Herbert Pieper

Zahlen aus Primzahlen

1974 Deutscher Verlag der Wissenschaften
MSB: Nr. 81
Abschrift und LaTex-Satz: 2023 https://mathematikalpha.de

Inhaltsverzeichnis

Vorwort

Dieses Büchlein stellt eine kurze Einführung in ein Teilgebiet der Mathematik, nämlich in die Arithmetik, in die Theorie der Zahlen dar. Hensel nannte es das "reinste und mathematischste Gebiet der Mathematik". Gauß sagte einmal, die Mathematik sei die Königin der Wissenschaften, die Zahlentheorie aber die Königin der Mathematik.

Carl Friedrich Gauß (30. April 1777-23. Februar 1855) selbst war es, der die Zahlentheorie als eine besondere mathematische Disziplin begründet hat.[1]
Er ist als Wunderkind in die Geschichte der Mathematik eingegangen. Schon als Kind zeigte er große Freude am numerischen Rechnen. Als er noch nicht drei Jahre alt war, sah er seinem Vater zu, wie dieser Lohnlisten für Bauarbeiter schrieb. Er machte dabei einen Rechenfehler, den sein Sohn entdeckte.
Gauß pflegte oft scherzhaft zu sagen, er habe früher rechnen, als sprechen können. Als Gauß und seine Mitschüler in der Schule einmal alle Zahlen von 1 bis 100 addieren sollten, schrieb der Neunjährige nach kurzer Zeit die Zahl 5050 auf seine Tafel. (Wie kam er so schnell auf das Ergebnis[2])

Als er vierzehn Jahre alt war, wurde der Herzog von Braunschweig auf ihn aufmerksam gemacht. Er gewährte die Mittel, die für die weitere Ausbildung dieses jugendlichen Talents erforderlich waren, und schickte ihn auf seine Kosten auf die höhere Schule und dann auf die Universität.
Gauß besuchte zunächst das Collegium Carolinum seiner Heimatstadt Braunschweig. Schon hier beschäftigte er sich intensiv mit der Mathematik, insbesondere mit der Zahlentheorie.

Mit 17 Jahren (im März 1795) entdeckte er induktiv das berühmte Quadratische Reziprozitätsgesetz. Im darauffolgenden Jahr - er ist inzwischen (im Oktober 1795) an der Universität zu Göttingen immatrikuliert worden - gibt er zwei Beweise für dieses zahlentheoretische Gesetz.
Im gleichen Jahre fand er, dass ein regelmäßiges Siebzehneck mit Zirkel und Lineal konstruierbar ist. Es ist somit möglich, mit Zirkel und Lineal den Umfang eines Kreises in 17 gleiche Abschnitte einzuteilen (also den Winkel $2\pi/17$ zu konstruieren).
Seit Euklids Zeiten kannte man die Konstruktion regelmäßiger Drei- und Fünfecke (und die daraus abzuleitenden Konstruktionen des 6-Ecks, 10-Ecks usw.). Doch es ist seit zwei Jahrtausenden den größten Mathematikern entgangen, was der junge Gauß durch Scharfsinn herausfand: die Konstruktion eben des regelmäßigen Siebzehnecks.

Es war der Morgen des 30. März 1796 - Gauß machte Osterferien in Braunschweig, er lag noch im Bett -, als ihm blitzartig (nach angestrengtem vergeblichem Nachdenken) die Erleuchtung kam, für welche Zahlen n die Teilung des Kreises in n gleiche Teile möglich ist.

Das regelmäßige n-Eck ist dann und nur dann mit Zirkel und Lineal konstruierbar, wenn n sich als Produkt

$$n = 2^k p_1 p_2 ... p_m$$

darstellen lässt, wobei $k \geq 1$, $m \geq 1$ sind und die Zahlen $p_1, ..., p_m$ verschiedene Primzahlen der Form

$$2^{2^l} + 1$$

[1] E. Worbs, C.F.Gauß. Ein Lebensbild. Leipzig 1955; C. F. Gauß-Gedenkband. Leipzig 1957; W.S. v. Waltershausen, Gauß zum Gedächtnis. Wiesbaden 1965 (Nachdruck der Leipziger Ausgabe von 1856).
[2] $1 + 2 + ... + 98 + 99 + 100 = (1 + 100) + (2 + 99) + ... + (50 + 51) = 50 \cdot 101 = 5050.$

sind. (Die einzigen solchen Primzahlen, die man kennt, sind $3 = 2+1$, $5 = 2^2+1$, $17 = 2^{2^2}+1$, $257 = 2^{2^3}+1$, $65537 = 2^{2^4}+1$. Ob es weitere gibt, ist noch ungewiss.)
Die Folge der regelmäßigen n-Ecke, die mit Zirkel und Lineal konstruierbar sind, beginnt also mit

$$n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, 20, 24, 30, ..., 257, ..., 65537, ...$$

Um die Ausführung der Konstruktion des 17-Ecks bemühte sich Gauß nicht. Er wurde vor allem von den geheimnisvollen Gesetzen im Reiche der Zahlen gefesselt.

Seine mathematische Arbeit galt auch weiterhin vorwiegend der Zahlentheorie. Die ersten Kapitel der "Disquisitiones arithmeticae" [3] entstanden. Zugleich lernte Gauß in der Universitätsbibliothek in Göttingen die Schriften seiner Vorgänger Fermat, Euler und Lagrange kennen.

Im Jahre 1798 beendet Gauß sein Studium in Göttingen. Kurz zuvor begann der Druck seiner "Disquisitiones", wurde aber mehrere Male ganz unterbrochen. Die "Disquisitiones arithmeticae" erschienen dann im Sommer 1801. Sie haben die Zahlentheorie als eine besondere mathematische Disziplin begründet.

War sie vor Gauß eine Sammlung von Einzelergebnissen (die ersten finden wir bereits bei den Pythagoreern (550 v. u. Z.)); so wurde sie jetzt zu einer geschlossenen Theorie zusammengefasst.
Das Werk galt zunächst als "unzugänglich und äußerst schwierig". Gauß' Nachfolger im Lehramt in Göttingen, Dirichlet, hat die "Disquisitiones arithmeticae" später durch seine Vorlesungen der mathematischen Welt erschlossen.
Die mitreißenden Vorlesungen Dirichlets sind auf eine große Anzahl von Zahlentheoretikern von größtem Einfluss gewesen, so auf Eisenstein, Kronecker, Riemann, Dedekind.

In den ersten vier Abschnitten des Werkes entwickelte Gauß systematisch und zusammenhängend die Grundlagen der Zahlentheorie. (Es gilt als sicher, dass er all dieses aus sich selbst heraus schon geschaffen hatte, noch ehe er die bereits von anderen Mathematikern, wie Euklid, Diophant, Fermat, Euler, Lagrange, Legendre in dieser Richtung erhaltenen Resultate studierte.)

Einiges davon wird man im ersten Kapitel dieses Büchleins kennenlernen. Dieses Kapitel, das man sorgfältig lesen muss, um die übrigen Teile zu verstehen, bringt einige Grundbegriffe der Zahlentheorie. Dabei werden die neuen zahlentheoretischen Aussagen stets bewiesen.
Oft wird man von ihrer Richtigkeit überzeugt sein und meinen, dass sie keiner Beweise mehr bedürfen. Man wird jedoch sehen, dass man erst nach dem Beweis sicher sein kann, dass die betreffenden Sätze richtig sind.
Beim ersten Lesen kann man durchaus einige Beweise übergehen und sich nur mit den Begriffsbildungen vertraut machen.

Der Kernbegriff ist der der Primzahl. Eine rationale Zahl r ist entweder eine Primzahl oder ein Produkt oder ein Quotient von Produkten von Primzahlen, also multiplikativ aus Primzahlen aufgebaut.
Bezeichnen wir die Primzahlen der Reihe nach mit $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, $p_4 = 7$, $p_5 = 11$, ..., so können wir jede Zahl r in der Form

$$r = p_1^{e_1} p_2^{e_2} p_3^{e_3} p_4^{e_4} p_5^{e_5} ...$$

[3] Disquisitiones arithmeticae (latein.) = Untersuchungen zur Arithmetik.

schreiben, worin die Exponenten e_i ganze (also auch negative) Zahlen sind. (Nur endlich viele der e_i sind von Null verschieden.)

Fixieren wir eine Primzahl und bezeichnen wir diese mit p, so können wir jede rationale Zahl r auch in der Form

$$r = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + ...$$

schreiben, worin die a_i ganze Zahlen sind. (Hier brauchen nicht nur endlich viele der a_i von Null verschieden zu sein.)
Eine solche Reihe (es ist eine unendliche Reihe) heißt p-adische Entwicklung der rationalen Zahl r. Die Folge der Koeffizienten a_0, a_1, a_2, ... ist dabei von einer bestimmten Stelle an periodisch.

Nimmt man nun beliebige solche Reihen (in denen die Folge der Koeffizienten a_i an den Potenzen von p nicht mehr notwendig periodisch zu sein braucht), so wird man zu den p-adischen Zahlen geführt.
Die Theorie der p-adischen Zahlen ist eine der großen zahlentheoretischen Neuschöpfungen von Hensel. Kurt Hensel (29. Dezember 1861-1. Juni 1941) gehört zu jenen großen Mathematikern, die gleich durch ihre erste Arbeit, ihre Doktorarbeit, Aufsehen erregten und sich einen Namen machten.

Er war Schüler von Kronecker. Ihm und Weierstraß (beide wirkten in Berlin) verdankte Hensel "wohl die hauptsächlichste Anregung für die Konzeption des Grundgedankens einer zahlentheoretischen Neuschöpfung".[4]

Bei Untersuchungen in einer anderen mathematischen Disziplin (der Theorie der rationalen Funktionen) schuf er (zwischen 1899 und 1913) mit den p-adischen Zahlen ein zahlentheoretisches Analogon zu den in jener Theorie auftretenden Potenzreihen.
Hensel setzte "kühn die formalen p-adischen Entwicklungen ... an, indem er einfach lehrte, wie man mit diesen neuartigen Gebilden aus einem bisher unbekannten Reservoir mathematischer Objekte rechnen und vergleichen sollte. Es handelt sich ... hier um eine echte, von Intuition und Phantasie eingegebene Neuschöpfung, die zunächst, wie jede revolutionierende Idee, lapidar und unbehauen hingeworfen wurde und ... zunächst des soliden logischen Fundaments entbehrte".

Die Henselsche p-adische Methode fand anfangs "von einem ganz kleinen Kreis begeisterter Schüler und Anhänger abgesehen, ... wenig Beachtung".
Zu den Wegbereitern der p-adik gehört Helmut Hasse[5]. Er ging 1921 nach Marburg, "um sich einer so ausgefallenen Sache wie der Henselschen p-adik ... zu widmen".
Er schreibt darüber:

"Ich kannte damals Hensel noch nicht, sondern hatte lediglich seine 'Zahlentheorie' in einem Antiquariat ... gesehen und, da sie sehr billig war, erworben. Bei der Lektüre bekam ich sofort den Eindruck von etwas sehr Schönem und Eigenartigem, das gerade dadurch seinen besonderen Reiz auf mich ausübte, dass ich es wegen der mangelnden Fundamentierung nicht von Grund aus verstand ...

Nachdem ich bei ihm (Hensel - d. Verf.) die Grundlagen der p-adik erlernt und von Grund aus verstanden hatte, lag mir klar vor Augen, welch mächtiges Instrument diese bisher eben nur in ihren Grundlagen entwickelte Methodik werden konnte, wenn man sie auf die höheren

[4] H. Hasse, Kurt Hensel zum Gedächtnis. Crelles J. 187 (1949), 1-13.
[5] Geb. 1898, em. Professor in Hamburg, Nationalpreisträger.

Probleme der algebraischen Zahlentheorie ... anwendete.....

Ich habe es immer als ein großes Glück empfunden, dass ich durch eigene und von mir angeregte Arbeiten dazu beitragen durfte, dem Lebenswerk meines verehrten Lehrers Hensel die ihm gebührende Anerkennung zu verschaffen.
Er selbst hat wohl gefühlt, wie wenig Geltung seine große Neuschöpfung, auf die er mit Recht stolz war, sich noch in den zwanziger Jahren erworben hatte, obwohl er sich nie darüber geäußert hat. Später hat er dann mit größter Freude und regster Anteilnahme an dem Aufstieg teilgenommen."

Hensel selbst sprach im Vorwort zu seiner "Zahlentheorie" "von der großen Freude ... welche" er "bei der mehrjährigen Beschäftigung mit diesen Fragen empfunden habe."

Von p-adischen Entwicklungen und p-adischen Zahlen handeln die Kapitel II und III dieses Büchleins. Die p-adischen Zahlen werden mathematisch exakt und einwandfrei definiert.
Wir lernen, wie man p-adische Zahlen addiert, subtrahiert, multipliziert, dividiert und wie man die Quadratwurzel ziehen kann. Das Problem des Quadratwurzelziehens führt in natürlicher Weise auf eines der schönsten Kapitel der elementaren Zahlentheorie, die Theorie der Quadratischen Reste, worüber man einiges erfahren wird.

So lernt man in diesem Büchlein einen mathematischen Begriff - den der p-adischen Zahl - kennen, der erst im 20. Jahrhundert entstanden ist und in den letzten Jahrzehnten in mehreren Gebieten der Mathematik von großer Bedeutung geworden ist.

Dieses Büchlein habe ich ausführlich geschrieben; es soll mit wenigen Vorkenntnissen verständlich sein. Doch oberflächlich lässt es sich nicht lesen. Man muss mit ihm arbeiten, die Abstraktionen und Schlüsse nachvollziehen, sich Schritt für Schritt die Kenntnisse aneignen, in den Stoff eindringen.

Es gibt keinen Königsweg zur Mathematik, sagte Euklid einst und meinte damit, dass auch für Könige der Weg zur Mathematik nicht bequemer gemacht werden kann. Möge dem Leser durch die Lektüre dieses Büchleins die Schönheit einer mathematischen Theorie bewusst werden.
Die ungarische Mathematikerin Rósza Peter sagte einmal[6]: "Nicht ich bin würdig, mich mit Mathematik zu befassen, sondern die Mathematik ist würdig, dass man sich mit ihr befasst ... ich zweifle nie daran, dass ich nichts Besseres und Schöneres tun könnte, als Mathematik zu treiben."

Ich möchte dem Herausgeber, Herrn Prof. Dr. Karl, für die Aufnahme der "Zahlen aus Primzahlen" in diese Reihe und für seine sehr wertvollen und zahlreichen Hinweise und Anregungen herzlich danken.
Mein Dank gilt ferner Herrn Dr. Boll, der das Entstehen des Büchleins wohlwollend gefördert hat, den Lektoren Frau Mai und Fräulein Arndt für die nützliche Hilfe und die freundlichen Gespräche, Inhalt und Form betreffend, und nicht zuletzt der Druckerei "Thomas Müntzer" für den hervorragenden Satz.

Berlin, Januar 1974 Herbert Pieper

[6] R. Peter, Die Mathematik ist schön. Math. in der Schule 2 (1964), 81.

1 Primzahlen

Die Zahlen

$$1, 2, 3, 4, 5, 6, 7, ...$$

heißen natürliche Zahlen. Die ersten unter diesen Zahlen lernt schon das Vorschulkind kennen. Es lernt zählen. Es spielt zuerst mit gewissen Mengen von Gegenständen, z. B. Bauklötzen.

Bald lernt es, die Elemente der einen Menge mit den Elementen einer anderen Menge zu vergleichen. Hat es rote und grüne Bausteinchen, so kann es, indem es etwa die roten auf die grünen legt, feststellen, von welcher Sorte es mehr hat. Liegt schon auf jedem grünen Klotz ein roter und sind noch rote übrig, so sieht es, dass eben mehr rote Steine da sind. Später geschieht das Zusammenzählen der Elemente der zu vergleichenden Mengen mit Hilfe der Zahlwörter.

Als naheliegendes Zählmaterial benutzt das Kind zuerst die Finger. Dann geht es über das Abzählen der zehn Finger hinaus und gelangt schließlich zu beliebig großen natürlichen Zahlen.

Über jede beliebig große Zahl kann man noch um eins weiterzählen.
Die Folge der natürlichen Zahlen ist also nicht endlich, es gibt keine größte natürliche Zahl; die Folge der natürlichen Zahlen ist unendlich. Die Anzahl der Elemente in jeder beliebigen Menge, die aus endlich vielen Dingen besteht, kann man daher mit einer natürlichen Zahl angeben. So ist 168 die Anzahl der Seiten dieses Büchleins.

Ein alter Schrank in Großmutters guter Stube habe 12 Schubfächer.
In einer Geldbörse seien 13 Münzen. Wenn alle diese Münzen auf die 12 Fächer verteilt werden, so dass wirklich in jedem Fach wenigstens eine Münze liegt, so gibt es ein Fach mit 2 Münzen. Sofern die Anzahl der Münzen größer ist als die Anzahl der Schubfächer, muss es immer mindestens ein Fach geben, in dem sich zwei Münzen oder mehr befinden, ganz gleich, wieviel Schubfächer vorhanden sind.

Bezeichnen wir mit n irgendeine natürliche Zahl, so können wir sagen: Sind n Schubfächer vorhanden und mindestens $n + 1$ Gegenstände (d.h. $n + 1$ Gegenstände oder mehr), die in diesen Fächern verteilt sind, dann ist mindestens ein Fach mit zwei Gegenständen da.
Ein Mensch hat nicht mehr als 150000 Haare auf dem Kopf.[7] Gibt es zwei Menschen, die die gleiche Anzahl auf dem Kopf haben ?

Um diese Frage zu beantworten, können wir im Prinzip wieder den "Schubfachschluss" anwenden, nämlich so: Auf der Erde leben wenigstens 2 Milliarden Menschen. Befände sich auf dem Kopf eines jeden Menschen eine unterschiedliche Anzahl Haare, so gäbe es wenigstens einen, tatsächlich sogar sehr viele Menschen, die mehr als 150000 Haare auf dem Kopf haben müssten, was aber nicht der Fall ist.

Dies ist ein indirekter Beweis. Wir haben die Gültigkeit der Behauptung ("Es gibt auf der Erde zwei Menschen, die die gleiche Anzahl Haare auf dem Kopf haben") dadurch bewiesen, dass wir zunächst ihr Gegenteil ("Auf dem Kopf eines jeden Menschen befindet sich eine unterschiedliche Anzahl Haare") als wahr angenommen haben, um dann zu demonstrieren, dass das Gegenteil gar nicht wahr sein kann (es gäbe nämlich Menschen, die mehr als 150000 Haare auf dem Kopf hätten).
Noch ein Beispiel für einen indirekten Beweis.

[7] Nach: Kleine Enzyklopädie "Natur", Leipzig 1957, S. 647 (Gesamtzahl der Haare auf dem Kopf: 830000 bis 140000).

Behauptung. Es gibt unendlich viele natürliche Zahlen.
Annahme. Es gibt nur endlich viele natürliche Zahlen.

Dies kann nicht wahr sein: Sei nämlich n die dann existierende größte größte natürliche Zahl. Man bilde $n+1$. Dies ist auch eine natürliche Zahl. Es müsste $n+1 < n$ sein (weil n die größte natürliche Zahl sein soll), also $n+2 < n+1$,d.h. $2 < 1$, was falsch ist. Daher die Annahme falsch, also die Behauptung richtig.

Man kann natürliche Zahlen addieren und erhält wieder natürliche Zahlen. Beim Abzählen addiert man immer die 1. Ist n eine beliebige natürliche Zahl, so kann man die Summe $n + n + ... + n$ bilden (hier mögen m Summanden stehen).
Man addiert m mal die Zahl n und bekommt als Summe mn; das ist das Produkt von m und n. Auch das Produkt zweier natürlicher Zahlen ist eine natürliche Zahl.

Folglich gibt es natürliche Zahlen, die sich als Produkt zweier Zahlen, die größer als 1 sind, darstellen lassen. Zum Beispiel sind 6, 60, 111 solche Zahlen; es ist nämlich $6 = 2{\cdot}3$, $60 = 4{\cdot}15$, $111 = 3 \cdot 37$.
Aber es existieren auch von 1 verschiedene natürliche Zahlen, die nicht ein solches Produkt sind, beispielsweise 2, 3 oder 37. Solche natürlichen Zahlen heißen Primzahlen.[8]

Die ersten Primzahlen, die kleiner als 10 sind, sind 2, 3, 5, 7. Man kann leicht weitere Primzahlen finden:

$$11, 13, 17, 19, 23, 29, 31, 37, ...$$

Natürliche Zahlen, die keine Primzahlen sind, heißen zusammengesetzte Zahlen. Sie sind also stets in ein Produkt zweier Zahlen, die größer als 1 sind, zerlegbar. Die Zerlegung in ein solches Produkt ist oft sogar auf verschiedene Weise möglich. So ist

$$60 = 2 \cdot 30 = 3 \cdot 20 = 4 \cdot 15 = 5 \cdot 12 = 6 \cdot 10$$

jedoch: besitzen $6 = 2 \cdot 3$, $111 = 3 \cdot 37$ nur diese eine Darstellung (natürlich kann man immer noch die Reihenfolge der Faktoren vertauschen, $6 = 2 \cdot 3 = 3 \cdot 2$).
In den folgenden Beispielen ist immer einer der beiden Faktoren eine Primzahl:

$$14 = 2 \cdot 7, 36 = 3 \cdot 12, 770 = 7 \cdot 110$$

Lässt sich jede Zahl, die keine Primzahl ist, in Form eines Produktes pa einer Primzahl p mit einer natürlichen Zahl a, die größer als 1 ist, schreiben ?
Es sind $144 = 12 \cdot 12$, $225 = 15 \cdot 15$ nicht in dieser Form dargestellt; dennoch sind auch diese Zahlen so darstellbar: $144 = 2 \cdot 72$, $225 = 5 \cdot 45$.

Können wir vermuten, dass das immer möglich ist? Es ist tatsächlich so. Hier ist der Beweis! Gegeben sei eine (beliebige) natürliche Zahl, die aber keine Primzahl sein soll. Wir bezeichnen sie mit m.

Dann ist m in der Form $m = ab = ba$ darstellbar, wobei $a > 1$, $b > 1$ ist (denn m soll eine zusammengesetzte Zahl sein). Hierbei ist natürlich $a < m$, $b < m$. Da es nur endlich viele natürliche Zahlen gibt, die kleiner als m sind (nämlich die Zahlen 1,2,3,...,$m-1$), ist m nur auf endlich viele verschiedene Arten als Produkt zweier Zahlen, die größer als 1 sind, darstellbar (denn jeder Faktor ist ja kleiner als m).
So ist $144 = 2 \cdot 72 = 3 \cdot 48 = 4 \cdot 36 = 6 \cdot 24 = 8 \cdot 18 = 9 \cdot 16 = 12 \cdot 12$.

[8] Warum die Zahl 1 nicht zu den Primzahlen rechnet, wird man später sehen.

Für die beliebige Zahl m schreiben wir nun alle diese Zerlegungen von m als Produkt zweier Zahlen größer als 1 auf. Unter den Faktoren gibt es eine kleinste Zahl (die mit p bezeichnet werde, so dass $m = pa$ ist). Diese Zahl p ist eine Primzahl!

Diese Behauptung lässt sich indirekt so beweisen: Wäre sie keine Primzahl, so wäre sie selbst Produkt zweier Zahlen größer als 1, also $p = cd$, $c > 1$, $d > 1$. Dann ist $c < p$, $d < p$. Es wäre $m = c(ad)$.
Die Zerlegungen von m in zwei Faktoren haben wir aber schon aufgeschrieben. Da p der kleinste aller Faktoren ist, muss $c > p$ sein. Dies widerspricht $c < p$.
Die Annahme, dass p keine Primzahl ist, ist falsch. Es ist $m = pa$ mit einer Primzahl p und einer natürlichen Zahl $a > 1$. Wir können unsere Erkenntnisse in dem folgenden Satz zusammenfassen.

Satz 1. Jede natürliche Zahl n lässt sich in der Form

$$n = pa$$

schreiben, wobei p eine Primzahl und a wieder eine natürliche Zahl ist.

Für natürliche Zahlen $n = m$, die keine Primzahlen sind, gilt der Satz. Dann ist sogar $a > 1$. Ist $n = p$ Primzahl, so ist Satz 1 selbstverständlich auch richtig $(a = 1)$.

Betrachten wir noch einmal das Beispiel $144 = 2 \cdot 72$. Es ist auch $72 = 2 \cdot 36$, $36 = 2 \cdot 18$, $18 = 2 \cdot 9$, $9 = 3 \cdot 3$, $3 = 3 \cdot 1$, zusammengefasst $144 = 2 \cdot 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3$. Die Zahl 144 ist ein Produkt von Primzahlen.

Ist jede zusammengesetzte Zahl m als ein Produkt von Primzahlen darstellbar? Natürlich!
Hat nämlich die natürliche Zahl m die Form eines Produktes, $m = pa$ (p Primzahl), und ist $a > 1$, so lässt sich auch a in einer solchen Form schreiben, $a = qb$ (q Primzahl).
Ist noch $b > 1$, so gilt das gleiche für b: $b = rc$ (r Primzahl).
Diesen Prozess der Zerlegung setzen wir nun fort.

Irgendwann gibt es aber keine Zerlegung in ein Produkt einer Primzahl mit einer Zahl größer 1 mehr, sondern nur noch eine Zerlegung in das Produkt einer Primzahl mit der Zahl 1. Es ist nämlich

$$\begin{aligned} m &= pa \quad (a > 1), \\ a &= qb \quad (b > 1), \\ b &= rc \quad (c > 1), ... \end{aligned}$$

also $a < m$, $b < a$, $c < b$, ..., d.h. $m > a > b > c > ... \geq 1$. Es gibt aber nur endlich viele natürliche Zahlen, die kleiner als m sind. Diese Folge a, b, c,... von natürlichen Zahlen, von denen die folgende Zahl sogar stets kleiner als die vorhergehende ist, muss daher abbrechen:

$$m > a > b > c > ... > e > f > g = 1$$

Es ist noch $e = tf$ $(f > 1)$ mit einer Primzahl t, aber schon $f = ug$ mit einer Primzahl u und $g = 1$. Wäre immer wieder der zweite Faktor > 1, so gäbe es zu jeder natürlichen Zahl zwischen m und 1 eine weitere, d.h., die obige Folge

$$m > a > b > c > ... > 1$$

enthielte unendlich viele Zahlen, was aber nicht sein kann. Es gibt also tatsächlich einmal einen zweiten Faktor $g = 1$.

Dann ist $m = pqr...tu$ Produkt der Primzahlen $p, q, r, ..., t, u$. Jede zusammengesetzte Zahl ist also als ein Produkt von Primzahlen darstellbar.

Beispiel.

$$4620 = 2 \cdot 2310, \quad 2310 = 2 \cdot 1155, \quad 1155 = 3 \cdot 385, \quad 385 = 5 \cdot 77,$$
$$77 = 7 \cdot 11, \quad 11 = 11 \cdot 1, \qquad 4620 = 2 \cdot 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11$$

Satz 2. Jede natürliche Zahl ist Produkt von (endlich vielen) Primzahlen. Diese sind nicht notwendig verschieden.

Ist eine Zahl nicht selbst Primzahl, so kann man sie also schrittweise in Faktoren so zerlegen, bis alle Faktoren Primzahlen sind. Das kann auf verschiedene Art geschehen. So ist z. B. auch

$$4620 = 11 \cdot 420 = 11 \cdot 5 \cdot 84 = 11 \cdot 5 \cdot 2 \cdot 42 = 11 \cdot 5 \cdot 2 \cdot 7 \cdot 6 = 11 \cdot 5 \cdot 2 \cdot 7 \cdot 3 \cdot 2$$

(und dieser Weg zur Zerlegung in ein Produkt von Primzahlen ist ein anderer als oben). Ist eine Zahl als Produkt von Primzahlen dargestellt, so kann man diese Primfaktoren (die Faktoren heißen Primfaktoren, weil sie Primzahlen sind) in beliebiger Reihenfolge anordnen. Doch abgesehen von dieser Willkür in der Anordnung führen die verschiedenen Wege der Zerlegung immer zur gleichen Primfaktorzerlegung der Zahl.

Satz 3. Die nach Satz 2 stets existierende Darstellung als Produkt von endlich vielen (nicht notwendig verschiedenen) Primzahlen ist überdies, von der willkürlichen Reihenfolge der Faktoren abgesehen, die einzige solche Darstellung.

(Diese eindeutige Darstellung heißt Primzahlzerlegung.)
Dass jede Zahl eine Primzahlzerlegung besitzt, folgt aus Satz 2. Dass diese Zerlegung aber eindeutig ist, ist durchaus nicht selbstverständlich, so naheliegend auch die Behauptung auf den ersten Blick erscheint. Der Beweis erfolgt wieder indirekt.

Wir nehmen an, dass es eine natürliche Zahl gibt, die wenigstens zwei (verschiedene) Zerlegungen besitzt[9], und leiten aus dieser Annahme einen Widerspruch her. Dieser Widerspruch zeigt, dass die Annahme falsch ist, dass folglich jede Zahl nur eine Zerlegung besitzt.

Angenommen also, die Zerlegung in Primfaktoren ist nicht für alle Zahlen eindeutig. Dann müsste es eine Zahl geben, die mindestens zwei Zerlegungen besitzt. Unter allen solchen Zahlen gibt es eine kleinste. Wir bezeichnen sie mit k.
Die Zahl k hat also wenigstens zwei verschiedene Zerlegungen in Primfaktoren. Mit p bezeichnen wir den kleinsten in k auftretenden Primfaktor. Es ist $k = pl$. Die natürliche Zahl l ist kleiner als k und daher eindeutig zerlegbar (da nämlich k als kleinste Zahl mit zwei - oder mehr - Zerlegungen gewählt wurde, besitzt jede Zahl, die kleiner als k ist, nur eine Zerlegung):

$$l = p_1 p_2 ... p_r$$

Eine zweite, von der ersten verschiedene Zerlegung von k kann den Faktor p nicht enthalten. Hätte k nämlich noch die Zerlegung $k = pl'$, so wäre $pl = pl'$, also $l = l'$, und da $l = l'$ nur eine Zerlegung besitzt, wären die beiden Zerlegungen von k einander gleich.

Es sei nun q ein in einer zweiten Zerlegung von k auftretender Primfaktor. Dann ist $q > p$ (weil p der kleinste in k überhaupt auftretende Primfaktor ist). Es sei $k = qu$.

[9] Die natürliche Zahl soll also mindestens zwei Zerlegungen besitzen, die sich nicht nur in der Reihenfolge der Faktoren unterscheiden, sondern auch unterschiedliche Primzahlen enthalten.

Die natürliche Zahl u ist kleiner als k und daher eindeutig zerlegbar: $u = q_1 q_2 ... q_s$. Diese Primzahlen $q_1, ..., q_s$ sind alle von p verschieden. Wir bilden die Zahl

$$k' = k - pu$$

Einerseits ist $k = pl$, also $k' = pl - pu = p(1-u)$, andererseits ist $k = qu$, also $k = qu - pu = (q-p)u$.
Wegen $q > p$ ist $k = (q-p)u$ eine natürliche Zahl. Sie ist wegen $k' = k - pu$ kleiner als k, besitzt also eine eindeutige Primfaktorzerlegung. Auch die Faktoren $l-u$, $q-p$ sind natürliche Zahlen, die kleiner als k sind, besitzen also auch eindeutige Primfaktorzerlegungen.

Wegen $k' = p(1-u)$ kommt in der Zerlegung von k' der Primfaktor p vor. Wegen $k' = (q-p)u$ muss daher der Primfaktor p auch in der Zerlegung von $q-p$ oder in der Zerlegung von u vorkommen (weil die Zerlegung von k' in Primfaktoren eindeutig ist).
In der Zerlegung $u = q_1 q_2 ... q_s$ kommt p nicht vor (denn die $q_1, ..., q_s$ sind sämtlich von p verschieden) Es müsste also p in der Zerlegung von $q-p$ vorkommen, also $q - p = ph$ (mit einer natürlichen Zahl h), d.h. $q = p(h+l)$ sein.
Hiernach wäre q eine zusammengesetzte Zahl.

Die Zahl q ist aber eine Primzahl (q sollte ja ein in einer zweiten Zerlegung von k auftretender Primfaktor sein). Die Zahl q wäre demnach sowohl Primzahl als auch zusammengesetzte Zahl, was unsinnig ist.

Dieser Widerspruch zeigt, dass die Annahme der Existenz einer Zahl mit zwei wesentlich verschiedenen Primfaktorzerlegungen unhaltbar ist, dass somit die Zerlegung in Primzahlen eindeutig ist (abgesehen von der unwesentlichen Reihenfolge der Faktoren). Das war zu beweisen.

Würde man die Zahl 1 zu den Primzahlen hinzunehmen, so würde Satz 3 nicht mehr gelten. Dann wären z.B. $1 \cdot 3 \cdot 37$ und $1 \cdot 1 \cdot 3 \cdot 37$ zwei verschiedene Primfaktorzerlegungen von 111. Wir zerlegen zur Übung noch einmal eine Zahl in Primfaktoren.

Beispiel.

$$\begin{aligned} 21420 &= 2 \cdot 10710 = 2 \cdot 2 \cdot 5355 = 2 \cdot 2 \cdot 3 \cdot 1785 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 595 \\ &= 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 119 = 2 \cdot 2 \cdot 3 \cdot 3 \cdot 5 \cdot 7 \cdot 17 \\ \text{kürzer} \quad 21420 &= 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 17 \end{aligned}$$

In dem Beispiel haben wir gleiche Primfaktoren zu Potenzen zusammengefasst. Dies kann man ja stets tun. Für jede natürliche Zahl n gewinnt man so eine (bis auf die Reihenfolge der Faktoren eindeutige) Darstellung

$$n = p_1^{a_1} \cdot ... \cdot p_r^{a_r}$$

als Potenzprodukt endlich vieler verschiedener Primzahlen $p_1, ..., p_r$ mit Exponenten $a_1, ..., a_r$ (die natürliche Zahlen sind). Man könnte übrigens die Reihenfolge der Primzahlpotenzfaktoren eindeutig festlegen, indem man vorschreibt, dass $p_1 < p_2 < ... < pr$ sein soll.

Aus der Folge aller Primzahlen treten immer nur endlich viele als Primfaktor in einer gegebenen natürlichen Zahl auf. Ist die Folge aller Primzahlen

$$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, ...$$

endlich, oder ist sie unendlich? Hören die Primzahlen irgendwo auf, gibt es eine größte Primzahl oder nicht?

Wir müssten uns einfach einmal eine Primzahltabelle anlegen, eine Tafel, in der wir alle Primzahlen bis zu einer gegebenen Zahl aufschreiben. Dann würden wir sehen, dass die Primzahlen immer seltener werden:
Zwischen 1 und 100 gibt es mehr Primzahlen als zwischen 101 und 200 usw. Bis 10 gibt es 4 Primzahlen, bis 100 gibt es 25, bis 1000 gibt es 168, bis 10000 gibt es 1229. Hören die Primzahlen vielleicht doch irgendwo auf?

Wie kann man eine Primzahltafel am schnellsten aufstellen?
Jede einzelne Zahl auf ihre Zerlegbarkeit in kleinere Faktoren zu überprüfen ist recht mühsam.

Ein berühmtes Beispiel für die Schwierigkeit, eine Primzahl zu erkennen, ist das der Zahl $2^{32}+1 = 4294967297$ (man multipliziert 32 mal die 2 mit sich selbst und addiert 1); diese Zahl hielt Fermat[10] für eine Primzahl, erst Euler[11] fand, dass sie zusammengesetzt ist: $641 \cdot 6700417$.

Das folgende Verfahren ist einfacher. Mit ihm lassen sich alle Primzahlen unterhalb einer gegebenen Zahl n auffinden.[12] Es werde hier für den Fall $n = 77$ beschrieben.
Wir schreiben uns die Zahlen von 2 bis 77 auf. Die erste Zahl ist 2. Jede zweite Zahl nach 2 ist ein Vielfaches von 2 (nämlich 4, 6, 8, 10, ...) und somit keine Primzahl. Diese Zahlen streichen wir durch.
Die erste Zahl nach 2, die nicht gestrichen wird, ist 3. Jede dritte Zahl nach 3 ist ein Vielfaches von 3 (nämlich 6, 9, ...) und daher keine Primzahl. Wir streichen auch diese Zahlen aus; nun sind einige Zahlen (nämlich die Vielfachen von 2 und 3) schon doppelt durchgestrichen:

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~
17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ 25 ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~ 31
~~32~~ ~~33~~ 34 35 ~~36~~ 37 ~~38~~ ~~39~~ ~~40~~ 41 ~~42~~ 43 ~~44~~ ~~45~~ ~~46~~
47 ~~48~~ 49 ~~50~~ ~~51~~ ~~52~~ 53 ~~54~~ 55 ~~56~~ ~~57~~ ~~58~~ 59 ~~60~~ 61
~~62~~ ~~63~~ ~~64~~ 65 ~~66~~ 67 ~~68~~ ~~69~~ ~~70~~ 71 ~~72~~ 73 ~~74~~ ~~75~~ ~~76~~ 77

Jetzt kämen alle Vielfachen von 4 dran, aber diese sind auch Vielfache von 2, also bereits gestrichen. Die erste noch nicht gestrichene Zahl nach 3 ist 5. Jede fünfte Zahl nach 5 ist ein Vielfaches von 5 (nämlich 10, 15, 20,....) und daher keine Primzahl.
Diese Zahlen streichen wir auch wieder durch. Schließlich streichen wir von 7 an jede siebente Zahl (also 14, 21, ...) durch:

2 3 ~~4~~ 5 ~~6~~ 7 ~~8~~ ~~9~~ ~~10~~ 11 ~~12~~ 13 ~~14~~ ~~15~~ ~~16~~
17 ~~18~~ 19 ~~20~~ ~~21~~ ~~22~~ 23 ~~24~~ ~~25~~ ~~26~~ ~~27~~ ~~28~~ 29 ~~30~~ 31
~~32~~ ~~33~~ ~~34~~ ~~35~~ ~~36~~ 37 ~~38~~ ~~39~~ ~~40~~ 41 ~~42~~ 43 ~~44~~ ~~45~~ ~~46~~
47 ~~48~~ ~~49~~ ~~50~~ ~~51~~ ~~52~~ 53 ~~54~~ ~~55~~ ~~56~~ ~~57~~ ~~58~~ 59 ~~60~~ 61
~~62~~ ~~63~~ ~~64~~ ~~65~~ ~~66~~ 67 ~~68~~ ~~69~~ ~~70~~ 71 ~~72~~ 73 ~~74~~ ~~75~~ ~~76~~ ~~77~~

Will man nun alle Vielfachen von 11 (nämlich 22, 33, 44, 55, 66, 77), von 13 (26, 39, 52, 65), von 17 (34, 51, 68), von 19 (38, 57,76), von 23 (46, 69), von 29 (58), von 31 (62), von 37

[10] Pierre de Fermat (1601-1665), französischer Zahlentheoretiker, der auch der Infinitesimal- und vor allem der Wahrscheinlichkeitsrechnung wichtige Impulse gab.

[11] Leonhard Euler (1707-1783), schöpferischer genialer Schweizer Mathematiker, der 886 mathematische Bücher und Aufsätze schrieb; ging 1727 nach Petersburg, 1741 an die Akademie de: Wissenschaften nach Berlin, 1766 erneut nach Petersburg.

[12] Das Verfahren heißt "Sieb des Eratosthenes" nach dem kyrenischen Mathematiker und Geographen Eratosthenes (275? bis 194? v. u. Z.), der wohl als erster auf diese Art und Weise alle Primzahlen $< n$ aussiebte. (Durch ihn erfolgte übrigens die erste Berechnung des Erdumfangs.)

(74) streichen, so bemerkt man, dass diese Zahlen bereits gestrichen sind. Wir können also aufhören.

Die nicht gestrichenen Zahlen sind Primzahlen, und das sind alle Primzahlen bis 77:

$$2, 3, 5, 711, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73$$

So kann man es mit jeder sogar beliebig großen Zahl n machen; man streicht zunächst alle geraden Zahlen >2, dann alle echten Vielfachen von 3, alle echten Vielfachen von 5 usw., bis schließlich nur noch Primzahlen stehen bleiben.
Gerade bei großen Zahlen - da, wo die Überprüfung, ob eine Zahl zerlegbar ist oder nicht, besonders schwierig ist - zeigt sich erst die Überlegenheit dieses Verfahrens gegenüber der Einzelnachprüfung. Wann man allgemein mit dem Durchstreichen aufhören kann, zeigt die folgende Überlegung.

Es sei m eine natürliche Zahl. Ist m nicht Vielfaches einer Primzahl p, für die $p^2 < m$ ist, so ist m eine Primzahl. (Die Zahl 37 ist nicht Vielfaches von 2, 3, 5, also ist 37 eine Primzahl. 2, 3, 5 sind ja die einzigen Primzahlen p mit $p^2 < 37$; schon $7^2 = 49$ ist größer als 37).

Angenommen, m wäre keine Primzahl, so schreibe man die Primzahlzerlegung von m auf: $m = p_1 p_2 ... p_r$ ($r \geq 2$). Da m nicht Vielfaches einer Primzahl p ist, für die $p^2 \leq m$ ist, gilt $p_1^2 > m$, $p_2^2 > m$, ..., $p_r^2 > m$, also

$$m^2 = p_1^2 p_2^2 \cdot ... \cdot p_r^2 > mm...m = m^r$$

was nur mit $r < 2$ möglich ist. Wir erhalten den Widerspruch $2 > r \leq 2$, d.h. $2 > 2$. Also ist die Annahme falsch, d.h., m ist tatsächlich Primzahl.

Beispiel. Alle Zahlen bis 77 enthalten in ihrer Primzahlzerlegung eine Primzahl, die kleiner oder gleich 7 ist (es ist $7^2 < 77$, aber $11^2 > 77$). Alle Zahlen bis $10000 = 100^2$ enthalten in ihrer Primzahlzerlegung eine Primzahl, die kleiner als 100 ist.
Um also die Primzahlen bis 10000 zu finden (es sind 1229), brauchen wir in der Folge aller Zahlen bis 10000 nur die Vielfachen der ersten 25 Primzahlen zu streichen.

Um nach dem angegebenen Verfahren alle Primzahlen unterhalb einer gegebenen Zahl n anzugeben, schreibt man sich also alle Zahlen von 2 bis n auf und streicht nacheinander alle echten Vielfachen von $2, 3, 5, 7, ..., p$ durch. Die letzte der Streichung zugrundeliegende Primzahl p ist die größte Primzahl, für welche gerade noch $p^2 \leq n$ ist (während das Quadrat der folgenden Primzahl bereits größer als n ist).

Jetzt fällt es uns nicht schwer, eine Primzahltafel aufzustellen, in der alle Primzahlen bis zu einer vorgegebenen Zahl stehen.
Zu Beginn unseres Jahrhunderts tabellierte der Mathematiker D.N. Lehmer alle Primzahlen, die kleiner sind als 10 Millionen.
Im Jahre 1959 stellten Baker und Gruenberger einen Mikrofilm her, der die ersten 6 Millionen Primzahlen enthält.

Bezeichnet p_k die k-te Primzahl, so ist beispielsweise $p_1 = 2$, $P_{10} = 29$, $p_{100} = 541$, $p_{1000} = 7917$, $p_{6000000} = 104395301$.
Es gibt 168 Primzahlen zwischen 1 und 1000, 135 zwischen 1000 und 2000, 127 zwischen 2000 und 3000, 120 zwischen 3000 und 4000 und 119 zwischen 4000 und 5000.
Die Primzahlen werden immer seltener. Aufgrund der Zahl $p_{6000000}$ kann man ausrechnen, dass je 1000 aufeinanderfolgende Zahlen bis 104 Millionen im Durchschnitt nur 58 Primzahlen

enthalten.

Es gibt aber in der Menge aller natürlichen Zahlen sogar beliebig lange (aber endliche) Folgen aufeinanderfolgender natürlicher Zahlen, in denen keine einzige Primzahl vorkommt!
Für eine beliebige (insbesondere eben recht große) Zahl n bilden wir einmal das Produkt der ersten $n+1$ natürlichen Zahlen,

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot ... \cdot (n-1)n(n+1)$$

und addieren nacheinander $2, 3, 4, ..., n, n+1$; dann ist nämlich

$$\begin{aligned}
&1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot ... \cdot (n-1)n(n+1) + 2 \\
&1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot ... \cdot (n-1)n(n+1) + 2 \\
&1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot ... \cdot (n-1)n(n+1) + 2 \\
&... \\
&1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot ... \cdot (n-1)n(n+1) + n \\
&1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdot ... \cdot (n-1)n(n+1) + n + 1
\end{aligned}$$

eine Folge von n aufeinanderfolgenden natürlichen Zahlen, in der keine Primzahl vorkommt.

Beispiel. Unter den 1000 Zahlen zwischen $1 \cdot 2 \cdot 3 \cdot ... \cdot 1001 + 2$ und $1 \cdot 2 \cdot 3 \cdot ... \cdot 1001 + 1001$ ist keine Primzahl. In der Tat, es ist

$$\begin{aligned}
&1 \cdot 2 \cdot 3 \cdot ... \cdot n(n-1) + 2 = 2a_1 && \text{mit } a_1 = 3 \cdot 4 \cdot ... \cdot (n+1) + 1 \\
&1 \cdot 2 \cdot 3 \cdot ... \cdot n(n-1) + 3 = 3a_2 && \text{mit } a_2 = 2 \cdot 4 \cdot ... \cdot (n+1) + 1 \\
&... \\
&1 \cdot 2 \cdot 3 \cdot ... \cdot n(n-1) + (n+1) = (n+1)a_n && \text{mit } a_n = 2 \cdot 3 \cdot ... \cdot n + 1
\end{aligned}$$

also ist jede Zahl Produkt zweier natürlicher Zahlen größer als 1.

Gibt es nun unendlich viele Primzahlen oder nicht? Die
Existenz von 455052512 Primzahlen bis zu 10 Milliarden hin, wie sie nach der nebenstehenden Tabelle feststeht, besagt natürlich logisch nichts darüber, ob auch nur eine einzige weitere Primzahl existiert, und schon gar nichts, ob die Folge der Primzahlen unendlich ist.

Tabelle 1[13]

n	Anzahl der Primzahlen zwischen 1 und n
10	4
100	25
1000	168
10000	1229
100000	9592
1000000	78498
10000000	664579
100000000	5761455
1000000000	50847534
10000000000	455052512

[13] Die letzten beiden Werte in dieser Tabelle wurden von D. H. Lehmer 1959 mit Hilfe elektronischer Rechenmaschinen gefunden. Tatsächlich kennt man nämlich nicht alle 455052512 Primzahlen bis 10000000000 ($= 10^{10}$).

Wenn wir in dem Ausdruck $n^2 - n + 41$ für n nacheinander die natürlichen Zahlen 1, 2, 3, 4, 5 einsetzen, so erhalten wir 41, 43, 47, 53, 61, und dies sind alles Primzahlen.
Ist das etwa immer so? Setzen wir weiter 6, 7, 8, ..., 39, 40 ein, so erhalten wir 71, 83, 97, 113, 131, ..., 1523, 1601. Auch dies sind Primzahlen.

Dürfen wir jetzt annehmen, dass der obige Ausdruck für jede natürliche Zahl n eine Primzahl ist? Nein!
Schon $41^2 - 41 + 41 = 41^2$ ist Quadrat von 41, also keine Primzahl. Man darf also nicht einfach von 5 oder 6 oder 10 oder 40 auf unendlich schließen.

Unter den ersten 10 Milliarden natürlichen Zahlen gibt es über 450 Millionen Primzahlen. Doch was sind 10 Milliarden gegen die unendliche Folge aller natürlichen Zahlen!
Es könnte ja sein, dass es danach keine einzige Primzahl mehr gibt. Dass dies tatsächlich nicht so ist, dass es nämlich zu jeder noch so großen natürlichen Zahl n eine Primzahl gibt, die größer ist als n, dass es also unendlich viele Primzahlen gibt, soll jetzt bewiesen werden. Das ist gar nicht so schwer.

Der schöne Beweis des folgenden Satzes geht auf Euklid[14] zurück.

Satz 4. Es gibt unendlich viele Primzahlen.

Beweis. Wir bilden aus den ersten bekannten Primzahlen $2, 3, 5, 7, 11, 13, 17, ...$ nacheinander die Zahlen

$$\begin{aligned} 2 + 1 &= 3, \\ 2 \cdot 3 + 1 &= 7, \\ 2 \cdot 3 \cdot 5 + 1 &= 31, \\ 2 \cdot 3 \cdot 5 \cdot 7 + 1 &= 211, \\ 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 &= 2311, \\ 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 + 1 &= 30031, \\ 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 + 1 &= 510511, \quad \text{usw.} \end{aligned}$$

$3, 7, 31, 211, 2311$ sind wieder Primzahlen, jedoch ist $30031 == 59 \cdot 509$ keine Primzahl, sondern Produkt der Primzahlen 59 und 509. Wir haben zu den gegebenen Primzahlen neue gefunden.

Aus 2 erhielten wir 3, aus 2 und 3 ergab sich 7, aus 2, 3, 5 also 31, aus 2, 3, 5, 7 schon 211, aus 2, 3, 5, 7, 11 bereits 2311, aber aus 2, 3, 5, 7, 11, 13 beispielsweise 59. Wesentlich ist, dass die neu erhaltenen Primzahlen von den links aufgeschriebenen jeweils verschieden sind.

Ist 510511 eine Primzahl? Nach Satz 1 lässt sich 510511 sicher in Form eines Produktes pa mit einer Primzahl p und einer natürlichen Zahl $a > 1$ darstellen.
Diese Primzahl p muss aber von 2, 3, 5, 7, 11, 13, 17 verschieden sein. Dividieren wir 510511 durch p, so erhalten wir a, und es bleibt kein Rest. Dividieren wir aber

$$510511 = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 13 \cdot 17 + 1$$

durch eine der Primzahlen 2, 3, 5, 7, 11, 13, 17, so bleibt als Rest 1. Also ist p eine von 2,3,5,7,11,13,17 verschiedene Primzahl.

[14] Euklid (um 300 v.u.Z.), griechischer Mathematiker. In seinem Lehrbuch "Elemente" gab dieser bedeutende Mathematiker erstmalig der Mathematik einen streng wissenschaftlichen Aufbau.

Nehmen wir einmal an, es gäbe eine letzte, eine größte Primzahl (sie ist gewiss eine große Zahl). Wir bezeichnen sie mit q. Dann schreiben wir die endlich vielen Primzahlen bis q auf:

$$2, 3, 5, 7, 11, ..., q$$

Jetzt bilden wir ihr Produkt, addieren 1 und bezeichnen das Resultat mit n:

$$n = 2 \cdot 3 \cdot 5 \cdot 11 \cdot q + 1$$

Diese Zahl n kann eine Primzahl sein oder nicht; in jedem Fall lässt sie sich in der Form pa schreiben, wobei p eine Primzahl und a eine natürliche Zahl ist.[15] Diese Primzahl p ist aber von 2, 3, 5, 7, 11, ..., q verschieden, weil man n ohne Rest durch p dividieren kann, jedoch die Division von n durch eine der Primzahlen 2, 3, 5, 7, 11, ..., q den Rest 1 lässt:

$$\begin{aligned} n &= (3 \cdot 5 \cdot ... \cdot q)2 + 1 \\ n &= (2 \cdot 5 \cdot ... \cdot q)3 + 1 \\ &... \\ n &= (2 \cdot 3 \cdot ... \cdot (q-1))q + 1 \end{aligned}$$

Dies ist ein Widerspruch, denn die endliche Folge 2, 3, 5, 7, ..., q sollte schon alle Primzahlen enthalten. Also ist die Annahme falsch. Zu jeder vorgelegten Menge von Primzahlen gibt es eine weitere. Die Folge der Primzahlen bricht nicht ab, was zu beweisen war.

In diesem Beweis haben wir natürliche Zahlen dividiert. Sind a und b natürliche Zahlen, so ist ihr Quotient $\frac{a}{b}$ im allgemeinen eine gebrochene Zahl: $\frac{1}{3}$, $\frac{11}{4}$, $\frac{5}{8}$, $\frac{10}{9}$. Die Zahl $\frac{a}{b}$ heißt echter Bruch, falls $a < b$ ist; - heißt unechter Bruch, falls $a \geq b$ ist.

Es sei $r = \frac{a}{b}$ ein unechter Bruch. Die größte natürliche Zahl $\geq r$ bezeichnet man mit $[r]$. Es ist $[r] \geq 1$. Wir setzen $[r] = 0$, falls r ein echter Bruch ist.

Beispiel.
$\left[\frac{11}{4}\right] = 2$, weil $2 < \frac{11}{4}$, aber $\frac{11}{4} < 3$.
$\left[\frac{10}{9}\right] = 1$, weil $1 < \frac{10}{9}$, aber $\frac{10}{9} < 2$.
$\left[\frac{1}{5}\right] = 0$, weil $\frac{1}{5}$ ein echter Bruch (und tatsächlich $0 < \frac{1}{5} < 1$.

Es sei $\frac{a}{b}$ ein Bruch und $q = \left[\frac{a}{b}\right]$. Dann ist $q \leq \frac{a}{b} < q + 1$, anders geschrieben also

$$qb \leq a < (q+1)b$$

$qb \leq a$ bedeutet, dass es eine Zahl $r \geq 0$ gibt, die, wenn man sie zu qb addiert, gerade a ergibt, also $a = qb + r$, wobei $r \geq 0$ ist, und $a < (q+1)b$ besagt, dass $r < b$ sein muss (wäre $r > b$, so müsste $r = a - qb \geq b$ sein, d.h. $a \geq b + qb = (q+1)b$, was $a < (q+1)b$ widerspricht). Es ist also

$$a = qb + r \qquad \text{mit} \qquad 0 \leq r < b \tag{1}$$

Dividiert man a durch b, so ergibt sich als Quotient gerade dieses $q = \frac{a}{b}$, und es bleibt als Rest ein r mit $0 \leq r < b$.

Beispiel.
$\left[\frac{21}{5}\right] = 4$, $21 = 4 \cdot 5 + 1 (1 < 5)$,

[15] Das haben wir schon in Satz 1 ausgesprochen und dort bewiesen.

$\left[\frac{77}{37}\right] = 2$, $77 = 2 \cdot 37 + 3 (3 < 37)$,
$\left[\frac{11}{111}\right] = 0$, $11 = 0 \cdot 111 + 11 (11 < 111)$,
$\left[\frac{111}{3}\right] = 37$, $111 = 3 \cdot 37 + 0 (r = 0)$

Für einen echten Bruch $\frac{a}{b}$ ist $q = 0$ und $r = a$. Für einen unechten Bruch erhält man $\frac{a}{b} = q + \frac{r}{b}$; hierbei ist $\frac{r}{b}$ ein echter Bruch. Die Zahl $q + \frac{r}{b}$ ist eine "gemischte Zahl", wenn $r \neq 0$ ist.

Beispiele.
$\frac{21}{5} = 4 + \frac{1}{5}$, $\frac{77}{37} = 2 + \frac{3}{37}$

Ist $r = 0$, so ist $\frac{a}{b}$ wieder eine natürliche Zahl q (z.B. $\frac{111}{3} = 37$). In diesem Fall ist a ein Vielfaches von b, nämlich qb. Die Zahl a heißt dann auch durch b teilbar, oder b heißt Teiler von a.
Ist b ein Teiler von a, so schreibt man dies kurz so: $b \mid a$ (in Worten: b teilt a). Ist $r \neq 0$, so ist a nicht durch b teilbar ($b \nmid a$, in Worten: b teilt nicht a).

Beispiele.
$5 \nmid 21$, $37 \nmid 77$, aber $3 \mid 111$, ferner $5 \mid 25$, $15 \mid 45$, $21 \mid 210$.

Jede gerade Zahl ist durch 2 teilbar. Jede ungerade Zahl lässt bei der Division durch 2 den Rest 1, ist also nicht durch 2 teilbar.
Jede natürliche Zahl a ist stets durch sich ($a \mid a$) und durch 1 ($1 \mid a$) teilbar (weil $\frac{a}{a} = 1$ und $\frac{a}{1} = a$ ist).

Primzahlen p besitzen nur die beiden Teiler 1 und p. Zusammengesetzte Zahlen $n \neq 1$ besitzen neben 1 und n noch wenigstens einen Teiler m, der von 1 und n verschieden ist (z. B. hat 4 die Teiler 1, 2, 4). Die Zahl 1 ist nur durch sich selbst teilbar.

Für welche natürlichen Zahlen n gilt

$$n + 1 \mid n^2 + 1$$

Es ist $n^2 + 1 = n(n + 1) - (n - 1)$. Wenn $n + 1 | n^2 + 1$, so $n^2 + 1 = (n + 1)m$ mit einer natürlichen Zahl m, also

$$(n + 1)m == n(n + 1) - (n - 1)$$

d.h., $n - 1 = (n + 1)(n - m)$,d.h. $n + 1 \mid n - 1$, was wegen $n - 1 < n + 1$ nur für $n - 1 = 0$, d.h. nur für $n = 1$ möglich ist. Für $n = 1$ gilt aber $n + 1 \mid n^2 + 1$ ($2 \mid 2$).

Für natürliche Zahlen a, k ist $a^k - 1$ durch $a - 1$ teilbar. In der Tat, es ist

$$a^k - 1 = (a - 1)(a^{k-1} + a_{k-2} + ... + a + 1)$$

Allgemeiner ist für natürliche Zahlen a, b, k auch $a^k - b^k$ durch $a - b$ teilbar,

$$a - b \mid a^k - b^k \tag{2}$$

Es ist ja

$$a^k - b^k = (a - b)(a^{k-1} + a^{k-2}b + a^{k-3}b^2 + ... + ab^{k-2} + b^{k-1})$$

Über die Teilbarkeitsbeziehung gelten die folgenden Sätze.

a) Aus $c \mid b$ und $b \mid a$ folgt $c \mid a$.

Aus $b = b_1 c$ und $a = a_1 b$ folgt nämlich $a = (a_1 b_1)c$, wobei $a_1 b_1$ eine natürliche Zahl ist.

b) Aus $b \mid a$ folgt $nb \mid na$ (für jedes natürliche n) und umgekehrt.

c) Aus $t \mid a$ und $t \mid b$ folgt $t \mid a+b$ und sogar $t \mid an+bm$ für beliebige natürliche Zahlen n, m.
Aus $a = a_1 t$, $b = b_1 t$ folgt ja $an + bm = a_1 tn + b_1 tm == (a_1 n + b_1 m)t$.
Ist $a > b$, so ist dann selbstverständlich auch $a - b$ Vielfaches von t.

d) Wenn $t \mid a+b$ gilt, so braucht weder a noch b Vielfaches von t zu sein (z.B. $5 \mid 2+8$).

Bemerkenswert ist dagegen folgende Aussage: Gilt $7 \mid a^2+b^2$ für natürliche Zahlen a und b, so ist sowohl a als auch b Vielfaches von 7. Dividiert man nämlich das Quadrat einer natürlichen Zahl, die nicht durch 7 teilbar ist, durch 7, so bleibt als Rest 1, 2 oder 4 (Beweis?), so dass die Summe zweier solcher Quadrate 1, 2, 3, 4, 5, 6 ist.
Ist also die Summe zweier Quadrate durch 7 teilbar (Rest 0), so muss wenigstens ein Summand (und dann auch der andere) durch 7 teilbar sein.

e) Aus $t \mid a$ und $t \mid b$ folgt $t \mid ab$.

f) Wenn $t \mid ab$ gilt, so braucht weder a noch b durch t teilbar zu sein (z.B. $10 \mid 4 \cdot 5$).

Nehmen wir einmal an, für eine natürliche Zahl q gelte:
Ist q ein Teiler eines Produktes ab, so folgt stets $q \mid a$ oder $q \mid b$ (oder beides). Wie auch das Produkt aussieht, stets soll q dann auch wenigstens einen der Faktoren teilen.
(Die Zahl 10 ist nicht eine solche Zahl; es ist zwar 10 ein Teiler von 20 · 3, und 10 teilt den Faktor 20, aber dies gilt nicht für alle Produkte, die durch 10 teilbar sind; für das Produkt 4 · 5 ist die Bedingung schon nicht erfüllt.)

Eine solche Zahl q muss notwendig eine Primzahl sein. Wäre q keine Primzahl, so gäbe es eine Zerlegung $q = cd$ in zwei natürliche Zahlen größer als 1. Dies bedeutet auch, dass $q \mid cd$.
Daher teilt q wenigstens einen der Faktoren c oder d (hier benutzen wir die vorausgesetzte Eigenschaft der Zahl q, dass sie nämlich, falls sie ein Produkt teilt, auch wenigstens einen der Faktoren teilt), z.B. $q \mid c$, d.h. $c = qf$ mit einer natürlichen Zahl f. Es folgt $q = cd = afd$, d.h. $fd = 1$, also $f = d = 1$.
Dies ist ein Widerspruch zu $d > 1$. Also ist die Annahme falsch und daher q tatsächlich eine Primzahl.

Dafür also, dass für jedes Produkt zweier Zahlen gilt: "Ist q ein Teiler des Produktes, so teilt q wenigstens einen der Faktoren, ist notwendig, dass q eine Primzahl ist.

Wir bezeichnen die Aussage "Für jedes Produkt zweier Zahlen gilt: ist q ein Teiler des Produktes, so teilt q wenigstens einen der Faktoren" mit A; ferner sei die Aussage "q ist eine Primzahl" mit B bezeichnet.
Oben zeigte sich: Aus A folgt B. Wir können auch sagen: Die Aussage A reicht aus, um aus ihr B zu folgern.
Kurz: A ist hinreichend für B. Die Aussage B gilt immer dann, wenn A gilt. D.h. aber: A gilt nur dann, wenn B gilt. B muss notwendigerweise richtig sein, wenn A richtig sein soll.
Kurz: B ist notwendig für A.

Wir nehmen jetzt einmal für C, D die folgenden Aussagen.
C: "Die Zahl n ist durch 6 teilbar."
D: "n ist eine gerade Zahl."

Ist n durch 6 teilbar, so ist $n = 6m$ mit einer natürlichen Zahl m, und daher ist $n = 2(3m)$,

d.h. n durch 2 teilbar, also gerade.
Auch hier zeigt sich: Aus C folgt D. Die Eigenschaft einer Zahl n, durch 6 teilbar zu sein, reicht dafür aus, dass n gerade ist. Oder: Ist eine Zahl durch 6 teilbar, so ist sie notwendig gerade.

Hier gilt nicht die Umkehrung! Eine gerade Zahl braucht nicht durch 6 teilbar zu sein. Die Eigenschaft einer Zahl n, gerade zu sein, ist nicht hinreichend dafür, dass sie durch 6 teilbar ist.

Man kann sich aber leicht überlegen: Aus B folgt A. Ist q eine Primzahl und teilt q ein Produkt, so ist wenigstens einer der Faktoren durch q teilbar. In der Tat, ist q eine Primzahl, gilt $q \mid ab$ und wäre q weder ein Teiler von a noch ein Teiler von b, so würde das Produkt der Primzahlzerlegungen von a und b eine Primzahlzerlegung von ab ergeben, in der q nicht vorkommt.

Andererseits ist q ein Teiler von ab, also $ab = qm$ mit einer natürlichen Zahl m. Zerlegt man m in Primfaktoren und multipliziert diese Zerlegung mit q, so erhält man dann eine Primzahlzerlegung von ab, in der q vorkommt.
Es gäbe also zwei Primzahlzerlegungen von ab, eine, in der q nicht vorkommt, und eine andere, in der q vorkommt. Dies widerspricht aber der Tatsache, dass ab nur eine einzige Primzahlzerlegung besitzt (Satz 3).
Daher ist die Annahme falsch, also ist q Teiler von wenigstens einem der Faktoren a, b. B ist also auch hinreichend für A. Die Aussage A gilt immer auch dann, wenn B gilt.

Die Aussagen A und B sind also gleichbedeutend. Jede Aussage folgt aus der anderen. B ist notwendig und hinreichend für A. Die Aussage A gilt (immer) dann und nur dann, wenn B gilt.
Kürzer: A gilt genau dann, wenn B gilt.
Wir können auch sagen: B gilt genau dann, wenn A gilt. Die Aussagen A und B sind ja gleichbedeutend: Aus A folgt B, und aus B folgt A.
(Dagegen gilt nicht: Aus D folgt C. D ist nur notwendig, aber nicht hinreichend für C; nur "Aus C folgt D" ist richtig.)
Wir erhalten folgende Charakterisierung der Primzahlen:

Satz 5. Dafür, dass für eine natürliche Zahl q und jedes Produkt gilt: "Ist q ein Teiler des Produktes, so teilt q wenigstens einen der Faktoren", ist notwendig und hinreichend, dass q eine Primzahl ist.

Wie kann man eigentlich aus der Primzahlzerlegung zweier Zahlen t und a ablesen, ob die Zahl t die Zahl a teilt?

Beispiel. $21420 = 2^2 \cdot 3^2 \cdot 5 \cdot 7 \cdot 17$.
Gilt $63 \mid 21420$, $34 \mid 21420$, $66 \mid 21420$, $54 \mid 21420$?

Die Primzahlzerlegungen der gegebenen Zahlen sind $63 = 3^2 \cdot 7$, $34 = 2 \cdot 17$, $66 = 2 \cdot 3 \cdot 11$, $54 = 2 \cdot 3^3$.
In der Zerlegung von 21420 kommen $3^2 \cdot 7$ und $2 \cdot 17$ vor, jedoch kommt 11 nicht vor und auch nicht 3^3, sondern nur 3^2. Es gilt daher
$63 \mid 21420$, $34 \mid 21420$, $66 \nmid 21420$, $54 \nmid 21420$.

Entscheidend sind also erstens die Primzahlen, die in a und t aufgehen, und zweitens die Vielfachheiten des Vorkommens dieser Primzahlen in der Primzahlzerlegung.

Beispiel. In 21420 kommen die Primzahlen 2, 3, 5, 7, 17 vor; sie haben die Vielfachheiten 2, 2, 1, 1, 1.

Ist n eine natürliche Zahl und p eine Primzahl, die in der Primzahlzerlegung von n vorkommt, und gilt $p^k \mid n$, aber $p^{k+1} \nmid n$, so gibt dieser Exponent k die Vielfachheit des Vorkommens von p in n an.
Wir bezeichnen diese Zahl k mit $e_p(n)$, denn sie hängt von n und p ab und ist der Exponent (daher der Buchstabe e) von p in der Primzahlzerlegung von n.[16]
Hat n die Primzahlzerlegung

$$n = p_1^{a_1} p_2^{a_2} ... p_r^{a_r}$$

so ist also $e_{p_1}(n) = a_1$, ..., $e_{p_r}(n) = a_r$. Geht p nicht in n auf, so setzen wir $e_p(n) = 0$. Es ist also $e_p(n) = 0$ für alle Primzahlen, die von p_1, p_2, ..., p_r verschieden sind, und $e_p(n) \geq 1$, falls $p \mid n$.
Da stets $p^{e_p(n)} \mid n$, aber $p^{e_p(n)+1} \nmid n$, ist für jede Primzahl p die Zahl n in der Form

$$n = p^{e_p(n)} n' \qquad (\text{mit } p \nmid n) \tag{3}$$

darstellbar.

Beispiel. $p = 7$. Es ist $77 = 7^1 \cdot 11$, $95 = 7^0 \cdot 95$, $1029 = 7^3 \cdot 3$.
Es ist auch $1715 = 7^2 \cdot 35$; hier gilt jedoch noch $7 \mid 35$, also erst $1715 = 7^3 \cdot 5$ ist die Darstellung in der verlangten Form wegen $7 \nmid 5$). Ferner ist $1001 = 7^1 \cdot 143$.

Ist $m = p^{e_p(m)} m'$ (mit $p \nmid m'$), so folgt

$$nm = p^{e_p(n)} n' p^{e_p(m)} m' = p^{e_p(n)+e_p(m)} n' m'$$

Hier gilt auch $p \nmid m'n'$. Andererseits ist $nm = p^{e_p(nm)} k$ (wobei $p \nmid k$). Wegen der Eindeutigkeit der Primzahlzerlegung ist daher $p^{e_p(n)+e_p(m)} = p^{e_p(nm)}$, d.h.

$$e_p(nm) = e_p(n) + e_p(m) \tag{4}$$

Der p-Exponent eines Produktes ist gleich der Summe der p-Exponenten der Faktoren.

Ist nun t ein Teiler einer Zahl a, so folgt $a = tu$ mit einer natürlichen Zahl u. Dann ist $e_p(a) = e_p(t) + e_t(u)$, also $e_p(a) \geq e_p(t)$, und dies gilt für jede Primzahl p.
Gilt umgekehrt für zwei Zahlen a und t, dass $e_p(t) \leq e_p(a)$ für jede Primzahl p ist, dann ist t ein Teiler von a. Hat nämlich a die Primzahlzerlegung $a = p_1^{a_1} ... p_r^{a_r}$, so ist $e_{p_1}(a) = a_1$, ..., $e_{p_r}(a) = a_r$, $e_q(a) = 0$ für alle Primzahlen q, die verschieden von $p_1, ..., p_r$ sind. Wegen $e_p(t) \leq e_p(a)$ für alle p hat t notwendig eine Zerlegung der Form $t = p_1^{t_1} ... p_r^{t_r}$, wobei $t_1 \leq a_1$, ..., $t_r \leq a_r$ ist (und einige der t_i gleich 0 sein können).

Dann ist $\frac{a}{t} = p^{a_1 - t_1} ... p^{a_r - t_r}$ wieder eine natürliche Zahl, d.h., in der Tat gilt $t \mid a$. Damit ist bewiesen:

Satz 6. Es gilt $t \mid a$ genau dann, wenn $e_p(t) \leq e_p(a)$ für alle Primzahlen p ist.

Es gilt $e_3(18) = 2 \leq e_3(27) = 3$, obwohl $18 \nmid 27$. Woran liegt das? Nun, $e_p(t) \leq e_p(a)$ muss für alle Primzahlen p erfüllt sein!
Hier ist nämlich schon $e_2(18) = 1 > e_2(27) = 0$, also nicht $e_2(18) \leq e_2(27)$.

Es kann auch für ein $t > a$ durchaus $e_p(t) < e_p(a)$ sein (z.B. ist zwar $12 > 9$, aber $e_3(12) =$

[16] Die Zahl $e_p(n)$ wird auch p-Exponent von n genannt.

$1 < e_3(9) = 2$). Dies kann aber nicht für alle Primzahlen p gelten; denn dann wäre t nach Satz 6 ein Teiler von a, also sicher $t \leq a$ und nicht $> a$.
Es ist eben immer dann und auch nur dann $e_p(t) \leq e_p(a)$ für alle Primzahlen p, wenn t ein Teiler von a ist.

Ist t auch Teiler einer anderen Zahl b, so heißt t gemeinsamer Teiler von a und b. Da jede Zahl nur endlich viele Teiler hat, gibt es auch nur endlich viele gemeinsame Teiler der Zahlen a und b. Daher gibt es unter diesen gemeinsamen Teilern eine größte Zahl. Dieser gemeinsame Teiler heißt größter gemeinsamer Teiler (abgekürzt: g. g. T.).

Beispiel. Die Zahlen 18 und 30 haben die gemeinsamen Teiler 1, 2, 3, 6; ihr größter gemeinsamer Teiler ist 6.

Den größten gemeinsamen Teiler von a und b bezeichnet man mit g.g.T.(a, b) oder kürzer (a, b).

Beispiel. $(7, 77) = 7$, $(8, 13) = 1$, $(24, 36) = 12$; dies erhält man sofort, wenn man zuerst alle Teiler der gegebenen Zahlen aufschreibt und dann unter den gemeinsamen den größten nimmt.

Zur Bestimmung des größten gemeinsamen Teilers von a und b schreibt man die Primzahlzerlegung von a und b auf, ermittelt aus ihr eben die gemeinsamen Teiler und findet leicht den größten.

Beispiel. Es ist $(126, 144)$ zu bestimmen.
Es gilt $126 = 2 \cdot 3^2 \cdot 7$, $144 = 2^4 \cdot 3^2$, die Teiler von 126 sind 1, 2, 3, 7, 3^2, $2 \cdot 3$, $2 \cdot 7$, $2 \cdot 3^2$, $3 \cdot 7$, $3^2 \cdot 7$, $2 \cdot 3^2 \cdot 7$, die Teiler von 144 sind 1, 2, 2^2, 2^3, 2^4, 3, 3^2, $2 \cdot 3$, $2^2 \cdot 3$, $2^3 \cdot 3$, $2^4 \cdot 3$, $2 \cdot 3^2$, $2^2 \cdot 3^2$, $2^3 \cdot 3^2$, $2^4 \cdot 3^2$, die gemeinsamen Teiler also 1, 2, 3, 3^2, $2 \cdot 3$, $2 \cdot 3^2$, und davon ist $2 \cdot 3^2$ der größte. Es ist also $(126, 144) = 18$.

Für gemeinsame Teiler t der Zahlen a und b gilt allgemein sowohl $e_p(t) \leq e_p(a)$ als auch $e_p(t) \leq e_p(b)$ (für jedes p). Auch die Umkehrung ist richtig:
Ist für Zahlen t, a, b

$$e_p(t) \leq e_p(a) \quad \text{und} \quad e_p(t) \leq e_p(b)$$

(für jede Primzahl p), so gilt sowohl $t \mid a$ als auch $t \mid b$, d.h, t ist gemeinsamer Teiler von a und b.

Sind n und m zwei natürliche Zahlen, so kann $n < m$, $n = m$ oder $n > m$ sein. Man setzt[17]

$$\min(n,m) = \begin{cases} n & \text{falls } n \leq m \\ m & \text{falls } m \leq n \end{cases}$$

Beispiel. $\min(5, 8) = 5$, $\min(77, 71) = 71$.

Die Zahl d, für die $e_p(d) = \min(e_p(a), e_p(b))$ für jedes p ist, ist gemeinsamer Teiler von a und b, weil $\min(e_p(a), e_p(b)) \leq e_p(a)$ und auch $\min(e_p(a), e_p(b)) \leq e_p(b)$ ist.

Beispiel. Für 126 und 144 ist $e_2(d) = \min(1,4) = 1$, $e_3(d) == \min(2,2) = 2$, $e_7(d) = \min(1,0) = 0$ und $e_p(d) = 0$ für alle p, die von 2, 3 und 7 verschieden sind, und daher

$$d = 2^{e_2(d)} 3^{e_3(d)} 5^{e_5(d)} 7^{e_7(d)} = 2^2 \cdot 3^2 = 18$$

[17] "min" kommt von "Minimum", $\min(n, m)$ ist gleich der kleineren der Zahlen n, m.

Für gemeinsame Teiler t ist sowohl $e_p(t) \leq e_p(a)$ als auch $e_p(t) \leq e_p(b)$, also auch $e_p(t) < \min(e_p(a), e_p(b)) = e_p(d)$ (für alle Primzahlen p). Hieraus folgt $t \mid d$.
Daher ist der gemeinsame Teiler d von a und b größer als jeder andere gemeinsame Teiler t, also d der größte gemeinsame Teiler. Jeder gemeinsame Teiler t von a und b teilt den größten gemeinsamen Teiler d.

Beispiel. Der größte gemeinsame Teiler von 320 und 600 ist zu bestimmen.
Es ist $320 = 2^6 \cdot 5$, $600 = 2^3 \cdot 3 \cdot 5^2$. Wir wählen aus den Primzahlzerlegungen die jeweils niedrigste Potenz der in beiden Zerlegungen auftretenden Primzahlen aus. Der g.g.T. ist das Produkt der gewählten Primzahlpotenzen:

$$(320, 600) = 2^3 \cdot 3^0 \cdot 5^1 = 40$$

Aus $1680 = 2^4 \cdot 3 \cdot 5 \cdot 7$, $1275 = 3 \cdot 5^2 \cdot 17$ folgt ebenso

$$(1275, 1680) = 2^0 \cdot 3^1 \cdot 5^1 \cdot 7^0 \cdot 17^0 = 15$$

Ist a durch b teilbar, so ist jeder Teiler von b auch Teiler von a, also gemeinsamer Teiler. Jeder gemeinsame Teiler teilt aber insbesondere b. Somit stimmt die Menge der gemeinsamen Teiler der Zahlen a und b mit der Teilermenge von b überein. Der größte Teiler von b ist b. Daher ist

$$(a,b) = b, \qquad \text{falls} \quad b \mid a \tag{5}$$

Ist b kein Teiler von a, so gibt es einen Quotienten q und einen Rest r $(0 < r < b)$, so dass $a = bq + r$ ist. Jeder gemeinsame Teiler von a, b teilt auch r, und jeder gemeinsame Teiler von b und r teilt a. Daher haben a und b sowie b und r dieselben gemeinsamen Teiler. Insbesondere stimmen die größten gemeinsamen Teiler überein, d.h., es ist

$$(a,b) = (b,r), \qquad \text{falls} \quad a = bq + r \quad (0 < r < b) \tag{6}$$

Beispiel. $77 = 25 \cdot 3 + 2$, $(77,25) = (25, 2)$.
$25 = 2 \cdot 12 + 1$, $(25,2) = (2,1) = 1$.

Man kann also die Bestimmung des g.g.T. der Zahlen a, b (z. B. sei $a > b$) auf die Bestimmung des g.g.T. von b und r zurückführen (wobei jetzt $b > r$).
Wollen wir den g.g.T. von 1680 und 1275 bestimmen, so finden wir durch Division

$$1680 : 1275 = 1 \text{ Rest } 405$$

also $1680 = 1275 \cdot 1 + 405$, und es ist $(1680, 1275) = (1275, 405)$.
Die Aufgabe, $(1680, 1275)$ zu finden, ist ersetzt worden durch eine Aufgabe mit kleineren Zahlen. Wir können das Verfahren fortsetzen! Es ist

$$1275 : 405 = 3 \text{ Rest } 60$$

oder $1275 = 405 \cdot 3 + 60$, also $(1275, 405) = (405, 60)$. Ferner ist $405 = 60 \cdot 6 + 45$, also $(405, 60) = (60, 45)$, und schließlich $60 = 45 \cdot 1 + 15$, d.h. $(60,45) = (45,15) = 15$. Wir erhalten eine Kette von Divisionen mit Rest:

$$\begin{aligned} 1680 : 1275 &= 1 \text{ Rest } 405, \\ 1275 : 405 &= 3 \text{ Rest } 60, \\ 405 : 60 &= 6 \text{ Rest } 45, \\ 60 : 45 &= 1 \text{ Rest } 15, \\ 45 : 15 &= 3 \text{ Rest } 0. \end{aligned}$$

Der letzte von 0 verschiedene Rest ist der g.g.T.!
Die Kette dieser Divisionen mit Rest kann man auch so schreiben:

$$\begin{aligned} 1680 &= 1275 \cdot 1 + 405, \\ 1275 &= 405 \cdot 3 + 60, \\ 405 &= 60 \cdot 6 + 45, \\ 60 &= 45 \cdot 1 + 15, \\ 45 &= 15 \cdot 3. \end{aligned}$$

Hat man nun den g.g.T. zweier beliebiger natürlicher Zahlen a und b zu bestimmen, so erhält man durch fortgesetzte Division mit Rest (die erhaltenen Quotienten bezeichnen wir nacheinander mit q_1, q_2, q_3,... die Reste mit r_1,r_2,r_3, ...)

$$\begin{aligned} a &= bq_1 + r_1 \qquad (1 \leq r_1 < b) \\ b &= r_1 q_2 + r_2 \qquad (1 \leq r_2 < r_1) \\ r_1 &= r_2 q_3 + r_3 \qquad (1 \leq r_3 < r_2) \\ &... \end{aligned}$$

Diese wiederholte Division setzt man so lange fort, wie die Reste noch größer als 0 sind. Die aufeinanderfolgenden Reste bilden eine ständig abnehmende Folge natürlicher Zahlen:

$$b > r_1 > r_2 > r_3 > ... \geq 1$$

Nach höchstens b Schritten (meist schon viel früher, da die Differenz zwischen zwei aufeinanderfolgenden Resten im allgemeinen größer als 1 ist) jedoch muss der Rest 0 auftreten. Ist r_n der letzte Rest > 1, also

$$r_{n-2} = r_{n-1} q_n + r_n \qquad (1 \leq r_n < r_{n-1})$$

so folgt

$$r_{n-1} = r_n q_{n+1} + 0$$

Damit bricht das Divisionsverfahren ab. Jetzt gilt

$$\begin{aligned} &(a, b) = (b, r_1); \qquad (b, r_1) = (r_1, r_2); \qquad (r_1, r_2) = (r_2, r_3); \quad ... \\ &(r_{n-2}, r_{n-1}) = (r_{n-1}, r_n); \qquad (r_{n-1}, r_n) = (r_n, 0) = r_n \end{aligned}$$

Somit ist $r_n = (a, b)$. Der gesuchte g.g.T. (a, b) wird durch den letzten von 0 verschiedenen Divisionsrest r_n gegeben.

Hiermit hat man ein systematisches Verfahren zur Berechnung des g.g.T. zweier Zahlen und ist nicht mehr auf das Probierverfahren zur Herstellung der Primzahlzerlegung angewiesen (um aus dieser Primzahlzerlegung der Zahlen den g.g.T. abzulesen).

Dieses Verfahren heißt Euklidischer Algorithmus[18] oder Divisionsalgorithmus.

Beispiel. Zur Übung berechnen wir mit Hilfe dieses Divisionsalgorithmus noch einen g.g.T. zweier Zahlen, z. B. $(461, 165)$. Wir erhalten (links steht die Nebenrechnung):

[18] Euklid beschrieb das Verfahren in geometrischer Form in seinen "Elementen", Buch IX.

$$462 : 165 = 2 \text{ Rest } 132 \quad 462 = 165 \cdot 2 + 132$$
$$165 : 132 = 1 \text{ Rest } 33 \quad 165 = 132 \cdot 1 + 33$$
$$132 : 33 = 4 \text{ Rest } 0 \quad 132 = 33 \cdot 4 + 0$$

Hier ist 33 der letzte von Null verschiedene Rest, also $(462, 165) = 33$.
Setzen wir in $165 = 132 + 33$ für 132 nun $462 - 165 \cdot 2$ aus der ersten Gleichung ein, so erhalten wir $165 = 462 - 165 \cdot 2 + 33$, also $33 = 165 \cdot 3 + 462 \cdot (-1)$.

Allgemeiner folgt aus dem Euklidischen Algorithmus:

Satz 7. Ist $(a,b) = d$, so gibt es ganze Zahlen m und n so, dass $d = am + bn$ ist.

Dies ist eine sehr wichtige Eigenschaft des g.g.T.!
Sind a und b teilerfremd, ist also $(a, b) = 1$, so gibt es hiernach also ganze Zahlen m, n so, dass $1 = am + bn$ ist.

Es ist klar, dass hier m und n nicht beide natürliche Zahlen sein können, sondern dass genau eine der Zahlen nichtpositiv (d.h. < 0) sein muss. Wären nämlich beide positiv, also $m \geq 1$, $n \geq 1$, so wäre $am \geq a$, $bn \geq b$, also $am + bn \geq a + b > d$.
Wären beide nichtpositiv, so wäre $m < 0$, $n < 0$, $am + bn \leq < 0 < d$ und nicht $am + bn = d$.
Dazu betrachten wir ein

Beispiel. $(14,5) = 1$

$$14 = 5 \cdot 2 + 4; \qquad 5 = 4 \cdot 1 + 1; \qquad 4 = 1 \cdot 4 + 0$$
$$1 = 5 - 4 \cdot 1 = 5 - (14 - 5 \cdot 2) - 1 = 5 - 14 + 5 \cdot 2 = 5 \cdot 3 + 14 \cdot (-1)$$

Der Beweis des Satzes 7 ist einfach. Man schreibe die Gleichungskette des Divisionsalgorithmus in der folgenden Form:

$$\begin{aligned} r_1 &= a - q_1 b \\ r_2 &= b - r_1 q_2 \\ r_3 &= r_1 - r_2 q_3 \\ &\ldots \\ r_{n-2} &= r_{n-4} - r_{n-3} q_{n-2} \\ r_{n-1} &= r_{n-3} - r_{n-2} q_{n-1} \\ r_n &= r_{n-2} - r_{n-1} q_n \end{aligned}$$

Setzt man r_{n-1} aus der vorletzten Gleichung in die letzte Gleichung ein, so ergibt sich

$$r_n = r_{n-2} - (r_{n-3} - r_{n-2} q_{n-1}) q_n = -q_n r_{n-3} + (1 + q_{n-1} q_n) r_{n-2}$$

Hierin ersetzt man r_{n-2} aus der drittletzten Gleichung. In die so erhaltene Gleichung setzt man r_{n-3} aus der viertletzten Gleichung ein. So geht es weiter.
Bald erhält man eine Gleichung der Form $r_n = kr_1 + lr_2$, (mit ganzen Zahlen k, l). Jetzt ersetzt man r_n aus der zweiten Gleichung und erhält $r_n = kr_1 + l(b - r_1 q_2) == lb + (k - lq_2) r_1$.
Setzt man endlich hierin r_1 aus der ersten Gleichung ein, so bekommt man

$$r_n = lb + (k - lq_2)(a - q_1 b) = a(k - lq_2) + b(l - kq_1 + lq_2 q_1)$$

also $r_n = (a, b) = am + bn$ mit ganzen Zahlen m, n. Damit ist Satz 7 bewiesen.
Hier noch ein

Beispiel. $(77, 111)$ soll bestimmt werden (die rechte Gleichungskette schreibt man von unten nach oben auf):

$$
\begin{array}{ll}
77 = 111 \cdot 0 + 77 & \\
111 = 77 \cdot 1 + 34 & 1 = (111 - 77) \cdot 34 - 77 \cdot 15 = 111 \cdot 34 - 77 \cdot 49 \\
77 = 34 \cdot 2 + 9 & 1 = 34 \cdot 4 - (77 - 34 \cdot 2) \cdot 15 = 34 \cdot 34 - 77 \cdot 15 \\
34 = 9 \cdot 3 + 7 & 1 = (34 - 9 \cdot 3) \cdot 4 - 9 \cdot 3 = 34 \cdot 4 - 9 \cdot 15 \\
9 = 7 \cdot 1 + 2 & 1 = 7 \cdot (9 - 7) \cdot 3 = 7 \cdot 4 - 9 \cdot 3 \\
7 = 2 \cdot 3 + 1 & 1 = 7 - 2 \cdot 3 \\
2 = 1 \cdot 2 &
\end{array}
$$

Ergebnis: $(111, 77) = 1 = 111 \cdot 34 + 77 \cdot (-49)$.

Wir können Satz 7 auch so formulieren: Ist $d = (a, b)$, so ist die Gleichung $ax + by = d$ (in den zwei Variablen x, y) in ganzen Zahlen lösbar (nämlich $x = m$, $y = n$).

Eine Gleichung der Form $ax + by = c$ mit natürlichen Zahlen a, b, c ist in positiven oder negativen gebrochenen Zahlen stets lösbar, z.B. $x = \frac{c}{a} - \frac{b}{a}$, $y = 1$.
Wann ist sie jedoch in ganzen Zahlen lösbar?

Das ist der Fall, wenn $c = d = (a, b)$ ist, aber auch, wenn c ein Vielfaches von d ist, $c = dc'$. Ist nämlich $d = am + bn$, so ist $a(mc') + b(nc') = c$.
Die Bedingung $d \mid c$ ist also hinreichend für die Lösbarkeit der Gleichung $ax+by = c$ in ganzen Zahlen. Ist sie auch notwendig?
Nun, wenn die Gleichung $ax + by = c$ in ganzen Zahlen lösbar ist, so ist jeder gemeinsame Teiler von a und b auch Teiler von c, speziell $(a,b) = d \mid c$. Damit ist der folgende Satz bewiesen:

Satz 8. Eine Gleichung $ax + by = c$ mit natürlichen Zahlen a, b, c ist in ganzen Zahlen dann und nur dann lösbar, wenn c ein Vielfaches von (a, b) ist.

Beispiel. Hiernach gibt es keine ganzen Zahlen n, m, für die $5n + 15m = 3$ ist, jedoch ist $111x + 77y = 33$ lösbar; ebenso ist $14x + 5y = 3$ lösbar.
Es ist $111 \cdot (34 \cdot 33) + 77 \cdot (-49 \cdot 33) = 33$, $14 \cdot (-3) + 5 \cdot 15 = 3$. Auch $5x + 15y = 5$ ist lösbar, es ist nämlich $5 \cdot (-2) + 15 \cdot 1 = 5$.
Übrigens ist auch $5 \cdot (-5) + 15 \cdot 2 = 5$ oder $5 \cdot (-8) + 15 \cdot 3 = 5$ oder $5 \cdot (-11) + 15 \cdot 4 = 5$ oder $5 \cdot (-14) + 15 \cdot 5 = 5$.
Wie kann man alle Lösungen bekommen ?

Satz 8 sagt nur etwas über die Existenz der Lösung aus, nichts über die Methode, wie man die Lösung bekommen kann. Wirklich angeben kann man eine Lösung mit Hilfe des Euklidischen Algorithmus.
Dass es mehr als eine Lösung geben kann, haben wir eben gesehen. Jetzt stellen wir die Frage nach einer Übersicht über alle Lösungen.

Es sei x_0, y_0 eine Lösung, d.h., x_0, y_0 seien ganze Zahlen, für die $ax_0 + by_0 = c$ ist. Diese Zahlen x_0, y_0 können wir mittels des Euklidischen Algorithmus finden.
Ist x_1, y_1 eine andere Lösung, dann gilt auch $ax_1+by_1 = c$. Subtrahieren wir die erste Gleichung $ax_0 + by_0 = c$ von dieser Gleichung $ax_1 + by_1 = c$, so erhalten wir

$$a(x_1 - x_0) + b(y_1 - y_0) = 0$$

Ist $d = (a,b)$, so ist daher

$$\frac{a}{d}(x_1 - x_0) = -\frac{b}{d}(y_1 - y_0)$$

d.h., $\frac{a}{d}$ ist ein Teiler von $y_1 - y_0$)[19] (weil $\frac{a}{d}$ uns $\frac{b}{d}$ teilerfremd sind).[20] Daher gibt es ein ganzes t_1, so dass $y_1 - y_0 = t_1 \frac{a}{d}$ ist. Dann ist

$$\frac{a}{d}(x_1 - x_0) = -\frac{b}{d}(y_1 - y_0) = -\frac{b}{d} t_1 \frac{a}{d}$$

$$\text{also} \qquad x_1 - x_0 = -\frac{b}{d} t_1$$

Ist x_0, y_0 eine spezielle Lösung, die mit dem Euklidischen Algorithmus gefunden wurde, so hat eine (beliebige) andere Lösung notwendig die Form

$$x_1 = x_0 - \frac{b}{d} t_1 \qquad , \qquad y_1 = y_0 + \frac{a}{d} t_1$$

Für jede ganze Zahl t ist aber mit x_0, y_0 tatsächlich auch $x = x_0 - \frac{b}{d}t$, $y = y_0 + \frac{a}{d}t$ eine ganzzahlige Lösung von $ax + by = c$. Es ist ja

$$a\left(x_0 - \frac{b}{d}t\right) + b\left(y_0 + \frac{a}{d}t\right) = ax_0 + by_0 - \frac{ab}{d}t + \frac{ab}{d}t = ax_0 + by_0 = c$$

Man erhält also wirklich alle ganzzahligen Lösungen der Gleichung $ax + by = c$, wenn man in

$$x = x_0 - \frac{b}{d}t \qquad , \qquad y = y_0 + \frac{a}{d}t$$

t alle ganzen Zahlen durchlaufen lässt (dabei ist x_0, y_0 eine spezielle Lösung).

Beispiele. 1. Die Gleichung $3x + 5y = 7$ hat die spezielle Lösung $x = 14$, $y = -7$, die wir mittels des Euklidischen Algorithmus finden:

$$\begin{array}{ll} 5 = 3 \cdot 1 + 2 & 1 = 3 - (5 - 3) = 3 \cdot 2 + 5 \cdot (-1) \\ 3 = 2 \cdot 1 + 1 & 1 = 3 - 2 \cdot 1 \\ 2 = 1 \cdot 2 + 0 & 1 = 3 \cdot 2 + 5 \cdot (-1), \text{ d.h. } 7 = 3 \cdot 14 + 5 \cdot (-7) \end{array}$$

Alle Lösungen sind gegeben durch

$$x = 14 - 5t \qquad , \qquad y = -7 + 3t$$

worin t eine beliebige ganze Zahl ist.

t	...	-3	-2	-1	0	1	2	3	4	...
x	...	29	24	19	14	9	4	-1	-6	...
y	...	-16	-13	-10	-7	-4	-1	2	5	...

2. Eine spezielle Lösung der Gleichung $11x + 33y = 22$ ist $x = -1$, $y = 1$, wie man sofort sieht. Alle Lösungen sind gegeben durch

$$x = -1 - 3t \qquad , \qquad y = 1 + t$$

worin t eine beliebige ganze Zahl ist.

[19] $y_1 - y_0$ kann auch negativ sein. Vereinbarung: Eine ganze Zahl g heißt Teiler einer ganzen Zahl h, falls $\frac{h}{g}$ eine ganze Zahl ist.

[20] Aus $nm = n'r$ und $(n,n') = 1$ folgt $n \mid r$.

Beweis. Aus (n,n') =1 folgt, dass $nx + n'y = 1$ in ganzen Zahlen lösbar ist. Daraus folgt mit ganzen Zahlen x, y

$$nrx + n'ry = r$$

Da $n \mid n'r$ (nach Voraussetzung), also $n'r = nm$ ist, gilt $nrx + nmy = n(rx + my) = r$, d.h. $n \mid r$.

t	...	-3	-2	-1	0	1	2	3	4	...
x	...	8	5	2	-1	-4	-7	-10	-13	...
y	...	-2	-1	0	1	2	3	4	5	...

Haben die natürlichen Zahlen a und b keinen von 1 verschiedenen gemeinsamen Teiler (ist also $(a,b)=1$), so ist die Gleichung $ax+by=k$ stets in ganzen Zahlen lösbar (auch k sei eine natürliche Zahl). Hieraus folgt

$$\frac{k}{ab}=\frac{x}{b}+\frac{y}{a}$$

Ist also ein echter Bruch $r=\frac{k}{l}$ und für den Nenner l eine Zerlegung $l=ab$ in teilerfremde Faktoren vorgegeben, dann lässt sich r als Summe zweier Brüche mit den Nennern a und b schreiben. Im Zähler dieser Brüche stehen positive oder negative ganze Zahlen.

Beispiel. Die Gleichung $3x+5y=7$ hat z.B. die Lösung $x=9$, $y=-4$ oder $x=-1$, $y=2$. Es folgt $\frac{7}{15}=\frac{9}{4}+\frac{-4}{3}=\frac{-1}{5}+\frac{2}{3}$.

Jede rationale Zahl hat die Form $r=\frac{m}{n}$, wobei m, n ganze Zahlen sind. Ist r eine positive rationale Zahl, so kann man annehmen, dass sowohl m als auch n positiv sind. Ist r eine negative rationale Zahl, so möge m negativ und n positiv sein.
Jede rationale Zahl kann also in der Form $r=\frac{m}{n}$ mit einer natürlichen Zahl n und einer ganzen Zahl m geschrieben werden.

Beispiele. $-\frac{7}{8}=\frac{-7}{8}$, $\frac{-2}{-3}=\frac{2}{3}$, $\frac{5}{-9}=\frac{-5}{9}$, $-\frac{-3}{4}=\frac{3}{4}$, $\frac{5}{-15}=\frac{-5}{15}$

Durch Kürzung etwaiger gemeinsamer Teiler in Zähler und Nenner kann man überdies erreichen, dass m und n teilerfremd sind:[21]

$$r=\frac{m}{n},\qquad n>0, m \text{ ganze Zahl}, (m,n)=1 \tag{7}$$

Satz 9. Jede rationale Zahl $r\neq 0$ besitzt eine Bruchdarstellung

$$r=\frac{m}{n}$$

mit ganzen teilerfremden Zahlen m, n, von denen $n>0$ ist (reduzierte Bruchdarstellung).

Beispiel. Die folgenden Zahlen sind in reduzierter Bruchdarstellung angegeben:

$$\begin{aligned}
1+\frac{1}{2}&=\frac{2+1}{2}=\frac{3}{2}\\
1+\frac{1}{2}+\frac{1}{3}&=\frac{3}{2}+\frac{1}{3}=\frac{9+2}{6}=\frac{11}{6}\\
1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}&=\frac{11}{6}+\frac{1}{4}=\frac{44+6}{24}=\frac{50}{24}=\frac{25}{12}\\
1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}&=\frac{25}{12}+\frac{1}{5}=\frac{125+12}{60}=\frac{137}{60}\\
1+\frac{1}{2}+\frac{1}{3}+\frac{1}{4}+\frac{1}{5}+\frac{1}{6}&=\frac{137}{60}+\frac{1}{6}=\frac{147}{60}=\frac{49}{20}
\end{aligned}$$

[21] Natürliche Zahlen a, b heißen teilerfremd oder zueinander prim, falls $(a,b)=1$ ist.

Den Teilbarkeitsbegriff für ganze Zahlen kann man auf den für natürliche Zahlen zurückführen, indem man setzt: $m \mid n$ (für ganze Zahlen m, n) dann und nur dann, wenn $|m| \mid |n|$ (hierbei sind $|m|$, $|n|$ natürliche Zahlen). Im Fall $m \mid n$ gibt es eine ganze Zahl g, für die $n=gm$ ist.

Man setzt $(m,n)=(|m|,|n|)$. m, n heißen auch teilerfremd, wenn die natürlichen Zahlen $|m|$ und $|n|$ es sind. Es kommt also bei Teilbarkeitsbetrachtungen in der Menge der ganzen Zahlen nicht aufs Vorzeichen der ganzen Zahlen an.

Gibt es eigentlich irgendeine natürliche Zahl $n > 1$, so dass

$$r_n = 1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + ... + \frac{1}{n}$$

einmal eine ganze Zahl ist? Eine solche Zahl gibt es nicht!
Diese Zahl r_n ist stets ein Bruch. Die reduzierte Bruchdarstellung von r_n hat nämlich einen geraden Nenner und einen ungeraden Zähler. Die Zahl r_n kann infolgedessen keine ganze Zahl sein. (Denn die reduzierte Bruchdarstellung einer ganzen Zahl hat den Nenner 1.) Das erkennt man wie folgt:

Um die Brüche $\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, ..., \frac{1}{n}$ zu addieren, suchen wir zunächst ihren Hauptnenner. Er werde mit h bezeichnet. Was ist h?
Der Hauptnenner ist die kleinste natürliche Zahl h, die 1,2,3,...,n als gemeinsame Teiler besitzt. Speziell teilt (wegen $n \geq 2$) die Zahl 2 den Hauptnenner h, d.h., h ist eine gerade Zahl. Mit dem Hauptnenner h gilt nun

$$\frac{1}{1} = \frac{h}{h}, \quad \frac{1}{2} = \frac{\frac{h}{2}}{h}, \quad \frac{1}{3} = \frac{\frac{h}{3}}{h}, \quad \frac{1}{4} = \frac{\frac{h}{4}}{h}, \quad ..., \quad \frac{1}{n} = \frac{\frac{h}{2}}{n}$$

Da h durch $1, 2, 3, 4, ..., n$ teilbar ist, stehen in den Zählern tatsächlich ganze Zahlen. Es folgt

$$r_n = \frac{h + \frac{h}{2} + \frac{h}{3} + ... + \frac{h}{n}}{h} = \frac{g}{h}$$

(mit der ganzen Zahl $g = h + \frac{h}{2} + \frac{h}{3} + ... + \frac{h}{n}$).
Es sei nun 2^k die höchste Potenz von 2, die unter den Zahlen $1, 2, 3, 4, 5, 6, 7, 2^3, 9, 10, ..., 2^k, ..., n$ vorkommt (also $1 < 2^k \leq n$, aber $2^{k+1} > n$). Dann ist offenbar $e_2(h) = k$, also $\frac{h}{2^k}$ eine ungerade Zahl. Die übrigen im Zähler g von r_n stehenden Summanden

$$h, \frac{h}{2}, ..., \frac{h}{2^k - 1}, \frac{h}{2^k + 1}, ..., \frac{h}{n} \qquad (*)$$

sind aber gerade ganze Zahlen (d.h. durch 2 teilbar).
In der Tat, diese ganzen Zahlen sind in nichtreduzierter Bruchdarstellung gegeben. Ihre Nenner sind höchstens durch $2^k - 1$ teilbar![22]
Ihr Zähler h ist durch 2^k teilbar; die (ganzen) Zahlen (*) sind also tatsächlich durch 2 teilbar. Die Summe s der Zahlen (*) ist also ebenfalls gerade, der Zähler g von r_n als Summe der geraden Zahl s und der ungeraden $\frac{h}{2^k}$ also ungerade. Hieraus folgt die Behauptung über die Zahl r_n. Sie ist nie eine ganze Zahl!

Wir nennen nun eine rationale Zahl $r = \frac{s}{t}$ echt gebrochen (r ist ein echter Bruch), falls $|s| < |t|$ ist.) Es gilt

Satz 10. Ein echter Bruch $r = \frac{k}{l}$, dessen Nenner l in zwei teilerfremde Faktoren $a \cdot b$ zerlegbar ist, lässt sich als Summe zweier echter Brüche mit den Nennern a und b schreiben (Partialbruchzerlegung).

Beweis. 1. Ist r eine positive rationale Zahl, so lässt sich $r = \frac{k}{ab}$ (k, a, b natürliche Zahlen)

[22] Die Nenner sind $1, 2, ..., 2^k - 1, 2^k + 1, ..., n$. Sie können in der Tat wegen der Wahl von k nicht durch 2^k teilbar sein. Dies ist für 1,2, ..., $2^k - 1$ unmittelbar klar (weil sie kleiner als 2^k sind). Wegen $2^k < 2^k + 1, 2^k + 2, ..., 2^k + m = n < 2^{k+1}$ kann aber 2^k auch keine der Zahlen $2^k + 1, 2^k + 2, ..., n$ teilen. Aus $2 \mid 2^k + b$ für ein $1 \leq b \leq m$ würde $2^k \mid b$ folgen, also müsste $b > 2^k$ sein, was wegen $2^k + m = n < 2^{k+1}$, also $b \leq m < 2^{k+1} - 2^k = 2^k$ nicht stimmt.

nach dem schon erhaltenen Ergebnis als Summe zweier Brüche mit den Nennern a und b schreiben.
Dass sie sogar als Summe zweier echter solcher Brüche darstellbar ist (falls sie selbst ein echter Bruch ist ($0 \leq r < 1$), besagt gerade unser Satz 10, ist also noch zu beweisen.

Ist (x_0, y_0) eine Lösung der Gleichung $ax + by = k$ in ganzen Zahlen, so ist stets eine der Zahlen x_0, y_0 positiv und eine nichtpositiv (vgl. die Bemerkung nach Satz 7). Sei beispielsweise $y_0 > 0$ (den Fall $x_0 > 0$ betrachtet man analog).
Aus einer speziellen Lösung x_0, y_0 erhält man die allgemeine Lösung vermöge $x = x_0 - bt$, $y = y_0 + at$ für alle ganzzahligen t.

Es gibt nun unter allen Lösungen eine mit einem $y < a$.
In der Tat, ist schon $y_0 < a$, so sind wir fertig. Ist jedoch noch $y_0 > a$, so dividieren wir y_0 durch a mit Rest:

$$y_0 = aq + y_1 \qquad (0 < y_1 < a)$$

Dann ist $x_1 = x_0 - b(-q) \leq 0$, $y_1 = y_0 + a(-q) > 0$ eine Lösung von $ax + by = k$ so, dass $y_1 < a$ ist, d. h., dass y_1/a echter Bruch ist.
Nun ist nach Voraussetzung $k < ab$ ($\frac{k}{ab}$ soll ein echter Bruch sein). Aus $y_1 < a$ folgt ferner $y_1 b < ab$. Die Differenz $k - y_1 b = ax_1$ ist nichtpositiv (wegen $x_1 \leq 0$), ihr Betrag[23] ist jedoch nicht negativ und wegen $0 < k < ab$ und $0 < y_1 b < ab$ auch kleiner als ab, $|ax_1| = |k - y_1 b| < ab$. Hieraus folgt $|a| \cdot |x_1| < ab$, d.h. $|x_1| < b$.

Beispiel. $\frac{7}{15} = \frac{-1}{5} + \frac{2}{3}$; $\quad (|-1| = 1 < 5, 2 < 3)$

2. Ist $r = \frac{k}{ab}$ eine negative rationale Zahl, so kann man diese Zahl in der Form $\frac{-k'}{ab}$ schreiben, wobei $\frac{k'}{ab}$ eine positive echt gebrochene Zahl ist, die (wie wir eben bewiesen haben) in der Form $\frac{x_1}{b} + \frac{y_1}{a}$ (mit $|x_1| < b$, $|y_1| < a$) darstellbar ist. Dann ist

$$\frac{k}{ab} = \frac{-x_1}{b} + \frac{-y_1}{a}$$

und auch $|-x_1| = |x_1| < b$, $|-y_1| = |y_1| < a$. Damit ist Satz 10 vollständig bewiesen.

Es sei p eine beliebige, aber im folgenden fixierte Primzahl und r eine rationale Zahl, die als reduzierter Bruch $\frac{m}{n}$ dargestellt ist.
Für die natürlichen Zahlen $|m|$ bzw. n gibt $e_p(|m|)$ bzw. $e_p(n)$ die Vielfachheit an, mit der p in der Primzahlzerlegung von $|m|$ bzw. n vorkommt.
Ist $e_p(n) > 0$, so kommt p im Nenner vor (dann ist $e_p(|m|) = 0$ wegen $(m, n) = 1$). Ist $e_p(n) = 0$, so kommt p nicht im Nenner vor. Setzen wir $e_p(r) = e_p(|m|) - e_p(n)$, so lässt sich die rationale Zahl r in der Form

$$r = p^{e_p(r)} \cdot \frac{m'}{n'}$$

schreiben, und in den Primzahlzerlegungen der natürlichen Zahlen $|m'|$ und n' kommt p nicht vor. Da m, n teilerfremd sind, ist entweder $e_p(r) = e_p(|m|)$, falls p nicht in n aufgeht, oder $e_p(r) = -e_p(n)$, falls p nicht in m aufgeht.

Beispiel. $p = 3$ $r = \frac{55}{72} = \frac{5 \cdot 11}{2^2 \cdot 3^2} = 3^2 \cdot \frac{55}{8}$, $e_3(r) = -2$;
$r = \frac{-21}{10} = -\frac{3 \cdot 7}{2 \cdot 5} = 3^1 \cdot \frac{-7}{10}$; $e_3(r) = 1$

[23] $|r| = \max(r, -r)$ (Max kommt von "Maximum"). $\max(r, s)$ ist gleich der größeren der beiden Zahlen r, s; $|r|$ ist stets eine nichtnegative Zahl.
Beispiele. $|-5| = 5$, $|3| = 3$, $|0| = 0$, $|77| = 77$, $|-\frac{1}{2}| = \frac{1}{2}$.

Ist $e_p(r) \geq 0$ (kommt also p nicht im Nenner vor), so heiße r für-p-ganz. Ist jedoch $e_p(r) < 0$, d.h. kommt p im Nenner vor (also dann nicht im Zähler), so heißt r für-p-gebrochen.
Jede rationale Zahl ist entweder für-p-ganz oder für-p-gebrochen.

Beispiele. $\frac{-21}{10}, \frac{1}{25}, \frac{99}{100}$ sind für-3-ganz.
$\frac{55}{72}, \frac{-35}{99}, \frac{1}{3}$ sind für-3-gebrochen.

Für-p-ganze Zahlen kann man addieren, subtrahieren und multiplizieren und erhält wieder für-p-ganze Zahlen (weil die Nenner dabei zu p teilerfremd bleiben).

Beispiele. $\frac{-21}{10} + \frac{1}{25} = \frac{-105+2}{50} = \frac{-103}{50}$,
$\frac{-21}{10} - \frac{1}{25} = \frac{-107}{50}$, $\frac{-21}{10} \cdot \frac{1}{25} = \frac{-21}{250}$ sind für-3-ganz, da $\frac{-21}{10}, \frac{1}{25}$ es sind.

Dividiert man aber für-p-ganze Zahlen, so kann der Quotient für-p-gebrochen sein.

Beispiel. $\frac{1}{25} : \frac{-21}{10} = \frac{1}{25} \cdot \frac{10}{-21} = \frac{-10}{3 \cdot 175}$ ist für-3-gebrochen.

Ist der Quotient $\frac{r}{t}$ für-p-ganzer Zahlen r und t jedoch wieder eine für-p-ganze Zahl, so heiße r durch t für-p-teilbar (Bezeichnung: $t \mid r(p)$).

Beispiel. $\frac{2}{15} \mid \frac{31}{4}(7)$, da $\frac{\frac{31}{4}}{\frac{2}{15}} = \frac{465}{8}$ für-7-ganz ist.

Jede natürliche Zahl ist für-p-ganz (da der Nenner 1 ist). Für natürliche Zahlen a, b gilt $a \mid b$, falls auch $\frac{b}{a}$ eine natürliche Zahl ist (laut Definition). Aus $a \mid b$ folgt daher $a \mid b(p)$ für jede Primzahl p.
Ist umgekehrt für natürliche Zahlen a, b

$$a \mid b(p)$$

für alle Primzahlen p, so ist $\frac{b}{a}$ eine Zahl, die für alle Primzahlen p für-p-ganz ist. Der Quotient $\frac{b}{a}$ ist daher eine ganze Zahl (da keine Primzahl im Nenner aufgeht, muss er gleich 1 sein), also (da a, b natürliche Zahlen sind) ist $\frac{b}{a}$ eine positive ganze, also natürliche Zahl, d.h. $a \mid b$.
Für natürliche Zahlen a, b gilt somit $a \mid b$ dann und nur dann, wenn für jede Primzahl p

$$a \mid b(p)$$

Selbstverständlich ist auch jede ganze Zahl erst recht für-p-ganz. Für ganze Zahlen g, h für die $\frac{h}{g}$ wieder eine ganze Zahl ist, gilt offenbar $g \mid h(p)$ für alle Primzahlen p.
Ist umgekehrt eine rationale Zahl r für alle Primzahlen p für-p-ganz, so ist r eine ganze Zahl.
Ist für ganze Zahlen g, h

$$g \mid h(p)$$

für alle Primzahlen p, so schreibt man hierfür $g|h$, was bedeutet, dass $\frac{h}{g}$ eine ganze Zahl ist (g heißt Teiler von h). Ist h speziell eine natürliche Zahl, so besitzt h Teiler, die natürliche Zahlen sind (natürliche Teiler), und Teiler, die negative ganze Zahlen sind.

Beispiel. $h = 6$. Die natürlichen Teiler sind 1, 2, 3, 6. Aber auch -1, -2, -3, -6 sind Teiler von 6.

Für-p-ganze Zahlen e, für die $\frac{1}{e}$ für-p-ganz ist, heißen Einheiten für p. Das Produkt und der Quotient zweier Einheiten für p sind offenbar wieder Einheiten für p.
Eine rationale Zahl r ist eine Einheit für p, wenn sowohl ihr Zähler als auch ihr Nenner zu p teilerfremd ist (dabei nehmen wir, wie vereinbart, die reduzierte Bruchdarstellung der Zahl). Es ist $e_p(r) = 0$.

Beispiele. $\frac{3}{8}, \frac{9}{4}$ sind Einheiten für 5, ebenso ihr Produkt $\frac{27}{32}$ und Quotient $\frac{1}{6}$. Dagegen sind $\frac{15}{8}, \frac{3}{5}$ keine Einheiten für 5.

Jede für-p-ganze Zahl ist durch jede Einheit für p teilbar. Ist nämlich r für-p-ganz und e Einheit für p, so ist auch $\frac{r}{e} = r \cdot \frac{1}{e}$ als Produkt der für-p-ganzen Zahlen r und $\frac{1}{e}$ für-p-ganz, d.h. $e \mid r(p)$.

Wir haben drei Teilbarkeitsbegriffe eingeführt.

I. Für natürliche Zahlen a, b: $a \mid b$ genau dann, wenn $\frac{b}{a}$ eine natürliche Zahl ist.
II. Für ganze Zahlen g, h: $g \mid h$ genau dann, wenn $\frac{h}{g}$ eine ganze Zahl ist.
III. Für für-p-ganze Zahlen r, s: $r \mid s(p)$ genau dann, wenn $\frac{s}{r}$ für-p-ganz ist.

Natürliche Zahlen sind ganze Zahlen; ganze Zahlen sind für-p-ganze rationale Zahlen.
Ist b eine natürliche Zahl, so gibt es natürliche Teiler (im Sinne von I), ganze Teiler (im Sinne von II) und für-p-ganze Teiler (im Sinne von III) für jede Primzahl p.

Beispiel. $b = 6$.
Die natürlichen Teiler von 6 sind 1, 2, 3, 6; die ganzen Teiler von 6 sind 1, -1, 2, -2, 3, -3, 6, -6; die für-2- ganzen Teiler von 6 sind alle diejenigen rationalen Zahlen r, für die $\frac{6}{r}$ für-2-ganz ist. (Alle solchen rationalen Zahlen r haben die Form $r = \frac{2^a m}{n}$, wobei $a = 0$ oder $a = 1$, m eine ungerade ganze Zahl und n eine beliebige zu $2^a m$ teilerfremde natürliche Zahl ist; z. B. $\frac{-5}{3}, \frac{10}{3}, \frac{-3}{7}, \frac{22}{9}$).

Die für-3-ganzen Teiler von 6 sind alle rationalen Zahlen r, für die $\frac{6}{3}$ für-3-ganz ist. (Alle solchen rationalen Zahlen r haben die Form $r = \frac{3^a m}{n}$, wobei $a = 0$ oder $a = 1$, m eine ganze Zahl, die nicht durch 3 teilbar ist, und n eine beliebige zu $3^a m$ teilerfremde natürliche Zahl ist; z.B. 3, $\frac{5}{9}$, $\frac{15}{22}$, ...)

Die für-p-ganzen Teiler von 6 (p eine von 2 und 3 verschiedene Primzahl) sind alle rationalen Zahlen r, für die $\frac{6}{r}$ für-p-ganz ist.
(Alle solchen rationalen Zahlen haben offenbar die Form $r = \frac{m}{n}$, wobei m eine ganze Zahl, die nicht durch p teilbar ist, und n eine beliebige zu m teilerfremde natürliche Zahl ist; z.B. $\frac{42}{17}, \frac{77}{22} = \frac{7}{2}$ für $p = 5$; $\frac{22}{13}, \frac{36}{7}$ für $p = 7$).

Ist h eine ganze Zahl, so hat sie ganze Teiler (im Sinn von II) und für jede Primzahl p für-p-ganze Teiler (im Sinne von III).
Wir fassen noch einmal einige Begriffsbildungen in Verbindung mit dem Teilbarkeitsbegriff zusammen.

I. Teiler der 1 (Einheit) ist nur die 1. Primzahlen p besitzen nur die Teiler 1 und p. Es ist $e_p(n) = 1$ nur für die Primzahl $n = p$.
Eine natürliche Zahl n ist durch die Angabe der p-Exponenten $e_p(n)$ für alle Primzahlen p bestimmt. (Dies folgt aus dem Satz 3 über die eindeutige Primzahlzerlegung einer natürlichen Zahl.)

Da jede Zahl n nur endlich viele Teiler hat, ist $e_p(n) \neq 0$ nur für endliche viele Primzahlen p, meist also $e_p(n) = 0$. Es gilt:
$a \mid b$ genau dann, wenn $e_p(a) \leq e_p(b)$ für alle Primzahlen p ist (Satz 6). Für den größten gemeinsamen Teiler d zweier Zahlen a und b gilt $e_p(d) = \min(e_p(a), e_p(b))$ für alle Primzahlen p. Es gibt ganze Zahlen g, h, so dass $d = ga + hb$ ist (Satz 7).

II. Teiler der 1 (Einheiten) sind $+1$, -1. Zahlen der Form $+p$ oder $-p$ besitzen nur die vier

Teiler +1, -1, $+p$, $-p$. Alle anderen ganzen Zahlen besitzen mehr als vier Teiler.
Es ist $e_p(n) = 1$ für nur die Zahlen $n = p$ oder $n = -p$. Eine ganze Zahl g ist durch die Angabe der p-Exponenten $e_p(g) = e_p(|g|)$ bis aufs Vorzeichen, d.h. bis auf eine Einheit als Faktor, bestimmt. Es gilt $g \mid k$ genau dann, wenn $e_p(g) \leq e_p(h)$ für alle Primzahlen p ist.

Bei Teilbarkeitsfragen kommt es nicht aufs Vorzeichen an (d.h. eben nicht auf Einheiten). Der größte gemeinsame Teiler der ganzen Zahlen g und h ist gleich dem größten gemeinsamen Teiler der natürlichen Zahlen $|g|$ und $|h|$.
Für den größten gemeinsamen Teiler d zweier ganzer Zahlen g und h gilt $e_p(d) = \min(e_p(g), e_p(h))$ für alle Primzahlen p. Es gibt ganze Zahlen g' und h', so dass $d = g'g + h'h$ ist (das folgt aus Satz 7).

III. Teiler der 1 (Einheiten für p) sind alle rationalen Zahlen der Form $\frac{m}{n}$ (reduzierte Bruchdarstellung), wobei sowohl m als auch n zu p teilerfremd sind.
Jede für-p-ganze Zahl lässt sich in der Form ${}^k e$ mit einer natürlichen Zahl k und einer Einheit für p darstellen. Diese Darstellung ist eindeutig.
Hieraus folgt, dass eine für-p-ganze Zahl r durch den p-Exponenten $e_p(r)$ bis auf eine Einheit als Faktor bestimmt ist. Nur für die Zahlen der Form $r = pe$ (mit einer Einheit e) gilt $e_p(r) = 1$.

Es gilt $r \mid s(p)$ genau dann, wenn $e_p(r) \leq e_p(s)$.

Für alle für-p-ganzen Zahlen r, s gilt daher entweder $r \mid s$ oder $s \mid r$. Der größte gemeinsame Teiler von r und s ist gleich r, falls $r \mid s$, bzw. gleich s, falls $s \mid r$ ist.
Jede für-p-ganze Zahl ist durch jede Einheit für-p-teilbar. Ist nämlich r für-p-ganz und e Einheit für p, so ist auch $\frac{r}{e} = r \cdot \frac{1}{e}$ als Produkt der für-p-ganzen Zahlen r und $\frac{1}{e}$ für-p-ganz, d.h. $e \mid r(p)$.

Es sei nun $r = \frac{m}{n}$ eine beliebige für-p-ganze Zahl ($n \geq 1$, $(m,n) = 1$). Dann ist $(p,n) = 1$. Es gibt daher ganze Zahlen x_0, y_0, so dass $1 = px_0 + ny_0$, also

$$m = p(x_0 m) + n(x_0 m) = px_1 + ny_1 \qquad (x_1 = x_0 m, y_1 = y_0 m)$$

ist. Es folgt $r = \frac{m}{n} = y_1 + \frac{x_1}{n} p$. Dividiert man y_1 durch p mit Rest, so ist $y_1 = pq + c$, wobei $0 \leq c \leq p - 1$. Daher ist

$$r = c + \left(q + \frac{x_1}{n}\right) p$$

also

$$r = c + r_0 p \qquad (0 \leq c \leq p - 1) \tag{8}$$

mit einer für-p-ganzen Zahl $r_0 \left(= q + \frac{x_1}{n}\right)$.

Beispiel. $p = 5$; $\frac{3}{8} = 1 + (-\frac{1}{8}) \cdot 5$.

Ist r' eine andere für-p-ganze Zahl, aber $r' = r'_0 p$ mit demselben c wie bei r (und einer für-p-ganzen Zahl r'_0), so ist $r - r' = (r_0 - r'_0)p$, also $\frac{r-r'}{p}$ eine für-p-ganze Zahl, d.h. $p \mid r - r'(p)$.

Umgekehrt folgt aus $p \mid r - r'(p)$, dass in der Darstellung (8) für r und r',

$$\begin{aligned} r &= c + r_0 p \qquad (0 \leq c \leq p - 1) \\ r' &= c' + r'_0 p \qquad (0 \leq c' \leq p - 1) \end{aligned}$$

$c = c'$ sein muss. In der Tat, aus $r = c + r_0 p$, $r' = c' + r'_0 p$ folgt

$$r - r' = c - c' + p(r_0 - r'_0)$$

Wegen $p \mid r - r'$ muss daher auch $p \mid c - c'$ gelten, was wegen $0 \leq c \leq p$, $0 \leq c' \leq p$ nur für $c - c' = 0$ möglich ist.
Solche Zahlen sollen kongruent für p (oder kongruent modulo p) heißen. Zwei für-p-ganze Zahlen r, r' heißen also kongruent für p, wenn $p \mid r - r'(p)$, also $r = r' + gp$ mit einer für-p-ganzen Zahl g ist.

Beispiele.
$\frac{1}{7} \equiv 3(5)$, weil $3 - \frac{1}{7} = \frac{20}{7} = 5 \cdot \frac{4}{7}$,
$\frac{3}{4} \equiv 2(5)$, weil $2 - \frac{3}{4} = 5 \cdot \frac{1}{4}$,
$-\frac{11}{6} \equiv 4(5)$, weil $4 + \frac{11}{6} = 5 \cdot \frac{7}{6}$,
$76 \equiv 1(5)$, weil $76 - 1 = 5 \cdot 15$.

Um auszudrücken, dass r und r' kongruent für p sind, schreiben wir kürzer $r \equiv r'(p)$ (oder auch $r \mod = r'$ (mod p)).[24] Diese Schreibweise geht auf Gauß[25] zurück.
Der Nutzen liegt darin, dass die Kongruenz für p viele der Eigenschaften der gewöhnlichen Gleichheit hat. Man kann mit Kongruenzen bezüglich der Addition, Subtraktion und Multiplikation wie mit Gleichungen umgehen!

Wenn $r \equiv s(p)$ und $t \equiv u(p)$ (mit für-p-ganzen Zahlen r, s, t, u), so ist

$$r + t \equiv s + u(p), \qquad r - t \equiv s - u(p), \qquad r \cdot t \equiv s \cdot u(p)$$

Dies ist für die Addition und Subtraktion leicht einzusehen.
Aus $r = s + g_1 p$, $t = u + g_2 p$ (mit für-p-ganzen Zahlen g_1, g_2) folgt $r \pm t = s \pm u + (g_1 \pm g_2)p$, also $r \pm t \equiv s \pm u(p)$ (weil auch $g_1 \pm g_2$ für-p-ganz ist).

Um die Behauptung für die Multiplikation zu beweisen, schreibt man die Differenz $rt - su$ am besten in der Form $rt - su = (r - s)t + s(t - u)$.
Da jetzt nach Voraussetzung sowohl $r - s$ als auch $t - u$ durch p teilbar ist, ist auch $(r - s)t + s(t - u)$, also $rt - su$ durch p teilbar, d.h. $rt \equiv su(p)$.

Sind r und r' für-p-ganze Zahlen, die nicht kongruent für p sind, so schreiben wir $r \not\equiv r'(p)$ (sprich: in kongruent für p).
Dies bedeutet, dass die Differenz $r - r'$ (die auch für-p-ganz ist) nicht durch p teilbar ist, d. h., in $r - r'$ kommt p sowohl nicht im Nenner (weil $r - r'$ für-p-ganz ist) als auch nicht im Zähler (wegen $p \nmid r - r'(p)$) vor, d.h., $r - r'$ ist eine Einheit für p.

Beispiel. $\frac{1}{7} \equiv 3(5)$, $\frac{3}{4} \equiv 2(5)$, also $\frac{1}{7} \not\equiv \frac{3}{4}(5)$. In der Tat ist $\frac{1}{7} - \frac{3}{4} = -\frac{17}{28}$ Einheit für 5.

Einheiten sind durch $r \not\equiv 0(p)$ gekennzeichnet. Für-p-ganze Zahlen, die nicht Einheiten für p sind, sind kongruent der Null für p.

Ist r eine für-p-ganze Zahl mit $r \not\equiv 0(p)$, so gibt es stets eine für-p-ganze Zahl r' so, dass $rr' \equiv 1(p)$ ist. In der Tat, $r' = \frac{1}{r}$ ist eine für-p-ganze Zahl (da r eine Einheit für p ist), und es ist $rr' = r\frac{1}{r} = 1$, also erst recht $rr' \equiv 1(p)$.

Ist r eine Einheit für p und t eine für-p-ganze Zahl, so gibt es stets eine für-p-ganze Zahl s, für die $rs \equiv t(p)$ gilt.
Ist nämlich $rr' \equiv 1(p)$, so ist $r(r't) \equiv t(p)$, d.h, $s = r't$ leistet das Verlangte.

[24] Sind $r = g$ und $r' = g'$ ganze Zahlen, so bedeutet $g \equiv g'(p)$, dass g eine für-p-ganze Zahl ist, also überhaupt ganz ist, d. h., p ist ein Teiler von $g - g'$.
[25] Über Gauß kann man im Vorwort etwas finden.

Nach (8) ist jede für-p-ganze Zahl einer und nur einer unter den Zahlen $0, 1, 2, ..., p-1$ kongruent für p. Ist insbesondere c eine unter den Zahlen $1, 2, 3, ..., p-1$, so gibt es stets ein c' unter diesen Zahlen $1, 2, ..., p-1$, für das $cc' \equiv 1(p)$ ist, d.h., $\frac{cc'-1}{p}$ ist für-p-ganz, also überhaupt ganz.

Für $c = 1$ ist offenbar auch $c' = 1$, ebenso ist für $c = p-1$ auch $c' = p-1$ (weil $(p-1)(p-1) = p^2 - 2p + 1 \equiv 1(p)$ ist). Für die übrigen Zahlen $2, 3, ..., p-2$ ist $c' \neq c$. Aus $c' = c$ folgt nämlich $c^2 \equiv 1(p)$, d.h. $(c-1)(c+1) \equiv 0(p)$.
Aus $p \mid l(c-1)(c+1)$ folgt aber $p \mid c-1$ oder $p \mid c+1$, d.h. $c \equiv 1(p)$ bzw. $c \equiv -1(p)$, also notwendig $c = 1$ bzw. $c = p-1$.

Beispiele. $p = 7$:

c	1	2	3	4	5	6
c'	1	4	5	2	3	6

$p = 13$:

c	1	2	3	4	5	6	7	8	9	10	11	12
c'	1	7	9	10	8	11	2	5	3	4	6	12

Betrachtet man nun das Produkt aller dieser Zahlen,

$$1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot ... \cdot (p-2) \cdot (p-1)$$

so erhält man, da jede Zahl c außer 1 und $p-1$ einen Kehrwert c' hat, für den $cc' \equiv 1(p)$ ist,

$$1 \cdot 2 \cdot 3 \cdot ... \cdot (p-1) \equiv 1 \cdot (p-1) \equiv -1(p)$$

Das Produkt der natürlichen Zahlen von 1 bis $p-1$ bezeichnen wir kürzer mit $(p-1)!$ (lies: $p-1$ Fakultät).[26]

Satz 11 (Wilson)[27]. Für jede Primzahl p ist $(p-1)! \equiv -1(p)$.

Es ist also für Primzahlen p stets $(p-1)! + 1$ durch p teilbar.[28]
Ist übrigens umgekehrt für eine natürliche Zahl n der Ausdruck $(n-1)! + 1$ durch n teilbar, so muss n eine Primzahl sein.

Wäre nämlich n eine zusammengesetzte Zahl, so wäre $n = ab$ mit natürlichen Zahlen a, b $(1 < a < n, 1 < b < n)$. Da hierin $a < n$, also $a \leq n-1$ ist, ist a ein Teil von $1 \cdot 2 \cdot 3 ... (n-1)$, denn dies ist ja das Produkt aller Zahlen $\leq n-1$.
Daher hat $(n-1)!+1$ bei der Division durch a den Rest 1, d.h. $a \nmid (n-1)!+1$. Andererseits ist aber $(n-1)!+1$ durch n, also auch durch a teilbar. Wir erhalten den Widerspruch $a \mid (n-1)!+1$ und $a \nmid (n-1)! + 1$.
Für Nichtprimzahlen $n > 1$ gilt also $n \nmid (n-1)! + 1$. [29]

[26] Allgemein wird das Produkt der natürlichen Zahlen von 1 bis n mit $n!$ (sprich: n Fakultät) bezeichnet: $n! = 1 \cdot 2 \cdot 3 \cdot ... \cdot (n-1) \cdot n$.

[27] Der englische Mathematiker Edward Waring (1734-1798) gab diesen Satz in seinem Werk "Meditationes Algebraicae" ohne Beweis an. Er schrieb, dass sein Schüler John Wilson ihn entdeckt hat. Einen ersten Beweis gab 1771 der französische Mathematiker Joseph-Louis Lagrange (1736-1813).

[28] Nach Satz 11 ist $\frac{(p-1)!+1}{p}$ für-p-ganz, also überhaupt ganz und damit eine natürliche Zahl.

[29] Wir erhalten eine neue Charakterisierung der Primzahlen. Die folgenden Aussagen sind für eine natürliche Zahl p äquivalent:
(1) p ist eine Primzahl.
(2) p besitzt nur die natürlichen Teiler 1 und p.
(3) p lässt sich nicht als Produkt zweier natürlicher Zahlen darstellen, die größer als 1 sind.
(4) Für beliebige natürliche Zahlen a, b gilt: Aus $p \mid ab$ folgt $p \mid a$ oder $p \mid b$ (Satz 5).
(5) Es gilt $(p-!)! + 1 \equiv 0(p)$ (Satz 11).

Ist m eine natürliche Zahl, die nicht durch p teilbar ist ($m \not\equiv 0(p)$), so ist der Rest bei der Division durch p gleich einer der Zahlen $1, 2, 3, ..., p-1$. Multipliziert man diese Zahlen mit m, so erhält man m, $2m$, $3m$, ..., $(p-1)m$, also $p-1$ verschiedene Zahlen, die bei der Division durch p einen Rest lassen, der gleich einer der Zahlen $1, 2, 3, ..., p-1$ ist.
Diese $p-1$ Reste sind aber auch alle verschieden, d.h., keine zwei der Zahlen m, $2m$, $3m$, ..., $(p-1)m$ können kongruent für p sein (warum ?). Daher ist die Gesamtheit der Zahlen m, $2m$, ..., $(p-1)m$ in unbekannter Reihenfolge der Gesamtheit der Zahlen 1, 2, ..., $p-1$ kongruent für p.

Bildet man das Produkt, so erhält man

$$m \cdot 2m \cdot ... \cdot (p-1)m = m^{p-1}(p-1)! \equiv (p-1)!(p)$$

d.h. $p \mid m^{p-1}(p-1)!$. Da $((p-1)!, p) =!$ ist, folgt $p \mid m^{p-1} - 1$, [30] also erst recht $p \mid (m^{p-1} - 1)m$, d.h. $m^p - m \equiv 0(p)$.
Diese Kongruenz gilt offenbar auch für ein $m \equiv 0(p)$. So folgt der

Satz 12 (Fermat). Für jede natürliche Zahl m und jede Primzahl p ist $m^p \equiv m(p)$. Für eine Primzahl p, die m nicht teilt, gilt $m^{p-1} \equiv 1(p)$.

Beispiele 1. $p = 11$, $m = 2$, $2^{10} \equiv 1(11)$. Wir können dies leicht nachprüfen:
$2^3 = 8 \equiv 8(11)$, $2^4 = 16 \equiv 5(11)$, $2^5 = 2^4 \cdot 2 \equiv 5 \cdot 2 \equiv -1(11)$, also $(2^5)^2 = 2^{10} \equiv 1(11)$.

2. $p = 5$, $m = 4$, $4^4 \equiv 1(5)$. Ausrechnen: $4 \equiv -1(5)$, $4^2 \equiv 1(5)$, $4^4 \equiv 1(5)$

Es kann übrigens $n \mid m^n - m$ (für eine natürliche Zahl m) auch für natürliche Zahlen n gelten, die nicht Primzahlen sind.

Beispiel. $m = 2$, $n = 341 = 11 \cdot 31$.
Es ist $2^{341} - 2 = ((2^{31})^{11} - 2^{11}) + (2^{11} - 2)$. Nun ist $2^{10} - 1 = 1023 = 3 \cdot 341$, also ist $2^{11} - 2 = 2(2^{10} - 1)$ durch 341 teilbar.
Auch $(2^{31})^{11} - 2^{11}$ ist durch 341 teilbar. Nach (2) ist $(2^{31})^{11} - 2^{11}$ nämlich durch $2^{31} - 2 = 2((2^{10})^3 - 1)$ teilbar, und ebenfalls nach (2) ist $(2^{10})^3 - 1$ durch $2^{10} - 1$ teilbar.
Daraus folgt die Behauptung. Somit ist $2^{341} \equiv 2(341)$.

In Verallgemeinerung des oben eingeführten Kongruenzbegriffs mögen zwei für-p-ganze Zahlen r, r' kongruent für p^h ($h \geq 1$) heißen, falls $p^h \mid r - r'(p)$, also $r = r' + gp^h$ mit einer für-p-ganzen Zahl g ist.
Symbolische Schreibweise: $r \equiv r'(p^h)$ oder auch $r \equiv r'$ (mod p^h). Dass man auch mit diesen Kongruenzen für p^h wie mit Gleichungen rechnen kann, sieht man leicht.

Aus $r \equiv r'(p^h)$ folgt $r \equiv r'(p^{h-1})$, also erst recht $r \equiv r'(p)$.
Aus $r \equiv r'(p^h)$ folgt im allgemeinen nicht $r \equiv r'(p^{h+1})$.

Beispiele. 1. $p^h \equiv 0(p^h)$, aber $p^h \not\equiv 0(p^{h+1})$.
2. $55 \equiv 37(3^2)$, aber $55 \not\equiv 37(3^3)$ (da $55 \equiv 1(3^3)$, $37 \equiv 10(3^3)$ ist).

Interessant ist folgende Aussage.
Für jedes $h > 1$ folgt aus $r \equiv r'(p^h)$ stets $r^p \equiv r'^p(p^{h+1})$. (Auf den Beweis verzichten wir. Kennt der Leser den binomischen Satz, so kann er die Behauptung leicht selbst beweisen.)

Beispiele. 1. Aus $13 \equiv 1(3)$ folgt $13^3 \equiv 1(9)$. 2. Aus $111 \equiv 1(5)$ folgt $111^5 \equiv 1(25)$.[31]

[30] Aus $m^{p-1}(p-1)! \equiv (p-1)!(p)$ folgt nach Satz 11 $m^{p-1} \cdot (-1) \equiv -1(p)$, also $m^{p-1} \equiv 1(p)$.
[31] $111^5 \equiv 11^5 \equiv 11^2 \cdot 11^2 \cdot 11 \equiv 121 \cdot 121 \cdot 11 \equiv 21 \cdot 21 \cdot 11 \equiv (-4) \cdot (-4) \cdot 11 \equiv (-9) \cdot 11 \equiv -99 \equiv 1(25)$

2 Die p-adische Entwicklung der rationalen Zahlen

Es sei p eine Primzahl und r eine beliebige rationale Zahl. Die Zahl r ist entweder für-p-ganz oder für-p-gebrochen.
Wir setzen zunächst voraus, dass r für-p-ganz ist. Dann hat r eine Darstellung der Form $r = \frac{a}{b}$, a und b teilerfremd, $p \nmid b$ ($b \geq 1$), a ganze Zahlen).

Ist $r \equiv a_0(p)$, wobei $0 \leq a_0 < p$ ist, so ist $r = a_0 + r_1 p$ mit einer für-p-ganzen Zahl r_1.
Ist $r_1 \equiv a_1(p)$, wobei $0 \leq a_1 < p$ ist, so ist $r_1 = a_1 + r_2 p$ mit einer für-p-ganzen Zahl r_2.

Beispiel. $\frac{31}{4} \equiv 4(5)$, $\frac{31}{4} = 4 + \frac{3}{4} \cdot 5$,
$\frac{3}{4} \equiv 2(5)$, $\frac{3}{4} = 2 + \frac{-1}{4} \cdot 5$,
$-\frac{1}{4} \equiv 1(5)$, $-\frac{1}{4} = 1 + \frac{-1}{4} \cdot 5$.

So fortfahrend erhält man eine Folge von Gleichungen

$$\begin{aligned} r &= a_0 + r_1 p \\ r_1 &= a_1 + r_2 p \\ r_2 &= a_2 + r_3 p \\ &... \\ r_{k-1} &= a_{k-1} + r_k p \end{aligned} \tag{9}$$

wobei die a_i eindeutig bestimmte Zahlen aus der Menge $\{0, 1, ..., p-1\}$ sind. Durch Einsetzen erhält man nacheinander

$$\begin{aligned} r &= a_0 + (a_1 + r_2 p)p = a_0 + a_1 p + r_2 p^2 \\ r &= a_0 + a_1 p + (a_2 + r_3 p)p^2 = a_0 + a_1 p + a_2 p^2 + r_3 p^3 \\ &... \end{aligned}$$

und schließlich

$$r = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + ... + a_{k-1} p^{k-1} + r_k p^k \tag{10}$$

mit einer für-p-ganzen Zahl r_k.

Beispiel. $\frac{31}{4} = 4 + 2 \cdot 5 + 5^2 + 5^3 + ... + 5^{k-1} + (-\frac{1}{4}) \cdot 5^k$ (für alle $k \geq 3$).

Man kann nun in der Darstellung (10) der für-p-ganzen Zahl r die Berechnung der Koeffizienten a_i in der angegebenen Weise immer weiter fortsetzen. Der Prozess, immer weitere Koeffizienten a_i zu berechnen, braucht nicht abzubrechen.
Betrachten wir als Beispiel etwa $r = -1$ und $p = 2$. Es ist $-1 = 1 + (-1) \cdot 2$ und somit

$$-1 = 1 + 2 + 2^2 + 2^3 + ... + 2^{k-1} + (-1) \cdot 2^k \qquad \text{(für alle } k\text{)}$$

Hier gilt $r_1 = r_2 = r_3 = ... = -1$ und $a_i = 1$ für alle i.
Ebenso ist für $r = -1$ und $p \neq 2$ (beliebige ungerade Primzahl) $-l = (p-1) + (-1)p$ und daher

$$-1 = (p-1) + (p-1)p + (p-1)p^2 + ... + (p-1)p^{k-1} + (-1)p^k$$

für alle natürlichen Zahlen k. (Hier ist $r_1 = r_2 = ... = -1$ und $a_i = p - 1$ für jedes i.)

Ist r eine nichtnegative ganze Zahl[32], so ist auch r_1 eine nichtnegative ganze Zahl, die überdies

[32]Eine Zahl $r \geq 0$ heißt nichtnegativ. Eine Zahl $r > 0$ heißt positiv.

kleiner als r ist (wegen $r = a_0 + r_1 p$ mit $0 \leq a_0 \leq p-1$). Ebenso ist r_2 eine nichtnegative ganze Zahl, die kleiner als r_1 ist. Entsprechendes gilt für die weiteren r_i:

$$r > r_1 > r_2 > ... \geq 0$$

Die Zahlen $r_1, r_2, r_3, ...$ sind verschiedene nichtnegative ganze Zahlen, die kleiner als r sind. Es gibt aber nur endlich viele (nämlich r) verschiedene nichtnegative ganze Zahlen, die kleiner als r sind (nämlich $0, 1, 2, 3, ..., r-1$).
Von einem bestimmten Index an müssen also alle r_i gleich 0 sein, und damit werden auch die a_i gleich 0. Ist somit r eine nichtnegative ganze Zahl, so bricht der Berechnungsprozess ab, d. h., von einer bestimmten Stelle an sind alle Koeffizienten gleich 0.

Sind umgekehrt von einer bestimmten Stelle an alle Koeffizienten gleich 0, so hat man eine endliche Summe der Form

$$a_0 + a_1 p + a_2 p^2 + ... + a_m p^m$$

(mit ganzen Zahlen zwischen 0 und $p-1$), die offenbar gleich 0 (falls $a_0 = a_1 = ... = a_m = 0$) oder eine natürliche Zahl ist.
Bei allen anderen für-p-ganzen Zahlen (außer der Null und den natürlichen Zahlen) brechen die Entwicklungen (10) nicht ab (d.h., man kann Koeffizienten $\neq 0$ beliebig weit berechnen).

Berechnet man nun die Koeffizienten sukzessive immer weiter, so ergibt sich jedoch stets von einer bestimmten Stelle an eine periodische Ziffernfolge a_i.
Vor dem Beweis dieser Behauptung betrachten wir noch zwei Beispiele.

Beispiele. 1. $p = 5$, $r = -\frac{17}{24}$
Wir suchen zunächst ein a_0 mit der Eigenschaft, dass $-\frac{17}{24} \equiv a_0(5)$, also $-17 = 24a_0(5)$ gilt, d.h. $3 = 4a_0(5)$ (wegen $-17 \equiv 3$, $24 \equiv 4$ (5)). Für a_0 kommen die Zahlen $1, 2, 3, 4$ in Frage; $a_0 \equiv 2(5)$ leistet das Verlangte. Es ist

$$-\frac{17}{24} = 2 + 5 \cdot \left(-\frac{13}{24}\right)$$

Aus $-\frac{13}{24} \equiv a_1(5)$ folgt $24a_1 \equiv -13(5)$, d.h. $4a_1 \equiv 2(5)$. Es ist $a_1 \equiv 3$ (5) und daher

$$-\frac{13}{24} = 3 + 5 \cdot \left(-\frac{17}{24}\right)$$

Nacheinander sehen wir auch, dass $-\frac{17}{24} \equiv a_2(5)$, $24a_2 \equiv -17(5)$, $4a_2 \equiv 3(5)$ ist, also $a_2 \equiv 2(5)$, d.h. wieder

$$-\frac{17}{24} = 2 + 5 \cdot \left(-\frac{13}{24}\right)$$

Wieder folgt

$$-\frac{13}{24} = 3 + 5 \cdot \left(-\frac{17}{24}\right)$$

Die Folge der Koeffizienten ist periodisch:

2, 3, 2, 3, 2, 3, ...

Es ist

$$-\frac{17}{24} = 2 + 3 \cdot 5 + 2 \cdot 5^2 + 3 \cdot 5^3 + ... + 3 \cdot 5^{2k-1} + \left(-\frac{17}{24}\right) \cdot 5^{2k}$$

(für alle $k \geq 0$).

2. $p = 5$, $r = \frac{17}{24}$
$\frac{17}{24} \equiv a_0(5)$, $2 \equiv 4a_0(5)$, $a_0 \equiv 3(5)$, $\frac{17}{24} = 3 + 5 \cdot \left(-\frac{11}{24}\right)$
$-\frac{11}{24} \equiv a_1(5)$, $4 \equiv 4a_1(5)$, $a_1 \equiv 1(5)$, $-\frac{11}{24} = 1 + 5 \cdot \left(-\frac{7}{24}\right)$
$-\frac{7}{24} \equiv a_2(5)$, $3 \equiv 4a_2(5)$, $a_2 \equiv 2(5)$, $-\frac{7}{24} = 2 + 5 \cdot \left(-\frac{11}{24}\right)$

$$\frac{17}{24} = 3 + 1 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3 + 2 \cdot 5^4 + ... + 1 \cdot 5^{2k-1} + 2 \cdot 5^{2k} + \left(-\frac{11}{24}\right) \cdot 5^{2k+1}$$

Die Koeffizientenfolge ist 3, 1, 2, 1, 2, ... Sie ist periodisch mit der Periode 1, 2. Vor der Periode tritt noch die Ziffer 3 auf.

Jetzt beweisen wir die Behauptung, dass die Koeffizientenfolge a_0,a_1,a_2,... von einem Index an stets periodisch wird.
Ist $r = 0$, so sind diese Zahlen alle gleich 0.
Ist r eine natürliche Zahl, so sind von einem bestimmten Index an alle Zahlen gleich 0 (die Zahlenfolge wird also ebenfalls periodisch; die Periode besteht aus der einen Zahl 0).
Ist $r = -1$, so ist die Koeffizientenfolge vom Index 0 an periodisch; die Periode besteht aus der einen Zahl $p - 1$ (also $a_0 = a_1 = ... = p - 1$).

Ist $r = (-1)n$ $(n \geq 1)$ eine negative ganze Zahl, so ist die Koeffizientenfolge von einem bestimmten Index ≥ 1 periodisch; die Periode besteht ebenfalls aus der einen Zahl $p - 1$.
In der Tat, es ist in (9) auch r_1 eine negative ganze Zahl, die überdies größer als r ist, $r_1 > r$. Dies folgt aus $0 < -r_1 < -r$. In der Tat ist $-r_1 < (-r_1)p$ und auch noch $-r_1 < (-r_1)p - a_0$ $(= -r)$ (Wegen $0 \leq a_0 \leq p - 1$ ist ja $-p < -a_0 \leq 0$.)
Ebenso ist r_2 größer als r_1. Entsprechendes gilt für alle weiteren r_i:

$$r < r_1 < r_2 < ... \leq -1$$

Die Zahlen $r_1, r2, r_3$,... sind verschiedene negative ganze Zahlen zwischen r und -1. Da es nur endlich viele solche Zahlen gibt (nämlich $r, r + 1, r + 2, ..., -2, -1$), müssen von einer Stelle (sagen wir k) an alle r_i gleich -1 sein:

$$\begin{aligned} -n &= a_0 + r_1 p \\ r_1 &= a_1 + r_2 p \\ &... \\ r_{k-1} &= a_{k-1} + r_k p \quad \text{mit} \quad r_k = -1 \\ r_k &= -1 = (p-1) + (-1)p \end{aligned}$$

Jetzt sei r eine für-p-ganze rationale Zahl, für die wir $0 \leq r < 1$ voraussetzen, also

$$r = \frac{a}{b}, \quad p \nmid b, \quad 0 \leq a < b, \quad (a,b) = 1 \tag{11}$$

Multipliziert man alle Gleichungen in (9) mit b, so erhält man

$$\begin{aligned} a &= a_0 b + s_1 p \\ s_1 &= a_1 b + s_2 p \\ &... \\ s_{k-1} &= a_{k-1} b + s_k p \end{aligned} \tag{12}$$

Hierin gilt $0 \leq a_i \leq p-1$, und $s_i = r_i b$ ist eine ganze Zahl (für alle i). Dabei gilt stets (für alle i) $|s_i| < b$)[33] Es ist also $-b < s_i < b$, so dass für s_i nur die Zahlen $-(b-1), ..., -1, 0, 1, ..., b-1$ möglich sind, und dies sind $2b-1$ Zahlen.
Nach höchstens $2b$ Gleichungen in (12) müssen also mindestens zwei gleiche Zahlen unter den $s_1, s_2, ..., s_{2b}$ vorliegen (Schubfachschluss!). Sind $t_0 \geq 0$ und $l \geq 1$ die kleinsten unter den Zahlen $1, 2, 3, ..., 2b$, für die $s_{t_0} = s_{t_0+l}$ ist, dann gilt also

$$\begin{aligned} s_{t_0-1} &= a_{t_0-1}b + s_{t_0}b \\ s_{t_0} &= a_{t_0}b + s_{t_0+1}b \\ &... \\ s_{t_0+l-1} &= a_{t_0+l-1}b + s_{t_0+l}b \\ s_{t_0+l} &= s_{t_0} = a_{t_0}b + s_{t_0+1}b (= a_{t_0+l}b + s_{t_0+l+1}p) \end{aligned}$$

Wegen der eindeutigen Bestimmtheit der a_i und s_i in den Gleichungen folgt dann $a_{t_0} = a_{t_0+1}$, $a_{t_0+1} = a_{t_0+l+1}$ usw., also $a_t = a_{t+l}$ für beliebige $t \geq t_0$. Die Ziffernfolge ist periodisch:

$$a_0, a_1, a_2, ..., a_{t_0-1}, \overline{a_{t_0}, a_{t_0+1}, ..., a_{t_0+l-1}}$$

(der überstrichene Teil deutet die Periode an, während $a_0, a_1, a_2, ..., a_{t_0-1}$ die Vorperiode darstellt).

Damit ist die behauptete Periodizität für alle ganzen Zahlen und für alle für-p-ganze Zahlen r zwischen 0 und 1 bewiesen.

Ist nun r' eine beliebige für-p-ganze rationale Zahl, so gilt

$$r' = [r'] + \{r'\}$$

Dabei ist $[r']$ die größte ganze Zahl, die nicht größer als r' ist.

Beispiele. $[5] = 5$, $[-3] = -3$, $[2 + \frac{1}{2}] = 2$, $[-(4 + \frac{1}{2})] = -5$.

Ferner ist $\{r'\} = r' - [r']$ der gebrochene Teil von r'. (Er ist als Differenz für-p-ganzer Zahlen ebenfalls für-p-ganz.) Für ihn gilt stets $0 \leq \{r'\} < 1$.

Beispiele. $\{5\} = 0$, $\{-3\} = 0$, $\{2 + \frac{1}{2}\} = \frac{1}{2}$, $\{-(4 + \frac{1}{3}\} = \frac{2}{3}$

Der Berechnungsprozess (9), angewendet auf die ganze Zahl $r = [r']$, liefert von einem Index an eine periodische Zahlenfolge $\{a_i\}$. (Die Periode besteht aus der Zahl 0, falls $r > 0$, bzw. aus der Zahl $p-1$, falls $r < 0$ ist.)

[33] Ist $s_k > 0$ und wäre $s_k \geq b$, so wäre

$$s_{k-1} = a_{k-1}b + s_k p \geq (a_{k-1} + p)b > b, ...$$

also schließlich $s_1 > b$, d.h. $a = a_0 b + s_1 p \geq b(a_0 + p) \geq b$, obwohl $a < b$ ist.
Ist $s_k < 0$ und wäre $-s_k > b$, d.h. $s_k < -b$, so wäre

$$s_{k-1} = a_{k-1}b + s_k p < -pb + a_{k-1}b = (ak - 1 - p)b, ...$$

also $-s_{k-1} > (p - a_{k-1})b \geq b$, ..., also schließlich auch $-s_1 > b$, d.h., $s_1 < -b$,

$$a = ba_0 + ps_1 < ba_0 - bp = b(a_0 - p) < 0$$

(wegen $0 \leq a_0 < p$), obwohl $a \geq 0$ ist.

Der Berechnungsprozess (9), angewendet auf die Zahl $r = \{r'\}$, liefert (wie gerade bewiesen wurde) ebenfalls eine periodische Zahlenfolge $\{a_i\}$. Hieraus folgt, dass auch der Berechnungsprozess (9), angewendet auf $r = r' = [r] + \{r\}$, von einem gewissen Index an eine periodische Ziffernfolge $\{a_i\}$ liefern muss.

Um dies einzusehen, schreiben wir uns zunächst die Folge (9) von Gleichungen zuerst für $r = [r']$ und dann für $r = \{r'\}$ auf. Für $[r']$ ist

$$\begin{aligned} [r'] &= b_0 + r_1 p \\ r_1 &= b_1 + r_2 p \\ &\ldots \\ r_k &= b_k + r_0 p \\ r_0 &= g + r_0 p \end{aligned} \tag{9'}$$

(wobei $r_0 = 0$ und $g = 0$, falls $[r'] \geq 0$, und $r_0 = -1$ und $g = p - 1$, falls $[r'] < 0$ ist). Die periodische Folge ist

$$b_0, b_1, b_2, ..., b_k, g, g, g, g, g, ...$$

Für $\{r'\}$ ist

$$\begin{aligned} \{r'\} &= c_0 + s_1 p \\ s_1 &= c_1 + s_2 p \\ &\ldots \\ s_t &= c_t + s_{t+1} p \\ u_1 = s_{t+1} &= h_1 + u_2 p \\ u_2 &= h_2 + u_3 p \\ &\ldots \\ u_l &= h_l + u_1 p \end{aligned} \tag{9''}$$

Die periodische Folge ist

$$c_0, c_1, c_2, ..., c_t, h_1, h_2, ..., h_l, h_1, h_2, ..., h_l, ...$$

Durch Addieren der Gleichungen von (9') zu den entsprechenden von (9'') erhalten wir

$$[r'] + \{r'\} = b_0 + c_0 + (r_1 + s_1)p, ...$$

usw., und von einer gewissen Stelle an

$$\begin{aligned} r_0 + u_1 &= g + h_1 + (r_0 + u_2)p \\ r_0 + u_2 &= g + h_2 + (r_0 + u_3)p \\ &\ldots \\ r_0 + u_l &= g + h_l + (r_0 + u_1)p \quad ... \end{aligned}$$

Die Folge

$$a'_0 = b_0 + c_0, \quad a'_1 = b_1 + c_1, \quad ..., \quad a'_{j+1} = g + h_1, \quad a'_{j+2} = g + h_2, \quad ..., \quad a'_{j+l} = g + h_l, \quad ...$$

ist periodisch, jedoch braucht die Forderung, die an die a_i in der Gleichungskette (9) gestellt wird, dass nämlich $0 \leq a_i \leq p - 1$ sein soll, nicht unbedingt erfüllt zu sein.

Ist $0 \leq a_0' \leq p-1$, so setzen wir $a_0 = a_0'$. Ist jedoch schon $a_0' > p-1$, so suchen wir ein a_0 mit $0 \leq a_0 \leq p-1$, so dass $a_0' \equiv a_0(p)$, also $a_0' = a_0 + d_1 p$ ist. (Im Fall $a_0 = a_0'$ ist $d_1 = 0$ zu setzen.) Dann ist

$$[r'] + \{r'\} = a_0 + (r_1 + s_1 + d_1)p \qquad \text{und} \qquad \text{(G 1)}$$

$$r_1 + s_1 + d_1 = a_1' + d_1 + (r_2 + s_2)p$$

Ist $0 \leq a_1' + d_1 \leq p-1$, so setzen wir $a_1 = a_1' + d_1$. Ist aber $a_1' + d_1 > p-1$, so suchen wir ein a_1 mit $0 \leq a_1 \leq p-1$, so dass $a_1' + d_1 \equiv a_1(p)$, also $a_1' + d_1 = a_1 + d_2 p$ ist. Dann ist

$$r_1 + s_1 + d_1 = a_1 + (r_2 + s_2 + d_2)p \qquad \text{und} \qquad \text{(G 2)}$$

$$r_2 + s_2 + d_2 = a_2' + d_2 + (r_3 + s_3)p$$

So setzen wir die "Reduktion" der a_i auf den Bereich zwischen 0 und $p-1$ fort. Die sich dabei ergebende Folge von Gleichungen (G 1), (G 2), ... entspricht der Gleichungskette (9) für $r = [r'] + \{r'?\}$, und es gilt $0 \leq a_i \leq p-1$.
Bei der Reduktion spielen offenbar nur die Zahlen a_i selbst eine Rolle (und nicht die r_i, s_i, u_i).

Wir können die Reduktion schrittweise an der Folge

$$a_0', a_1', a_2', a_3', ...$$

selbst vornehmen. Der erste Reduktionsschritt ($a_0' = a_0 + d_1 p$, $0 \leq a_0 \leq p-1$) liefert

$$a_0', a_1' + d_1, a_2', a_3', ...$$

Der zweite Reduktionsschritt ($a_1' + d_1 = a_1 + d_2 p$, $0 \leq a_1 \leq p-1$) liefert die Folge

$$a_0', a_1', a_2' + d_2, a_3', ...$$

So wird das Verfahren der schrittweisen Reduktion fortgesetzt. Dazu betrachten wir ein

Beispiel. $p = 3$,

$$a_0' = 7, a_1' = 2, a_2' = 1, a_3' = 5, a_4' = 2, a_5' = 5, a_6' = 2, ...$$

Die Folge ist $7, 2, 1, 3, 5, 2, 5, 2, ...$

Reduktionsschritt	Folge
Erster ($7 = 1 + 2 \cdot 3$)	$1, 4, 1, 5, 2, 5, 2, 5, 2, ...$
Zweiter ($4 = 1 + 1 \cdot 3$):	$1, 1, 2, 5, 2, 5, 2, 5, 2, ...$
Dritter und vierter ($2 = 2 + 0 \cdot 3$, $5 = 2 + 1 \cdot 3$):	$1, 1, 2, 2, 3, 5, 2, 5, 2, ...$
Fünfter ($3 = 0 + 1 \cdot 3$):	$1, 1, 2, 2, 0, 6, 2, 5, 2, 5, 2, ...$
Sechster ($6 = 0 + 2 \cdot 3$):	$1, 1, 2, 2, 0, 0, 4, 5, 2, 5, 2, ...$
Siebenter ($4 = 1 + 1 \cdot 3$)	$1, 1, 2, 2, 0, 0, \underline{1, 6, 2, 5, 2}, ...$
Achter ($6 = 0 + 2 \cdot 3$)	$1, 1, 2, 2, 0, 0, \overline{1, 0, 4, 5, 2}, ...$
Neunter ($4 = 1 + 1 \cdot 3$)	$1, 1, 2, 2, 0, 0, 1, 0, \underline{1, 6, 2, 5, 2}, 5, ...$ usw.

Die reduzierte Folge ist $1, 1, 2, 2, 0, 0, \overline{1, 0}$.

Weitere Beispiele (der überstrichene Teil der Folge ist die Periode).

1. $p = 3$. Ausgangsfolge: $\overline{1, 2, 3, 4, 5}$.
Schrittweise ergibt sich die reduzierte Folge:

$1, 2, 0, 5, 5, 1, 2, 3, 4, 5, 1, 2, 3, 4, 5, ...$
$1, 2, 0, 2, 6, 1, 2, 3, 4, 5, 1, 2, 3, 4, 5, ...$
$1, 2, 0, \underline{2, 0, 3, 2, 3}, 4, 5, 1, 2, 3, 4, 5, ...$
$1, 2, 0, \overline{2, 0, 0, 3, 3}, 4, 5, 1, 2, 3, 4, 5, ...$
$1, 2, 0, 2, 0, 0, 0, 4, 4, 5, 1, 2, 3, 4, 5, ...$
$1, 2, 0, 2, 0, 0, 0, 1, 5, 5, 1, 2, 3, 4, 5, ...$
$1, 2, 0, 2, 0, 0, 0, 1, 2, 6, 1, 2, 3, 4, 5, ...$
$1, 2, 0, 2, 0, 0, 0, 1, \underline{2, 0, 3, 2, 3}, 4, 5, ...$
usw.
Die reduzierte Folge lautet $1, 2, 0, \overline{2, 0, 0, 0, 1}$

2. $p = 5$. Ausgangsfolge: $1, 1, 7, 11, \overline{8, 3}$.
Die reduzierte Folge ist (wie man nach wenig Übung jetzt schon im Kopf ausrechnet):
$1, 1, 2, 2, 0, 0, 4, \overline{4, 3}$.

Die sich nach Reduktion ergebende Zahlenfolge

$$a_0, a_1, a_2, a_3, ... \qquad (0 \leq a_i \leq p-1)$$

ist offenbar stets periodisch, eben weil die Ausgangsfolge

$$a'_0, a'_1, a'_2, ...$$

periodisch ist.
Bisher haben wir vorausgesetzt, dass r für-p-ganz ist. Es sei nun r' eine rationale Zahl, die nicht für-p-ganz, also für-p-gebrochen ist: $r' = \frac{a}{b}$.
Dann teilt p den Nenner b. Es kann auch $p^2, p^3, ...$ den Nenner b teilen. Ist p^h die höchste Potenz von p, die in b aufgeht, so ist $b = p^h b'$ mit $b' \equiv 0(p)$. Schreiben wir jetzt r' in der Form

$$r' = \frac{a}{p^h b'} = \frac{\frac{a}{b'}}{p^h} = \frac{r}{p^h} \qquad (r = \frac{a}{b'}) \tag{13}$$

so ist r eine für-p-ganze Zahl. Für diese haben wir die Darstellung (10), also

$$r = a_0 + a_1 p + a_2 p^2 + ... + a_{k-1} p^{k-1} + r_k p^k$$

mit einer für-p-ganzen Zahl r_k.
Dividieren wir r durch p^h, so erhalten wir

$$r' = \frac{r}{p^h} = \frac{a_0}{p^h} + \frac{a_1}{p^{h-1}} + ... + \frac{a_{h-1}}{p} + a_h + a_{h+1} p + ... + a_{k-1} p^{k-1-h} + r_k p^{k-h}$$

Ist k groß genug (d.h., sind in (10) die Koeffizienten weit genug berechnet), so stehen die Potenzen von p von einer gewissen Stelle ab im Zähler (weil $k - i - h \geq 0$ wird für ein i). Wir können (nach geeigneter Änderung der Bezeichnungen) schreiben:

$$r' = \frac{b_{-n}}{p^n} + ... + \frac{b_{-1}}{p} + b_0 + b_1 p + b_2 p^2 + ... + b_{l-1} p^{-1} + r_l p^l \tag{14}$$

‚Beispiele. 1. $\frac{31}{20}$ ist für-5-gebrochen: $\frac{31}{20} = \frac{\frac{31}{4}}{5}$. Wegen

$$\frac{31}{4} = 4 + 2 \cdot 5 + 5^2 + 5^3 + ... + (-\frac{1}{4}) \cdot 5^k$$

(für alle $k \geq 3$) ist

$$\frac{31}{20} = \frac{4}{5} + 2 + 5 + 5^2 + ... + (-\frac{1}{4}) \cdot 5^{k-1}$$

für alle $k \geq 3$.

2. $\frac{31}{4}$ ist für-2-gebrochen. Es ist

$$31 = 1 + 2 + 2^2 + 2^3 + 2^4 \qquad , \qquad \frac{31}{4} = \frac{1}{2^2} + \frac{1}{2} + 1 + 2 + 2^2$$

Bei den für-p-gebrochenen Zahlen der Form $\frac{a}{p^h}$, wo $a \geq 0$ eine ganze Zahl ist, werden von einer bestimmten Stelle ab alle Koeffizienten gleich Null (weil die Entwicklung für a abbricht). Für die übrigen rationalen Zahlen ergibt sich eine unendliche, jedoch stets periodische Ziffernfolge, was aus dem obigen Ergebnis über für-p-ganze Zahlen folgt.

Beispiel. $p = 7$, $r = \frac{1}{84} = \frac{1/12}{7}$. Aus

$$\frac{1}{12} = 3 + 7 \cdot \left(-\frac{5}{12}\right), \qquad -\frac{5}{12} = 6 + 7 \cdot \left(-\frac{11}{12}\right), \qquad -\frac{11}{12} = 2 + 7 \cdot \left(-\frac{5}{12}\right)$$

folgt

$$\frac{1}{12} = 3 + 6 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 2 \cdot 7^4 + ... \quad \text{usw.}$$

Somit ist

$$\frac{1}{84} = \frac{3}{7} + 6 + 2 \cdot 7 + 6 \cdot 7^2 + 2 \cdot 7^3 + ... \quad \text{usw.}$$

Was bedeutet dieses "usw."? Es ist im vorhergehenden Beispiel

$$\begin{aligned}
\frac{1}{12} &= 3 + 6 \cdot 7 + 2 \cdot 7^2 + \left(-\frac{5}{12}\right) \cdot 7^3 \\
\frac{1}{12} &= 3 + 6 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + \left(-\frac{11}{12}\right) \cdot 7^4 \\
\frac{1}{12} &= 3 + 6 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 2 \cdot 7^4 + \left(-\frac{5}{12}\right) \cdot 7^5 \\
\frac{1}{12} &= 3 + 6 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 2 \cdot 7^4 + 6 \cdot 7^5 + \left(-\frac{11}{12}\right) \cdot 7^6
\end{aligned}$$

Wir können also beliebig lange solche Summen aufschreiben. Wir setzen

$$\begin{aligned}
s_0 &= 3 \\
s_1 &= 3 + 6 \cdot 7 = 45 \\
s_3 &= 3 + 6 \cdot 7 + 2 \cdot 7^2 = 143 \\
s_4 &= 3 + 6 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 = 2291 \qquad ...
\end{aligned}$$

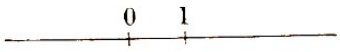
Dann ist

$$\begin{aligned}
\frac{1}{12} - 3 &= 7 \cdot \left(-\frac{5}{12}\right) \\
\frac{1}{12} - s_1 &= \frac{1}{12} - (3 + 6 \cdot 7) = 7^2 \cdot \left(-\frac{11}{12}\right) \\
\frac{1}{12} - s_2 &= \frac{1}{12} - (3 + 6 \cdot 7 + 2 \cdot 7^2) = 7^3 \cdot \left(-\frac{5}{12}\right) \quad ...
\end{aligned}$$

Die Zahlen s_i wachsen immer mehr, die Differenz wird durch eine immer größere Potenz von 7 teilbar[34]. Einerseits wachsen die Werte s_i, sie werden immer größer. Andererseits hat man das Gefühl, dass die Folge $s_0, s_1, s_2, ...$ sich der Zahl $\frac{1}{12}$ "nähert", also eigentlich die Differenzen $\frac{1}{12} - s_i$ immer "kleiner" werden müssten.
Die s_i sind ja die Teilsummen, die in der "Entwicklung" von r auftreten.

Was heißt eigentlich "größer", "kleiner"? Die Zahl 145 ist größer als 45, $6 \cdot 7^3$ ist größer als $2 \cdot 7$, $\frac{1}{4}$ ist größer als $\frac{1}{8}$.
Man kann die rationalen Zahlen anschaulich geometrisch auf der "Zahlengeraden" deuten. Die Größenbeziehung ist dann durch die natürliche Anordnung der rationalen Zahlen auf dieser Zahlengeraden gegeben. Von zwei Zahlen ist die weiter rechts liegende die größere.

Auf einer Geraden fixiert man einen Punkt und schreibt die Zahl 0 an diesen Punkt. Dann trägt man eine Strecke nach rechts ab, deren anderer Endpunkt die Zahl 1 sein soll. Die Länge der Strecke von 0 bis 1 setzt man als Längeneinheit fest:



Die positive ganze Zahl g ist dann g Längeneinheiten rechts vom Nullpunkt entfernt einzutragen, die negative ganze Zahl $-g$ ist g Längeneinheiten links von 0 entfernt einzutragen. Die positiven und die negativen ganzen Zahlen werden nun als eine Menge von äquidistanten Punkten auf dieser Zahlengeraden dargestellt.
Die positiven liegen rechts von 0, die negativen links von 0:

Natürlich kann man immer nur einen Teil der Geraden aufzeichnen. Man muss sie sich in beiden Richtungen verlängert denken.

Jetzt teile man jede Strecke der Länge 1 zwischen den Punkten, die ganze Zahlen darstellen, in n gleiche Teile. Die Teilpunkte sind dann die rationalen Zahlen mit den Nennern n.
Macht man dies für alle $n = 1,2,3,...$, so sind alle rationalen Zahlen durch Punkte auf der Zahlengeraden dargestellt. Die Entfernung eines Punktes r vom Nullpunkt wird der absolute Beitrag von r genannt und mit $|r|$ bezeichnet.
Wenn $r \geq 0$ ist, so ist $|r| = r$; wenn $r < 0$ ist, so ist $|r| = -r$.

Beispiele. $|-5| = 5$, $\left|\frac{5}{2}\right| = \frac{5}{2}$, $\left|-\frac{77}{78}\right| = \frac{77}{78}$, $|1| = 1$, $|-1| = 1$.

Es ist stets $|r| > 0$ (für $r \neq 0$) und $|0| = 0$. (15)
Leicht erkennt man, dass

$$|r+s| \leq |r| + |s| \qquad \text{und} \qquad |rs| = |r| \cdot |s| \tag{16,17}$$

ist.
Die rationale Zahl r heißt kleiner als die rationale Zahl r', falls $r' - r$ positiv ist. Dann liegt r' rechts von r auf der Zahlengeraden (symbolisch: $r < r'$); r' heißt größer als r (symbolisch: $r' > r$). Offenbar gelten folgende Aussagen:

a) $r < r$ ist für keine Zahl richtig.
b) Aus $r < r'$ und $r' < r''$ folgte $r < r''$.

[34] Genauer: für-7-teilbar.

c) Für rationale Zahlen r, r' gilt stets genau eine der Beziehungen $r < r'$ oder $r = r'$ oder $r' < r$.
d) Zu beliebigen positiven rationalen Zahlen r, r' gibt es stets eine natürliche Zahl n mit $nr > r'$ (hierbei mag r so klein und r' so groß gewählt sein, wie man will).

Die Aussage d) wird oft als archimedische Eigenschaft der Ordnungsrelation "$<$" bezeichnet, weil Archimedes[35] sich bei seinen Untersuchungen konsequent darauf stützte (er formulierte den Satz anschaulich geometrisch mit Strecken an Stelle der rationalen Zahlen).

Ist die eben beschriebene Möglichkeit die einzige, um die rationalen Zahlen zu ordnen? Sie ist es nicht!
Eine rationale Zahl r heiße absolut kleiner als die rationale Zahl r', falls $|r| < |r'|$ ist.

Beispiel. Es ist zwar $-\frac{1}{2} < \frac{1}{4}$, jedoch ist $\frac{1}{4}$ absolut kleiner als $-\frac{1}{2}$, wegen $\left|\frac{1}{4}\right| < \left|-\frac{1}{2}\right| = \frac{1}{2}$.

Die obigen Aussagen a), b), c), d) sind auch erfüllt, wenn man darin die Ordnungsrelation "ist kleiner als" durch "ist absolut kleiner als" ersetzt, wie man leicht nachprüfen kann.
Es gibt noch weitere Möglichkeiten, die rationalen Zahlen zu ordnen, und zwar unendlich viele solche Möglichkeiten (nämlich für jede Primzahl eine!).

Wir betrachten eine beliebige Primzahl p. Mittels der Primzahlzerlegung einer beliebigen rationalen Zahl r bekommt man den Exponenten $e_p(r)$. Er ist eine ganze Zahl.
Ist $e_p(r) \geq 0$, so ist r für-p-ganz; falls $e_p(r) < 0$ gilt, ist r für-p-gebrochen. Für rationale Zahlen r, s ist

$$e_p(rs) = e_p(r) + e_p(s) \tag{18}$$

(vgl. (4)). Ferner gilt

$$e_p(r+s) \geq \min(e_p(r), e_p(s)) \tag{19}$$

d.h., $e_p(r+s)$ ist stets größer oder gleich der kleineren der beiden Zahlen $e_p(r)$, $e_p(s)$. In der Tat, jede rationale Zahl lässt sich in der Form

$$r = p^{e_p(r)} r'$$

schreiben, wobei $e_p(r') = 0$ ist. Ferner sei $s = p^{e_p(s)} s'$ mit $e_p(s') = 0$. Es ist, falls z.B. $e_p(r) \geq e_p(s)$ gilt,

$$r + s = \left(r' p^{e_p(r) - e_p(s)} + s'\right) p^{e_p(s)} \tag{20}$$

Somit ist $e_p(r+s) \geq e_p(s)$ (weil nach (20) p auf jeden Fall zur $e_p(s)$-ten Potenz in $r+s$ aufgeht.).
Ist jedoch $e_p(r) \leq e_p(s)$, so folgt analog $e_p(r+s) \geq e_p(r)$. In jedem Fall gilt (19). (Man erkennt leicht, dass in (19) sogar das Gleichheitszeichen steht, sofern $e_p(r) \neq e_p(s)$ ist.)

Beispiele. $e_3(111) = 1$, $e_3(18) = 2$, $e_3(15) = 1$, $e_3(111+18) == e_3(129) = 1$ (wegen $129 = 3 \cdot 43$), $e_3(111+15) = e_3(126) = 2$ (wegen $126 = 3^2 \cdot 14$).

Jetzt setzen wir

$$|r|_p = \left(\frac{1}{p}\right)^{e_p(r)} \qquad \text{für} \quad r \neq 0 \tag{21}$$

Dann gilt

$$|rs|_p = |r|_p \cdot |s|_p \tag{22}$$

[35] Archimedes (287-212 v.u.Z.) ist einer der bedeutendsten griechischen Mathematiker. (Archimedes selbst empfand die Entdeckung einer Formel zur Berechnung des Inhalts einer Kugel als seine größte Leistung.)

wegen

$$|rs|_p = \left(\frac{1}{p}\right)^{e_p(rs)} = \left(\frac{1}{p}\right)^{e_p(r)+e_p(s)} = \left(\frac{1}{p}\right)^{e_p(r)} \left(\frac{1}{p}\right)^{e_p(s)} = |r|_p |s|_p$$

Ferner ist

$$|r+s|_p \leq \max(|r|_p, |s|_p) \leq |r|_p + |s|_p \tag{23}$$

(dies folgt aus (19)) sowie stets $|r|_p > 0$ (für $r \neq 0$) (24)
Für $r = 0$ setzen wir

$$|0|_p = 0 \tag{25}$$

Dies ist sinnvoll, da die Zahl 0 durch jede Potenz von p teilbar ist, also $e_p(0) = \infty$ zu setzen wäre, so dass $\left(\frac{1}{p}\right)^{e_p(0)} = 0$ wäre.
Da $|r|_p$ somit die wesentlichen Eigenschaften eines Betrages hat (vgl. (15), (16), (17) und (24), (25), (23), (22)), heißt $|r|_p$ der p-Betrag von r.

Es ist offenbar $|r|_p < |s|_p$ genau dann, wenn $e_p(r) > e_p(s)$ ist. Die rationale Zahl r heiße für-p-kleiner als die rationale Zahl s (symbolisch: $r < s(p)$), falls $|r|_p < |s|_p$, also $e_p(r) > e_p(s)$ ist; s heiße auch für-p-größer als r (symbolisch: $s > r(p)$).
Ferner sollen r und r' für-p-gleich heißen (symbolisch: $r = r'(p)$), falls $|r|_p = |r'|_p$, also $e_p(r) = e_p(r')$ ist.

Beispiele. $54 < 18(3)$, weil $e_3(54) = e_3(3^3 \cdot 2) = 3 > e_3(18) = e_3(3^2 \cdot 2) = 2$;
$100 < 15(5)$, weil $e_5(100) = e_5(5^2 \cdot 4) = 2 > e_5(15) = 1$;
$\frac{1}{7} > \frac{3}{7}(7)$, weil $e_7(\frac{1}{7}) = -1 < e_7(\frac{3}{5}) = 0$;
$\frac{1}{25} > \frac{3}{15}(5)$, weil $e_5(\frac{1}{25}) = -2 < e_5(\frac{3}{15}) = -1$;
$\frac{9}{8} < \frac{12}{7}(3)$, weil $e_3(\frac{9}{8}) = 2 > e_3(\frac{12}{7}) = 1$;
$\frac{9}{8} > \frac{12}{7}(2)$, weil $e_2(\frac{9}{8}) = -3 < e_2(\frac{12}{7}) = 2$;

Offensichtlich gelten wieder folgende Aussagen:

a) $r < r(p)$ ist für keine Zahl richtig.
b) Aus $r < r'(p)$ und $r' < r''(p)$ folgt $r < r''(p)$.
c) Für rationale Zahlen r, r' gilt stets genau eine der Beziehungen $r < r'(p)$ oder $r \sim r'(p)$ oder $r' < r(p)$.

Jedoch gilt nicht d), sondern
d') Ist $r < r'(p)$, so ist auch $nr < r'(p)$ für jede natürliche Zahl n (für jede ganze Zahl ist $n < 1(p)$ oder $n \sim 1(p)$).

In der Tat, $r < r'(p)$ bedeutet, dass $e_p(r) > e_p(r')$ ist, und dann ist $e_p(rn) = e_p(r) + e_p(n)$ erst recht größer als $e_p(r')$ wegen $e_p(n) \geq 0$; also ist $nr < r'(p)$.
Man sagt: Die rationalen Zahlen werden durch die Ordnungsrelation $< (p)$ nichtarchimedisch geordnet.

Jeder der Beträge gestattet auch die Definition eines Abstands (Entfernung) zwischen zwei rationalen Zahlen r und s. Der gewöhnliche Abstand (auf der Zahlengeraden) ist gegeben durch den absoluten Betrag der Differenz: $|r - s|$.
Der p-Betrag der Differenz, $|r - s|_p$, heißt p-Abstand.

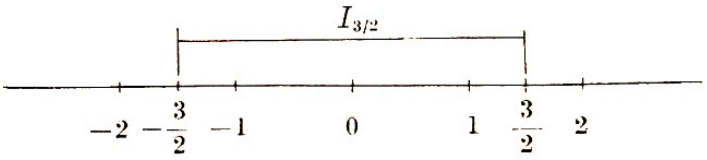
Der Abstand zwischen r und s ist genau dann gleich 0, wenn $r = s$ ist (weil $|r| = 0$ bzw. $|r|_p = 0$ nur für $r = 0$ richtig ist).
Ferner ist die Entfernung von r bis s gleich der von s bis r.

Ist t eine weitere rationale Zahl, so ist die Summe der p-Abstände zwischen r und t sowie s und t größer oder gleich dem Abstand zwischen r und s (Beweis als Aufgabe).
Der absolute Betrag $|r|$ bzw. p-Betrag $|r|_p$ einer rationalen Zahl r gibt somit den Abstand bzw. p-Abstand von r zu 0 an: $|r| = |r - 0|$, $|r|_p = |r - 0|_p$.

Ist r eine beliebige positive rationale Zahl, so bezeichnen wir die Menge aller rationalen Zahlen s, die der Bedingung

$$|s| \leq |r| = r \qquad \text{bzw.} \qquad |s|_p \leq |r|_p$$

genügen, als Intervall I_r bzw. p-Intervall I_r. Im ersten Fall ist ein Intervall anschaulich auf der Zahlengeraden die Menge der rationalen Punkte auf der Strecke zwischen $-r$ einschließlich bis $+r$ einschließlich:



Das p-Intervall I_r enthält alle rationalen Zahlen s, für die $e_p(s) \geq e_p(r)$ ist.
Jetzt haben wir genauere Vorstellungen von den Begriffen "größer" und "kleiner" bei den rationalen Zahlen.

Wir betrachten nun wieder die obige Folge der Zahlen

$$r - s_0, r - s_1, r - s_2, ...$$

Dies ist eine Folge von für-7-ganzen Zahlen, die durch eine immer größere Potenz von 7 teilbar sind, also aus absolut immer größer werdenden Zahlen besteht. Es ist

$$e_7(r - s_0) = 1, e_7(r - s_1) = 2, e_7(r - s_2) = 3, ...$$

also

$$|r - s_0|_7 = \frac{1}{7}, |r - s_1|_7 = \left(\frac{1}{7}\right)^2, |r - s_2|_7 = \left(\frac{1}{7}\right)^3, ...$$

Die 7-Beträge der Zahlen werden immer kleiner. Wenn wir "genügend weit" in der Folge gehen, können wir sicher sein, dass die 7-Beträge der einzelnen Glieder sich "beliebig wenig" von 0 unterscheiden. Wie weit ist aber "genügend weit" und wie wenig ist "beliebig wenig"?

Dies lässt sich gleich allgemeiner für beliebige Folgen rationaler Zahlen erklären. Eine Folge bestehe immer aus unendlich vielen rationalen Zahlen, so dass aufgrund einer bestimmten Vorschrift den natürlichen Zahlen $1, 2,3, ...$ je eine gewisse rationale Zahl $a_1, a_2, a_3, ...$ zugeordnet ist (symbolisch: $\{a_n\}$). Die einzelnen Zahlen a_n heißen Glieder der Folge. Im obigen Beispiel ist

$$a_1 = |r - s_0|_7 = \frac{1}{7}, a_2 = |r - s_1|_7 = \left(\frac{1}{7}\right)^2, a_3 = |r - s_2|_7 = \left(\frac{1}{7}\right)^3, ..., a_n = |r - s_{n-1}|_7 = \left(\frac{1}{7}\right)^n$$

Diese Zahlen werden "beliebig klein", wenn n unbegrenzt wächst, d. h., wenn n gegen unendlich strebt. Wie kann man das beschreiben?

Die Zahlen a_n werden nie gleich 0, auch wenn n noch so groß ist. Vielmehr unterscheiden sich die a_n von 0 immer weniger; die a_n nähern sich dem "Grenzwert" 0, wenn n gegen unendlich strebt (keinesfalls darf man sagen: unendlich "ist").

Eine Zahlenfolge $\{a_n\}$ heißt Nullfolge (symbolisch: $\lim\limits_{n\to\infty} a_n = 0$)[36], wenn sie die folgende Eigenschaft hat:

Ist I_r ein beliebiges Intervall, so liegen fast alle Zahlen a_n innerhalb von I_r. "Fast alle" heißt "alle, mit Ausnahme von höchstens endlich vielen". (Zum Beispiel sind fast alle natürlichen Zahlen größer als 1000000000.)
Wie klein auch I_r sein mag, alle Zahlen a_n„ deren Index größer oder gleich einer gewissen Zahl n_0 ist, liegen dann innerhalb von I_r, so dass also höchstens eine endliche Anzahl $n_0 - 1$ von Gliedern am Anfang der Folge $a_1, a_2, ..., a_{n_0-1}$ außerhalb von I_r liegen kann.

Wenn I_r sehr klein ist (also r sehr klein ist), kann n_0 sehr groß sein, es wird doch nur eine endliche Anzahl von Gliedern der Folge außerhalb I_r liegen, während die unendlich vielen übrigen Glieder innerhalb I_r liegen. I_r ist ein Intervall um 0.
Für jedes solche Intervall müssen also fast alle Zahlen a_n innerhalb I_r liegen, nicht nur für ein solches.

Hiernach ist die Folge $\frac{1}{7}$, $(\frac{1}{7})^2$, $(\frac{1}{7})^3$, ... tatsächlich eine Nullfolge

$$\lim_{n\to\infty} \left(\frac{1}{7}\right)^n = 0$$

Wählen wir nämlich irgendeine positive rationale Zahl r, die wir für sehr klein halten, z.B. $\frac{1}{200}$ oder $\frac{1}{1000}$ ist es möglich, ein Glied der Folge anzugeben, das noch absolut-kleiner ist als die gewählte Zahl und dessen nachfolgende Glieder auch alle kleiner sind als diese Zahl.
Für $r = \frac{1}{1000}$ liegen zwar $\frac{1}{7}, \frac{1}{7^2}, \frac{1}{7^3}$ außerhalb I_r, aber schon $\frac{1}{7^4}$ ist kleiner als $\frac{1}{1000}$, liegt also in I_r, und ebenso auch alle nachfolgenden Glieder. Und dies gilt für jede Zahl r, wie sie auch gewählt wurde, denn stets gibt es ein n, für das $\frac{1}{7^n} < r$ ist.
Bei jeder nur denkbaren Wahl von r liegen fast alle Glieder der Folge innerhalb I_r.

In einer Nullfolge braucht kein einziges Glied gleich 0 zu sein!
Jedoch, wie klein auch $r > 0$ gewählt ist, stets liegen fast alle Glieder a_n zwischen den Zahlen $-r$ und $+r$ (und höchstens endlich viele liegen nicht auf dieser Strecke der Zahlengeraden).

Eine rationale Zahl a heiße Grenzwert[37] einer Folge $a_1, a_2, a_3, ...$, (symbolisch: $\lim\limits_{n\to\infty} a_n = a$), falls

$$\lim |a - a_n| = 0$$

d.h. falls $|a - a_n|$ eine Nullfolge ist.

Eine rationale Zahl a heißt p-Grenzwert einer Folge a_1, a_2, a_3, (symbolisch: $p - \lim\limits_{n\to\infty} a_n = a$), falls

$$\lim_{n\to\infty} |a - a_n|_p = 0$$

ist, d.h. falls $|a - a_n|_p$ eine Nullfolge ist.
Jetzt können wir schreiben

$$7 - \lim_{n\to\infty} s_n = \frac{1}{12} \tag{26}$$

[36] "Limes" (hier abgekürzt: $\lim$) bedeutet "Grenze" und in der Mathematik "Grenzwert". Eine Nullfolge hat den Grenzwert 0.

[37] Über Folgen und Grenzwerte kann man auch in der "Kleinen Enzyklopädie Mathematik" (Leipzig 1965, S. 388 ff.) etwas nachlesen.

In der Tat, die Folge $\left|\frac{1}{12} - s_n\right|_7 = \left(\frac{1}{7}\right)^n$ ist ja eine Nullfolge. Die Zahl $\frac{1}{12}$ ist 7-Grenzwert der Folge

$$\begin{aligned} s_1 &= 3 + 6 \cdot 7 \\ s_2 &= 3 + 6 \cdot 7 + 2 \cdot 7^2 \\ s_3 &= 3 + 6 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 \\ s_4 &= 3 + 6 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 2 \cdot 7^4 \qquad ... \end{aligned}$$

Wir setzen formal

$$s = 3 + 6 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 2 \cdot 7^4 + 6 \cdot 7^5 + ...$$

die Punkte besagen: Man schreibe immer wieder vor den steigenden Potenzen von 7 erst den Koeffizienten 6, dann den Koeffizienten 2 und addiere. Es ist nun

$$\begin{aligned} s - 3 &= 6 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 2 \cdot 7^4 + 6 \cdot 7^5 + ... \\ (s-3)7^2 &= 6 \cdot 7^3 + 2 \cdot 7^4 + 6 \cdot 7^5 + ... \end{aligned}$$

Subtrahieren wir, so erhalten wir

$$s - 3 - (s-3)7^2 = 6 \cdot 7 + 2 \cdot 7^2 = 140$$

also $-48s = -4$, $s = \frac{1}{12}$.

Eigentlich ist s ja absolut "unendlich groß". Diese formale Rechnung erhält erst ihren Sinn durch den Grenzwertprozess (26). Die Teilsummen $s_1, s_2, s_3, s_4, ...$ haben den 7-Grenzwert $\frac{1}{12}$. Die Schreibweise

$$\frac{1}{12} = 3 + 6 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 2 \cdot 7^4 + ...$$

von $\frac{1}{12}$ als unendliche Summe ist nichts weiter als eine bequeme Schreibweise für die Aussage, dass $\frac{1}{12}$ der Grenzwert ist, dem sich die Folge der Teilsummen $s_1, s_2, s_3, ...$ bei wachsendem n nähert.

Ist r eine beliebige für-p-ganze rationale Zahl, so kann man die Zahlen $a_0, a_1, a_2, ...$ nach (9) berechnen. Für diese Zahlenfolge betrachten wir die Summen

$$s_k = a_0 + a_1 p + a_2 p^2 + ... + a_k p^k$$

Wegen (10) ist $r = s_k + r_{k+1} p^{k+1}$, also ist $r - s_k$ für genügend großes k durch jede noch so hohe Potenz von p teilbar, d.h., $r - s_k$ wird für genügend großes k beliebig p-klein.
Daher ist $\{|r - s_k|\}$ eine Nullfolge rationaler Zahlen, r ist p-Grenzwert der Folge $s_1, s_2, s_3, s_4, ...$:

$$r = \lim_{n \to \infty} s_k$$

Man kann dafür wieder

$$r = a_0 + a_1 p + a_2 p^2 + ... + a_k p^k + ... \tag{27}$$

schreiben. Diese unendliche Reihe heißt p-adische Entwicklung der für-p-ganzen Zahl r, symbolische Schreibweise:

$$r = a_0 a_1 a_2 a_3 a_4 ... (p)$$

Beispiele. $\frac{1}{12} = 3{,}6262...(7)$;
$\frac{17}{24} = 3{,}1212...(5)$;
$-\frac{17}{24} = 2{,}3232...(5)$.

Weitere Beispiele. $p = 3$, $r = -\frac{4}{7}$

$$
\begin{aligned}
-\frac{4}{7} &\equiv a_0(3), \quad -4 \equiv 7a_0(3), \quad 2 \equiv a_0(3), \quad -\frac{4}{7} = 2 + \left(-\frac{6}{7}\right)\cdot 3\\
-\frac{6}{7} &\equiv a_1(3), \quad -6 \equiv 7a_1(3), \quad 0 \equiv a_1(3), \quad -\frac{6}{7} = 0 + \left(-\frac{2}{7}\right)\cdot 3\\
-\frac{2}{7} &\equiv a_2(3), \quad -2 \equiv 7a_2(3), \quad 1 \equiv a_2(3), \quad -\frac{2}{7} = 1 + \left(-\frac{3}{7}\right)\cdot 3\\
-\frac{3}{7} &\equiv a_3(3), \quad -3 \equiv 7a_3(3), \quad 0 \equiv a_3(3), \quad -\frac{3}{7} = 0 + \left(-\frac{1}{7}\right)\cdot 3\\
-\frac{1}{7} &\equiv a_4(3), \quad -1 \equiv 7a_4(3), \quad 2 \equiv a_4(3), \quad -\frac{1}{7} = 2 + \left(-\frac{5}{7}\right)\cdot 3\\
-\frac{5}{7} &\equiv a_5(3), \quad -5 \equiv 7a_5(3), \quad 1 \equiv a_5(3), \quad -\frac{5}{7} = 1 + \left(-\frac{4}{7}\right)\cdot 3\\
&\qquad\qquad\qquad\qquad\qquad\qquad\quad -\frac{4}{7} = 2 + \left(-\frac{6}{7}\right)\cdot 3
\end{aligned}
$$

... periodisch weiter

$$-\frac{4}{7} = 2 + 0\cdot 3 + 1\cdot 3^2 + 0\cdot 3^3 + 2\cdot 3^4 + 1\cdot 3^5 + 2\cdot 5^6 + ... = 2{,}\overline{010212}(3)$$

Beispiele (zur Übung). $-\frac{4}{7} = \overline{3{,}021423}(5)$;
$-\frac{2}{3} = 1{,}\overline{31}(5)$;
$\frac{2}{3} = \overline{4{,}13}(5)$

Ist r' eine für-p-gebrochene rationale Zahl, so kann man s in der Form $r' = \frac{r}{p^h}$ darstellen, wobei r eine für-p-ganze Zahl ist. Setzt man

$$
\begin{aligned}
s_1 &= \frac{b_{-n}}{p^n} + ... + \frac{b_{-1}}{p} + b_0 + b_1 p\\
s_2 &= \frac{b_{-n}}{p^n} + ... + \frac{b_{-1}}{p} + b_0 + b_1 p + b_2 p^2\\
&...
\end{aligned}
$$

(vgl. (14), so ist $\{|r' - s_k|_p\}$ wieder eine Nullfolge und r' der p-Grenzwert von $\{s_k\}$. Man erhält eine Entwicklung der Form

$$r' = b_{-n}p^{-n} + ... + b_{-1}p^{-1} + b_0 + b_1 p + b_2 p^2 + ... \quad (b_{-n} \neq 0) \tag{28}$$

(p-adische Entwicklung der für-p-gebrochenen Zahl r'; symbolische Schreibweise:
$r = b_{-n}...b_{-1}b_0{,}b_1 b_2...(p)$).

Beispiele. $\frac{31}{4} = 111{,}11(2)$; $\frac{1}{84} = 36{,}\overline{26}(7)$.

Als Zusammenfassung unserer bisherigen Untersuchungen über p-adische Entwicklungen können wir nun den folgenden Satz formulieren:

Satz 13. Es sei p eine Primzahl und r eine rationale Zahl. Die Zahl r besitzt eine p-adische Entwicklung, d. h. ist eine unendliche Summe der Form

$$r = b_m p^m + ... + b_{-1}p^{-1} + b_0 + b_1 p + b_2 p^2 + ...$$

mit $b_m \neq 0$, $0 \leq b_i \leq p-1$ (m ist eine ganze Zahl). Ist r für-p-ganz, so ist $m \geq 0$; ist r für-p-gebrochen, so ist $m < 0$.
Ist r eine nichtnegative ganze Zahl oder eine gebrochene Zahl der Form $\frac{a}{p^h}$ (mit einer nichtnegativen ganzen Zahl a), so sind von einer bestimmten Stelle an alle Koeffizienten b_i gleich 0. Sonst bilden die Koeffizienten b_i eine periodische Ziffernfolge (eine Vorperiode zugelassen).

Es gibt ein altes, zunächst verblüffendes Verfahren zur Multiplikation natürlicher Zahlen m, n. Man dividiert m fortgesetzt durch 2 (ohne auf den Rest zu achten) und schreibt die Teiler bis zur Zahl 1 untereinander. Daneben schreibt man n, $2n$, $4n$, $8n$, ... usw. Man erhält zwei Spalten.

Beispiel. $m = 37$, $n = 3$

37	3
18	6
9	12
4	24
2	48
1	96

Nun streicht man alle Zeilen, in denen in der ersten Spalte eine gerade Zahl steht (diese Zeilen werden in den folgenden Beispielen durch * gekennzeichnet), addiert die übrigbleibenden Zahlen der zweiten Spalte und erhält als Summe mn.

Beispiele.

37	3		25	25		16	24*	
18	6*		12	50*		8	48*	
9	12		6	100*		4	96*	
4	24*		3	200		2	192*	
2	48*		1	400		1	384	
1	96			625	$= 23 \cdot 25$		384	$= 16 \cdot 24$
	111	$= 37 \cdot 3$						

12	45*		101	5	
6	90*		50	10*	
3	180		25	20	
1	360		12	40*	
	540	$= 12 \cdot 45$	6	80*	
			3	160	
			1	320	
				505	$= 101 \cdot 5$

Wieso führt dieses "Multiplikationsverfahren" zu richtigen Resultaten ?
Wir schreiben die 2-adische Entwicklung der natürlichen Zahl m auf. Es ist eine endliche Entwicklung:

$$m = a_0 + a_1 2 + a_2 2^2 + a_3 2^3 + ... + a_k 2^k$$

($a_i = 0$ oder 1 für $i = 0,1,2,...$). Dann ist

$$mn = a_0 n + a_1 2n + a_2 4n + a_3 8n + ... + a_k 2^k n$$

also ist mn Summe der Zahlen der Spalte

$$a_0 n, a_1 2n, a_2 4n, a_3 8n, ..., a_k 2^k n$$

Es bleibt zu zeigen, dass a_i dann und nur dann gleich 0 ist, wenn in der ersten Spalte des Multiplikationsverfahrens eine gerade Zahl steht. Die Zahlen der ersten Spalte sind aber

$$\begin{aligned}
b_0 &= a_0 + a_1 2 + a_2 2^2 + ... + a_k 2^k \\
b_1 &= a_1 + a_2 2 + a_3 2^2 + ... + a_k 2^{k-1} \\
b_2 &= a_2 + a_3 2 + a_4 2^2 + ... + a_k 2^{k-2} \\
b_3 &= a_3 + a_4 2 + a_5 2^2 + ... + a_k 2^{k-3} \\
b_4 &= a_4 + a_5 2 + a_6 2^2 + ... + a_k 2^{k-4} \qquad ...
\end{aligned}$$

also gilt tatsächlich: b_0 ist gerade genau dann, wenn $a_0 = 0$ ist; b_1 ist gerade genau dann, wenn $a_1 = 0$ ist; usw.
Eine Umkehrung von Satz 13 ist der

Satz 14. Gegeben sei eine Vorschrift, nach der jeder ganzen Zahl $i \geq 0$ eine Zahl a_i $(0 \leq a_i \leq p-1)$ zugeordnet wird. Zu der dadurch gegebenen Ziffernfolge $a_0, a_1, a_2, a_3, ...$ bilde man die Summen

$$\begin{aligned}
s_0 &= a_0 \\
s_1 &= a_0 + a_1 p \\
s_2 &= a_0 + a_1 p + a_2 p^2 \\
s_3 &= a_0 + a_1 p + a_2 p^2 + a_3 p^2 \qquad ...
\end{aligned} \tag{29}$$

Dies ist eine Folge ganzer Zahlen. Ist die Ziffernfolge $\{a_i\}$ periodisch (eine Vorperiode zugelassen), so gibt es eine für-p-ganze rationale Zahl r, für die $r = p - \lim\limits_{k\to\infty} s_k$ ist.

Beweis. Ist die Ziffernfolge a_i periodisch, so hat sie die Gestalt

$$(a_0, a_1, a_2,...) = (b_0,b_1,..., b_{m-1}, \overline{c_0, c_1, ..., c_{n-1}}, ...)$$

wobei $b_0, b_1, ..., b_{m-1}$ die Vorperiode und $c_0, c_1, ..., c_{n-1}$ die Hauptperiode darstellt. Setzt man nun

$$b = b_0 + b_1 p + ... + b_{m-1} p^{m-1} \qquad , \qquad c = c_0 + c_1 p + ... + c_{n-1} p^{n-1}$$

so ist

$$\begin{aligned}
s_{m-1} &= b \\
s_{m-1+n} &= b + p^m c \\
s_{m-1+2n} &= b + p^m c(1 + p^n) \\
s_{m-1+3n} &= b + p^m c(1 + p^n + p^{2n}) \\
&... \\
s_{m-1+ln} &= b + p^m c(1 + p^n + p^{2n} + p^{3n} + ... + p^{(l-1)2n})
\end{aligned}$$

Was ist

$$s = 1 + p^n + p^{2n} + p^{3n} + ... + p^{(l-1)n} \qquad ?$$

Bildet man

$$sp^n = p^n + p^{2n} + p^{3n} + ... + p^{(l-1)n} + p^{ln}$$

so ergibt Subtraktion

$$s - sp^n = 1 - p^{ln} \qquad \text{d.h.} \qquad s = \frac{1 - p^{ln}}{1 - p^n}$$

Somit folgt

$$s_{m-1+ln} = b + p^m c \left(\frac{1-p^{ln}}{1-p^n} \right)$$

Nun ist[38]

$$p - \lim_{l\to\infty} \frac{1-p^{ln}}{1-p^n} = \frac{1}{1-p^n}$$

und daher[39]

$$p - \lim_{l\to\infty} s_{m-1+ln} = b + p^m c \left(\frac{1}{1-p^n} \right)$$

Die für-p-ganze rationale Zahl

$$r = b + p^m \left(\frac{1}{1-p^n} \right) \tag{30}$$

ist also tatsächlich p-Grenzwert der Folge der Summen s_k.[40]

Beispiel. $p = 5$, $a_0 = 4$, $a_1 = 1$, $a_2 = 3$, $a_3 = 1$, $a_4 = 3$, ... (periodisch weiter, Periode $(1, 3)$); $m = 1$, $n = 2$, $b = 4$, $c = 1 + 3 \cdot 5 == 16$. Nach Formel (30) ist

$$r = 4 + 5 \cdot 16 \left(\frac{1}{1-25} \right) = \frac{16}{24} = \frac{2}{3}$$

Die Formel (30) braucht man aber gar nicht zu kennen. Wir wissen ja, dass die unendliche Summe

$$4 + 1 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + ...$$

[38] Es ist nämlich

$$\left| \frac{1-p^{ln}}{1-p^n} - \frac{1}{1-p^n} \right|_p = \left| \frac{-p^{ln}}{1-p^n} \right|_p = \left(\frac{1}{p} \right)^{ln}$$

(man beachte $(p, 1-p^n) = 1$, so dass p nicht im Nenner vorkommt, also $e_p\left(\frac{-p^{ln}}{1-p^n}\right) = ln$ ist) und $\lim_{l\to\infty} \left(\frac{1}{p}\right)^{ln} = 0$.

[39] Setzt man $r = b + p^m c \left(\frac{1}{1-p^n}\right)$, so ist

$$|r - s_{m-1+ln}| = \left| b - b + p^m c \left(\frac{1}{1-p^n} - \frac{1-p^{ln}}{1-p^n} \right) \right|_p = \left| p^m c \frac{p^{ln}}{1-p^n} \right|_p$$
$$= |c|_p \cdot \left| \frac{p^{m+ln}}{1-p^n} \right|_p = \left(\frac{1}{p} \right)^{e_p(c)} \left(\frac{1}{p} \right)^{m+ln} \quad \text{und} \quad \lim_{l\to\infty} \left(\frac{1}{p} \right)^{e_p(c)+m+ln} = 0$$

[40] Wir haben die Folgen $s_1, s_2, s_3, s_4, ...$ und $s_{m-1+n}, s_{m-1+2n}, s_{m-1+3n}, s_{m-1+4n}, ...$ die zweite ist eine Teilfolge der ersten und hat den p-Grenzwert $r = p - \lim_{l\to\infty} s_{m-1+ln}$. Dann gilt auch $p - \lim_{k\to\infty} s_k = r$.

Für jedes $k \geq m-1+n$ gibt es nämlich ein $l \geq 1$ (das von k abhängt), so dass $m-1+(l+1)n \geq k \geq m-1+ln$ ist, und dann ist

$$s_k = s_{m-1+ln} + c_0 p^{m+ln} + c_1 p^{m-ln+1} + ... + c_{i(k)} p^{m+ln+i(k)}$$

(mit einem $0 \leq i(k) \leq n-1$),

$$|r - s_k|_p = |r - s_{m-1+ln} - c_0 p^{m+ln} - ... - c_{i(k)} p^{m+ln+i(k)}|_p$$
$$\leq |r - s_{m-1+ln}|_p + |-c_0 p^{m+ln}|_p + ... + |-c_{i(k)} p^{m+ln+i(k)}|_p$$

Jeder der p-Beträge rechts strebt für $l \to \infty$ gegen: 0. Mit $k \to \infty$ gilt auch $l \to \infty$, und daher ist auch $\lim_{k\to\infty} |r - s_k|_p = 0$, d.h. $r = p - \lim_{k\to\infty} s_k$.

eine rationale Zahl r darstellt (das behauptet Satz 14); also

$$r = 4 + 1 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + ...$$

Dann ist

$$r - 4 = 1 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 + 3 \cdot 5^4 + ...$$

und

$$(r-4)5^2 = 1 \cdot 5^3 + 3 \cdot 5^4 + ...$$

Subtraktion liefert $(r-4)(1-5^2) = 1 \cdot 5 + 3 \cdot 5^2 = 5(1 + 3 \cdot 5)$, d.h.

$$r = 4 + 5 \cdot 16 \left(\frac{1}{1-25}\right) = \frac{2}{3}$$

wie oben.

Weiteres Beispiel. $p = 5$, $a_0 = 1$, $a_1 = 2$, $a_2 = 3$, $a_3 = 4$, $a_4 = 0$, $a_5 = 2$, $a_6 = 3$, $a_7 = 4$, $a_8 = 0$; ... (periodisch weiter, Periode $(2,3,4,0)$); $m = 1$, $n = 4$.
Es ist

$$\begin{aligned} r - 1 &= 2 \cdot 5 + 3 \cdot 5^2 + 4 \cdot 5^3 + 0 \cdot 5^4 + 2 \cdot 5^5 + ... \\ (r-1)5^4 &= 2 \cdot 5^5 + ... \\ (r-1) - 5^4(r-1) &= 2 \cdot 5 + 3 \cdot 5^2 + 4 \cdot 5^3 = 585 \\ r &= 1 - \frac{585}{624} = \frac{13}{108} = \frac{1}{16} \end{aligned}$$

also

$$\frac{1}{16} = 1,\overline{2340}(5)$$

In den p-adischen Entwicklungen

$$r = a_0,a_1a_2a_3...(p)$$

ist es nicht notwendig, die Zahlen a_i aus der Menge $0,1,2,...,p-1$ zu nehmen. In den Gleichungen (9) sind ja die Zahlen a_i so bestimmt, dass

$$r \equiv a_0(p), \quad r_1 \equiv a_1(p), \quad r_2 \equiv a_2(p), \quad ...$$

ist, und es muss durchaus nicht $0 \leq a_i \leq p-1$ sein.

Beispiel. $p = 7$, $r = \frac{1}{12}$

$$\frac{1}{12} \equiv a_0(7), \quad 1 \equiv 12a_0(7), \quad 1 \equiv 5a_0(7), \qquad (\text{da } 12 \equiv 5(7))$$

also $a \equiv 3(7)$, z.B. $a_0 = 10$:

$$\frac{1}{12} = 10 + 7 \cdot \left(-\frac{17}{12}\right), \quad -\frac{17}{12} \equiv a_1(7), \quad -17 \equiv 12a_1(7), \quad 4 \equiv 5a_1(7)$$

da $-17 \equiv 4(7)$ und $12 \equiv 5(7)$), also $a_1 \equiv 5(7)$, z.B. $a_1 = 5$:

$$-\frac{17}{12} = 5 + 7 \cdot \left(-\frac{11}{12}\right), \quad -\frac{11}{12} \equiv a_2(7), \quad -11 \equiv 12a_2(7), \quad 3 \equiv 5a_2(7)$$

also $a_2 \equiv= 2(7)$, z.B. $a_2 = 16$:

$$-\frac{11}{12} = 16 + 7 \cdot \left(-\frac{29}{12}\right), \quad -\frac{29}{12} \equiv a_3(7), \quad 6 \equiv 5a_3(7)$$

also $a_3 \equiv 4(7)$, z.B. $a_3 = 4$:

$$-\frac{29}{12} = 4 + 7 \cdot \left(-\frac{11}{12}\right)$$

Somit ist

$$\frac{1}{12} = 10{,}5\overline{164}(7)$$

Nimmt man also in den Gleichungen (9) nicht die kleinsten positiven ganzen Zahlen a_0, a_i $(0 \leq a_i \leq p-1)$, zu denen r bzw. r_i für p kongruent sind, sondern irgendwelche ganzen Zahlen a_0', a_i' (ohne die Einschränkung $(\geq 0, \leq p-1)$), so ergeben sich allgemeinere Entwicklungen

$$r = a_0' + a_1'p + a_2'p^2 + ...(p)$$

Die Darstellungen

$$r = a_0{,}a_1a_2a_3...(p)$$

mit $0 \leq a_i \leq p-1$ heißen reduzierte p-adische Entwicklungen, im Unterschied zu

$$r = a_0'{,}a_1'a_2'a_3'...(p)$$

(wo die a_i' nicht auf den Bereich zwischen 0 und $p-1$ eingeschränkt sind).
Es lässt sich leicht ein Verfahren für die Verwandlung der allgemeineren Entwicklungen in reduzierte p-adische Entwicklungen angeben.
Betrachten wir zunächst das obige Beispiel.

$\frac{1}{12} = 10{,}5\overline{164}(7)$, d.h.

$$\frac{1}{12} = 10 + 5 \cdot 7 + 16 \cdot 7^2 + 4 \cdot 7^3 + 16 \cdot 7^4 + 4 \cdot 5 + ...$$
$$\frac{1}{12} = (3+7) + 5 \cdot 7 + (2 + 2 \cdot 7) \cdot 7^2 + 4 \cdot 7^3 + (2 + 2 \cdot 7) \cdot 7^4 + 4 \cdot 5 + ...$$
$$\frac{1}{12} = 3 + \cdot 6 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + 2 \cdot 7^4 + 6 \cdot 7^5 + ...$$

also

$$\frac{1}{12} = 3{,}\overline{62}(7)$$

und dies ist die reduzierte 7-adische Entwicklung von $\frac{1}{12}$.

Allgemein sei in

$$r = a_0{,}a_1a_2a_3...a_{k-1}a_k'a'k + 1...(p)$$

a_k' die erste Zahl, die nicht aus der Menge $\{0{,}1{,}...{,}p-1\}$ ist.
Dann gilt $a_k' \equiv a_k(p)$ mit einer Zahl a_k, für die $0 \leq a_k \leq p-1$ ist, also $a_k' = a_k + b_{k+1}p$ (mit einer ganzen Zahl b_{k+1}). Dann ist auch

$$r = a_0{,}a_1a_2a_3...a_{k-1}a_k(b_{k+1} + a_{k+1}')a'k + 2...(p)$$

und hier ist bereits eine Zahl mehr aus $\{0{,}1{,}2{,}..{,}p-1\}$. So kann man weiter fortfahren.

Beispiele.

$$r_0 = 1{,}2\ 3\ 4\ 5\ 6\ 7\ 8\ 9\ 10\ 11\ 12\ 13\ 14\ 15\ ...(5)$$

Es ist (wie man schon im Kopf ausrechnen kann)

$$r_0 = 1{,}234\overline{01234}(5)$$

Ferner ist[41]

$$r_1 = p{,}p-1\ p-1\ p-1\ ... \equiv 0(p)$$
$$r_2 = p{,}2p-1\ 3p-2\ 4p-3\ ... \equiv 0(p)$$

Nun seien zwei Entwicklungen

$$a_0 + a_1p + a_2p^2 + a_3p^3 + ... \qquad , \qquad b_0 + b_1p + b_2p^2 + b_3p^3 + ...$$

gegeben, von denen wir wissen, dass sie rationale Zahlen r, r' darstellen. Wie kann man an diesen Entwicklungen ablesen, wann sie die gleiche rationale Zahl darstellen?

Ist $r = r'$, so ist erst recht $r \equiv r'(p^h)$ für jedes h. Diese Bedingung ist aber auch hinreichend: Sind die Entwicklungen für jede (noch so hohe) p-Potenz kongruent, so stellen sie die gleiche rationale Zahl dar. Ist also

$$\begin{gathered} a_0 \equiv b_0(p) \\ a_0 + a_1p \equiv b_0 + b_1p(p^2) \\ a_0 + a_1p + a_2p^2 \equiv b_0 + b_1p + b_2p^2(p^2) \\ ... \\ a_0 + a_1p + ... + a_hp^h \equiv b_0 + b_1p + ... + b_hp^h(p^{h+1}) \end{gathered}$$

für alle h, so ist $r = r'$ (Warum ?).
Sind die Entwicklungen reduziert, so gilt natürlich sogar:
Es ist $r = r'$ genau dann, wenn $a_i = b_i$ für alle i.

Beispiel.

$$r = 8 + 3 \cdot 5 + 9 \cdot 5^3 + 7 \cdot 5^4 + 6 \cdot 5^5$$
$$r' = 3 + 4 \cdot 5 + 4 \cdot 5^3 + 3 \cdot 5^4 + 2 \cdot 5^5 + 1 \cdot 5^6$$

Es ist

$$\begin{aligned} &r \equiv 8 \equiv 3 \equiv r'(5) \\ &r \equiv 8 + 3 \cdot 5 \equiv 3 + 4 \cdot 5 \equiv r'(5^2) \\ &r \equiv 3 + 4 \cdot 5 \equiv r'(5^3) \\ &r \equiv 8 + 3 \cdot 5 + 9 \cdot 5^3 \equiv 3 + 4 \cdot 5 + 4 \cdot 5^3 \equiv r'(5^4) \\ &r \equiv 8 + 3 \cdot 5 + 9 \cdot 5^3 + 7 \cdot 5^4 \equiv 3 + 4 \cdot 5 + 4 \cdot 5^3 + 3 \cdot 5^4 \equiv r'(5^5) \\ &r \equiv 3 + 4 \cdot 5 + 4 \cdot 5^3 + 3 \cdot 5^4 + 2 \cdot 5^5 \equiv r'(5^6) \\ &r \equiv 3 + 4 \cdot 5 + 4 \cdot 5^3 + 3 \cdot 5^4 + 2 \cdot 5^5 + 5^6 \equiv r'(5^k), \quad \text{für alle } k \geq 7 \end{aligned}$$

also $r = r'$ (was man nach einiger Übung meist such ohne schriftliche Rechnung - durch Kopfrechnen - überprüfen kann).

[41] Selbstverständlich ist auch

$$r'_n = 0{,}0...0pp-1p-1... \equiv 0(p)$$

ganz gleich, wieviel Nullen vor der Ziffer p stehen.

Wir können rationale Zahlen addieren, multiplizieren, subtrahieren und dividieren. Wie spiegeln sich nun diese Rechenoperationen in den p-adischen Entwicklungen wider?

Es sei

$$r = a_0,a_1a_2a_3...(p) \qquad , \qquad r' = b_0,b_1b_2b_3...(p)$$

Welche p-adische Entwicklung haben $r + r'$, rr', $r - r'$, $\frac{r}{r'}$?
Wir betrachten zunächst die Summe. Aus

$$r = a_0 + a_1p + a_2p^2 + a_3p^3 + ... \qquad , \qquad r' = b_0 + b_1p + b_2p^2 + b_3p^3 + ...$$

folgt

$$r \equiv a_0(p), \quad r \equiv a_0 + a_1p(p^2), \quad r \equiv a_0 + a_1p + a_2p^2(p^3), \quad ... \qquad \text{und}$$
$$r' \equiv b_0(p), \quad r' \equiv b_0 + b_1p(p^2), \quad r' \equiv b_0 + b_1p + b_2p^2(p^3), \quad ...$$

Addiert man diese Kongruenzen, so erhält man

$$\begin{aligned} r + r' &\equiv a_0 + b_0(p) \\ r + r' &\equiv (a_0 + b_0) + (a_1 + b_1)p(p^2) \\ r + r' &\equiv (a_0 + b_0) + (a_1 + b_1)p + (a_2 + b_2)p^2(p^3) \\ &... \end{aligned}$$

Setzt man $s = c_0 + c_1p + c_2p^2 + ...$ mit $c_i = a_i + b_i$ für alle $i \geq> 0$, so gilt

$$\begin{aligned} s &\equiv a_0 + b_0(p) \\ s &\equiv (a_0 + b_0) + (a_1 + b_1)p(p^2) \\ s &\equiv (a_0 + b_0) + (a_1 + b_1)p + (a_2 + b_2)p^2(p^3) \\ &... \end{aligned}$$

Die Zahlen $r + r'$ und s sind für jede noch so hohe Potenz von p kongruent, also sind sie gleich, und daher ist

$$r + r' = (a_0 + b_0) + (a_1 + b_1)p + (a_2 + b_2)p^2 + ...$$

Die p-adische Entwicklung der Summe zweier rationaler Zahlen hat als Koeffizienten die Summe der entsprechenden Koeffizienten der einzelnen Entwicklungen.

Beispiele $-\frac{2}{3} = 1,\overline{31}(5)$, $\frac{2}{3} = 4.\overline{13}(5)$, $(-\frac{2}{3}) + \frac{2}{3} = 0$

$$\begin{array}{r} 4,1313...\ (5) \\ +1,3131...\ (5) \\ \hline 5,4444...\ (5) \end{array} = 0\ (5)$$

$-\frac{4}{7} = 3,02142\overline{302142}(5)$, $-\frac{4}{7} + \frac{2}{3} = \frac{2}{21}$,

$$\begin{array}{r} 3,021423021423...\ (5) \\ +4,131313131313...\ (5) \\ \hline 7,152736152736...\ (5) \\ = 2,203241203241...\ (5) \end{array} = 2,\overline{203241}\ (5) = \frac{2}{21}$$

Zur Probe kann man die 5-adische Entwicklung von $\frac{2}{21}$ noch einmal bestimmen:

$$\begin{aligned}
&\frac{2}{21} \equiv 2(5), \qquad (2 \equiv 2 \cdot 21 = 42(5)), \qquad \frac{2}{21} - 2 = -\frac{40}{21} = 5 \cdot (-\frac{8}{21}) \\
&-\frac{8}{21} \equiv 2(5), \qquad (-8 \equiv 42(5)), \qquad -\frac{8}{21} - 2 = -\frac{50}{21} = 5 \cdot (-\frac{10}{21}) \\
&-\frac{10}{21} \equiv 0(5), \qquad -\frac{10}{21} = 5 \cdot (-\frac{2}{21}) \\
&-\frac{2}{21} \equiv 3(5), \qquad (-2 \equiv 63(5)), \qquad -\frac{2}{21} - 3 = -\frac{65}{21} = 5 \cdot (-\frac{13}{21}) \\
&-\frac{13}{21} \equiv 2(5), \qquad (-13 \equiv 42(5)), \qquad -\frac{13}{21} - 2 = -\frac{55}{21} = 5 \cdot (-\frac{11}{21}) \\
&-\frac{11}{21} \equiv 4(5), \qquad (-11 \equiv 84(5)), \qquad -\frac{11}{21} - 4 = -\frac{95}{21} = 5 \cdot (-\frac{19}{21}) \\
&-\frac{19}{21} \equiv 1(5), \qquad (-19 \equiv 21(5)), \qquad -\frac{19}{21} - 1 = -\frac{40}{21} = 5 \cdot (-\frac{8}{21})
\end{aligned}$$

Jetzt untersuchen wir das Produkt. Aus

$$\begin{aligned}
&r \equiv a_0(p), \quad r \equiv a_0 + a_1 p(p^2), \quad r \equiv a_0 + a_1 p + a_2 p^2(p^3), ... \\
&r' \equiv b_0(p), \quad r' \equiv b_0 + b_1 p(p^2), \quad r' \equiv b_0 + b_1 p + b_2 p^2(p^3), ...
\end{aligned}$$

folgt durch Multiplikation

$$\begin{aligned}
&rr' \equiv a_0 b_0(p) \\
&rr' \equiv a_0 b_0 + (a_0 b_1 + a_1 b_0) p(p^2) \\
&rr' \equiv a_0 b_0 + (a_0 b_1 + a_1 b_0) p + (a_0 b_2 + a_1 b_1 + a_2 b_0) p^2(p^3) \\
&\quad ...
\end{aligned}$$

Es sei $t = d_0 + d_1 p + d_2 p^2 + d_3 p^3 + ... + d_i p^i + ...$ mit

$$\begin{aligned}
&d_0 = a_0 b_0(p) \\
&d_1 = a_0 b_1 + a_1 b_0 \\
&d_2 = a_0 b_2 + a_1 b_1 + a_2 b_0 \\
&d_3 = a_0 b_3 + a_1 b_2 + a_2 b_1 + a_3 b_0 \\
&\quad ... \\
&d_i = a_0 b_i + a_1 b_{i-1} + a_2 b_{i-2} + ... + a_{i-2} b_2 + a_{i-1} b_1 + a_i b_0 \qquad ...
\end{aligned}$$

für alle $i \geq 0$. Dann gilt

$$t \equiv rr'(p), \quad t \equiv rr'(p^2), \quad t \equiv rr'(p^3), \quad ..., \quad t \equiv rr'(p^j)$$

für alle $j \geq 1$, also $t = rr'$. Die p-adische Entwicklung von rr' ist

$$rr' = a_0 b_0 + (a = b_1 + a_1 b_0) p + (a_0 b_2 + a_1 b_1 + a_2 b_0) p^2 + ...$$

Man kann - ähnlich wie bei der gewöhnlichen Multiplikation - das folgende Schema verwenden: Man multipliziert zuerst b_0 mit allen Koeffizienten $a_0, a_1, a_2, ...$, schreibt die Resultate nacheinander von links nach rechts in die Zeile 0, dann multipliziert man b_1 mit allen Koeffizienten a_0,a_1,a_2,... und schreibt die Resultate, um eine Spalte nach rechts verschoben, von links nach rechts in die Zeile 1 usw.
Dies muss hinreichend oft getan werden (so dass beim Resultat d_0,$d_1 d_2 d_3$... die Periode zu erkennen ist). Das Resultat erhält man durch Addition in den Spalten.

	$a_0,$	a_1	a_2	a_3	a_4	a_5	...	$\cdot b_0,b_1b_2b_3b_4...$
0	a_0b_0	a_1b_0	a_2b_0	a_3b_0	a_4b_0	a_5b_0		
1	↓	a_0b_1	a_1b_1	a_2b_1	a_3b_1	a_4b_1		
2		↓	a_0b_2	a_1b_2	a_2b_2	a_3b_2		
3			↓	a_0b_3	a_1b_3	a_2b_3		
4				↓	a_0b_4	a_1b_4		
5					↓	a_0b_5		
						↓		
	d_0	d_1	d_2	d_3	d_4	d_5	...	

Beispiel. $(-\frac{2}{3}) \cdot (\frac{2}{3}) = -\frac{9}{4}$; $p = 5$

4,	1	3	1	3	...	·	1,	3	1	3	1	...	
4	1	3	1	3	1	3	1	3	1	3	1	...	
↓	12	3	9	3	9	3	9	3	9	3	9	...	
	↓	4	1	3	1	3	1	3	1	3	1	...	
		↓	12	3	9	3	9	3	9	3	9	...	
			↓	4	1	3	1	3	1	3	1	...	
				↓	12	3	9	3	9	3	9	...	
					↓	4	1	3	1	3	1	...	
						↓	12	3	9	3	9	...	
							↓	4	1	3	1	...	
								↓	12	3	9	...	
									↓	4	1	...	
										↓	12	...	
											↓		
4	13	10	23	16	33	22	43	28	53	34	63	...	= 4,32012432012... (5)

Probe: In der Tat ist $-\frac{4}{9} = 4 + 5(-\frac{8}{9})$, $-\frac{8}{9} = 3 + 5(-\frac{7}{9})$,
$-\frac{7}{9} = 2 + 5(-\frac{5}{9})$, $-\frac{5}{9} = 0 + 5(-\frac{1}{9})$, $-\frac{1}{9} = 1 + 5(-\frac{2}{9})$, $-\frac{2}{9} = 2 + 5(-\frac{4}{9})$
also $-\frac{4}{9} = 4,\overline{320124}(5)$.

Für gebrochene Zahlen erfolgt die Multiplikation nach dem gleichen Schema.

Beispiel.[42]

123,4 · 102,03 (5)
1234
0000
2468
0000
36912
12040,1242 (5)

Probe: $1 \cdot 5^{-4} + 2 \cdot 5^{-3} + 4 \cdot 5^{-1} + 1 \cdot 5 + 2 \cdot 5^2 + 4 \cdot 5^3 + 2 \cdot 5^4 = 1805 + \frac{511}{625}$
$1 \cdot 5^{-2} + 2 \cdot 5^{-1} + 3 + 4 \cdot 5 = \frac{11}{25} + 23$
$1 \cdot 5^{-2} + 2 + 3 \cdot 5^2 = \frac{1}{25} + 77$
$(\frac{11}{25} + 23)(\frac{1}{25} + 77) = 1805 + \frac{511}{625}$

[42] Bestimmung der Kommastelle: Hat r vor dem Komma n Stellen und s vor dem Komma m Stellen, so hat rs vor dem Komma $(n-1)+(m-1))+1 = n+m-1$ Stellen.

Unmittelbar klar ist, dass

$$r + r' = (a_0 - b_0) + (a_1 - b_1)p + (a_2 - b_2)p^2 + ...$$

ist. Bei der praktischen Ausführung der Subtraktion ist es oft sinnvoll, zum Minuendus eine nicht-reduzierte Darstellung der Null, z.B. $0{,}000...0pp-1p-1...(p)$ hinzuzufügen.

Beispiele.

1.
5,6342 (7)	
-2,2311 (7)	
3,4031 (7)	

2.
0,005444	...(5)	
3,44123	(5)	
-0,22331	(5)	
3,2233644	... =3,22331 (5)	

3.
0,322222... (3)	
1,010101... (3)	
-0,121212... (3)	
1,211111... (3)	

Welche p-adische Entwicklung hat der Quotient $\frac{r}{r'}$ der beiden rationalen Zahlen $r = a_0{,}a_1a_2...(p)$, $r' = b_0{,}b_1b_2...(p)$ $(\neq 0)$?
Ist $r = 0$, so ist $r/r' = 0$. Sonst bedeutet es keine Einschränkung der Allgemeinheit, wenn wir voraussetzen, dass a_0 und b_0 nicht durch p teilbar sind $((p, a_0) = 1,\ (p, b_0) = 1)$. Gilt nämlich etwa $p \mid a_0$, $p \mid a_1$, ..., $p \mid a_{k-1}$, aber $p \nmid a_k$ (solch ein k gibt es, falls $r \neq 0$), so ist dies in reduzierten Entwicklungen nur für $a_0 = a_1 = ... = a_{k-1} = 0$ möglich, d.h.

$$r = a_k p^k + a_{k+1}p^{k+1} + ... = p^k(a_k + a_{k+1}p + ...)$$

mit $p \nmid a_k$, d.h. $a_k \neq 0$. Analog ist

$$r' = b_{k'}p^{k'} + b_{k'+1}p^{k'+1} + ... = p^{k'}(b_{k'} + a_{k'+1}p + ...)$$

mit $p \nmid b_k$, d.h. $b_{k'} \neq 0$. Es ist dann

$$\frac{r}{r'} = p^{k-k'}\frac{a_k + a_{k+1}p + ...}{b_{k'} + b_{k'1}p + ...}$$

und es sind noch die rationalen Zahlen

$$a_k + a_{k+1}p + ... \qquad \text{und} \qquad b_{k'} + b_{k'+1}p + ...$$

zu dividieren. Für diese ist aber tatsächlich $(p, a_k) = (p, b_{k'}) = 1$.
Ist $\frac{r}{r'} = q$, so $r = qr'$. Setzen wir $q = t_0 + t_1p + t_2p^2 + ...$, so finden wir

$$a_0 + a_1p + a_2p^2 + ... = t_0b_0 + (t_0b_1 + t_1b_0)p + ...$$

t_0, t_1, t_2, ... sind die zu bestimmenden Koeffizienten des Quotienten q, und es gilt

$$\begin{aligned} a_0 &\equiv t_0b_0(p) \\ a_0 + a_1p &\equiv t_0b_0 + (t_0b_1 + t_1b_0)p(p^2) \end{aligned}$$

Bei der praktischen Durchführung der Division $\frac{r}{r'}$ dividiert man also zuerst a_0 durch b_0, d. h., man bestimmt die reduzierte Zahl t_0, für die $b_0t_0 \equiv a_0(p)$ ist. Dieses t_0 erhält man meist leicht durch Probieren.
Dann bildet man die Differenz $r - r't_0$, also

$a_0,$	a_1	a_2	a_3	...
$-b_0t_0$	b_1t_0	b_2t_0	b_3t_0	...
$a_0 - b_0t_0$	$a_1 - b_1t_0$	$a_2 - b_2t_0$	$a_3 - b_3t_0$	...
$= 0$	a_1'	a_2'	a_3'	...

Nun dividiert man wieder a_1' durch b_0, bestimmt also t_1 so, dass $b_0 t_1 \equiv a_1'(p)$ ist, usw.
Man kann wie bei der gewöhnlichen Division das folgende Schema verwenden:

	a_0,	a_1	a_2	a_3	a_4	...	: b_0,$b_1b_2b_3... = t_0$,$t_1t_2...$
-	b_0t_0	b_1t_0	b_2t_0	b_3t_0	b_4t_0	...	
	$a_0 - b_0t_0$	$a_1 - b_1t_0$	$a_2 - b_2t_0$	$a_3 - b_3t_0$	$a_4 - b_4t_0$	...	
=	0	a_1'	a_2'	a_3'	a_4'	...	
-		b_0t_1	b_1t_1	b_2t_1	b_3t_1	...	
		$a_1' - b_0t_1$	$a_2' - b_1t_1$	$a_3' - b_2t_1$	$a_4' - b_3t_1$	...	
=			0	a_1''	a_2''	a_3''	...
-			b_0t_2	b_1t_2	b_2t_2	...	
			$a_1'' - b_0t_2$	$a_2'' - b_1t_2$	$a_3'' - b_2t_2$	...	
=			0	a_1'''	a_2'''	...	usw.

Beispiel. $p = 5$.

	0,00544...	
	1,23	:2,31 $= 3,\overline{104340}...(5)$
6,93=	1,001	
	0,23444...	
	231	
	003444...	
8,124=	3311	
	13344...	
	1001	
	3334...	
	3311	
	0023444...	

Probe: $1 + 2 \cdot 5 + 3 \cdot 5^2 = 86$, $2 + 3 \cdot 5 + 1 \cdot 5^2 = 42$.
$\frac{86}{42} = \frac{43}{21} = 3,\overline{104340}...(5)$, denn

$$\begin{aligned}
43 &= 3 \cdot 21 + 5 \cdot (-4) \\
-4 &= 1 \cdot 21 + 5 \cdot (-5) \\
-5 &= 0 \cdot 21 + 5 \cdot (-1) \\
-1 &= 4 \cdot 21 + 5 \cdot (-17) \\
-17 &= 3 \cdot 21 + 5 \cdot (-16) \\
-16 &= 4 \cdot 21 + 5 \cdot (-20) \\
-20 &= 0 \cdot 21 + 5 \cdot (-4) \\
-4 &= 1 \cdot 21 + 5 \cdot (-5), \qquad ...
\end{aligned}$$

Das Divisionsverfahren kann man nun bequem ausnutzen, um für eine gegebene (etwa positive) rationale Zahl r ihre p-adische Entwicklung zu berechnen. Hat r eine reduzierte Bruchdarstellung der Form $r = \frac{n}{m}$, so schreibt man zuerst die (endlichen) p-adischen Entwicklungen der natürlichen Zahlen n und m auf,

$$n = a_0 + a_1 p + a_2 p^2 + ... + a_h p^h \qquad , \qquad m = b_0 + b_1 p + b_2 p^2 + ... + b_k p^k$$

dividiert diese $(a_0,a_1...a_h; b_0,b_1...b_k)$ und erhält die p-adische Entwicklung von r.

Beispiele. $p = 5$, $r = \frac{3}{2}$:

5,44...	Nebenrechnung
3 : 2 = 4,22 ... (5)	$2t_0 \equiv 3(5)$, $t_0 = 4$
8	
044 ...	$2t_1 \equiv 4(5)$, $t_1 = 2$
4	
044 ...	usw.

$\frac{3}{2} = 4{,}\overline{2}(5) = 4 + 2 \cdot 5 + 2 \cdot 5^2 + 2 \cdot 5^3 + ...$

2. $p = 5$, $r = \frac{31}{4} = \frac{1+1\cdot 5+1\cdot 5^2}{4}$:

	0,544...	Nebenrechnung
	1,11 : 4 = 4,211 ... (5)	$4t_0 \equiv 1(5)$, $t_0 = 4$
16 =	13	
	03	$4t_1 \equiv 3(5)$, $t_1 = 2$
	31	
	0444	$4t_1 \equiv 4(5)$, $t_1 = 1$
	0444	
	4	
	0444	usw.

$\frac{31}{4} = 4{,}2\overline{1}(5) = 4 + 2 \cdot 5 + 1 \cdot 5^2 + 1 \cdot 5^3 + ...$

3. $p = 7$, $r = \frac{1}{12} = \frac{1}{5+1\cdot 7}$:

	0,766...	Nebenrechnung
	1 : 5,1 = 3,6262 ... (7)	$5t_0 \equiv 1(7)$, $t_0 = 3$
15,3 =	15	
	02666	$5t_1 \equiv 2(5)$, $t_1 = 6$
30,6=	231	
	356	$4t_1 \equiv 3(5)$, $t_1 = 2$
10,2=	33	
	2666...	usw.

$\frac{1}{12} = 3{,}\overline{62}(7) = 3 + 6 \cdot 7 + 2 \cdot 7^2 + 6 \cdot 7^2 + 6 \cdot 7^3 + 2 \cdot 7^4 ...$

Für für-p-gebrochene Zahlen werden die Rechenoperationen analog ausgeführt (genauer wird dies in Kapitel III beschrieben) Abschließend bringen wir hier ein einfaches Anwendungsbeispiel der Betrachtungen über p-adische Entwicklungen rationaler Zahlen.

Man bestimme für eine gegebene Zahl n den Wert $e_p(n!)$.
Hier gilt der

Satz 15. Ist n eine natürliche Zahl,

$$n = a_0 + a_1 p + a_2 p^2 + ... + a_{k-1} p^{k-1}$$

ihre p-adische Entwicklung und

$$s_n = a_0 + a_1 + ... + a_{k-1}$$

die p-adische Ziffernsumme von n, so steckt p in $n!$ zum Exponenten

$$\frac{n - s_n}{p - 1}$$

Beispiele. 1. $n = 100$, $p = 5$:
$100 = 0 + 0 \cdot 5 + 4 \cdot 5^2$, $s_{100} = 0 + 0 + 4 = 4$, $\frac{100-4}{4} = 24$
also $100! \equiv 0(5^{24})$; überdies weiß man, dass $5^{25} \nmid 100!$.

2. $n = 100$, $p = 7$:
$100 = 2 + 0 \cdot 7 + 2 \cdot 7^2$, $s_{100} = 2 + 0 + 2 = 4$, $\frac{100-4}{16} = 16$
also $100! \equiv 0(7^{16})$, aber $100! \not\equiv 0(717)$.

Beweis. Es stecke p in der natürlichen Zahl m zum Exponenten e, und es sei $m = 0{,}00...0a_e a_{e+1}...a_r(p)$ die p-adische Entwicklung von m in der reduzierten Form. Dann ist

$$m - 1 = p-1{,}p-1\ p-1...p-1\ a_e - 1\ a_{e+1}a_{e+2}...a_r(p)$$

Nebenrechnung:

p,	$p-1$	$p-1$	$p-1$	...	$p-1$	$p-1$	...	$p-1$	$p-1$	...
0,	0	0	0	...	0	a_e	...	a_r	0	...
-1,	0	0	0	...	0	0	...	0	0	...
$p-1$,	$p-1$	$p-1$	$p-1$	...	a_e-1	(a_e+p-1)	...	(a_r+p-1)	$p-1$	...

$= p-1, p-1\ p-1\ p-1\ ...p-1\ (a_e+1)...a_r00...$
Aus den beiden Ziffernsummen

$$s_m = a_e + a_{e+1} + ... + a_r \qquad , \qquad s_{m-1} = e(p+1) + a_e - 1 + a_{e+1} + ... + a_r$$

folgt durch Subtraktion

$$s_{m-1} - s_m = e(p-1) + (a_e - 1) - a_e \qquad \text{d.h.}$$

$$\frac{s_{m-1} - s_m + 1}{p-1} = e = e_p(m)$$

Wendet man dieses Resultat auf $m = 1, 2, 3, ...,n$ an, so ergibt sich

$$\begin{aligned} e_p(n!) &= e_p(1 \cdot 2 \cdot ... \cdot n) = e_p(1) + e_p(2) + ... + e_p(n) \\ &= \sum_{m=1}^{n} \frac{s_{m-1} - s_m + 1}{p-1} = \frac{1}{p-1} \sum_{m=1}^{n} (s_{m-1} - s_n + 1) \\ &= \frac{1}{p-1}((s_0 - s_1 + 1) + (s_1 - s_2 + 1) + ... + (s_{n-1} - s_n + 1)) = \frac{1}{p-1}(n - s_n) \end{aligned}$$

und das war zu beweisen.

Man kann übrigens $e_p(n!)$ auch anders berechnen. Es gilt

$$e_p(n!) = \left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + \left[\frac{n}{p^4}\right] + ... \qquad (*)$$

Beispiele.
$e_5(100!) = \left[\frac{100}{5}\right] + \left[\frac{100}{25}\right] = 20 + 4 = 24,$

$e_7(100!) = \left[\frac{100}{7}\right] + \left[\frac{100}{49}\right] = 14 + 2 = 16,$

$e_2(100!) = \left[\frac{100}{2}\right] + \left[\frac{100}{4}\right] + \left[\frac{100}{8}\right] + \left[\frac{100}{16}\right] + \left[\frac{100}{32}\right] + \left[\frac{100}{64}\right] = 50 + 25 + 12 + 6 + 3 + 1 = 97$

(Im letzten Beispiel lässt sich der p-Exponent von $n!$ nach der Formel des Satzes schneller finden.)

Zum Beweis von (*) bemerken wir, dass $n!$ das Produkt aller natürlichen Zahlen $\leq n$ ist, dass aber unter den Zahlen von 1 bis n genau $\left[\frac{n}{p}\right]$ vorkommen) die Vielfache von p sind (nämlich p, $2p$, ..., $\left[\frac{n}{p}\right] p$); davon sind $\left[\frac{n}{p^2}\right]$ Zahlen überdies Vielfache von p^2 (nämlich $p^2, 2p^2$, ..., $\left[\frac{n}{p^2}\right] p^2$) und von diesen wieder $\left[\frac{n}{p^3}\right]$ Vielfache von p^3 (nämlich p^3, $2p^3$, ..., $\left[\frac{n}{p^3}\right] p^3$), usw. Der genaue p-Exponent von $n!$ ist also die Summe

$$\left[\frac{n}{p}\right] + \left[\frac{n}{p^2}\right] + \left[\frac{n}{p^3}\right] + ...$$

Ist die Potenz p^k von p groß genug, nämlich $p^k > n$, so wird $\left[\frac{n}{p^k}\right] = 0$, so dass in (*) tatsächlich eine endliche Summe steht.

3 Die p-adischen Zahlen

Es gibt keine rationale Zahl r, so dass $r^2 = 2$ ist. Gäbe es eine solche rationale Zahl, so könnte man sie in der Form $r = \frac{a}{b}$ schreiben (mit ganzen Zahlen $b \neq 0$, a), und es wäre $a^2 = 2b^2$.

Jetzt kann man die 3-adischen Entwicklungen von a und b aufschreiben. Der erste von Null verschiedene Koeffizient der reduzierten 3-adischen Entwicklung von a^2 (und auch von b^2) muss 1 sein.[43]
Jedoch ist der erste von Null verschiedene Koeffizient von $2b^2$ gleich 2, so dass a^2 nicht gleich $2b^2$ sein kann!

Eine Kongruenz der Form

$$x^2 \equiv 2(p) \tag{31}$$

ist nicht für alle Primzahlen p lösbar. Ist z.B. $p = 3$, so gibt es kein solches x. (Es ist ja für $x \equiv 0, 1, 2(3)$ stets $x^2 \equiv 0, 1(3)$, also $x^2 \not\equiv 2(3)$.)
Auch für $p = 5$ nicht. Jedoch gibt es ein $x \equiv a_0(7)$, so dass $a_0^2 \equiv 2(7)$ ist; für $a_0 \equiv 3(7)$ ist z.B. $a_0^2 \equiv 9 \equiv 2(7)$.[44] (auch für $a_0 \equiv 4 \equiv -3(7)$ gilt $(-3)^2 \equiv 9 \equiv 2(7)$).

Auch $x^2 \equiv 2(7^2)$ ist lösbar. Da nämlich erst recht $x^2 \equiv 2(7)$ ist, hat x notwendig die Form $x \equiv a_0(7)$, also $x = a_0 + a_1 7$, z.B. $x = 3 + a_1 7$.
Es muss $(3 + a_1 7)^2 \equiv 2(7^2)$ sein, also

$$\begin{aligned} 9 + 6a_1 \cdot 7 + a_1^2 \cdot 7^2 &\equiv 2(7^2) \\ 1 + 6a_1 &\equiv 0(7) \\ a_1 &\equiv 1(7) \end{aligned}$$

In der Tat ist $(3 + 7)^2 = 10 \equiv 2(7^2)$.
Jetzt existiert auch ein a_2, für das $(3+7+a_2 \cdot 7^2)^2 \equiv 2(7^3)$ ist. $a_2 \equiv 2(7)$ leistet das Verlangte, denn es ist

$$(3 + 7 + 2 \cdot 7^2)^2 = 108^2 = 116624 = 2 + 34 \cdot 7^3$$

Es gibt ferner ein a_3 mit der Eigenschaft, dass

$$(3 + 7 + 2 \cdot 7^2 + a_3 7^3)^2 \equiv 2(7^4)$$

ist es muss

$$(3 + 7 + 2 \cdot 7^2)^2 + 2(3 + 7 + 2 \cdot 7^2)a_3 \cdot 7^3 + a_3^2 \cdot 7^6 \equiv 2(7^4)$$

sein, also (wegen $(3 + 7 + 2 \cdot 7^2)^2 = 2 + 34 \cdot 7^3$)

$$\begin{aligned} 34 \cdot 7^3 + 2(3 + 7 + 2 \cdot 7^2)a_3 \cdot 7^3 &\equiv 0(7^4) \\ 34 + 2 \cdot 108 a_3 &\equiv 0(7) \\ -1 + 2 \cdot 3a_3 &\equiv 0(7) \\ a_3 &\equiv -1(7) \end{aligned}$$

Hat man die Zahlen $a_0 = 3$, $a_1 = 1$, $a_2 = 2$, $a_3 06$, $a_4, a_5, ..., a_k$ so bestimmt, dass

$$(3 + 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + a_4 \cdot 7^4 + ... + a_k \cdot 7^k)^2 \equiv 2(7^{k+1})$$

[43] Ist $c \not\equiv 0(3)$, also $c \equiv 1$ oder $c \equiv 2$ (3), so ist stets $c^2 \equiv 1(3)$.

[44] In der Theorie der quadratischen Reste (einem der schönsten Abschnitte der elementaren Zahlentheorie) zeigt man: Die Kongruenz (31) ist genau für die Primzahlen lösbar, die sich in der Form $1 + 8n$ oder $-1 + 8m$ darstellen lassen; z. B. $p = 7, 17, 23, 31, 41$.

ist, so gibt es stets auch ein a_{k+1}, so dass

$$(3 + 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + a_4 \cdot 7^4 + ... + a_k \cdot 7^k + a_{k+1} \cdot 7^{k+1})^2 \equiv 2(7^{k+2})$$

ist. Man kann diesen Berechnungsprozess so lange durchführen, wie man will. Man erhält also eine unendliche Folge von Zahlen

$$3, 1, 2, 6, a_4, a_5, ..., a_k, ... \qquad (0 \leq a_k \leq 6)$$

Bilden wir mit diesen Zahlen nacheinander

$$\begin{aligned} s_1 &= 3 \\ s_2 &= 3 + 7 \\ s_3 &= 3 + 7 + 2 \cdot 7^2 \\ s_4 &= 3 + 7 + 2 \cdot 7^2 + 6 \cdot 7^3 \\ s_4 &= 3 + 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + a_4 \cdot 7^4 \quad , \qquad ... \end{aligned}$$

so gilt

$$s_1^2 - 2 \equiv 0(7), \quad s_2^2 - 2 \equiv 0(7^2), \quad s_3^2 - 2 \equiv 0(7^3), \quad s_4^2 - 2 \equiv 0(7^4), \quad s_5^2 - 2 \equiv 0(7^5), \quad ...$$

Somit ist die Folge der 7-Beträge

$$|s_1^2 - 2|_7, \quad |s_2^2 - 2|_7, \quad |s_3^2 - 2|_7, \quad ...$$

eine Nullfolge: $\lim\limits_{n\to\infty} |s_n^2 - 2|_7 = 0$, also

$$7 - \lim_{n\to\infty} s_n^2 = 2$$

Gäbe es eine rationale Zahl r mit $7 - \lim\limits_{n\to\infty} s_n^2 = r$, so wäre

$$2 = 7 - \lim_{n\to\infty} s_n^2 = 7 - \lim_{n\to\infty} s_n \cdot 7 - \lim_{n\to\infty} s_n = r \cdot r = r^2$$

also $r^2 = 2$. Eine solche rationale Zahl gibt es jedoch nicht.
Daher tritt die Koeffizientenfolge $3, 1, 2, 6, a_4, a_5, a_6, ...$ nicht in der 7-adischen Entwicklung einer rationalen Zahl auf (diese Folge ist also nicht periodisch).

Hätte die Folge der s_n überhaupt einen 7-Grenzwert s (der dann nicht rational ist), so wäre s in der Form

$$s = 3 + 7 + 2 \cdot 7^2 + 6 \cdot 7^3 + a_4 \cdot 7^4 + a_5 \cdot 7^5 + ...$$

bzw.

$$s = 3{,}126 a_4 a_5 a_6 ...(7)$$

aufzuschreiben. Für dieses s würde $s^2 = 2$ sein. Liegt es nicht nahe, zu sagen, dass die Folge der Zahlen $3, 1, 2, 6, a_4, a_5, a_6$, ... eine wohlbestimmte, aber unter den rationalen Zahlen eben nicht vorhandene Zahl bestimme ?
Diese Zahl könnte als 7-adische Zahl bezeichnet werden. 7-adische Zahlen wären dann alle unendlichen Summen der Form

$$a_0 + a_1 \cdot 7 + a_2 \cdot 7^2 + a_3 \cdot 7^3 + a_4 \cdot 7^4 + ... \quad (0 \leq a_i \leq 6)$$

bzw. die 7-Grenzwerte der rationalen Folgen $\{s_k\}$ mit

$$s_k = a_0 + a_1 \cdot 7 + a_2 \cdot 7^2 + a_3 \cdot 7^3 + ... + a_k \cdot 7^k$$

Dies wäre auch eine natürliche Verallgemeinerung der 7-adischen Entwicklungen der rationalen Zahlen. Dort und nur dort (bei den rationalen Zahlen) ist die Koeffizientenfolge periodisch.
Das Wesentliche an der 7-adischen Entwicklung sind ja die Koeffizienten an den 7-Potenzen, also die Ziffernfolge

$$a_0, a_1 a_2 a_3 ... (7)$$

Wesentlich ist, dass es eine Folge $a_0, a_1, a_2, ...$ von Zahlen gibt (diese können ganze Zahlen zwischen 0 und 7 - 1 sein, aber auch beliebige für-7-ganze rationale Zahlen). Hat man diese Ziffern zu einer gegebenen rationalen Zahl r berechnet , so gilt dann

$$r = 7 - \lim_{n \to \infty} (a_0 + a_1 7 + a_2 7^2 + ... + a_n 7^n)$$

Ein Bereich 7-adischer Zahlen sollte die rationalen Zahlen umfassen. Daher müssen Gleichheit, Anordnung, Addition, Multiplikation der neuen Zahlen so erklärt werden, dass sie für die rationalen Zahlen mit den dort bereits erklärten Begriffen gleichen Namens übereinstimmen.

Da für die für-7-gebrochenen rationalen Zahlen vor dem Komma noch eine endliche Ziffernfolge steht (ist n eine negative ganze Zahl, so schreibt man $r = b_n b_{n+1} ... b_{-1} b_0{,}b_1 b_2 ...$), so wären als 7-adische Zahlen also beliebige Folgen der Form

$$b_n b_{n+1} ... b_{-1} b_0{,}b_1 b_2 ...$$

zu nehmen (wo die b_i für-7-ganze Zahlen sind).
Es ist natürlich sinnvoll, an Stelle von 7 gleich eine beliebige (aber dann fixierte) Primzahl p zu nehmen und p-adische Zahlen zu definieren. Es sei also p eine Primzahl.

Definition A. Eine Folge

$$a_n, a_{n+1}, a_{n+2}, a_{n+3}, ...$$

von für-p-ganzen Zahlen, worin n eine ganze Zahl und $a_n \neq 0$ ist, heißt p-adische Zahl.[45]

Eine p-adische Zahl bezeichnen wir mit einem griechischen Buchstaben. Wir vereinbaren folgende Schreibweise:[46]

$$\alpha = a_n a_{n+1} a_{n+2} ... a_{-1} a_0{,}a_1 a_2 a_3 ... (p) \quad \text{für } n \leq 0$$
$$\alpha = 0{,}00...0 a_n a_{n+1} a_{n+2} ... (p) \quad \text{für } n > 0$$

Beispiele.
$n = -2$: $a_{-2} = 1$, $a_{-1} = 2$, $a_0 = 3$, $a_1 = 4$, $a_2 = 5$, $a_3 = 6$, $a_4 = 7$, ..., $\alpha = 123{,}45678...(p)$;

$n = 0$: $a_0 = 1$, $a_1 = 2$, $a_2 = 3$, $a_3 = 4$, ..., $\beta = 1{,}2345678...(p)$;

$n = 5$: $a_5 = 1$, $a_6 = 2$, $a_7 = 3$, ..., $\gamma = 0{,}000012345678...(p)$.

[45] Dass diese Definition wirklich sinnvoll ist, wird sich erst noch zeigen. Die Bezeichnung "p-adische Zahl" ist bis jetzt nur eine abkürzende Bezeichnung für eine Folge der angegebenen Form. Eine solche Folge ist gegeben durch eine ganze Zahl n und durch eine Folge $a_n, a_{n+1}, a_{n+2}, ...$ (deren erster Index gerade die Zahl n ist) von für-p-ganzen Zahlen (wobei $a_n \neq 0$).

[46] Es wird vereinbart, zwischen a_0 und a_1 ein Komma zu schreiben. Ist $n > 0$, so gibt es kein a_0, und es wird vereinbart, $a_0 = 0$, $a_1 = 0$, ..., $a_{n-1} = 0$ zu setzen.

Die Folge $1, 2, 3, 4, 5, 6, 7, 8, ...$ ist in den drei Fällen die Folge aller natürlichen Zahlen, jedoch sind die p-adischen Zahlen offenbar nicht als gleich anzusehen (es treten verschiedene ganze Zahlen n auf).

Wann sind zwei p-adische Zahlen als gleich anzusehen? Dazu müssen wir bedenken, wie sich die Gleichheit der rationalen Zahlen in ihren p-adischen Entwicklungen ausdrückt. Wir dürfen uns schon eine Darstellung der Form

$$a_n p^n + a_{n+1} p^{n+1} + ... \tag{32}$$

für eine p-adische Zahl vorstellen. Jedoch nach der Definition A ist diese nicht gegeben.
Es ist nur eine Folge a_n, a_{n+1}, ... für-p-ganzer rationaler Zahlen mit der Bedingung gegeben, dass der Anfangsindex n eine beliebige ganze (also auch negative) Zahl sein kann (und $a_n \neq 0$).

Schon die folgende Definition der Gleichheit zweier p-adischer Zahlen deutet die Darstellung (32) an. Wir setzen

$$s_k(\alpha) = a_n p^n + ... + a_k p^k \qquad \text{für } k = n,n+1,...$$
$$s_k(\alpha) = 0 \qquad \text{für } k \leq n-1$$

Dann gilt offenbar

$$s_k(\alpha) \equiv s_{k-1}(\alpha)(p^k)$$

da $\frac{s_k(\alpha) - s_{k-1}(\alpha)}{p^k} = a_k$ für-p-ganz ist.

Definition B. Zwei p-adische Zahlen

$$\alpha = a_n a_{n+1} a_{n+2} ...(p) \qquad , \qquad \beta = b_m b_{m+1} b_{m+2} ...(p)$$

heißen gleich (Bezeichnung: $\alpha = \beta$), wenn

$$s_{k-1}(\alpha) \equiv s_{k-1}(\beta)(p^k)$$

für alle k ist. Diese Gleichheit genügt den folgenden Regeln:

$$\alpha = \alpha \tag{33}$$

$$\text{aus } \alpha = \beta \text{ folgt } \beta = \alpha \tag{34}$$

$$\text{aus } \alpha = \beta \text{ und } \beta = \gamma \text{ folgt } \alpha = \gamma \tag{35}$$

(Denn es ist: $s_{k-1}(\alpha) \equiv s_{k-1}(\alpha)(p^k)$.
Ferner: Aus $s_{k-1}(\alpha) \equiv s_{k-1}(\beta)(p^k)$ folgt $s_{k-1}(\beta) \equiv s_{k-1}(\alpha)(p^k)$.
Und: Aus $s_{k-1}(\alpha) \equiv s_{k-1}(\beta)(p^k)$ und $s_{k-1}(\beta) \equiv s_{k-1}(\gamma)(p^k)$ folgt $s_{k-1}(\alpha) \equiv s_{k-1}(\gamma)(p^k)$ (für alle k)).

Erst durch die Definitionen A und B zusammen sind die p-adischen Zahlen definiert (dass es wirklich Zahlen im üblichen Sinne sind, wird sich noch zeigen).
Diese Art, neue Objekte zu definieren, ist für die Mathematik typisch. Es soll hier noch etwas näher darauf eingegangen werden.

Verwendet man in Definition A für eine dort angegebene Folge das Wort "p-adische Folge" (irgendeine Folge der angegebenen Form heiße also p-adische Folge), so sind p-adische Folgen $\alpha = a_n a_{n+1}...$, $\beta = b_m b_{m+1}...$ natürlich dann und nur dann gleich (identisch), falls $n = m$

und $a_n = b_n$, $a_{n+1} = b_{n+1}$, ... ist.

Nennt man (wie in Definition B) zwei p-adische Folgen p-adisch gleich ($\alpha =_p \beta$), wenn $s_{k-1}(\alpha) = s_{k-1}(\beta)(p^k)$ für alle k ist, so hat diese p-adische Gleichheit die Eigenschaften (33), (34), (35). Diese Eigenschaften kennzeichnen die p-adische Gleichheit als eine sogenannte Äquivalenzrelation zwischen den p-adischen Folgen.

Gegeben sei eine p-adische Folge α. Dann kann man aus der Menge aller p-adischen Folgen diejenigen aussondern, die zu α äquivalent (also p-adisch gleich) sind. Diese Folgen bilden eine Teilmenge der Menge aller p-adischen Folgen. Diese Teilmenge bezeichnen wir mit F_α.
Die Elemente von F_α, sind also alle p-adischen Folgen, die p-adisch gleich mit α sind.

Ist β eine weitere p-adische Folge und gilt $\beta =_p \alpha$, so gehört β zu F_α. Sonst gehört β nicht zu F_α. Nun kann man F_β bilden. F_β besteht aus allen p-adischen Folgen, die p-adisch gleich mit β sind.

Die Mengen F_α und F_β sind elementfremd (falls $\beta \neq_p \alpha$), d.h., es gibt keine p-adische Folge γ, die in beiden Mengen enthalten ist. Gäbe es nämlich eine solche Folge γ, so wäre sowohl $\gamma =_p \alpha$ als auch $\gamma =_p \beta$, also nach (34) und (35) $\alpha =_p \beta$. Dann ist aber jede Folge ξ aus F_α wegen $\xi =_p \alpha$, also $\xi =_p \beta$, auch in F_β enthalten und umgekehrt jede Folge η aus F_β wegen $\eta =_p \beta$, also $\eta =_p \alpha$, auch in F_α enthalten, d.h. $F_\alpha = F_\beta$.

Die Mengen F_α und F_β sind also entweder gleich oder elementfremd. Die Mengen $F_\alpha, F_\beta, ...$ werden auch als Klassen, genauer Äquivalenzklassen (bezüglich der gegebenen Äquivalenzrelation) bezeichnet.
Die Menge aller p-adischen Folgen ist in lauter zueinander elementfremde Klassen eingeteilt. Es ist $F_\alpha = F\beta$ dann und nur dann, wenn $\alpha =_p \beta$ist. (Ist $\gamma \neq_p \alpha$, so haben F_α und F_β kein Element gemeinsam.)
Alle Elemente einer Klasse sind einander äquivalent, und alle einem Klassenelement äquivalenten Elemente liegen in derselben Klasse. Die Klasse ist mithin durch jedes ihrer Elemente gegeben. Irgendein Element der Klasse heißt Repräsentant der Klasse.

Die Äquivalenzklassen heißen dann p-adische Zahlen. Eine p-adische Zahl, d.h. eine Klasse F_α von p-adischen Folgen, ist durch jede in dieser Klasse liegende p-adische Folge α gegeben.
Man kann vereinbaren, für die p-adischen Zahlen F_α wieder den Buchstaben α zu verwenden (wobei α eigentlich nur einen Repräsentanten aus F_α bezeichnet). Man rechnet dann prinzipiell mit den Repräsentanten, muss sich jedoch darüber im klaren sein, dass die durchgeführte Rechnung gar nicht von der Wahl des Repräsentanten in der Klasse abhängt.

Nun gilt: Zwei p-adische Zahlen α, β sind dann und nur dann gleich, wenn $s_{k-1}(\alpha) \equiv s_{k-1}(\beta)(p^k)$ für alle k ist. (Denn $\alpha = \beta$ bedeutet $F_\alpha = F_\beta$, d.h. $\alpha =_p \beta$, d.h. $s_{k-1}(\alpha) = s_{k-1}(\beta)(p^k)$ nach Definition B).

Bei der Definition der Gleichheit konnten wir uns an den p-adischen Entwicklungen der rationalen Zahlen orientieren. Da die rationalen Zahlen unter den p-adischen Zahlen vorkommen sollen, muss für rationale Zahlen r, r' gelten:
Es ist $r = r'$ (im üblichen Sinne) dann und nur dann, wenn $r = r'$ (falls man r, r' mittels ihrer p-adischen Entwicklungen als p-adische Zahl auffasst). Rationale Zahlen sind ja dann und nur dann gleich, wenn ihre p-adischen Entwicklungen für jede (noch so hohe) p-Potenz kongruent sind. Ist

$$r = a_n a_{n+1} ... a_0{,}a_1 a_2 ... (p) \qquad , \qquad r' = b_m b_{m+1} ... b_0{,}b_1 b_2 ... (p)$$

so gilt $r = r'$ genau dann, wenn

$$a_n p^n + ...a_{k-1}p^{k-1} \equiv b_m p^m + ...b_{k-1}p^{k-1}(p^k)$$

für alle k ist. Somit ist die geforderte Bedingung erfüllt: Die Gleichheit p-adischer Zahlen umfasst die Gleichheit rationaler Zahlen.
Für rationale Zahlen als Teilmenge aller p-adischen Zahlen stimmt dieser Gleichheitsbegriff mit dem schon bekannten überein.

Unter allen p-adischen Zahlen, die einer gegebenen p-adischen Zahl gleich sind, gibt es stets eine und nur eine, etwa $a_n a_{n+1} a_{n+2}...$, für die $a_i \in \{0,1,..,p-1\}$ für alle i ist. $\alpha = a_n a_{n+1} a_{n+2}...$ heißt dann die reduzierte Form der p-adischen Zahl α.

Beispiel. $\alpha = 1{,}2345678...(5)$. Es ist $1{,}\overline{2340}(5)$ die reduzierte Form von α.

In der Auffassung der p-adischen Zahlen als Äquivalenzklassen von p-adischen Folgen kann man diesen Sachverhalt auch so formulieren:
In jeder Äquivalenzklasse gibt es genau einen Repräsentanten der Form $a_n a_{n+1} a_{n+2}...(p)$ mit $0 \leq a_i \leq p-1$ für alle i.

Ist $\alpha = a_n a_{n+1} a_{n+2}...a_{l-1} a'_l a'_{l+1}...(p)$ eine p-adische Zahl und ist hierin a'_l die erste Zahl, die nicht aus der Menge $\{0,1,..,p-1\}$ ist, so gilt $a'_l \equiv a_l(p)$ mit einer Zahl a_l, für die $0 \leq a_l \leq p-1$ ist, also $a'_l = a_l + b_{l+1}p$ (mit einer für-p-ganzen Zahl b_{l+1}).
Dann ist $\beta = a_n a_{n+1} a_{n+2}...a_{l-1} a_l (b_{l+1} + a'_{l+1}) a'_{l+2}...(p)$ gleich der p-adischen Zahl α. Um dies einzusehen, muss man die Definition der Gleichheit verwenden.

Es ist nämlich $s_k(\alpha) = s_k(\beta)$ für $k = n,n+1,n+2,...,l-1$, also erst recht $s_k(\alpha) = s_k(\beta)(p^{k+1})$. Ferner ist

$$s_l(\alpha) = a_n p^n + ... + a_{l-1}p^{l-1} + a_l p^l \qquad , \qquad s_l(\beta) = a_n p^n + ... + a_{l-1}p^{l-1} + a'_l p^l$$

Wegen $a'_l p^l = a_l p^l + b_{l+1}p^{l+1}$ gilt dann $s_l(\alpha) = s_l(\beta)(p^{l+1})$. Außerdem ist

$$\begin{aligned} s_{l+1}(\alpha) &= a_n p^n + ... + a_{l-1}p^{l-1} + a'_l p^l + a'_{l+1}p^{l+1} \\ s_{l+1}(\beta) &= a_n p^n + ... + a_{l-1}p^{l-1} + a_l p^l + (b_{l+1} + a'_{l+1})p^{l+1} \end{aligned}$$

wegen

$$a_l p^l + b_{l+1}p^{l+1} = a'_l p^l \qquad \text{ist} \qquad s_{l+1}(\alpha) = s_{l+1}(\beta)$$

und ebenso $s_k(\alpha) = s_k(\beta)$ für alle $k \geq l+1$, also erst recht $s_k(\alpha) = s_k(\beta)(p^{k+1})$. Somit gilt

$$s_k(\alpha) = s_k(\beta)(p^{k+1})$$

für alle k, d.h. $\alpha = \beta$.

So kann man nacheinander eine beliebige p-adische Zahl in eine ihr gleiche reduzierte p-adische Zahl verwandeln. Reduzierte p-adische Zahlen sind dann und nur dann gleich, wenn sie identisch sind, wenn also ihre entsprechenden Koeffizienten übereinstimmen.

In jeder Äquivalenzklasse von p-adischen Folgen gibt es einen und nur einen Repräsentanten der Form $a_n a_{n+1}...(p)$ mit $0 \leq a_i \leq p-1$ für alle i. Eine zu einer solchen p-adischen Folge p-adisch gleiche Folge $b_m b_{m+1} : ..(p)$ mit $0 \leq b_i \leq p-1$ ist mit dieser gleich (d.h. $m = n$ und $a_n = b_n$, $a_{n+1} = b_{n+1}$, ...)

Beispiele.
$1{,}234567891011121314...(5) = 1{,}\overline{2340}...(5)$;
$p^2, 2p^2 - 2p\ 3p^2 - 4p + 1\ 4p^2 - 6p + 2\ ... = 0(p)$

Sind nun die in den Definitionen A und B festgelegten und als p-adische Zahlen bezeichneten Folgen in demselben Sinne Zahlen, in dem es die rationalen Zahlen sind? Darf man mit ihnen nach genau denselben Regeln rechnen wie mit den rationalen Zahlen?
Wie kann man p-adische Zahlen addieren ? Auch hier können wir uns an der Addition der p-adischen Entwicklung rationaler Zahlen orientieren; wir werden zu folgender naheliegender Definition der Addition p-adischer Zahlen geführt.

Definition (Addition). Ist

$$\alpha = a_n a_{n+1} a_{n+2} ...(p) \qquad , \qquad \beta = b_m b_{m+1} b_{m+2} ...(p)$$

so heißt

$$\begin{aligned} &a_n + 0a_{n+1} + 0...a_m + b_m a_{m+1} + b_{m+1}...(p) \qquad \text{falls } n \leq m \quad \text{bzw.} \\ &0 + b_m 0 + b_{m+1}...a_n + b_n a_{n+1} + b_{n+1}...(p) \qquad \text{falls } m \leq n \end{aligned}$$

die Summe $\alpha + \beta$ der p-adischen Zahlen α und β.

Es ist noch zu zeigen, dass diese Definition wirklich sinnvoll ist. Könnten nicht verschiedene Darstellungen von α und β zu verschiedenen Summen führen ?
Dies ist nicht möglich, denn aus $\alpha = \alpha'$, $\beta = \beta'$ folgt $\alpha + \beta = \alpha' + \beta'$. Ferner gilt

$$s_k(\alpha + \beta) = s_k(\alpha) + s_k(\beta)$$

Beides lässt sich leicht überprüfen.

Die Addition der p-adischen Zahlen ist repräsentantenweise erklärt worden. Man nimmt einen Repräsentanten α aus der Äquivalenzklasse F_α, einen Repräsentanten β aus der Klasse F_β und addiert diese p-adischen Folgen $(\alpha + \beta)$, wie in der Definition angegeben.
Man erhält eine neue p-adische Folge $\alpha + \beta$. Diese bestimmt wieder eine Äquivalenzklasse $F_{\alpha * \beta}$. Diese Äquivalenzklasse ist eindeutig durch F_α und F_β bestimmt:
Hätte man andere Folgen α', β' aus F_α und F_β gewählt und diese addiert $(\alpha' + \beta')$, so erhielte man wieder eine p-adische Folge $\alpha' + \beta'$ und eine Äquivalenzklasse $F_{\alpha' + \beta'}$; jedoch gilt

$$F_{\alpha+\beta} = F_{\alpha'+\beta'}$$

Die Definition der Addition der Äquivalenzklassen (p-adischer Zahlen) vermittels

$$F\alpha + F_\beta = F_{\alpha+\beta}$$

ist also sinnvoll, da sie unabhängig von der Auswahl der Repräsentanten aus den Klassen ist (denn aus $\alpha =_p \alpha'$, $\beta =_p \beta'$ folgt $\alpha + \beta =_p \alpha' + \beta'$.

Wir können für die Addition das folgende Schema verwenden (hierin sei $n < m$):

	a_n	a_{n+1}	a_{n+2}	...	a_{m-1}	a_m	a_{m+1}	... (p)
+	0	0	0	...	0	b_m	b_{m+1}	... (p)
	a_n	a_{n+1}	a_{n+2}	...	a_{m-1}	$a_m + b_m$	$a_{m+1} + b_{m+1}$	... (p)

Beispiel. $p = 5$, $\alpha = 20{,}34(5)$, $\beta = 34{,}03(5)$.

$$\begin{array}{rl} 20{,}34 & (5) \\ +34{,}03 & (5) \\ \hline 54{,}37 & = 0{,}421\ (5) \end{array}$$

$\alpha = 203{,}4333...(5)$, $\beta = 3{,}41111...(5)$.

$$\begin{array}{rl} 203{,}4333... & (5) \\ +003{,}4111... & (5) \\ \hline 206{,}8444... & 0\ 201{,}4000...\ (5) \end{array}$$

Man addiert stets von links nach rechts und kann dabei das Resultat sofort auf die reduzierte Form bringen.

Beispiele.

$$\begin{array}{rl} 34{,}312040 & ...(5) \\ +\ 0{,}024321 & ...(5) \\ \quad 1\ \ 1 & \\ \hline 34{,}331412 & ...(5) \end{array} \qquad \begin{array}{rl} 444{,}321040 & ...(5) \\ +\ 44{,}432104 & ...(5) \\ \quad 1\ 111 & \\ \hline 434{,}314144 & ...(5) \end{array}$$

Da wir schon wissen, wie sich die Multiplikation rationaler Zahlen in ihren p-adischen Entwicklungen widerspiegelt, ist es nicht schwer, eine Multiplikation p-adischer Zahlen so zu erklären, dass diese für rationale Zahlen mit der schon bekannten übereinstimmt.
Auch die Multiplikation wird repräsentantenweise erklärt.

Definition (Multiplikation). Ist

$$\alpha = a_n a_{n+1} a_{n+2}...(p) \qquad , \qquad \beta = b_m b_{m+1} b_{m+2}...(p)$$

so heißt

$$\begin{array}{ll} a_n + 0a_{n+1} + 0...a_m + b_m a_{m+1} + b_{m+1}...(p) & \text{falls } n \leq m \quad \text{bzw.} \\ 0 + b_m 0 + b_{m+1}...a_n + b_n a_{n+1} + b_{n+1}...(p) & \text{falls } m \leq n \end{array}$$

so heißt

$$\gamma = c_{n+m} c_{n+m+1} c_{n+m+2}...(p)$$

mit

$$c_l = \sum_{i+j=l} a_i b_j \quad \left\{ \begin{array}{l} i = n, n+1, ...; j = m, m+1, ... \\ l = n+m, n+m+1, ... \end{array} \right\}$$

das Produkt $\alpha\beta$ der Zahlen α und β.

Das Zeichen[47] $\sum\limits_{i+j=l} a_i b_j$ bedeutet: Man bildet alle Produkte $a_i b_j$, für die die Summe der Indizes i,j gleich $i + j = l$ ist, und addiert diese Produkte.

Beispiel. $\alpha = a_{-2}a_{-1}a_0{,}a_1(p)$, $\beta = b_{-2}b_{-1}b_0{,}b_1b_2(p)$;

$$\begin{array}{rcl} c_{-4} = a_{-2}b_{-2} & , & c_{-3} = a_{-2}b_{-1} + a_{-1}b_{-2} \\ c_{-2} = a_{-2}b_0 + a_{-1}b_{-1} + a_0 b_{-2} & , & c_{-1} = a_{-2}b_1 + a_{-1}b_0 + a_0 b_{-1} + a_1 b{-}2 \\ c_0 = a_{-2}b_2 + a_{-1}b_1 + a_0 b_0 + a_1 b{-}1 & , & c_1 = a_{-1}b_2 + a_0 b_1 + a_1 b_0 \\ c_2 = a_0 b_2 + a_1 b_1 & , & c_3 = a_1 b_2, \qquad c_4 = 0 \end{array}$$

Zahlenbeispiel. $\alpha = 210{,}1(5)$, $\beta = 1{,}2(5)$

[47] Für Summen verwendet man gern das Summenzeichen $\sum$. Man setzt $a_1 + a_2 + a_3 + ... + a_n = \sum\limits_{i=1}^{n} a_i$. Es kommt dabei selbstverständlich nicht auf die Bezeichnung des Summationsbuchstabens i an; z. B. ist $\sum\limits_{i=1}^{n} a_i = \sum\limits_{k=0}^{n-1} a_{k+1}$

$$\begin{array}{l} 210{,}1 \cdot 1{,}2(5) \\ \hline 2101 \\ \quad 4202 \\ \hline 252{,}12(5) = 203{,}12(5) \end{array}$$

Probe: $\alpha = 5 + \frac{7}{25}$, $\beta = 11$,
$\alpha\beta = 58 + \frac{2}{25} = \frac{2}{25} + 3 + 5 + 2 \cdot 5^2$

Auch hier ist keineswegs unmittelbar klar, dass es zu gegebenen Zahlen α und β eine und nur eine Zahl γ gibt, für die $\alpha\beta = \gamma$ gilt (und die dann als das Produkt von α und β bezeichnet wird).

Man kann zwar stets zu gegebenen p-adischen Zahlen α und β eine derartige Zahl γ bestimmen, indem man $a_n a_{n+1}...(p)$, $b_m b_{m+1}...(p)$ in der angegebenen Weise multipliziert (also die p-adischen Folgen wie in der Definition angegeben multipliziert und dann zu den Äquivalenzklassen übergeht; jedoch wäre es denkbar, dass man von anderen Repräsentanten der Zahlen, d.h. von anderen p-adischen Folgen, zu einem anderen Resultat kommt).

Es wäre denkbar, dass zwar $\alpha' = \alpha$, $\beta' = \beta$ (im Sinne der Gleichheit p-adischer Zahlen), jedoch $\alpha'\beta' = \gamma' \neq \gamma = \alpha\beta$ ist. Dies kann aber nicht eintreten.
Das Produkt $\alpha\beta$ ist unabhängig von der speziellen Auswahl der Repräsentanten, d.h. von der Auswahl der p-adischen Folgen $a_n a_{n+1}...(p)$, $b_m b_{m+1}...(p)$, die die Zahlen α, β repräsentieren.

In der Tat überlegen wir uns, dass aus $\alpha = \alpha'$ und $\beta = \beta'$ stets $\alpha\beta = \alpha'\beta'$ folgt.
Die repräsentantenweise Definition der Multiplikation,

$$F_\alpha F_\beta = F_{\alpha\beta}$$

ist also unabhängig von der Auswahl der Repräsentanten aus den Äquivalenzklassen.

Es genügt zu zeigen, dass aus $\alpha = \alpha'$ die Beziehung $\alpha\beta = \alpha'\beta$ folgt (wenden wir dieses Resultat noch einmal an: aus $\beta = \beta'$ folgt $\alpha\beta = \alpha'\beta'$, so ergibt sich nämlich $\alpha\beta = \alpha'\beta = \alpha'\beta'$, d.h. die Behauptung).
Nach Definition ist[48]

$$s_{k-1}(\alpha\beta) = \sum_{l=n+m}^{k-1} \left(\sum_{\substack{i+j=l \\ i=n,n+1,... \\ j=m,m+1,...}} a_i b_j \right) p^l = \sum_{i+j=n+m}^{k-1} a_i b_j p^{i+j}$$

hieraus ergibt sich

$$s_{k-1}(\alpha\beta) = \sum_{i+j=n+m}^{k-1} a_i p^i b_j p^j = \sum_{j=m}^{k-1} \sum_{i=n}^{k-1-j} a_i p^i b_j p^j = \sum_{j=m}^{k-1} s_{k-1-j}(\alpha) b_j p^j$$

[48] Wir verwenden auch hier das Summenzeichen $\sum$. Mit Hilfe dieses Zeichens lässt sich die Regel, wie man Summen multipliziert, folgendermaßen schreiben:

$$\left(\sum_{i=1}^{n} a_i \right) \left(\sum_{k=1}^{m} b_k \right) = \sum_{i=1}^{n} \sum_{k=1}^{m} a_i b_k = \sum_i \sum_k a_i b_k = \sum_{i,k} a_i b_k$$

Man kann die Reihenfolge der Summation über i und k vertauschen oder die Summe zu einer einzigen Doppelsumme zusammenfassen, da es auf die Reihenfolge der Summanden nicht ankommt.

Es folgt

$$\frac{s_{k-1}(\alpha\beta) - s_{k-1}(\alpha'\beta)}{p^k} = \sum_{j<k} \frac{s_{k-1-k}(\alpha) - s_{k-1-j}(\alpha')}{p^{k-j}} b_j$$

Aus $\alpha = \alpha'$ folgt aber

$$s_{k-1-j}(\alpha) - s_{k-1-j}(\alpha') \equiv 0(p^{k-j})$$

d.h. $\frac{s_{k-1}(\alpha\beta)-s_{k-1}(\alpha'\beta)}{p^k}$, ist für-$p$-ganz; es ist also

$$s_{k-1}(\alpha\beta) \equiv s_{k-1}(\alpha'\beta)(p^k) \quad \text{(für alle } k\text{), d.h. } \alpha\beta = \alpha'\beta$$

Über die Beziehung zwischen $s_k(\alpha\beta)$ und $s_k(\alpha)$, $s_k(\beta)$ lässt sich folgendes aussagen. Ist

$$\alpha = a_0,a_1a_2a_3...(p) \qquad , \qquad \beta = b_0,b_1b_2b_3...(p)$$

so ist

$$\alpha\beta = (a_0b_0), (a_0b_1 + a_1b_0)(a_0b_2 + a_1b_1 + a_2b_0)...(p)$$

also

$$\begin{aligned} s_k(\alpha\beta) &\equiv a_0b_0 + (a_0b_1 + a_1b_0)p + ... + (a_0b_k + a_1b_{k-1} + ... + a_kb_0)p^k \\ &\equiv (a_0 + a_1p + a_2p^2 + ... + a_kp^k)(b_0 + b_1p + b_2p^2 + ... + b_kp^k)(p^{k+1}) \\ s_k(\alpha\beta) &\equiv s_k(\alpha)s_k(\beta)(p^{k+1}) \end{aligned}$$

Treten auch negative Indizes auf, so sei z. B.

$$\alpha = a_{-2}a_{-1}a_0,a_1a_2...(p) \qquad , \qquad \beta = b_{-2}b_{-1}b_0,b_1b_2...(p)$$

und es ist

$$\begin{aligned} s_k(\alpha\beta) = &(a_{-2}b_{-2})p^{-4} + (a_{-2}b_{-1} + a_{-1}b_{-2})p^{-3} + ... + (a_{-2}b_k + a_{-1}b_{k-1} + ... + a_kb_{-2})p^{k-2} \\ &+ (a_{-2}b_{k+1} + a_{-1}b_k + ... + a_{k+1}b_{-2})p^{k-1} \\ &+ (a_{-2}b_{k+2} + a_{-1}b_{k+1} + a_0b_k + ... + a_{k+2}b_{-2})p^k \end{aligned}$$

also

$$s_k(\alpha\beta) \equiv (a_{-2}p^{-2} + ... + a_kp^k)(b_{-2}p^{-2} + ... + b_kp^k)(p^{k-1})$$

d.h.

$$s_k(\alpha\beta) \equiv s_k(\alpha)s_k(\beta)(p^{k-1})$$

(analog für andere negative Indizes).
Hier werden die Größen modulo p^{k-1} betrachtet. In dem Produkt $s_k(\alpha)s_k(\beta)$ gibt es ja a_{k+1}, a_{k+2}, b_{k+1}, b_{k+2} nicht, und diejenigen Glieder, die mit Potenzen $1, p, p^2, ..., p^{k-2}$ multipliziert sind, sind auf beiden Seiten gleich, während die höheren Potenzen von p modulo p^{k-1} fortgelassen werden können.

Wir können für die Multiplikation das folgende Schema verwenden

	a_n	a_{n+1}	a_{n+2}	a_{n+3}	... $(p) \cdot b_mb_{m+1}b_{m+2}...(p)$
1	a_nb_m	$a_{n+1}b_m$	$a_{n+2}b_m$	$a_{n+3}b_m$	...
2	$\downarrow$	a_nb_{m+1}	$a_{n+1}b_{m+1}$	$a_{n+2}b_{m+1}$	...
3		$\downarrow$	a_nb_{m+2}	$a_{n+1}b_{m+2}$	...
4			$\downarrow$	a_nb_{m+3}	...
				$\downarrow$	...
	c_{n+m}	c_{n+m+1}	c_{n+m+2}	c_{n+m+3}	... (p)

Man multipliziert zuerst b_m mit allen Zahlen $a_n, a_{n+1}, ...$ und schreibt die Produkte nacheinander von links nach rechts in die Zelle 1. Dann multipliziert man b_{m+1} mit allen Zahlen $a_n, a_{n+1}, ...$ und schreibt die Produkte von links nach rechts um eine Spalte verschoben in die Zeile 2 usw. Das Resultat erhält man durch Addition in den Spalten.
Die richtige Kommastelle lässt sich stets leicht bestimmen (weil das Produkt mit dem Index $n + m$ beginnt).

Beispiele.

1,	3	4	0	5	...	(5)				· 2,441... (5)		
2	6	8	0	10	...							
	4	12	16	0	20	...						
		4	12	16	0	20	...					
			1	3	4	0	5	...				
		2	5	6	7							
2,	0	1	4	0	...	(5)						

1	2	3,	4	5	6	7	8	...	(3)	· 123,45678... (3)		
1	2	3	4	5	6	7	8	...				
	2	4	6	8	10	12	14	...				
		3	6	9	12	15	18	...				
			4	8	12	16	20	...				
				5	10	15	20	...				
					6	12	18	...				
						7	14	...				
							8	...				
								...				
		1	3	7	14	23	35	51				
1	1	2	2,	0	1	2	2	...	(3)			

Jetzt können wir addieren und multiplizieren.
Zu vorgegebenen Zahlen α, β gibt es stets auch genau eine p-adische Zahl γ mit $\alpha + \gamma = \beta$. Die Zahl $\gamma = \alpha - \beta$ heißt die Differenz von α und β.

Zunächst überlegen wir uns, dass es zu jeder p-adischen Zahl α eine und nur eine p-adische Zahl γ gibt, für die $\alpha + \gamma = 0$ ist. Die Existenz ist unmittelbar klar.
Ist $\alpha = a_n a_{n+1} a_{n+2} ...(p)$, so leistet $\gamma = (-a_n)(-a_{n+1})(-a_{n+2})...(p)$ das Verlangte. Die Eindeutigkeit ergibt sich so:

Sind γ_1, γ_2 zwei p-adische Zahlen, für die $\alpha + \gamma_1 = 0$, $\alpha + \gamma_2 = 0$ gilt, so ist

$$\gamma_1 = 0 + \gamma_1 = (\alpha + \gamma_2) + \gamma_1 = \gamma_2 + (\alpha + \gamma_1) = \gamma_2 + 0 = \gamma_2$$

also $\gamma_1 = \gamma_2$.
Diese eindeutig bestimmte Zahl γ, für die $\alpha + \gamma = 0$ ist, heißt die zu α entgegengesetzte Zahl (Bezeichnung: $-\alpha$).
Nun folgt sofort, dass es zu p-adischen Zahlen α, β genau eine Zahl γ mit $\alpha + \gamma = \beta$ gibt.
In der Tat, es ist

$$\alpha + (\beta + (-\alpha)) = (a + (-\alpha)) + \beta = 0 + \beta = \beta$$

Die Zahl $\beta + (-\alpha)$ ist auch die einzige Zahl, für die dieses gilt. Aus $\alpha + \gamma_1 = \beta$ und $\alpha + \gamma_2 = \beta$ folgt $\alpha + \gamma_1 = \alpha + \gamma_2$, also

$$\gamma_1 = 0 + \gamma_1 = ((-\alpha) + \alpha) + \gamma_1 = (-\alpha) + (\alpha + \gamma_1) = (-\alpha) + +(\alpha + \gamma_2) = 0 + \gamma_2 = \gamma_2$$

Die üblichen Rechenregeln für die Addition und Subtraktion sind sämtlich erfüllt (wie man sich überlegen kann).
Wir können für die Subtraktion das folgende Schema verwenden:[49]

$$\begin{array}{lcccc} \alpha & a_n & a_{n+1} & a_{n+2} & ...\ (p) \\ \beta & b_n & b_{n+1} & b_{n+2} & ...\ (p) \\ \hline \alpha-\beta & a_n-b_n & a_{n+1}-b_{n+1} & a_{n+2}-b_{n+2} & ...\ (p) \end{array}$$

Die Subtraktion ist von links nach rechts auszuführen. Die Hinzufügung einer nichtreduzierten Darstellung der Null, z. B. $0{,}000...0p\ p-1\ p-1...(p)$ zum Minuenden α ist oft nützlich.

Die Differenz erscheint im allgemeinen in nichtreduzierter Form und ist dann erst in die reduzierte Form überzuführen.

Beispiele.

6,3452... (7)		0,05444...	
- 5,2140... (7)		3,41112...	(5)
1,1312... (7)		- 0,04404...	(5)
		3,42152...	
		= 3,42103...	(5)

Genauso, wie die ganzen Zahlen unter den rationalen Zahlen für die Arithmetik von besonderer Bedeutung sind, spielen die ganzen p-adischen Zahlen unter allen p-adischen Zahlen eine wichtige Rolle (vgl. auch: für-p-ganze und für-p-gebrochene rationale Zahlen). Sie werden durch die folgende Definition festgelegt.

Definition. Eine reduzierte p-adische Zahl der Form

$$\alpha = a_0{,}a_1a_2a_3...(p)$$

heißt ganze p-adische Zahl. Eine beliebige p-adische Zahl heißt ganz, wenn die ihr gleiche reduzierte ganz ist.

Die Menge aller ganzen p-adischen Zahlen werden mit Z_p bezeichnet. Ganze p-adische Zahlen, die rational sind, sind für-p-ganze rationale Zahlen.
Ganze p-adische Zahlen kann man addieren, subtrahieren und multiplizieren, und man erhält wieder ganze p-adische Zahlen. Die üblichen Rechenregeln sind erfüllt.

Sind α und β ganze p-adische Zahlen und gibt es eine ganze p-adische Zahl γ, für die $\alpha = \beta\gamma$ gilt, so heißt β ein Teiler von α.
Die Teiler der Zahl 1 heißen p-adische Einheiten. ε ist also eine p-adische Einheit, falls es ein ε' gibt, so dass $\varepsilon\varepsilon' = 1$ gilt.[50]

Satz 16. Eine ganze p-adische Zahl $\alpha = a_0{,}a_1a_2a_3...(p)$ ist eine p-adische Einheit genau dann, wenn $a_0 \neq 0(p)$ ist.

In der Tat, ist α eine p-adische Einheit, so existiert eine ganze p-adische Zahl $\beta = b_0{,}b_1b_2...(p)$, so dass $\alpha\beta = 1$ ist. Dann ist $s_0(\alpha\beta) = a_0b_0 \equiv 1(p)$ und folglich $a_0 \neq 0(p)$.

[49] Es bedeutet keine Einschränkung anzunehmen, dass n = m ist. Ist das nicht der Fall, so kann man einfach einige Nullen hinzufügen.

[50] Und dann gibt es nur ein solches ε'. Wäre auch $\varepsilon\varepsilon'' = 1$, so folgte durch Multiplikation mit ε'

$$(\varepsilon\varepsilon')\varepsilon'' = 1 \cdot \varepsilon'' = \varepsilon' \qquad \text{d.h.} \quad \varepsilon' = \varepsilon''$$

Umgekehrt sind ganze p-adische Zahlen[51] $\alpha = a_0{,}a_1a_2...(p)$ mit $a_0 \not\equiv 0(p)$ p-adische Einheiten. Tatsächlich gibt es ein $\xi = x_0{,}x_1x_2...(p)$ mit $\alpha\xi = 1$, d.h.

$$a_0x_0, (a_1x_0 + a_0x_1)(a_2x_0 + a_1x_1 + a_0x_2)...(p) = 1{,}000...(p)$$

Die Gleichung $\alpha\xi = 1$ wird nämlich sicher erfüllt, wenn $x_0{,}x_1x_2{,}...$ so gewählt werden, dass sie den Gleichungen

$$\begin{aligned} a_0x_0 &= 1 \\ a_1x_0 + a_0x_1 &= 0 \\ a_2x_0 + a_1x_1 + a_0x_2 &= 0 \qquad ... \end{aligned}$$

genügen. Hieraus kann man aber nacheinander diese Zahlen $x_0, x_1, x_2, ...$ bestimmen:

$$x_0 = \frac{1}{a_0}, \quad x_1 = -\frac{a_1}{a_0^2}, \quad x_2 = \frac{a_1^2 - a_0a_2}{a_0^3}, \quad ...$$

Alle Zahlen $x_0, x_1, x_2, ...$ sind für-p-ganz (da $p \nmid a_0$), so dass $x_0{,}x_1x_2x_3...(p)$ eine ganze p-adische Zahl ist.
Die eindeutig bestimmte Zahl ξ werde mit α^{-1} oder $\frac{1}{\alpha}$ bezeichnet und heiße die zu α reziproke Zahl.

Die Division durch eine Einheit ist stets, und zwar eindeutig innerhalb der Menge Z_p ausführbar. Ist ε eine Einheit und β eine beliebige ganze p-adische Zahl, so gibt es eine und nur eine ganze p-adische Zahl η, so dass $\varepsilon\eta = \beta$ ist. Diese eindeutig bestimmte Zahl η heißt Quotient von β und ε (Bezeichnung: $\frac{\beta}{\varepsilon}$):
Die Zahl $\eta = \beta\varepsilon' = \beta\varepsilon^{-1} = \beta \cdot \frac{1}{\varepsilon}$ leistet das Verlangte.

Ist speziell β eine Einheit, so ist auch $\frac{\beta}{\varepsilon}$ eine Einheit, so dass also der Quotient von Einheiten wieder eine Einheit ist.

Die Division einer p-adischen Einheit $\alpha = a_0{,}a_1a_2...$ durch eine andere $beta = b_0{,}b_1b_2...$ wird praktisch genauso ausgeführt wie die eines Dezimalbruches durch einen anderen.
Die Operation muss bei den Gliedern a_0 und b_0 begonnen und dann nacheinander von links nach rechts fortgeführt werden. Man dividiert also zuerst a_0 durch b_0, d.h. bestimmt (und das gelingt am leichtesten durch Probieren) die Zahl t_0 $(0 \leq t_0 < p)$, für die $b_0t_0 \equiv= a_0(p)$ ist. Dann bildet man die Differenz $\alpha - \beta t_0$, also

$$\begin{array}{rrrrl} a_0, & a_1 & a_2 & a_3 & ...\ (p) \\ -b_0t_0, & b_1t_0 & b_2t_0 & b_3t_0 & ...\ (p) \\ \hline 0, & a_1' & a_2' & a_3' & ...\ (p) \end{array}$$

(es ist $a_0 - b_0t_0 \equiv 0(p)$, so dass $a_0' = 0$ ist). Die Differenz behandelt man in derselben Art weiter. Wir können also das folgende Schema verwenden:

$$\begin{array}{rrrrll} a_0, & a_1 & a_2 & a_3 & ... & : b_0{,}b_1b_2... = t_0{,}t_1t_2... \\ -b_0t_0 & b_1t_0 & b_2t_0 & b_3t_0 & ... & \\ \hline 0 & a_1' & a_2' & a_3' & ... & \\ & -b_0t_1 & b_1t_1 & b_2t_1 & ... & \\ & \hline & 0 & a_1'' & a_2'' & ... \\ & & & -b_0t_2 & b_1t_2 & ... \\ & & & \hline & 0 & a_1''' & ... \\ & & & & -b_0t_3 & ... \\ & & & & \hline & & 0 & ... \end{array}$$

[51] Wir denken uns im folgenden ganze p-adische Zahlen stets in reduzierter Darstellung gegeben.

Beispiel

$$
\begin{array}{rll}
 & 0{,}0544\ldots & \\
 & 4{,}32 & : 2{,}34 = 2{,}\ 10211\ldots\ (5) \\
4{,}68 = & 4{,}141 & \\
\hline
 & 233444\ldots & \\
 & 234 & \\
\hline
 & 043444\ldots & \\
 & 0000 & \\
\hline
 & 434444\ldots & \\
 & 4141 & \\
\hline
 & 203444\ldots & \\
 & 234 & \\
\hline
 & 233444\ldots & \text{usw.}
\end{array}
$$

Um auch die Division beliebiger p-adischer Zahlen ($\neq 0$) durchführen zu können, zeigen wir zunächst, dass sich jede p-adische Zahl $\neq 0$ als Produkt einer geeigneten Potenz p^m von p mit einer gewissen Einheit ε schreiben lässt.
Ist dann $\alpha_1 p^{m_1}\varepsilon_1$, $\alpha_2 p^{m_2}\varepsilon_2$, so gilt

$$\frac{\alpha_1}{\alpha_2} = p^{m_1-m_2}\frac{\varepsilon_1}{\varepsilon_2}$$

es sind also in Wirklichkeit nur noch die Einheiten $\varepsilon_1, \varepsilon_2$ zu dividieren, was wir oben durchgeführt haben.

Satz 17. Jede p-adische Zahl α, außer Null, lässt sich eindeutig in der Form

$$\alpha = p^n\varepsilon$$

darstellen, wobei ε eine p-adische Einheit und n eine ganze Zahl ist.

Beweis. Ist $\alpha = a_0{,}a_1a_2\ldots(p)$ und $a_n \equiv 0(p)$, so kann man α so schreiben, dass $a_n = 0$ ist. Ist $\alpha \neq 0$, so kann man daher $a_n \not\equiv 0(p)$ annehmen. Dann ist $\alpha = \xi\varepsilon$ mit der p-adischen Zahl

$$\xi = c_nc_{n+1}c_{n+2}\ldots(p) \qquad \text{mit} \qquad c_n = 1, c_i = 0 \quad (i \neq n)$$

und

$$\varepsilon = b_0{,}b_1b_2\ldots(p) \qquad \text{mit} \qquad b_0 = a_n, b_1 = a_{n+1}, \ldots$$

Es ist $s_k(\xi) = p^n$ für alle $k \geq n$, $s_k(\xi) = 0$ für alle $k < n$. Die p-adische Zahl ξ ist gleich der rationalen Zahl p^n; also $\alpha = p^n\varepsilon$. Die Eindeutigkeit ist klar.

Zu jeder p-adischen Zahl $\alpha \neq 0$ gibt es stets (wie jetzt leicht zu sehen ist) genau eine p-adische Zahl δ, für die $\alpha\delta = 1$ ist. Die Eindeutigkeit (dass es also höchstens eine solche Zahl gibt) ist klar: Aus $\alpha\delta_1 = 1$, $\alpha\delta_2 = 1$ folgt

$$\delta_1 = 1 \cdot \delta_1 = (\alpha\delta_2)\delta_1 = \delta_2(\alpha\delta_1) = \delta_2 \cdot 1 = \delta_2$$

also $\delta_1 = \delta_2$.
Die Existenz ergibt sich so: Ist $\alpha = p^n\varepsilon$, so gilt für $\delta = p^{-n}\varepsilon^{-1}$ die Beziehung $\alpha\delta = 1$. Diese eindeutig bestimmte Zahl werde mit $\delta^{-1} = \frac{1}{\delta}$ bezeichnet.

Zu vorgegebenen p-adischen Zahlen $\alpha \neq 0$ und β gibt es stets eine und nur eine p-adische Zahl δ, für die $\alpha\delta = \beta$ gilt. Die Zahl $\delta = \beta\alpha^{-1}$ leistet das Verlangte und ist die einzige Zahl mit dieser Eigenschaft; δ heißt Quotient von β und α.

Die Division beliebiger p-adischer Zahlen läuft also auf die oben beschriebene und praktisch durchgeführte Division p-adischer Einheiten hinaus. Ist nämlich $\beta = p^n\varepsilon'$ und $\alpha = p^m\varepsilon$, so ist $\beta\alpha^{-1} = p^{n-m}\frac{\varepsilon'}{\varepsilon}$. Es muss also lediglich $\frac{\varepsilon'}{\varepsilon}$ werden.

Jetzt können wir p-adische Zahlen addieren und multiplizieren, subtrahieren und dividieren, wir können mit ihnen nach genau denselben Regeln rechnen wie mit den rationalen Zahlen.
Für die rationalen Zahlen sind aber neben den Grundgesetzen der Addition, der Subtraktion, der Multiplikation und der Division noch Grundgesetze der Anordnung und das Archimedische Grundgesetz gültig.
Die rationalen Zahlen bilden eine geordnete Menge, d.h., zwischen je zweien von ihnen, etwa r, s, besteht stets eine und nur eine der drei Beziehungen

$$r < s, \quad r = s, \quad r > s$$

Sind r und s positive Zahlen, so ist stets

$$r + r + ... + r > s$$

wenn die linke Summe eine geeignete Zahl von Summanden enthält. Hier bedeutet $<$ das gewöhnliche Kleinersein.

Schon für die rationalen Zahlen lernten wir aber den Begriff "p-kleiner" kennen. Durch $< (p)$ werden die rationalen Zahlen nichtarchimedisch geordnet. Dieser Begriff "p-kleiner" wird jetzt auf p-adische Zahlen verallgemeinert.

Nach Satz 17 lässt sich jede p-adische Zahl α, außer 0, eindeutig in der Form $\alpha = p^n\varepsilon$ darstellen, wobei ε eine p-adische Einheit und n eine ganze Zahl ist.
Die durch $\alpha \neq 0$ eindeutig bestimmte Zahl $n = e_p(\alpha)$ heißt p-Exponent von α. Wieder können wir zweckmäßig $e_p(0) = \infty$ setzen. Der p-Exponent hat folgende wichtige Eigenschaften (die man leicht nachrechnen kann):

$$e_p(\alpha\beta) = e_p(\alpha) + e_p(\beta)$$
$$e_p\left(\frac{\alpha}{\beta}\right) = e_p(\alpha) - e_p(\beta)$$
$$e_p(\alpha + \beta) \leq \min(e_p(\alpha), e_p(\beta))$$

Offenbar ist α eine ganze p-adische Zahl genau dann, wenn $e_p(\alpha) = 0$ ist. Für p-adische Einheiten ε ist $e_p(\varepsilon) = 0$. Für ganze p-adische Zahlen gilt $\beta \mid \alpha$ dann und nur dann, wenn $e_p(\beta) \leq e_p(\alpha)$ ist.
Gilt für ganze p-adische Zahlen α, β, γ

$$\gamma \mid \alpha - \beta$$

so heißen α und β kongruent für γ (auch: kongruent modulo γ), symbolisch $\alpha \equiv \beta(\gamma)$.
Ist $\gamma = p^m\varepsilon$, so ist $\alpha \equiv \beta(\gamma)$ gleichwertig mit $\alpha \equiv \beta(p^m)$.
Ist $\alpha = a_0{,}a_1a_2...(p)$ eine beliebige ganze p-adische Zahl, so ist $s_{m-1}(\alpha)$ eine ganze Zahl mit der p-adischen Entwicklung

$$a_0 + a_1p + a_2p^2 + ... + a_{m-1}p^{m-1}$$

also

$$s_{m-1}(\alpha) = a_0{,}a_1a_2a_3...a_{m-1}00...(p)$$

Daher ist

$$\alpha - s_{m-1}(\alpha) = 0{,}00...0a_m a_{m+1}...(p)$$

also

$$e_p(\alpha - s_{m-1}(\alpha)) \geq m = e_p(p^m)$$

d.h. $p^m \mid \alpha - s_{m-1}(\alpha)$, also

$$\alpha \equiv s_{m-1}(\alpha)(p^m) \qquad (\text{für } m \geq 1) \tag{36}$$

Jede ganze p-adische Zahl ist somit modulo p^m $(m \geq 1)$ einer ganzen rationalen Zahl kongruent.
Der p-Exponent bestimmt (wie bei den rationalen Zahlen) einen p-Betrag für p-adische Zahlen, definiert durch

$$|\alpha|_p = \left(\frac{1}{p}\right)^{e_p(\alpha)} \qquad \text{für } \alpha \neq 0$$

und $|0|_p = 0$.
Für Einheiten ε ist $|\varepsilon|_p = 1$.

Es gelten die Rechenregeln (22), (23) und (24). Es ist offenbar $|\alpha|_p < |\beta|_p$ genau dann, wenn $e_p(\alpha) > e_p(\beta)$ ist.
Die p-adische Zahl α heiße p-kleiner als die p-adische Zahl β (symbolisch: $\alpha < \beta(p)$), falls $|\alpha|_p < |\beta|_p$ ist. Die p-adischen Zahlen werden hierdurch nichtarchimedisch geordnet.

Charakterisiert sind p-kleine p-adische Zahlen durch große Werte ihrer p-Exponenten. So ist die Differenz $\alpha - \beta$ zweier p-adischer Zahlen hinreichend p-klein, wenn der Wert $e_p(\alpha - \beta)$ genügend groß ist.
Der p-Betrag gestattet die Definition eines Abstandes $|\beta - \alpha|$, zwischen p-adischen Zahlen α und β.

Eine p-adische Zahl α heißt p-Grenzwert einer Folge $\alpha_1, \alpha_2, \alpha_3, ...$ (symbolisch $p\text{-}\lim\limits_{n\to\infty} \alpha_n = \alpha$, falls $|\alpha - \alpha_n|_p$ eine Nullfolge ist.

Beispiele. 1. Ist $\alpha = a0{,}a_1a_2...(p)$ eine ganze p-adische Zahl und $s_{m-1}(\alpha) = \sum\limits_{i=0}^{m-1} a_i p^i$, so gilt

$$p - \lim_{m\to\infty} s_{m-1}(\alpha) = \alpha$$

In der Tat, wegen (36) ist $e_p(\alpha - s_{m-1}(\alpha)) \geq m$, also

$$\lim_{m\to\infty} |\alpha - s_{m-1}(\alpha)|_p = 0$$

2. Jede p-adische Zahl ist Grenzwert einer Folge rationaler Zahlen. Jede p-adische Zahl lässt sich in der Form $\frac{\alpha}{p^n}$ darstellen, wobei α eine ganze p-adische Zahl und $n \geq 0$ ist.
Ist $\beta = \frac{\alpha}{p^n}$ eine beliebige p-adische Zahl, so gilt

$$p - \lim_{m\to\infty} \frac{s_{m-1}(\alpha)}{p^n} = \beta$$

Dies folgt aus Beispiel 1 und

$$e_p\left(\frac{s_{m-1}(\alpha)}{p^n} - \beta\right) = e_p\left(\frac{s_{m-1}(\alpha) - \alpha}{p^n}\right) = e_p = (s_{m-1}(\alpha) - \alpha) - n \to \infty$$

für $m \to \infty$.
Die Tatsache, dass die Folge

$$\begin{aligned} s_0(\alpha) &= a_0 \\ s_1(\alpha) &= a_0 + a_1 p \\ s_2(\alpha) &= a_0 + a_1 p + a_2 p^2 \\ s_3(\alpha) &= a_0 + a_1 p + a_2 p^2 + a_3 p^3 \qquad ... \end{aligned}$$

die p-adische Zahl α als Grenzwert besitzt, wird auch durch die unendliche Reihe

$$\alpha = a_0 + a_1 p + a_2 p^2 + a_3 p^3 + ... = \sum_{i=0}^{\infty} a_i p^i \tag{37}$$

ausgedrückt.[52]
Als Zusammenfassung unserer bisherigen Ergebnisse schreiben wir den folgenden Satz auf:

Satz 18. Jede p-adische Zahl α, außer Null, lässt sich eindeutig in der Form

$$\alpha = p^n(a_0 + a_1 p + a_2 p^2 + ... + a_h p^h + ...) \tag{38}$$

darstellen, wobei $n = e_p(\alpha)$, $1 \leq a_0 < p$ und $0 \leq a_i < p$ ($i = 1,2,3,...$) ist. Eine p-adische Zahl ist rational genau dann, wenn die Ziffernfolge $\{a_i\}$ periodisch ist (Vorperiode ist zugelassen; vgl. Kap. II).

Die ganzen p-adischen Zahlen sind durch $n \geq 0$ gekennzeichnet. Für p-adische Einheiten gilt $n = 0$. Eine ganze p-adische Zahl

$$\alpha = p^n(a_0 + a_1 p + a_2 p^2 + ...)$$

ist durch eine andere ganze p-adische Zahl

$$\beta = p^m(b_0 + b_1 p + b_2 p^2 + ...)$$

teilbar, falls $m \leq n$ ist. β heißt assoziiert zu α, falls $\alpha = \beta\varepsilon$ mit einer Einheit ε ist. (β ist also Teiler von α mit der zusätzlichen Eigenschaft, dass $\frac{\alpha}{\beta}$ nicht nur eine ganze p-adische Zahl, sondern sogar eine Einheit ist).
β heißt echter Teiler von α, wenn β Teiler von α, aber nicht zu α assoziiert ist. Jede Einheit teilt die Zahl α. Für eine ganze p-adische Zahl α heißen die Einheiten und die zu α Assoziierten die trivialen Teiler von α.

Eine p-adische Zahl π heißt Primelement, wenn π eine ganze p-adische Zahl, von 0 und Einheiten verschieden ist und außer den trivialen Teilern keine Teiler hat.

Primelemente sind alle Elemente π mit $e_p(\pi) = 1$. In der Tat:
π ist ganz, d.h. $e_p(\pi) \geq 0$; ferner $\pi \neq 0$, d.h. $e_p(\pi) \neq \infty$; π ist keine Einheit, d.h. $e_p(\pi) \neq 0$; da π außer den trivialen Teilern keine Teiler hat, gibt es kein β mit $0 < e_p(\beta) < e_p(\pi)$. Daher muss $e_p(\pi) = 1$ sein. (Wäre $e_p(\pi) \geq 2$, so würde ein β mit $e_p(\beta) = 1$ echter Teiler von π

[52] Diese unendliche Reihe ist tatsächlich nichts weiter als eine symbolische Schreibweise für den Sachverhalt, dass

$$\alpha = p - \lim_{k \to \infty} (a_0 + a_1 p + a_2 p^2 + ... + a_k p^k)$$

ist.

sein.)

Die Zahl p ist wegen $e_p(p) = 1$ Primelement. Alle Primelemente sind assoziiert zu p. Die Darstellung

$$\alpha = p^n \varepsilon \qquad \text{(mit einer Einheit } \varepsilon \text{ und } n \geq 0) \tag{39}$$

ist die eindeutige Primelementzerlegung der Zahl. Die sämtlichen nichttrivialen Teiler der in der Form (39) angegebenen ganzen p-adischen Zahl α sind:

$$p, p^2, p^3, p, ^4, ..., p^{n-1}$$

(und die zu diesen assoziierten Zahlen).
Gilt $\gamma\alpha$ und $\gamma \mid \beta$, so heißt γ gemeinsamer Teiler von α und β.
Unter allen gemeinsamen Teilern von α, β gibt es wenigstens einen mit größtem p-Exponenten. Dieser ist bis auf Assoziierte eindeutig bestimmt und heißt größter gemeinsamer Teiler (g. g. T.) von α und β (Bezeichnung: (α, β)).
Ist $\alpha = p^n\varepsilon$, $\beta = p^m\varepsilon'$ und ist z.B. $n \geq m$, so gilt bereits $\beta \mid \alpha$, d.h., β ist gemeinsamer Teiler von β und α. Der Teiler β ist der g.g.T. von α und β. Es ist

$$(\alpha, \beta) = \begin{cases} \beta & \text{falls } m \leq n \\ \alpha & \text{falls } m \geq n \end{cases}$$

Der Begriff "g.g.T." ist also für ganze p-adische Zahlen bedeutungslos.

Die grundlegenden zahlentheoretischen Begriffe "Teiler", "größter gemeinsamer Teiler", "Primelement", "Primzerlegung" sind damit auch für ganze p-adische Zahlen bekannt.
Überhaupt werden wir jetzt anerkennen, dass die p-adischen Zahlen wirklich in demselben Sinne Zahlen sind, in dem es die rationalen Zahlen sind, und die ganzen p-adischen Zahlen in dem Sinne, wie es die für-p-ganzen rationalen Zahlen sind.
Die p-adischen Zahlen mit periodischer Ziffernfolge und nur sie sind rational.

Eine nichtrationale p-adische Zahl kann man ziffernmäßig überhaupt nicht vollständig angeben. Die eingangs untersuchte Folge 3,1,2,6,... für-7-ganzer Zahlen definiert eine 7-adische Zahl σ mit $\sigma^2 = 2$:

$$\sigma = 3{,}126a_4a_5...$$

Bereits die nächsten Glieder $a_4, a_5, ...$ sind uns noch unbekannt; wir haben aber ein Verfahren (wie dort beschrieben), um sie beliebig weit zu berechnen. Die Folge wird jedoch nie periodisch werden, da es eine rationale Zahl σ mit $\sigma^2 = 2$ nicht gibt. Die Tatsache, dass es eine bestimmte Vorschrift gibt, mit der man eine Folge von rationalen Zahlen

$$3; 3,1(7); \quad 3{,}12(7); \quad 3,126(7); \quad ...$$

herleiten kann, die 7-adisch gegen σ konvergiert, dass man also die mit 3,126... beginnende 7-adische Zahl in ganz bestimmter Weise beliebig weit berechnen kann, muss als Ersatz für die ziffernmäßig nicht mögliche vollständige Angabe von σ dienen.
Die Zahl 2 ist Quadrat dieser 7-adischen Zahl σ.

Ist eigentlich jede p-adische Zahl (also einschließlich der rationalen Zahlen) das Quadrat einer anderen p-adischen Zahl ? Sicher nicht.
Wir wissen, dass sich jede von 0 verschiedene p-adische Zahl α eindeutig in der Form $\alpha = p^m\varepsilon$ mit einer p-adischen Einheit ε darstellen lässt. Ist α Quadrat einer p-adischen Zahl $\gamma = p^k\varepsilon_1$, so muss $m = 2k$ und $\varepsilon = \varepsilon^2$ sein. (Ist also z. B. m ungerade, so kann α kein Quadrat sein.)

Um alle Quadrate unter den p-adischen Zahlen zu beschreiben, genügt es zu untersuchen, welche Einheiten Quadrate sind. Ist

$$\varepsilon = e_0 + e_1 p + e_2 p^2 + ... \qquad (0 \leq e_i < p, e_0 \neq 0)$$

und $\varepsilon = \eta^2$ und $\eta \equiv b(p)$ (b ganze rationale Zahl), so gilt $e_0 \equiv b^2(p)$,d.h., die Kongruenz $e_0 \equiv x^2(p)$ ist lösbar.

Ist für eine gegebene Primzahl p und eine Zahl $e_0 \not\equiv 0(p)$ eine Kongruenz der Form $x^2 \equiv e_0(p)$ lösbar, so heiße e_0 quadratischer Rest für p (andernfalls quadratischer Nichtrest). Dann gilt

Satz 19. Es sei $p \neq 2$. Dafür, dass eine p-adische Einheit

$$\varepsilon = e_0 + e_1 p + e_2 p^2 + ... \qquad (0 \leq e_i < p, e_0 \neq 0)$$

ein Quadrat ist, ist notwendig und hinreichend, dass e_0 quadratischer Rest für p ist.

Dass die Bedingung notwendig ist, haben wir eben gesehen. Dass sie auch hinreichend ist, muss noch bewiesen werden.

Es sei also

$$\varepsilon = e_0 + e_1 p + e_2 p^2 + ... = e_0{,}e_1 e_2 ...(p) \qquad (0 \leq e_i < p, e_0 \neq 0)$$

eine p-adische Einheit, in der die erste Ziffer e_0 quadratischer Rest für p ist. Dann ist es möglich, und das ist gerade zu zeigen, aus ε die Quadratwurzel zu ziehen, d.h., es gibt (wenigstens) eine p-adische Zahl η, so dass ($\sqrt{\varepsilon} = \eta$, d.h.) $\varepsilon = \eta^2$ gilt.

Da e_0 quadratischer Rest für p ist, gibt es eine ganze Zahl d_0, so dass $e_0 \equiv d_0^2(p)$ ist.[53] Für die p-adische Zahl $\eta_0 = d_0{,}...(p)$, deren erste Ziffer d_0 ist, gilt dann $\eta_0^2 \equiv \varepsilon(p)$.

Beispiel. $\varepsilon = 216 = 1 + 3 \cdot 5 + 3 \cdot 5^2 + 1 \cdot 5^3 = 1{,}331(5)$. Es gibt keine rationale Zahl r mit $r^2 = 216$.
Gäbe es eine solche, so könnte man $\sqrt{216} = \frac{p}{q}$ mit $(p,q) = 1$ ansetzen, also $216q^2 = p^2$. Hieraus folgt $2 \mid p^2$, also $2 \mid p$, d.h. $4 \mid p^2$; d.h. $216q^2 = p^2$, $113q^2 = 2p'$, also $2 \mid q^2$, d.h. $2 \mid q$ und damit $2 \mid (p,q) = 1$. Widerspruch.

Es gibt aber (nach Satz 19) eine 5-adische Zahl η mit $\eta^2 = \varepsilon$ (weil 1 quadratischer Rest für 5 ist). Es ist $e_0 = 1$, $d_0 = 4$ (wegen $4^2 = 16 \equiv 1(5)$). Für $\eta_0 = 4{,}...(5)$ gilt dann[54]

$$\eta_0^2 = 16{,}...(5) = 1{,}...(5)$$

Gesucht ist jetzt ein η_1 mit $\eta_1 \equiv \eta_0(p)$, für das

$$\eta_1^2 \equiv \varepsilon(p^2)$$

gilt. Setzen wir $\eta_1 = d_0 + d_1 p$ (dann ist $\eta_1 \equiv \eta 0(p)$), so ist

$$\eta_1^2 = d_0^2 + 2 d_0 d_1 p + d_1^2 p^2$$

Es muss (damit $\eta_1^2 \equiv \varepsilon(p^2)$ erfüllt wird)

$$d_0^2 + 2 d_0 d_1 p + d_1 p^2 \equiv e_0 + e_1 p(p^2)$$

[53] Es gilt auch $(-d_0)^2 \equiv e_0(p)$.
[54] Auch $d_0 = 1$ leistet es: $\eta_0 = 1, ...(5)$.

sein, also

$$2d_0d_1p \equiv e_0 + e_1p - d_0^2(p^2)$$

Wegen $e_0 \equiv d_0^2(p)$ ist $e_0 - d_0^2$ durch p teilbar, etwa $e_0 - d_0^2 = b_0p$. Es folgt[55]

$$2d_0d_1p \equiv b_0p + e_1p(p^2) \qquad \text{also} \qquad 2d_0d_1 \equiv b_0p + e_1 \equiv b_1(p)$$

Die Zahl d_1 muss so bestimmt werden, dass diese Kongruenz erfüllt ist. Wegen $2d_0 \not\equiv 0(p)$ (weil $p \neq 2$ und $p \nmid d_0$) gibt es ein d_1 mit dieser Eigenschaft. Für $\eta_1 = d_0 + d_1p$ mit einem so bestimmten d_1 gilt jetzt aber tatsächlich $\eta_1^2 \equiv \varepsilon(p^2)$.
In der Tat, es ist

$$\begin{aligned}\eta_1^2 - \varepsilon &\equiv d_0^2 + 2d_0d_1p + d_1^2p^2 - e_0 - e_1p(p^2) \equiv e_0 - b_0p + (2d_0d_1 - e_1)p - e_0(p^2)\\ &\equiv (2d_0d_1 - e_1 - b_0)p(p^2) \equiv 0(p^2)\end{aligned}$$

(hier benutzt man zuerst $d_0^2 = e_0 - b_0p$ und dann $2d_0d_1 - e_1b_0 \equiv 0(p)$ (so ist ja d_1 bestimmt worden)).

Beispiel.[56] $\varepsilon = 1{,}331(5)$, $\eta_0(5)$, $\eta_1 = 1{,}d_1(5)$, $(1-d_1)^2 = (1{,}2d_1d_2)^2(5)$.
Die Zahl d_1 ergibt sich aus $2d_1 \equiv 3(5)$ (wegen $b_0 = 0$ und $e_1 = 3$) zu $d_1 \equiv 4(5)$. Für $\eta_1 = 1{,}4(5)$ ist tatsächlich $\eta_1^2 \equiv 1{,}3(5)$.

Nebenrechnung:

1,	4	·1,	4	(5)	
1	4				
	4	16			
		1	3		
1,	3	2	3	≡	1,3 (5).

Hat man ein η_{n-1} gefunden, so dass $(\eta_{n-1} \equiv \eta_{n-2}(p^{n-1}))$

$$\eta_{n-1}^2 \equiv \varepsilon(p^n)$$

gilt, so kann man ein η_n, mit $\eta_n \equiv \eta_{n-1}(p^n)$, für das

$$\eta_n^2 \equiv \varepsilon(p^{n+1})$$

gilt, wie folgt finden. Man setzt η_n in der Form

$$\eta_n = \eta_{n-1} + d_np^n$$

an. Dann ist

$$\eta_n^2 = \eta_{n-1}^2 + 2\eta_{n-1}d_np^n + d_n^2p^{2n}$$

also

$$2\eta_{n-1}d_np^n = \eta_n^2 - \eta_{n-1}^2 - d_n^2p^{2n} \qquad \text{d.h.} \qquad 2\eta_{n-1}d_np^n \equiv \eta_n^2 - \eta_{n-1}^2(p^{n+1})$$

Soll $\eta_n^2 \equiv \varepsilon(p^{n+1})$ gelten, so muss also

$$2\eta_{n-1}d_np^n \equiv \varepsilon - \eta_{n-1}^2(p^{n+1}) \tag{40}$$

[55] Wegen $\varepsilon \equiv d_0^2(p)$ ist $\varepsilon - d_0^2 = b_1p$ mit einer ganzen p-adischen Zahl b_1:

$$\varepsilon - d_0^2 = (e_0 + p_1p + e_2p^2 + ...) - d_0^2 = e_0 - d_0^2 + e_1p + e_2p^2 + ... = b_0p + e_1p + e_2p^2 + ... = (e_1 + b_0)p + e_2p^2 + ...$$

also $b_1 = (e_1 + b_0) + e_2p + e_3p^2 + ... \equiv e_1 + b_0(p)$.

[56] Wir benutzen in diesen Rechnungen die Zifferndarstellung der 5-adischen Zahlen.

sein. Wegen $\varepsilon \equiv \eta_{n-1}^2(p^n)$ ist $\varepsilon - \eta_{n-1}^2 = b_n p^n$. Es folgt

$$2\eta_{n-1}d_n \equiv b_n(p)$$

Nun ist $\eta_{n-1} \equiv d_0(p)$. Die Zahl d_0 muss also so bestimmt werden, dass die Kongruenz $2d_0d_n \equiv b_n(p)$ erfüllt ist. Wegen $2d_0 \not\equiv 0(p)$ gibt es aber stets so ein d_n.
Für $\eta_n = \eta_{n-1} + d_n p^n$ mit einem so bestimmten d_n gilt nun in der Tat

$$\eta_n^2 \equiv \varepsilon(p^{n+1})$$

Es ist nämlich

$$\begin{aligned}\eta_n^2 - \varepsilon &\equiv \eta_{n-1}^2 + 2\eta_{n-1}d_n p^n + d_n^2 p^{2n} - \varepsilon(p^{n+1}) \equiv -b_n p^n + 2\eta_{n-1}d_n p^n(p^{n+1}) \\ &\equiv (2\eta_{n-1}d_n - b_n)p^n(p^{n+1}) \equiv 0(p^{n+1})\end{aligned}$$

(da $\eta_{n-1}^2 - \varepsilon \equiv -b_n p^n$ und $2\eta_{n-1}d_n - b_n \equiv 0(p)$).

Beispiel.[57] $\varepsilon = 1{,}331(5)$, $\eta_1 = 1{,}4(5)$, $\eta_2 = 1{,}4 + d_2 \cdot (0{,}1)^2$
Es ist

$$\eta_2^2 = (1{,}4)^2 + 2 \cdot (1{,}4) \cdot (0{,}1)^2 \cdot d^2 + d_2^2 \cdot (0{,}1)^2 = 1{,}323 + (0{,}0231) \cdot d_2 + (0{,}0001) \cdot d_2^2$$

$$(0{,}0231) \cdot d_2 = 1{,}331 - 1{,}323(5^2) \equiv 0{,}01344...(5^3)$$

Es muss $2d_1 \equiv 1(5)$, also z.B. $d_1 \equiv 3(5)$ sein. Für $\eta_2 = 1{,}43(5)$ gilt dann $\eta_2^2 \equiv \varepsilon \equiv 1{,}33(5^3)$.

Nebenrechnung:

1,	4	3		1,	4	3
1	4	3				
	4	16	12			
		3	12	9		
		1	4	5	2	
1,	3	3	3	4	2	(5)

Beispiel (Fortsetzung). $\varepsilon = 1{,}331(5)$, $\eta_2 = 1{,}43(5)$, $\eta_3 = 1{,}43 + d_3 \cdot (0{,}1)^3$.
Es muss (wegen (40)) $2 \cdot (1{,}43) \cdot d_3 \cdot (0,1)^2 \equiv \varepsilon - (1,43)^2(5^4)$ sein, also $(0{,}002121) \cdot d_3 \equiv 1{,}331 - 1{,}333(5^4) \equiv 0{,}003(5^4)$ sein.

Nebenrechnung:

	0,00544...
	1,331
-	1,333
	0,003444... (5)

Also muss $2d_3 \equiv 3(5)$ sein, z.B. $d_3 \equiv 4(5)$. Für $\eta_3 = 1{,}434(5)$ gilt dann $\eta_3^2 \equiv 1{,}331(5^4)$.

Nebenrechnung:

1,	4	3	4		1,	4	3	4
1	4	3	4					
	4	16	12	16				
		3	12	9	12			
			4	16	12	16		
		1	4	7	9	6	4	
1,	3	3	1	3	3	2	4	(5)

Beispiel (Fortsetzung). $\varepsilon = 1{,}331(5)$, $\eta_3 = 1{,}434(5)$, $\eta_4 = 1{,}434 + d_4 \cdot (0{,}1)^4$.

[57] Die Zifferndarstellung der 5 ist $5 = 0{,}1(5)$.

Es muss (wegen (40)) $2 \cdot (1{,}434) \cdot d_4 \cdot (0,1)^4 \equiv \varepsilon - (1{,}434)^2(5^5)$ sein, also $(0{,}00023) \cdot d_4 = 1{,}331 - 1{,}3313 \equiv 0{,}0002(5^5)$.

Nebenrechnung:

	1,434 · 2
	2,868
=	2,3241 (5)

	0,000544...
	1,331
-	1,3313
	0,000244

Es folgt $2d_4 \equiv 2(5)$, d.h. $d_4 \equiv 1(5)$. Für $\eta_4 = 1{,}4341$ gilt dann $\eta_4^2 = 1{,}331(5^5)$.

Nebenrechnung:

1,	4	3	4	1		1,	4	3	4	1
1	4	3	4	1						
	4	16	12	16	4					
		3	12	9	12	3				
			4	16	12	16	4			
				1	4	3	4	1		
		1	4	7	10	8	4	2		
1,	3	3	1	0	2	0	2	3	(5)	

Folgende Sprechweise könnte vereinbart werden: Eine p-adische Zahl η_n heißt Quadratwurzel mit einer Genauigkeit von $n+1$ Ziffern aus der p-adischen Zahl ε, wenn

$$\eta_n^2 \equiv \varepsilon(p^{n+1})$$

ist, also η_n^2 und ε die ersten $n+1$ Ziffern gemeinsam haben.
Im obigen Beispiel ist $\eta_4 = 1{,}4341$ eine Quadratwurzel mit einer Genauigkeit von 5 Ziffern aus 1,331 (5).

Da es keine rationale Zahl r mit $r^2 = 216$ gibt, ist die Ziffernfolge $1{,}4, 3{,}4{,}1{,}...$ nicht periodisch, wie weit man die Ziffern auch berechnet. Man kann die Ziffern beliebig weit berechnen, so dass man dann eine Quadratwurzel aus 1,331 (5) mit einer beliebig großen Genauigkeit erhält.[58]

Beispiel. $\sqrt{2}$ ist keine rationale Zahl. Es gibt jedoch eine 7-adische Zahl η, so dass $\eta^2 = 2$ ist. Wir berechnen solch ein η nach dem oben angegebenen Verfahren (wir verwenden dabei die Ziffernschreibweise):

$\varepsilon = 2(7)$. Es gibt ein d_0 mit $d_0^2 \equiv 2(7)$, z.B. $d_0 \equiv 3(7)$, $\eta_0 \equiv 3(7)$.
Setzt man $\eta_1 = 3 + d_1 \cdot (0,1)$, so ist $\eta_1^2 = 9 + 6d_1 \cdot (0{,}1) + d_1^2 \cdot (0,1)^2$. Es muss $6d_1 \cdot (0{,}1) = (0{,}6) \cdot d_1 \equiv 2 - 9 = 0{,}6(7^2)$ sein.

Nebenrechnung:

	7,66...
	2
-	9
	0,66 ...(7)

Also ist $6d_1 \equiv 6(7)$, d.h. $d_1 \equiv 1(7)$, und somit $\eta_1 = 3{,}1(7)$. In der Tat ist $\eta_1^2 \equiv \varepsilon = 2(7^2)$.

Nebenrechnung:

3,1 · 3,1
9 3
3 1
9 6 1 = 2,02 (7)

[58] Eine ziffernmäßig vollständige Angabe der nichtrationalen Zahl $\sqrt{216}$ durch eine reelle Zahl (Dezimalbruch) ist auch nicht möglich. Der mit 14,6969 beginnende und passend fortgeführte Dezimalbruch gibt $\sqrt{216}$ nur mit einer gewissen Genauigkeit wieder.

Man setze $\eta_2 = 3{,}1 + d_2 \cdot (0,1)^2$. Es muss $2 \cdot (3{,}1) \cdot d_2 \cdot (0{,}1)^2 = (0{,}061) \cdot d_2 \equiv 2 - 2{,}02 \equiv 0{,}05(7^3)$ sein.

Nebenrechnung:

	0,076...
	2
-	2,02
	0,056 ...(7)

Nebenrechnung: 0,076... Also $6d_2 \equiv 5(7)$, d.h. $d_2 \equiv 2(7)$. Für $\eta_2 = 3{,}12(7)$ ist tatsächlich $\eta_2^2 = 2(7^3)$.

Nebenrechnung:

3,12 · 3,12
9 3 6
3 1 2
6 2 4
1 1 2
2, 0 0 6 4 (7)

Wir setzen $\eta_3 = 3{,}12 + d_3 \cdot (0,1)^3$. Es muss $2 \cdot (3{,}12) \cdot d_3 \cdot (0,1)^3 = (0{,}00624) \cdot d_3 \equiv 2 - 2{,}0064 == 0{,}00126(7^4)$ sein.

Nebenrechnung:

	0,0076...
	2
-	2,0064
	0,00126 ...(7)

Somit ist $6d_3 \equiv 1(7)$, d.h. $d_3 \equiv 6(7)$. Für $\eta_3 = 3{,}126(7)$ ist $\eta_3^2 \equiv 2(7^4)$.

Nebenrechnung:

3,	1	2	6	·	3,	1	2	6
9	3	6	18					
	3	1	2	6				
		6	2	4	12			
			18	6	12	36		
	1	1	2	6	3	5	6	
2,	0	0	0	1	2	5	6	(7)

Ist $\varepsilon = e_0{,}e_1e_2...(p)$ eine p-adische Einheit, in der die erste Ziffer e_0 quadratischer Rest für p ist, so ist ε ein Quadrat, $\varepsilon = \eta^2$; η wird nach dem beschriebenen Verfahren sukzessive berechnet.
Satz 19 ist damit bewiesen.

Ist $p \neq 2$, so ist insbesondere jede p-adische Einheit $\varepsilon \equiv 1(p)$ Quadrat einer p-adischen Zahl. Die Zahl 1 ist ja quadratischer Rest für p.

Wann ist eigentlich ein $a \not\equiv 0(p)$ quadratischer Rest für p ($p \neq 2$)? Ist a quadratischer Rest für p, dann ist die Kongruenz $x^2 \equiv a(p)$ lösbar. Die Lösung x ist zu p teilerfremd, da $p \nmid a$. Wir können die Kongruenz mit $\frac{p-1}{2}$ potenzieren (da p ungerade ist, ist $\frac{p-1}{2}$ eine ganze Zahl) und erhalten

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

Nach dem Fermatschen Satz (Satz 12) ist nun $x^{p-1} \equiv 1(p)$. Also gilt notwendig

$$a^{\frac{p-1}{2}} \equiv 1(p) \tag{41}$$

falls a quadratischer Rest ist.

Diese Bedingung ist aber auch hinreichend, d.h., gilt (41) für eine zu p teilerfremde Zahl a, so ist a quadratischer Rest für p (diese Behauptung geben wir ohne Beweis an).

Satz 20 (Eulersches Kriterium). Für eine Primzahl $p \neq 2$ und eine ganze zu p teilerfremde Zahl a ist a quadratischer Rest für p genau dann, wenn

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

ist.
Betrachtet man den Fermatschen Satz in der Form

$$a^{p-1} - 1 \equiv \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \equiv 0(p)$$

so folgt hieraus

$$p \mid a^{\frac{p-1}{2}} - 1 \qquad \text{oder} \qquad p \mid a^{\frac{p-1}{2}} + 1$$

d.h.

$$a^{\frac{p-1}{2}} \equiv 1(p) \qquad \text{oder} \qquad a^{\frac{p-1}{2}} \equiv -1(p)$$

Eine der beiden Kongruenzen ist notwendig richtig, wegen $1 \not\equiv -1(p)$ aber auch nur eine.
Ein quadratischer Nichtrest für p, der ja die Kongruenz $a^{\frac{p-1}{2}} \equiv 1(p)$ nicht befriedigt, muss infolgedessen die Kongruenz $a^{\frac{p-1}{2}} \equiv -1(p)$ befriedigen. Setzen wir

$$\left(\frac{a}{b}\right) = \begin{cases} 1 & \text{falls } a \text{ quadratischer Rest für } p \text{ ist} \\ -1 & \text{falls } a \text{ quadratischer Nichtrest für } p \text{ ist} \end{cases}$$

($\left(\frac{a}{b}\right)$ heißt Legendre-Symbol) so folgt

Satz 21. $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}}(p)$.

Es ist also $\left(\frac{a}{p}\right) = 1$ oder -1, je nachdem, ob $a^{\frac{p-1}{2}} \equiv 1$ oder $-1(p)$ ist. Hieraus folgt

$$\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right) \tag{42}$$

d.h., das Produkt zweier quadratischer Reste oder Nichtreste ist ein quadratischer Rest für p, aber das Produkt eines quadratischen Restes mit einem Nichtrest ist ein Nichtrest (für p):

$$\begin{gathered} \text{Rest} \times \text{Rest} = \text{Rest}, \\ \text{Rest} \times \text{Nichtrest} = \text{Nichtrest}, \\ \text{Nichtrest} \times \text{Nichtrest} = \text{Rest} \end{gathered}$$

In der Tat, es ist

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}}(p) \qquad \text{und} \qquad \left(\frac{ab}{p}\right) \equiv (ab)^{\frac{p-1}{2}}(p)$$

d.h. $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)(p)$. Da das Legendre-Symbol nur die Werte +1 und -1 annimmt, folgt hieraus sofort

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

Ferner gilt:

Aus $a_1 \equiv a_2(p)$ folgt $\left(\frac{a_1}{p}\right) = \left(\frac{2}{p}\right)$ (43)

Aus $a_1 \equiv a_2(p)$ folgt nämlich $a_1^{\frac{p-1}{2}} \equiv a_2^{\frac{p-1}{2}}(p)$, also $\left(\frac{a_1}{p}\right) \equiv \left(\frac{a_2}{p}\right)(p)$ und daher wieder $\left(\frac{a_1}{p}\right) = \left(\frac{a_2}{p}\right)(p)$.

Beispiele.
1. $p = 11$; $a = 3$, $\left(\frac{3}{11}\right) \equiv 3^{\frac{11-1}{2}} = 3^5 = 243 = 21 \cdot 11 + 1 \equiv 1(11)$
d.h., 3 ist quadratischer Rest für 11.

Das Eulersche Kriterium liefert also den Nachweis, dass 3 quadratischer Rest für 11 ist, jedoch ist damit die Lösung von $x^2 \equiv 3(11)$ keineswegs gegeben (nur die Existenz der Lösung ist gesichert).
Durch Probieren findet man aber eine Lösung. Setzt man für x nacheinander 1,2,3,4,..., 10 ein, so muss wenigstens einmal $x^2 \equiv 3(11)$ sein:

$$1^2 \equiv 1(11), \quad 2^2 \equiv 4(11), \quad 3^2 \equiv 9(11), \quad 4^2 \equiv 5(11), \quad 5^2 \equiv 25 \equiv 2 \cdot 11 + 3 \equiv 3(11)$$

Fertig! $x \equiv 5(11)$ leistet schon das Verlangte. Dann tut es aber auch $x \equiv -5 \equiv 6(11)$.

2. $p = 7$, $a = 2$, $\left(\frac{2}{7}\right) = 2^{\frac{7-1}{2}} \equiv 2^3 \equiv 8 \equiv 1(7)$, d.h., 2 ist quadratischer Rest für 7.

3. $p = 5$, $a = 2$, $\left(\frac{2}{5}\right) = 2^2 \equiv 4 \equiv -1(5)$, d.h., 2 ist quadratischer Nichtrest für 5.

4. $p = 11$, $a = 2$, $\left(\frac{2}{11}\right) = 2^5 \equiv 32 \equiv -1(11)$, d.h, 2 ist quadratischer Nichtrest für 11.

5. $p = 5$, $a = 216$, $\left(\frac{216}{5}\right) = \left(\frac{1}{5}\right) \equiv 1$ wegen $216 \equiv 1(5)$, d. h., 216 ist quadratischer Rest für 5.

Ist nun eine Zahl $a \neq 0$ gegeben (z. B. $a = 2$ in den Beispielen 2 bis 4), so liegt die Frage nahe, für welche Primzahlen $p \neq 2$ diese gegebene Zahl a quadratischer Rest ist. Eine Antwort hierauf geben die folgenden drei Sätze.

Satz 22. a) 1 ist quadratischer Rest für alle Primzahlen;
b) -1 ist quadratischer Rest für und nur für die Primzahlen $p \equiv 1(4)$.
(Die Primzahlen $p \equiv 1(4)$ lassen sich in der Form $p = 4n + 1$ darstellen. Die ersten sind $5, 13, 17, 29, 37, 41, 53, 61, ...$) Der Satz folgt für $a = 1$ bzw. $a = -1$ aus dem Eulerschen Kriterium:

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

Da $\frac{p-1}{2}$ gerade ist, wenn p die Form $4n + 1$ hat, und ungerade, wenn p die Form $4n + 3$ hat, ist also -1 quadratischer Rest für jede Primzahl der Form $4n + 1$ und quadratischer Nichtrest für Primzahlen der Form $4n + 3$.

Satz 23. Die Zahl 2 ist quadratischer Rest für und nur für die Primzahlen $\equiv 1(8)$ oder $\equiv -1(8)$. (Ohne Beweis.)

Die Zahl 2 ist also quadratischer Rest für jede Primzahl der Form $8n \pm 1$ (d.h. $8n + 1$ oder $8n + 7$). Die ersten dieser Primzahlen sind $7, 17, 23, 31, 41, 47, 71, 79, ...$

Satz 24 (Gaußsches Reziprozitätsgesetz).
Für ungerade Primzahlen p, q ($p \neq q$) gilt

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

(Ohne Beweis.)

Haben die Primzahlen p und q die Form $p = 4n + 3$ und $q = 4n' + 3$, so ist das Produkt $\frac{p-1}{2} \cdot \frac{q-1}{2}$ eine ungerade Zahl, also ist $(-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}} = -1$ und daher

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

Hat aber wenigstens eine der Primzahlen p, q die Form $4n + 1$, so ist das Produkt $\frac{p-1}{2} \cdot \frac{q-1}{2}$ gerade und daher

$$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$$

Das Reziprozitätsgesetz gibt nun die Antwort auf die Frage, nach welchen Primzahlen $p \neq 2$, $\neq q$ die gegebene Primzahl $q = 2$ quadratischer Rest ist.
Hier haben wir nicht wie vorhin bei $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$ eine direkte explizite Bestimmung, sondern lediglich eine Beziehung von $\left(\frac{q}{p}\right)$ zu dem umgekehrten Symbol $\left(\frac{p}{q}\right)$ (daher die Bezeichnung "Reziprozitätsgesetz").

Ist $q \equiv 1(4)$ (also $q = 5, 13, 17,29, 31,37, 41, 53, 61, 73, 89, 97, 101, 109, 113,...$) so ist $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, also nach dem Eulerschen Kriterium

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

Die Primzahl q ist quadratischer Rest für alle Primzahlen p für die $p^{\frac{q-1}{2}} \equiv 1(p)$ ist.

Beispiel. $q = 5$, $\frac{q-1}{2} = 2$. Für welche Primzahlen p ist $p^2 \equiv 1(5)$?

p	3	7	11	13	17	19	23	29	31	37	...
$p \mod 5$	3	2	1	3	2	4	3	4	1	2	...
$p^2 \mod 5$	4	4	1	4	4	1	4	1	1	4	...

Ist $p \equiv 1(5)$ oder $p \equiv 4(5)$, so ist $p^2 \equiv 1(5)$.
Ist $p \equiv 2(5)$, $p \equiv 3(5)$, so ist $p^2 \equiv -1(5)$.
Also: 5 ist quadratischer Rest für alle Primzahlen $p \equiv 1(5)$ oder $p = -1(5)$. Die ersten solchen Primzahlen sind $11, 19, 29, 31, 41, 59, 61, 71, 79, ...$

Nach welchen Primzahlen p die Zahl $q \equiv 1(4)$ quadratischer Rest ist, hängt nur ab von dem Rest r mit $p \equiv r(q)$, $(1 \leq r \leq q - 1)$.
Ist $r^{\frac{q-1}{2}} \equiv 1(q)$, so ist q quadratischer Rest für p; ist $r^{\frac{q-1}{2}} \equiv -1(q)$, so ist q quadratischer Nichtrest für p.
Ist

$$q \equiv -1(4)$$

(also $q = 3, 7, 19, 23, 43, 47, 59, 67, 71, 79, 83, 103, 107, ...$), so ist

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

Die Primzahl q ist quadratischer Rest für alle Primzahlen p, für die gleichzeitig

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

oder gleichzeitig

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

ist (weil dann $\left(\frac{q}{p}\right) = 1$ wird).

Für alle Primzahlen p, für die also entweder sowohl $p \equiv 1(4)$ als auch $p^{\frac{q-1}{2}} \equiv 1(q)$ oder sowohl $p \equiv -1(4)$ als auch $p^{\frac{q-1}{2}} \equiv -1(q)$ ist, ist q quadratischer Rest.

Beispiel. $q = 3$, $\frac{q-1}{2} = 1$. Für welche Primzahlen p ist entweder sowohl $p \equiv (4)$ als auch $p \equiv 1(3)$ oder sowohl $p \equiv -1(4)$ als auch $p = -1(3)$?

p	5	7	11	13	17	19	23	29	31	37	...
$p \mod 4$	1	-1	-1	1	1	-1	-1	1	-1	1	...
$p \mod 3$	-1	1	-1	1	-1	1	-1	-1	1	1	...

Die ersten solchen Primzahlen sind $11, 13, 23, 37$ und weiter $47, 61, 71, 73, 83, 97, 107, 109, ...$ Es muss ja entweder $p - 1$ oder $p + 1$ durch 12 teilbar sein.

Weiteres Beispiel. $q = 7$, $\frac{q-1}{2} = 3$. Für welche Primzahlen p ist entweder $p \equiv 1(4)$ und $p^3 \equiv 1(7)$ oder $p \equiv -1(4)$ und $p^3 \equiv -1(7)$?

p	3	5	11	13	17	19	23	29	31	37	...
$p \mod 7$	3	5	4	6	3	5	2	1	3	2	...
$p^3 \mod 7$	-1	-1	1	-1	-1	-1	1	1	-1	1	...
$p \mod 4$	-1	1	-1	1	1	-1	-1	1	-1	1	...

Die ersten solchen Primzahlen sind $3,19,29,31,37$.
Für $p \equiv 1,2,4(7)$ ist $p^3 \equiv= 1(7)$, und für $p = 3,5,6(7)$ ist $p^3 \equiv -1(7)$.
Ist entweder sowohl $p \equiv 1(4)$ als auch $p \equiv 1,2,4(7)$ oder sowohl $p \equiv -1(4)$ als auch $p = 3,5,6(7)$, so ist 7 quadratischer Rest für p.

Gilt also $28 \mid p - 1$ oder $28 \mid p - 0$ oder $28 \mid p - 25$ der $28 \mid p - 3$ oder $28 \mid p - 19$ oder $28 \mid p - 27$, so ist 7 quadratischer Rest für p.[59]

Nach welchen Primzahlen p die Zahl $q = -1(4)$ quadratischer Rest ist, hängt nur ab vom Verhalten von q für 4 und für q. Es sei $p \equiv r(q)$ $(1 \leq r \leq q - 1)$.

Ist $r^{\frac{q-1}{2}} \equiv 1(q)$ und $p \equiv 1(4)$, so ist q quadratischer Rest für p.

Ist $r^{\frac{q-1}{2}} \equiv 1(q)$ und $p \equiv -1(4)$, so ist q quadratischer Nichtrest für p.

Ist $r^{\frac{q-1}{2}} \equiv -1(q)$ und $p \equiv 1(4)$, so ist q quadratischer Nichttest für p.

Ist $r^{\frac{q-1}{2}} \equiv -1(q)$ und $p \equiv -1(4)$, so ist q quadratischer Rest für p.

Nun ist auch die Frage zu beantworten, für welche ungeraden Primzahlen p eine gegebene Zahl $a \neq 0$ quadratischer Rest ist. Dabei sind $p = 2$ und die endlich vielen Primteiler von a außer Betracht zu lassen. (Das Legendre-Symbol $\left(\frac{p}{q}\right)$ ist nur für die Primzahlen p und Zahlen a mit $(a, p) = 1$ definiert.) Hat a die Primzahlzerlegung

$$a = (-1)^k 2^{e_2} \prod_{q \text{ Primzahl}, q \neq 2} q^{e_q}$$

[59] $p \equiv 1,9,25(28)$ oder $p \equiv 3, 19, 27(28)$.

($e_q \neq 0$ nur für endlich viele q), so ist für jede Primzahl p mit $p \neq 2$ und $p \nmid a$

$$\left(\frac{a}{p}\right) = \left(\frac{-1}{p}\right)^k \left(\frac{2}{p}\right)^{e_2} \prod_{q \text{ Primzahl}, q \neq 2} \left(\frac{q}{p}\right)^{e_q} \tag{44}$$

Über die Legendre-Symbole $\left(\frac{-1}{p}\right)$, $\left(\frac{2}{p}\right)$, $\left(\frac{q}{p}\right)$ $(q \neq 2, \neq p)$ ist alles bekannt; es ist also prinzipiell entscheidbar, wann das Produkt aller in (44) auftretenden Symbole 1 und wann -1 ergibt. Dies liefert Bedingungen für das Verhalten von p, gibt also eine Antwort auf die Ausgangsfrage.

Beispiel. $a = 21 = 3 \cdot 7$, $\left(\frac{21}{p}\right) = \left(\frac{3}{p}\right)\left(\frac{7}{p}\right)$.
In den vorigen Beispielen ist $\left(\frac{3}{p}\right)$, $\left(\frac{7}{p}\right)$ berechnet worden:

$$\left(\frac{3}{p}\right) = \begin{cases} 1 & \text{für } p \equiv 1(4) \text{ und } p \equiv 1(3), \text{bzw. für } p \equiv -1(4) \text{ und } p \equiv -1(3) \\ -1 & \text{sonst} \end{cases}$$

$$\left(\frac{7}{p}\right) = \begin{cases} 1 & \text{für } p \equiv 1(4) \text{ und } p \equiv 1,2,4(7), \text{bzw. für } p \equiv -1(4) \text{ und } p \equiv 3,5,6(7) \\ -1 & \text{sonst} \end{cases}$$

Daher ist sowohl $\left(\frac{3}{p}\right) = 1$ als auch $\left(\frac{7}{p}\right) = 1$, falls für $p \equiv 1(4)$

$$p \equiv 1(3) \qquad \text{und} \qquad p \equiv 1,2,4(7)$$

ist bzw. falls für $p \equiv -1(4)$

$$p \equiv -1(3) \qquad \text{und} \qquad p \equiv 3,5,6(7)$$

ist. Es ist sowohl $\left(\frac{3}{p}\right) = -1$ als auch $\left(\frac{7}{p}\right) = -1$, falls für $p \equiv 1(4)$

$$p \equiv -1(3) \qquad \text{und} \qquad p \equiv 3,5,6(7)$$

ist bzw. falls für $p \equiv -1(4)$

$$p \equiv 1(3) \qquad \text{und} \qquad p \equiv 1,2,4(7)$$

ist. Es kommt hier somit gar nicht auf das Verhalten von p mod 4 an, vielmehr nur auf das von p mod 7 und mod 3.
In den folgenden Fällen ist also $\left(\frac{21}{7}\right) = 1$, d.h. 21 quadratischer Rest für p:

$p \mod 7$	$p \mod 3$	Beispiele für p
1	1	337, 43
2	1	37, 79
4	1	109, 67
3	-1	17, 59
5	-1	5, 47
6	-1	41, 83

Für $p \neq 2$ ist nach Satz 19 (und den sich daran anschließenden Betrachtungen über quadratische Reste) bekannt, welche p-adischen Einheiten Quadrate sind. Für $p = 2$ gibt der folgende Satz Auskunft:

Satz 25. Eine 2-adische Einheit ε ist Quadrat einer 2-adischen Zahl dann und nur dann, wenn

$\varepsilon \equiv 1(8)$ ist.

Ist nämlich

$$\varepsilon = \eta^2, \qquad \eta = 1 + a_1 \cdot 2 + a_2 \cdot 2^2 + \ldots \quad (0 \leq a_i \leq 1)$$

so ist

$$\begin{aligned}\eta^2 &= (1 + a_1 \cdot 2 + a_2 \cdot 2^2 + \ldots)(1 + a_1 \cdot 2 + a_2 \cdot 2^2 + \ldots) \\ &= 1 + a_1 \cdot 2 + a_2 \cdot 2^2 + a_3 \cdot 2^3 + \ldots + a_1 \cdot 2 + a_1^2 \cdot 2^2 + a_1 a_2 \cdot 2^3 + \ldots \\ &\quad + a_2 \cdot 2^2 + a_1 a_2 \cdot 2^3 + \ldots + a_3 \cdot 2^3 + \ldots = 1 + 2a_1 \cdot 2 + (a_1^2 + 2a_2) \cdot 2^2 + (\ldots) \cdot 2^3 + \ldots \\ \eta^2 &= 1 + (a_1 + a_1^2 + 2a_2) \cdot 2^2 \equiv 1(2^3)\end{aligned}$$

(wegen $(a_1 + a_1^2 + 2a_2) \equiv 0(2)$).

Die Bedingung $\varepsilon \equiv 1(8)$ ist also notwendig dafür, dass ε Quadrat einer 2-adischen Zahl ist. Sie ist aber auch hinreichend: Ist $\varepsilon \equiv 1(8)$, so ist ε Quadrat einer 2-adischen Zahl.

Diese 2-adische Einheit hat die Eigenschaft, dass $\varepsilon \equiv 1(2^3)$ ist. Für jede 2-adische Einheit gilt $\varepsilon \equiv 1(2)$.[60]
Allgemein heiße nun eine 2-adische Einheit Einheit von der Stufe k, falls $\varepsilon = 1(2^k)$ ist. Jede Einheit von der Stufe k ist auch eine Einheit von der Stufe $k-1$ (weil mit $\varepsilon \equiv 1(2^k)$ erst recht $\varepsilon \equiv 1(2^{k-1})$ ist).
Die Einheit

$$-1 = 1 + 2 + 2^2 + 2^3 + \ldots$$

ist von der Stufe 1. Die Einheit

$$\eta_2 = 1 + 2^2$$

ist von der Stufe 2. Die Einheit

$$\eta_3 = \eta_2^2 = (1 + 2^2)^2 = 1 + 2^3 + \ldots$$

ist von der Stufe 3. Die Einheit

$$\eta_4 = (1 + 2^2)^{2^2} = 1 + 2^4 + \ldots$$

ist von der Stufe 4. Allgemein ist für $k = 2, 3, \ldots$

$$\eta_k = (1 + 2^2)^{2^{k-2}} = 1 + 2^k + \ldots$$

eine Einheit von der Stufe k.
Ist nun eine beliebige Einheit ε von der Stufe k gegeben, so hat sie die Form $\varepsilon = 1 + a_k 2^k + a_{k+1} 2^{k+1} + \ldots$, wobei $a_k \equiv 0$ oder $a_k \equiv 1(2)$ ist. Daher ist entweder

$$\varepsilon \equiv 1(2^{k+1}) \quad (\text{falls } a_k \equiv 0(2)) \qquad \text{oder} \qquad \varepsilon \equiv 1 + 2^k \equiv \eta_l(2^{k+1}) \quad (\text{falls } a_k \equiv 1(2))$$

Im ersten Fall ist ε also sogar Einheit von der Stufe $k+1$. Im zweiten Fall ist $\varepsilon = \eta_k \varepsilon'$, wobei $\varepsilon' \equiv 1(2^{k+1})$ ist (d.h., ε ist Produkt von η_k mit einer Einheit von der Stufe $k+1$).[61]

[60] Ist nämlich $\varepsilon \equiv 0(2)$ für eine 2-adische Zahl, so ist ε keine Einheit.

[61] In der Tat, es ist $\varepsilon \equiv \eta_k(2^{k+1})$. Daher ist die 2-adische Einheit $\varepsilon' = \frac{\varepsilon}{\eta_k} \equiv 1(2^{k+1})$. Aus $\varepsilon - \eta_k \equiv 0(2^{k+1})$ folgt nämlich

$$\varepsilon' - 1 = \frac{\varepsilon}{\eta_k} - \frac{\eta_k}{\eta_k} = \frac{\varepsilon - \eta_k}{\eta_k} \equiv 0(2^{k+1})$$

Jetzt sei irgendeine Einheit $\varepsilon \equiv 1(2)$ gegeben. Sie ist von der Stufe 1. Wendet man den eben durchgeführten Schluss auf ε an, so folgt $\varepsilon \equiv (-1)^b \varepsilon_2$ (mit $b = 0$ oder $b = 1$ und einer Einheit ε_2 von der Stufe 2). (Es ist nämlich ε sogar von der Stufe 2, also $b = 0$ oder $\varepsilon \equiv -1(2^2)$, d.h. $\varepsilon \equiv (-1)\varepsilon_2$ mit $\varepsilon_2 \equiv 1(2^2)$).
Der Schluss, auf ε_2 angewendet, liefert

$$\varepsilon_2 = \eta_2^{a_0} \varepsilon_3$$

mit einer Einheit ε_3 von der Stufe 3 und $a_0 = 0$ oder 1. (Es ist nämlich ε_2 sogar von der Stufe 3, also $a_0 = 0$ oder $\varepsilon_2 \equiv \eta_2(2^3)$, d.h. $\varepsilon_2 = \eta_2 \varepsilon_3$ mit $\varepsilon_3 \equiv 1(2^3)$).
Der obige Schluss, auf ε_3 angewendet, liefert

$$\varepsilon_3 = \eta_3^{a_1} \varepsilon_4$$

mit $a_2 = 0$ oder 1 und einer Einheit ε_4 von der Stufe 4. Ebenso folgt

$$\varepsilon_4 = \eta_4^{a_2} \varepsilon_5$$

mit $a_2 = 0$ oder 1 und einer Einheit ε_5 von der Stufe 5.

So fortsetzend, erhält man eine Folge ε_i 2-adischer Einheiten von der Stufe i:

$$\varepsilon_i \equiv 1(2^i)$$

d.h. $e_2(\varepsilon_i - 1) \geq i$, also

$$|\varepsilon_i - 1|_2 = \left(\frac{1}{2}\right)^{e_2(\varepsilon_i - 1)} \leq \frac{1}{2^i}$$

d.h., $|\varepsilon_i - 1|$ ist eine Nullfolge (wegen $\frac{1}{2^i} \to 0$ für $i \to \infty$) . Daher ist

$$2 - \lim_{i \to \infty} \varepsilon_i = 1$$

Nun ist

$$\varepsilon = (-1)^b \varepsilon_2 = (-1)^b \eta_2^{a_0} \varepsilon_3 = (-1) \eta_2^{a_0} \eta_3^{a_1} \varepsilon_4 = ...$$

also

$$\varepsilon = (-1)^b \eta_2^{a_0} \eta_3^{a_1} \eta_4^{a_2} ... \eta_k^{a_{k-2}} \varepsilon_{k+1}$$

Wegen

$$\eta_2 = 1 + 2^2, \quad \eta_3 = (1 + 2^2)^2, \quad \eta_4 = (1 + 2^2)^{2^2}, \quad ..., \quad \eta_k = (1 + 2^2)^{2^{k+1}}$$

folgt

$$\varepsilon = (-1)^b (1 + 2)^{a_0} (1 + 2^2)^{a_1 \cdot 2} ... (1 + 2^2)^{a_{k-2} \cdot 2^{k-2}} \varepsilon_{k+1}$$

(Die Exponenten a_i sind nach Konstruktion eindeutig bestimmt.) Es ergibt sich

$$\varepsilon = (-1)^b (1 + 2^2)^{a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + ... + a_{k-2} \cdot 2^{k-2}} \varepsilon_{k+1}$$

Nun ist einerseits

$$2 - \lim_{k \to \infty} \varepsilon = \varepsilon$$

andererseits

$$2 - \lim_{k \to \infty} \varepsilon = 2 - \lim_{k \to \infty} (-1)^b \cdot 2 - \lim_{k \to \infty} (1 + 2^2)^{a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + ... + a_{k-2} \cdot 2^{k-2}} \cdot 2 - \lim_{k \to \infty} \varepsilon_{k+1}$$

Es ist [62]

$$2 - \lim_{k\to\infty} (-1)^b = (-1)^b$$

$$2 - \lim_{k\to\infty} (1+2^2)^{a_0+a_1\cdot 2+a_2\cdot 2^2+\ldots+a_{k-2}\cdot 2^{k-2}} = (1+2^2)^{2-\lim\limits_{k\to\infty} a_0+a_1\cdot 2+a_2\cdot 2^2+\ldots+a_{k-2}\cdot 2^{k-2}} = (1+2^2)^{\alpha}$$

(mit der 2-adischen Zahl $\alpha = a_0 + a_1 \cdot 2 + a_2 \cdot 2^2 + ...$) sowie

$$2 - \lim_{k\to\infty} \varepsilon_{k+1} = 1$$

Hieraus folgt die (eindeutige) Darstellung

$$\varepsilon = (-1)^b (1+2^2)^{\alpha} \tag{45}$$

worin $b = 0$ oder 1 und α eine ganze 2-adische Zahl ist.
Ist nun $\varepsilon \equiv 1(8)$, also ε Einheit von der Stufe 3, so ist in

$$\varepsilon = (-1)^b (1+2^2)^{a_0+a_1\cdot 2+\ldots}$$

$b = 0$ und $a_0 = 0$, also

$$\varepsilon = (1+2^2)^{a_1\cdot 2+a_2\cdot 2^2+\ldots} = (1+2^2)^{2\alpha'}$$

mit $\alpha' = a_1 + a_2 \cdot 2 + a_3 \cdot 2^2 + ...$, also $\varepsilon = [(1+2^2)^{\alpha'}]^2$ Quadrat einer 2-adischen Einheit (womit Satz 25 bewiesen ist).

Dieser Beweis zeigt, dass ein $\varepsilon = 1(8)$ Quadrat einer 2-adischen Einheit η ($\varepsilon = \eta^2$) ist. Wie aber $\eta = (1+2^2)^{\alpha'}$ genauer aussieht, zeigt der Beweis nicht, da der Exponent α' bei einer Einheit, die in der Form

$$\varepsilon = 1 + e_3 \cdot 2^3 + e_4 \cdot 2^4 + ...$$

gegeben ist, unbekannt ist. Dieser Beweis ist ein reiner Existenzbeweis, er zeigt die Existenz einer Einheit η mit $\eta^2 = \varepsilon$. Wie man jedoch η bekommt, wie man η konstruieren kann, gibt er nicht an. Hierin unterscheidet er sich von dem Beweis des Satzes 19 im Fall $p \neq 2$.

Wir wollen auch im Fall $p = 2$ einen konstruktiven Beweis angeben. Zuvor bemerken wir noch, dass eine Darstellung der Form (45) auch für p-adische Einheiten im Fall $p \neq 2$ richtig ist. Ist $p \neq 2$, so lässt sich jede p-adische Einheit ε eindeutig in der Form

$$\varepsilon = \zeta^b (1+p)^{\alpha} \tag{46}$$

schreiben, worin α eine ganze p-adische Zahl ist, $b \in \{0, 1,..,p-2\}$ und ζ eine p-adische Zahl mit der Eigenschaft $\zeta^{p-1} = 1$, $\zeta^{p-2} \neq 1$ ist (dass es solch ein ζ gibt, ist nicht selbstverständlich und muss ebenso wie die Darstellung (46) erst bewiesen werden).
Aus (46) kann man übrigens auch den Satz 19 herleiten.

Aus den Darstellungen (45) bzw. (46) und Satz 17 folgt, dass jede p-adische Zahl $\beta \neq 0$ eindeutig in der Form

$$\beta = \begin{cases} 2^k (-1)^b (1+2^2)^{\alpha} & \text{für } p = 2 \\ p^k \zeta^b (1+p)^{\alpha} & \text{für } p \neq 2 \end{cases}$$

darstellbar ist, worin k eine ganze Zahl, α eine ganze p-adische Zahl und $b = 0, 1$ für $p = 2$ oder $b = 0, 1,..., p\_2$ für $p \neq 2$. Diese Darstellung hat für reelle Zahlen $\beta \neq 0$ ihr Analogon in der Darstellung

$$\beta = e^{\alpha} (-1)^a \tag{47}$$

[62] Es ist nämlich $\lim \eta^{a_i} = \eta^{\lim a_i}$.

mit einer reellen Zahl α und $a = 0{,}1$.

Wir geben nun noch einen konstruktiven Beweis für den Satz 25. (Oft ist ein solcher Beweis für mathematische Aussagen gar nicht möglich, und man muss sich mit reinen Existenzaussagen begnügen!) Dazu orientieren wir uns am Beweis von Satz 19.

Beweis des Satzes 25. Es ist noch zu zeigen, dass eine Einheit ε mit $\varepsilon \equiv 1(8)$ Quadrat einer 2-adischen Zahl η ist. Wegen $\varepsilon \equiv 1(8)$ können wir uns ein der Form

$$\varepsilon = 1 + e_3 \cdot 2^3 + e_4 \cdot 2^4 + e_5 \cdot 2^5 + \ldots \quad (e_i = 0 \text{ oder } 1)$$

gegeben denken. Wir konstruieren (wie beim Beweis von Satz 19) für jedes n Quadratwurzeln η_n mit einer Genauigkeit von $n+1$ Ziffern aus der 2-adischen Zahl ε, also für jedes $n \geq 0$ ein η_n mit

$$\eta_n^2 \equiv \varepsilon(2^{n+1})$$

Dazu setzen wir $\eta_0 = \eta_1 = \eta_2 = 1$ (wegen $\varepsilon = 1(2^3)$). Gesucht ist jetzt ein η_3 mit $\eta_3 \equiv \varepsilon(2^4)$. Wir setzen

$$\eta_3 = \eta_2 + d_3 \cdot 2^2 = 1 + d_3 \cdot 2^2$$

(hierin unterscheiden wir uns auch vom Fall $p \neq 2$, wo $\eta_3 = \eta_2 + d_3 p^3$ gesetzt wurde). Es ist

$$\eta_3^2 = 1 + 2d_3 \cdot 2^2 + d_3 \cdot 2^4$$

Es muss (damit $\eta_3^2 \equiv \varepsilon(2^4)$ erfüllt wird) $1 + d_3 \cdot 2^3 \equiv 1\text{ü} + e_3 \cdot 2^3(2^4)$, also $2^3 d_3 \equiv 2^3 e_3(2^4)$, d.h.

$$d_3 \equiv e_3(2)$$

sein. Für $\eta_3 = 1 + e_3 \cdot 2^2$ gilt nun tatsächlich

$$\eta_3^2 = 1 + e_3 2^3 + e_3^2 2^4 \equiv 1 + e_3 2^3 \equiv \varepsilon(2^4)$$

Nun setzen wir

$$\eta_4 = \eta_3 + d_4 \cdot 2^3$$

Dann ist

$$\eta_4^2 = \eta_3^2 + 2^4 \eta_3 d_4 + d_4^2 \cdot 2^6$$

Damit $\eta_4^2 \equiv \varepsilon(2^5)$ erfüllt wird, muss

$$2^4 \eta_3 d_4 \equiv \varepsilon - \eta_3^2(2^5)$$

sein. Aus $\eta_3^2 = \varepsilon(2^4)$ folgt

$$\varepsilon - \eta_3^2 = 2^4 b_4$$

mit einer ganzen p-adischen Zahl b_4. Die Zahl d_4 muss so bestimmt werden, dass $d_4 \eta_3 \equiv b_4(2)$ ist. Wegen $\eta_3 = 1(2)$ muss

$$d_4 \equiv b_2(2)$$

sein. In der Tat, mit $\eta_4 = \eta_2 + b_4 \cdot 2^3$ ist

$$\eta_4^2 \equiv \eta_3^2 + b_4 \cdot 2^4 \equiv \varepsilon(2^5)$$

Haben wir ein η_n ($n \geq 4$) gefunden, so dass $\eta_n \equiv \eta_{n-1}(2^{n-1})$ und $\eta_n^2 \equiv \varepsilon(2^{n+1})$ ist, so können wir ein η_{n+1} mit $\eta n + 1 \equiv \eta_n(2^n)$, für das $\eta_{n+1}^2 \equiv \varepsilon(2^{n+2})$ gilt, wie folgt finden. Wir setzen

$$\eta_{n+1} = \eta_n + d_{n+1} 2^n$$

Dann ist $\eta_{n+1}^2 = \eta_n^2 + 2\eta_n d_{n+1} 2^n + d_{n+1} 2^{2n}$, also

$$\eta_n d_{n+1} \cdot 2^{n+1} \equiv \eta_{n+1}^2 - \eta_n^2 (2^{n+2})$$

Soll $\eta_{n+1}^2 \equiv \varepsilon(2^{n+1})$ gelten, so muss

$$\eta_n d_{n+1} \cdot 2^{n+1} \equiv \varepsilon - \eta_n^2 (2^{n+2})$$

sein. Wegen $\varepsilon \equiv \eta_n^2 (2^{n+1})$ ist

$$\varepsilon - \eta_n^2 = b_{n+1} 2^{n+1}$$

Es folgt $\eta_n d_{n+1} \equiv b_{b+2}(2)$, also (wegen $\eta_n \equiv 1(2)$)

$$d_{n+1} \equiv b_{n+1}(2)$$

Für $\eta_{n+1} = \eta_n + b_{n+1} 2^n$ gilt dann tatsächlich

$$\eta_{n+1} - \varepsilon \equiv \eta_n^2 - \varepsilon + b_{n+1} 2^{n+1} \equiv 0(2^{n+2})$$

Die Quadratwurzeln η_n mit einer Genauigkeit von $n+1$ Ziffern aus $\varepsilon = 1 + e_2^2 3 + e_4 2^4 + ...$ sind also nacheinander wie folgt zu finden:

$$\begin{aligned}
&\eta_0 = \eta_1 = \eta_2 = 1 \\
&\eta_3 = 1 + e_3 \cdot 2^2, \qquad \varepsilon - \eta_3^2 = b_4 \cdot 2^4 \\
&\eta_4 = 1 + e_3 \cdot 2^2 + b_4 \cdot 2^3, \qquad \varepsilon - \eta_4^2 = b_5 \cdot 2^5 \\
&\eta_5 = 1 + e_3 \cdot 2^2 + b_4 \cdot 2^3 + b_5 \cdot 2^4, \qquad \varepsilon - \eta_5^2 = b_6 \cdot 2^6
\end{aligned}$$

usw. (es kommt jeweils nur auf b_i modulo 2 an).

Beispiel. $\varepsilon = 17$, also $\varepsilon = 1 + 1 \cdot 2^4 = 1{,}0001(2)$. Es ist $\varepsilon_3 = 0$, also $\eta_0 = \eta_1 = \eta_2 = \eta_3 = 1$, $\eta_3^2 = 1$, daher $\varepsilon - \eta_3^2 = 1{,}0001 - 1 = 0{,}0001(2)$, d.h. $b_4 = 1$. $\eta_4 = 1 + 2^3 = 1{,}001(2)$, $\eta_4^2 = 1{,}000101$, daher $\varepsilon - \eta_4^2 = 0{,}0000011...(2)$, d.h. $b_5 = 0$.

Nebenrechnungen:

1,001 · 1,001			0,000002111 ...
1001			1,0001
1001		-	1,000101
1,000 101 (2)			0,000001111 ... (2)

$\eta_5 = \eta_4$, $\varepsilon - \eta_5^2 = \varepsilon - \eta_4^2$, $b_6 = 1$
$\eta_6 = 1 + 2^3 + 2^5 = 1{,}00101(2)$, $\eta_6^2 = 1{,}0001001011(2)$, daher $\varepsilon - \eta_6^2 = 0{,}00000011...(2)$, $b_7 = 1$.

Nebenrechnungen:

1,00101 · 1,00101			0,0000002111 ...
100101			1,0001
100101		-	1,0001001011
100101			0,00000011 ... (2)
1,0001001011 (2)			

$\eta_7 = 1 + 2^3 + 2^5 + 2^6 = 1{,}001011(2)$, usw.
Die sich ergebende Ziffernfolge 1,0,0,1,0,1,1,... wird nicht periodisch, da es keine rationale Zahl r mit $r^2 = 17$ gibt (Warum ?).
Die 2-adische Zahl η mit $\eta^2 = 17$ ist $1{,}001011...(2)$.

Man kann p-adische Zahlen addieren, subtrahieren, multiplizieren und dividieren (sofern der

Divisor von 0 verschieden ist) und erhält stets wieder eine (sogar eindeutig bestimmte) p-adische Zahl.
Wann man radizieren kann, folgt aus den Sätzen 19 und 25. Die Frage nach einer Quadratwurzel aus der p-adischen Zahl ist gleichbedeutend mit der Frage, ob es im Bereich $\mathbb{Q}$, der p-adischen Zahlen eine Lösung der Gleichung

$$x^2 - \alpha = 0 \tag{48}$$

gibt. Hat α die Form $\alpha = p^k\varepsilon$ mit einer p-adischen Einheit

$$\varepsilon = e_0 + e_1 p + e_2 p^2 + \ldots \quad (0 \leq e_i < p, e_0 \neq 0)$$

so ist die Gleichung (48) dann und nur dann lösbar in Q_p, wenn

$$k \equiv 0(2)$$

und

$$\left\{ \begin{array}{l} e_0 \text{ quadratischer Rest für } p \text{ ist) im Fall } p \neq 2 \\ e_0 = 1 \text{ und } e_1 = e_2 = 0 \text{ ist) im Fall } p = 2 \end{array} \right\}$$

Beispiele. 1. $p = 2$. Die Gleichungen $x^2 - 2 = 0$, $x^2 - 3 = 0$, $x^2 - 5 = 0$, $x^2 - 6 = 0$, ferner $x^2 - r = 0$ mit $r = 7{,}8{,}10$ sind in Q_p unlösbar.
Die Gleichungen $x^2 - r = 0$ mit $r = 1$ oder 4 oder 9 oder 17 oder 33 sind in Q_p lösbar. Die Gleichung $x_2 + 1 = 0$ ist unlösbar.

2. $p = 7$. Es ist

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1 \qquad \text{und} \qquad \left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1$$

Die Gleichungen $x^2 - r = 0$ mit $r = 3, 5, 6, 7, 14, 28, 5 \cdot 49, -1$ sind in Q_p unlösbar. Die Gleichungen $x^2 - s = 0$ mit $s = 1, 2, 4, 49, 98, 196$ sind in Q_p lösbar.

Wir bemerken, dass in der Menge der reellen Zahlen eine Gleichung der Form (48) dann und nur dann lösbar ist, wenn α positiv ist.
Welche Beziehung besteht eigentlich zwischen reellen und p-adischen Zahlen ? In beiden Mengen sind die rationalen Zahlen enthalten. In den nachfolgenden Tabellen sind noch einmal einige Eigenschaften dieser Zahlen zusammengefasst (wobei wir die Eigenschaften der reellen Zahlen als bekannt voraussetzen, während die Eigenschaften der p-adischen Zahlen aus den oben bewiesenen Sätzen folgen).

Rationale Zahlen

Absoluter Betrag $\lvert r\rvert = \max(r, -r)$	p-Betrag $\lvert r\rvert_p = \left(\frac{1}{p}\right)^{e_p(r)}$
r ist absolut kleiner als r', falls $\lvert r\rvert < \lvert r'\rvert$. Zu beliebigen rationalen Zahlen r und r' gibt es stets eine natürliche Zahl n, so dass nr absolut größer als r' ist.	r ist für-p-kleiner als r', falls $\lvert r\rvert_p < \lvert r'\rvert_p$. Ist r für-p-kleiner als r', so ist für jede natürliche Zahl n auch nr für-p-kleiner als r'.
Eine rationale Zahl r heißt Grenzwert einer Folge r_1, r_2, r_3, ..., falls $\lim_{n\to\infty} \lvert r - r_n\rvert = 0$	Eine rationale Zahl r heißt p-Grenzwert einer Folge r_1, r_2, r_3, ..., falls $\lim_{n\to\infty} \lvert r - r_n\rvert_p = 0$
Eine Zahlenfolge, die einen Grenzwert besitzt, heißt konvergent.	Eine Zahlenfolge, die einen p-Grenzwert besitzt, heißt p-konvergent. Die Folge p, p^2, p^3, ... ist p-konvergent. (mit dem p-Grenzwert 0). Ist q eine Primzahl $\neq p$, so ist die Folge q, q^2, q^3, ... nicht p-konvergent.
Beispiele: Die Folge p, p^2, p^3, ... ist nicht konvergent. Die Folge $1, \frac{1}{10}, \frac{1}{10^2}, \frac{1}{10^3}, ...$ ist konvergent mit dem Grenzwert 0.	Die Folge $1, \frac{1}{10}, \frac{1}{10^2}, \frac{1}{10^3}, ...$ ist nicht p-konvergent wegen $\left\lvert\frac{1}{10^n}\right\rvert_2 = \left(\frac{1}{2}\right)^{-n} = 2^n$, $\left\lvert\frac{1}{10^n}\right\rvert_5 = \left(\frac{1}{5}\right)^{-n} = 5^n$, $\left\lvert\frac{1}{10^n}\right\rvert_p = \left(\frac{1}{p}\right)^{0} = 1$, (für $p \neq 2{,}5$)
Für eine konvergente Zahlenfolge r_1, r_2, r_3 ... gilt $\lim_{n,m\to\infty} \lvert r_n - r_m\rvert = 0$ (Beweis als Übungsaufgabe.) Die Umkehrung ist im allgemeinen falsch. Beispiel. Ist a_i die größte ganze Zahl mit $a_i^2 < 2^{2i+1}$, so gilt für die Folge $\{r_i = 2^{-i}a_i\}$ $\lim_{n,m\to\infty} \lvert r_n - r_m\rvert = 0$ (Übungsaufgabe). Die Folge $\{r_i\}$ hat jedoch keinen Grenzwert, da das Quadrat des Grenzwertes gleich 2 sein müsste. Eine solche Zahl gibt es jedoch nicht unter den rationalen Zahlen.	Für eine p-konvergente Zahlenfolge $\{r_i\}$ gilt $\lim_{n,m\to\infty} \lvert r_n - r_m\rvert_p = 0$ (Beweis als Übungsaufgabe). Die Umkehrung ist im allgemeinen falsch. Beispiel. $p = 7$. Die Zahl 2 ist quadratischer Rest modulo 7. Sei $a_0^2 \equiv 2(7)$. Man kann der Reihe nach ganze Zahlen $a_1, a_2, a_3, ...$ (mit $0 \leq a_i \leq 6$) bestimmen, so dass $e_7((a_0 + a_1 \cdot 7 + a_2 \cdot z^2 + ... + a_i \cdot 7^i)^2 - 2) \geq i + 1$ Für die Folge $\{r_i = a_0 + a_1 \cdot 7 + a_2 \cdot 7^2 + ... + a_i \cdot 7^i\}$ gilt $\lim_{n,m\to\infty} \lvert r_n - r_m\rvert_7 = 0$ (Übungsaufgabe). Die Folge hat jedoch keinen Grenzwert, da das Quadrat des Grenzwertes 2 sein müsste. Eine solche rationale Zahl gibt es jedoch nicht.
Eine Zahlenfolge $\{r_i\}$ mit der Eigenschaft $\lim_{n,m\to\infty} \lvert r_n - r_m\rvert = 0$ heißt Fundamentalfolge.	Eine Zahlenfolge $\{r_i\}$ mit der Eigenschaft $\lim_{n,m\to\infty} \lvert r_n - r_m\rvert_p = 0$ heißt Fundamentalfolge.

Nicht jede Fundamentalfolge (bzw. p-Fundamentalfolge) ist also konvergent, wie die obigen Beispiele zeigen.

p-adische Zahlen	**Reelle Zahlen**
p-Betrag $\|\alpha\|_p = \left(\frac{1}{p}\right)^{e_p(\alpha)}$	Absoluter Betrag $\|\gamma\| = \max(\gamma, -\gamma)$
α ist für-p-kleiner als α', falls $\|\alpha\|_p < \|\alpha'\|_p$. Ist α für-p-kleiner als α', so ist für jede natürliche Zahl n auch $n\alpha$ für-p-kleiner als α'.	γ ist absolut kleiner als γ', falls $\|\gamma\| < \|\gamma'\|$. Zu beliebigen reellen Zahlen γ, γ' gibt es stets eine natürliche Zahl n, so dass $n\gamma$ absolut größer als γ' ist.
Eine p-adische Zahl α heißt Grenzwert einer Folge $\alpha_1, \alpha_2, \alpha_3$, ... p-adischer Zahlen, falls $\lim_{n\to\infty} \|\alpha - \alpha_n\|_p = 0$ Eine Zahlenfolge, die einen Grenzwert besitzt, heißt konvergent.	Eine reelle Zahl γ heißt Grenzwert einer Folge $\gamma_1, \gamma_2, \gamma_3$, ... reeller Zahlen, falls $\lim_{n\to\infty} \|\gamma - \gamma_n\| = 0$ Eine Zahlenfolge, die einen Grenzwert besitzt, heißt konvergent.
Beispiele: Die Folge p, p^2, p^3, ... ist konvergent (mit dem Grenzwert 0). Ist q eine Primzahl $\neq p$, so ist die Folge q, q^2, q^3 ... nicht konvergent. Die Folge $1, \frac{1}{10}, \frac{1}{10^2}, \frac{1}{10^3}, \ldots$ ist nicht konvergent.	Beispiele: Die Folge p, p^2, p^3, ... ist nicht konvergent. Die Folge $1, \frac{1}{10}, \frac{1}{10^2}, \frac{1}{10^3}, \ldots$ ist konvergent mit dem Grenzwert 0.
Für eine konvergente Zahlenfolge $\{\alpha_i\}$ gilt $\lim_{n,m\to\infty} \|\alpha_n - \alpha_m\|_p = 0$ Die Umkehrung ist richtig. (Ohne Beweis.) Eine Zahlenfolge $\{\alpha_i\}$ mit der Eigenschaft $\lim_{n,m\to\infty} \|\alpha_n - \alpha_m\|_p = 0$ heißt Fundamentalfolge.	Für eine konvergente Zahlenfolge $\gamma_1, \gamma_2, \gamma_3$, ... gilt $\lim_{n,m\to\infty} \|\gamma_n - \gamma_m\| = 0$ Die Umkehrung ist richtig. (Ohne Beweis.) Eine Zahlenfolge $\{\gamma_i\}$ mit der Eigenschaft $\lim_{n,m\to\infty} \|\gamma_n - \gamma_m\| = 0$ heißt Fundamentalfolge.

Jede Fundamentalfolge ist konvergent. (Ohne Beweis).
Also: Fundamentalfolgen und nur sie sind konvergente Folgen.

Speziell: Jede p-Fundamentalfolge rationaler Zahlen besitzt einen Grenzwert, der eine p-adische Zahl ist.
Ferner gilt:
Jede p-adische Zahl ist p-Grenzwert einer Folge rationaler Zahlen.
Es gibt natürliche Zahlen a_i mit $0 \leq a_i \leq p-1$, so dass

$$\alpha = p - \lim_{n\to\infty} \sum_{i=m}^{n} a_i p^i$$

ist $(e_p(\alpha) = m)$, d. h.

$$\alpha = \sum_{i=m}^{\infty} a_i p^i \qquad (*)$$

$$\alpha = a_m p^m + a_{m+1} p^{m+1} + \ldots$$

Ziffernschreibweise:

$$\alpha = a_m a_{m+1} \ldots a_{-1} a_0, a_1 a_2 \ldots (p)$$

Speziell: Jede Fundamentalfolge rationaler Zahlen besitzt einen Grenzwert, der eine reelle Zahl ist.
Ferner gilt:
Jede reelle Zahl γ ist Grenzwert einer Folge rationaler Zahlen.
Es gibt natürliche Zahlen $0 \leq a_i \leq 9$, so dass

$$\gamma = \lim_{n\to\infty} \sum_{i=m}^{n} a_i \left(\frac{1}{10}\right)^i$$

ist, d. h.

$$\gamma = \sum_{i=m}^{\infty} a_i \left(\frac{1}{10}\right)^i \qquad (**)$$

$$\gamma = a_m \cdot 10^{-m} + a_{m+1} \cdot 10^{-m+1} + \ldots$$

Ziffernschreibweise:

$$\gamma = a_m a_{m+1} \ldots a_{-1} a_0, a_1 a_2 \ldots$$

Beispiel: $p = 5$:

$$4 \cdot \frac{1}{5^2} + 3 \cdot \frac{1}{5} + 2 + 3 \cdot 5 + 5^2 + ... = 432{,}31...(5)$$

α ist rational genau dann, wenn die Folge $a_m, a_{m+1}, ...$ von einer Stelle an periodisch wird. Die Entwicklung (*) heißt dann p-adische Entwicklung der rationalen Zahl α.

Alle rationalen Zahlen der Form $\frac{a}{p^n}$ (mit ganzen Zahlen $a \geq 0$ und n) und nur sie besitzen endliche p-adische Entwicklungen.

Der einfachste Weg zur Umwandlung einer (etwa für-p- ganzen positiven) rationalen Zahl $r = m/n$ in ihre p-adische Entwicklung ist, die endlichen p-adischen Entwicklungen von m und n zu dividieren.

Beispiel. $p = 7$, $r = \frac{1}{12} = \frac{1}{5+1\cdot 7}$
$1 : 5{,}1 = 3{,}6262...(7)$

Rechenoperationen (Beispiele)

Addition: $p = 7$

	2	5	6,	3	3	4	4	(7)
	1	5	0,	1	5	6	6	(7)
	3	10	6,	4	8	10	10	
=	3	3	0,	5	1	4	4	(7)

(Von links nach rechts addieren und reduzieren)

Subtraktion: $p = 7$

	0	7	6	6	6	6	6	6	...
	2	5	6,	3	3	4	4		
-	1	5	0,	1	5	6	6		
	1	7	12,	8	4	4	6	6	...
=	1	0	6,	2	5	4	4	6	...(7)

Multiplikation: $p = 7$

	2	5	6,	3	·	1,	5	(7)
	2	10						
		5	25					
			6	30				
				3	15			
	2	15	31,	33	15			
=	2	1	5,	2	6	2	(7)	

Beispiel:

$$4 \cdot 10^2 + 3 \cdot 10 + 2 + 3 \cdot \frac{1}{10} + 1 \cdot \frac{1}{10^2} + ... = 432{,}31...$$

γ ist rational genau dann, wenn die Folge $\{a_i\}$ von einer Stelle an periodisch wird. Die Entwicklung (**) heißt dann Dezimalbruchentwicklung der rationalen Zahl γ.

Alle rationalen Zahlen der Form $a \cdot 10^k$ (mit ganzen Zahlen a und k) und nur sie besitzen endliche Dezimalbruchentwicklungen.

Für rationale Zahlen mit Nennern der Form $2^i 5^j$ hat man die Darstellung durch einen endlichen oder durch einen unendlichen Dezimalbruch.
Beispiele.
$2 \cdot 10^{-1} = \frac{1}{5} = 0{,}2 = 0{,}1999...$
$4 \cdot 10^{-2} = 0{,}04 = 0{,}0399...$

Der einfachste Weg zur Umwandlung einer (etwa positiven) rationalen Zahl $r = m/n$ in einen Dezimalbruch ist, die Division $m : n$ durchzuführen.

Beispiel. $r = \frac{7}{6}, 7 : 6 = 1{,}166...$

Addition:

2	5	6,	3	3	4	4	
1	5	0,	1	5	6	6	
3	10	6,	4	8	10	10	

$= 406{,}4910$
(Von links nach rechts addieren und reduzieren)

Subtraktion:

256,3344
-150,1566
-106,1778

Multiplikation:

256,3 · 1,5
12815
2563
384,45

Sei α eine p-adische Zahl. Die Gleichung

$$x^2 - \alpha = 0$$

ist in p-adischen Zahlen lösbar, wenn $\alpha = p^k \varepsilon$ (ε Einheit) mit $k \equiv 0(2)$ und

$$\begin{cases} \varepsilon \equiv 1(8) & \text{für } p = 2 \\ \left(\frac{\varepsilon}{p}\right) = 1 & \text{für } p \neq 2 \end{cases}$$

Sei γ eine reelle Zahl. Die Gleichung

$$x^2 - \gamma = 0$$

ist in reellen Zahlen lösbar, wenn $\gamma \geq 0$.

Beweis. Sätze 19 und 25

Sei r eine rationale Zahl. Die Gleichung

$$x^2 - r = 0$$

ist in rationalen Zahlen lösbar genau dann, wenn die Gleichung $x^2 - r = 0$ in reellen Zahlen und für jede Primzahl p in p-adischen Zahlen lösbar ist.[63]

Setzt man für rationale Zahlen r entweder $b(r) = |r|$ oder $b(r) = |r|_p$, so gilt:

a) Es ist stets $b(r) \geq 0$, und $b(r) = 0$ nur für $r = 0$;
b) $b(rr') = b(r)b(r')$;
c) $b(r + r') \leq b(r) + b(r')$.

Eine Funktion b mit rationalen Argumenten und reellen Werten mit diesen Eigenschaften a), b), c) heiße Betragsfunktion, kürzer Betrag. Zwei Beträge b, b' mögen äquivalent heißen, wenn stets $b(r) < b(r')$ gleichbedeutend mit $b'(r) < b'(r')$ ist.
Man kann beweisen, dass jeder Betrag entweder äquivalent zum absoluten Betrag ist oder dass es eine Primzahl p gibt, so dass er äquivalent zum p-Betrag ist.
Bis auf Äquivalenz gibt es also in der Menge der rationalen Zahlen an Beträgen nur den absoluten Betrag und für jede Primzahl p den p-Betrag.

Ein Betrag b gestattet die Definition des Grenzwertes einer Folge rationaler Zahlen und damit die Definitionen von Konvergenz und Fundamentalfolgen.
Eine Folge rationaler Zahlen $r_1, r_2, r_3, \ldots$ besitzt (nach Definition) den b-Grenzwert r, falls die Folge $\{b(r_i - r)\}$ eine Nullfolge reeller Zahlen ist. Je nachdem, welchen Betrag man zugrundelegt, erhält man einen anderen Grenzwert und Konvergenzbegriff (eine Folge heiße b-konvergent, wenn sie einen b-Grenzwert besitzt).
Für äquivalente Beträge b und b' gilt: Eine Folge ist b-konvergent dann und nur dann, wenn sie b'-konvergent ist.

Da es in der Menge der rationalen Zahlen an Beträgen nur den absoluten Betrag und den

[63] Beweis. Ist die Gleichung $x^2 - r = 0$ in rationalen Zahlen lösbar, so selbstverständlich auch in reellen und für jede Primzahl p in p-adischen Zahlen. Sei diese Gleichung nun umgekehrt in reellen Zahlen und für jede Primzahl p in p-adischen Zahlen lösbar.

Da sie in reellen Zahlen lösbar sein soll, muss $r > 0$ sein. Sei

$$r = \prod_p p^{e_p(r)}$$

die Primzerlegung von r. Da die Gleichung in p-adischen Zahlen lösbar sein soll, ist r Quadrat einer p-adischen Zahl und daher $e_p(r) \equiv 0(2)$; dies gilt für alle Primzahlen p. Daher ist r Quadrat einer rationalen Zahl, d.h., die Gleichung ist in rationalen Zahlen lösbar.

p-Betrag (für jede Primzahl p) gibt, gibt es auch nur die oben beschriebenen Begriffe der Konvergenz und der p-Konvergenz. Die angegebenen Beispiele zeigen:
Konvergente Folgen brauchen nicht p-konvergent zu sein; p-konvergente Folgen brauchen nicht konvergent zu sein; p-konvergente Folgen brauchen nicht q-konvergent zu sein (falls p und q verschiedene Primzahlen sind).

Eine (p-)konvergente Folge rationaler Zahlen ist stets eine (p-)Fundamentalfolge.

(I) Eine (p-)Fundamentalfolge rationaler Zahlen braucht keinen (rationalen) (p-)Grenzwert zu besitzen.

(II) Nimmt man den p-Betrag, so besitzt jede p-Fundamentalfolge rationaler Zahlen einen Grenzwert, der eine p-adische Zahl ist.
Nimmt man den absoluten Betrag, so besitzt jede Fundamentalfolge rationaler Zahlen einen Grenzwert, der eine reelle Zahl ist.

(III) Jede p-adische Zahl ist Grenzwert mindestens einer p-Fundamentalfolge rationaler Zahlen. Jede reelle Zahl ist Grenzwert mindestens einer Fundamentalfolge rationaler Zahlen.

Wegen der Eigenschaften I, II, III heißen die Mengen der p-adischen Zahlen und der reellen Zahlen Vervollständigungen der Menge der rationalen Zahlen. Andere Vervollständigungen gibt es nicht (da es keine weiteren Beträge - also keine anderen Konvergenzbegriffe - in der Menge der rationalen Zahlen gibt, außer dem absoluten Betrag und für jede Primzahl p dem p-Betrag).

Die Menge der rationalen Zahlen besitzt unendlich viele Vervollständigungen:
1. die Menge der reellen Zahlen;
2. die Menge der p-adischen Zahlen (für jede der unendlich vielen Primzahlen).

In diesem Sinne sind die p-adischen Zahlen (für irgendeine Primzahl p) gleichberechtigt mit den reellen Zahlen. Diese Gleichberechtigung kommt auch in dem folgenden, oben bewiesenen Satz zum Ausdruck.

Satz 26. Die Gleichung $x^2 - r = 0$ (mit einer rationalen Zahl r) sei in reellen Zahlen und für jede Primzahl p in p-adischen Zahlen lösbar. Dann ist r Quadrat einer rationalen Zahl.

Ist die Gleichung also in allen Vervollständigungen der Menge der rationalen Zahlen lösbar, so ist sie bereits in rationalen Zahlen lösbar.

Genau so kommt die Gleichberechtigung der p-adischen Zahlen mit den reellen Zahlen auch in dem folgenden berühmten und schönen zahlentheoretischen Ergebnis (Satz von Legendre-Minkowski-Hasse über sogenannte ternäre quadratische Formen) zum Ausdruck, das wir ohne Beweis angeben. Es geht um die Lösung der Gleichung

$$ax^2 + bx + c = 0 \tag{49}$$

(a, b, c ganze Zahlen) in ganzen Zahlen. Offenbar ist diese Gleichung in ganzen Zahlen lösbar, wenn sie in rationalen Zahlen lösbar ist (mit dem Hauptnenner multiplizieren!). Es gilt
]1.5ex] Satz 27 (Minkowski-Hasse). Die Gleichung (49) ist in rationalen Zahlen lösbar genau dann, wenn sie in reellen Zahlen und in p-adischen Zahlen (für alle Primzahlen p) lösbar ist.
Damit die Gleichung in reellen Zahlen lösbar ist, dürfen a, b, c nicht alle dasselbe Vorzeichen haben.

Es gibt Kriterien dafür, wann (49) in p-adischen Zahlen lösbar ist. Benutzt man diese, so erhält

man den folgenden älteren

Satz 28 (Legendre). Die Gleichung (49), worin a, b, c paarweise teilerfremd, $\neq 0$ und quadratfrei sind, hat Lösungen in ganzen Zahlen x, y, z genau dann, wenn a, b, c nicht alle dasselbe Vorzeichen haben und $-bc$, $-ac$, $-ab$ bzw. quadratische Reste von a, b, c bzw. sind, d.h. die Kongruenzen

$$x^2 \equiv -bc(\mod a), \qquad x^2 \equiv -ca(\mod b), \qquad x^2 \equiv -ab(\mod c)$$

lösbar sind.

Beispiel. $2x^2 + 3y^2 - 5z^2 = 0$ ist in ganzen Zahlen lösbar.

Die Beweise findet man in den Büchern von Borewicz-Safarevic, Koch-Pieper und Serr (1970), die man studieren kann, sofern man die nötigen Grundkenntnisse aus der Algebra, Zahlentheorie und Analysis hat (vgl. das Literaturverzeichnis).

Hat eine Gleichung mit ganzen Koeffizienten eine Lösung in ganzen Zahlen (bzw. rationalen Zahlen), so erst recht in reellen und p-adischen Zahlen (für alle p). Die Umkehrung ist im Fall der Gleichung (49) ebenfalls richtig, muss aber nicht immer gelten. Den folgenden Satz geben wir ohne Beweis an.

Satz 29 (Reichardt[64]). Die Gleichung $x^4 - 17 = 2y^2$ ist in reellen Zahlen und in p-adischen Zahlen (für alle Primzahlen p) lösbar, besitzt jedoch keine Lösungen in rationalen Zahlen.

4 Literaturverzeichnis

I. Bücher, in denen auch die Theorie der p-adischen Zahlen behandelt wird

*BOREWICZ, S. J., und I. R. Safarevic, Zahlentheorie. Birkhäuser-Verlag, Basel und Stuttgart 1966 (Übersetzung aus dem Russischen).

DYNKIN, E.B., und W.A.Uspenski, Mathematische Unterhaltungen II (Aufgaben aus der Zahlentheorie). 4. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1968. (Übersetzung aus dem Russischen.)

*HASSE, H., Zahlentheorie. 2. Aufl., Akademie-Verlag, Berlin 1963.

*HENSEL, K., Zahlentheorie. Göschen'sche Verlagshandlung, Berlin- Leipzig 1913.

*KOCH, H., und H. Pieper, Methoden und Ergebnisse der Zahlentheorie. (In Vorbereitung beim VEB Deutscher Verlag der Wissenschaften, Berlin.)

*REDEI, L., Algebra I. Akad. Verlagsges., Leipzig 1959 (Übersetzung aus dem Ungarischen).

*SERRE, J.-P., Cours d'Arithmetique. Presses Univ. de France, Paris 1970.

*SERRE, J.-P., Corps locaux. Hermann, Paris 1968.

*VAN DER WAERDEN, B.L., Algebra I. Springer-Verlag, Berlin-Heidelberg-New York 1966.

[64] H. Reichardt, geb. 1908, em. Mathematik-Professor an der Humboldt-Universität zu Berlin und der Akademie der Wissenschaften der DDR; Nationalpreisträger. Den zitierten Satz entdeckte er 1942.

II. Auswahl von Büchern, die auch der Zahlentheorie gewidmet sind

*BUCHSTAB, A. A., Zahlentheorie. Ucpedgiz, Moskau 1960 (russ.).

CHINTSCHIN, A. J., Die Elemente der Zahlentheorie. In: Enzyklopädie der Elementarmathematik I, 7. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1974 (Übersetzung aus dem Russischen).

GELFOND, A. O., Die Auflösung von Gleichungen in ganzen Zahlen. 5. Aufl., VEB Deutscher Verlag der Wissenschaften, Berlin 1973 (Übersetzung aus dem Russischen).

*HASSE, H., Vorlesungen über Zahlentheorie. Springer-Verlag, Berlin- Göttingen-Heidelberg 1950 (2. Aufl. 1964).

*HOLZER, L., Zahlentheorie I. B. G. Teubner, Leipzig 1958.

KALOUJNINE, L. A., Primzahlzerlegung. VEB Deutscher Verlag der Wissenschaften, Berlin 1971 (Übersetzung aus dem Russischen).

LEHMANN, E., Übungen für Junge Mathematiker I (Zahlentheorie). 2 Aufl., BSB B. G. Teubner, Leipzig 1970.

MORDELL, L. J., Two Papers on Number Theory. VEB Deutscher Verlag der Wissenschaften, Berlin 1972.

*SIERPINSKI, W., Elementary Theory of Numbers. PWN, Warszawa 1964 (Übersetzung aus dem Polnischen).

SIERPINSKI, W., 250 Problems in Elementary Number Theory. American Elsevier Publ. Comp., New York/PWN, Warszawa 1970.

*WINOGRADOW, I. M., Elemente der Zahlentheorie. VEB Deutscher Verlag der Wissenschaften, Berlin/R. Oldenbourg, München 1955 (Übersetzung aus dem Russischen).

WOROBJOW, N.N., Die Fibonaccischen Zahlen. 2. Aufl, VEB Deutscher Verlag der Wissenschaften, Berlin 1971 (Übersetzung aus dem Russischen).

WOROBJOW, N.N., Teilbarkeitskriterien. VEB Deutscher Verlag der Wissenschaften, Berlin 1972 (Übersetzung aus dem Russischen).

(Die mit * gekennzeichneten Titel gehen über das mathematische Wissen, das beim Leser dieser Broschüre vorausgesetzt wird, weit hinaus.)