i]$ ist. □

Sei $\rho = a + bi \in \mathbb{Z}[i]$ prim (wobei $\rho \notin \mathbb{Z}$). Welche Primzahl $p \in \mathcal{P} \subset \mathbb{N}$ wird von ρ geteilt? Zunächst ist zu beachten, daß $p \equiv 3 \bmod 4$ nicht möglich ist[16].

- Falls $\rho | 2$, dann ist $a^2 + b^2 = 2$. D.h. $\rho = \pm 1 \pm i$.
- Falls $p \equiv 1 \bmod 4$, dann existieren (nach Satz 59) zwei Zahlen a, $b \in \mathbb{N}$ mit $p = a^2 + b^2$. Dann ist $p = (a + bi)(a - bi)$, und folglich ist p nicht prim in $\mathbb{Z}[i]$. Andererseits ist nach Satz 76 $a \pm bi$ prim. Da die Faktorisierung in Primzahlen eindeutig in $\mathbb{Z}[i]$ ist, gilt auch:

Satz 79. *Falls* $p \in \mathcal{P}$ *und* $p = a^2 + b^2$*, dann ist diese Darstellung eineindeutig. (D.h. falls* $p = a^2 + b^2 = c^2 + d^2$ *dann ist* $a = c$ *oder* d *und* $b = d$ *oder* c*.)*

Insgesamt haben wir dann:

Satz 80. *Die Primzahlen in* $\mathbb{Z}[i]$ *sind (bis auf Produkte mit Einheiten):*

- *Die Zahlen* $\pm 1 \pm i$.
- *Die rationalen Primzahlen* $p \in \mathcal{P}$*, wobei* $p \equiv 3 \bmod 4$.
- *Die Zahlen* $a + bi$ *mit* $a^2 + b^2 = p$*, für* $p \in \mathcal{P}$ *und* $p \equiv 1 \bmod 4$.

13.3 Das Zahlensystem $\mathbb{Z}[\rho]$

Nun, es gilt sowohl $\rho^3 = 1$ als auch $\rho^2 + \rho + 1 = 0$ oder $\rho^2 = -1 - \rho$. Daher gilt: sei $\alpha = a + b\rho$ und $\beta = c + d\rho$. Dann ist

$$\alpha\beta = (a + b\rho)(c + d\rho) = (ac - bd) + (ad + bc - bd)\rho.$$

Die Norm wird hier durch $N(\alpha) = N(a + b\rho) = a^2 - ab + b^2$ definiert. Da

$$\rho = \frac{-1 + \sqrt{3}i}{2}$$

folgt

$$\alpha = \left(a - \frac{b}{2}\right) + \frac{\sqrt{3}bi}{2}.$$

D.h.

$$N(\alpha) = \left(a - \frac{b}{2}\right)^2 + \left(\frac{\sqrt{3}b}{2}\right)^2 = |\alpha|^2.$$

[16] Falls $u \in \mathbb{Z}$ eine gerade Zahl ist: $u = 2v$, dann ist $u^2 \equiv 4v^2 \equiv 0 \bmod 4$. Falls $u = 2v + 1$ ungerade, dann ist $u^2 \equiv 1 \bmod 4$. Daher ist $a^2 + b^2$ entweder 0, 1 oder 2 mod4.

Eine einfache Rechnung mit komplexen Zahlen gibt dann $N(\alpha\beta) = N(\alpha)N(\beta)$ für alle α, $\beta \in \mathbb{Z}[\rho]$.

Die Einheiten in $\mathbb{Z}[\rho]$ sind wieder die Zahlen $\epsilon = a + b\rho$ mit $N(\epsilon) = 1$. D.h.

$$a^2 - ab + b^2 = 1$$

oder

$$(2a - b)^2 + 3b^2 = 4.$$

Die Möglichkeiten sind

$$\epsilon = \pm 1, \pm\rho, \pm\rho^2 = \mp(1 + \rho).$$

Die Definition von Primzahlen in $\mathbb{Z}[\rho]$ ist ähnlich wie vorher. Auch der Euklidische Algorithmus ist ähnlich:

Satz 81. *Gegeben $\alpha, \beta \in \mathbb{Z}[\rho]$ mit $\beta \neq 0$, dann existieren γ, $\kappa \in \mathbb{Z}[\rho]$ mit $\alpha = \kappa\beta + \gamma$ wobei $N(\gamma) < N(\beta)$.*

Beweis. Sei wie vorher $\alpha/\beta = R + S\rho$ und x, $y \in \mathbb{Z}$ mit

$$|R - x| \leq \frac{1}{2}, \quad |S - y| \leq \frac{1}{2}.$$

Dieses mal ist

$$N(\alpha/\beta - (x + y\rho)) = (R - x)^2 - (R - x)(S - y) + (S - y)^2 \leq \frac{3}{4}.$$

Der Beweis ist sonst ähnlich wie vorher. □

Daher gilt wieder...

Satz 82. *Der Satz über die eindeutige Primfaktorzerlegung von Integerzahlen gilt auch in $\mathbb{Z}[\rho]$.*

Die Frage ist nun, was sind denn die Primzahlen in $\mathbb{Z}[\rho]$? Sei $\tau \in \mathbb{Z}[\rho]$ prim. (Insbesondere ist τ keine Einheit.) Genau wie bei $\mathbb{Z}[i]$ gibt es eine eindeutige rationale Primzahl p mit $\tau|p$. Was ist p?

- Falls $p = 3$, dann ist

$$\begin{aligned} 3 = 2 + 1 &= 2 - \rho - \rho^2 \\ &= (1 - \rho)(2 + \rho) \\ &= (1 - \rho)(1 - \rho^2) \\ &= (1 + \rho)(1 - \rho)^2 \\ &= -\rho^2(1 - \rho)^2. \end{aligned}$$

  Aber ρ selbst ist eine Einheit ($N(\rho) = 1$). Wir setzen dann $\lambda = 1 - \rho$ und sehen, daß λ der einzige Primfaktor ist (bis auf Einheiten).

- Sei $p \equiv 2 \bmod 3$ und sei $\alpha = a + b\rho \in \mathbb{Z}[\rho]$ mit $b \neq 0$. (Bemerken Sie, daß $4p \equiv 4 \cdot 2 = 8 \equiv 2 \bmod 3$.) Unter der Annahme, daß $p = N(\alpha)$ haben wir dann

$$4p = 4N(\alpha) \equiv (2a - b)^2 + 3b^2 \equiv (2a - b)^2 \bmod 3.$$

  Da $\left(\frac{2}{3}\right) = -1$, ist $4N(\alpha) \equiv 2 \bmod 3$ unmöglich. Folglich ist p auch eine Primzahl in $\mathbb{Z}(\rho)$.

- Sei $p \equiv 1 \bmod 3$. Dann folgt $\left(\frac{-3}{p}\right) = 1$. (Übung!) Nach Satz 60 gibt es dann x, y (nicht beide null) und $k \in \mathbb{Z}$ mit $|k| \leq 3$ und

$$x^2 + 3y^2 = kp.$$

  Sei nun $a = x + y$ und $b = 2y$ und sei $\alpha = a + b\rho \in \mathbb{Z}[\rho]$. Es gilt

$$\begin{aligned} \alpha|\alpha\overline{\alpha} &= N(\alpha) = a^2 - ab + b^2 \\ &= (x + y)^2 - 2(x + y)y + 4y^2 \\ &= x^2 + 3y^2 = kp \end{aligned}$$

  Nun, falls $k = 1$ dann ist einfach $\alpha|p$. Falls $k = 2$, dann ist k eine Primzahl in $\mathbb{Z}[\rho]$ und $\alpha \not| 2$. Folglich gilt $\alpha|p$ auch hier. Schliesslich, falls $k = 3 = \epsilon(1 - \rho)^2$, wobei ϵ eine Einheit ist, dann ist entweder

$1-\rho \not| \alpha$; d.h. $\alpha | p$, oder

$\frac{\alpha}{1-\rho} = \beta$ etwa, wobei $\beta \in \mathbb{Z}[\rho]$ und $\beta | p$. D.h. $\alpha | p$.

Satz 83. *Die Primzahlen in $\rho \in \mathbb{Z}[\rho]$ sind (bis auf Produkte mit Einheiten)*

- $\lambda = 1 - \rho$,
- *rationale Primzahlen der Art* $p \equiv 2 \bmod 3$,
- *die Faktoren der rationalen Primzahlen der Art* $p \equiv 1 \bmod 3$.

13.4 Quadratische Zahlkörper

In diesem Abschnitt werden wir uns mit (komplexen) Zahlen der Art $u + v\sqrt{m}$ beschäftigen, (wobei $0 \neq m \in \mathbb{Z}$ keine Quadratzahl außer 1 als Faktor enthält) und u, $v \in \mathbb{Q}$ jeweils rationale Zahlen sind. Addition und Multiplikation sind:

- $(u_1 + v_1\sqrt{m}) + (u_2 + v_2\sqrt{m}) = (u_1 + u_2) + (v_1 + v_2)\sqrt{m}$
- $(u_1 + v_1\sqrt{m})(u_2 + v_2\sqrt{m}) = (u_1u_2 + v_1v_2m) + (u_1v_2 + u_2v_1)\sqrt{m}$.

Falls $u_2 + v_2\sqrt{m} \neq 0$ dann ist

$$\begin{aligned} \frac{u_1 + v_1\sqrt{m}}{u_2 + v_2\sqrt{m}} &= \frac{(u_1 + v_1\sqrt{m})(u_2 - v_2\sqrt{m})}{(u_2 + v_2\sqrt{m})(u_2 - v_2\sqrt{m})} \\ &= \frac{(u_1u_2 - v_1v_2m) + (u_2v_2 - u_1v_2)\sqrt{m}}{u_2^2 - v_2^2m} \end{aligned}$$

und $u_2^2 - v_2^2m \neq 0$, da m keine Quadratzahl ist. Wir werden die Gesamtheit aller solcher Zahlen mit $\mathbb{Q}(\sqrt{m})$ vezeichnen. Dann ist $\mathbb{Q}(\sqrt{m}) \subset C$ ein Teilkörper der komplexen Zahlen. Dies ist ein quadratischer 'Erweiterungskörper'. $\mathbb{Q}$ wird nämlich um die Zahl $\sqrt{m}$ erweitert, und dies ist die minimale solche Erweiterung. $\mathbb{Q}(\sqrt{m})$ kann als Vektorraum über $\mathbb{Q}$ betrachtet werden. Eine Basis ist $\{1, \sqrt{m}\}$. Man könnte auch sagen, daß $\mathbb{Q}(\sqrt{m})$ die Menge aller Polynome in $\sqrt{m}$ mit Koeffizienten in $\mathbb{Q}$ ist (wobei allerdings die Beziehung $\sqrt{m}^2 = m$ berüchsichtigt wird).

Alle Zahlen in $\mathbb{Q}(\sqrt{m})$ sind algebraische Zahlen der Ordnung 2 (oder weniger).[17] Alle Zahlen der Art $a + b\sqrt{m}$ mit a, $b \in \mathbb{Z}$ sind algebraische Integerzahlen. Es gibt allerdings auch eine weitere Klasse von Integerzahlen, falls $m \equiv 1 \bmod 4$.

Nun, eine algebraische Zahl ξ der Ordnung 2 ist eine Lösung einer (normierten) Gleichung

$$x^2 + a_1x + a_0 = 0,$$

mit $a_1, a_2 \in \mathbb{Q}$. Diese Gleichung ist eindeutig, denn sonst wäre sowohl

$$\xi^2 + a_1\xi + a_0 = 0$$

als auch

$$\xi^2 + b_1\xi + b_0 = 0,$$

[17] Zur Erinnerung: eine algebraische Zahl ist eine Lösung (Nullstelle) einer Polynomgleichung der Art

$$a_0 + a_1x + \cdots + a_nx^n = 0,$$

wobei $n > 0$, $a_j \in \mathbb{Z}$ für alle j, und $a_n \neq 0$. Falls $a_n = 1$, dann sind die entsprechenden Nullstellen algebraische *Integer*zahlen.
Falls $\alpha = a + b\sqrt{m}$ dann ist

$$\begin{aligned} \alpha^2 &= a^2 + 2ab\sqrt{m} + b^2 \\ &= 2a^2 + 2ab\sqrt{m} + b^2m - a^2 \\ &= 2a(a + b\sqrt{m}) + b^2 - a^2 \\ &= 2a\alpha + (b^2m - a^2). \end{aligned}$$

Daher ist α eine algebraische Zahl von der Ordnung höchstens 2.

wobei $a_0 \neq b_0$ und/oder $a_1 \neq b_1$. Dann würde gelten

$$(a_1 - b_1)\xi + (a_0 - b_0) = 0.$$

Ein Widerspruch. (Sonst wäre die Ordnung von ξ weniger als 2.)

Jede Zahl in $\mathbb{Q}(\sqrt{m})$ kann auch als

$$\xi = \frac{a + b\sqrt{m}}{c}$$

geschrieben werden, wobei $a, b \in \mathbb{Z}$ und $c \in \mathbb{N}$, und c so klein wie möglich ist. D.h.

$$(c\xi - a)^2 = mb^2,$$

oder

$$\xi^2 - \frac{2a}{c}\,\xi + \frac{a^2 - mb^2}{c^2} = 0.$$

Angenommen nun ξ ist eine algebraische Integerzahl. Dann sind die Zahlen

$$\frac{2a}{c} \quad \text{und} \quad \frac{a^2 - mb^2}{c^2}$$

Integerzahlen. D.h. $c|2a$ und $c^2|(a^2 - mb^2)$. Falls $d = ggt(c, a)$, dann folgt auch $d|b$, denn m enthält doch keine quadratischen Faktoren. D.h. $d = 1$ (a, b und c haben keine nicht-triviale gemeinsame Teiler) und daher $c|2$. Folglich ist $c = 1$ oder 2. Falls $c = 1$, dann haben wir unsere Integerzahlen $a + b\sqrt{m}$

Der Fall $c = 2$ ist etwas komplizierter. Falls a gerade, dann ist auch b gerade, (denn $4|(a^2 - mb^2)$). Dies widerspricht der Annahme, daß c so klein wie möglich ist. Daher ist a ungerade; folglich ist auch b ungerade, daher $a^2 \equiv b^2 \equiv 1 \bmod 4$ und folglich auch $m \equiv 1 \bmod 4$.

Eine Möglichkeit ist die Zahl τ, wobei

$$\tau = \frac{-1 + \sqrt{m}}{2}.$$

Denn sei etwa $m = 4u + 1$, mit $u \in \mathbb{Z}$. Dann ist

$$\begin{aligned} \tau^2 &= \frac{1 - 2\sqrt{m} + 4u + 1}{4} \\ &= \frac{2 + 4u}{4} - \frac{2\sqrt{m}}{4} \\ &= \frac{1 + 2u}{2} - \frac{\sqrt{m}}{2} \\ &= u - \tau \end{aligned}$$

und $u \in \mathbb{Z}$. Für dieses τ gilt $\sqrt{m} = 1 + 2\tau$.

Sei nun ξ eine beliebige Zahl von der Gestalt

$$\xi = \frac{c + d\sqrt{m}}{2},$$

wobei c und $d \in \mathbb{Z}$ ungerade sind. Wir schreiben $c = 2s - 1$, $d = 2t + 1$. D.h.

$$\begin{aligned} \xi &= \frac{(2s - 1) + (2t + 1)\sqrt{m}}{2} \\ &= s + t\sqrt{m} + \tau \\ &= s + t(1 + 2\tau) + \tau \\ &= (s + t) + (1 + 2t)\tau \end{aligned}$$

Mit anderen Wörten: Alle algebraische Integerzahlen in $\mathbb{Q}(\sqrt{m})$ sind Zahlen der Art $a + b\tau$, für gewisse a, $b \in \mathbb{Z}$. Umgekehrt gilt:

Proposition. *Seien* $a, b \in \mathbb{Z}$ *beliebig,* $m \equiv 1 \bmod 4$*. Dann ist* $\xi = a + b\tau$ *eine Integerzahl in* $\mathbb{Q}(\sqrt{m})$*.*

Beweis. ξ ist eine Integerzahl, da ξ die folgende normierte quadratische Polynomgleichung mit Integerkoeffizienten genügt.

$$\begin{aligned}
\xi^2 &= a^2 + 2ab\tau + b^2\tau^2 \\
&= a^2 + 2ab\tau + b^2(u - \tau) \\
&= (a^2 + b^2u) + (2ab - b^2)\tau \\
&= (a^2 + b^2u) - (2a^2 - ab) + (2a^2 - ab) + (2ab - b^2)\tau \\
&= (b^2u - a^2 + ab) + (2a - b)\xi
\end{aligned}$$

□

Insgesamt gilt dann:

Satz 84. *Die Integerzahlen von* $\mathbb{Q}(\sqrt{m})$ *sind*

- *die Zahlen* $a + b\sqrt{m}$*, falls* $m \equiv 2, 3 \bmod 4$
- *die Zahlen* $a + b\tau = a + \frac{b}{2}(\sqrt{m} - 1)$*, falls* $m \equiv 1 \bmod 4$*,*

und $a, b \in \mathbb{Z}$ *beliebig.*

Bemerkung. *Die Zahlen* $\mathbb{Z}[i]$ *und* $\mathbb{Z}[\rho]$ *sind die Integerzahlen in* $\mathbb{Q}[\sqrt{-1}]$ *bzw.* $\mathbb{Q}[\sqrt{-3}]$*.*

Definition 13.2. Für beliebige $\xi = x + y\sqrt{m} \in \mathbb{Q}(\sqrt{m})$ wird die Norm $N(\xi)$ durch $N(\xi) = x^2 - my^2$ definiert.

Für $m < 0$ ist dies die übliche Absolutbetrag-Funktion in C: $N(\xi) = \xi\overline{\xi} = |\xi|^2$. Für $m > 0$ kann $N(\xi)$ negativ sein. Es existieren sogar unendlich viele integerwertige Einheiten.

Es gilt $N(\xi)N(\zeta) = N(\xi\zeta)$ für beliebige $\xi, \zeta \in \mathbb{Q}(\sqrt{m})$. Falls ξ eine algebraische Integerzahl ist mit $N(\xi)$ prim (als rationale Zahl), dann ist, wie vorher, ξ auch prim als Integer in $\mathbb{Q}(\sqrt{m})$. (Falls $m > 0$, dann nehme $|N(\xi)|$ und beachte, daß die Integerzahl $|N(\xi)|$ nur dann 0 ist, wenn $\xi = 0$, und $|N(\xi)| = 1$ nur dann, wenn ξ eine Einheit ist.) Jede Integerzahl kann wieder als Produkt von Primzahlen dargestellt werden. Leider ist aber diese Darstellung <u>nicht</u> notwendigerweise eineindeutig, für manche m.

14 Die Gleichung $x^3 + y^3 = z^3$.

Die Diophantinische Gleichung $x^3 + y^3 = z^3$ hat <u>keine</u> nicht-triviale Lösungen[18]. Um dies zu beweisen, brauchen wir wieder die Theorie der algebraischen Zahlen $\mathbb{Z}[\rho]$ mit $\rho = \frac{-1+\sqrt{3}i}{2}$, denn...

$$x^3 + y^3 = (x + y)(x + \rho y)(x + \rho^2 y).$$

(Dies folgt, da $1 + \rho + \rho^2 = 0$.) Wir werden tatsächlich ein stärkeres Ergebnis beweisen:

Satz 85. *Es gibt keine Integerzahlen* $\alpha, \beta, \gamma \in \mathbb{Z}[\rho]$ *mit*

$$\alpha^3 + \beta^3 + \epsilon\gamma^3 = 0,$$

wobei ϵ *eine Einheit (z.B.* $\epsilon = -1$*) ist und* $\alpha\beta\gamma \neq 0$*.*

Zunächst erinnern wir uns daran, daß die Zahl $\lambda = 1 - \rho$ eine Primzahl in $\mathbb{Z}[\rho]$ ist mit $N(\lambda) = 3$. Wir können auch Kongruenzen in $\mathbb{Z}[\rho]$ betrachten.

Satz 86. *Sei* $\delta \in \mathbb{Z}[\rho]$ *beliebig. Dann ist* $\delta \equiv 0, \pm 1 \bmod \lambda$*.*

[18] Ganz allgemein sei bemerkt, daß die Gleichung $x^n + y^n = z^n$ immer triviale Lösungen besitzt: nämlich wenn $x = 0$ oder $y = 0$. Falls $n = kl$, für $k, l \in \mathbb{N}$, dann ist $(x^k)^l + (y^k)^l = (z^k)^l$. Auch wenn $\mathrm{ggt}(x, y) = d > 1$, dann ist $(x/d)^n + (y/d)^n = (z/d)^n$ eine kleinere Lösung. Um Fermat's großen Satz zu beweisen, brauchen wir deshalb nur die Fälle $\mathrm{ggt}(x, y) = 1$ und $n \in \mathcal{P}$ zu behandeln.

Beweis. Es ist nur nötig, zu zeigen, daß $\lambda|\delta$ oder $\lambda|\delta \pm 1$. Sei $\delta = a + b\rho$. Dann ist

$$\delta = a + b\rho = a + b - b(1-\rho) = (a+b) - b\lambda \equiv a + b \bmod \lambda.$$

Aber $\lambda|N(\lambda) = 3$ und falls $3 \not| (a+b)$, dann gilt immerhin $3|(a+b) \pm 1$. □

Wir werden nun unseren Satz 85 in dem einfachen Fall beweisen, daß $\lambda \not| \alpha\beta\gamma$.

Satz 87. *Es gibt keine Integerzahlen α, β, $\gamma \in \mathbb{Z}[\rho]$ mit $\alpha^3 + \beta^3 + \epsilon\gamma^3 = 0$, wobei ϵ eine Einheit ist und $\lambda \not| \alpha\beta\gamma \neq 0$.*

Beweis. Nach dem Satz über die eineindeutige Primfaktorzerlegung in $\mathbb{Z}[\rho]$ folgt, daß $\lambda \not| \alpha$, $\lambda \not| \beta$ und $\lambda \not| \gamma$. Sei nun $x \in \mathbb{Z}[\rho]$ mit $x \equiv 1 \bmod \lambda$. D.h. $x = 1 + t\lambda$, für ein $t \in \mathbb{Z}[\rho]$. Dann gilt

$$\begin{aligned}
x^3 - 1 &= \underbrace{(x-1)}_{t\lambda}(x-\rho)(x-\rho^2) \\
&= t\lambda((1+t\lambda)-\rho)((1+t\lambda)-\rho^2) \\
&= t\lambda(\underbrace{(1-\rho)}_{\lambda} + t\lambda)(\underbrace{(1-\rho^2)}_{(1+\rho)\lambda} + t\lambda) \\
&= t\lambda(\lambda + t\lambda)((1+\rho)\lambda + t\lambda) \\
&= t\lambda^3(1+t)(t-\rho^2)
\end{aligned}$$

Aber $\rho^2 \equiv 1 \bmod \lambda$ (denn $\rho^2 - 1 = (-1-\rho) - 1 = -3 + \lambda$, und $\lambda|3$, da $N(\lambda) = 3$). Nach Satz 86 ist $t \equiv 0 \bmod \lambda$, oder $t \equiv \pm 1 \bmod \lambda$. Daher ist $\lambda^4|x^3 - 1$, oder anders gesagt,

$$x^3 \equiv 1 \bmod \lambda^4.$$

(Falls $x \equiv -1 \bmod \lambda$ dann ist $-x \equiv 1 \bmod \lambda$ und $(-x)^3 \equiv 1 \bmod \lambda^4$. D.h. $x^3 \equiv -1 \bmod \lambda^4$.) Falls nun $\alpha^3 + \beta^3 + \epsilon\gamma^3 = 0$ eine nicht-triviale Lösung ist, dann gilt insbesondere $x^3 \not\equiv 0 \bmod \lambda$, für $x = \alpha, \beta$ und γ. Daher

$$\pm 1 \pm 1 \pm \epsilon \equiv 0 \bmod \lambda^4.$$

Aber $|\lambda^4| = 9$. Die Gleichung kann folglich nur aufgehen, wenn tatsächlich $\pm 1 \pm 1 \pm \epsilon = 0$. Aber keine Kombination von 'plus' und 'minus' erfüllt diese Bedingung. □

Die Situation ist etwas schwieriger, wenn $\lambda|\alpha\beta\gamma$. Da λ prim ist (und die anderen Zahlen sind zueinander relativ prim), muß λ eine einzige von diesen drei Zahlen teilen. Angenommen $\lambda|\gamma$. Dann ist $\gamma = \delta\lambda$ etwa, und unsere Annahme ist, daß $\alpha^3 + \beta^3 + \epsilon\lambda^3\delta^3 = 0$.

Satz 88. *Falls $\alpha^3 + \beta^3 + \epsilon\gamma^3 = 0$ mit $\lambda \not| \alpha\beta$, aber $\lambda|\gamma$, dann gilt auch $\lambda^2|\gamma$.*

Beweis. Da $\lambda \not| \alpha$ und $\lambda \not| \beta$, gilt

$$\pm 1 \pm 1 \equiv \epsilon\gamma^3 \bmod \lambda^4.$$

Es gibt nur zwei Möglichkeiten: $\pm 1 \pm 1 = 0$ oder $\pm 1 \pm 1 = \pm 2$. Falls $\pm 2 = \epsilon\gamma^3 \bmod \lambda^4$, dann ist

$$\pm 2 = \epsilon\gamma^3 + t\lambda^4 = \epsilon(\delta\lambda)^3 + t\lambda^4,$$

für ein $t \in \mathbb{Z}[\rho]$. D.h. $\lambda|2$, aber dies ist falsch (eine Primzahl wie λ kann nur eine einzige rationele Primzahl—nämlich 3 in diesem Fall—teilen).

Falls $\epsilon\gamma^3 \equiv 0 \bmod \lambda^4$, dann ist $\lambda^4|\gamma^3$. Die Primfaktorzerlegung von γ muß daher die Primzahl λ mehr als einmal enthalten. □

Satz 89. *Sei $\alpha^3 + \beta^3 + \epsilon\gamma^3 = 0$ mit $ggt(\alpha, \beta) = 1$, $\lambda \not| \alpha\beta$ und $\lambda^2|\gamma$. Sei $n = Ord_\lambda(\gamma)$ die größte Zahl mit $\lambda^n|\gamma$. Dann gibt es eine weitere Lösung*

$$\alpha_1^3 + \beta_1^3 + \epsilon_1\gamma_1^3 = 0$$

mit $ggt(\alpha_1, \beta_1) = 1$, $\lambda \not| \alpha_1\beta_1$ und $Ord_\lambda(\gamma_1) < Ord_\lambda(\gamma)$.

Beweis. Da

$$(\alpha+\beta)(\alpha+\beta\rho)(\alpha+\beta\rho^2)=\epsilon\gamma^3$$

und $\lambda^2|\gamma$, folgt, daß mindestens ein Faktor auch durch λ^2 teilbar ist. Aber ρ ist nur eine Einheit, daher kann gegebenenfalls β durch $\beta\rho$ oder $\beta\rho^2$ ersetzt werden, und folglich, ohne Beschränkung der Allgemeinheit, können wir annehmen, daß $\lambda^2|\alpha+\beta$. Andererseits ist dann

$$\mathrm{Ord}_\lambda(\alpha+\beta\rho)=\mathrm{Ord}_\lambda((\alpha+\beta)-(1-\rho)\beta)=\mathrm{Ord}_\lambda((\alpha+\beta)-\lambda\beta).$$

Kann es sein, daß $\lambda^2|\alpha+\beta-\lambda\beta$? Dann wäre

$$\lambda\beta=\kappa\lambda^2+\alpha+\beta,$$

für ein $\kappa\in\mathbb{Z}[\rho]$, oder

$$\beta=\kappa\lambda+\frac{\alpha+\beta}{\lambda}$$

und folglich $\lambda|\beta$, ein Widerspruch. Daher ist $\mathrm{Ord}_\lambda(\alpha+\beta\rho)=1$. Ähnlich ist

$$\begin{aligned}\mathrm{Ord}_\lambda(\alpha+\beta\rho^2) &= \mathrm{Ord}_\lambda(\alpha+(-1-\rho)\beta)\\ &= \mathrm{Ord}_\lambda((\alpha+\beta)-3\beta+(1-\rho)\beta)\\ &= \mathrm{Ord}_\lambda((\alpha+\beta)-3\beta+\lambda\beta)=1.\end{aligned}$$

(wobei $\lambda^2=(1-\rho)^2=(1-2\rho+\rho^2)=-3\rho|3$ und $\lambda^2|(\alpha+\beta)-3\beta$). Folglich ist

$$\mathrm{Ord}_\lambda(\alpha+\beta)=3\mathrm{Ord}_\lambda(\gamma)-2.$$

Sei jetzt $\pi\in\mathbb{Z}[\rho]$ prim, mit $\pi\neq\lambda$ (bis auf eine Einheit). Kann es sein, daß auch $\pi|\alpha+\beta$ und $\pi|\alpha+\beta\rho$? Dann wäre

$$\pi|(1-\rho)\beta=\lambda\beta$$

und folglich $\pi|\beta$; daher auch $\pi|(\alpha+\beta)-\beta=\alpha$. Aber dies widerspricht unsere Annahme, daß $\mathrm{ggt}(\alpha,\beta)=1$. Daher ist

$$\mathrm{ggt}(\alpha+\beta,\alpha+\beta\rho)=\lambda.$$

Es gilt auch $\mathrm{ggt}(\alpha+\beta,\alpha+\beta\rho^2)=\lambda$. (Denn ein gemeinsamer Teiler π ist auch ein Teiler von

$$(1-\rho^2)\beta=(1-\rho)(1+\rho)\beta=\lambda(1+\rho)\beta.$$

Nun, $1+\rho$ ist eine Einheit, daher muß $\pi|\beta$, falls $\pi\neq\lambda$.)

Schließlich ist $\mathrm{ggt}(\alpha+\beta\rho,\alpha+\beta\rho^2)=\lambda$. Dies folgt, da

$$(\rho-\rho^2)\beta=\rho(1-\rho)\beta=\rho\lambda\beta,$$

wobei ρ wiederum eine Einheit ist.

Sei daher

$$\begin{aligned}\alpha+\beta &= \epsilon_1\xi_1^3\lambda^t\\ \alpha+\beta\rho &= \epsilon_2\xi_2^3\lambda\\ \alpha+\beta\rho^2 &= \epsilon_3\xi_3^3\lambda\end{aligned}$$

oder

$$\begin{aligned}\alpha+\beta &= \epsilon_1\xi_1^3\lambda^t\\ \alpha\rho+\beta\rho^2 &= (\epsilon_2\rho)\xi_2^3\lambda\\ \alpha\rho^2+\beta\rho^4 &= (\epsilon_3\rho^2)\xi_3^3\lambda\end{aligned}$$

wobei ϵ_i Einheiten, $\lambda\not|\xi_i$ und $\mathrm{ggt}(\xi_i,\xi_j)=1$ für $i\neq j$. (Daß diese Darstellung möglich ist, folgt aus der eineindeutigen Primfaktordarstellung der Zahl γ^3. Die Potenz t ist dann $t=3\mathrm{Ord}_\lambda(\gamma)-2$.

Wir summieren diese drei Gleichungen, wobei die Tatsache, daß $1+\rho+\rho^2=0$ benutzt wird.[19] Heraus kommt:

$$0=\epsilon_1\xi_1^3\lambda^t+\underbrace{(\epsilon_2\rho)}_{\text{Einheit}}\xi_2^3\lambda+\underbrace{(\epsilon_3\rho^2)}_{\text{Einheit}}\xi_3^3\lambda.$$

Multipliziere mit $(\epsilon_2\rho)^{-1}$ und λ^{-1};

$$0=\nu\xi_1^3\lambda^{3\mathrm{Ord}_\lambda(\gamma)-1)}+\xi_2^3+\mu\xi_3^3,$$

wobei μ und ν Einheiten sind. Nun, unter der Annahme, daß $\mathrm{Ord}_\lambda(\gamma)-1>0$ ist, erhalten wir dann

$$0\equiv\pm1\pm\mu \bmod \lambda^2,$$

oder $\mu\equiv\pm1 \bmod \lambda^2$. Da $|\lambda^2|=3$ und $|\mu\pm1|\le 2$, aber $\lambda^2|\mu\pm1$, folgt daß tatsächlich $\mu\pm1=0$ oder $\mu=\pm1$. Falls $\mu=-1$, dann nehme $-\xi_3$ statt ξ_3. Jetzt haben wir

$$0=\nu\left(\xi_1\lambda^{(\mathrm{Ord}_\lambda(\gamma)-1)}\right)^3+\xi_2^3+\xi_3^3$$

und $\mathrm{Ord}_\lambda(\gamma)-1<\mathrm{Ord}_\lambda(\gamma)$. □

Der Beweis von Satz 85 folgt nun mit der Beobachtung, daß Satz 87 eine vollstandige Induktion ermöglicht.

15 π und e sind transzendente Zahlen

Ich werde hier der Beschreibung in dem Buch von Hardy und Wright folgen, wo die Transzendenz sowohl von e als auch von π als eine Einheit bewiesen wird.

Für jedes $r\in\mathbb{N}_0=\mathbb{N}\cup\{0\}$ und $x\in\mathbb{C}$, sei

$$u_r(x)=\frac{x}{r+1}+\frac{x^2}{(r+1)(r+2)}+\cdots=e^{|x|}\epsilon_r(x),$$

wobei eine weitere Zahl $\epsilon_r(x)$ dadurch auch definiert wird. Aber

$$e^{|x|}=1+|x|+\frac{|x|^2}{2!}+\cdots.$$

Daher ist $|u_r(x)|<e^{|x|}$ und folglich $|\epsilon_r(x)|<1$.

Wir werden nun eine neue Notation einführen. Sei etwa $f(x)=\sum_{k=0}^n a_k x^k$ irgendein Polynom in x. Dann wird die entsprechende Zahl $f(\aleph)$ definiert als

$$f(\aleph)=\sum_{k=0}^n a_k k!.$$

D.h. immer, wenn ein x-Potenz, etwa x^k, in $f(x)$ vorkommt, dann wird dies mit der Zahl $k!$ ersetzt.

Oder auch, wenn $F(x_1,\ldots,x_m)$ ein Polynom in m Variablen ist, dann wird etwa $F(x_1,\ldots,x_{m-1},\aleph)$ als ein Polynom in $m-1$ Variablen definiert, wobei jedes mal, wenn ein x_m^k vorkommt, wird dies mit der Zahl $k!$ ersetzt. Z.B. wenn $F(x,y)=\sum_{k=0}^n a_k(x+y)^k$ dann ist

$$F(x,\aleph)=\sum_{r=0}^m a_r(x+\aleph)^k=\sum_{r=0}^m a_r B(x,r),$$

wobei

$$B(x,r)=\sum_{k=0}^r\binom{r}{k}x^r\aleph^{r-k}=\sum_{k=0}^r\binom{r}{k}x^r(r-k)!$$

[19] Es gilt $\rho^4=\rho^2\rho^2=(-1-\rho)^2=1+2\rho+\rho^2=1+2\rho-1-\rho=\rho$. Daher $1+\rho^2+\rho^4=1-1-\rho+\rho=0$.

Aber vorsicht! Es ist ganz offensichtlich so, daß $\aleph^m\aleph^n \neq \aleph^{m+n}$. D.h. nach unserer Vereinbarung wird die Identifizierung von $\aleph^k$ mit $k!$ nur gemacht *nachdem* alle $\aleph$'s in ein Polynom zusammen multipliziert werden.

Nun sei

$$\phi(x) = \sum_{r=0}^{m} a_r x^r$$

ein Polynom mit Koeffizienten $a_r \in \mathbb{C}$, und sei

$$\psi(x) = \sum_{r=0}^{m} a_r \epsilon_r(x) x^r.$$

Mit diesen Vereinbarungen gilt

$$e^x \phi(\aleph) = \phi(x + \aleph) + \psi(x) e^{|x|}.$$

Um dies zu sehen, nehme irgendein $0 \leq r \leq m$ und betrachte den Term $e^x r!$. Es genügt, zu zeigen, daß

$$e^x r! = B(x, r) + e^{|x|} \epsilon_r(x) x^r.$$

Aber

$$\begin{aligned} B(x,r) &= r! + r(r-1)!x + \frac{r(r-1)}{2 \cdot 1}(r-2)!x^2 + \cdots + \frac{r!}{r!}x^r \\ &= r!\left(1 + x + \frac{x^2}{2!} + \cdots + \frac{x^r}{r!}\right) \\ &= r!e^x - u_r(x)x^r. \end{aligned}$$

Satz 90. *Angenommen $m \geq 2$, und $f(x)$ ist ein Polynom mit Integer- Koeffizienten. Seien*

$$F_1(x) = \frac{x^{m-1}}{(m-1)!} f(x), \quad F_2(x) = \frac{x^m}{(m-1)!} f(x).$$

Dann sind $F_1(\aleph)$, $F_2(\aleph)$ Integerzahlen, und es gilt

$$F_1(\aleph) \equiv f(0) \bmod m, \quad F_2(\aleph) \equiv 0 \bmod m.$$

Beweis. Sei

$$f(x) = \sum_{l=0}^{L} a_l x^l,$$

$a_l \in \mathbb{Z}$ für alle l. D.h.

$$F_1(x) = \sum_{l=0}^{L} a_l \frac{x^{l+m-1}}{(m-1)!},$$

und mit $\aleph$ statt x:

$$F_1(\aleph) = \sum_{l=0}^{L} a_l \frac{\aleph^{l+m-1}}{(m-1)!} = \sum_{l=0}^{L} a_l \frac{(l+m-1)!}{(m-1)!},$$

wobei

$$\frac{(l+m-1)!}{(m-1)!} = (l+m-1)(l+m-2)\cdots m.$$

Folglich ist m ein Teiler von $\frac{(l+m-1)!}{(m-1)!}$, falls $l > 0$. Nur der Term $l = 0$ bleibt übrig und wir haben

$$F_1(\aleph) \equiv a_0 \equiv f(0) \bmod m.$$

Für F_2 erhalten wir

$$F_2(\aleph) = \sum_{l=0}^{L} a_l \frac{(l+m)!}{(m-1)!}$$

und jeder Term wird durch m geteilt (auch $l = 0$). Daher

$$F_2(\aleph) \equiv 0 \bmod m.$$

□

Satz 91. *e ist transzendent.*

Beweis. Falls nicht, sei

$$\sum_{t=0}^{n} C_t e^t = 0$$

eine Polynomgleichung mit $C_t \in \mathbb{Z}$ für alle t, die e als Nullstelle hat. Falls $C_0 = 0$, dann wäre es möglich, das Polynom durch e zu teilen, um ein Polynom kleineren Grads mit Nullstelle e zu bekommen. Wir können daher annehmen, daß $C_0 \neq 0$.

Sei jetzt $p \in \mathcal{P}$ irgendeine Primzahl mit $p \geq \max\{n, |C_0|\}$. Wir betrachten die Funktion

$$\begin{aligned}\phi(x) &= \frac{x^{p-1}}{(p-1)!}\{(x-1)(x-2)\cdots(x-n)\}^p \\ &= \frac{x^{p-1}}{(p-1)!}f(x) \\ &= \sum_{r=0}^{s} a_r x^r,\end{aligned}$$

wobei $f(x) = \{(x-1)(x-2)\cdots(x-n)\}^p$. Nach Satz 90 gilt

$$\phi(\aleph) = f(0) = \{(-1)^n n!\}^p = (-1)^{pn}(n!)^p \not\equiv 0 \bmod p.$$

(Die letztere Gleichung folgt, da $p > n$ eine Primzahl ist.)

Multipliziere die Gleichung $\sum C_t e^t = 0$ mit $\phi(\aleph)$:

$$\begin{aligned}\phi(\aleph)\left\{\sum_{t=0}^{n} C_t e^t\right\} &= \sum_{t=0}^{n} C_t\left\{e^t\phi(\aleph)\right\} \\ &= \sum_{t=0}^{n} C_t\phi(t+\aleph) + \sum_{t=0}^{n} C_t\psi(t)e^t \\ &= S_1 + S_2 = 0,\end{aligned}$$

wobei

$$\psi(t) = \sum_{r=0}^{s} a_r \epsilon_r(t) t^r$$

und die Koeffizienten a_r identisch mit den Koeffizienten in dem Polynom $\phi(x)$ sind.

Sei jetzt t eine Integerzahl mit $1 \leq t \leq n$. Dann ist

$$\phi(t+x) = \frac{(t+x)^{p-1}}{(p-1)!}\{(x+t-1)(x+t-2)\cdots(x+t-n)\}^p.$$

Insbesondere ist ein Term der Art $(x+t-t)^p = x^p$ in diesem Produkt. D.h.

$$\phi(t+x) = G(x) = \frac{x^p}{(p-1)!}g(x),$$

wobei $g(x)$ irgendein Polynom mit Integerkoeffizienten ist. Nach Satz 90 ist

$$\phi(t+\aleph) = G(\aleph) \equiv 0 \bmod p.$$

D.h. S_1 ist eine Integerzahl mit

$$S_1 = \sum_{t=0}^{n} C_t\phi(t+\aleph) = C_0\phi(\aleph) = C_0(-1)^{pn}(n!)^p \not\equiv 0 \bmod p.$$

Daher ist $|S_1| \geq 1$ für alle hinreichend großen $p \in \mathcal{P}$.

Andererseits ist (von vorher) $|\epsilon_r(t)| < 1$ für alle r. Daher

$$\begin{aligned} |\psi(t)| &< \sum_{r=0}^{s} |a_r| t^r \\ &\leq \frac{t^{p-1}}{(p-1)!}\{(t+1)(t+2)\cdots(t+n)\}^p. \end{aligned}$$

Je größer die Zahl p ist, desto kleiner ist $|S_2|$. Insbesondere ist die Gleichung $S_2 = -S_1 \neq 0$ falsch, wenn $|S_2| < 1$. □

Satz 92. *π ist transzendent*

Der Beweis für π ist ähnlich, aber etwas komplizierter. Wir müssen zunächst einige Worte über die symmetrischen Polynome verlieren. Sei $P(x_1, \ldots, x_n)$ ein Polynom in n Unbekannten. P heißt *symmetrisch*, falls jede mögliche Permutation der Unbekannten das Polynom unverändert läßt. Z.B.

$$(x_1 + 1)(x_2 + 1)\cdots(x_n + 1)$$

ist offensichtlich symmetrisch. Wir multiplizieren alles aus:

$$x_1 x_2 \cdots x_n + \cdots + (x_1 + x_2 + \cdots + x_n) + 1.$$

Jeder Term hier ist für sich auch ein symmetrisches Polynom. Dies sind die 'elementaren symmetrischen Polynome'. Es ist leicht zu sehen (siehe etwa van der Waerden's Algebra I, Seite 100), daß jedes symmetrisches Polynom als Polynom in den elementaren symmetrischen Polynomen dargestellt werden kann.

Diese ganze Sache kann auch anders betrachtet werden. Sei nun

$$P(x) = dx^m + d_1 x^{m-1} + \cdots + d_m$$

ein Polynom in einer Unbekannten mit $d \neq 0$, und seien $\beta_1, \ldots, \beta_m$ die Nullstellen von P. (D.h. $P(\beta_j) = 0$, für alle j.) Bekannterweise gibt es dann die Darstellung

$$\begin{aligned} P(x) &= d(x - \beta_1)(x - \beta_2)\cdots(x - \beta_m) \\ &= d(x^m + (\beta_1 + \cdots + \beta_m)x^{m-1} + \cdots + (\beta_1\beta_2\cdots\beta_m)). \end{aligned}$$

Die elementaren Polynome—konstruiert aus den β_j's—sind also

$$\begin{aligned} d_1 &= d(\beta_1 + \cdots + \beta_m) \\ d_2 &= d(\beta_1\beta_2 + \beta_1\beta_3 + \cdots + \beta_{m-2}\beta_m + \beta_{m-1}\beta_m) \\ &\vdots \\ d_m &= d(\beta_1\beta_2\cdots\beta_m) \end{aligned}$$

Falls $P(x)$ nur Integerkoeffizienten hat (d.h. d, bzw. d_j sind Integerzahlen) dann sind die symmetrischen Polynome auf der rechten Seite hier auch Integerzahlen, wobei jedes Polynom mit d multipliziert wird. Andererseits, wenn wir ein beliebiges symmetrisches Polynom in

$$d\beta_1, d\beta_2, \ldots, d\beta_m$$

nehmen, dann handelt es sich um eine Integerzahl (und zwar ein Polynom in $d, d_1, \ldots, d_m$).

Satz 93. *Falls π eine algebraische Zahl ist, dann ist auch $i\pi$ algebraisch.*

Beweis. Angenommen, $a_0\pi^m + a_1\pi^{m-1} + \cdots + a_{m-1}\pi + a_m = 0$ mit $a_j \in \mathbb{Z}$ für alle j und $a_0 \neq 0$. Dann ist

$$\begin{aligned} &\left(a_0(i\pi)^m - a_2(i\pi)^{m-2} + \cdots + a_m\right) + \\ &\quad i\left(a_1(i\pi)^{m-1} - a_3(i\pi)^{m-3} + \cdots - a_{m-1}(i\pi)\right) = 0. \end{aligned}$$

(Dies ist der Fall $m \equiv 0 \bmod 4$. Die anderen Fälle sind ähnlich.) Daher

$$\begin{aligned}&\left(a_0(i\pi)^m - a_2(i\pi)^{m-2} + \cdots + a_m\right)^2 + \\ &\quad\left(a_1(i\pi)^{m-1} - a_3(i\pi)^{m-3} + \cdots - a_{m-1}(i\pi)\right)^2 = 0\end{aligned}$$

und dies ist eine Polynomgleichung mit Integer Koeffizienten. □

Unsere Annahme ist, daß $i\pi$ algebraisch ist. Unser Ziel ist es, dadurch zu einem Widerspruch zu gelangen. Sei daher

$$d(i\pi)^m + d_1(i\pi)^{m-1} + \cdots + d_m = 0$$

mit $d, d_j \in \mathbb{Z}$ für alle j, und $d \neq 0$. Seien $\omega_1, \ldots, \omega_m$ die Nullstellen. Da $e^{i\pi} = -1$, gilt

$$1 + e^{\omega_j} = 0,$$

für mindestens ein j. Daher ist

$$(1 + e^{\omega_1})(1 + e^{\omega_2}) \cdots (1 + e^{\omega_m}) = 1 + \sum_{t=1}^{2^m-1} e^{\alpha_t} = 0,$$

wobei $\alpha_1, \alpha_2, \ldots, \alpha_{2^m-1}$ die Zahlen

$$\omega_1, \ldots, \omega_m, \omega_1 + \omega_2, \omega_1 + \omega_3, \ldots, \omega_1 + \cdots + \omega_m$$

darstellen. Vielleicht sind manche α_i Null. Schreibe dann

$$\alpha_1, \alpha_2, \ldots, \alpha_n, 0, 0, \ldots, 0$$

wobei die Reihenfolge so ist, daß $\alpha_j \neq 0$ für $j = 1, \ldots, n$. Dann ist

$$1 + \sum_{t=1}^{2^m-1} e^{\alpha_t} = C + \sum_{t=1}^{n} e^{\alpha_t} = 0,$$

wobei $C = 2^m - n$. Sei $p \in \mathcal{P}$ mit

$$p > \max\{d, C, |d^n \alpha_1 \cdots \alpha_n|\}.$$

Sei

$$\phi(x) = \frac{x^{p-1}}{(p-1)!} d^{np+p-1}\{(x-\alpha_1)\cdots(x-\alpha_n)\}^p = \frac{x^{p-1}}{(p-1)!} \sum_{l=0}^{np} g_l x^l,$$

Jedes g_l ist dann ein symmetrisches Polynom in $d\alpha_1, \ldots, d\alpha_n$

Es ist nun möglich, die elementaren symmetrischen Polynome in

$$\alpha_1, \ldots, \alpha_n$$

zu ergänzen zu elementaren symmetrischen Polynome in

$$\alpha_1, \ldots, \alpha_n, \alpha_{n+1}, \ldots, \alpha_{2^m-1}.$$

Zum Beispiel, das erste Polynom, nämlich

$$\alpha_1 + \cdots + \alpha_n$$

wird zu

$$\alpha_1 + \cdots + \alpha_n + \underbrace{\alpha_{n+1} + \cdots + \alpha_{2^m-1}}_{0}.$$

Das letzte Polynom ist

$$\alpha_1 \alpha_2 \cdots \alpha_n$$

und wird zu

$$\alpha_1 \cdots \alpha_n + \underbrace{\alpha_1 \cdots \alpha_{n-1}\alpha_{n+1} + \cdots + \alpha_{2^n-1-n} \cdots \alpha_{2^n-1}}_{0}.$$

Daher ist jedes g_l auch ein symmetrisches Polynom in $\omega_1, \ldots, \omega_m$, und folglich ist jedes g_l eine Integerzahl. D.h. $\phi(\aleph)$ ist auch eine Integerzahl (hier ist unser $\aleph^r = r!$ gemeint; siehe Satz 90).

Wir haben nun

$$e^{\alpha_t}\phi(\aleph) = \phi(\alpha_t + \aleph) + \psi(\alpha_t)e^{|\alpha_t|},$$

wobei

$$\psi(\alpha_t) = \frac{\alpha_t^{p-1}}{(p-1)!}\sum_{l=0}^{np} g_l \epsilon_l(\alpha_t)\alpha_t^l.$$

Daher

$$\left(C + \sum_{t=1}^{n} e^{\alpha_t}\right)\phi(\aleph) = S_0 + S_1 + S_2 = 0,$$

wobei

$$\begin{aligned} S_0 &= C\phi(\aleph) \\ S_1 &= \sum_{t=1}^{n}\phi(\alpha_t + \aleph) \\ S_2 &= \sum_{t=1}^{n}\psi(\alpha_t)e^{|\alpha_t|} \end{aligned}$$

Nun, $\phi(\aleph) \in \mathbb{Z}$, und daher ist S_0 eine Integerzahl. Nach Satz 90 gilt

$$C\phi(\aleph) = Cd^{np+p-1}\{(-\alpha_1)\cdots(-\alpha_n)\}^p \not\equiv 0 \bmod p$$

da $p > \max\{d, C, |d^n\alpha_1 \cdots \alpha_n|\}$.

Was ist S_1? D.h. was ist $\phi(\alpha_t + \aleph)$, für $t = 1, \ldots, n$? Es gilt[20]

$$\begin{aligned} \phi(\alpha_t + x) &= \frac{(\alpha_t + x)^{p-1}}{(p-1)!}d^{np+p-1}\left\{\prod_{k=1}^{n}(\alpha_t + x - \alpha_k)\right\}^p \\ &= \frac{x^p}{(p-1)!}\sum_{l=0}^{np-1} f_{l,t}x^l \end{aligned}$$

wobei $f_{l,t}$ jeweils eine Summe von Produkten von Termen der Art $d\alpha_k$ ist. $f_{l,t}$ ist also symmetrisch in den Termen $d\alpha_k$, wobei $k \neq t$. Wir nehmen nun die Summe über alle t

$$F_l = \sum_{t=1}^{n} f_{l,t}.$$

Dann ist F_l ein symmetrisches Polynom in *allen* $d\alpha_k$, folglich in den Termen $\omega_1, \ldots, \omega_m$ und folglich ist F_l eine Integerzahl, für alle l. Daher

$$\Phi(x) = \sum_{t=1}^{n}\phi(\alpha_t + x) = \frac{x^p}{(p-1)!}\sum_{l=0}^{np-1} F_l x^l,$$

und nach Satz 90 ist $\Phi(\aleph) \in \mathbb{Z}$ mit

$$\Phi(\aleph) \equiv 0 \bmod p.$$

Auf jeden Fall ist $S_0 + S_1 \in \mathbb{Z}$ mit $S_0 + S_1 \not\equiv 0 \bmod p$. Insbesondere

$$|S_0 + S_1| \geq 1.$$

[20] Falls $k = t$ dann gilt $(\alpha_t + x - \alpha_k) = x$. Daher hat jeder Term ein Faktor x^p.

Andererseits (da $|\epsilon_r(\alpha_t)| < 1$) gilt

$$|\psi(\alpha_t)| \leq \frac{|d|^{np+p-1}|\alpha_t|^{p-1}}{(p-1)!}\{(|\alpha_t|+|\alpha_1|)\cdots(|\alpha_t|+|\alpha_n|)\}^p.$$

Dieses Produkt wird beliebig klein, je größer $p \in \mathcal{P}$ gewählt wird. Daher ist $S_0 + S_1 + S_2 \neq 0$ für hinreichend große p; ein Widerspruch.

Bemerkung. *Die Transzendenz von e und π ist von Hermite (1873), bzw. von Lindemann (1882) bewiesen worden.*