Eberhard Lehmann

Übungen für Junge Mathematiker 1
Zahlentheorie

1970 BSB B. G. Teubner Verlagsgesellschaft
MSB: Nr. 36
Abschrift und LaTex-Satz: 2022 https://mathematikalpha.de

Zur Herausgabe der Übungen für Junge Mathematiker

In den letzten Jahren hat die Mathematik nicht zuletzt durch die Olympiaden Junger Mathematiker in breitesten Kreisen in zunehmendem Maße an Wertschätzung gewonnen. Durch die Teilnahme an Arbeitsgemeinschaften und Zirkeln, durch die Beschäftigung mit in verschiedenen Publikationsorganen veröffentlichten Aufgaben dringen die Interessenten in mathematische Gebiete ein, die noch vor wenigen Jahren fast ausschließlich der Hochschule vorbehalten waren.

Die intensive Beschäftigung mit den z.B. bei den Olympiaden Junger Mathematiker gestellten Aufgaben und mit mathematischen Problemen erleichtert dem Schüler den Übergang von der Oberschule zur Hochschule.
In Zirkeln und Interessengemeinschaften, aber auch in speziellen Trainingslagern zur Vorbereitung auf die Olympiaden werden Einführungen in verschiedene Gebiete der Mathematik gegeben, für die es noch an geeigneter Literatur mangelt, in der von den in der Schule gewonnenen Kenntnissen ausgehend Ergänzungen und Erweiterungen vorgenommen werden, die den Anschluss an den Stoff der Hochschule gewährleisten.
Dies kann nicht ohne theoretische Betrachtungen, also nicht nur durch das Lösen von Übungsaufgaben geschehen.

Zu wirklichen Erfolgen in der Zirkelarbeit und auch bei der individuellen Beschäftigung mit mathematischen Problemen wird man nur dann kommen, wenn man bestimmte Gebiete systematisch behandelt und die dazu erforderliche Theorie sinnvoll mit der Lösung einer Reihe von Aufgaben verbindet.

Die Übungen für Junge Mathematiker sollen einerseits helfen, den Anschluss vom Schulstoff zum Stoff der Hochschule zu gewinnen, andererseits den Zirkelleitern Anregungen vermitteln und darüber hinaus den Schülern und natürlich auch Erwachsenen, die keine Möglichkeit haben, an Interessengemeinschaften teilzunehmen, das Eindringen zunächst in die Gebiete Zahlentheorie, Elementargeometrie und Ungleichungen zu ermöglichen.

Die Einführung mit Hilfe von Aufgaben ist vielleicht ungewohnt, versetzt aber selbst den weniger geübten Leser in die Lage, relativ rasch vorwärts zu schreiten.

Herausgeber und Autoren hoffen, dass mit dieser Aufgabensammlung eine vorhandene Lücke geschlossen wird, sind sich aber auch bewusst, dass bei dieser Form der Kenntnisvermittlung Vollständigkeit nicht erreicht werden konnte und zugunsten der bei den Olympiaden Junger Mathematiker behandelten Probleme auch nicht erreicht werden sollte.
Die Aufgaben selbst erheben nicht in jedem Falle Anspruch auf Originalität, sondern entstammen zum Teil weniger bekannter Literatur. Ihre Auswahl und Zusammenstellung erfolgte unter methodischen und didaktischen Gesichtspunkten von den Autoren des jeweiligen Teiles der zunächst auf 3 Bände veranschlagten Aufgabensammlung.

Für die große Unterstützung bei der Herausgabe und für manchen Hinweis, der zur qualitativen Verbesserung der Manuskripte führte, gilt besonderer Dank den Herren Prof. Dr. W. Engel, Rostock, Dr. E. Hameister, Magdeburg, und W. Arnold, Leipzig, und nicht zuletzt dem BSB B.G. Teubner Verlagsgesellschaft, Leipzig, für das entgegenkommende Eingehen auf das geplante Vorhaben und seine zügige Verwirklichung.

Mögen die Übungen für Junge Mathematiker dazu beitragen, bei dem einen Leserkreis vorhandene Kenntnisse zu festigen und zu vertiefen und einen anderen Teil von: Lesern durch die Freude an erhaltenen richtigen Lösungen zu immer weiterem systematischem Eindringen in sie interessierende Teilgebiete der Mathematik anregen.

Leipzig, Herbst 1967 — Gerhard Kleinfeld

Vorwort

Bereits nach kurzer Zeit der Beschäftigung mit Kongruenzen stellt man fest, welche Vorteile sich bei der Anwendung zahlentheoretischer Verfahren bieten. Deshalb fehlten bisher wohl in keiner Stufe der Olympiaden Junger Mathematiker Aufgaben, die man mit Hilfe von Kongruenzen elegant zu lösen vermag.

Das vorliegende Buch bildet eine Einführung, die für Schüler, Studenten und berufstätige Erwachsene gleichermaßen von Interesse ist.
Werden die in der Einleitung (1.) zusammengestellten Voraussetzungen erfüllt, so dürfte jeder Leser unabhängig sowohl vom Alter als auch davon, ob er das Büchlein im Kollektiv oder im "Alleingang" durcharbeiten will, auf keine größeren Schwierigkeiten mehr stoßen.

Die richtigen Lösungen der sich anschließenden Aufgaben, die sich auf diese Voraussetzungen beziehen, werden die nötige Sicherheit verleihen. Deshalb möge der Leser zunächst die Begriffe, Sätze und Aufgaben dieses ersten Abschnittes gründlich und systematisch durcharbeiten, bevor er mit der Lösung der Aufgaben der nächsten Abschnitte beginnt.
Bei allen Aufgaben sollte der Leser zuerst versuchen, die Probleme selbständig zu lösen und sich eigene Gedanken zur betreffenden Aufgabe machen, bevor er die angegebene Lösung durchsieht.
Mit einem • versehene Aufgaben sind als zusätzliche Übungsaufgaben gedacht, deren Lösungen im Anhang angegeben sind.

Im Abschnitt 5. wird auf logarithmische Tabellen eingegangen, und im Anhang befinden sich weitere Tabellen für Primzahlen kleiner als 100, die zur Lösung von Kongruenzen nützlich sein können.
Weiter sei darauf hingewiesen, dass in einigen Bemerkungen bestimmte Begriffe, wie z.B. Variationen, Ring, Körper usw. genannt werden, über die der Leser Näheres erfährt, wenn er die Literatur heranzieht, die in dazugehörenden Fußnoten angegeben ist und über den Rahmen dieser Aufgabensammlung hinaus tiefer in das Gebiet der Zahlentheorie führt.

Sowohl dort als auch bei den Literaturhinweisen am Ende des Buches wurde darauf geachtet, möglichst die Literatur zu nennen, die in Schülerbibliotheken im allgemeinen greifbar bzw. im Buchhandel zu erhalten ist.
Es ist mir ein besonderes Anliegen, außer den vom Herausgeber genannten Herren vor allem noch Herrn Dr. L. Michler und Herrn G. Kleinfeld sowie dem BSB B. G. Teubner Verlagsgesellschaft zu danken für manchen Ratschlag und die Unterstützung bei der Abfassung dieses Buches.

Rostock, Herbst 1967 Eberhard Lehmann

Vorwort zur zweiten Auflage

Da der 1. Teil der "Übungen für Junge Mathematiker" einen derartigen Anklang gefunden hat, machte sich, nachdem die 1. Auflage innerhalb eines Jahres vergriffen war, eine Nachauflage erforderlich, zumal auch die Teile 2 und 3 ausgeliefert worden sind.
Es war daher das Bestreben von Verlag und Herausgeber, möglichst kurzfristig die 2. Auflage des 1. Teiles fertigzustellen, damit alle drei Teile komplett greifbar sind. Bei der Nachauflage sind keine wesentlichen Änderungen vorgenommen worden, lediglich sind Druckfehler beseitigt, sowie Hinweise und Vorschläge, die sich aus der Arbeit mit dem Teil 1 in Schülerzirkeln ergeben haben, berücksichtigt worden.

Gedankt sei allen Kollegen, die durch manchen Hinweis zur Präzisierung verschiedener Aufgaben und Lösungen beigetragen haben, und nicht zuletzt dem BSB B.G. Teubner Verlagsgesellschaft für die zügige Bearbeitung der Nachauflage.

Leipzig, Rostock, Sommer 1969 Gerhard Kleinfeld, Eberhard Lehmann

Inhaltsverzeichnis

1 Einleitung

1.1 Voraussetzungen

Das Rechnen mit natürlichen Zahlen n ($n = 0, 1, 2, ...$).
Das Rechnen mit rationalen Zahlen.
Gesetze der Bruchrechnung.

Satz: Ein Produkt ist dann und nur dann gleich Null, wenn mindestens ein Faktor gleich Null ist.

Kommutativgesetze: $a + b = b + a$, $a \cdot b = b \cdot a$
Assoziativgesetze: $a + (b + c) = (a + b) + c$, $a \cdot (bc) = (ab) \cdot c$
Distributivgesetz: $a \cdot (b + c) = ab + ac$

Das Rechnen mit Gleichungen und Ungleichungen.
Speziell die Beziehungen:
$a > b$: a ist größer als b.
$a < b$: a ist kleiner als b, a steht in der geordneten Menge der natürlichen Zahlen vor b.
Aus $a < b$ und $b < c$ folgt $a < c$.
$a \neq b$: a ist von b verschieden.
$a \leq b$: a ist nicht größer als b.
$a \geq b$: a ist nicht kleiner als b.

Begriff der Potenz, Gesetze der Potenzrechnung.
Begriff des Logarithmus, Gesetze der Logarithmenrechnung.

Die Summe der ersten n natürlichen Zahlen

$$s_n = 1 + 2 + 3 + ... + n = \frac{n(1+n)}{2}$$

Die Verwendung des Summenzeichens. Beispiel:

$$\sum_{k=1}^{7} \frac{k}{k+1} = \frac{1}{2} + \frac{2}{3} + \frac{3}{4} + \frac{4}{5} + \frac{5}{6} + \frac{6}{7} + \frac{7}{8}$$

Die Verwendung des Produktzeichens. Beispiele:

$$\prod_{k=1}^{5} \frac{k}{k+1} = \frac{1}{2} \cdot \frac{2}{3} \cdot \frac{3}{4} \cdot \frac{4}{5} \cdot \frac{5}{6} = \frac{1}{6}$$

$$\prod_{k=1}^{n} k = 1 \cdot 2 \cdot 3 \cdot ... \cdot n = n! \qquad \text{gelesen: } n \text{ Fakultät}$$

Der Binomische Satz:

$$(a+b)^n = \sum_{k=0}^{n} \binom{n}{k} a^{n-k} b^k \qquad , \qquad \binom{n}{k} = \frac{n(n-1)(n-2) \cdot ... \cdot (n-k+1)}{1 \cdot 2 \cdot 3 \cdot ... \cdot k}$$

gelesen: n über k

1.2 Primzahlen

Eine Primzahl ist eine natürliche Zahl, die nur durch 1 und durch sich selbst teilbar ist. Die Zahl 1 ist keine Primzahl.

Die Primzahlen kleiner als N (N sei eine festgewählte natürliche Zahl) bestimmt man mit dem Siebverfahren des Erathostenes.[1] Man notiert alle natürlichen Zahlen bis zur Zahl N, unterstreicht die Zahl 2 als Primzahl und durchstreicht alle anderen durch 2 teilbaren Zahlen. Die erste nicht durchstrichene Zahl 3 unterstreicht man als Primzahl, die anderen durch 3 teilbaren Zahlen werden gestrichen. Die nächste nicht gestrichene Zahl 5 ist wiederum Primzahl. Alle anderen durch 5 teilbaren Zahlen werden gestrichen.

Man setzt das Verfahren fort bis zur größten Zahl $\leq \sqrt{N}$ und hat alle Primzahlen kleiner als N erhalten.

1.3 Schluss von k auf (k+1)

1. Es ist nachzuweisen, dass die vermutete Eigenschaft oder Gesetzmäßigkeit für eine bestimmte natürliche Zahl $n = n_0$ richtig ist.

2. Unter der Annahme, dass die Gesetzmäßigkeit für die natürliche Zahl $n = k$ gilt, ist zu beweisen, dass sie auch für die auf k folgende natürliche Zahl $(k + 1)$ gilt.
Ist dieser Beweis geführt, so ist die vermutete Gesetzmäßigkeit für alle natürlichen Zahlen $n > n_0$ richtig.

1.4 Kleinstes gemeinschaftliches Vielfaches

Das kleinste gemeinschaftliche Vielfache (kgV) zweier oder mehrerer natürlicher Zahlen n_k ist die kleinste natürliche Zahl m, in der die Zahlen n_k als Faktoren enthalten sind.

1.5 Größter gemeinsamer Teiler

Der größte gemeinsame Teiler (ggT) zweier oder mehrerer natürlicher Zahlen n_k ist die größte natürliche Zahl d, die in allen Zahlen n_k als Faktor enthalten ist.

1.6 Diophantische Gleichungen

Unter diophantischen[2] Gleichungen versteht man unbestimmte Gleichungen, die unter der Nebenbedingung zu lösen sind, dass nur ganzzahlige Lösungen gelten.[3]

1.7 Aufgaben zu den Abschnitten 1.2. bis 1.6.

(1) Man ermittle alle Primzahlen $p_k < 250$ mit Hilfe des Siebverfahrens von Erathostenes.

Lösung: (Darstellung nächste Seite)
Die Primzahlen im Bereich $1 < n < 250$ sind:

[1] Erathostenes, griechischer Mathematiker, 275-194 v. u. Z.
[2] Diophantos, griechischer Mathematiker, um 250 v.u.Z.
[3] Siehe: Kleine Enzyklopädie, Mathematik; 3. Aufl., S. 122 und 720, Leipzig 1968

2, 3, 5, 7, 11, 43, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 74, 73, 79, 83, 89, 97, 104, 103, 107, 109, 113, 127, 134, 137, 139, 149, 154, 157, 163, 167, 173, 179, 181, 191, 193, 197, 199, 211, 223, 227, 229, 233, 239, 241.

	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~~	~~78~~	**79**	~~80~~
~~81~~	~~82~~	**83**	~~84~~	~~85~~	~~86~~	~~87~~	~~88~~	**89**	~~90~~
~~91~~	~~92~~	~~93~~	~~94~~	~~95~~	~~96~~	**97**	~~98~~	~~99~~	~~100~~
101	~~102~~	**103**	~~104~~	~~105~~	~~106~~	**107**	~~108~~	**109**	~~110~~
~~111~~	~~112~~	**113**	~~114~~	~~115~~	~~116~~	~~117~~	~~118~~	~~119~~	~~120~~
~~121~~	~~122~~	~~123~~	~~124~~	~~125~~	~~126~~	**127**	~~128~~	~~129~~	~~130~~
131	~~132~~	~~133~~	~~134~~	~~135~~	~~136~~	**137**	~~138~~	**139**	~~140~~
~~141~~	~~142~~	~~143~~	~~144~~	~~145~~	~~146~~	~~147~~	~~148~~	**149**	~~150~~
151	~~152~~	~~153~~	~~154~~	~~155~~	~~156~~	**157**	~~158~~	~~159~~	~~160~~
~~161~~	~~162~~	**163**	~~164~~	~~165~~	~~166~~	**167**	~~168~~	~~169~~	~~170~~
~~171~~	~~172~~	**173**	~~174~~	~~175~~	~~176~~	~~177~~	~~178~~	**179**	~~180~~
181	~~182~~	~~183~~	~~184~~	~~185~~	~~186~~	~~187~~	~~188~~	~~189~~	~~190~~
191	~~192~~	**193**	~~194~~	~~195~~	~~196~~	**197**	~~198~~	**199**	~~200~~
~~201~~	~~202~~	~~203~~	~~204~~	~~205~~	~~206~~	~~207~~	~~208~~	~~209~~	~~210~~
211	~~212~~	~~213~~	~~214~~	~~215~~	~~216~~	~~217~~	~~218~~	~~219~~	~~220~~
~~221~~	~~222~~	**223**	~~224~~	~~225~~	~~226~~	**227**	~~228~~	**229**	~~230~~
~~231~~	~~232~~	**233**	~~234~~	~~235~~	~~236~~	~~237~~	~~238~~	**239**	~~240~~
241	~~242~~	~~243~~	~~244~~	~~245~~	~~246~~	~~247~~	~~248~~	~~249~~	~~250~~

(2) Man zeige, dass beim Siebverfahren nach Erathostenes nur die Zahlen kleiner oder gleich $\sqrt{N}$ untersucht zu werden brauchen, wenn alle Primzahlen kleiner als N gesucht sind.

Lösung:
Die erste Primzahl größer als $\sqrt{N}$ sei q. Annahme, alle ganzzahligen Vielfachen der Primzahlen kleiner als q seien bereits gestrichen.
Es treten bis zur Zahl N noch gewisse Vielfache von q auf, die wir mit $k \cdot q$ bezeichnen ($k = 1, 2, 3, ..., m$). Die Zahlen k sind aber kleiner als q, da q^2 schon größer als N ist und da Zahlen größer als N nicht mehr untersucht werden sollen. Folglich wurden die Vielfachen von q schon vor Betrachtung der Primzahl q gestrichen.

(3) Man stelle eine Formel für die Summe der ersten n Kubikzahlen auf ($n = 1, 2, 3, ...$) und beweise diese Formel durch den Schluss von k auf $(k + 1)$.

Lösung:
Wir betrachten zunächst die Summen der ersten n Kubikzahlen für $n = 1, 2, 3$ und 4.

$$s_1 = 1^3 = 1$$
$$s_2 = 1^3 + 2^3 = 9$$
$$s_3 = 1^3 + 2^3 + 3^3 = 36$$
$$s_4 = 1^3 + 2^3 + 3^3 + 4^3 = 100$$

Die Ergebnisse sind die Quadrate der Summen der natürlichen Zahlen für $n = 1, 2, 3$ und 4.

$$\begin{aligned} s_1 &= 1^3 = 1^2 \\ s_2 &= 1^3 + 2^3 = 3^2 \\ s_3 &= 1^3 + 2^3 + 3^3 = 6^2 \\ s_4 &= 1^3 + 2^3 + 3^3 + 4^3 = 10^2 \end{aligned}$$

Wir kommen zu der Vermutung, dass die Formel für die Summe der ersten n Kubikzahlen folgende Gestalt hat:

$$s_n = \sum_{k=1}^{n} = \left[\frac{n(1+n)}{2}\right]^2$$

Beweis:
1. Die Formel gilt für $n = 1$: $s_1 = \left(\frac{1+1}{2}\right)^2 = 1$.
2. Unter der Annahme, dass die Formel für die natürliche Zahl $n = k$ gilt $\left(s_k = \left[\frac{k(1+k)}{2}\right]^2\right)$, behaupten wir, dass sie auch für die auf k folgende natürliche Zahl $(k+1)$ gilt $\left(s_{k+1} = \left[\frac{(k+1)(k+2)}{2}\right]^2\right)$.

$$\begin{aligned} s_{k+1} = s_k + (k+1)^3 &= \left[\frac{k(k+1)}{2}\right]^2 + (k+1)^3 = (k+1)^2\left(\frac{k^2}{4} + k + 1 +\right) \\ &= \frac{1}{4}(k+1)^2(k^2+4k+4) = \frac{1}{4}(k+1)^2(k+2)^2 = \left[\frac{(k+1)(k+2)}{2}\right]^2 \qquad \text{q.e.d.} \end{aligned}$$

Für alle natürlichen Zahlen $n > 1$ gilt $\sum\limits_{k=1}^{n} k^3 = \left[\frac{n(1+n)}{2}\right]^2$.

(4) Man beweise durch den Schluss von k auf $(k+1)$ die Formel

$$\sum_{k=1}^{n} \frac{1}{k(k+1)(k+2)} = \frac{1}{1\cdot 2\cdot 3} + \frac{1}{2\cdot 3\cdot 4} + \ldots + \frac{1}{n(n+1)(n+2)} = \frac{n(n+3)}{4(n+1)(n+2)}$$

Lösung: Die Formel gilt für $n = 1$:

$$s_1 = \frac{1}{1\cdot 2\cdot 3} = \frac{1}{6} \qquad , \qquad s_1 = \frac{1(1+3)}{4(1+1)(1+2)} = \frac{1}{6}$$

Unter der Annahme, dass die Formel für die natürliche Zahl $n = k$ gilt $\left(s_k = \frac{k(k+3)}{4(k+1)(k+2)}\right)$ behaupten wir, dass sie auch für die auf k folgende $(k+1)$ richtig ist $\left(s_{k+1} = \frac{(k+1)(k+4)}{4(k+3)(k+3)}\right)$.
Beweis:

$$\begin{aligned} s_{k+1} = s_k + \frac{1}{(k+1)(k+2)(k+3)} &= \frac{k(k+3)}{4(k+1)(k+2)} + \frac{1}{(k+1)(k+2)(k+3)} \\ = \frac{k(k+3)^2+4}{4(k+1)(k+2)(k+3)} &= \frac{k^3+6k^2+9k+4}{4(k+1)(k+2)(k+3)} \end{aligned}$$

Da der Zähler des Bruches durch $(k+1)$ ohne Rest teilbar ist, erhält man:

$$s_{k+1} = \frac{(k^2+5k+4)(k+1)}{4(k+1)(k+2)(k+3)}$$

oder

$$s_{k+1} = \frac{(k^2+5k+4)}{4(k+2)(k+3)} = \frac{(k+1)(k+4)}{(k+2)(k+3)} \qquad \text{q.e.d.}$$

Die Formel $\sum_{k=1}^{n} \frac{1}{k(k+1)(k+2)} = \frac{n(n+3)}{4(n+1)(n+2)}$ gilt für alle natürlichen Zahlen $n \geq 1$.

Bemerkung: Anstelle der Division des Zählerpolynoms durch $(k+1)$ und anschließender Zerlegung in Faktoren hätte auch gleich die Identität der Ausdrücke $\frac{(k+1(k+4)}{4(k+2)(k+3)}$ und $\frac{k^3+6k^2+9k+4}{4(k+1)(k+2)(k+3)}$ nachgewiesen werden können.

(5) Wie groß ist die Anzahl aller zweistelligen natürlichen Zahlen z, die sich mit n voneinander verschiedenen Ziffern darstellen lassen $(n = 1, 2, 3, ..., 9)$?
a) In jeder Zahl z sind alle Ziffern voneinander verschieden.
b) In den Zahlen z sind Wiederholungen der gegebenen n Ziffern gestattet.

Lösung:
Die gegebenen voneinander verschiedenen Ziffern seien $n = 1, 2, 3, ...$ Die Anzahl der zweistelligen Zahlen z, die sich mit n voneinander verschiedenen Ziffern darstellen lassen, sei s_n.

a) Es treten in einer Zahl z nur voneinander verschiedene Ziffern auf.

n	1	2	3	4	5
z	-	12	12	12 31	12 24 41 53
		21	13	13 32	13 25 42 54
			21	14 34	14 31 43
			23	21 41	15 32 45
			31	23 42	21 34 51
			32	24 43	23 35 52
s_n	0	2	6	12	20

Behauptung:
Die Anzahl der Möglichkeiten ist $s_n = n(n-1)$.
Für spezielle Werte von n gilt die Behauptung, wie aus der Tabelle zu ersehen ist. Unter der Annahme, dass die Behauptung für $n = k$ richtig ist $(s_k = k(k-1))$, wird bewiesen, dass sie auch für die auf k folgende natürliche Zahl $(k+1)$ gilt $(s_{k+1} = k(k+1))$.

Zunächst gelten auch hier alle Möglichkeiten, die für k gelten. Hinzu kommen die Zahlen $1(k+1)$, $2(k+1)$,..., $k(k+1)$ und $(k+1)1$, $(k+1)2$, ..., $(k+1)k$. Das sind aber genau $2k$ Zahlen.

$$s_{k+1} = s_k + 2k = k(k-1) + 2k = k(k+1) \qquad \text{q.e.d.}$$

Für alle natürlichen Zahlen n gilt unter den gegebenen Voraussetzungen:

$$s_n = n(n-1)$$

b) Wiederholungen von Ziffern in einer Zahl z sind gestattet.

n	1	2	3	4
z	11	11 12	11 21 31	11 21 31 41
		21 22	12 22 32	12 22 32 42
			13 23 33	13 23 33 43
				14 24 34 44
s_n	1	4	9	16

Behauptung:
Die Anzahl der Möglichkeiten ist $s_n = n^2$.
Für spezielle Werte von n gilt die Behauptung, wie aus der Tabelle ersichtlich ist. Unter der Annahme, dass die Behauptung für $n = k$ richtig ist ($s_k = k^2$), ist nachzuweisen, dass sie auch für den nächstfolgenden Fall $n = k + 1$ gilt ($S_{k+1} = (k + 1)^2$).

Zunächst treten auch für $k+1$ wieder alle für k gegebenen Möglichkeiten auf, außerdem dann die folgenden Zahlen $1(k+1)$, $2(k+1)$, $3(k+1)$, ..., $k(k+1)$, $(k+1)(k+1)$ sowie $(k+1)1$, $(k+1)2$, $(k+1)3$, ..., $(k+1)k$.
Das sind genau $2k + 1$ hinzukommende Zahlen.

$$s_{k+1} = s_k + 2k + 1 = k^2 + 2k + 1 = (k + 1)^2 \qquad \text{q.e.d.}$$

Für alle natürlichen Zahlen n gilt unter den gegebenen Voraussetzungen:

$$s_n = n^2$$

Bemerkung: Es handelt sich in dieser Aufgabe im Fall a) um Variationen ohne Wiederholung von n Elementen zur Klasse 2. Allgemein gilt für die Anzahl der Variationen ohne Wiederholung von n Elementen zur m-ten Klasse mit $n > m$

$$V_n^m = n(n-1)(n-2) \cdot ... \cdot (n - [m-1])$$

Im Fall b) liegen Variationen von n Elementen zur Klasse m mit Wiederholung vor.[4] Allgemein gilt

$$\overline{V}_n^m = n^m$$

(6)• Gegeben sind n Geraden in der Ebene ε ($n = 1, 2, 3, ...$), von denen nicht 2 zueinander parallel verlaufen und von denen sich nicht mehr als 2 in einem Punkt schneiden.
In wieviel Teilebenen wird die Ebene ε durch die n Geraden zerlegt?
Man stelle eine Behauptung für die Anzahl der Teilebenen auf und beweise die Behauptung durch den Schluss von k auf $(k + 1)$.

(7)• Man stelle eine Formel für die Summe der ersten n Quadratzahlen auf ($n = 1, 2, 3, ...$) und beweise diese Formel durch den Schluss von k auf $(k + 1)$.

(8) Man zeige, dass $z = 891^n - 403^n$ für jede natürliche ungerade Zahl n durch 61 teilbar ist.

Lösung:
Der Beweis für die Teilbarkeit durch 61 wird durch den Schluss von k auf $(k + 1)$ geführt.
Für $n = 1$ gilt $z = 891 - 403 = 488 = 8 \cdot 61$.
Für ein spezielles $n = 1$ ist z durch 61 teilbar.

Behauptung:
$z = 891^n - 403^n$ ist für jede natürliche ungerade Zahl n durch 61 teilbar.
Unter der Voraussetzung, dass die Behauptung für $n = k$ gilt, wird nachgewiesen, dass die Teilbarkeit durch 61 auch für den auf k folgenden ungeraden Exponenten gilt.

Voraussetzung:
$z_k = 891^k - 403^k$ ist für $n = k$ (k ungerade) durch 61 teilbar.
Behauptung:

[4] Siehe auch Kleine Enzyklopädie, Mathematik, 3. Aufl., S. 646, Leipzig 1968

$z_{k+2} = 891^{k+2} - 403^{k+2}$ ist durch 61 teilbar.

Beweis:

$$\begin{aligned} z_{k+2} &= 891^2 \cdot 891^k - 403^2 \cdot 403^k + 891^2 \cdot 403^k - 891^2 \cdot 403^k \\ &= 891^2(891^k - 403^k) + 403^k(891^2 - 403^2) \\ &= 891^2(891^k - 403^k) + 403^k(891 + 403)(891 - 403) \end{aligned}$$

Für die erste Klammer $(891^k - 403^k)$ wurde die Teilbarkeit durch 61 für $n = k$ vorausgesetzt, für die letzte Klammer $(891 - 403)$ wurde die Teilbarkeit durch 61 oben gezeigt.
Damit ist z_{k+2} auch durch 61 teilbar und somit ist $z = 891^n - 403^n$ für jede natürliche ungerade Zahl n durch 61 teilbar.

Bemerkung: Die Lösung der Aufgabe ist auf andere Art einfacher möglich. Man vergleiche die Lösung der Aufgabe (67).

(9) Man zeige, dass $z = 14557^{1968} + 6230 \cdot 2059^{1968}$ durch 2077 teilbar ist.

Lösung:
Es gilt $2077 = 31 \cdot 67$. Also ist z genau dann durch 2077 teilbar, wenn z durch 31 und durch 67 teilbar ist.

a) Teilbarkeit durch 31.
Da $6231 = 201 \cdot 31$, also durch 31 teilbar ist, erscheint es zweckmäßig, statt $6230 \cdot 2059^{1968}$ den äquivalenten Ausdruck $6231 \cdot 2059^{1268} - 2059^{1968}$ zu benutzen.
Damit wird $z = 14557^{1968} + 6231 \cdot 2059^{1968} - 2059^{1968}$.
Der mittlere Term ist durch 31 teilbar, es braucht nur die Zahl $z' = 14557^{1968} - 2059^{1968}$ auf Teilbarkeit durch 31 untersucht zu werden.

Wir betrachten die Zahl $z_n = 14557^{2n} - 2059^{2n}$ und setzen zunächst $n = 1$.

$$z_1 = 14557^2 - 2059^2 = (14557 - 2059)(14557 + 2059) = 16616 \cdot 12498$$

$16616 = 536 \cdot 31$. z_1 ist durch 31 teilbar.
Unter der Annahme, dass z für $n = k$ durch 31 teilbar ist, wird gezeigt, dass z auch für die auf k folgende natürliche Zahl $(k + 1)$ durch 31 teilbar ist.

Voraussetzung:
$z_k = 14557^{2k} - 2059^{2k}$ ist durch 31 teilbar.
Behauptung:
$z_{k+1} = 14557^{2(k+1)} - 2059^{2(k+1)}$ ist durch 31 teilbar.

Beweis:

$$\begin{aligned} z_{k+1} &= 14557^2 \cdot 14557^{2k} - 2059^2 \cdot 2059^{2k} + 14557^2 \cdot 2059^{2k} - 14557^2 \cdot 2059^{2k} \\ &= 14557^2(14557^{2k} - 2059^{2k}) + 2059^{2k}(14557^2 - 2059^2) \end{aligned}$$

Die Teilbarkeit durch 31 wurde für die erste Klammer vorausgesetzt, für die zweite Klammer oben gezeigt. Es ist z_{k+1} durch 31 teilbar und damit ist z für jeden natürlichen geraden Exponenten $2n$ durch 31 teilbar.

b) Teilbarkeit durch 67. $6231 = 93 \cdot 67$.

$$z = 14557^{1968} + 6231 \cdot 2059^{1968} - 2059^{1968}$$

Der mittlere Term ist durch 67 teilbar, es braucht nur die Zahl $z' = 14557^{1968} - 2059^{1968}$ auf Teilbarkeit durch 67 untersucht zu werden.

$$z_n = 14557^{2n} - 2059^{2n}$$

Für $n = 1$ gilt:

$$z_1 = 14557^2 - 2059^2 = (14557 - 2059)(14557 + 2059) = 16616 \cdot 12498$$

$16616 = 248 \cdot 67$, folglich ist z_1 durch 67 teilbar.
Der im Fall a) durchgeführte Schluss gilt auch hier, und damit ist z für jeden natürlichen geraden Exponenten durch 67 teilbar. Da nun z durch 31 und durch 67 teilbar ist, so ist die Teilbarkeit durch $2077 = 31 \cdot 67$ für jeden natürlichen geraden Exponenten und speziell auch für den Exponenten $2n = 1968$ bewiesen.

Bemerkung: Die Lösung dieser Aufgabe ist später einfacher unter Verwendung sehr viel kleinerer Zahlen möglich. Man vergleiche die Lösung der Aufgabe (68).

10)• Man zeige, dass $z = 852^n - 1$ für jede natürliche Zahl $n > 0$ durch 23 teilbar ist.

(11)• Für welche Ziffer $x \neq 0$ ist $z = xxxxx^n + 59^n$ durch 671 teilbar, wenn n eine beliebige ungerade natürliche Zahl ist?

(12) Man bestimme das kleinste gemeinschaftliche Vielfache m der Zahlen
a) $n_1 = 413, n_2 = 767, n_3 = 1239$
b) $n_1 = 102, n_2 = 204, n_3 = 306, n_4 = 1224.$

Lösung:

a)
$$\begin{array}{rl} 413 = & 7 \cdot 59 \\ 767 = & 13 \cdot 59 \\ 1239 = & 3 \cdot 7 \cdot 59 \\ \hline \mathrm{m} = & 3 \cdot 7 \cdot 13 \cdot 59 = 16107 \end{array}$$

b)
$$\begin{array}{r} 102 = 2 \cdot 3 \cdot 17 \\ 204 = 2^2 \cdot 3 \cdot 17 \\ 306 = 2 \cdot 3^2 \cdot 17 \\ 1224 = 2^3 \cdot 3^2 \cdot 17 \\ \hline \mathrm{m} = 2^3 \cdot 3^2 \cdot 17 = 1224 \end{array}$$

(13) Man bestimme den größten gemeinsamen Teiler d der Zahlen $n_1 = 876$, $n_2 = 1898$, $n_3 = 584$, $n_4 = 2482$.

Lösung:

$$\begin{array}{rl} 876 & = 2^2 \cdot 3 \cdot 73 \\ 1898 & = 2 \cdot 13 \cdot 73 \\ 584 & = 2^3 \cdot 73 \\ 2482 & = 2 \cdot 17 \cdot 73 \\ \hline \mathrm{d} & = 2 \cdot 73 = 146 \end{array}$$

(14) Mit welcher Ziffer enden die Potenzen
a) 11^{100}, b) 12^{100}, c) 13^{100}, d) 14^{100}, e) 15^{100}, f) 16^{100}, g) 17^{100}, h) 18^{100}, i) 19^{100}?

Lösung:
a) $1^n = 1$, folglich endet 11^{100} mit der Ziffer 1.

b) 12^1 endet mit der Ziffer 2, 12^2 endet mit der Ziffer 4, 12^3 endet mit der Ziffer 8, 12^4 endet mit der Ziffer 6, 12^5 endet mit der Ziffer 2.

Allgemein endet 12^{4k+1} auf 2, 12^{4k+2} auf 4, 12^{4k+3} auf 8 und 12^{4k} auf 6, damit endet auch 12^{100} mit der Ziffer 6.

c) 13^1 endet mit der Ziffer 3, 13^2 endet mit der Ziffer 9, 13^3 endet mit der Ziffer 7,
13^4 endet mit der Ziffer 1, 13^5 endet mit der Ziffer 3,
Allgemein endet 13^{4k+1} auf 3, 13^{4k+2} auf 9, 13^{4k+3} auf 7 und 13^{4k} auf 1, damit endet auch 13^{100} mit der Ziffer 1.

d) 14^2 endet auf 6, 14^4 endet auf 6, damit endet 14^{2k}, speziell auch 14^{100} mit der Ziffer 6.
e) 5^k endet stets mit der Ziffer 5, also auch speziell 15^{100},
f) 6^k endet stets mit der Ziffer 6, also auch speziell 16^{100}.
g) 17^2 endet auf 9, 17^4 auf 1, damit endet auch 17^{100} mit der Ziffer 1.
h) 18^2 endet auf 4, 18^4 auf 6, damit endet auch 18^{4k} mit der Ziffer 6.
i) 19^2 endet mit der Ziffer 1, also auch 19^{2k} und damit speziell 19^{100}.

Bemerkung: Die Lösung dieser und ähnlicher Aufgaben ist später nach Einführung der Kongruenzen einfacher und übersichtlicher darstellbar.
Man vergleiche die Aufgaben (70) und (71).

(15)• Welchen Rest lässt die Potenz $z = 17^{1968}$ bei der Division durch 16?

(16)• Welchen Rest lässt die Potenz $z = 7^{129}$ bei der Division durch 50?

(17)• Welchen Rest lässt die Potenz $z = 13^{137}$ bei der Division durch 471?

(18) Gegeben sind drei verschiedene Sorten von Kugeln, 0,3-Gramm- Kugeln, 1,5-Gramm-Kugeln und 7-Gramm-Kugeln. 100 Kugeln sollen genau die Masse 100 Gramm besitzen. Wieviel Kugeln von jeder Sorte müssen genommen werden?

Lösung:

Die Anzahl der 0,3-Gramm-Kugeln sei x, die Anzahl der 1,5-Gramm-Kugeln sei y, die Anzahl der 7,0-Gramm-Kugeln sei z.
Es gelten die Beziehungen

$$0,3x + 1,5y + 7z = 100 \qquad , \qquad x + y + z = 100$$

sowie die Bedingung, dass x, y und z ganzzahlig sein sollen. Nach Multiplikation der Gleichungen mit 2 bzw. 3 folgt

$$0,6x + 3y + 14z = 200 \qquad , \qquad 3x + 3y + 3z = 300$$

und nach Subtraktion

$$2,4x - 11z = 100 \qquad , \qquad z = \frac{24x}{110} - \frac{100}{11} = \frac{12x - 500}{55}$$

Es gilt die Bedingung $41 < x < 100$, da z nicht negativ sein kann und kleiner als 100 sein muss. Ferner gilt, dass der Zähler $12x - 500$ durch 55 teilbar sein muss, da z ganzzahlig ist. Erst für $x = 60$ ist diese letzte Bedingung erfüllt.

$$12 \cdot 60 - 500 = 720 - 500 = 220 = 4 \cdot 55$$

Der nächste mögliche Wert für x wäre dann x= 115, er erfüllt. aber nicht mehr die obige Ungleichung $x < 100$.

Allgemein gilt:

$$\begin{aligned} x &= 60 + 55k \\ y &= \frac{12(60+55k)-500}{55} = \frac{220+12\cdot 55k}{55} = 4 + 12k \\ z &= 100 - 60 - 55k - 4 - 12k = 36 - 67k \end{aligned}$$

k kann für die gegebene Aufgabe nur den Wert 0 annehmen.
Es müssen genau 60 Kugeln zu je 0,3 Gramm, 36 Kugeln zu je 1,5 Gramm und 4 Kugeln zu je 7 Gramm genommen werden.

Probe:

$$60 \cdot 0,3 + 36 \cdot 1,5 + 4 \cdot 7 = 18 + 54 + 28 = 100$$

(19) Nach der Facharbeiterprüfung sollen an einer Schule 36 Lehrlinge mit je einem Buch ausgezeichnet werden. Es stehen 400,- M zur Verfügung, die restlos ausgegeben werden sollen. Es kommen drei Fachbücher für die Auszeichnung in Frage zum Preise von 9,50, 11,- und 13,75 M. Wieviel Bücher von jeder Sorte müssen gekauft werden?

Lösung:
Die Anzahl der Bücher zum Preise von 9,50, 11,- und 13,75 M seien x,y und z. Es gilt:

$$\begin{aligned} 9,50x + 11y + 13,75z &= 400 \\ x + y + z &= 36 \end{aligned} \quad \text{oder} \quad \begin{aligned} 9,50x + 11y + 13,75z &= 400 \\ 11x + 11y + 11z &= 396 \\ \hline -1,5x + 2,75z &= 4 \end{aligned}$$

$z = \frac{1,5x+4}{2,75} = \frac{6x+16}{11}$. $x = 1$ ist eine ganzzahlige Lösung der Gleichung.

Allgemein gilt: $x = 41 + 11k$; $z = 2 + 6k$; $y = 33 - 17k$.
Es soll die Lösungsmenge in einer Tabelle angegeben werden.

k	x	y	z	Probe I	Probe II
0	1	33	2	36	400
1	12	16	8	36	400
2	23	-1	Keine Lösung!		(y negativ!)

(20)• Man ermittle die ganzzahligen Lösungen der Gleichung $67x + 28y = 1500$.

(21)• Man ermittle die positiven, ganzzahligen Lösungen des Gleichungssystems

$$\begin{aligned} 72 + 11y + 13z &= 3000 \\ 32 + 7y + 17z &= 3000 \end{aligned}$$

(22)• Es sei n eine Zahl, die bei der Division durch 7 den Rest 1 liefert. Subtrahiert man von n den Rest sowie das bei der Division erhaltene "Siebtel", so erhält man die Zahl n_1.
Dividiert man n_1 durch 5, so bleibt wiederum der Rest 1. Subtrahiert man von n_1 den Rest 1 und das erhaltene "Fünftel", so ergibt sich die Zahl n_2. Dividiert man schließlich die Zahl n_2 durch 3, so bleibt wiederum ein Rest 1. Subtrahiert man diesen Rest 1 und das "Drittel" von n_2, so entsteht eine Zahl n_3, die bei Division durch 3 wiederum den Rest 1 liefert.
Welches ist die kleinste natürliche Zahl n, die den gegebenen Bedingungen genügt? Welche anderen natürlichen Zahlen n genügen den gegebenen Bedingungen?

2 Zahlenbereiche, Dirichletsches Schubfachprinzip

2.1 Zahlenbereiche

(23) Betrachtet werden a) die Menge der natürlichen Zahlen, b) die Menge der ganzen Zahlen und c) die Menge der rationalen Zahlen.
Es ist zu untersuchen, in welchen von diesen Mengen die 4 Grundrechenoperationen unbeschränkt ausführbar sind, d. h. in welchen, von diesen Mengen die Verknüpfung zweier Elemente mit Hilfe der 4 Grundrechenoperationen wieder ein Element aus der betreffenden Menge ergibt.

Lösung:
a) Addition und Multiplikation zweier Elemente aus der Menge der natürlichen Zahlen liefern stets wieder eine natürliche Zahl. Für die Umkehrungen der Addition und Multiplikation gilt das im allgemeinen nicht, zum Beispiel sind die Gleichungen $23 + x = 18$ und $9x = 7$ in der Menge der natürlichen Zahlen nicht lösbar.
Ergebnis: In der Menge der natürlichen Zahlen sind nur Addition und Multiplikation unbeschränkt ausführbar.

b) Addition, Subtraktion und Multiplikation zweier Elemente aus der Menge der ganzen Zahlen liefern stets wieder eine ganze Zahl. Für die Division gilt das im allgemeinen nicht, zum Beispiel ist die Gleichung $7x + 1 = 0$ in der Menge der ganzen Zahlen nicht lösbar.
Ergebnis: In der Menge der ganzen Zahlen sind Addition, Subtraktion und Multiplikation unbeschränkt ausführbar.

c) Addition, Subtraktion, Multiplikation und Division zweier Elemente aus der Menge der rationalen Zahlen ergeben stets wieder eine rationale Zahl (mit Ausnahme der Division durch Null!).
Ergebnis: In der Menge der rationalen Zahlen sind die 4 Grundrechenoperationen (bis auf die Division durch Null) unbeschränkt ausführbar.

Bemerkung: Eine Menge zusammen mit zwei in dieser Menge eindeutig erklärten Verknüpfungen - einer sogenannten Addition und einer sogenannten Multiplikation - die beliebigen Elementen a, b dieser Menge in dieser Reihenfolge ein eindeutig bestimmtes Element $a + b$ (die Summe von a und b) und ein eindeutig bestimmtes Element $a \cdot b$ (das Produkt von a und b) zuordnen, heißt ein "Ring", wenn für beliebige Elemente $a, b, c,...$ dieser Menge gilt!):

I. Assoziatives Gesetz für die Addition und Multiplikation:

$$a + (b + c) = (a + b) + c \qquad \text{und} \qquad a(bc) = (ab)c$$

II. Kommutatives Gesetz der Addition:

$$a + b = b + a$$

III. Unbeschränkte Ausführbarkeit der Subtraktion, d.h. zu zwei Elementen a und b gibt es stets ein x, so dass $a + x = b$ ist,

IV. Distributives Gesetz:

$$a(b + c) = ab + ac \qquad \text{und} \qquad (b + c)a = ba + ca$$

Ein Ring heißt ein "Körper", wenn er mindestens zwei Elemente enthält und $a \cdot b = b \cdot a$ für beliebige Elemente des Ringes gilt und wenn die Gleichung $ax = b$ für jedes $a \neq 0$ durch ein

zum Ring gehöriges Element x lösbar ist.[5]

Die Menge der ganzen Zahlen bildet einen Ring mit der üblichen Addition und Multiplikation ganzer Zahlen als Verknüpfung.
Die Menge der rationalen Zahlen bildet einen Körper mit der üblichen Addition und Multiplikation rationaler Zahlen als Verknüpfung.
Jeder Körper stellt auch einen Ring dar. Die Umkehrung gilt jedoch nicht.

(24) Es ist zu untersuchen, ob die Menge der Polynome Ring- oder Körpereigenschaften hat.

Lösung:
Es sei $f_1(x) = a_0x^n + a_1x^{n-1} + ... + a_kx^{n-k} + ... + a_{n-1}x + a_n$
und $f_2(x) = b_0x^m + b_1x^{m-1} + ... + b_kx^{m-k} + ... + b_{m-1}x + b_m$

Unter der Summe der gegebenen Polynome versteht man das Polynom $g(x)$, dessen Koeffizienten die Summen der entsprechenden Koeffizienten der gegebenen Polynome $f_1(x)$ und $f_2(x)$ sind.
Es sei $n = m + r$. Damit wird

$$g(x) = f_1(x)+f_2(x) = a_0x^n+...+(a_r+b_0)x^{n-r}+(a_{r-1}+b_1)x^{n-r-1}+...+(a_{n-1}+b_{m-1})x+a_n+b_m$$

Damit ist die Addition definiert und, wie man leicht erkennt, unbeschränkt ausführbar.

Unter der Differenz der gegebenen Polynome versteht man das Polynom $h(x)$, das zu $f_2(x)$ addiert, $f_1(x)$ ergibt.

$$h(x) = f_1(x) - f_2(x), \qquad \text{wenn} \qquad h(x) + f_2(x) = f_1(x)$$

Damit ist auch die Subtraktion definiert, sie liefert stets wieder ein Polynom und ist somit unbeschränkt ausführbar.

Gesucht ist das Produkt der Polynome $f_1(x)$ und $f_2(x)$.

$$\begin{aligned} f_1(x) \cdot f_2(x) &= (a_0x^n + ... + a_{n-1}x + a_n) \cdot (b_0x^m + ... + a_{m-1}x + a_m) \\ &= a_0b_0x^{n+m} + (a_0b_1 + a_1b_0)x^{n+m-1} + ... + (a_{n-2}b_m + b_{m-2}a_n + a_{n-1}b_{m-1})x^2 \\ &+ (a_{n-1}b_n + b_{m-1}a_n)x + a_nb_m \end{aligned}$$

Die so eingeführte Produktbildung ist für alle Polynome definiert, sie bildet stets wieder ein Polynom und ist im Bereich der Polynome unbeschränkt ausführbar.

Bei der Division genügt es, ein Gegenbeispiel anzuführen, um zu zeigen, dass der Quotient zweier Polynome im allgemeinen kein Polynom ist.
Es sei $f_1 = x^2 - 16$ und $f_2(x) = x - 5$.

$$\frac{f_1(x)}{f_2(x)} = x + 5 + \frac{9}{x - 5}$$

Die Division ist hier im Bereich der Polynome nicht ausführbar, das Ergebnis ist kein Polynom. Da auch Assoziativ-, Kommutativ- und Distributivgesetze für Polynome gelten, bildet die Menge aller Polynome einen Ring mit der eben eingeführten Addition und Multiplikation von Polynomen als Verknüpfung.

[5] Siehe auch Alexandroff, Einführung in die Gruppentheorie, Berlin 1964

2.2 Dirichletsches Schubfachprinzip

(25) Man zeige, dass von den Schülern einer Schule mit 400 Schülern gewiss zwei darunter sind, die am gleichen Tag Geburtstag haben.

Lösung:
Da das Jahr höchstens 366 Tage hat und mehr Schüler an der Schule als Tage im Jahr vorhanden sind, muss es Schüler geben, die am gleichen Tag Geburtstag haben.

(26) Man zeige, dass man von den durch 7 teilbaren ganzen Zahlen im Bereich $1000 \leq x \leq 1100$ nicht 9 voneinander verschiedene gerade Zahlen auswählen kann.

Lösung:
Das angegebene Intervall umfasst 101 Zahlen, darunter befinden sich 14 durch 7 teilbare Zahlen, von denen 7 gerade und 7 ungerade sind. Es ist also nicht möglich, 9 voneinander verschiedene gerade Zahlen unter ihnen auszuwählen.

(27) Man zeige, dass von den durch 13 teilbaren natürlichen Zahlen im Bereich $k + 1000 \leq x \leq k + 2000$ mindestens eine durch 57 teilbar ist.
k sei eine beliebige natürliche Zahl.

Lösung:
Das angegebene Intervall umfasst 1001 natürliche Zahlen, darunter befinden sich mindestens 76 durch 13 teilbare Zahlen, die sich darstellen lassen durch

$$r \cdot 13, (r+1) \cdot 13, (r+2) \cdot 13, ..., (r+76) \cdot 13$$

Unter den Zahlen $r, r+1, r+2, ..., r+76$, die 77 aufeinanderfolgende natürliche Zahlen darstellen, ist aber mindestens eine durch 57 teilbar.

Bemerkung: Allgemein gilt das "Schubfachprinzip von Dirichlet[6]":

1. Werden n Elemente auf m Klassen verteilt und befinden sich in keiner Klasse zwei oder mehr Elemente, so befindet sich in jeder Klasse genau ein Element, wenn keine Klasse leer ausgeht, und es ist $n = m$
Oder:
2. Werden n Elemente auf m Klassen verteilt und ist $n > m$, so gibt es mindestens eine Klasse, in der zwei oder mehr Elemente vorhanden sind.

(28) Gegeben sind alle m-stelligen Zahlen z, die sich durch die Ziffern $1, 2, 3, ...n \leq 9$ darstellen lassen.
Es ist zu zeigen, dass sich für jedes $m > 1$ und für jedes $n > 2$ mindestens $\left(\frac{n-1}{2}\right)^m$ voneinander verschiedene Zahlen auswählen lassen, für die das Produkt aller ihrer Ziffern ungerade ist.

Lösung: Es sollen zunächst für einige Zahlen m und n die möglichen Darstellungen angegeben werden.

	n	3	4	5	6	7
$m = 2$	z	11	11	11 35	11 35	11 33 55 77
		13	13	13 51	13 51	13 35 57
		31	31	15 53	15 53	15 37 71
		33	33	31 55	31 55	17 51 73
				33	33	31 53 75
	s_n	4	4	9	9	16

[6]Dirichlet, Peter Gustav Lejeune, deutscher Mathematiker (1805-1859)

$m = 3$

n	3	4	5
z	111	111	111 155 353 551
	113	113	113 311 355 553
	131	131	115 313 511 555
	133	133	131 315 513
	311	311	133 331 515
	313	313	135 333 531
	331	331	151 335 533
	333	333	153 351 535
s_n	8	8	27

Für alle geraden Zahlen n ist die Anzahl der Möglichkeiten gleich der Anzahl für $(n-1)$. Nur für eine neue ungerade Zahl n kommen weitere Möglichkeiten hinzu. Es genügt also, nur ungerade Zahlen n zu betrachten.

Behauptung: Für alle ungeraden Zahlen n gilt: $s_n = \left(\frac{n+1}{2}\right)^m$.

Die Formel gilt, wie aus der Tabelle hervorgeht, für ein spezielles $n = 3$ und ein bestimmtes $m = 2$.
m sei zunächst fest gewählt: $m = 2$. Unter der Annahme, dass die Formel für die ungerade Zahl $n = k$ $(k > 2)$ richtig ist $\left(s_k = \left(\frac{k+1}{2}\right)^2\right)^2$ wird behauptet, dass sie auch für die auf k folgende ungerade Zahl $(k+2)$ gilt $\left(s_{k+2} = \left(\frac{k+3}{2}\right)^2\right)$.

Beweis:
Bei Hinzunahme der auf k folgenden ungeraden Zahl $(k+2)$ bleiben alle Möglichkeiten für k erhalten, außerdem treten die folgenden Zahlen hinzu:

$$1(k+2), 3(k+2), 5(k+2), ..., k(k+2), (k+2)(k+2) \quad \text{sowie}$$

$$(k+2)1, (k+2)3, (k+2)5, ..., (k+2)k$$

Das sind $k+2$ neu hinzukommende Zahlen. Es gilt:

$$s_{k+2} = s_k + k + 2 = \left(\frac{k+1}{2}\right)^2 + k + 2 = \left(\frac{k+3}{2}\right)^2$$

Damit gilt die Formel bei festgewähltem $m = 2$ für alle ungeraden Zahlen $n > 2$.
Es sei jetzt $m > 1$ beliebig ganzzahlig. Unter der Annahme, dass die Formel für $m = k$ richtig ist, wird behauptet, dass sie auch für die auf k folgende natürliche Zahl $(k+1)$ richtig ist.

Beweis:
Lässt man eine weitere Stellenzahl zu, so bleibt die Anzahl der Möglichkeiten zunächst erhalten, wenn man die erste der n zulässigen ungeraden Ziffern vor alle möglichen Zahlen der Stellenzahl k setzt. Die gleiche Anzahl erhält man aber, wenn jede andere der n zulässigen ungeraden Ziffern vor diese Zahlen gesetzt werden.
Es ergeben sich also für $(k+1)$-stellige Zahlen

$$s_{k+1} = \left(\frac{n+1}{2}\right)^k \cdot \left(\frac{n+1}{2}\right) = \left(\frac{n+1}{2}\right)^{k+1}$$

Möglichkeiten, da es $\frac{n+1}{2}$ ungerade Zahlen gibt, die kleiner oder gleich der ungeraden Zahl n sind.

Die Formel gilt also für alle natürlichen Zahlen $n > 2$ und für alle natürlichen Zahlen $m > 1$ bei den für die Aufgabe gültigen Voraussetzungen.

Es ist nun bei $s_n = \left(\frac{n+1}{2}\right)^m$ vorhandenen Fächern stets möglich, $\left(\frac{n-1}{2}\right)^m$ verschiedene Fächer genau einmal zu belegen.

(29) Gegeben ist die Menge aller Dreiecke, die einem Halbkreis mit dem Radius r einbeschrieben sind. (Eine Dreiecksseite ist gleich dem Durchmesser des Halbkreises.)
Es ist zu zeigen, dass es darunter mindestens 5 Dreiecke gibt, deren, Gradmaße der Winkel ganzzahlig sind, wobei die Größe des einen Winkels genau das n-fache der Größe eines anderen Winkels ist.

Lösung:
Nach dem Satz des Thales handelt es sich um rechtwinklige Dreiecke, deren Hypotenuse der Kreisdurchmesser ist. Die Summe der Gradmaße der der Hypotenuse anliegenden Winkel beträgt $90°$. Ein Winkel habe das Gradmaß x, dann gilt: $(n+1)x = 90°$.

n	1	2	4	5	8	9	14	17	29	44	89
1. Winkel x	$45°$	$30°$	$18°$	$15°$	$10°$	$9°$	$6°$	$5°$	$3°$	$2°$	$1°$
2. Winkeln nx	$45°$	$60°$	$72°$	$75°$	$80°$	$81°$	$84°$	$85°$	$87°$	$88°$	$89°$

In der Tabelle sind alle Möglichkeiten erfasst. Nach dem Prinzip von Dirichlet ist es bei 11 vorhandenen Fächern stets möglich, 5 Fächer mit verschiedenen Elementen genau einmal zu belegen.

(30) Es ist zu zeigen, dass in einer Millionenstadt mindestens 100000 Menschen leben, von denen jeder mit mindestens einem anderen im gleichen Jahr, am gleichen Tag und zur gleichen Stunde geboren ist.

Lösung: In der Stadt leben nach Voraussetzung mehr als 1000000 Einwohner.
Angenommen, es gibt 1000000 Einwohner, die das 100. Lebensjahr noch nicht überschritten haben, dann wurden diese Einwohner in einem Zeitraum von $100 \cdot 365 \cdot 24 = 876000$ Stunden geboren.
Nach dem Prinzip von Dirichlet heißt das, dass bei einer Belegung der 876000 Fächer mit 1000000 Elementen mindestens 100000 Fächer doppelt belegt werden.

(31)• Es seien $2n$ Elemente in linearer Anordnung gegeben:

$$x_1, x_2, x_3, ..., x_{k-1}, x_k, x_{k+1}, ..., x_{2n}$$

Zwei Nachbarelemente in dieser Anordnung sollen verwandt heißen. So ist x_1 mit x_2 verwandt, ebenso x_7 mit x_6 und mit x_8 oder x_k mit x_{k-1} und mit x_{k+1}. In der gegebenen Anordnung nicht nebeneinanderstehende Elemente sind nicht verwandt miteinander.
Nun soll die Anordnung durch Auswechseln der Elemente so verändert werden, dass keine verwandten Elemente Nachbarelemente sind. Man zeige, dass es mindestens n^2 solcher Anordnungen gibt bei $n > 3$.

(32)• a) Man zeige, dass es im Intervall $100 < n! < x < (n+1)!$ mindestens eine natürliche Zahl x gibt, die durch n^3 teilbar ist.
b) Man zeige, dass es im Intervall $2^n \leq x \leq 2^{n+1}$ mindestens eine natürliche Zahl x gibt, die durch n^2 teilbar ist.

3 Primzahlzerlegungen, Euklidischer Algorithmus

In den nun folgenden Abschnitten beschäftigen wir uns nur mit ganzen Zahlen.
Gilt $a = mq$, so sagen wir: a ist durch m teilbar oder m ist ein Teiler von a, geschrieben $m \mid a$.

3.1 Teiler, Primzahlzerlegungen

(33) Man zeige: Ist a Teiler der Zahl b und b Teiler von c, so ist a Teiler von c.
Oder: Mit $a \mid b$ und $b \mid c$ gilt $a \mid c$.

Lösung:
a heißt Teiler von b ($a \mid b$), wenn die Gleichung $ax = b$ eine Lösung besitzt, wenn b also ein Vielfaches von a ist. Es ist nun zu zeigen, dass aus den Lösungen der Gleichungen $ax = b$ ($a \mid b$) und $by = c$ ($b \mid c$) die Lösung der Gleichung $az = c$ folgt, was bedeutet, dass $a \mid c$.

Durch Substitution von $b = ax$ in $by = c$ folgt $axy = c$. Nach Voraussetzung existieren die Lösungen x und y, es existiert also auch die ganze Zahl $z = xy$. Daraus folgt $az = c$ oder $a \mid c$.

(34) Man zeige, dass es unendlich viele Primzahlen gibt, dass es also zu jeder noch so großen Primzahl p_n stets eine noch größere Primzahl p_{n+1} gibt.

Lösung (nach Euklid)[7]
Es sei p_n die n-te Primzahl. Man bildet das Produkt aller Primzahlen p_k mit $k \leq n$.

$$w = \prod_{k=1}^{n} p_k = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_n$$

Dieses Produkt ist durch jede der ersten n Primzahlen teilbar. Vergrößert man dieses Produkt um 1, so ist der entstehende Ausdruck durch keine dieser ersten n Primzahlen teilbar, denn bei der Division des Ausdrucks $(w + 1)$ durch irgendeine der betrachteten Primzahlen p_i ($i \leq n$) würde stets der Rest 1 bleiben.

$$w + 1 = \prod_{k=1}^{n} p_k + 1 = p_1 \cdot p_2 \cdot p_3 \cdot ... \cdot p_n + 1$$
$$\frac{w+1}{p_i} = \frac{p_1 \cdot p_2 \cdot ...p_{i-1} \cdot p_i \cdot p_{i+1} \cdot ... \cdot p_n + 1}{p_i} = p_1 \cdot p_2 \cdot ...p_{i-1} \cdot p_{i+1} \cdot ... \cdot p_n + \frac{1}{p_i}$$

1. Fall. Der Ausdruck $(w + 1)$ ist selbst Primzahl p^*.
Es gilt $p^* \neq p_k$ ($k \leq n$) und $p^* > p_n$.

Beispiele:
$n = 2$; $p_1 = 2$; $p_2 = 3$ $\quad w + 1 = 7$, 7 ist Primzahl.
$n = 3$; $p_1 = 2$; $p_2 = 3$; $p_3 = 5$ $\quad w + 1 = 31$, 31 ist Primzahl.
$n = 4$; $p_1 = 2$; $p_2 = 3$; $p_3 = 5$; $p_4 = 7$ $\quad w + 1 = 211$, 211 ist Primzahl.

2. Fall. Der Ausdruck $(w + 1)$ ist keine Primzahl.
Der kleinste von 1 verschiedene in $(w + 1)$ enthaltene Teiler muss aber eine Primzahl p^{**} sein, wobei $p^{**} \neq p_k$ ($k \leq n$) und $p^{**} > p_n$, da von den ersten n Primzahlen keine als Teiler in $(w + 1)$ enthalten ist, wie oben gezeigt wurde.

[7] Euklid, griechischer Mathematiker, um 250 v. u. Z. in Alexandrien.

Beispiel:
$n = 6$; $p_1 = 2$; $p_2 = 3$; $p_3 = 5$; $p_4 = 7$; $p_5 = 11$; $p_6 = 13$; $w = 30030$; $w + 1 = 30031$;
$30031 = 59 \cdot 509$ (59 und 509 sind Primzahlen).

Man erhält in jedem Fall durch den Ausdruck $(w + 1)$ eine neue Primzahl p_z, die größer ist als p_n. Auch diese neue Primzahl p_z kann nicht die "letzte" sein.

Das Produkt $v = \prod_{k=1}^{z} p_k = p_1 \cdot p_2 \cdot ... \cdot p_n \cdot ... \cdot p_z$ ist durch alle Primzahlen p_j $(j < z)$ teilbar. Der Ausdruck

$$v + 1 = \prod_{k=1}^{z} p_k + 1 = p_1 \cdot p_2 \cdot ... \cdot p_n \cdot ... \cdot p_z + 1$$

ist durch keine der Primzahlen p_j $(j \leq z)$ teilbar. Die Zerlegung von $(v + 1)$ liefert wiederum mindestens eine neue Primzahl p' mit $p' > p_z$.
Ergebnis: Es gibt unendlich viele Primzahlen. Zu jeder Primzahl p_n gibt es stets eine größere Primzahl p_{n+1}.

Bemerkung: Wir kennen keine geschlossene Darstellung für die unendliche Folge der Primzahlen, wie zum Beispiel für die Folge der ungeraden Zahlen oder wie für die Folge der Kubikzahlen, und dennoch sind die Primzahlen abzählbar, sie lassen sich den Elementen der Menge der natürlichen Zahlen eindeutig zuordnen, wodurch eine Indizierung der Primzahlen gerechtfertigt ist.

$$p_1 = 2; p_2 = 3; p_3 = 5; p_4 = 7; p_5 = 11; p_6 = 13; p_7 = 17; ...$$

(35) Man zeige: Im Bereich der natürlichen Zahlen ist jede Zahl $n > 1$ als Produkt von Primzahlpotenzen darstellbar.

Lösung:
1. Fall: $n > 1$ ist Primzahl, $n = p$.
2. Fall: $n > 1$ ist Nichtprimzahl.
Es existiert eine kleinste Primzahl p_ν, die Teiler von n ist, und es gilt $n = p_\nu \cdot n_1$ mit $n_1 < n$. Ist n_1 wiederum Nichtprimzahl, so gibt es wieder eine kleinste Primzahl p_μ, die Teiler von n_1 ist, und es gilt $n_1 = p_\mu \cdot n_2$ mit $n_2 < n_1$. Die Zerlegung wird fortgesetzt, bis man eine Zahl n_k erhält, die Primzahl ist $(n_k = p_\sigma)$. Die Darstellung der Zahl n ist damit:

$$n = p_\nu \cdot p_\mu \cdot ... \cdot p_\sigma$$

Beispiele:
$n_1 = 8300609 = 2^3 \cdot 5^2 \cdot 7^3 \cdot 11^2$
$n_2 = 1048756 = 2^{20}$
$n_3 = 294311 = 2943111$ (294311 ist Primzahl).

(36) Man zeige: Im Bereich der natürlichen Zahlen ist jede Zahl n eindeutig als Produkt von Primzahlpotenzen darstellbar.

Lösung (nach Zermelo)[8]
Der Beweis für die Eindeutigkeit der Zerlegung in Primzahlpotenzen soll indirekt geführt werden. Man nimmt an, es gibt Zahlen n mit zwei voneinander verschiedenen Zerlegungen.
Dann gibt es eine kleinste Zahl n_1, die zwei voneinander verschiedene Zerlegungen zulässt. p sei die kleinste in n_1 enthaltene Primzahl und es sei $n_1 = pn_2$. Hierbei ist n_2 auf nur eine Art zerlegbar, weil $n_2 < n_1$ und weil n_1 die kleinste Zahl mit zwei voneinander verschiedenen

[8] Zermelo, Ernst, 1871-1953, einer der Begründer der axiomatischen Mengenlehre

Zerlegungen sein sollte.

1. Fall: Die zweite Zerlegung enthalte auch die Primzahl p als Faktor.
$n_1 = p \cdot n_k$. Es ergibt sich sofort ein Widerspruch zur Annahme, dass es nämlich zwei Zerlegungen für n_1 gibt, denn aus $n_1 = p \cdot n_2$ und $n_1 = p \cdot p_k$ folgt $p \cdot n_2 = p \cdot n_k$ oder $n_2 = n_k$, was aber Eindeutigkeit der Zerlegung bedeutet.

2. Fall: Die zweite Zerlegung enthalte nicht die Primzahl p, sondern die Primzahl q als Faktor mit $q \neq p$.
Es gilt $n_1 = q \cdot n_3$ mit $q > p$, da p die kleinste in n_1 enthaltene Primzahl sein sollte.
Man bildet die Differenz $d = n_1 - p \cdot n_3$, die eine eindeutige Zerlegung zulassen muss, weil $d < n_1$. Setzt man für n_1 die Zerlegung $q \cdot n_3$ ein, so ergibt sich

$$d = n_1 - p \cdot n_3 = q \cdot n_3 - p \cdot n_3 = n_3(q - p)$$

Andererseits kann man für n_1 den Wert $p \cdot n_2$ setzen und erhält

$$d = n_1 - p \cdot n_3 = p \cdot n_2 - p \cdot n_3 = p(n_2 - n_3)$$

Daraus folgt $n_3(q - p) = p(n_2 - n_3)$.
n_3 kann den Faktor p nicht enthalten, weil n_1 den Faktor p nicht enthält (Voraussetzung für den Fall 2). Es muss also die Differenz $(q - p)$ den Faktor p enthalten

$$q - p = k \cdot p \qquad \text{oder} \qquad q = k \cdot p + p = p(k + 1)$$

Dies bedeutet aber, dass q zerlegbar ist und also nicht Primzahl sein kann. Auch hier hat man einen Widerspruch zur Annahme erhalten.

Ergebnis: Jede natürliche Zahl n ist eindeutig als Produkt von Primzahlpotenzen darstellbar.

$$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdot ... \cdot p_r^{\alpha_r}$$

(37) Es ist zu zeigen, dass $z = p^3 - p$ für jede Primzahl $p > 2$ durch 24 teilbar ist.

Lösung:

$$z = p^3 - p = p(p^2 - 1) = (p - 1) \cdot p \cdot (p + 1)$$

Mit p ungerade sind $(p - 1)$ und $(p + 1)$ gerade Zahlen und somit durch 2 teilbar, während entweder $(p-1)$ oder $(p+1)$ zusätzlich noch durch 4 teilbar ist. Von 3 aufeinanderfolgenden natürlichen Zahlen ist eine durch 3 teilbar, folglich ist z durch $2 \cdot 4 \cdot 3 = 24$ teilbar.

3.2 Teilbarkeitsaufgaben

(38) Es ist zu zeigen, dass $z = p^4 - 1$ für jede Primzahl $p > 5$ durch 240 teilbar ist.

Lösung:
Es gilt die Zerlegung

$$z = p^4 - 1 = (p^2 + 1)(p^2 - 1) = (p^2 + 1)(p + 1)(p - 1)$$

Da p ungerade ist, so müssen $(p + 1)$, $(p - 1)$ und $(p^2 + 1)$ gerade sein; außerdem muss entweder $(p - 1)$oder $(p + 1)$ eine durch 4 teilbare Zahl sein. Hieraus folgt, dass z durch 16 teilbar ist.

Da von 3 aufeinanderfolgenden natürlichen Zahlen stets eine durch 3 teilbar ist und $p > 5$ nicht durch 3 teilbar ist, so muss entweder $(p-1)$ oder $(p+1)$ durch 3 teilbar sein, folglich ist z durch 3 teilbar.

Primzahlen größer als 5 können nur auf die Ziffern 1, 3, 7 oder 9 enden, die Quadrate dieser Primzahlen enden auf 1 oder 9. Daraus folgt, dass entweder (p^2-1) oder (p^2+1) durch 5 teilbar sein muss, also ist z durch 5 teilbar.
Wenn z durch 3, durch 5 und durch 16 teilbar ist, dann ist z durch $3 \cdot 5 \cdot 16 = 240$ teilbar.

(39) Es ist zu zeigen, dass $z = p^4 - 10p^2 + 9$ für jede Primzahl $p > 5$ durch 1920 teilbar ist.

Lösung:

$$z = p^4 - 10p^2 + 9 = (p^2-9)(p^2-1) = (p-3)(p-1)(p+1)(p+3)$$

Von 4 aufeinanderfolgenden geraden Zahlen sind stets zwei durch 4 teilbar, von denen eine sogar durch 8 teilbar ist. Folglich ist z durch $8 \cdot 4 \cdot 2 \cdot 2 = 128$ teilbar.
Mindestens eine der 4 aufeinanderfolgenden geraden Zahlen ist durch 3 teilbar, und genau eine dieser Zahlen ist auch durch 5 teilbar, woraus folgt, dass auch z durch 3 und durch 5 teilbar ist.
z ist durch $128 \cdot 3 \cdot 5 = 1920$ teilbar.

(40) Für welche geraden Zahlen n ist $z = n^4 - 1$ durch 5 teilbar?

Lösung:

$$n = 2k; \qquad z = n^4 - 1 = (n^2-1)(n^2+1) = (4k^2+1)(4k^2-1)$$

Man betrachtet die möglichen Endziffern der Zahlen $2k$ und ihrer Quadrate und erhält:

$2k$	2	4	6	8	0
$4k^2$	4	6	6	4	0
$4k^2+1$	5	7	7	5	1
$4k^2-1$	3	5	5	3	9

Aus der Tabelle ersieht man, dass für alle geraden Zahlen n, die nicht auf Null enden, entweder $(4k^2+1)$ oder $(4k^2-1)$ durch 5 teilbar ist.

(41) Es ist zu zeigen, dass $z_n = n^3 + 11n$ für jede natürliche Zahl n durch 6 teilbar ist.

Lösung:
$z_n = n(n^2+11)$. Für jede natürliche Zahl n gilt die Darstellung $n = 6k + r$ mit $r = 0, \pm 1, \pm 2, \pm 3$.
Es werden die möglichen Fälle auf ihre Teilbarkeit durch 6 hin untersucht.

$r = 0$; $n = 6k$, z_n ist durch 6 teilbar.
$r = \pm 1$; $n^2 + 11 = 36k^2 \pm 12k + 12$, z_n ist durch 6 teilbar
$r = \pm 2$; $n^2 + 11 = 36k^2 \pm 24k + 15 = 3(12k^2 \pm 8k + 5)$ $\quad n = 6k \pm 2 = 2(3k \pm 1)$, z_n ist durch $2 \cdot 3 = 6$ teilbar.
$r = \pm 3$; $n^2 + 11 = 36k^2 + 36k + 20 = 2(18k^2 + 18k + 10)$ $\quad n = 6k + 3 = 3(2k+1)$, z_n ist durch $2 \cdot 3 = 6$ teilbar.

Damit ist für alle Möglichkeiten die Teilbarkeit durch 6 bewiesen:
Die Teilbarkeit durch 6 soll nochmals durch den Schluss von k auf $(k+1)$ nachgewiesen werden.

Behauptung:
$z_n = n(n^2 + 11)$ ist für jede natürliche Zahl $n > 0$ durch 6 teilbar.
$z_1 = 12$ ist durch 6 teilbar.

Unter der Annahme, dass $z_k = k(k^2 + 11)$ durch 6 teilbar ist, wird nun gezeigt, dass z_n auch für die auf k folgende natürliche Zahl $k+1$ durch 6 teilbar ist ($z_{k+1} = (k+1)(k^2+2k+12)$).

$$\begin{aligned} z_{k+1} &= k(k^2 + 2k + 12) + k^2 + k + 12 = k(k^2 + 11) + k(2k + 1) + k^2 + 2k + 12 \\ &= k(k^2 + 11) + 3k^2 + 3k + 12 = z_k + 3k(k + 1) + 12 \end{aligned}$$

z_k ist nach Voraussetzung durch 6 teilbar, von den zwei aufeinanderfolgenden natürlichen Zahlen k und $(k + 1)$ ist eine durch 2, folglich ist $3k(k + 1)$ durch $3 \cdot 2 = 6$ teilbar. Damit ist $z_n = n^3 + 11n$ für jede natürliche Zahl n > 0 durch 6 teilbar.

Es soll eine dritte Lösung der Aufgabe angeschlossen werden. Es gilt:

$$z_n = n^3 + 11n = n^3 - n + 12n = n(n^2 - 1) + 12n = (n - 1) \cdot n \cdot (n + 1) + 12n$$

Von den drei aufeinanderfolgenden natürlichen Zahlen $(n - 1)$, n und $(n + 1)$ ist mindestens eine durch 2 und genau eine durch 3 teilbar, womit z_n durch 6 teilbar ist.

(42) Es ist zu zeigen, dass $z_n = n^7 - n$ für jede natürliche Zahl $n > 1$ durch 42 teilbar ist.

Lösung:

$$\begin{aligned} z_n &= n^7 - n = n(n^3 + 1)(n^3 - 1) = n(n - 1)(n^2 + n + 1)(n + 1)(n^2 - n + 1) \\ &= (n - 1) \cdot n \cdot (n + 1)(n^2 - n + 1)(n^2 + n + 1) \end{aligned}$$

Von drei aufeinanderfolgenden natürlichen Zahlen $(n-1)$, n und $(n+1)$ ist eine durch 3 und mindestens eine durch 2 teilbar, folglich ist z_n durch 6 teilbar.
Für jede natürliche Zahl n gilt nun die Darstellung $n = 7k + r$ mit $r = 0, \pm1, \pm2, \pm3$.

$r = 0$; $n = 7k$, z_n ist durch 7 teilbar.
$r = 1$; $n = 7k + 1$, $(n - 1) = 7k$, z_n ist durch 7 teilbar.
$r = -1$; $n = 7k - 1$, $(n + 1) = 7k$, z_n ist durch 7 teilbar.
$r = 2$; $n = 7k + 2$, $(n^2 + n + 1) = 49k^2 + 28k + 4 + 7k + 2 + 1$, z_n ist durch 7 teilbar.
$r = -2$; $n = 7k - 2$, $(n^2 - n + 1) = 49k^2 - 35k + 7$, z_n ist durch 7 teilbar.
$r = 3$; $n = 7k + 3$, $(n^2 - n + 1) = 49k^2 + 35k + 7$, z_n ist durch 7 teilbar.
$r = -3$; $n = 7k - 2$, $(n^2 + n + 1) = 49k^2 - 35k + 7$, z_n ist durch 7 teilbar.

Also ist z_n durch $6 \cdot 7 = 42$ teilbar.

Die Teilbarkeit durch 7 soll noch einmal durch den Schluss von k auf $(k+1)$ bewiesen werden.
$n = 1$; $z_1 = 0$. Jede natürliche Zahl ist Teiler von Null.
$n = 2$; $z_2 = 128 - 2 = 126 = 7 \cdot 18$. z_2 ist durch 7 teilbar.
Unter der Annahme, dass z_n für $n = k$ durch 7 teilbar ist ($z_k = k^7 - k$), wird behauptet, dass z_n auch für die auf k folgende natürliche Zahl $(k+1)$ durch 7 teilbar ist ($z_{k+1} = (k+1)^7 - (k+1)$).

Beweis:

$$\begin{aligned} z_{k+1} &= (k + 1)^7 - (k + 1) = k^7 + 7k^6 + 21k^5 + 35k^4 + 35k^3 + 21k^2 + 7k + 1 - k - 1 \\ &= k^7 - k + 7k^6 + 21k^5 + 35k^4 + 35k^3 + 21k^2 + 7k \\ &= z_k + 7(k^6 + 3k^5 + 5k^4 + 5k^3 + 3k^2 + k) \end{aligned}$$

z_k war nach Voraussetzung durch 7 teilbar. Folglich ist $z_n = n^7 - n$ für jede natürliche Zahl n durch 7 teilbar.

(43) Man zeige, dass $z_n = 12^{512} - 1$ durch 4147 teilbar ist.

Lösung:
Es gilt die Zerlegung $4147 = 11 \cdot 13 \cdot 29$ und weiter

$$z_n = 12^{512} - 1 = (12^{256+1})(12^{128} + 1)(12^{64} + 1)(12^{32} + 1)(12^{16} + 1)(12^8 + 1)(12^4 + 1)$$
$$(12^2 + 1)(12^1+)(12^0 - 1)$$

$12^2 + 1 = 145 = 5 \cdot 29$, $12^1 + 1 = 13$, $12^1 - 1 = 11$. z_n ist durch $29 \cdot 13 \cdot 11 = 4147$ teilbar.

Bemerkung: Auch die Faktoren $(12^4 - 1)$, $(12^{16} - 1)$, $(12^{256} - 1)$ sind zum Beispiel Teiler von z_n, und diese Faktoren sind nach dem kleinen Satz von Fermat[9] durch 5, durch 17 und durch 257 teilbar.
Folglich sind auch 5, 17 und 257 Teiler von z_n.

(44)• Man zeige, dass $z = 18^{128} - 1$ durch 104975 teilbar ist.

(45)• Man zeige, dass $z_n = n^5 + 4n$ für jede natürliche Zahl n durch 5 teilbar ist.

(46)• Man zeige, dass $z_n = p^4 + 4$ für jede Primzahl $p > 5$ durch 5 teilbar ist.

(47)• Mit welcher Ziffer endet die 12. Potenz einer Primzahl $p > 100$?

3.3 Kleinstes gemeinschaftliches Vielfaches, größter gemeinsamer Teiler

(48) Gegeben seien zwei natürliche Zahlen n_1 und n_2 sowie die Primzahlproduktdarstellungen dieser Zahlen mit nichtnegativen ganzzahligen Exponenten.

$$n_1 = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r} \qquad , \qquad n_2 = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot ... \cdot p_s^{\beta_s}$$

Gesucht ist die kleinste natürliche Zahl m sowie die Produktdarstellung dieser Zahl m, in der n_1 und n_2 als Faktoren enthalten sind.

Beispiele:
a) $n_1 = 48$, $n_2 = 84$ b) $n_1 = 1125$, $n_2 = 35$.

Lösung:
Es sei angenommen, dass $s > r$. Man konstruiert Exponenten γ_i derart, dass $\gamma_i = \alpha_i$, wenn $\alpha_i \geq \beta_i$ und dass $\gamma_i = \beta_i$, falls $\beta_i > \alpha_i$.

$$m = [n_1, n_2] = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot ... \cdot p_s^{\gamma_s}$$

In m sind n_1 und n_2 als Faktoren enthalten.
m ist die kleinste natürliche Zahl mit der Eigenschaft, n_1 und n_2 als Faktor zu enthalten, denn gäbe es eine kleinere Zahl m' mit der geforderten Eigenschaft, dann müsste eine der Potenzen $p_i^{\gamma_i}$ verkleinert werden, und diese eine Potenz würde dann von $p_i^{\alpha_i}$ oder von $p_i^{\beta_i}$ übertroffen, so dass n_1 oder n_2 kein Teiler von m' wäre.

Beispiele: a) $n_1 = 48$, $n_2 = 84$, $n_1 = 2^4 \cdot 3^1$, $n_2 = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^1$

[9] Siehe Aufgabe (114)

$\gamma_1 = 4$, $\gamma_2 = 1$, $\gamma_3 = 0$, $\gamma_4 = 1$, $m = 2^4 \cdot 3^1 \cdot 5^0 \cdot 7^1 = 336$

b) $n_1 = 1125$, $n_2 = 35$, $n_1 = 2^0 \cdot 3r \cdot 5^3$, $n_2 = 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^1$
$\gamma_1 = 0$, $\gamma_2 = 2$, $\gamma_3 = 3$, $\gamma_4 = 1$, $m = 2^0 \cdot 3^2 \cdot 5^3 \cdot 7^1 = 7875$

Bemerkung: m heißt das "kleinste gemeinschaftliche Vielfache" (kgV) der Zahlen n_1 und n_2. Durch analoge Überlegung kommt man auch zum kgV von k natürlichen Zahlen

$$m = [n_1, n_2, n_3, ..., n_7]$$

Das kgV ist Teiler aller anderen gemeinschaftlichen Vielfachen m_j, da andere gemeinschaftliche Vielfache nur durch Vergrößerung der γ_i oder durch Multiplikation des Produktes mit einem Faktor K entstehen können und da m_j also nur die Form

$$m_j = K \cdot p_1^{\mu_1} \cdot p_2^{\mu_2} \cdot p_3^{\mu_3} \cdot ... \cdot p_s^{\mu_s}$$

mit $\mu_i \geq \gamma_i$ haben kann. Es ist jetzt aber möglich, die Potenzen aufzuspalten und folgende Form zu erreichen

$$m_j = K \cdot p_1^{\lambda_1} \cdot p_2^{\lambda_2} \cdot p_3^{\lambda_3} \cdot ... \cdot p_s^{\lambda_s} \cdot (p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot ... \cdot p_s^{\gamma_s}) = k^* \cdot m$$

Bei größeren natürlichen Zahlen wird das oben angegebene Verfahren zur Gewinnung des kgV recht kompliziert und langwierig. Durch den Euklidischen Algorithmus wird später ein brauchbares Verfahren entwickelt (man vergleiche Aufgabe (50)).

(49) Gegeben seien zwei natürliche Zahlen n_1 und n_2 sowie die Primzahlproduktdarstellungen dieser Zahlen mit nichtnegativen ganzzahligen Exponenten.

$$n_1 = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r} \qquad , \qquad n_2 = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot ... \cdot p_s^{\beta_s}$$

Gesucht ist die größte natürliche Zahl d, die sowohl in n_1 als auch in n_2 als Faktor enthalten ist.

Beispiele: a) $n_1 = 48$, $n_2 = 84$ b) $n_1 = 1125$, $n_2 = 35$.

Lösung:
Es sei angenommen, dass $s \geq r$ gilt. Man konstruiert Exponenten δ_1 derart, dass $\delta_1 = \alpha_i$, wenn $\alpha_i \leq \beta_i$ und dass $\delta_i = \beta_i$, falls $\beta_i \leq \alpha_i$.

$$d = (n_1, n_2) = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot p_3^{\delta_3} \cdot ... \cdot p_r^{\delta_r}$$

d ist in n_1 und in n_2 als Faktor enthalten, da $\delta_i \leq \alpha_i$ und $\delta_i \geq \beta_i$ sowie $s \geq r$.

d ist die größte Zahl mit der Eigenschaft, Teiler von n_1 und n_2 zu sein, denn gäbe es eine größere Zahl d' mit der geforderten Eigenschaft, dann müsste mindestens eine der Potenzen $p_i^{\delta_i}$ vergrößert werden und diese Potenz würde $p_i^{\alpha_i}$ oder $p_i^{\beta_i}$ übertreffen, so dass dann entweder d' kein Teiler von n_1 oder aber kein Teiler von n_2 wäre.

Beispiele:
a) $n_1 = 48$, $n_2 = 84$, $n_1 = 2^4 \cdot 3^1$, $n_2 = 2^2 \cdot 3^1 \cdot 5^0 \cdot 7^1$,
$\delta_1 = 2$, $\delta_2 = 1$, $\delta_3 = 0$, $\delta_4 = 0$, $d = 2^2 \cdot 3^1 = 12$.

b) $n_1 = 1125$, $n_2 = 35$, $n_1 = 2^0 \cdot 3^2 \cdot 5^3$, $n_2 = 2^0 \cdot 3^0 \cdot 5^1 \cdot 7^1$,
$\delta_1 = 0$, $\delta_2 = 0$, $\delta_3 = 1$, $\delta_4 = 0$, $d = 2^0 \cdot 3^0 \cdot 5^1 = 5$.

Bemerkung: d heißt "größter gemeinsamer Teiler" (ggT) der Zahlen n_1 und n_2. Durch analoge Überlegung kommt man auch zum ggT d von k natürlichen Zahlen

$$d = (n_1, n_2, n_3, ..., n_k)$$

Der ggT ist Vielfaches aller anderen gemeinsamen Teiler. Alle anderen gemeinsamen Teiler d, der betrachteten natürlichen Zahlen sind in d als Faktor enthalten. Andere gemeinsame Teiler können aus d nur dadurch entstehen, dass gewisse δ_i verkleinert werden. Dann gilt:

$$d_j = p_1^{\rho_1} \cdot p_2^{\rho_2} \cdot p_3^{\rho_3} \cdot ... \cdot p_r^{\rho_r}$$

mit $\rho_i \leq \delta_i$. Es ist jetzt aber möglich, die Potenzen von d aufzuspalten, so dass

$$d = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot p_3^{\delta_3} \cdot ... \cdot p_r^{\delta_r} = p_1^{\sigma_1} \cdot p_2^{\sigma_2} \cdot p_3^{\sigma_3} \cdot ... \cdot p_r^{\sigma_r} \cdot (p_1^{\rho_1} \cdot p_2^{\rho_2} \cdot p_3^{\rho_3} \cdot ... \cdot p_r^{\rho_r}) = k \cdot d_j$$

Ist der ggT zweier natürlicher Zahlen n_1 und n_2 gleich 1, so heißen die Zahlen "teilerfremd" oder "prim" zueinander. Auch k Zahlen heißen teilerfremd, wenn $d = (n_1, n_2, ..., n_k) = 1$, sie heißen "paarweise teilerfremd"wenn je zwei der Zahlen $n_1, n_2, ..., n_k$ zueinander teilerfremd sind.

3.4 Euklidischer Algorithmus

(50) Gesucht ist ein Verfahren zur Bestimmung des ggT zweier natürlicher Zahlen n_1 und n_2 (Euklidischer Algorithmus).

Beispiele:
a) $n_1 = 196$, $n_2 = 91$; b) $n_1 = 297$, $n_2 = 140$
c) $n_1 = 1632$, $n_2 = 833$; d) $n_1 = 2744$, $n_2 = 675$.

Lösung:
Es sei angenommen, dass $n_1 > n_2$. Man denkt sich den beiden natürlichen Zahlen n_1 und n_2 Strecken auf dem Zahlenstrahl zugeordnet.
Es wird nun ein solches Vielfaches der Strecke n_2 auf der Strecke n_1 abgetragen, dass ein Rest $R_1 < n_2$ übrig bleibt. Nun werden die Strecken n_2 und R_1 auf dem Zahlenstrahl aufgetragen, und von der Strecke n_2 wird ein solches Vielfaches der Strecke R_1 subtrahiert, dass ein Rest R_2 bleibt mit $R_2 < R_1$.

Man setzt das Verfahren fort und trägt schließlich die Strecken R_k und R_{k+1} auf dem Zahlenstrahl ab ($R_{k+1} < R_k$). Man subtrahiert von R_k wiederum ein Vielfaches der Strecke R_{k+1} und erhält den Rest R_{k+2} mit $R_{k+2} < R_{k+1}$.

Bei den Zahlen n_1, n_2 und R_k handelt es sich um ganze positive Zahlen, so dass bei Fortsetzung des Verfahrens der Wert 0 erreicht wird. Irgendwann muss R_n Teiler von R_{n-1} sein. Eventuell muss das Verfahren fortgesetzt werden, bis $R_n = 1$ sicher Teiler des vorhergehenden Restes, einer positiven ganzen Zahl, wird.
Der letzte Rest R_n ist in jedem Fall ggT der natürlichen Zahlen n_1 und n_2. Es gilt

$$\begin{aligned}
R_{n-1} &= k_1 \cdot R_n \\
R_{n-2} &= k_2 \cdot R_{n-1} + R_n = k_1 \cdot k_2 \cdot R_n + R_n = k_3 \cdot R_n \\
R_{n-3} &= k_4 \cdot R_{n-2} + R_{n-1} = k_4 \cdot k_3 \cdot R_n + k_1 \cdot R_n = k_5 \cdot R_n \\
&... \\
n_2 &= k_i \cdot R_1 + R_2 = k_j \cdot R_n \\
n_1 &= k_l \cdot n_2 + R_1 = k_i \cdot k_j \cdot R_n + R_1 = k \cdot R_n
\end{aligned}$$

Beispiele:
a) $n_1 = 196$, $n_2 = 91$.
Man denkt sich die Strecken $n_1 = 196$ und $n_2 = 91$ aufgetragen und subtrahiert das Zweifache der Strecke n_2 von n_1

$$n_1 - 2n_2 = 196 - 2 \cdot 91 = 14 = R_1$$

Man denkt sich die Strecken $n_2 = 91$ und $R_1 = 14$ aufgetragen und subtrahiert das Sechsfache der Strecke R_1 von n_2.

$$n_2 - 6R_1 = 91 - 6 \cdot 14 = R_2 = 7$$

Da $R_2 = 7$ Teiler von $R_1 = 14$ ist, erhalten wir $d = (196, 91) = 7$.

b) $n_1 = 297$, $n_2 = 140$.
$n_1 - 2n_2 = 297 - 2 \cdot 140 = R_1 = 17$,
$n_2 - 8R_1 = 140 - 8 \cdot 17 = R_2 = 4$,
$R_1 - 4R_2 = 17 - 4 \cdot 4 = R_3 = 1$, $d = (297, 140) = 1$.
Die Zahlen $n_1 = 297$ und $n_2 = 140$ sind teilerfremd oder prim zueinander.

c) $n_1 = 1632$, $n_2 = 833$.
Wir lösen uns von der geometrischen Anschauung und schreiben kurz

$$1632 = 833 \cdot 1 + 799; \qquad 833 = 179 \cdot 1 + 34; \qquad 799 = 34 \cdot 23 + 17; \qquad 33 = 17 \cdot 2 + 0$$

$d = (1632, 833) = 17$. Oder noch kürzer:

$$d = (1632, 833) = (833, 799) = (799, 34) = (34, 17) = 17$$

d) $n_1 = 2744$, $n_2 = 675$.

$$2744 = 675 \cdot 4 + 44; \qquad 675 = 44 \cdot 15 + 15; \qquad 4 = 15 \cdot 2 + 14; \qquad 15 = 14 \cdot 1 + 1;$$

$$14 = 1 \cdot 14 + 0 \qquad , \qquad d = (2744, 6755) = 1$$

Oder kürzer:

$$d = (2744, 675) = (675, 44) = (44, 15) = (15, 14) = (14, 1) = 1$$

Bemerkung: Das hier angegebene Rechenverfahren (Algorithmus) zur Bestimmung des ggT stammt von Euklid.
Es ist bei diesem Verfahren oft angebracht, negative Reste einzuführen, falls diese ein Rechnen mit kleineren Zahlen zur Folge haben.

Für die Aufgaben c) und d) würde sich ergeben:
c) $n_1 = 1632$, $n_2 = 833$.

$$1632 = 833 \cdot 2 - 34; \qquad 833 = 34 \cdot 24 + 17; \qquad 3 = 17 \cdot 2$$

$d = (1632, 833) = 17$. Oder kürzer: $d = (1632, 833) = (833, 34) = (34, 17) = 17$.

d) $d = (2744, 675) = (675, 44) = (44, 15) = (15, 1) = 1$.

Durch analoge Überlegung gelangt man zu einem Verfahren zur Bestimmung des ggT von k natürlichen Zahlen ($k > 2$). Es sollen hier nur zwei Beispiele angeschlossen werden.

$$d = (750, 330, 336) = (330, 90, 6) = (6, 0, 0) = 6$$
$$d = (396, 286, 156, 108) = (108, 36, 38, 48) = (36, 0, 12, 2) = (2, 0, 0, 0) = 2$$

(51)• Man bestimme den ggT der Zahlen
a) $n_1 = 41275$, $n_2 = 4572$
b) $n_1 = 5661$, $n_2 = 5291$, $n_3 = 4292$
c) $n_1 = 7576$, $n_2 = 6591$, $n_3 = 4913$
d) $n_1 = 325104$, $n_2 = 221946$, $n_3 = 90654$, $n_4 = 53142$
e) $n_1 = 2125$, $n_2 = 1716$, $n_3 = 1534$, $n_4 = 1213$.

(52) Es ist zu zeigen: Das Produkt aus dem ggT und dem kgV zweier natürlicher Zahlen n_1 und n_2 ist gleich dem Produkt dieser beiden Zahlen. Oder:

$$d \cdot m = (n_1, n_2) \cdot [n_1, n_2] = n_1 \cdot n_2$$

Lösung: Die Produktdarstellungen in Primzahlpotenzen der beiden gegebenen Zahlen seien (Vgl. Aufgabe (36))

$$n_1 = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot ... \cdot p_r^{\alpha_r} \qquad , \qquad n_2 = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdot ... \cdot p_s^{\beta_s}, \qquad r \leq s$$

Es gilt

$$m = p_1^{\gamma_1} \cdot p_2^{\gamma_2} \cdot ... \cdot p_s^{\gamma_s} \qquad , \qquad d = p_1^{\delta_1} \cdot p_2^{\delta_2} \cdot ... \cdot p_r^{\delta_r} \qquad \text{(Vgl. Aufgabe (48) und (49))}$$

Damit wird das Produkt

$$d \cdot m = p_1^{\gamma_1+\delta_1} \cdot p_2^{\gamma_2+\delta_2} \cdot ... \cdot p_r^{\gamma_r+\delta_r} \cdot p_{r+1}^{\gamma_{r+1}} \cdot ... \cdot p_s^{\gamma_s} \qquad \text{und}$$
$$n_1 \cdot n_2 = p_1^{\alpha_1+\beta_1} \cdot p_2^{\alpha_2+\beta_2} \cdot ... \cdot p_r^{\alpha_r+\beta_r} \cdot p_{r+1}^{\beta_{r+1}} \cdot ... \cdot p_s^{\beta_s}$$

Für $\alpha_i < \beta_i$ ist $\gamma_i = \beta_i$ und $\delta_i = \alpha_i$
Für $\alpha_i > \beta_i$ ist $\gamma_i = \alpha_i$ und $\delta_i = \beta_i$
Die Summe $\alpha_i + \beta_i$ ist also in jedem Fall gleich der Summe $\gamma_i + \delta_i$, was zu zeigen war.

Bemerkung: Mit Hilfe des Satzes in Aufgabe (52) ist die Bestimmung des kgV über den Euklidischen Algorithmus möglich. Als Beispiel soll die Bestimmung des kgV der Zahlen $n_1 = 714$ und $n_2 = 476$ angeschlossen werden.

$$d = (714, 476) = (476, 238) = (238, 0) = 238 \qquad , \qquad m = \frac{n_1 \cdot n_2}{d} = \frac{714 \cdot 476}{238} = 1428$$

(53) Zu bestimmen ist das kgV der Zahlen $n_1 = 459$, $n_2 = 306$, $n_3 = 235$, $n_4 = 204$.

Lösung:
Zunächst bestimmt man die ggT der Zahlen n_1 und n_2 und der Zahlen n_3 und n_4.

$$d_{12} = (459, 306) = (306, 153) = (153, 0) = 153$$
$$d_{34} = (255, 204) = (204, 51) = (51, 0) = 51$$

Aus d_{12} und d_{34} lassen sich die kgV der entsprechenden Zahlen ermitteln

$$m_{12} = \frac{459 \cdot 306}{153} = 918 \qquad , \qquad m_{34} = \frac{255 \cdot 204}{51} = 1020$$

Es folgt $d = (1020, 918) = (918, 102) = (102, 0) = 102$.
Damit wird das kgV der 4 gegebenen natürlichen Zahlen

$$m = [459, 306, 255, 204] = \frac{1020 \cdot 918}{102} = 9180$$

(54)• Man bestimme das kgV der Zahlen
a) $n_1 = 1554$, $n_2 = 666$
b) $n_1 = 831$, $n_2 = 137$
c) $n_1 = 4891$, $n_2 = 4221$, $n_3 = 1407$,
d) $n_1 = 7612$, $n_2 = 3114$, $n_3 = 1903$, $n_4 = 1038$,
e) $n_1 = 19224$, $n_2 = 3204$, $n_3 = 2403$, $n_4 = 1068$, $n_5 = 712$.

(55) Gegeben sind zwei natürliche Zahlen n_1 und n_2 sowie ihr ggT $d = (n_1, n_2)$. Gesucht wird der ggT d^* der Ausdrücke $z_1 = x_1 \cdot n_1 + y_1 \cdot n_2$ und $z_2 = x_2 \cdot n_1 + y_2 \cdot n_2$.
x_k und y_k sind beliebige ganze Zahlen.

Beispiel:
$n_1 = 792$, $x_1 = 71$, $y_1 = 21$, $n_2 = 462$, $x_2 = 28$, $y_2 = -5$.

Lösung:
Nach Voraussetzung ist d Teiler von n_1 und von n_2. Also gilt: $n_1 = ad$ und $n_2 = bd$ (a, b ganzzahlig). Damit wird

$$\begin{aligned} z_1 &= (ax_1 + by_1) \cdot d = k_1 \cdot d \\ z_2 &= (ax_2 + by_2) \cdot d = k_2 \cdot d \\ d^* &= (z_1, z_2) = (k_1 \cdot d, k_2 \cdot d) = k \cdot d, \quad \text{wobei } k = (k_1, k_2) \text{ ist} \end{aligned}$$

Ergebnis: Der ggT der Zahlen z_1 und z_2 ist ein Vielfaches des ggT der Zahlen n_1 und n_2.

Beispiel:
$d = (792, 462) = (462, 330) = (330, 132) = (132, 66) = 66$
$z_1 = 7 \cdot 792 + 21 \cdot 462 = 15246$
$z_2 = 28 \cdot 792 - 5 \cdot 462 = 19866$
$d^* = (z_1, z_2) = (19866, 15246) = (15246, 4620) = (4620, 1386) = (1386, 462) = (462, 0) = 462 = 7 \cdot 66$

Bemerkung: Der Ausdruck $z = xn_1 + yn_2$ (x, y beliebige ganze Zahlen) heißt "Linearkombination" der Zahlen n_1 und n_2. Die Menge aller Linearkombinationen der Zahlen n_1 und n_2 bildet einen Ring mit der üblichen Addition und Multiplikation dieser Zahlen als Verknüpfung, nämlich den Ring der durch d teilbaren Zahlen.
d ist die kleinste positive Zahl dieses Ringes. Durch analoge Betrachtung erhält man das gleiche Ergebnis für die Linearkombinationen von drei und mehr natürlichen Zahlen.

Umgekehrt lässt sich jede Zahl des Ringes in der Form $z = xn_1 + yn_2$ darstellen, wobei x und y ganze Zahlen sind.

4 Das Rechnen mit Kongruenzen

4.1 Einführung, Definition

(56) Gegeben sind die voneinander verschiedenen natürlichen Zahlen n_1 und n_2. Gesucht wird eine notwendige und hinreichende Bedingung dafür, dass die Zahlen n_1 und n_2 bei der Division durch eine bestimmte natürliche Zahl m denselben Rest R lassen.

Lösung:
Wenn n_1 und n_2 bei der Division durch m den Rest R lassen, so gilt

$$n_1 = k_1 \cdot m + R, \quad R < n_1 \qquad ; \qquad n_2 = k_2 \cdot m + R, \quad R < n_2 \quad \text{mit } k_1 \neq k_2$$

Durch Subtraktion ergibt sich

$$n_1 - n_2 = m \cdot (k_1 - k_2) = m \cdot k$$

Die Differenz der gegebenen Zahlen n_1 und n_2 ist durch m teilbar. Ist nun die Differenz zweier natürlicher Zahlen n_1 und n_2 durch m teilbar, so gilt $n_1 - n_2 = m \cdot k$.
Angenommen, n_2 lasse bei der Division durch m den Rest R, also $n_2 = k' \cdot m + R$. Für n_1 gilt dann:

$$n_1 = mk + n_2 = mk + mk' + R = m(k + k') + R$$

Die Zahlen n_1 und n_2 lassen bei der Division durch m denselben Rest R.

Ergebnis: Zwei natürliche Zahlen n_1 und n_2 lassen bei der Division durch m genau dann denselben Rest R, wenn ihre Differenz durch m teilbar ist.

Definition: Zwei ganze Zahlen a und b, die bei der Division durch m den selben Rest lassen, heißen "kongruent" nach dem "Modul" m.

Als Zeichen verwenden wir $a \equiv b$ mod m (a kongruent b modulo m) oder kurz $a \equiv b(m)$.

Wir bezeichnen die Gesamtheit aller ganzen Zahlen, die modulo m denselben Rest lassen, als eine Restklasse.

Beispiel:
Die Zahlen 9, 23, 51, 79, 93 gehören modulo 7 alle derselben Restklasse an, sie sind alle kongruent modulo 7, weil sie bei der Division durch 7 alle denselben Rest R= 2 lassen. Es gilt:

$$9 \equiv 23 \equiv 51 \equiv 79 \equiv 93 \equiv 2 \pmod 7$$

Die Differenzen je zweier der angegebenen Zahlen sind stets durch $m = 7$ teilbar.

(57) Welche der Zahlen $n_1 = 11$, $n_2 = 17$, $n_3 = 27$, $n_4 = 81$, $n_5 = 61$, $n_6 = 66$ sind nach dem Modul 7 (10, 13, 17) untereinander kongruent?

Lösung:

$11 \equiv 4 \bmod 7$	$11 \equiv 1 \bmod 10$	$11 \equiv 11 \bmod 13$	$11 \equiv 11 \bmod 17$
$17 \equiv 3 \bmod 7$	$17 \equiv 7 \bmod 10$	$17 \equiv 4 \bmod 13$	$17 \equiv 0 \bmod 17$
$27 \equiv 6 \bmod 7$	$27 \equiv 7 \bmod 10$	$27 \equiv 1 \bmod 13$	$27 \equiv 10 \bmod 17$
$81 \equiv 4 \bmod 7$	$81 \equiv 1 \bmod 10$	$81 \equiv 3 \bmod 13$	$81 \equiv 13 \bmod 17$
$61 \equiv 5 \bmod 7$	$61 \equiv 1 \bmod 10$	$61 \equiv 9 \bmod 13$	$61 \equiv 10 \bmod 17$
$66 \equiv 3 \bmod 7$	$66 \equiv 6 \bmod 10$	$66 \equiv 1 \bmod 13$	$66 \equiv 15 \bmod 17$
$11 \equiv 81 \equiv 4 \bmod 7$	$11 \equiv 81 \equiv 61 \equiv 1 \bmod 10$	$17 \equiv 66 \equiv 3 \bmod 7$	$17 \equiv 27 \equiv 7 \bmod 10$
$27 \equiv 66 \equiv 1 \bmod 13$	$27 \equiv 61 \equiv 10 \bmod 17$		

Bemerkung: $a \equiv 0 \bmod m$ bedeutet, dass a durch m teilbar ist. Alle durch m teilbaren Zahlen gehören derselben Restklasse an, $k \cdot m \equiv 0 \bmod m$.
Als nicht negative Reste $R < m$ kommen $0, 1, 2, 3, ..., (m-1)$ modulo m in Frage. Das sind genau m Elemente als Vertreter für die einzelnen Restklassen.

4.2 Addition, Subtraktion, Multiplikation, Rechenkontrollen

(58) Man zeige: Aus $a \equiv b \bmod m$ und $c \equiv d \bmod m$ folgt

$$a + c \equiv b + d \bmod m$$

Lösung:
Aus $a \equiv b \bmod m$ und $c \equiv d \bmod m$ folgt $a = k_1 \cdot m + b$ und $c = k_2 \cdot m + d$. Durch Addition ergibt sich die Behauptung

$$a + c = (k_1 + k_2) \cdot m + b + d = k \cdot m + b + d \quad \text{oder} \quad a + c \equiv b + d \bmod m$$

Ergebnis: Die Summe der Reste zweier Zahlen bei der Division durch m ist kongruent dem Rest, den die Summe dieser Zahlen bei der Division durch m lässt.

Oder: Die Differenz aus der Summe zweier Zahlen a und b und der Summe der Reste, die diese Zahlen bei der Division durch m lassen, ist durch m teilbar.

Beispiele:
$57 \equiv 6 \bmod 17$, $121 \equiv 2 \bmod 17$, $57 + 121 = 178 \equiv 8 \bmod 17$
$6 + 2 \equiv 8 \bmod 17$, $8 \equiv 8 \bmod 17$.
$98 \equiv 10 \bmod 11$, $64 \equiv 9 \bmod 11$, $98 + 64 = 162 \equiv 8 \bmod 11$.
$10 + 9 = 19 \equiv 8 \bmod 11$, $8 \equiv 8 \bmod 11$.

Bemerkung: Zur Überprüfung der Rechnung bei größeren Summen kann der hier hergeleitete Satz angewendet werden. Bei richtiger Rechnung muss die Summe der Reste der Summanden bei der Division durch eine beliebige Zahl m mit dem Rest der Summe bei der Division durch die gleiche Zahl m übereinstimmen bis auf evtl. ein Vielfaches von m.
Man vergleiche die in Aufgabe (90) behandelte Neuner- und Elferprobe.

(59) Man überprüfe die Summe der Zahlen

$$387 + 1437 + 2093 + 4618 + 517 + 1632 + 971 = 11655$$

mod 7, mod 9 und mod 11.

Lösung:

$387 \equiv 2 \bmod 7$	$387 \equiv 0 \bmod 9$	$387 \equiv 2 \bmod 11$
$1437 \equiv 2 \bmod 7$	$1437 \equiv 6 \bmod 9$	$1437 \equiv 7 \bmod 11$
$2093 \equiv 0 \bmod 7$	$2093 \equiv 5 \bmod 9$	$2093 \equiv 3 \bmod 11$
$4618 \equiv 5 \bmod 7$	$4618 \equiv 1 \bmod 9$	$4618 \equiv 9 \bmod 11$
$517 \equiv 6 \bmod 7$	$517 \equiv 4 \bmod 9$	$517 \equiv 0 \bmod 11$
$1632 \equiv 1 \bmod 7$	$1632 \equiv 3 \bmod 9$	$1632 \equiv 4 \bmod 11$
$971 \equiv 5 \bmod 7$	$971 \equiv 8 \bmod 9$	$971 \equiv 3 \bmod 11$
$11655 \equiv 0 \bmod 7$	$11655 \equiv 0 \bmod 9$	$11655 \equiv 6 \bmod 11$

Die Summen der Reste sind $21 \equiv 0 \bmod 7$, $27 \equiv 0 \bmod 9$, $28 \equiv 6 \bmod 11$.
Die Proben stimmen, es ist deshalb anzunehmen, dass die gegebene Summe richtig berechnet wurde.

(60) Man zeige: Aus $a \equiv b \bmod m$ und $c \equiv d \bmod m$ folgt

$$a - c \equiv b - d \bmod m$$

Lösung:
Bei der Subtraktion $a - c = x$ wird diejenige Zahl x gesucht, die, zu c addiert, die Zahl a ergibt, In der Kongruenz $a - c \equiv x \bmod m$ kann x auch negativ sein. Durch Addition eines Vielfachen des Moduls m erhält man dann den positiv kleinsten Rest.

Aus $a \equiv b \bmod m$ und $c \equiv d \bmod m$ folgt $a = k_1 \cdot m + b$ und $b = k_2 \cdot m + d$. Durch Subtraktion ergibt sich die Behauptung

$$a - c = (k_1 - k_2) \cdot m + b - d = k \cdot m + b - d \quad \text{oder} \quad a - c \equiv b - d \bmod m$$

Falls $b < d$, so addiert man zum Ergebnis den Modul m.
Ergebnis: Die Differenz der Reste zweier Zahlen bei der Division durch m ist kongruent dem Rest, den die Differenz dieser Zahlen bei der Division durch m lässt.

Beispiele:
$19 \equiv 5 \bmod 7$, $16 \equiv 2 \bmod 7$, $19 - 16 \equiv 3 \bmod 7$.
$5 - 2 \equiv 3 \bmod 7$, $3 \equiv 3 \bmod 7$.
$87 \equiv 2 \bmod 17$, $63 \equiv 12 \bmod 17$, $87 - 63 = 24 \equiv 7 \bmod 17$.
$2 - 12 \equiv -10 \equiv -10 + 17 \equiv 7 \bmod 17$, $7 \equiv 7 \bmod 17$.

Bemerkung: Nach den Aufgaben (58) und (60) können die Überprüfungen von Rechenergebnissen jetzt auf Summen und Differenzen ausgedehnt werden. Man vergleiche die Bemerkung in Aufgabe (58).

(61) Man zeige: Aus $a \equiv b \bmod m$ und $c \equiv d \bmod m$ folgt

$$ac \equiv bd \bmod m$$

Lösung:
Aus $a \equiv b \bmod m$ und $c \equiv d \bmod m$ folgt $a = k_1 \cdot m + b$ und $c = k_2 \cdot m + d$. Durch Multiplikation ergibt sich die Behauptung

$$ac \equiv (k_1 m + b)(k_2 m + d) = (k_1 k_2 m + d k_1 + b k_2) \cdot m + bd \quad \text{oder } ac \equiv bd \bmod m$$

Ergebnis: Das Produkt der Reste zweier Zahlen bei der Division durch m ist kongruent dem Rest, den das Produkt dieser Zahlen bei der Division durch m lässt.

Beispiele:
$27 \equiv 1 \bmod 13$, $43 \equiv 4 \bmod 13$, $27 \cdot 43 = 1161 \equiv 4 \bmod 13$.
$1 \cdot 4 \equiv 4 \bmod 13$, $4 \equiv 4 \bmod 13$.
$49 \equiv 4 \bmod 5$, $2 \equiv 2 \bmod 5$, $49 \cdot 82 = 40188 \equiv 3 \bmod 5$.
$4 \cdot 2 = 8 \equiv 3 \bmod 5$, $3 \equiv 3 \bmod 5$.

Bemerkung: Die Überprüfungen von numerischen Rechnungen können nun auch auf Multiplikationen ausgedehnt werden. Alle Rechnungen, in denen Additionen, Subtraktionen und Multiplikationen enthalten sind, können modulo m überprüft werden.

Führt man die angegebenen Rechenoperationen mit den Resten modulo m (m beliebig) aus, so erhält man ein Ergebnis, das bei richtiger Rechnung dem angegebenen Ergebnis modulo m kongruent sein muss.

Man beachte: Die genannten Überprüfungen gelten im allgemeinen nicht für Divisionen. Darauf wird in Aufgabe (105) eingegangen werden, Man beachte auch den Hinweis in Aufgabe (90), wonach bei richtiger Probe angenommen werden darf, dass die Rechnung richtig ist, wonach bei falscher Probe jedoch sicher ein Fehler in der Rechnung enthalten ist.

(62) Man überprüfe die Richtigkeit der Berechnung

$$12536^2 - 153 \cdot 6483 + 27333^2 = 904252286$$

mod 7, mod 9 und mod 11.

Lösung:
$12536 \equiv 6 \bmod 7$, $153 \equiv 6 \bmod 7$, $6483 \equiv 1 \bmod 7$, $27333 \equiv 5 \bmod 7$
$90425228 \equiv 0 \bmod 7$, $36 - 6 + 25 \equiv 6 \bmod 7$.

Schon die Probe modulo 7 führt zu unterschiedlichen Ergebnissen, es ist mit Sicherheit ein Fehler in der Rechnung enthalten. Auf die weiteren Proben modulo 9 und modulo 11 kann also verzichtet werden.

(63) Man zeige: Aus $a \equiv b \bmod m$ und $n > 0$ folgt $a^n \equiv b^n \bmod m$.

Lösung:
Aus $a \equiv b \bmod m$ folgt $a = km + b$. Durch Potenzieren mit dem Exponenten n ergibt sich die Behauptung

$$\begin{aligned} a^n &= (km+b)^n \\ &= \left(k^n m^{n-1} + \binom{n}{1} k^{n-1} m^{n-2} b + \ldots + \binom{n}{k} k^{n-k} m^{n-k-1} b^k + \ldots + k b^{n-1}\right) \cdot m + b^n \end{aligned}$$

oder $a^n \equiv b^n \bmod m$.

Ergebnis: Der Rest einer Potenz bei der Division durch m ist kongruent der Potenz des Restes der Basis unter Beibehaltung des Exponenten.

Beispiele:
$4 \equiv 1 \bmod 3$, $4^6 = 4096 \equiv 1 \bmod 3$, $1^6 \equiv 1 \bmod 3$, $1 \equiv 1 \bmod 3$
$7 \equiv 3 \mod 4$, $7^3 = 343 \equiv 3 \bmod 4$, $3^3 = 27 \equiv 3 \bmod 4$, $3 \equiv 3 \bmod 4$.

(64) Gegeben ist der Ausdruck

$$123^6 - 27^8 = 3180396455208$$

Man überprüfe das Ergebnis durch Proben mod 7, mod 9 und mod 11.

Lösung:
$123 \equiv 4 \bmod 7$, $4^2 = 16 \equiv 2 \bmod 7$, $4^6 \equiv 2^3 \equiv 1 \bmod 7$, $27 \equiv 6 \bmod 7$, $6^2 = 36 \equiv 1 \bmod 7$, $6^8 \equiv 1 \bmod 7$.
$1 - 1 \equiv 0 \bmod 7$, $3180396455208 \equiv 0 \bmod 7$.

$123 \equiv 6 \bmod 9$, $6^2 = 36 \equiv 0 \bmod 9$, $6^6 \equiv 0 \bmod 9$, $27 \equiv 0 \bmod 9$, $27^8 \equiv 0 \bmod 9$, $3180396455208 \equiv 0 \bmod 9$.

$123 \equiv 2 \bmod 11$, $2^6 = 64 \equiv 9 \bmod 11$, $25 \equiv 5 \bmod 11$, $5^2 \equiv 3 \bmod 11$, $5^4 \equiv 9 \bmod 11$, $5^8 \equiv 4 \bmod 11$,
$9 - 4 = 5 \equiv 0 \bmod 11$, $3180396455208 \equiv 5 \bmod 11$.

Die Proben mod 7, mod 9 und mod 11 liefern für beide Seiten der gegebenen Gleichung die gleichen Ergebnisse. Es ist demnach anzunehmen, dass der gegebene Ausdruck richtig berechnet wurde.

(65) Man berechne den Ausdruck

$$z = (11^3 + 7^5)^4 - 427^{19}(47^5 - 132^3)^7$$

a) mod 17, b) mod 19, c) mod 23.

Lösung:

a)
$11^2 \equiv 2 \bmod 17$ $11^3 \equiv 5 \bmod 17$ $7^2 \equiv -2 \bmod 17$ $7^4 \equiv 4 \bmod 17$
$7^5 \equiv 11 \bmod 17$ $427 \equiv 2 \bmod 17$ $427^4 \equiv -1 \bmod 17$ $427^{16} \equiv 1 \bmod 17$
$427^{19} \equiv 8 \bmod 17$ $47 \equiv -4 \bmod 17$ $47^2 \equiv -1 \bmod 17$ $47^5 \equiv -4 \bmod 17$
$-4 \equiv 13 \bmod 17$ $132 \equiv -4 \bmod 17$ $132^2 \equiv -1 \bmod 17$ $132^3 \equiv 4 \bmod 17$

$(11^3 + 7^5)^4 \equiv (-1)^4 \equiv 1 \bmod 17$; $427^{19}(47^5 - 132^3)^7 \equiv -3 \bmod 17$; $z \equiv 4 \bmod 17$

b)
$11^2 \equiv 7 \bmod 19$ $11^3 \equiv 1 \bmod 19$ $7^2 \equiv 11 \bmod 19$ $7^4 \equiv 4 \bmod 19$
$7^5 \equiv 11 \bmod 19$ $427 \equiv 11 \bmod 19$ $427^4 \equiv 11 \bmod 19$ $427^{16} \equiv 11 \bmod 19$
$427^{19} \equiv 11 \bmod 19$ $47 \equiv 9 \bmod 19$ $47^2 \equiv 5 \bmod 19$ $47^5 \equiv -3 \bmod 19$
$132 \equiv -1 \bmod 19$ $132^3 \equiv -1 \bmod 19$

$(11^3 + 7^5)^4 \equiv (-7)^4 \equiv 7 \bmod 19$; $427^{19}(47^5 - 132^3)^7 \equiv 14 \bmod 19$; $z \equiv 12 \bmod 19$

c)
$11^2 \equiv 6 \bmod 23$ $11^3 \equiv -3 \bmod 23$ $7^2 \equiv 3 \bmod 23$ $7^5 \equiv -6 \bmod 23$
$427 \equiv 13 \bmod 23$ $427^4 \equiv -5 \bmod 23$ $427^{16} \equiv 4 \bmod 23$ $427^{19} \equiv 2 \bmod 23$
$47 \equiv 1 \bmod 23$ $47^5 \equiv 1 \bmod 23$ $132 \equiv -6 \bmod 23$ $132^2 \equiv 13 \bmod 23$
$132^3 \equiv 14 \bmod 23$

$(11^3 + 7^5)^4 \equiv (-9)^4 \equiv 6 \bmod 23$; $427^{19}(47^5 - 132^3)^7 \equiv 5 \bmod 23$; $z \equiv 1 \bmod 23$

(66)• Man berechne

$$z = (18^5 - 7^3)^7 - 31^{16}(44^9 - 3^{10})^5 \bmod 17$$

4.3 Teilbarkeitsaufgaben

(67) Man zeige, dass $z = 43^7 - 87^{13}$ durch 44 teilbar ist.

Lösung:
$z \equiv (-1)^7 - (-1)^{13} \equiv -1 + 1 \equiv 0 \bmod 44$.
z ist durch 44 teilbar.

(68) Es ist zu zeigen, dass $z_n = 174^{2n-1} + 1212 \cdot 1037^{2n+1}$ für jede natürliche Zahl n durch 3633 teilbar ist.

Lösung:
Es gilt die Zerlegung $3633 = 3 \cdot 7 \cdot 173$.
z_n ist durch 3 teilbar, weil sowohl 174 als auch 1212 durch 3 teilbar sind.

$174 \equiv 6 \equiv -1$ mod 5, $1212 \equiv 1$ mod 7, $1037 \equiv 1$ mod 7.
$z_n \equiv (-1)^{2n-1} + 1 \cdot 1^{2n+1} \equiv -1 + 1 \equiv 0$ mod 7, z_n ist durch 7 teilbar.

$174 \equiv 1$ mod 173, $1212 \equiv 1$ mod 173, $1037 \equiv 172 \equiv -1$ mod 173.
$z_n \equiv 1^{2n-1} + 1 \cdot (-1)^{2n+1} \equiv 1 - 1 \equiv 0$ mod 173, z_n ist durch 173 teilbar.

(69)• Man löse die Aufgaben (8) und (9) mit Hilfe von Kongruenzen.

(70) Mit welcher Ziffer enden die Potenzen
a) 6^{343}, b) 3^{1000}, c) 2^{999} ?

Lösung:
a) Jede Potenz der Zahl 6 endet wiederum mit der Ziffer 6. Speziell gilt: $6^{343} \equiv 6$ mod 10.
b) $3^4 \equiv 1$ mod 10, $3^{1000} = (3^4)^{250} \equiv 1$ mod 10
c) $2^4 \equiv 6$ mod 10, $2^{999} = (2^4)^{249} \cdot 2^3 \equiv 6 \cdot 8 \equiv 8$ mod 10.
Im Fall a) endet die gegebene Potenz mit der Ziffer 6, im Fall b) mit der Ziffer 1 und im Fall c) mit der Ziffer 8.

(71) Man bestimme die Reste der Potenzen
a) 2^{147}, b) 3^{500}, c) 4^{701}, d) 5^{100}
bei der Division durch 5, durch 7 und durch 11.

Lösung:
a) $2^2 \equiv -1$ mod 5, $2^{147} = (2^2)^{73} \cdot 2 \equiv (-1) \cdot 2 \equiv 3$ mod 5.
$2^3 \equiv 1$ mod 7, $2^{147} = (2^3)^{49} \equiv 1$ mod 7.
$2^5 \equiv -1$ mod 11, $2^{147} = (2^5)^{29} \cdot 2^2 \equiv (-1) \cdot 4 \equiv 7$ mod 11.

b) $3^2 \equiv -1$ mod 5, $3^{500} \equiv (-1)^{250} \equiv 1$ mod 5.
$3^3 \equiv -1$ mod 7, $3^{500} = (3^3)^{166} \cdot 3^2 \equiv 2$ mod 7.
$3^2 \equiv 9$ mod 11, $3^4 \equiv 4$ mod 11, $3^5 \equiv 1$ mod 11, $3^{500} = (3^5)^{100} \equiv 1$ mod 11.

c) $4 \equiv -1$ mod 5, $4^{701} \equiv -1 \equiv 4$ mod 5.
$4^3 \equiv -1$ mod 7, $4^{701} = (4^3)^{233} \cdot 4^2 \equiv 2$ mod 5.
$4^2 \equiv 5$ mod 11, $4^4 \equiv 3$ mod 11, $4^5 \equiv 1$ mod 11, $4^{701} = (4^5)^{140} \cdot 4 \equiv 4$ mod 11.

d) 5^n und speziell 5^{1001} ist durch 5 teilbar und liefert also bei der Division durch 5 den Rest Null. $5^{1001} \equiv 0$ mod 5.
$5^3 \equiv -1$ mod 7, $5^{1001} = (5^3)^{333} \cdot 5^2 \equiv (-1) \cdot 4 \equiv 3$ mod 7.
$5^2 \equiv 3$ mod 11, $5^4 \equiv -2$ mod 11, $5^5 \equiv 1$ mod 11, $5^{1001} = (5^5)^{200} \cdot 5 \equiv 5$ mod 11.

(72) Welche Möglichkeiten der Zerlegung der Zahl 1 in zwei Faktoren gibt es mod 7, mod 10 und mod 13?

Lösung:
$1 \cdot 1 \equiv 2 \cdot 4 \equiv 3 \cdot 5 \equiv 1$ mod 7
$1 \cdot 1 \equiv 3 \cdot 7 \equiv 9 \cdot 9 \equiv 1$ mod 10
$1 \cdot 1 \equiv 3 \cdot 9 \equiv 4 \cdot 10 \equiv 6 \cdot 11 \equiv 12 \cdot 12 \equiv 1$ mod 13

(73)• Welchen Rest lässt die Potenz $z = 17^{37}$ bei der Division durch 19?

(74) Man zeige, dass 7^n für $n = 1, 2, 3, ...$ in den letzten drei Ziffern periodisch ist. Man gebe die Länge der Periode an.

Lösung:
Mit den Ziffern $0, 1, 2, ..., 9$ lassen sich 1000 voneinander verschiedene Zahlen < 1000 schreiben. Von diesen Zahlen haben jeweils 100 dieselbe Endziffer.
Da bei den Potenzen von 7 nur die Endziffern 7, 9, 3 und 1 auftreten, kommen für die Potenzen von 7 nur höchstens 400 voneinander verschiedene Zahlen < 1000 als letzte 3 Ziffern in Frage. Nach endlich vielen, nach höchstens 400 Schritten kommt man also zu einer Endziffer, die in den letzten 3 Stellen schon einmal auftrat.
Modulo 1000 gilt:

$$\begin{array}{lllll} 7^1 \equiv 7 & 7^2 \equiv 49 & 7^3 \equiv 343 & 7^4 \equiv 401 & 7^5 \equiv 807 \\ 7^6 \equiv 649 & 7^7 \equiv 543 & 7^8 \equiv 801 & 7^9 \equiv 607 & 7^{10} \equiv 249 \\ 7^{11} \equiv 743 & 7^{12} \equiv 201 & 7^{13} \equiv 407 & 7^{14} \equiv 849 & 7^{15} \equiv 943 \\ 7^{16} \equiv 601 & 7^{17} \equiv 207 & 7^{18} \equiv 449 & 7^{19} \equiv 143 & 7^{20} \equiv 1 \\ 7^{21} \equiv 7 & 7^{22} \equiv 49 & 7^{23} \equiv 243 & ... & 7^{r+20k} \equiv 7^r \end{array}$$

(75) Man bestimme die natürliche Zahl n mit $990 < n < 1010$ und $3^n \equiv 69$ mod 100.

Lösung: Modulo 100 gilt ...

$$\begin{array}{lllll} 3^1 \equiv 3 & 3^2 \equiv 9 & 3^3 \equiv 27 & 3^4 \equiv 81 & 3^5 \equiv 43 \\ 3^6 \equiv 29 & 3^7 \equiv 87 & 3^8 \equiv 61 & 3^9 \equiv 83 & 3^{10} \equiv 49 \\ 3^{11} \equiv 47 & 3^{12} \equiv 41 & 3^{13} \equiv 23 & 3^{14} \equiv 69 & 3^{15} \equiv 7 \\ 3^{16} \equiv 21 & 3^{17} \equiv 63 & 3^{18} \equiv 89 & 3^{19} \equiv 67 & 3^{20} \equiv 1 \\ ... & 3^{r+20k} \equiv 3^r & 3^{14+20k} \equiv 69 & & \end{array}$$

$k = 49$, $n = 994$.

(76) Man zeige, dass für alle mit der Ziffer 1 endenden natürlichen Zahlen n gilt: $n^n \equiv n$ mod 100.

Lösung:
Jede zweiziffrige, auf 1 endende natürliche Zahl n hat die Form $n = 10a + 1$.

Behauptung:

$$z' = n^n - n \equiv n(n^{n-1} - 1) \equiv 0 \bmod 100$$

Nach dem binomischen Satz gilt:

$$z' = (10a+1)\left[\binom{n-1}{0}(10a)^{n-1} + \binom{n-1}{1}(10a)^{n-2} + ... + \binom{n-1}{n-2}10a + \binom{n-1}{n-1} - 1\right]$$

Alle Summanden der zweiten Klammer bis auf die letzten drei sind durch 100 teilbar. Damit folgt

$$\begin{aligned} z' &\equiv (10a+1)\left[\binom{n-1}{1}10a + 1 - 1\right] \equiv (10a+1)[(n-1)10a] \\ &\equiv (10a+1)(10a \cdot 10a) \equiv (10a+1)100a^2 \equiv 0 \bmod 100 \qquad \text{q.e.d.} \end{aligned}$$

Bemerkung: $n^n \equiv n$ mod 100 gilt außerdem noch für die folgenden zweiziffrigen Zahlen $n = 16, 25, 36, 49, 56, 57, 75, 76, 93, 96, 99$.

(77)• Man zeige, dass $z_n = 2^n + 1$ für keine natürliche Zahl n die fünfte Potenz einer natürlichen Zahl ist.

(78) Für welche Zahlen m gilt der Satz: Ein Produkt modulo m ist dann und nur dann kongruent Null mod m, wenn ein Faktor kongruent Null ist?

Lösung:
Ist $m = 10$, so kann ein Produkt auch Null sein, wenn keiner der beiden Faktoren gleich Null ist. Zum Beispiel gilt:

$$2 \cdot 5 \equiv 4 \cdot 5 \equiv 6 \cdot 5 \equiv 0 \bmod 10$$

oder $3 \cdot 6 \equiv 0$ mod 9.

Ist m nun Primzahl ($m = p$) und sind a und b Zahlen aus dem Bereich $0, 1, 2, 3, ..., (p-1)$, dann bedeutet $ab \equiv 0$ mod p, dass das Produkt ab in der gewöhnlichen Arithmetik durch p teilbar ist.
Ein Produkt ist aber nur dann durch eine Primzahl teilbar, wenn einer der Faktoren durch p teilbar ist. Da aber sowohl a als auch b die Zahlen $0, 1, ..., (p-1)$, also kleiner als p sind, können a und b nicht durch p teilbar sein. Folglich kann auch das Produkt ab nicht durch p teilbar sein.

$ab \equiv 0$ mod p gilt nur für $a \equiv 0$ mod p oder für $b \equiv 0$ mod p.
Andererseits folgt aus $a \equiv 0$ mod p oder $b \equiv 0$ mod p $ab \equiv 0$ mod p.

Ist $m > 1$ dagegen Nichtprimzahl, so lässt m eine Zerlegung in Primzahlpotenzen zu, und diese Primzahlen liegen im Bereich der Zahlen $2, 3, ..., (m-1)$. Zu jedem Teiler d mit $1 < d < m$ des Moduls m gibt es eine Zahl k mit $k \not\equiv$ mod m, so dass gilt $dk \equiv 0$ mod m.

Beispiel:
$m = 24 = 2^3 \cdot 3 = 8 \cdot 3$.
$3 \cdot 8 \equiv 6 \cdot 8 \equiv 9 \cdot 8 \equiv 12 \cdot 8 \equiv 15 \cdot 8 \equiv 18 \cdot 8 \equiv 21 \cdot 8 \equiv 3 \cdot 16 \equiv 6 \cdot 16 \equiv 9 \cdot 16 \equiv 12 \cdot 16 \equiv 15 \cdot 16 \equiv 18 \cdot 16 \equiv 21 \cdot 16 \equiv 0$ mod 24.

Folgerung: Ist m Nichtprimzahl ($m \neq p$), so gibt es modulo m keine eindeutige Umkehrung der Multiplikation (vgl. Aufgabe (104)). Zum Beispiel würden $x_1 = 2$, $x_2 = 4$ $x_3 = 6$ und $x_4 = 8$ die Kongruenz $5x \equiv 0$ mod 10 befriedigen.
Ist m dagegen Primzahl ($m = p$), so hat die Kongruenz $ax \equiv b$ mod p mit $a \neq 0$ mod p stets eine und nur eine Lösung.

4.4 Tabellen für die Summen, Produkte und Potenzen

(79) Man ordne die Summen je zweier Elemente mod m für $m = 3, 7, 9, 10$ und 11 übersichtlich in Tabellenform an und gebe charakteristische Eigenschaften dieser Tabellen an.
(Wenn wir hier, und im folgenden von den Elementen mod m sprechen, so meinen wir damit die Zahlen $0, 1, 2, ..., (m-1)$, die die Restklassen mod m vertreten.)

Lösung:

$m = 3$

	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

$m=7$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

$m=9$	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

$m=10$	0	1	2	3	4	5	6	7	8	9
0	0	1	2	3	4	5	6	7	8	9
1	1	2	3	4	5	6	7	8	9	0
2	2	3	4	5	6	7	8	9	0	1
3	3	4	5	6	7	8	9	0	1	2
4	4	5	6	7	8	9	0	1	2	3
5	5	6	7	8	9	0	1	2	3	4
6	6	7	8	9	0	1	2	3	4	5
7	7	8	9	0	1	2	3	4	5	6
8	8	9	0	1	2	3	4	5	6	7
9	9	0	1	2	3	4	5	6	7	8

$m=11$	0	1	2	3	4	5	6	7	8	9	10
0	0	1	2	3	4	5	6	7	8	9	10
1	1	2	3	4	5	6	7	8	9	10	0
2	2	3	4	5	6	7	8	9	10	0	1
3	3	4	5	6	7	8	9	10	0	1	2
4	4	5	6	7	8	9	10	0	1	2	3
5	5	6	7	8	9	10	0	1	2	3	4
6	6	7	8	9	10	0	1	2	3	4	5
7	7	8	9	10	0	1	2	3	4	5	6
8	8	9	10	0	1	2	3	4	5	6	7
9	9	10	0	1	2	3	4	5	6	7	8
10	10	0	1	2	3	4	5	6	7	8	9

Charakteristische Merkmale: Jedes Element modulo m tritt in jeder Zeile und in jeder Spalte genau einmal auf. Die Reihenfolge der Elemente ist abgesehen vom Anfangselement in jeder Zeile die gleiche.
Jede neue Zeile entsteht aus der vorhergehenden durch Verschiebung der Elemente um 1 nach links. Es tritt kein Unterschied auf zwischen den Tabellen, in denen m Primzahl ist, im Vergleich zu denen, in denen m Nichtprimzahl ist. Tabellen dieser Art heißen Additionstabellen.

(80)• Man stelle Additionstabellen auf für $m = 6$, $m = 8$, $m = 13$.

(81) Man ordne die Produkte je zweier Elemente mod m für $m = 3, 7, 9, 12$ und 17 in Tabellenform an und nenne charakteristische Eigenschaften dieser Tabellen.

Lösung:

$m=3$	0	1	2
0	0	0	0
1	0	1	2
2	0	2	1

$m=7$	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1

$m=9$	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

$m=12$	0	1	2	3	4	5	6	7	8	9	10	11
0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11
2	0	2	4	6	8	10	0	2	4	6	8	10
3	0	3	6	9	0	3	6	9	0	3	6	9
4	0	4	8	0	4	8	0	4	8	0	4	8
5	0	5	10	3	8	1	6	11	4	9	2	7
6	0	6	0	6	0	6	0	6	0	6	0	6
7	0	7	2	9	4	11	6	1	8	3	10	5
8	0	8	4	0	8	4	0	8	4	0	8	4
9	0	9	6	3	0	9	6	3	0	9	6	3
10	0	10	8	6	4	2	0	10	8	6	4	2
11	0	11	10	9	8	7	6	5	4	3	2	1

$m=17$	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2	0	2	4	6	8	10	12	14	16	1	3	5	7	9	11	13	15
3	0	3	6	9	12	15	1	4	7	10	13	16	2	5	8	11	14
4	0	4	8	12	16	3	7	11	15	2	6	10	14	1	5	9	13
5	0	5	10	15	3	8	13	1	6	11	16	4	9	14	2	7	12
6	0	6	12	1	7	13	2	8	14	3	9	15	4	10	16	5	11
7	0	7	14	4	11	1	8	15	5	12	2	9	16	6	13	3	10
8	0	8	16	7	15	6	14	5	13	4	12	3	11	2	10	1	9
9	0	9	1	10	2	11	3	12	4	13	5	14	6	15	7	16	8
10	0	10	3	13	6	16	9	2	12	5	15	8	1	11	4	14	7
11	0	11	5	16	10	4	15	9	3	14	8	2	13	7	1	12	6
12	0	12	7	2	14	9	4	16	11	6	1	13	8	3	15	10	5
13	0	13	9	5	1	14	10	6	2	15	11	7	3	16	12	8	4
14	0	14	11	8	5	2	16	13	10	7	4	1	15	12	9	6	3
15	0	15	13	11	9	7	5	3	1	16	14	12	10	8	6	4	2
16	0	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

Charakteristische Merkmale: Es liegt Symmetrie der Elemente zur Haupt- und zur Nebendiagonalen (nach Streichen der 1. Zeile und 1. Spalte) vor. Abgesehen von der Zeile Null und der Spalte Null treten in der k-ten Zeile (k-ten Spalte) die Elemente der $(m-k)$-ten Zeile ($[m-k]$-ten Spalte) in umgekehrter Reihenfolge auf.

Ist m Primzahl, so tritt in jeder Zeile und in jeder Spalte jedes Element der Menge $\{0,1,2,...,(m-1)\}$ genau einmal auf.
Ist m Nichtprimzahl, so tritt in jeder Zeile und in jeder Spalte jedes Element der angegebenen Menge nur dann genau einmal auf, wenn die Zeilen- bzw. Spaltennummer zu m teilerfremd ist. Ist die Zeilen- bzw.Spaltennummer Teiler von m,so treten nicht alle Elemente der Menge $\{0,1,2,3,...,(m-1)\}$ in der betreffenden Kolonne auf, die auftretenden Elemente wiederholen sich zyklisch, die Länge des jeweiligen Zyklus ist stets Teiler der Zahl m.
Tabellen dieser Art heißen Multiplikationstabellen.

Folgerung: Für diejenigen Zeilen der Multiplikationstabellen, in denen sich Elemente zyklisch wiederholen, ist eine Umkehrung der Multiplikation, also die Division nicht erklärt, weil sie nicht eindeutig ist oder weil ein Ergebnis nicht existiert.
In der Kongruenz $4x \equiv 8$ mod 12 würden die Werte $x_1 = 2$, $x_2 = 5$, $x_3 = 8$ und $x_4 = 11$ die Kongruenz befriedigen, was der Forderung nach Eindeutigkeit des Ergebnisses widersprechen würde.
Für $4x \equiv 7$ mod 12 gibt es kein x, das die Kongruenz erfüllt.

Ist m Primzahl oder ist m teilerfremd zur betreffenden Zeilennummer, so treten keine Wiederholungen der Elemente auf, jedes Element ist in jeder Zeile genau einmal vertreten. In diesen Fällen wird eine Umkehrung der Multiplikation, also eine Einführung der Division möglich. Die Division wird in diesen Fällen stets und eindeutig ausführbar sein.

Beispiele:
$5x \equiv 4$ mod 12, $x = 8$, weil $5 \cdot 8 \equiv 4$ mod 12.
$9x \equiv 3$ mod 17, $x = 6$, weil $9 \cdot 6 \equiv 3$ mod 17.

Auf die Umkehrung der Multiplikation wird in Aufgabe (104) eingegangen.

(82)• Man stelle Multiplikationstabellen auf für $p = 11$, $m = 18$, $p = 19$.

(83) Man ordne die Potenzen a^k für die Elemente $a \not\equiv 0$ mod m und $k = 1,2,3,...$ für gewisse natürliche Zahlen $m > 2$ in Tabellenform an und nenne charakteristische Eigenschaften dieser

Tabellen.

Lösung: $m = 3$, $a^k \equiv b \bmod 3$.

k	1	2	3	4	5	...
$a = 1$	1	1	1	1	1	...
$a = 2$	2	1	2	1	2	...

$m = 7$, $a^k \equiv b \bmod 7$.

k	1	2	3	4	5	6	7	...
$a = 1$	1	1	1	1	1	1	1	...
$a = 2$	2	4	1	2	4	1	2	...
$a = 3$	3	2	6	4	5	1	3	...
$a = 4$	4	2	1	4	2	1	4	...
$a = 5$	5	4	6	2	3	1	5	...
$a = 6$	6	1	6	1	6	1	6	...

$m = 9$, $a^k \equiv b \bmod 9$.

k	1	2	3	4	5	6	7	8	9	10	11	12	...
$a = 1$	1	1	1	1	1	1	1	1	1	1	1	1	...
$a = 2$	2	4	8	7	5	1	2	4	8	7	5	1	...
$a = 3$	3	0	0	0	0	0	0	0	0	0	0	0	...
$a = 4$	4	7	1	4	7	1	4	7	1	4	7	1	...
$a = 5$	5	7	8	4	2	1	5	7	8	4	2	1	...
$a = 6$	6	0	0	0	0	0	0	0	0	0	0	0	...
$a = 7$	7	4	1	7	4	1	7	4	1	7	4	1	...
$a = 8$	8	1	8	1	8	1	8	1	8	1	8	1	...

$m = 17$, $a^k \equiv b \bmod 17$.

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	...
$a = 1$	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	1	...
$a = 2$	2	4	8	16	15	13	9	1	2	4	8	16	15	13	9	1	...
$a = 3$	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1	...
$a = 4$	4	16	13	1	4	16	13	1	4	16	13	1	4	16	13	1	...
$a = 5$	5	8	6	13	14	2	10	16	12	9	11	4	3	15	7	1	...
$a = 6$	6	2	12	4	7	8	14	16	11	15	5	13	10	9	3	1	...
$a = 7$	7	15	3	4	11	9	12	16	10	2	14	13	6	8	5	1	...
$a = 8$	8	13	2	16	9	4	15	1	8	13	2	16	9	4	15	1	...
$a = 9$	9	13	15	16	8	4	2	1	9	13	15	16	8	4	2	1	...
$a = 10$	10	15	14	4	6	9	5	16	7	2	3	13	11	8	12	1	...
$a = 11$	11	2	5	4	10	8	3	16	6	15	12	13	7	9	14	1	...
$a = 12$	12	8	11	13	3	2	7	16	5	9	6	4	14	15	10	1	...
$a = 13$	13	16	4	1	13	16	4	1	13	16	4	1	13	16	4	1	...
$a = 14$	14	9	7	13	12	15	6	16	3	8	10	4	5	2	11	1	...
$a = 15$	15	4	9	16	2	13	8	1	15	4	9	16	2	13	8	1	...
$a = 16$	16	1	16	1	16	1	16	1	16	1	16	1	16	1	16	1	...

Charakteristische Eigenschaften: Die Potenzen wiederholen sich zyklisch.
Die Länge der Zyklen ist höchstens $(m-1)$. Diese Länge wird aber nur dann erreicht, wenn m Primzahl ist. Für $m = p$ ist die Länge der Zyklen stets Teiler der Zahl $(p-1)$, für mindestens eine Basis a ist die Länge des entsprechenden Zyklus gleich $(p-1)$.
Bei Nichtprimzahlen ist die Länge der Zyklen kleiner als $(m-1)$. Tabellen dieser Art heißen Potenztabellen.

Folgerung: Ist m Primzahl, so gibt es für eine Basis einen Zyklus, der die Länge $(p-1)$ hat, in dem alle auftretenden Elemente voneinander verschieden sind. In diesem Fall ist eine eindeutige

Zuordnung der Exponenten zu den Potenzwerten möglich, weiter besteht in diesem Fall die Möglichkeit der Umkehrung der Potenzrechnung.
Auf logarithmische Tabellen und die Anwendung dieser Tabellen wird in Aufgabe (152) eingegangen.

(84)• Man stelle Potenztabellen auf für $m = 5$, $m = 11$, $m = 13$.

4.5 Teilbarkeitsaufgaben, Teilbarkeitsregeln

(85) Man zeige, dass die Summe $s = \sum_{k=1}^{998} k^3$ durch 999 teilbar ist.

Lösung:

$$s = 1^3 + 2^3 + 3^3 + ... + 498^3 + 499^3 + 500^3 + 501^3 + ... + 997^3 + 998^3$$

Es gilt
$998 \equiv -1$ mod 999, $997 \equiv -2$ mod 999, $996 \equiv -3$ mod 999, ..., $502 \equiv -497$ mod 999, $501 \equiv -498$ mod 999, $500 = -499$ mod 999.

Beim Potenzieren mit ungeraden Exponenten bleiben die negativen Vorzeichen erhalten.

$$s \equiv 1^3 + 2^3 + ... + 498^3 + 499^3 - 499^3 - 498^3 - ... - 2^3 - 1^3 \equiv 0 \bmod 999$$

Folglich ist die Summe $s = \sum_{k=1}^{998} k^3$ durch 999 teilbar.

Es ist eine Verallgemeinerung dieser Aufgabe möglich, wenn man beachtet, dass eine gerade Anzahl von Summanden und ein ungerader Exponent vorhanden sein müssen.

(86) Erhebt man die ersten m natürlichen Zahlen, wobei m gerade ist, in ein und dieselbe ungerade Potenz und addiert alle diese Potenzen, so ist diese Summe durch $(m + 1)$ teilbar. Oder:

$$s = \sum_{k=0}^{m-1} k^r \equiv 0 \bmod m, \qquad \text{falls } m, r \text{ gerade sind}$$

Lösung:

$$s = 1^r + 2^r + ... + \left(\frac{m-1}{2} - 1\right)^r + \left(\frac{m-1}{2}\right)^r + \left(\frac{m-1}{2} + 1\right)^r + \\ + \left(\frac{m-1}{2} + 2\right)^r + ... + (m-2)^r + (m-1)^r$$

$$m - 1 \equiv -1 \bmod m, \qquad m - 2 \equiv -2 \bmod m, ...$$

$$\frac{m-1}{2} + t \equiv -\frac{m+1-2t}{2} \equiv -\left(\frac{m-1}{2} - (t-1)\right) \bmod m$$

$$\frac{m-1}{2} + 2 \equiv -\left(\frac{m-1}{2} - 1\right) \bmod m$$

$$\frac{m-1}{2} + 1 \equiv -\left(\frac{m-1}{2}\right) \bmod m, ...$$

Beim Potenzieren mit dem ungeraden Exponenten r bleibt das negative Vorzeichen erhalten. Für die Summe ergibt sich

$$s \equiv 1^r + 2^r + \left(\frac{m-1}{2} - 1\right)^r + \left(\frac{m-1}{2}\right)^r - \left(\frac{m-1}{2}\right)^r - \left(\frac{m-1}{2} - 1\right)^r - ... - 2^r - 1^r$$
$$\equiv 0 \bmod m$$

Es ist eine weitere Verallgemeinerung dieser Aufgabe möglich:

(87) Potenziert man alle Glieder a_k der speziellen arithmetischen Folge erster Ordnung d, $2d$, $3d$,...., nd bei gerader Gliederanzahl n mit dem gleichen ungeraden Exponenten r und addiert die so erhaltenen Potenzen, so ist die entstehende Summe durch $a_{n+1} = (n+1)d$ teilbar. Oder:

$$s = \sum_{k=1}^{n} (kd)^r \equiv 0 \bmod [(n+1)d]$$

falls n gerade und r ungerade.

Lösung:

$$\begin{aligned} s = d^r + (2d)^r + (3d)^r + ... + \left[\left(\frac{n}{2} - k\right) d\right]^r + ... + \left[\left(\frac{n}{2} + k + 1\right) d\right]^r + ... \\ + [(n-2)d]^r + [(n-1)d]r + (nd)^r \\ nd \equiv nd - (n+1)d \equiv nd - nd - d \equiv -d \bmod [(n+1)d] \\ \left(\frac{n}{2} + k + 1 +\right) d \equiv -\left(\frac{n}{2} - k\right) d \bmod [(n+1)d] \end{aligned}$$

Beim Potenzieren mit einem ungeraden Exponenten bleiben die negativen Vorzeichen erhalten, und es folgt

$$\begin{aligned} s = d^r + (2d)^r + (3d)^r + ... + \left[\left(\frac{n}{2} - 1\right) d\right]^r + \left[\left(\frac{n}{2}\right) d\right]^r - \left[\left(\frac{n}{2}\right) d\right]^r - \left[\left(\frac{n}{2} - 1\right) d\right]^r \\ - ... - (3d)^r - (2d)^r - d^r \equiv 0 \bmod [(n+1)d] \end{aligned}$$

Beispiele:
Die Summe der ersten 50 natürlichen Zahlen ist durch 51 teilbar.

$$\sum_{k=1}^{50} k = 1275 \equiv 0 \bmod 51$$

Die Summe der ersten 20 geraden Zahlen ist durch 42 teilbar.

$$\sum_{k=1}^{20} 2k = 420 \equiv 0 \bmod 42$$

Die Summe der ersten 18 durch 7 teilbaren Zahlen ist durch $19 \cdot 7 = 133$ teilbar.

$$\sum_{k=1}^{18} 7k = 1197 \equiv 0 \bmod 133$$

Die Summe der ersten n durch k teilbaren Zahlen ist bei geradem n durch $k(n+1)$ teilbar.

$$\sum_{j=1}^{n} kj = \frac{n}{2}(2k + [n-1]k) = \frac{nk}{2}(n+1) \equiv 0 \bmod k(n+1)$$

Die Summe der ersten 40 Kubikzahlen ist durch 11 teilbar.

$$\sum_{k=1}^{40} k^3 = 3025 \equiv 0 \bmod 11$$

(88) Man leite eine Regel für die Teilbarkeit durch 9 her.

Lösung:
$10 \equiv 1$ mod 9, $10^n \equiv 1$ mod 9.
Eine Zahl z lässt bei der Division durch 9 denselben Rest wie ihre Quersumme.
Eine Zahl z ist dann und nur dann durch 9 teilbar, wenn ihre Quersumme durch 9 teilbar ist.
34748215 ist nicht durch 9 teilbar, weil die Quersumme $3+4+7+4+8+2+1+5 = 34$ inkongruent Null modulo 9 ist. 134784 ist durch 9 teilbar, da $1+3+4+7+8+4 = 27 \equiv 0$ mod 9.

(89) Man leite eine Regel für die Teilbarkeit durch 11 her.

Lösung:
$10 \equiv -1$ mod 11, $10^{2n} \equiv 1$ mod 11, $10^{2n-1} \equiv -1$ mod 11.
Eine Zahl z lässt bei der Division durch 11 denselben Rest wie ihre alternierende Quersumme.
Eine Zahl ist durch 11 dann und nur dann teilbar, wenn ihre alternierende Quersumme durch 11 teilbar ist.
343546719 ist nicht durch 11 teilbar, weil die alternierende Quersumme $9+7+4+3+3-(1+6+5+4) = 26-16 = 10 \equiv -1 \neq 0$ mod 11.
463882166 ist durch 11-teilbar, weil $6+1+8+3+4-(6+2+8+6) = 22-22 \equiv 0$ mod 11.

(90) Man führe Rechenkontrollen mit Hilfe der Neuner- und Elferprobe durch für die Ausdrücke
a) $54729 \cdot 543 = 29717847$
b) $477773 \cdot 535353 = 255778208869$
c) $67435 \cdot 1234 = 83241790$
d) $47315 \cdot 68205 = 3227911575$.

Lösung:
a) $5+4+7+2+9 = 27 \equiv 0$ mod 9, $5+4+3 = 12 \equiv 3$ mod 9,
$2+9+7+41+7+8+4+7 = 45 \equiv 0$ mod 9.
$9+7+5-2-4 = 15 \equiv 4$ mod 11, $3+5-4 = 4 \equiv 4$ mod 11,
$7+8+1+9-4-7-7-2 \equiv 5$ mod 11.
Neuner- und Elferprobe stimmen[10]. Es ist anzunehmen, dass das Produkt richtig berechnet wurde.

b) $4+7+7+7+3 = 35 \equiv -1$ mod 9,
$5+3+5+3+5+3 = 24 \equiv -3$ mod 9,
$2+5+5+7+7+8+2+0+8+8+6+9 = 67 \equiv$ mod 9.
Schon die Neunerprobe zeigt, dass der gegebene Ausdruck sicher falsch berechnet worden ist.

c) $6+7+4+3+5 = 25 \equiv -2$ mod 9, $1+2+3+4 = 10 \equiv 1$ mod 9, $8+3+2+4+1+7+9 = 34 \equiv 17$ mod 9.
Die Neunerprobe stimmt.
$5+4+6-3-7 = 5 \equiv 5$ mod 11, $4+2-3-1 = 2 \equiv 2$ mod 11, $7+4+3-9-1-2-8 = -6 \equiv 5$ mod 11.
Die Elferprobe zeigt, dass der gegebene Ausdruck falsch berechnet wurde. Es liegt die Vermutung nahe, dass im Ergebnis nur zwei Ziffern miteinander vertauscht wurden, da die Neunerprobe stimmt.
Das richtige Ergebnis ist 83214790.

[10] Siehe Ergebnis von Aufgabe (61)

d) $4+7+3+1+5=20\equiv 2$ mod 9, $6+8+2+5=21\equiv 3$ mod 9, $3+2+2+7+9+1+1+5+7+5=42\equiv 6$ mod 9.
$5+3+4-1-7\equiv 4$ mod 11, $5+2+6-8\equiv 5$ mod 11, $5+5+1+7+2-7-1-9-2-3=-2\equiv 9$ mod 11.
Neuner- und Elferprobe stimmen, und dennoch ist das Ergebnis falsch. Das richtige Ergebnis ist 3227119575.

Bemerkung: Stimmen Neuner- und Elferprobe, so ist es nicht immer sicher, ob die Rechnung richtig ist. Stimmt dagegen eine Probe nicht, so ist der betreffende Ausdruck mit Sicherheit falsch berechnet worden.

(91)• Man überprüfe die folgenden Rechnungen mit Hilfe der Neuner- und der Elferprobe
a) $1683^2+79^4+17^9+23^8=196940644348$
b) $138^2\cdot 21+46^3\cdot 19+37^4\cdot 23=45361311$
c) $2^{10}\cdot 12+3^7\cdot 13+4^6\cdot 17+5^5\cdot 19+6^4\cdot 21=195918$.

(92) Man leite eine Regel für die Teilbarkeit durch 101 her.

Lösung:

$$\begin{aligned} z &= a_0 10^n + a_1 10^{n-1} + a_2 10^{n-2} + ... + a_k 10^{n-k} + ... + a_{n-1}10 + a_n \\ 10^2 &\equiv -1 \bmod 101, \qquad 10^{4k-2} \equiv -1 \bmod 101 \\ 10^4 &\equiv 1 \bmod 101, \qquad 10^{4k} \equiv 1 \bmod 101 \\ z &\equiv (a_n + 10a_{n-1}) - (a_{n-2} + 10a_{n-3}) + (a_{n-3} + 10a_{n-4}) - + ... \bmod 101 \end{aligned}$$

Ist die alternierende Summe der Zweiergruppen einer Zahl z (wobei man mit der Bildung der Zweiergruppen am Ende der Zahl beginnt) durch 101 teilbar, dann ist auch die Zahl z durch 101 teilbar.

Beispiele:
$z_1=397205134673453$ ist nicht durch 101 teilbar, da $z_1\equiv 53-34+67-34+51-20+97-3\equiv 76\not\equiv 0$ mod 101.

$z_2=176358243673006008$ ist durch 101 teilbar, da $z_2\equiv 8-60-73+36-24+58-63+17\equiv 0$ mod 101.

(93) Man zeige, dass die Zahl

$$z=(\underbrace{xxxx...x}_{4n\text{ Ziffern}}-\underbrace{yyyy...y}_{4n\text{ Ziffern}}$$

für alle Ziffern x und y durch 101 teilbar ist.

Lösung:
Die Untersuchung der Ausdrücke in der Klammer mit der Teilbarkeitsregel für 101 liefert sofort das Ergebnis. Gleichziffrige Zahlen mit einer durch 4 teilbaren Stellenzahl sind kongruent Null modulo 101.

$$(v+10v)-(v+10v)+-...+(v+10v)-(v+10v)\equiv 0 \bmod 101$$

Damit wird auch $z\equiv 0$ mod 101.

(94) Man leite eine Regel für die Teilbarkeit durch 37 her.

Lösung:
Jede natürliche Zahl z lässt sich wiederum darstellen durch

$$z = a_0 10^n + a_1 10^{n-1} + a_2 10^{n-2} + ... + a_{n-3} 10^3 + a_{n-2} 10^2 + a_{n-1} 10 + a_n$$

Da $999 = 27 \cdot 37$ ist, gilt:

$$1000 = 10^3 \equiv 1 \bmod 37 \qquad , \qquad 10^{3k} \equiv 1 \bmod 37$$

Damit wird

$$z \equiv (a_n + 10a_{n-1} + 100a_{n-2}) + (a_{n-3} + 10a_{n-4} + 100a_{n-5}) + ... \bmod 37$$

Eine Zahl z ist durch 37 teilbar, wenn die Summe der Dreiergruppen dieser Zahl z durch 37 teilbar ist.
(Unter Dreiergruppen einer Zahl versteht man die dreistelligen Zahlen, in die z zerlegt werden kann, wenn man am Ende der Zahl beginnend jeweils drei Stellen abstreicht.)

Beispiel:
$z = 9387428545$ ist durch 37 teilbar, weil
$z = 545 + 428 + 387 + 9 = 1369 \equiv 369 + 1 \equiv 370 \equiv 0$ mod 37.

(95) Für welche Stellenzahl $n = 7k$ ist die Zahl $z = \underbrace{1111...111}_{n \text{ Ziffern}}$ durch 37 teilbar?

Lösung:
$z'111 \equiv 0$ mod 37, $z'' = c \cdot 111 \equiv 0$ mod 37,
$z = \underbrace{1111...111}_{21 \text{ Ziffern}} \equiv 0$ mod 37.

(96) Man leite eine Regel für die Teilbarkeit durch 13 her.

Lösung:

$$\begin{aligned} z &= a_0 10^n + a_1 10^{n-1} + a_2 10^{n-2} + ... + a_{n-2} 10^2 + a_{n-1} 10 + a_n \\ 10^3 &\equiv -1 \bmod 13, \qquad 10^{6n-3} \equiv -1 \bmod 13 \\ 10^6 &\equiv 1 \bmod 13, \qquad 10^{6n} \equiv 1 \bmod 13 \\ z &\equiv (a_n + 10a_{n-1} + 100a_{n-2}) - (a_{n-3} + 10a_{n-4} + 100a_{n-5}) + - ... \bmod 13 \end{aligned}$$

Eine Zahl z ist durch 13 teilbar, wenn die alternierende Summe der Dreiergruppen der Zahl z durch 13 teilbar ist.

Beispiele:
$z_1 = 37256813477$ ist durch 13 teilbar, da $z_1 \equiv 477 - 813 + 256 - 37 = -117 \equiv 0$ mod 13.

$z_2 = 71026549546$ ist nicht durch 13 teilbar, da $z_2 = 546 - 549 + 26 - 71 = -48 \equiv 0$ mod 13.

Es soll noch eine zweite Regel für die Teilbarkeit durch 13 angegeben werden.

$$z = a_0 10^n + a_1 10^{n-1} + a_2 10^{n-2} + ... + a_{n-2} 10^2 + a_{n-1} 10 + a_n = 10A + a_n$$

Die Differenz der Zahl z und eines Vielfachen von 13 ist genau dann durch 13 teilbar, wenn z durch 13 teilbar ist; 91 ist ein Vielfaches von 13, ebenso das 91fache der letzten Ziffer a_n.

Man reduziert die Zahl z durch Subtraktion des 91fachen der letzten Ziffer und Streichen der letzten Ziffer der Differenz, die stets Null ist und erhält

$$z_1 = \frac{z - 91a_n}{10}$$

z ist genau dann durch 13 teilbar, wenn z_1 durch 13 teilbar ist. Nun wird z_1 analog reduziert usw., bis man einen genügend kleinen Rest R erhält. Ist dieser Rest R durch 13 teilbar, so sind es auch alle z_k und speziell die vorgegebene Zahl z.

Ist $R \equiv 0$ mod 13, so gilt das auch für alle z_k und speziell für die Zahl z. Die Subtraktion des 91fachen der letzten Ziffer und Streichung der letzten Ziffer der Differenz geschieht formal wie folgt:
Man streicht die letzte Ziffer der Zahl z und subtrahiert das 9fache dieser letzten Ziffer von der durch die Streichung erhaltenen Zahl.

$$z = 10A + a_n; \qquad z_1 = A - 9a_n = \frac{10A + a_n - a_n}{10} - 9a_n = \frac{10A + a_n - 91a_n}{10} = \frac{z - 91a_n}{10}$$

Beispiel:
$z = 68343549547$
z ist durch 13 teilbar.

z	$= 68343549547$
	63
z_1	$= 6834354891$
	9
z_2	$= 683435480$
	72
z_3	$= 6834282$
	18
z_4	$= 683410$
	9
z_5	$= 6825$
	45
z_6	$= 637$
	63
R	$= 0$

Bemerkung: Gilt für den Rest R nicht nur $R \equiv 0$ mod 13, sondern sogar $R \equiv 0$ mod 91, so ist z sogar durch 91 teilbar. Die im Beispiel behandelte Zahl z ist durch 91 teilbar. Man vergleiche die in der nächsten Aufgabe angegebene Regel für die Teilbarkeit durch 7.

(97) Man leite eine Regel für die Teilbarkeit durch 7 her.

Lösung:

$$\begin{aligned}
z &= a_0 10^n + a_1 10^{n-1} + a_2 10^{n-2} + ... + a_{n-2} 10^2 + a_{n-1} 10 + a_n \\
10^3 &\equiv -1 \bmod 7, \qquad 10^{6n-3} \equiv -1 \bmod 7 \\
10^6 &\equiv 1 \bmod 7, \qquad 10^{6n} \equiv 1 \bmod 7 \\
z &\equiv (a_n + 10a_{n-1} + 100a_{n-2}) - (a_{n-3} + 10a_{n-4} + 100a_{n-5}) + -... \bmod 7
\end{aligned}$$

Eine Zahl z ist durch 7 teilbar, wenn die alternierende Summe der Dreiergruppen dieser Zahl durch 7 teilbar ist.

Beispiele:
$z_1 = 2420467161$ ist durch 7 teilbar da $z_1 \equiv= 161 - 467 + 420 - 2 \equiv 112 \equiv 0$ mod 7.

$z_2 = 470598141043$ ist durch 7 teilbar, da $z_2 = 13 - 14 + 598 - 470 \equiv 0$ mod 7.

Für z_2 gilt aber außerdem $z_2 = 0$ mod 1001, folglich ist z_2 auch durch 11 und durch 13 teilbar. $(7 \cdot 11 \cdot 13 = 1001)$

Bemerkung: Die angegebenen Regeln für die Teilbarkeit durch 7 und 13 benutzen die Tatsache, dass $1000 \equiv -1$ mod 7 und $1000 \equiv -1$ mod 13 ist.
Da nun $1000 \equiv -1$ mod 1001, so kann die Regel auf alle in der Zahl 1001 enthaltenen Primfaktoren erweitert werden. Es käme hier jedoch nur eine Erweiterung auf die Teilbarkeit durch 11 in Frage, die aber andererseits nicht sinnvoll ist, weil die Teilbarkeit einer Zahl z durch 41 mit Hilfe einer bedeutend einfacheren Regel (Aufgabe (89)) nachgewiesen werden kann.
Es können aber die hier angegebenen Regeln auf alle Primfaktoren erweitert werden, die in den Zahlen $10^n \pm 1$ enthalten sind.

Zum Beispiel gilt für $n = 4$: $10001 = 73 \cdot 137$. $10000 \equiv -1$ mod 73, $10000 \equiv -1$ mod 137.

$$z = (a_n + 10a_{n-1} + 100a_{n-2} + 1000a_{n-3}) - (a_{n-4} + 10a_{n-5} + 100a_{n-6} + 1000a_{n-7}) + -... \mod 10001$$

Beispiel:
$z = 826165485$ ist durch 137 teilbar, weil $z = 5485 - 2616 + 8 \equiv 2877 \equiv 21 \cdot 137 \equiv 0$ mod 137.

Von praktischem Wert sind diese Teilbarkeitsregeln jedoch kaum, da der Nachweis für die Teilbarkeit einer Zahl z durch einen Faktor g durch direkte Division meistens schneller zum Ziel führt.

(98) Es ist die in Aufgabe (96) angegebene zweite Regel für die Teilbarkeit einer Zahl z durch 13 zu verallgemeinern.

Lösung:
Eine Verallgemeinerung dieser Regel ist möglich für alle mit der Ziffer 1 endenden Zahlen k und die in ihnen enthaltenen Primfaktoren p. Soll eine Zahl z auf die Teilbarkeit durch eine Zahl $k = 10a + 1$ oder eine Zahl p mit $p \mid k$ hin untersucht werden, so streicht man die letzte Ziffer von z und subtrahiert das a-fache der letzten Ziffer.
Die so erhaltene Zahl z_1 ist durch k teilbar, wenn z durch k teilbar ist, denn von z wurde das $(10a + 1)$- fache, also das k-fache der letzten Ziffer subtrahiert.

$$z = a_0 10^n + a_1 10^{n-1} + a_2 10^{n-2} + ... + a_{n-2} 10^2 + a_{n-1} 10 + a_n = 10A + a_n$$
$$z_1 = \frac{z - a_n}{10} - a \cdot a_n = \frac{z - (10a + 1)a_n}{10} = \frac{z - ka_n}{10}$$

Ist bei wiederholter Anwendung des Verfahrens der auftretende Rest R durch k oder durch p mit $p \mid k$ teilbar, so ist auch z durch k oder durch p teilbar.

(99) Man untersuche, ob die Zahlen z durch die Primzahlen p teilbar sind

a) $z = 16821588$, $p = 7$ b) $z = 10720353$, $p = 17$ c) $z = 31748569$, $p = 3$
d) $z = 12673182$, $p = 4$ e) $z = 403243$, $p = 61$ f) $z = 28891371$, $p71$
g) $z = 3491906$, $p = 31$

Lösung:
a) $p = 17$, $k = 24$, $a = 2$. $z = 16821588$
b) $p = 17$, $k = 51$, $a = 5$. $z = 10720353$

c) $p = 3$, $k = 3$, $a = 3$. $z = 31748569$
d) $p = 41$, $k = 4$, $a = 4$. $z = 12673182$

$$\begin{array}{r} z = 16821588 \\ \hline 16 \\ \hline z_1 = 1682142 \\ \hline 4 \\ \hline z_2 = 168210 \\ \hline 2 \\ \hline z_3 = 1680 \\ \hline 16 \\ \hline R = 0 \end{array} \qquad \begin{array}{r} z = 10720353 \\ \hline 15 \\ \hline z_1 = 1072020 \\ \hline 10 \\ \hline z_2 = 10710 \\ \hline 5 \\ \hline z_3 = 102 \\ \hline 10 \\ \hline R = 0 \end{array}$$

$$\begin{array}{r} z = 31748569 \\ \hline 27 \\ \hline z_1 = 3174829 \\ \hline 27 \\ \hline z_2 = 317455 \\ \hline 15 \\ \hline z_3 = 31730 \\ \hline 9 \\ \hline z_4 = 308 \\ \hline 24 \\ \hline R \neq 0 \end{array} \qquad \begin{array}{r} z = 12673182 \\ \hline 8 \\ \hline z_1 = 1267310 \\ \hline 4 \\ \hline z_2 = 12669 \\ \hline 36 \\ \hline z_3 = 1230 \\ \hline 12 \\ \hline R = 0 \end{array}$$

a) z ist durch 17 und auch durch 51 teilbar.
b) z ist durch 7 und sogar durch 21 teilbar.
c) z ist nicht durch 31 teilbar.
d) z ist durch 41 teilbar.

e) $p = 61$, $k = 61$, $a = 6$, $z = 21032473$
f) $p = 71$, $k = 17$, $a = 1$. $z = 28899137$
g) $p = 37$, $k = 111$, $a = 11$. $z = 34919046$

$$\begin{array}{r} z = 21032473 \\ \hline 18 \\ \hline z_1 = 2103229 \\ \hline 54 \\ \hline z_2 = 210268 \\ \hline 48 \\ \hline z_3 = 20978 \\ \hline 48 \\ \hline z_4 = 2049 \\ \hline 54 \\ \hline R \neq 0 \end{array} \qquad \begin{array}{r} z = 288991371 \\ \hline 7 \\ \hline z_1 = 28899130 \\ \hline 21 \\ \hline z_2 = 288970 \\ \hline 49 \\ \hline z_3 = 2840 \\ \hline 28 \\ \hline R = 0 \end{array}$$

$$\begin{array}{r} z = 34919046 \\ \hline 66 \\ \hline z_1 = 3491838 \\ \hline 88 \\ \hline z_2 = 349095 \\ \hline 55 \\ \hline z_3 = 34854 \\ \hline 44 \\ \hline z_4 = 3441 \\ \hline 11 \\ \hline z_5 = 333 \\ \hline 33 \\ \hline R = 0 \end{array}$$

e) z ist nicht durch 61 teilbar.
f) z ist durch 71 teilbar.
g) z ist durch 37 und auch durch 111 teilbar.

Bemerkung: Für die praktische Anwendung werden auch diese Teilbarkeitsregeln kaum von Wert sein, da die direkte Division bei annähernd gleichem Zeitaufwand zum Ziel führen wird.

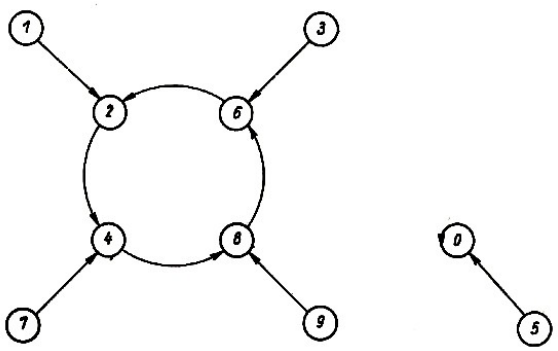
(100)• Man untersuche, welche der folgenden Zahlen durch 9, 11, 13, 17, 37, 61 oder 71 teilbar sind.
a) $z = 5148$, b) $z = 1989$, c) $z = 9372$, d) $z = 1887$, e) $z = 11407$, f) $z = 5291$.
Man wende die Teilbarkeitsregeln der vorigen Aufgaben an.

4.6 Grafische Darstellung der Multiplikation

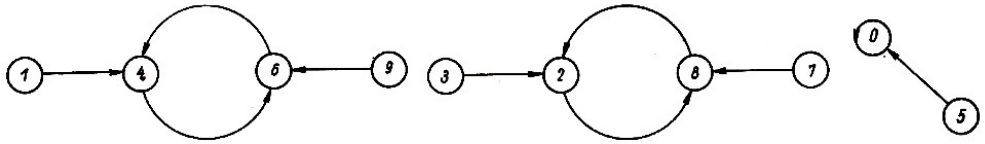
Unter der grafischen Darstellung der Multiplikation mod m wollen wir folgendes verstehen: Den Elementen $\{0, 1, 2, 3, ..., (m-1)\}$ mod m seien Felder (bzw. Kreise) zugeordnet. Die Multiplikation eines Elementes b mit dem Element a wird durch einen vom Feld b ausgehenden und zum Ergebnisfeld verlaufenden Pfeil dargestellt. So wird zum Beispiel $b \cdot a \equiv c$ mod m veranschaulicht durch das Bild ⓑ —a→ ⓒ.

(101) Man stelle die Multiplikationen $2b \equiv x$ mod 10, $4b \equiv x$ mod 10 und $5b \equiv x$ mod 10 grafisch dar für $b = 0, 1, 2, ..., 9$.

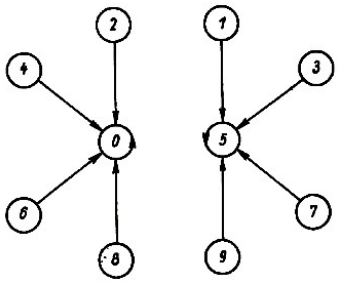
Lösung: $2b \equiv x$ mod 10



$4b \equiv x$ mod 10



$5b = x$ mod 10

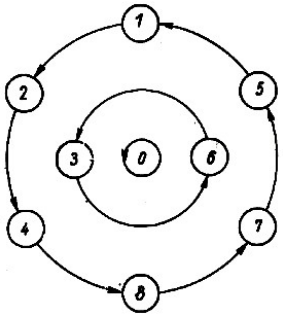


Bemerkung: Man nennt eine Folge von Elementen, bei denen nach endlich vielen Schritten wieder das Ausgangselement erreicht wird, einen Zyklus. Die Anzahl der diesen Zyklus bildenden Elemente heißt Länge des Zyklus.

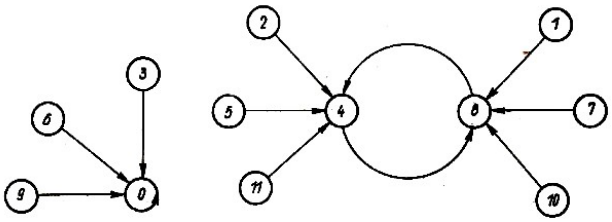
Das Element "Null" bildet jeweils einen Einerzyklus, der Zyklus ist entartet, er hat die Länge 4. Bei der Multiplikation des Elementes Null mit irgendeinem anderen Element ergibt sich wieder das Element Null. Die Null geht bei der Multiplikation in sich selbst über.
Die Elemente 2, 4, 8, 6 bilden für $a = 2$ einen Zyklus der Länge 4.
Für $a = 4$ bilden die Elemente 4 und 6 sowie die Elemente 2 und 8 je einen Zweierzyklus. Für $a = 5$ tritt neben dem entarteten Nullzyklus ein weiterer Einerzyklus für das Element 5 auf.

(102) Man stelle die Multiplikationen $2b \equiv x$ mod 9 für $b = 0, 1, 2, 3, .., 8$ und $8b \equiv x$ mod 12 für $b = 0, 1, 2, 3, ..., 11$ grafisch dar.

Lösung: $2b \equiv x$ mod 9



$8b \equiv x$ mod 12



Bemerkung: Schemata für eine Division würden formal durch Umkehrung der Pfeilrichtungen aus den Multiplikationsschemata entstehen. Für eine Nichtprimzahl als Modul existiert diese Umkehrung im allgemeinen nicht, weil sie für bestimmte Fälle nicht ausführbar und für andere Fälle nicht eindeutig ausführbar ist.

Bei Umkehrung der Pfeilrichtungen in dem Multiplikationsschema der Kongruenz $8b \equiv x$ mod 12 würden von den Elementen 0, 4 und 8 jeweils 4 Pfeile ausgehen. Das bedeutet, dass die Kongruenzen $8x \equiv 0$ mod 12, $8x \equiv 4$ mod 12 und $8x \equiv 8$ mod 12 nicht eindeutig lösbar sind. Von den Elementen 1, 2, 3, 5, 6, 7, 9, 10 und 14 würden bei Umkehrung der Pfeilrichtungen keine Pfeile ausgehen. Das bedeutet, dass die Kongruenzen $8x \equiv 1$ mod 12, $8x \equiv 2$ mod 12, ..., $8x \equiv 11$ mod 12 nicht lösbar sind, es existiert in diesen Fällen keine Lösung.

Bei Umkehrung der Pfeilrichtung in dem Multiplikationsschema der Kongruenz $2b \equiv x$ mod 9 würde von jedem Element genau ein Pfeil ausgehen, und zu jedem Element würde genau ein Pfeil führen. Das bedeutet eindeutige Lösbarkeit der Kongruenzen $2x \equiv b$ mod 9 für $b = 0, 1, 2, ..., 8$.
Man beachte: In den betrachteten Beispielen haben die auftretenden Zyklen unterschiedliche Länge.

(103)• Man stelle die Multiplikationen $ab \equiv x$ mod 12 für $a = 2, 3, 4, 5, 6, 7$ und für $b = 0, 1, 2, 3, ..., 11$ grafisch dar.

(104) Man zeige:

Die Kongruenz $ax \equiv b$ mod m ist genau dann eindeutig lösbar, wenn a und m teilerfremd sind, wenn also gilt: $(a, m) = 1$.
(a, b, x seien Elemente der Menge $\{0, 1, 2, ..., (m-1)\}$).
Wenn a und m teilerfremd sind, so zerfällt das Multiplikationsschema der Kongruenz $ax \equiv b$ mod m in Zyklen.

Lösung:
Gegeben sei die Kongruenz $ax \equiv b$ mod m.

Voraussetzung: $d = (a, m) = 1$.
Annahme, es gäbe zwei positive Zahlen x_1 und x_2 mit $x_2 < x_1 < m$, die die Kongruenz lösen. Dann gilt:
$ax_1 = k_1 m + b$ und $ax_2 = k_2 m + b$ und nach Subtraktion $a(x_1 - x_2) = m(k_1 - k_2)$.

Das bedeutet aber, dass die linke Seite $a(x_1 - x_2)$ durch m teilbar ist. Da a und m nach Voraussetzung keinen gemeinsamen Teiler besitzen, muss m als Faktor in der Differenz $(x_1 - x_2)$ enthalten sein. Dies ist unmöglich, da $x_2 < x_1 < m$ und erst recht $(x_1 - x_2) < m$.

Durchläuft nun x alle Zahlen modulo m $(0, 1, 2, ..., m-1)$, so treten genau m voneinander verschiedene Ergebnisse b auf (vgl. Aufgabe (102)), da die Multiplikation eindeutig ausführbar ist. Da nun andererseits zu keinem Element b zwei oder mehr voneinander verschiedene Elemente x gehören, so gehört zu jedem x genau ein b und zu jedem b genau ein Element x. Es besteht eine eineindeutige Zuordnung, was sofort aus dem Schubfachprinzip von Dirichlet folgt.

Das Ergebnis der Aufgabe soll noch einmal geometrisch gedeutet werden.
Multipliziert man modulo m ein Element a mit dem Element, so erhält man einen Pfeil, der von a zum Produkt $ax \equiv b$ mod m führt. Sind a und m teilerfremd, so kommen in einem Ergebnisfeld niemals zwei oder mehr Pfeile an.
Werden nun der Reihe nach alle Zahlen modulo m $(0, 1, ..., m-1)$ mit a multipliziert, so erhält man genau m Pfeile. Da in keinem Feld zwei oder mehr Pfeile ankommen, so muss nach Dirichlet in jedem Feld genau ein Pfeil ankommen.

Kehrt man die Aufgabenstellung um und betrachtet die Kongruenz $ax \equiv b$ mod m, so kehren sich auch alle Pfeilrichtungen um, und von jedem b führt genau ein Pfeil zu der eindeutig existierenden Lösung x.
Die Multiplikationsdarstellungen zerfallen in Zyklen, wenn a und m teilerfremd sind. Das geht sofort daraus hervor, dass in keinem Feld zwei oder mehr Pfeile ankommen und dass in jedem Feld genau ein Pfeil ankommt.

Bemerkung: Für den Fall, dass a und m teilerfremd sind, ist die Division erklärt und eindeutig ausführbar. Man verwendet der Übersicht halber für die Darstellung $ax \equiv b$ mod m auch die Bruchdarstellung $x \equiv \frac{b}{a}$ mod m.
Es sei aber deutlich hervorgehoben, dass mit dieser Bruchdarstellung keineswegs die rationalen Zahlen eingeführt werden. Es geht nur um eine übersichtlichere Darstellung der Kongruenz $ax \equiv b$ mod m. Diese Darstellung ist, wie nochmals betont werden soll, nur gestattet, wenn a und m teilerfremd sind.

4.7 Bruchdarstellung der Kongruenzen

(105) Man zeige, dass die Gesetze der Bruchrechnung auch formal für die Bruchdarstellungen von Kongruenzen gelten.

Lösung:
1. Erweitert oder kürzt man die Bruchdarstellung einer Kongruenz mit einer zu m teilerfremden Zahl c, so bleibt der Wert der Kongruenz erhalten.

$$x \equiv \frac{b}{a} \equiv \frac{bc}{ac} \bmod m$$

Aus $x \equiv \frac{b}{a}$ mod m oder $ax \equiv b$ mod m folgt $ax = k_1 m + b$. Nach Multiplikation mit c folgt weiter $acx = ck_1 m + bc$, oder $acx - bc = ck_1 m$.
Die Differenz $(acx - bc)$ ist also durch den Faktor m teilbar, woraus $acz - bc \equiv 0$ mod m oder $acz \equiv bc$ mod m folgt, also gilt die Behauptung.

Andererseits folgt aus $x \equiv \frac{bc}{ac}$ mod m oder $ac \equiv bc$ mod m $acc = k_2 m + bc$, $acx - bc = k_2 m$ oder $c(ax - b) = k_2 m$.
Die linke Seite der letzten Beziehung muss durch m teilbar sein. Da c zu m teilerfremd ist, muss die Differenz $(a - b)$ durch m teilbar sein, woraus folgt, dass $ax - b \equiv 0$ mod m oder $ax \equiv b$ mod m, also gilt

$$x \equiv \frac{bc}{ac} \equiv \frac{b}{a} \bmod m$$

2. Man multipliziert die Bruchdarstellung einer Kongruenz mit einer Zahl, indem man den Zähler der Darstellung mit der Zahl multipliziert.

Aus $x \equiv \frac{b}{a}$ mod m folgt $xc \equiv \frac{bc}{a}$ mod m. $d = (c, m) = 1$.
Multipliziert man die Gleichung $ax = km + b$ mit c, so folgt $acx = ckm + bc$ oder $acx \equiv bc$ mod m, woraus aber $cx \equiv \frac{bc}{a}$ mod m folgt.

3. Man multipliziert die Bruchdarstellungen zweier Kongruenzen miteinander, indem man das Produkt der Zähler durch das Produkt der Nenner dividiert.

Aus $x_1 \equiv \frac{b-1}{a-1}$ mod m und $x_2 \equiv \frac{b-2}{a-2}$ mod m folgt $x_1 x_2 \equiv \frac{b-1 b-2}{a-1 a-2}$ mod m.

Durch Multiplikation der Gleichungen $a_1 x_1 = k_1 m + b_1$ und $a_2 x_2 = k_2 m + b_2$ folgt

$$a_1 x_1 a_2 x_2 = km + b_1 b_2 \qquad \text{oder} \qquad a_1 a_2 x_1 x_2 \equiv b_1 b_2 \bmod m$$

und hieraus ergibt sich die Bruchdarstellung $x_1 x_2 \equiv \frac{b_1 b_2}{a_1 a_2}$ mod m.

4. Die Bruchdarstellungen von Kongruenzen werden addiert oder subtrahiert, indem man sie gleichnamig macht und dann addiert oder subtrahiert.

Aus $x_1 \equiv \frac{b_1}{a_1}$ mod m und $x_2 \equiv \frac{b_2}{a_2}$ mod m folgt $x_1 \pm x_2 \equiv \frac{b_1 a_2 \pm b_2 a_1}{a_1 a_2}$ mod m.

Löst man die Gleichungen $a_1 x_1 = k_1 m + b_1$ und $a_2 x_2 = k_2 m + b_2$ nach x_1 und x_2 auf und addiert oder subtrahiert die so entstehenden Ausdrücke, so folgt

$$x_1 \pm x_2 = \frac{km + b_1 a_2 \pm b_2 a_1}{a_1 a_2} = \frac{km}{a_1 a_2} + \frac{b_1 a_2 \pm b_2 a_1}{a_1 a_2}$$
$$a_1 a_2 (x_1 \pm x_2) = km + b_1 a_2 \pm b_2 a_1 \quad \text{oder}$$
$$a_1 a_2 (x_1 \pm x_2) \equiv b_1 a_2 \pm b_2 a_1 \bmod m$$

woraus man die Bruchdarstellung $x_1 \pm x_2 \equiv \frac{b_1 a_2 \pm b_2 a_1}{a_1 a_2}$ mod m erhält.

(106) Man löse die Kongruenzen
a) $25x \equiv 1$ mod 99; b) $18x \equiv 17$ mod 71; c) $12x \equiv 21$ mod 97;
d) $58x \equiv 47$ mod 111; e) $81x \equiv 101$ mod 143; f) $243x \equiv 127$ mod 290.

Lösung: a) $x \equiv \frac{1}{25} \equiv \frac{1+99}{25} \equiv 4 \bmod 99$
Probe: $25 \cdot 4 = 100 = 99 + 1$

b) $x \equiv \frac{17}{18} \equiv \frac{88}{18} \equiv \frac{44}{9} \equiv -\frac{27}{9} \equiv -3 \equiv 68 \bmod 71$
Probe: $18 \cdot 68 = 1224 = 17 \cdot 71 + 17.$

c) $x \equiv \frac{21}{12} \equiv \frac{7}{4} \equiv \frac{104}{4} \equiv 26 \bmod 97$
Probe: $12 \cdot 26 = 312 = 3 \cdot 97 + 21$

d) $x \equiv \frac{47}{58} \equiv \frac{158}{58} \equiv \frac{79}{29} \equiv \frac{16}{41} \equiv -\frac{8}{35} \equiv -\frac{17}{5} \equiv -70 \equiv 41 \bmod 111$
Probe: $58 \cdot 41 = 2378 = 21 \cdot 111 + 47$

e) $x \equiv \frac{101}{81} \equiv -\frac{42}{81} \equiv -\frac{14}{27} \equiv \frac{43}{9} \equiv \frac{62}{3} \equiv -\frac{81}{3} \equiv -27 \equiv 116 \bmod 143$
Probe: $81 \cdot 116 = 9396 = 65 \cdot 143 + 101$

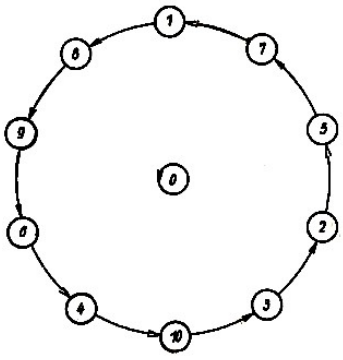
f) $x \equiv \frac{127}{243} \equiv \frac{139}{81} \equiv \frac{143}{27} \equiv -\frac{49}{9} \equiv -\frac{113}{3} \equiv \frac{177}{3} \equiv 59 \bmod 290$
Probe: $243 \cdot 59 = 14337 = 49 \cdot 290 + 127$

(107)• Man löse die Kongruenzen
a) $113x \equiv 36$ mod 17; b) $36x \equiv 91$ mod 113; c) $115x \equiv 81$ mod 117;
d) $17x \equiv 37$ mod 71; e) $111x \equiv 137$ mod 149; f) $64x \equiv 201$ mod 243;
g) $243x \equiv 317$ mod 401; h) $75x \equiv 526$ mod 1001; i) $120x \equiv 861$ mod 1523.

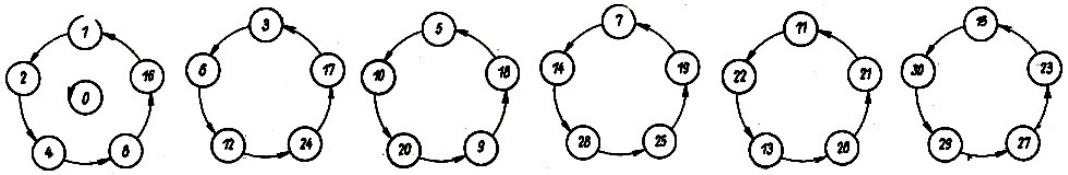
4.8 Der kleine Satz von Fermat

(108) Man stelle die Multiplikationen
$6b \equiv x$ mod 11 für $b = 0, 1, 2, ..., .10$ und $2b \equiv x$ mod 31 für $b = 0, 1, 2, ..., 30$ grafisch dar.

Lösung: $8b \equiv x$ mod 11



$2b \equiv x$ mod 31



Bemerkung: Es wurde in Aufgabe (104) gezeigt, dass die Kongruenz $ax \equiv b$ mod m stets eindeutig lösbar ist, wenn a und m teilerfremd sind. Dies gilt nun erst recht, wenn m eine Primzahl ist $(m = p)$.
Die Darstellung der Multiplikation zerfällt stets in Zyklen. Aus den Multiplikationsdarstellungen entstehen durch Umkehrung der Pfeilrichtungen Schemata für die stets ausführbare Division.

(109)• Man stelle die Multiplikationen
$4b \equiv x$ mod 7 für $b = 0, 1, 2, ..., 6$,
$7b \equiv x$ mod 13 für $b = 0, 1, 2, ..., 12$ und
$12b \equiv x$ mod 23 für $b = 0, 1, 2, ..., 22$ grafisch dar.

(110) Es ist zu zeigen, dass $z = 6^{30} - 1$ durch 31 teilbar ist.

Lösung:
$6^2 \equiv 5$ mod 31, $6^3 \equiv -1$ mod 31, $6^{30} \equiv (6^3)^{10} \equiv 1$ mod 31.
$6^{30} - 1 \equiv 1 - 1 \equiv 0$ mod 31, z ist durch 31 teilbar.

(111) Es ist zu zeigen, dass $z = 48^{72} - 1$ durch 73 teilbar ist.

Lösung:
$48^2 \equiv -32$ mod 73, $48^4 \equiv 2$ mod 73, $48^{24} \equiv 2^6 \equiv -9$ mod 73,
$48^{72} \equiv (-9)^3 \equiv -72 \equiv 1$ mod 73,
$48^{72} - 1 \equiv 0$ mod 73, z ist durch 73 teilbar.

(112) Man zeige: Die Potenzen a^k mod p mit $(a, p) = 1$ wiederholen sich zyklisch; $(k = 1, 2, 3, ...)$.

Lösung:
Wie gezeigt wurde, ist die Kongruenz $ax \equiv y$ mod p für jedes x eindeutig lösbar. Nun gilt:

$$\begin{aligned} a^1 &= a \equiv a \equiv y_1 \bmod p \\ a^2 &= a \cdot a \equiv a y_1 \equiv y_2 \bmod p \\ a^3 &\equiv a y_2 \equiv y_3 \bmod p \\ &... \\ a^k &\equiv a y_{k-1} \equiv y_k \bmod p \qquad ... \end{aligned}$$

Man setzt die Multiplikation fort, bis man den Wert $y_s = 1$ erhält. Es sind alle y_k mit $k < s$ voneinander verschieden.

Annahme, y_k sei der erste Wert, der vorher schon einmal als Ergebnis aufgetreten ist, etwa $y_k = y_n$ $(n < k < s)$, dann gilt

$$a y_{n-1} \equiv y_k \bmod p \qquad \text{und} \qquad a y_{k-1} \equiv y_k \bmod p \qquad \text{oder}$$

$$a(y_{k-1} - y_{n-1}) \equiv 0 \bmod p$$

also $y_{k-1} = y_{n-1}$, da $d = (a, p) = 1$.
Das führt zu einem Widerspruch zur Annahme, dass nämlich y_k der erste Wert sein sollte, der vorher schon einmal auftrat. Bei Fortsetzung der Multiplikationstabelle erhält man sicher den Wert $y_s = 1$.

Wie gezeigt wurde, treten als Ergebnisse der Multiplikationen stets neue Werte auf, die aber

alle der endlichen Menge $\{1, 2, 3, ..., p-1\}$ angehören. Mindestens nach $(p-1)$ Schritten muss also der Wert $y_s = 1$ auftreten. Es gilt

$$a^s \equiv ay_{s-1} \equiv y_s \equiv 1 \bmod p$$
$$a^{s+1} \equiv ay_s \equiv a \equiv y_1 \bmod p \qquad ...$$

Die Potenzen a^k mod p wiederholen sich zyklisch, die Länge des Zyklus ist s.
(Man vergleiche die Aufgabe (83) sowie die Aufgaben (108) und (109) über die grafische Darstellung der Multiplikationen mod p.)

(113) Man zeige: Die Länge s des Zyklus a^k mod p mit $a \not\equiv 0$ mod p ist Teiler von $(p-1)$.

Lösung:
In dem Zyklus der Länge s sind alle y_k voneinander verschieden, wie in der vorigen Aufgabe gezeigt wurde.
Multipliziert man die Elemente dieses ersten Zyklus mit der beliebigen Zahl b aus der Menge $\{2, 3, 4, ..., (p-1)\}$, so erhält man wiederum einen Zyklus der Länge s, in dem die Ergebnisse z_k wiederum alle voneinander verschieden sind.

$$a^1 b \equiv y_1 \cdot b \equiv z_1 \bmod p$$
$$a^2 \cdot b \equiv y_2 \cdot b \equiv z_2 \bmod p$$
$$a^3 \cdot b \equiv y_3 \cdot b \equiv z_3 \bmod p$$
$$...$$
$$a^k \cdot b \equiv y_k \cdot b \equiv z_k \bmod p$$
$$...$$
$$a^s \cdot b \equiv y_s \cdot b \equiv z_s \bmod p$$
$$a^{s+1} \cdot b \equiv y_1 \cdot b \equiv z_1 \bmod p$$

Annahme, z_k sei der erste Wert, der vorher schon einmal als Ergebnis aufgetreten ist, etwa $z_k = z_n$ $(n < k < s)$, dann gilt

$$by_{n-1} \equiv z_k \bmod p \qquad \text{und} \qquad by_{k-1} \equiv z_k \bmod p \qquad \text{oder}$$

$$b(y_{k-1} - y_{n-1}) \equiv 0 \bmod p \qquad \text{also} \qquad y_{k-1} = y_{n-1}$$

Das ist ein Widerspruch zur Voraussetzung, welche besagt, dass alle Werte y_k voneinander verschieden sein sollen.
Multipliziert man nun die Elemente des ersten Zyklus mit allen Elementen $\neq 0$, also mit den Elementen $1, 2, 3, 4, ..., (p-1)$, so erhält man $(p-1) \cdot s$ Ergebnisse, die sich in der folgenden Tabelle anordnen lassen.

	1	2	3	...	b	...	$(p-1)$
y_1	y_1			...	$z-1$	...	
y_2	y_2			...	z_2	...	
y_3	y_3			...	z_3	...	
...							
y_k	y_k			...	z_k	...	
...							
y_s	y_s			...	z_s	...	

Die Elemente einer Spalte sind alle voneinander verschieden. Jede Spalte ist in sich zyklisch. Es treten nur die Elemente $1, 2, 3, ..., (p-1)$ auf, folglich ist jedes Element in genau s verschiedenen Spalten vorhanden, wobei diese s voneinander verschiedenen Spalten aber jeweils denselben Zyklus darstellen.

Streicht man nun alle überflüssigen Spalten fort, so dass nur noch voneinander verschiedene Zyklen übrig bleiben, so bleiben genau die $(p-1)$ Elemente stehen. Jedes Element tritt genau einmal in einem der übrig bleibenden Zyklen auf.

Es folgt: Die Anzahl der Elemente $(p-1)$ ist durch die Zyklenlänge s teilbar. $(p-1) = N \cdot s$, wobei N die Anzahl der vorhandenen Zyklen der Länge s angibt.

(114) Man zeige: Es gilt der kleine Satz von Fermat[11]:
Sind a und p teilerfremd, so ist die um verminderte $(p-1)$-te Potenz von a durch p teilbar.
Oder: $a^{p-1} - 1 \equiv 0$ mod p, wenn $(a, p) = 1$.

Lösung:
Wie in der vorigen Aufgabe gezeigt wurde, gilt $a^2 \equiv 1$ mod p und $N \cdot s = p - 1$. Es folgt

$$(a^s)^N = a^{sN} = a^{p-1} \equiv 1 \bmod p \qquad \text{oder} \qquad a^{p-1} - 1 \equiv 0 \bmod p$$

(115) Man zeige: Jede Potenz mit einer Primzahl als Exponent liefert bei der Division durch diese Primzahl die Basis als Rest.

$$a^p \equiv a \bmod p \qquad \text{oder} \qquad a^p - a \equiv 0 \bmod p$$

Lösung:
Es ist $0^p \equiv 0$ mod p und bei $a \not\equiv 0$ mod p folgt aus dem kleinen Satz von Fermat $a^{p-1} \equiv 1$ mod p durch Multiplikation mit a

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

(116) Man zeige, dass $z = 8^{34} - 8^{18} - 8^{16} + 1$ durch 323 teilbar ist.

Lösung:
$323 = 17 \cdot 19$, $z = (8^18 - 1)(8^16 - 1)$.
Nach dem kleinen Satz von Fermat ist der erste Faktor durch 19, der zweite durch 17 teilbar. Folglich ist z durch $19 \cdot 17 = 323$ teilbar.

(117) Man zeige, dass $43^{100} - 1$ durch 101 teilbar ist.

Lösung:
Die Behauptung folgt sofort aus dem kleinen Satz von Fermat.

(118) Man zeige: 78^{136} liefert bei der Division durch 137 den Rest 1.

Lösung:
Nach Fermat gilt: $78^{136} - 1 \equiv 0$ mod 137.

(119) Man zeige, dass $7^{89} - 7$ durch 89 teilbar ist.

Lösung:
Die Behauptung folgt sofort aus dem kleinen Satz von Fermat.

(120) Man zeige: 99^{293} liefert bei der Division durch 293 den Rest 99.

[11] Fermat, Pierre, französischer Mathematiker, 1601-1665

Lösung:
Nach Fermat gilt: $99^{292} - 1 \equiv 0$ mod 293. Nach Multiplikation mit 99 gilt $99^{293} - 99 \equiv 0$ mod 293 oder $99^{293} \equiv 99$ mod 293.

(121) Man zeige, dass $z = 2^{136} - 2^{134} - 2^{132} + 2^{130} - 2^6 + 2^4 + 2^2 - 1$ durch 1965 teilbar ist.

Lösung: $1965 = 3 \cdot 5 \cdot 131$,

$$z = 2^{130}(2^6 - 2^4 - 2^2 + 1) - 2^6 + 2^4 + 2^2 - 1 = (2^{130} - 1)(2^4 - 1)(2^2 - 1)$$

Die Faktoren sind nach dem kleinen Satz von Fermat durch 131, durch 5 und durch 3 teilbar, somit ist z durch 1965 teilbar.

(122) Man zeige, dass $z = 35^{18} - 7^{18} - 5^{18} + 1$ durch 361 teilbar ist.

Lösung:
$361 = 1)^2$, $z = 7^{18}(5^{18} - 1) - 5^{18} + 1 = (5^{18} - 1)(7^{18} - 1)$.
Nach Fermat ist jeder Faktor durch 19 und damit z durch 19^2 teilbar.

(123) Man zeige, dass $z = 2^{12} - 2^7 + 1$ durch 49 teilbar ist.

Lösung:
$z = 2^{12} - 2 \cdot 2^6 + 1 = (2^6 - 1)^2$
Nach Fermat ist $(2^6 - 1)$ durch 7 teilbar, also ist z durch $7^2 = 49$ teilbar.

(124) Man zeige, dass $z = 3^{30} - 3^{21} + 3^{11} - 1$ durch 1331 teilbar ist.

Lösung:
$1331 = 11^3$, $z = 3^{30} - 3 \cdot 3^{20} + 3 \cdot 3^{10} - 1 = (3^{10} - 1)^3$
Nach dem kleinen Satz von Fermat ist $(3^{10} - 1)$ durch 11 und damit ist z durch $11^3 = 1331$ teilbar.

(125) Man zeige, dass der Ausdruck $z = 16459^{360360} - 1$ durch mindestens 12 Primzahlen teilbar ist.

Lösung:
$16459 = 151 \cdot 109$, $360360 = 2^3 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 13$

1. z ist durch 2 teilbar, weil $16459^{360360} = 2n + 1$	$2 \mid z$
2. $z = (a^{180180})^2 - 1 \equiv 0$ mod 3,	$3 \mid z$
3. $z = (a^{90090})^4 - 1 \equiv 0$ mod 5,	$5 \mid z$
4. $z = (a^{60060})^6 - 1 \equiv 0$ mod 7,	$7 \mid z$
5. $z = (a^{36036})^{10} - 1 \equiv 0$ mod 11,	$11 \mid z$
6. $z = (a^{30030})^{12} - 1 \equiv 0$ mod 13,	$13 \mid z$
7. $z = (a^{20020})^{18} - 1 \equiv 0$ mod 19,	$19 \mid z$
8. $z = (a^{16380})^{22} - 1 \equiv 0$ mod 23,	$23 \mid z$
9. $z = (a^{12870})^{28} - 1 \equiv 0$ mod 29,	$29 \mid z$
10. $z = (a^{12012})^{30} - 1 \equiv 0$ mod 31,	$31 \mid z$
11. $z = (a^{10010})^{36} - 1 \equiv 0$ mod 37,	$37 \mid z$
12. $z = (a^{9009})^{40} - 1 \equiv 0$ mod 41,	$41 \mid z$

Die in den Klammern stehenden Potenzen von $a = 16459$ sind zu den betrachteten Primzahlen jeweils teilerfremd, so dass der kleine Satz von Fermat in allen Fällen Anwendung finden kann. Es soll die Probe mittels anderer Berechnung angeschlossen werden. $16459 = a$.

$a \equiv 1$ mod 3, $a^n \equiv 1$ mod 3, $z \equiv 0$ mod 3.
$a \equiv -1$ mod 5, $a^{2n} \equiv 1$ mod 5, $z \equiv 0$ mod 5.
$a \equiv 2$ mod 7, $2^3 \equiv 1$ mod 7, $a^{3n} \equiv 1$ mod 7, $z \equiv 0$ mod 7.
$a \equiv 3$ mod 11, $3^5 \equiv 1$ mod 11, $a^{5n} \equiv 1$ mod 11, $z \equiv 0$ mod 11.
$a \equiv 1$ mod 13, $a^n \equiv 1$ mod 13, $z \equiv 0$ mod 13.
$a \equiv 5$ mod 19, $5^9 \equiv 1$ mod 19, $a^{9n} \equiv 1$ mod 19, $z \equiv 0$ mod 19.
$a \equiv 14$ mod 23, $14^{22} \equiv 1$ mod 23, $a^{22n} \equiv 1$ mod 23, $z \equiv 0$ mod 23.
$a \equiv 16$ mod 29, $16^7 \equiv 1$ mod 29, $a^{7n} \equiv 1$ mod 29, $z \equiv 0$ mod 29.
$a \equiv -2$ mod 31, $(-2)^{10} \equiv 1$ mod 31, $a^{10n} \equiv 1$ mod 31, $z \equiv 0$ mod 31.
$a \equiv -6$ mod 37, $(-6)^4 \equiv 1$ mod 37, $a^{4n} \equiv 1$ mod 37, $z \equiv 0$ mod 37.
$a \equiv 18$ mod 41, $18^5 \equiv 1$ mod 41, $a^{5n} \equiv 1$ mod 41, $z \equiv 0$ mod 41.

Bemerkung: Auch die Lösungen der Aufgaben (110) und (111) ergeben sich sofort aus dem kleinen Satz von Fermat.
Als großer Satz von Fermat wird die noch immer unbewiesene Behauptung bezeichnet, wonach $x^n + y^n = z^n$ für $n > 2$ in ganzen Zahlen x, y und z nicht lösbar ist.

(126)• Man zeige, dass $z = q^{36} + 665$ durch 37 teilbar ist, wenn q eine Primzahl größer als 100 ist.

(127)• Gesucht ist die kleinste natürliche Zahl n, für die $z = 5^n - 1$ durch 7, durch 11, durch 13, durch 17 und durch 41 teilbar ist.

(128)• Für welche natürlichen Zahlen n und k ist $z = n^k - 1$ durch 17 teilbar?

(129)• Es ist zu zeigen, dass

$$z = p^{16} - p^{12} - 2p^{10} + 2p^6 + p - 1$$

durch 245 teilbar ist, wenn p eine Primzahl größer als 10 ist.

(130)• Für welche natürliche Zahl k ist $z = 3^{198} - 3^{133} + k$ durch 343 teilbar?

4.9 Reziproke Werte, Satz von Wilson

(131) Man zeige, dass die Kongruenz $ax \equiv 1$ mod p stets eindeutig lösbar ist und bestimme die Elemente modulo p, die mit sich selbst multipliziert, das Element 1 ergeben.

Man entwickle Tabellen für die reziproken Werte der Elemente $1, 2, 3, ..., (p-1)$ modulo p für $p = 7, 11, 17$ und 31.

Lösung:
In Aufgabe (104) wurde gezeigt, dass die Kongruenz $ax \equiv b$ mod p stets eindeutig lösbar ist. Setzt man nun speziell $b = 1$, so folgt daraus die eindeutige Lösung der Kongruenz $ax \equiv 1$ mod p. Die Lösung dieser Kongruenz heißt das zu a "reziproke Element".

Es sei x ein Element, das mit sich selbst multipliziert den Wert 1 ergibt. Dann folgt

$$x \cdot x = 1 \bmod p, \qquad x^2 - 1 \equiv 0 \bmod p, \qquad (x+1)(x-1) \equiv 0 \bmod p$$

Ein Produkt modulo p ist aber dann und nur dann kongruent Null, wenn ein Faktor kongruent Null ist. Daraus ergibt sich

$$x - 1 = 1 \qquad , \qquad x_2 \equiv 1 \equiv (p-1) \bmod p$$

Die Elemente 1 und $(p-1)$ sind zu sich selbst reziprok.

$p = 7$

k	1	2	3	4	5	6
$\frac{1}{k}$	1	4	5	2	3	6

$p = 11$

k	1	2	3	4	5	6	7	8	9	10
$\frac{1}{k}$	1	6	4	3	9	2	8	7	5	10

$p = 17$

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\frac{1}{k}$	1	9	6	13	7	3	5	15	2	12	14	10	4	11	8	16

$p = 31$

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
$\frac{1}{k}$	1	16	21	8	25	26	9	4	7	28	17	13	12	20	29
k	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30
$\frac{1}{k}$	2	11	19	18	14	3	24	27	22	5	6	23	10	15	30

(132) Man zeige, dass $(p-1)! + 1$ durch p teilbar ist. Oder: $(p-1)! + 1 \equiv 0$ mod p.

Lösung:
Die Kongruenz $ax \equiv 1$ mod p ist eindeutig lösbar, zu jedem Element a gibt es genau ein Element x, das zu a reziprok ist. In dem Ausdruck

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

sind nur die Elemente 1 und $(p-1)$ zu sich selbst reziprok. Jedes andere Element hat genau einen reziproken Partner, mit dem es multipliziert den Wert 1 ergibt. Es gilt:

$$(p-1)! \equiv 1 \cdot 1 \cdot 1 \cdot ... \cdot (p-1) \equiv (p-1) \bmod p$$

Damit wird $(p-1)! + 1 \equiv (p-1) + 1 \equiv p \equiv= 0$ mod p.

Beispiel:
$(12! + 1)$ ist durch 13 teilbar.
$12! = (13-1)! = 479001600$; $(12! + 1) = 479001601 = 36846277 \cdot 13$.

Bemerkung: Der Satz $(p-1)! + 1 \equiv 0$ mod p heißt "Satz von Wilson"[12].

(133) Man zeige, dass $z = (18! + 1)^3$ durch 6859 teilbar ist.

Lösung:
$6859 = 19^3$. Nach dem Satz von Wilson ist $(18! + 1)$ durch 19 teilbar, damit ist z durch $19^3 = 6859$ teilbar.

(134) Man zeige, dass $z = (p!)^2 - p^2$ für jede Primzahl durch die dritte Potenz dieser Primzahl teilbar ist.

Lösung:

$$(p!)^2 - p^2 = (p! + p)(p! - p) = p^2[(p-1)! + 1][(p-1)! - 1]$$

Die erste Klammer ist nach dem Satz von Wilson durch p teilbar, folglich ist z durch p^3 teilbar.

(135)• Man stelle Tabellen auf für die reziproken Werte der Elemente modulo p für
a) $p = 13$, b) $p = 19$, c) $p = 23$.

[12]Wilson, Sir John, englischer Mathematiker, 1741-1793

4.10 Tabellen der Quadratzahlen

(136) Es sind die Tabellen der Quadratzahlen für die Elemente modulo m $(1, 2, 3, ..., (m-1))$ aufzustellen für $m = 9$, $m = 15$ und $m = 2$.

Lösung: Tabelle der Quadratzahlen modulo 9:

a	1	2	3	4	5	6	7	8
a^2	1	4	0	7	7	0	4	1

Tabelle der Quadratzahlen modulo 15:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14
a^2	1	4	9	1	10	6	4	4	6	10	1	9	4	1

Tabelle der Quadratzahlen modulo 24:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a^2	1	4	9	16	1	12	1	16	9	4	1	0	1	4	9

a	16	17	18	19	20	21	22	23
a^2	16	1	12	1	16	9	4	1

Aus den Tabellen ersieht man, dass nur gewisse Elemente als Quadratzahlen auftreten und dass diese Elemente mit unterschiedlicher Häufigkeit auftreten. Andere Elemente modulo m treten in den Tabellen der Quadratzahlen nicht auf.
So sind zum Beispiel die Elemente 2, 3, und 5 in keiner der Tabellen als Ergebnis vertreten. Es lässt sich modulo 9, modulo 15 und modulo 24 keine Zahl finden, die mit sich selbst multipliziert 2, 3 oder 5 ergibt.

Eine charakteristische Eigenschaft der Tabellen ist, dass $a^2 \equiv (m-a)^2 \bmod m$. Es ist $(m-a) \equiv -a \bmod m$. Beim Quadrieren verschwindet das negative Vorzeichen, und es folgt

$$a^2 \equiv (m-a)^2 \bmod m$$

(137) Es sind die Quadratzahltabellen für die Elemente modulo p aufzustellen für $p = 7$, $p = 11$, $p = 17$ und $p = 23$.

Lösung:
Tabelle der Quadratzahlen modulo 7:

a	1	2	3	4	5	6
a^2	1	4	2	2	4	1

Tabelle der Quadratzahlen modulo 11:

a	1	2	3	4	5	6	7	8	9	10
a^2	1	4	9	5	4	4	5	9	4	1

Tabelle der Quadratzahlen modulo 17:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
a^2	1	4	9	16	8	2	15	13	13	15	2	8	16	9	4	1

Tabelle der Quadratzahlen modulo 23:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
a^2	1	4	9	16	2	13	3	18	12	8	6	6	8	12	18

a	16	17	18	19	20	21	22
a^2	3	13	2	16	9	4	1

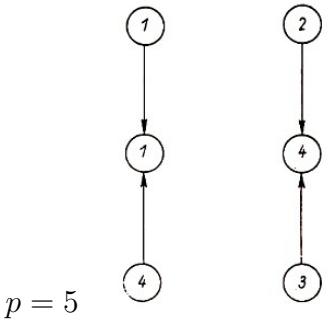
Die in den Tabellen der Quadratzahlen auftretenden Werte treten jeweils genau zweimal auf.

Es gilt wiederum:
$a^2 \equiv (p-a)^2 \bmod p$ (Symmetrieeigenschaft der Tabellen).

(138)• Man stelle Quadratzahltabellen auf für $p = 13$, $p = 19$, $p = 37$.

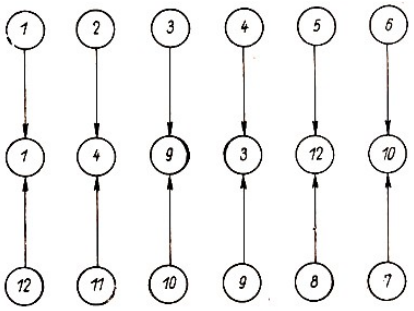
(139) Es sind grafische Darstellungen für die Quadratzahlen modulo 5, modulo 13 und modulo 19 zu entwickeln. (Man vergleiche die grafische Darstellung der Multiplikation auf den vorherigen Seiten)

Lösung:



$p = 5$

Auch die grafischen Darstellungen sind in Bezug auf den Wert $\frac{p}{2}$ symmetrisch. Es treten $\frac{p-1}{2}$ voneinander verschiedene Ergebnisse auf. Jedes Ergebnis tritt genau zweimal auf.

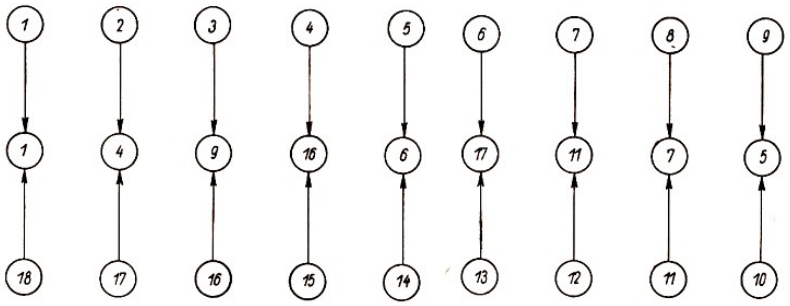


$p = 13$

Von jedem Element modulo p geht genau ein Pfeil aus. Zu jedem Element a^2 führen genau zwei Pfeile. Aus den Elementen a^2 lassen sich die Quadratwurzeln ziehen, was grafisch Umkehrung der Pfeilrichtungen bedeutet.

Existiert die Quadratwurzel aus einem Element modulo p, dann liefert sie genau zwei Lösungen (mit Ausnahme der Quadratwurzel aus dem Element 0, $\sqrt{0} \equiv 0 \bmod p$).

Beispiel:
$\sqrt{3} \equiv 4 \bmod 13$, $\sqrt{3} \equiv 9 \bmod 13$.



$p = 19$

Zum Grundbereich gehören alle ganzzahligen Elemente modulo p. Der Wertevorrat besteht aus einer Menge von $\frac{p-1}{2}$ ganzzahligen Werten. Für gewisse Primzahlen ist das Element $(p-1)$ Quadratzahl, für andere Primzahlen gehört das Element $(p-1)$ nicht zum Wertevorrat.

4.11 Quadratische Kongruenzen

(140) Es ist zu zeigen, dass sich die Quadratzahlen modulo p eindeutig den Elementen $1, 2, 3, ..., \frac{p-1}{2}$ zuordnen lassen.

Lösung:
Es sei c eine Quadratzahl modulo p und es gelte $a^2 \equiv c$ mod p. Annahme, es sei außerdem $b^2 \equiv c$ mod p mit $b \neq a$ und $0 < a < p$, $0 < b < p$.

Durch Subtraktion folgt:

$$a^2 - b^2 \equiv 0 \bmod p \qquad \text{oder} \qquad (a+b)(a-b) \equiv 0 \bmod p$$

Da die Differenz $(a - b) \equiv 0$ mod p, gilt:

$$a + b \equiv 0 \bmod p \qquad \text{oder} \qquad b \equiv -a \bmod p$$

Ist a ein beliebiges Element aus der Menge $\left\{1, 2, 3, ..., \frac{p-1}{2}\right\}$, so kann b nicht auch dieser Menge angehören, da sonst die Summe $(a + b) \neq 0$ mod p wäre.
Oder: Die Quadratzahlen c modulo p lassen sich den Elementen a aus der Menge $\left\{1, 2, 3, ..., \frac{p-1}{2}\right\}$ eindeutig zuordnen.

(141) Man zeige:
Ist p eine Primzahl der Form $p = 4n + 1$ und lässt sich die Quadratwurzel aus dem Element c modulo p ziehen, so lässt sich die Wurzel auch aus dem Element $(p - c) \equiv -c$ mod p ziehen.

Lösung:
Voraussetzung: $p = 4n + 1$, die Quadratwurzel aus c existiert.
Es sei $a^2 \equiv c$ mod p. Nach dem Satz von Wilson gilt:

$$-c \equiv c(-1) \equiv c(p-1)! \equiv c \cdot 1 \cdot 2 \cdot ... \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot ... \cdot (p-1) \bmod p$$

Es gilt: $(p - k) = -k$ mod p und speziell:

$$p - 1 \equiv -1 \bmod p, \qquad p - 2 \equiv -2 \bmod p, \qquad ...$$
$$\frac{p+1}{2} \equiv \frac{p+1}{2} - p \equiv \frac{p+1-2p}{2} \equiv \frac{1-p}{2} \equiv -\frac{p-1}{2} \bmod p$$

Es folgt:

$$-c \equiv c\left(1 \cdot 2 \cdot ... \cdot \frac{p-1}{2}\right)\left[(-1) \cdot (-2) \cdot ... \cdot \left(-\frac{p-1}{2}\right)\right] \bmod p$$

Das Produkt der zweiten Klammer ist positiv wegen der geraden Anzahl von Faktoren ($p = 4n - 1$, $\frac{p-1}{2} = 2n$), es ist somit identisch zum Wert des Produktes der ersten Klammer.

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

Mit $a^2 \equiv c$ mod p folgt:

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

Das Element wurde als vollständiges Quadrat dargestellt, es existiert also $\sqrt{-c}$ mod p.

Beispiel:
$4^2 \equiv 3 \bmod 13$, $-3 \equiv (4 \cdot 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6)^2 \equiv 7^2 \bmod 13$.

Bemerkung 1: Wäre die gegebene Primzahl von der Form $p = 4n + 3$, so ließe sich das Element $(-c)$ nicht als vollständiges Quadrat darstellen, da die Anzahl der negativen Glieder in der zweiten Klammer ungerade wäre ($p = 4n + 3$, $\frac{p-1}{2} = 2n + 1$).

Bemerkung 2: Für $c = 1$ folgt speziell: Die Quadratwurzel aus dem Element (-1) existiert, wenn $p = 4n + 1$, sie existiert nicht, wenn $p = 4n + 3$.

(142) Man zeige:
Existiert modulo p mit $\sqrt{c}$ auch $\sqrt{-c}$, so hat p die Form $p = 4n + 1$.

Lösung:
Es sei $a \equiv c \bmod p$ und $b^2 \equiv -c \bmod p$ mit $0 < a < p$ und $0 < b < p$.
Nach Potenzieren der zweiten Kongruenz mit dem Exponenten $\frac{p-1}{2}$ folgt:

$$(b^2)^{\frac{p-1}{2}} \equiv (-c)^{\frac{p-1}{2}} \bmod p \qquad \text{und} \qquad b^{p-1} \equiv (-1)^{\frac{p-1}{2}} \cdot (c)^{\frac{p-1}{2}} \bmod p$$

$$b^{p-1} \equiv (-1)^{\frac{p-1}{2}} \cdot (a^2)^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{2}} \cdot a^{p-1} \bmod p$$

Nach dem kleinen Satz von Fermat gilt:

$$b^{p-1} \equiv 4 \bmod p \qquad \text{und} \qquad a^{p-1} \equiv 4 \bmod p$$

Die sich daraus ergebende Kongruenz $(-1)^{\frac{p-1}{2}} \equiv 1 \bmod p$ ist nur erfüllt für $\frac{p-1}{2} = 2n$ oder $p = 4n + 1$.
Sie ist nicht erfüllt für ungerade Exponenten $\frac{p-1}{2} = 2n + 1$, also nicht für $p = 4n + 3$.

(143) Es ist eine Bedingung dafür herzuleiten, dass die quadratische Kongruenz $x^2 + ax + b \equiv 0 \bmod p$ lösbar ist.

Lösung:
Es gilt die Identität

$$x^2 + ax + b = \left(x + \frac{a}{2}\right)^2 - \frac{a^2}{4} + b = \left(x + \frac{a}{2}\right)^2 - \frac{a^2 - 4b}{4}$$

Die gegebene Kongruenz ist also äquivalent der Kongruenz

$$\left(x + \frac{a}{2}\right)^2 - \frac{a^2 - 4b}{4} \equiv 0 \bmod p$$

und es gilt

$$\left(x + \frac{a}{2}\right)^2 \equiv \frac{a^2 - 4b}{4} \bmod p$$

Die Quadratwurzel aus der Diskriminante $D = (a^2 - 4b)$ ist genau dann zu ziehen, wenn die gegebene Kongruenz $x^2 + ax + b \equiv 0 \bmod p$ eine Lösung besitzt.
In diesem Fall folgt für die Lösung x:

$$x \equiv -\frac{a}{2} \pm \frac{1}{2}\sqrt{a^2 - 4b}$$

Es existiert keine Lösung der Kongruenz $x^2 + ax + b \equiv 0 \bmod p$, wenn sich die Quadratwurzel aus der Diskriminante $D = (a^2 - 4b)$ nicht ziehen lässt.

Es existiert genau eine Lösung der Kongruenz $x^2 + ax + b \equiv 0$ mod p, wenn $a^2 \equiv 4b$ mod p. Es existieren zwei Lösungen der gegebenen Kongruenz, wenn sich die Quadratwurzel aus $D = (a^2 - 4b) \equiv 0$ mod p ziehen lässt.

Bemerkung: Die hergeleitete Formel gilt nur für $p > 2$, da für $p = 2$ eine Division durch Null auftreten würde.

(144) Man löse die quadratischen Kongruenzen

a) $x^2 + 5x + 4 \equiv 0$ mod 19 b) $x^2 + 12x + 11 \equiv 0$ mod 23
c) $x^2 - 18x + 19 \equiv 0$ mod 31 d) $x^2 + 21x - 13 \equiv 0$ mod 67
e) $x^2 + 16x - 10 \equiv 0$ mod 73 f) $x^4 - 10x^2 + 5 \equiv 0$ mod 101
g) $2x^2 - 3x + 1 \equiv 0$ mod 17 h) $x^2 - 2x \pm 2 \equiv 0$ mod 19

Lösung:
a) $a = 5$, $b = 4$, $D = 9$.
Die Quadratwurzel aus der Diskriminante lässt sich ziehen, ihre Lösungen sind 3 und -3 $\equiv$ 16 mod 19.

$$x_1 \equiv -\frac{5}{2} + \frac{3}{2} \equiv -1 \equiv 18 \bmod 19 \quad , \quad x_2 \equiv -\frac{5}{2} + \frac{16}{2} \equiv \frac{11}{2} \equiv \frac{30}{2} \equiv 15 \bmod 19$$

Probe: $18^2 + 5 \cdot 18 + 4 = 418 = 22 \cdot 19$, $22 \cdot 19 \equiv 0$ mod 19,
$15^2 + 5 \cdot 15 + 4 = 304 = 16 \cdot 19$, $16 \cdot 19 \equiv 0$ mod 19,

b) $a = 12$, $b = 11$, $D = 100 \equiv 8$ mod 23.
Aus der Tabelle der Quadratzahlen (Aufgabe (137)) folgt, dass sich die Quadratwurzel aus 8 ziehen lässt, die Lösungen sind 10 und 13.

$$x_1 \equiv -6 + 5 \equiv -1 \equiv 22 \bmod 23 \quad , \quad x_2 \equiv -6 + \frac{13}{2} \equiv \frac{1}{2} \equiv \frac{24}{2} \equiv 12 \bmod 23$$

Probe: $22^2 + 12 \cdot 22 + 11 = 759 = 33 \cdot 23$, $33 \cdot 23 \equiv 0$ mod 23,
$12^2 + 12 \cdot 12 + 11 = 299 = 13 \cdot 23$, $13 \cdot 23 \equiv 0$ mod 23,

c) $a = -18$, $b = 19$, $D = 24 \equiv 0$ mod 31.
Es ergibt sich nur eine Lösung der Kongruenz $x \equiv 9$ mod 31.
Probe: $9^2 - 18 \cdot 9 + 19 = -62 = -2 \cdot 31$, $-2 \cdot 31 \equiv 0$ mod 31.

d) $a = 21$, $b = -13$, $D = 493 \equiv 24$ mod 67.
Es ist zu untersuchen, ob sich die Quadratwurzel aus der Zahl 24 mod 67 ziehen lässt. Es brauchen nur die Elemente $s \leq 33$ betrachtet zu werden.

s	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
s^2	1	4	9	16	25	36	49	64	14	33	54	10	35	62	24

Die Quadratwurzel lässt sich modulo 67 aus der Zahl 24 ziehen, die Lösungen sind 15 und -15 $\equiv$ 52 mod 67.

$$x_1 = -\frac{21}{2} + \frac{15}{2} \equiv -3 \equiv 64 \bmod 67 \quad , \quad x_2 = -\frac{21}{2} + \frac{52}{2} \equiv \frac{31}{2} \equiv 49 \bmod 67$$

Probe: $64^2 + 21 \cdot 64 - 13 = 5427 = 81 \cdot 67$, $81 \cdot 67 \equiv 0$ mod 67,
$49^2 + 21 \cdot 49 - 13 = 3417 = 51 \cdot 67$, $51 \cdot 67 \equiv 0$ mod 67,

e) $a = 16$, $b = -10$, $D = 296 \equiv 4$ mod 73.

Die Quadratwurzel aus der Diskriminante D hat die Lösungen 2 und -2 $\equiv$ 71 mod 73.

$$x_1 = -8 + 1 \equiv -7 \equiv 66 \bmod 73 \qquad , \qquad x_2 = -8 + \frac{71}{2} \equiv \frac{55}{2} \equiv 64 \bmod 67$$

Probe: $66^2 + 16 \cdot 66 - 10 = 5402 = 74 \cdot 73$, $74 \cdot 73 \equiv 0$ mod 73,
$64^2 + 16 \cdot 64 - 10 = 5110 = 70 \cdot 73$, $70 \cdot 73 \equiv 0$ mod 73,

f) Es liegt eine biquadratische Kongruenz vor, die man durch die Substitution $x^2 = z$ auf eine normale quadratische Kongruenz zurückführt:

$$z^2 - 10z + 5 \equiv 0 \bmod 101, \qquad a = -10, b = 5, D = 80$$

Es ist zu untersuchen, ob sich die Quadratwurzel aus der Zahl 80 mod 101 ziehen lässt. Dabei brauchen nur die Elemente $s \leq 50$ betrachtet zu werden, wobei auch auf die Zahl $-80 \equiv 21$ mod 101 zu achten ist.
Da $101 = 4n + 1$, so existiert die Quadratwurzel aus der Zahl 80 genau dann, wenn sie aus der Zahl $-80 \equiv 21$ mod 101 existiert.

s	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
s^2	1	4	9	16	25	36	49	64	81	100	20	43	68	95	23	54	87	21

Da die Quadratwurzel aus der Zahl 21 existiert, muss auch die Quadratwurzel aus der Zahl 80 existieren.

s	19	20	21	22
s^2	58	97	37	80

Die Lösungen der Quadratwurzel aus der Zahl 80 sind 22 und -22 $\equiv$ 79 mod 101.

$$z_1 = 5 + 11 \equiv 16 \bmod 101 \qquad , \qquad z_2 = 5 + \frac{79}{2} \equiv 95 \bmod 101$$

Nun war $x^2 = z$. Die Elemente 16 und 95 treten als Quadratzahlen in der Tabelle auf. Die Kongruenzen $x^2 = 16$ mod 101 und $x^2 = 95$ mod 101 sind also lösbar.
$x_1 \equiv 4$ mod 101 und $x_2 \equiv -4 \equiv 97$ mod 101 sind die Lösungen der Kongruenz $x^2 \equiv 16$ mod 101.
$x_3 \equiv 14$ mod 101 und $x_4 \equiv -14 \equiv 87$ mod 101 sind die Lösungen der Kongruenz $x^2 \equiv 95$ mod 101.

Damit sind die Lösungen der gegebenen biquadratischen Kongruenz $x_1 \equiv 4$ mod 101, $x_2 \equiv 97$ mod 101, $x_3 \equiv 14$ mod 101, $x_4 \equiv 87$ mod 101.

Probe: $4^4 - 10 \cdot 4^2 + 5 = 101$, $101 \equiv 0$ mod 101,
$97^4 - 10 \cdot 97^2 + 5 = 88435196 = 875596 \cdot 101$, $875596 \cdot 101 \equiv 0$ mod 101,
$14^4 - 10 \cdot 14^2 + 5 = 36461 = 361 \cdot 101$, $361 \cdot 101 \equiv 0$ mod 101,
$87^4 - 10 \cdot 87^2 + 5 = 57214076 = 566476 \cdot 101$, $566476 \cdot 101 \equiv 0$ mod 101,

g) $x^2 - \frac{3}{2}x + \frac{1}{2} \equiv 0$ mod 17.
$a = -\frac{3}{2}$, $b = \frac{1}{2}$, $D = \frac{1}{4} \equiv -\frac{16}{4} \equiv -4 \equiv 13$ mod 17

Aus der Tabelle (Aufgabe (137)) entnimmt man die Lösungen für die Quadratwurzel aus der Zahl 13 mod 17. Die Lösungen sind 8 und 9.

$$x_1 = \frac{3}{4} + 4 \equiv \frac{19}{4} \equiv \frac{1}{2} \equiv \frac{18}{2} \equiv 9 \bmod 17 \qquad , \qquad x_2 = \frac{3}{4} + \frac{9}{2} \equiv \frac{21}{4} \equiv 1 \bmod 17$$

Probe: $2 \cdot 9^2 - 3 \cdot 9 + 1 = 136 = 8 \cdot 17$, $8 \cdot 17 \equiv 0$ mod= 17,
$2 \cdot 1^2 - 3 \cdot 1 + 1 = 0$, $0 \equiv 0$ mod= 17,

h) $a = -2$, $b = \pm 2$, $D_1 = -4 \equiv 13$ mod 17, $D_2 = 12 \equiv 12$ mod 17.

Aus der graphischen Darstellung (Aufgabe (139)) erkennt man, dass die Quadratwurzeln aus den Zahlen 12 und 13 mod 19 nicht existieren. Es existiert keine Lösung der gegebenen Kongruenz.

(145) Man gebe alle Lösungen der Kongruenz an:

$$x^8 - 15x^6 + 3x^4 - 18x^2 + 6 \equiv 0 \bmod 19$$

Lösung:
Die Kongruenz achten Grades wird durch die Substitution $x^2 = z$ auf eine Kongruenz vierten Grades zurückgeführt

$$z^4 - 15z^3 + 3z^2 - 18z + 6 \equiv 0 \bmod 19$$

Es ist eine Zerlegung in zwei Faktoren möglich, wenn man beachtet, dass die Koeffizienten der Variablen durch Addition eines beliebigen Vielfachen von 19 verändert werden dürfen. Es gilt die Kongruenz:

$$z^4 - 15z^3 + 3z^2 - 18z + 6 \equiv (z^2 + 13z + 4)(z^2 - 2z + 11) \bmod 19$$

($4 \cdot 11 \equiv 6$ mod 19, $8 + 143 \equiv 18$ mod 19, $11 + 4 + 26 \equiv 3$ mod 19)

$a = -13$, $b = 4$, $D = 153 \equiv 1$ mod 19.
Die Lösungen der Quadratwurzel aus D sind 1 und $-1 \equiv 18$ mod 19.

$$z_1 \equiv \frac{13}{2}5 + \frac{1}{2} \equiv 7 \bmod 19 \qquad , \qquad z_2 \equiv \frac{13}{2} + 9 \equiv 6 \bmod 101$$

Aus der grafischen Darstellung der Quadratzahlen modulo 19 (Aufgabe (139)) findet man die Lösungen für x.
$x_1 \equiv 8$ mod 19 und $x_2 \equiv 11$ mod 19 sind die Lösungen der Kongruenz $x^2 \equiv 7$ mod 19.
$x_3 \equiv 5$ mod 19 und $x_4 \equiv 14$ mod 19 sind die Lösungen der Kongruenz $x^2 \equiv 6$ mod 19.

$z^2 - 27 + 11 \equiv 0$ mod 19. $a = -2$, $b = 11$, $D = -40 \equiv 17$ mod 19.
Die Lösungen der Quadratwurzel aus D entnimmt man wiederum der grafischen Darstellung der Quadratzahlen modulo 19, die Lösungen sind 6 und 13.

$$z_3 \equiv 1 + 3 \equiv 4 \bmod 19 \qquad , \qquad z_4 \equiv 1 + \frac{13}{2} \equiv 17 \bmod 19$$

$x_5 \equiv 2$ mod 19 und $x_6 \equiv 17$ mod 19 sind die Lösungen der Kongruenz $x^2 \equiv= 4$ mod 19.
$x_7 \equiv 6$ mod 19 und $x_8 \equiv 13$ mod 19 sind die Lösungen der Kongruenz $x^2 \equiv= 17$ mod 19.

Damit sind die Lösungen der gegebenen Kongruenz
$x_1 \equiv 8$ mod 19, $x_2 \equiv 11$ mod 19, $x_3 \equiv 5$ mod 19, $x_4 \equiv 14$ mod 19, $x_5 \equiv 2$ mod 19, $x_6 \equiv 17$ mod 19, $x_7 \equiv 6$ mod 19, $x_8 \equiv 13$ mod 19.

Probe: $8^8 - 15 \cdot 8^6 + 3 \cdot 8^4 - 18 \cdot 8^2 + 6 \equiv 7 - 15 + 14 + 7 + 6 \equiv 0$ mod 19
$11^8 - 15 \cdot 11^6 + 3 \cdot 11^4 - 18 \cdot 11^2 + 6 \equiv 7 - 15 + 14 + 7 + 6 \equiv 0$ mod 19
$5^8 - 15 \cdot 5^6 + 3 \cdot 5^4 - 18 \cdot 5^2 + 6 \equiv 4 - 10 - 6 + 6 + 6 \equiv 0$ mod 19
$14^8 - 15 \cdot 14^6 + 3 \cdot 14^4 - 18 \cdot 14^2 + 6 \equiv 0$ mod 19

$2^8 - 15 \cdot 2^6 + 3 \cdot 2^4 - 18 \cdot 2^2 + 6 \equiv 9 - 10 - 9 + 4 + 6 \equiv 0 \mod 19$
$17^8 - 15 \cdot 17^6 + 3 \cdot 17^4 - 18 \cdot 17^2 + 6 \equiv 0 \mod 19$
$6^8 - 15 \cdot 6^6 + 3 \cdot 6^4 - 18 \cdot 6^2 + 6 \equiv -3 + 6 + 12 - 2 + 6 \equiv 0 \mod 19$
$13^8 - 15 \cdot 13^6 + 3 \cdot 13^4 - 18 \cdot 13^2 + 6 \equiv 0 \mod 19$

4.12 Tabellen der Kubikzahlen

(146) Man stelle Tabellen für die Kubikzahlen modulo p auf für $p = 7$, $p = 11$, $p = 1$.

Lösung: Tabelle der Kubikzahlen modulo 7:

a	1	2	3	4	5	6
a^3	1	1	6	1 6	6	

Tabelle der Kubikzahlen modulo 11:

a	1	2	3	4	5	6	7	8	9	10
a^3	1	8	5	9	4	7	2	6	3	10

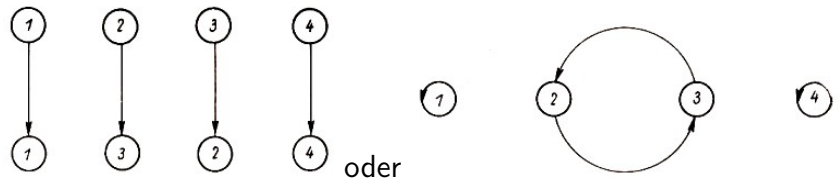
Tabelle der Kubikzahlen modulo 17:

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
a^3	1	8	10	13	6	12	3	2	15	14	5	11	4	7	9	16

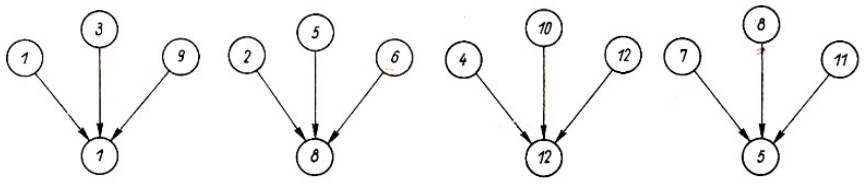
Modulo 7 treten nur die Elemente 1 und 6 als Kubikzahlen auf. Nur aus diesen Zahlen lässt sich die dritte Wurzel modulo 7 ziehen.
In den Tabellen modulo 11 und modulo 17 treten alle Elemente modulo p als Kubikzahlen auf. Hier lassen sich die Kubikzahlen eindeutig den Elementen modulo p zuordnen. Aus jedem Element modulo p lässt sich die dritte Wurzel ziehen.

(147) Es sind grafische Darstellungen für die Kubikzahlen modulo 5, modulo 13 und modulo 19 zu entwickeln.
(Man vergleiche die grafische Darstellung der Multiplikation)

Lösung:

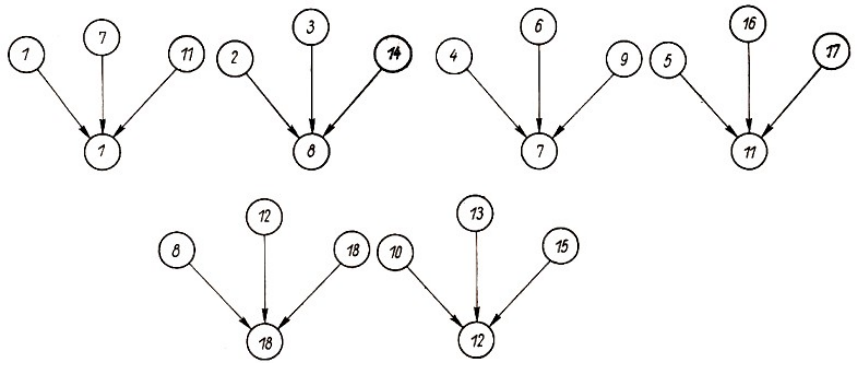
$p = 3$  oder

Aus jedem Element modulo 5 lässt sich die dritte Wurzel ziehen. Man erhält die grafische Darstellung für die Kubikwurzeln durch Umkehrung der Pfeilrichtungen in den grafischen Darstellungen der Kubikzahlen.

$p = 13$ 

Es treten nur die Elemente 1, 5, 8 und 12 als Kubikzahlen auf. Die Kubikwurzeln aus diesen Elementen liefern jeweils drei voneinander verschiedene Lösungen.

$p = 19$



Es treten als Kubikzahlen die Elemente $1, 7, 8, 11, 42$ und 18 auf. Die Kubikwurzeln aus diesen Elementen liefern jeweils drei voneinander verschiedene Lösungen.

(148)• Man stelle Tabellen für die Kubikzahlen modulo p auf für $p = 13$, $p = 23$, $p = 31$.

4.13 Kubische Kongruenzen

(149) Es ist zu zeigen, dass sich die Kubikwurzeln aus den Elementen modulo p ziehen lassen und dass eine eindeutige Zuordnung aller Elemente modulo p zu den Kubikwurzeln dieser Elemente besteht, wenn p die Form $p = 3n + 2$ hat.

Lösung:
Es soll zunächst gezeigt werden, dass genau eine Lösung der Kongruenz $x^3 \equiv 1$ mod p existiert. Nach dem kleinen Satz von Fermat gilt $x^{p-1} \equiv 1$ mod p. Mit $p = 3n + 2$ folgt $x^{3n+1} \equiv 1$ mod p. Durch Potenzieren der Kongruenz $x^3 \equiv 1$ mod p mit dem Exponenten n ergibt sich $x^{3n} \equiv 1$ mod p. Die Division beider Kongruenzen liefert

$$\frac{x^{3n+1}}{x^{3n}} \equiv 1 \bmod p \qquad \text{oder} \qquad x \equiv 1 \bmod p$$

Die Kongruenz $z^3 \equiv 1$ mod p hat genau die eine Lösung $x \equiv 1$ mod p.

Es wird nun gezeigt, dass auch die Kongruenz $x^3 \equiv c$ mod p $(0 < c < p)$ genau eine Lösung besitzt.
Man führt den Beweis indirekt und nimmt an, dass $x_1 \equiv a$ mod p und $x_2 \equiv b$ mod p zwei voneinander verschiedene Lösungen der Kongruenz $x^3 \equiv c$ mod p sind. Es folgt:
$a^3 \equiv c$ mod p und $b^3 \equiv c$ mod p und nach Division:

$$\frac{a^3}{b^3} \equiv 1 \bmod p \qquad \text{und} \qquad \left(\frac{a}{b}\right)^3 \equiv 1 \bmod p$$

Oben wurde gezeigt, dass die Kongruenz $x^3 \equiv 1$ mod p genau die eine Lösung $x = 1$ mod p besitzt. Daraus folgt:

$$\frac{a}{b} \equiv 1 \bmod p \qquad \text{oder} \qquad a \equiv b \bmod p$$

Für jedes a hat die dritte Wurzel aus a nur eine Lösung.

Erhebt man nun alle Elemente modulo p in die dritte Potenz, so erhält man lauter voneinander verschiedene Ergebnisse, weil nicht zwei Elemente das gleiche Ergebnis liefern können. Folglich ist die Anzahl der voneinander verschiedenen Ergebnisse gleich der Anzahl der Elemente modulo p.

Nach dem Dirichletschen Prinzip ist eine eindeutige Zuordnung aller Elemente modulo p zu den Kubikzahlen dieser Elemente gegeben, wenn $p = 3n + 2$ ist. Aus jedem Element modulo p lässt sich dann die dritte Wurzel ziehen.

(150) Es ist zu zeigen, dass die dritte Wurzel aus dem Element 1 modulo p drei voneinander verschiedene Lösungen liefert, wenn die Quadratwurzel aus dem Element -3 existiert.

Lösung:
Es sei die Kongruenz $x^3 \equiv 1$ mod p gegeben. Es gilt die Identität

$$x^3 - 1 \equiv (x-1)(x^2 + x + 1)$$

Aus $x^3 \equiv 1$ mod p folgt

$$x^3 - 1 \equiv (x-1)(x^2 + x + 1) \equiv 0 \bmod p$$

Aus $(x-1) \equiv 0$ mod p folgt $x_1 \equiv 1$ mod p.
Die Lösung der quadratischen Kongruenz $x^2 x + 1 \equiv 0$ mod p liefert

$$x_{2;3} = -\frac{1}{2} \pm \frac{1}{2}\sqrt{-3} \bmod p$$

Drei Lösungen der Kongruenz $x^3 \equiv 1$ mod p existieren also genau dann, wenn die Quadratwurzel aus dem Element -3 mod p existiert.

Bemerkung: Es ist eine Verallgemeinerung der Aufgabe möglich, wenn man die Identität $x^3 - a^3 \equiv (x-a)(x^2 + ax + a^2)$ mod p zugrunde legt.
Die Kongruenz $x^3 \equiv a^3$ mod p liefert folgende Lösungen:

$$x_1 \equiv a \bmod p \qquad , \qquad x_{2;3} \equiv -\frac{a}{2} \pm \frac{a}{2}\sqrt{-3} \bmod p$$

Allgemein gilt: Existiert aus einem Element modulo p die dritte Wurzel, so gehören drei Elemente zur Lösungsmenge, falls die Quadratwurzel aus dem Element -3 mod p existiert.

(151) Man löse die Kongruenzen
a) $x^3 \equiv 1$ mod 73, b) $x^3 \equiv 28$ mod 97,
c) $x^3 + 2 \equiv 0$ mod 109, d) $x^3 - 79 \equiv 0$ mod 307.

Lösung:
a) $x^3 - 1 \equiv 0$ mod 73, $(x-1)(x^2 + x + 1) \equiv 0$ mod 73.
$\sqrt{-3} \equiv 17$ mod 73 $\quad (289 \equiv -3$ mod 73)
$x_1 = 1$ mod 73, $\quad x_{2;3} = -\frac{1}{2} \pm \frac{17}{2}$ mod 73, $\quad x_2 = 8$ mod 73, $\quad x_3 = -9 \equiv 64$ mod 73,

Probe:
$8^3 - 1 = 511 = 7 \cdot 73$, $7 \cdot 73 \equiv 0$ mod 73,
$64^3 - 1 = 262143 = 3591 \cdot 73$, $3591 \cdot 73 \equiv 0$ mod 73,

b) $x^3 \equiv 28 \equiv 28 + 97 \equiv 125$ mod 97
$x^3 - 125 \equiv (x-5)(x^2 + 5x + 25) \equiv 0$ mod 97.
$x_1 \equiv 5$ mod 97, $\quad \sqrt{-3} \equiv 26$ mod 97
$x_{2;3} \equiv -\frac{5}{2} \pm 65$ mod 97, $\quad x_2 \equiv 14$ mod 97, $\quad x_3 \equiv 78$ mod 97,

Probe:
$5^3 = 125 = 1 \cdot 97 + 28$

$14^3 = 2744 = 28 \cdot 97 + 28$
$78^3 = 474552 = 4892 \cdot 97 + 28$

c) $x^3 \equiv -2 \equiv 216$ mod 109.
$x^3 - 216 \equiv (x-6)(x^2+6x+36) \equiv 0$ mod 109.
$x_1 \equiv 6$ mod 109, $\sqrt{-3} \equiv 18$ mod 109
$x_{2;3} \equiv -3 \pm 54$ mod 109, $x_2 \equiv 51$ mod 109, $x_3 \equiv -57 \equiv 52$ mod 109

Probe:
$6^3 + 2 = 216 + 2 = 218 = 2 \cdot 109$,
$51^3 + 2 = 132653 = 1217 \cdot 109$,
$52^3 + 2 = 140610 = 1290 \cdot 109$

d) $x^3 \equiv 79$ mod 307, $79 \equiv 1000$ mod 307
$x^3 - 1000 \equiv (x-10)(x^2+10x+100) \equiv 0$ mod 307.
$x_1 \equiv 10$ mod 307, $\sqrt{-3} \equiv 35$ mod 307.
$x_{2;3} \equiv -5 \pm 175$ mod 307, $x_2 \equiv 170$ mod 307, $x_3 \equiv 127$ mod 307

Probe:
$10^3 - 79 = 1000 - 79 = 921 = 3 \cdot 307$,
$170^3 - 79 = 4912921 = 16003 \cdot 307$,
$127^3 - 79 = 6672 \cdot 307$

5 Logarithmen modulo p

5.1 Logarithmentabellen, Gesetze

Definition: Sind für eine Zahl a mod p die Potenzen $a^k \equiv x$ mod p für $k = 0, 1, 2, ..., (p-2)$ alle voneinander verschieden, so heißt k der "Logarithmus" von x, die Zahl a heißt "Basis".

Als Zeichen verwenden wir $k = \log_a x$ (Logarithmus x zur Basis a).
Die Zahl Null hat keinen Logarithmus. Für $k = 0$ und $k = (p-1)$ sind für jede Basis a die Potenzen a^k jeweils kongruent modulo p. Statt "Logarithmus" x sagt man auch "Index" von x $(\operatorname{ind} x)$.

(152) Man entwickle eine logarithmische Tabelle für $p = 17$. Man löse die Kongruenz $x \equiv \frac{9 \cdot 11^3}{7^4}$ mod 17.

Lösung:
Gesucht ist jetzt eine Basis a, für die die Potenzen a^k mod 17 für $k = 0, 1, ..., 15$ ($a^{16} \equiv 1$ mod 17) gerade alle von Null verschiedenen Elemente mod 17 ergeben.
Für $a = 2$ ergibt sich folgende Potenztabelle:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$2^k \equiv x$ mod 17	1	2	4	8	16	15	13	9	1	2	4	8	16	15	13	9	1

Aus der Tabelle ersieht man, dass eine eineindeutige Zuordnung der Elemente modulo 17 zu den Potenzen modulo 17 für $a = 2$ nicht existiert. Zum Beispiel ist $2^5 \equiv 15$ mod 17 und auch $2^{13} \equiv 15$ mod 17.
$a = 2$ kann als Basis für eine logarithmische Tabelle nicht in Frage kommen.

Für $a = 3$ ergibt sich folgende Potenztabelle:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$3^k \equiv x$ mod 17	1	3	9	10	13	5	15	11	16	14	8	7	4	12	2	6	1

Schränkt man die Bedingung für k ein und fordert $k < p - 1 = 16$, so ist in dieser Tabelle eine eineindeutige Zuordnung der Exponenten k zu den Potenzwerten $a^k \equiv x \not\equiv 0$ mod 17 gegeben.
Während man bei den Potenzwerten nach dem Modul 17 rechnet, muss man bei den Exponenten k nach dem Modul $p - 1 = 16$ rechnen. Zu jedem Exponenten k mod 16 gehört genau ein Potenzwert x mod 17, und umgekehrt gehört zu jedem Potenzwert x mod 17 genau ein Exponent k mod 16.
Aus $3^k \equiv x$ mod 17 folgt $k = \log_3 x$ mod 16.

Logarithmengesetze:

1. $\log_3 xy \equiv \log_3 x + \log_3 y$ mod 16

Aus $\log_3 x \equiv k_1$ mod 16 und $\log_3 y \equiv k_2$ mod 16 folgt $x \equiv 3^{k-1}$ mod 17 und $y \equiv 3^{k-2}$ mod 17.
Aus $3^{k_1+k_2} \equiv xy$ mod 17 folgt schließlich $k_1 + k_2 \equiv \log_3 xy$ mod 16.
Ein Produkt wird logarithmiert, indem man die Logarithmen der Faktoren addiert.

2. $\log_3 \frac{x}{y} \equiv \log_3 x - \log_3 y$ mod 16

$3^{k_1-k_2} \equiv \frac{x}{y}$ mod 17 ergibt $k_1 - k_2 \equiv \log_3 \frac{x}{y}$ mod 16
Ein Quotient wird logarithmiert, indem man den Logarithmus des Nenners vom Logarithmus

des Zählers subtrahiert.

3. $\log_3 x^n = n \cdot \log_3 x$ mod 16

$(3^{k_1})^n = 3^{nk_1} \equiv x^n$ mod 17 liefert $nk_1 \equiv \log_3 x^n$ mod 16.
Eine Potenz wird logarithmiert, indem man den Exponenten mit dem Logarithmus der Basis multipliziert.

Die Umkehrung der Potenztabelle für $a = 3$ ergibt die gesuchte logarithmische Tabelle für den Modul $p = 17$.

x mod 17	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
$\log_3 x$ mod 16	0	14	1	12	5	15	11	10	2	3	7	13	4	9	6	8

Lösung der Kongruenz $x \equiv \frac{9 \cdot 11^3}{7^4}$ mod 17.

$$\log_3 x \equiv \log_3 9 + 3 \cdot \log_3 11 - 4 \log_3 7 \bmod 16 \equiv 2 + 21 - 44 \equiv -21 \equiv 11 \bmod 16$$

Daraus folgt: $x \equiv 7$ mod 17.

Probe: $11^2 \equiv 2$ mod 17, $11^3 \equiv 5$ mod 17, $9 \cdot 11^3 \equiv 11$ mod 17, $7^2 \equiv 15 \equiv -2$ mod 17, $7^4 \equiv (-2)^4 \equiv 4$ mod 17.
$x \equiv \frac{11}{4} \equiv 7$ mod 17, da $4 \cdot 7 \equiv 11$ mod 17.

Bemerkung: Für jede Primzahl p kann eine derartige Logarithmentabelle entwickelt werden. In den Potenztabellen modulo p treten Zyklen auf, und für mindestens eine Basis a sind alle Elemente $1, 2, 3, ..., (p-1)$ in einem einzigen Zyklus enthalten.
Für ein solches a ist eine eineindeutige Zuordnung der Exponenten k mod $(p-1)$ zu den Potenzwerten $a^k \equiv x$ mod p stets gegeben.

Die logarithmische Rechnung bietet gewisse Vorteile gegenüber der gewöhnlichen Rechnung. Es treten keine approximierten, sondern exakte Lösungen auf. Man benötigt keine umfangreichen Tabellenbücher mit etwa 4-, 5- oder gar 7stelligen Logarithmen.
Nachteile gegenüber der gewöhnlichen Logarithmenrechnung sind, dass man hier für jeden anderen Primzahlmodul eine neue Logarithmentabelle entwickeln muss. Im Anhang sind logarithmische Tabellen für die Primzahlen kleiner als 100 angegeben.

Für Nichtprimzahlen existieren derartige Logarithmentabellen nicht, weil bei Nichtprimzahlen eine eineindeutige Zuordnung bei den Potenztabellen fehlt.

5.2 Das Rechnen mit Logarithmentabellen

Man stelle eine Logarithmentabelle für den Modul $p = 67$ auf und berechne mit Hilfe dieser Tabelle

a) $2475x \equiv 3648$ mod 67
b) $x \equiv \frac{37}{38}$ mod 67
c) $x \equiv 37^{38}$ mod 67
d) $x \equiv 1965^{1967}$ mod 67
e) $x \equiv \frac{27^1 3 \cdot 25^{19} \cdot 19^{23}}{37^{23} \cdot 35^{29} \cdot 31^{31}}$ mod 67
f) $x \equiv \frac{808^{707}}{707^{808}}$ mod 67
g) $x \equiv 2222^{3333}$ mod 67
h) $x \equiv 11111^{22222} + 33333^{44444}$ mod 67
i) $x \equiv \frac{487^{11}}{513^{13}} + \frac{9216^{17}}{10327^{19}}$ mod 67

sowie die ganzzahligen Lösungen der Gleichungen

$$\text{k) } 67x - 168y = 366 \quad \text{l) } 1005x - 2431y = 307.$$

Lösung:
Potenztabelle für die Basis $a = 2$ mod 67:

k	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2^k	1	2	4	8	16	32	64	61	55	43	19	38	9	18	36	5	10
k	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33
2^k	20	40	13	26	52	37	7	14	28	56	45	23	46	25	50	33	66
k	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50
2^k	65	63	59	51	35	3	6	12	24	48	29	58	49	31	62	57	47
k	51	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66	
2^k	27	54	41	15	30	60	53	39	11	22	44	21	42	17	34	1	

Wie aus der Tabelle ersichtlich, ist eine eineindeutige Zuordnung der Menge der Exponenten k mod 66 zu den Elementen der Menge der Potenzen 2^k mod 67 gegeben. Daraus ergibt sich die Logarithmentabelle für $p = 67$ ($y = \log_2 x$ mod 66):

x mod 67	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
y	0	1	39	2	15	40	23	3	12	16	59	41	19	24	54	4	64
x mod 67	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34
y	13	10	17	62	60	28	42	30	20	51	25	44	55	47	5	32	65
x mod 67	35	36	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51
y	38	14	22	11	58	18	53	63	9	61	27	29	50	43	46	31	37
x mod 67	52	53	54	55	56	57	58	59	60	61	62	63	64	65	66		
y	21	57	52	8	26	49	45	36	56	7	48	35	6	34	33		

a) $2475 \equiv 63$ mod 67, $3648 \equiv 30$ mod 67, $632 \equiv 30$ mod 67.
$\log_2 x \equiv \log_2 30 - \log_2 63 \equiv 55 - 35 \equiv 20$ mod 66, $x \equiv 26$ mod 67.

Probe: $63 \cdot 26 = 1638 = 24 \cdot 67 + 30$.

b) $\log_2 x = \log_2 37 - \log_2 38 \equiv 22 - 11 = 11$ mod 66, $x \equiv 38$ mod 67.

Probe: $38 \cdot 38 = 1444 = 21 \cdot 67 + 37$.

c) $\log_2 x \equiv 38 \cdot \log_2 37 \equiv 38 \cdot 22 \cdot 836 \cdot 44$ mod 66, $x \equiv 29$ mod 67.

Probe: $37^2 \equiv 29$ mod 67, $37^4 \equiv 37$ mod 67, $37^{4k-2} \equiv 29$ mod 67.

d) $1965 \equiv 22$ mod 67, $1967 \equiv 53 \equiv -13$ mod 66.
$\log_2 x \equiv (-13) \log_2 22 \equiv -13 \cdot 60 \equiv 78 \equiv 12$ mod 66, $x \equiv 9$ mod 67.

Probe: $22^2 \equiv 15$ mod 67, $22^4 \equiv 24$ mod 67, $22^8 \equiv 40$ mod 67, $22^{16} \equiv -8$ mod 67, $22^{32} \equiv -3$ mod 67, $22^{53} = 3 \cdot 8 \cdot 24 \cdot 22 \equiv 9$ mod 67.

e) $\log_2 x \equiv 13 \log_2 27 + 19 \log_2 25 + 23 \log_2 19 - 23 \log_2 37 - 29 \log_2 35 - 31 \log_2 31 \equiv$
$\equiv 13 \cdot 51 + 19 \cdot 30 + 23 \cdot 10 - 23 \cdot 22 - 28 \cdot 38 - 31 \cdot 47 \equiv 3 + 42 + 32 - 44 - 46 - 5 \equiv$
$\equiv -18 \equiv 48$ mod 66, $x \equiv 62$ mod 67.

Probe: $27^{13} \equiv 8$ mod 67, $25^{19} \equiv 24$ mod 67, $19^{23} \equiv 33$ mod 67, $37^{23} \equiv 29$ mod 67,

$35^{29} \equiv 49$ mod 67, $31^{31} \equiv 32$ mod 67.
$x = \frac{38}{46} = \frac{19}{23}$ mod 67,
$23x \equiv 19$ mod 67, $23 \cdot 62 \equiv 19$ mod 67, $19 = 19$

f) $808 \equiv 4$ mod 67, $707 \equiv 37$ mod 67, $808 \equiv 16$ mod 66, $707 \equiv 47$ mod 66.
$x \equiv 47 \log_2 4 - 18 \log_2 37 \equiv 47 \cdot 2 - 16 \cdot 22 = 6$ mod 66, $x \equiv 64$ mod 67.

Probe: $808^{707} \equiv 23$ mod 67, $707^{808} \equiv 37$ mod 67.
$x \equiv \frac{23}{37}$ mod 67, $37x \equiv 23$ mod 67.
$37 \cdot 64 \equiv 23$ mod 67, $23 = 23$,

g) $2222 \equiv 11$ mod 67,
$\log_2 x \equiv 33 \log_2 11 \equiv 33 \cdot 59 \equiv 33$ mod 66. $x \equiv 66$ mod 67.

Probe: $2222^{3333} \equiv 11^{33}$ mod 67, $11^{32} \equiv 6$ mod 67, $11^{33} \equiv 66$ mod 67, $66 = 66$.

h) $111141 \equiv 56$ mod 67, $33333 \equiv 34$ mod 67, $22222 \equiv 46$ mod 66, $44444 \equiv 26$ mod 66.
$x \equiv a + b$ mod 67, $\log_2 a \equiv 46 \log_2 56 \equiv 46 \cdot 26 \equiv 8$ mod 66,
$x \equiv a + b \equiv 61$ mod 67.

Probe: $56^{46} \equiv 55$ mod 67, $34^2 4 \equiv 6$ mod 67.

i) $x \equiv a + b$ mod 67, $487 \equiv 18$ mod 67, $513 \equiv 44$ mod 67,
$9216 \equiv 37$ mod 67, $10327 \equiv 9$ mod 67.
$\log_2 a \equiv 11 \log_2 18 - 13 \log_2 44 \equiv 10$ mod 66; $a \equiv 19$ mod 67.
$\log_2 b \equiv 17 \log_2 37 - 19 \log_2 9 \equiv 44$ mod 66; $b \equiv 36$ mod 67.
$x \equiv a + b \equiv 55$ mod 67.

Probe: $18^{11} \equiv 38$ mod 67, $44^{13} \equiv 2$ mod 67, $a \equiv 19$ mod 67,
$37^{17} \equiv 29$ mod 67, $9^{19} \equiv 25$ mod 67, $b \equiv \frac{29}{25} \equiv 36$ mod 67.

k) $-168y \equiv -34y \equiv 33y \equiv 366 \equiv 31$ mod 67.
$\log_2 y \equiv \log_2 31 - \log_2 33 \equiv 47 - 32 \equiv 15$ mod 66, $y \equiv 5$ mod 67, $y = 67k + 5$.
Durch Einsetzen in die Ausgangsgleichung folgt
$67x - 168 \cdot 67k - 168 \cdot 5 = 366$
$67x - 67 \cdot 168k - 67 \cdot 18 = 0$, $z = 168k + 18$.

Probe für $k = 0$: $z = 18$, $y = 5$. $67 \cdot 18 - 168 \cdot 5 = 366$, $366 = 366$.

l) $1005 = 3 \cdot 5 \cdot 67$.
$-243ly \equiv -y \equiv 307 \equiv 1$ mod 3, $y \equiv -1 \equiv 2$ mod 3.
$-243ly \equiv -y \equiv 307 \equiv 2$ mod 5, $y \equiv -2 \equiv 3$ mod 5.
$-243ly \equiv -19y \equiv 48y \equiv 307 \equiv 39$ mod 67
$\log_2 y \equiv \log_2 39 - \log_2 48 \equiv 58 - 43 \equiv 15 mod 66$, $y \equiv 5$ mod 67.

Es ist nun die natürliche Zahl y zu bestimmen, die bei der Division durch 3, 5 und 67 die Reste 2, 3 und 5 lässt.

Ansatz:
$x_1 = 5 \cdot 67y_1 = 335y_1$, $x_2 = 3 \cdot 67y_2 = 201y_2$, $x_3 = 3 \cdot 5y_3 = 15y_3$
$x_1 \equiv 2$ mod 3, $x_2 \equiv 3$ mod 5, $x_3 \equiv 5$ mod 67
$x_1 \equiv 335y_1 \equiv 2$ mod 3, $x_2 \equiv 201y_2 \equiv 3$ mod 5, $x_3 \equiv 15y_3 \equiv 5$ mod 67
$2y_1 \equiv 2$ mod 3, $y_2 \equiv 3$ mod 5, $y_1 = 1$, $y_2 = 3$

$\log_2 y_3 \equiv \log_2 5 - \log_2 15 \equiv 15 - 54 \equiv -39 \equiv 27$ mod 67, $y_3 \equiv 45$ mod 67, $y_3 = 45$
Damit ergibt sich
$x - 1 = 335$, $x_2 = 603$ $x_3 = 675$ und es wird $y = x_1 + x_2 + x_3 = 335 + 603 + 675 = 1613$.

Durch Einsetzen in die Ausgangsgleichung ergibt sich

$$1005x - 2431 \cdot 608 = 307 \qquad , \qquad x = 1471$$

Eine spezielle Lösung der diophantischen Gleichung ist $x = 1471$, $y = 608$ ($1613 \cdot 608$ mod 1005).
Die allgemeine Lösung lautet $x = 1471 + 2431k$, $y = 608 + 1005k$.

Probe für $k = 0$: $1005 \cdot 1471 - 2431 \cdot 608 = 1478355 - 1478048 = 307$, $307 = 307$

(154)• Man stelle eine logarithmische Tabelle für $p = 83$ auf und löse die Kongruenzen
a) $67x \equiv 17$ mod 83, b) $37^{39} \equiv x$ mod 83.

5.3 Diophantische Gleichungen

(155) Man ermittle die ganzzahligen Lösungen der Gleichung

$$17x + 37y = 100$$

Lösung:
Wir betrachten die gegebene Gleichung modulo 17 und erhalten $17x \equiv 0$ mod 17, $37y \equiv 3y$ mod 17, $100 \equiv 15$ mod 17.
Es gilt also $3y \equiv 15$ mod 17 oder $y = 17k + 5$.
Nach Einsetzen in die Ausgangsgleichung folgt

$$\begin{aligned} 17x + 37 \cdot 17k + 37 \cdot 5 - 100 &= 0 \\ 17x + 37 \cdot 17k + 37 \cdot 5 - 20 \cdot 5 &= 0 \\ 17x + 37 \cdot 17k + 17 \cdot 5 &= 0 \\ x + 37k + 5 &= 0 \qquad \text{oder} \qquad x = -37 - 5 \end{aligned}$$

Probe für $k = 0$: $a = -5$, $y = 5$, $-85 + 185 = 100$; $100 = 100$

(156) Man ermittle die ganzzahligen Lösungen der Gleichung $17x - 94y = 243$ mit Hilfe der in Aufgabe (152) aufgestellten Logarithmentabelle.

Lösung:
Es gilt $-9y \equiv 5$ mod 17, $9y \equiv -5 \equiv 12$ mod 17, $y = \frac{4}{3}$ mod 17,
$\log_3 y \equiv \log_3 4 - \log_3 3 \equiv 12 - 1 \equiv 11$ mod 16. $y \equiv 7$ mod 17, $y = 17k + 7$.

$$\begin{aligned} 17x - 94 \cdot 17k - 94 \cdot 7 - 243 &= 0 \\ 17x - 94 \cdot 17k - 901 &= 0 \\ 17x - 94 \cdot 17k - 53 \cdot 17 &= 0 \\ x - 94k - 53 &= 0 \qquad , \qquad x = 94k + 53 \end{aligned}$$

Probe für $k = 0$: $a = 53$, $y = 7$, $901 - 658 = 243$; $243 = 243$.

(157)• Gegeben ist eine Menge von n Elementen ($n < 160$) in linearer Anordnung.

Fasst man die Elemente in Dreiergruppen zusammen, so bleibt ein Element übrig. Dieses eine sowie das jeweils letzte in jeder Dreiergruppe nimmt man aus der ursprünglichen Menge heraus.

Fasst man die übriggebliebenen Elemente wieder in Dreiergruppen zusammen, so bleibt wieder ein Element übrig. Dieses eine sowie das jeweils letzte in jeder Dreiergruppe nimmt man aus der Menge heraus. Die restlichen Elemente fasst man wiederum in Gruppen zu je drei Elementen zusammen.
Dabei bleibt wiederum ein Element übrig. Dieses eine sowie das jeweils letzte Element jeder Gruppe nimmt man nochmals aus der Menge heraus. Die verbleibenden Elemente fasst man nochmals in Gruppen zu je drei Elementen zusammen, wobei wiederum ein Element übrig bleibt. Dieses eine sowie das jeweils letzte Element jeder Gruppe nimmt man nochmals aus der Menge heraus.
Wieviele Elemente hatte die ursprüngliche Menge?

(158)• Gegeben sind die natürlichen Zahlen $n_1, n_2, n_3, ..., n_m$. Für jede folgende Zahl n_{k+1} gilt in Bezug auf die vorhergehende Zahl n_k:

$$n_{k+1} = \frac{m-1}{m}(n_k - 1)$$

Man berechne n_1 für $m = 5$.

(159)• Vor einigen Jahren stellte ein Mathematiklehrer die folgende Aufgabe:

"Dividiere ich die Zahl meines Geburtsjahres durch 41, durch 31 und durch 21, so erhalte ich die Reste 33, 28 bzw. 8. Dividiere ich die Zahl meines Geburtsjahres jedoch durch 67, durch 29 und durch 17, so erhalte ich als Reste das Alter, das ich in diesem Jahr erreiche, die Zahl meines Geburtsmonats und die Zahl meines Geburtstages."
In welchem Jahr wurde diese Aufgabe gestellt? Wann wurde der Lehrer geboren?

5.4 Divisionsreste

(160) Welche natürlichen Zahlen lassen bei der Division durch 7 den Rest 2, bei der Division durch 13 den Rest 5?

Lösung:
Ansatz: $x = 7u + 13v$
Es gilt: $x \equiv 13v \equiv 2$ mod 7, $6v \equiv -v \equiv 2$ mod 7, $v \equiv -2$ mod 7.
$x \equiv 7u \equiv 5$ mod 13, $7u \equiv 5$ mod 13,
$u \equiv \frac{5}{7} \equiv \frac{4}{3}\frac{4+26}{3} \equiv 10$ mod 13

$x = 7 \cdot 10 + 13 \cdot (-2) = 44$ ist eine Lösung der Aufgabe.
Durch Addition eines beliebigen Vielfachen von $7 \cdot 13 = 91$ erhält man weitere Lösungen. Die allgemeine Lösung lautet $x = 44 + 91k$.

Probe: für $k = 0$: $x = 44$, $44 \equiv 2$ mod 7, $44 \equiv 5$ mod 13.
für $k = 1$: $x = 135$, $135 \equiv 2$ mod 7, $135 \equiv 5$ mod 13.

(161) Welche natürlichen Zahlen lassen bei der Division durch 31 den Rest 17 und bei der Division durch 41 den Rest 23?

Lösung:
$x = 31u + 41v$.

$x \equiv 41v \equiv 17 \bmod 31$, $10v \equiv 17 \bmod 31$, $v \equiv \frac{17}{10} \equiv \frac{24}{5} \equiv \frac{55}{5} \equiv 11 \bmod 31$
$x \equiv 31u \equiv 23 \bmod 41$, $31u \equiv 23 \bmod 41$, $u \equiv \frac{23}{31} \equiv \frac{9}{5} \equiv \frac{50}{5} \equiv 10 \bmod 41$

$x = 31 \cdot 10 + 41 \cdot 11 = 761$
Allgemeine Lösung: $x = 761 + 41 \cdot 31k = 761 + 1271k$.

Probe: $k = 0$, $x = 761$, $761 \equiv 17 \bmod 31$, $761 \equiv 23 \bmod 41$.
$k = 1$, $x = 2032$, $2032 \equiv 17 \bmod 31$, $2032 \equiv 23 \bmod 41$.

(162) Welche natürlichen Zahlen lassen bei der Division durch 7 den Rest 5, bei der Division durch 11 den Rest 8 und bei der Division durch 13 den Rest 11?

Lösung:
Der Ausdruck $x = 7u + 11v + 13w$ würde modulo 7, modulo 11 oder modulo 13 noch stets zwei unbekannte Variable enthalten. Man geht deshalb von folgendem Ansatz aus:

$$x = 7 \cdot 11u + 7 \cdot 13v + 11 \cdot 13w = 77u + 91v + 143w$$

Es gilt:
$x \equiv 143w \equiv 5 \bmod 7$, $w \equiv \frac{5}{3} \equiv \frac{12}{3} \equiv 4 \bmod 7$.
$x \equiv 91v \equiv 8 \bmod 11$, $v \equiv \frac{8}{3} \equiv 10 \bmod 11$.
$x \equiv 77u \equiv 11 \bmod 13$, $u \equiv -11 \equiv 2 \bmod 13$.
$x = 77 \cdot 2 + 91 \cdot 10 + 143 \cdot 4 = 1636$.

Da es auf Vielfache der Zahl $7 \cdot 11 \cdot 13 = 1001$ nicht ankommt, gilt $x = 635$. Damit wird die allgemeine Lösung: $x = 635 + 1001k$.

Probe: $k = 0$, $z = 63$, $635 \equiv 5 \bmod 7$, $635 \equiv 8 \bmod 11$, $635 \equiv 11 \bmod 13$.

(163)• Welche natürlichen Zahlen lassen bei der Division durch 11 den Rest 5 und bei Division durch 17 den Rest 7?

(164)• Welche natürlichen Zahlen lassen bei der Division durch 23 den Rest 19 und bei Division durch 37 den Rest 31?

(165)• Welche natürlichen Zahlen x mit $3000 < x < 4000$ lassen bei der Division durch 31 den Rest 18 und bei Division durch 41 den Rest 7?

(166)• Gesucht ist die kleinste natürliche Zahl n, die bei der Division durch 2 den Rest 1, bei Division durch 3 den Rest 2, bei der Division durch 5 den Rest 4 und bei der Division durch 7 den Rest 6 lässt!

(167)• Gesucht sind alle natürlichen Zahlen, die bei der Division durch 11 den Rest 7, bei der Division durch 31 den Rest 18 und bei der Division durch 61 den Rest 39 lassen.

5.5 Das Lösen von Kongruenzen

(168) Man löse die Kongruenz $573x \equiv 1733 \bmod 1547$.

Lösung:
Es gilt: $1547 = 7 \cdot 13 \cdot 17$.
Man betrachtet die gegebene Kongruenz zunächst modulo 7, modulo 13 und modulo 17.

$573x_1 \equiv 6x_1 \equiv -x_1 \equiv 733 \equiv 5 \bmod 7$, $x_1 \equiv -5 \equiv 2 \bmod 7$
$573x_2 \equiv x_2 \equiv 733 \equiv 5 \bmod 13$, $x_2 \equiv 5 \bmod 13$

$573x_3 \equiv 12x_3 \equiv 733 \equiv 2 \bmod 17$, $x_3 \equiv 3 \bmod 17$

Es wird nun die natürliche Zahl x gesucht, die bei der Division durch 7 den Rest 2, bei Division durch 13 den Rest 5 und bei Division durch 17 den Rest 3 lässt.
$x = 91u + 119v + 221w$
$x \equiv 221w \equiv 2 \bmod 7$, $w \equiv \frac{1}{2} \equiv 4 \bmod 7$
$x \equiv 119v \equiv 5 \bmod 13$, $v \equiv \frac{5}{2} \equiv 9 \bmod 13$
$x \equiv 91u \equiv 3 \bmod 17$, $u \equiv \frac{1}{2} \equiv 9 \bmod 17$

Damit wird: $x = 91 \cdot 9 + 119 \cdot 9 + 221 \cdot 4 = 2774$.
$x \equiv 2774 \equiv 1227 \bmod 1547$ ist die Lösung der gegebenen Kongruenz.

Probe: $573 \cdot 1227 = 703071 = 454 \cdot 1547 + 733$.

Bemerkung: Das hier angegebene Verfahren der Zurückführung eines Moduls m auf kleinere Moduln ist stets dann möglich, wenn die in m enthaltenen Faktoren paarweise teilerfremd sind. Es wird hier nur auf den Fall eingegangen, wo paarweise Teilerfremdheit vorliegt.

(169) Zu lösen ist die Kongruenz $13877x = 8733 \bmod 24035$.

Lösung:
Es gilt: $24035 = 5 \cdot 11 \cdot 19 \cdot 23$.
Man betrachtet die gegebene Kongruenz modulo 5, modulo 11, modulo 19 und modulo 23.

$13877x_1 \equiv 2x_1 \equiv 8733 \equiv 3 \bmod 5$, $x_1 \equiv \frac{3}{2} \equiv 4 \bmod 5$.
$13877x_2 \equiv 6x_2 \equiv 8733 \equiv 10 \bmod 11$, $x_2 \equiv \frac{5}{3} \equiv 9 \bmod 11$.
$13877x_3 \equiv 7x_3 \equiv 8733 \equiv 12 \bmod 19$, $x_3 \equiv -1 \equiv 18 \bmod 19$.
$13877x - 4 \equiv 8x - 4 \equiv 8733 \equiv 16 \bmod 23$, $x - 4 \equiv \frac{16}{8} \equiv 2 \bmod 23$.

Es wird nun die natürliche Zahl x gesucht, die bei Division durch 5 den Rest 4, bei Division durch 11 den Rest 9, bei Division durch 19 den Rest 18 und bei Division durch 23 den Rest 2 lässt.

Ansatz:
$x = 5 \cdot 11 \cdot 19u + 5 \cdot 11 \cdot 23v + 5 \cdot 19 \cdot 23w + 11 \cdot 29 \cdot 23z$
Es gilt:

$x \equiv 4 \bmod 5$, $x \equiv 11 \cdot 19 \cdot 23z \equiv 1 \cdot 4 \cdot 3z \equiv 2z \equiv 4 \bmod 5$, $z \equiv 2 \bmod 5$,
$x \equiv 9 \bmod 11$, $x \equiv 5 \cdot 19 \cdot 23w \equiv 7w \equiv 9 \bmod 11$, $w \equiv 6 \bmod 11$,
$x \equiv 18 \bmod 19$, $x \equiv 5 \cdot 11 \cdot 23v \equiv 11v \equiv 18 \bmod 19$, $v \equiv 12 \bmod 19$,
$x \equiv 2 \bmod 23$, $x \equiv 5 \cdot 11 \cdot 19u \equiv 10u \equiv 2 \bmod 23$, $u \equiv 14 \bmod 23$,

Damit wird:

$$x = 5 \cdot 11 \cdot 19 \cdot 14 + 5 \cdot 11 \cdot 23 \cdot 12 + 5 \cdot 19 \cdot 23 \cdot 6 + 11 \cdot 19 \cdot 23 \cdot 2 = 52534$$

$x \equiv 52534 \equiv 4464 \bmod 24035$ ist die Lösung der gegebenen Kongruenz.

Probe: $13877 \cdot 4464 = 61946928 = 2577 \cdot 24035 + 8733$.

(170)• Man löse die Kongruenz $561x \equiv 432 \bmod 665$.

6 Anhang

6.1 Lösungen der zusätzlichen Aufgaben

(6)• Eine Gerade zerlegt die Ebene ε in 2 Teilebenen, zwei Geraden zerlegen die Ebene ε in 4 Teilebenen.

Behauptung:
n Geraden zerlegen die Ebene ε in $s_n = \frac{n(n+1)}{2} + 1$ Teilebenen.
Die Behauptung ist richtig für ein spezielles $n = 1$,

$$s_1 = \frac{1 \cdot 2}{2} + 1 = 2$$

Annahme, die Behauptung sei richtig für $n = k$:

$$s_k = \frac{k(k+1)}{2} + 1$$

Es wird gezeigt, dass die Behauptung auch für den nächstfolgenden Fall $(k+1)$ richtig ist:

$$s_{k+1} = \frac{(k+1)(k+2)}{2} + 1$$

Beweis:
Nach Voraussetzung zerlegen k Geraden die Ebene ε in $s_k = \frac{k(k+1)}{2} + 1$ Teilebenen. Bei Hinzunahme der $(k+1)$-sten Geraden entstehen $(k+1)$ zusätzliche Teilebenen, so dass gilt:

$$s_{k+1} = s_k + (k+1) = \frac{k(k+1)}{2} + 1 + k + 2 = \frac{k^2 + 3k + 2}{2} + 1 = \frac{(k+1)(k+2)}{2} + 1 \qquad \text{q.e.d.}$$

(7)• Die Quadratzahlen sind $1, 4, 9, 16, 25, ...$ und die Partialsummen der Folge der Quadratzahlen

$$s_1 = 1, s_2 = 5, s_3 = 14, s_4 = 30, ...$$

Vergleicht man die Glieder dieser Partialsummenfolge mit dehnen der Partialsummen der Folge der natürlichen Zahlen

$$s'_1 = 1, s'_2 = 3, s'_3 = 6, s'_4 = 10, ...$$

so erkennt man, dass der Quotient zweier entsprechender Glieder

$$\frac{s'_k}{s_k} = \frac{3}{2k+1}$$

ist.
Behauptung für die Summe der ersten n Quadratzahlen:

$$s_n = \frac{2n+1}{3} s'_n = \frac{2n+1}{3} \cdot \frac{n(n+1)}{2} = \frac{n(n+1)(1+2n)}{6}$$

Die Behauptung ist richtig für ein spezielles $n = 1$:

$$s_1 = \frac{1 \cdot 2 \cdot 3}{6} = 1$$

Annahme, die Behauptung sei richtig für $n = k$:

$$s_k = \frac{k(k+1)(1+2k)}{6}$$

Es wird gezeigt, dass die Behauptung auch für den nächstfolgenden Fall $(k+1)$ richtig ist:

$$s_{k+1} = \frac{(k+1)(k+2)(3+2k)}{6}$$

Beweis:

$$s_{k+1} = s_k + (k+1)^2 = \frac{1}{6}(k+1)(2k^2+7k+6) = \frac{1}{6}(k+1)(2k+3)(k+2) \qquad q.e.d.$$

(10)• Für $n = 0$ und $n = 1$ gilt $23 \mid z_n$.
Annahme, $z_k = 852^k - 1$ sei durch 23 teilbar. Es wird gezeigt, dass die Behauptung auch für den nächstfolgenden Exponenten $(k+1)$ gilt.

$$z_{k+1} = 852^{k+1} - 1 = 852 \cdot 852^k - 851 \cdot 852^k + 851 \cdot 852^k - 1 = (852^k - 1) + 851 \cdot 852^k$$

Der erste Term ist nach Voraussetzung durch 23 teilbar, im zweiten Term ist $851 = 37 \cdot 23$ durch 23 teilbar. q.e.d.

(11)• Für $n = 1$ gilt (Rest bei Division durch 671):

x	1	2	3	4	5	6	7	8	9
Rest	434	138	513	217	592	296	0	375	79

Behauptung:
$z_n = 77777^n + 59^n$ ist für jede ungerade Zahl n durch 671 teilbar.

Die Teilbarkeit durch 671 wurde für ein spezielles $n = 1$ nachgewiesen. Unter der Annahme, dass $z_k = 77777^k + 59^k$ bei ungeradem k durch 671 teilbar ist, wird gezeigt, dass z auch für den nächstfolgenden ungeraden Exponenten durch 671 teilbar ist. Es gilt:

$$\begin{aligned} z_{k+2} &= 77777^{k+2} + 59^{k+2} = 77777^{k+2} + 77777^2 \cdot 59^{k+2} - 77777^2 \cdot 59^{k+2} + 59^{k+2} \\ &= 77777^2(77777^k + 59^k) - 59^k(77777 + 59)(77777 - 59) \end{aligned}$$

Die Klammer des ersten Terms ist nach Voraussetzung durch 671 teilbar. Die Teilbarkeit der ersten Klammer des 2. Terms durch 671 wurde oben gezeigt. Damit ist z für jede ungerade Zahl n durch 671 teilbar.

(15)• $z = (16+1)^{1968} = k \cdot 16 + 1^{1968} = k \cdot 16 + 1$.
z lässt bei der Division durch 16 den Rest 1.

(16)• $z = 7 \cdot 7^{28} = 7 \cdot (7^2)^{64} = 7(50-1)^{64} = 7(k \cdot 50 + 1) = 7k \cdot 50 + 7$.
z lässt bei der Division durch 50 den Rest 7.

(17)•

$$\begin{aligned} z &= 13 \cdot 13^{136} = 13(13^2)^{68} = 13(171-2)^{68} = 13(k \cdot 171 + 2^{68}) = 13(k \cdot 171 + [2^9]^7 \cdot 2^5) \\ &= 13(171k + [513-1]^7 \cdot 2^5) = 13(171k + [3 \cdot 171 - 1]^7 \cdot 2^5) \\ &= 13(171k_1 - 32) = 13(171[k_1 - 1] + 139) \end{aligned}$$

z lässt bei der Division durch 171 denselben Rest wie das Produkt $13 \cdot 139 = 1807 = 10 \cdot 171 + 97$.
z lässt bei der Division durch 171 den Rest 97.

(20)• $x = \frac{1500-28y}{67}$. Nur für $y = 44$ ist der Zähler durch 67 teilbar. Damit wird $x = 4$.

(21)•

$$\begin{aligned} 21x + 33y + 39z &= 9000 \\ \underline{21x + 49y + 119z} &= \underline{21000} \\ 16y + 80z &= 12600 \\ y + 5z &= 750 \end{aligned}$$

$z = \frac{750-y}{4}$. y muss die Form $y = 5k$ haben. Damit wird $z = 150 - k$ und $x = 150 - 6k$.
Es gilt einerseits $k > 0$, weil y positiv sein soll, andererseits $k < 25$, weil sonst x negativ wird.

$$x = 150 - 6k, \quad y = 5k, \quad z = 150 - k, \quad k \in [1, 24]$$

(22)• $n = 7k + 1$, $n_1 = 6k = 5r + 1$, $n_2 = 4r = 3s + 1$, $n_3 = 2s = 3t + 1$.
$s = \frac{3t+1}{2}, r = \frac{9t+5}{8}, k = \frac{45t+33}{48}$, $\qquad n = \frac{315t+279}{48} = \frac{105t+93}{16}$

Die kleinste Zahl t, für die $105t + 93$ durch 16 teilbar ist, ist $t = 11$. Damit wird $n = 78$.

Allgemein erfüllt jedes $t = 11 + 16m$ die gegebene Bedingung, so dass $n = 78 + 105m$ für $m = 0, 1, 2, ...$ die allgemeine Lösung der Aufgabe ist.
Man wählt die Elemente mit ungeraden Indizes aus und setzt sie an den Anfang der linearen Anordnung. Die Anzahl dieser Elemente ist n.

Alle diese Elemente sind nicht verwandt miteinander und die darauf folgenden n Elemente sind wiederum nicht verwandt miteinander. Es gibt nun $n!$ Möglichkeiten, diese jeweils nicht verwandten n Elemente linear anzuordnen (Permutationen ohne Wiederholung!). Für $n > 3$ gilt aber $n! > n^2$, so dass es nach dem Dirichletschen Schubfachprinzip mindestens n^2 solcher Anordnungen gibt.

$$\begin{aligned} (n-2)^2 &> 2 \qquad \text{für } n > 3 \\ n^2 - 4n + 2 &> 0 \\ n^2 - 3n + 2 &> n \\ (n-2)(n-1) &> n \\ 1 \cdot 2 \cdot 3 \cdot ... \cdot (n-2)(n-1) &> n \\ 1 \cdot 2 \cdot 3 \cdot ... \cdot (n-2)(n-1)n &> n^2 \\ n! &> n^2 \qquad \text{für } n > 3 \end{aligned}$$

(32)• a) $100 > n!$ bedeutet $n > 4$. Es gilt:

$$\begin{aligned} n^3 + 2n^2 &> 0 \qquad \text{für } n > 0 \\ (n - (n-1))n^3 + 2n^2 &> 0 \\ n^4 - (n-1)n^3 + 2n^2 &> 0 \end{aligned}$$

Für $n > 4$ gilt $(n-1)n^3 \geq 4n^3$. Damit wird

$$\begin{aligned} n^4 - 4n^3 + 2n^2 &> 0 \\ n^4 - 3n^3 + 2n^2 &> n^3 \\ (n-2)(n-1)n^2 &> n^3 \\ 1 \cdot 2 \cdot 3 \cdot ... \cdot (n-1)n^2 &> n^3 \\ \cdot 2 \cdot ... \cdot (n-1) \cdot n \cdot (n+1) - 1 \cdot 2 \cdot ... \cdot (n-1) \cdot n &> n^3 \\ (n+1)! - n! &> n^3 \qquad \text{für } n > 4 \end{aligned}$$

Das gegebene Intervall enthält mehr als n^3 aufeinanderfolgende natürliche Zahlen, folglich ist mindestens eine dieser Zahlen des Intervalls durch n^3 teilbar.

b) Das angegebene Intervall besteht aus $2^n + 1$ aufeinanderfolgenden natürlichen Zahlen. Es gilt:
$n = 1$; $2 \leq x \leq 4$ Jede der Zahlen des Intervalls ist durch $n^2 = 1$ teilbar.
$n = 2$; $4 \leq x \leq 8$ Die Elemente 4 und 8 sind durch $n^2 = 4$ teilbar.
$n = 3$; $8 \leq x \leq 16$ Das Element 9 ist durch $n^2 = 9$ teilbar.

Behauptung: für $n > 3$: $2^n > n^2$.
Die Behauptung ist für ein spezielles $n = 4$ richtig, $2^4 > 4^2$. Unter der Annahme, dass die Behauptung für $n = k$ gilt $(2^k \geq k^2)$, wird gezeigt, dass die Behauptung auch für den Fall $(k + 1)$ gilt $(2^{k+1} \geq (k + 1)^2)$.

$$\begin{aligned} (k-1)^2 &\geq 2 \qquad \text{für } k > 2 \\ k^2 - 2k + 1 &\geq 2 \\ 2k^2 &\geq k^2 + 2k + 1 \\ 2 \cdot 2^k = 2^{k+1} &\geq (k+1)^2 \end{aligned}$$

Für alle $n > 3$ gilt $2^n > n^2$. In dem betrachteten Intervall liegen mehr als n^2 aufeinanderfolgende natürliche Zahlen, folglich ist nach dem Dirichletschen Prinzip mindestens eine unter ihnen durch n^2 teilbar.

(44)• Es gilt: $104975 = 5 \cdot 5 \cdot 43 \cdot 47 \cdot 49$ und ferner

$$\begin{aligned} z &= (18^{64} + 1)(18^{32} + 1)(18^{16} + 1)(18^8 + 1)(18^4 + 1) \cdot 325 \cdot 19 \cdot 17 \\ &= (18^{64} + 1)(18^{32} + 1)(18^{16} + 1)(18^8 + 1)(18^4 + 1) \cdot 104975 \end{aligned}$$

(45)• Ist z durch 5 teilbar, so auch $z + 5a$.
Ist z nicht durch 5 teilbar, so auch $z + 5a$ nicht.
Man untersucht die Zahl $z' = z + 5a$ mit $a = -n^3$.

$$z' = n^5 - 5n^3 + 4n = n(n^2 - 1)(n^2 + 4) = (n - 2)(n - 1)n(n - 1)(n + 2)$$

Von 5 aufeinanderfolgenden natürlichen Zahlen ist stets eine durch 5 teilbar.

(46)• Die möglichen Endziffern einer Primzahl $p > 5$ sind $1, 3, 7, 9$.
Die möglichen Endziffern der Quadrate dieser Primzahlen $1, 9, 9, 1$.
Die möglichen Endziffern der vierten Potenzen sind dann $1, 1, 1, 1$.
Addiert man zu den vierten Potenzen die Zahl 4, so entsteht stets eine durch 5 teilbare Zahl.

(47)• Die möglichen Endziffern einer Primzahl $p > 5$ sind $1, 3, 7, 9$; der Quadrate dieser Primzahlen $1, 9, 9, 1$; der vierten Potenzen dieser Primzahlen. $1, 1, 1, 1$; der achten Potenzen $1, 1, 1, 1$; und damit der zehnten Potenzen $1, 9, 9, 1$.
Die 12. Potenz einer Primzahl endet damit auf 1. Dies gilt für alle Primzahlen $p > 5$, also auch speziell für alle Primzahlen $p > 100$.

(51)• a) $d = (41275, 4572) = (4572, 127) = (127, 0) = 127$

b) $d = (5661, 5291, 4292) = (4292, 1369, 999) = (999, 296, 370) = (370, 111, 74) = (74, 0, 37) = 37$

c) $d = (7576, 6591, 4913) = (4913, 2250, 1678) = (1678, 121, 572) = (121, 16, 88) = (16, 9, 8) = 1$

d) $d = (325104, 221946, 90654, 53142)(53142, 6252, 9378, 15630) = (6252, 3126, 3126, 3136) =$

$= (3126, 0, 0, 0) = 3126$

e) $d = (2125, 1716, 1534, 1213) = (1213, 304, 503, 324) = (301, 9, 9, 20) = (9, 4, 0, 2) = 1.$

(54)• a) $d = (1554, 666) = (666, 222) = 222$; $m = \frac{1554 \cdot 666}{222} = 4662$

b) $d = (831, 137) = (137, 9) = 9, 2) = 1$; $m = [831, 137] = 831 \cdot 137 = 113847$

c) $d = (4891, 4221, 1407) = (1407, 737, 0) = (737, 67, 0) = (67, 0, 0) = 67$;
$m = [4891, 4221, 1407] = 308133$

d) $d = (7612, 3114, 1903, 1038) = (1038, 346, 0, 173) = (173, 0, 0, 0) = 173$;
$m = [7612, 3114, 1903, 1038] = 68508$

e) $d = (19224, 3204, 2403, 1068, 712) = (712, 0, 356, 267, 356) = (267, 89, 0, 89, 89) = 89$;
$m = [19224, 3204, 2403, 1068, 712] = 19224.$

(66)• $z \equiv (1-3)^7 - 3^{16}(7+9)^5 \equiv -9 - (-1)^5 \equiv -8 \equiv 9$ mod 17.

(69)• $891 \equiv 37$ mod 64, $403 \equiv 37$ mod 61.
Damit wird $z \equiv 37^n - 37^n \equiv 0$ mod 61. z ist für jedes natürliche n durch 61 teilbar.

$14557 \equiv 18$ mod 31, $6230 \equiv -1$ mod 31, $2059 \equiv 13$ mod 31, $13 \equiv -18$ mod 31.
$z \equiv 18^{2n} - 1 \cdot (-18)^{2n} \equiv 18^{2n} - 18^{2n} \equiv= 0$ mod 31.

$14557 \equiv 18$ mod 67, $6230 \equiv -1$ mod 67, $2059 \equiv 49 \equiv -18$ mod 67.
$z \equiv 18^{2n} - 18^{2n} \equiv 0$ mod 67.
z ist durch 31 und 67, folglich auch durch $31 \cdot 67 = 2077$ teilbar.

(73)• z lässt bei der Division durch 19 den Rest 17.

(77)• $z = 2^n + 1$ ist ungerade. Falls z die fünfte Potenz einer natürlichen Zahl ist, so kann z nur die fünfte Potenz einer ungeraden Zahl sein.

$$z = 2^n + 1 = (2k+1)^5 = 32k^5 + 80k^4 + 80^k 3 + 40k^2 + 10k + 1$$
$$2^n = 2k(16k^4 + 40k^3 + 40k^2 + 20k + 5)$$

Der Klammerausdruck ist eine ungerade Zahl, er kann also nicht Teiler einer Zweierpotenz sein.

(80)•

$m = 6$

	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

$m = 8$

	0	1	2	3	4	5	6	7
0	0	1	2	3	4	5	6	7
1	1	2	3	4	5	6	7	0
2	2	3	4	5	6	7	0	1
3	3	4	5	6	7	0	1	2
4	4	5	6	7	0	1	2	3
5	5	6	7	0	1	2	3	4
6	6	7	0	1	2	3	4	5
7	7	0	1	2	3	4	5	6

$m = 13$

	0	1	2	3	4	5	6	7	8	9	10	11	12
0	0	1	2	3	4	5	6	7	8	9	10	11	12
1	1	2	3	4	5	6	7	8	9	10	11	12	0
2	2	3	4	5	6	7	8	9	10	11	12	0	1
3	3	4	5	6	7	8	9	10	11	12	0	1	2
4	4	5	6	7	8	9	10	11	12	0	1	2	3
5	5	6	7	8	9	10	11	12	0	1	2	3	4
6	6	7	8	9	10	11	12	0	1	2	3	4	5
7	7	8	9	10	11	12	0	1	2	3	4	5	6
8	8	9	10	11	12	0	1	2	3	4	5	6	7
9	9	10	11	12	0	1	2	3	4	5	6	7	8
10	10	11	12	0	1	2	3	4	5	6	7	8	9
11	11	12	0	1	2	3	4	5	6	7	8	9	10
12	12	0	1	2	3	4	5	6	7	8	9	10	11

(82)•

$p = 11$

	0	1	2	3	4	5	6	7	8	9	10
0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10
2	0	2	4	6	8	10	1	3	5	7	9
3	0	3	6	9	1	4	7	10	2	5	8
4	0	4	8	1	5	9	2	6	10	3	7
5	0	5	10	4	9	3	8	2	7	1	6
6	0	6	1	7	2	8	3	9	4	10	5
7	0	7	3	10	6	2	9	5	1	8	4
8	0	8	5	2	10	7	4	1	9	6	3
9	0	9	7	5	3	1	10	8	6	4	2
10	0	10	9	8	7	6	5	4	3	2	1

$m = 18$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17
2	0	2	4	6	8	10	12	14	16	0	2	4	6	8	10	12	14	16
3	0	3	6	9	12	15	0	3	6	9	12	15	0	3	6	9	12	15
4	0	4	8	12	16	2	6	10	14	0	4	8	12	16	2	6	10	14
5	0	5	10	15	2	7	12	17	4	9	14	1	6	11	16	3	8	13
6	0	6	12	0	6	12	0	6	12	0	6	12	0	6	12	0	6	12
7	0	7	14	3	10	17	6	13	2	9	16	5	12	1	8	15	4	11
8	0	8	16	6	14	4	12	2	10	0	8	16	6	14	4	12	2	10
9	0	9	0	9	0	9	0	9	0	9	0	9	0	9	0	9	0	9
10	0	10	2	12	4	14	6	16	8	0	10	2	12	4	14	6	16	8
11	0	11	4	15	8	1	12	5	16	9	2	13	6	17	10	3	14	7
12	0	12	6	0	12	6	0	12	6	0	12	6	0	12	6	0	12	6
13	0	13	8	3	16	11	6	1	14	9	4	17	12	7	2	15	105	
14	0	14	10	6	2	16	12	8	4	0	14	10	6	2	16	12	8	4
15	0	15	12	9	6	3	0	15	12	9	6	3	0	15	12	9	6	3
16	0	16	14	12	10	8	6	4	2	0	16	14	12	10	8	6	4	2
17	0	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

$p = 19$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
2	0	2	4	6	8	10	12	14	16	18	1	3	5	7	9	11	13	15	17
3	0	3	6	9	12	15	18	2	5	8	11	14	17	1	4	7	10	13	16
4	0	4	8	12	16	1	5	9	13	17	2	6	10	14	18	3	7	11	15
5	0	5	10	15	1	6	11	16	2	7	12	17	3	8	13	18	4	9	14
6	0	6	12	18	5	11	17	4	10	16	3	9	15	2	8	14	1	7	13
7	0	7	14	2	9	16	4	11	18	6	13	1	8	15	3	10	17	5	12
8	0	8	16	5	13	2	10	18	7	15	4	12	1	9	17	6	14	3	11
9	0	9	18	8	17	7	16	6	15	5	14	4	13	3	12	2	11	1	10
10	0	10	1	11	2	12	3	13	4	14	5	15	6	16	7	17	8	18	9
11	0	11	3	14	6	17	9	1	12	4	15	7	18	10	2	13	5	16	8
12	0	12	5	17	10	3	15	8	1	13	6	18	1	4	16	9	2	14	7
13	0	13	7	1	14	8	2	15	9	3	16	10	4	17	11	5	18	12	6
14	0	14	9	4	18	13	8	3	17	12	7	2	16	11	6	1	15	10	5
15	0	15	11	7	3	18	14	10	6	2	17	13	9	5	1	16	12	8	4
16	0	16	13	10	7	4	1	17	14	11	8	5	2	18	15	12	9	6	3
17	0	17	15	13	11	9	7	5	3	1	18	16	14	12	10	8	6	4	2
18	0	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1

(84)• $p = 5$, $a^k \equiv b$ mod 5.

k	1	2	3	4	5	...
$a = 1$	1	1	1	1	1	...
$a = 2$	2	4	3	1	2	...
$a = 3$	3	4	2	1	3	...
$a = 4$	4	1	4	1	4	...

$p = 13$, $a^k \equiv b$ mod 13.

k	1	2	3	4	5	6	7	8	9	10	11	12
$a = 1$	1	1	1	1	1	1	1	1	1	1	1	1
$a = 2$	2	4	8	3	6	12	11	9	5	10	7	1
$a = 3$	3	9	1	3	9	1	3	9	1	3	9	1
$a = 4$	4	3	12	9	10	1	4	3	12	9	10	1
$a = 5$	5	12	8	1	5	12	8	1	5	12	8	1
$a = 6$	6	10	8	9	2	12	7	3	5	4	11	1
$a = 7$	7	10	5	9	11	12	6	3	8	4	2	1
$a = 8$	8	12	5	1	8	12	5	1	8	12	5	1
$a = 9$	9	3	1	9	3	1	9	3	1	9	3	1
$a = 10$	10	9	12	3	4	1	10	9	12	3	4	1
$a = 11$	11	4	5	3	7	12	2	9	8	10	6	1
$a = 12$	12	1	12	1	12	1	12	1	12	1	12	1

$p = 11$, $a^k \equiv b$ mod 11.

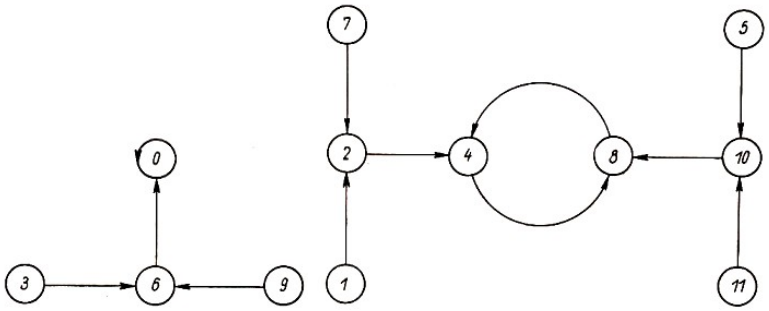
k	1	2	3	4	5	6	7	8	9	10	11	...
$a = 1$	1	1	1	1	1	1	1	1	1	1	1	...
$a = 2$	2	4	8	5	10	9	7	3	6	1	2	...
$a = 3$	3	9	5	4	1	3	9	5	4	1	3	...
$a = 4$	4	5	9	3	1	4	5	9	3	1	4	...
$a = 5$	5	3	4	9	1	5	3	4	9	1	5	...
$a = 6$	6	3	7	9	10	5	8	4	2	1	6	...
$a = 7$	7	5	2	3	10	4	6	9	8	1	7	...
$a = 8$	8	9	6	4	10	3	2	5	7	1	8	...
$a = 9$	9	4	3	5	1	9	4	3	5	1	9	...
$a = 10$	10	1	10	1	10	1	10	1	10	1	10	...

(91)• a) linke Seite $\equiv 0 + 7 + 8 + 7 \equiv 4$ mod 9; rechte Seite $\equiv 4$ mod 9.
linke Seite $\equiv 0 + 5 + 2 + 1 \equiv 8$ mod 11; rechte Seite $\equiv 8$ mod 11.
Neuner- und Elferprobe stimmen.

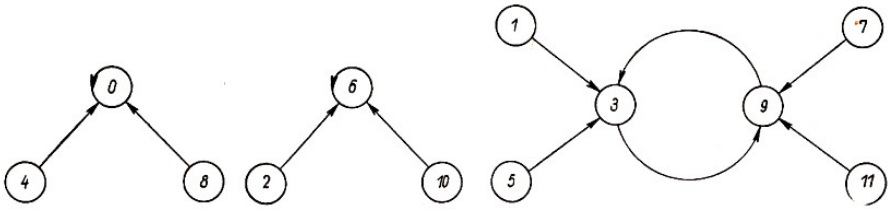
b) Die Neunerprobe stimmt, die Elferprobe nicht, es liegt ein Fehler in der Aufgabe vor. Das richtige Ergebnis lautet 45355011.
c) Neuner- und Elferprobe stimmen.

(100)• Die Anwendung der Teilbarkeitsregeln liefert folgende Produktdarstellungen
a) $z = 4 \cdot 9 \cdot 11 \cdot 13$, b) $z = 9 \cdot 13 \cdot 17$, c) $z = 3 \cdot 4 \cdot 11 \cdot 71$, d) $z = 3 \cdot 17 \cdot 37$, e) $z = 11 \cdot 17 \cdot 61$, f) $z = 11 \cdot 43 \cdot 37$.

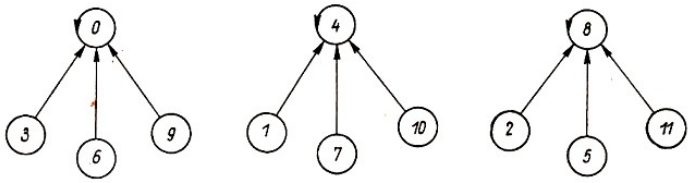
(103)• $2b \equiv x$ mod 12



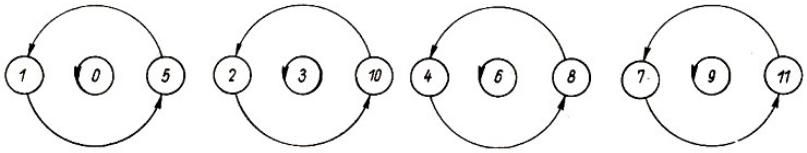
$3b \equiv x$ mod 12



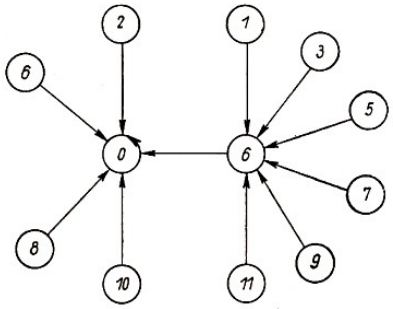
$4b \equiv x$ mod 12



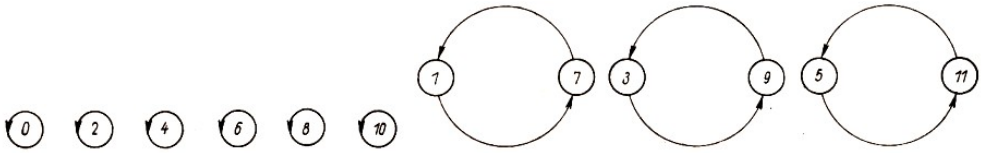
$5b \equiv x$ mod 12



$6b \equiv x$ mod 12



$7b \equiv x$ mod 12



(107)• a) $x \equiv \frac{2}{11} \equiv -\frac{36}{6} \equiv -6$ mod 17.
Probe: $1243 = 71 \cdot 17 + 36$.

b) $x \equiv \frac{91}{36} \equiv \frac{204}{36} \equiv \frac{17}{3} \equiv \frac{243}{3} \equiv 81$ mod 113.
Probe: $2916 = 25 \cdot 113 + 91$.

c) $x \equiv -\frac{198}{2} \equiv -99 \equiv 18$ mod 117.
Probe: $2070 = 17 \cdot 117 + 81$.

d) $x \equiv \frac{37}{17} \equiv -\frac{108}{54} \equiv -2 \equiv 69$ mod 71.
Probe: $1173 = 16 \cdot 71 + 37$.

e) $x \equiv \frac{6}{19} \equiv -\frac{31}{26} \equiv -\frac{90}{13} \equiv -133 \equiv 16$ mod 149.
Probe: $1776 = 11 \cdot 149 + 137$.

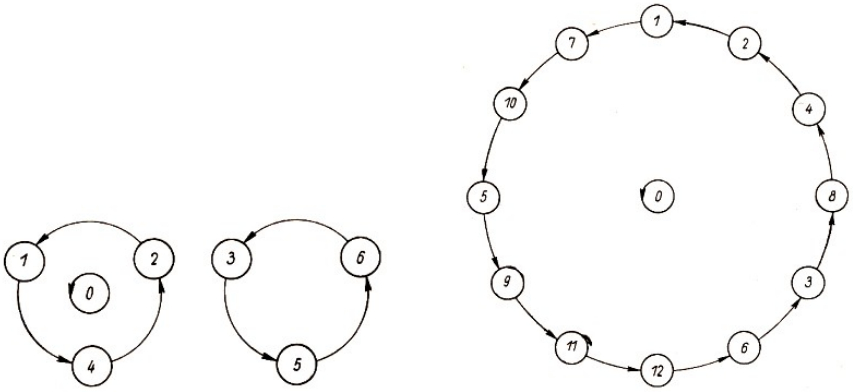
f) $x \equiv \frac{111}{16} \equiv \frac{177}{8} \equiv \frac{105}{2} \equiv 174$ mod 243.
Probe: $11136 = 45 \cdot 243 + 201$.

g) $x \equiv \frac{1119}{243} \equiv \frac{373}{81} \equiv \frac{86}{9} \equiv \frac{296}{3} \equiv 366$ mod 401.
Probe: $88938 = 221 \cdot 401 + 317$.

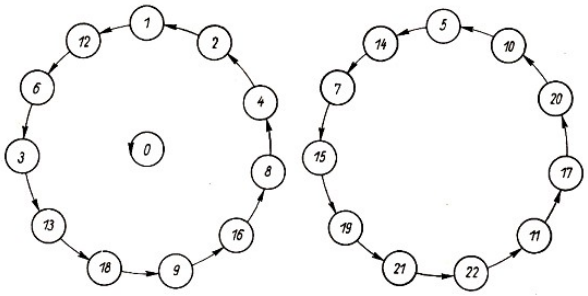
h) $x \equiv -\frac{19}{3} \equiv -\frac{1020}{3} \equiv -340 \equiv 661$ mod 1001.
Probe: $49575 = 49 \cdot 1001 + 526$.

i) $x \equiv -\frac{331}{60} \equiv -\frac{309}{10} \equiv -1097 \equiv 426$ mod 1523.
Probe: $51120 = 33 \cdot 1523 + 861$.

(109)• $4b \equiv x$ mod 7 $\qquad$ $7b \equiv x$ mod 13



$12b \equiv x$ mod 23.



(126)• $665 \equiv -1$ mod 37. Damit ist z nach dem kleinen Satz von Fermat durch 37 teilbar.

(127)• $5^{p-1} - 1 \equiv 0$ mod p, $p - 1 = 6, 10, 12, 16, 40$.
$m = \{6, 10, 12, 16, 40\} = 240$.
$5^{240} - 1 \equiv (5^{40})^6 - 1 \equiv (5^{24})^{10} - 1 \equiv (5^{20})^{12} - 1 \equiv (5^{15})^{16} - 1 \equiv (5^6)^{40} - 1 \equiv 0$ mod 7, 11, 13, 17,41

(128)• z ist für $k = 16m$ $(m = 1, 2, 3, ...)$ und $d = (n, 17) = 1$ durch 17 teilbar.

(129)• Es gilt die Zerlegung $z = (p^4 - 1)(p^6 - 1)^2$. Nach dem kleinen Satz von Fermat ist $(p^4 - 1)$ durch 5, $(p^6 - 1)$ durch 7 und damit z durch $5 \cdot 7^2 = 245$ teilbar.

(130)• $343 = 7^3$. Nach dem kleinen Satz von Fermat ist $3^{6n} - 1$ durch 7 teilbar. Daraus folgt $(3^{6n} - 1)^3 \equiv 0$ mod 7^3.
$3^{18n} - 3 \cdot 3^{12n} + 3 \cdot 3^{6n} - 1 \equiv 0$ mod 343.
Es folgt $n = 11$ und $k = 3^{67} - 1$.

(135)• a)

k	1	2	3	4	5	6	7	8	9	10	11	12
$\frac{1}{k}$	1	7	9	10	8	11	2	5	3	4	6	12

b)

k	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\frac{1}{k}$	1	10	13	5	4	16	11	12	17	2	7	8	3	15	14	6	9	18

c)

k	1	2	3	4	5	6	7	8	9	10	11
$\frac{1}{k}$	1	12	8	6	14	4	10	3	18	7	21
k	12	13	14	15	16	17	18	19	20	21	22
$\frac{1}{k}$	2	16	5	20	13	19	9	17	15	11	22

(138)• $p = 13$

a	1	2	3	4	5	6	7	8	9	10	11	12
a^2	1	4	9	3	12	10	10	12	3	9	4	1

$p = 19$

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
a^2	1	4	9	16	6	17	11	7	5	5	7	11	17	6	16	9	4	1

$p = 37$

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
a^2	1	4	9	16	25	36	12	27	7	26	10	33	21	11	3	34	30	28
a	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
a^2	28	30	34	3	11	21	33	10	26	7	27	12	36	25	16	9	4	1

(148)• $p = 13$

a	1	2	3	4	5	6	7	8	9	10	11	12
a^3	1	8	1	12	8	8	5	5	1	12	5	12

$p = 23$

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
a^3	1	8	4	18	10	9	21	6	16	11	20	3	12	7	17	2	14	13
a	19	20	21	22														
a^3	5	19	15	22														

$p = 37$

a	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
a^3	1	8	27	27	14	31	10	31	26	1	36	26	14	6	8	26	29	23
a	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
a^3	14	8	11	29	31	23	11	1	36	11	6	27	6	23	27	10	29	36

(154)• $p = 83$

x	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
$\log x$	0	1	72	2	27	73	8	3	62	28	24	74	77	9	17	4	56	63
x	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36
$\log x$	47	29	80	25	60	75	54	78	52	10	12	18	38	5	14	57	35	64
x	37	38	39	40	41	42	43	44	45	46	47	48	49	50	51	52	53	54
$\log x$	20	48	67	30	40	81	71	26	7	61	23	76	16	55	46	79	59	53
x	55	56	57	58	59	60	61	62	63	64	65	66	67	68	69	70	71	72
$\log x$	51	11	37	13	34	19	66	39	70	6	22	15	45	58	50	36	33	65
x	73	74	75	76	77	78	79	80	81	82								
$\log x$	69	21	44	49	32	68	43	31	42	41								

a) $\log x \equiv \log 17 - \log 67 \equiv 56 - 45 \equiv 11$ mod 82,
$x \equiv 56$ mod 83, Probe: $3752 = 45 \cdot 83 + 17$.

b) $\log x \equiv 39 \cdot \log 37 \equiv 39 \cdot 20 \equiv 42$ mod 82, $z \equiv 81$ mod 83.

(157)• $n \equiv 4 \bmod 3$, $n = 3k+1$, $R_1 = \frac{2}{3}(n-1)$,
$R_1 \equiv 1 \bmod 3$, $R_1 = 3l+1$, $R_2 = \frac{2}{3}(R_1-1)$,
$R_2 \equiv 1 \bmod 3$, $R_2 = 3r+1$, $R_3 = \frac{2}{3}(R_2-1)$,
$R_3 \equiv 1 \bmod 3$, $R_3 = 3s+1$, $R_4 = \frac{2}{3}(R_3-1)$,

$R_3 = \frac{3}{2}R_4 + 1 = \frac{2}{3}(R_2-1)$, $\quad \frac{9}{4}R_4 + \frac{3}{2} = R_2 - 1$
$R_2 = \frac{9}{4}R_4 + \frac{5}{2} = \frac{2}{3}(R_1-1)$, $\quad \frac{27}{8}R_4 + \frac{15}{4} = R_1 - 1$
$R_1 = \frac{27}{8}R_4 + \frac{19}{4} = \frac{2}{3}(n-1)$, $\quad \frac{81}{16}R_4 + \frac{57}{8} = n - 1$
$n = \frac{81}{16}R_4 + \frac{65}{8} = \frac{81R_4+130}{16}$

$81R_4 + 130 \equiv 0 \bmod 16$, $R_4 + 2 \equiv 0 \bmod 16$
$R_4 \equiv -2 \equiv 14 \bmod 16$, $R_4 = 14 + 16k$
$$n = \frac{81 \cdot 14 + 81 \cdot 16k + 130}{16} = 79 + 81k$$

Nur für $k = 0$ gilt die Bedingung $n < 160$. Daraus folgt $n = 79$.

(158)• Gegeben sind die Zahlen n_1 und $n_2 = \frac{4}{5}(n-1)$,

$$n_3 = \frac{4}{5}(n_2-1), \qquad n_4 = \frac{4}{5}(n_3-1), \qquad n_5 = \frac{4}{5}(n_4-1)$$
$$n_4 = \frac{5}{4}(n_5+1)$$
$$n_3 = \frac{5}{4}(n_4+1) = \frac{25}{16}n_5 + \frac{9}{4}$$
$$n_2 = \frac{5}{4}(n_3+1) = \frac{125}{64}n_5 + \frac{61}{16}$$
$$n_1 = \frac{5}{4}(n_2+1) = \frac{625}{256}n_5 + \frac{369}{64} = \frac{625 \cdot n_5 + 1476}{256}$$

n sollte eine natürliche Zahl sein, folglich gilt
$625n_5 + 1476 \equiv 0 \bmod 256$, $113n_5 - 60 \equiv 0 \bmod 256$,
$n_5 \equiv \frac{60}{113} \equiv -4 \equiv 252 \bmod 256$, $n_5 = 252 + 256k$
$n_1 = \frac{158976+625\cdot 256k}{256} = 621 + 625k$.

Probe: $n_2 = 496 + 500k$, $n_4 = 316 + 320k$, $n_3 = 396 + 400k$, $n_5 = 252 + 256k$.

(159)• Das Geburtsjahr sei x. $x \equiv 31 \cdot 21r + 41 \cdot 21s + 41 \cdot 31t$.

$x \equiv 31 \cdot 21r \equiv 36r \equiv 33 \bmod 41$, $r \equiv 18 \bmod 41$
$x \equiv 41 \cdot 21s \equiv 24s \equiv 28 \bmod 31$, $s \equiv 27 \bmod 31$
$x \equiv 41 \cdot 31s \equiv 11t \equiv 8 \bmod 21$, $t \equiv 16 \bmod 21$
$x = 55301 + 26691k$

Nur $k = -2$ liefert eine den Bedingungen entsprechende Lösung:
$x = 55301 - 53382 = 1919$.
$1919 = 43 \bmod 67$, $1919 = 5 \bmod 29$, $1919 = 15 \bmod 17$.
Im Jahr 1962 wurde die Aufgabe gestellt, das gesuchte Geburtsdatum ist der 15. Mai 1919.

(163)• $x = 11u + 17v$, $6v \equiv 5 \bmod 11$, $v \equiv 10 \bmod 11$, $v = 11k + 10$
$11u \equiv 7 \bmod 17$, $u \equiv 13 \bmod 17$, $u = 17k + 13$

Spezielle Lösung: $x = 126$. Allgemeine Lösung: $x = 126 + 187n$.

(164)• $x = 23u + 37v$, $14v \equiv 49 \bmod 23$, $v = 3 \bmod 23$, $v = 3 + 23k$.
$23u \equiv 31 \bmod 377$, $u \equiv 11 \bmod 37$, $u = 11 + 37m$.

Spezielle Lösung: $x = 364$. Allgemeine Lösung: $x = 364 + 851n$.

(165)• $x = 31u + 41v$, $19v \equiv 18 \bmod 31$, $v = 8 \bmod 31$, $v = 8 + 31k$.
$31u \equiv 7 \bmod 41$, $u \equiv 28 \bmod 41$, $u = 28 + 41m$. $x = 1196 + 1271n$.
Die einzige Lösung ergibt sich für $n = 2$: $x = 3738$.

Probe: $3738 = 120 \cdot 31 + 18 = 91 \cdot 41 + 77$.

(166)• $n^* = 105x + 70y + 42z + 30u$,
$x \equiv 1 \bmod 2$, $x = 1 + 2k - 1$,
$y \equiv 2 \bmod 3$, $y = 2 + 3k - 2$,
$z \equiv 2 \bmod 5$, $z = 2 + 5k - 3$,
$u \equiv 3 \bmod 7$, $u = 3 + 7k - 4$,
$n^* = 4149 + 210k$. Für $k = -1$ ergibt sich die kleinste natürliche Zahl mit den oben angegebenen Eigenschaften, nämlich $n = 209$.

(167)• $n = 1891x + 671y + 341z$.
$10x \equiv 7 \bmod 11$, $x \equiv 4 \bmod 11$, $x = 4 + 11k - 1$
$20y \equiv 18 \bmod 31$, $y \equiv 4 \bmod 31$, $y = 4 + 31k - 2$
$36z \equiv 39 \bmod 61$, $z \equiv 57 \bmod 61$, $z = 57 + 61k - 3$
$n = 8884 + 20801k$.

(170)• $665 = 5 \cdot 7 \cdot 19$,
$561x \equiv x \equiv 2 \bmod 5$, $561x \equiv x \equiv 5 \bmod 7$,
$561x \equiv 10x \equiv 14 \bmod 19$, $x \equiv 9 \bmod 19$

$x = 133r + 955 + 35t$.
$x \equiv 3r \equiv 2 \bmod 5$, $r \equiv 4 \bmod 5$,
$x \equiv 4s \equiv 5 \bmod 7$, $s \equiv 3 \bmod 7$,
$x \equiv -3t \equiv 9 \bmod 19$, $t \equiv 16 \bmod 19$,
$x = 1377 + 665k$. Für $k = -2$ erhält man $x = 47$.

Probe: $561 \cdot 47 = 26367 = 39665 + 432$.

6.2 Logarithmische Tabellen

$\log_a x \bmod (p-1)$

p	3	5	7	11	13	17	19	23	29	31	37	41
a	2	2	3	2	2	3	2	5	2	3	2	7
$x = 1$	0	0	0	0	0	0	0	0	0	0	0	0
2	1	1	2	1	1	14	1	2	1	24	1	14
3	-	3	1	8	4	1	13	16	5	1	26	25
4	-	2	4	2	2	12	2	4	2	18	2	28
5	-	-	5	4	9	5	16	1	22	20	23	18
6	-	-	3	9	5	15	14	18	6	25	27	39
7	-	-	-	7	11	11	6	19	12	28	32	1
8	-	-	-	3	3	10	3	6	3	12	3	2
9	-	-	-	6	8	2	8	10	10	2	16	10
10	-	-	-	5	10	3	17	3	23	14	24	32
11	-	-	-	-	7	7	12	9	25	23	30	37
12	-	-	-	-	6	13	15	20	7	19	28	13
13	-	-	-	-	-	4	5	14	18	11	11	9
14	-	-	-	-	-	9	7	21	13	22	33	15
15	-	-	-	-	-	6	11	17	27	21	13	3
16	-	-	-	-	-	8	4	8	4	6	4	16
17	-	-	-	-	-	-	10	7	21	7	7	7
18	-	-	-	-	-	-	9	12	11	26	17	24
19	-	-	-	-	-	-	-	15	9	4	35	31
20	-	-	-	-	-	-	-	5	24	8	25	6
21	-	-	-	-	-	-	-	13	17	29	22	26
22	-	-	-	-	-	-	-	11	26	17	31	11
23	-	-	-	-	-	-	-	-	20	27	15	4
24	-	-	-	-	-	-	-	-	8	13	29	27
25	-	-	-	-	-	-	-	-	16	10	10	36

$\log_a x \bmod (p-1)$

p	43	47	53	59	61	67	71	73	79	83	89	97
a	3	5	2	2	2	7	7	5	3	2	3	5
$x = 1$	0	0	0	0	0	0	0	0	0	0	0	0
2	27	18	1	1	1	23	6	8	4	1	16	34
3	1	20	17	50	6	39	26	6	1	72	1	70
4	12	36	2	2	2	46	12	16	8	2	32	68
5	25	1	47	6	22	15	28	1	62	27	70	1
6	28	88	18	51	7	62	32	14	5	73	17	8
7	35	32	14	18	49	1	1	33	53	8	81	31
8	39	8	3	3	3	3	18	24	12	3	48	6
9	2	40	34	42	12	12	52	12	2	62	2	44
10	10	19	48	7	23	38	34	9	66	28	86	35
11	30	7	6	25	15	37	31	55	68	24	84	86
12	13	10	19	52	8	19	38	22	9	74	33	42
13	32	11	24	45	40	41	39	59	34	77	23	25
14	20	4	15	19	50	24	7	41	57	9	9	65
15	26	21	12	56	28	54	54	7	63	17	71	71
16	24	26	4	4	4	26	24	32	16	4	64	40
17	38	16	10	40	47	20	49	21	21	56	6	89
18	29	12	35	43	13	35	58	20	6	63	18	78
19	19	45	37	38	26	32	16	62	32	47	35	81
20	37	37	49	8	24	61	40	17	70	29	14	69
21	36	6	31	10	55	40	27	39	54	80	82	5
22	15	25	7	26	16	60	37	63	72	25	12	24
23	16	5	39	15	57	50	15	46	26	60	57	77
24	40	28	20	53	9	42	44	30	13	75	49	76
25	8	2	42	12	44	30	56	2	46	54	52	2

$\log_a x \bmod (p-1)$

p	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97
a	2	3	2	7	3	5	2	2	2	7	7	5	3	2	3	5
$x =$																
26	19	5	12	23	17	29	25	46	41	64	45	67	38	78	39	59
27	15	3	6	35	3	14	51	34	18	51	8	18	3	52	3	18
28	14	16	34	29	5	22	16	20	51	47	13	49	61	10	25	3
29	-	9	21	33	41	35	46	28	35	22	68	35	11	12	59	13
30	-	15	14	17	11	39	13	57	29	11	60	15	67	18	87	9
31	-	-	9	12	34	3	33	49	59	25	11	11	56	38	31	46
32	-	-	5	30	9	44	5	5	5	49	30	40	20	5	80	74
33	-	-	20	22	31	27	23	17	21	10	57	61	69	14	85	60
34	-	-	8	21	23	34	11	41	48	43	55	29	25	57	22	27
35	-	-	19	19	18	33	9	24	11	16	29	34	37	35	63	32
36	-	-	18	38	14	30	36	44	14	58	64	28	10	64	34	16
37	-	-	-	8	7	42	30	55	39	44	20	64	19	20	11	91
38	-	-	-	5	4	17	38	39	27	55	22	70	36	48	51	19
39	-	-	-	34	33	31	41	37	46	14	65	65	35	67	24	95
40	-	-	-	20	22	9	50	9	25	18	46	25	74	30	30	7
41	-	-	-	-	6	15	45	14	54	31	25	4	75	40	21	85
42	-	-	-	-	21	24	32	11	56	63	33	47	58	81	10	39
43	-	-	-	-	-	13	22	33	43	9	48	51	49	71	29	4
44	-	-	-	-	-	43	8	27	17	17	43	71	76	26	28	58
45	-	-	-	-	-	41	29	48	34	27	10	13	64	7	72	45
46	-	-	-	-	-	23	40	16	58	7	21	54	30	61	73	15
47	-	-	-	-	-	-	44	23	20	28	9	31	59	23	54	84
48	-	-	-	-	-	-	21	54	10	65	50	38	17	76	65	14
49	-	-	-	-	-	-	28	36	38	2	2	66	28	16	74	62
50	-	-	-	-	-	-	43	13	45	53	62	10	50	55	68	36

$\log_a x \bmod (p-1)$

p	53	59	61	67	71	73	79	83	89	97
a	2	2	2	7	7	5	3	2	3	5
$x =$										
51	27	32	53	59	5	27	22	46	7	63
52	26	47	42	21	51	3	42	79	55	93
53	-	22	33	57	23	53	77	59	78	10
54	-	35	19	8	14	26	7	53	19	52
55	-	31	37	52	59	56	52	51	66	87
56	-	21	52	4	19	57	65	11	41	37
57	-	30	32	5	42	68	33	37	36	55
58	-	29	36	45	4	43	15	13	75	47
59	-	-	31	36	3	5	31	34	43	67
60	-	-	30	34	66	23	71	19	15	43
61	-	-	-	29	69	58	45	66	69	64
62	-	-	-	48	17	19	60	39	47	80
63	-	-	-	13	53	45	55	70	83	75
64	-	-	-	6	36	48	24	6	8	12
65	-	-	-	56	67	60	18	22	5	26
66	-	-	-	33	63	69	73	15	13	94
67	-	-	-	-	47	50	48	45	56	57
68	-	-	-	-	61	37	29	58	38	61
69	-	-	-	-	41	52	27	50	58	51
70	-	-	-	-	35	42	41	36	79	66
71	-	-	-	-	-	44	51	33	62	11
72	-	-	-	-	-	36	14	65	50	50
73	-	-	-	-	-	-	44	69	20	28
74	-	-	-	-	-	-	23	21	27	29
75	-	-	-	-	-	-	47	44	53	72

p	79	83	89	97
a	3	2	3	5
$x =$				
76	40	49	67	53
77	43	32	77	21
78	39	68	40	33
79	-	43	42	30
80	-	31	46	41
81	-	42	4	88
82	-	41	37	23
83	-	-	61	17
84	-	-	26	73
85	-	-	76	90
86	-	-	45	38
87	-	-	60	83
88	-	-	44	92
89	-	-	-	54
90	-	-	-	79
91	-	-	-	56
92	-	-	-	49
93	-	-	-	20
94	-	-	-	22
95	-	-	-	82
96	-	-	-	48

x mod p

p	3	5	7	11	13	17	19	23	29	31	37	41
a	2	2	3	2	2	3	2	5	2	3	2	7
$\log_a x =$												
0	1	1	1	1	1	1	1	1	1	1	1	1
1	2	2	3	2	2	3	2	5	2	3	2	7
2	-	4	2	4	4	9	4	2	4	9	4	8
3	-	3	6	8	8	10	8	10	8	27	8	15
4	-	-	4	5	3	13	16	4	16	19	16	23
5	-	-	5	10	6	5	13	20	3	26	32	38
6	-	-	-	9	12	15	7	8	6	16	27	20
7	-	-	-	7	11	11	14	17	12	17	17	17
8	-	-	-	3	9	16	9	16	24	20	34	37
9	-	-	-	6	5	14	18	11	19	29	31	13
10	-	-	-	-	10	8	17	9	9	25	25	9
11	-	-	-	-	7	7	15	22	18	13	13	22
12	-	-	-	-	-	4	11	18	7	8	26	31
13	-	-	-	-	-	12	3	21	14	24	15	12
14	-	-	-	-	-	2	6	13	28	10	30	2
15	-	-	-	-	-	6	12	19	27	30	23	14
16	-	-	-	-	-	-	5	3	25	28	9	16
17	-	-	-	-	-	-	10	15	21	22	18	30
18	-	-	-	-	-	-	-	6	13	4	36	5
19	-	-	-	-	-	-	-	7	26	12	35	35
20	-	-	-	-	-	-	-	12	23	5	33	40
21	-	-	-	-	-	-	-	14	17	15	29	34
22	-	-	-	-	-	-	-	-	5	14	21	33
23	-	-	-	-	-	-	-	-	10	11	5	26
24	-	-	-	-	-	-	-	-	20	2	10	18
25	-	-	-	-	-	-	-	-	11	6	20	3

$x \bmod p$

p	43	47	53	59	61	67	71	73	79	83	89	97
a	3	5	2	2	2	7	7	5	3	2	3	5
$\log_a x =$												
0	1	1	1	1	1	1	1	1	1	1	1	1
1	3	5	2	2	2	7	7	5	3	2	3	5
2	9	25	4	4	4	49	49	25	9	4	9	25
3	27	31	8	8	8	8	59	52	27	8	27	28
4	38	14	16	16	16	56	58	41	2	16	81	43
5	28	23	32	32	32	57	51	59	6	32	65	21
6	41	21	11	5	3	64	2	3	18	64	17	8
7	37	11	22	10	6	46	14	15	54	45	51	40
8	25	8	44	20	12	54	27	2	4	7	64	6
9	32	40	35	40	24	43	47	10	12	14	14	30
10	10	12	17	21	48	33	45	50	36	28	42	53
11	30	13	34	42	35	30	31	31	29	56	37	71
12	4	18	15	25	9	9	4	9	8	29	22	64
13	12	43	30	50	18	63	28	45	24	58	66	29
14	36	27	7	41	36	39	54	6	72	33	20	48
15	22	41	14	23	11	5	23	30	58	66	60	46
16	23	17	28	46	22	35	19	4	16	49	2	36
17	26	38	3	33	44	44	62	20	48	15	6	83
18	35	2	6	7	27	40	8	27	65	30	18	27
19	19	10	12	14	54	12	56	62	37	60	54	38
20	14	3	24	28	47	17	37	18	32	37	73	93
21	42	15	48	56	33	52	46	17	17	74	41	77
22	40	28	43	53	5	29	38	12	51	65	34	94
23	34	46	33	47	10	2	53	60	74	47	13	82
24	16	42	13	35	20	14	16	8	64	11	39	22
25	5	22	26	11	40	31	41	40	34	22	28	13

x mod p

p	29	31	37	41	43	47	53	59	61	67	71	73	79	83	89	97
a	2	3	2	7	3	5	2	2	2	7	7	5	3	2	3	5
$\log_a x =$																
26	22	18	3	21	15	16	52	22	19	16	3	54	23	44	84	65
27	15	23	6	24	2	33	51	44	38	45	21	51	69	5	74	34
28	-	7	12	4	6	24	49	29	15	47	5	36	49	10	44	73
29	-	21	24	28	18	26	45	58	30	61	35	34	68	20	43	74
30	-	-	11	32	11	36	37	57	60	25	32	24	46	40	40	79
31	-	-	22	19	33	39	21	55	59	41	11	47	59	80	31	7
32	-	-	7	10	13	7	42	51	57	19	6	16	19	77	4	35
33	-	-	14	29	39	35	31	43	53	66	42	7	57	71	12	78
34	-	-	28	39	31	34	9	27	45	60	10	35	13	59	36	2
35	-	-	19	27	7	29	18	54	29	18	70	29	39	35	19	10
36	-	-	-	25	21	4	36	49	58	59	64	72	38	70	57	50
37	-	-	-	11	20	20	19	39	55	11	22	68	35	57	82	56
38	-	-	-	36	17	6	38	19	49	10	12	48	26	31	68	86
39	-	-	-	6	8	30	23	38	37	3	13	21	78	62	26	42
40	-	-	-	-	24	9	46	17	13	21	20	32	76	41	78	16
41	-	-	-	-	29	45	39	34	26	13	69	14	70	82	56	80
42	-	-	-	-	-	37	25	9	52	24	57	70	52	81	79	12
43	-	-	-	-	-	44	50	18	43	34	44	58	77	79	59	60
44	-	-	-	-	-	32	47	36	25	37	24	71	73	75	88	9
45	-	-	-	-	-	19	41	13	50	58	26	63	61	67	86	45
46	-	-	-	-	-	-	29	26	39	4	40	23	25	51	80	31
47	-	-	-	-	-	-	5	52	17	28	67	42	75	19	62	58
48	-	-	-	-	-	-	10	45	34	62	43	64	67	38	8	96
49	-	-	-	-	-	-	20	31	7	32	17	28	43	76	24	92
50	-	-	-	-	-	-	40	3	14	23	48	67	50	69	72	72

x mod p

p	53	59	61	67	71	73	79	83	89	97
a	2	2	2	7	7	5	3	2	3	5
$\log_a x =$										
51	27	6	28	27	52	43	71	55	38	69
52	-	12	56	55	9	69	55	27	25	54
53	-	24	51	50	63	53	7	54	75	76
54	-	48	41	15	15	46	21	25	47	89
55	-	37	21	38	34	11	63	50	52	57
56	-	15	42	65	25	55	31	17	67	91
57	-	30	23	53	33	56	14	34	23	67
58	-	-	46	36	18	61	42	68	69	44
59	-	-	31	51	55	13	47	53	29	26
60	-	-	-	22	30	65	62	23	87	33
61	-	-	-	20	68	33	28	46	83	68
62	-	-	-	6	50	19	5	9	71	49
63	-	-	-	42	66	22	15	18	35	51
64	-	-	-	26	36	37	45	36	16	61
65	-	-	-	48	39	39	56	72	48	14
66	-	-	-	-	60	49	10	61	55	70
67	-	-	-	-	65	26	30	39	76	59
68	-	-	-	-	29	57	11	78	50	4
69	-	-	-	-	61	66	33	73	61	20
70	-	-	-	-	-	38	20	63	5	3
71	-	-	-	-	-	44	60	43	15	15
72	-	-	-	-	-	-	22	3	45	75
73	-	-	-	-	-	-	66	6	46	84
74	-	-	-	-	-	-	40	12	49	32
75	-	-	-	-	-	-	41	24	58	63

p	79	83	89	97
a	3	2	3	5
$\log_a x =$				
76	44	48	85	24
77	53	13	77	23
78	-	26	53	18
79	-	52	70	90
80	-	21	32	62
81	-	42	7	19
82	-	-	21	95
83	-	-	63	87
84	-	-	11	47
85	-	-	33	41
86	-	-	10	11
87	-	-	30	55
88	-	-	-	81
89	-	-	-	17
90	-	-	-	85
91	-	-	-	37
92	-	-	-	88
93	-	-	-	52
94	-	-	-	66
95	-	-	-	39

Literaturhinweise

1. Dynkin / Uspenski, Mathematische Unterhaltungen 11; Aufgaben aus der Zahlentheorie, Deutscher Verlag der Wissenschaften, Berlin 1956, MSB Nr. 20

2. Gelfond, Die Auflösung von Gleichungen in ganzen Zahlen, Deutscher Verlag der Wissenschaften, Berlin 1960, MSB Nr. 22

3. Holzer, Zahlentheorie Teil I, B. G. Teubner Verlagsgesellschaft, Leipzig 1958

4. Jung, Einführung in die Zahlentheorie, Fachbuchverlag, Leipzig 1951

5. Lemann-Schoeneberg, Vom periodischen Dezimalbruch zur Zahlentheorie, B. G. Teubner Verlagsgesellschaft, Leipzig 1952

6. Neiß, Einführung in die Zahlentheorie, S. Hirzel Verlag, Leipzig 1952

7. Sominski, Die Methode der vollständigen Induktion, Deutscher Verlag der Wissenschaften, Berlin 1964, MSB Nr. 8

8. Winogradow, Elemente der Zahlentheorie, Deutscher Verlag der Wissenschaften, Berlin 1955

9. Worobjow, Die Fibonaccischen Zahlen, Deutscher Verlag der Wissenschaften, Berlin 1954, MSB Nr. 19