Vom Zahlentee

der heißen und leckeren Königin der Mathematik

* *

*

von
Trappaschmidti,
Demel,
Gauss & Leuler

27. April 2002

Vorwort

Wenn man lange Weile Langeweile hat, dann kann es schon mal vorkommen, daß man – nur mal so aus Spaß – ein Bier trinkt. Und dann noch eins. Und noch eins. Man sagt sich: Es heißt hinähn. Hinähn und hinähn. Immer wieder hinähn.
Irgendwann fragt man sich: Wo oft hieß es denn jetzt hinähn? Man fängt an zu zählen. Und weil es doch so Langweilig ist (z.B. in einer Sternwarte) zählt man alles mögliche. Die Finger, die Minuten, die Stunden, die Sterne, die Sternschnuppen, die Schuppen. Die herunterfallen, wenn man sich am Kopf kratzt.
Weil das alles immer noch sehr langweilig ist, guckt man mal, durch welche Zahlen sich die Zahlen teilen lassen, die man da die ganze Zeit gezählt hat. Dann zählt man die Anzahl der Teiler einer gezählten Zahl. Und vielleicht noch bei einer anderen Zahl. Man freut sich, dass diese Anzahlen übereinstimmen. Dann trinkt man ein Bier. Dann sieht man, dass die Anzahl der Teiler gleich der Summe der beiden Zahlen ist. Man trinkt schnell noch zwei Bier. Man sagt, die Zahlen heißen befreundet, freut sich, trinkt noch ein Bier und kratzt sich am Kopf, um weitere Zahlen zu erzeugen.
Wenn man diese Spielereien weitertreibt, so kommt dabei allerlei heraus. Bei den meisten Leuten kommt dabei hauptsächlich das getrunkene Bier wieder heraus. Aber wenn man sogar Chef einer Sternwarte ist, und es einen ganz doll am Kopf juckt, dann kann da schon mal mehr herauskommen.
Den kleinen Carl-Friedrich hat es ganz stark gejuckt. (Das kommt vom vielen Trinken.) Es hat ihn so stark gejuckt, daß man sich heutzutage bei dem Anblick eines 10-DM Scheins unwillkürlich an den Kopf fassen muss, vor lauter Jucken.
Andere hat es auch gejuckt. Wen es an welchen Stellen gejuckt hat, und was dabei herausgekommen ist, darüber will diese Schrift berichten. Viel Spass beim Kratzen wünschen

Trappaschmidti und Demel

Alles was zählt ist Zählen.

Inhaltsverzeichnis

1 Grundregeln zum Kochen von Zahlentee

1.1 Teilbarkeit

Definition. $\boxed{t|n :\Leftrightarrow \exists z \in \mathbb{Z} : tz = n.}$

Wegen $t|n \Rightarrow -t|n \wedge t|-n \wedge -t|-n$ reicht es völlig, die Teilerrelation in $\mathbb{N}$ und nicht mehr im stressigen $\mathbb{Z}$ zu betrachten.

Satz 1:
Die Teilerrelation ist eine (nicht-lineare) Ordnungsrelation.
Beweis. Es gilt:
$n|n$ (Reflexivität),
$m|n \wedge n|m \Rightarrow m = n$ (Antisymmetrie) und
$l|m \wedge m|n \Rightarrow l|n$ (Transitivität).
Hingegen ist $n|m \vee m|n \vee n = m$ (Linearität) i. a. nicht erfüllt. □

Satz 2:
Für natürliche a, b, t und ganze r, s stimmt: $t|a \wedge t|b \Rightarrow t|ra + sb$ stets mit der Wahrheit überein.
Beweis. Es gilt: $t|a \wedge t|b \Rightarrow \exists k_1, k_2 \in \mathbb{N} : k_1 t = a \wedge k_2 t = b \Rightarrow ra + sb = k_1 at + k_2 bt = (k_1 a + k_2 b)t \Rightarrow t|ra + sb.$ □

Korrolar:
$t|a \wedge t|b \Leftrightarrow t|a - qb \wedge t|b \Leftrightarrow t|a \wedge t|b - qa.$

Definition. $\boxed{T_n := \{t : t|n\}}$

Alle Aussagen über Teilbarkeit übertragen sich auf analoge Aussagen über Teilermengen.

Satz 3:
Es ist wahr, daß $T_a \cap T_b = T_{a-qb} \cap T_b = T_a \cap T_{b-qa}$.
Beweis. Als wahr erkannt wurde bereits:
$t|a \wedge t|b \Leftrightarrow t|a - qb \wedge t|b \Leftrightarrow t|a \wedge t|b - qa.$ □

1.2 Der größte gemeinsame Teiler und EUKLIDs Algorithmus

Geschichtliche Belehrung. 1) EUKLID von Alexandria lebte um 300 v. Chr. Am bekanntesten ist sein Werk mit dem Titel *Elemente*, in dem er das mathematische Wissen seiner Zeit darstellte, wobei er vor allem Wert auf strenge Beweisführungen legte. Teile dieses Werkes wurden noch im 18. Jahrhundert in Schulen als Unterrichtsbuch verwendet. Ein nach EUKLID benannter Satz muß nicht immer von diesem gefunden worden sein, der wahre Entdecker ist meistens nicht mehr bekannt.

2) „Algorithmus“ ist eine Verarschung von AL CHWARIZMI, dem Namen eines arabischen Gelehrten des 9. Jahrhunderts, dessen Schriften mit dazu beitrugen, das indisch-arabische Ziffernsystem zu verbreiten.

Definition. $\boxed{\mathrm{ggT}(a,b) := \max T_a \cap T_b}$

Satz 1 (EUKLID):
Es ist: $\underline{\mathrm{ggT}(a,b) = \mathrm{ggT}(a-b,b) = \mathrm{ggT}(b-a,a) = \mathrm{ggT}(b,a).}$
Beweis. $T_a \cap T_b = T_{a-qb} \cap T_b = T_a \cap T_{b-qa}$ □

Definition. Für $a, b \in \mathbb{N}$ bezeichnet man die folgende Kette von Divisionen mit Rest als **Euklidischen Algorithmus:**

$$\begin{aligned}
a &= q_0 b + r_1 && \text{mit } 0 < r_1 < b \\
b &= q_1 r_1 + r_2 && \text{mit } 0 < r_2 < r_1 \\
r_1 &= q_2 r_2 + r_3 && \text{mit } 0 < r_3 < r_2 \\
&\vdots \\
r_{n-2} &= q_{n-1} r_{n-1} + r_n && \text{mit } 0 < r_n < r_{n-1} \\
r_{n-1} &= r_n q_n
\end{aligned}$$

Darin soll r_n der letzte von Null verschiedene Rest in dieser Divisionskette sein. Ein solcher existiert, da die Folge der Reste $b, r_1, r_2, r_3, ..., r_{n-1}, r_n$ streng monoton fallend ist.

Satz 2:
Der letzte von Null verschiedene Rest r_n ist der größte gemeinsame Teiler von a und b.
Beweis. Satz 1. □

Korrolar: Daraus folgt, daß es ganze Zahlen u und v gibt mit $\mathrm{ggT}(a,b) = ua + vb$. Mit den obigen Bezeichnungen gilt nämlich:

$$\begin{aligned} r_n &= r_{n-2} + (-v_{n-1})r_{n-1} \\ &= r_{n-2} + (-v_{n-1})(r_{n-3} + (-v_{n-2})r_{n-2}) \\ &= r_{n-4} + (-v_{n-3})r_{n-3} + (-v_{n-1})(r_{n-3} + (-v_{n-2})(r_{n-4} + (-v_{n-3})r_{n-3})) \\ &\vdots \end{aligned}$$

1.3 Primzahlen

Definition. Eine Zahl, die genau zwei Teiler hat, heißt **Primzahl.**

$\boxed{p \text{ Primzahl} :\Leftrightarrow |T_p| = 2}$

Definition. Die Menge aller Primzahlen wird mit $\mathbb{P}$ bezeichnet.

$\boxed{\mathbb{P} := \{p : p \text{ Primzahl}\}}$

Definition. Natürliche Zahlen a und b heißen **relativ prim**, wenn $\mathrm{ggT}(a,b) = 1$.

$\boxed{a, b \text{ relativ prim} :\Leftrightarrow \mathrm{ggT}(a,b) = 1}$

Trivialitäten.

1. Für $p \in \mathbb{P}$ gilt: $p|ab \Rightarrow p|a \vee p|b$
2. Wenn m und n relativ prim zueinander sind, gilt: $m|a \wedge n|a \Rightarrow mn|a$

1.4 Fundamentalsatz der Arithmetik

Satz 1 (Fundamentalsatz der Arithmetik):
Jede von Eins verschiedene natürliche Zahl ist als Produkt endlich vieler Primzahlen darstellbar, besitzt also eine **Primfaktorzerlegung.** Die Darstellung ist bis auf die Reihenfolge eindeutig.

Beweis.
(i) *Existenz:* (vollständige Induktion)
Induktionsanfang: Da 2 eine Primzahl ist, rufen wir: „HOSSA!“
Induktionsschluß: Tun wir mal so, als besäßen alle Zahlen m mit $1 < m < n$ eine Primfaktorzerlegung. Zu zeigen ist, daß auch n eine solche besitzt. Falls n eine Primzahl ist, sind wir unsere Sorgen los. Falls nicht, gibt es $k, l \in \mathbb{N}$ mit $1 < k, l < n$ und $n = k \cdot l$. Da k und l aber stolze Primfaktorzerlegungsbesitzer sind, gilt solches auch für n.
(ii) *Eindeutigkeit:*
1. Beweis (Zermelo). Nimmt man an, daß es natürliche Zahlen > 1 mit verschiedenen Primfaktorzerlegungen gibt, so gibt es eine kleinste derartige Zahl n. Seien $n = \prod_{i=1}^{r} p_i = \prod_{j=1}^{s} q_j$ zwei verschiedene Primfaktorzerlegungen von n in Primfaktoren. Dann sind die Mengen $\{p_1, ..., p_r\}$ und $\{q_1, ..., q_s\}$ disjunkt: Wäre nämlich p_k ein gemeinsames Element, so hätte auch $p_1 \cdot ... \cdot p_{k-1} \cdot p_{k+1} \cdot ... \cdot p_r < n$ zwei verschiedene Zerlegungen. Sei nun o. B. d. A. $p_1 < q_1$.
Dann gilt für $m := (q_1 - p_1) \cdot q_2 \cdot ... \cdot q_s = p_1(p_2 \cdot ... \cdot p_r - q_2 \cdot ... \cdot q_s)$ offensichtlich $m < n$; m besitzt also eine eindeutige Primfaktorzerlegung. Jedoch erkennt man in $p_1 \nmid (q_1 - p_1)$ und $p_1 \nmid q_2 \cdot ... \cdot q_s$, aber $p_1 | p_1(p_2 \cdot ... \cdot p_r - q_2 \cdot ... \cdot q_s)$ einen Widerspruch. □

2. Beweis (Euklid).
Fundamentallemma: Wenn eine Primzahl p das Produkt $a \cdot b$ zweier ganzer Zahlen a, b teilt, dann teilt sie mindestens einen der Faktoren.
Beweis des Lemmas nach Euklid. $(p \in \mathbb{P} \wedge p | a \cdot b)$, d. h. $\mathrm{ggT}(p, a \cdot b) = p$.
Sei $p \nmid a$, d. h. $\mathrm{ggT}(a, p) = 1$. Dann gibt es $x, y \in \mathbb{Z}$ mit $1 = ax + py$. Das ist schön und es folgt $b = abx + bpy$. Wegen $p | abx$ und $p | bpy$ muß dann auch $p | abx + bpy = b$ gelten. □
Mit vollständiger Induktion kann man weiter zeigen, daß, falls ein Produkt $n = \prod_{i=1}^{r} n_i$ von $r > 2$ ganzen Zahlen durch eine Primzahl p teilbar ist, mindestens ein Faktor durch p teilbar ist.

Gäbe es nun eine Zahl $n \in \mathbb{N}$ mit zwei verschiedenen Primfaktorzerlegungen,
so gäbe es Primzahlen $p_1, ..., p_r, q_1, ..., q_s$ mit $p_1 \cdot ... \cdot p_r = q_1 \cdot ... \cdot q_s$ und $\{p_1, ..., p_r\} \cap \{q_1, ..., q_s\} = \emptyset$. So geht's aber nicht, denn es folgt $p_1 = q_i$ für ein $i \in \{1, ..., s\}$ aus $p_1 | q_1 \cdot ... \cdot q_s$. □

3. Beweis (Gauss).
Wie auch der gerade geführte benutzt auch dieser Beweis das Fundamentallemma.

Beweis des Lemmas nach Gauss:
Es sei $p \in \mathbb{P}$ und $p|ab$ und es sei $E := \{x \in \mathbb{N}\backslash\{0\} : p|ax\}$.
(i) Es gilt: $p \in E$, $b \in E$ und es gibt eine kleinste Zahl $c \in \mathbb{N}\backslash\{0\}$ mit $c \in E$.
(ii) Es gilt: $\forall y \in E : c|y$.
Zu y und c gibt es nämlich $q, r \in \mathbb{N}$ mit $y = qc + r$ und $0 \leq r < c$. Aus $p|ay$, $p|ac$ und $ar = ay - q(ac)$ folgt $p|ar$. Daraus folgt $r = 0$, weil $r > 0$ wegen $r < c$ der Minimalität von c widerspräche. Mithin gilt: $y = qc$, also $c|y$.
(iii) Wegen $p \in E$ folgt $c|p$, also $c = 1$ oder $c = p$.
(iv) Aus $c = 1$ folgt $p|a$ wegen $p|ac$; aus $c = p$ folgt $p|b$ wegen $b \in E$. □
Wie im vorangegangenen Beweis ergibt sich jetzt aus dem Lemma die Eindeutigkeit der Primfaktorzerlegungen natürlicher Zahlen. □

4. Beweis (Beweis des Lemmas nach Suranyi (1962)):
Es sei $n = a \cdot b$ die kleinste Zahl, für die das Lemma nicht gilt. Ohne Einschränkung *Warum?* sei $a < p$. Dann ist $a > a' := a - p > 0$. Aus $n = ab > a'b = ab - pb$ folgt $p|a'b < n$, für welches aber das Lemma gilt, also $p|b \vee p|a' = a - p \Rightarrow p|a$. □

5. Beweis der Eindeutigkeit (nach Klappauf):
Es sei $n = p_1 \cdot \ldots \cdot p_r = q_1 \cdot \ldots \cdot q_s$ die kleinste Zahl, für die das Lemma nicht gilt, und es sei $p_1 \leq \ldots \leq p_r \wedge q_1 \leq \ldots \leq q_s$. O. B. d. A. ist $q_1 < p_1$ die kleinste aller Primzahlen. Jedes p_i läßt sich darstellen als $p_i = Q_i q_1 + R_i$ mit $0 < R_i < q_1$ ($R_i \neq 0$ wegen $q_1 < p_i$). Betrachte jetzt $n = \prod_1^r p_i = Qq_1 + R$ mit $R = \prod_1^r R_i \neq 0$. Das heißt $R = n - Qq_1$, also $q_1|R = \prod_1^r R_i$, d. h. (da $R < n$) $q_1|R_i > 0$ für ein $i \in \{1, ..., r\}$, d. h. $q_1 \leq R_i$, im Widerspruch zu $0 < R_i < q_1$. Das heißt: *q. e. d.* □

Geschichtliche Belehrung. Carl Friedrich Gauss (1777 - 1855) wird vielfach als der bedeutenste Mathematiker aller Zeiten angesehen (nicht von Werner Raab), man spricht von ihm als dem *princeps mathematicorum.* Obwohl er fast alle Gebiete der Mathematik weiterentwickelte und auch wesentliche Beiträge zur Astronomie und Geodäsie lieferte, galt seine Liebe vor allem der Zahlentheorie, die er die „Königin der Mathematik“ nannte. Im Jahr 1801 erschien seine Arbeit mit dem Titel *Disquisitiones Arithmeticae,* welche ein Meilenstein in der Entwicklung der Zahlentheorie ist; geschrieben hat er diese Arbeit als Achtzehnjähriger. Gauss leerte in Göttingen, wo er ab 1807 Professor der Astronomie und Direktor der Sternwarte war, so manchen Krug. Ehrenvolle Berufungsangebote an andere Universitäten hat er stets abgelehnt.

1.4.1 Folgerungen

Folgerung 1:
Für alle $n, m \in \mathbb{N}$ ist $\sqrt[m]{n}$ entweder eine ganze oder eine irrationale Zahl.
Beweis: Gibt es Zahlen $a, b \in \mathbb{N}$ mit $\sqrt[m]{n} = \frac{a}{b}$, also $n \cdot b^k = a^k$, dann gilt für die Exponenten α_i, β_i und ν_i in der kanonischen PFZ der Zahlen a, b und n

$$\nu_i + k\beta_i = k\alpha_i (i = 1, 2, 3, \ldots).$$

Es folgt $k|\nu_i$ $(i = 1, 2, 3, \ldots)$, also ist n eine k-te Potenz. □

Folgerung 2:
Ist y eine reelle Lösung der Polynomgleichung $x^n + a_1 x^{n-1} + \cdots + a_{n-1}x + a_n = 0$ mit ganzzahligen Koeffizienten $a_1, \ldots, a_n$, dann ist y entweder eine ganze oder eine irrationale Zahl.
Beweis: Sei y rational, also $y = \frac{p}{q}$ mit $p, q \in \mathbb{Z}$ und $b \neq 0$. Die obige Gleichung hat dann (nach Multiplikation mit q^n) die Form

$$p^n + a_1 p^{n-1} q + \cdots + a_{n-1} p q^{n-1} + a_n q^n = 0.$$

Da q die n letzten Summanden der Summe teilt, muß q auch p^n teilen. Jeder Primteiler von q ist daher auch ein Primteiler von p. Setzt man in der Darstellung $y = \frac{p}{q}$ den Bruch als durchgekürzt voraus, so muß also $q = 1$ gelten, die Zahl y ist daher ganz. □

Folgerung 3:
Für $n, m \in \mathbb{N}$ mit $m, n \geq 2$ ist $\log_n m$ irrational, wenn m mindestens einen Primteiler hat, den n nicht hat, oder umgekehrt.
Beweis: Aus $\log_n m = \frac{p}{q}$ folgt $n^{\frac{p}{q}} = m$, also $n^p = m^q$, woraus sich die Behauptung ergibt. □

Folgerung 4:
Die LEULERsche Zahl $e = \sum_{n=0}^{\infty} \frac{1}{n!}$ ist irrational.
Beweis: Für jedes $m \in \mathbb{N}$ gilt $m!e = \sum_{n=0}^{m} \frac{m!}{n!} + r_m$ mit $r_m = \sum_{n=m+1}^{\infty} \frac{m!}{n!}$.
Wegen $0 < r_m < \frac{1}{m+1} \sum_{k=0}^{\infty} \left(\frac{1}{m+2}\right)^k = \frac{m+2}{(m+1)^2} < 1$ kann für kein $m \in \mathbb{N}$ ganz sein. □

Geschichtliche Belehrung. LEONHARD EULER, genannt LEULER, (1707 - 1783) stammte aus Basel und gilt bei WERNER RAAB als der größte Mathematiker aller Zeiten. Er verbrachte den größten Teil seines Lebens in St. Petersburg als Mitglied der dortigen Akademie, von 1741 bis 1766 war er Mitglied der Königlichen Akademie in Berlin. LEULERs Werk gilt als beispiellos, nicht nur bezüglich seines Umfanges:

Er verfaßte mehr als 850 wissenschaftliche Arbeiten und schrieb etwa 20 Bücher; in den 26 Bänden mathematischer Abhandlungen, die die Petersburger Akademie von 1727 bis 1783 herausgab, stammte mehr als die Hälfte der Beiträge von LEULER. Er beschäftgte sich auch mit naturwissenschaftlichen und philosophischen Fragen, der Schwerpunkt seiner Arbeit lag aber in der Mathematik. Hier hat er fast jedes Gebiet mit neuen Ideen und Theorien bereichert, u. a. natürlich auch die Zahlentheorie.

1.4.2 Struktur des ggT und seines Bruders kgV

Ist $a = \prod p^{w_p(a)}$, $b = \prod p^{w_p(b)}$, so gilt $g|a \Leftrightarrow w_p(g) \leq w_p(a)$ und $g|b \Leftrightarrow w_p(g) \leq w_p(b)$.
Ist also g der $\mathrm{ggT}(a,b)$, dann ist $w_p(g) = \min(w_p(a), w_p(b))$.
Wie man sich leicht überlegt, gilt dann auch der folgende Satz:

Satz:
$\mathrm{ggT}(a_1, \ldots, a_n) = \prod_{p \in \mathbb{P}} p^{\min(w_p(a_i);\, i=1,\ldots,n}$
$\mathrm{kgV}(a_1, \ldots, a_n) = \prod_{p \in \mathbb{P}} p^{\max(w_p(a_i);\, i=1,\ldots,n}$
$\mathrm{ggT}(a_1, a_2) \cdot \mathrm{kgV}(a_1, a_2) = a_1 \cdot a_2$

Definition. $(V, \oplus, \odot)$ heißt **Verband**, wenn Kommutativgesetz, Assoziativgesetz und Absorptionsgesetz $(\forall a, b \in V : a \odot (a \oplus b) = a \wedge a \oplus (a \odot b) = a)$ gelten. Gelten für $a, b, c \in V$ auch die Distributivgesetze $a \oplus (a \odot c) = (a \oplus b) \odot (a \oplus c)$ und $a \odot (a \oplus c) = (a \odot b) \oplus (a \odot c)$, dann heißt $(V, \oplus, \odot)$ ein **distributiver Verband**.

Feststellung. (T_n, ggT, kgV) ist, wie man leicht nachprüft, ein distributiver Verband.

Definition. Ein distributiver Verband $(V, \oplus, \odot)$ mit $\underline{0} \in V$ und $\underline{1} \in V$, so daß $a \oplus \underline{0} = a$ und $a \odot \underline{1} = a$, wo $\forall a \in V \exists x \in V : a \oplus x = \underline{1} \wedge a \odot x = \underline{0}$ (x heißt komplementäres Element von a) gilt, heißt **Boolsche Algebra**.

Satz:
Hat n keine mehrfachen Primfaktoren, so ist (T_n, ggT, kgV) eine Boolsche Algebra.
Beweis. Es gilt natürlich in (T_n, ggT, kgV):
i) Es gibt ein Nullelement: $\mathrm{ggT}(a, n) = a$.
ii) Es gibt ein Einselement: $\mathrm{kgV}(a, 1) = a$.
Es gilt $\mathrm{ggT}(a, \tilde{a}) = 1 \Leftrightarrow \min(w_p(a), w_p(\tilde{a})) = 0 \Rightarrow w_p(a) = 0 \vee w_p(\tilde{a}) = 0$ und analog $\mathrm{kgV}(a, \tilde{a}) = n \Leftrightarrow \max(w_p(a), w_p(\tilde{a}) = w_p(n)) \Rightarrow w_p(a) + w_p(\tilde{a}) = w_p(n)$.

1.5 Primzahlverteilung

1.5.1 Es gibt unendlich viele Primzahlen!

Definition. $\boxed{\pi(x) := |\{p : p \in \mathbb{P} \wedge p \leq x\}|}$

Satz 1 EUKLID:
Es gibt unendlich viele Primzahlen.

Nun:
1. Beweis (EUKLID). Gäbe es nur endlich viele dieser Lümmel, so könnte man sie in einer endlichen Menge P sammeln: sagen wir mal $P = \{p_1, p_2, ..., p_n\}$. Dann wäre aber $p := \prod_{i=1}^{n} p_i + 1$ durch keinen dieser Lümmel teilbar. So aber geht's nicht!! □

2. Beweis. $\forall n \in \mathbb{N}\ \exists p \in \mathbb{P} : p|(n! + 1) \wedge p > n.$ □

3. Beweis (LEULER). $\sum_{p\in\mathbb{P}} \frac{1}{p}$ divergiert: Wegen $\log\left(\frac{1}{1-x}\right) = \sum_{i=1}^{\infty} x^i$ für $|x| < 1$ gilt:
$\log\zeta(s) - \sum_{p\in\mathbb{P}} \frac{1}{p^s} = \log\prod_{p} \in \mathbb{P}\frac{1}{1-\frac{1}{p^s}} - \sum_{p\in\mathbb{P}} \frac{1}{p^s} = \sum_{p\in\mathbb{P}} \sum_{k=2}^{\infty} \frac{1}{k}\left(\frac{1}{p^s}\right)^k = \sum_{p\in\mathbb{P}} \frac{1}{2}\left(\frac{1}{p^s}\right)^2 \sum_{k=0}^{\infty} \frac{2}{k+2}\left(\frac{1}{p^s}\right)^k$
$< \sum_{p\in\mathbb{P}} \frac{1}{2}\left(\frac{1}{p^s}\right)^2 \sum_{k=0}^{\infty} \left(\frac{1}{p^s}\right)^k = \sum_{p\in\mathbb{P}} \frac{1}{2}\left(\frac{1}{p^s}\right)^2 \frac{1}{\frac{1}{1-\frac{1}{p^s}}} = \frac{1}{2}\sum_{p\in\mathbb{P}} \frac{1}{p^s(p^s-1)} \leq \frac{1}{2}\sum_{n=2}^{\infty} \frac{1}{n(n-1)} = \frac{1}{2}.$
Weil $\zeta(s)$ für $s \to 1$ unbeschränkt wächst, gilt dasselbe für $\sum_{p\in\mathbb{P}} \frac{1}{p^s}$,
also divergiert $\sum_{p\in\mathbb{P}} \frac{1}{p}$. □

4. Beweis (LEULER). Es ist: $\frac{1}{1-\frac{1}{p}} = \sum_{n=0}^{\infty} \left(\frac{1}{p}\right)^n$ Also: $\prod_{p\in\mathbb{P}} \frac{1}{1-\frac{1}{p}} = \prod_{p\in\mathbb{P}} \left(\sum_{n=0}^{\infty} \left(\frac{1}{p}\right)^n\right) =$
$\prod_{p\in\mathbb{P}} \left(1 + \frac{1}{p} + \frac{1}{p^2} + ...\right) = \sum_{i=1}^{\infty} \frac{1}{n} > \infty$ □

5. Beweis. Für die n-te Primzahl gilt: $p_n \leq 2^{2^{n-1}}$.
$\forall x \in \mathbb{N}\ \exists n \in \mathbb{N} : 2^{2^{n-1}} \leq x < 2^{2^n} \Rightarrow \ln\ln x < \ln(2^n \cdot \ln 2) = \ln\ln 2 + n \cdot \ln 2 \Rightarrow$
$\frac{\ln\ln x}{\ln 2} < n = \pi(p_n) \leq \pi(2^{2^{n-1}}) < \pi(x)$. Ergo gilt mit $\pi(x) > \frac{\ln\ln x}{\ln 2}$ auch:
$\lim_{x\to\infty} \pi(x) > \infty = \lim_{x\to\infty} \frac{\ln\ln x}{\ln 2}$. □

6. Beweis (ERIC WYNALDA). Für alle natürlichen n und m sind $2^{2^n} + 1$ und $2^{2^m} + 1$ teilerfremd:
Sagen wir mal, es sei $n < m$, d. h. $m = n + k$ mit k aus $\mathbb{N}$. Dann wird $2^{2^{n+k}} - 1$ von $2^{2^n} + 1$ geteilt, da aus $2^{2^{n+1}} - 1 = (2^{2^n} + 1) \cdot (2^{2^n} - 1)$ sofort $2^{2^{n+k}} - 1 = (2^{2^{n+k-1}} + 1) \cdot (2^{2^{n+k-1}} - 1) = (2^{2^{n+k-1}} + 1) \cdot (2^{2^{n+k-2}} + 1) \cdot (2^{2^{n+k-2}} - 1) = ... = (2^{2^{n+k-1}} + 1) \cdot (2^{2^{n+k-2}} + 1) \cdot ... \cdot (2^{2^{n+1}} + 1) \cdot (2^{2^n} + 1) \cdot (2^{2^n} - 1)$ folgt. Wenn aber $2^{2^{n+k}} - 1$ von $2^{2^n} + 1$ geteilt wird, dann können $2^{2^{n+k}} + 1$ und $2^{2^n} + 1$ höchstens 2 als

gemeinsamen Teiler besitzen. Da $2^{2^{n+k}}+1$ und $2^{2^n}+1$ indes 2 offensichtlich nicht als Teiler besitzen, sind $2^{2^{n+k}}+1$ und $2^{2^n}+1$ teilerfremd. Mithin kann man unendlich viele verschiedene Zahlen der Form $2^{2^n}+1, n \in \mathbb{N}$, bilden, die paarweise teilerfremd sind, die also sämtlichst verschiedene Primteiler besitzen. Und gerade dies macht die Behauptung des Satzes trivial. □

7. Beweis. $\prod_{p\in\mathbb{P}} \frac{1}{1-\frac{1}{p^2}} = \sum_{i=1}^{\infty} \frac{1}{n^2} = \zeta(2) = \frac{\pi^2}{6} \notin \mathbb{Q}$

Ach ja:
Hier habe ich frech die Kenntnis zweier Trivialitäten vorausgesetzt: $\zeta(2) = \frac{\pi^2}{6}$ und $\pi^2 \notin \mathbb{Q}$.
Nun:
Die eine Sache: Natürlich ist $\zeta(2) = \frac{\pi^2}{6}$...
Es ist nämlich:
$\pi\cot(\pi z) - \frac{1}{z} = \sum_{m=1}^{\infty} \frac{2z}{z^2-m^2} = -2z \sum_{m=1}^{\infty} \frac{1}{m^2} \frac{1}{1-\frac{z^2}{m^2}} = -2z \sum_{m=1}^{\infty} \frac{1}{m^2} \sum_{n=0}^{\infty} \left(\frac{z^2}{m^2}\right)^n =$
$-2z \sum_{m=1}^{\infty}\sum_{n=1}^{\infty} \frac{z^{2n-2}}{m^{2n}} = -2 \sum_{n=1}^{\infty} z^{2n-1} \sum_{m=1}^{\infty} \frac{1}{m^{2n}} = -2 \sum_{n=1}^{\infty} z^{2n-1}\zeta(2n)$ (*). Und man definiert:
$\frac{z}{e^z-1} =: g(z) =: \sum_{k=0}^{\infty} B_k \frac{z^k}{k!}$. Die B_k werden die **Bernoullischen Zahlen** genannt; man berechnet sie mittels Potenzreihendivision aus der obigen Gleichung. Es ist: $B_0 = 1, B_1 = -\frac{1}{2}, B_2 = \frac{1}{6}, B_3 = 0, B_4 = -\frac{1}{30}, B_5 = 0, ...$; es gilt stets: $B_{2k+1} = 0$ für $k \in \{1, 2, 3, ...\}$.
Und es ist:
$\pi\cot(\pi z) = i\,\pi\,\frac{e^{i\pi z}+e^{-i\pi z}}{e^{i\pi z}-e^{-i\pi z}} = i\,\pi\left(1+\frac{2}{e^{2\pi i z}-1}\right) = i\,\pi + \frac{1}{z}g(2\pi i z) = i\,\pi + \frac{1}{z}\sum_{k=0}^{\infty} B_k \frac{(2\pi i z)^k}{k!} =$
$i\pi + \frac{1}{z}\sum_{k=0}^{\infty} B_{2k+1}\frac{(2\pi i z)^{2k+1}}{(2k+1)!} + \frac{1}{z}\sum_{k=0}^{\infty} B_{2k}\frac{(2\pi i z)^{2k}}{(2k)!} = i\pi + \frac{1}{z}B_1\frac{(2\pi i z)}{1!} + \frac{1}{z}\sum_{k=0}^{\infty}(-1)^k B_{2k}\frac{(2\pi z)^{2k}}{(2k)!} =$
$i\pi + \frac{1}{z}\frac{-1}{2}(2\pi i z) + \frac{1}{z}\sum_{k=0}^{\infty} B_{2k}\frac{(2\pi i z)^{2k}}{(2k)!} = \frac{1}{z}\sum_{k=0}^{\infty}(-1)^k B_{2k}\frac{(2\pi z)^{2k}}{(2k)!} = \frac{1}{z} + \sum_{k=1}^{\infty}(-1)^k B_{2k}\frac{(2\pi)^{2k} z^{2k-1}}{(2k)!}$,
also:
$\pi\cot(\pi z) - \frac{1}{z} = \sum_{k=1}^{\infty}(-1)^k B_{2k}\frac{(2\pi)^{2k} z^{2k-1}}{(2k)!}$. (**)
Aus (*) und (**) erhält man durch Koeffizientenvergleich: $-2\zeta(2k) = (-1)^k B_{2k}\frac{(2\pi)^{2k}}{(2k)!}$.
Im Falle $k = 1$ folgt daher: $-2\zeta(2) = (-1)B_2\frac{(2\pi)^2}{(2)!} = (-1)\frac{1}{6}2\pi^2 \Leftrightarrow \boxed{\zeta(2) = \frac{\pi^2}{6}.}$
Die andere Sache: Zu glauben, es gäbe natürliche a, b mit $\pi^2 = \frac{a}{b}$, ist Quatsch!
(i) Es sei $p_n(x) := \frac{1}{n!}x^n(1-x)^n$ $n \geq 1$. Dann ist:
(+) $0 < p_n(x) < 1$ für $0 < x < 1$ (triv.) und (++) $p_n^{(k)}(0), p_n^{(k)}(1) \in \mathbb{Z}$ für $k \in \mathbb{N}_0$ (vollst. Ind.).
(ii) Es sei $P_n(x) := b^n \cdot \left(\sum_{i=0}^{n}(-1)^n \pi^{2n-2i} p_n^{2i}(x)\right)$ mit $b \in \mathbb{R}$. Dann ist:
(*) $\frac{\partial}{\partial x}(P_n'(x)\sin(\pi x) - \pi P_n(x)\cos(\pi x)) = P_n''(x) + \pi^2 P_n(x) = b^n\pi^{2n+2}p_n(x)\sin(\pi x)$.
(iii) Es sei $\pi^2 \in \mathbb{Q}$, d. h. (#) $\pi^2 = \frac{a}{b}$ mit natürlichen a, b. Daraus muß nun Quatsch abgeleitet werden.
Mit diesem Hintergedanken stellt man fest, daß wegen (++) und (#) gilt: $P_n(0)$ und $P_n(1)$ sind *mit diesem* b ganze Zahlen. Zudem lehrt uns (#), daß $b^n\pi^{2n+2} = a^n\pi^2$.

(iv) $a^n\pi \int_0^1 p_n(x)\sin(\pi x)dx \overset{(*)}{=} [\pi^{-1}P_n'(x) - P_n(x)\cos(\pi x)]_0^1 = P_n(0) + P_n(1) \in \mathbb{Z}$.

(v) Aus $(+)$ und $0 < \sin(\pi x) \leq 1$ für $0 < x < 1$ folgt:

$0 < a^n\pi \int_0^1 p_n(x)\sin(\pi x)dx \leq \pi\frac{a^n}{n!} < 1$ für große n.

(iv) und (v) zusammen ergeben den erhofften Quatsch; also ist $\boxed{\pi^2 \notin \mathbb{Q}.}$ □

1.5.2 Lücken

Definition. Sind sowohl p als auch $p+2$ Primzahlen, so nennt man sie Primzahlzwillinge.
Sind $p, p+2$ und $p+6$ oder $p, p+4$ und $p+6$ Primzahlen, so nennt man sie Primzahldrillinge.

$\boxed{n, m \text{ Primzahlzwillinge} :\Leftrightarrow n, m \in \mathbb{P} \wedge |n-m| = 2}$

$\boxed{l, n, m \text{ Primzahldrillinge} :\Leftrightarrow l, n, m \in \mathbb{P} \wedge \max\{|l-n|, |n-m|, |m-l|\} = 6}$

Ungewißheit:
Natürlich gibt es allerhand Primzahlzwillinge, -drillinge und -vierlinge, aber keiner weiß, wieviele.

Satz 2:
In der Folge der Primzahlen gibt es beliebig große Lücken.
Beweis. Unter den $n-1$ Zahlen $n!+2, n!+3, ..., n!+n$ ist keine Primzahl, da $k|n!+k$ für $k = 2, 3, ..., n$. □

Satz 3 (Dirichlet):
In jeder arithmetischen Progression $(a + k \cdot m)_{k\in\mathbb{N}}$ mit $\text{ggT}(a, m) = 1$ gibt es unendlich viele Primzahlen. (Das muß man auch ohne Beweis glauben.)

Satz 4:
Es gibt kein Polynom über $\mathbb{Z}$, welches nur Primzahlen liefert.
Beweis. Sei $y = f(x) = \sum_{i=0}^{n} a_i x^i, n > 0, a_n > 0$ (o.B.d.A!!!), $a_i \in \mathbb{Z}$ für $i = 0, 1, ..., n$.
(i) Für genügend großes x_0 ist $y_0 = f(x_0) > 1$:
Sei $x_0 > 4 \cdot \max\{|a_i|\}$ (*). Dann ist:
$f(x_0) = \sum_{i=0}^{n} a_i x_0^i \geq a_n x_0^n - \sum_{i=0}^{n-1} |a_i| x^i \overset{(*)}{>} a_n x_0^n - \frac{x_0}{4} \sum_{i=0}^{n-1} x^i = a_n x_0^n - \frac{x_0}{4} \frac{x_0^n - 1}{x_0 - 1} >$
$a_n x_0^n - \frac{1}{2}(x_0^n - 1) > a_n \frac{x_0^n}{2} > 1$.
(ii) Es sei $x_1 = x_0 + y_0^2$. Dann ist:
$y_1 = f(x_1) = f(x_0 + y_0^2) = \sum_{i=0}^{n} a_i (x_0 + y_0^2)^i = f(x_0) + y_0^2 \cdot g(x_0, y_0) =$
$y_0 \cdot (1 + y_0 \cdot g(x_0, y_0)) =: y_0 \cdot q_1$.
Also: $y_1 = f(x_1) = y_0 \cdot q_1$ und $y_0 = f(x_0) > 1$. Hm. Wenn $q_1 > 1$, ist ein kleiner Orgasmus fällig!
(iii) Es gilt: $x_1 = x_0 + y_0^2 > 4 \cdot \max\{|a_i|\}$. Daher ist:
$y_1 \overset{(s.o.)}{>} a_n \frac{x_1^n}{2} \overset{(x_1 = x_0 + y_0^2)}{>} a_n \frac{y_0^n}{2} \overset{(y_0 > 1)}{>} y_0$.
Also: $q_1 > 1$. ($\rightarrow$ Orgasmus!)
Alles zusammen macht uns klar: $f(x_1) \notin \mathbb{P}$!!! □

2 Zahlentheoretische Funktionen

2.1 Allgemeines. τ, σ und σ_k

Definition. Sei $n = \prod_{p\in\mathbb{P}} p_i^{\alpha_i}$. Dann ist $\boxed{\omega_p(n) := \begin{cases} 0, \text{ wenn } p\nmid n \\ \alpha_i, \text{ wenn } p|n \end{cases}}$

Definition. Eine zahlentheoretische Funktion ist eine Abbildung von $\mathbb{N}$ nach $\mathbb{R}$ (bzw. $\mathbb{C}$).
$\boxed{f : \mathbb{N} \to \mathbb{C} \text{ heißt zahlentheoretische Funktion}}$

Definition. $\boxed{\tau(n) := |T_n|}$

Satz 1:
Ganz allgemein gilt: $\tau(n) = \prod_{p\in\mathbb{P}} (\omega_p(n) + 1)$.

Beweis. Für $n = \prod_{p\in\mathbb{P}} p^{\omega_p(n)}$ gilt: $t|n \Leftrightarrow t = \prod_{p\in\mathbb{P}} p^{\omega_p(t)}$ mit $\omega_p(n) \geq \omega_p(t)$. □

Folgerung:
$\text{ggT}(a,b) = 1 \Rightarrow \tau(a\cdot b) = \tau(a)\cdot\tau(b) \Rightarrow$
$|T_{ab}| = |T_a|\cdot|T_b|$ und $T_a \cap T_b = \{1\} \Rightarrow$
$(\text{ggT}(a,b) = 1 \Rightarrow \forall t \in T_{ab} \dot{\exists} u \in T_a \dot{\exists} v \in T_b : t = uv)$.

Definition. $\boxed{\sigma(n) := \sum_{t|n} t}$

Satz 2:
$\text{ggT}(a,b) = 1 \Rightarrow \sigma(a\cdot b) = \sigma(a)\cdot\sigma(b)$
Beweis. $\text{ggT}(a,b) = 1 \Rightarrow \forall t \in T_{ab} \dot{\exists} u \in T_a \dot{\exists} v \in T_b : t = uv$. Also:
$\sum_{t|ab} t = \sum_{u|a}\sum_{v|b} uv = \left(\sum_{u|a} u\right)\left(\sum_{v|b} v\right)$. □

Satz 3:
Man spricht die Wahrheit, wenn man sagt: $\sigma(n) = \prod_{p\in\mathbb{P}} \frac{p^{\omega_p(n)+1}-1}{p-1}$.

Beweis. $\sigma(p^\alpha) = \sum_{i=0}^{\alpha} p^i = \frac{p^{\alpha+1}-1}{p-1}$ □

Definition. Eine zahlentheoretische Funktion f, für die $f(a \cdot b) = f(a) \cdot f(b)$ gilt, falls a, b relativ prim sind, heißt **multipikativ.**

$$\boxed{f \text{ multiplikativ} :\Leftrightarrow [\text{ggT}(a,b) = 1 \Rightarrow f(a \cdot b) = f(a) \cdot f(b)]}$$

Satz 4:
Wenn f eine multiplikative zahlentheoretische Funktion ist, dann gilt:
(i) $f(1) = 1$, falls $f \not\equiv 0$,
(ii) $f(n) = f(\prod_{p \in \mathbb{P}} p^{\omega_p(n)}) = \prod_{p \in \mathbb{P}} f(p^{\omega_p(n)})$, und
(iii) τ und σ sind multiplikativ.

Beweis. (i): Es ist: $\text{ggT}(n, 1) = 1 \Rightarrow f(n) = f(n \cdot 1) = f(n) \cdot f(1)$. □
(ii): Das ist nicht mehr als die Definition der Multiplikativität zahlentheoretischer Funktionen. Mit anderen Worten: VÖLLIG TRIVIAL!!
(iii) Siehe oben.

Definition. $\boxed{\sigma_k(n) := \sum_{t|n} t^k}$

Bemerkung. Es sind $\sigma_0 = \tau$ und $\sigma_1 = \sigma$.

Definition. Sei f eine zahlentheoretische Funktion. Dann heißt $F(n) := \sum_{t|n} f(t)$ **Summatorfunktion** oder **summatorische Funktion von f.**

$$\boxed{F \text{ Summatorfunktion von } f \ :\Leftrightarrow F(n) = \sum_{t|n} f(t)}$$

Satz 5:
Wenn f multiplikativ ist, dann auch F.

Beweis: Es sei $n = n_1 \cdot n_2$ und $\text{ggT}(n_1, n_2) = 1$. Dann ist:
$\sum_{t|n_1 n_2} f(t) = \sum_{t_1|n_1, t_2|n_2} f(t_1 t_2)$, denn einerseits folgt aus der Eindeutigkeit der Primfaktorzerlegung von n, daß sich jeder Teiler t von n schreiben läßt als $t = t_1 t_2$ mit *eindeutig bestimmten* $t_1|n_1$ und $t_2|n_2$; andererseits ergibt jedes Paar t_1, t_2 mit $t_1|n_1$ und $t_2|n_2$ ein $t = t_1 t_2$ mit $t|n$.
Daher ist: $F(n) = F(n_1 n_2) = \sum_{t|n_1 n_2} f(t) = \sum_{t_1|n_1, t_2|n_2} f(t_1 t_2) = \sum_{t_1|n_1} \sum_{t_2|n_2} f(t_1 t_2) =$

$$\sum_{t_1|n_1} \sum_{t_2|n_2} f(t_1) f(t_2) = \left(\sum_{t_1|n_1} f(t_1) \right) \cdot \left(\sum_{t_2|n_2} f(t_2) \right) = F(n_1) F(n_2). \qquad \square$$

Folgerung:
σ_k ist multiplikativ.
Beweis: Betrachte $\sigma_k(n) = \sum_{t|n} t^k$ als Summatorfunktion von n^k. □

Folgerung aus der Folgerung:
$\sigma_k(n) = \prod_{i=1}^{\infty} \frac{p_i^{k(\alpha_i+1)}-1}{p_i^k-1}$, falls $k > 0$ und $n = \prod_{i=1}^{r} p_i^{\alpha_i}$.
Beweis: $\sigma_k(p^\alpha) = \sum_{i=0}^{\alpha} p^{ik} = \frac{p^{k(\alpha+1)}-1}{p^k-1}$. □

Satz 6:
Zu jeder zahlentheoretischen Funktion $F(n)$ gibt es genau eine Funktion $f(n)$ derart, daß $F(n)$ die summatorische Funktion von $f(n)$ ist.
Beweis: Vollständige Induktion nach n.

Satz 7:
(i) Ist $F(n)$ multiplikativ, so auch $f(n)$,
und mit $n = \prod p^\alpha$ und $F(n) = \sum_{t|n} f(t)$ gilt:
(ii) $f(n) = \prod_p (F(p^\alpha) - F(p^{\alpha-1}))$.
Beweis: Aus $F(p^\alpha) = f(1) + f(p) + ... + f(p^\alpha)$ folgt: $f(p^\alpha) = F(p^\alpha) - F(p^{\alpha-1})$. Für den Spezialfall $n = p^\alpha$ stimmt dann die Funktion

$$h(n) := \prod_p (F(p^\alpha) - F(p^{\alpha-1})), \text{ wenn } n = \prod p^\alpha,$$

mit $f(n)$ überein. Mit $h(n)$ ist auch die summatorische Funktion $H(n)$ multiplikativ, und wegen $h(p^\alpha) = f(p^\alpha)$ gilt $H(p^\alpha) = F(p^\alpha)$. Da beide Funktionen distributiv sind, folgt $H(n) = F(n)$, also auch $h(n) = f(n)$. □

2.2 Vollkommen?

Definition. Eine Zahl $n \in \mathbb{N}$ heißt **vollkommen**, wenn gilt: $\sigma(n) = 2n$.
Bemerkung: Die Bestimmung *aller* vollkommener Zahlen ist noch heute ein ungelöstes Problem. Man hat bisher noch keine *ungeraden* vollkommene Zahlen gefunden (man weiß: die kleinste ist $> 10^{50}$). Die *geraden* vollkommenen Zahlen lassen sich jedoch vollständig angeben. Um dies zu tun, bemerkt man, daß sich jede gerade Zahl n schreiben läßt als $n = 2^{s-1} \cdot b$, wobei $s \geq 2$ und b ungerade ist.

Satz 1 (Charakterisierung der geraden vollkommenen Zahlen):
Sei $n = 2^{s-1} \cdot b, s \geq 2$ und b ungerade, dann gilt:

$$b \in \mathbb{P} \ \wedge \ b = 2^s - 1 \Leftrightarrow n \text{ ist vollkommen}$$

Beweis. "$\Rightarrow$" $b \neq 2 \in \mathbb{P} \Rightarrow n = 2^{s-1} \cdot b$ ist PFZ von n. $\sigma(n) = \frac{2^s-1}{2-1}\frac{b^2-1}{b-1} = (2^s-1)(b+1)$. $b+1 = 2^s = 2 \cdot 2^{s-1} \Rightarrow \sigma(n) = (2^s-1)2 \cdot 2^{s-1} = 2n$.
"$\Leftarrow$" $n = 2^{s-1} \cdot b$, da b ungerade, sind alle PF von $b > 2$. $2^s b = 2n = \sigma(n) = \sigma(2^{s-1}) \cdot \sigma(b) = (2^s-1)\sigma(b) \Rightarrow \sigma(b) = \frac{2^s b}{2^s-1} = b + c$, mit $c := \frac{b}{2^s-1} > 0$. $\sigma(b) \in \mathbb{N} \ \wedge \ b \in \mathbb{N} \Rightarrow c \in \mathbb{N}$. $b = c(2^s-1) \Rightarrow c|b$. $\sigma(b) = b + c \Rightarrow c, b$ sind einzige Teiler von b. $b = (2^s-1)c \geq 3$ (wegen $s \geq 2, c \geq 1$) $\Rightarrow \in \mathbb{P} \Rightarrow c = 1 \Rightarrow b = 2^s - 1 \in \mathbb{P}$ $\square$

Definition. $n \in \mathbb{N}$ heißt **defizient**, wenn gilt: $\sigma(n) < 2n$.
$n \in \mathbb{N}$ heißt **abundant**, wenn gilt: $\sigma(n) > 2n$.

Satz 2 (Beispiele):
Für prime p und q gilt:
(i) $n = p^r$ ist defizient.
(ii) $6 \neq n = p \cdot q$ ist defizient.
(iii) $n = p^r \cdot q^s$ ist defizient.
(iv) 12, 18, 20, 24, 30 sind abundant.
(v) Jedes Vielfache einer abundanten Zahl ist abundant.
(vi) Jedes echte Vielfache einer vollkommenen Zahl ist abundant.

Beweis. (i) $\sigma(n) = \sigma(p^r) = \sum_{i=0}^{r} p^i = \sum_{i=0}^{r-1} p^i + p^r = p^r + \frac{p^r-1}{p-1} = n + \frac{n-1}{p-1} < n + \frac{n}{p-1} \leq n + n = 2n$
(ii) $\sigma(pq) = \sigma(p)\sigma(q) = (p+1)(q+1) = pq + p + q + 1 < pq + pq = 2pq$ für $pq \neq 6$.
(iii) z.z.: $\sigma(p^r q^s) < 2p^r q^s$ Betrachte $\frac{\sigma(p^r q^s)}{p^r q^s} = \frac{\sigma(p^r)}{p^r}\frac{\sigma(q^s)}{q^s} = \frac{p^{r+1}-1}{(p-1)p^r}\frac{q^{s+1}-1}{(q-1)q^s} < \frac{p}{p-1}\frac{q}{q-1} \leq \frac{3}{2}\frac{5}{4} < 2$.
(iv) Popechnen.
(v) $\sigma(n) > 2n \Rightarrow \sigma(kn) \geq \sum_{d|n} kd = k \cdot \sigma(n) > k \cdot 2n = 2 \cdot kn$.
(vi) $\sigma(n) = 2n \ \wedge \ k \geq 2 \Rightarrow \sigma(kn) \geq 1 + \sum_{d|n} kd = 1 + k \cdot \sigma(n) = 1 + k \cdot 2n > 2 \cdot kn$. $\square$

2.3 Mersennesche Primzahlen

Durch die Charakterisierung der geraden vollkommenen Zahlen wird die Frage aufgeworfen: Für welche s ist $2^s - 1$ eine Primzahl? Man definiert:

Definition. Es sei $M_s := 2^s - 1$, für $s \in \mathbb{N}$.
Falls M_s prim ist, heißt M_s **Mersennesche Primzahl**.

Historische Notiz. Marin Mersenne lebte von 1588 bis 1648, war also Zeitgenosse von Rene Descartes.

Satz 1:
$M_s = 2^s - 1$ ist höchstens dann eine Primzahl, wenn s prim ist.
Beweis. Es sei $\mathbb{P} \ni 2^s - 1 \wedge s = uv$, mit $u > 1, v > 1$. Dann gilt $2^s - 1 = (2^u)^v - 1 = (2^u - 1) \sum_{i=0}^{v-1} (2^u)^i$, beide Faktoren rechts sind > 1, da schlägt dann wohl der Blitz ein. □

Bemerkung: Bis heute sind nur 30 Mersennesche Primzahlen bekannt, und zwar für die folgenden Werte von p: 2, 3, 5, 7, 13, 19, 31,..., 86243, 132049, 216091. Zur Zeit sind M_{86243}, M_{132049} und M_{216091} die drei größten bekannten Primzahlen überhaupt.

2.4 Fermatsche Primzahlen

Geschichtliche Belehrung. Pierre de Fermat (1601 - 1665) lebte als höherer Verwaltungsbeamter („königlicher Parlamentsrat“) in Toulouse („At two to two two to Toulouse“). Er gilt als Vater der neuzeitlichen Zahlentheorie, obwohl seine mathematische Arbeit größtenteils nur in Briefen an seine Zeitgenossen (u. a. Descartes, Mersenne, Pascal) enthalten ist. Diophants *Arithmetica* regte Fermat zu interessanten zahlentheoretischen Überlegungen an. Auf dem Rand des Buches notierte er, daß er die Unlösbarkeit der Gleichung $x^n + y^n = z^n$ für $n \geq 3$ in ganzen Zahlen beweisen könne, der Rand des Buches aber zu wenig Platz biete. Bei der Suche nach dem Beweis haben sich großartige mathematische Theorien entwickelt. Inzwischen ist der Beweis der „Fermatschen Vermutung“ aber gefunden.

Satz 1:
$2^s + 1$ ist höchstens dann eine Primzahl, wenn s eine 2er-Potenz ist.
Beweis. Es sei $s = kv$ mit $k = 2^t, t \in \mathbb{N}$, und $v \in \mathbb{N}$ ungerade. Wegen $(-1^v) = -1$ ist dann: $1 + 2^s = 1 - (-2^k)^v$. Die endliche geometrische Reihe liefert: $1 + 2^s = (1 + 2^k)(1 - 2^k + 2^{2k} - 2^{3k} + -... + 2^{(v-1)k})$. Ist $v > 1$, so gilt $k < s$ und damit $1 < 1 + 2^k < 1 + 2^s$. Dann stehen rechts zwei Faktoren > 1, man hat eine echte Zerlegung von $2^s + 1$. Also muß notwendig $v = 1$ sein, d.h. s muß eine Zweierpotenz sein. □

Definition. Die Zahlen $F_n := 2^{2^n} + 1$ für $n \in \mathbb{N}$ heißen **Fermatsche Zahlen**.

Bemerkung: 1. Man kennt nur 5 Fermatsche Primzahlen, nämlich 3, 5, 17, 257 und 65537. Man weiß, daß die Fermatschen Zahlen F_n für $n \leq 21$ zusammengesetzt sind, F_{22}, F_{24} und F_{28} sind die drei kleinsten solchen Zahlen, von denen man noch nicht weiß, ob sie sie prim sind. Nur F_5, F_6, F_7 und F_8 sind heute vollständig faktorisiert, von der zusammengesetzten Zahl F_{14} kennt man noch nicht mal einen Faktor.
2. Die Fermatsche Primzahlen spielen eine wichtige Rolle in der Theorie der Kreisteilung: Gauß hat bewiesen: Es sei $m \geq 3$ eine ungerade natürliche Zahl. Dann ist das reguläre m-Eck genau dann mit Zirkel und Lineal konstruierbar, wenn m ein quadratfreies Produkt Fermatscher Primzahlen ist. Die größte bisher bekannte Zahl m ist (natürlich) $3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537 = 2^{32} - 1$.

2.5 Echte Freunde

Definition. Zwei natrliche Zahlen a und b nennt man befreundet, wenn $\sigma(a) = a + b = \sigma(b)$.
$\boxed{\sigma(a) = a + b = \sigma(b)}$

Satz 1:
Sind a und b befreundet, so gilt die merkwürdige Beziehung:

$$\Big(\sum_{t|a,t>1} \frac{1}{t}\Big) \cdot \Big(\sum_{t|b,t>1} \frac{1}{t}\Big) = 1.$$

Beweis. $\Big(\sum_{t|a,t>1} \frac{1}{t}\Big) \cdot \Big(\sum_{t|b,t>1} \frac{1}{t}\Big) = \Big(\sum_{t|a,t<a} t\Big) \cdot \Big(\sum_{t|b,t<b} t\Big) = \frac{\sigma(a)-a}{a} \cdot \frac{\sigma(b)-b}{b} = \frac{b}{a} \cdot \frac{a}{b} = 1.$

Bemerkung. Das kleinste Paar befreundeter Zahlen ist (220,284); dieses Paar kannten schon Pythagoras und Aristoteles.

Satz 2 (Thabit, $\sim$ 9. Jahrhundert n. Chr.):
Sind für $n > 1$ die Zahlen

$$u = 3 \cdot 2^{n-1} - 1, \quad v = 3 \cdot 2^n - 1 \text{ und } w = 9 \cdot 2^{2n-1} - 1$$

Primzahlen, dann sind die Zahlen

$$a = 2^n \cdot u \cdot v \text{ und } b = 2^n \cdot w$$

befreundet.
Beweis. Es gilt $(1 + u) \cdot (1 + v) = 1 + w$. Sind nun u, v und w Primzahlen, so ist:
$\sigma(a) = \sigma(2^n) \cdot \sigma(u) \cdot \sigma(v) = (2^{n+1} - 1) \cdot (u + 1) \cdot (v + 1) = (2^{n+1} - 1) \cdot 9 \cdot 2^{2n-1}$,
$\sigma(b) = \sigma(2^n) \cdot \sigma(w) = (2^{n+1} - 1) \cdot (w + 1) = (2^{n+1} - 1) \cdot 9 \cdot 2^{2n-1}$,
$a + b = 2^n \cdot (uv + w) = 2^n \cdot (9 \cdot 2^{2n-1} - 3 \cdot 2^{n-1} - 3 \cdot 2^n + 1 + 9 \cdot 2^{2n-1} - 1) =$
$2^n \cdot (9 \cdot 2^{2n} - 9 \cdot 2^{n-1}) = (2^{n+1} - 1) \cdot 9 \cdot 2^{2n-1}$ $\square$

2.6 Die DIRICHLET-Faltung

Definition. Sind α und β zahlentheoretische Funktionen, so heißt die durch

$$(\alpha \star \beta)(n) := \sum_{t|n} \alpha(t)\beta\Big(\frac{n}{t}\Big)$$

erklärte zahlentheoretische Funktion $\alpha\star\beta$ die **DIRICHLET-Faltung (oder DIRICHLET-Produkt) von α und β.**

$$\boxed{(\alpha \star \beta)(n) = \sum_{t|n} \alpha(t)\beta\Big(\tfrac{n}{t}\Big)}$$

Satz 1:
Es seien α, β und γ zahlentheoretische Funktionen. Dann gilt:

(i) $\alpha \star \beta = \beta \star \alpha$ (Kommutativität)
(ii) $(\alpha \star \beta) \star \gamma = \alpha \star (\beta \star \gamma)$ (Assoziativität)
(iii) Für $\boxed{\varepsilon(n) = \begin{cases} 1 \text{ für } n=1 \\ 0 \text{ für } n>1 \end{cases}}$ gilt:
$\alpha \star \varepsilon = \alpha$ (neutrales Element).

Beweis. (i) Trivial.
(ii) Ausrechnen.
(iii) $\alpha \star \varepsilon(n) = \sum_{t|n} \alpha(t)\varepsilon\Big(\frac{n}{t}\Big) = \alpha(n) \cdot 1 = \alpha(n).$ □

Satz 2:
Die Menge der zahlentheoretischen Funktionen bilden einen kommutativen Ring bezüglich der gewöhnlichen Addition + und dem DIRICHLET-Produkt $\star$. Der Ring besitzt mit der durch

$$o(n) = 0 \quad \text{für alle } n \in \mathbb{N}$$

definierten Funktion o ein Null- und mit der Funktion ε ein Einselement.
Da man außerdem zeigen kann, daß der Ring nullteilerfrei ist, ist der Ring der zahlentheoretischen Funktionen sogar ein Integritätsring.
Genau die Elemente besitzen ein multiplikatives Inverses, für die $\alpha(1) \neq 0$ gilt.
Beweis. Rechnerische Kleinarbeit.

Satz 3:
Die multiplikativen zahlentheoretischen Funktionen bilden bezüglich der DIRICHLET-Faltung eine kommutative Gruppe.
Beweis. Wenn $\mathrm{ggT}(n_1, n_2) = 1$, dann gilt (vgl. Satz 2.1.5):

$$\sum_{t_1 t_2 = n_1 n_2} \alpha(t_1)\beta(t_2) = \sum_{\substack{t_{11}t_{21}=n_1 \\ t_{12}t_{22}=n_2}} \alpha(t_{11}t_{12})\beta(t_{21}t_{22}).$$

Da für multiplikative zahlentheoretische Funktionen außerdem stets $\alpha(1) = 1$ gilt, ist der Satz bewiesen: □

Definition. Die Funktionen ι und ν werden definiert durch:

$$\iota(n) = 1 \text{ für alle } n \in \mathbb{N} \quad \text{bzw.} \quad \nu(n) = n \text{ für alle } n \in \mathbb{N}.$$

$$\boxed{\iota(n) = 1 \; \forall n \in \mathbb{N} \text{ und } \nu(n) = n \; \forall n \in \mathbb{N}}$$

Satz 4:
Es gilt[1]:

$$\tau = \iota \star \iota, \quad \sigma = \nu \star \iota, \quad \nu = \varphi \star \iota.$$

Beweis. (i) $(\iota \star \iota)(n) = \sum_{t|n} \iota(t)\iota\left(\frac{n}{t}\right) = \sum_{t|n} 1 \cdot 1 = \tau(n)$.

(ii) $(\nu \star \iota)(n) = \sum_{t|n} \nu(t)\iota\left(\frac{n}{t}\right) = \sum_{t|n} t \cdot 1 = \sum_{t|n} t = \sigma(n)$.

(iii) $(\varphi \star \iota)(n) = \sum_{t|n} \varphi(t)\iota\left(\frac{n}{t}\right) = \sum_{t|n} \varphi(t) \cdot 1 = \sum_{t|n} \varphi(t) = n = \nu(n)$.

Definition. Für $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ mit $\alpha_i \neq 0$ wird die MÖBIUS-**Funktion** (nach AUGUST FERDINAND MÖBIUS, 1790 - 1868) definiert durch:

$$\mu(n) := \begin{cases} (-1)^r, \text{ falls } n \text{ quadratfrei ist} & (\text{d. h. } 1, \quad \text{falls } n = 1), \\ 0 \text{ falls } n \text{ nicht quadratfrei ist.} \end{cases}$$

Quadratfrei soll dabei bedeuten, daß keine Quadratzahl ($\neq 1$) n teilt.

Satz 5:
(i) μ ist multiplikativ, und
(ii) Es gilt: $\underline{\mu = \iota^{-1}}$.

Beweis. (i) Die Behauptung, daß $\mu(n) = \prod_{i=1}^{r} \mu(p_i^{\alpha_i})$, ist klar für $n = 1$, ist klar für $n \neq 1$ und quadratfrei, und sie ist klar für n nicht quadratfrei.
(ii) Wegen (i) genügt es zu zeigen, daß $((\mu \star \iota))(p^\alpha) = \varepsilon(p^\alpha)$:
$((\mu \star \iota))(p^\alpha) = \sum_{t|p^\alpha} \mu(t)\iota\left(\frac{n}{t}\right) = \sum_{t|p^\alpha} \mu(t) \cdot 1 = \sum_{i=0}^{\alpha} \mu(p^i) = 1 + (-1) = 0.$ □

Korrolar: Aus $\tau = \iota \star \iota$ folgt $\tau \star \mu = \iota$,
aus $\sigma = \nu \star \iota$ folgt $\sigma \star \mu = \nu$, und
aus $\nu = \varphi \star \iota$ folgt $\nu \star \mu = \varphi$.

[1]Die Erwähnung der EULERschen φ-Funktion an dieser Stelle ist ein Vorgriff. Definition und Eigenschaften finden sich an späterer Stelle. Zunächst einmel genügt es zu wissen, daß die summatorische Funftion der φ-Funktion die Funktion ν ist.

Bemerkung: Da die multiplikativen zahlentheoretischen Funktionen eine Gruppe bilden, folgt aus $\tau = \iota \star \iota, \sigma = \nu \star \iota$ und $\varphi = \nu \star \mu$ die Multiplikativität von τ, σ und φ.

Satz 6 (MÖBIUS scher Umkehrsatz):
Es gilt:

$$F(n) = \sum_{t|n} f(t) \Leftrightarrow f(n) = \sum_{t|n} F(t)\mu\Big(\frac{n}{t}\Big).$$

Beweis. Dieser Satz folgt vermöge

$$f \star \iota = F \Leftrightarrow f = F \star \mu$$

sofort aus dem vorangegangenen.

3 Der leckere Algebraten

3.1 Des Bratens Sprache & Elementares

Definition. Sei R ein Ring mit von 0 verschiedenem Einselement 1.
Ein Element a heißt **Einheit** von R, wenn es ein Element $b \in R$ gibt mit $ab = ba = 1$.
$\boxed{a \text{ Einheit} :\Leftrightarrow \exists b \in R : b = a^{-1}}$
Die Menge der Einheiten bezeichnet man mit R^* oder mit E.

Beispiele. $\mathbb{Z}^* = \{-1, 1\}; \mathbb{Z}[i]^* = \{1, i, -1, -i\}$.

Definition. Zwei Elemente $a, b \in R$, die sich nur um eine Einheit als Faktor unterscheiden, nennt man **assoziiert**. Dies bedeutet also, daß eine Einheit e existiert mit $a = e \cdot b$.

Lemma: $(E, \cdot)$ ist eine abelsche Gruppe.

Definition. Ein Element p von R heißt **Primelement** von R, wenn gilt:
(i) $a \neq 0 \ \wedge \ a \notin R^*$
(ii) $\forall a, b \in R : (p|ab \Rightarrow (p|a \vee p|b))$.

Definition. Ein Element p von R heißt **irreduzibel**, wenn gilt:
(i) $a \neq 0 \ \wedge \ a \notin R^*$
(ii) $\forall a, b \in R : (p = ab \Rightarrow (a \in R^* \vee p \in R^*))$.

Aufgemerkt! $2 \in \mathbb{Z}[\sqrt{-5}]$ ist irreduzibel, aber nicht prim. Es gilt aber der

Satz:
In Integritätsringen ist jedes Primelement irreduzibel.

Definition: Eine Untergruppe I der additiven Gruppe $(R, +)$ eines Ringes R heißt **Ideal**, wenn $RI \subset R$ ist.

Beispiele:
i) $\{0\}$ und R sind Ideale in R, die sogenannten trivialen Ideale.
ii) R kommutativ, $a \in R \Rightarrow Ra := \{xa | x \in R\}$ ist ein Ideal in R.
iii) I Ideal in $\mathbb{Z} \Leftrightarrow \exists m \in \mathbb{N} : I = m\mathbb{Z}$.

Bemerkung:
i) Jedes Ideal in R ist ein Unterring von R.
ii) $\bigcap_{I \in R} I$ ist ein Ideal.
iii) Enthält ein Ideal I in R eine Einheit, so ist $I = R$.

iv) Es gilt der Satz: In einem Hauptidealring R gilt: $d = \text{ggT}(a,b) \Leftrightarrow I(a,b) = I(d)$ und $d = ax + by$ mit $x, y \in R$.
Beweis. "$\Leftarrow$" $a \in I(d) \Rightarrow a = x \cdot d \Rightarrow d|a$ $b \in I(d) \Rightarrow b = y \cdot d \Rightarrow d|b$, also $d = \text{gT}(a,b)$. $d \in I(a,b) \Rightarrow d = ax + by$, aber wenn $t|a \vee t|b \Rightarrow t|d \Rightarrow d = \text{ggT}(a,b)$. "$\Rightarrow$" Jedes Ideal kann von einem Element erzeugt werden, wegen der Hinrichtung ist dies für a, b der ggT. □

3.2 Ringe aller Sorten

Definitionen.
$(R, +, \cdot)$ heißt **Halbring**, falls $(R, +)$ eine Halbgruppe ist, die Verknüpfung $\cdot$ assoziativ ist und die Distributivgesetze $a \cdot (b+c) = a \cdot b + a \cdot c$ und $(b+c) \cdot a = b \cdot a + c \cdot a$ gelten.
Beispiel: $\mathbb{N}$

Ein Halbring $(R, +, \cdot)$ heißt **Ring**, falls $(R, +)$ ein Gruppe ist.
Beispiel: $\mathbb{Z}$

Ein Ring $(R, +, \cdot)$ heißt **Integritätsring**, falls R nullteilerfrei, kommutativ und stolzer Besitzer eines (von 0 verschiedenen) Einselements ist.
Beispiel: $\mathbb{Z}$, $\mathbb{Z}[i]$, $\mathbb{Q}[X]$

Ein Ring $(R, +, \cdot)$ heißt **ZPE-Ring** oder **faktorieller Ring**, falls R ein Integritätsring ist und jedes Element eine Zerlegung in Primelemente besitzt.
Bemerkung: $(\mathbb{Z}[\sqrt{-5}], +, \cdot)$ ist *kein* ZPE-Ring, da z.B. die vier Teiler des Elements $6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$ keine Primelemente in $\mathbb{Z}[\sqrt{-5}]$ sind.

Ein Ring R heißt **euklidisch**, wenn in R eine Division mit Rest möglich ist. Jeder euklidische Ring ist ein ZPE-Ring.
Bemerkung: $\mathbb{Z}[X]$ ist ein ZPE-Ring, aber *kein* euklidischer Ring.

Ein Ring R heißt **noethersch**, wenn jedes Ideal in R eine endliche Basis besitzt.

Ein **Hauptidealring** R ist ein Ring, in dem jedes Ideal ein Hauptideal, also von einem Element erzeugt ist.

Ein Ring R heißt **dedekindsch** oder **ZPI-Ring**, wenn jedes Ideal in R eine Zerlegung in Primideale besitzt.

Wir werden einen speziellen Integritätsring im folgenden etwas genauer betrachten.

3.3 Die Sache mit $\mathbb{Z}[i]$

$\mathbb{Z}[i]$ ist ein Ring, seine Elemente lassen sich schreiben als $a + ib$ oder $\left(\begin{smallmatrix} a & -b \\ b & a \end{smallmatrix}\right)$.
Welche Zahlen sind prim in $\mathbb{Z}[i]$?
Zunächst erinnert man sich, daß ein Element n eines Ringes Primelement heißt, wenn gilt $n|a \cdot b \Longrightarrow n|a \vee n|b$.
Man könnte vermuten, daß die Primzahlen aus $\mathbb{N}$, kurz $\mathbb{P}_{\mathbb{N}}$, auch die Primelemente in $\mathbb{Z}[i]$, kurz $\mathbb{P}_{\mathbb{Z}[i]}$, sind also $p \in \mathbb{P}_{\mathbb{N}} \Leftrightarrow p \in \mathbb{P}_{\mathbb{Z}[i]}$ gilt.
Betrachten wir dazu die $2 \in \mathbb{P}_{\mathbb{N}}$:

$$2|(1+i)(1-i) = 2, \text{ aber } 2 \not|(1+i) \ \wedge \ 2 \not|(1-i),$$

d.h. 2 ist nicht prim in $\mathbb{Z}[i]$.
Wie überprüft man, ob für ein $p \in \mathbb{P}_{\mathbb{N}}$ auch $p \in \mathbb{P}_{\mathbb{Z}[i]}$ gilt?
Führe dazu folgende Norm ein: $N(\alpha) = a^2 + b^2$, für $\alpha = a + ib$.
Dann gilt für beliebige $\pi \in \mathbb{Z}[i]$:

$$N(\pi) \in \mathbb{P}_{\mathbb{N}} \Longrightarrow \pi \in \mathbb{P}_{\mathbb{Z}[i]},$$

da wenn $\pi = \alpha \cdot \beta$ wäre, $N(\pi) = N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta) \notin \mathbb{P}_{\mathbb{N}}$ ist. Die Umkehrung der Aussage gilt natürlich nicht, da z.B. $3 \in \mathbb{P}_{\mathbb{Z}[i]}$ und $N(3) = 9 \notin \mathbb{P}_{\mathbb{N}}$ ist.
Satz (Kriterium für prim in $\mathbb{Z}[i]$):
Die Primzahl p ist genau dann eine Gaußsche Primzahl, wenn sie sich nicht als Summe zweier Quadrate ganzer Zahlen schreiben läßt; oder kurz:

$$\forall p \in \mathbb{P}_{\mathbb{N}}: \quad p \in \mathbb{P}_{\mathbb{Z}[i]} \Longleftrightarrow \forall a, b \in \mathbb{N} : a^2 + b^2 \neq p.$$

Beweis: Ist $p = a^2 + b^2$ $(a, b \in \mathbb{N})$, so ist $p = (a + ib)(a - ib)$, wobei die Faktoren Gaußsche Primzahlen sind, weil sie die Norm p haben. Ist $p = \alpha \cdot \beta$ $(\alpha, \beta \in \mathbb{Z}[i])$, wobei α, β keine Einheiten sind, dann ist $p^2 = N(p) = N(\alpha)N(\beta)$, also $N(\alpha) = N(\beta) = p$; die Primzahl p ist demnach als Summe zweier Quadrate darstellbar. $\square$

4 Kongruenzen

4.1 Simplicissimus

Definition. (nach Carl Friedrich Gauss**)** Für natürliche Zahlen a, b, m sagt man, a ist **kongruent** b **modulo** m, $a \equiv b \bmod m$, wenn $m|a-b$.
$\boxed{a \equiv b \bmod m :\Leftrightarrow m|a-b}$

Es gilt:

1. Die Kongruenz modulo m ist eine Äquivalenzrelation, d. h.
   $a \equiv a \bmod m$; $a \equiv b \bmod m \Leftrightarrow b \equiv a \bmod m$ und
   $(a \equiv b \bmod m \wedge b \equiv c \bmod m) \Rightarrow a \equiv c \bmod m$.

2. Bei festem m hat jede der m Äquivalenzklassen genau einen Repräsentanten in $0, 1, ..., m-1$. Man sagt in solchem Fall, $0, 1, ..., m-1$ sei ein **vollständiges Restklassensystem modulo** m. Die Menge der Äquivalenzklassen (Restklassen) bezeichnet man mit $\mathbb{Z}/m\mathbb{Z}$ oder mit $\mathbb{Z}_m$.
   Die Äquivalenzklassen $[0], [1], [2], ..., [m-1]$ werden vereinfachend mit $0, 1, 2, ...,$ $m-1$ bezeichnet.

3. Die Menge der Restklassen ist ein kommutativer Ring.

4. $a \equiv b \bmod m \Rightarrow a \equiv b \bmod d$ für $d|m$.

5. Wenn n und m relativ prim sind, gilt:
   $(a \equiv b \bmod m$ und $a \equiv b \bmod n) \Rightarrow a \equiv b \bmod mn$.

Satz 1:
Im kommutativen Ring $\mathbb{Z}_m$ haben genau diejenigen Elemente ein multiplikatives Inverses, die relativ prim zu m sind, es ist also
$\{a \in \mathbb{Z}_m : \exists b \in \mathbb{Z}_m : ab \equiv 1 \bmod m\} = \{a \in \mathbb{Z}_m : \ \mathrm{ggT}(a, m) = 1\}$.

Bemerkung. Das zu a inverse Element bezeichnet man mit a^{-1} und dessen n-te Potenz mit a^{-n}.

Beweis. Sei $d = \text{ ggT}(a, m)$ und $ab \equiv 1 \bmod m$ für ein $b \in \mathbb{Z}$. Dann gilt $d|m$, also auch $d|ab - 1$, und wegen $d|a$ gilt dann $d|1$, also $d = 1$.
Anderseits existieren, wenn $\text{ggT}(a, m) = 1$ (und o.B.d.A. $a < m$ nach Eigenschaft 2 der Kongruenz), nach dem Korollar zu Satz 3 ganze Zahlen u und v mit $ua + vm = 1$. u ist dann das inverse Element zu a in $\mathbb{Z}_m$, denn es gilt dann $m|ua - 1$, also $ua \equiv 1 \bmod m$. □

Korollar 1: Im Restklassenring $\mathbb{Z}_p$ für $p \in \mathbb{P}$ hat jedes Element ein Inverses, und $\mathbb{Z}_p$ ist ein Körper. Er wird häufig auch mit $\mathbb{F}_p$ bezeichnet.

Korollar 2: Die lineare Kongruenz $ax \equiv b \bmod m$ hat genau dann eine Lösung, wenn $\text{ggT}(a, m) = d|b$.
Die allgemeine Lösung hat dabei die Gestalt: $x = x_0 + t\frac{m}{d}$, wobei x_0 eine spezielle Lösung ist.

Beweis. Für $\text{ggT}(a, m) = 1$ hat $ax \equiv b \bmod m$ nach Satz 4 nämlich die Lösung $x_0 = a^{-1}b$ und die weiteren Lösungen $x_0 + nm$.
Für $1 < d|b$ ist $ax \equiv b \bmod m$ äquivalent zu $\frac{a}{d}x \equiv \frac{b}{d} \bmod \frac{m}{d}$ (wegen $\frac{a}{d}, \frac{b}{d}$ und $\frac{m}{d} \in \mathbb{N}$ und den Definitionen von Kongruenz und Teiler), und es ist $\text{ggT}(\frac{a}{d}, \frac{m}{d}) = 1$.
Gilt hingegen $\text{ggT}(a, m) \nmid b$, so ist $ax \equiv b \bmod m \Leftrightarrow m|ax - b \Leftrightarrow km = ax - b$ für ein $k \in \mathbb{Z} \Leftrightarrow b = ax - km$ für kein $x \in \mathbb{Z}$ erfüllbar, da $\text{ggT}(a, m)|ax - km$, aber $ggT(a, m) \nmid b$.

Bleibt die Frage: Wie findet man eine spezielle Lösung? Hier drei Wynaldische Vorschläge.

1. Probieren ...

2. $ax \equiv b \bmod m \Leftrightarrow \frac{a}{d}x \equiv \frac{b}{d} \bmod \frac{m}{d} \Leftrightarrow a'x \equiv b' \bmod m'$ mit $\text{ggT}(a', b') = 1$. Und $b' \equiv b' \bmod m' \overset{kl.Fer.}{\Leftrightarrow} a'b'(a')^{\varphi(m)-1} \equiv b' \bmod m'$ bringts voll, denn $x_0 = b'(a')^{\varphi(m)-1}$ ist dann eine Lösung der linearen Kongruenz.

3. $ax \equiv b \bmod m$ entpricht der linearen diophantischen Gleichung $ax + my = b \Leftrightarrow \frac{a}{d}x + \frac{m}{d}y = \frac{b}{d} \Leftrightarrow a'x + m'y = b'$, der $\text{ggT}(a, m) = 1$ ist mit Hilfe des Euklidischen Algorithmus darstellbar: $1 = ax_0 + by_0$, mit $x, y \in \mathbb{Z}$.

Geschichtliche Belehrung. DIOPHANT von Alexandria lebte vermutlich um 250 n. Chr. Er ist der Verfasser eines arithmetischen Werkes (*Arithmetica*), bestehend aus 13 „Büchern“. Bis vor kurzer Zeit waren nur sechs dieser Bücher bekannt, im Jahr 1973 wurden vier weitere Bücher in einer arabischen Übersetzung entdeckt. Ein wesentlicher Teil seines Werkes befaßt sich mit dem Lösen von Gleichungen. Da hierbei nur rationale Lösungen gesucht sind, nennt man noch heute eine Gleichung, für welche man rationale oder gar nur ganzzahlige Lösungen sucht, eine DIOPHANTische Gleichung.

Korollar 3: Wenn $a \equiv b \bmod m$, $c \equiv d \bmod m$ und $\mathrm{ggT}(c, m) = 1$ (und somit auch $\mathrm{ggT}(d, m) = 1$), dann ist $ac^{-1} \equiv bd^{-1} \bmod m$.

Beweis. Aus $c(ac^{-1} - bd^{-1}) \equiv acc^{-1} - bdd^{-1} \equiv a - b \equiv 0 \bmod m$ und $\mathrm{ggT}(c, m) = 1$ folgt $m | ac^{-1} - bd^{-1}$.

4.2 Drei Theoreme

4.2.1 Chinesischer Restsatz

Theorem 1 (Chinesischer Restsatz):
Das folgende System von Kongruenzen

$$\begin{aligned} x &\equiv a_1 \bmod m_1 \\ x &\equiv a_2 \bmod m_2 \\ &\vdots \\ x &\equiv a_r \bmod m_r \end{aligned}$$

mit $\mathrm{ggT}(m_i, m_j) = 1$ fur $i \neq j$ hat eine gemeinsame Lösung x für alle Kongruenzen, und alle Lösungen sind kongruent modulo $M = \prod_{k=1}^{r} m_k$.

Beweis. *Existenz:* Sei $M_i = \frac{M}{m_i}$. Wegen $\mathrm{ggT}(m_i, M_i) = 1$ gibt es dann nach Satz 4 ein N_i mit $M_i N_i \equiv 1 \bmod m_i$.
$x = \sum_{k=1}^{r} a_k M_k N_k$ ist dann eine Lösung des obigen Systems: Wegen $m_i | M_j$ für $i \neq j$ gilt $x = \sum_{k=1}^{r} a_k M_k N_k \equiv a_i M_i N_i \equiv a_i \bmod m_i$ für jedes $i \in \{1, 2, ..., r\}$.
Eindeutigkeit: Seien x' und x'' zwei Lösungen. Dann ist $x = x'' - x' \equiv 0 \bmod m_i$ für alle $i \in \{1, 2, ..., r\}$, also auch $x \equiv 0 \bmod M$.

4.2.2 Satz von Euler-Fermat

Definition. $\boxed{\mathbb{Z}_m^* := \{x \in \mathbb{Z}_m : \ \mathrm{ggT}(x,m) = 1\}}$

Definition. Man definiert die **Eulersche φ-Funktion** als $\varphi(m) := |\mathbb{Z}_m^*|$.
$\boxed{\varphi(m) := |\mathbb{Z}_m^*|}$

Theorem 2 (Satz von Euler-Fermat):
Für alle $m \in \mathbb{N}$ und $a \in \mathbb{Z}_m^*$ mit $\mathrm{ggT}(a,m) = 1$ gilt:

$$\underline{a^{\varphi(m)} \equiv 1 \bmod m.}$$

Beweis. Sei $a \in \mathbb{Z}_m^*$. Dann ist, wie man sich leicht überlegt, $\mathbb{Z}_m^* =$

$$\{a \cdot a_i \bmod m : a_i \in \mathbb{Z}_m^*\} :$$

Für alle $i \in \{1, 2, ...\varphi(m)\}$ gilt wegen $a \in \mathbb{Z}_m^*$ und $a_i \in \mathbb{Z}_m^*$:

$$a \cdot a_i \bmod m \in \mathbb{Z}_m^*;$$

wegen $\mathrm{ggT}(a,m) = 1$ hat a ein multiplikatives Inverses, und es folgt $a_i = a_j$ aus $a \cdot a_i = a \cdot a_j$, d. h. es ist

$$a \cdot a_i \neq a \cdot a_j \text{ für } i \neq j.$$

Daher ist

$$a^{\varphi(m)} \cdot \prod_{i=1}^{\varphi(m)} a^i = \prod_{i=1}^{\varphi(m)} a \cdot a^i \equiv \prod_{i=1}^{\varphi(m)} a^i \bmod m,$$

$$\text{also:} \quad a^{\varphi(m)} \equiv 1 \bmod m.$$

Korollar: (Kleiner Fermatscher Satz): Für $p \in \mathbb{P}$ und $A \in \mathbb{Z}$ gilt:

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

1. Beweis. Für $m = p$ folgt aus Theorem 2: $a^{p-1} \equiv 1 \bmod p$, daraus folgt durch Multiplizieren mit a die Behauptung.

2. Beweis (direkt und nach Euler). Vollständige Induktion nach a:
Induktionsanfang: $a = 1 : 1^p \equiv 1 \bmod p$ ist wohl o.k.
Induktionsannahme: Es sei $a^p \equiv a \bmod p$.
Induktionsschritt: $(a+1)^p = \sum_{k=0}^{p} \binom{p}{k} a^k = \binom{p}{p} a^p + \sum_{k=1}^{p-1} \binom{p}{k} a^k + \binom{p}{0} \equiv a^p + 0 + 1$ (da $p | \binom{p}{k}$ für $0 < k < p$) $\equiv a + 1 \bmod p$ nach Induktionsannahme. □

Dieser Satz ist ein *notwendiges* Kriterium für die Primzahleigenschaft. Insbesondere gilt $p|2^p-2$ für jede Primzahl p. Chinesische Gelehrte vermuteten vor etwa 2500 Jahren, daß auch die Umkehrung gilt, daß nämlich aus $n|2^n-2$ folgt, daß n eine Primzahl ist. Diese Vermutung ist falsch (das kleinste Gegenbeispiel ist $n = 341$, es gilt $2^{341} \equiv 2 \bmod 341$ und $341 = 11 \cdot 13$).

Definition. Man bezeichnet eine zusammengestzte Zahl n mit $n|2^n-2$ als **Pseudoprimzahl** oder auch als **chinesische Primzahl**.

Korollar: Aus $a \nmid p$ $(p \in \mathbb{P})$ und $n \equiv m \bmod (p-1)$ folgt $a^n \equiv a^m \bmod p$.

Beweis. O.B.d.A. sei $n > m$. Wegen $p-1|n-m$ gibt es $k \in \mathbb{N}$ mit $n = m+k(p-1)$. Da mit $a^{p-1} \equiv 1 \bmod p$ (Theorem 2) auch $(a^{p-1})^k \equiv 1^k \bmod p$, also $a^{k(p-1)} \equiv 1 \bmod p$, und $a^{k(p-1)}a^m \equiv 1 \cdot a^m \bmod p$, also $a^{m+k(p-1)} \equiv a^m \bmod p$ gilt, folgt die Behauptung.

Satz 1:
Die Eulersche φ-Funktion ist multiplikativ, d. h. es gilt:
$\varphi(mn) = \varphi(m) \cdot \varphi(n)$, falls $\mathrm{ggT}(m,n) = 1$.

Beweis. Sei $\mathrm{ggT}(m,n) = 1$. Für jedes $j \in \{1,2,...,mn-1\}$ sei j_1 der kleinste nichtnegative Rest von j modulo m (d. h. $0 \le j_1 < m$ und $j \equiv j_1 \bmod m$) und j_2 der kleinste nichtnegative Rest von j modulo n (d. h. $0 \le j_2 < n$ und $j \equiv j_2 \bmod n$). Für jedes Paar j_1, j_2 gibt es dann wegen $\mathrm{ggT}(m,n) = 1$ nach dem Chinesischen Restsatz *genau ein* $j \in \{1,2,...,mn-1\}$ mit $j \equiv j_1 \bmod m$ und $j \equiv j_2 \bmod n$.
Außerdem gilt:
$\mathrm{ggT}(j,mn) = 1 \Leftrightarrow \mathrm{ggT}(j,m) = 1 \wedge \mathrm{ggT}(j,n) = 1$
$\Leftrightarrow \mathrm{ggT}(j_1,m) = 1 \wedge \mathrm{ggT}(j_2,n) = 1$
Daraus ergibt sich:
$|\{j \in \{1,2,...mn-1\} : \mathrm{ggT}(j,mn) = 1\}|$
$= |\{(j_1,j_2) : 0 \le j_1 < m, \mathrm{ggT}(j_1,m) = 1 \wedge 0 \le j_2 < n, \mathrm{ggT}(j_2,n) = 1\}|$.
Die Behauptung folgt wegen $|\{j \in \{1,2,...mn-1\} : \mathrm{ggT}(j,mn) = 1\}| = \varphi(mn)$ und $|\{(j_1,j_2) : 0 \le j_1 < m, \mathrm{ggT}(j_1,m) = 1 \wedge 0 \le j_2 < n, \mathrm{ggT}(j_2,n) = 1\}| = \varphi(m) \cdot \varphi(n)$.
□

4.2.3 Theorem von Euler

Theorem 3 (Euler)**:**
Es gilt:

$$\underline{\sum_{d|m} \varphi(d) = m.}$$

Beweis. Sei $\varphi_d(m) := |\{x \in \mathbb{Z}_m : \ \mathrm{ggT}(x,m) = d\}|$. Es ist klar, daß, $\varphi_d(m) = \varphi(m/d)$, falls $d|m$ ($d|m \Rightarrow (\ \mathrm{ggT}(x,m) = d \Leftrightarrow \ \mathrm{ggT}(x/d, m/d) = 1)$). Weil für alle $n \in \{1,...,m\}$ genau ein d existiert mit $n \in \{x \in \mathbb{Z}_m : \ \mathrm{ggT}(x,m) = d\}$, gilt außerdem: $\sum\limits_{d|m} \varphi_d(m) = m$. Daraus folgt

$$m = \sum_{d|m} \varphi_d(m) = \sum_{d|m} \varphi(m/d) = \sum_{d|m} \varphi(d).$$

□

Satz 2:
Es gilt:

$$\underline{\varphi(m) = m \cdot \prod_{p|m} \left(1 - \frac{1}{p}\right).}$$

Beweis. Theorem 3 besagt, daß m die summatorische Funktion von $\varphi(m)$ ist. Also gilt (nach Satz 2.1.7):

$$\varphi(m) = \prod_{p|m} (p^\alpha - p^{\alpha-1}) = \prod_{p|m} (p-1)p^{\alpha-1} = n \cdot \prod_{p|m} \left(1 - \frac{1}{p}\right). \quad \square$$

5 Primzahlsatz und Primzahltests

5.1 Der Primzahlsatz

Definition. Die π-Funktion $\pi(n)$ ist für alle natürlichen Zahlen definiert als die Anzahl aller Primzahlen bis n:

$$\pi(n) := |\{x \in \mathbb{N} : x \in \mathbb{P} \wedge x \leq n\}|$$

Theorem 1 (Primzahlsatz, HADAMARD und POUSSIN, 1896):
Es gilt für große natürliche Zahlen $n \in \mathbb{N}$:

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

Der Beweis dieses Satzes würde den Rahmen bei weitem sprengen. Er basiert auf dem von BERNHRAD RIEMANN im Jahr 1859 entdeckten Zusammenhang zwischen dem Primzahlsatz und der komplexen Funktion ζ.
Es ist aber möglich, eine auf TSCHEBYSCHEW zurückgehende (für die meisten Anwendungen ausreichende) schwächere Version des Satzes zu beweisen (gleich...).

Geschichtliche Belehrung. PAFNUTIJ LWOWITSCH TSCHEBYSCHEW (1821 - 1894), einer der bedeutensten russischen Mathematiker des 19. Jahrhunderts, bewies, daß es Konstanten a und A mit $a + A = 2$ und

$$a \cdot \frac{n}{\log n} < \pi(n) < A \cdot \frac{n}{\log n}$$

(ab einer gewissen Stelle n_0) gibt.
Ebenfalls von TSCHEBYSCHEW wurde bewiesen, daß wenn

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

existiert, dieser Grenzwert gleich 1 ist. Jetzt zeigen wir aber nur die folgende Einsicht TSCHEBYSCHEWS:

$$\frac{2}{3} \cdot \frac{n}{\log n} < \pi(n).$$

Dazu benötigt man zunächst folgendes

Lemma: Für $n, k \in \mathbb{N}$ gilt:

$$\binom{n}{k} \leq n^{\pi(n)}.$$

Dabei bezeichnet $\binom{n}{k}$ den **Binomialkoeffizienten.** Es ist $\binom{n}{k} = \frac{n!}{k!\cdot(n-k)!}$.

Beweis. In diesem Beweis soll p stets eine Primzahl bezeichnen.
Es sind genau $[n/p^t]$ der Zahlen $1, 2, ..., n$ durch p^t teilbar[2] (nämlich jede p^t-te Zahl).

[2] [ ] soll die **Gaußklammer** bezeichnen: $[x] := \max\{n \in \mathbb{N} : n \leq x\}$.

Für $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r} = \prod_{p_i \in \mathbb{P}} p_i^{\alpha_i}$ mit $\alpha_i \in \mathbb{N}$ sei

$$\omega_p(m) := \begin{cases} 0, & \text{wenn } p \nmid m \\ \alpha_i, & \text{wenn } p \mid m \end{cases}$$

die **Multiplizität** von n bezüglich p, damit ist $m = \prod_{p \in \mathbb{P}} p^{\omega_p(m)}$.
Offensichtlich zählt $\omega_p(m)$ also, wie oft p als Faktor in m enthalten ist; es ist $\omega_p(m) = \max\{l \in \mathbb{N} : p^l \mid m\}$.
Es sei außerdem

$$D_{p;e} := \{d \in \mathbb{N} : 1 \leq d \leq n \wedge p^e | d\};$$

aus dieser Definition folgt sofort:

$$|D_{p;e}| = \left[\frac{n}{p^e}\right], \text{ und es ist } D_{p;1} \supseteq D_{p;2} \supseteq ... \supseteq D_{p;e} \supseteq D_{p;e+1} \supseteq ...$$

Weiterhin sind die Definitionen so gewählt, daß für $1 \leq d \leq n$ gilt:

$$d \in D_{p;\omega_p(d)} \subseteq ... \subseteq D_{p;1}, \text{ aber: } d \notin D_{p;\omega_p(d)+1}.$$

Damit ist klar, daß jedes d mit $1 \leq d \leq n$ in die Summe $\sum_{e \geq 1} |D_{p;e}|$ genau $\omega_p(d)$-mal eingeht.
Daraus folgt:

$$\omega_p(n!) = \sum_{d=1}^{n} \omega_p(d) = \sum_{e \geq 1} |D_{p;e}| = \sum_{e \geq 1} \left[\frac{n}{p^e}\right].$$

Daraus und aus der Definition des Binomialkoeffizienten folgt, daß

$$\omega_p\left(\binom{n}{k}\right) = \omega_p(n!) - \omega_p(k!) - \omega_p((n-k)!) = \sum_{e \geq 1} \left(\left[\frac{n}{p^e}\right] - \left[\frac{k}{p^e}\right] - \left[\frac{n-k}{p^e}\right]\right)$$

In dieser Summe ist jeder Summand entweder gleich Null oder gleich eins, und für $e > \log n / \log p$ verschwinden alle Summanden.
Daher ist

$$\omega_p\left(\binom{n}{k}\right) \leq \left[\frac{\log n}{\log p}\right] \text{ und also } p^{\omega_p(\binom{n}{k})} \leq n.$$

Nun folgt die Behauptung aus

$$\binom{n}{k} = \prod_{p \leq n} p^{\omega_p(\binom{n}{k})} \leq n^{\pi(n)}.$$

□

Theorem 2 (Tschebyschew)**:**
Für $n > 200$ gilt:

$$\frac{2}{3} \cdot \frac{n}{\log n} < \pi(n).$$

Beweis (nach Don Zagier**):** Wenn man für $k = 0, 1, ..., n$ einsetzt und die daraus resultierenden Ungleichungen addiert, dann folgt aus dem Lemma:

$$2^n = \sum_{k=0}^{n} \binom{n}{k} \leq (n+1)n^{\pi(n)}.$$

Logarithmiert man nun die beiden Seiten der Ungleichung, so erhält man:

$$\log(2^n) = n \cdot \log 2 \leq \log(n+1) + \pi(n) \cdot \log n = \log((n+1)n^{\pi(n)})$$

$$\Leftrightarrow \pi(n) \geq \frac{n \cdot \log 2}{\log n} - \frac{\log(n+1)}{\log n}.$$

Für $n > 200$ gilt schließlich:

$$\pi(n) \geq \frac{n \cdot \log 2}{\log n} - \frac{\log(n+1)}{\log n} > \frac{2n}{3 \cdot \log n}$$

Die rechte Seite dieser Ungleichung ergibt sich dabei aus $n \cdot (\log 2 - \frac{2}{3}) > \log(n+1)$:
$n \cdot (\log 2 - \frac{2}{3}) > n \cdot 0,025$ gilt für alle $n \in \mathbb{N}$ und $n \cdot 0,025 > \log(n+1)$ gilt für $n > 200$. □

5.2 Primzahltests

5.2.1 Das Sieb des Eratosthenes

Satz 1:
Für jede zusammengesetzte Zahl $n \in \mathbb{N}$ existiert ein Primteiler $p \in \mathbb{P}$ mit

$$p \leq \sqrt{n}.$$

Beweis. Wie man sich leicht überlegt, ist der kleinste von eins verschiedene Teiler von n eine Primzahl. Dann ist auch $\frac{n}{p}$ ein Teiler von n, und es gilt: $p \leq \frac{n}{p}$, also $p^2 \leq n$.

Das Sieb des Eratosthenes :
Mittels des **Siebes von Eratosthenes** findet man alle Primzahlen bis zu einer vorgegebenen Zahl $n \in \mathbb{N}$. Näheres dazu findet sich im Kapitel **„Non vitae, sed scholae discibunt“.**

5.2.2 Satz von Wilson

Lemma (Heiratslemma):
Es sei M die aus $p-3$ Individuen bestehende Menge $M := \{2, 3, 4, ..., p-3, p-2\}$, wobei wie immer $p \in \mathbb{P}$ sei. Man nennt a und $\tilde{a}$ ein **Paar**, wenn gilt: $a\tilde{a} \equiv 1(p)$. Dann gilt:
1. $\forall a \in M\ \dot{\exists}\tilde{a} : a, \tilde{a}$ sind ein Paar.
2. Sind $a, \tilde{a}$ ein Paar, so auch $\tilde{a}, a$.
3. Für jedes Paar $a, \tilde{a}$ gilt: $a \neq \tilde{a}$.

Beweis. 1. *Existenz:* $\forall\, a \in M : \mathrm{ggT}(a, p) = 1$. Also gibt es ein $\tilde{a} \in \mathbb{Z}$ mit $a\tilde{a} \equiv 1(p)$. Mit $\tilde{a}$ lösen auch alle Zahlen $\tilde{a} + np, n \in \mathbb{Z}$ die Kongruenz, deshalb kann man Œ $0 \leq a < p$ annehmen (sonst Division mit Rest von $\tilde{a}$ durch p). $\tilde{a} = 0$ geht ja gar nicht, da $a \cdot 0 \equiv 0 \not\equiv 1(p)$. $\tilde{a} = 1$ oder gar $\tilde{a} = p - 1$ ist auch unmöglich, denn $a \cdot 1 \equiv 1(p)$ bedeutet $a|p-1$ und $a(p-1) \equiv 1(p)$ bedeutet $p|a+1$, was beides aufgrund von $2 \leq a \leq p-2$ nicht geht. Damit ist $\tilde{a} \in M$, d.h. $a, \tilde{a}$ bilden ein Paar. *Eindeutigkeit:* Alle Lösungen von $aX \equiv 1(p)$ sind zueinander kongruent mod p und da verschiedene Elemente aus M stets inkongruent mod p sind, ist $\tilde{a}$ das einzige Element aus M mit $a\tilde{a} \equiv 1(p)$. 2. El Triv 3. Sei $a^2 \equiv 1(p)$, d.h. $(a-1)(a+1) \equiv 0(p)$, dann gälte $a \equiv 1(p)$ oder $a \equiv -1 \equiv p-1(p)$. Aber kein Element aus M besitzt die Unverschämtheit zu 1 oder zu $p-1$ kongruent sein zu wollen. □

Lemma:
Es gilt: $(p-2)! \equiv 1(p)$, für jedes $p \in \mathbb{P}$.

Beweis. Für $p = 2$ und $p = 3$ ist die Sache wohl klar. Ist $p \geq 5$, dann kann man wegen des Heiratslemmas die $p-3$ Faktoren des Produkts (p-2)! so zu Paaren zusammenfassen, daß jeweis $a\tilde{a} \equiv 1(p)$ gilt. Also ist $(p-2)! = \prod a\tilde{a} \equiv 1(p)$. □

Satz (Wilson):
Für jedes $p \in \mathbb{P}$ gilt: $(p-1)! \equiv -1(p)$.

Beweis. $(p-1)! = (p-2)!(p-1) \equiv (p-1) \equiv -1(p)$ □

5.2.3 Faktorsierungsalgorithmen

Zu einer gegebenen Zahl n die Primfaktorzerlegung zu bestimmen, ist prinzipiell ein sehr einfach. Man überprüft n einfach auf die Teilbarkeit durch die ersten $[\sqrt{n}]$ Zahlen. Diese Methode ist jedoch schon für vergleichsweise kleine Zahlen nicht mehr praktikabel. Mit Hilfe von überwiegend erst in der letzten Zeit entwickelten Faktorisierungsalgorithmen ist man jedoch in der Lage, Zahlen in erstaunlicher Größenordnung zu faktorisieren.

Mit der **Elliptische-Kurven-Methode** kann man bis zu 43-stellige Zahlen faktorisieren.

Das **Quadratische Sieb** ist ein deutlich leistungsfähigerer Algorithmus als die Elliptische-Kurven-Methode. Er ist der momentan schnellste Algorithmus für bis zu 110-stellige Zahlen.

Der beste bekannte Faktorisierungsalgorithmus ist jedoch das **Zahlkörpersieb**. Für die größten überhaupt noch faktorisierbaren Zahlen ist dies der schnellste Algorithmus. Zudem ist er noch relativ neu, so daß es wahrscheinlich ist, daß er noch weiter verbessert werden kann.

6 Übergang zu quadratischen Resten

6.1 Allerlei zu quadratischen diophantischen Gleichungen

Definition. Ein primitives pythagoreisches Zahlentripel ist ein Tripel $(x, y, z) \in \mathbb{N}^3$ mit $x^2 + y^2 = z^2$ und $\text{ggT}(x, y, z) = 1$.

Bemerkung. Wegen $x^2 + y^2 = z^2$ folgt aus $\text{ggT}(x, y, z) = 1$ auch $\text{ggT}(x, y) = 1$, $\text{ggT}(x, z) = 1$ und $\text{ggT}(y, z) = 1$.
Offensichtlich ist genau eine der Zahlen x, y gerade:
Sie können nicht beide gerade sein wegen $\text{ggT}(x, y, z) = 1$; sie können aber auch nicht beide ungerade sein, weil dann mit $x^2 \equiv 1 \bmod 4$ und $y^2 \equiv 1 \bmod 4$ auch $x^2 + y^2 \equiv 1 \bmod 4$ gelten müßte, im Widerspruch zu $z^2 \not\equiv 1 \bmod 4$.

Satz 1:
Alle primitiven pythagoreischen Zahlentripel (x, y, z) mit geradem y sind folgendermaßen darstellbar:

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

mit $a, b \in \mathbb{N}$, $\text{ggT}(a, b) = 1, a > b$ und $a \not\equiv b \bmod 2$.

Beweis. (i) Das so konstruierte Zahlentripel (x, y, z) ist ein primitives pythagoreisches:
$x^2 + y^2 = z^2$ gilt, und es ist $\text{ggT}(x, y, z) = 1$: Aus $p|x$ und $p|z$ folgt $p \neq 2$ (da $a \not\equiv b \bmod 2$) und $p|2a^2$ und $p|2b^2$, also $p|a$ und $p|a$. Das gehört sich aber nicht.
(ii) Wegen der obigen Bemerkung können wir $x = 2u + 1, y = 2v$ und $z = 2w + 1$ annehmen.Daraus folgt:

$$y^2 = z^2 - x^2 = (z + x)(z - x) = (2w + 2u + 2)(2w - 2u) = 4rs$$

mit $r = w + u + 1$ und $s = w - u$.
Wegen $\text{ggT}(z+x, z-x) = 2$ folgt $\text{ggT}(r, s) = 1$, und r und s müssen beides Quadrate sein: $r = a^2$ und $s = b^2$, $a, b \in \mathbb{N}$. □

Satz 2:
Eine ungerade Primzahl p kann genau dann als Summe zweier Quadratzahlen dargestellt werden, wenn $p \equiv 1 \bmod 4$.

Satz 3:
eine natürliche Zahl n ist genau dann als Summe von zwei Quadraten darstellbar, wenn für jede Primzahl p mit $p \equiv 3 \bmod 4$ der Exponent in der kanonischen Primfaktorzerlegung gerade ist.

7 Quadratische Reste

7.1 Das Aufwärmprogramm

Satz 1:
Die Menge $m\mathbb{Z} := \{m \cdot z : m \in \mathbb{N}^+ \wedge z \in \mathbb{Z}\}$ ist ein Ideal, also insbesondere auch ein Unterring von $\mathbb{Z}$.

Definition. Für $m \in \mathbb{N}^+$ ist $\boxed{R_m := \{1, 2, ..., m-1\}}$ und
$\boxed{R_m^* := \{z \in R_m : \text{ggT}(z, m) = 1\}}$.

Bemerkung: Zu $m \in \mathbb{N}^+$ und $z \in \mathbb{Z}$ gibt es stets eine Zahl $r_m(z)$ mit $r_m(z) \in R_m$ und $r_m(z) \equiv z \bmod n$.

Satz 2:
Für $m \in \mathbb{N}^+$ ist der sogenannte **Restklassenring modulo** m, d. h. die Menge $\mathbb{Z}_m = \mathbb{Z}/m\mathbb{Z}$, ein Ring. Ist $m \in \mathbb{P}$, so ist $\mathbb{Z}_m$ ein Körper.
Die Menge $\mathbb{Z}_m^* = \{r + m\mathbb{Z} : r \in R_m^*\}$ ist in bezug auf die Restklassenmultiplikation eine Gruppe.

7.2 Hinähn

Definition. $a \in \mathbb{Z}_m^*$ heißt **quadratischer Rest** modulo m, falls $\exists x \in \mathbb{Z}_m^* : a \equiv x^2 \bmod m$. $a \in \mathbb{Z}_m^*$ heißt **quadratischer Nichtrest** modulo m, falls a kein quadratischer Rest modulo m ist. Die Menge aller quadratischer Reste modulo m soll mit QR_m bezeichnet werden, die der quadratischen Nichtreste modulo m mit QNR_m.

Bemerkung. Offenbar gilt: $QR_m = \mathbb{Z}_p^{*2} = \{r^2 + m\mathbb{Z} : r \in R_m^*\}$.

Satz 1:
Es sei $m = m_1 m_2 \cdot ... \cdot m_r$ mit $m \geq 2$ und $\forall i, j \in \{1, 2, ..., r\} : \text{ggT}(m_i, m_j) = 1$.
Dann ist
a ein quadratischer Rest modulo m genau dann, wenn
a ein quadratischer Rest modulo jeder Zahl m_i für $i \in \{1, 2, ..., r\}$.
Durch diesen Satz lassen sich Überlegungen im Modul n auf solche im Modul p^k $(p \in \mathbb{P}, k \in \mathbb{N}^+)$ zurückführen.

Satz 2:
Es sei $k \geq 3$. Dann sind folgende Aussagen über eine Zahl $a \in \mathbb{Z}$ äquivalent:

(i) a ist ein quadratischer Rest modulo 2^k.
(ii) a ist ein quadratischer Rest modulo 2^3.
(iii) $a \equiv 1 \bmod 8$

Beweis. (i) $\Rightarrow$ (ii): Trivial wegen $k \geq 3$.
(ii) $\Rightarrow$ (i): Induktion nach k. Induktionsanfang ist $k = 3$. (ii) $\Leftrightarrow$ (iii): $1^2 \equiv 3^2 \equiv 5^2 \equiv 7^2 \equiv 1 \bmod 8$.

Satz 3:
Es sei $p \in \mathbb{P}$ eine ungerade Primzahl, und $k \in \mathbb{N}^+$. Dann sind folgende Aussagen über eine Zahl $a \in \mathbb{Z}$ äquivalent:

(i) a ist ein quadratischer Rest modulo p^k.
(ii) a ist ein quadratischer Rest modulo p.

Nun gilt es also, sich mit den Primzahlmoduln $p \neq 2$ auseinander zu setzen:

Satz 4:
Wenn $p \in \mathbb{P}$ eine von zwei verschiedene Primzahl ist, dann gibt es genau $\frac{p-1}{2}$ quadratische Reste modulo p und genau $\frac{p-1}{2}$ quadratische Nichtreste modulo p.
Beweis. Der Kern des Epimorphismus $f : \mathbb{Z}_p^* \to \mathbb{Z}_p^{*2}$, $f(r + p\mathbb{Z}) = r^2 + p\mathbb{Z}$ ist die Menge $\mathbb{E}_p^* = \{1 + p\mathbb{Z}, -1 + p\mathbb{Z}\}$. Nach dem Homomorphiesatz der Gruppentheorie ist daher $\mathbb{Z}_p^{*2}$ isomorph zu $\mathbb{Z}_p^*/\mathbb{E}_p^*$, es gilt also: $\frac{p-1}{2} = \varphi(p)|\mathbb{Z}_p^{*2}| = |\mathbb{Z}_p^*/\mathbb{E}_p^*|$.

7.3 Der Weg zu Gauss' Reziprozitätsgesetz

Definition. Für $p \in \mathbb{P}$ und $a \in \mathbb{Z}_m^*$ heißt

$$(a|p) := \begin{cases} 1, & \text{falls } a \in QR_p \\ -1, & \text{falls } a \in QNR_p \end{cases}$$

das **Legendre-Symbol** von a modulo p.

Satz 1 (Kriterium von Euler:)
Für alle $p \in \mathbb{P}, p \neq 2$, und $x \in \mathbb{Z}_p^*$ gilt:

$$x^{\frac{p-1}{2}} \equiv (x|p) \bmod p.$$

Beweis. (i) Sei $(x|p) = 1$, d. h. $x^2 \equiv a \bmod p$ mit $\mathrm{ggT}(a, p) = 1$ und also auch $\mathrm{ggT}(x, p) = 1$. Dann gilt nach dem (kleinen) Satz von Fermat:

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

Jeder quadratischer Rest löst daher die Polynomkongruenz $X^{\frac{p-1}{2}} - 1 \bmod p$; diese hat nach dem Satz von Lagrange höchstens $\frac{p-1}{2}$ inkongruente Lösungen. Da es

andererseits genau $\frac{p-1}{2}$ verschiedene quadratische Reste modulo p gibt, ist der Satz für den Fall $(x|p) = 1$ bewiesen.
Da stets $a^{\frac{p-1}{2}} \bmod p$ oder $a^{\frac{p-1}{2}} \bmod p$ gilt, folgt die Aussage des Satzes auch für $(x|p) = -1$.

Theorem 1 (Quadratisches Reziprozitätsgesetz, GAUSS:)
Für alle ungeraden $p, q \in \mathbb{P}$ mit $\mathrm{ggT}(p, q) = 1$ gilt:

$$(p|q) \cdot (q|p) = (-1)^{\frac{(p-1)(q-1)}{4}}.$$

8 Anwendungen

8.1 Der RSA-Algorithmus

Mit ihrer Arbeit „New Directions in Cryptography“ begründeten Diffie und Hellman aus dem Jahr 1976 die Public-Key-Kryptographie. Es wird in der Arbeit aber nur das *Prinzip* der Public-Key-Kryptographie beschrieben. In ihr ist zwar auch eine allgemeine Lösung des Signatur-Problems enthalten, doch *konkrete* Chiffriersysteme werden nicht angegeben. Es dauerte aber nur ein halbes Jahr, bis drei Wissenschaftlern vom Massachusetts Institute of Technology (MIT) auch dieses gelang. Nachdem Ronald Rivest, Adi Shamir und Leonard Adleman mehrere Monate lang verschiedene vor allem von Ronald Rivest erdachte Systeme auf ihre Tauglichkeit als sicheres Public-Key-Kryptosystem hin geprüft hatten (das war vor allem die Aufgabe von Leonard Adleman; Adi Shamir widmete sich beiden Tätigkeiten), fanden sie schließlich in dem später nach ihnen benannten **RSA-Algorithmus** ein Kryptosystem, das ihren hohen Anforderungen genügte. Dieser Erfolg, den sie inder Arbeit „A Method for Obtaining Digital Signatures and Public-Key Crypto-Systems“ veröffentlichten, kam für die drei Kryptologen eigentlich recht überraschend: Sie hatten ursprünglich zeigen wollen, daß Public-Key-Kryptographie unmöglich ist.
Rivest, Shamir und Adleman fanden im Faktorisierungsproblem (Die Funktion $f : \mathbb{N}^2 \to \mathbb{N}, (p, q) \mapsto n$ ist für $n = p \cdot q$ mit $p, q \in \mathbb{P}$ effizient, aber ihre Umkehrung ist für geeignete große Primzahlen p, q hart, f ist also eine Einwegfunktion.) den entscheidenden Grundbaustein für ihr Kryptosystem. Ein auf dieser Idee basierendes Kryptosystem ist auf der einen Seite einfach zu implementieren, auf der anderen Seite ist das Faktorisierungsproblem von Alters her eines der zentralen Probleme der Zahlentheorie. Die oben erwähnte Annahme, daß es praktisch unmöglich ist, für geeignete große Primzahlen p, q die Zahl $n = pq$ zu faktorisieren, stützt sich auf eine lange Geschichte gescheiterter Versuche, einen mit erträglichem Zeitaufwand verbundenen Algorithmus zur Berechnung der Faktorisierung zu finden.

8.1.1 Die Schlüsselvergabe

Anhand des RSA-Algorithmus erkennt man den großen Vorteil der Public-Key-Kryptosysteme, daß nicht, wie in den symmetrischen Kryptosystemen, je zwei Teilnehmer einem gemeinsamen Schlüssel benötigen (so daß bei einem System mit n Teilnehmern $\frac{n(n-1)}{2}$ Schlüssel benötigt werden), sondern daß jeder Teilnehmer nur einen geheimen und einen öffentlichen Schlüssel benötigt.

Die Schlüsselvergabe wird von einer unabhängigen Schlüsselvergabestelle durchgeführt.
Für jeden Teilnehmer P des Systems wählt sie zwei große, d. h. mindestens 100-stellige Primzahlen p und q und berechnet $n = pq$.

Im nächsten Schritt berechnet die Schlüsselvergabestelle

$$\varphi(n) = \varphi(pq) = \varphi(p)\varphi(q) = (p-1)(q-1).$$

Im letzten Schritt wählt sie eine Zahl e mit $\text{ggT}(e, \varphi(n)) = 1$. Wegen $\text{ggT}(e, \varphi(n)) = 1$ läßt sich die lineare Kongruenz

$$x \cdot e \equiv 1 \bmod 1$$

lösen; die Schlüsselvergabestelle kann damit und eine Zahl f bestimmen mit

$$e \cdot f \equiv 1 \bmod \varphi(n) \text{ und } 1 < f < \varphi(n).$$

Die Zahlen p, q und $\varphi(n)$ werden im folgenden nicht mehr benötigt und daher aus Sicherheitsgründen gelöscht. Nun wird das Paar (e, n) als öffentlicher Schlüssel bekanntgegeben, der Teilnehmer P erhält die Zahl f als geheimen Schlüssel.
Es ist dabei sinnvoll, im letzten Schritt der Berechnungen die Zahl e so zu wählen, daß es möglichst einfach ist, mit dieser Zahl zu potenzieren.

8.1.2 Beschreibung des RSA-Algorithmus

Wenn eine Person P_1 eine Nachricht an eine Person P_2 senden möchte, dann muß P_1 als erstes den öffentlichen Schlüssel von P_2 (e, n) aus einer (dem Telefonbuch vergleichbaren) öffentlichen Datei in Erfahrung bringen.
Danach muß die Nachricht erst in eine Zifferfolge umgewandelt und dann in Zahlen m, die weniger als 100 Ziffern haben, aufgeteilt werden.
Die Verschlüsselung einer solchen Zahl m erfolgt nun mit Hilfe des öffentlichen Schlüssels durch Potenzieren mit e im Restklassenring $\mathbb{Z}_n$. Die Verschlüsselungsfunktion f_E hat also die Form

$$f_E : \mathbb{Z}_n \to \mathbb{Z}_n \quad m \mapsto c = m^e \bmod n.$$

Die verschlüsselte Nachricht c kann P_1 nun an P_2 senden.
P_2 (und nur P_2) kann die Nachricht wieder entschlüsseln, indem P_2 c mit dem geheimen Schlüssel f potenziert. Dadurch erhält P_2:

$$c^f \bmod n = (m^e)^f \bmod n = m^{e \cdot f} \bmod n.$$

Die Zahlen e und f waren aber gerade so konstruiert, daß

$$e \cdot f \equiv 1 \bmod \varphi(n) \Leftrightarrow e \cdot f - 1 = k \cdot \varphi(n) \text{ für ein } k \in \mathbb{N}.$$

Es folgt:

$$c^f \bmod n = m^{e \cdot f} \bmod n = m^{k \cdot \varphi(n)+1} = m \cdot m^{k \cdot \varphi(n)}.$$

Der Satz von Fermat-Euler besagt, daß $m^{\varphi(n)} \bmod n$, falls $\mathrm{ggT}(m,n) = 1$. Da p und q *mindestens* 100 Stellen haben, m dagegen *höchstens* 100 Stellen, $n = pq$ und m also teilerfremd sind, sind die Voraussetzungen des Satzes erfüllt. Daher gilt:

$$m \cdot m^{k\cdot\varphi(n)} \equiv m \cdot 1^k \equiv m \bmod n, \text{ also:}$$

$$c^f \bmod n = m \cdot m^{k\cdot\varphi(n)} \equiv m \bmod n.$$

Es ist also gewährleistet, daß durch das Potenzieren mit f der verschlüsselte Text m wieder entschlüsselt wird.

Bemerkung. Es ist außerordentlch schwierig, echte Primzahlen in der für die Sicherheit des Systems benötigten Größenordnung ($\sim 100 - 200$ Dezimalstellen) zu finden. Man verwendet daher in der kryptographischen Praxis meist Pseudoprimzahlen, Zahlen also, die alle bekannten und mit machbarem Aufwand überprüfbaren Primzahltests erfüllen.

8.1.3 Die Sicherheit des RSA-Algorithmus

Der RSA-Algorithmus läßt grundsätzlich zwei Arten von Angriffen der Kryptoanalyse zu. Der eine Angriff besteht darin, daß der private Schlüssel f eines Teilnehmers P an einem RSA-Kryptosystem aus der Kenntnis des öffentlichen Schlüssels (e, n) erschlossen wird. Bei der zweiten Art von Angriffen wird versucht, den Geheimtext zu dechiffrieren, ohne den geheimen Schlüssel zu kennen. Diese Angriffe (zumindest die bis jetzt bekannten) beruhen auf der Hoffnung, durch eine Unzahl von Versuchen zum Erfolg zu kommen. Wenn der Kryptoanalytiker einen an einen Teilnehmer P adressierten Text kennt, kann er versuchen, alle möglichen Klartexte mit dem öffentlichen Schlüssel von P zu chiffrieren und mit dem ihm bekannten Text zu vergleichen.
Dieser Angriff auf das RSA-System scheitert aber ebenso wie andere unter den Namen Brute-Force-Attack bekannte Bemühungen, durch unsystematisches Versuchen zum Erfolg zu kommen, an der Rechnerkapazität.
Prinzipiell erfolgsversprechender sind die Angriffe der ersten Art. Bei ihnen wird versucht, den privaten Schlüssel f zu erschließen. Das dazu nötige Hilfsmittel ist die Zahl $\varphi(n)$. $\varphi(n)$ liefert f ohne größeren Aufwand über den Euklidischen Algorithmus. Da $\varphi(n)$ sich für $n = pq$ als

$$\varphi(n) = (p-1)(q-1)$$

bestimmt, läßt sich $\varphi(n)$ sehr leicht bestimmen, wenn man die Primfaktorzerlegung von n kennt. Die Primfaktorzerlegung einer Zahl $n = pq$ mit über 100-stelligen Primzahlen p und q zu finden (n hat also über 200 Stellen), ist heutzutage aber noch nicht möglich, obwohl es bereits gelungen ist, Zahlen mit über 100 Stellen zu faktorisieren.
Noch größere Zahlen scheinen, wenn sie nicht anfällig gegen bekannte Attacken wie über spezielle Primfaktorzerlegungen sind, (noch) sicher zu sein. Wenig anfällig sind Zahlen $n = pq$, wenn sich ihre (über 100 liegende) Stellenzahl nur wenig unterscheidet, wenn der ggT(p-1,q-1) klein ist und wenn jede der Zahlen $p-1$, $p+1$, $q-1$ und $q+1$ mindestens einen großen Primfaktor besitzt. Endgültiges läßt sich über die Möglichkeiten von Faktorisierungen in solcher Größenordnung - und damit auch über die Anfälligkeit des RSA - nichts sagen.
Es ist kein polynomaler Faktorisierungsalgorithmus bekannt, aber man ist auch nicht in der Lage zu zeigen, daß ein solcher Algorithmus nicht gefunden werden kann.

9 Non vitae, sed scholae discibunt...

9.1 Das Sieb des Eratosthenes

Satz 1:
Für jede zusammengesetzte Zahl $n \in \mathbb{N}$ existiert ein Primteiler $p \in \mathbb{P}$ mit

$$p \leq \sqrt{n}.$$

Beweis. Wie man sich leicht überlegt, ist der kleinste von eins verschiedene Teiler von n eine Primzahl. Dann ist auch $\frac{n}{p}$ ein Teiler von n, und es gilt: $p \leq \frac{n}{p}$, also $p^2 \leq n$.

Das Sieb des Eratosthenes :
Mittels des **Siebes von Eratosthenes** findet man alle Primzahlen bis zu einer vorgegebenen Zahl $n \in \mathbb{N}$. Die Vorgehensweise ist die folgende:

1. Als erstes schreibt man die ersten n natürlichen Zahlen in rechteckiger Anordnung auf.
2. Danach kennzeichnet man die Zahl 2 als erste Primzahl und streicht jede zweite Zahl.
3. In jedem weiterem Durchgang kennzeichnet man die erste nicht gestrichene Zahl k als Primzahl und streicht jede k-te Zahl.
4. Den letzten Schritt wiederholt man solange, bis alle Zahlen, die kleiner als $\sqrt{n}$ sind, entweder gestrichen oder als Primzahl markiert sind.
5. Die Menge aller Primzahlen bis n besteht aus allen nichtgestrichenen Zahlen.

9.2 Leckeres aus der Teilbar?

An der dekadischen Zifferndarstellung einer natürlichen Zahl kann man leicht ablesen, ob sie durch 2 oder durch 5 teilbar ist – dies hängt nur von der letzten Ziffer ab. Man will aber oft auch wissen, ob eine Zahl durch 3, 7, 11, 13 und weitere Primzahlen teilbar ist. Dazu wird zunächst ein neuer Begriff definiert:

Definition. Es sei

$$\begin{aligned} n &= (a_k a_{k-1} ... a_2 a_1 a_0)_{10} \\ &= a_k 10^k + a_{k-1} 10^{k-1} + ... + a_2 10^2 + a_1 10 + a_0 \end{aligned}$$

eine im Zehnersystem dargestellte Zahl. Dann heißt

$$Q_1(n) = a_0 + a_1 + a_2 + ... + a_k$$

Quersumme erster Stufe von n,

$$Q_1'(n) = a_0 - a_1 + a_2 - + ... + (-1)^k a_k$$

alternierende Quersumme erster Stufe von n,

$$Q_2(n) = (a_1 a_0)_{10} + (a_3 a_2)_{10} + (a_5 a_4)_{10} + ...$$

Quersumme zweiter Stufe von n,

$$Q_2'(n) = (a_1 a_0)_{10} - (a_3 a_2)_{10} + (a_5 a_4)_{10} - + ...$$

alternierende Quersumme zweiter Stufe von n,

$$Q_s(n) = \sum_{i=0}^{\infty} (a_{is+s-1} ... a_{is+1} a_{is})_{10}$$

Quersumme s-ter Stufe von n und

$$Q_s'(n) = \sum_{i=0}^{\infty} (-1)^i (a_{is+s-1} ... a_{is+1} a_{is})_{10}$$

alternierende Quersumme s-ter Stufe von n. Man denke sich im Bedarfsfall die Zehnerdarstellung von n nach links durch Nullen ergänzt. Übrigens sind die Summen nur formal unendlich, da n nur endlich viele von 0 verschiedene Ziffern besitzt.

Satz:
Für $n, s \in \mathbb{N}$ gilt:

$$n \equiv Q_s(n) \bmod (10^s - 1) \quad \text{und} \quad n \equiv Q_s'(n) \bmod (10^s + 1).$$

Beweis: $n = \sum_{j=0}^{\infty} a_j 10^j = \sum_{i=0}^{\infty} (a_{is+s-1}...a_{is+1}a_{is})_{10} \cdot 10^{is}$. Aus $10^s \equiv 1 \bmod (10^s - 1)$ folgt durch Potenzieren $10^{is} \equiv 1 \bmod (10^s - 1)$ für $i = 1, 2, ...$ und daraus $n \equiv Q_s(n) \bmod (10^s - 1)$. Ebenso folgt aus $10^s \equiv -1 \bmod (10^s + 1)$ durch Potenzieren $10^{is} \equiv (-1)^i \bmod (10^s + 1)$ für $i = 1, 2, ...$ und daraus $n \equiv Q'_s(n) \bmod (10^s + 1)$. □

Für $s = 1, 2, 3$ erhält man der Reihe nach :

$$\begin{array}{llll} n \equiv & Q_1(n) \bmod 9 & n \equiv & Q'_1(n) \bmod 11 \\ n \equiv & Q_2(n) \bmod 99 & n \equiv & Q'_2(n) \bmod 101 \\ n \equiv & Q_3(n) \bmod 999 & n \equiv & Q'_3(n) \bmod 1001. \end{array}$$

Daraus ergeben sich die folgenden Teilbarkeitskriterien:

$$\begin{array}{rcrrcr} 9|n & \Leftrightarrow & 9|Q_1(n) & 11|n & \Leftrightarrow & 11|Q'_1(n) \\ 99|n & \Leftrightarrow & 99|Q_2(n) & 101|n & \Leftrightarrow & 101|Q'_2(n) \\ 999|n & \Leftrightarrow & 999|Q_3(n) & 1001|n & \Leftrightarrow & 1001|Q'_3(n) \end{array} .$$

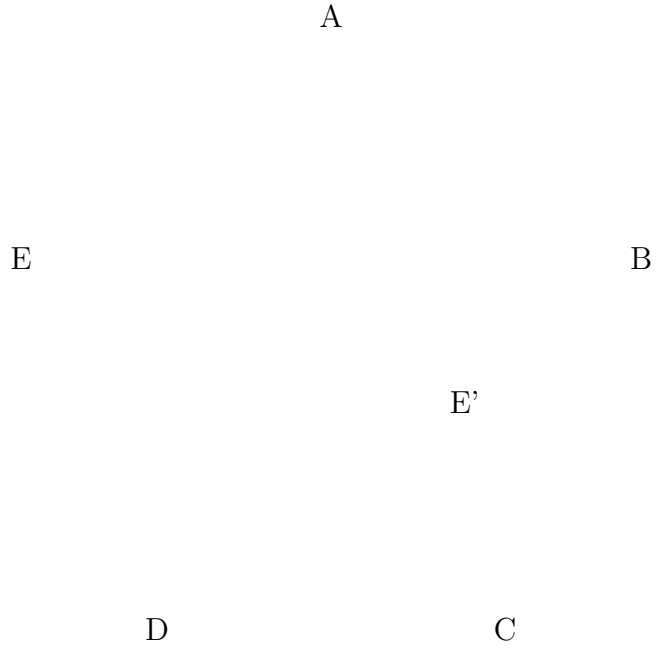
In der Regel interessiert man sich aber nur für die Teilbarkeit durch eine Primzahl; man zerlegt also die Moduln 9, 99 usw. in Primfaktoren und erhält so Kriterien für die Teilbarkeit durch Primzahlen. Wegen $9 = 3^2$, $99 = 3^2 \cdot 11$, $999 = 3^3 \cdot 37$ und $1001 = 7 \cdot 11 \cdot 13$ ergeben sich folgende Kriterien:

$$\begin{array}{rcr} 3|n & \Leftrightarrow & 3|Q_1(n) \\ 7|n & \Leftrightarrow & 7|Q'_3(n) \\ 11|n & \Leftrightarrow & 11|Q'_1(n) \\ 13|n & \Leftrightarrow & 13|Q'_3(n) \\ 37|n & \Leftrightarrow & 37|Q_3(n) \\ 101|n & \Leftrightarrow & 101|Q'_2(n) \end{array} .$$

9.3 Goldene Schnittchen

9.3.1 Das Pentagon

Aus Symmetriegründen gilt am Pentagon:



$\overline{AE}||\overline{BE'}$, $\overline{AD}||\overline{BC'}$ und $\overline{DE}||\overline{CE'}$, d.h. $\triangle AED$ ist ähnlich $\triangle BE'C$, also gilt $\frac{\overline{AD}}{\overline{AE}} = \frac{\overline{BC}}{\overline{BE'}}$. Außerdem ist $\overline{BE'} = \overline{BD} - \overline{BC}$, da $\overline{BC} = \overline{AE} = \overline{DE}$, wegen $\overline{AE}||\overline{DB}$ und $\overline{DE}||\overline{AC}$. Es gilt also:

$$\frac{\text{Diagonale}}{\text{Seite}} = \frac{\text{Seite}}{\text{Diagonale} - \text{Seite}}$$

Bezeichne die Diagonale mit a_0, die Seite mit a_1, deren Differenz mit $a_2 = a_0 - a_1$. Aus der Gleichung $\frac{a_0}{a_1} = \frac{a_1}{a_0 - a_1}$ erhält man mit $a_0^2 - a_0 a_1 = a_1^2$, also $a_0 = \frac{1}{2}a_1(1 \pm \sqrt{5})$ das Verhältnis $\frac{a_0}{a_1} = \frac{1}{2}(1 + \sqrt{5})$. Dieses Verhältnis nennt man auch den **Goldenen Schnitt**.
Da $\sqrt{5} \notin \mathbb{Q}$, sind Seite und Diagonale im Pentagon *inkommensurable* Strecken, d.h. sie besitzen kein gemeinsames Maß.

9.3.2 Kettenbrüche

Mit Hilfe von Brüchen kann der euklidische Algorithmus auch folgendermaßen geschrieben werden:

$$\begin{array}{rcll}
\frac{a}{b} & = & v_0 + \frac{r_1}{b} & \text{mit } v_0 \in \mathbb{N}_0 \quad \text{und} \quad 0 < r_1 < b \\
\frac{b}{r_1} & = & v_1 + \frac{r_2}{r_1} & \text{mit } v_1 \in \mathbb{N} \quad \text{und} \quad 0 < r_2 < r_1 \\
\frac{r_1}{r_2} & = & v_2 + \frac{r_3}{r_2} & \text{mit } v_2 \in \mathbb{N} \quad \text{und} \quad 0 < r_3 < r_2 \\
 & & \cdots\cdots\cdots & \\
\frac{r_{n-3}}{r_{n-2}} & = & v_{n-2} + \frac{r_{n-1}}{r_{n-2}} & \text{mit } v_{n-2} \in \mathbb{N} \quad \text{und} \quad 0 < r_{n-1} < r_{n-2} \\
\frac{r_{n-2}}{r_{n-1}} & = & v_{n-1} + \frac{r_n}{r_{n-1}} & \text{mit } v_{n-1} \in \mathbb{N} \quad \text{und} \quad 0 < r_n < r_{n-1} \\
\frac{r_{n-1}}{r_n} & = & v_n & \text{mit } v_n \in \mathbb{N}.
\end{array}$$

Setzt man diese Bruchterme ineinander ein, so ergibt sich

$$\frac{a}{b} = v_0 + \cfrac{1}{v_1 + \cfrac{1}{v_2 + \cfrac{1}{\ddots + \cfrac{1}{v_{n-2} + \cfrac{1}{v_{n-1} + \cfrac{1}{v_n}}}}}}.$$

Dies nennt man die **Kettenbruchdarstellung** von $\frac{a}{b}$ und schreibt

$$\frac{a}{b} = [v_0, v_1, \ldots, v_n].$$

Historische Bemerkung: Die Theorie der Kettenbrüche entwickelte sich aus dem Bedürfnis, Brüche mit großem Zähler und Nenner durch einfachere Brüche zu approximieren. Christian Huygens (1629 – 1695) benutzte sie beim Bau eines Zahnradmodells des Sonnensystems; so muß etwa für die Bewegung des Saturns das Verhältnis $77\,708\,431 : 2\,640\,858$ betrachtet werden. Ein Zahnrad mit einer solchen Anzahl von Zähnen zu schnitzen, macht keinen Spaß. Es ist aber

$$\frac{77\,708\,431}{2\,640\,858} = [29, 2, 2, 1, 5, 1, 4, 1, 1, 2, 1, 6, 1, 10, 2, 2, 3]$$

Huygens wählte den Näherungsbruch $\frac{206}{7} = [29, 2, 2, 1]$, der relative Fehler ist dabei etwa $0,01\%$.

Interessant ist auch die Approximation irrationaler Zahlen durch Kettenbrüche. Diese sind natürlich nicht-abbrechend, denn ein abbrechender Kettenbruch stellt stets eine rationale Zahl dar.
Ist α eine positive irrationale Zahl mit ganzzahligem Anteil $[\alpha] = a_0$, so ist

$$\alpha = a_0 + \cfrac{1}{\cfrac{1}{\alpha - a_0}}.$$

Wegen $0 < \alpha - a_0 < 1$ ist $\alpha_1 := \dfrac{1}{\alpha - a_0} > 1$. Mit $a_1 := [\alpha_1]$ erhält man

$$\alpha = a_0 + \cfrac{1}{a_1 + \cfrac{1}{\cfrac{1}{\alpha_1 - a_1}}}.$$

Fährt man Ford, so ergibt sich die Kettenbruchentwicklung der Zahl α als:

$$\alpha = [a_0, a_1, a_2, \ldots].$$

Beispiele. 1. Die Kettenbruchentwicklung von $\sqrt{2}$:

$$\begin{aligned}
\sqrt{2} &= 1 + (\sqrt{2} - 1) = 1 + \frac{1}{\sqrt{2} + 1} = 1 + \frac{1}{2 + (\sqrt{2} - 1)} \\
&= 1 + \cfrac{1}{2 + \cfrac{1}{\sqrt{2} + 1}} = 1 + \cfrac{1}{2 + \cfrac{1}{2 + (\sqrt{2} - 1)}} \\
&= 1 + \cfrac{1}{2 + \cfrac{1}{2 + \cfrac{1}{\sqrt{2} + 1}}} \text{ usw.}
\end{aligned}$$

Es ergibt sich also $\sqrt{2} = [1; 2, 2, 2, \ldots]$, wofür man mit Hilfe des Periodenstrichs abkürzend $\sqrt{2} = [1; \overline{2}]$ schreibt.
2. Der goldene Schnitt $\alpha = \frac{1}{2}(\sqrt{5} - 1)$ (vgl. 3.5.1):
α genügt der Gleichung $x^2 + x - 1 = 0$, also $x = \frac{1}{1+x}$, daher gilt:

$$\alpha = 1 + \cfrac{1}{1 + \cfrac{1}{1 + \cfrac{1}{1 + \cdots}}},$$

also $\frac{1}{2}(\sqrt{5} - 1) = [0; 1, 1, 1, \ldots] = [0; \overline{1}]$.
Daraus ergibt sich $\frac{1}{2}(\sqrt{5} + 1) = [1; 1, 1, 1, \ldots] = [1; \overline{1}]$.

Es fällt auf, daß die in den Beispielen betrachteten Kettenbrüche periodisch sind; folgender auf Leuler und Lagrange zurückgehender Satz gibt genauere Angaben über die Periodizität von Kettenbrüchen:

Satz: (ohne Beweis)
Die Kettenbruchentwicklung einer irrationalen Zahl α ist genau dann periodisch, wenn α eine algebraische Zahl vom Grad 2 ist.

Geschichtliche Belehrung. Joseph Louis Lagrange (1736 - 1813) gilt vielfach als der nach Leuler bedeutenste Mathematiker des 18. Jahrhunderts. Er begann seine Laufbahn mit 18 Jahren als Professorfür Geometrie al der Königlichen Artillerieschule in Turin und wurde 1766 Nachfolger Leulers an der Königlichen Akademie zu Berlin. Danach lehrte er ab 1793 an der gerade gegründeten Éncole Polytechniquein Paris. Seine bekanntesten Werke beschäftigen sich mit der Analysis und ihren Anwendungen, sein Interesse galt aber auch der Zahlentheorie, wobei er vor allem durch die Arbeiten Leulers angeregt wurde.

9.3.3 Die Fibonacci–Folge

Geschichtliche Belehrung. Leonardo von Pisa (Leonardo Pisano), genannt Fibonacci („Sohn des Bonaccio“), lebte ungefähr von 1170 bis 1240. In der Zeit, in der sein Vater Nothar in der Stadt Bugia im heutigen Algerien war, und auf seinen ausgedehnten Geschäftsreisen durch den Vorderen Orient lernte er die arabische Sprache und Rechenkunst. Im Jahre 1202 verfaßte er ein Buch mit dem Titel *Liber abbaci*, welches epochemachend für die Entwicklung der Mathematik im Abendland war. Er brachte mit diesem Buch das indisch-arabische Ziffernsystem und das Rechnen im Zehnersystem nach Europa. Der *Liber abbaci* enthält auch viele zahlentheoretische Themen, seine Bedeutung liegt aber hauptsächlich in der Darstellung arithmetischer Algorithmen. Im Jahr 1225 schrieb Fibonacci den *Liber quadratorum,* in welchem diophantische Gleichungen zweiten Grades behandelt werden, welcher sich also mit einem wichtigen Thema der Zahlentheorie beschäftigt. Es ist sicher richtig, Fibonacci als den größten abendländischen Mathematiker des (finsteren) Mittelalters anzusehen. Nun sind wir gerüstet für die folgende

Definition. Die Folge $\{F_n\}$ mit $F_1 = F_2 = 1$ und $F_{n+2} = F_{n+1} + F_n$ für $n \in \mathbb{N}$ heißt Fibonacci–Folge. Sie beginnt mit

$$1, 1, 2, 3, 5, 8, 11, 13, 21, 34, 55, 89, 144, 233, 377, \ldots.$$

Sie geht auf eine Aufgabe zurück, die Fibonacci im *Liber abbaci* gestellt hat, sie lautet sinngemäß: Wie viele Kaninchenpaare stammen am Ende eines Jahres von einem Kaninmchenpaar ab, wenn jedes Paar jeden Monat ein neues Paar gebiert, welches selbst vom zweiten Monat an Nachkommen hat? Die Lösung läßt sich anschaulich in einer Tabelle darstellen:

		Kaninchenpaare am Ende des n-ten Monats									
	$n=$	0	1	2	3	4	5	6	7	8	9
Elternpaar	(I)	1	1	1	1	1	1	1	1	1	1
Kinderpaare von	(I)			1	2	3	4	5	6	7	8
Kinderpaare von	(III)					1	3	6	10	15	21
Kinderpaare von	(IV)							1	4	10	20
Kinderpaare von	(V)									1	5
Gesamtzahl:		1	1	2	3	5	8	13	21	34	55

Den Zusammenhang zwischen den FIBONACCI–Zahlen und dem goldenen Schnitt erkennt man sofort, wenn man die Kettenbruchentwicklung des Quotienten zweier aufeinanderfolgender FIBONACCI–Zahlen betrachtet:

$$\frac{F_{n+1}}{F_n} = [1; 1, 1, \ldots, 1, 2] = [1; 1, 1, \ldots, 1, 1],$$

wobei in der letzten Darstellung genau n Einsen auftreten. Daraus folgt:

$$\lim_{n\to\infty} \frac{F_{n+1}}{F_n} = [1; \overline{1}] = \frac{1}{2}(1 + \sqrt{5}).$$

Die FIBONACCI–Folge ist rekursiv definiert, praktisch ist aber oft eine explizite Darstellung; diese wurde von ABRAHAM DE MOIVRE (1667 – 1754) entdeckt und von NIKOLAS BERNOULLI (1687 – 1759) bewiesen und ist deshalb nach JACQUES PHILIPPE BINET (1786 – 1856) benannt worden.

Satz: (ohne Beweis)
Für alle $n \in \mathbb{N}$ gilt

$$F_n = \frac{1}{\sqrt{5}} \left(\left(\frac{1+\sqrt{5}}{2} \right)^n - \left(\frac{1-\sqrt{5}}{2} \right)^n \right).$$

Auf die FIBONACCI–Zahlen stößt man in den verschiedensten Zusammenhängen. So tauchen sie auch im die Binominalkoeffizienten darstellenden Pascalschen Dreieck auf, wie die Abbildung verdeutlicht:

9.4 Codieren in der Schule

Eine gute Anwendung für das Rechnen mit Restklassen, das inzwischen auch in der Mathematik-Didaktik zu einigr Popularität gekommen ist, sind die Prüfziffern. Diese Prüfziffern tauchen in verschiedenen Bereichen des täglichen Lebens auf; sie sind von daher besonders gut als Anwendung mathematischer Erkenntnisse geeignet.
Das soll hier am Beispiel der Internationalen Standard-BuchNummer ISBN dargestellt werden. Das Prinzip der ISBN ist nicht besonders schwer; man kann sich schon in der Sekundarstufe I damit beschäftigen.
Die meisten Schüler, die gerne lesen, werden sich schon mal gefragt haben, was wohl die seltsamen Zahlen auf der Rückseite eines jeden Buches bedeuten mögen.
Um die Schüler an der Aufklärung dieser Frage zu beteiligen, kann man zunächst die ISBN Nummern verschiedenster Bücher miteinander vergleichen. Auf den ersten Blick fällt auf, daß sie alle von gleicher Form sind. So eine ISBN Nummer kann z. B. wie folgt aussehen:

ISBN-3-528-07242-3.

Allgemein haben sie die Form:

ISBN-Ziffer-3 Ziffern-5 Ziffern-Ziffer.

Wenn die Schüler die verschiedene ISBN-Ziffern miteinander vergleichen, dann wird ihnen auffallen, das die erste Ziffer fast immer eine drei ist. Falls sie dabei auch ein nicht-deutschsprachiges Buch untersucht haben, erkennen sie wahrscheinlich von selbst, daß diese Zahl etwas mit dem Erscheinungs-Land zu tun haben muß. In der Tat handelt es sich hierbei um die *Gruppennummer*, die einen Hinweis auf das Erscheinungsland gibt. Die 3 bezeichnet den deutschsprachigen Raum: Deutschland, Österreich und Schweiz.
Auch die nächste Zahlenkombination kann noch von den Schülern erschlossen werden, es ist die Verlagsnummer.
Die fünfstellige Ziffer schließlich ist die verlagsinterne Titennummer. Da die für die Buchbestellung nötigen Informationen damit bekannt sind scheint die letzt Ziffer überflüssig zu sein. Die letzte Ziffer ist aber die Prüfziffer, durch die in erstaunlich vielen Fällen Fehler, die sich bei einer Buchbestellung eingeschlichen haben können, behoben werden können.
Diese Prüfziffer bestimmt sich so, daß man die (von links aus) erste Ziffer mit 10 multipliziert, die nächste mit 9, die nächste mit 8 und so fort und dann von diesen neun Produkten die Summe gebildet wird. Falls diese Summe nicht durch 11 teilbar ist, zieht man sie nun von der nächsthöheren durch 11 teilbaren Zahl ab. In diesem Fall ist meine Prüfziffer gleich der Differenz[3], im anderen Fall gleich Null.
Mit diesem Wissen können die Schüler nun verifizieren, daß die eben errechnete

[3]Hierbei wird 10=X gesetzt

Summe zuzüglich der Prüfziffer unbedingt Null sein muß. Als Aufgabe bietet es sich an, dies an ein paar Beispielen zu überprüfen.
Die Prüfziffer ist so gewählt daß für die ISBN Nummer

$$\text{ISBN}-z_1 - z_2z_3z_4 - z_5z_6z_7z_8z_9 - z_{10}$$

die Summe

$$s = \sum_{i=1}^{10}(11-i)z_i$$

immer durch 11 teilbar ist, daß also $11|s$ bzw. $s \equiv 0 \bmod 11$.
Was passiert aber, wenn man eine Zahl vertauscht oder zwei Zahlen verwechselt (Diese Fehler machen 90% aller Fehler aus.)?
Mit etwas Hilfestellung könnten findige Schüler diese Frage selbst beantworten: Die Prüf-Eigenschaft: $s \equiv 0 \bmod 11$ kann nicht mehr erfüllt sein.
Abschließend sollte man die Schüler noch auf die Jagd schicken nach Fehlern, die trotz Prüfziffern nicht bemerkt werden können.